# Deployment and Installation Center

Websense® TRITON™ Enterprise

**v7.6.x**

**Deployment and Installation Center**

**Websense TRITON Enterprise version 7.6**

**April 2012**

# Summary Contents

# Contents

# 1 Deployment and Installation Center

## Applies to

- Web Filter v7.6.x
- Web Security v7.6.x
- Web Security Gateway v7.6.x
- Web Security Gateway Anywhere v7.6.x
- Data Security v7.6.x
- Email Security Gateway v7.6.x
- V10000 v7.6.x
- V10000 G2 v7.6.x
- V5000 G2 v7.6.x

## In this topic



## Overview

The Deployment and Installation Center is a section of the Websense Technical Library providing deployment and installation instructions for Websense products. The information is organized by basic deployment scenarios. For each scenario, there are deployment, installation, and initial configuration instructions.

## Deployment scenarios

- *Web Filter or Web Security (software-based)*, page 69
- *Web Security Gateway (software-based)*, page 161
- *Web Security All*, page 75
- *Web Security Gateway Anywhere (software-based)*, page 351
- *Data Security*, page 435
- *Web Security Gateway (appliance-based)*, page 405
- *Web Security Gateway Anywhere (appliance-based)*, page 419
- *Email Security Gateway (V10000 G2)*, page 585
- *Email Security Gateway (V5000 G2)*, page 575
- *Web and Email Security Gateway (V10000 G2)*, page 607
- *Web Security Gateway Anywhere and Email Security Gateway (V10000 G2)*, page 621
- *TRITON Enterprise (V10000 G2)*, page 637

If none of these match your current or planned deployment, refer to *Custom Deployment*, page 657.

## Upgrade scenarios

- *Upgrading Web Security or Web Filter to 7.6.0*, page 829
- *Upgrading Websense Content Gateway to 7.6.0*, page 853
- *Upgrading to Data Security 7.6.0*, page 879
- *Upgrading to Websense Web Security Gateway Anywhere to v7.6.0*, page 871
- *Upgrading V-Series Appliance to 7.6*, page 907
- *Upgrading Websense software to the latest v7.6.x*, page 821

## How to use the Deployment and Installation Center

The Deployment and Installation Center is a collection of online topics (roughly equivalent to pages or sections in a document) covering deployment and installation of Websense products.

In most cases, the Websense Technical Library's search function will be the primary entry point into this information, directing you to the topic containing the particular information you searched for. This is most useful if you already have deployed Websense products and wish to find a specific item of information regarding deployment or installation.

If you are planning a deployment, it is recommended you start at the main topic for your deployment scenario (see the links under *Deployment scenarios* above). On the main page for a scenario, you can access deployment guidelines, installation instructions, and initial configuration instructions for that scenario.

In most cases, one of the deployment scenarios listed above should match your deployment. If a scenario is close but does not exactly match your deployment, it is recommended that you read the information for that scenario. In some cases, there will be information about "customizing" the scenario in certain ways that might match your particular deployment (for example, installing a particular component somewhere other than the standard location).

## Previous version deployment and installation documentation

Deployment and installation information for prior version products can be found in other parts of the Websense Technical Library. Note that prior to version 7.6, deployment and installation information was organized in a different way. Instead of scenarios, the information is organized around particular products and components.

# 2 System Requirements

## Applies to

- Web Filter v7.6.x
- Web Security v7.6.x
- Web Security Gateway v7.6.x
- Web Security Gateway Anywhere v7.6.x
- Email Security Gateway v7.6.x
- Data Security v7.6.x

## In this topic



## TRITON management server

The machine on which *TRITON Unified Security Center* and certain optional components are installed is referred to as the *TRITON management server*.

## Operating system

The following operating systems are supported for a TRITON management server.

| | Windows Server 2003 R2 32-bit* | Windows Server 2008 32-bit | Windows Server 2008 R2 64-bit** | V-Series Appliance |
|---|---|---|---|---|
| TRITON – Data Security | ✓ | | ✓ | |
| TRITON – Web Security | ✓ | ✓ | ✓ | ✓ |
| TRITON – Email Security | | | ✓ | |

*Windows 2003 supported for a single module (TRITON – Web Security or TRITON – Data Security) but not for a combination of applications. In such deployments, TRITON infrastructure is installed plus the relevant module. In this case, the TRITON Unified Security Center will run with one module enabled, and the other two disabled.

** Windows Server 2008 R2 64-bit supports both Standard and Enterprise versions.

# Hardware requirements

The following are minimum hardware recommendations for a TRITON management server. The requirements are different depending on whether SQL Server 2008 R2 Express is installed on the management server (local database) or a remote installation of SQL Server is used (remote database).

## With local database

| TRITON Unified Security Center Module(s) | Minimum Requirements |
|---|---|
| TRITON - Web Security | 4 CPU cores (2.5 GHz), 4 GB RAM, 100 GB Disk Space |
| TRITON - Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space |
| TRITON - Web Security and<br>- Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space |
| TRITON - Email Security and<br>- Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space |
| TRITON - Web Security,<br>- Data Security, and<br>- Email Security | 8 CPU cores (2.5 GHz), 16 GB RAM, 240 GB Disk Space |

Notes:

- Data Security allows installation of the Forensics repository on a remote location. If you use this mode and store your forensics on a separate hard drive you can deduct 90GB from the above stated disk space requirements.
- It is strongly recommended you have more disk space than the minimum specified above to allow for scaling with use.
- If you choose to install the Websense product on a drive other than the main Windows drive (typically C drive), then you must have at least 2GB free on the main Windows drive to accommodate for files to be extracted to this drive.

### With remote database

| TRITON Unified Security Center Module(s) | Minimum Requirements |
|---|---|
| TRITON - Web Security | 4 CPU cores (2.5 GHz), 4 GB RAM, 7 GB Disk Space |
| TRITON - Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 140 GB Disk Space |
| TRITON - Web Security and<br>- Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space |
| TRITON - Email Security and<br>- Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space |
| TRITON - Web Security,<br>- Data Security, and<br>- Email Security | 8 CPU cores (2.5 GHz), 16 GB RAM, 146 GB Disk Space |

Note:

- It is strongly recommended you have more disk space than the minimum specified above to allow for scaling with use.
- If you choose to install the Websense product on a drive other than the main Windows drive (typically C drive), then you must have at least 2GB free on the main Windows drive to accommodate for files to be extracted to this drive.

## Browser

The following Web browsers are supported by TRITON Unified Security Center.

| Browser | Versions |
|---|---|
| Internet Explorer | 7, 8*, and 9 |
| Firefox | 3.5, 3.6, and 4 |

* For Internet Explorer 8 only, do not use compatibility mode.

## Virtualization systems

All TRITON management components are supported on these virtualization systems.

| Supported Virtualization Systems |
|---|
| Hyper-V over Windows Server 2008 R2 (x64, 64-bit) |
| VMware – Any version that supports virtualization of Windows 2008 and above. |

## TRITON local database system

"Local" database system refers to one installed on the TRITON management server itself. The local database system provided by Websense is SQL Server 2008 R2 Express (32-bit version). For smaller enterprises, if you want to run SQL Server on the TRITON management server, it is a best practice to use SQL Server 2008 R2 Express. For larger enterprises, however, it is a best practice to run the TRITON Unified Security Center and SQL Server on separate physical machines. Note: the 32-bit version may be installed on any of the operating systems supported for the TRITON management server (see *Operating system*, page 42).

## TRITON remote database system

"Remote" database system refers to one installed on a server separate from the TRITON management server. The following are supported.

| Supported Databases | Data Security | Web Security | Email Security |
|---|---|---|---|
| SQL Server 2005* | | ✓ | |
| SQL Server 2008** | ✓ | ✓ | ✓ |
| SQL Server 2008 R2 Express | ✓ | ✓ | ✓ |
| SQL Server 2008 R2*** | ✓ | ✓ | ✓ |

*All editions except Web, Express, and Compact; all service packs; 32- and 64-bit, but not IA64.

**All editions except Web, Express, and Compact; all service packs, 32- and 64-bit, but not IA64.

***All editions except Web and Compact; all service packs, 32- and 64-bit, but not IA64.

Note: Clustering supported for all supported versions of SQL Server noted above.

## Directory Services for Administrators

TRITON Unified Security Center can authenticate administrator accounts against the following:

- Microsoft Active Directory
- Novell eDirectory
- Lotus Notes
- Oracle Directory Server
- Generic LDAP directories

# Web Security and Web Security Gateway

## Software deployments

Web Security components supports the following operating systems with a few exceptions:

- Windows Server 2003 R2 32-bit
- Windows Server 2008 32-bit
- Windows Server 2008 R2
- Red Hat Enterprise Linux 4
- Red Hat Enterprise Linux 5

Websense Content Gateway supports

- Red Hat Enterprise Linux 5

  See *System requirements for Websense Content Gateway*, page 366 for more information.

Exceptions:

- The following components are Windows only (do not support Linux)
  - Linking Service
  - Log Server
  - DC Agent
  - Real-Time Monitor

## Appliance deployments

The following components do not run on appliances; they must be installed off-appliance.

- Real-Time Monitor
- Web Security Log Server
- Linking Service
- Sync Service
- Remote Filtering Server
- All transparent identification agents:
  - DC Agent
  - eDirectory Agent
  - Logon Agent
  - RADIUS Agent

## Client OS

| Application | Windows 7 | Windows XP | Windows Vista | Windows Server 2003 | Windows Server 2008 |
|---|---|---|---|---|---|
| Logon App | ✓ | ✓ | ✓ | ✓ | ✓ |
| Remote Filtering | ✓ | ✓ | ✓ | ✓ | ✓ |
| Web Endpoint | ✓ | ✓ | ✓ | ✓ | ✓ |

Note: Both 32- and 64-bit versions of all these operating systems are supported by these applications

## Integrations

Websense Web Security may be integrated with the following products.

| Product | Version(s) |
|---|---|
| Microsoft ISA Server | 2004 Standard and Enterprise,<br>2006 Standard and Enterprise |
| Microsoft Forefront TMG | 2008 or later |
| Cisco PIX Firewall | v5.3 or later |
| Cisco ASA | PIX v7.0 or later |
| Cisco Content Engine | ACNS v5.5 or 5.6 |
| Cisco Router | IOS v12.3 or later |
| Check Point Firewall-1 | FP1 or later, NG AI, NGX |
| Check Point UTM-1 Edge | n/a |
| Check Point VPN-1 Edge | n/a |
| Squid Web Proxy Cache | STABLE v2.5 and v2.6 |
| Citrix MetaFrame Presentation Server | 3.0 |
| Citrix Presentation Server | 4.0, 4.5 |
| Citrix XenApp | 5.0 |
| | 6.0 |

## Directory Services

| Directory Service | Version(s) |
|---|---|
| Microsoft Active Directory (native or mixed mode) | 2008, 2003 |
| Microsoft Windows NT Directory | v2, v1 |
| Novell eDirectory | v8.5.1 or later |
| Oracle Directory Services Enterprise Edition | 11g |
| Sun Java | 7, 6.2 |

## RADIUS

Most standard RADIUS servers are supported. The following have been tested:

- Microsoft IAS
- Merit AAA
- Livingston (Lucent) 2.x
- Cistron RADIUS server
- NMAS authentication

## Web endpoint

Web Endpoint can be deployed on the following operating systems:

- Windows XP with Service Pack 2 or higher (32-bit and 64-bit)
- Windows Vista with Service Pack 1 or higher (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)

The following Web browsers fully support the endpoint on both 32-bit and 64-bit operating systems:

- Internet Explorer 7, 8, and 9
- Firefox 3.x, 4.x, 5, 6, and 7
- Full support means that the browser supports all installation methods, and both Web scanning and filtering and proxy manipulation. All Web browsers support GPO deployment, and Web scanning and filtering with the endpoint.

# Email Security Gateway

Email Security Gateway is exclusively appliance-based (V10000 G2 or V5000 G2) except for the following components:

- TRITON – Email Security (see *TRITON management server*, page 41)
- Email Security Log Server

## Email Security Log Server

This is the only Email Security component that can be located off-management-server or appliance.

| Email Security Gateway Component | Supported Operating System |
|---|---|
| Email Security Log Server | Windows 2008 (x86 and x64) |
| | Windows 2003 (x86) |

# Data Security

## Operating system

| Data Security Component | Supported Operating Systems | 32-bit | 64-bit |
|---|---|---|---|
| Management server and supplemental servers | Windows Server 2003 Standard or Enterprise, R2 SP2 | ✓ | |
| | Windows Server 2008 Standard or Enterprise | | ✓ |
| | Windows Server 2008 Standard or Enterprise, R2 | | ✓ |
| Crawler agent | Windows Server 2003 Standard or Enterprise, R2 SP2 | ✓ | |
| | Windows Server 2008 Standard or Enterprise | | ✓ |
| | Windows Server 2008 Standard or Enterprise, R2 | | ✓ |
| SMTP Agent | Windows Server 2003 Standard or Enterprise, R2 | ✓ | ✓ |
| | Windows Server 2003 Standard or Enterprise, R2 SP2 | ✓ | |
| ISA Agent (ISA Server 2004/2006) | Windows Server 2003 Standard or Enterprise | ✓ | |
| | Windows Server 2003 Standard or Enterprise, R2 | ✓ | ✓ |
| | Windows Server 2003 Standard or Enterprise, R2 SP2 | ✓ | |
| TMG Agent (Forefront TMG) 2008 | Windows Server 2008 R2 | | ✓ |
| Printer agent | Windows Server 2003 Standard or Enterprise | ✓ | |
| | Windows Server 2003 Standard or Enterprise, R2 | ✓ | |
| | Windows Server 2003 Standard or Enterprise, R2 SP2 | ✓ | |
| Protector*** | CentOS 5.5** | | |
| Mobile Agent | CentOS 5.5** | | |

| Data Security Component | Supported Operating Systems | 32-bit | 64-bit |
|---|---|---|---|
| Data Endpoint client | Windows 7 | ✓ | ✓ |
| | Windows Vista | ✓ | ✓ |
| | Windows XP | ✓ | ✓ |
| | Windows Server 2008 | ✓ | ✓ |
| | Windows Server 2003 | ✓ | ✓ |
| | Red Hat Enterprise Linux/CentOS 4.8 | ✓ | ✓ |
| | Red Hat Enterprise Linux/CentOS 5.1 with stock kernel 2.6.18-53.el5 | ✓ | ✓ |
| | Red Hat Enterprise Linux/CentOS 5.4 and on, including stock kernel 2.6.18-164.el5 and above) | ✓ | ✓ |

Note: by default, Windows Server 2003 or XP support only 3 agents per client. If your endpoint clients will be running multiple agents—for example the endpoint agent, an antivirus agent, and an antispam agent—they should be updated to Windows XP SP3 or Windows Server 2003 SP2. In addition, you must modify their registry entries.

*Requires .NET 2.0 installed on system.

**This operating system is installed as part of the Protector "soft appliance" installation.

***Protector is supported on virtualization systems in the Mail Transport Agent (MTA) mode and/or as an ICAP server with remote analysis (no local analysis). Other modes of deployment are not certified.

## Data Security Server hardware requirements

| Data Security Server | Minimum Requirements | Recommended |
|---|---|---|
| CPU | 2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent | 2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent |
| Memory | 2 GB | 4 GB |
| Hard drives | Four 72 GB | Four 146 GB |
| Disk space | 72 GB | 292 GB |
| Free space | 70 GB | 70 GB |
| Hardware RAID | 1 | 1 + 0 |
| NICs | 1 | 2 |

## Data Security Server software requirements

The following requirements apply to all Data Security servers:

- For optimized performance of Websense Data Security, verify that the operating system's file cluster is set to 4096B. For more information, see the Websense knowledge article: "File System Performance Optimization."
- Windows installation requirements:
  - Set the partition to 1 NTFS Partition. For more information, see the Websense knowledge-base article: "File System Performance Optimization."
  - Regional Settings: should be set according to the primary location. If necessary, add supplemental language support and adjust the default language for non-Unicode programs.
  - Configure the network connection to have a static IP address.
  - The Data Security Management Server computer name must not include an underscore sign. Internet Explorer does not support such URLs.
  - Short Directory Names and Short File Names must be enabled. (See http://support.microsoft.com/kb/121007.)
  - Create a local administrator to be used as a service account. If more than one Data Security Server will be in your deployment, use a domain account (or the same username and password on each server if using local accounts).
  - It's necessary to set the system time accurately on the server onto which you install the TRITON management server.

# Protector hardware requirements

| Protector | Minimum Requirements | Recommended |
|---|---|---|
| CPU | 2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent | 2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent |
| Memory | 2 GB | 4 GB |
| Hard drives | 2 - 72 GB | 4 - 146 GB |
| Disk space | 70 GB | 292 GB |
| Hardware RAID | none | 1 + 0 |
| NICs | 2 (monitoring), 3 (inline) | 2 (monitoring), 3 (inline) |

## Recommended (optional) additional NICs for inline mode:

The following Silicom network cards are supported by the Data Security appliance. NICs SKUs are:

- PEG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI-Express Bypass Server Adapter
- PEG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI-Express Bypass Server Adapter
- PXG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter
- PXG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter
- PEG2Fi - Intel-based Dual-Port Fiber (SX) Gigabit Ethernet PCI-Express Server Adapter
- PXG2Fi - Intel-based Dual-Port Fiber (SX) Gigabit Ethernet PCI-X Server Adapter

**Note**

Websense does *not* support bypass products with -SD drivers. If you are ordering a NIC based on Intel chips 82546 or 82571, be sure to order them in non-SD mode.

# Mobile Agent hardware requirements

| Mobile Agent | Minimum Requirements | Recommended |
|---|---|---|
| CPU | 4 core processors (for example, Single quad or two dual core processors), 2.0 GHz Intel Xeon or AMD equivalents | 4 core processors (for example, Single quad or two dual core processors), 2.0 GHz Intel Xeon or AMD equivalents |
| Memory | 8 GB | 8 GB |

| Mobile Agent | Minimum Requirements | Recommended |
|---|---|---|
| Hard drives | 2 - 72 GB | 4 - 146 GB |
| Disk space | 70 GB | 292 GB |
| Hardware RAID | none | 1 + 0 |
| NICs | 2 | 2 |

# Data Endpoint hardware requirements

## Windows

- Pentium 4 (1.8 GHz or above)
- At least 512 MB RAM on Windows XP or 1GB RAM on Windows Vista, Windows 7, Windows Server 2003, or Windows Server 2008
- At least 200 MB free hard disk space

## Linux

- At least 1 GB RAM
- 1 GB free hard disk space (not including contained files and temporary buffers; see the TRITON - Data Security Help for information about contained files and allocating enough disk storage for them)

# 3 Preparing for Installation

## Applies to

- V-Series Appliance 7.6.x
- Web Filter 7.6.x
- Web Security 7.6.x
- Web Security Gateway 7.6.x
- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6v
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## In this topic

# Overview

This section contains information about procedures to perform or things to consider before installing Websense components. The*All* section applies to all installations, the remaining sections apply to particular products.

# All

Do not install any Websense components on a Domain Controller (DC) machine. Before installing any Websense module or product, see the following sections.

## Disk space required on Windows drive

In addition to the space required by the Websense installer itself, further disk space is required on the main Windows drive (i.e., the drive on which Windows is installed;

typically C) to accommodate for temporary files to be extracted to this drive as part of the installation process. For information on minimum disk space requirements, see *Hardware requirements*, page 43.

## Windows updates

On Windows systems, make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.

## Websense installer

The Websense installer is the main installer for Websense products. Use it to install TRITON Unified Security Center; Web Security, Data Security, and Email Security components; and SQL Server 2008 R2 Express. The Websense installer is also used to upgrade most prior-version components.

Download the Websense installer (**WebsenseTRITON76Setup.exe**) from mywebsense.com.

## Starting the Websense installer

The Websense installer is named WebsenseTRITON76Setup.exe. Double-click it to start.

If you have previously run the Websense installer on a machine, you may be able to start it from the Windows **Start** menu without having to extract files again. See *Keeping installer files*, page 58. If you chose to keep installer files, start the installer by selecting **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.

## Web Security installer for Linux

Use the Linux version of the Web Security installer to install Web Security components on Linux. Download the WebsenseWeb76Setup_Lnx.tar.gz package from mywebsense.com.

## Synchronizing clocks

If you are distributing Websense components across different machines in your network, synchronize the clocks on all machines where a Websense component is installed. It is a good practice to point the machines to the same Network Time Protocol server.

**Note**

If you are installing components that will work with a Websense V-Series appliance, you must synchronize the machine's system time to the appliance's system time.

## Antivirus

Disable any antivirus on the machine prior to installing Websense components. Be sure to re-enable antivirus after installation. Certain Websense files should be excluded from antivirus scans to avoid performance issues; see *Excluding Websense Files from Antivirus Scans*, page 939.

## Microsoft hotfix for large installers (Windows Server 2003)

Microsoft released a hotfix for Windows Server 2003 to address an issue with large installers. When launching the Websense installer on unpatched systems, you may receive one of the following messages:

- Installation Failed: This installation is forbidden by system policy. Contact your system administrator.
- The system administrator has set policies to prevent this installation.
- Error 1718. File FileName was rejected by digital signature policy.

If this occurs, install the hotfix and then launch the Websense installer again. See (http://support.microsoft.com/kb/925336) for more information and to download the hotfix.

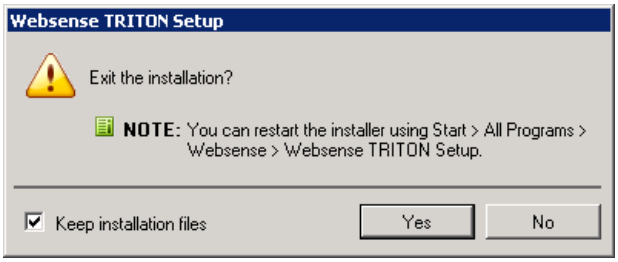
## .NET Framework 2.0

.NET Framework version 2.0 or higher is required to run the Websense installer. .NET 2.0, if not already installed, is available from Microsoft (www.microsoft.com). Note that .NET 3.5 SP1 is required to install SQL Server Express; see*.NET Framework 3.5 SP1*, page 59.

> **Note**
> Both .NET Framework 2.0 and 3.5 SP1 are required if you are installing SQL Server Express.

## Keeping installer files

The Websense installer extracts temporary installation files when it starts up. If you cancel the installer, the following dialog box appears.



Selecting the **Keep installation files** option allows you to restart the Websense installer (from the Windows Start menu) without having to extract the files again. Note that the files occupy approximately 2 GB of disk space.

### No underscores in FQDN

For best practices, do not install Websense components on a machine whose fully-qualified domain name (FQDN) contains an underscore.

The use of an underscore character in an FQDN is not a supported Internet Engineering Task Force (IETF) standard, an official Internet standard, that Websense complies with.

> **Note**
> Further details of this limitation can be found in the IETF specifications RFC-952 and RFC-1123.

## TRITON Unified Security Center

In addition to the general preparation actions (see *All*, page 56), see the following if you will be installing TRITON Unified Security Center.

### Do not install on a Domain Controller

Do not install the TRITON Unified Security Center on a Domain Controller machine.

### Local SQL Server

If you want to run SQL Server on the same machine as the TRITON Unified Security Center, it is a best practice to only use SQL Server 2008 R2 Express installed by the Websense installer. For a remote (i.e., not on the same machine) SQL Server, you can use any of the supported versions (see *System Requirements*, page 41)

If you choose to install SQL Server yourself on the same machine as the TRITON Unified Security Center, be sure to **not** install SQL Server Reporting Services, which can interfere with the operation of Data Security management components.

## SQL Server 2008 R2 Express

### .NET Framework 3.5 SP1

.NET Framework version 3.5 SP1 is required to install SQL Server 2008 R2 Express. Although the Websense installer will automatically install this when you choose to

install SQL Server 2008 R2 Express, it is a best practice to install it prior to running the Websense installer.

> **Note**
> Both .NET 2.0 and 3.5 SP1 are required if you are installing SQL Server Express.

### Windows Installer 4.5

Windows Installer 4.5 is required to install SQL Server 2008 R2 Express. Although the Websense installer will automatically install this when you choose to install SQL Server 2008 R2 Express, it is a best practice to install it prior to running the Websense installer.

### Windows PowerShell 1.0

Windows PowerShell 1.0 is required to install SQL Server 2008 R2 Express. On Windows Server 2008 R2, PowerShell is installed by default. PowerShell is available from Microsoft (www.microsoft.com). Note that the Websense installer will automatically install this if you choose to install SQL Server 2008 R2 Express.

### Log in as domain user

If you will use SQL Server 2008 R2 Express to store and maintain Web Security data, you must log in to the machine as a domain user when installing it (i.e., log in to the machine as a domain user prior to running the Websense installer). Service Broker, which is installed as part of SQL Server 2008 R2 Express, must be able to authenticate itself against a domain. Logging in as a domain user when running the installer makes sure Service Broker is installed to run as the domain user.

## Web security

In addition to the general preparation actions (see *All*, page 56), see the following if you will be installing Web Filter, Web Security, Web Security Gateway, or Web Security Gateway Anywhere components.

### Filtering Service Internet access

To download the Websense Master Database and enable filtering, each machine running Websense Filtering Service must be able to access the download servers at:

- download.websense.com
- ddsdom.websense.com
- ddsint.websense.com

- portal.websense.com
- my.websense.com

Make sure that these addresses are permitted by all firewalls, proxy servers, routers, or host files that control the URLs that Filtering Service can access.

## Domain Administrator privileges

Websense components are typically distributed across multiple machines. Additionally, some components access network directory services or database servers. To install Websense components, it is a best practice to log in to the machine as a user with domain administration privileges. Otherwise, components may not be able to properly access remote components or services.

**Important**

If you plan to install SQL Server 2008 R2 Express and will use it to store and maintain Web Security data, you must log in as a domain user when installing it (i.e., log in to the machine as a domain user prior to running the Websense installer).

## Firewall

Disable any firewall on the machine prior to installing Websense components. Be sure to disable it before starting the Websense installer and then re-enable it after installation. Open ports as required by the Websense components you have installed.

**Note**

The Websense installer adds two inbound rules to the public profile of Windows Firewall. Ports 9443 and 19448 are opened for Websense EIP Infra - TRITON Central Access. These ports must be open to allow browsers to connect to the TRITON Unified Security Center. Also, additional rules may be added to Windows Firewall when installing Websense Data Security components.

See *Default ports*, page 927 for more information about ports used by Websense components.

## Computer Browser Service (Windows Server 2008)

To install Websense software on a Windows Server 2008 machine, the Computer Browser Service must be running (note: on most machines you will find it disabled by default).

# Network Agent

If you are installing Network Agent, ensure that the Network Agent machine can monitor all client Internet requests, and then responses to those requests.

If you install Network Agent on a machine that cannot monitor client requests, basic HTTP filtering (stand-alone installation only) and features such as protocol management and Bandwidth Optimizer cannot work properly.

**Important**

*Do not* install Network Agent on a machine running a firewall. Network Agent uses packet capturing that may conflict with the firewall software. Do not install any Websense components on a Domain Controller (DC).

## Network interface card

The network interface card (NIC) that you designate for use by Network Agent during installation must support *promiscuous* mode. Promiscuous mode allows a NIC to listen to IP addresses other than its own. If the NIC supports promiscuous mode, it is set to that mode by the Websense installer during installation. Contact your network administrator or the manufacturer of your NIC to see if the card supports promiscuous mode.

On Linux, do **not** choose a NIC without an IP address (stealth mode) for Network Agent communications.

**Note**

If you install Network Agent on a machine with multiple NICs, after installation you can configure Network Agent to use more than one NIC. See the *Network Configuration* topic in the TRITON - Web Security Help for more information.

After installation, you can run the Network Traffic Detector to test whether the selected NIC can see the appropriate Internet traffic. See the *Network Configuration* topic in the TRITON - Web Security Help for instructions.

## Network Agent using multiple NICs on Linux

If Network Agent is installed on a Linux machine, using one network interface card (NIC) for blocking and another NIC for monitoring, make sure that either:

- The blocking NIC and monitoring NIC have IP addresses in different network segments (subnets).
- You delete the routing table entry for the monitoring NIC.

If both the blocking and monitoring NIC on a Linux machine are assigned to the same subnet, the Linux operating system may attempt to send the block via the monitoring NIC. If this happens, the requested page or protocol is not blocked, and the user is able to access the site.

# Installing on Linux

Most Web security components can be installed on Linux. If you are installing on Linux complete the instructions below.

**Note**

Some Web security components cannot be installed on Linux, see *Installing Web Security Components on Linux* for more information.

## SELinux

Before installing, if SELinux is enabled, set it to *permissive* or disable it and restart the machine.

## Linux firewall

If Websense software is being installed on a Linux machine on which a firewall is active, shut down the firewall before running the installation.

1. Open a command prompt.
2. Enter **service iptables status** to determine if the firewall is running.
3. If the firewall is running, enter **service iptables stop**.
4. After installation, restart the firewall. In the firewall, be sure to open the ports used by Websense components installed on this machine. See *Default ports*, page 927.

**Important**

*Do not* install Websense Network Agent on a machine running a firewall. Network Agent uses packet capturing that may conflict with the firewall software. See *Network Agent*. Do not install any Websense components on a Domain Controller (DC).

## Hostname

Before installing to a Linux machine, make sure the **hosts** file (by default, in /etc) contains a hostname entry for the machine, in addition to the loopback address. (Note: you can check whether a hostname has been specified in the **hosts** file by using the `hostname -f` command.)

To configure hostname:

1. Set the hostname:

```
hostname <host>
```

where <*host*> is the name you are assigning this machine.

2. Update the HOSTNAME entry in the **/etc/sysconfig/network** file:

   ```
   HOSTNAME=<host>
   ```

   where <*host*> is the same as in Step 1.

3. In the **/etc/hosts** file, specify the IP address to associate with the hostname. This should be static, and not served by DHCP. Do not delete the second line in the file (the one that begins with 127.0.0.1).

   ```
   <IP address>   <FQDN>    <host>
   127.0.0.1       localhost.localdomain   localhost
   ```

   where <*FQDN*> is the fully-qualified domain name of this machine (i.e., <*host*>.<*subdomain(s)*>.<*top-level domain*>)—for example, myhost.example.com—and <*host*> is the same as in Step 1.

> **Important**
> The hostname entry you create in the**hosts** file must be the first entry in the file.

## TCP/IP only

Websense software supports only TCP/IP-based networks. If your network uses both TCP/IP- and non-IP-based network protocols, only users in the TCP/IP portion of the network are filtered.

# Data Security

See below for information about preparing to install Data Security components.

## Preparing a machine for SMTP agent

The following procedure describes how to prepare a Windows 2003 Server for the Data Security SMTP agent.

1. Install Microsoft IIS with SMTP. (In Windows control panel, select**Add/Remove programs** > **Windows Components**.
   a. Rename the default SMTP server to “Inbound”.
   b. Under Messages, deselect all message “Limits”. (These should be enforced by the mail server).
   c. Select **Delivery** > **Outbound Connections**, then set the port to 10025.
   d. Select **Delivery** > **Advanced**, then set the Smart host to [127.0.0.1].

Recommended: For increased security, you can change the relay settings for the Inbound mail server to only allow relay mail from your Mail Server's IP. The relay settings are under **Access > Relay > Only the list below**.

2. Set up a new SMTP Virtual Server in IIS with the below settings:

```
Name:  Outbound
IP:    127.0.0.1
Port:  10025
Home Directory: C:\inetpub\outbound
```

Recommended: For increased security, you can change the relay settings for the Outbound mail server to only relay mail from itself (127.0.0.1 as well as any IPs assigned to the server). If you plan on using this as the release or notification gateway, make sure you also allow relaying from the Data Security Management Server. The relay settings are under **Access > Relay > Only the list below**.

Optional: If your next-hop MTA requires Transport Layer Security (TLS), you can enable and configure the options under **Delivery > Outbound Security**.

## Do not install Data Security Server on a DC

Do not install Data Security Server on a Domain Controller (DC) machine.

## Domain considerations

The servers running the Data Security software can be set as part of a domain or as a separate workgroup. If you have multiple servers or want to perform run commands on file servers in response to discovery, we recommend you make the server(s) part of a domain.

However, strict GPOs may interfere and affect system performance, and even cause the system to halt. Hence, when putting Data Security servers into a domain, it is advised to make them part of organizational units that don't enforce strict GPOs.

Also, certain real-time antivirus scanning can downgrade system efficiency, but that can be relieved by excluding some directories from that scanning (see *Excluding Websense Files from Antivirus Scans*, page 939). Please contact Websense Technical Support for more information on enhancing performance.

## 1 GB disk space required for ISA Agent

ISA Agent requires 1 GB free disk space on the ISA Server machine. The installer will not allow you to install ISA Agent if available space is less.

# 4 Obtaining SQL Server

## Applies to

- Web Filter v7.6.x
- Web Security v7.6.x
- Web Security Gateway v7.6.x
- Web Security Gateway Anywhere v7.6.x
- Email Security Gateway v7.6.x
- Data Security v7.6.x

## SQL Server

Prior to installing Websense components, SQL Server must be installed and running on a machine in your network. See *System Requirements* for supported versions of SQL Server. Note that SQL Server must be obtained separately; it is not included with your Websense subscription. Refer to Microsoft documentation for installation and configuration instructions.

If you do not have SQL Server, you can use the Websense installer to install SQL Server 2008 R2 Express, a free-of-charge, limited performance version of SQL Server 2008 R2. If you choose to use SQL Server 2008 R2 Express, you must use the Websense installer to install it. Do not download and install it from any other source. Also, this is the only *Express* edition of SQL Server you can use with Websense version 7.6 solutions.

SQL Server 2008 R2 Express can be installed either on the TRITON management server or on a separate machine. For smaller enterprises, if you want to run SQL Server on the TRITON management server, it is a best practice to use SQL Server

2008 R2 Express. For larger enterprises, however, it is a best practice to run the TRITON Unified Security Center and SQL Server on separate physical machines.

> **Note**
> It is a best practice to use SQL Server in production environments. SQL Server 2008 R2 Express is most appropriate for non-production or evaluation environments. See Administering Websense Databases for more information.

To install SQL Server 2008 R2 Express on the TRITON management server, choose to do so during the installation of TRITON Infrastructure. See *Creating a TRITON Management Server*, page 645 for more information.

To install SQL Server 2008 Express R2 on any other machine run the Websense installer in custom installation mode and select SQL Server Express. See *Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)*, page 704.

# 5 Web Filter or Web Security (software-based)

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



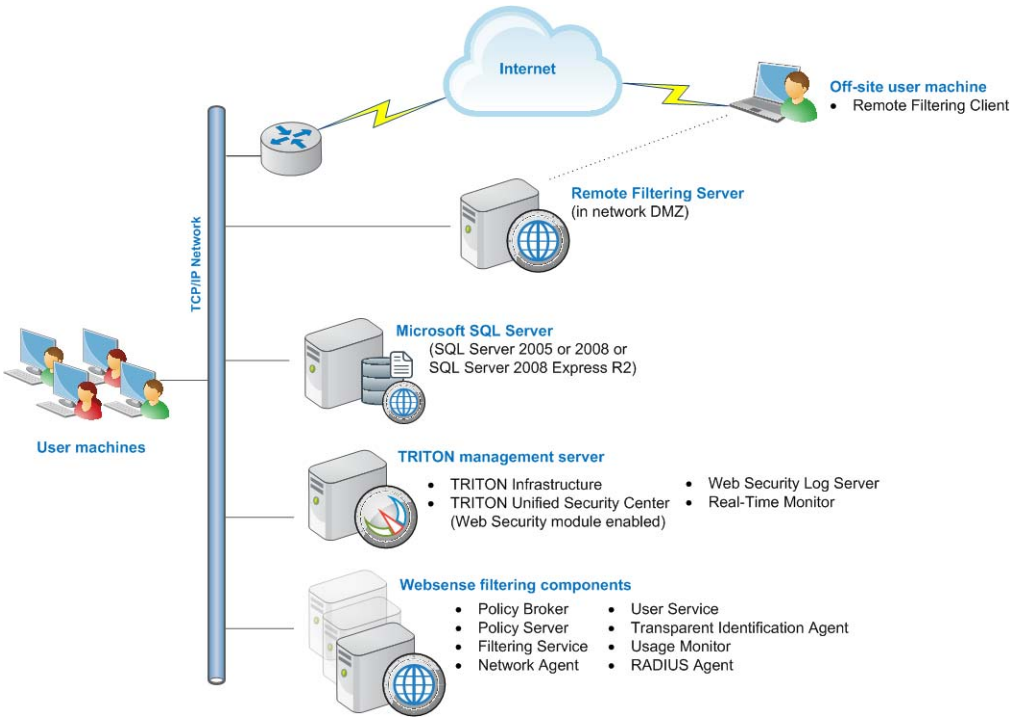
## Overview

This section contains information and instructions for a software-based deployment of Websense Web Filter or Web Security. In this deployment scenario, all Websense components are installed on servers in your network. Websense components are typically distributed across several machines.

Websense Web Filter or Web Security software consists of components that work together to monitor Internet requests, log activity, apply Internet usage filters, and report on activity. Websense software is highly distributable, providing the flexibility to scale a deployment to suit your needs. Components can be installed together on one machine for smaller organizations; or they can be distributed across multiple machines, and multiple sites, to create a high-performing deployment for larger organizations. The appropriate deployment is determined by network size and configuration, Internet request volume, hardware performance, and filtering needs.

The following illustration is a high-level diagram of a basic software-based deployment of Websense Web Filter or Web Security. Note that this illustration is

intended to show the general distribution of components and does not include network details (such as segmenting, internal firewalls, routing, switching, and so forth).




Websense filtering components may be installed on the same machine or distributed across several machines. Additionally, you can install multiple instances (on different machines) of certain components, to scale to your organization's needs.

Web Filter or Web Security can be integrated with a number of third-party proxy, firewall, and router products (such as, Microsoft ISA Server/Forefront TMG, Cisco PIX, and Squid Web Proxy Cache) or Citrix application servers. Note that an integration product is not represented in the illustration above. The integration product communicates with Websense *Filtering Service* to evaluate whether the Internet requests passing through it should be blocked or allowed. See *System Requirements*, page 41 for a list of supported integration products. If you do not use an integration product, Websense *Network Agent* can be used to monitor and filter HTTP/HTTPS/FTP requests.

Microsoft SQL Server is used to store Websense data (including log and reporting data). SQL Server must be obtained separately; it is not included as part of a Websense subscription. When you are installing Websense components, SQL Server must be already installed and running, typically on its own machine, as shown above. SQL Server Express (installed using the Websense installer) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

*TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and any or all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security). Additional components may also be installed on the management server, for

example, *Web Security Log Server* and *Real-Time Monitor*. (Note that these components may be installed on another machine; they are not required to be located on the TRITON management server).

Websense *Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users who are outside the corporate network (such as traveling personnel or telecommuters).

> **Note**
> It is possible to install TRITON management server and Websense filtering components on a single machine, rather than distributed as shown above. See *Web Security All*, page 75.

## Deployment

- *System Requirements*, page 41
- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Hardware recommendations for stand-alone deployments of Web Filter or Web Security*, page 98
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Integrating Web Security with Content Gateway*, page 126
- *Integrating Web Security with Microsoft ISA Server or Forefront TMG*, page 128
- *Integrating Web Security with Cisco*, page 132
- *Integrating Web Security with Check Point*, page 136
- *Integrating Web Security with Squid Web Proxy Cache*, page 139
- *Integrating Web Security with Citrix*, page 143
- *Other integrations for Web Security*, page 145
- *Web Security Distributed Enterprise Deployments*, page 147

## Installation

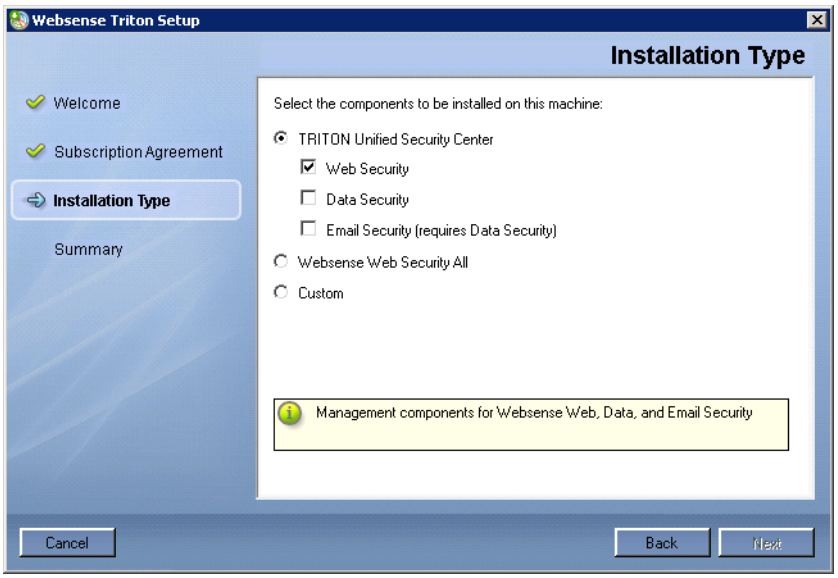
Complete the following main steps (the links go to detailed procedures or information for each step).

1. *Preparing for Installation*, page 55
2. *Obtaining SQL Server*, page 67
3. *Installing Web Security components*, page 668

   **Important**: Be sure to install *Policy Broker* and *Policy Server* before creating a TRITON management server (in the next step).

4. *Creating a TRITON Management Server*, page 645

   **Important**: When following the instructions under *Creating a TRITON Management Server*, page 645, choose to install only the Web Security module of the TRITON Unified Security Center. When you reach the **Installation Type** screen of the Websense installer, select only **Web Security** (under TRITON Unified Security Center).




You can choose to install the other modules of the TRITON Unified Security Center. However, they will be enabled only if the subscription key you enter includes those features.

# Initial configuration

- *Ports*, page 765
- *Antivirus configuration*, page 765
- *Disable Enhanced Security Configuration in Internet Explorer*, page 765
- *Accessing the TRITON Unified Security Center*, page 765
- *Entering subscription key*, page 766
- *SQL Server 2008 R2 Express*, page 766
- *Getting Started Help*, page 767
- *Windows Server 2008*, page 767
- *Logon script for Logon Agent*, page 768

# 6 Web Security All

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



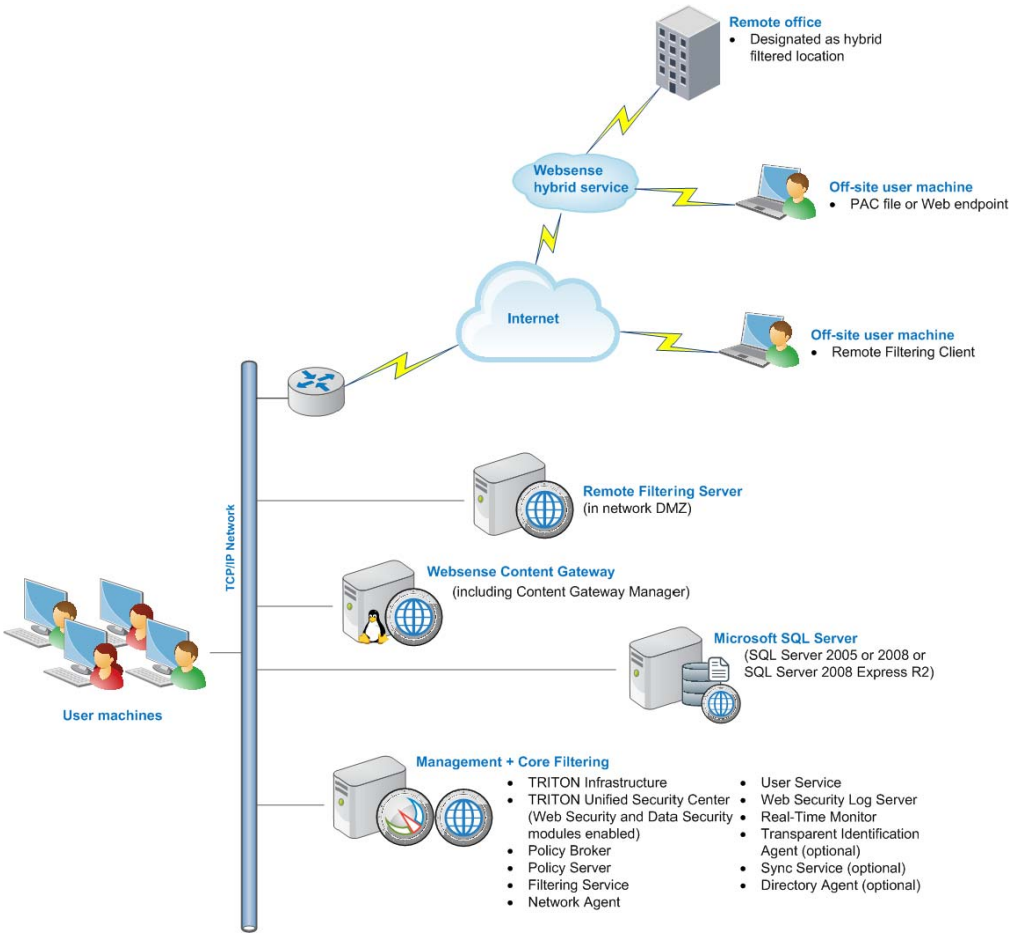
## Overview

A Web Security All deployment places all Web security filtering and management components on one machine. Typically, this type of deployment is for evaluation purposes or small organizations.

A Web Security All deployment can include Web Security, Web Security Gateway, and Web Security Gateway Anywhere features.

Websense Web security software monitors Internet requests, logs activity, applies Internet usage filters, and reports on activity. In addition, Web Security Gateway Anywhere (if included in your subscription) protects you from data loss over the Web, providing security for outbound content as well. You identify sensitive data and define whether you want to audit or block attempts to post it to HTTP, HTTPS, FTP, or FTP-over-HTTP channels.

The following illustration is a high-level diagram of a basic Web Security All deployment. Note that this illustration is intended to show the general distribution of components and does not include network details (such as segmenting, internal firewalls, routing, switching, and so forth).




Microsoft SQL Server is used to store Websense data (including log and reporting data). SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using the Websense installer) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

Websense Content Gateway is a Web proxy that passes HTTP, HTTPS, FTP over HTTP, and FTP traffic to Websense software for inspection and policy enforcement. Content Gateway Manager—the Web-browser-based management UI for Content Gateway—runs on the Content Gateway machine, but is typically accessed from within TRITON Unified Security Center. Content Gateway is necessary if your subscription includes Web Security Gateway or Web Security Gateway Anywhere.

With Web Security Gateway Anywhere, small remote offices can be filtered through the Websense hybrid service. This is accomplished by designating a remote office as a hybrid filtered location. See *Initial Configuration* for more information.

Off-site users (e.g., telecommuters or traveling personnel) can be filtered using the Websense hybrid service or Websense Remote Filtering. To use the hybrid service, a PAC file or the Websense Web endpoint is installed on the user's machine. This directs Web browsing to be filtered through the hybrid service according to policies in place.

Websense Remote Filtering is accomplished using a Remote Filtering Server and Remote Filtering Client. Websense*Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users that are outside the corporate network.

A combination of hybrid service and Remote Filtering can be used for off-site users—i.e., some filtered through the hybrid service, others filtered by Remote Filtering.

## Deployment



## Installation

Complete the following main steps (the links go to detailed procedures or information for each step).

1. *Preparing for Installation*

2. *Obtaining SQL Server*
3. *Installing Web Security components*
4. *Websense Content Gateway* (optional, only if you have Web Security Gateway or Web Security Gateway Anywhere)
5. *Adding the TRITON - Data Security module* (optional, only if you have Web Security Gateway Anywhere)

## Initial configuration

- *Ports*, page 765
- *Antivirus configuration*, page 765
- *Disable Enhanced Security Configuration in Internet Explorer*, page 765
- *Accessing the TRITON Unified Security Center*, page 765
- *Entering subscription key*, page 766
- *SQL Server 2008 R2 Express*, page 766
- *Getting Started Help*, page 767
- *Windows Server 2008*, page 767
- *Logon script for Logon Agent*, page 768
- *Messenger Service for Network Agent block messages*, page 769
- *Administrator privileges for User Service, DC Agent, or Logon Agent*, page 769
- *Configuring Transparent Identification*, page 769
- *Network Agent and multiple NICs*, page 769
- *Remote Filtering*, page 769
- *Identifying Filtering Service by IP address*, page 769

If you subscription includes Web Security Gateway

- *Starting Content Gateway Manager*, page 779
- *Entering a subscription key for Content Gateway*, page 780
- *Enabling SSL Manager in Content Gateway*, page 781
- *Enabling WCCP for Content Gateway*, page 781

If your subscription includes Web Security Gateway Anywhere:

- *Registering Websense Content Gateway with Data Security*, page 771
- *Configuring the Content Gateway policy engine*, page 773
- *Verifying Web and data security linking*, page 774
- *Configure filtering for remote offices and off-site users*, page 774

# Installing Web Security All components

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Installing Web Security All components

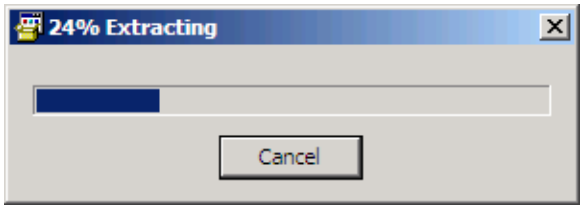
Follow these instructions to perform a Web Security All installation which installs all Web Security management and core filtering components on one machine.

1. Download or copy the Websense installer to this machine.

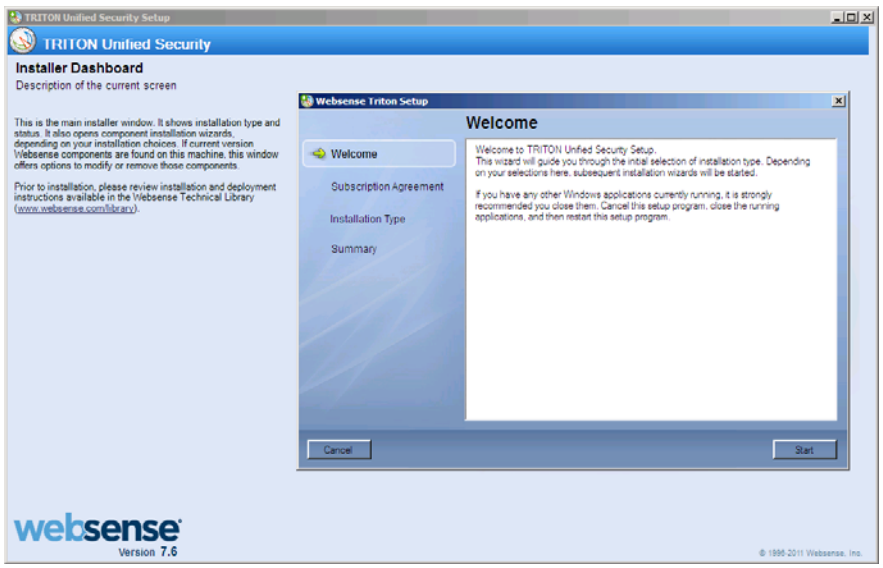
   See *Websense installer*, page 57.

2. Double-click the downloaded installer to launch the Websense installer.

   A progress dialog box appears, as files are extracted:




3. On the **Welcome** screen, click **Start**.




   Note that the Installer Dashboard remains on-screen throughout this process.

4. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
5. On the **Installation Type** screen, select **Websense Web Security All**.
6. On the **Summary** screen, click **Next** to continue the installation.
7. TRITON Infrastructure Setup launches. Follow the instructions in *Installing TRITON Infrastructure*.
8. When you click **Finish** in TRITON Infrastructure Setup.

   You are returned to the Install Dashboard and the Web Security installer starts.
9. On the Active Directory screen, specify whether your network uses Active directory.

   See *Active Directory Screen* for instructions.
10. If you are using Active Directory, the **Computer Browser** screen appears.

    See *Computer Browser Screen* for instructions.
11. On the **Integration Option** screen, select whether your Web Security deployment will be integrated with a third-party product.

    See *Integration Option Screen* for instructions.

    **Important**

    If your subscription includes Web Security Gateway or Web Security Gateway Anywhere, select **Websense Content Gateway** as the integration product. Also, install *Websense Content Gateway*.

12. If you selected **Integrated with another application or device** on the **Integration Option** screen:
    a. On the **Select Integration** screen, select the product you want to integrate with.

       See *Select Integration Screen* for instructions
    b. If the **Filtering Plug-in** screen appears, see *Filtering Plug-In Screen* for instructions.
13. On the **Network Card Selection** screen, select the network interface card (NIC) to be used by Network Agent.

    See *Network Card Selection Screen* for instructions.
14. If the **Multiple Network Cards** screen appears, select the NIC(s) to be used by Network Agent for monitoring.

    See *Multiple Network Cards Screen* for instructions.
15. On the **Log Database Location** screen, specify the location in which you want the Websense log database stored.

    See *Log Database Location Screen* for instructions.
16. On the **Optimize Log Database Size** screen, select options for optimizing the size of log database records.

    See *Optimize Log Database Size Screen* for instructions.

17. On the **Filtering Feedback** screen, choose whether to send categorization feedback to Websense, Inc.

    See *Filtering Feedback Screen* for instructions.

18. On the **Web Security Gateway Anywhere Components** screen, select whether you want to install Websense Web Security Gateway Anywhere components on this machine. Then click **Next**.

    - **Install Web Security Gateway Anywhere Components**: Select this option to install these components and then check the box for the components (**Sync Service** and/or **Directory Agent**) you want to install.
    - **Do not install Web Security Gateway Anywhere Components**: Select this option to not install these components.

19. On the **Transparent User Identification** screen, select whether to use Websense transparent identification agents to identify users and then click**Next**. This allows Websense software to apply user- or group-based filtering policies without prompting users for logon information.

    If Websense software is integrated with a third-party product (firewall, proxy server, cache, or network appliance) providing user authentication, a transparent identification agent may not be necessary.

    To transparently identify remote users accessing the network via VPN, use Websense RADIUS Agent. Later in this installation process, you will be given the option to install RADIUS Agent.

    - **Use Logon Agent to identify users logging on to local machines**: This option installs Websense Logon Agent on this machine. Logon Agent identifies users as they log onto Windows domains. Logon Agent is for use with Windows-based client machines on a network that uses Active Directory or Windows NT Directory.

      To use Logon Agent, you must modify the Group Policy on domain controllers so it launches a logon application (LogonApp.exe) as part of the logon script. Client machines must use NTLM (v1 or v2) when authenticating users (NTLMv1 only, in the case of Windows Server 2008; see note below).

      For instructions on configuring domain controllers and client machines to use Logon Agent, see *Creating and running the script for Logon Agent*, page 782.

      **Note**

      Do not use Logon Agent in a network that already includes eDirectory Agent.

    - **Use eDirectory Agent to identify users logging on via Novell eDirectory Server**: This option installs eDirectory Agent on this machine. Use this agent for a network using Novell eDirectory. eDirectory Agent queries the eDirectory Server at preset intervals to identify users currently logged on.

      **Note**

      Do not use eDirectory Agent in a network that already includes DC Agent or Logon Agent.

- **Do not install a transparent identification agent now**: Select this option if
  - Websense software will be integrated with a third-party product that provides user authentication.
  - You plan to install a transparent identification agent on another machine.
  - You do not want different filtering policies applied to users or groups.
  - You want users to be prompted for logon information when they open a browser to access the Internet.

> **Note**
> When integrated with Cisco products, Websense software cannot use Cisco Secure Access Control Server (ACS) for user authentication for more than 1 user domain. If there are multiple user domains, use a transparent identification agent instead.

20. On the **Directory Service Access** screen, supply a domain administrator account to access directory service information.

    See *Directory Service Access Screen* for instructions.

21. On the **RADIUS Agent** screen, select **Install RADIUS Agent** if you have remote users that are authenticated by a RADIUS server and then click **Next**. This allows Websense software to apply user- or group-based filtering policies on these remote users without prompting for logon information.

22. On the **Pre-Installation Summary** screen, verify the information shown.

    The summary shows the installation path and size, and the components to be installed.

23. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

24. If you chose to install the ISA Server filtering plug-in, the **Stop Microsoft Firewall Service** screen appears. Do the following:

a. Stop the Microsoft Firewall service and then click **Next**.

> **Note**
> Leave the Websense installer running as you stop the Microsoft Firewall service. Then return to the installer and click **Next** to continue installation.

> **Important**
> In order to correctly install the ISA Server filtering plug-in, the Microsoft Firewall Service must be stopped. Installation of the plug-in files and registration of the plug-in in the system registry cannot occur while the Microsoft Firewall Service has certain files locked. Stopping the Microsoft Firewall Service unlocks these files.

To stop the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click Microsoft Firewall, and then select **Stop**. When the service has stopped, return to the Websense installer and continue the installation process. The Firewall Service may also be stopped from the ISA Server Management console or Command Prompt (using the command `net stop fwsrv`). See Microsoft's documentation for more information.

b. When the following message appears, start the Microsoft Firewall service and then click **OK**:

> **Important**
> When the Microsoft Firewall service is stopped, ISA Server goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service needs to be stopped for only a few minutes as the ISA Server filtering plug-in is installed and configured.

*The Websense ISAPI Filter has been configured, you can now start the Microsoft Firewall Service*.

To start the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click Microsoft Firewall, and then select **Start**. The Firewall Service may also be started from the ISA Server Management console or Command Prompt (using the command `net start fwsrv`). See Microsoft's documentation for more information.

25. On the **Installation Complete** screen, click **Done**.
26. You are returned to the Installer Dashboard and it closes.

# Adding the TRITON - Data Security module

## Applies to

- Web Security Gateway Anywhere v7.6

## Adding the TRITON - Data Security module

If your subscription includes Web Security Gateway Anywhere, you should add the TRITON - Data Security module to the TRITON Unified Security Center already installed.

1. Start the Websense installer: go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.
2. In **Modify Installation** dashboard, click the **Install** link for Data Security.

   The Data Security component installer is started.

3. Proceed as if you were performing a custom installation. Select Data Security Server and Crawler Agent for installation (selected by default).

   See *Installing Data Security Components*, page 692 for instructions.

# 7 General Deployment Recommendations for Web Security

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Topics



## Network considerations

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Network considerations

To ensure effective filtering, Web Filter and Web Security must be installed so that:

- Filtering Service can receive HTTP requests from Websense Content Gateway; an integrated firewall, proxy server, caching application; or Websense Network Agent.

  In a multi-segmented network, Filtering Service must be installed in a location where it can both receive and manage Internet requests from the integration product and communicate with Network Agent.

- Network Agent:
  - Must be deployed where it can see all internal Internet traffic for the machines that it is assigned to monitor.
  - Can be installed on a dedicated machine to increase overall throughput.
  - Must have bidirectional visibility into Internet traffic to filter non-HTTP requests (such as instant messaging, chat, streaming media, and other Internet applications and protocols).
  - Multiple instances of Network Agent may be required in larger or distributed networks. Each Network Agent monitors a specific IP address range or network segment.

    Using multiple Network Agents ensures that all network traffic is monitored, and prevents server overload. The required number of Network Agents depends on network size and Internet request volume.

  For more information, see *Deploying Network Agent*, page 105.

- As a network grows and the number of Internet requests increases, components can be deployed to additional, non-dedicated machines to improve processing performance on the dedicated machines.
  - You can deploy multiple Filtering Service instances, connected to one Policy Server. This is useful for remote or isolated sub-networks.
  - Multiple Policy Servers may be necessary, because it is a best practice to have a maximum of 10 Filtering Service instances per Policy Server (see *Filtering Services per Policy Server*, page 88).

**Note**

Network Agent can be deployed with the filtering components or on a separate machine. Network Agent should **not** be deployed on the same machine as response-critical components. For more information, see *Deploying Network Agent*, page 105.

**Important**

**Do not** install Websense components on a domain controller or on a firewall machine.

# Component limits and ratios

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

Some components are limited to a single instance in the entire network, or to a single instance of components that depend on them. When deploying Websense software, consider the following restrictions.

## Component Limits

> **Note**
> Even when the number of dependent components is not limited to one, there are best practice component-to-dependent-component ratios. See *Component ratios*, page 88.

Per entire deployment:

- One Policy Broker
- One Sync Service (Websense Web Security Gateway Anywhere deployments)

Per Policy Broker:

- One TRITON Unified Security Center

Per Policy Server:

- One Web Security Log Server
- One User Service
- One Usage Monitor

- One Directory Agent (Websense Web Security Gateway Anywhere deployments; see *Multiple Directory Agent instances*, page 90 for additional information)

Per Filtering Service:

- One primary Remote Filtering Server

# Component ratios

Best practice component deployment ratios may vary, based on network configuration and Internet traffic volume.

Larger systems (more than 2500 users) may require a more distributed deployment for load balancing and support of multiple languages.

- Multiple Network Agent instances may be required, for example, to detect outbound traffic on individual network segments.
- It may be appropriate to install multiple Filtering Service instances for load balancing. Some load balancing configurations allow the same user to be filtered by different Filtering Service instances, depending on the current load.

For limits on transparent identification agents, see *Deploying transparent identification agents*, page 91.

For more information about the interaction of Websense components, see the TRITON - Web Security Help.

## Network Agents per Filtering Service

As a best practice, no more than 4 Network Agent instances should be deployed per Filtering Service. One Filtering Service instance may be able to handle more than 4 Network Agents, depending on the number of Internet requests, but if Filtering Service or Network Agent capacities are exceeded, filtering and logging inconsistencies may occur.

Network Agent can typically monitor 50 Mbps of traffic per second, or about 800 requests per second. The number of users that Network Agent can monitor depends on the volume of Internet requests from each user, the configuration of the network, and the location of Network Agent in relation to the computers it is assigned to monitor. Network Agent functions best when it is close to those computers.

Contact your Websense software provider for technical assistance with specific Network Agent sizing guidelines.

## Filtering Services per Policy Server

As a best practice, no more than 10 Filtering Service instances should be deployed per Policy Server. A Policy Server instance may be able to handle more, depending on the load. However, if the number of Filtering Service instances exceeds the Policy Server's capacity, responses to Internet requests may be slowed.

Multiple Filtering Service instances are useful to manage remote or isolated sub-networks.

The appropriate number of Filtering Service instances for a Policy Server depends on:

- The number of users per Filtering Service
- The configuration of the Policy Server and Filtering Service machines
- The volume of Internet requests
- The quality of the network connection between the components

  If a ping command sent from one machine to another receives a response in fewer than **30 milliseconds (ms)**, the connection is considered high-quality. See *Testing the connection*, page 89 for more information.

If Filtering Service and Policy Server become disconnected, all Internet requests are either blocked or permitted, depending on which option you have chosen in the TRITON - Web Security console. For more information, see the *Getting Started* topic in the TRITON - Web Security Help.

Filtering Service machines running behind firewalls or running remotely (at a great topological distance, communicating through a series of routers) may need their own Policy Server instance. In a multiple Policy Server environment, a single Websense Policy Database holds the policy settings for all Policy Server instances. See the TRITON - Web Security Help for more information.

### Testing the connection

Run a **ping** test to check the response time and connection between the Policy Server and Filtering Service machines. A response time of fewer than 30 milliseconds is recommended.

1. Open a command prompt (Windows) or terminal session (Linux) on the Policy Server machine.
2. Enter the following command:

   ```
   ping <IP address or hostname>
   ```

   Here, *<IP address or hostname>* identifies the Filtering Service machine.

### Interpreting your results

When you run the **ping** command on a Windows machines, the results resemble the following:

```
C:\>ping 11.22.33.254
Pinging 11.22.33.254 with 32 bytes of data:
Reply from 11.22.33.254: bytes=32 time=14ms TTL=63
Reply from 11.22.33.254: bytes=32 time=15ms TTL=63
Reply from 11.22.33.254: bytes=32 time=14ms TTL=63
Reply from 11.22.33.254: bytes=32 time=15ms TTL=63
Ping statistics for 11.22.33.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 15ms, Average = 14ms
```

In a Linux environment, the results look like this:

```
[root@localhost root]# ping 11.22.33.254
PING 11.22.33.254 (11.22.33.254) 56(84) bytes of data.
64 bytes from 11.22.33.254: icmp_seq=2 ttl=127 time=0.417 ms
64 bytes from 11.22.33.254: icmp_seq=3 ttl=127 time=0.465 ms
64 bytes from 11.22.33.254: icmp_seq=4 ttl=127 time=0.447 ms
64 bytes from 11.22.33.254: icmp_seq=1 ttl=127 time=0.854 ms
```

Ensure that **Maximum** round trip time or the value of**time=x.xxx ms** is fewer than 30 ms. If the time is greater than 30 ms, move one of the components to a different network location and run the ping test again. If the result is still greater than 30 ms, locate and eliminate the source of the slow response.

## Multiple Directory Agent instances

Typically, only one Directory Agent instance is required in a deployment. Multiple instances may be deployed if necessary. However, specific configuration of the additional Directory Agent instances is required. See the TRITON - Web Security Help for more information and configuration instructions.

**Important**

In a V-Series Appliance-based deployment of Websense Web Security Gateway Anywhere, be aware that Directory Agent is already installed on the appliance. Additional instances of Directory Agent are not typically necessary. If you need to deploy additional instances, see the TRITON - Web Security Help for important configuration instructions.

# Required external resources

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Overview

Websense software relies on certain external resources and network characteristics to function properly in your network.

## TCP/IP

Websense software provides filtering in TCP/IP-based networks only. If your network uses both TCP/IP and non-TCP protocols, only those users in the TCP/IP portion of your network are filtered.

## DNS server

A DNS server is used to resolve requested URLs to an IP address. Websense software or your integration product requires efficient DNS performance. DNS servers should be fast enough to support Websense filtering without becoming overloaded.

## Directory services

If Websense software is configured to apply user- and group-based policies, User Service queries the directory service for user information. Although these users and group relationships are cached by Websense software, directory service machines must have the resources to respond rapidly if Websense software requests user information. See *System Requirements*, page 41 for supported directory services.

For information on configuring Websense software to communicate with a supported directory service, see the TRITON - Web Security Help. Websense software does not need to run on the same operating system as the directory service.

## Network efficiency

The ability to connect to resources such as the DNS server and directory services is critical to Websense software. Network latency must be minimized if Filtering Service is to perform efficiently. Excessive delays under high load circumstances can impact the performance of Filtering Service and may cause lapses in filtering.

# Deploying transparent identification agents

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

If you are using Websense software as a stand-alone deployment, or if your integration product does not send user information to Websense software, use Websense transparent identification agents to identify users without prompting them for a user name and password.

There are 4 optional transparent identification agents:

- DC Agent
- eDirectory Agent
- Logon Agent
- RADIUS Agent

> **Note**
> DC Agent must have domain administrator privileges to retrieve user information from the domain controller.

If you have deployed Websense software in a single network location, it is a best practice to have a single transparent identification agent instance.

In deployments that cover multiple locations, you can install an agent instance in multiple domains.

For example:

- One **DC Agent** instance can handle multiple trusted domains. Add additional instances based on:
  - The load placed on DC Agent
  - Whether a DC Agent instance can see all the domains on the network, including remote offices

  Load results from the number of user logon requests. With a large number of users (10,000+ users, 30+ domains), having multiple DC Agent instances allows for faster identification of users.

  If multiple Filtering Services are installed, each Filtering Service instance must be able to communicate with all DC Agent instances.
- One **eDirectory Agent** is required for each eDirectory Server.
- One **Logon Agent** is required for each Filtering Service instance.
- One **RADIUS Agent** instance is required for each RADIUS server.

It is a best practice to install and run RADIUS Agent and the RADIUS server on separate machines. (The agent and server cannot have the same IP address, and must use different ports.)

In some environments, a combination of transparent identification agents may be appropriate within the same network, or on the same machine. See *Combining transparent identification agents*, page 93.

See *Installing Web Security components*, page 668 for transparent identification agent installation instructions. See the TRITON - Web Security Help for detailed configuration information. More information is also available in the Transparent Identification of Users technical paper.

## Combining transparent identification agents

Websense software can work with multiple transparent identification agents. If your environment requires multiple agents, it is best to install them on separate machines.

- eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service, or on a separate server on the same network.
- Do not run eDirectory Agent and DC Agent in the same deployment.

The following table lists supported combinations of transparent identification agents.

| Combination | Same machine? | Same network? | Configuration required |
|---|---|---|---|
| Multiple DC Agents | No | Yes | Ensure that all instances of DC Agent can communicate with Filtering Service, and that the individual DC Agents are not monitoring the same domain controllers. |
| Multiple RADIUS Agents | No | Yes | Configure each agent to communicate with Filtering Service.<br>Multiple instances of the RADIUS Agent cannot be installed on the same machine. |
| Multiple eDirectory Agents | No | Yes | Configure each instance to communicate with Filtering Service. |
| Multiple Logon Agents | No | Yes | Configure each instance to communicate with Filtering Service. |
| DC Agent + RADIUS Agent | Yes | Yes | Each agent must use a unique port number to communicate with Filtering Service. By default, DC Agent uses port 30600; RADIUS Agent uses port 30800. |

| Combination | Same machine? | Same network? | Configuration required |
|---|---|---|---|
| DC Agent + eDirectory Agent | No | No | Communication with both a Windows directory service and Novel eDirectory is not supported in the same deployment. However, both agents can be installed, with only one agent active. |
| DC Agent + Logon Agent | Yes | Yes | Configure each agent to use a unique port to communicate with Filtering Service. By default, DC Agent uses port 30600; Logon Agent uses port 30602. |
| RADIUS Agent + Logon Agent | Yes | Yes | Configure all agents to communicate with Filtering Service. |
| eDirectory Agent + Logon Agent | No | No | Communication with both Novell eDirectory and a Windows- or LDAP-based directory service in the same deployment is not supported. However, both agents can be installed, with only one agent active. |
| RADIUS Agent + eDirectory Agent | Yes | Yes | Configure each agent to use a unique port to communicate with Filtering Service. By default, eDirectory Agent uses port 30700; RADIUS Agent uses port 30800.<br>When adding agents to TRITON - Web Security, use an IP address to identify one, and a machine name to identify the other. See the *Transparent Identification of Users* white paper for details. |
| DC Agent + Logon Agent + RADIUS Agent | Yes | Yes | This combination is rarely required.<br>Configure each agent to use a unique port to communicate with Filtering Service. By default, DC Agent uses port 30600; Logon Agent uses port 30602; RADIUS Agent uses port 30800. |

# Maximizing system performance

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

Adjust Websense components to improve filtering and logging response time, system throughput, and CPU performance.

## Network Agent

Network Agent can be installed on the same machine as other Websense components, or on a separate machine.

As the number of users grows, or if Network Agent does not block Internet requests as expected, place Network Agent on a different machine from Filtering Service and Policy Server. You can also add a second Network Agent and divide the network monitoring between the 2 agents.

If Websense software is running in a high-load environment, or with a high capacity Internet connection, you can increase throughput and implement load balancing by installing multiple Network Agent instances. Install each agent on a different machine, and configure each agent to monitor a different portion of the network.

**Important**

Network Agent must have bidirectional visibility into the network segment that it monitors.

If multiple Network Agents are installed, each agent must monitor a different network segment (IP address range).

If a Network Agent machine connects to a switch, the monitor NIC must plug into a port that mirrors, monitors, or spans the traffic of all other ports. *Locating Network Agent in multiple segment network*, page 110, and *Network Agent location*, page 107, discuss locating Network Agent in more detail.

## HTTP reporting

You can use Network Agent or an integration product to track HTTP requests and pass the information to Websense software, which uses the data to filter and log requests.

Network Agent and some integration products also track bandwidth activity (bytes sent and received), and the duration of each permitted Internet request. This data is also passed to Websense software for logging.

When both Network Agent and the integration product provide logging data, the amount of processor time required by Filtering Service increases.

If you are using both Network Agent and an integration product, you can avoid extra processing by configuring Websense software to use Network Agent to log HTTP requests (enhanced logging). When this feature is enabled, Websense software does not log HTTP request data sent by the integration product. Only the log data provided by Network Agent is recorded.

Consult the TRITON - Web Security Help for configuration instructions.

## SQL Server

Microsoft SQL Server (as opposed to SQL Server Express) works best for larger networks, or networks with a high volume of Internet activity, because of its capacity for storing large amounts of data over longer periods of time (several weeks or months). See *System Requirements*, page 41 for which versions of SQL Server are supported.

Under high load, Microsoft SQL Server operations are resource intensive, and can be a performance bottleneck for Websense software reporting. You can tune the database to improve performance, and maximize the hardware on which the database runs:

- If Websense Log Server is installed on the database-engine machine, alleviate resource conflicts between Log Server and Microsoft SQL Server by increasing the CPU speed or the number of CPUs.
- Provide adequate disk space to accommodate the growth of the Log Database. Microsoft SQL Client Tools can be used to check database size.
- Use a disk array controller with multiple drives to increase I/O bandwidth.
- Increase the RAM on the Microsoft SQL Server machine to reduce time-consuming disk I/O operations.

> **Note**
> Consult Microsoft documentation for detailed information about optimizing Microsoft SQL Server performance.

### SQL Server 2008 R2 Express

Microsoft SQL Server 2008 R2 Express (SQL Server Express) is a free, limited-performance database engine best-suited to smaller networks, organizations with a

low volume of Internet activity, or organizations planning to generate reports on only short periods of time (for example, daily or weekly archived reports, rather than historical reports over longer time periods). SQL Server Express cannot be optimized.

If the Log Database is rolling over frequently, consider upgrading to Microsoft SQL Server.

# Log Database disk space recommendations

Log Database requirements vary, based on the size of the network and the volume of Internet activity.

## Logging visits (default setting)

When you log *visits*, one log record is created for each Web page requested by a user, rather than each separate file included in the Web page request. This creates a smaller database and allows faster reporting.

## Logging hits

When you log *hits*, a separate log record is generated for each HTTP request to display any element of a Web page, including graphics and ads. This type of logging results in a larger and more detailed database than the logging visits option.

Due to the large amount of disk space required, and due to the performance impact on reporting, it is a best practice not to keep live data from large networks for a year. When you break up the database into smaller pieces, you can generate reports much more quickly.

## Logging full URLs

Enabling full URL logging creates a larger database than with logging hits, and also provides the most detailed reports. Log records include the domain name and the full path to specific pages requested. Use this option if you want reports of real-time scanning activity.

If the Log Database is growing too quickly, you can turn off full logging to decrease the size of each entry and slow growth.

Configure URL logging options in the TRITON - Web Security console. See the TRITON - Web Security Help for details.

## Consolidation

Consolidation helps to reduce the size of the database by combining Internet requests that share the same value for all of the following elements, within a certain interval of time (1 minute, by default):

- Domain name (for example: www.websense.com)
- Category
- Keyword

- Action (for example: Category Blocked)
- User

For example, the user visits *www.cnn.com* and receives multiple pop-ups during the session. The visit is logged as a record.

- If consolidation is turned off (the default), and the user returns to the site later, a second visit is logged.
- If consolidation is turned on, additional visits to the site within a specified period are logged as a single record, with a hits (i.e., visits) count indicating the number of times the site was visited in that period.

### Protocol logging

If your deployment includes Network Agent, you have the option to log non-HTTP protocol traffic (for example, instant messaging or streaming media traffic) in addition to HTTP and HTTPS traffic.

The more protocols you choose to log, the greater the impact on the size of the Log Database. See the TRITON - Web Security Help for information about filtering and logging non-HTTP protocols.

# Hardware recommendations for stand-alone deployments of Web Filter or Web Security

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Hardware recommendations for stand-alone deployments of Web Filter or Web Security

When Web Security or Web Filter is deployed as a stand-alone product, then Network Agent (rather than a third-party integration product, such as a firewall, proxy, or gateway product or device) monitors network traffic and enables filtering of all protocols, including HTTP, HTTPS, and FTP.

In a stand-alone deployment, Network Agent:

- Detects all TCP/IP Internet requests (HTTP and non-HTTP)
- Communicates with Filtering Service to see if each request should be blocked
- Calculates the number of bytes transferred
- Sends a request to Filtering Service to log Internet activity

For more information, see the TRITON - Web Security Help.

Components may need to be distributed over multiple machines for load balancing and improved performance in larger networks.

The table below provides hardware recommendations for stand-alone deployments of Web Filter and Web Security solutions, based on network size. System needs vary, depending on the volume of Internet traffic. Note the table does not include information for the TRITON management server; see *System Requirements*, page 41.

The following baseline is used to create the recommendations:

- 1 - 500 users = 1 - 100 requests/second
- 500 - 2,500 users = 100 - 500 requests/second
- 2,500 - 10,000 users = 500 - 2,250 requests/second

If your network traffic exceeds these estimates, more powerful systems or greater distribution of components may be required.

**Important**

- Do not install Websense components on a domain controller. Do not install Websense components on a firewall machine. Firewall and Websense software function and performance may be affected.
- Each Network Agent machine must be positioned to see all Internet requests for the machines that it is assigned to monitor.
- eDirectory Agent or RADIUS Agent can be installed on the same machine as Filtering Service, or on a separate machine in the same network, but not on the same machine as Websense Log Server.

| Network Size | Filtering Components | Reporting (Windows) |
|---|---|---|
| 1 - 500 users | **Windows** or **Linux**<br>• Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater<br>• 4 GB RAM<br>• 10 GB free disk space (Free space must equal at least 20% of total disk space.) | **Windows**<br>• Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater<br>• 4 GB RAM<br>• 100 GB free disk space<br>• Microsoft SQL Server 2008 or 2005, or SQL Server 2008 R2 Express required for Log Database |
| 500 - 2,500 users | **Windows** or **Linux**<br>• Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater<br>• 4 GB RAM<br>• 10 GB free disk space (Free space must equal at least 20% of total disk space.) | **Windows**<br>• Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater<br>• 4 GB RAM<br>• 100 GB free disk space<br>• Microsoft SQL Server 2008 or 2005, or SQL Server 2008 R2 Express required for Log Database |
| 2,500 - 10,000 users | **Windows** or **Linux**<br>• Load balancing required<br>• Quad-Core Intel Xeon 5450 or better processor, 3.0 GHz or greater<br>• 4 GB RAM<br>• 10 GB free disk space (Free space must equal at least 20% of total disk space.) | **Windows**<br>• Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater<br>• 4 GB RAM<br>• 200 GB free disk space with a disk array (The Log Database requires a disk array to increase I/O reliability and performance.)<br>• High-speed disk access<br>• Microsoft SQL Server 2008 or 2005 required for Log Database |

**Important**

At least two Network Agent instances, running on separate machines, are required for networks with 2,500-10,000 users. The machines should have:

- Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater
- At least 1 GB of RAM

Multiple Filtering Service machines may also be needed. Machine requirements depend on the number of users being monitored and filtered.

To run both filtering and reporting on the same machine in the two smaller network sizes, increase the RAM to 6 GB (if supported by your operating system), and consider using a faster processor and hard drive to compensate for the increased load.

# Remote Filtering Server and Client

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Remote Filtering Server and Client

For all Web Filter and Web Security solutions, you can monitor computers outside your network using remote filtering components. The **Remote Filtering Client** must be installed on each remote machine.

The remote clients communicate with a **Remote Filtering Server**, which acts as a proxy to Filtering Service. This communication is authenticated and encrypted.

**NOTE**

If you have Websense Web Security Gateway Anywhere, you can also use the hybrid service to monitor users outside your network. This does not require software installation on remote machines. See *Web Security Gateway Anywhere (software-based)*, page 351 or *Web Security Gateway Anywhere (appliance-based)*, page 419 for more information.

When installing remote filtering components:

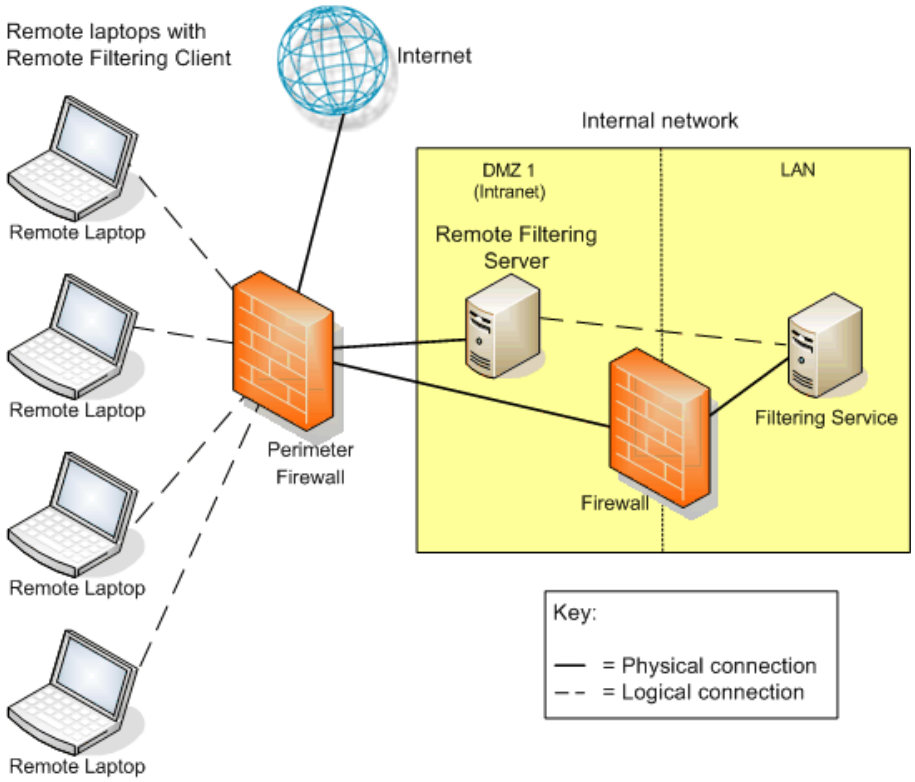
- The Remote Filtering Server should be installed on a dedicated machine that can communicate with the Filtering Service machine.
- Do **not** install any Websense component on a domain controller.
- Remote Filtering Server on the same machine as Filtering Service or Network Agent.
- Each Filtering Service instance can have only one primary Remote Filtering Server.
- As a best practice, the Remote Filtering Server should be installed inside the outermost firewall, in the DMZ outside the firewall protecting the rest of the corporate network. This is strongly recommended.
- See *System Requirements*, page 41, for operating system requirements for Remote Filtering Server.

| Network Size | Hardware Recommendations |
|---|---|
| 1-500 clients | **Windows** or **Linux**<br>• Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater<br>• 2 GB RAM<br>• 20 GB free disk space |
| 500+ clients | **Windows** or **Linux**<br>• Quad-Core Intel Xeon 5450 or better processor, 3.2 GHz or greater<br>• 4 GB RAM<br>• 20 GB free disk space |

Remote Filtering Client system recommendations:

- Pentium 4 or greater
- Free disk space: 25 MB for installation; 15 MB to run the application
- 512 MB RAM

The following illustration provides an example of a Remote Filtering deployment. The illustration does not include all Websense components. For more information, see the Websense Remote Filtering Software technical paper.


Remote laptops with
Remote Filtering Client
Internet
Internal network
DMZ 1
(Intranet)
LAN
Remote Filtering
Server
Remote Laptop
Remote Laptop
Remote Laptop
Remote Laptop
Perimeter
Firewall
Firewall
Filtering Service
Key:
= Physical connection
= Logical connection

# 8 Deploying Network Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Overview

When your Websense software deployment includes Network Agent, the positioning of Network Agent and other Websense filter components depends on the composition of your network.

For the most part, Ethernet networks are built of **segments** (very simple networks are an exception). A segment is a neighborhood for a group of machines, which are connected to the rest of the network via a central connection point (router, bridge, switch, or smart hub). Most of these devices keep local traffic within a segment, while passing the traffic intended for machines on other segments. This architecture reduces network congestion by keeping unnecessary traffic from passing to the whole network.

A very simple network may require only a single Network Agent. A segmented network may require (or benefit from) a separate Network Agent instance for each segment. Network Agent functions best when it is closest to the computers that it is assigned to monitor.

See the following for more information:


- *Network Agent*, page 106
- *Network Agent location*, page 107
- *Locating Network Agent in single segment network*, page 109
- *Locating Network Agent in multiple segment network*, page 110
- *Connecting Network Agent to a hub*, page 114
- *Switched networks with a single Network Agent*, page 114

# Network Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

Network Agent manages Internet protocols (including HTTP, HTTPS, and FTP), by examining network packets and identifying the protocol.

As with third-party integration products (like firewalls, routers, proxies, or network appliances), Network Agent can be configured to monitor HTTP requests and query Filtering Service to determine whether to allow or block a request, and then log the results of the query. Network Agent can also be configured to do the same for non-HTTP requests.

Network Agent must be installed on the **internal** side of the corporate firewall, in a location where it can see all Internet requests for the machines it is assigned to monitor. The agent then monitors HTTP and non-HTTP requests from those machines, and the responses that they receive.

Network Agent monitors and manages only the traffic that passes through the network device (switch or hub) to which it is attached. Multiple Network Agent instances may be needed, depending on the network size, volume of Internet requests, and the network configuration.

The Network Agent machine can connect to the network via a switch or a hub. See *Connecting Network Agent to a hub*, page 114, and *Switched networks with a single Network Agent*, page 114.

Network Agent can be installed on the same machine as some integration products. See *Network Agent on gateway*, page 120.

**Warning**

Do **not** install Network Agent on a machine running a firewall or Remote Filtering Server. On a firewall, Network Agent's packet-capturing may conflict with the firewall software. On a Remote Filtering Server, machine resources may be too heavily taxed.

## Network Agent settings

Configure Network Agent global settings (applying to all agent instances) and local settings (specific to a single agent instance) in the TRITON - Web Security console. These settings tell Network Agent which machines to monitor and which to ignore.

- Global settings:
  - Specify which machines are part of your network.
  - Identify any machines in your network that Network Agent should monitor for **incoming** requests (for example, internal Web servers).
  - Specify bandwidth calculation and protocol logging behavior.
- Local settings:
  - Specify which Filtering Service is associated with each Network Agent.
  - Identify proxies and caches used by the machines that this Network Agent monitors.
  - Determine which network interface card (NIC) the Network Agent instance uses to monitor requests and which NIC it uses to send block pages.

    Configuration settings for the NIC used to monitor requests determine which segment of the network the agent instance monitors.

# Network Agent location

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Network Agent location

Network Agent must be able to see all outgoing and incoming Internet traffic on the network segment that it is assigned to monitor.

- Multiple Network Agents may be needed for larger or high-traffic organizations.
- A Network Agent instance can be placed in each internal network segment. Each instance should monitor its own segment without overlapping any other agent's segment.

The Network Agent machine may be:

- Connected to a **switch**.
  - Configure the device to use a mirror or span port, and connect Network Agent to this port, to allow the agent to see Internet requests from all monitored machines. (On most switches, you can change a port mode to spanning, mirroring, or monitoring mode. The term varies by manufacturer; the function is the same.)

    **Note**
    Not all switches support port spanning or mirroring. Contact the switch vendor to verify that spanning or mirroring is available, and for configuration instructions.

  - It is a best practice to use a switch that supports bidirectional spanning. This allows Network Agent to use a single network interface card (NIC) to both monitor traffic and send block pages.

    If the switch does not support bidirectional spanning, the Network Agent machine must have at least 2 NICs: one for monitoring and one for blocking. See *Network Agent and multiple NICs*, page 121.
- On a dedicated machine, connected to an **unmanaged, unswitched hub** located between an external router and the network.

To ensure that Network Agent is able to monitor the expected traffic, you must position the Network Agent machine appropriately and configure Network Agent settings in the TRITON - Web Security console. See the TRITON - Web Security Help for instructions.

The following sections illustrate possible single- and multiple-Network Agent configurations:


- *Locating Network Agent in single segment network*, page 109
- *Locating Network Agent in multiple segment network*, page 110
- *Connecting Network Agent to a hub*, page 114
- *Switched networks with a single Network Agent*, page 114
- *Switched networks with multiple Network Agents*, page 119

# Locating Network Agent in single segment network

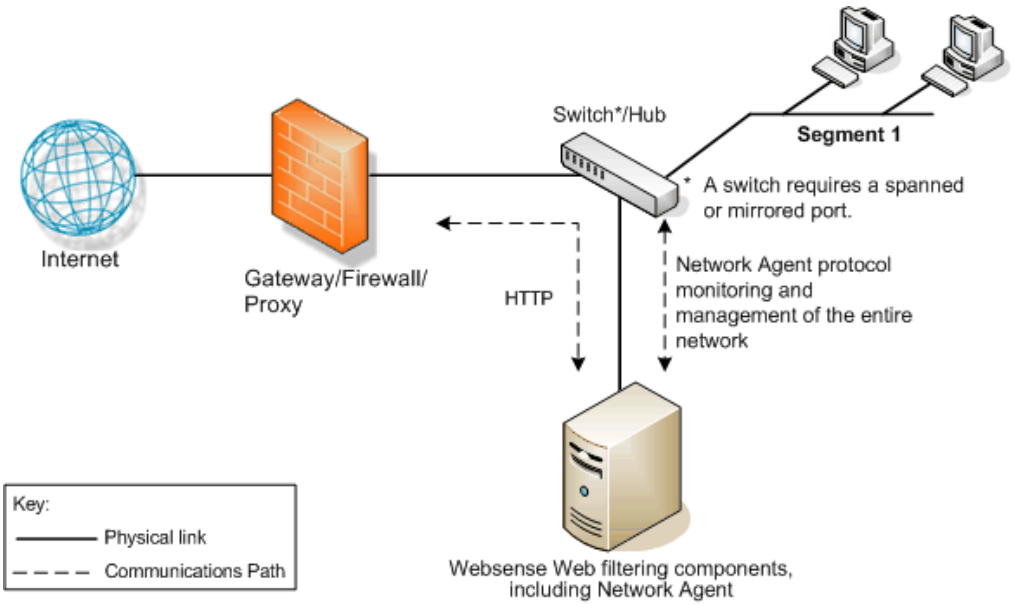
## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Locating Network Agent in single segment network

A single segment network is a series of logically connected nodes (computers, printers, and so on) operating in the same portion of the network. In a single segment network, Filtering Service and Network Agent must be positioned to monitor Internet traffic across the entire network.

The following illustration shows the filtering components in a stand-alone deployment of Websense software, installed in a central location to see both HTTP and non-HTTP traffic.




To learn more about installing Network Agent in a network:

- With a hub, see *Connecting Network Agent to a hub*, page 114.
- With a switch, see *Switched networks with a single Network Agent*, page 114.
- With a gateway, see *Network Agent on gateway*, page 120.

# Locating Network Agent in multiple segment network

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

Depending on the device used to connect network segments, some traffic may not be sent to all segments. A router, bridge, or smart hub serves as traffic control, preventing unneeded traffic from being sent to a segment. In this environment, the Web Filter and Web Security components must be deployed to see all network traffic.

- Filtering Service must be installed where it can receive and manage Internet requests from the integration product, if any, and communicate with Network Agent.
- Each Network Agent instance must be able to see all Internet requests on the segment or segments that it is configured to monitor.

## Deploying multiple Network Agents

Multiple Network Agent instances may be needed in a multiple segment network to capture all Internet requests. A Network Agent can be installed on each segment to monitor the Internet requests from that segment.

**Note**

A limit of 4 Network Agents is suggested for each Filtering Service. It may be possible to use more agent instances, depending on system and network configuration and the volume of Internet requests. See *Network Agents per Filtering Service*, page 88.

If multiple Network Agent instances are installed:

- Ensure that the instances are deployed such that they, together, monitor the entire network. Partial deployment results in incomplete filtering and loss of log data in network segments not watched by Network Agent.
- Network Agent instances must not be configured to monitor overlapping IP address ranges. An overlap can result in inaccurate logging and network bandwidth measurements, and improper bandwidth-based filtering.

  The network segment or IP address range monitored by each Network Agent is determined by the NIC settings for the agent configured in the TRITON - Web Security console. See the TRITON - Web Security Help for instructions.
- Avoid deploying Network Agent across different LANs. If you install Network Agent on a machine in the 10.22.x.x network, and configure it to communicate with a Filtering Service machine in the 10.30.x.x network, communication may be slow enough to prevent Network Agent from blocking an Internet request before the site is returned to the user.

For examples of central and distributed Network Agent placement, see:

- *Connecting Network Agent to a hub*, page 114
- *Switched networks with a single Network Agent*, page 114.
- *Network Agent on gateway*, page 120

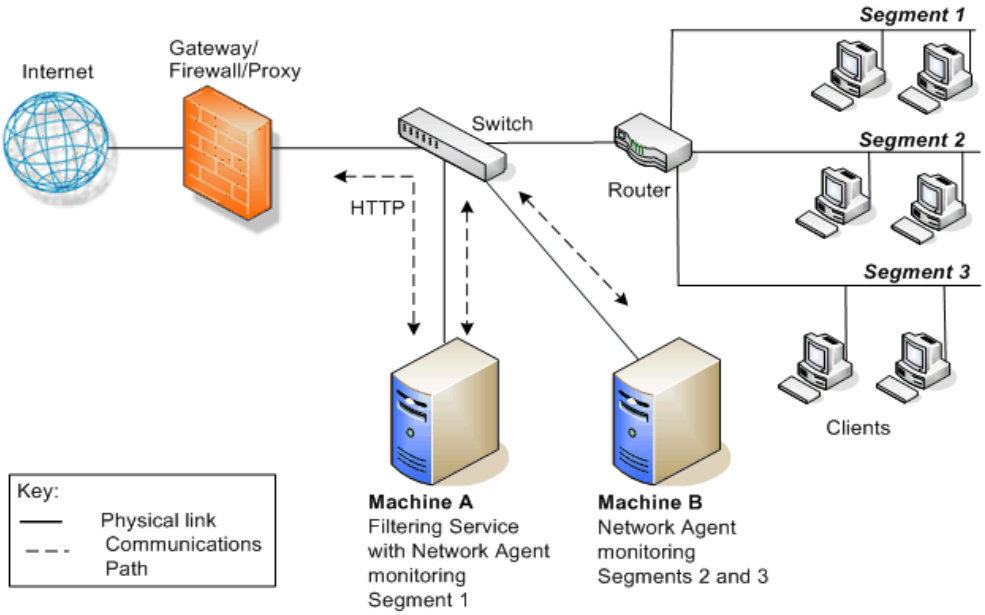
## Central Network Agent placement

A network with multiple segments can be filtered from a single location. Install Filtering Service where it can receive Internet requests from both the integration product, if any, and each Network Agent.

If the network contains multiple switches, Network Agent instances are inserted into the network at the last switch in the series. This switch must be connected to the gateway that goes out to the Internet.

In the following illustration:

- One Network Agent instance is installed with Filtering Service on Machine A. This machine is connected to the network via a switch that is configured to mirror or span the traffic of network Segment 1.
- A second Network Agent is installed on Machine B, which is connected to the same switch as Machine A. Machine B is connected to a different port that is configured to mirror the traffic of Segments 2 and 3.
- Each Network Agent is positioned to see all traffic for the network segment it monitors, and to communicate with other Websense components.
- The switch is connected to the gateway, allowing the Network Agent instances to monitor network traffic for all network segments.



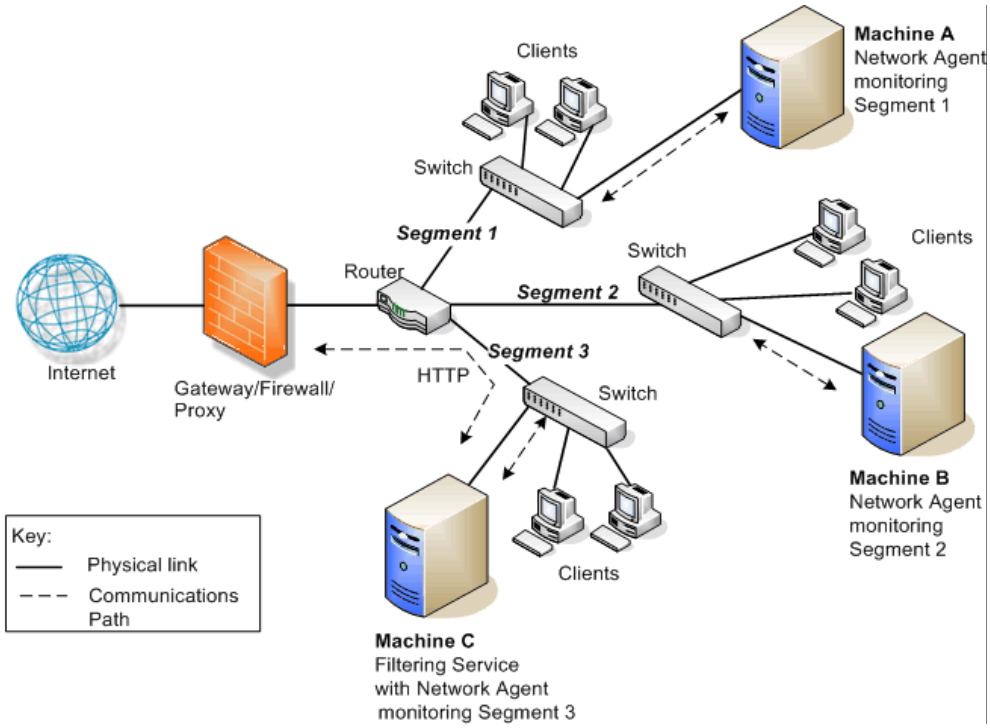

## Distributed Network Agent placement

The network diagram below shows a single Filtering Service with 3 Network Agents, one for each network segment. A deployment like this might be useful in organizations with satellite offices, for example.

- Filtering Service (Machine C) must be installed where it is able to receive and manage Internet requests from both the integration product (if any) and each of the Network Agent instances in all network segments.
- Each Network Agent (machines A, B and C) is connected to the network segment it monitors via the span or mirror port of a switch.

See *Deploying multiple Network Agents*, page 110, for more information.

In the following illustration, the switches are not connected in a series. However, each switch is connected to the router, which is connected to the gateway.



# Connecting Network Agent to a hub

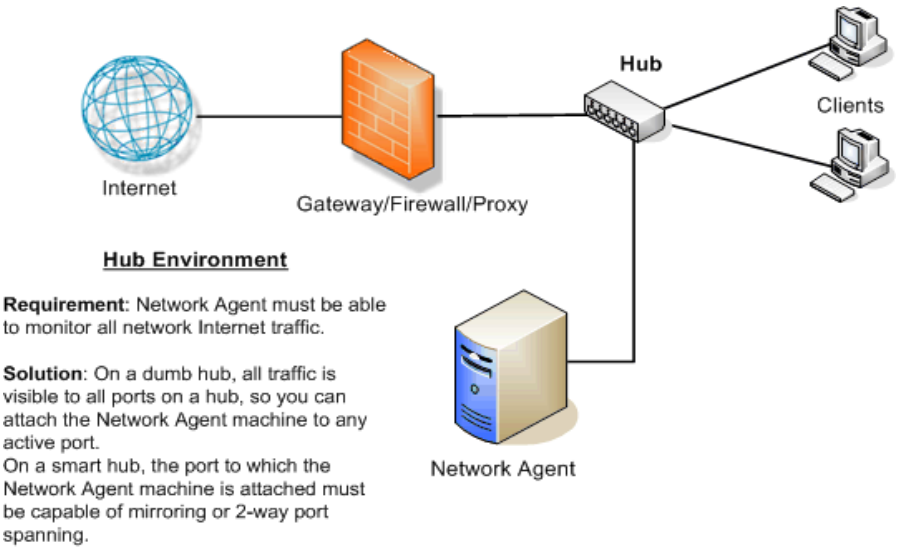
## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Connecting Network Agent to a hub

At the simplest level, a network hub provides a central connection point for the segments in a network and the devices in those segments. The port to which the Network Agent machine connects is dependent on the type of hub. Some hubs broadcast traffic to all of their ports, while others do not.

Network Agent must be able to see the traffic for the network segment(s) it is assigned to monitor.




# Switched networks with a single Network Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Switched networks with a single Network Agent

A switch is a bridge that routes traffic between network segments. It prevents all traffic from going to all segments, reducing network congestion. Because not all traffic going through a switch is visible to all devices on the network, the machine running Network Agent must be connected at a point where it can monitor all Internet traffic for the network.

Connect the Network Agent machine to the port on the switch that mirrors, monitors, or spans the traffic on the gateway or firewall port. The span or mirror port sees all the traffic that leaves each network segment.

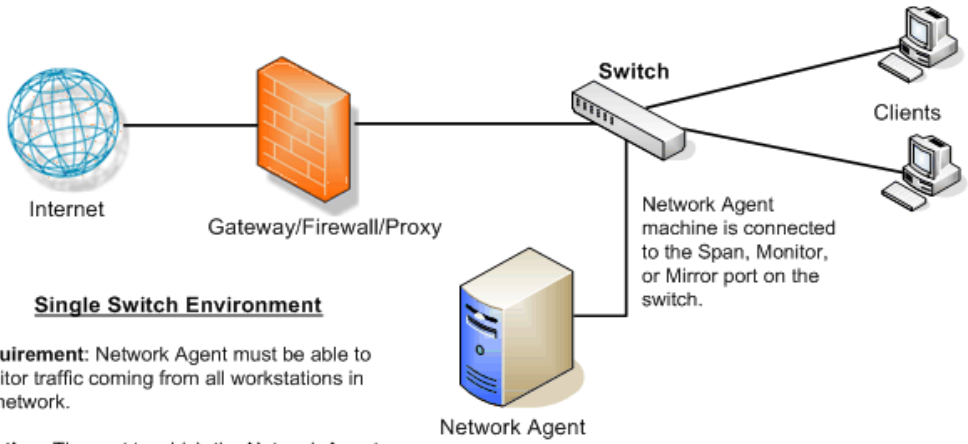
**Note**

Not all switches support bidirectional port spanning or mirroring. Contact the switch vendor to verify that spanning or mirroring is available, and for configuration instructions.

If bidirectional communication is not available, at least 2 network interface cards (NICs) are needed to monitor traffic and communicate with other Websense components.

If port spanning is not available, Network Agent cannot properly monitor the network.

The following illustration shows a network with a single switch. The Network Agent machine is attached to the port that mirrors all traffic from connected clients. Subsequent illustrations show multiple switch and multiple subnetwork configurations.

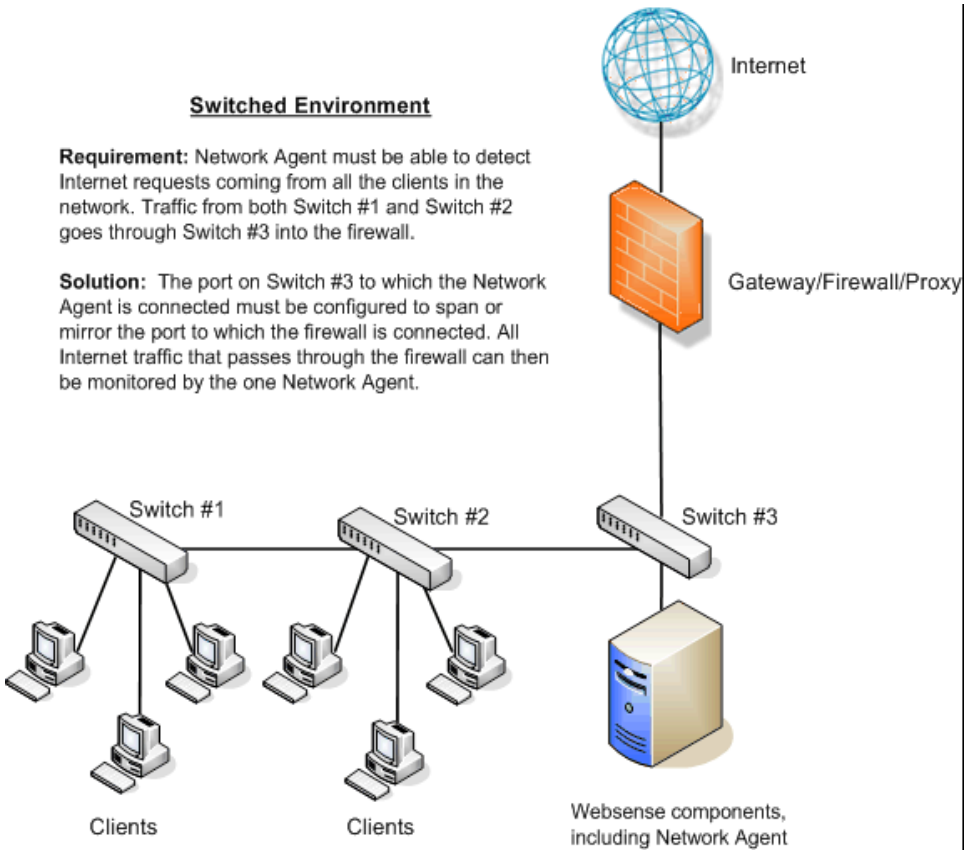



**Single Switch Environment**

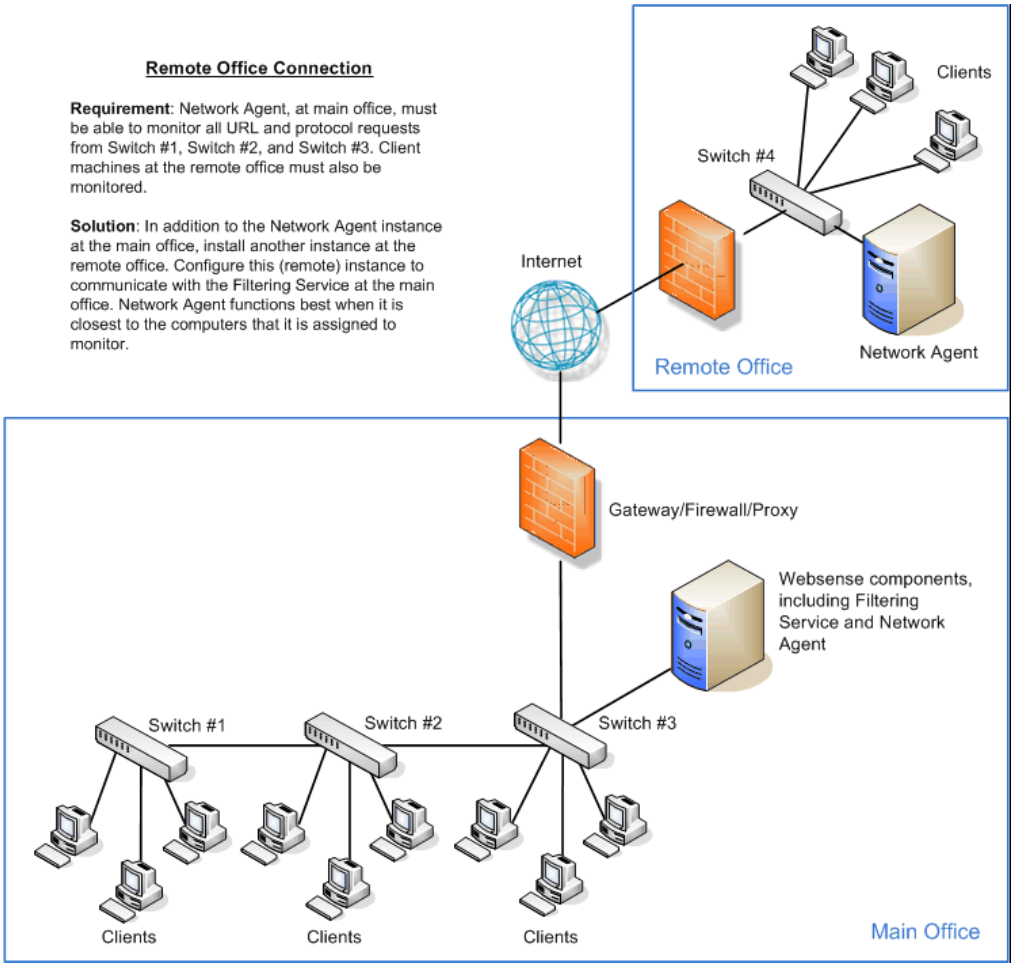
**Requirement**: Network Agent must be able to monitor traffic coming from all workstations in the network.

**Solution**: The port to which the Network Agent is connected must be configured to span or mirror the port to which the gateway/firewall/proxy is connected. All Internet traffic that passes through the gateway/firewall/proxy can then be monitored by Network Agent.

The following illustration shows the use of additional switches to create 2 network segments. All Internet traffic from these network segments must pass through Switch #3, to which Network Agent is attached. In a multiple-switch environment, failure to enable port spanning or mirroring could result in missed filtering and inaccurate reports.



The following illustration also contains multiple network segments. A remote office is filtered by installing another instance of Network Agent and configuring it to communicate with the Filtering Service at the main office.




To improve performance, Network Agent can be deployed on its own, dedicated machine. Network Agent can also be positioned closer to the clients, as shown in the illustration *Switched networks with multiple Network Agents*, page 119.

# Switched networks with multiple Network Agents

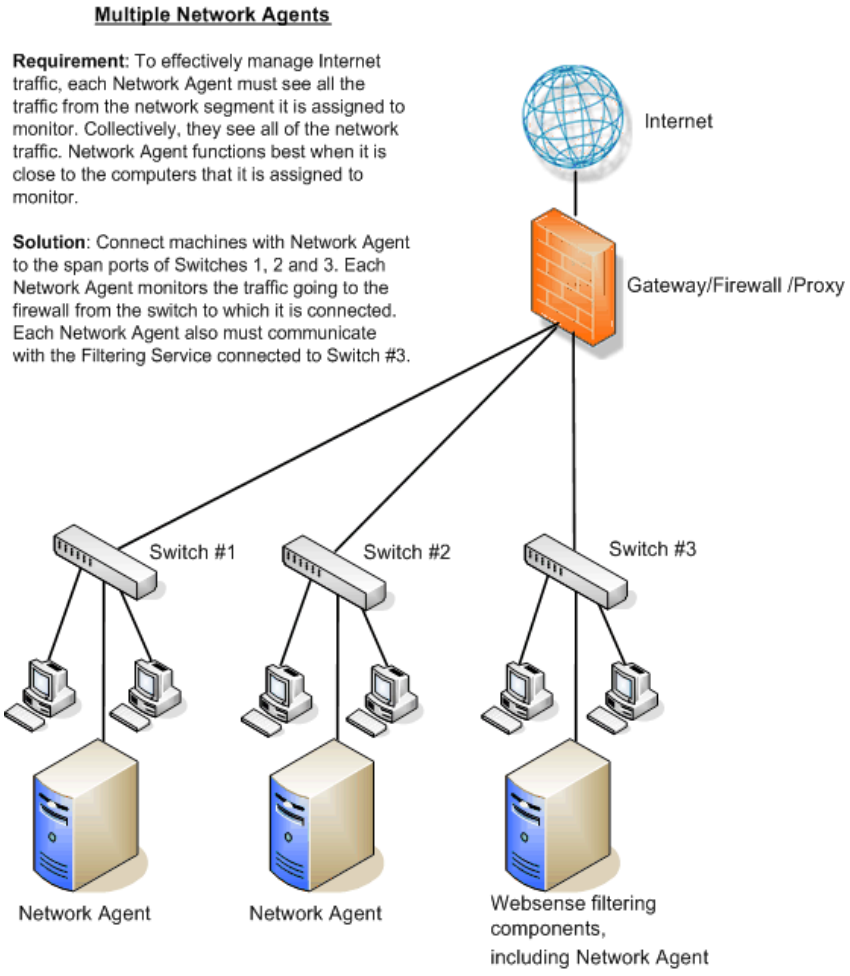
## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Switched networks with multiple Network Agents

A busy network may need multiple Network Agents to monitor different network segments or IP address ranges. Network Agent operates best when it is close to the computers it is assigned to monitor. The following illustration shows a network in which multiple Network Agent instances monitor separate network segments.

See *Deploying multiple Network Agents*, page 110, for more information.



# Network Agent on gateway

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Network Agent on gateway

A gateway provides a connection between two networks. The networks do not need to use the same network communication protocol. The gateway can also connect a network to the Internet.

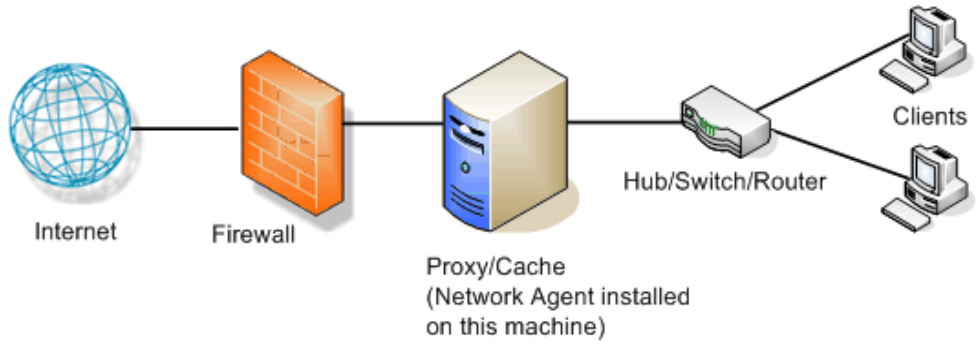
Network Agent can be installed on the gateway machine, allowing Network Agent to manage and monitor all Internet traffic. The gateway can either be a third-party proxy server or a network appliance. Do **not** install Network Agent on a firewall.

**Important**

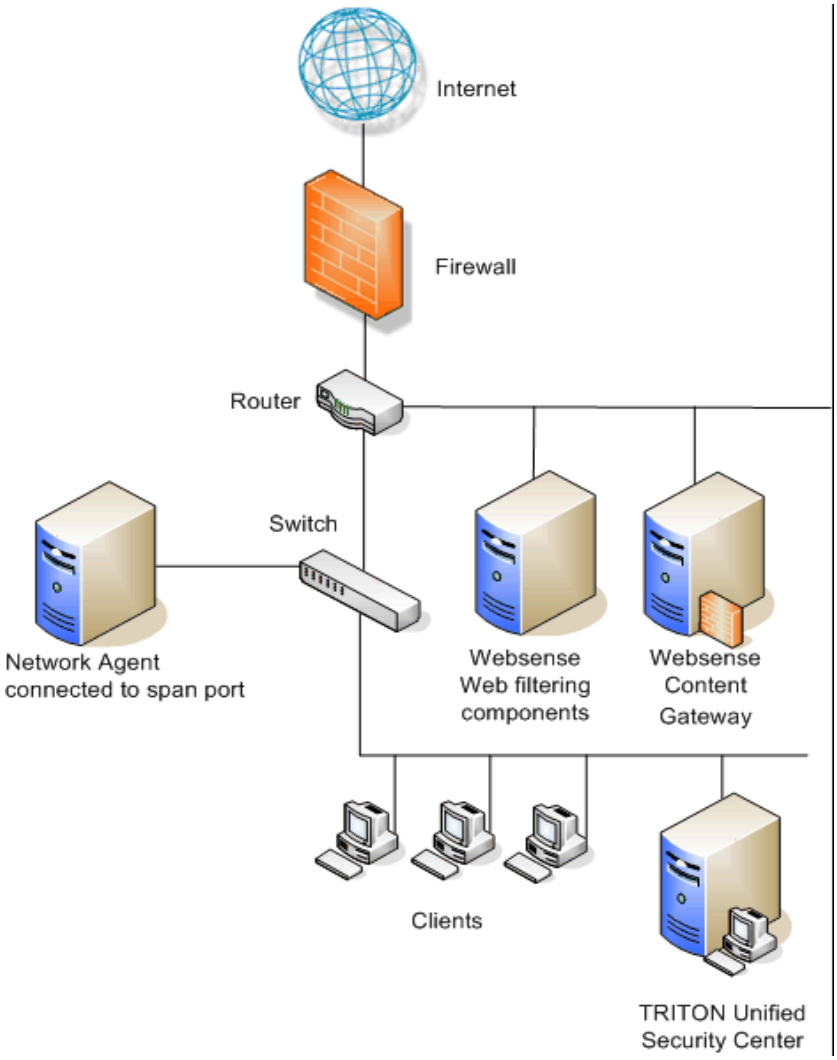
The gateway configuration shown here is best used in small to medium networks.

In larger networks, performance can suffer as a result of resource competition between the gateway software and Network Agent.

The following illustration shows Network Agent monitoring the Internet traffic at the proxy gateway or caching appliance directly attached to the firewall.



The following illustration shows Network Agent deployed in a network that includes Websense Content Gateway. Do not install Network Agent on the same machine with Websense Content Gateway.




# Network Agent and multiple NICs

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Network Agent and multiple NICs

Network Agent is capable of using more than one network interface card (NIC).

- Best practices suggest a maximum of 5 NICs.
- The NICs can be connected to ports on the same network device (switch or router), or to different network devices.

If the machine running Network Agent has multiple NICs:

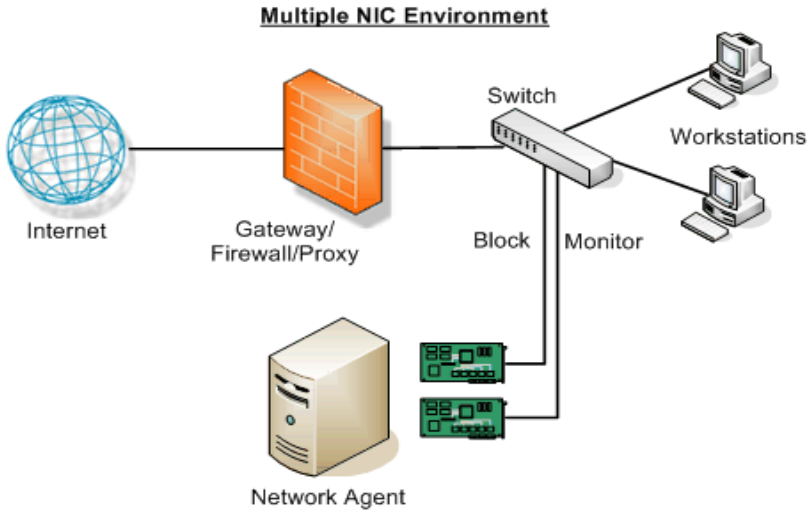
- Only one instance of Network Agent can be installed on the machine.
- The blocking or inject NIC (used to serve block pages) must have an IP address.
- Each NIC can be configured to monitor or block Internet requests, or both.
- Each NIC can be configured to monitor a different network segment.
- At least one NIC must be configured for blocking.

When you configure separate network cards to monitor traffic and send block messages (shown in the illustration below):

- The monitoring and blocking NIC do not have to be assigned to the same network segment.
- The monitoring NIC must be able to see all Internet traffic in the network segment that it is assigned to monitor.
- Multiple monitoring NICs can use the same blocking NIC.
- The blocking NIC must be able to send block messages to all machines assigned to the monitoring NICs, even if the machines are on another network segment.
- A monitoring NIC can be set for **stealth mode**. For information on configuring stealth mode, see *Configuring a stealth mode NIC*, page 788.
- The blocking NIC **must** have an IP address (cannot be set to stealth mode).

During installation, you specify which NIC is used by Websense software for communication and which NIC or NICs are used by Network Agent. For more information, see *Installing Web Security components*, page 668.

For information on configuring multiple NICs, see the TRITON - Web Security Help.




# NAT and Network Agent deployment

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## NAT and Network Agent deployment

If you use Network Address Translation (NAT) on internal routers, Network Agent may be unable to identify the source IP address of client machines. When Network Agent detects traffic after it is passed through such a router, the agent sees the IP address of the router's external interface as the source of the request, rather than the IP address of the client machine.

To address this issue, either disable NAT, or install Network Agent on a machine located **between** the NAT router and the monitored clients.

# 9 Integrating Web Security with Other Products

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## Integrating Web Security with other products

Web Filter and Web Security can be integrated with third-party products such as a firewall, proxy, or caching application.

# Integrating Web Security with Content Gateway

## Applies to

- Web Security Gateway v7.6

## Integrating Web Security with Content Gateway

Websense Content Gateway™ is a central gateway for controlling Web content that offers:

- The advantages of a proxy cache, improving bandwidth usage and network performance by storing requested Web pages and, if the page is still considered "fresh," serving the Web page to the requesting client.
- Real-time content categorization. This feature examines the content of uncategorized sites and sites that include rapidly changing content, and then returns a recommended category to Filtering Service.

Websense Content Gateway can run in explicit or transparent proxy mode.

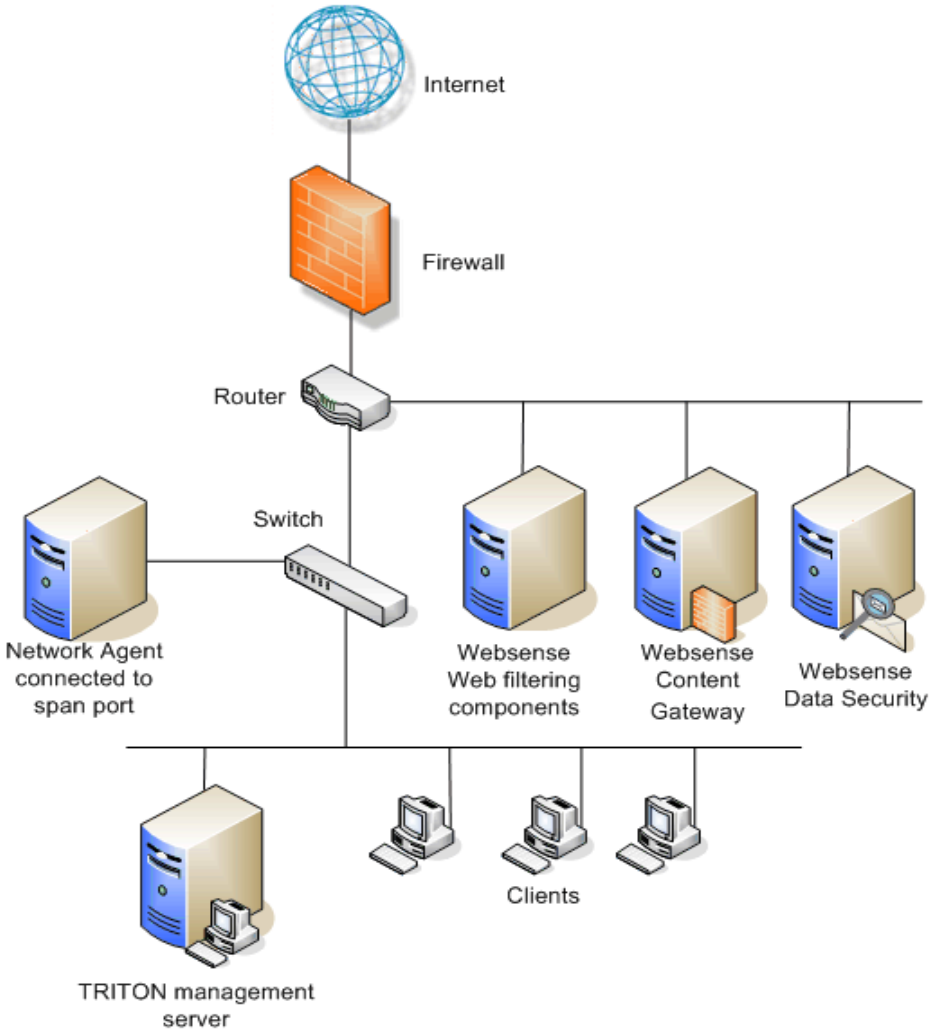
- In explicit proxy mode, client browsers must be configured to point to Content Gateway.
- In transparent proxy mode, the client request is intercepted and redirected to the proxy. Traffic is redirected through a router or a Layer 4 switch and the ARM (Adaptive Redirection Module) feature of Content Gateway.

Content Gateway can participate in flexible cache hierarchies, where Internet requests not fulfilled in one cache can be routed to other regional caches. Content Gateway also scales from a single node into multiple nodes to form a cluster, improving system performance and reliability.

Content Gateway is installed on a Linux machine, separate from other Websense components. See *Websense Content Gateway*, page 357, for more information.

The following illustration shows Websense Content Gateway and Websense Data Security deployed with Websense Web filtering components (including Policy Broker, Policy Server, Filtering Service, User Service, and a transparent identification agent).

- Data Security, Content Gateway, and Websense filtering component machines access network traffic through a router.
- Network Agent is installed on a separate machine, attached to the span port on a switch.




The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines.

# Integrating Web Security with Microsoft ISA Server or Forefront TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

> **Note**
> In this section, ISA/TMG refers to ISA Server and Forefront TMG collectively. When information differs for the two products, they are referred to specifically as ISA Server or Forefront TMG.

When you integrate Websense software with Microsoft ISA/TMG, the Websense ISAPI Filter must be installed on the ISA/TMG machine. The Websense ISAPI Filter allows ISA/TMG to communicate with Filtering Service, and must be installed on every ISA/TMG machine that communicates with Websense software.

You can install Policy Broker, Policy Server, Filtering Service, and User Service on the same machine as Microsoft ISA Server.

> **Important**
> No Websense components, other than the ISAPI Filter plug-in and Control Service, can be installed on a Forefront TMG machine. Control Service is automatically installed when you install the ISAPI Filter plug-in.

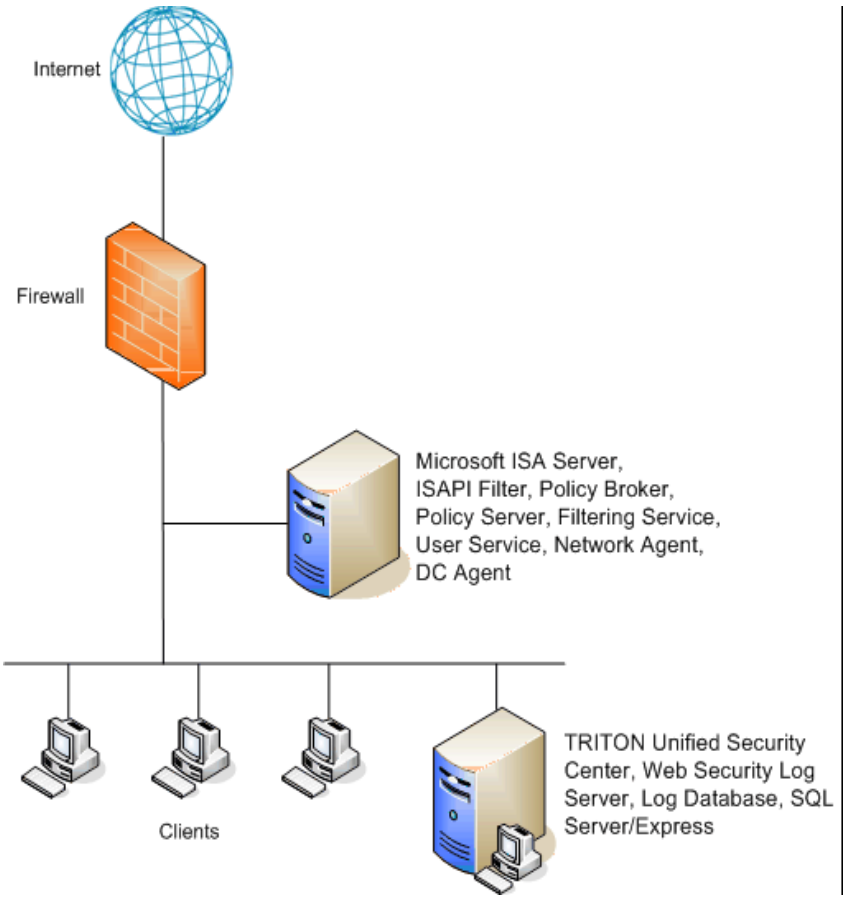
If your environment includes an array of ISA/TMG machines, install Websense software on a machine outside the array.

For more information, see *Microsoft ISA Server or Forefront TMG Integration*, page 227.

## Single Microsoft ISA/TMG configuration

The following illustration shows all Websense components, including the Websense ISAPI Filter, running on the same machine as a pre-TMG version of Microsoft ISA Server. Unless the Internet traffic volume is light, this configuration requires a powerful machine.

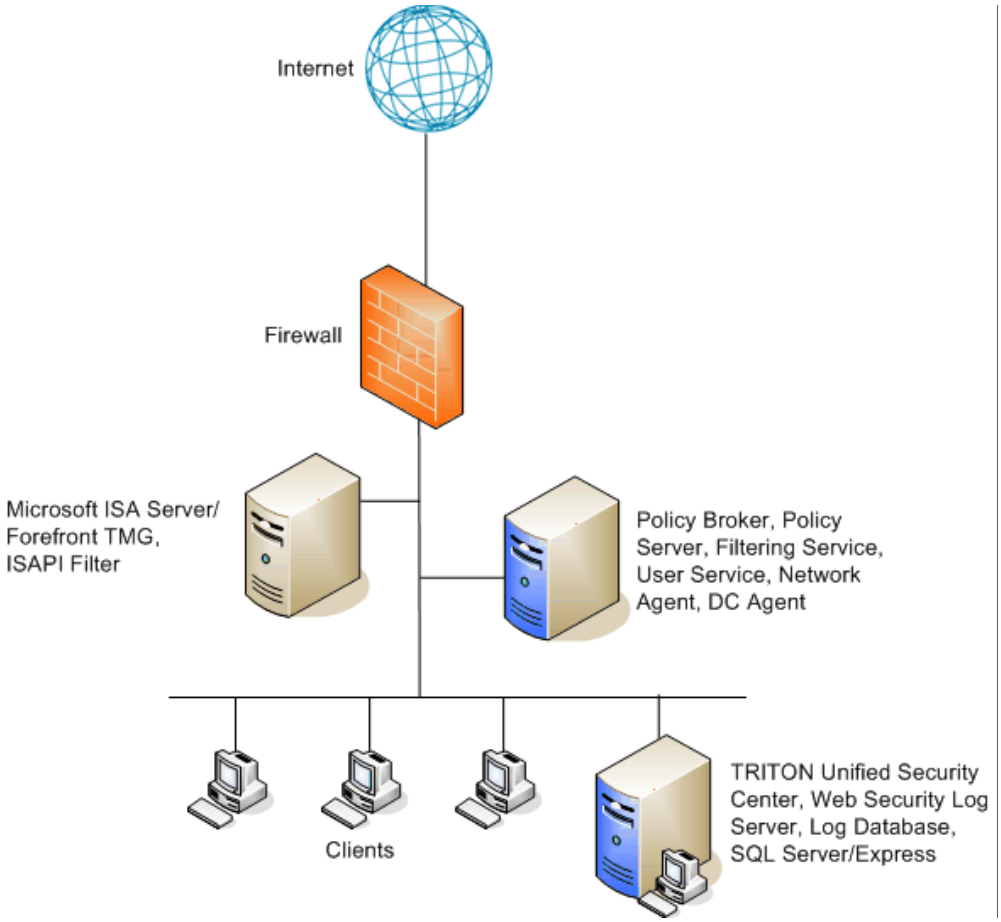
> **Important**
> No Websense components, other than the ISAPI Filter plug-in and Control Service, can be installed on a Forefront TMG machine.




The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Logon Agent can be used instead of or in combination with DC Agent.

An alternative setup, shown in the following illustration, places Websense filtering components on a Windows machine separate from the ISA/TMG machine. This configuration is required if you are using Forefront TMG, and eases the load on the machine for earlier versions of ISA.

- The ISAPI Filter must be installed on the ISA/TMG machine so that Internet activity information can be communicated to Filtering Service.
- The Filtering Service and ISA/TMG machines must be able to communicate over the network.

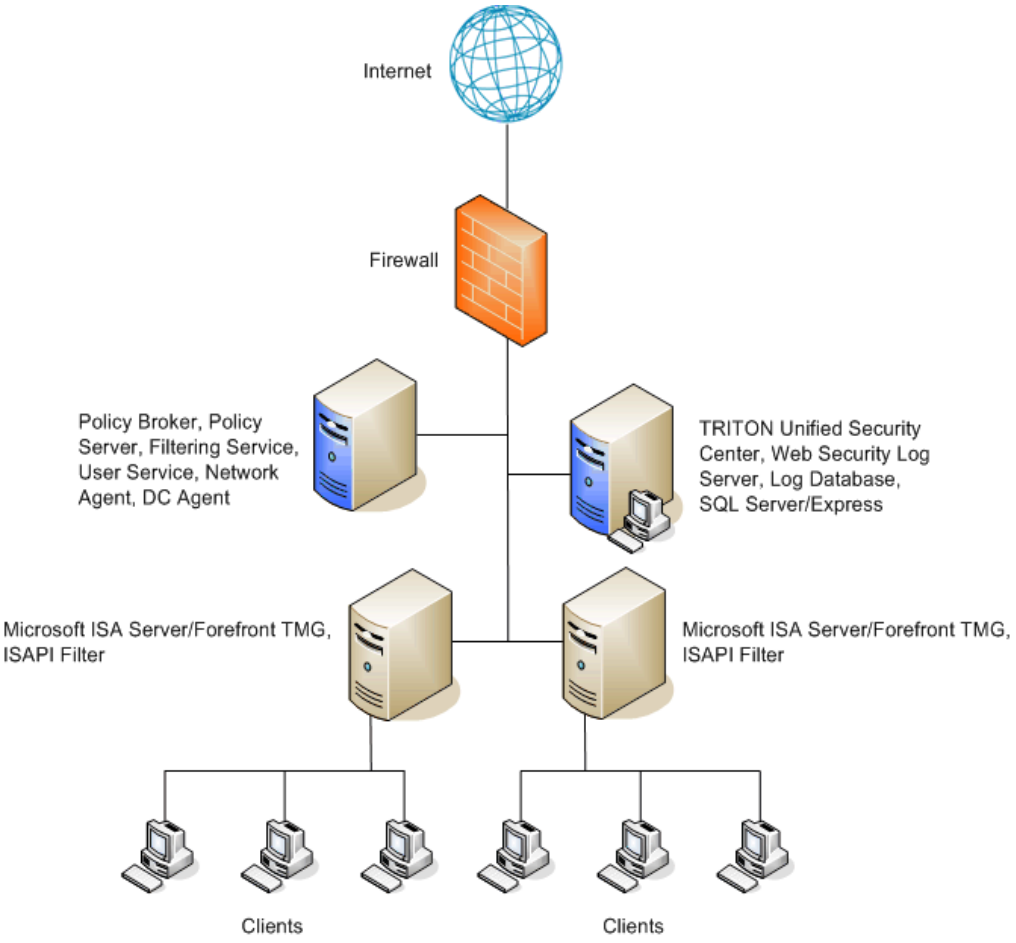



The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Logon Agent can be used instead of or in combination with DC Agent.

## Array configuration

Websense software is compatible with most array configurations, including Cache Array Routing Protocol (CARP) arrays. It is a best practice to install Websense software outside an array of ISA/TMG machines. Install the Websense ISAPI Filter on each member of the array. See the following illustration.

When Websense software is deployed in this configuration, all array members send Internet requests to Filtering Service outside the array.




Other configurations are possible. See your Microsoft ISA/TMG documentation for information about ISA/TMG configurations.

The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Logon Agent can be used instead of or in combination with DC Agent.

# Integrating Web Security with Cisco

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



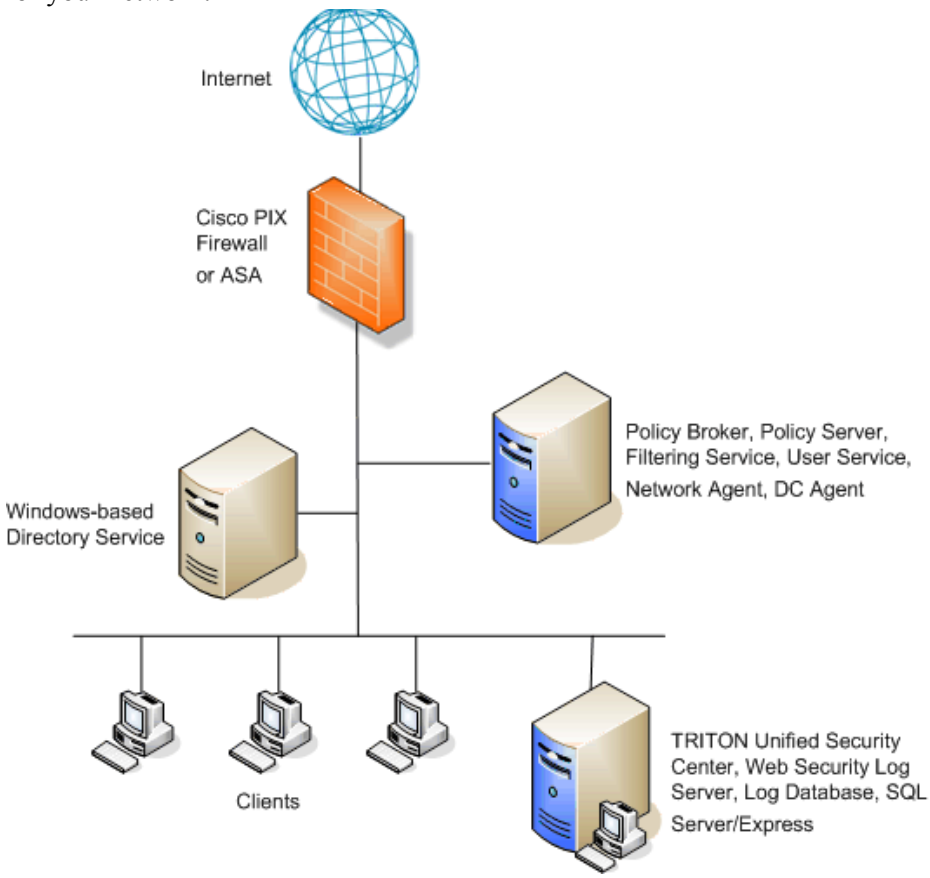
## Cisco PIX/ASA

A simple and common network topology places Websense filtering components on a single machine, or group of dedicated machines, communicating with a Cisco PIX Firewall or Cisco Adaptive Security Appliance (ASA) via TCP/IP.

- TRITON Unified Security Center and reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

See *Cisco Integration*, page 193 for configuration instructions.

Other configurations are possible. See your Cisco PIX Firewall or ASA documentation and the information in this section to determine the best configuration for your network.



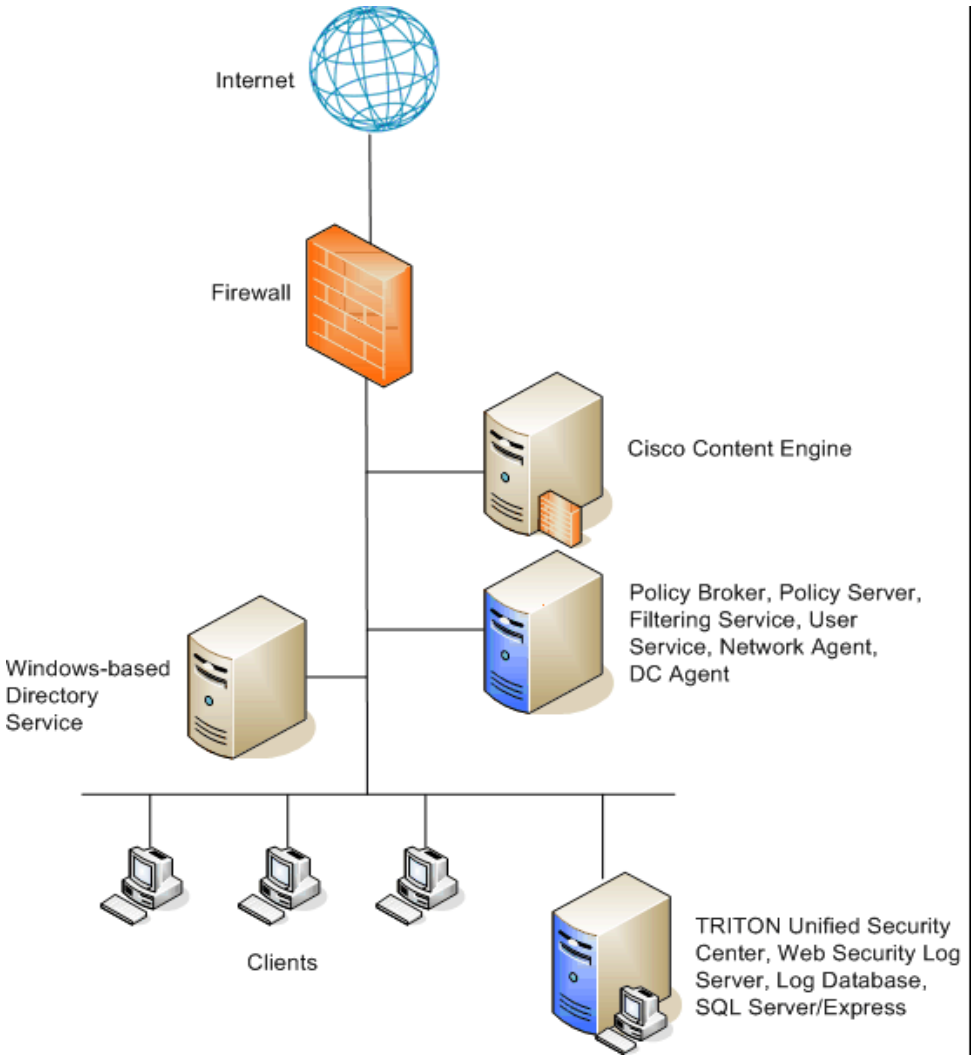

The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Logon Agent can be used instead of or in combination with DC Agent.

## Cisco Content Engine

In this common configuration, Websense filtering components are installed on a single machine, communicating with the Cisco Content Engine through TCP/IP.

- TRITON Unified Security Center and reporting components are installed on a separate machine.

- If you install Network Agent, it must be positioned to see all traffic on the internal network.




Other configurations are possible. See your Content Engine documentation and the information in this chapter to determine the best configuration for your network.

The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Logon Agent can be used instead of or in combination with DC Agent.

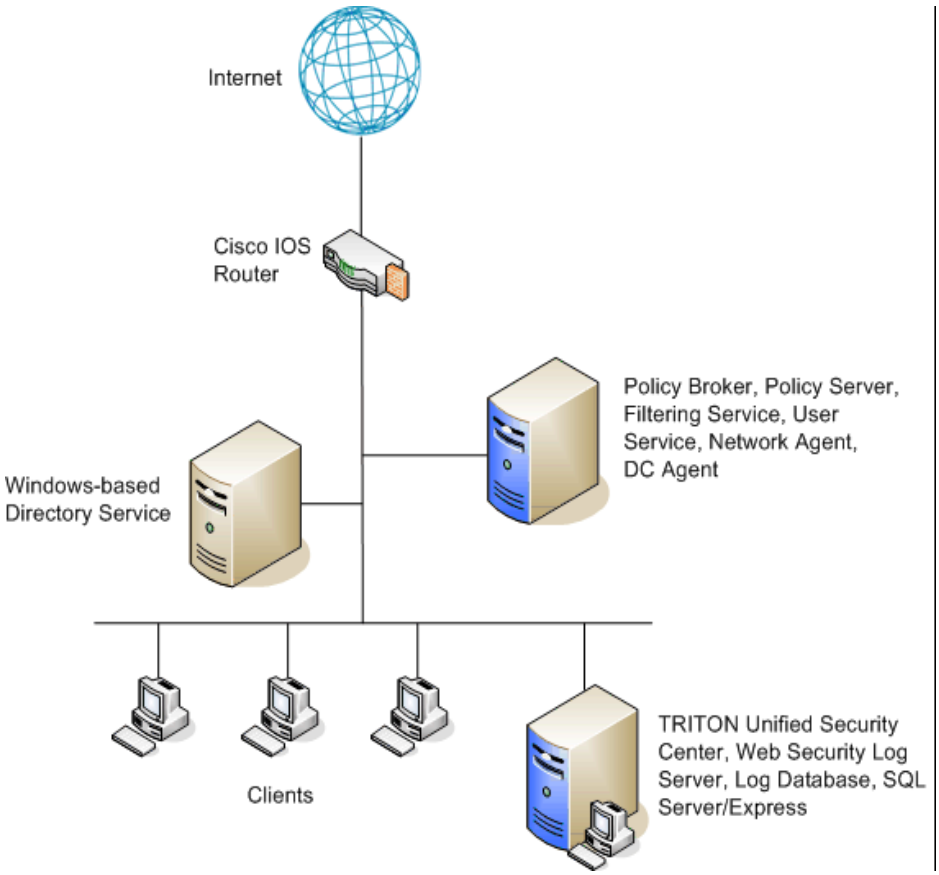
## Cisco IOS Routers

In this common configuration, Websense filtering components are installed on a single machine, communicating with the Cisco IOS Router.

- TRITON Unified Security Center and reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

The router has firewall functionality and can be used with or without an accompanying firewall.

If the Cisco IOS Router is used with a separate firewall, ensure that all Internet traffic is configured to pass through the router and is not set to bypass the router and go directly to the firewall. Traffic filtered through the separate firewall cannot be filtered by the Websense software.




Other configurations are possible. See your Cisco Router documentation and the information in this chapter to determine the best configuration for your network.

The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Logon Agent can be used instead of or in combination with DC Agent.

# Integrating Web Security with Check Point

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



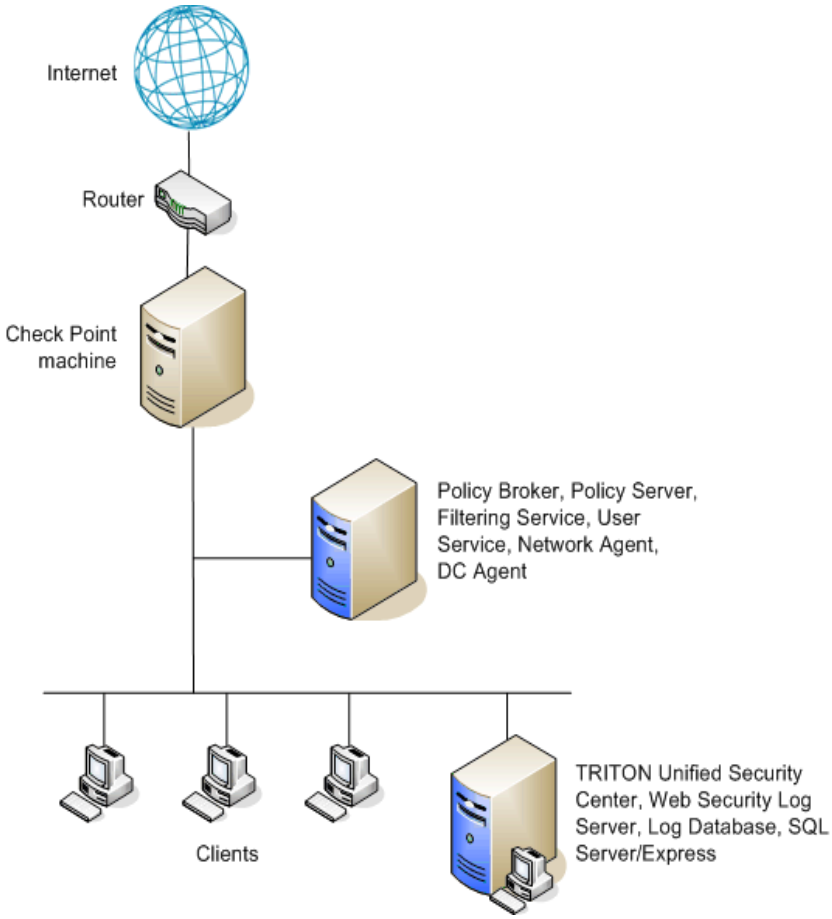
## Overview

This section includes a general discussion of 2 common Check Point integration deployment options: simple deployment with unified components, and distributed deployment. See *Check Point Integration*, page 285 for configuration instructions.

## Simple

In the simplest and most common network topology, an organization has one firewall that resides on a dedicated server. All Web Security components are installed on a separate machine on the internal network.

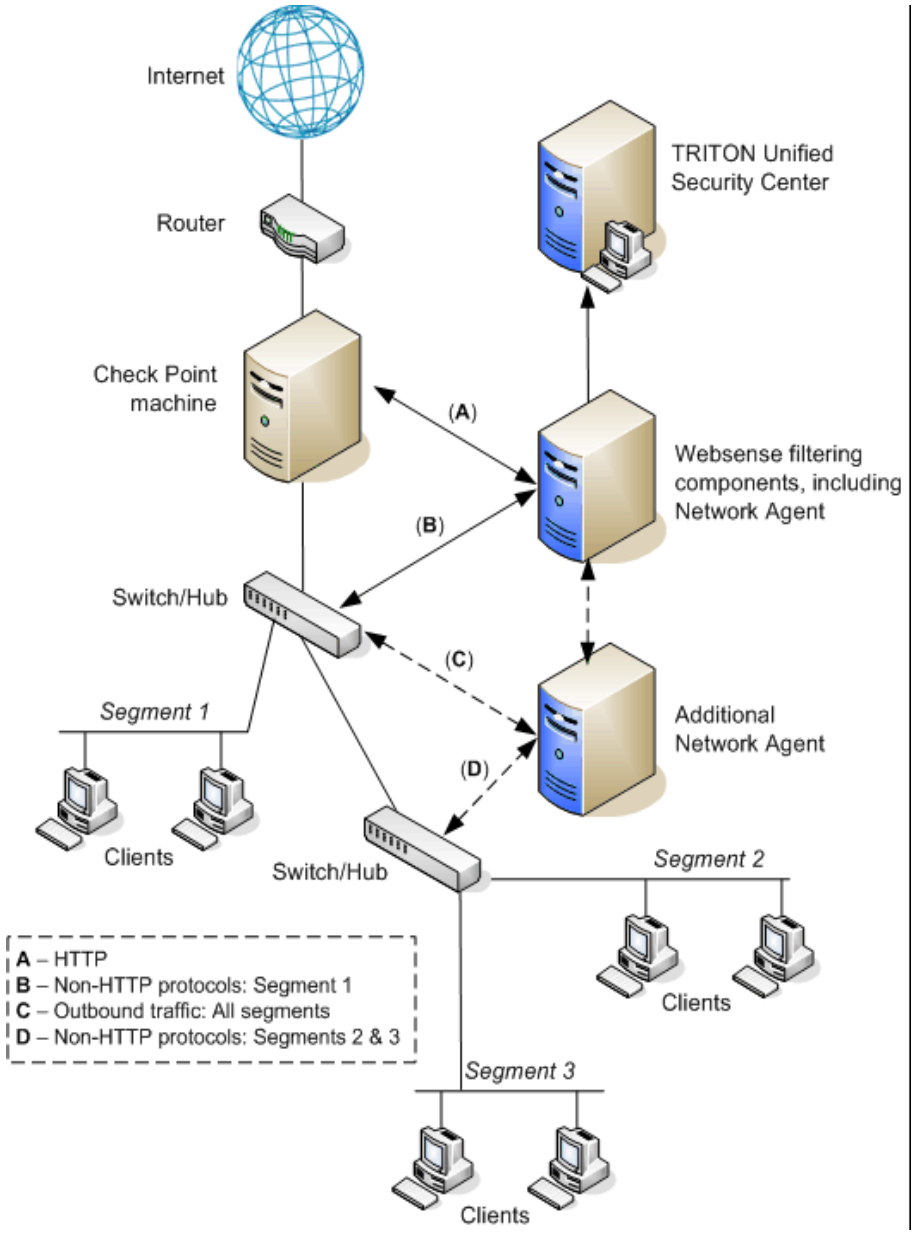
- TRITON Unified Security Center and reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network. HTTP requests are handled by the Check Point appliance, and non-HTTP traffic is managed by Network Agent, which is positioned to detect all outbound traffic.




The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Logon Agent can be used instead of or in combination with DC Agent.

## Distributed

In the following illustration, Websense filtering software is installed on a single machine in a central location where it can manage both non-HTTP and HTTP traffic. HTTP requests are handled by the Check Point appliance, and the non-HTTP traffic is managed by Network Agent, which is positioned to detect all outbound traffic.




The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines.

To avoid performance and security issues, do **not** install Websense components on a machine running Check Point software. Network Agent will not function correctly if installed on the Check Point machine.

**Warning**

Websense, Inc., and Check Point do not recommend installing Websense software and Check Point on the same machine. Do **not** install Network Agent on the same machine as Check Point software.

# Integrating Web Security with Squid Web Proxy Cache

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



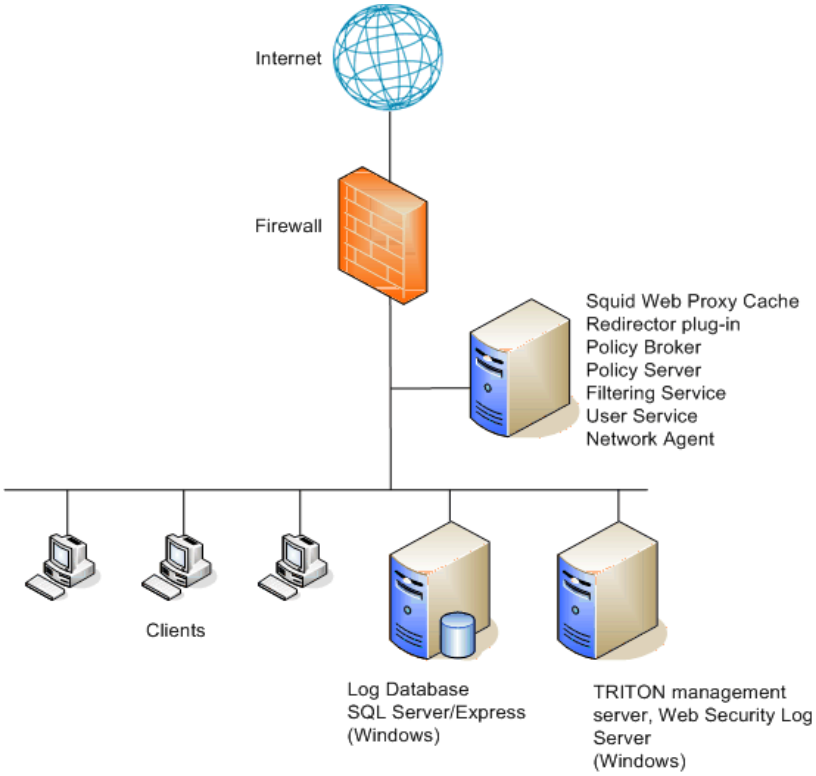
## Overview

Websense filtering components can be installed on the same machine as Squid Web Proxy Cache, on a separate machine, or on multiple machines. Squid Web Proxy Cache machines may be deployed in an array to share the load in a larger network. A Websense Squid redirector plug-in must be installed on each machine running Squid Web Proxy Cache.

## Single Squid Web Proxy Cache configuration

The following illustration shows the Websense filtering components, the Websense redirector plug-in, and Squid Web Proxy Cache running on the same machine. You

can also install a Websense transparent identification agent on the same machine, or on a separate machine.




The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines.

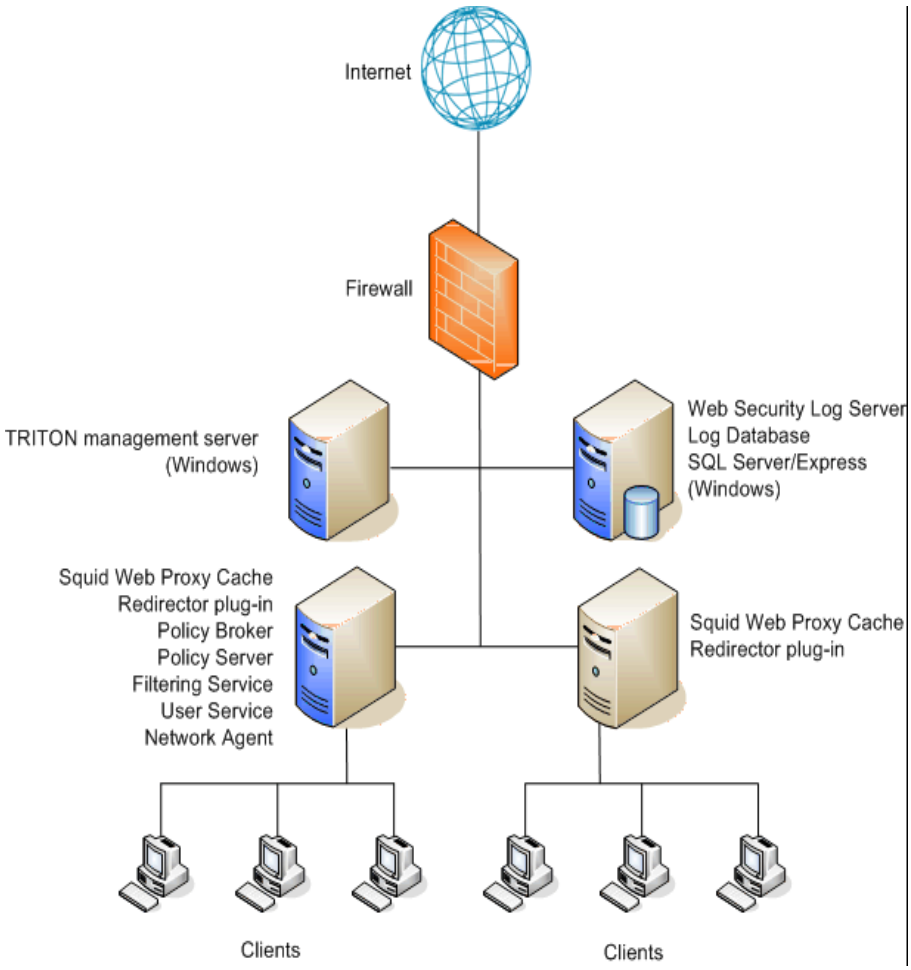
An alternative deployment places all Websense filtering components on a separate machine from Squid Web Proxy Cache. This configuration eases the load on the Squid Web Proxy Cache machine.

- The Websense redirector plug-in must be installed on the Squid Web Proxy Cache machine to enable communication with Filtering Service.
- The Filtering Service and Squid Web Proxy Cache machines must be able to communicate over the network

## Array configuration

Websense software is compatible with most array configurations, including Cache Array Routing Protocol (CARP) arrays. If the Squid Web Proxy Cache machines in an array can run Websense software without a performance impact, install the main Websense filtering components on one of the array machines.

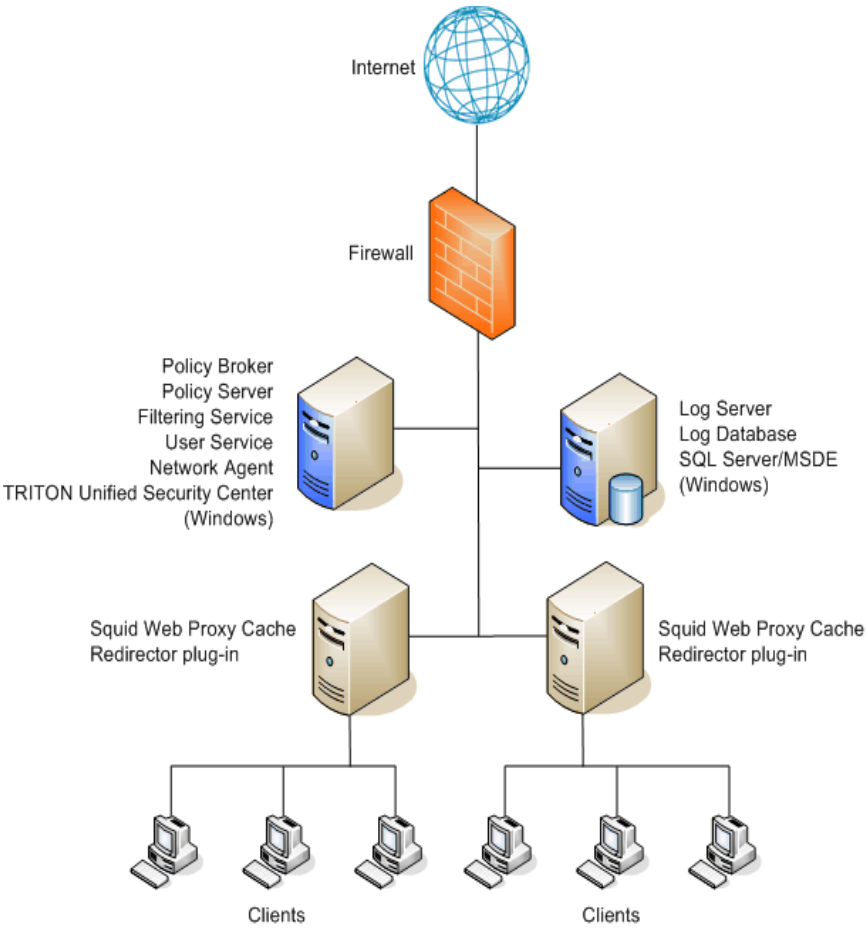
The following illustration shows the Websense filtering components running on a Squid Web Proxy Cache machine, with Websense reporting components on a separate machine.




The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines.

If installing Websense filtering components on the Squid Web Proxy Cache machine is likely to have a performance impact, install Websense software on a separate machine outside the array, and then install the Websense redirector plug-in on each member of the array. See the following illustration.

When Websense software is installed in this configuration, all array members send Internet requests to Filtering Service outside the array.




Other configurations are possible. See your Squid Web Proxy Cache documentation for information about array configurations. See *Squid Web Proxy Cache Integration*, page 259 Websense software configuration instructions.

The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines. Also, the Web filtering components are shown above on a Windows machine. The TRITON Unified Security Center must run on Windows; the remaining components can be installed on Linux instead.

# Integrating Web Security with Citrix

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Integrating Web Security with Citrix

Websense software integrated with a Citrix server can monitor HTTP, FTP, and SSL requests from individual Citrix users. Network Agent can be used to filter other protocols, if needed.

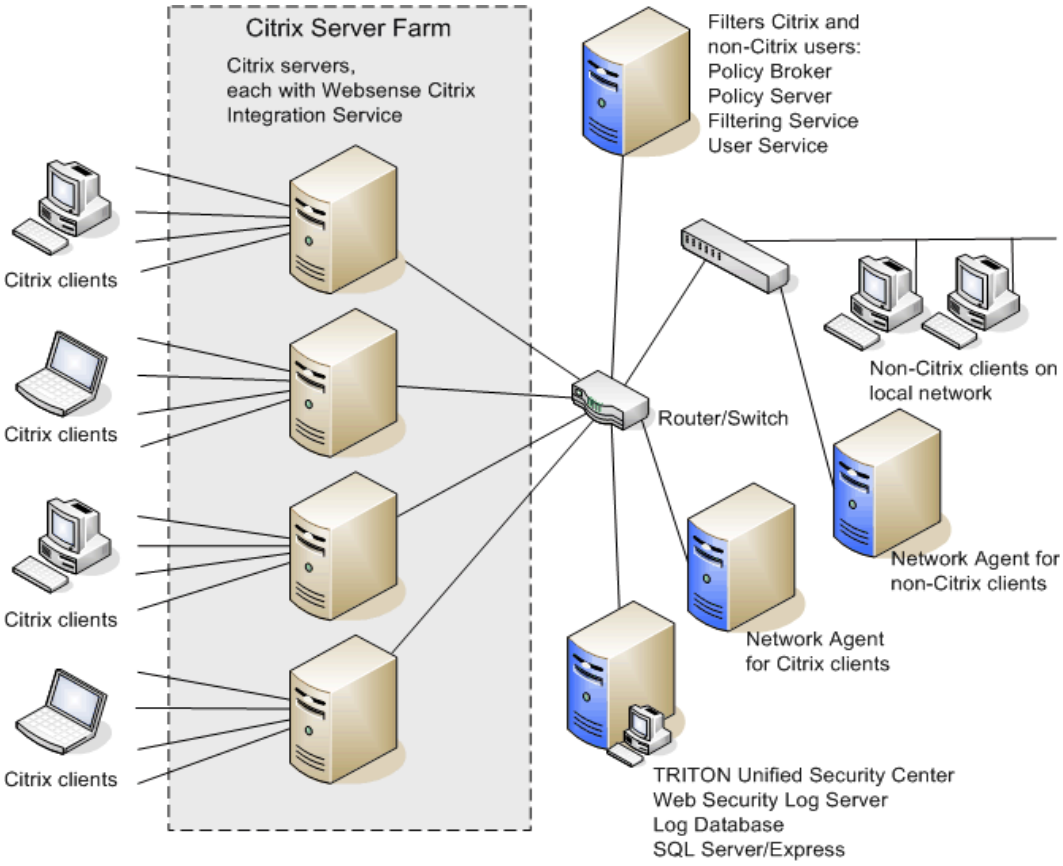
> **Note**
> "Citrix server" refers to Citrix Presentation Server or XenApp. For the versions supported by Websense software, see *System Requirements*, page 41.

The following illustration shows a typical deployment used to filter both users who access the Internet through a Citrix server and users who access the Internet locally.

- The Websense filtering components are installed on a dedicated machine that can filter Citrix server clients (non-Citrix clients are filtered by a separate integration product or Network Agent; see *Citrix Integration*, page 167).
- The Websense Citrix Integration Service must be installed on each Citrix server to allow it to communicate with Filtering Service.
- No other Websense components can be installed on a Citrix server.

Separate Network Agent instances are needed for the Citrix and non-Citrix users.

To simplify the diagram, not all individual Websense components are shown.




Other integrations also can be used in the non-Citrix portion of the network. See *Citrix Integration*, page 167 for Websense software configuration instructions.

The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines.

# Other integrations for Web Security

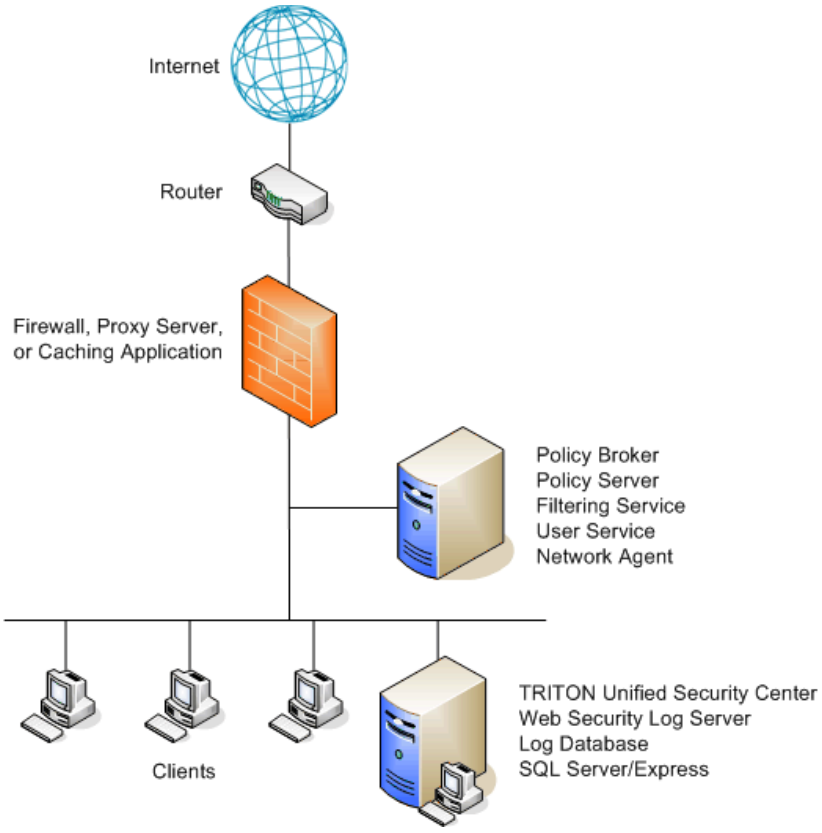
## Applies to

- Web Filter v7.6
- Web Security v7.6

## Other integrations for Web Security

Check the list of Websense Technology Partners at www.websense.com/global/en/Partners/TAPartners/SecurityEcosystem/ to see if Websense software can be integrated with a third-party product. If your integration product is listed, that product has been specifically enhanced to integrate with Websense software.

Typical configurations include networks with a single firewall, proxy server, or caching application, and networks with an array of firewalls, proxy servers, or caching appliances. A Websense transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent) can be installed on the Filtering Service machine or on a separate machine.




Other configurations are possible. See your integration product's documentation for other recommendations. See *Universal Integrations*, page 323 for Websense software configuration instructions.

The diagram provides a general overview and best practice location for your integration product, but does not show all Websense components. Larger networks require Websense components to be distributed across several dedicated machines.

# 10 Web Security Distributed Enterprise Deployments

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Web Security distributed enterprise deployments

Distributed enterprise networks may have many remote locations, ranging from dozens to thousands of small sites. Typically, between 5 and 50 employees work at each remote site. Many of these sites have Internet access, but no dedicated IT staff.

Some organizations use a decentralized network topology that provides each remote site with its own Internet connection. The challenge is to apply consistent, cost-effective filtering of Internet requests across the entire organization.

Distributed enterprises with remote Internet connectivity have a complex set of filtering considerations:

- Remote sites must have Internet access.
- Internet access is provided by independent Internet service providers, often using low to medium-bandwidth connections.
- Web page requests are sent directly to the Internet and are not first routed through a central corporate network.
- Internet access must be filtered to permit only appropriate content.
- Cost considerations prohibit deploying a dedicated filtering server at each site.
- Given the relative low speed of each office's Internet connection, a slightly slower response from the filtering product is acceptable.
- All remote sites can be filtered using the same policies.

Websense Web Filter, Web Security, and Web Security Gateway are on-premises solutions in which Websense filtering components can be deployed regionally and communicate over the Internet to apply uniform filtering policies across all offices.

> **Note**
> In this and related sections about Web Security, the information generally applies to Web Filter as well. For the purposes of these sections, *Websense Web Security* should be taken to refer to both solutions collectively, unless otherwise stated.

Websense Web Security Gateway Anywhere is a hybrid solution, allowing a combination of on-premises and in-the-cloud filtering. Additionally, off-site users outside the network of any site (such as telecommuters or traveling employees) can be filtered through the hybrid service.

See the following for more information:

- *Web Security basic distributed enterprise topology*, page 148
- *Web Security filtering remote sites*, page 151
- *Web Security distributed enterprise deployment models*, page 154
- *Web Security distributed deployments and secure VPN connections*, page 160

# Web Security basic distributed enterprise topology

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



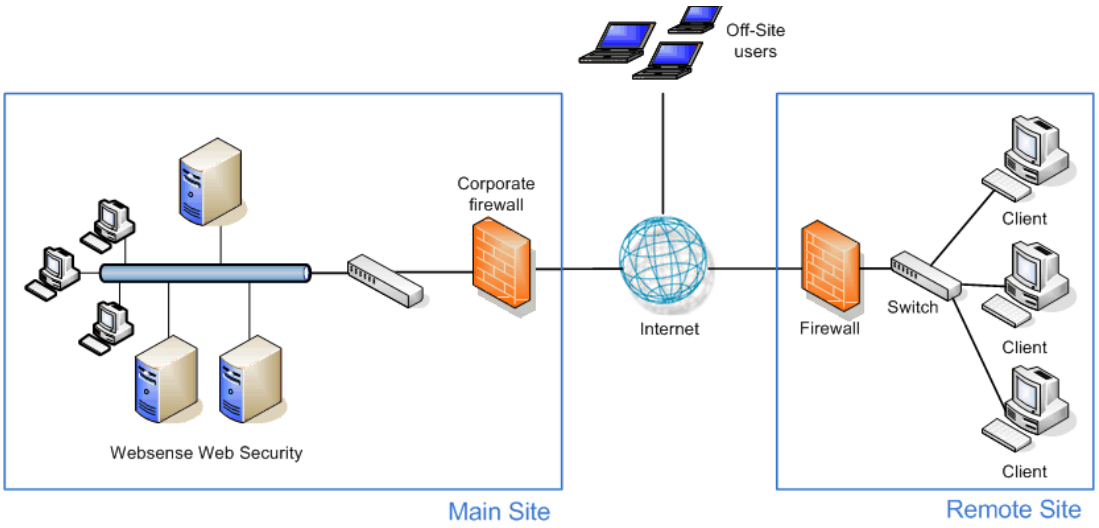
## Web Security and Web Security Gateway

To reduce network infrastructure costs, each remote-site firewall in a decentralized network is connected directly to the Internet, rather than to a corporate WAN.

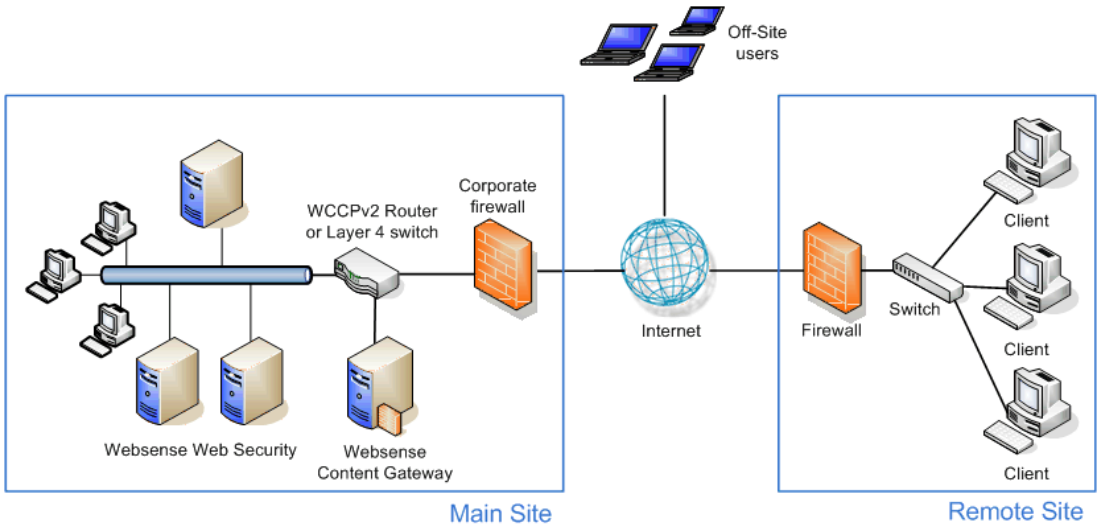
A small office/home office (SOHO) firewall is connected to an ISDN, DSL/cable, or T1 connection. Except for corporate application data that may use a virtual private

network (VPN) connection, each outbound Internet request from a remote site is sent through a local Internet service provider (ISP) to the Internet.

The illustration below shows a sample network topology of this type of remote site for Websense Web Security.




Websense Web Security Gateway adds Websense Content Gateway to the deployment, as shown below.

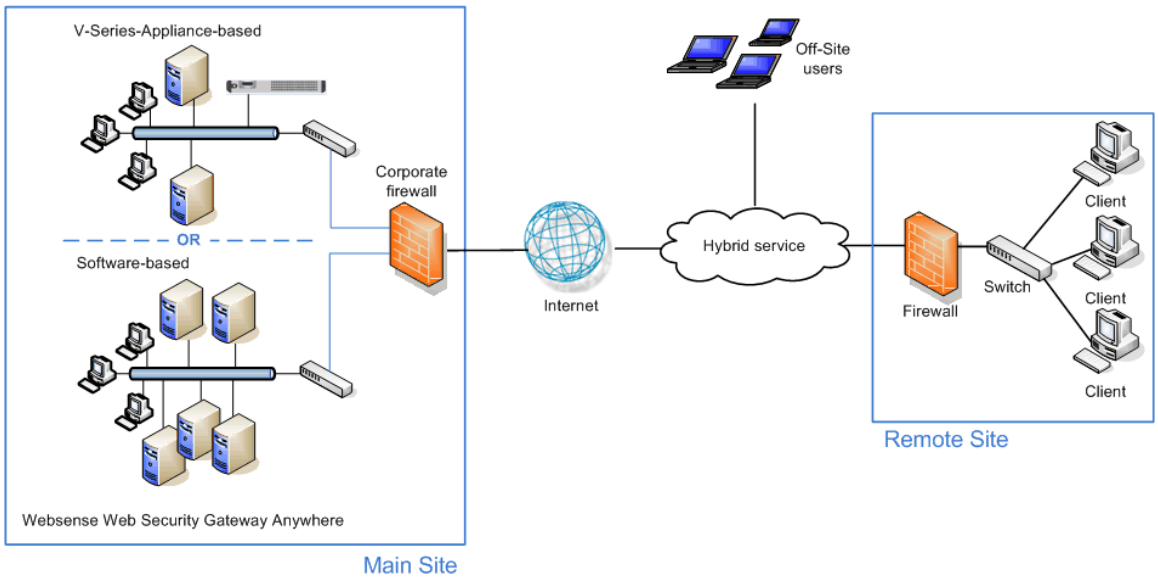



Off-site users (remote users outside the corporate or remote-site network) can be filtered using Websense Remote Filtering. Note that the Remote Filtering Server must be deployed in the main site network (Remote Filtering Server not depicted in the above illustrations) and Remote Filtering Client must be installed on each off-site machine. See Remote Filtering Software technical paper.

The above two illustrations show a high-level scheme only. Details about how distributing across separate machines, Content Gateway deployment, Network Agent placement, use of an integration product, and so forth are not included. Do not install any Websense components on a domain controller.

# Websense Web Security Gateway Anywhere

In a basic Web Security Gateway Anywhere deployment, the remote site and off-site users can be filtered through the hybrid service rather than by the filtering software at the main site..




A V-Series-appliance-based or software-based deployment of Web Security Gateway Anywhere is installed at the main site. A V-Series-appliance-based deployment consists of a Websense V-Series appliance running core filtering components, plus additional servers running reporting and interoperability components (allowing communication between Web and data security components and also between on-premises components and the hybrid service). A software-based deployment consists of all the same components, distributed across a number of servers.

No additional software is required at remote sites or on off-site machines to be filtered through the hybrid service (some configuration at the main site and deployment of a PAC file to client machines is required; see the TRITON - Web Security Help for more information).

# Web Security filtering remote sites

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Websense Web Security or Web Security Gateway

In centralized organizations that route all outbound Internet requests through a single large Internet connection, the servers running Websense software are normally placed physically close to the firewall, proxy server, or network appliance.

Remote sites in a distributed enterprise have a direct local connection to the Internet, and no centralized point of control.

Rather than deploying Websense software at each remote-site firewall, you can deploy Websense components in a geographically central location. Since Websense software is accessible from the Internet, the Websense components should be protected by a firewall that allows URL lookup requests to pass through.

Filtering is performed by the Websense components at the main site. Remote sites must be equipped with a firewall that can be integrated with Websense software (configured to check with Websense software to permit or block Web requests), or an instance of Websense Network Agent must be deployed at the remote site*Firewall* is used here as a generic term to refer to a firewall, gateway, or proxy.

Websense, Inc. has tested this configuration in cooperation with several of its integration partners. The same deployment methodology described here can be used with any supported network security product integrated with Websense software. A full list of supported integration products can be found at:

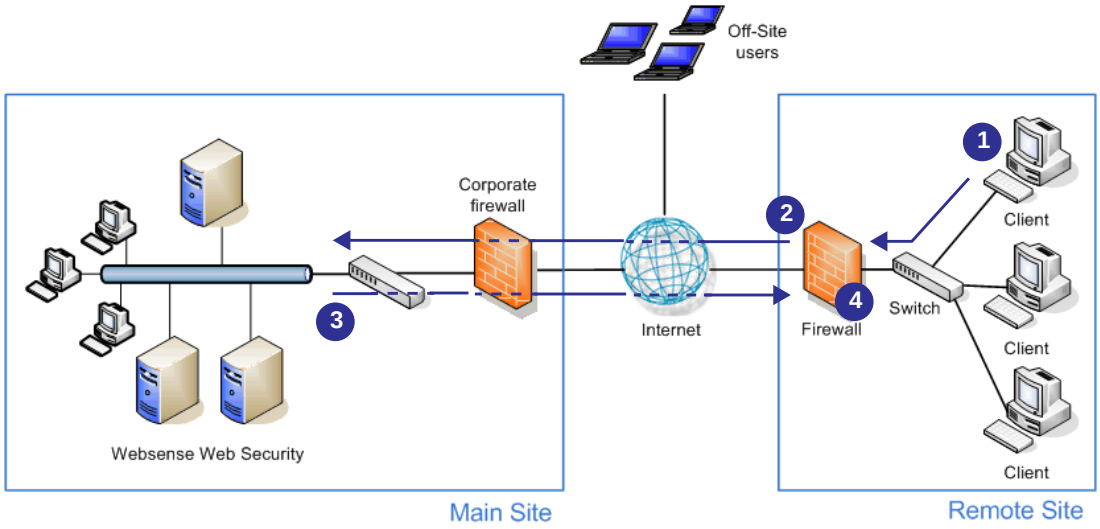
www.websense.com/global/en/Partners/TAPartners/SecurityEcosystem/

Centralized filtering:

- Provides distributed enterprises with Websense filtering for each remote site.
- Eliminates the need for a separate Websense software installation at each location.
- Provides uniform filtering policies at each remote site.

- Eliminates the cost of additional hardware to provide filtering servers at each remote site.
- Allows the enterprise to centrally configure, administer, and maintain a limited number of Websense filtering machines.

The following illustration shows a typical sequence of events in filtering a client machine at a remote site.




1. User requests a Web page.
2. Local firewall checks the URL of the requested page with Websense Web Security/Web Security Gateway over the Internet.
3. Websense Web Security/Web Security Gateway responds over the Internet, indicating whether the request should be permitted or blocked.
4. Local firewall permits or blocks the request as directed.

Note the preceding illustration is a simplified diagram showing the main conceptual sequence of events. Do not install any Websense components on a domain controller.

Details of Websense component distribution and placement in the corporate network, network routing and internal firewall usage, segmentation of networks, and so forth are addressed in other sections of the Deployment Center.

In the case of multiple remote sites, each remote site communicates with Websense components at the main site in the same manner shown above.

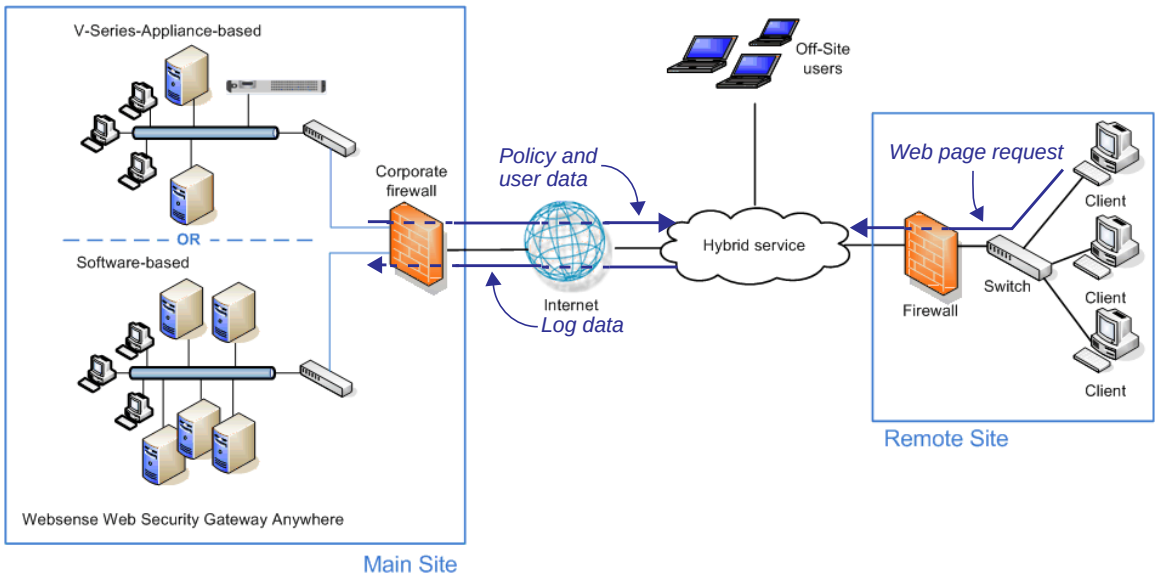
Off-site user machines are filtered by deploying Websense Remote Filtering Server at the main site. Websense Remote Filtering Client is installed on each off-site machine to be filtered. See Remote Filtering Software technical paper for details.

# Websense Web Security Gateway Anywhere

In a Web Security Gateway Anywhere deployment, remote sites can be filtered by the hybrid service rather than the Websense software or appliance at the main site.

Network latency issues are addressed by the fact that a remote site and off-site users are filtered by the nearest Websense hybrid service cluster.

The following illustration shows how remote-site filtering works in Web Security Gateway Anywhere. Remote site client machines are filtered by the hybrid service directly rather than instructing the local firewall to permit or block a request. A user's request for a Web page is directed to the hybrid service, which permits or blocks the request based on the applicable policy.




Policy settings are defined at the main site and uploaded automatically to the hybrid service at preset intervals. User information, for user- or group-based filtering, is also uploaded.

Log data for reporting is downloaded from the hybrid service to the main site automatically and is incorporated into the Websense Log Database (at the main site). Thus, reports can cover users at all offices.

Off-site users are filtered by the hybrid service as well. Alternatively, off-site users can be filtered using Websense Remote Filtering Server (deployed at the main site). In that case, Websense Remote Filtering Client must be installed on each off-site user's machine. See Remote Filtering Software technical paper for details.

# Web Security distributed enterprise deployment models

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

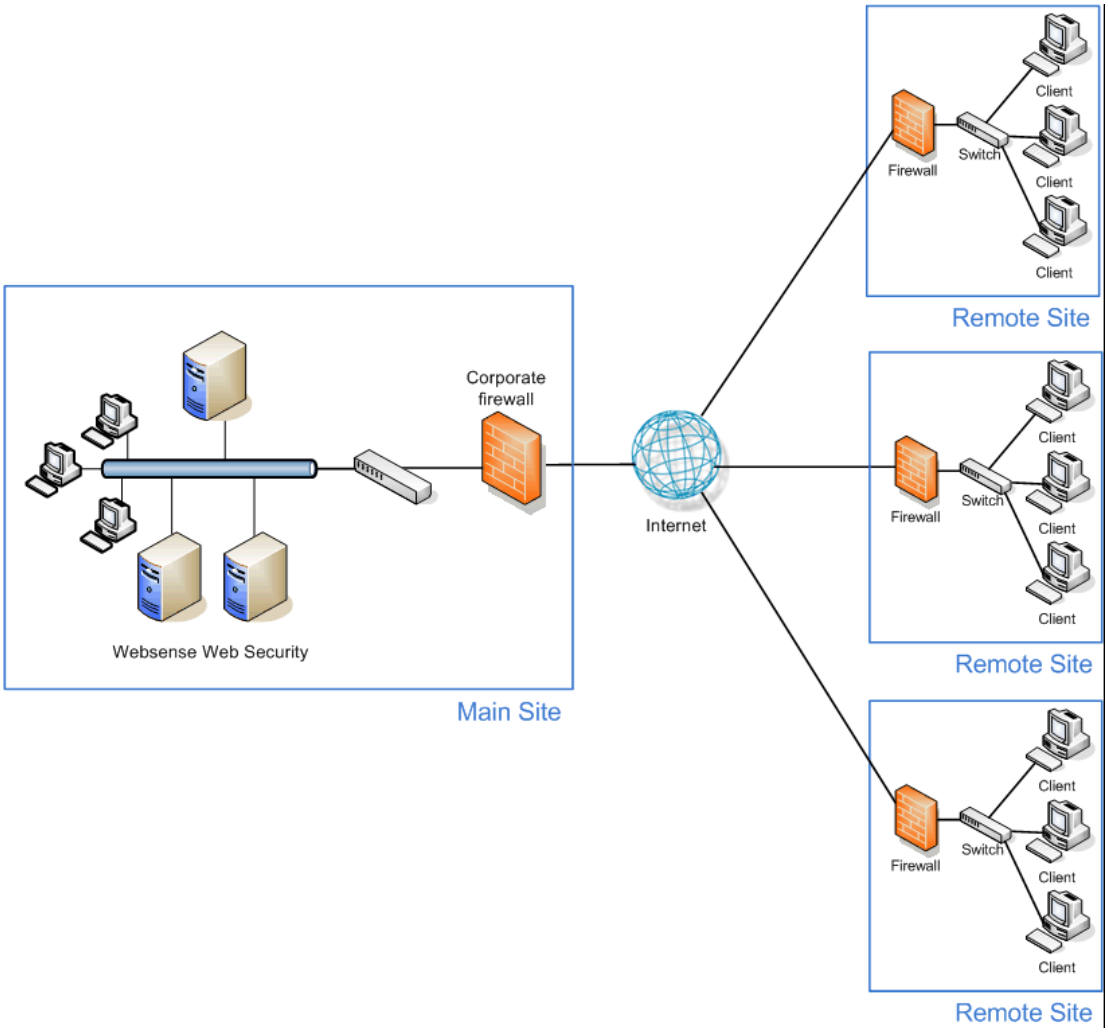
Deployment scenarios vary with different enterprise configurations. For example, an organization with 50 remote sites, all located in the same general region, deploys Websense software differently than a company with remote sites spread throughout the world. This section discusses 3 basic example models for distributed enterprises:

- *Sites in a region*, page 154: Remote sites located within one region
- *Expanding sites in a region*, page 155: Remote sites located within one region, with a growing number of employees or sites (or both)
- *National or worldwide offices*, page 157: Remote sites located nationally or globally

## Sites in a region

The simplest Websense deployment for a distributed enterprise is a network with remote sites in a single region, such as San Diego County, California, U.S.A. Most organizations with sites like this can use a single Websense Web Security or Web

Security Gateway deployment, centrally located within that region, to provide filtering for all clients. See the following illustration.




Each remote site would be filtered as shown in the illustration under *Websense Web Security or Web Security Gateway*, page 151. The site in which Websense software is deployed is represented as the "main site", but need not be truly a main site in your organization. It is whichever one houses Websense software.

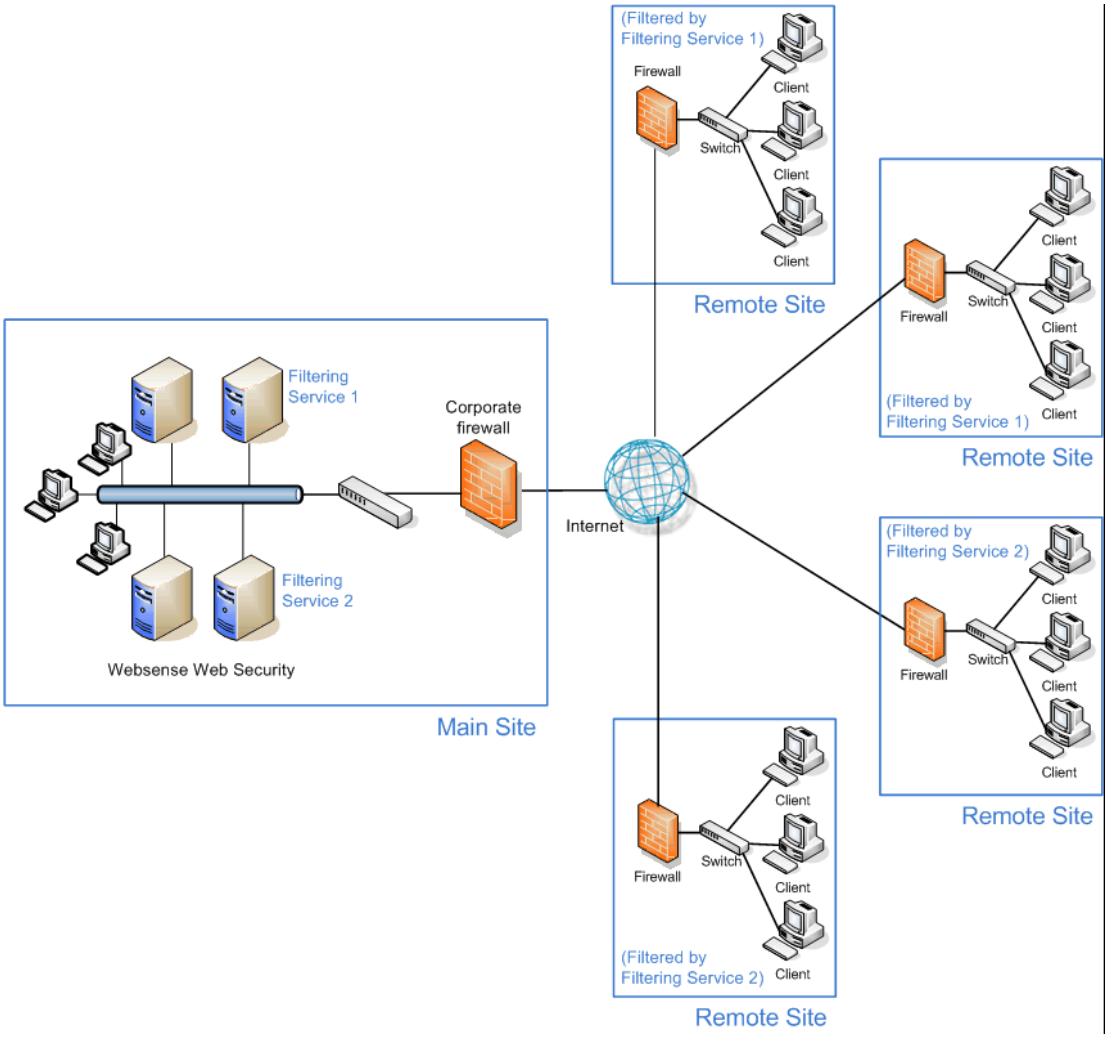
Off-site users, not shown in the above illustration, can be filtered using Websense Remote Filtering Server (deployed at the main site). Websense Remote Filtering Client must be installed on each off-site user's machine. See Remote Filtering Software technical paper for details.

## Expanding sites in a region

Some organizations deploy Web Security or Web Security Gateway within a given region and later decide to increase the number of remote sites in that area.

To compensate for the additional sites and employees, the organization can:

- **Improve the performance of the machines running Websense components**. Increasing the RAM and CPU, and installing faster hard drives on the Websense machines allows Websense software to respond to an increased number of requests without additional latency. This type of upgrade can help with a moderate increase in head count, or the addition of a few more offices.
- **Deploy additional machines to run Websense components.** If a significant number of new users or sites is added, the deployment of additional instances of certain Websense components, such as Filtering Service and Network Agent, distributes the load and provides optimum performance for each remote site..




Additional instances of Websense components can be deployed within the region as the number of offices continues to grow.

Do not install any Websense components on a domain controller.

Off-site users, not shown in the preceding illustration, can be filtered by Websense Remote Filtering Server (deployed at the main site). Websense Remote Filtering Client must be installed on each off-site user's machine. See Remote Filtering Software technical paper for details.

# National or worldwide offices

## Websense Web Security or Web Security Gateway

Some organizations have hundreds of remote sites spread through a country or around the world. In such cases, one or two Web Security or Web Security Gateway installations are not enough because:

- Each remote site would be geographically distant from the Websense components. Request lookups would have to travel farther over the Internet to reach Websense software. This distance increases the total latency of the response and may lead to slower Internet access for end users.
- Large numbers of employees generate more Internet requests than recommended for one or two Websense machines, leading to delays in returning Web pages to requesting clients.

These organizations should divide their sites into logical regions and deploy Websense software in each region. For example, a distributed enterprise might group their United States sites into a western region, a central region, and an eastern region. Websense software is deployed at a central site in each region.

The logical division of sites into regions depends on the location and grouping of remote sites and the total number of employees at each site. For example, a company with a large number of remote sites in a concentrated area, such as New York City, may need to deploy multiple machines running Websense software within that area. Or an enterprise may only have three sites in California with 100 to 250 employees each. In this case, a single Websense software installation might be deployed for all three sites. This enterprise also can deploy Websense software locally at each site (rather than using a distributed approach), particularly if IT staff is present at each location.You may consider installing instances of Filtering Service, Network Agent, and possibly Policy Server and Content Gateway to improve response time for filtering.

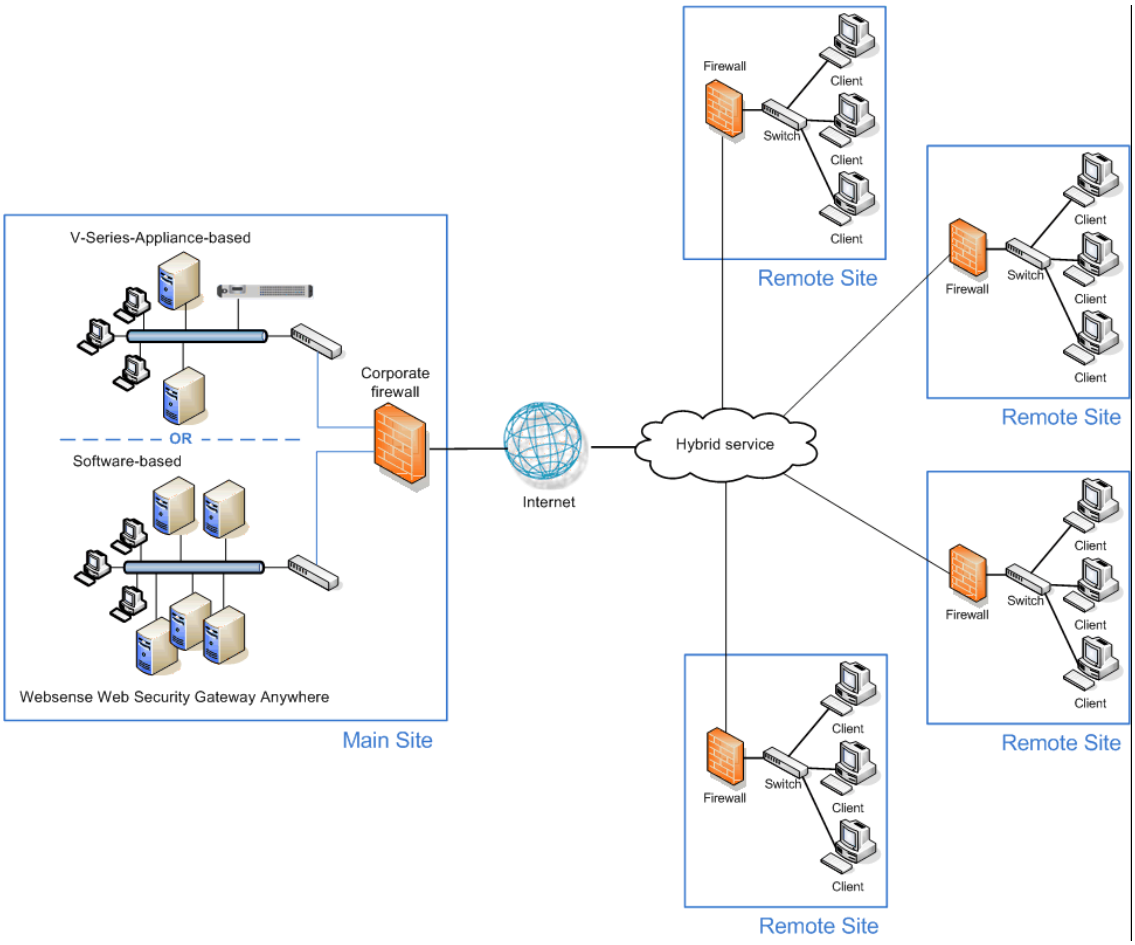
Given the significant number of variables, large organizations should contact a Websense partner or Websense Sales Engineering to plan a rollout strategy before deployment.

## Websense Web Security Gateway Anywhere

Websense Web Security Gateway Anywhere is particularly well-suited for organizations with sites distributed nationally or worldwide.

### Single main site

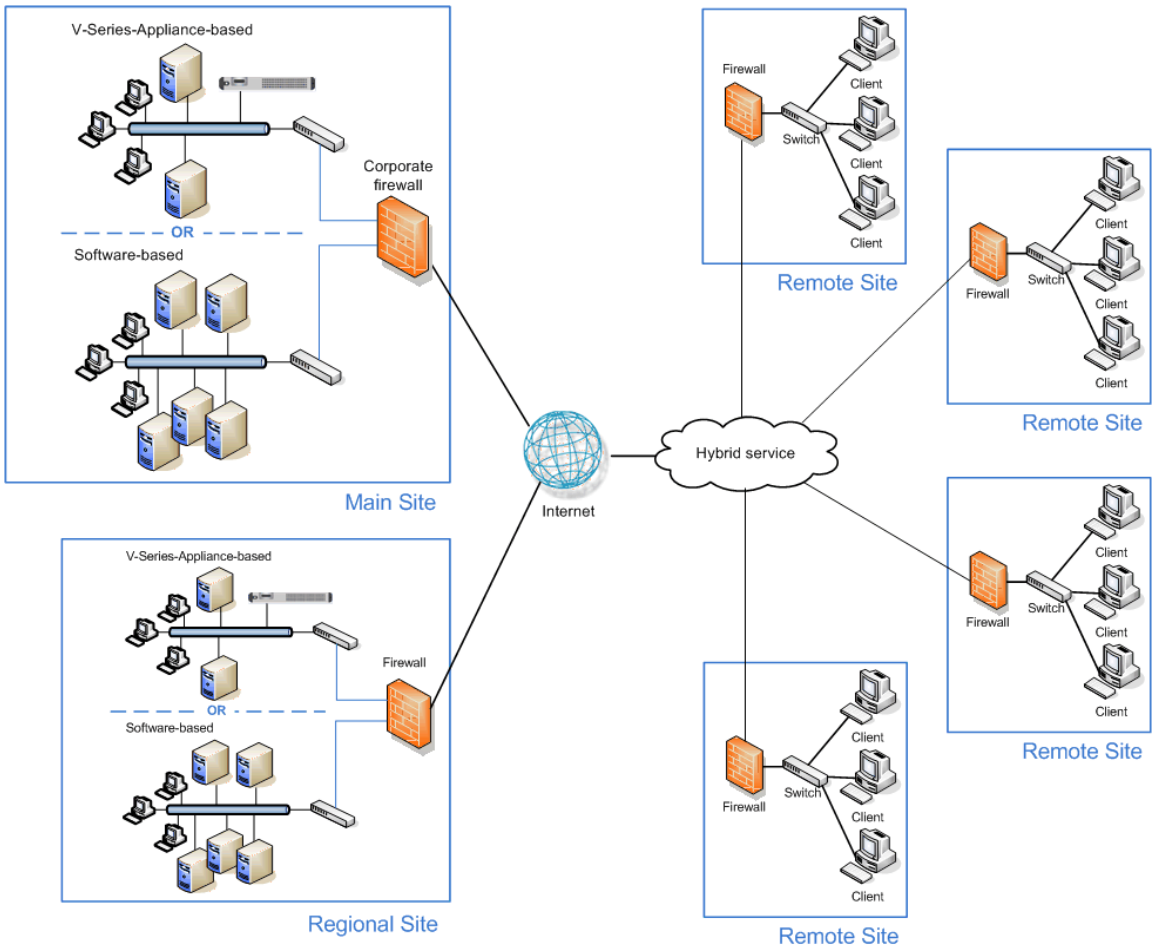
An organization with one main site (such as headquarters office or main campus) and multiple, geographically dispersed remote or branch sites can deploy Websense software at the main site (with main-site users filtered by the on-premises components) and have all remote sites filtered through the hybrid service. See the following illustration.




Off-site users, not shown in the above illustration, are filtered through the hybrid service. Alternatively, they could be filtered by Websense Remote Filtering Server (deployed at the main site). In that case, Websense Remote Filtering Client must be installed on each off-site user's machine. See Remote Filtering Software technical paper for details.

### Multiple large sites

Organizations with multiple large sites (such as main headquarters and regional headquarters) can deploy on-premises filtering at the larger sites while filtering small, remote sites through the hybrid service.




When there are multiple on-premises deployments of Web Security Gateway Anywhere components:

- There must be only one Policy Broker and one Sync Service in the entire deployment (at the main site). See *Component limits and ratios*, page 87 and the TRITON - Web Security Help for more information.
- For unified configuration and policy-application, V-Series appliances deployed at regional sites should be configured to use the appliance at the main site as the *policy source*. See the *Getting Started Guide* for Websense V-Series Appliance and the Websense Appliance Manager Help.
- All Log Server instances should be configured to send data to the main Log Database at the main site. See the TRITON - Web Security Help for more information.

Off-site users, not shown in the preceding illustration, are filtered through the hybrid service. Alternatively, they could be filtered by Websense Remote Filtering Server

(deployed at the main site or a regional site). In that case, Websense Remote Filtering Client must be installed on each off-site user's machine. See the Remote Filtering Software technical paper for details.

# Web Security distributed deployments and secure VPN connections

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## Web Security distributed deployments and secure VPN connections

For URL lookup requests and replies, some firewalls allow administrators to set up a secure VPN connection between the remote-site firewalls and Websense software. Permitted requests then are fulfilled directly from the Internet, providing an optimum combination of speed and security. See the firewall documentation to determine if the firewall supports this capability.

If a RADIUS server is being used with the VPN service, Websense RADIUS Agent can be used for transparent user identification. See *Deploying transparent identification agents*, page 91. For information about installing RADIUS Agent, see *Installing Web Security components*, page 668.

# 11 Web Security Gateway (software-based)

## Applies to

- Web Security Gateway v7.6

## In this topic



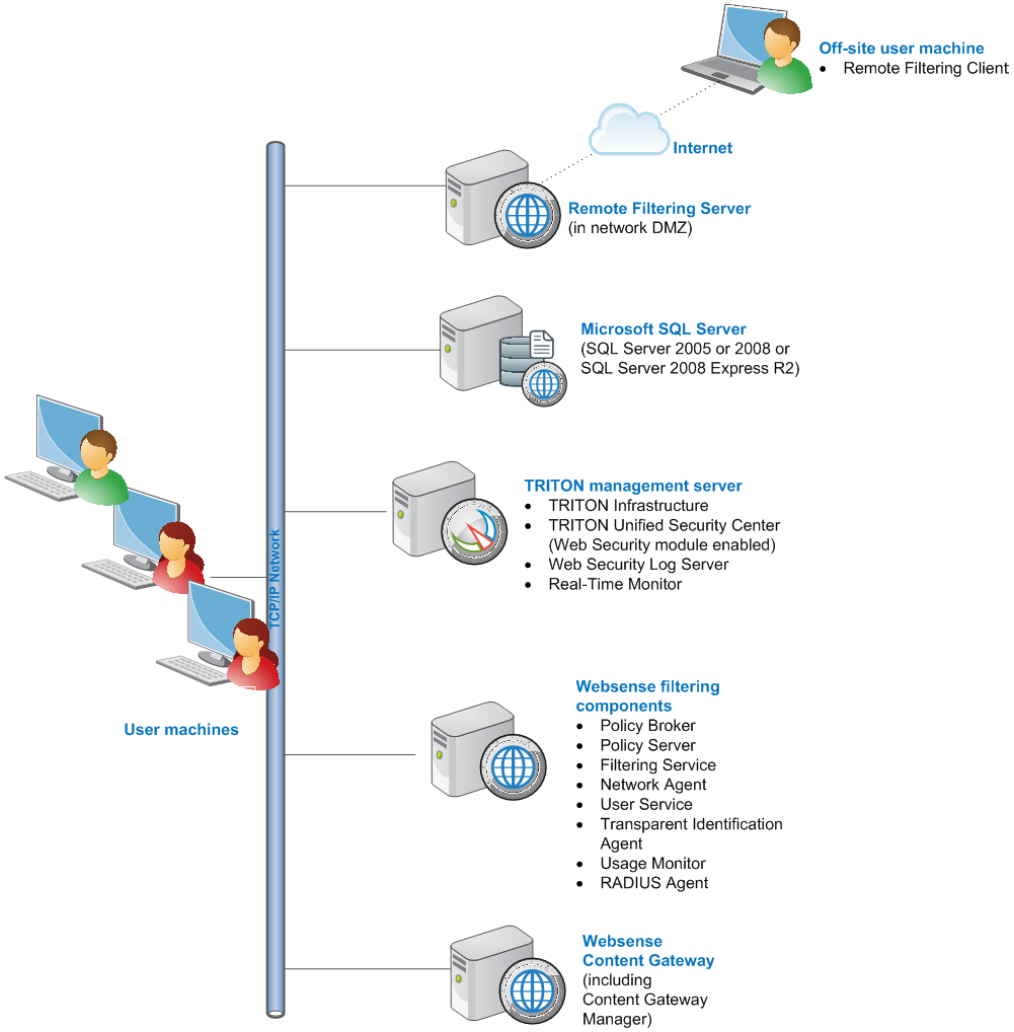
## Overview

This section contains information and instructions for a software-based deployment of Websense® Web Security Gateway. In this deployment scenario, all Websense components are installed on servers in your network. Components are typically distributed across several machines. For information about a Websense-appliance-based deployment, see *Web Security Gateway (appliance-based)*, page 405.

Websense Web Security Gateway software consists of components that work together to monitor Internet requests, log activity, apply Internet usage filters, and report on activity. Websense software is highly-distributable, providing the flexibility to scale a deployment to suit your needs. Components can be installed together on one machine for smaller organizations; or they can be distributed across mutliple machines, and multiple sites, to create a high-performing deployment for larger organizations. The appropriate deployment is determined by network size and configuration, Internet request volume, hardware performance, and filtering needs.

The following illustration is a high-level diagram of a basic software-based deployment of Web Security Gateway. Note that this illustration is intended to show

the general distribution of components and does not include network details (such as segmenting, internal firewalls, routing, switching, and so forth).




Microsoft SQL Server is used to store Websense data (including log and reporting data). SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using the Websense installer) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

*TRITON management server* is the term used to refer to the machine on which*TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON™ Infrastructure and any or all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security). Additional components may also be installed on this machine. For example, Web Security Log Server and Real-Time Monitor (note that these components may be installed on another machine; they are not required to be located on the TRITON management server).

Websense filtering components may be installed on the same machine or distributed across several machines. Additionally, you can install multiple instances (on different machines) of certain components to scale to your organization's needs.

Websense Content Gateway is a Web proxy that passes HTTP, HTTPS, FTP over HTTP, and native FTP traffic to Websense software for filtering. Content Gateway Manager—the Web-browser-based management UI for Content Gateway—runs on the Content Gateway machine, but is typically accessed from within TRITON Unified Security Center.

Websense *Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users that are outside the corporate network (e.g., traveling personnel or telecommuters).

## Deployment


- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Hardware recommendations for stand-alone deployments of Web Filter or Web Security*, page 98
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Integrating Web Security with Content Gateway*, page 126
- *Integrating Web Security with Microsoft ISA Server or Forefront TMG*, page 128
- *Integrating Web Security with Cisco*, page 132
- *Integrating Web Security with Check Point*, page 136
- *Integrating Web Security with Squid Web Proxy Cache*, page 139
- *Integrating Web Security with Citrix*, page 143
- *Other integrations for Web Security*, page 145
- *Web Security Distributed Enterprise Deployments*, page 147


## Installation

Complete the following main steps (the links go to detailed procedures or information for each step).

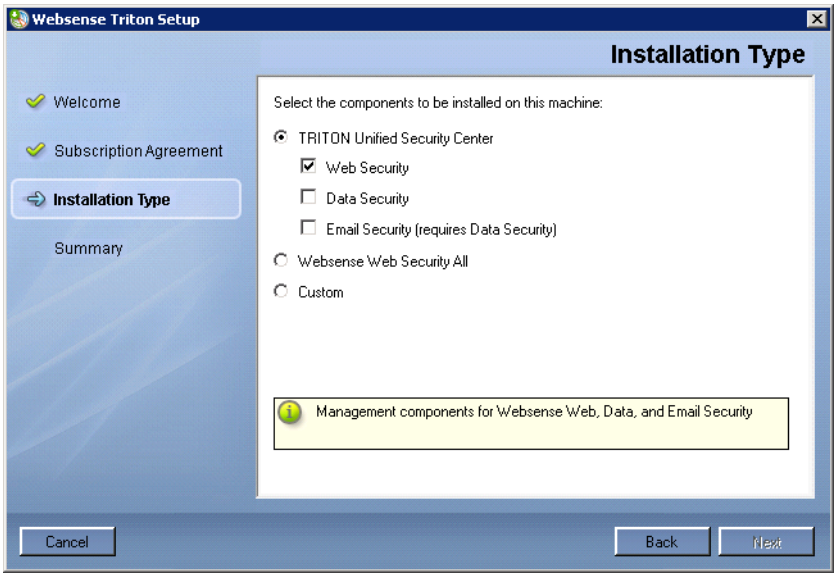

1. *Preparing for Installation*, page 55
2. *Obtaining SQL Server*, page 67

3. *Installing Web Security components*, page 668

   **Important**: Be sure to install *Policy Broker* and *Policy Server* before creating a TRITON management server (in the next step).

4. *Websense Content Gateway*, page 357
5. *Creating a TRITON Management Server*, page 645

   **Important**: When following the instructions under *Creating a TRITON Management Server*, page 645, choose to install only the Web Security module of the TRITON Unified Security Center. When you reach the **Installation Type** screen of the Websense installer, select only **Web Security** (under TRITON Unified Security Center).




You can choose to install the other modules of the TRITON Unified Security Center. However, they will be enabled only if the subscription key you enter includes those features.

# Initial configuration

- *Ports*, page 765
- *Antivirus configuration*, page 765
- *Disable Enhanced Security Configuration in Internet Explorer*, page 765
- *Accessing the TRITON Unified Security Center*, page 765
- *Entering subscription key*, page 766
- *SQL Server 2008 R2 Express*, page 766
- *Getting Started Help*, page 767
- *Windows Server 2008*, page 767
- *Logon script for Logon Agent*, page 768
- *Messenger Service for Network Agent block messages*, page 769

- *Administrator privileges for User Service, DC Agent, or Logon Agent*, page 769
- *Configuring Transparent Identification*, page 769
- *Network Agent and multiple NICs*, page 769
- *Remote Filtering*, page 769
- *Identifying Filtering Service by IP address*, page 769
- *Starting Content Gateway Manager*, page 779
- *Entering a subscription key for Content Gateway*, page 780
- *Enabling SSL Manager in Content Gateway*, page 781
- *Enabling WCCP for Content Gateway*, page 781

# 12 Citrix Integration

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## Citrix integration

This section of the Websense Technical Library provides information about integrating a software-base deployment of Websense Web Filter or Web Security with Citrix® XenApp™, Presentation Server™, or MetaFrame® Presentation Server.

> **Note**
> In this section, the term *Citrix server* is used to refer to MetaFrame Presentation Server, Presentation Server, and XenApp collectively. If information or an instruction applies to one of these products only, it is referred to by name.

Integrating Websense Web Filter or Web Security with a Citrix product involves the following components:

- **Websense Citrix Integration Service**: The Integration Service must be installed on each Citrix server to allow that server to communicate with *Filtering Service*.
- **Websense Network Agent**: Manages Internet protocols that are not managed by your Citrix server integration. It can also detect HTTP network activity and instruct Filtering Service to log this information.

> **Note**
> If your Citrix server runs applications that use protocols other than HTTP, FTP, or SSL, Network Agent can apply protocol filtering to those applications based on a computer or network policy, or the Default policy. It cannot apply user- and group-based policies to protocol filtering of applications running on the Citrix server.

See the following for information about integrating with Citrix products:



# Supported Citrix versions

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## Supported versions

The following Citrix products are supported by Websense Citrix Integration Service:

| Product | Operating System |
|---|---|
| XenApp 6.0 | Windows Server 2008 R2 |
| XenApp 5.0 | Windows Server 2008 (32- and 64-bit)<br>Windows Server 2003 (32- and 64-bit) |
| Presentation Server 4.5/4.0 | Windows Server 2003 (32-bit) |
| MetaFrame Presentation Server 3.0 | Windows Server 2003 (32-bit) |

# Citrix client computers

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

### Citrix client computers

- To be filtered by Websense Web Filter or Web Security, Citrix client computers must access the Internet through a Citrix server.
- Non-Citrix clients in the network also may be filtered by the same installation of Websense Web Filter or Web Security. This instance can be either stand-alone or integrated with another product. See *Combining Citrix with another integration*, page 186 for more information.

## Filtering Citrix server users

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

### In this topic



### Overview

Websense Web Filter or Web Security integrated with a Citrix server can monitor individual Citrix users for HTTP, HTTPS, FTP, and SSL. Network Agent can be used to filter other protocols, based on policies set for the server.

The machines running as Citrix servers communicate with Websense Filtering Service using a Websense component called the Citrix Integration Service, which is installed on the Citrix server machine.

When Websense Web Filter or Web Security is integrated with Citrix:

- The number of Citrix servers per Filtering Service may vary, and depends on user load.

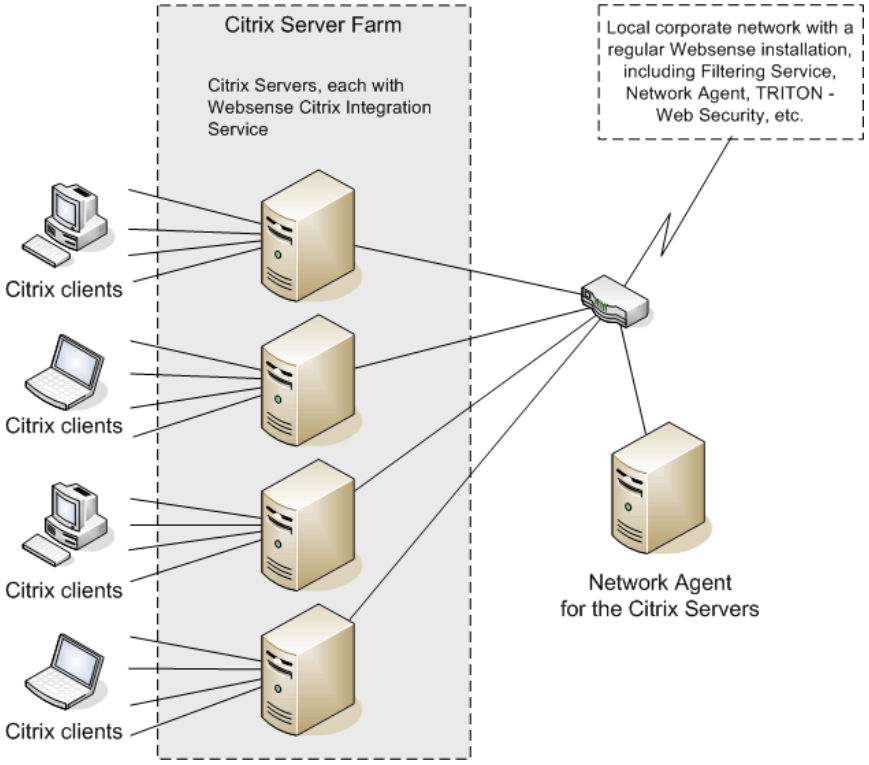
  The recommended maximum is up to 10 Citrix servers per Filtering Service.
- The Filtering Service and Network Agent monitoring Citrix traffic should be installed on a dedicated machine, and not on a Citrix server.
- The Filtering Service and Network Agent monitoring Citrix traffic use the same Policy Broker, Policy Server, User Service, and other Websense components that are used to monitor non-Citrix traffic.
- Separate Network Agents must be used to monitor non-Citrix traffic.

- Do not configure a separate Websense integration to filter HTTP, HTTPS, FTP, or SSL requests from Citrix servers.
- If you want to use Network Agent to filter protocol traffic from the Citrix Servers:
  - Network Agent must be located where it can see all of the traffic between the Citrix servers and the Filtering Service instances. For example, the machine running Network Agent could be connected to a span port on the same network switch as the machines running Filtering Service.
  - If the Citrix server is configured to use virtual IP addresses, configure Network Agent to monitor the entire range of the IP addresses. Also, a single policy should be set for this range. See the Network Configuration topic in TRITON - Web Security Help for instructions on configuring IP ranges for Network Agent.
  - If you are running Websense Web Filter or Web Security in stand-alone mode, a separate instance of Network Agent must be installed to monitor users of the Citrix servers. Do not monitor non-Citrix traffic with this Network Agent.

    While Network Agent can be used to filter protocols for Citrix, user-based and group-based policies cannot be applied. Policies can be applied to individual computers and network ranges, identified by IP addresses or IP address ranges. Otherwise, the Default policy is applied to all users.

    Also, Network Agents monitoring non-Citrix traffic (users who access the Internet without going through a Citrix server) must not be used to monitor Citrix traffic.

This diagram shows a typical deployment to filter users who access the Internet through a Citrix server. To simplify the diagram, not all individual Websense components are shown.




The main Websense filtering components are installed on a separate, dedicated machine that can communicate with all of the Citrix server machines, and non-Citrix users, if applicable. The Websense Citrix Integration Service must be installed on each Citrix server to allow it to communicate with Filtering Service. No other Websense components should be installed on the Citrix server machines.

## Filtering both Citrix and non-Citrix users

If your network includes some users who access the Internet via a Citrix server, and others who access the Internet through another gateway (firewall, caching appliance, or proxy server), the integrations can be configured to work together.

- To install the Citrix Integration Service on a Citrix Server, see page 173.
- If you have Citrix users and non-Citrix users in your network, the same Websense components, except for Network Agent, can be used for both sets of users. A separate installation of Network Agent is needed for the Citrix users. See *Installing Web Security to integrate with Citrix* for instructions.
- To configure the Websense components installed with the non-Citrix integration to communicate with Citrix, refer to the section pertaining to your integration in *Combining Citrix with another integration*, page 186.

# Installing the Citrix Integration Service

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## In this topic



## Overview

Most Websense components must be installed on a separate machine from the Citrix server. Only the Citrix Integration Service is installed on each Citrix server machine.

If you have a v7.5.x or earlier version of the Citrix Integration Service installed, you must remove it completely before deploying the version 7.6.x service. See *Upgrading Citrix Integration Service to 7.6*, page 183.

**Important**

Installing the v7.6.x Citrix Integration Service on a machine where the v7.5.x or earlier Citrix Integration Service is running does not upgrade or remove the old components. The services attempt to run concurrently, and filtering problems are likely to result.

Please make sure you have used the Windows Add/Remove tool to uninstall the prior-version Citrix Integration Service before deploying the v7.6.x service.

If Websense will be filtering both Citrix and non-Citrix users, refer to *Combining Citrix with another integration*, page 186, after installing the Websense Citrix Integration Service.

## Installing Web Security to integrate with Citrix

The core Websense Web filtering components, including Network Agent, must be installed before you install the Websense Citrix Integration Service on your Citrix servers.

> **Note**
> Only the Citrix Integration Service is installed on the Citrix server. All other Websense components must reside on a separate machine.

To prepare Web Security filtering components to integrate with Citrix:

1. When you install **Filtering Service**:
   - On the **Integration Option** screen, select **Integrated with another application or device**.
   - On the **Select Integration** screen, select **Citrix**.

   Note that while Filtering Service cannot be installed on the Citrix server, it can be installed with other Web Security components, including Policy Broker, Policy Server, and User Service.

   > **Important**
   > Because you are integrating with Citrix, do not install Network Agent on the same machine as Filtering Service.

   For detailed instructions on performing a custom installation of Web Security components, see *Installing Web Security components*, page 668.
2. Perform a custom Web Security installation to install **Network Agent** on a separate machine from Filtering Service. The Network Agent machine must be positioned where it can view traffic from Citrix users, in order to enable filtering for protocols other than HTTP, HTTPS, and FTP.

   For instructions on performing a custom installation of Web Security components, see *Installing Web Security components*, page 668.

## Installing the Citrix Integration Service on a Citrix Server

After Filtering Service is installed in Citrix integration mode, the Citrix Integration Service must be installed on every Citrix server machine in your network that will be integrated with Websense Web Security. The Citrix Integration Service can be installed only on Windows-based Presentation Servers or XenApp.

> **Important**
> Make sure any v7.5.x or earlier versions of the Citrix Integration Service are uninstalled before continuing.

Installing Citrix Integration Service is a three-stage process:

1. *Installing the Citrix configuration package*, page 174
2. *Customizing the Citrix installation package*, page 175
3. *Installing the Citrix Integration Service*, page 180

## Installing the Citrix configuration package

The Citrix configuration package can be installed directly onto the Citrix server or on a separate machine. The configuration package consists of:

- A self-extracting archive containing the Citrix configuration utility.
- A default Citrix installation package to use as a template (consisting of an MSI file, several DLLs, and configuration files).

The configuration utility is used to customize the template installation package for your deployment.

Note that if you use the Websense installer to install the Citrix configuration package directly on the Citrix server, other Websense files and utilities that are not strictly required are also installed. If you do not want these extra files on the Citrix server, you can:

- Install the Citrix configuration package on a separate machine, then use that machine to "stage" the Citrix installation package.
- Copy the Citrix configuration package from the TRITON management server (or any other Windows server that includes Web filtering components).

  By default, the files are located in the **C:\Program Files (x86)\Websense\Web Security\CitrixPlugin** directory.

The configuration utility can run on most Windows platforms, and does not have to be run on a server. Run the configuration utility on your workstation (or any convenient Windows machine) then deploy the customized Citrix installation packages to the appropriate Citrix servers. See *Customizing the Citrix installation package* for more information about configuring for multiple Citrix servers.

If you want to use the Websense installer to specifically install the Citrix configuration package, rather than copying the files from a machine where other Websense Web filtering components are installed:

> **Note**
>
> If you are running version **7.6.0**, a Citrix Integration Service hotfix is available from mywebsense.com.
>
> 1. Log on to MyWebsense and click the **Downloads** tab.
> 2. Select **Hotfixes & Patches**.
> 3. Enter your product, and version **7.6.0**.
> 4. Select the **v7.6 Citrix Plugin** hotfix to download.
> 5. Follow the instructions in the hotfix ReadMe file to complete the installation.

6. Start the Websense installer, and perform a custom Web Security installation.

   During installation:

   - On the **Select Components** screen, select **Filtering Plug-in**.
   - On the **Select Integration** screen, select **Citrix**.

   For instructions on performing a custom installation of Web Security components, see *Installing Web Security components*, page 668.

7. The Citrix configuration package is installed to **C:\Program Files (x86)\Websense\Web Security\CitrixPlugin\32-bit** or **64-bit**, by default.

   Note that there are 32- and 64-bit versions of the configuration package. Be sure to use the version appropriate for the target Citrix server's operating system. For example, if the Citrix server is running on Windows Server 2008 R2, you should use the 64-bit endpoint package.

## Customizing the Citrix installation package

The Citrix configuration package is a self-extracting archive containing the Citrix configuration utility and a default Citrix installation package (consisting of an MSI file, several DLLs, and configuration files) to use as a template. The configuration utility is used to customize the installation package for your deployment.

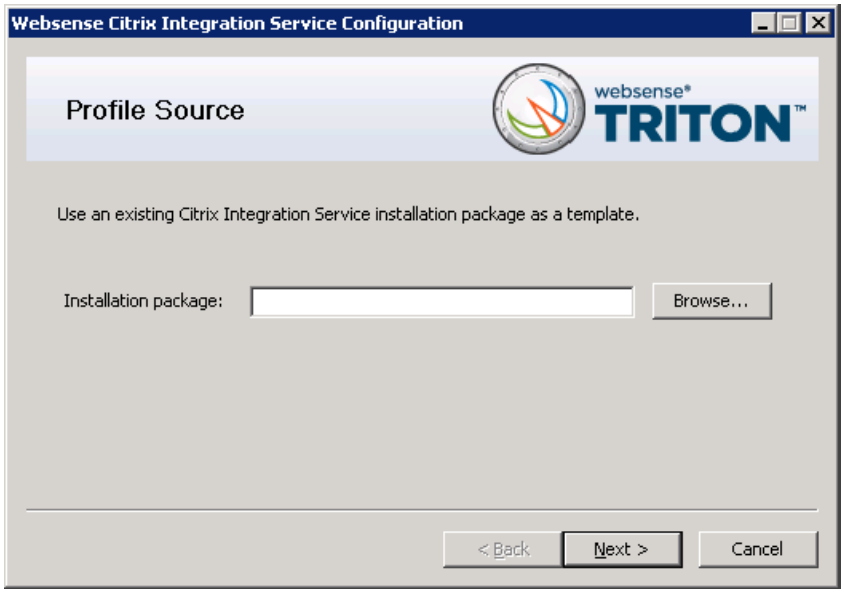
1. Navigate to the folder containing the appropriate configuration package (32-bit or 64-bit), then double-click the self-extracting executable and click **Extract**. The configuration package self-extracting executables are:

   - **WCISUtil_Win32_*nnnn*.exe** (32-bit)
   - **WCISUtil_x64_*nnnn*.exe** (64-bit)

2. To launch the configuration utility, double-click **Websense Citrix Integration Service Configuration.exe**.

   **Important**
   Both the 32- and 64-bit versions of the configuration utility have the same name. Make sure you are in the correct folder.

3. On the **Profile Source** screen, click **Browse**, then navigate to the folder containing the Citrix installation package.



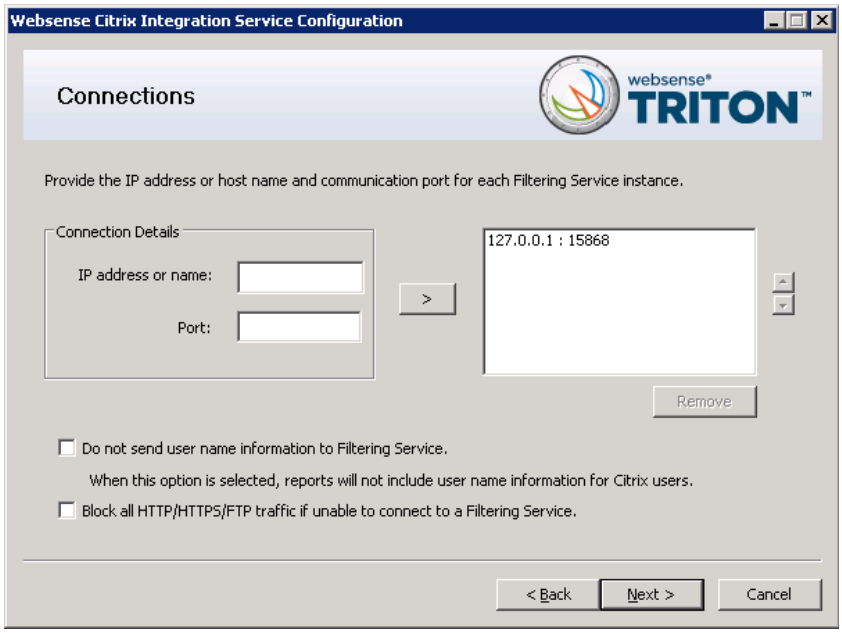

   The template package is located in the C:\Program Files (x86)\Websense\Web Security\CitrixPlugin\32-bit or 64-bit folder.

4. Click **Next**.

   If an error message alerts you that "The selected installation package does not include all of the necessary files," make sure that all files from the extracted Citrix configuration package are present in the specified directory.

   A complete list of files is provided at the start of the next section, *Installing the Citrix Integration Service*, page 180.

5. On the **Connections** screen, specify all Filtering Service instances the Citrix server should use for Web filtering, then click **Next**.




   a. If **127.0.0.1:15868** appears (as shown above), select the entry and click **Remove**.

      This should not be used because Filtering Service should never be installed on the Citrix server machine.

   b. Add the IP address and port (15868, by default) for each Filtering Service you want the Citrix Server to use, then click the right arrow key to add it to the selected list.

> **Note**
>
> The port Filtering Service uses to communicate with integration products and Network Agent must be in the range 1024-65535. To determine which port Filtering Service is using, check the **eimserver.ini** file—located in C:\Program Files\Websense\Web Security\bin (Windows) or /opt/Websense/bin (Linux)—on the Filtering Service machine. Look for the **WebsenseServerPort** value.
>
> **Important**: Do not modify the eimserver.ini file.

Multiple Filtering Service instances might be specified in case one instance is down. If the first Filtering Service is not available, the Citrix Integration Service attempts to contact the next instance in the list.

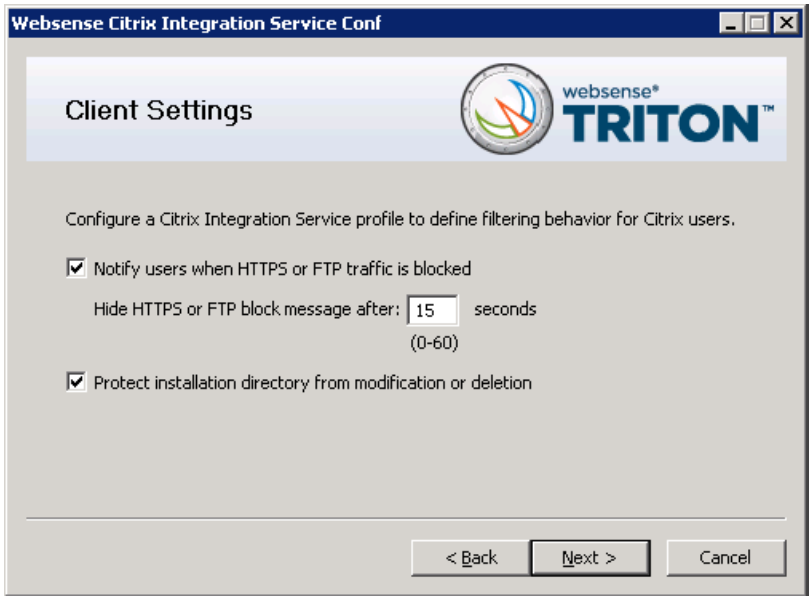
> **Note**
> Each Filtering Service instance tracks continue, quota, and password override information independently. If the Citrix Integration Service fails over from one Filtering Service instance to another, usage quotas may be different and override passwords may need to be entered again.

If no Filtering Service instance responds, the Citrix Integration Service continues to attempt communication every 1 minute. Until communication is established, the Citrix Integration Service either permits all requests (fails open) or blocks all requests (fails closed), depending on your configuration. See Step d.

c. If you do not want user names (when available) to be sent to Filtering Service for use in filtering and logging, select **Do not send user name information to Filtering Service**. This selection applies to all Filtering Service instances listed.

d. If you want the Citrix Integration Service to fail closed when it cannot contact Filtering Service, select **Block all HTTP/HTTPS/FTP traffic if unable to connect to a Filtering Service**.

6. On the **Client Settings** screen, configure user notification and anti-tampering controls, as described below, then click **Next**.




- **Notify users when HTTPS or FTP traffic is blocked**: When this option is enabled, users see a pop-up message when HTTPS or FTP traffic is blocked. If you enable this option, specify how long the pop-up message should stay visible to the user.

- **Protect installation directory from modification or deletion**: This option prevents tampering with the Citrix Integration Service on the Citrix server. Attempts to delete it, replace files, or modify registry entries are not allowed.

7. On the **Trusted Sites** screen, specify any URLs or domains that should not be filtered, then click **Next**.


a. Click **Add**.

b. In the dialog box that appears, enter a URL or a regular expression specifying a set of URLs. Any regular expression adhering to ISO/IEC TR 19768 (within the character-number limit) is valid.

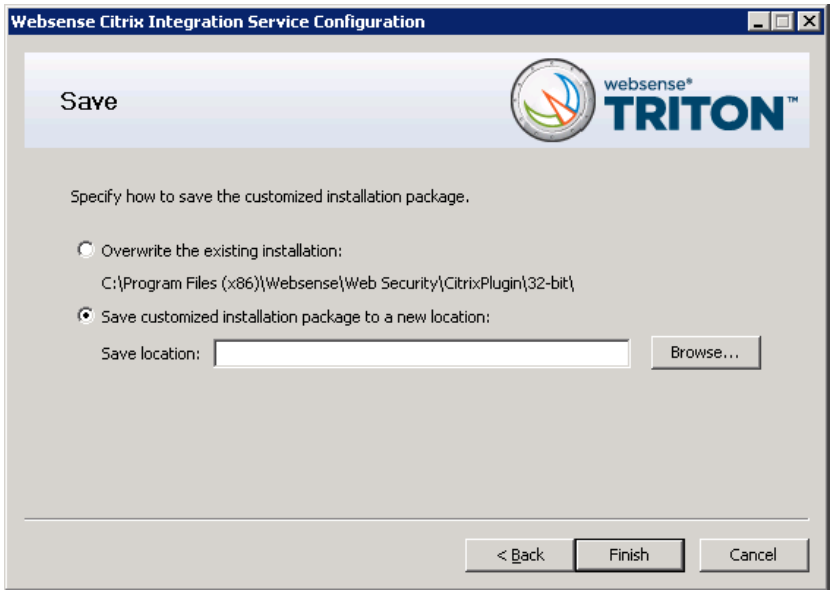
c. Click **OK**.

To edit a URL or regular expression, select it and then click **Edit**.

To remove a URL or regular expression, select it and then click **Remove**.

Note that the URLs you specify here are trusted by the particular Citrix server on which this Citrix Integration Service will be installed. It has no bearing on how Filtering Service instances filter requests from non-Citrix users and other Citrix servers not using the same Citrix Integration Service configuration.

8. On the **Save** screen, specify how you want the customized installation package saved, then click **Finish**.




- **Overwrite the existing installation**: Select this option to overwrite the Citrix installation package you used as a template. This is the package residing in the folder you selected in Step 3, page 176.
- **Save the customized installation package to a new location**: Select this option to save the customized installation package to a different location. Click **Browse**, and select the folder to which you want to save (note that the folder must already exist; if not, use a Windows file explorer to create the folder). The package you used as a template remains unchanged (unless you choose to save to the same folder). It is a best practice to save to an empty folder. Then, you can be certain that all files in that folder are part of the installation package.

The Citrix installation package is now ready for use to install Citrix Integration Service.

If you have multiple Citrix servers for which you want different customized settings, repeat this procedure, starting at Step 2, to create an installation package for each. Save each customized installation package to different folders.

## Installing the Citrix Integration Service

A Citrix installation package consists of the following files:

- 0x0409.ini
- CI.cab
- CIClientConfig.hsw
- CIClientMessage.hsw
- setup.exe

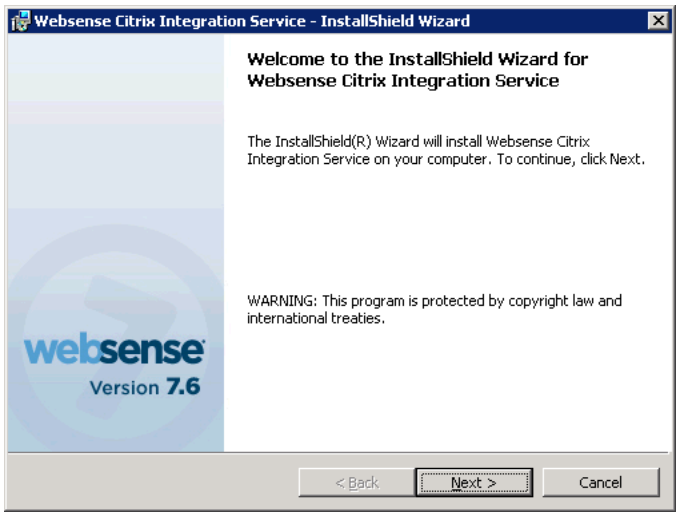
- Setup.ini
- Websense Citrix Integration Service.msi
- WEP.cab

> **Note**
> If you want to use the same Citrix Integration Service configuration on multiple Citrix servers, use the same Citrix installation package for all of them.

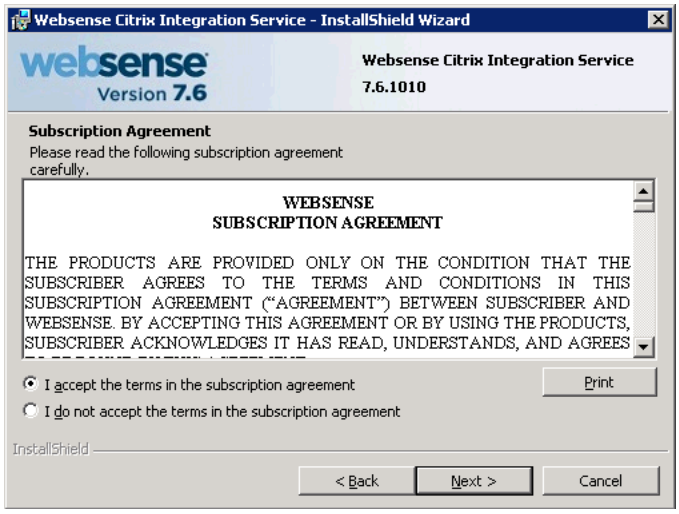
To install the Citrix Integration Service.

1. Log on with **local** administrator privileges to the machine running Citrix Presentation Server, MetaFrame Presentation Server, or XenApp.
2. Close all applications and stop any antivirus software.
3. Copy the Citrix installation package (all files listed above) to the Citrix server. Keep the files in the same folder.

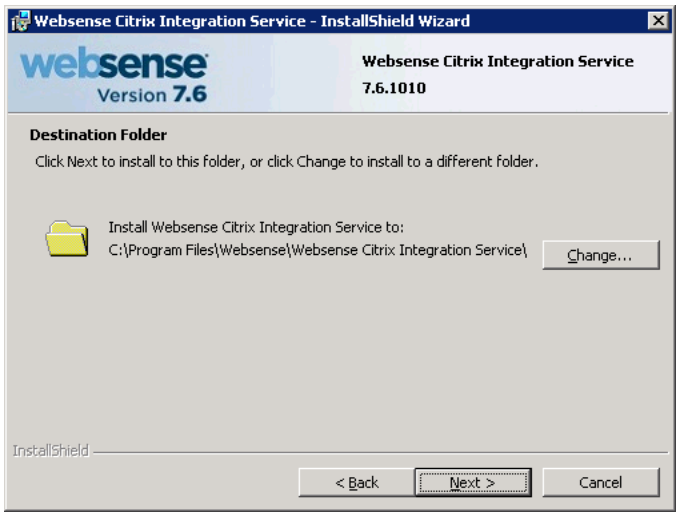
   If you installed the Citrix endpoint package to the Citrix server itself, and customized the installation package there, skip this step.
4. Double-click **setup.exe** to start the Citrix Integration Service installer. When the installer starts, click **Next**.



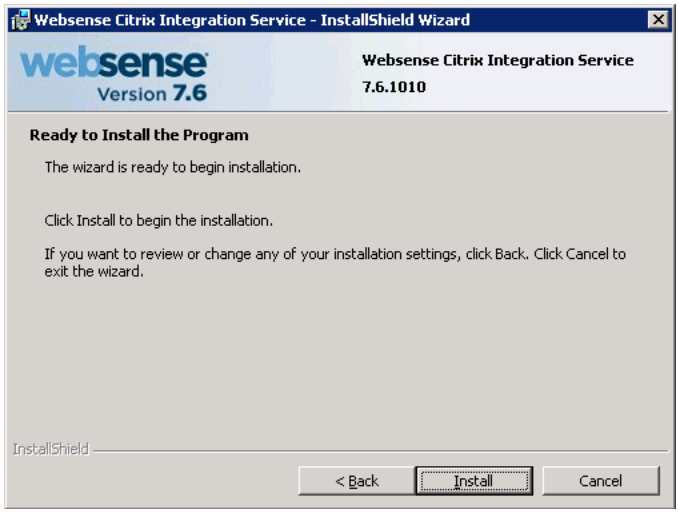
5. on the **Subscription Agreement** screen, click **I accept the terms in the subscription agreement**, then click **Next**.



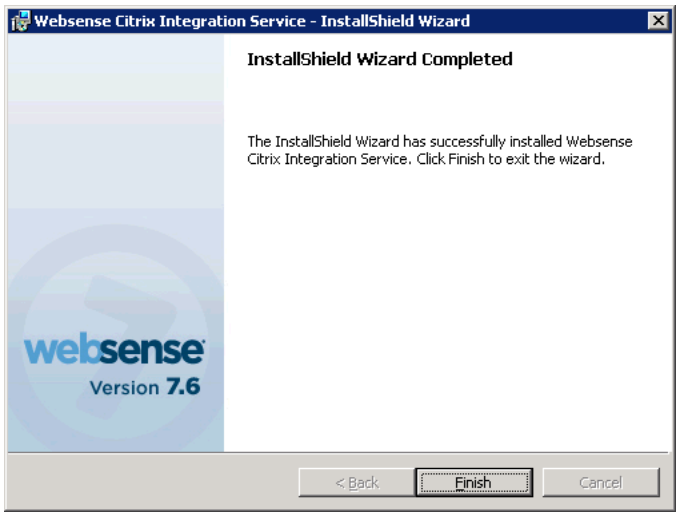

6. On the **Destination Folder** screen, accept the default location shown or click **Change** to select a different location, then click **Next**.



7. On the **Ready to Install the Program** screen, click **Install** to install the Citrix Integration Service.




8. Wait until the **InstallShield Wizard Completed** screen appears, then click **Finish**.




9. If you stopped your antivirus software, be sure to start it again.

# Upgrading Citrix Integration Service to 7.6

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## Upgrading Citrix Integration Service to 7.6

The Websense v7.6 filtering plug-in for Citrix Presentation Server has been redesigned so it is not upgradable. Earlier Citrix plug-ins must be removed before you upgrade Web filtering components, then reinstalled after the upgrade is complete.

To move from a previous version of the Citrix Integration Service to v7.6:

1. Use the Windows Control Panel to uninstall the prior-version Citrix Integration Service.
   - Windows 2003: Start > Control Panel > Add or Remove Programs.
   - Windows 2008: Start > Control Panel > Programs > Uninstall a program.
2. When the uninstall process is complete, make sure that the Websense installation directory was removed.
3. Upgrade the core Websense Web Security components to the current version.

   See *Upgrading Web Security or Web Filter to 7.6.0*, page 829.

   **Warning**
   Do **not** run the version 7.6 Websense installer on the Citrix machine. A separate tool is used to create installation packages for the Citrix Integration Service. See the next step.

4. Use a custom Citrix installation package (created using the Citrix Integration Service Configuration utility) to install the new Citrix Integration Service.

   See *Installing the Citrix Integration Service*, page 172.

# Configuring user access on Citrix servers

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## In this topic

## Overview

To allow Websense Web Filter or Web Security to apply policies to individual users and groups defined in a directory service, you must configure user access for your published applications in Citrix. The procedure varies according to the Citrix version.

## Citrix Presentation Server v4.0

User access is configured in the Citrix Publish Application wizard. See the Citrix documentation for more information on this wizard.

1. Log on to the Citrix server as an administrator.
2. Open the Publish Application wizard.
3. Go to the Specify Users screen.
4. Specify all users who can access the application so that they must log on with **domain** credentials.

**Important**

- Do **not** allow users to log on with local or administrative credentials.
- Do **not** allow anonymous connections.

## Citrix Presentation Server v4.5 and XenApp 5.0

Following is an overview of the procedure for configuring user access in Citrix Presentation Server v4.5. For XenApp 5.0, the process is similar. See Citrix documentation for more information on this wizard or for information about XenApp 6.0.

1. Log on to the Citrix server Access Management Console as an administrator.
2. Select **Applications** in the left navigation pane, or select a particular application you have published.
3. Under **Other Tasks**, select **Permissions**.
4. Click **Add** in the Permissions for folder “Applications” dialog box.
5. Click **Add** in the Add access to folder dialog box.
6. Select the computer or domain for adding users, and select the **Show users** check box.
7. Select a user, and click **Add** to move that user into the Configured Accounts list.
8. Repeat step 7 to add other users to the Configured Accounts list.
9. Click **OK** twice to save the newly added users.

If you need to change the permissions for a user, use the Edit button in the Permissions for folder “Applications” dialog box.

**Important**

- Do **not** allow users to log on with local or administrative credentials.
- Do **not** allow anonymous connections.

# Initial Setup of Citrix integration

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## In this topic



## Configuring for Citrix Virtual IP Addresses

If an integrated Citrix server is configured to use virtual IP addresses, you must configure Network Agent to monitor the entire range of the IP addresses.

You should also set a single Websense filtering policy for this range of virtual IP addresses.

See the Network Configuration topic in TRITON - Web Security Help for instructions on adding and editing IP address ranges for Network Agent, and configuring policies for specific IP address ranges.

## Combining Citrix with another integration

Websense Web Filter or Web Security can be set up to filter both Citrix and non-Citrix users. This section provides instructions for configuring Websense Web Filter or Web

Security (deployed either as stand-alone or integrated with another integration product) to work with the Citrix integration product.

Some configurations allow a single installation of Websense Web Filter or Web Security in the same network to filter both Citrix users and non-Citrix users. Citrix users may be working from remote locations, while non-Citrix users may be located in the office where Websense Web Filter or Web Security is installed.

## Deployment scenarios

The corporate network (non-Citrix users) can access the Internet through an integration product, such as Cisco® PIX®; Check Point®; Microsoft® Internet Security and Acceleration (ISA) Server or Forefront TMG; or Network Agent (in a stand-alone deployment of Websense Web Filter or Web Security, Network Agent serves in the place of an integration product). The integration product sends Internet requests to Websense Web Filter or Web Security for filtering.

Citrix clients access the network through a Citrix Presentation Server, MetaFrame Presentation Server, or XenApp. Depending on the number of Citrix users, the access may be through one server, or through a server farm consisting of multiple Citrix servers. For more information on deploying Websense Web Filter or Web Security with Citrix, see *Filtering Citrix server users*, page 169.

Websense filtering is accomplished by installing the Websense Citrix Integration Service on each Citrix server. See *Installing the Citrix Integration Service*, page 172, for instructions.

In lower volume networks, each Integration Service communicates with the same Filtering Service. The non-Citrix users can be pointed to the same instance of Filtering Service as the Integration Service.

## Deploying with Network Agent

If Websense Web Filter or Web Security is deployed as stand-alone, using Network Agent for filtering, separate instances of Network Agent are needed for the Citrix and non-Citrix users. See *Stand-Alone Websense Web Filter or Web Security configuration*, page 190 for configuration information.

## Configuration

If Websense Web Filter or Web Security is used to filter both Citrix users and users accessing the Internet through another integration product, the non-Citrix integration must be installed and running before integrating with the Citrix product.

1. Install Websense Web Filter or Web Security as integrated with the non-Citrix integration product first. See Installing Websense Web Filter or Web Security to integrate with the non-Citrix product.
2. Ii ns tall the Websense Citrix Integration Service on each Citrix server. See *Installing the Citrix Integration Service*, page 172, for instructions.

   This component sends requests from Citrix clients to Filtering Service for filtering. Up to 10 Integration Services can be pointed to the same Filtering

Service. If more than 10 Citrix servers are deployed, then additional Filtering Services can be used.

3. Configure the non-Citrix integration product, as described in this chapter, to ensure that requests coming from the Citrix clients are not filtered twice.

### Installing Websense Web Filter or Web Security to integrate with the non-Citrix product

Before the Citrix environment can be integrated, Websense Web Filter or Web Security must have been installed integrated with the non-Citrix integration product. If an older version of Websense Web Filter or Web Security is already installed, upgrade it first.

Websense Web Filter or Web Security installed in stand-alone mode uses Websense Network Agent in place of a third-party integration product.

The Websense Technical Library (www.websense.com/library) provides instructions for integrating Websense Web Filter or Web Security with supported integration products.

Only the following integration products may be combined with a Citrix integration:

- Cisco PIX v6.3. See *Cisco PIX configuration*, page 188.
- Check Point FireWall-1 NGX. See *Check Point FireWall-1 configuration*, page 189.
- Microsoft Internet Security and Acceleration (ISA) Server 2006 or Forefront TMG. See *Microsoft ISA Server/Forefront TMG configuration*, page 189.
- Network Agent (i.e., Websense Web Filter or Web Security in stand-alone mode). See *Stand-Alone Websense Web Filter or Web Security configuration*, page 190.

## Configuring the non-Citrix integration

Before the integrations can be used together, the non-Citrix integration must be set up to prevent Internet requests sent via the Citrix servers from being filtered twice.

A request from a Citrix client is passed to the Citrix server. The Citrix Integration Service sends the request to Filtering Service for filtering. The request is either blocked or permitted by Websense Web Filter or Web Security. Simultaneously, the Citrix server sends the same request to the non-Citrix integration, which must be configured to allow the request to pass to the Internet without sending it to Websense Web Filter or Web Security for filtering.

### Cisco PIX configuration

Use a console or TELNET session to configure your Cisco PIX Firewall (security appliance). This configuration has been tested for Cisco PIX version 6.3 and later.

1. Access the security appliance and enter your password.
2. Put the security appliance into privilege EXEC mode by entering `enable`, followed by your enable password.

3. To activate the configure mode, enter `configure terminal`.

> **Note**
> For help with individual commands, enter `help` followed by the command. For example, `help filter` shows the complete syntax for the filter command, and explains each of the options.

4. Use the **filter url except** command with the IP address or addresses for the Citrix servers to disable the second filtering by Websense Web Filter or Web Security of requests from Citrix users.
   - For a group of Citrix servers in a server farm, you can enter a range:

     **`filter url except`** <*IP address range*>
   - For one or two Citrix servers, you can add the commands individually:

     **`filter url except`** <*internal IP address*> <*internal subnet mask*> <*external IP address*> <*external subnet mask*>

     Here, the *internal IP address* and *subnet mask* refer to the Citrix server, and the *external IP address* and *subnet mask* are for a secondary machine, other than the PIX firewall, that is used for Internet access. The external settings are generally set to zero:

     `0.0.0.0 0.0.0.0.`
5. Type **exit** to leave configure mode.

   See Cisco's PIX documentation and the Websense Technical Library (www.websense.com/library) for more information on this integration.

### Check Point FireWall-1 configuration

To configure Check Point FireWall-1 to work properly with a Citrix integration, you must define a rule on FireWall-1 to allow requests from the Citrix server to pass to the Internet without sending those requests to Websense Web Filter or Web Security for filtering.

- Using the Firewall-1 SmartDashboard™ (or Policy Editor in older versions) add the Citrix Presentation Servers to the Allow Rule. Do **not** add the Presentation Servers to the Block rule.

See Check Point's FireWall-1 documentation and the Websense Technical Library (www.websense.com/library) for more information.

### Microsoft ISA Server/Forefront TMG configuration

The Websense ISAPI plug-in must be set to ignore traffic from the Citrix servers. This configuration is done by adding the host name of each Citrix server to the **isa_ignore.txt** file on the Microsoft ISA Server/Forefront TMG (ISA/TMG) machine.

Also, ensure that none of the Citrix servers are set to use the ISA/TMG machine as a proxy server.

1. On the ISA/TMG machine, go to the **WINDOWS\system32** directory and open the **isa_ignore.txt** file in a text editor.

   > **Note**
   > The default **isa_ignore.txt** file installed with Websense Web Filter or Web Security contains the following URL: **url=http://ms_proxy_intra_array_auth_query/**
   >
   > Do not delete this URL. It is used by ISA/TMG machines in a CARP array for communication. This URL must be ignored by Websense Web Filter or Web Security to allow filtering and logging to work properly when multiple ISA Servers are deployed in an array.

2. Enter the host name for each Citrix server on its own line in the **isa_ignore.txt** file.

   > **Important**
   > You must enter each host name in the exact same format that ISA/TMG passes it to Filtering Service.

   Use the following format: **hostname=**<*host_name*>

   Replace <*host_name*> with the name of the Citrix server machine.

3. Restart the ISA/TMG machine.

See Microsoft's ISAPI documentation and the Websense Technical Library (www.websense.com/library) for more information.

### Stand-Alone Websense Web Filter or Web Security configuration

If Websense Web Filter or Web Security is running in stand-alone mode, separate instances of Network Agent must be installed to filter Citrix and non-Citrix users. The Network Agent monitoring non-Citrix users must be set to ignore the Citrix servers. This configuration allows protocol filtering of both Citrix and non-Citrix requests.

1. Open TRITON - Web Security, and go to **Settings** > **Network Agent**.
2. In the left navigation pane, select the IP address of the NIC used for monitoring Internet requests to open its Local Settings page.
3. Under **Monitor List Exceptions**, add each Citrix server that Network Agent should exclude from monitoring.
   a. To identify a machine, click **Add**, and then enter the Citrix server's IP address, or a range of IP addresses for a group of Citrix servers in a server farm. Then, click **OK**.
   b. Repeat this process until all Citrix servers have been added, either individually or as part of a range.
4. Click **OK** to cache your changes and return to the NIC Settings page. Changes are not implemented until you click **Save All**.

See the Network Agent section under the Network Configuration topic in TRITON - Web Security Help for instructions on configuring NIC settings.

# 13 Cisco Integration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



Related topics:



## Overview

Web Filter and Web Security can be integrated with Cisco® Adaptive Security Appliance (ASA), Cisco PIX® Firewall, Cisco IOS routers, and Cisco Content Engine.

Integrating with a Cisco product involves the following components:

- **Filtering Service**: The integrated Cisco product and Network Agent work with Filtering Service to filter Internet requests. For redundancy, two or more instances of Filtering Service may be used. Only one instance will be active at any given time—referred to as the primary server. URL look-up requests will be sent only to

the primary server. For more information see the configuration chapter, in this supplement, for your Cisco product. Also see Cisco documentation for detailed explanations of configuration commands.

- **Network Agent**: Manages Internet protocols that are not managed by your integrated Cisco product. Network Agent can also provide information for reports on bandwidth and block HTTP(S) internet requests based on bandwidth consumption.

  If Network Agent is installed, you must define the IP addresses of all proxy servers through which computers route their Internet requests. See *Network Configuration* in the TRITON - Web Security Help for instructions.

- **Configure your Cisco integration**: You must direct Internet requests through your Cisco integration product, and configure it for use with Websense software.
  - *Configuring a Cisco Security Appliance*, page 199 discusses Cisco PIX Firewall and Adaptive Security Appliance (ASA)
  - *Configuring a Cisco IOS Router*, page 211 discusses Cisco IOS router.
  - *Configuring a Cisco Content Engine*, page 219 discusses Cisco Content Engine.
- **User authentication**: If HTTP(S) or FTP authentication are enabled on Cisco ASA, IOS router or Cisco content, the Websense User Service component must be installed in the same domain (Windows), or the same root context (LDAP) as authenticated users, in order to get correct user information and provide it to filtering service component for accurate user-based filtering.

  If you are using a Websense transparent identification agent or manual authentication, this configuration is not necessary.

## How Websense filtering works with Cisco products

To be filtered by Websense software, a client's Internet requests must pass through the Cisco product.

- If Websense software is integrated with a Cisco PIX Firewall or ASA, browser requests must go through the PIX Firewall or ASA to reach the Internet.
- If Websense software is integrated with a Cisco Content Engine, client browser requests may be forwarded to the Content Engine transparently or explicitly. See *Cisco Content Engine and browser access to the Internet*, page 224.

When it receives an Internet request, the Cisco product queries Filtering Service to determine if the requested Web site should be blocked or permitted. Filtering Service consults the policy assigned to the user. Each policy designates specific time periods and lists the category filters that are applied during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database.

- For HTTP, if the site is assigned to a blocked category, the user receives a block page instead of the requested site.

- For HTTPS or FTP, if the site is assigned to a blocked category, the user is not allowed access and recieves a blank page.
- If the site is assigned to a permitted category, Filtering Service notifies the Cisco product that the site is not blocked, and the client is allowed to visit the site.

> **Note**
> Before enabling Websense URL filtering, make sure there is not another URL filtering scheme configured, such as N2H2. There can be only one active URL filtering scheme at a time.

## Supported Cisco integration product versions

See *System Requirements*, page 41 for which Cisco products are supported for integration with Web Security or Web Filter.

## Installation of Web Filter or Web Security

Install Web Filter or Web Security as directed in *Web Filter or Web Security (software-based)*, page 69. When installing Filtering Service, be sure to do the following.

- On the **Integration Option** screen, select **Integrated with another application or device**.
- On the **Select Integration** screen, select one of the following and then click **Next**:
  - **Cisco Adaptive Security Appliances**
  - **Cisco Content Engine**
  - **Cisco PIX Firewall**
  - **Cisco Routers**
- Do not install a transparent identification agent if you plan to configure user authentication through your Cisco product.

  In a Web Security All installation, the **Transparent User Identification** screen is used to select a transparent identification agent. Select **Do not install a transparent identification agent now** if you will authenticate users through your Cisco product.

  In a custom installation (or when adding components), on the **Select Components** screen, do not select any of the components under **User identification** if you will authenticate users through your Cisco product.

# Upgrading Websense Web Filter or Web Security

When Websense software, already integrated with a Cisco product, is upgraded no additional configuration is necessary on the Cisco product. See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for upgrading instructions.

If you are upgrading your Websense deployment and changing your Cisco product, see *Migrating between integrations after installation*, page 196.

# Migrating between integrations after installation

You can change the Cisco integration product (for example, change from a PIX Firewall to an IOS router) after installing Websense software without losing configuration data.

1. Install and configure your new Cisco integration product. See Cisco documentation for instructions.

   Ensure that it is deployed so that it can communicate with Filtering Service.
2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
3. Close all applications on the Filtering Service machine, and stop any antivirus software.
4. Remove Filtering Service. See*Removing Web Security components*, page 808 for instructions.
5. Restart the machine (Windows only).
6. Use the Websense installer to reinstall Filtering Service. See *Installing Web Security components*, page 668 for instructions.
7. On the **Select Integration** screen, select the new Cisco product, and then follow the on-screen instructions to complete the installation.

   The installer adds the new integration data to the Websense software configuration files, while preserving existing configuration data.
8. Restart the machine (Windows only).
9. Check to be sure that Filtering Service has started.
   - Windows: Use the Windows **Services** dialog box to verify that **Websense Filtering Service** has started.
   - Linux: Navigate to the Websense installation directory (/opt/Websense, by default), and use the following command to verify that **Websense Filtering Service** is running:

     ```
     ./WebsenseAdmin status
     ```

   For instructions on starting Websense services, see *Starting or Stopping Web Security Services*, page 923.

10. In the TRITON Unified Security Center, in the Web Security module, identify which Filtering Service instance is associated with each Network Agent.
    a. Using a supported browser (see *System Requirements*, page 41), go to **https://<IP address>:9443/triton**. Where <IP address> is the IP address of the machine on which TRITON Unified Security Center is installed.
    b. Click the **Web Security** module button.
    c. Open the **Settings** tab.
    d. Go to **Settings > Network Agent** and click the appropriate IP address in the navigation pane to open the **Local Settings** page.
    e. Under **Filtering Service Definition**, select the IP address for the machine running Filtering Service. During the migration, the setting may have been reset to None.
    f. Log out of TRITON - Web Security.

    For more information, see the information about configuring local settings in the *Network Configuration* section of TRITON - Web Security Help.
11. If you stopped your antivirus software, be sure to start it again.

# Network Agent enhanced logging

Network Agent can also provide information for reports on bandwidth information and block HTTP(S) internet protocols based on bandwidth consumption. However, bandwidth information is not recorded by default.

To configure Network Agent to record bandwidth information for reporting, or filter HTTP(S) or FTP requests based on bandwidth consumption, follow these steps:

1. In a supported browser, navigate to: http://<IP address>:9443/triton (<IP address> is the IP address of the machine on which TRITON Unified Security Center is installed).
2. Select the **Web Security** module button.
3. Navigate to the **Settings** > **Network Agent** tab and select the appropriate IP address in the navigation pane to open the Local Settings page.
4. Under **Network Interface Card**, click the appropriate NIC monitoring the relevant traffic.
5. Under **Integration**, enable the Log HTTP requests option.

For information on configuring bandwidth blocking for category and protocol, please refer to the Bandwidth Optimizer section of the TRITON - Web Security Help.

# 14 Configuring a Cisco Security Appliance

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Configuring a Cisco security appliance

After Websense Web Filter or Web Security is installed, the Cisco security appliance, PIX firewall, or Adaptive Security Appliance (ASA) must be configured to work with Websense software. The Cisco firewall passes each Internet request to Filtering Service, which analyzes the request and determines whether to block or permit access, or limit access by using quotas set in Websense policies.

See the TRITON - Web Security Help for information about implementing filtering policies.

See the following for information about configuring Websense integration with Cisco PIX Firewall or Adaptive Security Appliance (ASA) through a console or Telnet session:

- *Cisco integration command conventions*, page 200
- *Cisco integration configuration procedure*, page 200
- *User-based filtering for Cisco integration*, page 208
- *Upgrading Cisco PIX Firewall software to version 7.0 may stop Web filtering*, page 210

For information on configuring your security appliance through the management interface, see the documentation for your Cisco product, available at www.cisco.com.

**Note**

In this topic, the term *security appliance* is used to refer to both Cisco PIX Firewall and ASA collectively.

# Cisco integration command conventions

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Command conventions

The following conventions are used for commands in this document:

- **`Boldface`** indicates commands and keywords that are entered as shown.
- Angle brackets (< >) containing text in *italics* indicate variables that must be replaced by a value in the command.
- Square brackets ([ ]) indicate an optional element or value.
- Braces ({ }) indicate a required choice.
- A forward slash (/) separates each value within curly braces.
- Vertical bars ( | ) separate alternative, mutually exclusive elements

# Cisco integration configuration procedure

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Configuration procedure

To configure your security appliance to send Internet requests to Websense software for filtering:

1. Access the security appliance from a console or from a remote terminal using telnet for access
2. Enter your password.
3. Enter **enable**, followed by the enable password to put the security appliance into privileged EXEC mode.

4. Enter **configure terminal** to activate configure mode.

> **Note**
> For help with individual commands, enter **help** followed by the command. For example, **help filter** shows the complete syntax for the **filter** command and explains each option.

5. Use the **url-server** command to enable URL filtering by Websense software.

```
url-server (<if_name>) vendor websense host <ip_address>
[timeout <seconds>] [protocol {TCP | UDP} version {1 | 4}
[connections <num_conns>]]
```

The **url-server** command takes the following parameters:

| Parameter | Definition |
|---|---|
| **(**<*if_name*>**)** | The network interface where Websense Filtering Service resides.<br>In v7.0 of the Cisco security appliance software, a value for this parameter must be entered.<br>In v6.3.1 and earlier, <*if_name*> defaults to `inside` if not specified.<br>You must type the parentheses ( ) when you enter a value for this parameter. |
| **vendor websense** | Indicates the URL filtering service vendor is Websense. |
| <*ip_address*> | IP address of the machine running Filtering Service. |
| **timeout** <*seconds*> | The amount of time, in seconds, that the security appliance waits for a response before switching to the next Filtering Service that you defined as a **url-server**, or, if specified, going into allow mode and permitting all requests.<br>If a timeout interval is not specified, this parameter defaults to 30 seconds in v7.0(1) and later, and 5 seconds in earlier versions of the Cisco PIX or ASA software.<br>• v7.0(1) and later: Range: 10 - 120; Default: 30<br>• v6.3: Range: 1 - 30; Default: 5 |

| Parameter | Definition |
|---|---|
| **protocol** {**TCP** \| **UDP**} **version** {**1** \| **4**} | Defines whether the Cisco security appliance should use TCP or UDP protocol to communicate with Filtering Service, and which version of the protocol to use.<br>**TCP** is the recommended and default setting. The recommended protocol version is **4**. The default is 1. (*Note*: To send authenticated user information to Filtering Service, TCP version 4 must be selected.) |
| **connections** <*num_conns*> | Limits the maximum number of TCP connections permitted between the Cisco security appliance and Filtering Service.<br>If this parameter is not specified, it defaults to **5**, which is the recommended setting.<br>If you select the UDP protocol, this option is not available.<br>Range: 1 - 100; Default: 5. |

Example:

```
url-server (inside) vendor websense host 10.255.40.164
timeout 30 protocol TCP version 4 connections 5
```

The **url-server** command communicates the location of Filtering Service to the Cisco security appliance. More than one **url-server** command can be entered. Multiple commands allow redirection to another Filtering Service after the specified timeout period, if the first server becomes unavailable.

6. Configure the security appliance to filter HTTP requests with the **filter url** command.
   - To review the current URL server rules, enter **show running-config url-server** (v7.0) or **show url-server** (v6.3).
   - To review all the filter rules, enter**show running-config filter** (v7.0) or **show filter** (v6.3).

   To configure HTTP request filtering, use the following command:

   **filter url http** <*port*>[-<*port*>] <*local_ip*> <*local_mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

   For an explanation of the **filter url** parameters, see *Parameters for the filter commands*, page 207.

Examples:

| Command example | Action |
|---|---|
| `filter url http 0 0 0 0` | Filters every HTTP request to all destinations.<br>Filtering is applied to traffic on port 80. |
| `filter url http 10.5.0.0 255.255.0.0 0 0` | Filters the 10.5.x.x network going to any destination.<br>Filtering is applied to traffic on port 80. |
| `filter url http 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255` | Filters the 10.5.0.69 host going to the 132.239.29.189 destination.<br>Filtering is applied to traffic on port 80. |

Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows access from the specified local IP address to all Web sites, as filtered by Websense software

You can enter multiple **filter url** commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. Use a general **filter url** command for all computers to be filtered, and then use TRITON - Web Security to apply filtering policies to individual clients (computers, networks, users, groups, and domains [OUs]).

See the TRITON - Web Security Help for information about implementing filtering policies.

7. Configure the security appliance to filter HTTPS requests with the **filter https** command.
   - To review the current URL server rules, enter **show run url-server** (v7.0) or **show url-server** (v6.3.1).
   - To review all the filter rules, enter **show run filter** (v7.0) or **show filter** (v6.3.1).
   - If you are running v7.0 of Cisco software, enter**exit** to go up a level to run the show command.

   **Note**
   The **filter https** command is supported in v6.3.1 and higher of the Cisco PIX Firewall/ASA software.

   To configure HTTPS request filtering, use the following command:

   **filter https** *<port> <local_ip> <local_mask> <foreign_ip> <foreign_mask>* **[allow]**

   For an explanation of the **filter https** parameters, see *Parameters for the filter commands*, page 207.

Examples:

| Command example | Action |
|---|---|
| `filter https 443 0 0 0 0` | Filters all HTTPS requests to all destinations. Filtering is applied to traffic on port 443. |
| `filter https 443 10.5.0.0 255.255.0.0 0 0` | Filters the 10.5.x.x network going to any destination.<br>Filtering is applied to traffic on port 443. |
| `filter https 443 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255` | Filters the 10.5.0.69 host going to the 132.239.29.189 destination.<br>Filtering is applied to traffic on port 443. |

Using zeroes for the last two entries, <*foreign_ip*> and <*foreign_mask*>, allows access from the specified local IP address to all Web sites, as filtered by Websense software.

You can enter multiple **filter https** commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. Use a general **filter https** command for all computers to be filtered, and then use TRITON - Web Security to apply filtering policies to individual clients (computers, networks, users, groups, and domains [OUs]).

See the TRITON - Web Security Help for information about implementing filtering policies.

8. Configure the Cisco security appliance to filter FTP requests with the **filter ftp** command.
   - To review the current URL server rules, enter **show run url-server** (v7.0) or **url-server** (v6.3.1).
   - To review all the filter rules, enter **show run filter** (v7.0) or **show filter** (v6.3.1).
   - If you are running v7.0 of Cisco software, enter**exit** to go up a level to run the **show** command.

   **Note**

   The **filter ftp** command is supported in v6.3.1 and higher of the Cisco PIX Firewall/ASA software.

   To configure FTP request filtering, use the following command:

   **`filter ftp`** *`<port> <local_ip> <local_mask> <foreign_ip> <foreign_mask>`* **`[allow] [interact-block]`**

   For an explanation of the **filter ftp** parameters, see *Parameters for the filter commands*, page 207.

Examples:

| Command example | Action |
|---|---|
| **filter ftp 21 0 0 0 0** | Filters every FTP request to all destinations.<br>Filtering is applied to traffic on port 21. |
| **filter ftp 21 10.5.0.0 255.255.0.0 0 0** | Filters the 10.5.x.x network going to any destination.<br>Filtering is applied to traffic on port 21. |
| **filter ftp 21 10.5.0.69 255.255.255.255 132.239.29.189 255.255.255.255** | Filters the 10.5.0.69 host going to the 132.239.29.189 destination.<br>Filtering is applied to traffic on port 21. |

Using zeroes for the last two entries, <*foreign_ip*> and <f*oreign_mask*>, allows access via Websense software from the specified local IP address to all Web sites.

You can enter multiple **filter ftp** commands to set up different portions of the network for filtering. Set up the smaller groups first, followed by the larger groups, to assure that all groups are filtered properly. Use a general **filter ftp** command for all computers to be filtered, and then use TRITON - Web Security to apply filtering policies to individual clients (computers, networks, users, groups, and domains [OUs]).

See the TRITON - Web Security Help for information about implementing filtering policies.

9. After entering commands to define filtering for HTTP, HTTPS, and FTP requests, you can define any required exceptions to these filtering rules by adding the **except** parameter to the **filter** command:

   **filter** {**url** | **https** | **ftp**} **except** <*local_ip*> <*local_mask*> <*foreign_ip*> <*foreign_mask*>

   This command allows you to bypass Websense filtering for traffic coming from, or going to a specified IP address or addresses.

   For example, suppose that the following filter command was entered to cause all HTTP requests to be forwarded to Filtering Service:

   **filter url http 0 0 0 0**

   You could then enter:

   **filter url except 10.1.1.1 255.255.255.255 0 0**

   This would allow any outbound HTTP traffic from the IP address 10.1.1.1 to go unfiltered.

10. Configure the security appliance to handle long URLs using the **url-block url-mempool** and **url-block url-size** commands:

> **Note**
>
> The **url-block** commands are supported in v6.2 and higher of the Cisco PIX Firewall/ASA software.

a. Increase the size of the security appliance's internal buffer to handle long URL strings. If the URL buffer size is set too low, some Web pages may not display.

   To specify the amount of memory assigned to the URL buffer, enter:

   **`url-block url-mempool`** *<memory_pool_size>*

   Here, <*memory_pool_size*> is the size of the buffer in KB. You can enter a value from 2 to 10240. The recommended value is 1500.

b. Increase the maximum permitted size of a single URL by adding the following line to the configuration:

   **`url-block url-size`** *<long_url_size>*

   Here, <*long_url_size*> is the maximum URL size in KB. You can enter a value from 2 to 4. The recommended value is 4.

11. Configure the URL response block buffer using the **url-block block** command to prevent replies from the Web server from being dropped in high-traffic situations.

> **Note**
> The **url-block** commands are supported in v6.2 and higher of the Cisco PIX Firewall/ASA software.

On busy networks, the lookup response from Filtering Service may not reach the security appliance before the response arrives from the Web server.

The HTTP response buffer in the security appliance must be large enough to store Web server responses while waiting for a filtering decision from the Filtering Service.

To configure the block buffer limit, use the following command:

**`url-block block`** *<block_buffer_limit>*

Here, <*block_buffer_limit*> is the number of 1550-byte blocks to be buffered. You can enter a value from 1 to 128.

- To view the current configuration for all 3 **url-block** commands, enter **show running-config url-block** (v7.0) or **show url-block** (v6.3).
- Enter **show url-block block statistics** to see how the current buffer configuration is functioning. The statistics include the number of pending packets held and the number dropped. The **clear url-block block statistics** command clears the statistics.

12. If you need to discontinue filtering, enter the exact parameters in the original **filter** command, preceded by the word **no**.

    For example, if you entered the following to enable filtering:

    **`filter url http 10.0.0.0 255.0.0.0 0 0`**

    Enter the following to disable filtering:

    **`no filter url http 10.0.0.0 255.0.0.0 0 0`**

    Repeat for each filter command issued, as appropriate.

13. Save your changes in one of the following ways:

- **copy run start**
- **exit**
  **write memory**

Websense software is ready to filter Internet requests after the Websense Master Database is downloaded and the software is activated within the Cisco security appliance. See the Websense *Installation Guide* and the TRITON - Web Security Help for information about configuring Websense software and downloading the Master Database.

## Parameters for the filter commands

The parameters used by the **filter http**, **filter https**, and **filter ftp** commands include the following. Note that some of the parameters listed do not apply to all 3 commands.

| Parameter | Applies to | Definition |
|---|---|---|
| `http <port>[-<port>]` | `filter http` | Defines which port number, or range of port numbers, the security appliance watches for HTTP requests. If you do not specify a port number, port 80 is used by default.<br>The option to set a custom Web port or port range is only available in v5.3 and higher of Cisco software.<br>**Note:**<br>In Cisco software versions 5.3 to 6.3, it is not mandatory to enter **http** before the port number; you can either enter **http** (to use port 80), or you can enter a port number.<br>In Cisco software version 7.0, you must always enter **http**. |
| *<port>* | `filter https`<br>`filter ftp` | Defines the port number the security appliance watches for https or ftp requests.<br>The standard HTTPS port is **443**.<br>The standard FTP port is **21**. |
| *<local_ip>* | `filter http`<br>`filter https`<br>`filter ftp` | IP address requesting access.<br>You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all internal clients. This address is the source for all connections to be filtered. |
| *<local_mask>* | `filter http`<br>`filter https`<br>`filter ftp` | Network mask of the **local_ip** address (the IP address requesting access).<br>You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the local network. |
| *<foreign_ip>* | `filter http`<br>`filter https`<br>`filter ftp` | IP address to which access is requested.<br>You can use 0.0.0.0 (or in shortened form, 0) to specify all external destinations. |

| Parameter | Applies to | Definition |
|---|---|---|
| *<foreign_mask>* | `filter http`<br>`filter https`<br>`filter ftp` | Network mask of the **foreign_ip** address (the IP address to which access is requested).<br>Always specify a mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the external network. |
| `[allow]` | `filter http`<br>`filter https`<br>`filter ftp` | Lets outbound connections pass through the security appliance without filtering when Filtering Service is unavailable.<br>If you omit this option, and Filtering Service becomes unavailable, the security appliance stops all outbound HTTP, HTTPS, or FTP traffic until Filtering Service is available again. |
| `[cgi-truncate]` | `filter http` | Sends CGI scripts to Filtering Service as regular URLs. When a URL has a parameter list starting with a question mark (?), such as a CGI script, the URL is truncated. All characters after, and including the question mark, are removed before sending the URL to Filtering Service.<br>(Supported in Cisco PIX v6.2 and higher.) |
| `[interact-block]` | `filter ftp` | Prevents users from connecting to the FTP server through an interactive FTP client.<br>An interactive FTP client allows users to change directories without entering the complete directory path, so Filtering Service cannot tell if the user is requesting something that should be blocked. |
| `[longurl-truncate \| longurl-deny]` | `filter http` | Specify how to handle URLs that are longer than the URL buffer size limit.<br>• Enter **longurl-truncate** to send only the host name or IP address to Filtering Service.<br>• Enter **longurl-deny** to deny the request without sending it to Filtering Service.<br>(Supported in Cisco PIX v6.2 and higher.) |
| `[proxy-block]` | `filter http` | Enter this parameter to prevent users from connecting to an HTTP proxy server.<br>(Supported in Cisco PIX v6.2 and higher.) |

# User-based filtering for Cisco integration

## Applies to

- Web Filter v7.6

- Web Security v7.6

## In this topic



## Overview

If http, https or ftp authentication is enabled on Cisco Security Appliance, Websense User Service must be installed in the same domain (Windows), or the same root context (LDAP) as authenticated users in order to get correct user information to the Websense Filtering Service component for accurate user-based filtering.

> **Note**
> Cisco Secure ACS can provide user information for one domain only. To transparently identify users in multiple domains, use a Websense transparent identification agent. See the Websense *Installation Guide* for information about installing transparent identification agents.

If user authentication is not enabled on Cisco Security Appliance, manual authentication or transparent identification agents can be used for user-based filtering. See the TRITON - Web Security Help for information about configuring manual authentication, or configuring transparent identification agents.

## Enable protocol filtering

If user authentication information is provided by Cisco Security Appliance, it can only be used for HTTP(S) and FTP filtering by default.

To enable internet protocol filtering, follow these steps:

1. Log on to the machince on which Filtering Service is installed.
2. Stop Filtering Service (See Stopping and starting Websense services in the Installation Guide).
3. Navigate to C:\Program Files\Websense\bin (or, /opt/Websense/bin on Linux).
4. Open **eimserver.ini**.
5. Add the parameter “CacheWISPUsers=on” in the **[WebsenseServer]** section.
6. Restart Filtering Service (See Stopping and starting Websense services in the Installation Guide).

If user authentication is provided by manual authentication or transparent identification agents, it can be used for both HTTP(S), FTP and internet protocol filtering.

# Upgrading Cisco PIX Firewall software to version 7.0 may stop Web filtering

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Upgrading Cisco PIX Firewall software to version 7.0 may stop Web filtering

In version 7.0(1) of the Cisco PIX Firewall software, the **url-server** command was changed to increase the minimum value for the timeout parameter to **10** seconds.

In previous versions, the minimum value for this parameter was 1 second, and the default value was 5 seconds.

If the timeout was set to a value less than 10 seconds, the **url-server** command was deleted when you upgraded your software.

To resolve this issue, re-enter the **url-server** command.

See Cisco documentation for more information.

# 15 Configuring a Cisco IOS Router

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Overview

After Websense Web Filter or Web Security is installed, you must configure the Cisco IOS router to send HTTP requests to Websense software. This configuration is done through a console or telnet session. Websense software analyzes each request and tells the router whether or not to permit access or to limit access with quotas, defined in Websense filtering policies.



## Cisco IOS startup configuration

### Applies to

- Web Filter v7.6
- Web Security v7.6

### Startup configuration

Before Websense software can filter Internet requests, the Cisco IOS router must be configured to use Filtering Service as a URL filter.

1. Access the router's software from a console, or from a remote terminal using telnet.

2. Enter your password.
3. Enter **enable** and the enable password to put the router into enabled mode.
4. Enter **configure terminal** to activate configure mode.
5. Enter the following command to identify the Filtering Service machine that will filter HTTP requests:

   **ip urlfilter server vendor websense** <*ip-address*> [**port** <*port-number*>] [**timeout** <*seconds*>] [**retransmit** <*number*>]

| Variable | Description |
|---|---|
| <*ip-address*> | The IP address of the machine running Websense Filtering Service. |
| <*port-number*> | The Filtering Service port (also referred to as the integration communication port), default 15868. |
| <*seconds*> | The amount of time the Cisco IOS router waits for a response from Filtering Service.<br>The default timeout is 5 seconds. |
| <*number*> | How many times the Cisco IOS router retransmits an HTTP request when there is no response from Filtering Service.<br>The default is 2. |

   An example of this command is:

   **ip urlfilter server vendor websense 12.203.9.116 timeout 8 retransmit 6**

   To define an additional Filtering Service instance as a backup, repeat the command using the IP address of the second Filtering Service machine.

   The configuration settings you create in the following steps are always applied to the primary server.

   Only one Filtering Service instance is used at a time—referred to as the primary server; all other instances are referred to as secondary. If the primary server becomes unavailable, one of the secondary servers is designated primary. The system goes to the beginning of the list of configured servers (i.e. Filtering Service instances) and attempts to activate the first one. If the first server is not available, the system attempts to activate the next one. This continues until an available server is found or the end of the list of configured servers is reached. If all servers are down, the router goes into allow mode.
6. Enable the logging of system messages to Filtering Service by entering the following command:

   **ip urlfilter urlf-server-log**

   This setting is disabled by default. When logging is enabled, the Cisco IOS router sends a log request immediately after the URL lookup request.
7. Tell the Cisco IOS router how to filter URL requests by entering the following commands, in sequence:

   **ip inspect name** <*inspection-name*> **http urlfilter**

**interface** <*type*> <*slot/port*>

**ip inspect** <*inspection-name*> {**in**|**out**}

Examples of these commands are:

**ip inspect name fw_url http urlfilter**

**interface FastEthernet 0/0**

**ip inspect fw_url in**

For this sequence to function properly, you must create an inspection rule called *fw_url* and apply that rule to the inbound interface of the router.

See Cisco documentation for information about creating and applying inspection rules.

To improve performance, Cisco suggests disabling the Java applet scanner. Java applet scanning increases CPU processing load. To disable the Java applet scanner, use the following commands, in sequence:

**access-list** <*num*> **permit any**

**ip inspect name** <*inspection–name*> **http java-list** <*num*> **urlfilter**

See Cisco documentation for more information about these commands.

8. To save your changes:
   a. Enter the **exit** command twice to leave the configure mode.
   b. Enter **write memory**.

   These commands store the configuration settings in the Cisco IOS router's startup configuration so they are not lost if the router is shut down or loses power.
9. Use the following commands to view various aspects of your installations:

| Command | Action |
|---|---|
| **show ip inspect name** <*inspection-name*> | Displays a specific inspection rule. |
| **show ip inspect all** | Displays all available inspection information. |
| **show ip urlfilter config** | Displays all URL filtering information. |
| <*command-name*> **?** | Displays help on individual commands.<br>For example, **ip inspect ?** displays the complete syntax for the **inspect** command, and explains each argument. |

10. To discontinue filtering or to change a Filtering Service, enter the following command to remove a server configured in Step 5, page 212.

    **no ip urlfilter server vendor websense** <*ip-address*>

# Cisco IOS configuration commands

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Configuration commands

These commands are used to configure the Cisco IOS router to filter HTTP requests through Websense Filtering Service. These configuration settings can be saved into the startup configuration. See Step 8 in the preceding procedure for instructions.

> **Note**
> To turn off a feature or service, add the value **no** before the command.

**ip inspect name** <*inspection-name*> **http urlfilter** [**java-list** <*access-list*>] [**alert** {**on**|**off**}] [**timeout** <*seconds*>] [**audit-trail** {**on**|**off**}]

This global command turns on HTTP filtering. The **urlfilter** value associates URL filtering with HTTP inspection rules. You may configure two or more inspections in a router, but the URL filtering feature only works with those inspections in which the **urlfilter** field is enabled. This setup command is required.

**ip port-map http port** <*num*>

Use this command to filter proxy traffic on port <*num*> through Websense Filtering Service.

**ip urlfilter server vendor websense** <*IP-address*> [**port** <*num*>] [**timeout** <*secs*>] [**retrans** <*num*>]

This setup command is required to identify Filtering Service to the Cisco IOS router and configure additional values. When using this command, the Cisco IOS router checks for a primary Filtering Service—one that is active and being sent URL lookup requests. If a primary server is configured, the router marks the server being added as a secondary server.

| Parameter | Description |
|---|---|
| **port** <*num*> | The Filtering Service port (referred to as the integration communication port) you entered during Websense installation.<br>The default port number is 15868. |
| **timeout** <*secs*> | The amount of time the Cisco IOS router waits for a response from Websense Filtering Service.<br>The default timeout is 5 seconds. |
| **retrans** <*secs*> | How many times the router retransmits an HTTP request when there is no response from Filtering Service.<br>The default value is 2. |

### ip urlfilter alert

This optional setting controls system alerts. By default, system alerts are enabled. The following messages can be displayed when alerts are enabled:

- %URLF-3-SERVER_DOWN: Connection to the URL filter server <*IP address*> is down.

  This level three LOG_ERR type message appears when a configured Filtering Service goes down. The router marks the offline server as a secondary server. It then attempts to use a defined secondary server as the primary server. If the router cannot find another Filtering Service, the URLF-3-ALLOW_MODE message is displayed.

- %URLF-3-ALLOW_MODE: Connection to all URL filter servers is down and ALLOW MODE is OFF.

  This message appears when the router cannot find a defined Filtering Service. When the **allowmode** flag is set to **off**, all HTTP requests are blocked.

- %URLF-5-SERVER_UP: Connection to a URL filter server <*IP address*> is made. The system is returning from ALLOW MODE.

  This LOG_NOTICE type message is displayed when a Filtering Service is detected as being up and the system returns from the ALLOW MODE.

- %URLF-4-URL_TO_LONG: URL too long (more than 3072 bytes), possibly a fake packet.

  This LOG_WARNING message is displayed when the URL in a GET request is too long.

- %URLF-4-MAX_REQ: The number of pending requests has exceeded the maximum limit <*num*>.

  This LOG_NOTICE message is displayed when the number of pending requests in the system exceeds the maximum limit defined. Subsequent requests are dropped.

### ip urlfilter audit-trail

This command controls the logging of messages into the syslog server and is disabled by default. The messages logged are:

- %URLF-6-URL_ALLOWED: Access allowed for URL <*site's URL*>; client <*IP address:port number*> server <*IP address:port number*>

  This message is logged for each URL requested that is allowed by Websense software. The message includes the allowed URL, the source IP address/port number, and the destination IP address/port number. Long URLs are truncated to 300 bytes and then logged.
- %URLF-6-URL_BLOCKED: Access denied URL <*site's URL*>; client <*IP address:port number*> server <*IP address:port number*>

  This message is logged for each URL requested that is blocked by Websense software. The message includes the blocked URL, the source IP address/port number, and the destination IP address/port number. Long URLs are truncated to 300 bytes and then logged.
- %URLF-4-SITE-BLOCKED: Access denied for the site <site's URL>; client <IP address:port number> server <IP address:port number>

  This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list.

### `ip urlfilter urlf-server-log`

This command is used to control the logging of system messages to Filtering Service and is disabled by default. To allow logging (and consequently reporting) of Internet activity on your system, you must enable this feature.

When logging is enabled, the Cisco IOS router sends a log request immediately after the URL lookup request. The log message contains information such as the URL, host name, source IP address, and destination IP address.

### `ip urlfilter exclusive-domain {permit|deny} <domain-name>`

This optional command is used to add a domain to, or remove a domain from, the exclusive domain list. Cisco IOS router URL filtering allows you to specify a list of domain names for which the router does not send lookup requests to Websense Filtering Service.

The `permit` flag permits all traffic to <*`domain-name`*>. The `deny` flag blocks all traffic to <*`domain-name`*>.

For example, if www.yahoo.com is added to the exclusive domain list, all the HTTP traffic whose URLs are part of this domain (such as www.yahoo.com/mail/index.html, www.yahoo.com/news, and www.yahoo.com/sports) are permitted without sending a lookup request to Filtering Service.

You may also specify a partial domain name. For example, you can enter .cisco.com instead of the complete domain name. All URLs with a domain name ending with this partial name (such as www.cisco.com/products, www.cisco.com/eng, people-india.cisco.com/index.html, and directory.cisco.com) are permitted or denied without having to send a lookup request to Filtering Service. When using partial domain names, always start the name with a dot (i.e., period).

For example:

```
ip urlfilter exclusive-domain permit .sdsu.edu
```

Use the `no` form of this command (i.e., add the keyword `no` to the beginning) to undo permitting or blocking of a domain name. The permitting or blocking of a domain name stays in effect until the domain name is removed from the exclusive list. Using the `no` form of this command removes the specified domain name from the exclusive list. For example, to stop the automatic permitting of traffic (and send lookup requests to Filtering Service) to www.example.com:

```
no ip urlfilter exclusive-domain permit www.example.com
```

As another example, to stop the automatic blocking of traffic to the same domain name:

```
no ip urlfilter exclusive-domain deny www.example.com
```

**`ip urlfilter allowmode {on|off}`**

This command controls the default filtering policy if Filtering Service is down. If the **allowmode** flag is set to **on**, and the Cisco IOS router cannot find a Filtering Service, all HTTP requests are permitted.

If **allowmode** is set to **off**, all HTTP requests are blocked when Filtering Service becomes unavailable. The default for **allowmode** is **off**.

**`ip urlfilter max-resp-pak <number>`**

Use this optional command to configure the maximum number of HTTP responses that the Cisco IOS router can store in its packet buffer.

The default value is 200 (this is also the maximum you can specify).

**`ip urlfilter max-request <number>`**

Use this optional command to set the maximum number of outstanding requests that can exist at a given time. When this number is exceeded, subsequent requests are dropped. The **allowmode** flag is not considered in this case because it is only used when Filtering Service is down.

The default value is 1000.

# Cisco IOS executable commands

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## Executable commands

These Cisco IOS router commands allow you to view configuration data and filtering information. These settings cannot be saved into the startup configuration.

### `show ip urlfilter config`

This command shows configuration information, such as number of maximum requests, **allowmode** state, and the list of configured Filtering Services.

Technical Support typically requests this information when trying to solve a problem.

### `show ip urlfilter statistics`

This command shows statistics of the URL filtering feature, including:

- Number of requests sent to Filtering Service
- Number of responses received from Filtering Service
- Number of requests pending in the system
- Number of requests failed
- Number of URLs blocked

### `debug ip urlfilter {function-trace/detailed/events}`

This command enables the display of debugging information from the URL filter system.

| Parameter | Description |
|---|---|
| `function-trace` | Enables the system to print a sequence of important functions that get called in this feature. |
| `detailed` | Enables the system to print detailed information about various activities that occur in this feature. |
| `events` | Enables the system to print various events, such as queue events, timer events, and socket events. |

# 16 Configuring a Cisco Content Engine

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Overview

After Websense Web Filter or Web Security software is installed, you must activate it within the Cisco Content Engine. This configuration is done through the Cisco Web-based interface, or through a console or Telnet session.

> **Note**
> If load bypass or authentication bypass is enabled in the Content Engine, Internet requests that are rerouted are filtered by Websense software. See your Content Engine documentation for more information.

# Cisco Content Engine Web-based interface

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Cisco Content Engine Web-based interface

1. Open a Web browser and connect to the Cisco Content Engine at:
   - **https://<IP address>:8003** (secure connection)
   - **http://<IP address>:8001** (non-secure connection)

   Here, *<IP address>* is the IP address of the Content Engine machine.

   By default, ACNS is configured for secured access to the Content Engine GUI (i.e., HTTPS on port 8003).

   > **Note**
   > The Content Engine GUI may be configured for either secured or non-secured access, but not both. For example, if the Content Engine GUI is configured for secured access, non-secured connections (i.e., HTTP on port 8001) are not allowed.

2. The **Enter Network Password** dialog box appears. Enter a user name and password to access the initial management page.
3. Select **Caching > URL Filtering**.
4. Select the filtering option appropriate to your ACNS version.
   - For ACNS versions 5.5 and 5.6, select **Websense Filtering (Remote)**.
5. Enter the following information in the appropriate fields:

| Field | Description |
|---|---|
| **Websense Filtering Service** or **Websense Server** | The host name or IP address of the machine running Filtering Service. |
| **Port** | The Filtering Service port (also referred to as the integration communication port) you entered during installation for Websense software.<br>The default is 15868. |

| Field | Description |
|---|---|
| **Timeout** | The amount of time (between 1 and 120 seconds) that the Content Engine waits for a response from Filtering Service before permitting a site.<br>The default is 20. |
| **Allowmode** | When allowmode is enabled, the Content Engine allows HTTP traffic if Filtering Services does not respond.<br>When allowmode is disabled, the Content Engine blocks all HTTP traffic that is served through it if Filtering Service does not respond. |
| **Connections** | The number of persistent connections (1-250) per CPU. Use this option to configure the number of persistent connections to Filtering Service. The default is 40. Do not change from the default value unless you know for certain that a different value is required. |

6. If Websense software is filtering on a cluster of Content Engines, configure each Content Engine as described in steps -5.

For more information on using the Web-based interface, see Cisco documentation, available at www.cisco.com.

# Cisco Content Engine console or telnet session

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Cisco Content Engine console or telnet session

If you cannot access the Web-based interface, or prefer to use the command-line interface, use the procedure below to configure the Cisco Content Engine.

1. Access the Cisco Content Engine from a console or from a remote terminal using telnet for access.
2. Enter the global configuration mode with the **configure** command.

   You must be in global configuration mode to enter global configuration commands.

   ```
   Console# configure
   Console(config)#
   ```
3. To enable Websense URL filtering, use the **url-filter** global configuration command.

```
url-filter http websense server {<ip-address>} [port <port-
number>] [timeout <seconds>] [connections <number-of-
connections>]
```

| Variable | Description |
|---|---|
| <*ip-address*> | The host name or IP address of the machine running Filtering Service. |
| <*port-number*> The | Filtering Service port you entered during the installation of Websense software.<br>The default is 15868. |
| <*seconds*> | The amount of time (0-240) in seconds that the Content Engine waits for a response from Filtering Service.<br>The default is 20. |
| <*number-of-connections*> | The number of persistent connections (1-250) per CPU. Use this option to configure the number of persistent connections to Filtering Service. The default is 40. Do not change from the default value unless you know for certain that a different value is required. |

4. Use the **url-filter http websense allowmode enable** command to configure the Content Engine to permit requests after a Websense Filtering Service timeout.
5. Use the **url-filter http websense enable** command to enable Websense software as the current URL filtering scheme for HTTP.
6. To save your changes:
   a. Enter the **exit** command to leave **configure** mode.
   b. Enter **write memory**.
7. If Websense software is filtering on a cluster of Content Engines, configure each Content Engine as described in steps 1-6.

Websense software is ready to filter Internet requests after the Websense Master Database is downloaded and the software is activated within the Cisco Content Engine.

See the TRITON - Web Security Help for information about configuring Websense software and downloading the Master Database.

# Verifying Cisco Content Engine configuration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Verifying Cisco Content Engine configuration

Use the following console commands to view current configuration information.

**`show url-filter http`**

Displays the currently enabled filtering scheme for HTTP traffic and also configuration information about Websense Filtering Service (e.g., IP address and integration communication port).

**`show statistics url-filter http websense`**

Displays request-reply statistics about the communication between the Content Engine and Websense Filtering Service. Included are number of requests sent, replies received, pages blocked, pages allowed, and failure cases.

# Configuring firewalls or routers when integrating with Cisco Content Engine

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

## Configuring firewalls or routers when integrating with Cisco Content Engine

To prevent users from circumventing Websense filtering, your firewall or Internet router should be configured to allow outbound HTTP, HTTPS, and FTP requests only from the Cisco Content Engine.

The Content Engine and Websense software transparently handle Internet requests sent from routers using Web Cache Communication Protocol (WCCP).

Network Agent cannot perform protocol filtering on traffic encapsulated with WCCP.

> **Note**
>
> For Internet connectivity, Filtering Service may require authentication through a proxy server or firewall for HTTP traffic. To allow downloads of the Websense Master Database, configure the proxy or firewall to accept clear text or basic authentication.
>
> See the proxy or firewall documentation for configuration instructions.
>
> See the TRITON - Web Security Help for instructions on running the Websense Master Database download.

# Cisco Content Engine and browser access to the Internet

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Cisco Content Engine and browser access to the Internet

Cisco Content Engine can regulate Internet activity either transparently or explicitly. In transparent mode, the firewall or Internet router is configured to send Internet requests to the Cisco Content Engine, which queries Filtering Service. All configuration changes can be performed through the Content Engine and any connected firewalls or routers, with no special configuration required on client computers. To run transparently, you must enable WCCP on both the Content Engine and the firewall or router.

When regulating Internet activity explicitly, Web browsers on all client computers are configured to send Internet requests to the Content Engine. See Cisco Content Engine documentation for instructions.

To prevent users from circumventing Websense filtering, your firewall or Internet router should be configured to allow outbound HTTP and FTP requests only from the Cisco Content Engine.

To set up promptless, browser authentication for NTLM or LDAP, refer to Cisco documentation.

# Cisco Content Engine clusters

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Cisco Content Engine cluster

If you have several Content Engines running in a cluster, you must configure each Content Engine to use Filtering Service as an HTTP, HTTPS, and FTP filter. Several Content Engines can use the same Filtering Service. See Cisco Content Engine documentation for details on setting up a cluster.

# 17 Microsoft ISA Server or Forefront TMG Integration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Overview

This section of the Websense Technical Library provides information specific to integrating Websense Web Filter or Web Security with Microsoft® Internet Security and Acceleration (ISA) Server and Forefront™ Threat Management Gateway (TMG). Refer to *Web Filter or Web Security (software-based)*, page 69 as your primary source of installation instructions. Only additional or alternate steps required to integrate Web Filter or Web Security with ISA/TMG are provided here.

> **Notes**
> In these instructions, "ISA/TMG" refers to ISA Server and Forefront TMG collectively. When instructions or information differ for the two products, they are referred to specifically as "ISA Server" or "Forefront TMG".

An integration with ISA/TMG affects the following Websense components:

- **Websense ISAPI Filter plug-in**: This additional Websense component is installed on the machine running ISA/TMG. The ISAPI Filter plug-in configures ISA/TMG to communicate with Websense Filtering Service.
- **Websense Filtering Service**: Interacts with ISA/TMG and Websense Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.

  After the Filtering Service is installed, the ISAPI Filter plug-in must be installed on every ISA/TMG machine in your network.

- **Websense Network Agent**: Internet protocols that are not managed by ISA/TMG are managed by Network Agent.

  > **Note**
  > If ISA/TMG is used only as a proxy server and not firewall, Network Agent may be installed on the ISA/TMG machine.

- **Transparent identification agents**: Generally, ISA/TMG provides user authentication information for Web Filter or Web Security. If ISA/TMG is not configured to provide user information to Web Filter or Web Security, install the appropriate Websense transparent identification agent. See theTransparent Identification of Users technical paper for more information about these agents.

If your environment includes an array of ISA/TMG machines, it is a best practice to install Web Filter or Web Security on a machine outside the array.

The following discusses various aspects of integrating with ISA/TMG:



# How Websense filtering works with ISA/TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## How Websense filtering works with ISA/TMG

To be filtered by Web Filter or Web Security, a computer must access the Internet through ISA/TMG.

When ISA/TMG receives an Internet request from a user, it communicates with Websense Filtering Service to find out if the requested site should be blocked or permitted. Filtering Service checks the policy assigned to the client. Each policy designates specific time periods and lists the category filters that are applied during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database.

- If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies ISA/TMG that the site is not blocked, and the client is given access to the site.

# Supported ISA Server and Forefront TMG versions

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Supported ISA Server and Forefront TMG versions

Web Filter or Web Security can be integrated with the following Microsoft products.

- Microsoft ISA Server 2004, Standard Edition and Enterprise Edition
- Microsoft ISA Server 2006, Standard Edition and Enterprise Edition
- Microsoft Forefront TMG 2010 or later

Supported ISA/TMG clients are:

- Firewall Client/Forefront TMG Client
- SecureNAT clients
- Web Proxy clients

# Installing Web Security to integrate with ISA Server or Forefront TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic

- *Websense software and ISA Server on the same machine*, page 236

## Overview

Typically, Web Filter or Web Security is not installed on the same machine as ISA Server. The only Websense component installed on the ISA/TMG Server machine is the ISAPI Filter plug-in. See *Web Filter or Web Security and ISA/TMG on separate machines*, page 230.

**Notes**

- It is a best practice to not install Websense components, except the ISAPI Filter plug-in, on the same machine as ISA Server.
- When the ISAPI Filter plug-in is installed, Websense Control Service is installed automatically as well.

However, if the machine has sufficient resources, Web Filter or Web Security may be installed on an ISA Server machine. The machine must have sufficient resources or the performance of both Web Filter or Web Security, and ISA Server may be affected.

**Notes**

Installing Websense components on the same machine as Forefront TMG is not supported. Forefront TMG runs on native 64-bit Windows Server 2008, while other Websense components are currently 32-bit running on Windows on Windows (WoW) subsystem over Windows Server 2008.

The following topics are covered in this section:



## Web Filter or Web Security and ISA/TMG on separate machines

Typically, Web Filter or Web Security components are installed on machines separate from ISA/TMG. In this case, installation is a two-part process:

1. Install Websense software.

See *Web Filter or Web Security (software-based)*, page 69 for instructions.

> **Note**
> Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on the ISA/TMG machine. When installing Filtering Service, it must be installed as integrated with ISA/TMG.

2. Install the ISAPI Filter plug-in on the ISA/TMG machine.

> **Note**
> Port 55933 (Websense Control Service communication port) must be open locally, for the ISAPI Filter plug-in to be installed successfully. If installing other Websense components on the ISA Server machine, see *Default ports*, page 927.

- ISA Server:

  Run the Websense installer on the ISA Server machine and choose to install the plug-in only. See *Installing the ISAPI Filter plug-in for ISA Server*, below.

> **Note**
> Do not attempt to install the ISAPI Filter plug-in for ISA Server on Windows Server 2008. This plug-in supports ISA Server 2004 and 2006 only, which are not supported on Windows Server 2008.

- Forefront TMG:

  A separate installer from Websense, referred to as the *Forefront TMG plug-in installer*, is used to install the ISAPI plug-in for Forefront TMG. See *Installing the ISAPI Filter plug-in for Forefront TMG*, page 234.

> **Important**
> The ISAPI Filter plug-in for Forefront TMG is supported on **only** Windows 2008 R2 and Windows 2008 SP2 (x64). Do not attempt to run the Forefront TMG plug-in installer on any operating system but Windows 2008 R2 or Windows 2008 SP2 (x64).

## Installing the ISAPI Filter plug-in for ISA Server

The Websense installer is used to install the Websense ISAPI Filter plug-in on the ISA Server machine. The following procedure is performed on the ISA Server machine.

> **Note**
> As part of the installation process, you must stop the Microsoft Firewall service. Depending on your network configuration, doing so may stop network traffic. It is a best practice to perform this installation during a time when such stoppage would least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.

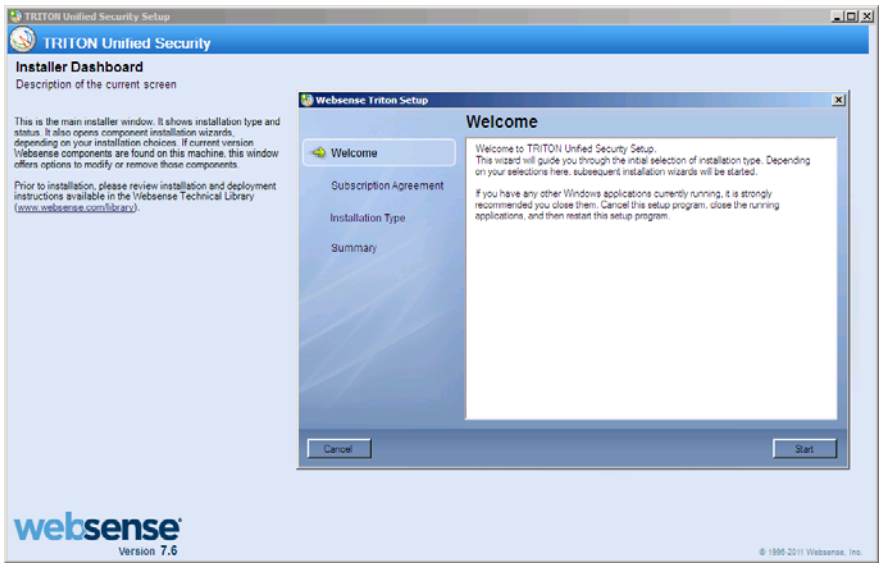
> **Note**
> Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on this machine. When installing Filtering Service, be sure to specify it as integrated with ISA Server.

> **Note**
> Port 55933 (Websense Control Service communication port) must be open locally, for the ISAPI Filter plug-in to be installed successfully.

1. Perform any required preparation steps described in *Preparing for Installation*, page 55.
2. Download or copy the Websense installer to this machine.

   See *Websense installer*, page 57 for instructions.
3. Close all applications and stop any antivirus software.
4. Start the Websense installer.

5. On the **Welcome** screen, click **Start**.




6. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
7. On the **Installation Type** screen, select **Custom**.
8. On the **Summary** screen, click **Next** to continue the installation.
9. Follow the instructions in *Installing Web Security components*, page 668 to install the ISAPI Filter plug-in.

   The link above goes to general instructions for installing any Web Security component. In the case of installing the ISAPI Filter plug-in, do the following as you complete the general procedure:

   - On the **Select Components** screen, select **Filtering Plug-in**.
   - On the **Select Integration** screen, select **Microsoft Internet Security and Acceleration Server**.
10. If you stopped antivirus software on this machine, restart it now.
11. You can verify successful installation of the ISAPI Filter plug-in by logging into the ISA Server Management console.

    In the console, go to **Configuration** > **Add-ins** > **Web Filters**. WsISAFilter should be present in the list of Web Filters.

## Installing the ISAPI Filter plug-in for Forefront TMG

The Forefront TMG plug-in installer is used to install the Websense ISAPI Filter plug-in for Forefront TMG. The following procedure is performed on the Forefront TMG machine.

> **Important**
> The ISAPI Filter plug-in for Forefront TMG is supported on **only** Windows 2008 R2. Do not attempt to run the Forefront TMG plug-in installer on any operating system other than Windows 2008 R2.

> **Note**
> As part of the installation process, you must stop the Microsoft Forefront TMG Firewall service (Firewall service). Depending on your network configuration, doing so may stop network traffic. It is a best practice to perform this installation during a time when such stoppage would least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.

> **Note**
> Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on this machine. When installing Filtering Service, be sure to specify it as integrated with Forefront TMG.

> **Note**
> Port 55933 (Websense Control Service communication port) must be open locally, for the ISAPI Filter plug-in to be installed successfully.

1. Download or copy the Forefront TMG plug-in installer to this machine.
   This installer is available at mywebsense.com.
2. Close all applications and stop any antivirus software.
3. Start the Forefront TMG plug-in installer.
4. On the **Introduction** screen, click Next.
5. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click Next.

6. On the **Filtering Service Communication** screen, enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). Then click **Next**.

   > **Note**
   > The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535. Filtering Service may have been automatically configured to use a port other than the default 15868. When Filtering Service is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Filtering Service, check the `eimserver.ini` file—located in `C:\Program Files\Websense\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.
   >
   > **Important**: Do not modify the `eimserver.ini` file.

7. On the **Installation Directory** screen, accept the default location and click **Next**.
8. On the **Pre-Installation Summary** screen, verify the information shown.

   **Filtering Plug-in** should be listed as the only component to be installed.
9. Click **Install** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
10. When the **Stop Microsoft Forefront TMG Firewall Service** screen appears, stop the Microsoft Forefront TMG Firewall service (Firewall service) and then click **Next**.

    > **Note**
    > Leave the Websense installer running as you stop the Firewall service, and then return to the installer to continue installation.

    To stop the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click Microsoft Forefront TMG Firewall, and then select **Stop**. When the service has stopped, return to the Websense installer and continue the installation process. The Firewall service may

also be stopped from the Forefront TMG management console. See Microsoft's documentation for more information.

> **Important**
> When the Firewall service is stopped, Forefront TMG goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

11. When the following message appears, start the Firewall service and then click **OK**:

    *The Websense ISAPI Filter has been configured, you can now start the Microsoft Firewall Service*.

    > **Note**
    > Leave the Websense installer running as you start the Firewall service, and then return to the installer to continue installation.

12. To start the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click Microsoft Forefront TMG Firewall, and then select **Start**. The Firewall Service may also be started from the Forefront TMG management console. See Microsoft's documentation for more information.On the **Installation Complete** screen, click **Done**.
13. If you stopped antivirus software on this machine, restart it now.
14. You can verify successful installation of the ISAPI Filter plug-in by logging into the Forefront TMG management console.

    In the console, go to **System** > **Web Filters**. WsISAFilter should be present in the list of Web Filters.

## Websense software and ISA Server on the same machine

1. If the machine has sufficient resources, Websense software may be installed on the same machine as ISA Server. Install the Websense components you want on the other machines (i.e., those other than the ISA Server machine).

See *Web Filter or Web Security (software-based)*, page 69 for instructions.

**Note**

- Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on the ISA Server machine. If Filtering Service will be on the ISA Server machine, it can be installed at the same time as ISAPI Filter plug-in. When installing Filtering Service, be sure to specify it as integrated with ISA Server.
- If TRITON - Web Security is installed on the same machine as ISA Server, you must manually edit the ISA Server port as both TRITON - Web Security and ISA Server use port 8080 by default. After changing the ISA Server port, you need add it to the **HTTP Traffic Managed by Integration** list on the **Settings** > **Network Agent** > (Network Agent IP address) screen under **Advanced Settings** in TRITON - Web Security.

1. Install Websense components (including the ISAPI Filter plug-in) on the ISA Server machine:
   a. Download or copy the Websense installer to the ISA Server machine.
   b. Close all applications and stop any antivirus software.
   c. Start the Websense installer.
   d. Follow the installation instructions in *Web Filter or Web Security (software-based)*, page 69 to select and install components.

      On the **Select Components** screen, be sure to select **Filtering Plug-In** along with any other Websense components to be installed on the ISA Server machine.
   e. If you stopped antivirus software on this machine, restart it now.

# Upgrading Web Security when integrated with ISA Server or Forefront TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Upgrading Web Security when integrated with ISA Server or Forefront TMG

- Upgrade Websense Filtering Service before upgrading the ISAPI Filter plug-in. This ensures proper communication between Filtering Service and ISA/TMG.
- To upgrade the ISAPI Filter plug-in:
  - ISA Server: Run the Websense installer on the ISA Server machine and follow the on-screen instructions.
  - Forefront TMG: Run the Forefront TMG plug-in installer on the Forefront TMG machine and follow the on-screen instructions.

> **Note**
> As part of the upgrade process, you must stop the Microsoft Firewall service. Depending on your network configuration, doing so may stop network traffic. It is a best practice to perform this upgrade during a time when such stoppage would least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.

# Removing the ISAPI Filter Plug-In

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Removing the ISAPI Filter Plug-In

Detailed instructions for removing Websense filtering components are provided in the *Removing Components*, page 805. However, additional steps are required when you remove the ISAPI Filter plug-in from an ISA/TMG machine.

1. Log on with **local** administrator privileges.
2. Choose to uninstall a program:
   - Windows Server 2003: Go to Windows **Control Panel** > **Add or Remove Programs**.
   - Windows Server 2008 (x64): Go to Windows **Control Panel** > **Control Panel Home** > **Uninstall a program** (under **Programs**).
3. Select **Websense Web Security / Web Filter**, and then click **Change/Remove** (Windows Server 2003) or **Uninstall/Change** (Windows Server 2008).

   This launches the Websense uninstaller.

4. On the **Remove Components** screen, select **Filtering Plug-in** and any other components to be removed, and then click **Next**.
5. When the **Stop Microsoft Firewall Service** screen appears, stop the Microsoft Firewall service and then click **Next**.

   > **Note**
   > Leave the Websense uninstaller running as you stop the Microsoft Firewall service, and then return to the uninstaller to continue.

   To stop the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click **Microsoft Firewall** (ISA Server) or **Microsoft Forefront TMG Firewall** (Forefront TMG), and then select **Stop**. When the service has stopped, return to the Websense installer and continue the uninstallation process.

   > **Important**
   > When the Firewall service is stopped, ISA/TMG goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

6. When the following message appears, start the Firewall service and then click **OK**:

   *The Websense ISAPI Filter has been unconfigured, you can now start the Microsoft Firewall Service.*

   > **Note**
   > Leave the Websense uninstaller running as you start the Firewall service, and then return to the uninstaller to continue.

   To start the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click **Microsoft Firewall** (ISA Server) or **Microsoft Forefront TMG Firewall** (Forefront TMG), and then select **Start**.
7. On the **Websense Software Removed** screen, choose whether you want to restart now or later and then click **Done**.

# Converting to an integration with ISA Server or Forefront TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

You can convert an existing stand-alone deployment of Websense Web Filter or Web Security to one that is integrated with ISA/TMG, without losing any configuration settings. The conversion process preserves such settings as policies, port numbers, and IP addresses.

## Tasks

The following are the main tasks to convert a stand-alone deployment to one integrated with ISA/TMG.

**Task 1:** Upgrade to the current version of Websense software. Keep it as a stand-alone deployment. See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.

**Task 2:** Restart the installation machine.

**Task 3:** Uninstall and reinstall Filtering Service in integrated mode, selecting ISA Server or Forefront TMG as the integration product.

If Websense software, including Network Agent, is running on the machine on which ISA Server will be installed, then Network Agent must be moved to another machine.

See the *Installation Guide* for instructions on removing components and installing them separately.

**Task 4:** Convert the stand-alone deployment to a system integrated with ISA/TMG.

The procedure varies based on where Websense software is installed:

- If Websense software is running on a different machine than ISA/TMG, follow the procedures in *Converting to an integrated system on a separate machine*, page 241.

- If Websense software is running on the same machine as ISA, follow the procedures in *Converting to an integration on the same machine*, page 242.

**Task 5:** Complete the setup tasks, as described later in this supplement.

**Task 6:** Enable authentication so that users can be properly identified and filtered. For instructions, see *Authentication when integrated with ISA Server or Forefront TMG*, page 251.

## Converting to an integrated system on a separate machine

When ISA/TMG is running on a different machine than the Websense software, you must remove the existing Websense Filtering Service, reinstall it to be integrated with ISA/TMG, and then install the ISAPI Filter plug-in on the machine running ISA/TMG. These procedures are described below.

> **Note**
> If you are upgrading to a new version of Websense software, perform the upgrade before converting the deployment to be integrated with ISA/TMG.

See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions on backing up files, removing components, and running the installer.

### Upgrade Websense software and remove Filtering Service

1. If you have not done so, upgrade your Websense software to the current version.

   See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.
2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
3. Make sure Websense software is running. The uninstaller looks for Policy Server during the removal process.

   > **Warning**
   > Do not remove Websense components without the associated Policy Server running. Policy Server keeps track of Websense configuration and component locations. If Policy Server is not running, files for the selected components are still removed, but configuration information is not updated for those components. Problems could occur later if you attempt to reinstall these components.

4. Remove Filtering Service on its machine.

   See *Removing Web Security components*, page 808 for instructions. Be sure to remove **only** Filtering Service.

### Reinstall Filtering Service

After Filtering Service is removed, reinstall it as integrated with ISA/TMG.

See *Adding Web Security components*, page 794 for instructions. As you follow those instructions do the following on the screens noted below:

- On the **Select Components** screen, select **Filtering Service**.
- On the **Integration Option** screen, select **Integrated with another application or device**.
- On the **Select Integration** screen, select **Microsoft Internet Security and Acceleration Server** or **Microsoft Forefront Threat Management Gateway**.

  **Note**

  Select the particular integration product you are using (ISA Server or Forefront TMG).

- (This applies only if ISA Server was selected) On the **Filtering Plug-In** screen, select *only* **Install other selected components**.

### Install the Websense ISAPI Filter Plug-In

Next, install the ISAPI Filter plug-in on the ISA/TMG machine. This plug-in allows Websense software and ISA/TMG to communicate. For instructions, see:

- *Installing the ISAPI Filter plug-in for ISA Server*, page 232 or
- *Installing the ISAPI Filter plug-in for Forefront TMG*, page 234

## Converting to an integration on the same machine

After upgrading a stand-alone deployment of Websense software, you can convert it to be integrated with ISA installed on the same machine.

To convert Websense software to be integrated with ISA Server, Websense Filtering Service and Network Agent must be removed and then reinstalled after ISA Server is installed.

**Note**

- Internet requests are not filtered until this process is completed.
- Installing Websense components on the same machine as Forefront TMG is not supported.

1. If you have not done so, upgrade your Websense software.

   See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.

2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions
3. Make sure Websense software is running. The installer looks for Policy Server during the installation process.

> **Warning**
> Do not remove Websense components without the associated Policy Server running. Policy Server keeps track of Websense configuration and component locations. If Policy Server is not running, files for the selected components are still removed, but configuration information is not updated for those components. Problems could occur later if you attempt to reinstall these components.

4. Remove Filtering Service (and Network Agent if installed) on its machine.

   See *Removing Web Security components*, page 808 for instructions. Be sure to remove **only** Filtering Service (and Network Agent).

> **Note**
> Network Agent must be removed because it should not run on the same machine as ISA. After reinstalling Filtering Service (see below), you will install Network Agent on a separate machine. An exception to this case is if ISA firewall is not enabled. If ISA is running only as a proxy server, Network Agent may be installed on the same machine.

After Network Agent and Filtering Service are removed, you can install ISA. See Microsoft documentation for instructions.

After ISA is installed:

1. Run the Websense installer to reinstall Filtering Service and install the Websense ISAPI Filter plug-in.

   See *Adding Web Security components*, page 794 for instructions. As you follow those instructions do the following on the screens noted below:

   - On the **Select Components** screen, select **Filtering Service**.
   - On the **Integration Option** screen, select **Integrated with another application or device**.
   - On the **Select Integration** screen, select **Microsoft Internet Security and Acceleration Server**.

> **Note**
> Select the particular integration product you are using (ISA Server or Forefront TMG).

- On the **Filtering Plug-In** screen, select *both* **Yes, install the plug-in on this machine** and **Install other selected components**.

2. On a separate machine, install Network Agent.

   See *Web Filter or Web Security (software-based)*, page 69 for instructions.

# ISA Server or Forefront TMG initial setup

## Applies to

- Web Filter v7.6
- Web Security v7.6

## ISA Server or Forefront TMG initial setup

- If you installed the Web Security Log Server on a Windows server, see *Enabling communication with the Log Database when integrated with ISA Server or Forefront TMG*, page 245.
- To use Websense filtering in a network that uses SOCKS or WinSOCK proxy server, see *WinSOCK and SOCKS proxy servers*, page 246, for instructions.
- Additional configuration of the Websense ISAPI Filter is required if you are using non-Web proxy clients with ISA/TMG. These ISA/TMG clients include the Firewall/Forefront TMG Client with proxy server disabled, and SecureNAT clients.

  See *Configuring for ISA/TMG using non-Web-Proxy clients*, page 246, for instructions.
- To configure Websense software to ignore certain traffic based on the user name, host name, or URL, see *Configuring the ISAPI Filter plug-in to ignore specific traffic*, page 248, for instructions.
- If Network Agent was installed, configure Network Agent with the IP addresses of all proxy servers through which computers route their Internet requests. See *Network Configuration* in the TRITON - Web Security Help for instructions.
- If you installed Remote Filtering Server in your Websense deployment, configure ISA/TMG to not monitor (i.e., ignore) the machine on which Remote Filtering Server is installed. If ISA/TMG monitors this machine, it could interfere with remote filtering. See your ISA/TMG documentation for instructions.

# Enabling communication with the Log Database when integrated with ISA Server or Forefront TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Enabling communication with the Log Database when integrated with ISA Server or Forefront TMG

When you install Web Security Log Server, ISA/TMG must be configured to permit communication with the Log Database. This **must** be completed before filtering activity can be logged.

The following procedure applies to ISA Server 2006 and Forefront TMG. See Microsoft documentation for assistance with ISA Server 2004.

1. On the ISA/TMG machine, open the ISA Server or Forefront TMG management console (management console).

   To open the management console: **Start > Programs > Microsoft ISA Server** or **Microsoft Forefront TMG > ISA Server Management** or **Forefront TMG Management**.
2. In the left navigation pane, select **Firewall Policy**.
3. On the **Tasks** tab (on the right side of the console), click **Edit System Policy**.

   The **System Policy Editor** dialog box appears.
4. Under **Configuration Groups**, select **Logging > Remote Logging (SQL)**.
5. On the **To** tab, click **Add**.
6. Select **Networks > Internal**, and then click **Add**.

   You are returned to the System Policy Editor dialog box.
7. On the **General** tab, select **Enable this configuration group**.
8. Click **OK** to accept your changes.

   You are returned to the management console.
9. Click **Apply** at the top of the window to save the changes and update the configuration.

# WinSOCK and SOCKS proxy servers

## Applies to

- Web Filter v7.6
- Web Security v7.6

## WinSOCK and SOCKS proxy servers

Websense software filters HTTP, HTTPS, and FTP requests sent to ISA/TMG, but *cannot* filter traffic tunneled over a SOCKS or WinSOCK proxy server.

The Firewall/Forefront TMG Client replaced these proxy servers after ISA Server 2000. To use Websense filtering in a network that uses a SOCKS or WinSOCK proxy server, you can either:

- Disable the WinSOCK or SOCKS service.
- Use the WinSOCK or SOCKS proxy client to disable the specific protocols that you want Websense software to filter (HTTP, HTTPS, and FTP), then configure browsers on client computers to point to ISA/TMG for each of these protocols.

  For information about disabling a protocol, see the ISA/TMG online help.

# Configuring for ISA/TMG using non-Web-Proxy clients

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic

## Overview

> **Note**
> Ensure that TCP/IP stacks are installed on all the client computers if protocols have been disabled on the SOCKS or WinSOCK proxy server, and sent through the normal proxy server for filtering by Websense software.

If you are using non-Web-Proxy clients with ISA Server 2004/2006 or Forefront TMG, additional configuration is required so that Websense software can filter Internet requests correctly. The term non-Web-Proxy clients refers to:

- Firewall/Forefront TMG Client with the proxy server disabled
- SecureNAT clients

## Firewall/Forefront TMG Client

If you are using Firewall/Forefront TMG Client with ISA Server 2004/2006 or Forefront TMG, and the proxy server is enabled (default setting), Websense software filters Internet requests normally.

However, if the proxy server is disabled, Websense software cannot filter Internet requests without additional configuration.

Check the Firewall/Forefront TMG Client machine to see if the proxy server is disabled.

1. Open the Firewall/Forefront TMG Client configuration screen, and select the **Web Browser** tab.
2. View the **Enable Web browser automatic configuration** check box.
   - If it is marked, the proxy server is enabled. Websense software requires no additional configuration.
   - If it is cleared, the proxy server is disabled. See *Configuring the ISAPI Filter plug-in*, page 248, for additional configuration steps.

> **Note**
> If the proxy server is disabled, then Websense software filters HTTP only; it will not be able to filter HTTPS.

## SecureNAT clients

SecureNAT clients require that you configure the default gateway so that all traffic to the Internet is sent through ISA/TMG. If you need information about configuring and using SecureNAT clients, see your ISA/TMG documentation.

See *Configuring the ISAPI Filter plug-in*, page 248, for additional configuration steps.

## Configuring the ISAPI Filter plug-in

If you are using the ISA/TMG Firewall Client with the proxy server disabled, or SecureNAT clients, the ISAPI Filter plug-in must be configured to ignore requests going directly to the ISA/TMG and to filter only those requests going out to the Internet.

> **Note**
> If you are using the ISA/TMG Server Firewall Client with the proxy server disabled, then Websense software filters HTTP only; it will not be able to filter HTTPS.

1. On the ISA/TMG machine, create a file called **ignore.txt** in the Windows **system32** directory.
2. Enter the host name or IP address of the ISA/TMG machine in the text file.

   Host names must be entered in ALL CAPS. Entries that are not in all capital letters are not used.
3. If the ISA/TMG machine hosts multiple Web sites, add the names of all the Web sites being hosted. For example: **webmail.rcd.com**.

   If only one Web site is hosted, do not add it to this file.
4. Restart the ISA/TMG machine.

# Configuring the ISAPI Filter plug-in to ignore specific traffic

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic

## Configuring the ISAPI Filter plug-in to ignore specific traffic

You can configure the ISAPI Filter plug-in to bypass both filtering and logging for certain traffic, based on the user name, host name, or URL. This may be used for a small group of Web sites or users, or for machines in a complex proxy-array or proxy-chaining configuration.

To prevent filtering and logging of this traffic, add the user names, host names, and URLs that you do not want Websense software to filter to the **isa_ignore.txt** file.

1. On the ISA/TMG machine, open the**isa_ignore.txt** file in a text editor. This file is located in the Windows **system32** directory.

   **Important**

   The default **isa_ignore.txt** file installed during a Websense upgrade or installation contains the following URL:

   ```
   url=http://ms_proxy_intra_array_auth_query/
   ```

   Do **not** delete this URL. It is used by ISA/TMG in a CARP array for communication. This URL must be ignored by Websense software to allow filtering and logging to work properly when multiple ISA/TMG instances are deployed in an array.

2. Enter each user name, host name, or URL that you want Websense software to ignore. Enter each item on its own line in the file, using the formats below.

   **Important**

   You must enter each user name, host name, or URL in the exact same format that ISA Server passes it to Filtering Service.

   - **User name**: Enter the name of a user whose Internet requests should not be filtered or logged by Websense software:

     **username=**<*user_name*>

     Examples:

     **username=jsmith**
     **username=domain1/jsmith**

   - **Host name**: Enter a destination host name that Websense software should not filter or log user visits to:

     **hostname=**<*host_name*>

     Example:

     **hostname=yahoo.com**

   - **URL**: Enter a URL that Websense software should not filter or log user visits to:

     **url=**<*URL*>

Example:

```
url=http://mail.yahoo.com/
url=mail.yahoo.com/
```

**Note**

To assure that the correct format is available for all situations, it is recommended that you enter the same name in all available configurations. For example, make 2 entries for user name: one with and one without the domain. Make 2 entries for URL: one with and one without the protocol.

3. Restart the ISA/TMG service.

## Client computer configuration

Internet browsers on client computers should be configured to use ISA/TMG to handle HTTP, HTTPS, and FTP requests.

An exception to this configuration is browsers in an ISA/TMG environment using Firewall/Forefront TMG Clients or SecureNAT. These browsers must point to the same port, 8080, that ISA/TMG uses for each protocol.

See the browser online help for configuration instructions.

## Firewall configuration

To prevent users from circumventing Websense filtering, configure your firewall or Internet router to allow outbound HTTP, HTTPS, and FTP requests only from ISA Server.

Contact your router or firewall vendor for information about configuring access lists on the router or firewall.

**Important**

If Internet connectivity of Websense software requires authentication through a proxy server or firewall for HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication to enable the Websense Master Database download.

# Authentication when integrated with ISA Server or Forefront TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

Authentication is the process of identifying an individual within a network who has an account in a directory service. Depending on the authentication method selected, ISA/TMG can obtain user identification and send it to Websense Filtering Service with the Internet request. Filtering Service can filter requests based on policies assigned to directory clients (users, groups, and domains [OUs] defined in a supported directory service).

**Note**

In any environment, Websense software can filter based on computer (individual IP address) or network (IP address range) policies.

To filter Internet access for directory clients, Websense software must be able to identify the user making the request. This requires one or more of the following:

- Enable an authentication method within ISA/TMG that sends user information to Websense software.
- Install a Websense transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent) to identify users, if user information is not supplied by ISA/TMG.

  See the Transparent Identification of Users technical paper for more information.

- Enable manual authentication within Websense software. Users who cannot be identified by other means are prompted for logon information when they open a browser.

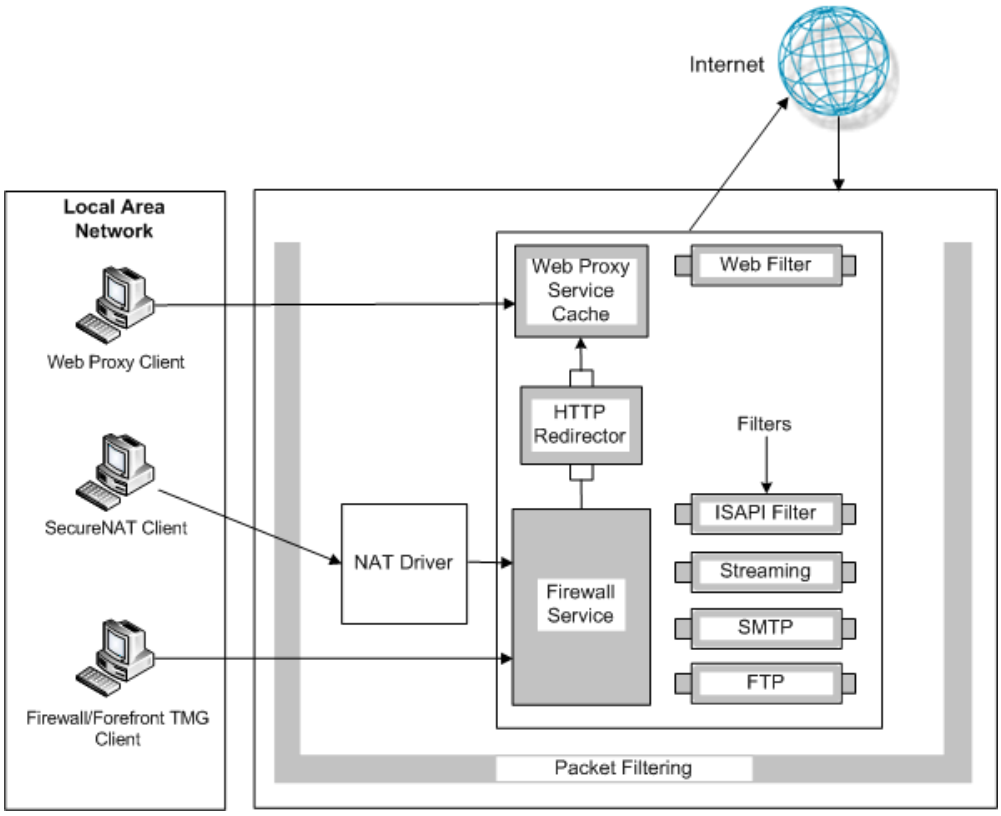
  See *Manual Authentication* in the TRITON - Web Security Help for more information.

## ISA/TMG clients

These ISA/TMG clients are supported:

- Firewall/Forefront TMG (see *Firewall/Forefront TMG and SecureNAT clients*, page 253)
- SecureNAT (see *Firewall/Forefront TMG and SecureNAT clients*, page 253)
- Web Proxy (see *Web Proxy clients*, page 253)

The term **clients** in this environment refers to computers or applications that run on computers and rely on a server to perform some operations. In the following diagram of ISA/TMG Firewall architecture, the relationship between ISA/TMG and the Firewall/Forefront TMG, SecureNAT, and Web Proxy clients is shown.




ISA/TMG Firewall Architecture

Each type of client can be configured so that Websense software can obtain user identification and filter Internet requests based on user and group policies.

## Firewall/Forefront TMG and SecureNAT clients

Firewall/Forefront TMG and SecureNAT clients cannot identify users transparently without special settings. These clients require a Websense transparent identification agent to authenticate users. To enable user-based filtering policies with these clients, select one of these options:

- Configure computer browsers to access the Internet through ISA/TMG. This configuration allows Firewall/Forefront TMG and SecureNAT clients to also work as Web Proxy clients.

  If you choose this option, see *Web Proxy clients* for more information.
- If you are using a Windows-based directory service, disable all authentication methods within ISA/TMG and use Websense transparent identification. This method allows Websense Filtering Service to obtain user identification from the network's domain controllers or directory services.

  See *Transparent identification*, page 256, for more information.
- Enable Websense software to prompt users for authentication (manual authentication). This method allows Websense software to obtain the user information it needs if neither the ISA/TMG nor a Websense transparent identification agent provides the information.

  See *Manual Authentication* in the TRITON - Web Security Help for more information.

## Web Proxy clients

After the browser is configured to use ISA/TMG as a proxy server, Web Proxy clients send Internet requests directly to ISA/TMG. You can assign individual user or group policies with one of the following methods.

- If your network uses only Microsoft Internet Explorer® browsers, version 5.0 or later, you can enable Integrated Windows Authentication within ISA/TMG to identify users transparently.
- If you are using a Windows-based directory service with various browsers, you can identify users transparently by disabling all authentication methods within ISA/TMG and implementing Websense transparent identification.

  See *Transparent identification*, page 256, for more information.
- If the network uses a mixture of browsers, you can enable one or more of ISA/TMG's authentication methods. Some of these methods may require users to authenticate manually for certain older browsers.

  See *Authentication Methods*, page 254, for more information.
- Enable Websense software to prompt users for authentication (manual authentication). This method allows Websense software to obtain the user information it needs if neither ISA/TMG nor a Websense transparent identification agent provides the information.

  See *Manual Authentication* in the TRITON - Web Security Help for more information.

# Authentication Methods

ISA/TMG provides four methods of authentication:

- *Basic authentication*
- *Digest authentication*
- *Integrated Windows authentication*
- *Client Certificate authentication*

Microsoft Internet Explorer, version 5.0 and later, supports all of these authentication methods. Other Web browsers may support only the Basic authentication method. By default, ISA/TMG has Integrated Windows authentication enabled.

You can configure both incoming and outgoing request properties within ISA/TMG. Client Web browsers must be able to use at least one of the authentication methods that you specify in an array's incoming and outgoing Web request dialog boxes. Without this authentication, the client cannot access the requested Internet site.

When no authentication method is enabled in ISA/TMG, it cannot receive any information about who is making the Internet request. As a result, Websense software does not receive user information from ISA/TMG. When this problem occurs, you can:

- Filter with computer and network policies.
- Enable Websense manual authentication to permit user-based filtering.

  See *Manual Authentication* in the TRITON - Web Security Help for more information.
- Enable Websense transparent identification to permit user-based filtering.

  See *Transparent identification*, page 256, for more information.

## Basic authentication

Basic authentication prompts users to authenticate (log on) each time they open a browser. This authentication allows ISA/TMG to obtain user identification, regardless of the browser, and send the information to Websense software, which filters Internet requests based on individual user and group policies.

If Basic authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted for a user name and password.

## Digest authentication

Digest authentication is a secure authentication method used in Windows Server 2003 domains. The features are the same as Basic authentication, but the user name and password are scrambled when they are sent from the browser to ISA/TMG. The user can authenticate to ISA/TMG without the user name and password being intercepted.

User information is sent to Websense software, which then filters Internet requests based on individual user and group policies.

If Digest authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted for a user name and password.

## Integrated Windows authentication

Integrated Windows authentication provides secure authentication. With this authentication enabled, ISA/TMG obtains user identification transparently from browsers using Microsoft Internet Explorer 5.0 and later. User information is sent to Websense software, which then filters Internet requests based on individual user and group policies.

If your network has a mixture of Microsoft Internet Explorer browsers and other browsers, you can enable both Basic and Integrated Windows authentication, or Digest and Integrated Windows authentication. In either configuration:

- Users with Microsoft Internet Explorer browsers are identified transparently.
- Users with other browsers are prompted for a user name and password.

> **Note**
> To transparently identify all users in a mixed browser environment, you can disable Basic or Digest authentication and use Websense transparent identification (see *Transparent identification*, page 256) in conjunction with Integrated Windows authentication.

## Client Certificate authentication

Client Certificate authentication identifies users requesting information about a Web site. If Client Certificate is used, ISA/TMG requests the certificate and verifies that it belongs to a client that is permitted access, before allowing the Internet request.

> **Note**
> To use Websense transparent identification, you must disable Client Certificate authentication.
>
> Before changing authentication methods, consider the impact of the change on other ISA/TMG functions.

For more information about ISA/TMG authentication and how to configure these authentication methods, see Microsoft's documentation.

## Transparent identification

Websense transparent identification allows Websense software to filter Internet requests from users identified in a directory service, without prompting them to authenticate manually. If the authentication method enabled within ISA/TMG does not send user information to Filtering Service, you can use a Websense transparent identification agent to identify users.

For example, if ISA/TMG is configured to obtain user identification from the browser, and you want to use Network Agent to filter protocols by user or group name, use a Websense transparent identification agent to identify users for protocol traffic.

Install and configure Websense transparent identification agents to transparently identify users from a directory service. DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent can be installed on the same machine as Filtering Service, or on a different machine.

Websense also offers secure manual authentication with Secure Sockets Layer (SSL) encryption to protect user names and passwords being transmitted between client computers and Filtering Service. By default, secure manual authentication is disabled. See *Secure Manual Authentication* in the TRITON - Web Security Help for more information and instructions on activating this feature.

After Filtering Service is configured to communicate with a transparent identification agent, user information is obtained from a supported directory service and sent to Filtering Service. When Filtering Service receives the IP address of a computer making an Internet request, the address is matched with the corresponding user name provided by the transparent identification agent.

See *Web Filter or Web Security (software-based)*, page 69 for instructions on installing individual Websense components. See *User Identification* in the TRITON - Web Security Help for information about configuring transparent identification agents.

# Troubleshooting integration with ISA Server or Forefront TMG

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic

## Overview

The following information applies to Web Filter or Web Security integrated with ISA Server or Forefront TMG.


- *SecureNAT clients are not being filtered*, page 257
- *No filtering occurs after the ISAPI Filter plug-in is installed*, page 257


## SecureNAT clients are not being filtered

If you are using non-Web proxy clients (for example, Firewall Client with proxy server disabled, or SecureNAT clients) with ISA/TMG, additional configuration of the Websense ISAPI filter is required. Follow the instructions in *Configuring for ISA/TMG using non-Web-Proxy clients*, page 246.

## No filtering occurs after the ISAPI Filter plug-in is installed

Users are still not being filtered after the Websense ISAPI Filter plug-in has been installed on the machine running the ISA/TMG Server.

- If the ISAPI Filter plug-in is the only Websense component installed on the integration machine, the plug-in may not be communicating with the Websense filtering components installed on other machines. Verify that the ISAPI Filter plug-in is pointing to the correct IP address and port for the machine running Filtering Service.

  1. Go to the Windows **system32** directory and open the **wsMSP.ini** file.
  2. Under **[initSection]**, check the **EIMServerIP** and **EIMServerPort** parameters (these are the Filtering Service IP address and port, respectively). For example:

     ```
     [initSection]
     EIMServerIP=10.203.136.36
     EIMServerPort=15868
     ```

     The default port number is 15868.

- If other Websense components are installed on the same machine as ISA/TMG Server and the plug-in, try restarting the Microsoft Firewall service.

Verify an ISA/TMG firewall rule allows access to Filtering Service on the Filter port (default 15868).

> **Note**
>
> Filtering Service may be automatically configured to use a port other than the default 15868. When Filtering Service is installed, the installation program checks whether the default port is already in use on that machine. If it is already in use, the port number is automatically incremented until a free port is found.
>
> To find the port used by Filtering Service for communication with integration products, check the **eimserver.ini** file—located in C:\Program Files or Program Files (x86)\Websense\Web Security\bin (Windows) or /opt/Websense/bin (Linux)—on the Filtering Service machine. Look for the **WebsenseServerPort** value.
>
> **Important**: Do not modify the **eimserver.ini** file.

- If some Websense components are installed on the ISA/TMG Server machine, while others are installed on a separate machine, be sure the proper ports are open for communication.

  Refer to the help in the ISA/TMG Server Management console for instructions on setting a port. See *Default ports*, page 927 for ports used by Websense solutions.

# 18 Squid Web Proxy Cache Integration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Overview

This section of the Websense Technical Library provides information specific to integrating Websense® Web Filter or Web Security with Squid Web Proxy Cache. Refer to *Web Filter or Web Security (software-based)*, page 69 as your primary source of installation instructions. Only additional or alternative steps required to integrate Web Filter or Web Security with Squid Web Proxy Cache are provided here.

When Websense software is integrated with Squid Web Proxy Cache, the following components are configured differently than in a stand-alone installation:

- **Websense Squid plug-in** must be installed on each Squid Web Proxy Cache machine (Squid machine) to allow Squid Web Proxy Cache to communicate with Filtering Service.
- **Websense Network Agent** is configured to manage only the Internet protocols not managed by Squid Web Proxy Cache (e.g., instant messaging, streaming media, peer-to-peer). Typically, Network Agent runs on a machine connected to a bi-directional span port (or mirror port) on a network switch processing the traffic to be monitored. Network Agent monitors the non-HTTP(S)/FTP traffic directed through the switch. You can install Network Agent on the same machine as Squid Web Proxy Cache. If you do so, a span port on a switch is not necessary for Network Agent to operate—it will be able to monitor the same traffic visible to the Squid machine.

See the following discusses various aspects of integrating with Squid Web Proxy Cache:

- *Supported Squid versions*, page 260
- *Client computers and Squid integration*, page 260

# Supported Squid versions

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Supported Squid versions

- Websense Web Security and Websense Web Filter are compatible with STABLE releases of Squid Web Proxy Cache v2.5 and 2.6.
- The Websense Squid plug-in for the Squid Web Proxy Cache is supported only on 32-bit Red Hat Enterprise Linux 4.7, 5.3 and 5.5.

# Client computers and Squid integration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Client computers and Squid integration

- To be filtered by Websense software, a client computer must access the Internet through the Squid Web Proxy Cache.
- Browsers must be set for proxy-based connections.

# How Websense filtering works when integrated with Squid Web Proxy Cache

## Applies to

- Web Filter v7.6
- Web Security v7.6

## How Websense filtering works when integrated with Squid Web Proxy Cache

When Squid Web Proxy Cache receives an Internet request from a client, it queries Websense Filtering Service to find out if the requested site should be blocked or permitted.

- If the site is blocked, the user receives a block page.
- If the site is permitted, Filtering Service notifies Squid Web Proxy Cache and the client is given access to the site.

See *Filtering Order* in the TRITON - Web Security Help for information about how Filtering Service determines whether a site should be blocked.

# HTTPS blocking when integrated with Squid

## Applies to

- Web Filter v7.6
- Web Security v7.6

## HTTPS blocking when integrated with Squid

To block HTTPS traffic, you must configure the Squid integration with one of these options:

- Install Network Agent, the Websense component that performs protocol filtering, and configure it to block HTTPS traffic.

  For instructions on installing Network Agent, see *Installing Web Security components*, page 668. See *Deploying Network Agent*, page 105 for location information and the TRITON - Web Security Help for configuration instructions.
- If Squid acts as a proxy server, you can configure it to filter all HTTPS traffic.
  1. Go to the **/etc/wsLib/** directory and open the **wsSquid.ini** file in a text editor.
  2. Under **initSection**, change the value of **UseHTTPSBlockPage** to **yes**.

The default setting is **no**, which causes Squid to permit all HTTPS traffic.

3. Save your changes.
4. Restart Squid Web Proxy Cache.

All requests for HTTPS pages are filtered, but if a request is blocked, Squid Web Proxy Cache sends a Squid-generated error page to the user. Users do not see the Websense block page, because Squid Web Proxy Cache is unable to deliver it.

> **Note**
> In some cases, when HTTPS is blocked, the Websense block page may be delivered to the user's browser, or a blank page is displayed, instead of the Squid-generated error page. Regardless, HTTPS is filtered properly. If a request should be blocked, it is blocked.

# Installing Web Filter or Web Security to integrate with Squid Web Proxy Cache

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

The Squid plug-in must be installed on the Squid Web Proxy Cache machine (Squid machine) to allow Websense Filtering Service and the Squid software to communicate.

> **Note**
> Prior to installing Websense software verify you have a correctly installed and operating version of Squid Web Proxy Cache. See Squid documentation and support resources for installation and configuration instructions.

You can install the Websense components on the Squid machine or on a different machine. If you install Filtering Service on the Squid machine, you must still install the Squid plug-in as well.

If you install Filtering Service on a separate machine from Squid Web Proxy Cache, you must subsequently install the Squid plug-in on every Squid machine that communicates with Filtering Service.

**Important**

If you are installing Websense software on a machine running an SELinux-enabled Red Hat Enterprise Linux operating system* with the version of Squid that is prepackaged with the Red Hat installation, Squid cannot launch the Websense Squid plug-in (**WsRedtor**).

If the plug-in does not launch, Websense filtering cannot occur. Configure SELinux permissions so that **WsRedtor** can launch. See your Red Hat Enterprise Linux documentation for details.

*Websense software supports Red Hat Enterprise Linux 4.7, 5.3 and 5.5.

This section contains:



## Websense software and Squid Web Proxy Cache on separate machines

In this case, installation is a two-part process:

1. Install Websense software.

   On the designated machine or machines, install Websense components. See *Installing Web Security components*, page 668 for instructions.

   Websense Filtering Service must be installed on its machine before installing the Websense Squid plug-in on the Squid machine. Filtering Service must be installed as integrated with Squid Web Proxy Cache.

   Install Websense Network Agent to filter non-HTTP(S)/FTP traffic (e.g., instant messaging, streaming media, peer-to-peer, and so forth) which is not handled by Squid Web Proxy Cache. If Network Agent is installed on a separate machine, it must be connected to a bi-directional span port on a network switch (see the *Deploying Network Agent*, page 105 for information about where to place Network Agent in your network). If Network Agent is installed on the Squid machine, connecting to a span port is not necessary.
2. Install the Websense Squid plug-in on the Squid machine.

Run the Web Security Linux installer on the Squid machine and choose to install the plug-in only. See *Installing the Squid plug-in*, page 264.

## Installing the Squid plug-in

The Squid plug-in is installed on the Squid machine to allow Websense Filtering Service and Squid software to communicate.

> **Note**
> The Squid plug-in is supported only on Linux.

If Filtering Service is installed on a separate machine from the Squid machine, it must be installed before you install the Squid plug-in. When it is installed, Filtering Service must be installed as integrated with Squid Web Proxy Cache. You must specify the location of Filtering Service when installing the Squid plug-in, otherwise the installer will not proceed.

When installing the Squid plug-in, the installer checks for Squid Web Proxy Cache on the installation machine. If Squid Web Proxy Cache is detected, the installer continues.

If Squid Web Proxy Cache is not detected, installation of the Squid plug-in cannot proceed.

> **Note**
> The following instructions are a supplement to the full instructions in the *Installing Web Security components*, page 668. These instructions cover only those installer screens involved in installing the Websense Squid plug-in.

The Web Security Linux installer is used to install the Websense Squid plug-in on the Squid machine. The following procedure is performed on the Squid machine.

> **Note**
> Websense Filtering Service must be installed on its machine before installing the Squid plug-in on this machine.

> **Important**
> Make sure `visible_hostname` is set in the squid.conf file **before** installing the Squid plug-in. See your Squid documentation for instructions.

1. Close all applications and stop any antivirus software.
2. Download and start the Web Security Linux installer.

See *Starting the Web Security Linux installer*, page 330.

**Notes**

These instructions refer to GUI installer screens. There are GUI and command-line versions of the Web Security Linux installer. In the command-line version, prompts are displayed that correspond to each GUI screen. Instructions for a screen also apply to the corresponding command-line prompt. The main difference is how options are selected. Rather than clicking items in a screen, you will enter menu-item numbers or characters.

To cancel the command-line installer, press Ctrl-C. However, do **not** cancel the installer, after the **Pre-Installation Summary** screen, as it is installing components. In this case allow the installation to complete and then uninstall the components you did not want to install.

3. On the **Introduction** screen, click Next.
4. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click Next.
5. On the **Installation Type** screen, select **Custom** and then click Next.
6. On the **Custom Installation** screen, select **Filtering Plug-in** and then click Next.
7. On the **Filtering Service Communication** screen, enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). Then click **Next**.

   The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535. Filtering Service may have been automatically configured to use a port other than the default 15868. When Filtering Service was installed, if the installation program found the default port to be in use, it was automatically incremented until a free port is found. To determine what port is used by Filtering Service, check the `eimserver.ini` file—located in `C:\Program Files or Program Files (x86)\Websense\Web Security\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.

   **Important**

   Do not modify the `eimserver.ini` file.

8. On the **Select Integration** screen, select **Squid Web Proxy Cache**.
9. On the **Squid Configuration** screen, enter paths to the squid.conf and squid executable files, and then click **Next**.

   The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to

navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

> **Note**
> The installer will automatically start Squid Web Proxy Cache once installation is complete. Verify it is running after installation is complete (Step 14 below).

10. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click Next.
11. On the **Pre-Installation Summary** screen, verify the information shown.

    **Filtering Plug-in** should be listed as the only component to be installed.
12. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
13. On the **Installation Complete** screen, click **Done**.
14. Start Squid Web Proxy Cache if necessary.

    The installer attempts to start Squid Web Proxy Cache once installation is complete. In some cases, it must be manually started:

    a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.

    b. If it is not running, start it.

    See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.
15. If you stopped antivirus software on this machine, restart it now.

## Websense software and Squid on the same machine

If the machine has sufficient resources, Websense software may be installed on the same machine as Squid Web Proxy Cache. You may install all core Websense components (see below) or particular components (see *Particular Websense components on the Squid machine*, page 268)

### All core Websense components on the Squid machine

> **Note**
> Installing all core Websense components on one machine is typically appropriate for small networks (less than 500 users, or less than 25 Internet requests per second).

Follow the installation instructions in *Filtering installation*, page 330. The steps below provide specific options to select, or alternate instructions to be used, as you

follow the instructions in the installation materials. Unless a specific option or alternative instruction is provided here, you should follow the steps as described in the installation materials.

> **Note**
> Following this procedure installs Websense Network Agent on this machine. Network Agent can be used to filter non-HTTP(S)/FTP traffic (e.g., instant messaging, streaming media, peer-to-peer, and so forth) which is not handled by Squid Web Proxy Cache.

1. On the **Introduction** screen, click **Next**.
2. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.
3. On the **Installation Type** screen, select **Filtering** and then click **Next**.
4. At the **Integration Option** screen, select **Integrated with another application or device**.
5. On the **Select Integration** screen, select **Squid Web Proxy Cache**.
6. On the Filtering Plug-In screen, select both **Yes, install the plug-in on this machine** and **Install other selected components**.

   See *Filtering Plug-In Screen*, page 343 for more information about these options.
7. On the **Squid Configuration** screen, enter paths to the squid.conf and squid executable files, and then click **Next**.

   The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

   Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

   > **Note**
   > The installer will automatically start Squid Web Proxy Cache once installation is complete. Verify it is running after installation is complete (Step 9 below).

8. Complete the remaining steps as described in *Filtering installation*, page 330.
9. Start Squid Web Proxy Cache if necessary.

   The installer attempts to start Squid Web Proxy Cache once installation is complete. In some cases, it must be manually started:

   a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.
   b. If it is not running, start it.

See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.

10. If you stopped antivirus software on this machine, restart it now.

## Particular Websense components on the Squid machine

This section describes how to install particular components on the Squid machine (as opposed to installing all core components; see *All core Websense components on the Squid machine*, page 266).

Web Security components may be distributed across multiple machines. Depending on the size of your deployment (i.e., number of users and amount of network traffic) there are best practices of grouping certain components together on the same machine and separating certain components onto their own machine (e.g. reporting components). See the *General Deployment Recommendations for Web Security*, page 85 for information about distributing components across machines.

1. Install the Websense components you want on the other machines (i.e., those other than the Squid machine).

   See *Web Filter or Web Security (software-based)*, page 69 for instructions.

   **Note**

   Websense Filtering Service must be installed on its machine before installing the Websense Squid plug-in on the Squid machine. Additionally, Filtering Service must be installed as integrated with Squid Web Proxy Cache. If Filtering Service will be on the Squid machine, it can be installed at the same time as the Squid plug-in.

2. Install Websense components (including the Squid plug-in) on the Squid machine:
   a. Close all applications and stop any antivirus software.
   b. Download and start the Web Security Linux installer.

      See *Starting the Web Security Linux installer*, page 330.
   c. Follow the installation instructions in *Custom installation*, page 330 to select and install components. Follow the instructions to completion.

      On the **Select Components** screen, be sure to select **Filtering Plug-In** along with any other Websense components to be installed on the Squid machine.

      You can install Websense Network Agent to filter non-HTTP(S)/FTP traffic (e.g., instant messaging, streaming media, peer-to-peer, and so forth) which is not handled by Squid Web Proxy Cache. If Network Agent is installed on the Squid machine it does not need to be connected to a span port on a network switch (as it would if installed on a separate machine). See the *Deploying Network Agent*, page 105 for more information about the placement of Network Agent in a network.
3. Start Squid Web Proxy Cache if necessary.

To install the filtering plug-in (i.e., Squid plug-in), the installer stops Squid Web Proxy Cache. At the end of the installation process, the installer automatically starts Squid Web Proxy Cache. In some cases, the installer is unable to start Squid Web Proxy Cache and it must be manually started:

a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.

b. If it is not running, start it.

   See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.

4. If you stopped antivirus software on this machine, restart it now.

# Upgrading the Squid plug-in

## Applies to

- Web Filter v7.6
- Web Security v7.6

## Upgrading the Squid plug-in

To upgrade the Squid plug-in, run the Web Security Linux installer on the Squid Web Proxy Cache machine and follow the onscreen instructions. For proper communication to be established with Squid Web Proxy Cache, upgrade Websense Filtering Service **before** upgrading the Squid plug-in.

When you upgrade a previous version of Websense Web Filter or Web Security integrated with Squid Web Proxy Cache, pre-existing Websense tags in the Squid Web Proxy Cache configuration file (squid.conf) are reset to default. A backup copy of the file with pre-upgrade settings can be found in the backup directory (/opt/Websense/backup/).

If you had custom values in place in this file before the upgrade, you can either manually edit the tags after upgrade or make the backup squid.conf file active in the system (See Squid documentation for more information).

The following tags in squid.conf are affected.

- Squid v2.5: redirect_program, redirect_children and redirector_bypass
- Squid v2.6: url_rewrite_program, url_rewrite_children and redirector_bypass

# Squid Web Proxy Cache integration initial setup

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

- Be sure to install the Squid plug-in on each Squid Web Proxy Cache machine so that Filtering Service and Squid Web Proxy Cache can communicate.
- Network Agent deployment:
  - Network Agent can be installed with other Websense components on the Squid machine, or on a separate machine.
  - Network Agent must be installed to use protocol management.
  - If Network Agent is installed, the IP addresses of all proxy servers through which computers route their Internet requests must be defined. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 270, for instructions.
  - Identify the port used for HTTP traffic by the Squid integration. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 270, for instructions.
- Configure authentication of users. See *Authentication when integrated with Squid Web Proxy Cache*, page 278 for more information.
- To block HTTPS traffic, you must configure Squid appropriately. See *HTTPS blocking when integrated with Squid*, page 261, for instructions.
- Configure browsers on client computers. See *Client computer configuration*, page 271, for instructions.

## Identifying the Proxy Cache and the HTTP port for Network Agent

If you have installed Network Agent, you must provide the IP addresses of all Squid Web Proxy Cache machines through which filtered Internet requests are routed. You also must provide the port that Squid uses for HTTP traffic. Without this data, Network Agent cannot filter or log requests properly.

1. Open TRITON - Web Security.
2. In the **Settings** tab, expand **Network Agent**.
3. Select the appropriate IP address in the left navigation pane to open the Local Settings page.
4. **Add** the IP addresses for all proxy servers under **Proxies and Caches**.
5. Click **Advanced Network Agent Settings**.
6. For **Ports used for HTTP traffic**, enter the port used by Squid Web Proxy Cache for HTTP traffic (default: 3128).
7. Click **OK** to cache changes on the Local Settings page. Changes are not implemented until you click **Save All**.

See the *Network Configuration* topic in the TRITON - Web Security Help for more information.

## Client computer configuration

Client computers must have a Web browser that supports proxy-based connections and Java technology.

Internet browsers on client computers must be configured to use the Squid Web Proxy Cache to handle HTTP, HTTPS, FTP, and Gopher requests. Browsers must point to the same port (default: 3128) that Squid Web Proxy Cache uses for each protocol.

See your browser online help for instructions on configuring the browser to send all Internet requests to the proxy server, Squid Web Proxy Cache.

## Configuring firewalls or routers

To prevent users from circumventing Websense filtering, your firewall or Internet router should be configured to allow outbound HTTP, HTTPS, FTP, and Gopher requests only from Squid Web Proxy Cache. See your router or firewall documentation for information about configuring access lists on the router or firewall.

# Converting Web Filter or Web Security to be integrated with Squid Web Proxy Cache

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic

## Overview

You can convert an existing stand-alone deployment of Websense Web Filter or Web Security to an integrated system without losing any configuration settings. The conversion process preserves settings such as policies, port numbers, and IP addresses.

Websense and Squid software can be installed on the same machine or a separate machines.

## Tasks

**Task 1:** Upgrade to the current version of stand-alone Web Filter or Web Security. Keep it as a stand-alone deployment.

**Task 2:** Restart the installation machine.

**Task 3:** Uninstall and reinstall Filtering Service and Network Agent.

See *Removing Components*, page 805 and *Installing Web Security components*, page 668 for instructions.

**Task 4:** Convert the stand-alone deployment to a system integrated with Squid Web Proxy Cache.

The procedure depends on where Websense software is installed:

- If Websense software is running on a different machine than Squid Web Proxy Cache, follow the procedures in*Converting to an integrated system on separate machines*, page 272.
- If Websense software is running on the same machine as Squid Web Proxy Cache, follow the procedures in *Converting to an integration on the same machine*, page 275.

**Task 5:** Complete the Initial Setup tasks (see *Squid Web Proxy Cache integration initial setup*, page 270).

**Task 6:** Enable authentication so that users can be properly identified and filtered. See *Authentication when integrated with Squid Web Proxy Cache*, page 278 for instructions

## Converting to an integrated system on separate machines

When Squid Web Proxy Cache is running on a different machine than Websense software, you must remove the existing Filtering Service, reinstall it as integrated with Squid Web Proxy Cache, and then install the Squid plug-in on the machine running Squid Web Proxy Cache. Network Agent also must be removed and reinstalled.

## Upgrade Websense and remove Filtering Service

1. Log on to the machine running Filtering Service:
   - **Linux**: Log in as the **root** user.
   - **Windows**: Log in with administrative privileges.
2. If you have not done so, upgrade your Websense software to the current version.
3. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
4. Ensure that Websense software is running. The uninstaller looks for Policy Server during the removal process.
5. Close all applications and stop any antivirus software.
6. Run the uninstaller.
   - **Linux**: Go to the Websense installation directory (by default, /opt/Websense) and enter the following command:

     ```
     ./uninstall.sh
     ```

     A GUI version is available on English versions of Linux:

     ```
     ./uninstall.sh -g
     ```
   - **Windows**: see *Removing Web Security components*, page 808.

   The uninstaller detects the installed Websense components and lists them.
7. Select Filtering Service and Network Agent for removal, and then click **Next**.

   > **Note**
   >
   > If there are multiple Network Agents for the same Filtering Service, uninstall all those Network Agents before you uninstall the associated Filtering Service.
   >
   > Trying to uninstall Network Agent *after* its associated Filtering Service has been removed causes an error message.

8. Follow the prompts to complete the removal process.

If Policy Server is not running, a message tells you that removing Websense components may require communication with Policy Server. You must exit the uninstaller, start the Policy Server service, and then run the uninstaller again.

**Warning**

Do not remove Websense components without the associated Policy Server running. Policy Server keeps track of Websense configuration and component locations. If Policy Server is not running, files for the selected components are still removed, but configuration information is not updated for removed components. Problems could occur later if you attempt to reinstall these components.

## Reinstall Filtering Service

After Filtering Service is removed, reinstall it as integrated with Squid Web Proxy Cache. Network Agent also must be reinstalled.

1. Stop any antivirus program and firewall on the machine.
2. Reinstall Filtering Service and Network Agent.

   See *Installing Web Security components*, page 668 for instructions.
3. When installing Filtering Service:
   a. On the **Integration Option** screen, select **Integrated with another application or device** and then click **Next**.
   b. On the **Select Integration** screen, select **Squid Web Proxy Cache**.
   c. On the **Filtering Plug-In** screen, select *only* **Install other selected components** (do *not* select **Yes, install the plug-in on this machine**).
4. Follow the remaining installer prompts to complete the installation.
5. If you stopped your antivirus software, start it.
6. If you stopped a firewall, start it.
7. Make sure that all Websense components are running.
   - **Linux**: Go to the Websense installation directory (/opt/Websense, by default) and enter the following command:

     ```
     ./WebsenseAdmin status
     ```

     If some services are not running, stop and then start them again by entering:

     ```
     ./WebsenseAdmin restart.
     ```

     **Warning**

     Do NOT use the **kill -9** command to stop Websense services. This procedure may corrupt the services.

   - **Windows**: Use the Windows **Services** dialog box.

8. Provide Network Agent with the IP address and port (default 3128) of all Squid Proxy Cache machines. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 270.

### Install the Squid plug-in

Next, the Squid plug-in must be installed on the machine running Squid Web Proxy Cache to enable communication between Websense software and Squid Web Proxy Cache.

See *Installing the Squid plug-in*, page 264.

## Converting to an integration on the same machine

After upgrading Web Filter or Web Security, you can convert it to be integrated with Squid Web Proxy Cache that is installed on the same machine.

**Important**

If you are installing Websense software on a machine running an SELinux-enabled Red Hat Enterprise Linux ES 4 operating system with the version of Squid that is prepackaged with the Red Hat installation, Squid cannot launch the Websense Squid plug-in (**WsRedtor**).

If the plug-in does not launch, Websense filtering cannot occur. Configure SELinux permissions so that **WsRedtor** can launch. See your Red Hat Enterprise Linux documentation for details.

For more information, and a discussion of other options for addressing this issue, see the troubleshooting topic *Internet requests are not being filtered*, page 282.

To convert to an integrated system, Websense Filtering Service and Network Agent must be removed and then reinstalled after Squid Web Proxy Cache is installed.

**Note**

Internet requests are not filtered until this process is completed.

1. Log on to the installation machine as **root**.
2. Install Squid Web Proxy Cache, following the instructions provided with that product.

   > **Important**
   > Be sure to install and configure Squid Web Proxy Cache so it is functional before integrating Websense software with it. See Squid documentation and support resources for instructions.

3. If you have not done so, upgrade your Websense software to the current version.
4. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
5. Close all non-Websense applications, including any firewall and antivirus software.
6. Ensure that Websense software is running. The uninstaller looks for Policy Server during the removal process.
7. Run the Web Security Linux uninstaller:
   a. Navigate to the Websense installation directory (/opt/Websense, by default).
   b. Run the following command:
      ```
      ./uninstall.sh
      ```
      A GUI version is available on English versions of Linux:
      ```
      ./uninstall.sh -g
      ```
   The installer detects the installed Websense components and lists them.
8. Select Filtering Service and Network Agent (if installed), and then click **Next**.
9. Follow the prompts to remove the components.
10. Restart the machine, if prompted.
11. Start the Web Security Linux installer again.
12. On the **Add Components** screen, select **Install additional components on this machine**, and then click **Next**.
13. On the **Custom Installation** screen, select the following components and then click **Next**:
    - **Filtering Service**
    - **Network Agent**
    - **Filtering Plug-in**
14. On the **Integration Option** screen, select **Integrated with another application or device**.
15. On the **Select Integration** screen, select **Squid Web Proxy Cache**.
16. On the **Squid Configuration** screen, enter paths to the squid.conf and squid executable files, and then click **Next**.

The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

> **Note**
> The installer will automatically start Squid Web Proxy Cache once installation is complete. Verify it is running after installation is complete (Step 18 below).

17. Follow the remaining installer prompts to complete the installation.
18. Start Squid Web Proxy Cache if necessary.

    To install the filtering plug-in (i.e., Squid plug-in), the installer stops Squid Web Proxy Cache. At the end of the installation process, the installer automatically starts Squid Web Proxy Cache. In some cases, the installer is unable to start Squid Web Proxy Cache and it must be manually started:

    a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.
    b. If it is not running, start it.

       See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.
19. If you stopped a firewall, start it again.
20. To make sure that all Websense components are running, navigate to the Websense installation directory (/opt/Websense, by default) and enter the following command:

    ```
    ./WebsenseAdmin status
    ```

> **Warning**
> Do NOT use the **kill -9** command to stop Websense services. This procedure may corrupt the services.

21. If you stopped your antivirus software, start it again.
22. Provide Network Agent with the IP address for all Squid Proxy Cache machines. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 270.

# Authentication when integrated with Squid Web Proxy Cache

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

Authentication is the process of identifying a user within a network based on an account in a directory service. Depending on the authentication method selected, Squid Web Proxy Cache can obtain user identification and send it to Websense Filtering Service along with an Internet request. Filtering Service can filter requests based on policies assigned to individual directory objects, defined as either a user or group of users.

> **Note**
> In any environment, Websense software can filter based on computer or network policies. Workstations are identified in Websense software by their IP addresses, and networks are identified as IP address ranges

To filter Internet access for individual directory objects, Websense software can identify the user making the request, imploying the following methods:

- Enable an authentication method within Squid Web Proxy Cache so that it sends user information to Websense software.
- Enable Websense software to identify users transparently, if it does not receive user information from Squid Web Proxy Cache. You can install one of the Websense transparent identification components: DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent.

  See the Transparent Identification of Users technical paper and the User Identification topic in the TRITON - Web Security Help for more information.

- Enable manual authentication within Websense software. If users cannot be identified transparently, they are prompted for authentication when they open a browser.

  See the Manual Authentication topic in the TRITON - Web Security Help for more information.

## Client types

In this context, the term **clients** refers to computers or applications that run on computers and rely on a server to perform some operations. Each type of client can be configured so that Filtering Service is able to obtain user identification and filter Internet requests based on user and group policies.

Squid works with two types of clients:

- Firewall
- Web Proxy

### Firewall clients

If a client is located behind a firewall, that client cannot make direct connections to the outside world without the use of a parent cache. Squid Web Proxy Cache does not use ICP queries for a request if it is behind a firewall or if there is only one parent.

Use the following lists in the **squid.conf** file to handle Internet requests.

- **never_direct**: Specifies which requests must be forwarded to the parent cache outside the firewall.
- **always_direct**: Specifies which requests must not be forwarded.

See Squid documentation and support resources for more information.

### Web Proxy clients

Web Proxy clients send Internet requests directly to Squid Web Proxy Cache after the browser is configured to use Squid as the proxy server.

You can assign individual user or group policies:

- Enable one or more of the Squid authentication methods, discussed in *Authentication methods*, page 280 if the network uses multiple types of browsers. Some of these methods may require users to authenticate manually.
- Enable Websense software to prompt users for authentication. This allows Websense software to obtain the user information it needs if it does not receive that information from Squid Web Proxy Cache. See the Manual Authentication section of the *User Identification* topic in the TRITON - Web Security Help.

# Authentication methods

Squid Web Proxy Cache v2.5 and 2.6 offer the following authentication methods:

- *Anonymous authentication*
- *Basic authentication*
- *Digest authentication*
- *Integrated Windows authentication*

See Squid documentation for information about enabling authentication within Squid Web Proxy Cache.

**Important**

Before changing authentication methods, consider the impact the change would have on other proxy server functions.

## Anonymous authentication

When anonymous authentication is enabled within Squid Web Proxy Cache, user identification is not received from the browser that requests a site.

Users cannot be filtered based on individual user or group policies unless anonymous authentication is disabled and another method of authentication is enabled, or you configure Websense software to identify users.

Anonymous authentication allows Internet filtering based on computer or network policies, if applicable, or by the Default policy.

## Basic authentication

When basic authentication is enabled within Squid, users are prompted to authenticate (log on) each time they open a browser. This allows Squid to obtain user identification, regardless of the browser, and send it to Websense Filtering Service, which then filters Internet requests based on individual user and group policies. Basic authentication can be enabled in combination with Integrated Windows authentication, discussed later in this section.

## Digest authentication

Digest authentication is a secure authentication method used only in Windows 2000 and Windows Server 2003 domains. The features are the same as Basic authentication, but the user name and password are scrambled when they are sent from the browser to Squid Web Proxy Cache. The user can authenticate to Squid Web Proxy Cache without the user name and password being intercepted. Digest authentication can be enabled in combination with Integrated Windows authentication, discussed later in this section.

### Integrated Windows authentication

Integrated Windows authentication provides secure authentication. With this authentication enabled, Squid Web Proxy Cache obtains user identification transparently from Microsoft Internet Explorer 5.0 and later. User information is sent to Websense software, which then filters Internet requests based on individual user and group policies.

> **Note**
> Squid Integrated Windows Authentication cannot obtain user identification information transparently from browsers other than Microsoft Internet Explorer.

If your network has a mixture of Microsoft Internet Explorer browsers and other browsers, you can enable both Basic and Integrated Windows authentication, or Digest and Integrated Windows authentication. In either configuration:

- Users with Microsoft Internet Explorer browsers are identified transparently.
- Users with other browsers are prompted to authenticate.

> **Note**
> To transparently identify all users in a mixed-browser environment, you can enable Anonymous authentication within Squid Web Proxy Cache and use Websense transparent identification. See *Transparent identification*, page 281.

## Transparent identification

If Squid Web Proxy Cache is not configured to send user information to Websense software, you can install a Websense transparent identification agent to identify users without prompting them to log on when they open a browser. There are 4 transparent identification agents: DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent. They communicate with domain controllers or directory services to match users names with IP addresses for use in applying user- and group-based policies.

The transparent identification agents can be installed individually or in specific combinations, and can reside on the Filtering Service machine, or on a different machine. See the Transparent Identification of Users technical paper and TRITON - Web Security Help for more information about deploying and configuring Websense transparent identification agents.

# Troubleshooting Squid Web Proxy Cache integration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

This information applies to Web Filter or Web Security when integrated with Squid Web Proxy Cache.

## Network Agent is not filtering or logging accurately

If you have configured your Squid machine to act as a proxy server for Internet traffic, you must define the IP address of the proxy server machine in TRITON - Web Security. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 270.

## Internet requests are not being filtered

If you integrated Websense software with the Squid Web Proxy Cache on a machine running the Red Hat Enterprise Linux 4.7 operating system, and Websense filtering is not working, the problem may be the Security-enhanced Linux (SELinux) configuration.

The Red Hat Enterprise Linux 4.7 operating system installs SELinux by default. The SELinux installation is a kernel modification that reduces root user and hierarchical privilege vulnerabilities. The default SELinux installation packaged with Red Hat Enterprise Linux 4.7 prevents Squid from launching the Websense Squid Plug-in (**WsRedtor**). If **WsRedtor** does not launch, filtering cannot occur.

To determine if this is the problem, verify that **WsRedtor** is not launching on the Red Hat Enterprise Linux machine:

- **WsRedtor** does not appear in the process command list, although other Websense services do.

- Error messages associated with **WsRedtor** appear in the Squid **cache.log** (see Squid documentation for the location of this log file).
- Error messages associated with **WsRedtor** appear in the Linux system log (located by default at /var/log/messages).

If you determine that **WsRedtor** is not launching, there are several options to resolve the issue:

- Do not install Websense software on a machine using an SELinux-enabled Red Hat Enterprise Linux operating system and the version of Squid prepackaged with that Red Hat installation. If SELinux is **not** enabled, you can install Websense software on a machine using a Red Hat Enterprise Linux operating system and the prepackaged version of Squid.
- Before you install Websense software on a machine using an SELinux-enabled Red Hat Enterprise Linux operating system, you can install Squid Web Proxy Cache directly from the official Squid Web site at www.squid-cache.org. This Squid installation does not stop `WsRedtor` as does the version packaged with the Red Hat Enterprise Linux ES release 4 operating system.
- If you are familiar with configuring permissions for SELinux-enabled Red Hat, you can configure permissions so that `WsRedtor` can launch. See your Red Hat Enterprise Linux ES documentation for instructions. Additional information about SELinux is available at www.nsa.gov/selinux/.

## Outgoing Internet traffic seems slow

If outgoing Internet traffic is slower than expected, increase the number of redirectors spawned by Squid. In the**squid.conf** file, go to the**redirect_children** tag (v2.5) or the **url_rewrite_children** tag (v2.6), and increase the number by 10. The current default is **30**.

If the performance continues to be slow, consult Squid documentation and check your network settings.

## Squid Web Proxy Cache crashes because it cannot launch Squid plug-in (WsRedtor)

If Squid Web Proxy Cache fails to start, check the**cache.log** file (by default, located in **/usr/local/squid/logs/**).

> **Note**
> This section discusses only one possible reason for Squid Web Proxy Cache to crash. Squid Web Proxy Cache may have crashed for some other reason (for example, configuration error). See your Squid documentation.

After startup messages, the log indicates startup of WSRedtor processes. For example:

```
<timestamp>| helperOpenServers: Starting 30 'WsRedtor'
processes
```

The log may then indicate errors while starting the processes due to a missing file. For example (message appears multiple times):

```
(WsRedtor): error while loading shared libraries:
<filename>: cannot open shared object file: No such file or
directory
```

After that, the log indicates redirectors (i.e., WsRedtor) failed. For example (message appears multiple times):

```
<timestamp>| WARNING: redirector #<x> (FD <y>) exited
```

Finally, the log indicates a fatal error. For example:

```
FATAL: The redirector helpers are crashing too rapidly, need
help!
```

If you see entries like this in cache.log, a file required by the redirectors is missing. Such files reside in two places: **../Websense/bin** and **/etc/wsLib**. A copy of each file must be in both directories. The above errors are occurring because a file is missing from the **/etc/wsLib** directory.

To correct this issue:

1. Look in **../Websense/bin** for the missing file indicated in cache.log (i.e., <*filename*> in the example log entry above).

   If you do not find the missing file in **../Websense/bin**, then the crash may be due to another issue. Contact Websense Technical Support.

   > **Note**
   > Websense Technical Support can provide support for Squid Web Proxy Cache for issues related to Websense software only. If you are experiencing problems with your installation of Squid Web Proxy Cache for reasons unrelated to Websense software, you must refer to Squid documentation and support resources.

2. Copy the missing file from **../Websense/bin** to **/etc/wsLib**.

   > **Important**
   > **Copy**, do not move, the file. A copy of the file must reside in both **../Websense/bin** and **/etc/wsLib**.

3. Start Squid Web Proxy Cache.

   Note that if more than one file is missing from **/etc/wsLib**, you must repeat these steps for each file. Squid Web Proxy Cache indicates only one missing file at a time in cache.log.

# 19 Check Point Integration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



Related topics:



## Overview

This section of the Websense Technical Library provides information specific to integrating Websense Web Filter or Web Security with Check Point® products. Refer to *Web Filter or Web Security (software-based)*, page 69 as your primary source of

installation information. Only additional or alternative steps required to integrate Web Filter or Web Security with Check Point prodcuts are provided here.

## Supported Check Point product versions

Websense Web Security and Websense Web Filter are compatible with the following Check Point products:

- FireWall-1 Feature Pack 1 or greater
- FireWall-1 NG AI
- FireWall-1 NGX

## How Websense filtering works with Check Point products

An integration with a Check Point product works with Websense components as follows:

- **Filtering Service**: Interacts with the Check Point product and Network Agent to filter Internet requests.
- **Network Agent**: Manages Internet protocols that are not managed by the Check Point product.

**Important**

Do *not* install Network Agent on the Check Point machine.

Check Point products provide network security and a framework for content filtering. Websense software communicates with the Check Point product via URL Filtering Protocol (UFP). Websense software is implemented as a UFP Server, and communicates with the Check Point product over TCP sockets. By default, Websense software listens on port 18182 for messages from the Check Point product.

To begin filtering:

- Client computers must point to the machine running the Check Point product as their default gateway. Typical networks implement this configuration for security reasons unrelated to filtering.

- The Check Point product must be configured to use a rule to analyze all HTTP requests, as well as FTP requests issued by a browser that proxies to the Check Point product. The rule must use the URI Specifications for HTTP.

> **Note**
> If Websense software must download the Master Database through a proxy server or firewall that requires authentication for any HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication.

When Websense software is integrated with a Check Point product, you define policies within TRITON - Web Security (the configuration interface for Websense software). These policies identify which of the Websense categories are blocked or permitted during different times and days. Within the Check Point product, you typically define a rule that directs the firewall to reject requests for sites in Websense categories whose action is set to block, limit by quota, or confirm. If a client selects an option to view a site with quota time on a block page, Websense software tells the Check Point product to permit the site.

When the Check Point product receives an Internet request for either an HTTP site or an FTP site requested by a browser that uses the firewall as a proxy, it queries Websense Filtering Service to determine if the site should be blocked or permitted.

Filtering Service checks the policy assigned to the client. Each policy designates specific time periods and lists the category filters that are in effect during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database to locate the category for the requested URL:

- If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies the Check Point product that the site is not blocked, and the client is allowed to see the site.

## Distributed environments

When the SmartCenter™ server (FireWall-1 Management Server in FireWall-1) is separated from the Enforcement Module (FireWall-1 Module in FireWall-1), modify your Rule Base to allow the SmartCenter Server to communicate with Websense Filtering Service during setup. This allows the Check Point product to load the Websense dictionary, which contains the categories Blocked and Not Blocked.

All other communication is between Filtering Service and the Enforcement Module. See Check Point documentation for instructions on modifying the Rule Base.

> **Note**
> It is a best practice to install Websense components on a different machine than the Check Point product. If you choose to install Websense software and the Check Point product on the same machine, see the Websense Knowledge Base for configuration instructions. Search the Websense Knowledge Base (at www.websense.com/SupportPortal/) for the terms*Installing Websense software on Check Point Firewall-1*.

## Client computers and Check Point products

Check Point products process HTTP requests transparently, so no Internet browser changes are required on client computers. You can have clients proxy to the firewall to enable user authentication within that firewall, or to enable filtering of FTP requests from a browser. See Check Point product documentation for instructions on handling FTP requests.

If clients use the firewall as a proxy, browsers on client computers must be configured to support proxy-based connections.

## Communicating with Websense software

Depending on which Check Point product is running, Websense software may communicate with the firewall through a secure connection or a clear connection.

- A secure connection requires that communication between the Check Point product and the Websense UFP Server is authenticated before any data is exchanged.
- A clear connection allows Websense software and the Check Point product to transfer data without restrictions.

The connection options for each supported Check Point product version are similar, but have some slight differences.

- **FireWall-1 NGX** or **FireWall-1 NG with Application Intelligence (AI)**: clear connection is the default. An authenticated connection can be established, but is not recommended because of performance issues. In addition, a clear connection is required to use the Enhanced UFP Performance feature described in the next section.

- **FireWall-1 NG Feature Pack 1 or later**: clear connection is the default, but a Secure Internal Communication (SIC) trust connection can be configured within both Check Point and Websense software.

See *Chapter 20: Configuring Check Point Products to Work with Web Filter or Web Security, Configuring Check Point Products to Work with Web Filter or Web Security* for the appropriate procedures to establish secure or clear communication with the Websense software.

## Enhanced UFP performance

The enhanced UFP performance feature increases the amount of traffic that Websense software and the Check Point product can filter while reducing CPU load.

Configuring enhanced UFP performance requires the proper settings in both Websense software and the Check Point product. See *Configuring enhanced UFP performance*, page 302 for detailed configuration procedures.

**Note**

To use enhanced UFP performance, Websense software and the Check Point product must be configured for clear communication.

## Installing Web Filter or Web Security to integrate with Check Point

Refer to *Installing Web Security components*, page 668 for complete installation instructions. When installing Filtering Service, follow the installation instructions until prompted to select an integration option.

- On the **Integration Option** screen, select **Integrated with another application or device**.
- On the **Select Integration** screen, select **Check Point**.
- If Network Agent is included in this installation, a warning advises against installing Network Agent on the same machine as the firewall. An exception allows Websense software and the firewall to be installed on an appliance with separate virtual processors to accommodate both products.
  - Select **Yes, install Network Agent** only if the machine has separate virtual processors.
- Follow the remaining screens in the Websense installer to complete the installation.

- See *Configuring Check Point Products to Work with Web Filter or Web Security*, page 291 for information on configuring the firewall integration with Websense software.

## Initial setup

If Filtering Service is installed on a multihomed machine, or on the machine that is running the Check Point product (not recommended), identify Filtering Service by its IP address in your network so that Websense block messages can be sent to users.

See *Identifying Filtering Service by IP address*, page 769 for instructions.

## Upgrade

Before upgrading Websense software, make sure your Check Point product is supported by the new version. See *Supported Check Point product versions*, page 286.

Follow the instructions in *Upgrading Web Security or Web Filter to 7.6.0*, page 829.

Update the Check Point dictionary with new Websense settings, and update the Websense Resource Object in SmartCenter before you begin filtering with the new version of Websense software.

For more information, see *Configuring Check Point Products to Work with Web Filter or Web Security*, page 291.

## Migrating between Check Point versions

If you plan to upgrade your Check Point product (from FireWall-1 NG to FireWall-1 NGX, for example), do so *after* upgrading the Websense software.

**Important**

Do not make any additional modifications to your Websense software until after you have upgraded your firewall product.

See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions on upgrading Websense software.

See Check Point documentation for information on upgrading the Check Point software.

See *Configuring Check Point Products to Work with Web Filter or Web Security*, page 291 for the necessary configuration procedures to ensure that your new version of the Check Point product can communicate with Websense software.

# 20 Configuring Check Point Products to Work with Web Filter or Web Security

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

In addition to defining Websense filtering policies and assigning them to the appropriate clients, you must set up the Check Point product with the necessary objects and rules. In describing these objects and rules, this chapter assumes that you are familiar with general Check Point product concepts.

The following tasks must be completed before you begin to configure the Check Point product to communicate with Websense software:

- Both the Check Point product and either Websense Web Security or Websense Web Filter must be installed and running.
- In the Check Point product, create:
  - An object for the firewall itself, if it does not already exist (it typically is created by default upon installation of the Check Point product).
  - Objects that represent your network topology (as needed for filtering).

  See Check Point product documentation for more information on objects.

Configuring FireWall-1 NG, FireWall-1 NG with AI, and FireWall-1 NGX for Websense content filtering involves the following procedures:

- Create a network object for the machine running Websense Filtering Service. See *Creating a network object*, page 292.
- Create an OPSEC™ application object for the Websense UFP Server. See *Creating an OPSEC application object*, page 294.
- Create URI resource objects for the dictionary categories that Websense software sends to the Check Point product. See *Creating Resource Objects*, page 296.
  - When creating the URI resource objects, you can configure both Websense software and the Check Point product to use Secure Internal Communication (SIC), rather than the default clear communication. See *Establishing Secure Internal Communication*, page 307.
  - To return to clear communication, see *Restoring Clear Communication*, page 315.
- Define rules that govern how the Check Point product behaves when it receives a response from Websense software. See *Defining rules*, page 299.
- Optionally, you can configure the Check Point product for enhanced UFP performance. This applies only to FireWall-1 NG with Application Intelligence and FireWall-1 NGX. Make sure that you have configured the Check Point product for Websense content filtering before this procedure. See *Configuring enhanced UFP performance*, page 302.

**Note**

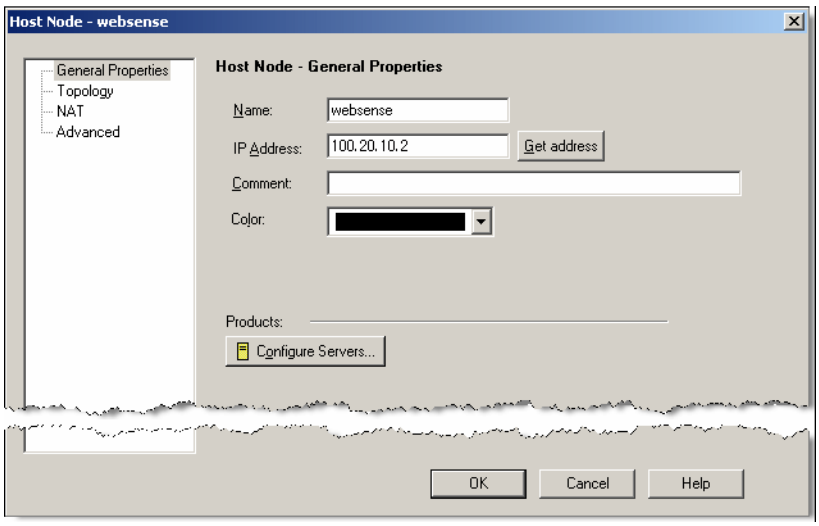
The procedures and illustrations in this chapter are based on FireWall-1 NGX. If FireWall-1 NG or FireWall-1 NG with Application Intelligence (AI) is running, you may notice slight differences in screens and field names.

# Creating a network object

1. Open a Check Point SmartConsole, such as SmartDashboard™ (*Policy Editor* in earlier versions). See your Check Point product documentation for detailed instructions on using SmartConsole.
2. If you have not already done so, create a network object (**Manage > Network Objects > New > Node > Host**) for the machine running Filtering Service.

   This object is required only if Websense software runs on a separate machine behind the firewall, as recommended.

3. Select **General Properties** in the left column. The following dialog box appears.



4. Complete the items in the page:

| Field | Description |
|---|---|
| **Name** | Enter a descriptive name for the network object representing the machine on which Filtering Service is running, such as **Websense** (make a note of this name for later use).<br>Note: If your DNS is configured to resolve machines within your network, enter the Filtering Service machine's host name here. Then, for IP Address, you can click **Get address** to resolve the host name to its IP address automatically. |
| **IP Address** | Enter the IP address of the machine running Filtering Service.<br>Note: If you entered a host name for Name, you can click **Get address** to find the machine's IP address automatically. See the description for Name, above, for more information. |
| **Comment** | Enter a description for this object. |
| **Color** | Select a color for displaying this object in SmartDashboard. |

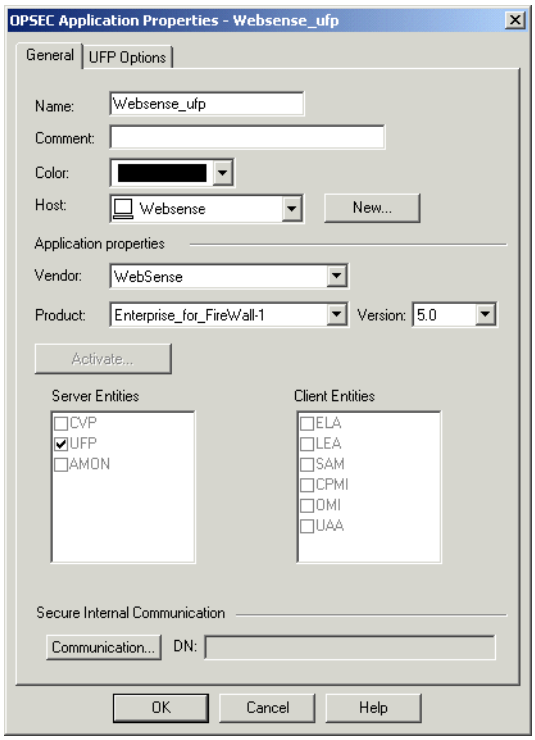
5. Click **OK**.

## Creating an OPSEC application object

After you create the network object for the machine running Filtering Service, you must create an OPSEC application object for the Websense UFP Server. The UFP server was installed with the other components when you chose Check Point as your integration product during installation.

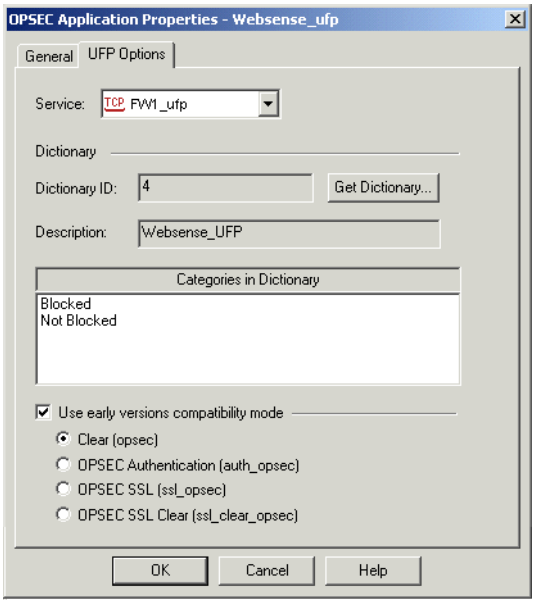
1. Open SmartDashBoard, if it is not already open.
2. Select **Manage > Servers and OPSEC Applications**.
3. Click **New**, and then select **OPSEC Application** from the drop-down list.
4. Select the **General** tab in the OPSEC Application Properties dialog box.

5. Complete the items on the tab:




| Field | Description |
|---|---|
| **Name** | Enter a descriptive name, such as **Websense_ufp** (make a note of this name for later use). |
| **Comment** | Enter a description for this object. |
| **Color** | Select a color for displaying this object in SmartDashboard. |
| **Host** | Select the network object created in the previous section. This object identifies the machine running Filtering Service.<br>If you have not yet created this object, click **New** to create it. See *Creating a network object*, page 292 for instructions. |
| **Vendor** | Select **Websense**. |
| **Product** | This value is not used in creating an object and does not need to be changed. |
| **Version** | This value is not used in creating an object and does not need to be changed. |
| **Server Entities** | **UFP** is checked automatically when you select Websense as the Vendor, and.cannot be changed. |

6. Select the **UFP Options** tab.




OPSEC Application Properties – UFP Options tab

7. Check the **Use early versions compatibility mode** option (**Backwards Compatibility** in earlier versions).
   - If Secure Internal Communication (SIC) is used, go to *Establishing Secure Internal Communication*, page 307, to complete this section.
   - If SIC is not used, select **Clear (opsec)**.
8. Click **Get Dictionary**.

   Websense software provides the Check Point product with a dictionary containing these categories: **Blocked** and **Not Blocked**. The full set of Websense categories is configured via TRITON - Web Security. See TRITON - Web Security Help for more information.
9. Click **OK**.
10. Close the OPSEC Applications dialog box.
11. Select **Policy** > **Install** to install the policy on the firewall.

    See the Check Point product documentation for more information.

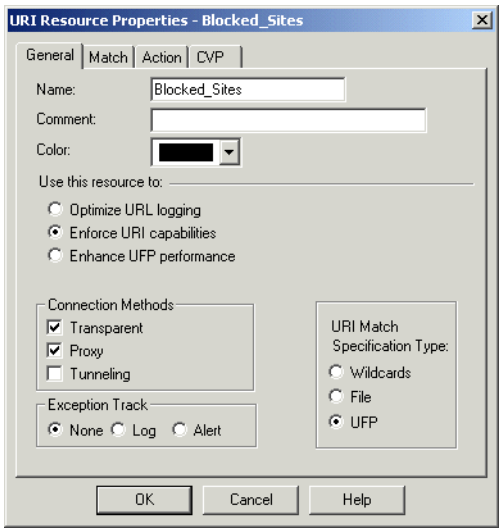
# Creating Resource Objects

Create a Resource Object to define a Uniform Resource Identifier (URI) that uses the HTTP protocol. This URI identifies the Websense dictionary category *Blocked*.

1. Open SmartDashboard and select **Manage** > **Resources**.

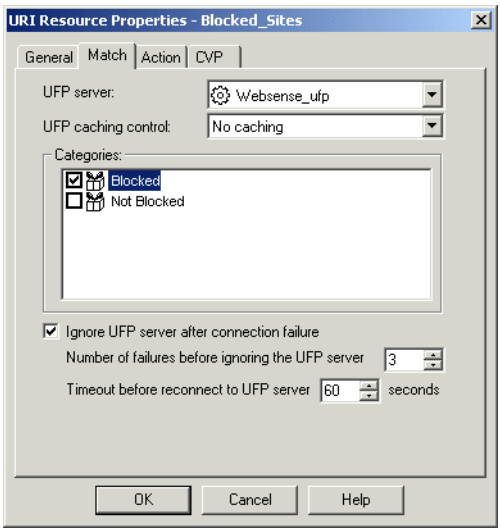
   The Resources dialog box appears.

2. Click **New**, and choose **URI** from the submenu to display the URI Resource Properties dialog box.
3. Select the **General** tab, and complete the items in the tab.




| Field | Description |
|---|---|
| **Name** | Enter a name for this URI Resource Object, such as **Blocked_Sites**. |
| **Comment** | Enter a description for this object. |
| **Color** | Select a color for this object's icon. |
| **Use this resource to** | Select **Enforce URI capabilities**.<br>This option enables all other functionality of the URI resource, such as configuring CVP checking on th**€CVP** tab.<br>All basic parameters defining schemes, hosts, paths, and methods apply. The URL is checked for these parameters. |
| **Connection Methods** | Mark both the Transparent and the Proxy check boxes. |
| **Exception Track** | Select the desired method for tracking exceptions. See the Check Point product documentation for more information. |
| **URI Match Specification Type** | Select **UFP**. |

4. Select the **Match** tab, and complete the items in the tab.




| Field | Description |
|---|---|
| **UFP server** | Select the OPSEC Application object that was created for the Websense UFP Server in *Creating an OPSEC application object*, page 294. |
| **UFP caching control** | Select a caching option.<br>**No caching** is the recommended setting for most networks. |
| **Categories** | Mark the **Blocked** check box. |
| **Ignore UFP server after connection failure** | • Mark this check box to permit full HTTP and FTP access if Websense Filtering Service is not running or cannot be contacted.<br>Dependent fields allow you to set the number of times the Check Point product tries to contact Websense software before ignoring it, and the length of time the Check Point product ignores Websense software before attempting to reconnect.<br>• Clear this check box to block all HTTP and FTP access when Filtering Service is not running. |

5. Click **OK**.
6. Close the Resources dialog box.
7. Select **Policy** > **Install** to install the policy on the firewall.

   See Check Point product documentation for more information.

# Defining rules

This section describes a content filtering scenario and its configuration. It includes information about the objects and rules that are needed to implement the suggested configuration.

> **Note**
>
> The configuration described in this section assumes that all clients have a default route set to the firewall and do not proxy to the firewall.
>
> This configuration also assumes that the recommended network configuration is being used: Websense software is running on a separate machine, behind the firewall, and caching is disabled.

In this scenario, the Check Point product denies access to any site that Websense software indicates is blocked, and allows access to any site that Websense software indicates is not blocked. The actual sites blocked may vary according to the computer making the request.

Use TRITON - Web Security to define policies that block the appropriate categories, and assign them to the desired computers or directory objects.

For example, you might modify the Default policy to use a category filter that blocks access to all categories except the Travel, and Business and Economy categories. This policy is applied to most computers.

A separate, more liberal policy could be defined for managers, which blocks only those categories considered a liability risk, such as Adult Material and Gambling. This policy, called Management, would be assigned to the computers used by top managers.

After the Websense policies are configured, you define rules in the Check Point product to prevent access to any site that Websense software indicates is blocked.

To set up this configuration in the Check Point product, you must create one URI Resource Object and one Network Object, and define two rules.

- Create a URI Resource Object for the Blocked category as described in *Creating Resource Objects*, page 296.

  In this example, the URI Resource Object is called Blocked_Sites because Websense software is configured to block sites that are not required for business purposes.
- Create a Network Object that encompasses all machines on the internal network. This example assumes that everyone in the company is on the internal network. For this example, the Network Object is called Internal_Network.

- Add the rules to the Security Rules Base. The sequence of the rules is important, because the Check Point product evaluates the rules sequentially, from top to bottom.

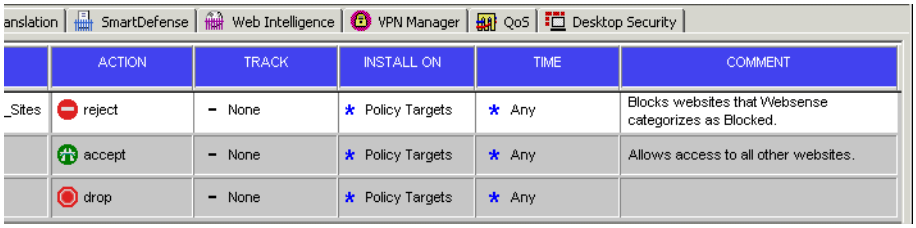
  **RULE 1**: Blocks access to undesirable Web sites. Add the new rule at an appropriate location in the Rule Base:

| | |
|---|---|
| **Name** | (NGX only) Enter a descriptive name for the rule, such as **Websense Block** |
| **Source** | Add Internal_Network |
| **Destination** | Any (default) |
| **Service** | Add with Resource<br>In the Service with Resource dialog box, select **HTTP**. Under **Resource**, select **Blocked_Sites** from the drop-down menu. This object was created in *Creating Resource Objects*, page 296. |
| **Action** | Reject |
| **Track** | None |
| **Install On** | Policy Targets |
| **Time** | Any (default) |
| **Comment** | (NGX only) Enter a more detailed description of the rule. |

  **RULE 2**: The second rule allows access to all other Web sites. Add the second rule *after* Rule 1.

| | |
|---|---|
| **Name** | (NGX only) Enter a descriptive name for the rule, such as **Websense Allow** |
| **Source** | Add Internal_Network |
| **Destination** | Any (default) |
| **Service** | Add/HTTP |
| **Action** | Accept |
| **Track** | None |
| **Install On** | Policy Targets |
| **Time** | Any (default) |
| **Comment** | (NGX only) Enter a more detailed description of the rule. |

The following illustrations provide examples of Security Rule Base after the rules are defined.


After defining the rules described above,**Verify** and **Install** the policy from the**Policy** menu. See Check Point product documentation for more information.

**Important**

For normal operation, set **Track** to **None** in the Websense rules. This disables logging in the Check Point product.

When logging is enabled for these rules, the log files become very large, and adversely impact performance. Configure other options in the **Track** field only when you are testing and troubleshooting.

When the Check Point product receives an HTTP request, it sends Websense software the address of the requested site, as well as the IP address of the computer requesting the site.

For example, the CNN Web site is requested by a top manager. Websense software categorizes the site as News and Media. Websense software indicates that the site is Not Blocked under the Management policy that you defined in TRITON - Web Security. The Check Point product allows the site according to Rule 2.

If the CNN site was requested from an accounting clerk's computer, Websense software indicates that the site is Blocked because that computer is governed by the Websense Default policy, which blocks the News and Media category. The Check Point product denies the request according to Rule 1, and a Block Page is displayed on the clerk's computer.

Any time a computer requests a site not categorized by the Websense Master Database, Websense software indicates that the site is not in the database. The Check Point product allows access to the site according to Rule 2.

# Configuring enhanced UFP performance

Enhanced UFP performance improves the performance of the UFP Server by increasing the amount of traffic that Websense software and the Check Point product can filter while reducing CPU load.

Configuring enhanced UFP performance requires the proper settings in Websense Web Security or Websense Web Filter, and in the Check Point product. In order to use enhanced UFP Performance, clear communication is required between Websense software and the Check Point product.

> **Note**
> Before performing the following procedures, make sure you have configured the Check Point product for content filtering with Websense software, as described earlier in this chapter.

## Websense configuration

Before configuring the Check Point product for enhanced UFP performance, open the **ufp.conf** file and make sure Websense software is configured for clear communication:

1. On the Websense Filtering Service machine, navigate to the directory where the Check Point integration files are installed. The default directories are:
   - **Windows**: C:\Program Files or Program Files (x86)\Websense\Web Security\bin
   - **Linux**: /opt/Websense/bin
2. Open the **ufp.conf** file in any text editor.

   The file must contain the following line to be configured for clear communication:

   ```
   ufp_server port 18182
   ```

   Additional lines that appear in this file are used for Secure Internal Communication, and must be commented out using the comment symbol (#):

   ```
   #ufp_server auth_port 18182
   #opsec_sic_policy_file ufp_sic.conf
   #opsec_sic_name “place_holder_for_opsec_SIC_name”
   #opsec_sslca_file opsec.p12
   ```
3. Edit the file, if necessary, to match the commands in the previous step.
4. Save and close the **ufp.conf** file.
5. Stop and restart the Websense UFP Server:
   - **Windows**: Use the Windows Services dialog box.
   - **Linux**: Use the **./WebsenseAdmin restart** command.

See *Starting or Stopping Web Security Services*, page 923 for instructions on stopping and restarting Websense services. See also *Stopping and restarting the UFP Server*, page 313.

## Check Point product configuration

To configure for enhanced UFP performance in the Check Point product:

- Configure the OPSEC Application object for the Websense UFP Server to operate in *early versions compatibility mode* (previously known as *backwards compatibility mode*) for clear communication.

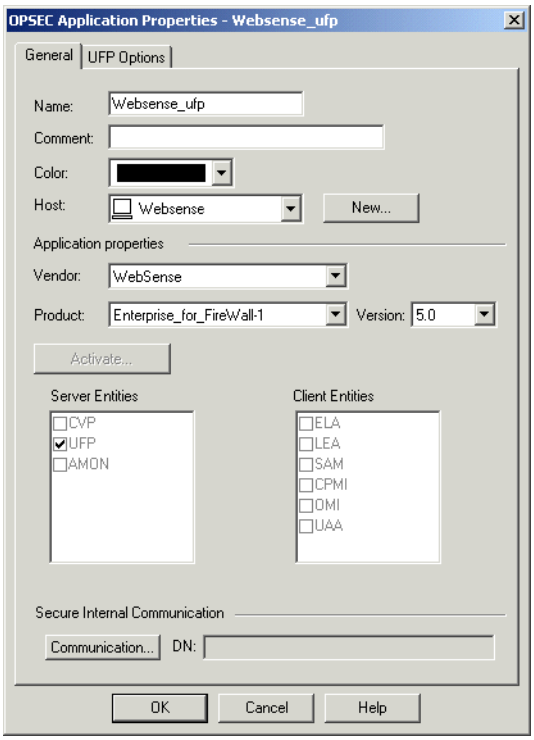
  Clear communication is the default for FireWall-1 NG with AI and FireWall-1 NGX. See *Early versions compatibility mode*, page 303.
- Configure the URI Resource Object that identifies the Websense dictionary category Blocked for enhanced UFP performance. See *Enhanced UFP performance*, page 305.

### Early versions compatibility mode

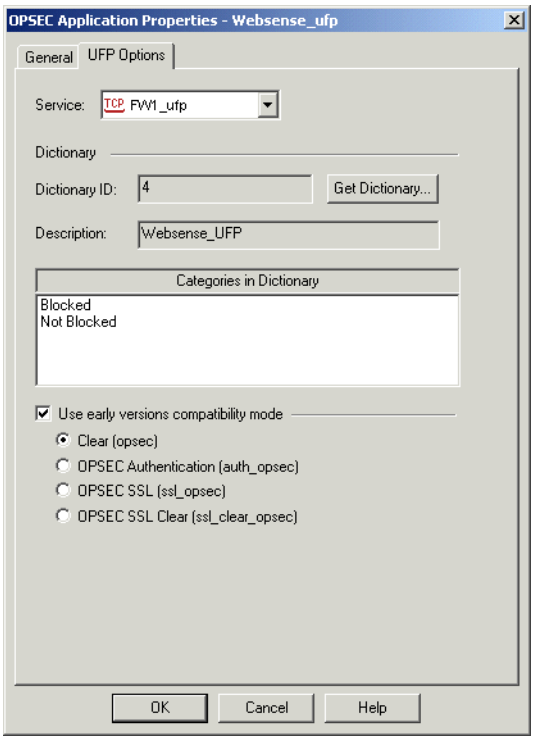
Follow these steps to configure the previously created OPSEC Application object for the Websense UFP Server to operate in early versions compatibility mode (clear communication) for enhanced UFP performance.

1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
2. Double-click on the OPSEC Application object you created for the Websense UFP Server in *Creating an OPSEC application object*, page 294.

The OPSEC Application Properties dialog box for this object appears.




3. Select the **UFP Options** tab.




4. Select **Use early versions compatibility mode** (**Backwards Compatibility** in earlier versions).
5. Select **Clear (opsec)**.

6. Click **OK**.
7. Close the Servers and OPSEC Applications dialog box.
8. Select **Policy** > **Install** to install the policy on the firewall. See Check Point product documentation for more information.

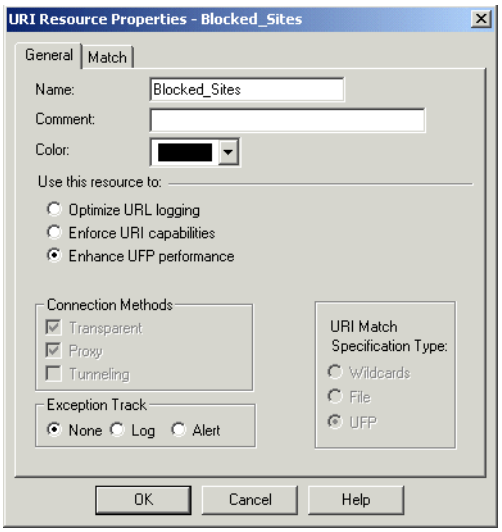
## Enhanced UFP performance

To configure the previously created URI Resource Object that identifies the Websense dictionary category Blocked for enhanced UFP performance:

1. Open the SmartDashboard, and select **Manage** > **Resources**.

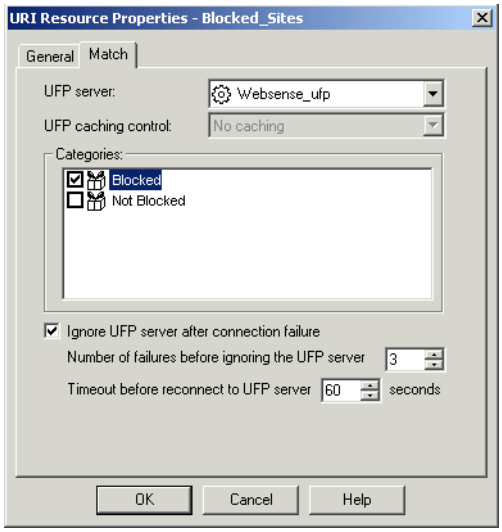
   The Resources dialog box appears.
2. Double-click on the Resource Object you created for the Websense dictionary category Blocked in *Creating Resource Objects*, page 296.

   The URI Resource Properties dialog box for this resource appears.




3. In the **General** tab, select **Enhance UFP performance**.

4. Select the **Match** tab.




5. Reselect the OPSEC Application object for the Websense UFP Server in the**UFP server** field. In this example, the object is named **Websense_ufp**.
6. Clear and then mark the **Blocked** category, and click **OK**.
7. Close the Resources dialog box.
8. Select **Policy > Install** to install the policy on the firewall. See the Check Point product documentation for more information.

# 21 Configuring Check Point Secure Communication

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

Secure Internal Communication (SIC) may be needed when you integrate a Check Point product with Websense software. Following are instructions for enabling this communication method, as well as instructions for disabling this communication method (see *Restoring Clear Communication*, page 315).

## Establishing Secure Internal Communication

If Websense software is integrated with a FireWall-1 NG version, you can configure both programs to use Secure Internal Communication (SIC). A secure connection requires that communication between the Check Point product and the Websense UFP Server be authenticated before any data is exchanged.

> **Note**
> The use of SIC with Websense software creates performance problems and is not recommended for networks with more than 100 users.

After installing Filtering Service, establish an SIC trust between the Check Point product and Websense software:

- Configure the OPSEC Application object for the Websense UFP Server within the Check Point product to use Secure Internal Communication. See *Configuring the Check Point product to use SIC*, page 309.
- Configure Websense software to use Secure Internal Communication. See *Configuring Websense software to use SIC*, page 311.
- Update the OPSEC Application object within the Check Point product to receive secure communications from Websense software. See *Updating the OPSEC Application object*, page 313.

## Prerequisites

The following must be completed before you begin to configure the Check Point product to communicate with Websense software, as described in Chapter 2 of this Supplement.

- Both the Check Point product and Websense software must already be installed and running.
- In the Check Point product, create the following objects:
  - An object for the firewall. Consult Check Point product documentation for instructions.
  - Network Objects that represent your network topology (as needed for your filtering goals) must exist. Consult Check Point product documentation for instructions.
  - You must create the OPSEC Application object for the Websense UFP Server before Websense software can establish SIC. If you have not already done this, see the procedures in *Creating an OPSEC application object*, page 294.

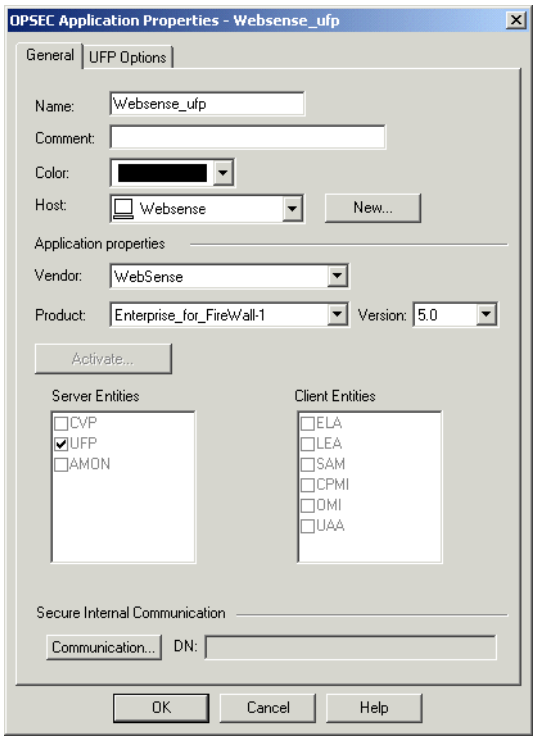
**Note**

Do **not** perform the procedures in this section if you are using an earlier version of FireWall-1 (before FireWall-1 NG Feature Pack 1).

## Configuring the Check Point product to use SIC

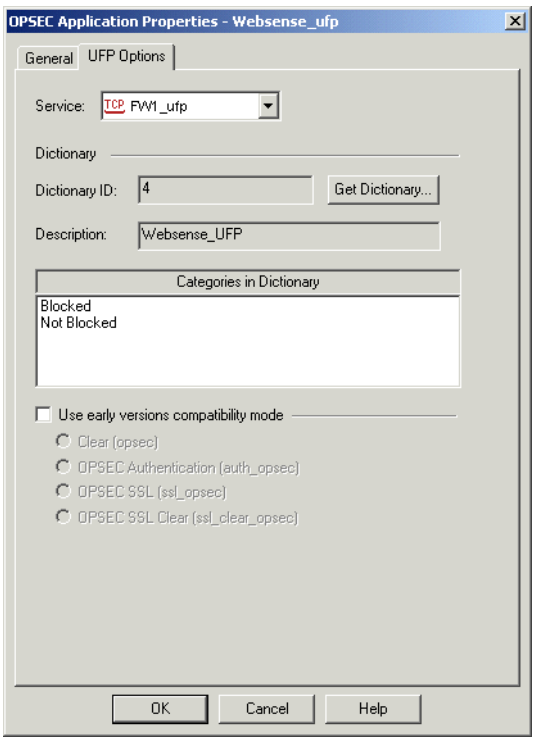
1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
2. Double-click the OPSEC Application object you created for the Websense UFP Server in *Creating an OPSEC application object*, page 294.

   The OPSEC Application Properties dialog box for this object appears.



3. If clear communication (for early version compatibility mode) is enabled, disable it:

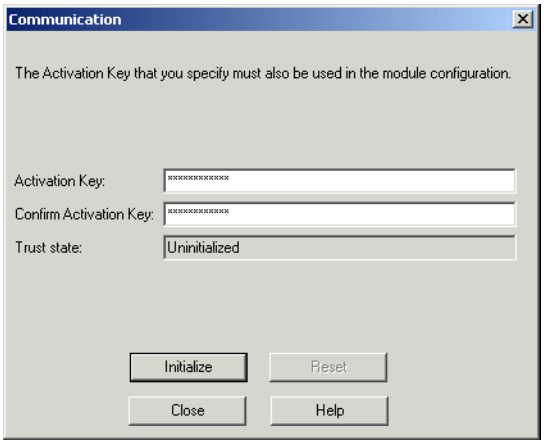
   a. Go to the **UFP Options** tab of the OPSEC Application Properties dialog box for this object.




   b. Make sure the **Use early versions compatibility mode** check box is *not* selected. (This field was called **Use backwards compatibility mode** in earlier versions.)

4. Click **Communication**.

   The Communication dialog box appears.



5. Enter and confirm an **Activation Key** (password) for communication between Websense Filtering Service and the Check Point product. (Make a note of this password for later use.)
6. Click **Initialize**.

   The **Trust state** field must show **Initialized but trust not established**.
7. Click **Close** to return to the OPSEC Application Properties dialog box.
8. Click **OK**.
9. Close the Servers and OPSEC Applications dialog box.
10. Select **Policy** > **Install** to install the policy on the firewall. See the Check Point product documentation for more information.

## Configuring Websense software to use SIC

Use this procedure to obtain a SIC certificate from the Check Point product, and configure Websense software to use it. After you complete this procedure, Websense software sends this certificate each time it communicates with the Check Point product.

1. Open a command prompt on the Websense Filtering Service machine and navigate to the directory containing the Check Point integration files (C:\Program Files or Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin, by default).
2. Enter the following command:

   **opsec_pull_cert –h** <*host*> **-n** <*object*> **-p** <*password*> **-o** <*path*>

   The table below explains the variables for this command.

| Variable | Description |
|---|---|
| <*host*> | The IP address or machine name of the computer on which the SmartCenter Server (Management Server in earlier versions) is installed. This IP address may be the same machine as the Enforcement (FireWall) Module or a different machine. |
| <*object*> | The name of the OPSEC Application object created for the Websense UFP Server. |
| <*password*> | The activation key that you entered for the named OPSEC Application object. See *Configuring the Check Point product to use SIC*, page 309. |
| <*path*> | Path to the output certificate file, **opsec.p12**. This variable must be expressed as a complete path.<br>• If the OPSECDIR variable already exists, the default path is **$OPSECDIR/opsec.p12**.<br>• If the OPSECDIR variable does not exist, the opsec.p12 file is created in the same folder as the **opsec_pull_cert.exe** file (Websense\bin or Websense/bin/FW1). |

This command contacts the firewall and downloads the Secure Internal Communication certificate that authorizes Websense software to communicate with the Check Point product, and saves the certificate in a file, **opsec.p12**.

The command line displays information similar to the following example:

```
opsec_pull_cert –h 10.201.254.245 –n Websense_UFP –p
firewall –o "C:\Program Files\Websense\bin\opsec.p12"
The full entity sic name is:
CN=Websense_UFP,0=fw1_server..dwz26v
Certificate was created successfully and written to
"opsec.p12".
```

3. Write down the SIC name displayed by the `opsec_pull_cert` command.

   In the example above, the SIC name is:

   ```
   CN=Websense_UFP,0=fw1_server..dwz26v
   ```

4. Open the **ufp.conf** file, located by default in the C:\Program Files or Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin directory.

   The default file contains the following syntax:

   ```
   ufp_server port 18182
   #ufp_server auth_port 18182
   #opsec_sic_policy_file ufp_sic.conf
   #opsec_sic_name "place_holder_for_opsec_SIC_name"
   #opsec_sslca_file opsec.p12
   ```

   The first line is used for clear communication.

   The remaining lines are used for SIC. If the file does not contain the lines for SIC shown above, enter them.

5. To enable secure communication, comment out the first line and remove the comment symbol (#) from the remaining four lines.

   ```
   #ufp_server port 18182
   ufp_server auth_port 18182
   opsec_sic_policy_file ufp_sic.conf
   opsec_sic_name "place_holder_for_opsec_SIC_name"
   opsec_sslca_file opsec.p12
   ```

6. On the **opsec_sic_name** line, replace the placeholder with the SIC name recorded in Step 3.

   The name must be enclosed in quotation marks. For example:

   ```
   opsec_sic_name "CN=Websense_UFP,0=fw1_server..dwz26v"
   ```

   The completed file:

   ```
   #ufp_server port 18182
   ufp_server auth_port 18182
   opsec_sic_policy_file ufp_sic.conf
   opsec_sic_name "CN=Websense_UFP,0=fw1_server..dwz26v"
   opsec_sslca_file opsec.p12
   ```

7. Save and close the file.

8. Stop and restart the Websense UFP Server:
   - **Windows**: Use the Windows Services dialog box.
   - **Linux**: Use the **./WebsenseAdmin restart** command.

   See *Starting or Stopping Web Security Services*, page 923 for instructions on stopping and restarting Websense services. See also *Stopping and restarting the UFP Server*, page 313.

## Stopping and restarting the UFP Server

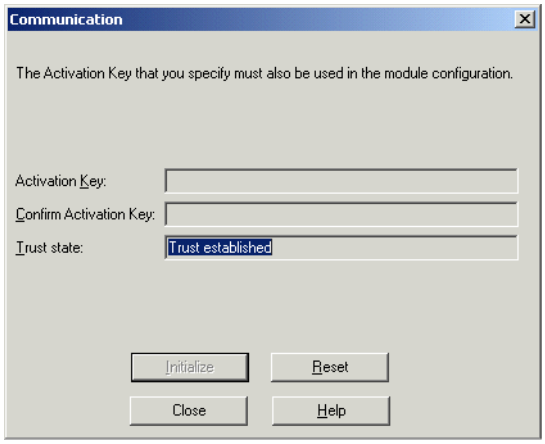
Filtering Service must be running for the Websense UFP Server to function. When the Filtering Service is stopped, the UFP Server is automatically shut down. The UFP Server must be restarted manually. If the UFP Server is started first, it automatically starts the Filtering Service. Stopping or starting the UFP Server while the Filtering Service is running has no effect on the Filtering Service.

## Updating the OPSEC Application object

After Websense software has been configured to use SIC, update the OPSEC Application object created for the Websense UFP Server.

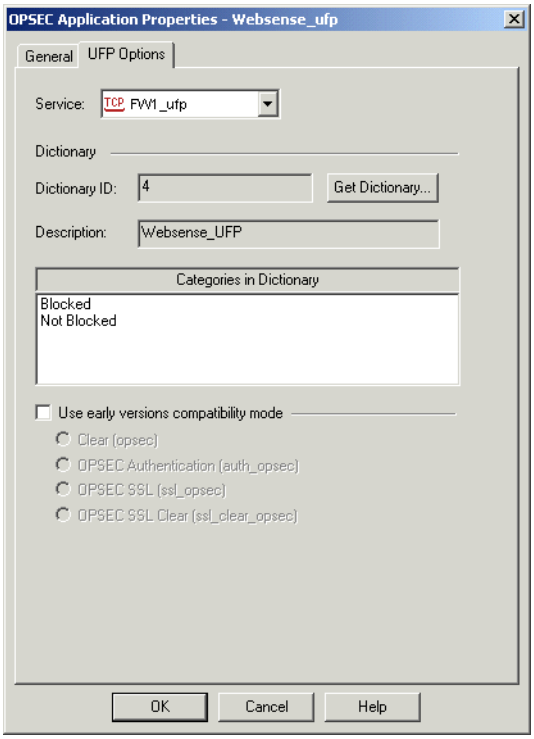
1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
2. Double-click on the OPSEC Application object you created for the Websense UFP Server in *Creating an OPSEC application object*, page 294.

   The OPSEC Application Properties dialog box for this object appears.
3. Click **Communication**.
4. Verify that the **Trust state** field shows **Trust established**.




5. Click **Close** to return to the OPSEC Application Properties dialog box.
6. Click **OK**.
7. Close the Servers and OPSEC Applications dialog box.

8. Select **Policy** > **Install** to install the policy on the firewall. See Check Point product documentation for more information.
9. Open the OPSEC Application object created for the Websense UFP Server again.
10. Go to the **UFP Options** tab of the OPSEC Application Properties dialog box for this object.




11. Make sure the **Use early versions compatibility mode** check box is *not* selected. (This field was called **Use backwards compatibility mode** in earlier versions.)
12. Click **Get Dictionary**.

    Websense software provides the Check Point product with a dictionary of 2 categories: Blocked and Not Blocked. The full set of Websense categories is configured through TRITON - Web Security.

    See TRITON - Web Security Help for more information.

> **Important**
> Before continuing, make sure the **Use early versions compatibility mode** check box is *not* selected.

13. Click **OK**.
14. Close the Servers and OPSEC Applications dialog box.
15. Select **Policy** > **Install** to install the policy on the firewall. See Check Point product documentation for additional information.

The SIC trust is established now between Websense software and the Check Point product. Continue with the configuration in *Creating Resource Objects*, page 296.

# Restoring Clear Communication

To restore clear communication (*early versions compatibility* mode) on a system configured for Secure Internal Communication (SIC):

1. On the Websense Filtering Service machine, navigate to the directory where the Check Point integration files are installed (C:\Program Files or Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin, by default).
2. Open the **ufp.conf** file in any text editor.

   When the Check Point product is configured for SIC, this file contains the following syntax:

   ```
   #ufp_server port 18182
   ufp_server auth_port 18182
   opsec_sic_policy_file ufp_sic.conf
   opsec_sic_name "place_holder_for_opsec_SIC_name"
   opsec_sslca_file opsec.p12
   ```

   When SIC is fully configured, the contents of the quotation marks in line 4 are replaced with an actual `opsec_SIC_name`, such as `CN=Websense_UFP,0=fw1_server..dwz26v`
3. To restore clear communication, remove the comment symbol (#) from the first line, and comment out the remaining lines:

   ```
   ufp_server port 18182
   #ufp_server auth_port 18182
   #opsec_sic_policy_file ufp_sic.conf
   #opsec_sic_name "place_holder_for_opsec_SIC_name"
   #opsec_sslca_file opsec.p12
   ```
4. Save the file.
5. Stop and start the Websense UFP Server:
   - **Windows**: Use the Windows Services dialog box.
   - **Linux**: Use the **./WebsenseAdmin restart** command.

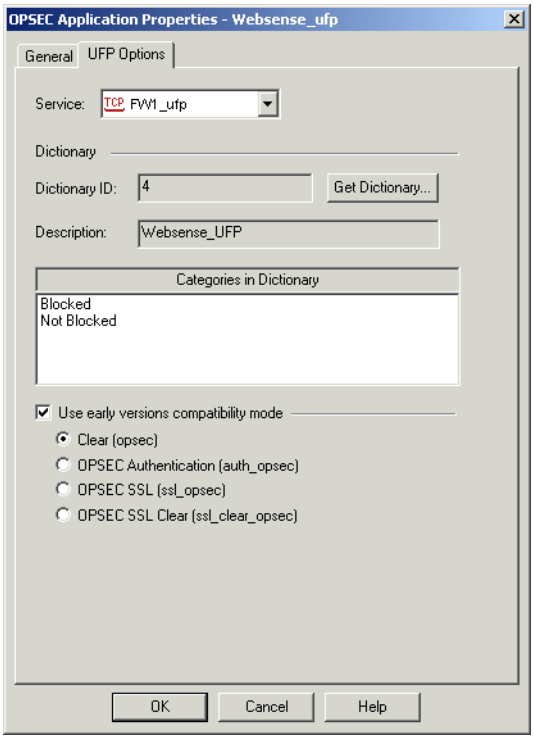
   See *Starting or Stopping Web Security Services*, page 923 for instructions on stopping and restarting Websense services. See also *Stopping and restarting the UFP Server*, page 313.
6. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
7. Double-click on the OPSEC Application object for the Websense UFP Server.

   The OPSEC Application Properties dialog box for this object appears.
8. Click **Communication**.

   The Communication dialog box appears.
9. Click **Reset** to revoke the SIC certificate and stop SIC.

   A confirmation dialog box is displayed.

10. Click **Yes** to continue.
11. Click **Close** to return to the OPSEC Application Properties dialog box.
12. Go to the **UFP Options** tab.




13. Check the **Use early versions compatibility mode** option (**Backwards Compatibility** in earlier versions of FireWall-1 NG).
14. Select **Clear (opsec)**.
15. Click **Get Dictionary**.

    Websense software provides the Check Point product with a dictionary of 2 categories: Blocked and Not Blocked. The full set of Websense categories is configured via TRITON - Web Security.
16. Click **OK**.
17. Close the OPSEC Applications dialog box.
18. Select **Policy** > **Install** to install the policy on the firewall. See Check Point product documentation for more information.

# 22 Troubleshooting Check Point Integration

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Where can I find download and error messages?

Websense software creates **Websense.log** and **ufpserver.log** files when errors occur. These files are located in the Websense **bin** directory, (C:\Program Files or Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin, by default.)

These log files record error messages and other messages pertaining to database downloads. **Websense.log** is located only on the machine running Policy Server.

## The Master Database does not download

In addition to the subscription and access problems discussed in the Websense , a rule in the firewall could be blocking the download. Create a rule in the Check Point product at the top of the rule base that allows all traffic (outbound) from the Websense Filtering Service machine. If this test succeeds, move the rule down systematically until the problematic rule is found.

# Websense dictionary does not load in the Check Point product

The Get Dictionary process occurs between the Check Point SmartCenter Server and Websense Filtering Service. If the SmartCenter Server is not installed on the same machine as the Check Point Enforcement Module, you may need to configure the Check Point product to allow communication between the machines running the SmartCenter Server and Filtering Service. See *Distributed environments*, page 287 for more information.

Three causes are listed below as to why the dictionary might not load within the Check Point product.

## Port mismatch

If the FW1_ufp Service defined in the Check Point product uses a different port than Filtering Service filtering port (default 18182), Websense software cannot communicate with the Check Point product. As a result, the Check Point product cannot retrieve the Websense dictionary entries.

Check for mismatched port entries in the following locations:

- Check the FW1_ufp Service definition in the Check Point product.
  1. From the Check Point client, choose **Manage > Services**.
  2. Select **FW1_ufp** from the list of services.
  3. Click **Edit**.

     The TCP Services Properties dialog box appears.
  4. Make sure the port number displayed is the same as the port number defined for the filtering port when you installed Filtering Service.
- Open the **ufp.conf** file in a text editor. The file is located by default in the C:\Program Files or Program Files (x86)\Websense\Web Security\bin\FW1 or /opt/Websense/bin/FW1 directory. Check the port value to make sure it matches the port setting for the FW1_ufp Service in the Check Point product.
- In the Check Point product, the filtering port specified in the **fwopsec.conf** file must match the port number set for the FW1_ufp Service and the port defined in the Websense **ufp.conf** file.

> **Note**
> If the SmartCenter Server and the Enforcement Module are installed on separate machines, both contain an **fwopsec.conf** file. You must reconcile the filtering port number in each of these files.

## Communication mismatch

If the Websense dictionary does not load, check your communication settings. The method of communication selected in the OPSEC Application object must be consistent with that defined in the **ufp.conf** file (SIC or clear communication).

For example, if you have selected *early version compatibility* mode in the OPSEC Application Properties dialog box (see *Early versions compatibility mode*, page 303), the first line in the **ufp.conf** file must be:

```
ufp_server port 18182
```

If you have selected SIC, the first line in the **ufp.conf** file must be:

```
ufp_server auth_port 18182
```

## Policy properties

Although it is enabled by default, some environments need to disable the **Accept Outgoing Packet Originating from Gateway** setting in the Check Point product's policy properties. Since the firewall cannot send any traffic in this environment, it cannot request the dictionary.

To enable the dictionary request, add the following rule to the Rule Base anywhere before the cleanup rule:

| | |
|---|---|
| **Source** | Check Point product workstation object |
| **Destination** | Any, or the Filtering Service workstation object |
| **Service** | FW1_ufp |
| **Action** | Accept |
| **Track** | Long (or any desired setting) |
| **Install On** | SRC (*Required*) |
| **Time** | Any |

## SIC trust configuration in FireWall-1 NG

When you click **Get Dictionary** in the **Match** tab of the URI Definition dialog box, FireWall-1 NG (Feature Pack 1 or later) contacts Websense Filtering Service via SIC trust to retrieve a list of categories for use in Check Point rules. If the SIC trust was not configured correctly, this contact fails and no categories can be retrieved.

To set up the SIC trust, see *Establishing Secure Internal Communication*, page 307.

If you established the SIC trust, but still cannot get the dictionary, you can re-establish the trust.

1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.

   The Servers and OPSEC Applications dialog box appears.

2. Select the Websense UFP Server object in the list, and click **Edit**.

   The OPSEC Application Properties dialog box appears.

3. Click **Communication**.

   The Communications dialog box appears.

4. Click **Reset** to remove the SIC trust initialized previously, then click **Yes** in the confirmation dialog box that appears.
5. Click **Close** in the Communications dialog box.
6. Click **OK** to close the OPSEC Application Properties dialog box.
7. Click **Close** to close the Servers and OPSEC Applications dialog box.
8. Select **Policy** > **Install** to install the policy on the firewall.
9. Create the SIC trust again as described under *Establishing Secure Internal Communication*, page 307.

**Note**

*Do not* create a new OPSEC Application object for the Websense UFP Server; edit the object that already exists.

## No filtering occurs after enabling enhanced UFP performance

Users who have configured FireWall-1 NG with AI for enhanced UFP performance may not be able to filter Internet requests. This is a Check Point licensing issue and not a configuration problem. A license from an older version of NG cannot work with the newer version of NG with AI. Contact Check Point to update your license for your version of FireWall-1 NG with AI.

## FTP requests are not being blocked as expected

Websense software cannot block FTP requests when the Check Point product is configured to act as a proxy server.

The FTP request is sent as**ftp://**. The Check Point product then sends the packet to the Websense software with an **http://** header. Websense software performs a lookup against HTTP categories instead of performing a protocol lookup, and the FTP request is blocked or permitted according to the category assigned to the HTTP version of the same URL.

It is recommended that you use the capability of the Check Point product to block the FTP protocol.

1. In the Check Point product, create a rule that blocks on the FTP service. See Check Point product documentation for more information.

2. Place this rule above the Websense rule.
3. Save the policy.

   Users receive the Check Point block page instead of the Websense block page.

> **Note**
> In this case, it is not necessary to set the FTP protocol to be blocked in TRITON - Web Security.

# 23 Universal Integrations

## Applies to

- Web Filter v7.6
- Web Security v7.6

## In this topic



## Overview

There are instructions for integrating Web Filter or Web Security with specific products:

- *Check Point Integration*, page 285
- *Cisco Integration*, page 193
- *Citrix Integration*, page 167
- *Microsoft ISA Server or Forefront TMG Integration*, page 227
- *Squid Web Proxy Cache Integration*, page 259

This topic discusses integrating Web Filter or Web Security with a product not represented in the list above.

Go to www.websense.com/global/en/Partners/TAPartners/SecurityEcosystem/. Check the list of Technology Partners to see if Websense software supports an integration with your firewall, proxy server, caching application, or network

appliance. If your integration product is listed, that product has been specifically enhanced to integrate with Websense software.

Integrating Websense software with another product or device affects the following components:

- **Filtering Service**: Interacts with your integration product and Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.
- **Network Agent**: Internet protocols that are not managed by your integration product are managed by Network Agent. It can detect HTTP network activity and instructs the Filtering Service to log this information.

  If Network Agent is installed, you must define the IP addresses of all proxy servers through which computers route their Internet requests. See the Network Configuration topic in TRITON - Web Security help for instructions.

  If Network Agent is installed separately from other filtering components, be sure to install Filtering Service in integrated mode (universal integration). This ensures that bandwidth filtering can be applied in the integrated environment.

## How Websense filtering works with your integration

When the integration product receives an Internet request, it queries Websense Filtering Service to find out if the requested site should be blocked or permitted. Filtering Service consults the policy assigned to the client to determine which categories are blocked, and then checks the Websense Master Database to find out how the requested site is categorized.

- If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies the integration product that the site is not blocked, and the client is allowed to see the site.

## Installing Web Filter or Web Security to be integrated

Follow the installation instructions in the installation materials to install the Websense components you want. The steps below provide specific options to select or alternate instructions to be used as you follow the instructions in the installation materials. Unless a specific option or alternative instruction is provided here, you should follow the steps as described in the installation materials.

1. Start the Websense installer, and follow the prompts.

   See the installation materials for instructions on downloading and starting the installer.

2. On the **Integration Option** screen, select **Integrated with another application or device**.
3. On the **Select Integration** screen, select **Other (Universal Integration)**.
4. On the **Transparent User Identification** screen you can choose whether to install a Websense transparent identification agent. Transparent identification agents identify users without prompting them for logon information. This enables filtering via user and group-based policies.

   Select **None** if you plan to configure authentication of users through your integration product, or if you plan to assign policies to computers and networks (IP addresses or IP address ranges) only.

   See the installation materials for more information about this installer screen.

   See the Transparent Identification of Users technical paper for more information about transparent identification agents.
5. Follow the remaining installer prompts to complete the installation.

   See the installation materials for instructions on the prompts.

**Note**

To prevent users from circumventing Websense filtering, configure your firewall or Internet router to allow outbound HTTP, HTTPS, FTP, and Gopher requests only from your integration product.

Contact your router or firewall vendor for information about configuring access lists for that product.

**Important**

If Internet connectivity of Websense software requires authentication through a proxy server or firewall for HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication to enable the Websense Master Database download.

# Upgrading when integrated

See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions on upgrading Websense software. After the upgrade, Websense software and your integration product should continue to work together as before.

# Initial setup

Depending on the integration product you are using, you may need to configure client computers to access the Internet through it to enable Websense filtering. Consult your integration product's documentation to make this determination.

# Migrating to a different integration after installation

You can change your integration product or version after installing Websense software without losing any of your configuration data.

1. Install and configure your new integration product. See your integration product documentation for instructions.

   Ensure that it is deployed in your network such that it can communicate with Filtering Service and Policy Server.
2. Use the Websense Backup Utility to backup the Websense configuration and initialization files. See TRITON - Web Security Help for instructions
3. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.
4. Remove Filtering Service using the procedures for removing components in the installation materials.

   **Warning**

   Remove Filtering Service only. Do **not** remove the associated Policy Server.
5. Restart the machine (Windows only).
6. Close any open applications, and stop any antivirus software.
7. Run the Websense installer again.
8. Add Filtering Service using the procedures for installing individual components in the installation materials.
9. On the **Integration Option** screen, select **Integrated with another application or device**.
10. On the **Select Integration** screen, select **Other (Universal Integration)**.
11. Follow the installer prompts to complete the installation.

    The installer adds the new integration data, while preserving the previous configuration data.
12. Restart the machine (Windows only).

13. Verify that Filtering Service has started.
    - **Windows**: Open the Services dialog box (Start > Programs > Administrative Tools > Services) and check to see if **Websense Filtering Service** is started.
    - **Linux**: Navigate to the Websense installation directory (/opt/Websense, by default), and enter the following command to see if **Websense Filtering Service** is running:

      ```
      ./WebsenseAdmin status
      ```

    To start a service, follow the instructions in the installation materials.
14. Open TRITON - Web Security to identify which Filtering Service instance is associated with each Network Agent.
    a. Open the **Settings** tab.
    b. Go to the **Settings > Network Agent**, then choose the appropriate IP address to open the **Local Settings** page.
    c. Under **Filtering Service Definition**, select the IP address for the machine running Filtering Service. During the migration, the setting may have been reset to None.
    d. Log out of TRITON - Web Security.

    For more information, see the Network Configuration> Local Configuration topic in the TRITON - Web Security Help.
15. If you stopped your antivirus software, be sure to start it again.

# 24 Installing Web Security Components on Linux

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

This section provides instructions for running the Web Security Linux installer to install Websense Web security components on Linux. Most Web security components can be installed on Linux. However, the following components cannot be installed on Linux and must be installed separately on a Windows machine:

- TRITON Unified Security Center (includes TRITON - Infrastructure, TRITON - Web Security, TRITON - Data Security, TRITON - Email Security
- Web Security Log Server
- Real-Time Monitor
- DC Agent
- Linking Service
- Remote Filtering Client Pack
- Citrix Integration Service (i.e., Filtering Plug-in)
- ISA Server ISAPI plug-in (i.e., Filtering Plug-in)

- TMG ISAPI plug-in (i.e., Filtering Plug-in)

For more information, see *System Requirements*, page 41.

On Linux, there are two types of Web security installation:

- **Custom**: Select which components you want installed on this machine. See *Custom installation*, page 330.
- **Filtering**: Install all Web security components (that are Linux-compatible) on this machine. See *Filtering installation*, page 330.

# Filtering installation

A filtering installation on Linux installs all Web security components that can be installed on Linux, with the exception of Remote Filtering Server (which should be installed on its own machine and not with any other Web security components; see the *Remote Filtering Software* technical paper in the Websense Technical Library (www.websense.com/library) for more information).

It is important to note that on Linux no management and reporting components are installed (e.g., *TRITON Unified Security Center* and *Web Security Log Server*). These must be installed on a Windows machine.

Complete the following main steps (the links go to detailed procedures or information for each step).

1. *Preparing for Installation*, page 55
2. *Starting the Web Security Linux installer*, page 330
3. *Installing all Web security filtering components on Linux*, page 332*s*

# Custom installation

Complete the following main steps (the links go to detailed procedures or information for each step).

1. *Preparing for Installation*, page 55
2. *Starting the Web Security Linux installer*, page 330
3. *Installing Web Security components on Linux*, page 336

# Starting the Web Security Linux installer

## Applies to

- Web Filter v7.6

- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Starting the Web Security Linux installer

1. Log on to the installation machine with administrative privileges (typically, **root**).
2. Create a setup directory for the installer files. For example:

   ```
   /root/Websense_setup
   ```

3. Download the Web Security Linux installer package from mywebsense.com:
   - WebsenseWeb76Setup_Lnx.tar.gz

   Place the installer tar archive in the setup directory you created.
4. Extract the installer files:

   In the setup directory, enter the following commands to uncompress and extract files:

   ```
   gunzip WebsenseWeb76Setup_Lnx.tar.gz
   tar xvf WebsenseWeb75Setup_Lnx.tar
   ```

   This places the following files into the setup directory:

   | File | Description |
   |---|---|
   | `install.sh` | Installation program |
   | `Setup.bin` | Archive file containing installation files and documents |

5. Lanch the installer using the following command (from the setup directory):

   ```
   ./install.sh -g
   ```

   This launches a GUI-based installer and is available on English versions of Linux only. A text-only, command-line version can be launched by omitting the -g switch:

   ```
   ./install.sh
   ```

If the installation program displays error messages that it is having difficulty locating other machines, disable any firewall running on the installation machine.

**Note**

The following instructions refer to installer screens. In the command-line Linux installer, prompts are displayed that correspond to each screen. Instructions for a screen also apply to the corresponding command-line prompt. The main difference is how options are selected. Rather than clicking items in a screen, you will enter menu-item numbers or characters.

**Note**

To cancel the command-line Linux installer, press Ctrl-C. However, do **not** cancel the installer, after the **Pre-Installation Summary** screen, as it is installing components. In this case allow the installation to complete and then uninstall the unwanted components.

# Installing all Web security filtering components on Linux

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Installing all Web security filtering components on Linux

1. It is assumed you have already downloaded and started the Web Security Linux installer. If not, see *Starting the Web Security Linux installer*, page 330 for instructions.
2. If no Web security components have been installed on this machine:
   a. On the **Introduction** screen, click **Next**.
   b. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.
   c. On the **Installation Type** screen, select **Filtering** and then click **Next**.
3. If there are Web security components already installed on this machine, the **Add Components** screen appears.

   Select **Install additional components on this machine** and then click **Next**.

If there are already components on this machine, you can only perform a custom installation. See *Custom installation*, page 330

4. On the Integration Option screen, indicate whether this is a stand-alone or integrated installation, and then click **Next**.

   See *Integration Option Screen* for instructions.

5. If you chose **Integrated with another application or device** (on the Integration Option screen), the **Select Integration** screen appears.

   See *Select Integration Screen* for instructions.

6. If the **Filtering Plug-in** screen appears, see *Filtering Plug-In Screen* for instructions.
7. If the **Squid Configuration** screen appears, see *Squid Configuration Screen* for instructions.
8. If the **Network Card Selection** screen appears, see *Network Card Selection Screen* for instructions.
9. If the **Multiple Network Cards** screen appears, see *Multiple Network Cards Screen* for instructions.
10. On the **Filtering Feedback** screen, select whether you want Websense software to send feedback to Websense, Inc. to improve accuracy. Then click **Next**.

    See *Filtering Feedback Screen* for instructions.

11. On the **Web Security Gateway Anywhere Components** screen, select whether you want to install Websense Web Security Gateway Anywhere components on this machine. Then click **Next**.
    - **Install Web Security Gateway Anywhere Components**: Select this option to install these components and then check the box for the components (**Sync Service** and/or **Directory Agent**) you want to install.
    - **Do not install Web Security Gateway Anywhere Components**: Select this option to not install these components.
12. On the **Transparent User Identification** screen, select whether to use Websense transparent identification agents to identify users and then click**Next**. This allows Websense software to apply user- or group-based filtering policies without prompting users for logon information.

    If Websense software is integrated with a third-party product (firewall, proxy server, cache, or network appliance) providing user authentication, a transparent identification agent may not be necessary.

    To transparently identify remote users accessing the network via VPN, use Websense RADIUS Agent. Later in this installation process, you will be given the option to install RADIUS Agent.

    It is possible to run multiple instances of the same transparent identification agent, or certain combinations of different transparent identification agents, in a network. (Note, however, you cannot run both DC Agent and eDirectory Agent, or Logon Agent and eDirectory Agent, in the same network.) To install another instance of a transparent identification agent or a different transparent

identification agent, run this installation program on the other machine and use the Custom installation type. For information about multiple instances or combinations of transparent identification agents, see the *Transparent Identification of Users* technical paper in the Websense Technical Library (www.websense.com/library).

- **Use Logon Agent to identify users logging on to local machines**: This option installs Websense Logon Agent on this machine. Logon Agent identifies users as they log onto Windows domains. Logon Agent is for use with Windows-based client machines on a network that uses Active Directory or Windows NT Directory.

  To use Logon Agent, you must modify the Group Policy on domain controllers so it launches a logon application (LogonApp.exe) as part of the logon script. Client machines must use NTLM (v1 or v2) when authenticating users (NTLMv1 only, in the case of Windows Server 2008; see note below).

  For instructions on configuring domain controllers and client machines to use Logon Agent, see *Creating and running the script for Logon Agent*, page 782.

  **Note**
  Do not use Logon Agent in a network that already includes eDirectory Agent.

  **Note**
  If using Logon Agent with a Windows Server 2008 domain controller, client machines must be configured to use NTLMv1 when authenticating a user. To do this, modify the security policy so **Network security: LAN Manager authentication level** is set to **Send NTLM response only**. This can be done on each individual client machine by modifying the local security policy, or on all machines in a domain by modifying the security policy of a Group Policy Object. For instructions, see *Creating and running the script for Logon Agent*, page 782.

- **Use eDirectory Agent to identify users logging on via Novell eDirectory Server**: This option installs eDirectory Agent on this machine. Use this agent for a network using Novell eDirectory. eDirectory Agent queries the eDirectory Server at preset intervals to identify users currently logged on.

  **Note**
  Do not use eDirectory Agent in a network that already includes DC Agent or Logon Agent.

- **Do not install a transparent identification agent now**: Select this option if
  - Websense software will be integrated with a third-party product that provides user authentication.

- You plan to install a transparent identification agent on another machine.
- You do not want different filtering policies applied to users or groups.
- You want users to be prompted for logon information when they open a browser to access the Internet.

**Note**

When integrated with Cisco products, Websense software cannot use Cisco Secure Access Control Server (ACS) for user authentication for more than 1 user domain. If there are multiple user domains, use a transparent identification agent instead.

13. On the **RADIUS Agent** screen, select **Install RADIUS Agent** if you have remote users that are authenticated by a RADIUS server and then click **Next**. This allows Websense software to apply user- or group-based filtering policies on these remote users without prompting for logon information.
14. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

    The installation path must be absolute (not relative). The default installation path is:

    - **Linux**: /opt/Websense/

    The installer creates this directory if it does not exist.

**Important**

The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

    The installer compares the installation's system requirements with the machine's resources.

    - Insufficient disk space prompts an error message. The installer closes when you click **OK**.
    - Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.
15. On the **Pre-Installation Summary** screen, verify the information shown.

    The summary shows the installation path and size, and the components to be installed.

16. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

> **Note**
> If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) the installer after the **Pre-Installation Summary** screen, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

17. On the **Installation Complete** screen, click **Done**.

# Installing Web Security components on Linux

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Installing Web Security components on Linux

1. It is assumed you have already downloaded and started the Web Security Linux installer. If not, see *Starting the Web Security Linux installer*, page 330.
2. If no Web security components have been installed on this machine:
   a. On the **Introduction** screen, click **Next**.
   b. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.
   c. On the **Installation Type** screen, select **Custom** and then click **Next**.
3. If there are Web security components already installed on this machine, the **Add Components** screen appears.

   Select **Install additional components on this machine** and then click **Next**.
4. On the **Select Components** screen, select the components you want to install on this machine.

   See the following for more information about each component:

   - *Policy Broker*
   - *Policy Server*
   - *Filtering Service*
   - *Network Agent*
   - *RADIUS Agent*
   - *Logon Agent*
   - *Filtering Plug-in*
   - *Remote Filtering Server*

- *Usage Monitor*
- *User Service*
- *eDirectory Agent*
- *Sync Service*
- *Directory Agent*

5. Depending on the components you have selected, some or all of the following installer screens appear. (In the following list, after a screen name, is the component-selection or machine condition that causes the screen to appear.) Click a screen name below for instructions.
   - *Policy Server Connection Screen* (Filtering Service, Network Agent, Usage Monitor, User Service, DC Agent, eDirectory Agent, RADIUS Agent, Logon Agent, Remote Filtering Server, Sync Service, or Directory Agent)
   - *Policy Broker Connection Screen* (Policy Server, Sync Service, or Directory Agent).
   - *Multiple Network Cards Screen* (if multiple NICs detected)
   - *Integration Option Screen* (Filtering Service)
   - *Select Integration Screen* (Filtering Service, to be integrated with a third-party product, or Filtering Plug-In)
   - *Network Agent and Firewall Screen* (Filtering Service and Network Agent; Filtering Service to be integrated with a Check Point product)
   - *Filtering Plug-In Screen* (Filtering Service, to be integrated with Citrix, Microsoft ISA Server, or Squid Web Proxy Cache)
   - *Squid Configuration Screen* (Filtering Service, to be integrated with Squid Web Proxy Cache, or Filtering Plug-In)
   - *Network Card Selection Screen* (Network Agent)
   - *Filtering Feedback Screen* (Filtering Service or Network Agent)
   - *Directory Service Access Screen* (User Service, DC Agent, or Logon Agent)
   - *Remote Filtering Communication Screen* (Remote Filtering Server)
   - *Remote Filtering Pass Phrase Screen* (Remote Filtering Server)
   - *Filtering Service Information for Remote Filtering Screen* (Remote Filtering Server)
   - *Filtering Service Communication Screen* (Network Agent, a filtering plug-in, or Linking Service)
6. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

   The installation path must be absolute (not relative). The default installation path is: /opt/Websense/

   The installer creates this directory if it does not exist.

   **Important**

   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

The installer compares the installation's system requirements with the machine's resources.

- Insufficient disk space prompts an error message. The installer closes when you click **OK**.
- Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.

7. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

8. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

   **Note**
   If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) the installer after the **Pre-Installation Summary** screen, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

9. On the **Installation Complete** screen, click **Done**.

## Policy Server Connection Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This installer screen appears if any of the following is selected for installation but Policy Server is not:

| | |
|---|---|
| Filtering Service | RADIUS Agent |
| Network Agent | Logon Agent |
| Usage Monitor | Remote Filtering Server |
| User Service | Sync Service |
| eDirectory Agent | Directory Agent |

It is assumed Policy Server is installed on another machine. Enter the IP address of the machine and the port Policy Server uses to communicate with other Websense components (default is 55806). If this is a Websense-appliance-based deployment, Policy Server is already installed on the Web-security-mode appliance designated *policy source*. In this case, enter the IP address of the appliance's C interface for the Policy Server IP address.

The port used by Policy Server to communicate with other Websense components must be in the range 1024-65535. In a software-based deployment, Policy Server may have been automatically configured to use a port other than the default 55806. When Policy Server is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Policy Server, check the `websense.ini` file—located in `C:\Program Files or Program Files (x86)\Websense\Web Security\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Policy Server machine. In this file, look for the **PolicyServerPort** value.

**Important**

Do not modify the `websense.ini` file.

If Policy Server is not installed yet, anywhere in your network, you must install it before installing any of the components listed above. To install it on this machine, click **Previous** and select **Policy Server** in addition to already selected components. To install it on another machine, run this installer on that machine (prior to installing components on this machine).

## Policy Broker Connection Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This installer screen appears if Policy Server, Sync Service, or Directory Agent is selected for installation, but Policy Broker is not.

In a software-base deployment, enter the IP address of the machine on which Policy Broker is installed and the port Policy Broker uses to communicate with other Websense components (default is 55880). If it is installed on this machine, enter its IP address (actual address, not loopback).

In an appliance-based deployment, Policy Broker is already installed on the appliance designated *full policy source*. Enter the IP address of the appliance's C interface and use the default port (55880).

The communication port must be in the range 1024-65535. Policy Broker may have been automatically configured to use a port other than the default 55880 for communication with other Websense components. When Policy Broker is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Policy Broker, check the `BrokerService.cfg` file—located in `C:\Program Files or Program Files (x86)\Websense\Web Security\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Policy Broker machine. In this file, look for the **listen_port** value.

**Important**

Do not modify the `BrokerService.cfg` file.

If Policy Broker is not installed yet, anywhere in your network, you must install it before installing any other Websense Web security component. To install it on this machine, click **Previous** and select **Policy Broker** in addition to already selected components. To install it on another machine, run this installer on that machine.

## Filtering Service Communication Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if Network Agent or a filtering plug-in is selected for installation.

Enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). If Filtering Service is installed on this machine, enter the IP address of this machine (note: actual IP address, not the loopback address, 127.0.0.1).

In an appliance-based deployment, Filtering Service is already installed on a Web-security-mode appliance. Enter the IP address of the appliance's C interface and use the default port (15868). Note that a deployment may contain multiple appliances, each with a Filtering Service running. In that case, enter the C-interface IP address of the appliance with the Filtering Service you want Network Agent or the filtering plug-in (i.e., integration product)to use.

The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535. In a software-base deployment, Filtering Service may have been automatically configured to use a port other than the default 15868. When Filtering Service is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Filtering Service, check the `eimserver.ini` file—

located in `C:\Program Files or Program Files (x86)\Websense\Web Security\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.

> **Important**
> Do not modify the `eimserver.ini` file.

If Filtering Service is not installed yet, anywhere in your network, you must install it before installing Network Agent, a filtering plug-in, Linking Service. To install it on this machine, click **Previous** and select **Filtering Service** in addition to already selected components. To install it on another machine, run this installation program on that machine (prior to installing Network Agent, a filtering plug-in, or Linking Service on this machine).

> **Important**
> In the case of a filtering plug-in, when installing Filtering Service, be sure to do so as integrated with the integration product.

## Multiple Network Cards Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This installer screen appears if multiple network interface cards (NICs) are detected on this machine.

Select the IP address of the NIC to be used by Websense software on this machine. This is the NIC that will be used to send block pages when a user requests filtered content. You will specify later whether this NIC is also used by Network Agent to monitor Internet traffic and send protocol block messages.

> **Note**
> If the selected NIC will be used by Network Agent, it must support promiscuous mode.

## Integration Option Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This installer screen appears if Filtering Service is selected for installation.

Indicate whether this is a stand-alone or integrated installation, and then click **Next**.

- **Stand-alone**: Websense software will not be integrated with a third-party product. Websense Network Agent monitors all Internet requests and sends them to Websense Filtering Service. Network Agent also sends block messages to users attempting to access filtered content.

  > **Note**
  > In a stand-alone environment, Network Agent must be installed (either on this machine or a networked machine). See *Deploying Network Agent*, page 105 for more information.

- **Integrated with another application or device**: Websense software is installed in integrated mode, ready to integrate with a third-party firewall, proxy server, cache, or network appliance, referred to as an *integration product* (for example, Microsoft ISA Server or Cisco PIX Firewall).The integration product queries Websense Filtering Service to determine whether to allow Internet requests. Filtering Service sends block pages, if necessary, to users attempting to access filtered content. In an integrated environment, Websense Network Agent is used only to filter requests on Internet protocols not managed by the integration product (for example, protocols for instant messaging). Network Agent sends block messages and alerts when necessary. Refer to the Websense Technical Library (www.websense.com/library) for more information.

  > **Note**
  > In an integrated environment, Network Agent is optional.

## Select Integration Screen

### Applies to

- Web Filter v7.6

- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if you selected**Integrated with another application or device** in the *Integration Option Screen*, page 342. (A alternative version of this screen appears if you selected Filtering Plug-In for installation; see below.)

Select your integration product and then click **Next**.

> **Note**
> If your subscription includes Websense Web Security Gateway or Web Security Gateway Anywhere, select **Websense Content Gateway** as the integration product.

If you selected Filtering Plug-In for installation, the Select Integration screen shows only Squid Web Proxy Cache.

## Network Agent and Firewall Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if you select Check Point as the integration product on the *Select Integration Screen*, page 342 and you have chosen Network Agent as a component to install (in addition to Filtering Service).

Network Agent should not be installed on the Check Point machine (unless the machine has separate processors or virtual processors to separately support Network Agent and the firewall software). Network Agent uses packet capturing that may conflict with the firewall software. Choosing to not install Network Agent does not affect installation of the other Websense components, they will still be installed.

## Filtering Plug-In Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6

- Web Security Gateway Anywhere v7.6

### Description

This screen appears if you selected Squid Web Proxy in the*Select Integration Screen*, page 342. Select options as described below and then click **Next**.

You can choose either or both of the options in the **Filtering Plug-In** screen:

- **Yes, install the plug-in on this machine**: This option installs only the filtering plug-in on this machine. Enter the IP address and port for Websense Filtering Service.
- **Install other selected components**: This option installs all selected Websense components, but not the plug-in. Note: Selecting this option installs Websense software in integrated mode, ready to integrate with Squid Web Proxy Cache.

> **Note**
> To install both the plug-in and selected Websense components, you must select both of the above options. When you select **Install other selected components**, the Filtering Service **IP address** and **Port** boxes are greyed out because you do not need to specify them; Filtering Service is being installed on this machine.

## Squid Configuration Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if you selected Squid Web Proxy Cache as the integration product on the *Select Integration Screen*, page 342. It also appears if you selected Filtering Plug-In for installation and chose Squid Web Proxy Cache.

Enter paths to the squid.conf and squid executable files. The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

> **Note**
> The installer will automatically start Squid Web Proxy Cache once installation is complete.

## Network Card Selection Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if Network Agent is selected for installation.

Select the network interface card (NIC) to be used by Network Agent and then click **Next**.

> **Note**
> This screen appears even if the machine does not have multiple NICs. In this case, only one NIC is listed.

This is the NIC that Network Agent will use to communicate with other Websense software components. All enabled NICs with an IP address are listed.

> **Note**
> For Network Agent to operate, this machine must be connected to a bi-directional span port (or mirror port) on a switch or hub that processes the network traffic to be monitored.

You may select multiple NICs. After installation, use TRITON - Web Security to configure how Network Agent will use each selected NIC (for more information, see the TRITON - Web Security Help).

On Linux, NICs without an IP address are also listed. Do not choose a NIC without an IP address.

After installation, you can configure Network Agent to use NICs without an IP address to monitor Internet requests. See *Configuring a stealth mode NIC*, page 788.

## Filtering Feedback Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if Filtering Service or Network Agent is selected for installation.

Select whether you want Websense software to send feedback to Websense, Inc. to improve accuracy and then click **Next**.

Choosing to allow feedback to Websense, Inc. helps improve the accuracy of Websense software for all customers. The feedback consists of any URLs that could not be categorized by Websense software. Such uncategorized URLs are evaluated by Websense, Inc. If warranted, they are investigated in more detail and put into an appropriate category. The Websense Master Database is updated with this information. When your Websense software downloads the updated database, it will be able to categorize those URLs and filter them according to the policies you have set.

**Important**

No information about users or your network is collected. The information is only about the visited URLs themselves. Only uncategorized URLs and the frequency of requests to them are collected. Uncategorized intranet URLs are not included in feedback.

**Note**

You can later choose to enable or disable feedback (the feedback mechanism is known as WebCatcher) using the Log Server Configuration utility. For more information, see Log Server Configuration Help.

## Directory Service Access Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if User Service or Logon Agent is selected for installation.

Enter the domain, user name, and password of an account that is a member of the Domain Admins group on the domain controller. This must be the domain controller for the users you wish to apply user- or group-based filtering policies to. User Service uses this account to query the domain controller for user information.

> **Note**
> User information on domain controllers trusted by the domain controller in question will also be accessible.

If you choose not to specify a Domain Admin account now (by leaving the fields blank), you can specify it after installation. Specify a Domain Admin account to be used by User Service. For more information, see *Troubleshooting > User Identification* in the TRITON - Web Security Help.

## Remote Filtering Communication Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if Remote Filtering Server is selected for installation.

The external IP address or host name of the firewall or gateway must be visible from outside the network. If you enter a host name, it must be in the form of a fully-qualified domain name: <*machine name*>.<*domain name*>

> **Important**
> Remember whether you entered an IP address or a host name here. When installing the Remote Filtering Client on user machines, you must enter this address in the same form (IP address or domain name).

> **Note**
> It is a best practice to use IP addresses, rather than host names, unless you are confident of the reliability of your DNS servers. If host names cannot be resolved, Remote Filtering Clients will be unable to connect to the Remote Filtering Server.

The external communication port can be any free port in the range 10-65535 on this machine. This port receives HTTP/HTTPS/FTP requests from external Remote Filtering Client machines (i.e. user machines, running Remote Filtering Client, outside the network). The default is 80. If a Web server is running on this machine, it may be necessary to use a different port.

> **Note**
> The external network firewall or gateway must be configured to route traffic, typically via PAT or NAT, from Remote Filtering Client machines to the internal IP address of this machine.

The internal communication port can be any free port in the range 1024-65535 on this machine. The default is 8800. This is the port to which remote client heartbeats are sent to determine whether a client machine is inside or outside the network. The external network firewall must be configured to block traffic on this port. Only internal network connections should be allowed to this port.

For more information, see the *Remote Filtering Software* technical paper in the Websense Technical Library (www.websense.com/library).

## Remote Filtering Pass Phrase Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if Remote Filtering Server is selected for installation.

The pass phrase can be any length. This pass phrase is combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

If you want this instance of Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.

The pass phrase must include only ASCII characters but cannot include spaces. Do not use extended ASCII or double-byte characters.

You must use this pass phrase when you install the Remote Filtering Client on user machines that will connect to this Remote Filtering Server.

## Filtering Service Information for Remote Filtering Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if Remote Filtering Server is selected for installation.

- **Internal IP address**: Enter the actual IP address of the Filtering Service machine to be used by this instance of Remote Filtering Server.

  **Filtering port and Block page port**: The filtering port is used by Filtering Service to communicate with other Websense components. The block page port is used by Filtering Service to send block pages to client machines. These ports must be in the range 1024-65535. These ports must be open on any firewall between the Remote Filtering Server and Filtering Service.

  Filtering Service may have been automatically configured to use ports other than the default 15868 (filtering port) and 15871 (block page port). When Filtering Service is installed, the installation program checks whether these default ports are already in use on that machine. If either is already in use, the port is automatically incremented until a free port is found.

  To find the ports used by Filtering Service, check the `eimserver.ini` file—located in `C:\Program Files or Program Files (x86)\Websense\Web Security\bin` (Windows) or /opt/Websense/bin (Linux)—on the Filtering Service machine. Look for the **WebsenseServerPort** (filtering port) and **BlockMsgServerPort** (block page port) values.

  **Important**

  Do not modify the `eimserver.ini` file.

- **Translated IP address**: Use this box to provide the translated IP address of Filtering Service if it is behind a network-address-translating device. You must

check **A firewall or other network device performs address translation between Remote Filtering Server and Filtering Service** to activate this box.

# 25 Web Security Gateway Anywhere (software-based)

## Applies to

- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

Web Security Gateway Anywhere is a hybrid on-premises and in-the-cloud Web filtering solution. Users inside your corporate network are filtered by on-premises Websense components. Small, remote offices and off-site users can be filtered by Websense hybrid service clusters located across the globe.

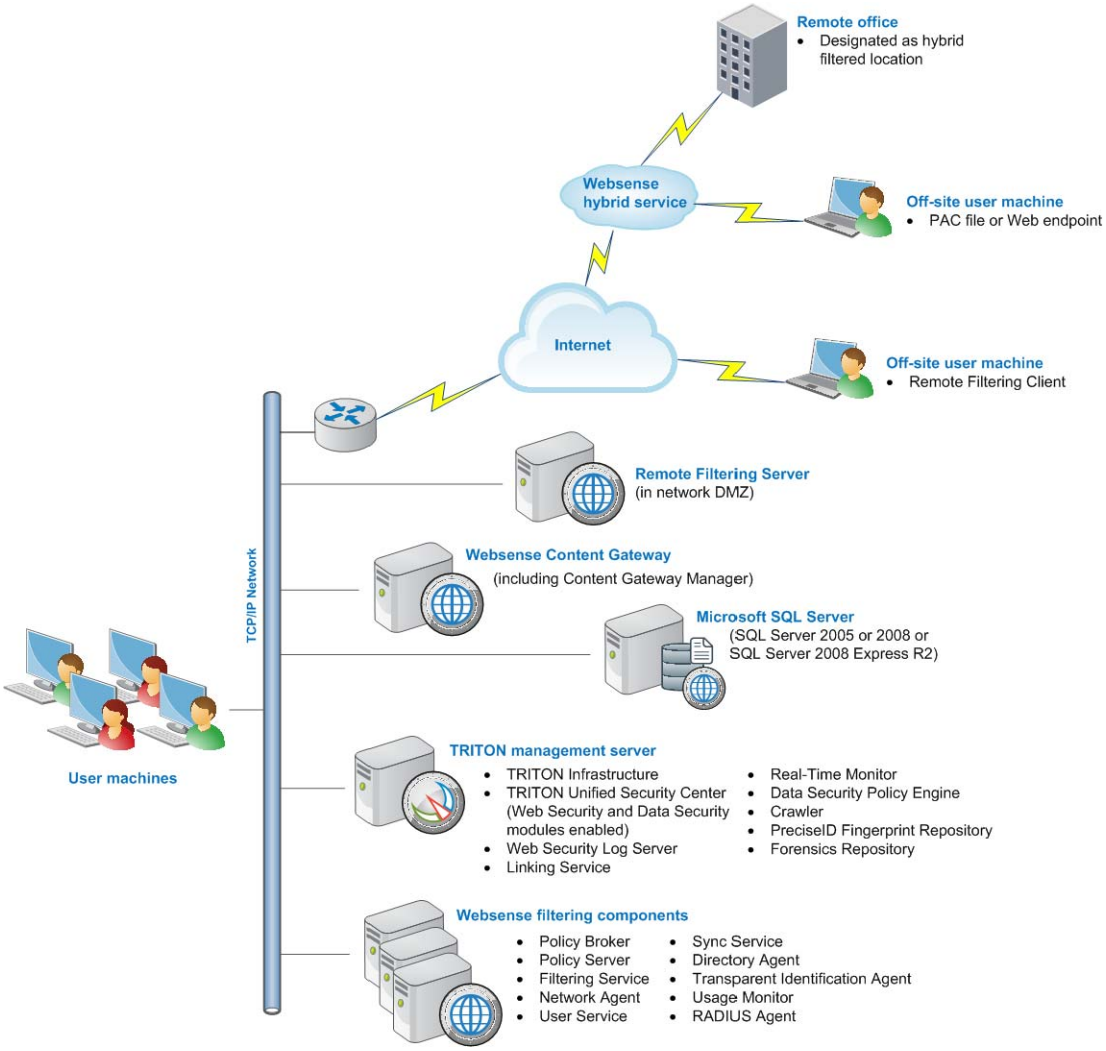
For information about a Websense-appliance-based deployment, see *Web Security Gateway Anywhere (appliance-based)*, page 419.

Websense Web Security Gateway Anywhere software consists of components that work together to monitor Internet requests, log activity, apply Internet usage filters, and report on activity. In addition, Web Security Gateway Anywhere protects you from data loss over the Web, providing security for outbound content as well. You identify sensitive data and define whether you want to audit or block attempts to post it to HTTP, HTTPS, FTP, or FTP-over-HTTP channels.

Websense software is highly-distributable, providing the flexibility to scale a deployment to suit your needs. Components can be installed together on one machine for smaller organizations; or they can be distributed across mutliple machines, and multiple sites, to create a high-performing deployment for larger organizations. The

appropriate deployment is determined by network size and configuration, Internet request volume, hardware performance, and filtering needs.

The following illustration is a high-level diagram of a basic software-based deployment of Web Security Gateway Anywhere. Note that this illustration is intended to show the general distribution of components and does not include network details (such as segmenting, internal firewalls, routing, switching, and so forth).




Microsoft SQL Server is used to store Websense data (including log and reporting data). SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using the Websense installer) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

*TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and any or all of the

TRITON Unified Security Center modules (Web Security, Data Security, and Email Security). In Web Security Gateway Anywhere deployments, both the Web Security and Data Security modules of the TRITON Unified Security Center are enabled. *Linking Service* is typically installed on this machine. Additional components may also be installed on this machine. For example, Web Security Log Server and Real-Time Monitor (note that these components may be installed on another machine; they are not required to be located on the TRITON management server).

Websense filtering components may be installed on the same machine or distributed across several machines. Additionally, you can install multiple instances (on different machines) of certain components to scale to your organization's needs.

Websense Content Gateway is a Web proxy that passes HTTP, HTTPS, FTP over HTTP, and native FTP traffic to Websense software for filtering. Content Gateway Manager—the Web-browser-based management UI for Content Gateway—runs on the Content Gateway machine, but is typically accessed from within TRITON Unified Security Center.

Small remote offices can be filtered through the Websense hybrid service. This is accomplished by designating a remote office as a hybrid filtered location. See *Initial Configuration*, page 763 for more information.

Off-site users (e.g., telecommuters or traveling personnel) can be filtered using the Websense hybrid service or Websense Remote Filtering. To use the hybrid service, a PAC file or the Websense Web endpoint is installed on the user's machine. This directs Web browsing to be filtered through the hybrid service according to policies in place.

Websense Remote Filtering is accomplished using a Remote Filtering Server and Remote Filtering Client. Websense*Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users that are outside the corporate network.

A combination of hybrid service and Remote Filtering can be used for off-site users—i.e., some filtered through the hybrid service, others filtered by Remote Filtering.

# Deployment

- *Web Security Distributed Enterprise Deployments*, page 147

# Installation

Complete the following main steps (the links go to detailed procedures or information for each step).

1. *Preparing for Installation*, page 55
2. *Obtaining SQL Server*, page 67
3. *Installing Web Security components*, page 668

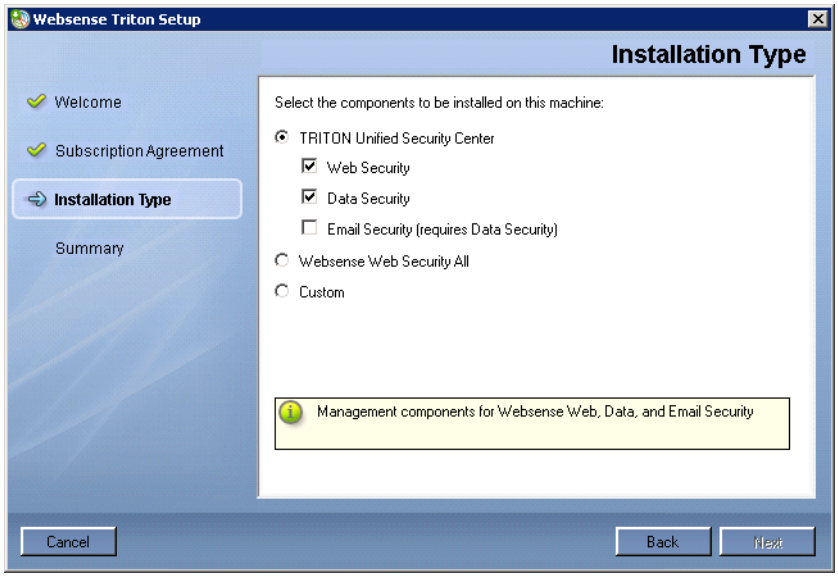
   **Important**: When following these instructions, designate Filtering Service to be integrated with Websense Content Gateway:

   a. On the *Integration Option Screen*, select **Integrated with another application or device.**

   b. On the *Select Integration Screen*, select **Websense Content Gateway**.

   Also install *Policy Broker* and *Policy Server* before creating a TRITON management server.
4. *Websense Content Gateway*, page 357
5. *Creating a TRITON Management Server*, page 645

   **Important**: When following these instructions, choose to install both the Web Security and Data Security modules of the TRITON Unified Security Center. When you reach the **Installation Type** screen of the Websense installer, select both **Web Security** and **Data Security** (under TRITON Unified Security Center).



# Initial configuration

# 26 Websense Content Gateway

## Applies to

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

Websense Content Gateway (Content Gateway) is a Linux-based, high-performance Web proxy and cache that provides real-time content scanning and Web site classification to protect network computers from malicious Web content while controlling employee access to dynamic, user-generated Web 2.0 content. Web content has evolved from a static information source to a sophisticated platform for 2-way communications, which can be a valuable productivity tool when adequately secured.

Content Gateway offers:

- Automatic categorization of dynamic Web 2.0 sites
- Automatic categorization of new, unclassified sites
- HTTPS content inspection
- Enterprise proxy caching capabilities

In a Websense-appliance-based deployment, Content Gateway is already installed on any Web-security-mode appliance.

In a software-based deployment, Content Gateway is a required part of Websense Web Security Gateway and Web Security Gateway Anywhere deployments. Content Gateway must be installed on a Linux machine. Typically, the machine is dedicated to running Content Gateway.

Content Gateway can also provide Web caching, improving bandwidth usage and network performance by storing requested Web pages and, while a stored page is considered fresh, serving that Web page to the requesting client.

In addition, Content Gateway can scan for content categorization. This feature examines the content on Web pages that are not included in the Websense Master Database and on pages that Websense has determined to have rapidly changing content. After this examination, Content Gateway returns a recommended category to Websense filtering software, which then permits or blocks the Web page depending on the policy in effect.

Websense Web Security Gateway and Web Security Gateway Anywhere subscribers get the following features, in addition to the standard Websense filtering and proxy features:

- Security scanning, which inspects incoming Web pages to immediately block malicious code, such as phishing, malware, and viruses.
- Advanced file scanning, which offers both traditional antivirus scanning and advanced detection techniques for discovering and blocking infected and malicious files users are attempting to download.
- Content stripping, which removes active content (code written in selected scripting languages) from incoming Web pages.

See the TRITON - Web Security Help for information on the scanning options.

When installed as part of Websense Web Security Gateway Anywhere, Content Gateway also works with Websense Data Security Management Server to prevent data loss over Web channels. For more information, see *Web Security Gateway Anywhere (software-based)*, page 351.

Content Gateway can behave as an explicit or transparent proxy.

- In an explicit proxy deployment, client browsers must be configured to point to Content Gateway.
- In a transparent proxy deployment, client requests are intercepted and redirected to Content Gateway by an external network device (required).

If you enable SSL Manager, in addition to filtering HTTPS URLs, the content on those pages is decrypted, examined for security issues, and, if appropriate, re-encrypted and forwarded to the destination.

When you run Content Gateway with Websense Data Security, which inspects HTTPS and FTP traffic, you must enable the SSL Manager feature. See the Content Gateway Manager Help for information on SSL Manager.

## Deployment



## Installation

These installation instructions are for installing Content Gateway software on a server. In Websense-appliance-based deployment of Websense Web Security Gateway or Web Security Gateway Anywhere, Content Gateway is already installed on the appliance and these instructions do not apply.

Complete the following procedures.

1. *Installing Web Security components to work with Websense Content Gateway*, page 360
2. *Preparing to install Websense Content Gateway*, page 361
3. *Installing Websense Content Gateway*

## Initial configuration

# Online Help

Select the **Help** option in Websense Content Gateway Manager to display detailed information about using the product.

**IMPORTANT**

Default Microsoft Internet Explorer settings may block operation of the Help. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

# Installing Web Security components to work with Websense Content Gateway

## Applies to

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Installing Web Security components to work with Websense Content Gateway

If you are installing Websense Content Gateway (Content Gateway) as part of a software-based deployment of Websense Web Security Gateway or Web Security Gateway Anywhere, you must install the Web filtering components prior to installing Content Gateway. For instructions, see:

- *Web Security Gateway (software-based)*, page 161
- *Web Security All*, page 75
- *Web Security Gateway Anywhere (software-based)*, page 351

During installation of filtering components:

- On the *Integration Option Screen*, be sure to select Integrated with another application or device. In the *Select Integration Screen* that follows, select Websense Content Gateway as the integration product.

- Note the IP address(es) of Policy Server and Filtering Service. You will need them when installing Websense Content Gateway.

**Note**

Be sure host name and DNS are configured before installing your Websense products (see *System requirements for Websense Content Gateway*. In addition, synchronize the time on the filtering-software and Content Gateway machines. It is a best practice to use a Network Time Protocol (NTP) server.

# Preparing to install Websense Content Gateway

## Applies to

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

Before installing Websense Content Gateway (Content Gateway) on a machine, perform the following tasks or consider the following issues.

## Downloading the installer

1. Download the **WebsenseCG76Setup_Lnx.tar.gz** installer tar archive, from mywebsense.com to a temporary directory.
2. Create a directory for the tar archive, and then move the archive to the new directory. For example:

```
mkdir wcg_v76
mv <installer tar archive> wcg_v76
```

3. Change to the directory you created in Step 2.

   ```
   cd wcg_v76
   ```

4. Unpack the tar archive:

   ```
   tar -xvzf <installer tar archive>s
   ```

# Internet connectivity

It is recommended that the Content Gateway machine have Internet connectivity before starting the installation procedure.The software will install without Internet connectivity, but Websense license keys (and licensed features) cannot be validated until Internet connectivity is available.

# Security of the Websense Content Gateway machine

Consider these security issues prior to installing Websense Content Gateway (Content Gateway):


- *Physical security*, page 362
- *Root permissions*, page 362
- *Ports*, page 362


## Physical security

Physical access to the system can be a security risk. Unauthorized users could gain access to the file system, and under more extreme circumstances, examine traffic passing through Content Gateway. It is strongly recommended that the Content Gateway server be locked in an IT closet and that a BIOS password be enabled.

## Root permissions

Ensure that root permissions are restricted to a select few persons. This important restriction helps preclude unauthorized access to the Websense Content Gateway file system.

## Ports

Websense Content Gateway uses the following ports. They must be open to support the full set of Websense Web Security Gateway features. These are all TCP ports, unless otherwise noted.

> **Note**
> If you customized any ports that Websense software uses for communication, replace the default port shown below with the custom port you implemented.

Restrict inbound traffic to as many other ports as possible on the Websense Content Gateway server. In addition, if your subscription does not include certain features, you can restrict inbound traffic to the unneeded ports. For example, if your subscription does not include Websense Data Security, you may choose to restrict inbound traffic to those ports related to Websense Data Security (e.g., 5819, 5820, 5821, and so forth).

| Port | Function |
|---|---|
| 21 | FTP |
| 22 | SSH for command-line access |
| 53 | DNS |
| 80 | HTTP |
| 443 | Inbound for transparent HTTPS proxy |
| 2121 | FTP |
| 2048 | WCCP for transparent proxy (if used) |
| 3130 | (UDP) ICP for ICP Cache Hierarchy |
| 5819 | Websense Data Security fingerprint detection |
| 5820 | Websense Data Security fingerprint synchronization |
| 5821 | Websense Data Security fingerprint configuration |
| 5822 | Websense Data Security fingerprint configuration |
| 5823 | Websense Data Security fingerprint configuration |
| 8070 | SSL inbound |
| 8071 | SSL Manager interface |
| 8080 | Inbound for explicit HTTP and HTTPS proxy |
| 8081 | Websense Content Gateway management interface |
| 8083 | Autoconfiguration for clustering |
| 8084 | Process Manager for clustering |
| 8085 | Logging server for clustering |
| 8086 | Clustering |
| 8087 | Reliable service for clustering |
| 8088 | (UDP) Multicast for clustering |
| 8090 | HTTPS outbound (between Websense Content Gateway and the SSL outbound proxy) |
| 8880 | Websense Data Security configuration |
| 8888 | Websense Data Security configuration deployment and system health information |
| 8889 | Websense Data Security configuration deployment and system health information |
| 8892 | Websense Data Security system logging |

| Port | Function |
|---|---|
| 9080 | Websense Data Security statistics and system health information |
| 9081 | Websense Data Security statistics and system health information |
| 9090 | Websense Data Security diagnostics |
| 9091 | Websense Data Security diagnostics |
| 18303 | Websense Data Security local analysis |
| 18404 | Websense Data Security remote analysis |
| 55826 | |
| 55827 | |

### IPTables Firewall

If your server is running the Linux IPTables firewall, you must configure the rules in a way that enables Websense Content Gateway to operate effectively. See the IPTables for Content Gateway article in the Websense Technical Library.

## Explicit or Transparent Proxying by Websense Content Gateway

Websense Content Gateway (Content Gateway) can be used as an explicit or transparent proxy. This section contains the following topics:



### Explicit proxy

Explicit proxy deployment requires directly pointing client Web browsers to Content Gateway for HTTP, or HTTPS, or FTP-over-HTTP traffic. This is accomplished by a using a PAC file, WPAD, or by having the user edit browser settings to point to Content Gateway. Explicit proxy deployment does not require a WCCP-enabled router.

One issue to consider with explicit deployment is that a user can point his or her browser to another destination to bypass Content Gateway. You can address this concern by setting and propagating browser configuration in your organization through Group Policy. For more information about Group Policy, search the Microsoft TechNet Web site at http://technet.microsoft.com. An additional way to mitigate the risk of users bypassing Content Gateway is the use of corporate outbound firewall rules.

Multiple proxies can provide for redundancy using Virtual Router Redundancy Protocol (VRRP). Using a single IP address, requests are sent to an alternate proxy in the event of failure. VRRP is not invoked until there is a failure with one of the proxies. See RFC 3768 for information on VRRP.

## Configuring client browsers for explicit proxy

For explicit proxy deployments, you must configure each client browser to send Internet requests to Content Gateway, over the ports that Content Gateway uses for the associated protocol.

The default proxy port in Content Gateway for both HTTP and HTTPS traffic is 8080.

Use the instructions below to configure client browsers manually. Alternatively, use a PAC or WPAD file to configure client browsers.

> **Note**
> The instructions below are for the most common client browsers. For other client browsers refer to the browser's documentation for instructions on manual explicit proxy configuration.

## Configuring Internet Explorer 7.0 and later for explicit proxy by Content Gateway

1. In Internet Explorer, select **Tools** > **Internet Options** > **Connections** > **LAN Settings**.
2. Select **Use a proxy server for your LAN**.
3. **Click** Advanced.
4. For **HTTP**, enter the Content Gateway IP address and specify port 8080.
5. For **Secure**, enter the Content Gateway IP address and specify port 8080.
6. Clear **Use the same proxy server for all protocols**.
7. Click **OK** to close each screen in this dialog box.

## Configuring Firefox 3.x for explicit proxy by Content Gateway

1. In Firefox, select **Tools** > **Options** > **Advanced**, and then select the **Network** tab.
2. Select **Settings**.
3. Select **Manual proxy configuration.**

4. For **HTTP Proxy**, enter the Content Gateway IP address and specify port 8080.
5. For **SSL Proxy**, enter the Content Gateway IP address and specify port 8080.
6. Click **OK** to close each screen in this dialog box.

### Transparent proxy

In transparent deployments, client requests are intercepted and redirected to Content Gateway, without client involvement, via a WCCPv2-enabled router or Layer 4 switch in your network. In multiple-proxy deployment, a WCCPv2-enabled router can also facilitate load balancing among the proxies.

See the Content Gateway Manager Help for additional information on configuring a WCCPv2-enabled router or a Layer 4 switch, and about the ARM (Adaptive Redirection Module).

### Configuring a router for transparent proxy by Content Gateway

For transparent proxy deployment, configure your router to use WCCP v2, which can support both the HTTP and HTTPS protocols. See the Content Gateway Manager Help for additional information on configuring a WCCPv2-enabled router or a Layer 4 switch and on the ARM (Adaptive Redirection Module).

## System requirements for Websense Content Gateway


- *Hardware*, page 366
- *Software*, page 367
- *Preparing a cache disk for use by Websense Content Gateway*, page 370


### Hardware

| | |
|---|---|
| CPU | Quad-core running at 2.8 GHz or faster |
| Memory | 4 GB |
| Disk space | 2 disks:<br>• 100 GB for the operating system, Websense Content Gateway, and temporary data. |

| | |
|---|---|
| | • 147 GB for caching<br>If caching will not be used, this disk is not required.<br>The caching disk:<br>– Should have minimum size of 2 GB, maximum 147 GB for optimal performance<br>– Must be a raw disk, not a mounted file system (for instructions on creating a raw disk from a mounted file system.)<br>– Must be dedicated<br>– Must *not* be part of a software RAID<br>– Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64MB of write-through cache |
| Network Interfaces | 2 |

### To support transparent proxy deployments

| | |
|---|---|
| Router | Must support WCCP v2.<br>A Cisco router must run IOS 12.2 or later.<br>Client machines, the destination Web server, and Websense Content Gateway must reside on different subnets. |
| **—or—** | |
| Layer 4 switch | You may use a Layer 4 switch rather than a router.<br>To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later).<br>Websense Content Gateway must be Layer 2 adjacent to the switch.<br>The switch must be able to rewrite the destination MAC address of frames traversing the switch.<br>The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80). |

## Software

### Linux operating system

- Websense Content Gateway version 7.6 is certified on Red Hat Enterprise Linux 5 series, updates 3, 4, 5, or 6 base or Advanced Platform (32-bit only), and the corresponding CentOS version (number corresponds to the Red Hat version).
  - Although not certified, Websense, Inc. provides "best effort" support for newer versions of Red Hat Enterprise Linux. Under "best effort" support, Websense Technical Support makes a best effort to troubleshoot cases in

standard fashion unless the issue is deemed a Red Hat Enterprise Linux-specific issue, at which point you must contact Red Hat directly for assistance.

> **Note**
> Red Hat Enterprise Linux 6 series is **not** supported at this time.

- Only kernels shipped with the above Linux versions are supported by Websense Content Gateway. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:
  `/bin/uname -r`

- PAE (Physical Address Extension)-enabled kernel required
  - By default, Red Hat Enterprise Linux 5, update 3 and later has PAE enabled. If you are running the non-PAE kernel, reboot with the PAE-enabled kernel before installing Websense Content Gateway.
- RPM compat-libstdc++-33-3.2.3-47.3.i386.rpm (or higher version of this package)
  - To display a list of RPMs installed on your system with the string "compat-libstdc" in their name, enter the command:
    `rpm -qa |grep compat-libstdc`
- libgdbm.so.2 required
- RPM krb5-workstation-*.rpm

  This must be the version of the krb5-workstation RPM that is bundled with your version of Red Hat Enterprise Linux.
  - To display a list of RPMs installed on your system with the string "krb5-workstation" in their name, enter the command:
    `rpm -qa |grep krb5-workstation`
- GNU C library (glibc) version 2.5-42 or later
  - Note that Red Hat Enterprise Linux 5, update 3 ships with glibc version 2.5-34. Be sure to update it to version 2.5-42 or later.
  - Example command to update this library (running as `root`): `yum update glibc`.
- SELinux set to permissive or disabled

> **Important**
> If SELinux is enabled, set it to permissive or disable it before installing Websense Content Gateway.

### Websense Web filtering components

(Websense Web Security Gateway, Websense Web Security, Websense Web Filter)

- Version 7.6

> **Important**
> Websense filtering software must be installed prior to Websense Content Gateway. When the filtering software is installed, Websense Content Gateway must be specified as the integration product. See *Web Security Gateway (software-based)*, page 161, *Web Security All*, page 75, or *Web Security Gateway Anywhere (software-based)*, page 351.

### Integration with Websense Data Security

- Version 7.6 (to take advantage of the co-located Data Security policy engine)

  The order of installation does not matter. Websense Data Security may be installed before or after Websense Content Gateway.
- Any version can be used via the ICAP interface. See the Content Gateway Manager Help for configuration instructions.

### Web browsers

- Websense Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway Manager. Content Gateway Manager supports the following Web browsers:
  - Internet Explorer 7, 8, and 9
  - Mozilla Firefox 3 and later

> **Note**
> The browser restrictions mentioned above apply only to the Content Gateway Manager and not to client browsers proxied by Websense Content Gateway.

## Hostname and DNS configuration for Websense Content Gateway

Configure a hostname for the Websense Content Gateway (Content Gateway) machine and also configure DNS name resolution. Complete these steps on the machine on which you will install Content Gateway.

1. Configure the hostname:

   `hostname <host>`

   where <*host*> is the name you are assigning this machine.

   > **Important**
   > The hostname must be 15 characters or less.

2. Update the HOSTNAME entry in the **/etc/sysconfig/network** file:

   ```
   HOSTNAME=<host>
   ```

   where <*host*> is the same as in Step 1.

3. Specify the IP address to associate with the hostname in the **/etc/hosts** file. This should be static, and not served by DHCP. The proxy uses this IP address in features such as transparent authentication and hierarchical caching. This must be the first line in the file. Do not delete the second line in the file (the one that begins with 127.0.0.1).

   ```
   xxx.xxx.xxx.xxx   <FQDN>    <host>
   127.0.0.1       localhost.localdomain   localhost
   ```

   where <*FQDN*> is the fully-qualified domain name of this machine (i.e., <*host*>.<*subdomain(s)*>.<*top-level domain*>)—for example, myhost.example.com—and <*host*> is the same as in Step 1.

4. Configure DNS in the **/etc/resolv.conf** file.

   ```
   search <subdomain1>.<top-level domain> <subdomain2>.<top-level domain> <subdomain3>.<top-level domain>
   nameserver xxx.xxx.xxx.xxx
   nameserver xxx.xxx.xxx.xxx
   ```

   This example demonstrates that more than one domain can be listed on the search line. Listing several domains may have an impact on performance, because each domain is searched until a match is found. Also, this example shows a primary and secondary nameserver being specified.

5. Gather this information:
   - Default gateway (or other routing information)
   - List of your company's DNS servers and their IP addresses
   - DNS domains to search, such as internal domain names. Include any legacy domain names that your company might have acquired.
   - List of additional firewall ports to open beyond SSH (22) and the proxy ports (8080-8090). See *Ports*.

## Preparing a cache disk for use by Websense Content Gateway

For Websense Content Gateway to operate as a caching proxy, it must have access to at least one raw disk. Otherwise, Content Gateway can function as a proxy only.

To create a raw disk for the proxy cache when all disks have a mounted file system:

> **Note**
>
> This procedure is necessary only if you want to use a disk already mounted to a file system as a cache disk for Content Gateway. Perform this procedure**before** installing Content Gateway.

**Warning**
Do not use an LVM (Logical Volume Manager) volume as a cache disk.

**Warning**
The Content Gateway installer will irretrievably clear the contents of cache disks.

1. Enter the following command at the prompt to examine which file systems are mounted on the disk you want to use for the proxy cache:
   ```
   df -k
   ```
2. Open the file /etc/fstab and comment out or delete the file system entries for the disk.
3. Save and close the file.
4. Enter the following command for each file system you want to unmount:
   ```
   umount <file_system>
   ```
   where <*file_system*> is the file system you want to unmount.

When the Content Gateway installer prompts you for a cache disk, select the raw disk you created.

**Note**
It is possible to add cache disks after Content Gateway is installed. For instructions, see the Content Gateway Manager Help.

## Preparing for a clustered deployment of Websense Content Gateway

If you plan to deploy multiple, clustered instances of Websense Content Gateway (Content Gateway):

- Find the name of the network interface you want to use for cluster communication. This must be a dedicated interface.
- Find or define a multicast group IP address.
- Enter the following at a command line to define the multicast route:
  **route add** <*multicast.group address*>*/32* **dev** <*interface_name*>
  where <*interface_name*> is the name of the interface used for cluster communication. For example:
  ```
  route add 224.0.1.37/32 dev eth1
  ```

# Installing Websense Content Gateway

## Applies to

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Installing Websense Content Gateway

Complete these steps to install Websense Content Gateway (Content Gateway) on a server in a software-base deployment of Websense software. In a Websense-appliance-based deployment, Content Gateway is already installed on the appliance.

Before you begin, be sure to read *Preparing to install Websense Content Gateway*.

1. Disable any currently running firewall on this machine for the duration of Content Gateway installation. Bring the firewall back up after installation is complete, opening ports used by Content Gateway.

   For example, if you are running IPTables:

   a. At a command prompt, enter **service iptables status** to determine if the firewall is running.

   b. If the firewall is running, enter **service iptables stop**.

   c. After installation, restart the firewall. In the firewall, be sure to open the ports used by Content Gateway on this machine. See *Ports* for more information.

2. Download the **WebsenseCG76Setup_Lnx.tar.gz** tar archive, from mywebsense.com to a temporary directory:

   a. Create a directory for the tar archive, and then move the archive to the new directory. For example:

   ```
   mkdir wcg_v76
   mv <installer tar archive> wcg_v76
   ```

   b. Change to the directory you created in Step a.

   ```
   cd wcg_v76
   ```

   c. Unpack the tar archive:

   ```
   tar -xvzf <installer tar archive>s
   ```

   > **Important**
   > If SELinux is enabled, set it to permissive or disable it before installing Websense Content Gateway. Do not install or run Websense Content Gateway with SELinux enabled.

3. Make sure you have root permissions:

```
su root
```

4. In the directory where you unpacked the tar archive, begin the installation, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

   The installer will install Websense Content Gateway to /opt/WCG. It is installed as **root**.

   > **Note**
   > Up to the configuration summary (Step 17 below), you can quit the installer by pressing CTRL-C. If you choose to continue the installation past the configuration summary and you want to quit, do **not** use CTRL-C. Instead, allow the installation to complete and then uninstall it.
   >
   > If you want to change your answer to any of the installer prompts, you will be given a chance to start over at the first prompt once you reach the configuration summary; you do not have to quit the installer.

5. If your system does not meet the minimum recommended requirements, you receive a warning. For example:

   ```
   Warning: Websense Content Gateway requires at least 2
   gigabytes of RAM.


   Do you wish to continue [y/n]?
   ```

   Enter **n** to end the installation, and return to the system prompt.

   Enter **y** to continue the installation. If you choose to run Content Gateway after receiving this warning, performance may be affected

6. Read the subscription agreement. At the following prompt, enter **y** to continue installation or **n** to cancel installation.

   ```
   Do you accept the above agreement [y/n]? y
   ```

7. Enter and confirm a password for the Content Gateway Manager administrator account:

   ```
   Enter the administrator password for the Websense Content
   Gateway management interface.
   Username: admin
   Password:> (note: cursor will not move as you type)
   Confirm password:>
   ```

   This account enables you to log on to the management interface for Content Gateway, known as Content Gateway Manager. The default username is **admin**.

To create a strong password (recommended), use 8 or more characters, with at least 1 each of the following: capital letter, lower case letter, number, special character.

**Important**

The password length must be 16 characters or less. Also, it cannot contain the following characters:

- space
- $ (dollar symbol)
- : (colon)
- ‘ (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- “ (double-quote)

**Note**

As you type a password, it may seem that nothing is happening—the cursor will not move nor masked characters shown—but the characters are being accepted. After typing a password, press **Enter**. Then repeat to confirm it.

8. Enter an email address where Websense Content Gateway can send alarm messages:

   ```
   Websense Content Gateway requires an email address for alarm
   notification.
   Enter an email address using @ notation: [] >
   ```

   Be sure to use @ notation (for example, user@example.com). Do not enter more than 64 characters for this address.

9. Enter the IP address for Policy Server:

   ```
   Enter the Policy Server IP address (leave blank if
   integrating with Data Security only): [] >
   ```

   Use dot notation (i.e., xxx.xxx.xxx.xxx). Press **Enter** to leave this field blank if this Content Gateway deployment is with Websense Data Security only.

10. Enter the IP address for Filtering Service:

    ```
    Enter the Filtering Service IP address: [<Policy Server
    address>] >
    ```

    The default is the same address as Policy Server. This field does not appear if you did not enter an IP address for Policy Server in Step 9.

11. Review default Content Gateway ports:

```
Current port assignments:
-------------------------------------------
'1'  Websense Content Gateway Proxy Port  8080
'2'  Web Interface port                   8081
'3'  Auto config port                     8083
'4'  Process manager port                 8084
'5'  Logging server port                  8085
'6'  Clustering port                      8086
'7'  Reliable service port                8087
'8'  Multicast port                       8088
'9'  HTTPS inbound port                   8070
'N'  HTTPS outbound port                  8090
'M'  HTTPS management port                8071
'D'  Download Service port                30900

Enter the port assignment you would like to change:
‘1-9,N,M,D’ - specific port changes
‘X’  - no change
‘H’  - help
[X] >
```

Ports preceded by numbers in the list are considered the 9 ports for Content Gateway. Ports preceded by letters are needed if you have subscribed to Websense Web Security Gateway or Web Security Gateway Anywhere.

Change a port assignment if it will conflict with another application or process on the machine. Otherwise, leave the default assignments in place.

If you do not want to use these ports for Content Gateway, or if the installation program indicates that a port conflict exists, make any necessary changes. Any new port numbers you assign must be between 1025 and 65535, inclusive.

12. For clustering, at least two network interfaces are required. If your machine has only one, the following prompt appears:

    ```
    Websense Content Gateway requires at least 2 interfaces to
    support clustering. Only one active network interface is
    detected on this system.
    ```

    Press ENTER to continue installation and skip to Step 14.

13. If two or more network interfaces are found on this machine, you are asked whether this instance of Content Gateway should be part of a cluster:

    ```
    '1' - Select '1' to configure Websense Content Gateway
            for management clustering. The nodes in the cluster
            will share configuration/management information
            automatically.
    '2' - Select '2' to operate this Websense Content Gateway
            as a single node.

    Enter the cluster type for this Websense Content Gateway
    installation:
    ```

```
[2] >
```

Enter the number that represents your clustering environment. If you do not want this instance of Content Gateway to be part of a cluster, enter 2.

If you select 1, provide information about the cluster:

```
Enter the name of this Websense Content Gateway cluster.
><cluster_name>
```

Note: All members of a cluster must use the same cluster name.

```
Enter a network interface for cluster communication.
Available interfaces:
<interface, e.g., eth0>
<interface, e.g., eth1>
Enter the desired cluster network interface:
>

Enter a multicast group address for cluster <cluster_name>.
Address must be in the range <IP address range>:
[<default IP address>] >
```

14. For Content Gateway to act as a Web cache, a raw disk must be present on this machine. If no raw disk is detected, the following prompt appears:

    ```
    No disks are detected for cache.
    Websense Content Gateway will operate in PROXY_ONLY mode.
    ```

    Content Gateway will operate as a proxy only and will not cache Web pages. Press ENTER to continue the installation and skip to Step 16.

15. If a raw disk is detected, you can enable the Web cache feature of Content Gateway:

    ```
    Would you like to enable raw disk cache [y/n]? y
    ```

    a. Select available disks from the list. Selected disks become dedicated cache disks and cannot be used for any other purpose. Cache disks must be raw. Aggregate disk cache size should not exceed 147 GB.

    ```
    Select available disk resources to use for the cache.
    Remember that space used for the cache cannot be used for
    any other purpose.

    Here are the available drives
    (1) /dev/sdb 146778685440 0x0
    ```

    Note: The above drive is only an example.

    **Warning**

    Although it might be listed as available, do **not** use an LVM (Logical Volume Manager) volume as a cache disk.

b. Indicate if you want to add or remove disks individually or as a group.

```
Choose one of the following options:
'A'   - Add disk(s) to cache
'R'   - Remove disk(s) from cache
'S'   - Add all available disks to cache
'U'   - Remove all disks from cache
'X'   - Done with selection, continue Websense
        Content Gateway installation.

Option: > A
[ ] (1) /dev/sdb 146778685440 0x0
```

c. Specify which disk(s) to use for the cache.

```
Enter number to add item, press 'F' when finished:
[F] >1
Item '1' is selected
[F] >
```

d. Your selections are confirmed. Note the "x" before the name of the disk.

```
Here is the current selection
[X] (1) /dev/sdb 146778685440 0x0
```

e. Continue based on your choice in Step b, pressing **X** when you have finished configuring cache disks.

```
Choose one of the following options:
'A'   - Add disk(s) to cache
'R'   - Remove disk(s) from cache
'S'   - Add all available disks to cache
'U'   - Remove all disks from cache
'X'   - Done with selection, continue Websense
        Content Gateway installation.

Option: >X
```

16. You can elect to send Websense, Inc., information about scanned content (Note: individual users are never identified):

```
Websense Content Gateway can send information about scanned
content to Websense, Inc. This information helps Websense,
Inc. improve filtering and scanning technology and accuracy.

Websense software never includes information that would
identify specific users.

Do you want to enable the Websense Content Gateway Feedback
Agent [y/n]?
```

17. A configuration summary appears, showing your answers to the installer prompts (note: summary below is an example):

```
Configuration Summary
```

```
-------------------------------------------------------------
Websense Content Gateway Install Directory : /opt/WCG
Admin Username for Content Gateway Manager: admin
Alarm Email Address                        : <email address>

Policy Server IP Address                   : <IP address>
Filtering Service IP Address               : <IP address>

Websense Content Gateway Cluster Type      : NO_CLUSTER

Websense Content Gateway Cache Type        : LRAW_DISK
  Cache Disk                               : /dev/sdb
  Total Cache Partition Used               : 1

                  ******************
                  *  W A R N I N G  *
                  ******************
    CACHE DISKS LISTED ABOVE WILL BE CLEARED DURING
    INSTALLATION!! CONTENTS OF THESE DISKS WILL BE
    COMPLETELY LOST WITH NO CHANCE OF RETRIEVAL.

    Installer CANNOT detect all potential disk mirroring
    systems. Please make sure the cache disks listed
    above are not in use as mirrors of active file
    systems and do not contain any useful data.

Do you want to continue installation with this configuration
[y/n]?
```

If you want to make changes, enter **n** to restart the installation process at the first prompt. To continue and install Content Gateway configured as shown, enter **y**.

**Important**

If you enter **y** to proceed but you decide you want to cancel the installation, do not attempt to quit the installer by pressing CTRL-C. Allow the installation to complete. Then uninstall it.

18. Wait for the installation to complete.

    Note the location of the certificate required for Content Gateway Manager: **/root/WCG/content_gateway_ca.cer**. See the Getting Started section of the Content Gateway Manager Help for information on importing this certificate.

    You may receive an email from Websense Content Gateway (to the address you specified during installation for receiving alerts) with "WCG license download failed" in the subject line. This does not mean a problem occurred with the installation; this alert is generated because a subscription key has not been entered yet. You will enter a key as part of initial configuration tasks.

19. When installation is complete, reboot the Websense Content Gateway server.
20. When the reboot is complete, check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

All services should be running. These include:

- Content Cop
- Websense Content Gateway
- Content Gateway Manager
- Websense Download Service
- Analytics Server

# 27 Deploying Websense Content Gateway

## Applies to

- Web Security Gateway v76.x
- Web Security Gateway Anywhere v7.6.x

## Deploying Websense Content Gateway

Websense® Content Gateway is a high-performance Web proxy that provides real-time content scanning and Web site classification to protect network computers from malicious Web content while controlling employee access to dynamic, user-generated Web 2.0 content. Web content has evolved from a static information source to a sophisticated platform for 2-way communications, which can be a valuable productivity tool when adequately secured.

The dilemma for administrators is how much access to allow. Web 2.0 sites rely primarily on HTTP/HTTPS protocols, which cannot be blocked without halting all Internet traffic. Malicious content can use this means of entry into a company network.

The Websense Content Gateway module offers:

- Automatic categorization of dynamic Web 2.0 sites
- Automatic categorization of unclassified sites
- HTTPS content inspection
- Enterprise proxy caching capabilities

Websense Content Gateway is deployed as an add-on module with Websense Web Security. Websense Content Gateway can also be an important piece of the following Websense deployments:

- Web Security Gateway for on-premises deployments. On-premises deployments may be implemented on Websense V-Series appliances or as software running on general purpose servers.
- Hosted Web Security Gateway for software as a service (SaaS) deployments

- Web Security Gateway Anywhere for distributed enterprises with one or more branch offices and multiple remote users

Deploying Websense Content Gateway can improve network efficiency and performance by caching frequently accessed information at the edge of the network. However, the increasing use of dynamic Web content that cannot be cached limits the effectiveness of this feature.

The following topics provide discuss deployment of Content Gateway:

- *Content Gateway deployment issues*, page 382
- *Content Gateway explicit and transparent proxy deployments*, page 386
- *Special Content Gateway deployment scenarios*, page 391
- *Chaining Content Gateway with other Proxies*, page 401

For more information about deploying Web filtering software, see *Web Security Gateway (software-based)*, page 161.

For more information on Websense Content Gateway operation, see the Content Gateway Manager online Help.

# Content Gateway deployment issues

## Applies to

- Web Security Gateway v7.6.x
- Web Security Gateway Anywhere v7.6.x

## In this topic



## Overview

A plan to deploy Websense Content Gateway as a proxy in your network involves more than physical site requirements like plant size, the power and cooling requirements for the hardware, available rack space, and network connectivity. You should also consider some of the following issues:

- Websense Content Gateway system requirements
- Advantages and disadvantages of various proxy network configuration options

- User authentication considerations
- Possible HTTPS content inspection
- A plan for handling special proxy/client issues

# Proxy deployment options

Websense Content Gateway is used in either an explicit or transparent proxy deployment. With an explicit proxy deployment, client software is configured to send a request for Internet content directly to Websense Content Gateway. In a transparent proxy deployment, a client request for Web content is intercepted (usually by a router) and sent to the proxy, and the client is unaware that it is communicating with a proxy.

Both options have advantages and disadvantages that should be investigated for Websense Content Gateway deployment. See *Content Gateway explicit and transparent proxy deployments*, page 386 for more information.

Other deployment options for the proxy are described in this section.

## Management clustering

A Websense Content Gateway deployment can scale from a single node to multiple nodes to form management cluster. With management clustering, all the nodes in a cluster share configuration information. A configuration change on one node is automatically made in all other nodes.

When SSL Manager is enabled to perform HTTPS content inspection, SLL configuration information can also be propagated around the cluster, however it uses a different mechanism that requires separate configuration.

See *Clusters* in Content Gateway Manager online Help for information about configuring proxy clusters.

## IP spoofing

When enabled, the IP spoofing feature directs the proxy to use the client IP address when establishing a connection to an origin server, rather than the proxy's IP address. With this option, a request appears to be from the client, not the proxy. IP spoofing is supported only in transparent proxy deployments. You should note that if IP spoofing is implemented, the client IP address is used for *all* HTTP and HTTPS requests in transparent proxy deployments.

**Warning**

Deploying IP spoofing requires precise control of the routing paths on your network, overriding the normal routing process for traffic running on TCP port 80 and 443.

With IP spoofing enabled, traditional debugging tools such as **traceroute** and **ping** have limited utility.

You might want to implement this feature, for example, if an upstream network device is used to log HTTP/S traffic, perform authentication, or access controls based on the client IP address.

For information about how to enable IP spoofing, see*Transparent Proxy Caching and ARM* in the Content Gateway Manager online Help.

# User authentication

Authentication is the process of verifying a user via a username and password. User authentication may be configured on Websense Content Gateway. User identification is the process of identifying a user based on the client IP address. TRITON - Web Security offers a robust set of user identification agents.

## Content Gateway user authentication

Websense Content Gateway can be configured for *transparent user authentication* -- with Integrated Windows® Authentication (IWA) and Legacy NTLM -- in which case users are not prompted for credentials, or for *prompted (*or *manual) authentication*, in which case users are required to enter a username and password for network access.

> **Note**
> Not all Web browsers support both transparent and prompted authentication modes. See *Security* in the Content Gateway Manager online Help for specific browser limitations.

In the manual authentication process, Content Gateway prompts a user for proxy login credentials when that user requests Internet content. After the user enters those credentials, the proxy sends them to a directory server, which validates the data. If the directory server accepts the user's credentials, the proxy delivers the requested content. Otherwise, the user's request is denied.

The issue of proxy authentication is important in a deployment in which multiple proxies are chained. Authentication by the proxy closest to the client is preferred, but may not be possible given a particular network's configuration. Other issues include whether Content Gateway is chained with a third-party proxy and which proxy is designated to perform authentication. See *In a proxy chain*, page 396 for more information.

Websense Content Gateway supports the following user authentication methods:

- Integrated Windows Authentication (with Kerberos)
- Legacy NTLM (Windows NT® LAN Manager, NTLMSSP)
- LDAP (Lightweight Directory Access Protocol)
- RADIUS (Remote Authentication Dial-In User Service)

Content Gateway supports both transparent and prompted authentication for Integrated Windows Authentication and Legacy NTLM. LDAP and RADIUS support prompted authentication.

Content Gateway also supports **multiple realm authentication**. Multiple realm authentication is for environments that have multiple domains that are essentially isolated for the purposes of user authentication by a lack of mutual inbound and outbound trust relationships. Therefore, users in these domains must be authenticated by a domain controller within their domain. Multiple realm authentication allows distinct authentication rules to be written for each domain, thereby supporting the ability to use multiple authentication methods (IWA, legacy NTLM, LDAP) at the same time.

See *Security* in the Content Gateway Manager online Help for detailed information about configuring all these proxy authentication options.

### TRITON - Web Security user identification

You can configure user identification in TRITON - Web Security rather than user authentication on the proxy. Methods of user identification include the use of Websense transparent identification (XID) agents like Logon Agent or DC Agent, which identify users transparently. Prompted authentication, which requires users to enter login credentials, can also be configured in TRITON - Web Security. See *User Identification* in the TRITON - Web Security Help for more information.

## HTTPS content inspection

When you use Websense Content Gateway with SSL Manager enabled, HTTPS data can be decrypted, inspected for policy, and then re-encrypted as it travels from the client to the origin server and back. Enabling this feature also means that traffic from the server to the client can be inspected for Web 2.0 and uncategorized sites. The SSL feature includes a complete set of certificate-handling capabilities. See the Content Gateway Manager online Help for information on managing certificates.

Deploying Content Gateway with SSL Manager enabled may require the following modifications to your system:

- Creation of trusted Certificate Authority (CA) certificates for each proxy to use for SSL traffic interception, and the installation of those certificates in each trusted root certificate store used by proxied applications and browsers on each client
- In explicit proxy deployments, additional client configuration in the form of Proxy Auto-Configuration (PAC) files or Web Proxy Auto-Discovery (WPAD)
- In transparent proxy deployments, integration with WCCP v2-enabled network devices

**Note**

HTTPS content inspection can also affect system hardware resources like processing capacity and memory requirements.

When Content Gateway is configured to handle HTTPS traffic, category bypass settings can be used to specify categories of Web sites for which decryption and inspection are bypassed. You can also maintain a list of hostnames or IP addresses for which SSL decryption is not performed. See *Scanning and SSL Bypass Options* in TRITON - Web Security Help for more information.

## Handling special cases

Any Websense Content Gateway deployment must be able to handle Web site requests and applications that are not compatible with the proxy or that should bypass the proxy. For example, requests for data from some internal, trusted sites could be configured to bypass the proxy, for system performance reasons. In explicit proxy deployments, a PAC file can be used to list the traffic that is allowed to bypass proxy inspection. In transparent proxy deployments, the proxy must be installed in a way that allows static bypass. See the "Static bypass rules" section of *Transparent Proxy Caching and ARM* in Content Gateway Manager online Help.

The deployment should also be able to manage situations in which key fobs or tokens are used to access the network and for cases of highly coupled client/server Web applications. The type of proxy deployment determines how these situations are handled.

# Content Gateway explicit and transparent proxy deployments

## Applies to

- Web Security Gateway v7.6.x
- Web Security Gateway Anywhere v7.6.x

## In this topic



## Overview

Websense Content Gateway provides the following proxy deployment options:

- *Explicit proxy deployment,* where the user's client software is configured to send requests directly to Websense Content Gateway

- *Transparent proxy deployment*, where user requests are automatically redirected to a Websense Content Gateway proxy, typically by a switch or router, on the way to their eventual destination

For more information about configuring explicit and transparent proxy options in Websense Content Gateway see *Explicit Proxy Caching* and *Transparent Proxy Caching and ARM* in the Content Gateway Manager online Help.

## Explicit proxy deployment

Use of Websense Content Gateway in an explicit proxy deployment is an easy way to handle Web requests from users. This type of deployment is recommended for simple networks with a small number of users. Explicit proxy is also used effectively when proxy settings can be applied by group policy. It requires minimal network configuration, which can be an advantage for troubleshooting efforts.

For explicit proxy deployment, individual client browsers may be manually configured to send requests directly to the proxy. They may also be configured to download proxy configuration instructions from a Proxy Auto-Configuration (PAC) file. A group policy that points to a PAC file for configuration changes is a best practice for explicit proxy deployments. Another option is the use of Web Proxy Auto-Discovery (WPAD) to download configuration instructions from a WPAD server. See *Explicit Proxy Caching* in Content Gateway Manager online Help for a sample PAC file and more information about how to implement these options.

Exception handling instructions can also be included in the PAC file or WPAD instructions. For example, requests for trusted sites can be allowed to bypass the proxy.

Disadvantages of explicit proxy deployment include a user's ability to alter an individual client configuration and bypass the proxy. To counter this, you can configure the firewall to allow client traffic to proceed only through the proxy. Note that this type of firewall blocking may result in some applications not working properly.

You can also use a Group Policy Option (GPO) setting to prevent users from changing proxy settings. If you cannot enforce group policy settings on client machines, this type of configuration can be difficult to maintain for a large user base because of the lack of centralized management.

**Note**

Non-browser client applications that cannot specify a proxy server may not work with explicit proxy deployment.

## Transparent proxy deployment

In a transparent proxy deployment, the user's client software (typically a browser) is unaware that it is communicating with a proxy. Users request Internet content as usual, without any special client configuration, and the proxy serves their requests.

The Adaptive Redirection Module (ARM) component of Websense Content Gateway processes requests from a switch or router and redirects user requests to the proxy engine. The proxy establishes a connection with the origin server and returns requested content to the client. ARM readdresses returned content as if it came directly from the origin server. For more information, see*Transparent Proxy Caching and ARM* in Content Gateway Manager online Help.

Note that in a transparent proxy deployment, *all* Internet traffic from a client goes through the proxy (not just traffic from Web browsers), including:

- traffic tunneled over HTTP and HTTPS by remote desktop applications
- instant messaging clients
- software updaters for Windows and anti-virus applications
- custom internal applications

Many of these programs are not developed with proxy compatibility in mind. For a successful transparent proxy deployment, the network must be configured to allow the proxy's static bypass feature to work. See the "Static bypass rules" section of *Transparent Proxy Caching and ARM* in Content Gateway Manager online Help.

Because traffic management is centralized, users cannot easily bypass the proxy.

This type of deployment requires the implementation of at least one other network device that is not required in the explicit proxy deployment. Added equipment presents compatibility issues, as all network devices must work together smoothly and efficiently. The overall system is often more complex and usually requires more network expertise to construct and maintain.

The use of a Layer 4 switch or WCCPv2-enabled router to redirect traffic in a transparent proxy deployment can provide redundancy and load distribution features for the network. These devices not only route traffic intelligently among all available servers, but can also detect whether a proxy is nonfunctional. In that case, the traffic is re-routed to other, available proxies.

Exception handling can be included in switch or router configuration. For example, requests for data from some internal, trusted sites can be allowed to bypass the proxy.

## Layer 4 switch

You can implement policy-based routing (PBR) for a transparent proxy deployment with the use of a Layer 4 switch, which can be configured to redirect a request to the proxy, as follows:

1. Create an access control list (ACL) that identifies the Web traffic that should be intercepted.
2. Develop a route map to define how the intercepted Web traffic should be modified for redirection.
3. Apply a "redirect to proxy" policy to the switch interface.

See *Transparent Proxy Caching and ARM* in Content Gateway Manager online Help for more information about the use of a Layer 4 switch.

## WCCP-enabled router

> **Note**
> Websense Content Gateway supports WCCP v2 only.

WCCP is a protocol used to route client request traffic to a specific proxy. A WCCP-enabled router can distribute client requests based on the proxy server's IP address, routing traffic to the proxy most likely to contain the requested information.

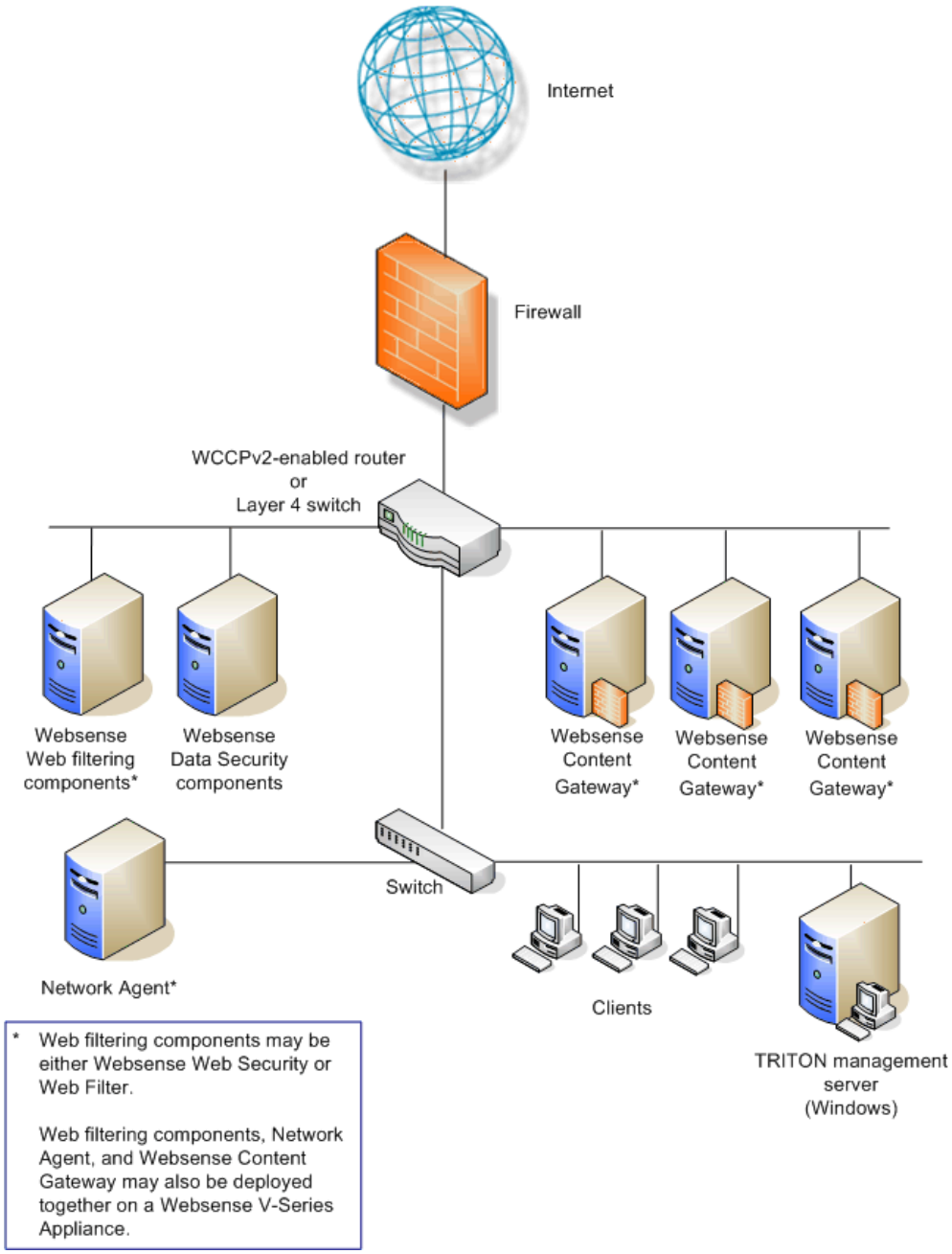
The router may use Generic Routing Encapsulation (GRE) to forward IP packets to the proxy. GRE is a tunneling protocol that allows point-to-point links between multiple traffic routing hops.

A router may also use Layer 2 (L2), which does not use GRE. Websense recommends the use of L2 if the router supports it. With L2 redirection, Content Gateway must be on the same subnet as the WCCP device (that is, Layer 2 adjacent).

> **Important**
> If using L2 the router or switch must be Layer 2-adjacent (in the same subnet) as Content Gateway.

A proxy and a router communicate via a set of WCCP "Here I am" and "I see you" messages. A proxy that does not send a "Here I am" message for 30 seconds is removed from service by the router, and client requests that would have been directed to that proxy are sent to another proxy.

The following illustration shows an example transparent proxy deployment.



A comparison of how some activities are handled in explicit and transparent proxy deployments appears in the following table:

| Activity | Explicit Proxy Deployment | Transparent Proxy Deployment | Proxy Chain |
|---|---|---|---|
| Client HTTP request | Direct connection to proxy by browser to port 8080 (default) | Redirected to proxy by network device using GRE encapsulation or by rewriting the L2 destination MAC address to the proxy's address | Direct connection to parent proxy from child proxy |
| Exception management | Exclude site, CIDR, etc., using browser configuration settings and PAC file settings. | Static or dynamic bypass rules | Child/parent proxy configuration rules |
| Proxy authentication | Proxy challenge using 407 Proxy Authentication Required code | Challenge using server-based authentication scheme (client is not aware of proxy) | Proxies in a chain may share credential information, or a single proxy in the chain can perform authentication. |
| Redundancy Proxy | virtual IP pool shared across multiple proxies | WCCP pool with multiple proxies | Parent/child configuration points to proxy virtual IP addresses. |
| Proxy management | Management clustering | Management clustering | Management clustering |
| Load balancers | Supported | N/A | Supported |

# Special Content Gateway deployment scenarios

## Applies to

- Web Security Gateway v7.6.x
- Web Security Gateway Anywhere v7.6.x

## In this topic

# Overview

Websense Content Gateway can be deployed in proxy clusters with failover features that contribute to high availability. The proxy can also be deployed in a chain, either with other Websense Content Gateway proxies or third-party proxies. This section describes some examples of these deployment scenarios.

# Highly available Web proxy

A highly available Web proxy provides continuous, reliable system operation. Minimizing system downtime increases user access and productivity.

Proxy high availability may be accomplished via a proxy cluster that uses various failover contingencies. Such deployments may involve either an explicit or transparent proxy configuration, load balancing, virtual IP addresses, and a variety of switching options. This section summarizes some possibilities for highly available Web proxy deployments.

## Using explicit proxy

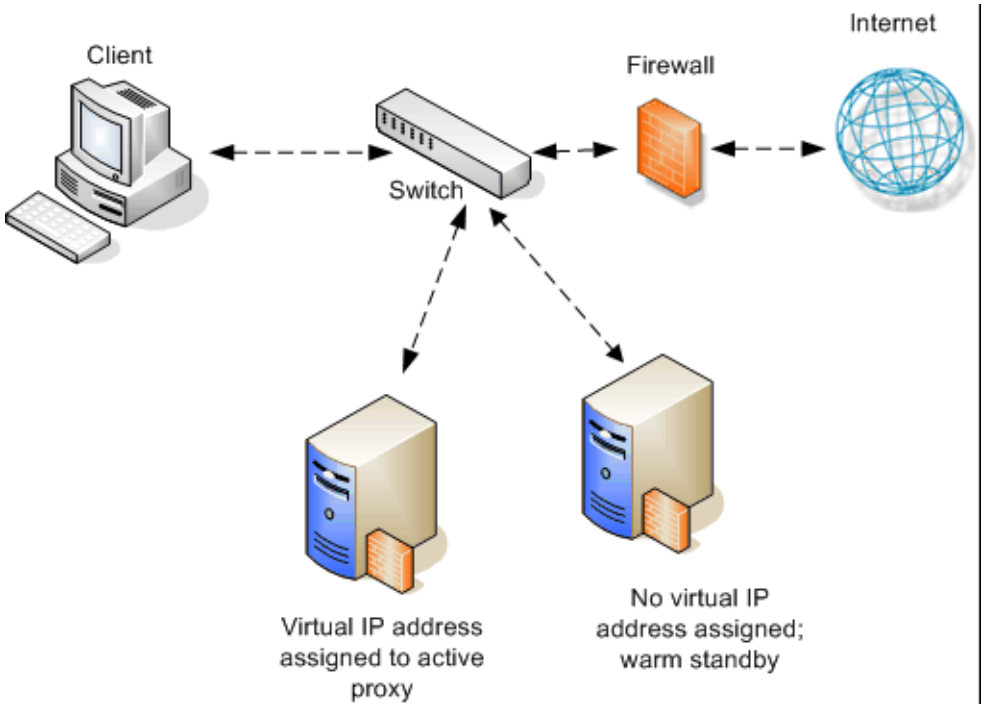
As previously mentioned for the explicit proxy deployment, clients are specifically configured to send requests directly to a proxy. The configuration can be accomplished manually, or via a PAC file or a WPAD server.

An explicit proxy deployment for high availability can benefit from the use of *virtual IP failover*. IP addresses may be assigned dynamically in a proxy cluster, so that one proxy can assume traffic-handling capabilities when another proxy fails. Websense Content Gateway maintains a pool of virtual IP addresses that it distributes across the nodes of a cluster. If Content Gateway detects a hard node failure (such as a power supply or CPU failure), it reassigns IP addresses of the failed node to the operational nodes.

### Active/Standby

In the simple case of an active/standby configuration with 2 proxies, a single virtual IP address is assigned to the virtual IP address “pool.” The virtual IP address is assigned to one proxy, which handles the network traffic that is explicitly routed to it. A second proxy, the standby, assumes the virtual IP address and handles network traffic only if the first proxy fails.

This deployment assumes the proxy machines are clustered in the same subnet, and management clustering is configured (that is, both proxies have the same configuration). Below is an example.



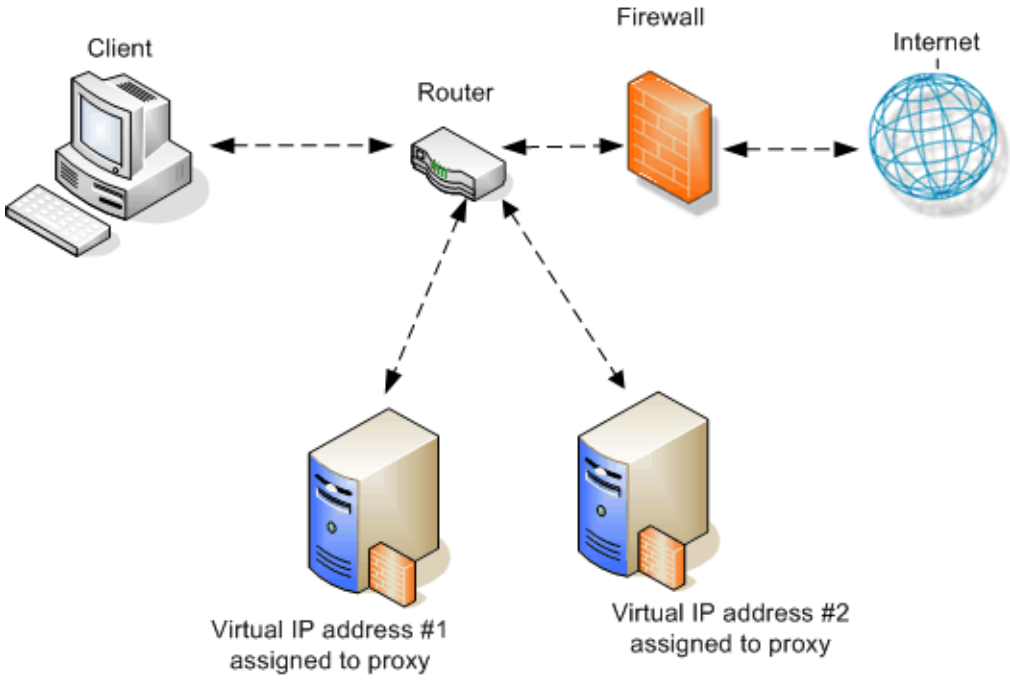

### Active/Active

In an active/active configuration with 2 proxies, more than one virtual IP address is assigned to the virtual IP address pool. At any point in time, one proxy handles the network traffic that is explicitly directed to it. This deployment is scalable for larger numbers of proxies.

Clients requesting the IP address of a proxy can be crudely distributed using round robin DNS. Round robin DNS is not a true load balancing solution, because there is no way to detect load and redistribute it to a less utilized proxy. Management clustering should be configured.

An increase in the number of proxy machines makes the use of a PAC file or WPAD for specifying client configuration instructions convenient. A PAC file may be modified to adjust for proxy overloads, in a form of load balancing, and to specify Web site requests that can bypass the proxy.

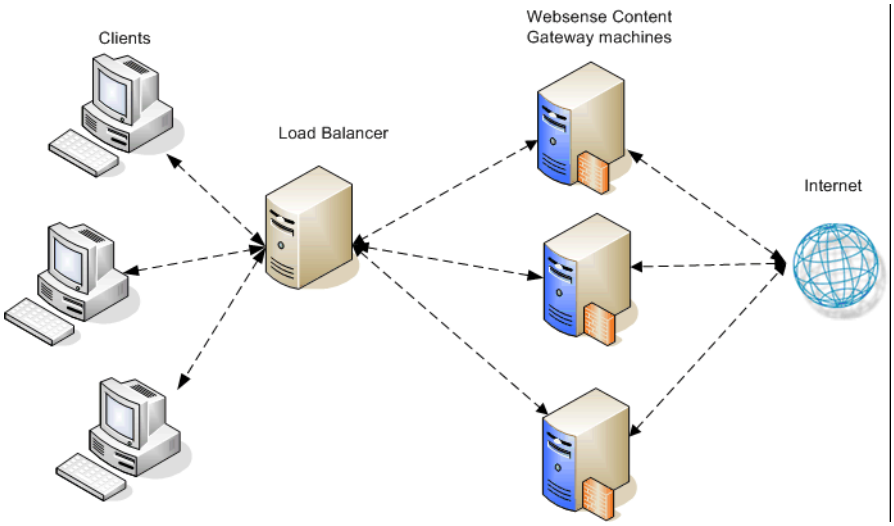
As with the active/standby configuration, an available proxy can assume a failed proxy's load. Below is an example.




### With load balancing

A load balancer is a network device that not only distributes specific client traffic to specific servers, but also periodically checks the status of a proxy to ensure it is operating properly and not overloaded. This monitoring activity is different from simple load distribution, which routes traffic but does not account for the actual traffic load on the proxy.

A load balancer can detect a proxy failure and automatically re-route that proxy's traffic to another, available proxy. The load balancer also handles virtual IP address assignments. Below is an example.



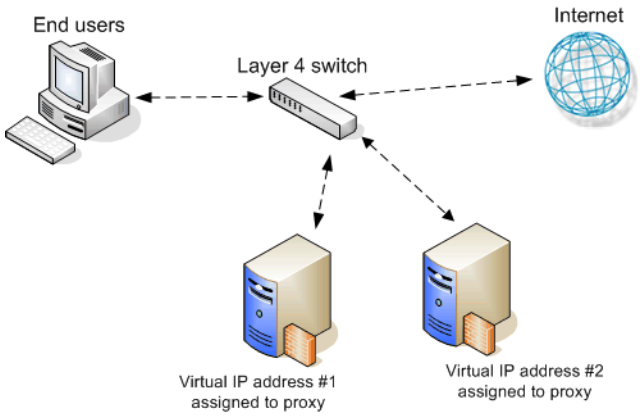

## Using transparent proxy

In a transparent proxy deployment for high availability, traffic forwarding may be accomplished using a Layer 4 switch or a WCCP v2-enabled router. Routers or switches can redirect traffic to the proxy, detect a failed proxy machine and redirect its traffic to other proxies, and perform load balancing.

### Using a Layer 4 switch

In one simple form of transparent proxy, a hard-coded rule is used to write a proxy's Media Access Control (MAC) address as the destination address in IP packets in order to forward traffic to that proxy. Traffic that does not include the specified proxy address for forwarding is passed directly to its destination. See below for an example.

As described for the explicit proxy, virtual IP addresses can be used in this scenario to enhance availability in case a proxy machine fails.



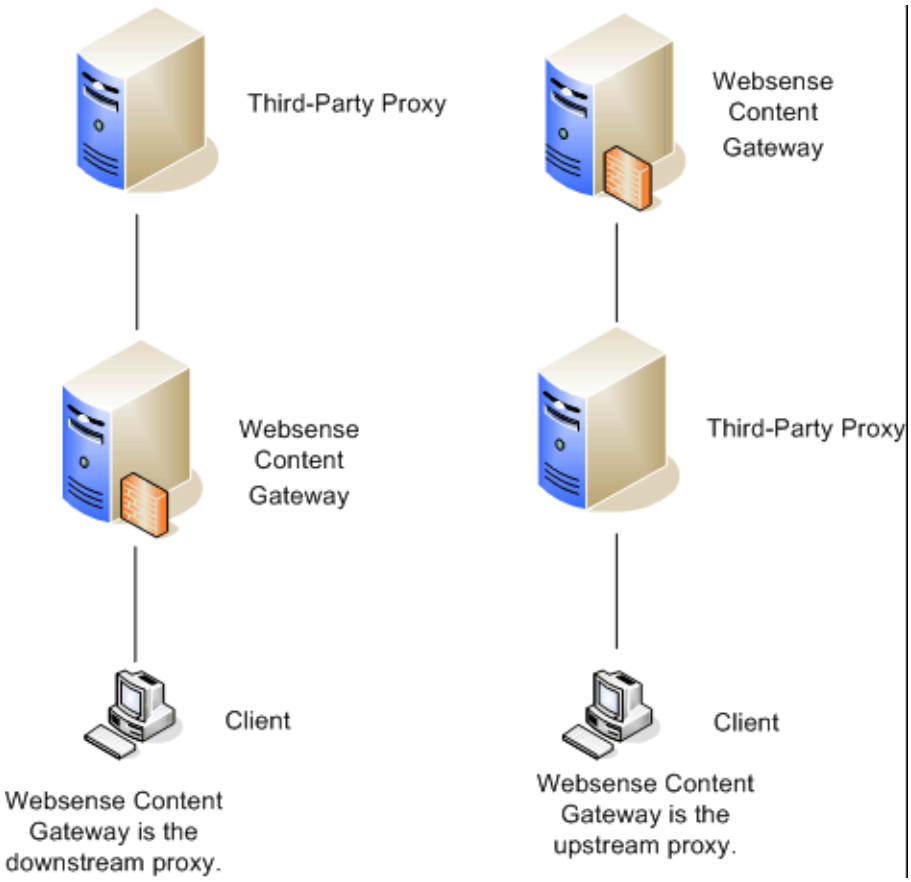
### Using a WCCPv2-enabled router

WCCP is a service that is advertised to a properly configured router, allowing that router to automatically direct network traffic to a specific proxy. In this scenario, WCCP distributes client requests based on the proxy server's IP address, routing traffic to the proxy most likely to contain the requested information.

## In a proxy chain

Websense Content Gateway can be deployed in a network that contains multiple proxy machines, including one or more third-party proxies. A *proxy chain* deployment can involve different scenarios, depending on where Websense Content Gateway is located in relation to the client. The proxy that is closest to the client is called the *downstream* proxy. Other proxies are *upstream*.

Below is a simple example of proxy chaining. On the left, Websense Content Gateway is the downstream proxy. On the right, Websense Content Gateway is upstream.




See *Chaining Content Gateway with other Proxies*, page 401 for specific instructions on using Blue Coat® ProxySG® or Microsoft ISA server as the downstream proxy.

## Websense Content Gateway is downstream

A simple deployment has Websense Content Gateway as the downstream proxy, closest to the client. In this scenario, Websense Content Gateway security features are well positioned for maximum protection and network performance.

In this scenario, use of Websense Content Gateway authentication to validate client credentials is preferred. You must disable authentication on the third-party proxy.

However, if the upstream third-party proxy requires authentication, you must disable authentication on Websense Content Gateway and enable the pass-through authentication feature via an entry in the **records.config** file (in the /WCG/config/ directory by default). An example **records.config** entry is as follows:

```
CONFIG proxy.config.http.forward.proxy_auth_to_parent INT 1
```

You can then use a transparent identification agent (for example, Logon Agent) to facilitate client identification. Websense Content Gateway can additionally send the client IP address to the upstream third-party proxy using the X-Forwarded-For HTTP header via an entry in **records.config**. To enable this function, the following entry would be made:

```
CONFIG proxy.config.http.insert_squid_x_forwarded_for INT 1
```

The X-Forwarded-For HTTP header is the *de facto* standard for identifying the originating IP address of a client connecting through an HTTP proxy. Some proxies do not utilize the X-Forwarded-For header.

For information about installing and deploying transparent identification agents, see *Deploying transparent identification agents*, page 91 and *Installing Web Security components*, page 668.

## Websense Content Gateway is upstream

When Websense Content Gateway is the upstream proxy, the downstream third-party proxy can perform authentication and send client IP and username information in the HTTP request headers. Websense Content Gateway authentication must be disabled.

In this scenario, caching must be disabled on the third-party proxy. Allowing the third-party proxy to cache Web content effectively bypasses Websense Content Gateway's filtering and inspection capabilities for any Web site that was successfully accessed previously from the third-party proxy.

For an upstream Websense Content Gateway to identify users:

- Enable authentication on the third-party proxy.
- Designate Websense Content Gateway as the parent proxy in the third-party proxy's configuration.
- Set the **Read authentication from child proxy** option in the Websense Content Gateway Configure pane (**Configure** > **My Proxy** > **Basic** > **Authentication**). This option allows Websense Content Gateway to read the X-Forwarded-For and X-Authenticated-User HTTP headers. The downstream third-party proxy passes

the client IP address via the X-Forwarded-For header and the user domain and username in the X-Authenticated-User header.

If the third-party proxy can send the X-Forwarded-For header but not the X-Authenticated-User header, the following step is also required:

- Deploy a transparent identification agent to facilitate client identification by Websense Content Gateway. For information*Deploying transparent identification agents*, page 91 and *Installing Web Security components*, page 668.

Websense Content Gateway can be configured to read authentication from the following proxies in the downstream position:

| | |
|---|---|
| Blue Coat ProxySG | 210 and later |
| Microsoft Internet Security and Acceleration (ISA) Server | 2004 and later |

For detailed configuration instructions for Blue Coat ProxySG and Microsoft ISA server, see *Chaining Content Gateway with other Proxies*, page 401.

## Proxy cache hierarchy

Another form of proxy chain is a flexible proxy cache hierarchy, in which Internet requests not fulfilled in one proxy can be routed to other regional proxies, taking advantage of their contents and proximity. For example, a cache hierarchy can be created as a small set of caches for a company department or a group of company workers in a specific geographic area.

In a hierarchy of proxy servers, Websense Content Gateway can act either as a parent or child cache, either to other Websense Content Gateway systems or to other caching products. Having multiple parent caches in a cache hierarchy is an example of *parent failover*, in which a parent cache can take over if another parent has stopped communicating.

As mentioned earlier, the increasing prevalence of dynamic, user-generated Web content reduces the need for Content Gateway caching capabilities.

See Content Gateway Manager online Help (*Hierarchical Caching*) for more information on this topic.

## SSL chaining

Routing SSL traffic in a proxy chain involves the same parent proxy configuration settings used with other proxy-chained traffic. You identify the ports on which HTTPS requests should be decrypted and policy applied when SSL is enabled in the**Protocols > HTTP > HTTPS Ports** option in the Configure tab. Parent proxy rules established in **parent.config** for HTTPS traffic (destination port 443) determine the next proxy in the chain for that traffic.

Enable the Configure tab **Content Routing > Hierarchies > HTTPS Requests Bypass Parent** option to disable SSL traffic chaining when all other traffic is chained.

If you want to exclude SLL traffic from the parent proxy and tunnel the traffic directly to the origin server, enable the **Tunnel Requests Bypass Parent** option in the Configure tab **Content Routing > Hierarchies**. This option can be used for any tunneled traffic.

# 28 Chaining Content Gateway with other Proxies

## Applies to

- Web Security Gateway v7.6.x
- Web Security Gateway Anywhere v7.6.x

## In this topic



## Blue Coat ProxySG

You can configure the Blue Coat proxy to send X-Forwarded-For and X-Authenticated-User headers for Websense Content Gateway to read either by manually editing a policy text file or defining the policy in a Blue Coat graphical interface called Visual Policy Manager.

Note that for Blue Coat to service HTTPS requests properly with the following setup, you must have a Blue Coat SSL license and hardware card.

### Editing the local policy file

In the Blue Coat Management Console Configuration tab, click **Policy** in the left column and select **Policy Files**. Enter the following code in the current policy text file, using an Install Policy option:

```
<Proxy>
action.Add[header name for authenticated user](yes)

define action dd[header name for authenticated user]
```

```
set(request.x_header.X-Authenticated-User, "WinNT://
$(user.domain)/$(user.name)")
end action Add[header name for authenticated user]

action.Add[header name for client IP](yes)

define action dd[header name for client IP]
set(request.x_header.X-Forwarded-For,$(x-client-address))
end action Add[header name for client IP]
```

## Using the Blue Coat graphical Visual Policy Manager

Before you configure the Blue Coat header policy, ensure that NTLM authentication is specified in the Blue Coat Visual Policy Manager (**Authentication > Windows SSO**). Set Websense Content Gateway as the forwarding host (in the Blue Coat Management Console Configuration tab, **Forwarding > Forwarding Hosts**).

In the Blue Coat Management Console Configuration tab, click **Policy** and select **Visual Policy Manager**. Click **Launch** and configure the header policy as follows:

1. In the Policy menu, select **Add Web Access Layer** and enter an appropriate policy name in the Add New Layer dialog box.
2. Select the **Web Access Layer** tab that is created.
3. The Source, Destination, Service, and Time column entries should be **Any** (the default).
4. Right-click the area in the Action column, and select **Set**.
5. Click **New** in the Set Action Object dialog box and select **Control Request Header** from the menu.
6. In the Add Control Request Header Object dialog box, enter a name for the client IP Action object in the Name entry field.
7. Enter **X-Forwarded-For** in the Header Name entry field.
8. Select the **Set value** radio button and enter the following value:

   ```
   $(x-client-address)
   ```
9. Click **OK**.
10. Click **New** and select **Control Request Header** again.
11. In the Add Control Request Header Object dialog box, enter a name for the authenticated user information Action object in the Name entry field.
12. Enter **X-Authenticated-User** in the Header Name entry field.
13. Select the **Set value** radio button and enter the following value:

    ```
    WinNT://$(user.domain)/$(user.name)
    ```
14. Click **OK**.
15. Click **New** and select **Combined Action Object** from the menu.

16. In the Add Combined Action Object dialog box, enter a name for a proxy chain header in the Name entry field.
17. In the left pane, select the previously created control request headers and click **Add**.
18. Select the combined action item in the Set Action Object dialog box and click **OK**.
19. Click **Install Policy** in the Blue Coat Visual Policy Manager.

## Microsoft Internet Security and Acceleration (ISA) server and Forefront Threat Management Gateway (TMG)

Microsoft ISA server or Forefront TMG can be used as a downstream proxy from Websense Content Gateway via a plug-in from Websense, Inc. This plug-in allows Websense Content Gateway to read the X-Forwarded-For and X-Authenticated-User headers sent by the downstream ISA server or Forefront TMG.

Two versions of the plug-in are available, packaged in the following zip files:

- **Websense-AuthForward.ISAPI32.zip** for 32-bit ISA servers
- **Websense-AuthForwardTMG_Plugin-64.zip** for 64-bit Forefront TMG

The zip files are available on the MyWebsense Downloads page.

Install a plug-in as follows:

1. Unzip the package and copy the appropriate **Websense-AuthForward.dll** file (for 32-bit or 64-bit) to the Microsoft ISA or Forefront TMG installation directory. (For example, for ISA the default directory is **C:\Program Files\Microsoft ISA Server**)

   For the ISA version, in addition to **Websense-AuthForward.dll**, install the following files in the ISA installation directory :

   **Microsoft.VC90.CRT.manifest**
   **msvcm90.dll**
   **msvcp90.dll**
   **msvcr90.dll**
2. Open a Windows command prompt and change directory to the Microsoft ISA or Forefront TMG installation directory.
3. From the command prompt, type

   ```
   regsvr32 Websense-AuthForward.dll
      (to register the 32-bit plug-in)

   regsvr32 Websense-AuthForward.dll
      (to register the 64-bit plug-in)
   ```

4. Verify the plug-in was registered in the ISA or Forefront TMG management user interface (For example, **Start > Programs > Microsoft ISA Server > ISA Server Management**). In the Configuration (for 32-bit) or System (for 64-bit) section, select **Add-ins**, then click the Web-filter tab. The **WsAuthForward** plug-in should be listed.

To uninstall the plug-in, run the following command in a Windows command prompt from the ISA or Forefront TMG installation directory.

```
regsvr32 /u Websense-AuthForward.dll
   (to unregister the 32-bit plug-in)

regsvr32 /u Websense-AuthForward.dll
   (to unregister the 64-bit plug-in)
```

# 29 Web Security Gateway (appliance-based)

## Applies to

- Web Security Gateway v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## In this topic

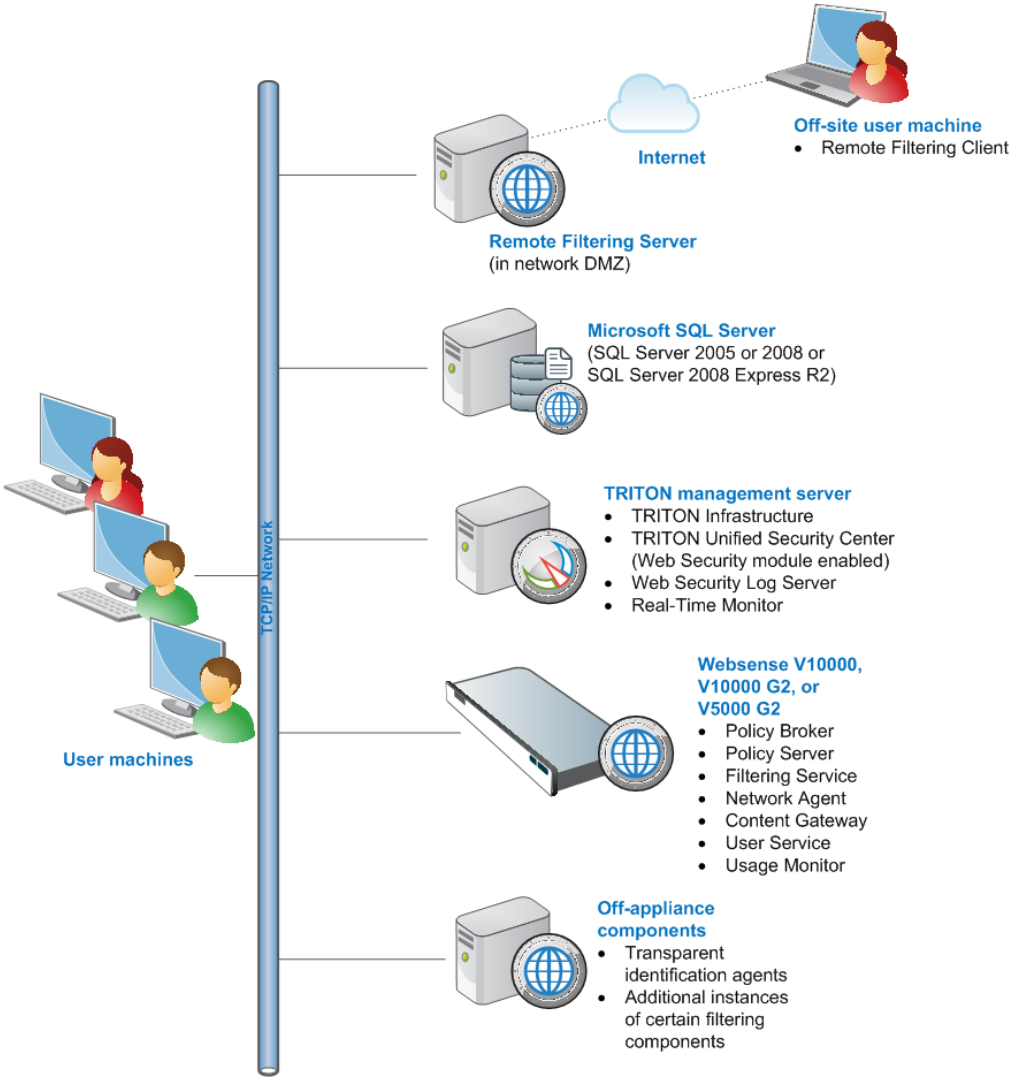


## Overview

This section contains information and instructions for a Websense-appliance-based deployment of Websense Web Security Gateway. In this deployment scenario, a Websense V10000, V10000 G2, or V5000 G2 appliance provides the majority of Web Security Gateway functions. For information about a software-based deployment of Web Security Gateway, see *Web Security Gateway (software-based)*, page 161.

The following illustration is a high-level diagram of a basic single-appliance-based deployment of Web Security Gateway. Note that this illustration is intended to show

the general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).




The Websense appliance provides the majority of Web Security Gateway functions.

Microsoft SQL Server is used to store Websense data (including log and reporting data). SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using the Websense installer) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

*TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your entire Websense deployment. It includes TRITON Infrastructure and any or all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security). Additional components may also be installed on this machine, e.g., Web Security Log Server and Real-Time Monitor (note that these components may be

installed on another machine; they are not required to be located on the TRITON management server).

Transparent identification agents (*DC Agent*, *Logon Agent*, *eDirectory Agent*, and *RADIUS Agent*) must be installed on a separate machine from the appliance.

Websense *Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users that are outside the corporate network (e.g., traveling personnel or telecommuters).

## Deployment


- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Web Security Distributed Enterprise Deployments*, page 147


## Installation

Complete the following procedures in the order in which they are listed.

1. *Obtaining SQL Server*, page 67
2. *Setting up the appliance*, page 408
3. *Installing off-appliance or optional components*, page 417
4. *Creating a TRITON Management Server*, page 645

   The above link goes to general instructions for creating a TRITON management server. As you follow them:

   - Install only the TRITON - Web Security module of the TRITON Unified Security Center. When you reach the **Installation Type** screen of the Websense installer, select **Web Security** (under TRITON Unified Security Center).. Note that you can install any of the other modules, but only the TRITON - Web Security module is necessary for a Web Security Gateway deployment.

     **Important**

     If you enabled TRITON Unified Security Center on the appliance itself (when setting up the appliance, Step 2), do not create a TRITON management server.

# Initial configuration



# Setting up the appliance

## Applies to

- Web Security Gateway v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## In this topic

## Overview

The Quick Start poster, included in the appliance shipping box, shows you all items included in each Websense appliance shipping box. The 2-page Quick Start explains how to set up the hardware and shows how to connect the cables to the appliance and to your network.

Network interface C and the proxy interface (typically P1) must be able to access a DNS server. Both interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C and P1 are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure that this address is permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the C and P1 interfaces can access.

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance. See the next section, for instructions.

## Perform initial command-line configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for the network interface labeled C and a few other general items. You can run the script again if you want to examine your settings or change settings. You can also change settings through the Appliance Manager (browser-based management application) after firstboot has been executed.

Gather the following information before running firstboot. Some of this information may have been written down on the Quick Start during hardware setup.

| | |
|---|---|
| Hostname | |
| IP address for network interface C | |
| Subnet mask for network interface C | |

| | |
|---|---|
| Default gateway for network interface C (IP address) *Optional*<br><br>NOTE: If you do not provide access to the Internet for interface C, configure:<br>• P1 or P2 to download Master URL database updates from Websense<br>Configuring these interfaces to access the Internet for database downloads is done through the Appliance Manager and through the TRITON Unified Security Center. See the Appliance Manager Help for information about configuring the interfaces. See the TRTION - Web Security Help for information about configuring database downloads. | |
| Primary DNS server for network interface C (IP address) | |
| Secondary DNS server for network interface C (IP address) *Optional* | |
| Tertiary DNS server for network interface C (IP address) *Optional* | |
| Unified password (8 to 15 characters, at least 1 letter and 1 number)<br>This password is for the following:<br>• Appliance Manager<br>• TRITON - Web Security<br>• Content Gateway Manager | |

When you have gathered the necessary information, run the initial command line configuration, as follows.

1. Access the appliance through a USB keyboard and monitor or a serial port connection.

   **Note**

   To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

   - 9600 bits per second
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```

4. At the first prompt, select **Web Security only** mode:

   On a V10000, you are not asked to choose a security mode. The V10000 can run only in *Web Security only* mode.

5. Follow the on-screen instructions to provide the information collected above.

After the activation script has been completed successfully, use the **Logon Portal** to access the Appliance Manager. To reach the**Logon Portal**, open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

## Configure the appliance

The Appliance Manager is the Web-based configuration interface for the appliance. Through it you can view system status, configure network and communication settings, and perform general appliance administration tasks.

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces N and P1 (and optionally P2), which are used for communication by Network Agent and Websense Content Gateway. Appliance models V10000 and V10000 G2 also offer expansion interfaces (E1 and E2) that can be bonded with P1 and P2, respectively, either for load balancing or standby. Note that on a V5000 G2, there are no E1 and E2 interfaces.

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway. For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCPv2 router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see **Configure** > **Networking** > **WCCP**).

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

| | |
|---|---|
| Primary NTP server<br>*Optional*<br>Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C. | Domain: |
| Secondary NTP server<br>*Optional* | Domain: |
| Tertiary NTP server<br>*Optional* | Domain: |
| IP address for network interface P1 | IP address: |

| | |
|---|---|
| Subnet mask for network interface P1 | Subnet mask: |
| Default gateway for network interface P1 and P2 (if used)<br>If both P1 and P2 are used, the default gateway is automatically assigned to whichever interface is in the same subnet with it. If both P1 and P2 are in the same subnet, the default gateway is automatically assigned to P2 (which is bound to eth1). | IP address: |
| Primary DNS server for network interface P1 and P2 (if used) | IP address: |
| Secondary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| IP address for network interface P2<br>*Required only if P2 is enabled* | IP address: |
| Subnet mask for network interface P2<br>*Required only if P2 is enabled* | Subnet mask: |
| Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic (interface C or interface N) | Choose one: C or N |
| If interface N transports blocking information, N must be connected to a bidirectional span port | Verify interface N setup |
| IP address for network interface N | IP address: |
| Subnet mask for network interface N | Subnet mask: |
| Default gateway for network interface N<br>*Required only if network interface N carries blocking information* | IP address: |
| Primary DNS server for network interface N | IP address: |
| Secondary DNS server for network interface N<br>*Optional* | IP address: |
| Tertiary DNS server for network interface N<br>*Optional* | IP address: |
| Bond expansion interface E1 to P1? Yes or No<br>*Optional; V10000 or V10000 G2 only* | If Yes, choose one: Active/standby or Load balancing |
| Bond expansion interface E2 to P2? Yes or No<br>*Optional; V10000 or V10000 G2 only* | If Yes, choose one: Active/standby or Load balancing |

| | |
|---|---|
| Full policy source IP address | This appliance provides (choose one):<br>• Full policy source<br>• User directory and filtering (you must specify the IP address of a machine running Policy Broker, which can be a *full policy source* appliance)<br>• Filtering only (you must specify IP address of a machine running Policy Server, which can be a *full policy source* or *user directory and filtering* appliance). |
| TRITON Unified Security Center location (user interface for managing Web Security Gateway)<br>TRITON Unified Security Center can run on this appliance or on a separate Windows server. By default it is enabled to run on the appliance. During the setup procedure below you will decide where it should run.<br>Note: Organizations with high traffic volume or large reporting needs are encouraged to install and run TRITON Unified Security Center on a separate Windows server, to optimize performance. | • Choose:<br>Runs on this appliance or<br>• Runs on separate server |

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to enable default proxy caching and filtering. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

   (See *Perform initial command-line configuration*.)
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration > System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.

c. Click **Save** in the Time and Date area.

5. In the left navigation pane, click **Configuration > Network Interfaces**.
6. Under **Websense Content Gateway Interfaces**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

   To configure the P interfaces:

   a. Select whether **P1 only** or both **P1 and P2** are used.

      If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

      If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

   b. Click **Save** in the **Websense Content Gateway Interfaces** area when you are done.

   **Important**

   When you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.

   For example, suppose you are using transparent proxy, and the P1 interface is connected to the WCCPv2 router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager: **Configure > Networking > WCCP**).

   When only P1 is used, it handles both inbound and outbound traffic for the proxy module (i.e., Content Gateway).

   Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2 on the **Configuration > Routing** page. For example, you might set outbound traffic to go through P2.

   Additionally, you can use P1 as a communication channel for multiple Content Gateway servers in a cluster. In this scenario, P1 cannot be used for outbound traffic. For additional information on clusters, see the Content Gateway Manager Help.

7. Under **Network Agent Interface (N)**, configure the N interface.

   The N interface is used by the Network Agent module. It must be connected to a span (or mirror) port on a switch allowing it to monitor Internet requests going through the switch. (Note: be sure to configure the switch so the span port is monitoring all the ports carrying the traffic of interest; see your switch manufacturer's documentation for configuration instructions). For non-HTTP/

HTTPS protocols, the N interface can also be used to send block information to enforce policy.

> **Note**
> The appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

To configure the N interface:

a. Under **Send blocking information for non-HTTP/HTTPS traffic via**, select whether non-HTTP/HTTPS blocking information is sent via the C or N interface.

b. Enter IP address, subnet mask, default gateway (only if you select interface N for sending blocking information), and DNS IP addresses for the N interface.

c. Click **Save** in the **Network Agent Interface (N)** area.

8. Under **Expansion Interfaces (E1 and E2)**, choose whether to bond to P1 and P2 interfaces. (This applies to the V10000 and V10000 G2 only; E1 and E2 interfaces are not present on the V5000 G2.)

   Interfaces E1 and E2 can be cabled to your network and then bonded through software configuration to P1 and P2 (the Websense Content Gateway interfaces). If you choose to bond the interfaces, E1 must be bonded to P1 and E2 to P2. No other pairing is possible.

   You can choose to bond or not bond each Websense Content Gateway interface (P1 and P2) independently. You do not have to bond at all. You do not have to bond both. Also, you can choose different bonding modes for P1 and P2 (e.g., P1/E1 could be **Active/Standby** while P2/E2 could be **Load balancing**).

   Make sure all interfaces are cabled properly before configuring bonding.

   To bond E1 to P1:

   a. Under **E1**, select the check box for **Bond to P1 interface**.

   b. Under E1/P1 bonding mode, select:

      - **Active/Standby**: Select this for failover. P1 is active, and E1 is in standby mode. Only if the primary interface fails would its bonded interface (E1) become active.
      - **Load balancing**: Select this for load balancing. If your switch or router supports load balancing, then traffic to and from the primary interface is balanced between the primary interface (P1) and its bonded interface (E1).

   c. Click **Save** in the **Expansion Interfaces (E1 and E2)** area.

   To bond E2 to P2:

   Follow the instruction above for bonding E1 to P1, substituting E2 in place of E1 and P2 in place of P1. Make sure P2 is enabled. Otherwise the **E2** options will be inactive. (See Step 6 for instructions on activating P2.)

9. Configure routes if necessary:

   a. In the left navigation pane, click **Configuration > Routing**.

   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

See the Appliance Manager Help for more information about static and module routes.

10. Select the policy mode of this appliance:

    a. In the left navigation pane, click **Configuration > Web Security Components**.

    b. Specify the role of this appliance with respect to Websense Web Security policy information.

    - Choose **Full policy source** if Websense Policy Broker and Policy Database for your deployment will run on the appliance being configured. (Only one appliance in the network runs these two components, as well as the other filtering components.) Policy Server must also be run on the*full policy source* appliance; Policy Server can run in multiple locations.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

    - Choose **User directory and filtering** if the appliance currently being configured is *not* the location of the policy information, but will run Policy Server and User Service. Then, enter the **IP address** of the machine running Policy Broker (i.e., the policy source). The policy source can be another appliance that is running in *full policy source* mode. In this case, enter the IP address of that appliance's C network interface.
    - Choose **Filtering only** if the appliance being configured will not run any policy components. (There are some disadvantages to this reduced role, as explained in the Appliance Manager Help.) Then, enter the**IP address** of the machine serving as policy source, which in this case is a machine running Policy Server. The policy source can also be another appliance running in either*full policy source* or *user directory and filtering* mode. In this case, enter the IP address of that appliance's C network interface.

    c. Click **Save**.

11. Enable/disable TRITON Unified Security Center on this appliance
    a. If you have not done so already, in the left navigation pane, click **Configuration** > **Web Security Components**.
    b. Under **TRITON - Web Security**, select:
       - **Off**: the TRITON Unified Security Center runs on a separate machine from the appliance.
       - **On**: the TRITON Unified Security Center runs on this appliance.

       TRITON - Web Security is the Web Security module of the TRITON Unified Security Center. For a Websense Web Security Gateway deployment, you can choose to run the TRITON Unified Security Center on or off the appliance.

       For other deployments requiring more than the Web Security module of the TRITON Unified Security Center (i.e., Data Security or Email Security modules), the TRITON Unified Security Center must be installed on a separate machine from the appliance. In this case, be sure to disable it here.

       **Note**
       Organizations with high traffic volume or large reporting needs are encouraged to install and run the TRITON Unified Security Center on a separate machine, to optimize performance.

12. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

# Installing off-appliance or optional components

## Applies to

- Web Security Gateway v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Installing off-appliance or optional components

The following Websense components must run off-appliance (i.e., on a separate machine):

- *Web Security Log Server* (if creating a TRITON management server, Web Security Log Server is typically installed on that machine).
- Transparent identification agents:
  - *DC Agent*
  - *Logon Agent*
  - *eDirectory Agent*

    - *RADIUS Agent*
- *Remote Filtering Server*

Also, additional instances of Web security filtering components may be installed on machines in your network to provide additional functions or distribute processing load. For example, you can install additonal Websense *Network Agent* instances on a machines in your network.

To install components like these, perform a custom installation on the machine on which you want to install the the component. See *Installing Web Security components* for instructions.

# 30 Web Security Gateway Anywhere (appliance-based)

## Applies to

- Web Security Gateway Anywhere v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## In this topic

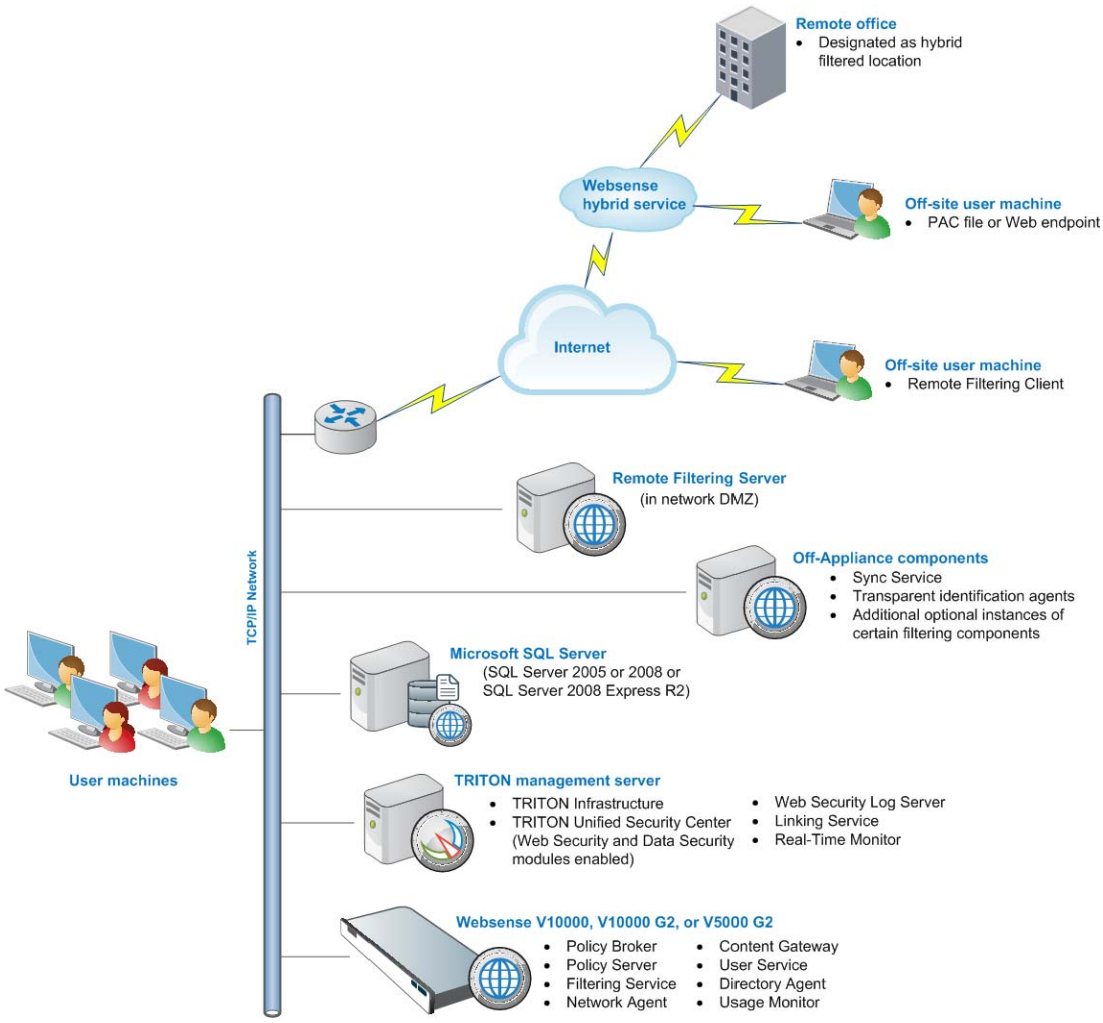


## Overview

This section contains information and instructions for a Websense-appliance-based deployment of Websense Web Security Gateway Anywhere. In this deployment scenario, a Websense V10000, V10000 G2, or V5000 G2 appliance provides the majority of Web Security Gateway Anywhere functions. For information about a software-based deployment of Web Security Gateway Anywhere, see *Web Security Gateway Anywhere (software-based)*.

The following illustration is a high-level diagram of a basic single-appliance-based deployment of Web Security Gateway Anywhere. Note that this illustration is

intended to show the general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).




The Websense appliance provides the majority of Web Security Gateway functions.

Microsoft SQL Server is used to store Websense data (including log and reporting data). SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using the Websense installer) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

*TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and any or all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security). In Web Security Gateway Anywhere deployments, both the Web Security and Data Security modules of the TRITON Unified Security Center are enabled. *Linking Service* is typically installed on this machine. Additional components may

also be installed on this machine. For example, *Web Security Log Server* and *Real-Time Monitor* (note that these components may be installed on another machine; they are not required to be located on the TRITON management server).

*Sync Service* and Transparent identification agents (*DC Agent*, *Logon Agent*, *eDirectory Agent*, and *RADIUS Agent*) must be installed on a separate machine from the appliance.

Small remote offices can be filtered through the Websense hybrid service. This is accomplished by designating a remote office as a hybrid filtered location. See *Initial Configuration* for more information.

Off-site users (e.g., telecommuters or traveling personnel) can be filtered using the Websense hybrid service or Websense Remote Filtering. To use the hybrid service, a PAC file or the Websense Web Endpoint is installed on the user's machine. This directs Web browsing to be filtered through the hybrid service according to policies in place. See Deploying Websense Endpoints for more information.

Websense Remote Filtering is accomplished using a Remote Filtering Server and Remote Filtering Client. Websense*Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users that are outside the corporate network. A combination of hybrid service and Remote Filtering can be used for off-site users—i.e., some filtered through the hybrid service, others filtered by Remote Filtering.

## Deployment

- *System Requirements*, page 41
- *TRITON management server as policy source for filtering-only appliance*, page 433
- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Web Security Distributed Enterprise Deployments*, page 147

## Installation

Complete the following procedures.

1. *Obtaining SQL Server*

2. *Setting up the appliance*
3. *Installing off-appliance or optional components*
4. *Creating a TRITON Management Server*

   The above link goes to general instructions for creating a TRITON management server. In the case of Web Security Gateway Anywhere, choose to install both the Web Security and Data Security modules of TRITON Unified Security Center: when you reach the **Installation Type** screen of the Websense installer, select both **Web Security** and **Data Security** (under TRITON Unified Security Center).

**Important**

Policy Broker and Policy server must already be running in your deployment prior to creating a TRITON management server.

If, during appliance setup (see Step 2 above), you chose to run the appliance in full policy source mode, then these components are already running.

You can choose to install them at the same time as TRITON Unified Security Center (on the TRITON management server) or install them

# Initial configuration

- *Configuring the Content Gateway policy engine*, page 773
- *Verifying Web and data security linking*, page 774
- *Configure filtering for remote offices and off-site users*, page 774


# Setting up the appliance

## Applies to

- Web Security Gateway Anywhere v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## In this topic



## Overview

**Note**

If you have already completed the appliance set up steps provided in the *Websense V-Series Getting Started* guide, skip to *Installing off-appliance or optional components*, page 432 now.

The Quick Start poster, which comes in the shipping box with your appliance, shows you all items included in each Websense appliance shipping box. The 2-page Quick Start explains how to set up the hardware and shows how to connect the cables to the appliance and to your network.

Network interface C and the proxy interface (typically P1) must be able to access a DNS server. Both interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C and P1 are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure that this address is permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the C and P1 interfaces can access.

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance. See next section , for instructions.

## Perform initial command-line configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for the network interface labeled C and a few other general items. You can run the script again if you want to examine your settings or change settings. You can also change settings through the Appliance Manager (browser-based management application) after firstboot has been executed.

Gather the following information before running firstboot. Some of this information may have been written down on the Quick Start during hardware setup.

| | |
|---|---|
| Hostname | |
| IP address for network interface C | |
| Subnet mask for network interface C | |
| Default gateway for network interface C (IP address) *Optional*<br><br>**Note:** If you do not provide access to the Internet for interface C, configure:<br>• P1 or P2 to download Master URL database updates from Websense (Web Security mode)<br>Configuring these interfaces to access the Internet for database downloads is done through the Appliance Manager and through the TRITON Unified Security Center. See the Appliance Manager Help for information about configuring the interfaces. See the TRTION - Web Security Help for information about configuring database downloads. | |
| Primary DNS server for network interface C (IP address) | |
| Secondary DNS server for network interface C (IP address) *Optional* | |

| | |
|---|---|
| Tertiary DNS server for network interface C (IP address) *Optional* | |
| Unified password (8 to 15 characters, at least 1 letter and 1 number)<br>This password is for the following:<br>• Appliance Manager<br>• TRITON - Web Security<br>• Content Gateway Manager | |

When you have gathered the necessary information, run the initial command line configuration, as follows.

1. Access the appliance through a USB keyboard and monitor or a serial port connection.

   **Note**

   To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

   - 9600 bits per second
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```

4. At the first prompt, select a **Web Security only** mode:

   On a V10000, you are not asked to choose a security mode. The V10000 can run only in *Web Security only* mode.

5. Follow the on-screen instructions to provide the information collected above.

After the activation script has been completed successfully, use the **Logon Portal** to access the Appliance Manager. To reach the**Logon Portal**, open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

# Configure the appliance

The Appliance Manager is the Web-based configuration interface for the appliance. Through it you can view system status, configure network and communication settings, and perform general appliance administration tasks.

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces N and P1 (and optionally P2), which are used for communications by Network Agent and Websense Content Gateway. Appliance models V10000 and V10000 G2 also offer expansion interfaces (E1 and E2) that can be bonded with P1 and P2, respectively, either for load balancing or standby. Note that on a V5000 G2, there are no E1 and E2 interfaces.

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway. For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see **Configure** > **Networking** > **WCCP, General** tab).

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

| | |
|---|---|
| Primary NTP server<br>*Optional*<br>Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C. | Domain: |
| Secondary NTP server<br>*Optional* | Domain: |
| Tertiary NTP server<br>*Optional* | Domain: |
| IP address for network interface P1 | IP address: |
| Subnet mask for network interface P1 | Subnet mask: |
| Default gateway for network interface P1 and P2 (if used)<br>If both P1 and P2 are used, the default gateway is automatically assigned to whichever interface is in the same subnet with it. If both P1 and P2 are in the same subnet, the default gateway is automatically assigned to P2 (which is bound to eth1). | IP address: |
| Primary DNS server for network interface P1 and P2 (if used) | IP address: |

| | |
|---|---|
| Secondary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| IP address for network interface P2<br>*Required only if P2 is enabled* | IP address: |
| Subnet mask for network interface P2<br>*Required only if P2 is enabled* | Subnet mask: |
| Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic. (interface C or interface N) | Choose one: C or N |
| If interface N transports blocking information, N must be connected to a bidirectional span port. | Verify interface N setup. |
| IP address for network interface N | IP address: |
| Subnet mask for network interface N | Subnet mask: |
| Default gateway for network interface N<br>*Required only if network interface N carries blocking information* | IP address: |
| Primary DNS server for network interface N | IP address: |
| Secondary DNS server for network interface N<br>*Optional* | IP address: |
| Tertiary DNS server for network interface N<br>*Optional* | IP address: |
| Bond expansion interface E1 to P1? Yes or No<br>*Optional; V10000 or V10000 G2 only* | If Yes, choose one: Active/standby or Load balancing |
| Bond expansion interface E2 to P2? Yes or No<br>*Optional; V10000 or V10000 G2 only* | If Yes, choose one: Active/standby or Load balancing |

| | |
|---|---|
| Full policy source IP address | This appliance provides (choose one):<br>• Full policy source<br>• User directory and filtering (you must specify the IP address of a machine running Policy Broker, which can be a *full policy source* appliance)<br>• Filtering only (you must specify IP address of a machine running Policy Server, which can be a *full policy source* or *user directory and filtering* appliance). |
| TRITON Unified Security Center location (user interface for managing Web Security Gateway)<br>TRITON Unified Security Center can run on this appliance or on a separate Windows server. By default it is enabled to run on the appliance. During the setup procedure below you will decide where it should run.<br>**Note:** Organizations with high traffic volume or large reporting needs are encouraged to install and run TRITON Unified Security Center on a separate Windows server, to optimize performance. | Choose: runs on this appliance or runs on separate server |

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to enable default proxy caching and filtering. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

   (See *Perform initial command-line configuration*.)
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration** > **System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.

- **Manually set time and date**: select this option to enter a system time and date yourself.

c. Click **Save** in the Time and Date area.

5. In the left navigation pane, click **Configuration > Network Interfaces**.
6. Under **Websense Content Gateway Interfaces**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

   To configure the P interfaces:

   a. Select whether **P1 only** or both **P1 and P2** are used.

      If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

      If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

   b. Click **Save** in the **Websense Content Gateway Interfaces** area when you are done.

   **Important**

   When you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.

   For example, suppose you are using transparent proxy, and the P1 interface is connected to the WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager: **Configure > Networking > WCCP, General** tab).

   When only P1 is used, it handles both inbound and outbound traffic for the proxy module (i.e., Content Gateway).

   Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2 on the **Configuration > Routing** page. For example, you might set outbound traffic to go through P2.

   Additionally, you can use P1 as a communication channel for multiple Content Gateway servers in a cluster. In this scenario, P1 cannot be used for outbound traffic. For additional information on clusters, see the Content Gateway Manager Help.

7. Under **Network Agent Interface (N)**, configure the N interface.

   The N interface is used by the Network Agent module. It must be connected to a span (or mirror) port on a switch allowing it to monitor Internet requests going through the switch. (Note: be sure to configure the switch so the span port is

monitoring all the ports carrying the traffic of interest; see your switch manufacturer's documentation for configuration instructions). For non-HTTP/HTTPS protocols, the N interface can also be used to send block information to enforce policy.

> **Note**
> The appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

To configure the N interface:

a. Under **Send blocking information for non-HTTP/HTTPS traffic via**, select whether non-HTTP/HTTPS blocking information is sent via the C or N interface.

b. Enter IP address, subnet mask, default gateway (only if you select interface N for sending blocking information), and DNS IP addresses for the N interface.

c. Click **Save** in the **Network Agent Interface (N)** area.

8. Under **Expansion Interfaces (E1 and E2)**, choose whether to bond to P1 and P2 interfaces. (This applies to the V10000 and V10000 G2 only; E1 and E2 interfaces are not present on the V5000 G2.)

   Interfaces E1 and E2 can be cabled to your network and then bonded through software configuration to P1 and P2 (the Websense Content Gateway interfaces). If you choose to bond the interfaces, E1 must be bonded to P1 and E2 to P2. No other pairing is possible.

   You can choose to bond or not bond each Websense Content Gateway interface (P1 and P2) independently. You do not have to bond at all. You do not have to bond both. Also, you can choose different bonding modes for P1 and P2 (e.g., P1/E1 could be **Active/Standby** while P2/E2 could be **Load balancing**).

   Make sure all interfaces are cabled properly before configuring bonding.

   To bond E1 to P1:

   a. Under **E1**, select the check box for **Bond to P1 interface**.

   b. Under E1/P1 bonding mode, select:

      - **Active/Standby**: Select this for failover. P1 is active, and E1 is in standby mode. Only if the primary interface fails would its bonded interface (E1) become active.
      - **Load balancing**: Select this for load balancing. If your switch or router supports load balancing, then traffic to and from the primary interface is balanced between the primary interface (P1) and its bonded interface (E1).

   c. Click **Save** in the **Expansion Interfaces (E1 and E2)** area.

   To bond E2 to P2:

   Follow the instruction above for bonding E1 to P1, substituting E2 in place of E1 and P2 in place of P1. Make sure P2 is enabled. Otherwise the **E2** options will be inactive. (See Step 6 for instructions on activating P2.)

9. Configure routes if necessary:

   a. In the left navigation pane, click **Configuration > Routing**.

b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

See the Appliance Manager Help for more information about static and module routes.

10. Select the policy mode of this appliance:

a. In the left navigation pane, click **Configuration** > **Web Security Components**.

b. Specify the role of this appliance with respect to Websense Web Security policy information.

- Choose **Full policy source** if Websense Policy Broker and Policy Database for your deployment will run on the appliance being configured. (Only one appliance in the network runs these two components, as well as the other filtering components.) Policy Server must also be run on the *full policy source* appliance; Policy Server can run in multiple locations.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

- Choose **User directory and filtering** if the appliance currently being configured is *not* the location of the policy information, but will run Policy Server and User Service. Then, enter the **IP address** of the machine running Policy Broker (i.e., the policy source). The policy source can be another appliance that is running in *full policy source* mode. In this case, enter the IP address of that appliance's C network interface.
- Choose **Filtering only** if the appliance being configured will not run any policy components. (There are some disadvantages to this reduced role, as explained in the Appliance Manager help system.) Then, enter the **IP address** of the machine serving as policy source, which in this case is a machine running Policy Server. The policy source can also be another

appliance running in either*full policy source* or *user directory and filtering* mode. In this case, enter the IP address of that appliance's network interface C.

c. Click **Save**.

11. Disable TRITON Unified Security Center on this appliance
    a. If you have not done so already, in the left navigation pane, click **Configuration > Web Security Components**.
    b. Under **TRITON - Web Security**, select **Off**.

       Web Security Gateway Anywhere requires both the Web and Data Security modules of the TRITON Unified Security Center. TRITON Unified Security Center must be installed off the appliance.
12. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

# Installing off-appliance or optional components

## Applies to

- Web Security Gateway Anywhere v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Installing off-appliance or optional components

The following Websense components must run off-appliance (i.e., on a separate machine):

- *Web Security Log Server*
- *Real-Time Monitor*
- *Sync Service*
- Transparent identification agents:
  - *DC Agent*
  - *Logon Agent*
  - *eDirectory Agent*
  - *RADIUS Agent*
- *Remote Filtering Server*

Also, additional instances of Web security filtering components may be installed on machines in your network to provide additional functions or distribute processing load. For example, you can install additonal Websense *Network Agent* instances on a machines in your network.

To install components like these, perform a custom installation on the machine on which you want to install the the component. See *Installing Web Security components* for instructions.

# TRITON management server as policy source for filtering-only appliance

## Applies to

- Web Security Gateway Anywhere v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## TRITON management server as policy source for filtering-only appliance

This section discusses a scenario in which *Policy Broker* and *Policy Server* are installed on the *TRITON management server* and a Websense appliance (running in *filtering only* mode) uses the TRITON management server as its policy source.

It is important to set up the appliance and TRITON management server in the following order.

1. Set up the appliance to run in **full policy source** mode.

   See *Setting up the appliance*, page 423 for instructions.
2. Create a TRITON management server with both the Web and Data Security modules of the TRITON Unified Security Center.

   See *Creating a TRITON Management Server*, page 645 for instructions. **Important**: while following those instructions, during the Web Security module installation, choose to install Policy Broker and Policy Server on the machine along with TRITON - Web Security, but do **not** choose to install *Linking Service*. Note that you can choose to install any of the other optional components as well, just not Linking Service.
3. Configure the appliance to filtering only mode, specifying the TRITON management server as the policy source.

   See the Appliance Manager Help for instructions on changing the policy mode of the appliance.
4. On the TRITON management server, run the Websense installer again and add Linking Service. When asked for the IP address of Filtering Service, specify the C interface of the appliance.

   See *Adding Web Security components*, page 794 for instructions on adding Linking Service.

5. Install off-appliance components as necessary.
   See *Installing off-appliance or optional components*, page 432.

# 31 Data Security

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

This section of the Websense Technical Library contains information and instructions for installing Websense Data Security (Data Security).

Data Security is a comprehensive data loss prevention (DLP) system that discovers, monitors, and protects your critical information holdings, whether that data is stored on your servers, currently in use or located in off-network endpoints. Data Security protects against data loss by quickly analyzing data and enforcing customized policies automatically, whether users are on the network or offline. Administrators manage *who* can send *what* information, *where*, and *how*. Data Security can also work as a part of Websense TRITON Enterprise to protect the whole of your enterprise.

The basic components of Websense Data Security are:

- The Data Security Management Server
- Optional Data Security servers
- The protector
- Agents
- Endpoints

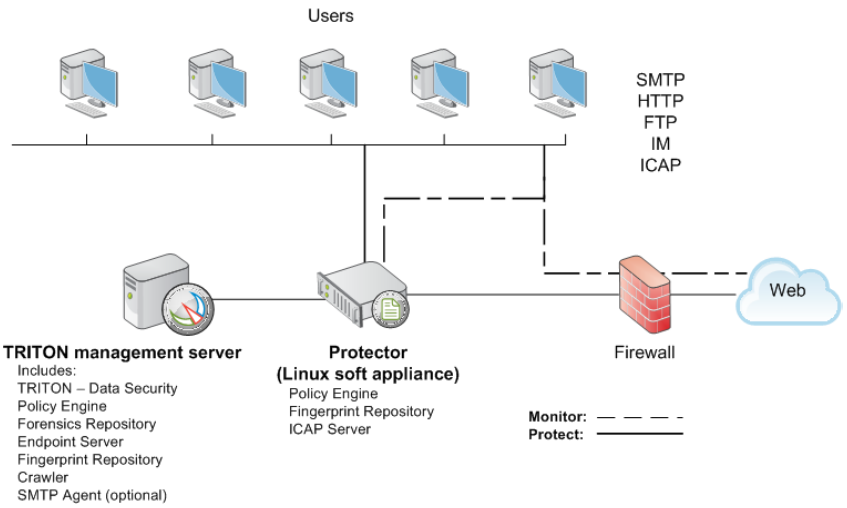
The *Data Security Management Server*, which resides on the TRITON management server, is the core of the system, providing complete data loss prevention analysis to the network. In addition, the Data Security Management Server gathers and stores all management statistics. For load balancing purposes, analysis can be shared among a number of Data Security servers. The *protector* can provide added blocking capabilities to the loss-prevention system.

The protector works in tandem with the Data Security Management Server. The Data Security Management Server performs discovery (performed by Crawler) and provides advanced analysis capabilities. The protector sits on the network, intercepts and analyzes traffic, and can either monitor or block traffic as needed. The protector supports analysis of SMTP, HTTP, FTP, Generic Text and IM traffic (chat and file transfer). The protector is also an integration point for third-party solutions that support ICAP.

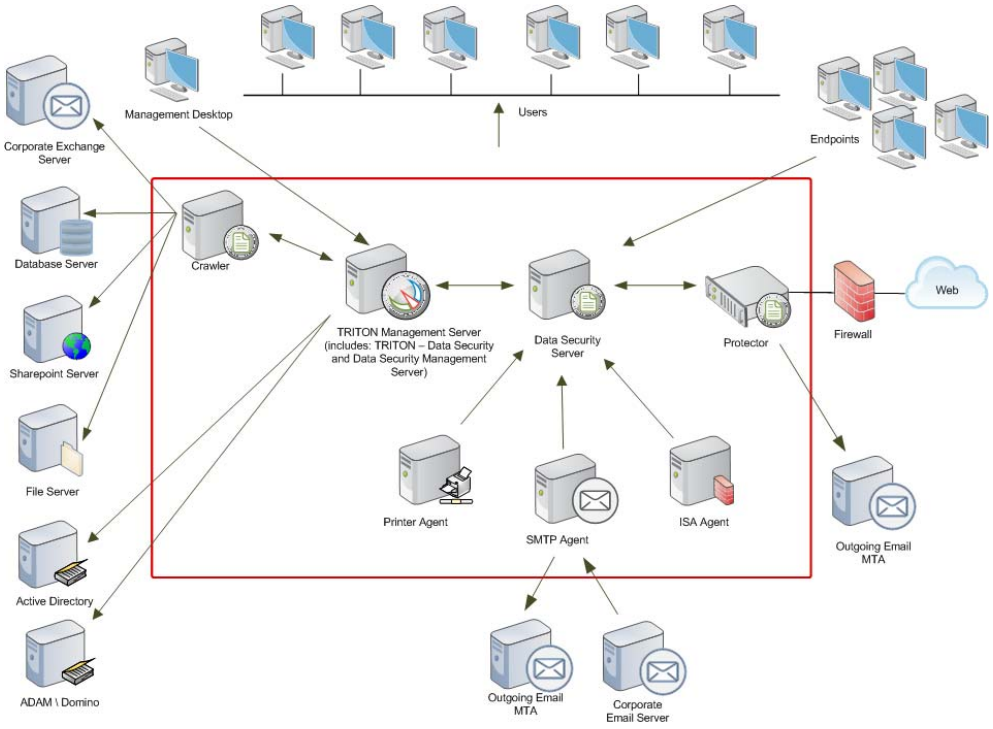
The protector fits into your existing network with minimum configuration and necessitates no network infrastructure changes.

Websense Data Security *agents* are also an integral part of the system. These agents are installed on the relevant servers (the ISA agent on the Microsoft ISA server, printer agent on the print server, etc.) to enable Data Security to access the data necessary to analyze the traffic from these servers. Agents, such as the Data Endpoint, enable administrators to analyze content within a user's working environment (PC, laptop, etc.) and block or monitor policy breaches.

An example basic deployment has just one management server and one protector. The protector includes several agents, including SMTP, HTTP, FTP, IM, and ICAP. The servers are easily configurable to simply monitor or monitor and protect sensitive data. It is ideal for small to medium businesses with a single Internet egress point. The following illustration is a high-level diagram of a basic deployment of Data Security. Such a deployment is ideal for a smaller- to medium-sized organization with a single Internet egress point. Note that this illustration is intended to show the general distribution of components and does not include network details (such as segmenting, internal firewalls, routing, switching, and so forth).



The following illustration is a high-level diagram of a larger deployment of Data Security.




This shows the extended capabilities of Data Security incorporated into a more complex network environment. It shows an extra Data Security server and several additional agents deployed for businesses with larger transaction volumes and numbers of users. Such a deployment is suited for large organizations with multiple Internet egress points distributed over multiple geographical locations. Very large deployments can have multiple Data Security servers and protectors.

# Deployment


- *Planning Data Security Deployment*, page 449
- *Choosing and Deploying Data Security Agents*, page 473
- *Integrating Data Security with Existing Infrastructure*, page 519
- *Scaling Data Security*, page 553
- *Data Security Protector CLI*, page 561

# Installation

Complete the following main steps (the links go to detailed procedures or information for each step).

> **Note**
> The Websense installer is not used to install a Data Security Protector. Instead, a separate installer is used. See *Protector*, page 476.

> **Note**
> The Websense installer is not used to install a Data Security Endpoint. Instead, you must create a specialized installation package and distribute it to endpoint machines using SMS or GPO. See *Printer agent*, page 508

1. *Preparing for Installation*
2. *Obtaining SQL Server*
3. *Creating a TRITON Management Server*

   The above link goes to general instructions for creating a TRITON management server. As you follow those instructions:

   - Install only the TRITON - Data Security module of the TRITON Unified Security Center. When you reach the **Installation Type** screen of the Websense installer, select **Data Security** (under TRITON Unified Security Center). Note that you can install the other modules if you want, but TRITON - Data Security is the only one necessary for a Data Security deployment.
4. *Installing Data Security Components*

# Initial configuration

- *SMTP Agent*, page 775
- *ISA Agent*, page 777
- *Crawler Agent*, page 777
- *General Setup*, page 777

# Installing Data Security on a virtual machine

## Applies to

- Data Security v7.6.x

# Installing Data Security on a virtual machine

Websense Data Security supports installations over Virtual Machines (VM), but Microsoft SQL Server must be present to support the incident and policy database. See *System Requirements*, page 41 for supported versions of SQL Server. If you are performing a clean install of Websense Data Security, SQL Server 2008 R2 Express is included.

If you have a subscription to Websense Web Security Gateway Anywhere, you should install the TRITON Management Server with both the TRITON - Web Security and TRITON - Data Security modules on the same VM.

If you have a subscription to Websense Email Security Gateway or Email Security Gateway Anywhere, you should install the TRITON Management Server with both the TRITON - Email Security and TRITON - Data Security modules on the same VM.

The following VM platforms are supported. You can obtain them from the VMware site: www.vmware.com.

- VMware ESXi 3.5 update 2
- VMware ESXi 4 update 1

> **Note**
> While downloading ESXi, a license key is generated and displayed on the download page. Make a note of this license key for use during installation.

Before installing Websense modules on a VM via ESXi, ensure that your VMware tools are up to date. All of your hardware must be compatible with VMware ESXi. In addition, ensure that the following hardware specifications are met:

| VMware Server | Requirements |
|---|---|
| CPU | • At least 4 cores 2.5 GHz (for example, 1 QuadXeon 2.5 GHz). 8 cores are required if you are installing TRITON - Web Security, - Data Security, and - Email Security |
| Disk | • 300 GB, 15 K RPM, RAID 10 |
| Memory | • 8 GB (12 GB if you are installing TRITON - Web Security, - Data Security, and - Email Security |
| NICs | • 2*1000 |

| VMware Infrastructure Client | Requirements |
|---|---|
| CPU | • At least 500 MHz |
| Disk storage | • 150 MB free disk space required for basic installation.<br>• An additional 55 MB free on the destination drive during installation<br>• 100 MB free on the drive containing the %temp% folder |
| Memory | • 512 MB |
| Networking | • Gigabit Ethernet recommended |

| Module | Requirements for VM installation |
|---|---|
| TRITON Management Server | • Windows Server 2008 R2 64-bit<br>• Windows Server 2003 R2 32-bit (if installing TRITON - Data Security only)<br>• 8GB RAM<br>• 150 GB Disk<br>• 2 CPU cores |

The steps for installing on a virtual machine are as follows:

- *Installing the ESXi platform*
- *Customizing ESXi*
- *Installing the VMware Client*
- *Installing the license and setting the time*
- *Configuring an additional NIC*
- *Creating the Data Security virtual machine*

## Installing the ESXi platform

### Applies to

- Data Security v7.6.x

### Installing the ESXi platform

1. Download the version of ESXi that you want to use from www.vmware.com.
2. Once the download is complete, burn the download file to a CD.
3. On the machine that will host your VMware server, insert the ESX Server CD into the CD drive
4. Set the BIOS to boot from the CD.
5. Follow the instructions in the installer to complete the installation process.
6. When the installation has finished, remove the CD and reboot the host machine.

# Customizing ESXi

## Applies to

- Data Security v7.6.x

## Customizing ESXi

We recommend that you customize the ESXi platform as follows:

- Assign a password to the root account.
- Set up a management IP address for the ESXi server.

  By default the management IP address is dynamically obtained using DCHP. However, we recommend that you set up a static IP address.

To configure the ESXi platform:

1. Press **F2** to access the Customize System screen.
2. Select **Configure Password**, and enter a password for the root account.
3. To set up a static IP address, select the **Configure Management Network** menu.
4. Select **IP Configuration**, and on the screen that appears enter the following information:
   - Management IP address
   - Subnet mask
   - Default gateway
5. From the **Configure Management Network** menu, select **DNS Configuration**.
6. Configure static DNS information by entering the following:
   - Host name (fully qualified)
   - Primary and secondary DNS server addresses
7. Reboot the server.

# Installing the VMware Client

## Applies to

- Data Security v7.6.x

## Installing the VMware Client

**Note**

The VMware client for ESX 4i is called the vSphere Client. Although the instructions in this section refer to the VMware Infrastructure Client that is available with ESX 3.5i, all instructions also apply to the vSphere Client.

The VMware Infrastructure Client (VI Client) manages the ESXi platform. Install the client on a Windows machine with network access to the ESXi server.

1. On the machine where you intend to install the client, open a browser and access the ESXi server using HTTPS and the management IP address you entered in the previous section (for example, https://10.15.21.100). If you see an error page, accept the server certificate.
2. On the VMware ESX Server Welcome page, click the **Download VMware Infrastructure Client** link.
3. Download and run the client installation program.

## Installing the license and setting the time

### Applies to

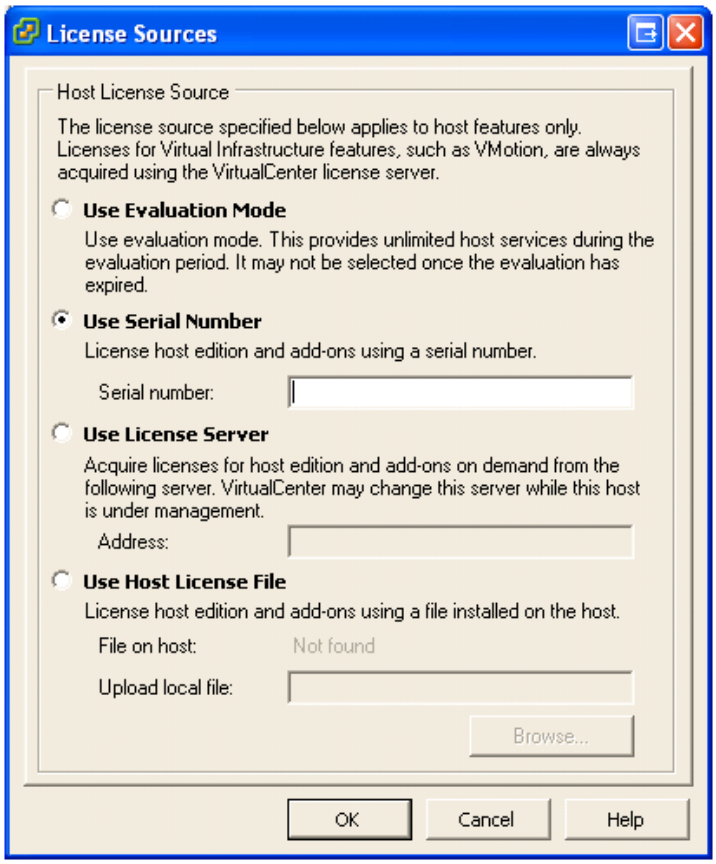
- Data Security v7.6.x

### Installing the license and setting the time

You received your license number as part of the ESXi download.

1. Start the VI Client by selecting **Start > Programs > VMware > VMware Infrastructure Client**.
2. Connect to your ESXi server using the IP address you set up during configuration. For user credentials, enter the user name**root** and the password that you set up for the root account.
3. On the **Configuration** tab, select **Licensed Features**.

4. To the right of the **License Source** label, click the **edit** link.




5. Select **Use Serial Number**, and enter your license number in the field provided. Then click **OK**.
6. On the **Configuration** tab, select **Time Configuration**.
7. Select **Properties**, and then set your server's time. Click **OK** when done.

## Configuring an additional NIC

### Applies to

- Data Security v7.6.x

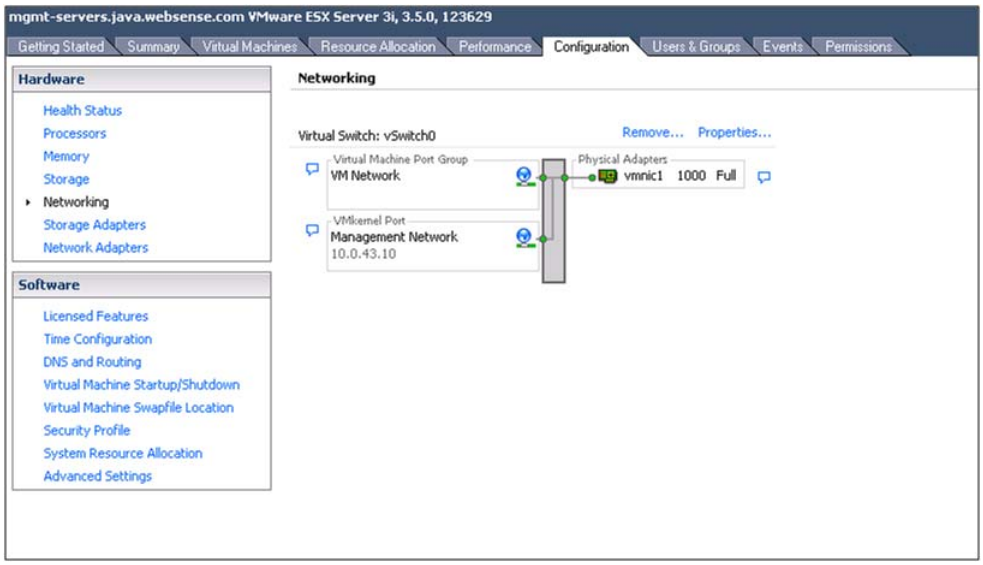
### Configuring an additional NIC

When setting up the ESXi server, you configured one NIC as the ESXi platform management interface. This NIC can also be used by the virtual machines. However, this setup requires an additional NIC, for redundancy and to perform load balancing.

To set up an additional NIC:

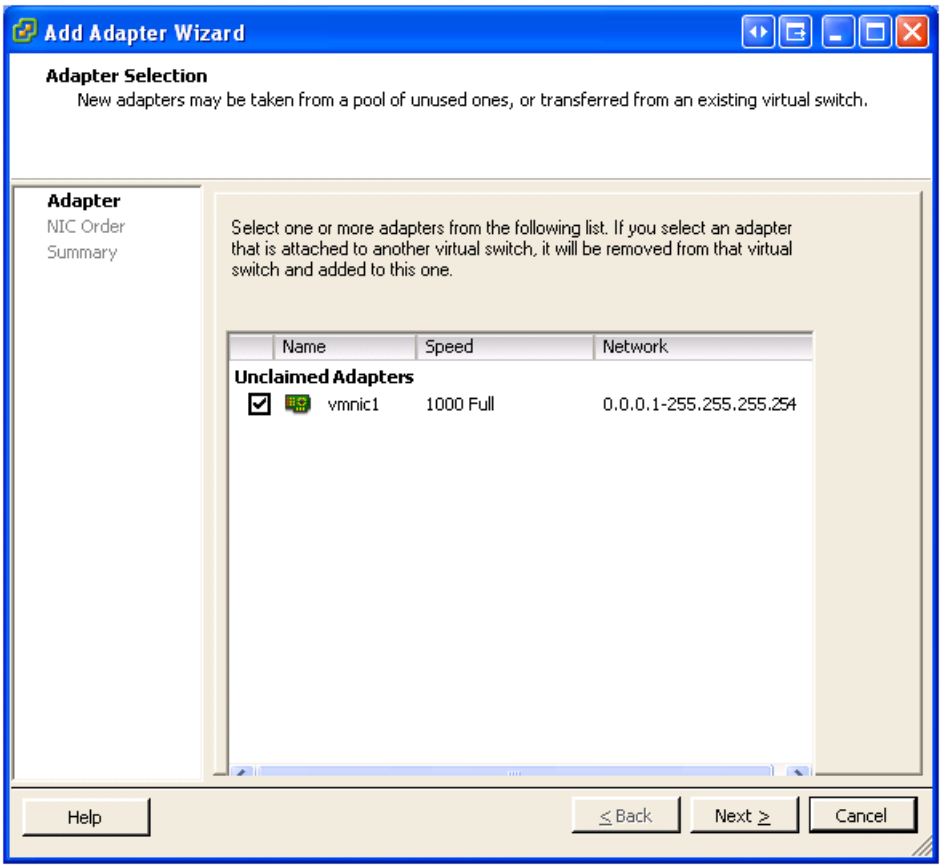
1. On the **Configuration** tab, select **Networking**.

When the system was started, the ESXi platform configured the server to have one virtual switch (vSwitch) using the management NIC. With this configuration, the Networking screen should look similar to the one below.



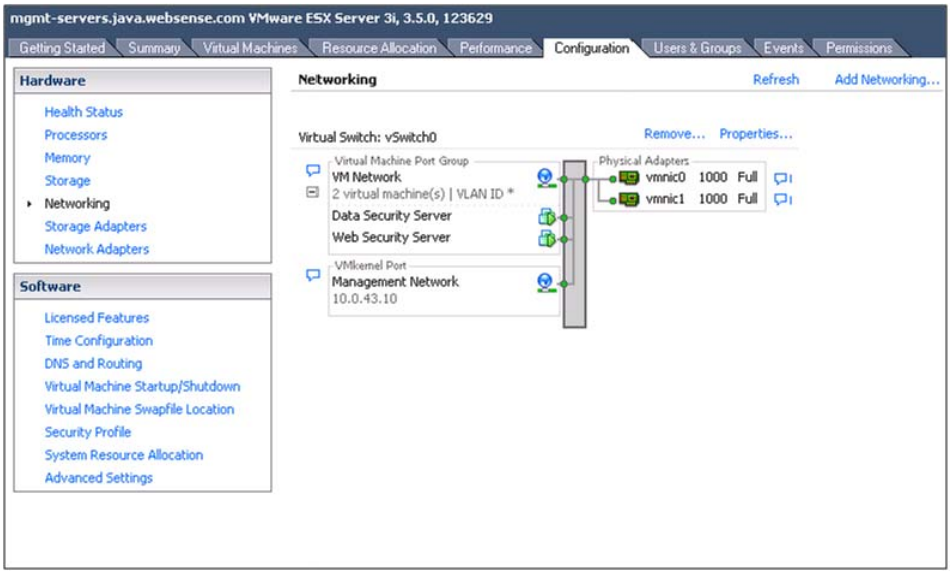

2. To add a new NIC to the virtual switch, select the **Properties** link.

3. In the Properties popup window, select the**Network Adapters** tab and click **Add**. The Add Adapter Wizard opens.




4. Select the adapter you want from the list, then click **Next** twice.
5. Click **Finish** to close the wizard, then close the Properties window.

After adding the additional network adapter to the virtual switch, the network layout should look similar to the one below:




## Creating the Data Security virtual machine

### Applies to

- Data Security v7.6.x

### Creating the Data Security virtual machine

1. In the VI Client, select the **Summary** tab and then select **New Virtual Machine**. The New Virtual Machine Wizard opens.
2. Select **Custom**, and click **Next**.
3. Set the machine name to be TRITON Management Server, and click **Next**.
4. Select the only available datastore (datastore1), and click **Next**.
5. Select Microsoft Windows as the guest operating system, and set the version to one of the following:
   - For Web Security Gateway Anywhere or Email Security Gateway deployments, select Microsoft Windows Server 2008 R2 (64 bit).
   - For Data Security only deployments, select either Microsoft Windows Server 2008 R2 (64 bit) or Microsoft Windows Server 2003 R2 (32 bit)

   Then click **Next**.
6. Set the number of virtual processors according to the TRITON management server for your deployment, and click**Next**. See *System Requirements*, page 41 for more information.
7. Set the virtual machine memory to a minimum of 8 GB, depending on your deployment, and click **Next**. See *System Requirements*, page 41 for more information.

8. Accept the defaults on the Network page and the I/O Adapters page, clicking **Next** to continue.
9. Select **Create a new virtual disk** and click **Next**.
10. Set the disk capacity to 150 GB.
11. Click **Next** to progress through the Advanced Options page without changing the defaults.
12. Review your configuration and then click **Finish**.

### Setting the CPU affinity

Once you have configured the virtual machine, set its dedicated CPUs as follows:

1. In the VI Client, select the virtual machine you just created from the tree on the left.
2. Select the Summary view, and click **Edit Settings**.
3. Select the **Resources** tab.
4. Select **Advanced CPU**.
5. In the Scheduling Affinity group, select **Run on processor(s)**, then select processors zero and one.
6. Click **OK**.

### Installing the operating system and VMware tools

Install the operating system on your virtual machine, and then reboot. We recommend that you also install the VMware tools before installing the TRITON management server. To do this:

1. Log on to the virtual machine.
2. From the VI Client, select **Inventory > Virtual Machine > Install/Upgrade VMware Tools**.
3. Follow the instructions on screen to install the tools.

### Installing the TRITON management server

Follow the instructions in *Creating a TRITON Management Server*, page 645 to install the TRITON management server on your virtual machine.

# 32 Planning Data Security Deployment

## Applies to

- Data Security v7.6.x

## Overview

Before you begin setting up your data security system, it is important to analyze your existing resources and define how security should be implemented to optimally benefit your specific organization. Plan your deployment by:

1. *Deciding what data to protect*, page 449
2. *Determining where your confidential data resides*, page 451
3. *Determining your information flow*, page 453
4. *Defining the business owners for the data*, page 453
5. *Deciding who will manage incidents*, page 454
6. *Planning access control*, page 454
7. *Analyzing network structure*, page 455
8. *Planning network resources*, page 456
9. *Planning a phased approach*, page 469

## Deciding what data to protect

### Applies to

- Data Security v7.6.x

### In this topic

- *Overview*

## Overview

What data should you protect? What are the applicable regulations for your organization?

Answers to these questions depend on the geographical regions in which the organization operates, the industry and sector, whether it is a public company and other particulars of your organization.

Consider the following:

## Geographical

- Each region may have its own regulations/laws that require protecting various types of sensitive information, such as private, financial, and medical.
- Global enterprises may be bound to multiple laws if they have branch offices in different regions. (For example, they may have to abide by different state laws if they have offices in several different states)

## Industry

- Each type of industry may have its own laws and regulations. For example:
  - GLBA for finance
  - HIPAA for healthcare
- If your enterprise develops new technologies, you may want to protect intellectual property and trade secrets (such as designs, software code, drawings, or patent applications).

## Sector

- Government agencies and organizations that are affiliated with the government are subjected to special requirements and regulations imposed by the government office, such as DIACAP for units and contractors related to the US Department of Defense and FISMA for US federal agencies and their contractors.
- For public companies, additional regulations may apply (such as the Sarbanes-Oxley Act in the U.S., or regulations that are published by the regulatory body of the relevant stock markets).

## General

- Most organizations want to keep their marketing information away from competitors:
  - Upcoming press releases
  - Marketing campaigns
  - Leads
  - Existing customer data
  - Many organizations have individualized needs for data protection that might not fall into typical categories, but Data Security can accommodate them.

The TRITON - Data Security first-time policy wizard assists you in defining your region and industry and it displays the relevant policies, making it easier to select them. Besides predefined policies, you may want to protect specific information, such as:

- Designs
- Drawings
- Marketing materials
- Legal documents
- Strategic planning documents, such as business plans
- Financial and pricing information
- All documents marked “Confidential”

# Determining where your confidential data resides

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

Based on experience from numerous data-loss protection deployments, it’s evident that most sensitive company information resides within:

- Corporate file servers or shared drives

- In-house databases
- Personal laptops, workstations and removable media

## Corporate file servers and shared drives

There are a few ways to determine where your confidential information is stored:

### Ask

- Talk to appropriate data owners in your organization and they may point you to relevant locations. This may cover a big part of the information that needs to be protected and is a good start. Your review of locations based on their revelations will undoubtedly reveal other critical data branchings and parallel storage places.

### Discover

- Use Websense Data Security to classify file servers, shared drives, and endpoints by running it with the relevant predefined policies enabled. This should give you bulk estimations of where data is located in your enterprise.

Combining the results gives you a good idea of the location of your confidential information.

## In-house databases

As in case of file servers and shared drives, the best ways to understand which databases are critical is to ask:

- Talk to people that manage in-house applications relying on internal databases (such as customer relations, orders processing, and accounting).
- Talk to database administrators (DBAs) and find out what are the most accessed databases. The more a database is accessed, the more chances there are for data loss. Your IT department may also be able to elaborate on discoveries from both instances described above.

**Discover:**

- Use Websense Data Security to classify databases by running it with the relevant predefined policies enabled. This should let you know primarily where your vital records are located.

Based on the above information, you can narrow down the most critical database servers, databases and tables to protect.

# Determining your information flow

## Applies to

- Data Security v7.6.x

## Determining your information flow

Analyze the flow of information through your enterprise today.

- Where is information typically coming from? Internal users? Partners? Vendors?
- Where does it need to be sent?
- What are all the potential pathways for information?
- What processes are in place, if any, to govern data flow?
- How many HTTP, SMTP and FTP exits or egress points are there in the organization?

These questions are vital to ensuring that protector(s) are placed appropriately so that nothing escapes analysis.

# Defining the business owners for the data

## Applies to

- Data Security v7.6.x

## Defining the business owners for the data

The business owners of information normally come from the departments where the information was created. For example, if you wish to protect marketing materials, the head of marketing is normally the business owner, and should be consulted about deployments. (He/she may delegate the responsibility to other people in his/her department.) Normally, marketing principals—and principals from other departments—would want to get notifications about data losses containing information originating from their department (even and especially if the sender is from a different department).

# Deciding who will manage incidents

## Applies to

- Data Security v7.6.x

## Deciding who will manage incidents

How should you delegate incident management across your organization?

As in the case of business owners, you should identify who is responsible for data management in various departments. If you are unsure who that person is, you may either consult with the department manager or train one of the employees that you trust from that department.

Once incident managers are identified, you can assign the proper roles and policy category groups to the relevant users through the TRITON - Data Security Web user interface.

# Planning access control

## Applies to

- Data Security v7.6.x

## Planning access control

Standard network installations provide access control (preventing personnel from viewing unauthorized files) by giving each user a login and password, and authorizing each user to view only the network directories required for the user's job function. However, authorized users can still send content they are authorized to use to unauthorized recipients.

Planning Data Security Deployment augments access control by providing Information Distribution Management (IDM) capabilities, thereby greatly enhancing the level of information security. Websense Data Security protects digital content from being sent from your company’s network to people outside of the company, as well as protecting classified information from being sent to unauthorized users within the local network.

Typically, these user privileges were defined individually, without considering grouping or security clearances for groups of people. Utilizing data security capabilities involves delineating users as belonging to groups or security levels, enabling a more sophisticated, higher level of control over classified data.

Naturally, when considering the policies discussed in this chapter, it is important to consider how these policies are impacted by or impact other content policies in your company. The TRITON - Data Security software has the flexibility to accommodate the full range of enterprise security needs.

# Analyzing network structure

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

To best employ data security, you need to analyze your network structure, determine the location of confidential information, note which documents need to be protected and where they are located, and whether you need to make changes to the network directory structure in order to group documents differently for security purposes.

In most organizations, user rights have been determined and built into the network directory structure, according to your organization's logic. You may conclude that the network configuration is fine as it is, or that the internal network definitions change to some degree due to today's higher security needs.

Any changes you need to implement internally in the directory structure should be implemented with these increased security measures in mind.

## Structural guidelines

It is possible to configure the system so that a particular user cannot access a certain document through the network, but can receive the document by email. For example, a manager would not want employees to access documents in his or her personal folder, but would want to be able to send the documents to them by email. It is therefore important that you perform this analysis together with the network administrator, so that your desired changes will be implemented internally in a smooth, logical fashion, as well as within the Websense structure.

Typically, your network directories are organized functionally, according to the different business units in the company. Within this structure, functional groups are usually entitled to look at documents within their business unit.

We recommended that you use this as your process map:

- Take a network map of all the directories, and look at how the network access is organized
- Determine what types of classified documents you have, and where they are located
- Determine whether documents of similar confidentiality are together in similar directories
  - Organize/group information that is critical to your organization and information whose security is legally mandated. For example, financial institutions may start by considering customer data (such as Social Security numbers or account numbers) and highly confidential business information
  - Organize/group important proprietary and confidential information with medium or low change-frequency
  - Arrange all major information assets within your organization so that you understand data locations, relationships and security-value hierarchies

The result of this analysis should be a table corresponding to the directories in the network that need to be protected, indicating what types of users should be able to receive those files and to provide a look at access issues.

You may want to rearrange some areas of your network access, and set the data security accordingly. See below for recommended procedures.

# Planning network resources

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

To decide on things like disk space allocation, number of servers, and network distribution, start by answering these questions:

- What volume of daily data do you expect in the number of transactions?
- What is your user count?
- Are you covering geographically distributed offices?

- What is your user directory structure (Active Directory, ADAM, Domino) and the IP addresses of the LDAP servers?
- Which ports are used and what are the port numbers?

## Allocating disk space

Disk space for archiving fingerprint and forensic repositories is allocated by the Websense Data Security by default. The default settings are the nominal values defined by Websense; however, you can modify these values. The tables below indicates the default and maximum disk space for archives, forensics repository and endpoint client incident storage, log file and fingerprint storage.

### On TRITON management server

| Type | Description | Default Setting | Max Disk Space |
|---|---|---|---|
| Archive | The disk space of the incident archive folder on a local or external partition. | 50 GB | No Max. |
| Forensic repository | The disk space of the forensic records stored in the archive folder. | 40 GB | No Max. |

### On endpoint client

| Type | Description | Default Setting | Max Disk Space |
|---|---|---|---|
| Endpoint client incident storage | The disk space that each endpoint client should allocate for incident storage when the endpoint host is disconnected from the TRITON Management Server. | 100 MB | 100 MB |
| Endpoint client log file | The disk space of the log file viewed on the endpoint client. | 16 MB | 100 MB |
| Endpoint client PreciseID fingerprint storage | The disk space that each endpoint client should allocate for storing directory and SharePoint fingerprints. | 50 MB | 1,000 MB |

## Modifying the disk space setting

Follow the instructions below to modify the default disk-space settings for either archives, endpoint client incident storage, PreciseID fingerprint or forensic repositories.

**To modify disk space settings:**

1. Access TRITON - Data Security and choose the **Settings** tab.

2. Depending on the disk space to modify, do the following:
   a. Archives:
   Select **Settings > Configuration > System > Archive Storage**. In the Maximum archive disk space field, modify the value.
   b. Forensics repository:
   Select **Settings > Deployment > System Modules**. In the list of modules, select the **Forensics Repository** entry. In the Maximum Disk Space field, set the value.
   c. Endpoint client (incident storage, log file and fingerprint storage):
   Select **Settings > Configuration > System > Endpoint.** In the section labeled Disk Space, modify the relevant disk-space value.
3. Click **OK**. The disk space values are set and changes saved.
4. Click **Deploy** to deploy your settings.

# Distributing resources

Websense Data Security supports multi-site, distributed deployments. You can have a local policy engine on the protector, for example, and distributed (primary and secondary) fingerprint repositories.

You can have a management server in one location and one or more supplemental Data Security servers in other locations.

You can utilize the crawlers on the Data Security servers alone to do your fingerprint and discovery scans, or you can install the crawler agent on additional servers to improve performance.

These are just a few of the possibilities.

Your network architecture and the geographical location of your offices determine how you will want to distribute your resources.

See *Most common deployments*, page 459 for distributions our customers commonly use.

## Load balancing

In a multi-component system, you can configure load-balancing by selecting **Settings > Deployment > System Modules** in TRITON - Data Security and then clicking the **Load Balancing** button at the top of the screen.

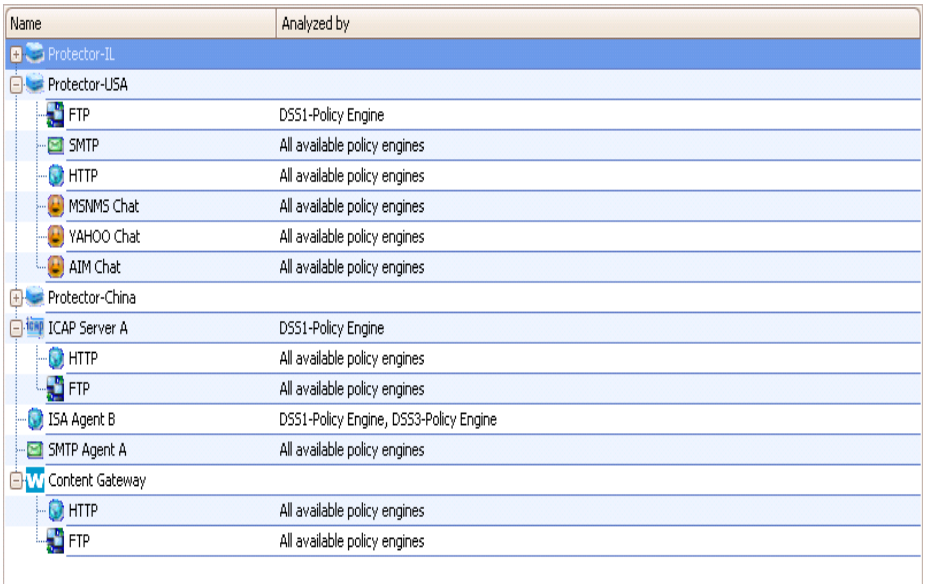
Load balancing enables you to manage how each module sends its data to specified policy engines for analysis. This lets you distribute the load, but more important, it ensures that your vital email and HTTP performance is never harmed. For example, you can designate 1-2 dedicated servers to analyze inline HTTP traffic (where analysis latency is critical) and use another set of servers to analyze other channels.

An agent or a protector service can be analyzed by all listed policy engines or it can be analyzed by specifically selected policy engines. (Note that protector services can be

analyzed only by local or Windows-based policy engines.) In addition, you can choose which policy engine analyzes a specific agent or service of the protector.

> **Note**
> Websense recommends that you do not distribute the load to the TRITON management server.

The Load Balancing screen shows a list of items where each item represents a protector or agent.




Click each item in the tree to define which policy engine it should be analyzed by. For further information on load balancing, refer to the TRITON - Data Security Help.

# Most common deployments

## Applies to

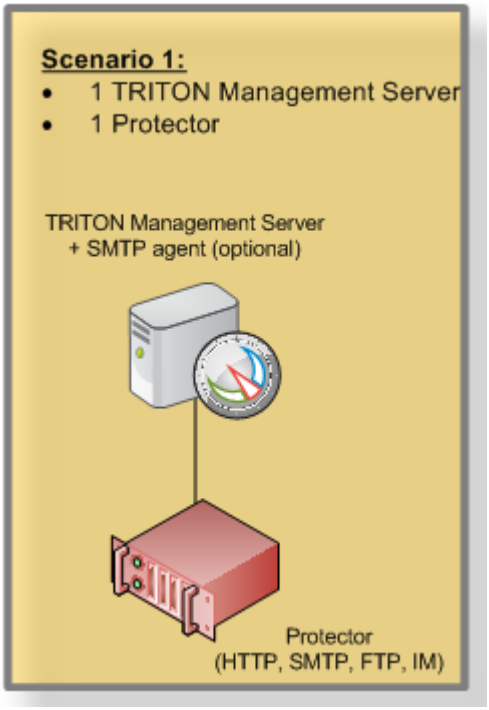
- Data Security v7.6.x

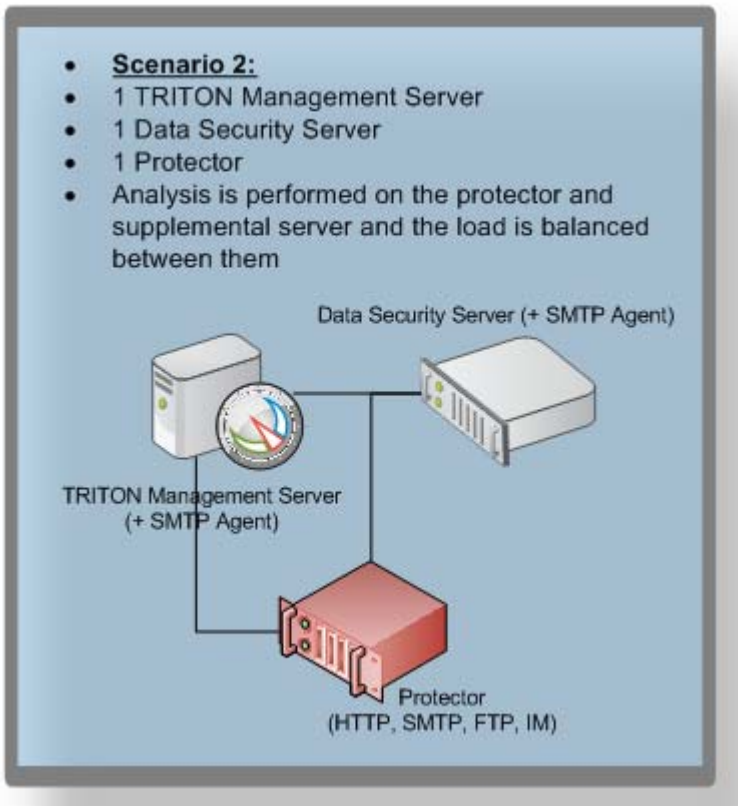
## In this topic

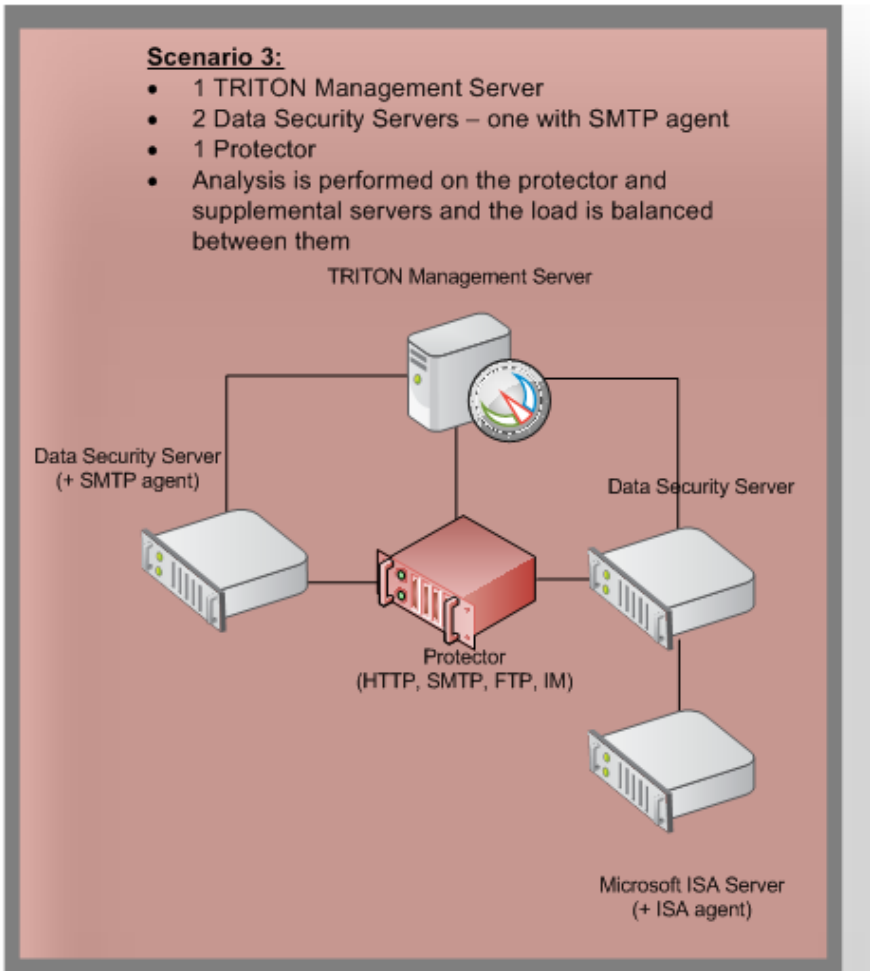
## Overview

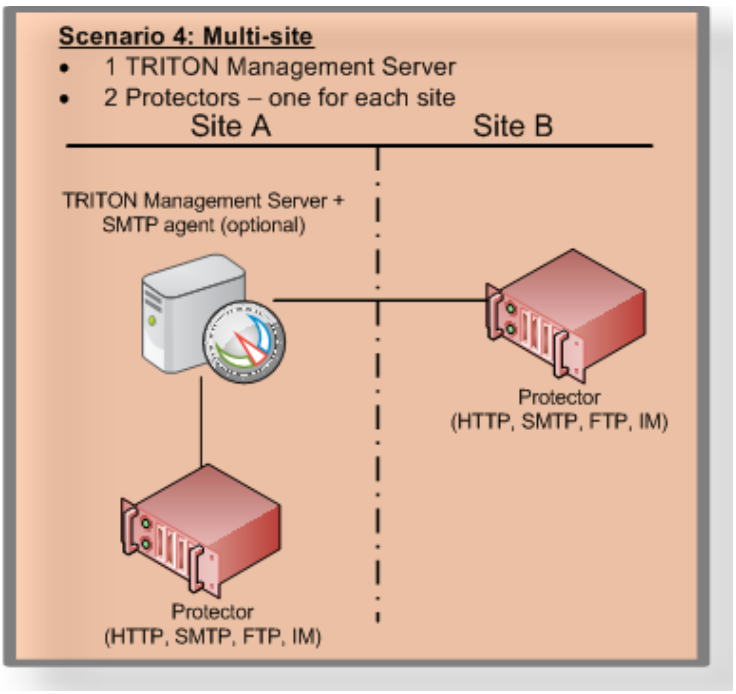
Websense Data Security is a flexible system that affords you various, customizable deployment scenarios. Each scenario is based on an organization's practical needs and purposes—of course, individual hardware/software setups vary. Be sure to obtain guidance and advisement from your Websense sales representative to assure that the appropriate deployment option is tailored for your organization.

Below are the most common single and multi-site deployment scenarios.



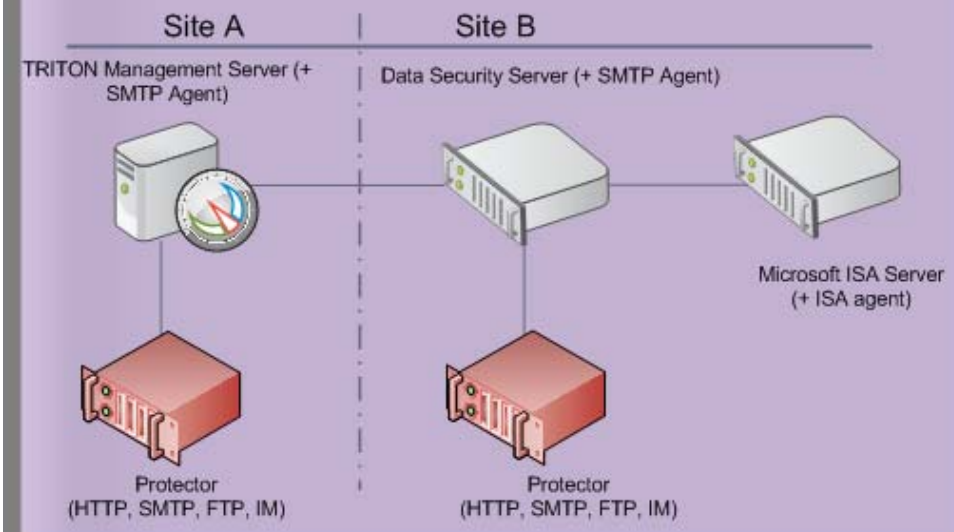

Scenario 3:
1 TRITON Management Server
2 Data Security Servers – one with SMTP agent
1 Protector
Analysis is performed on the protector and supplemental servers and the load is balanced between them
TRITON Management Server
Data Security Server (+ SMTP agent)
Data Security Server
Protector (HTTP, SMTP, FTP, IM)
Microsoft ISA Server (+ ISA agent)


Scenario 4: Multi-site
1 TRITON Management Server
2 Protectors – one for each site
Site A
Site B
TRITON Management Server + SMTP agent (optional)
Protector (HTTP, SMTP, FTP, IM)
Protector (HTTP, SMTP, FTP, IM)

**Scenario 5: Multi-site Deployment**

- 1 TRITON Management Server
- 2 Data Security Servers – one for each site
- 2 Protectors – one for each site

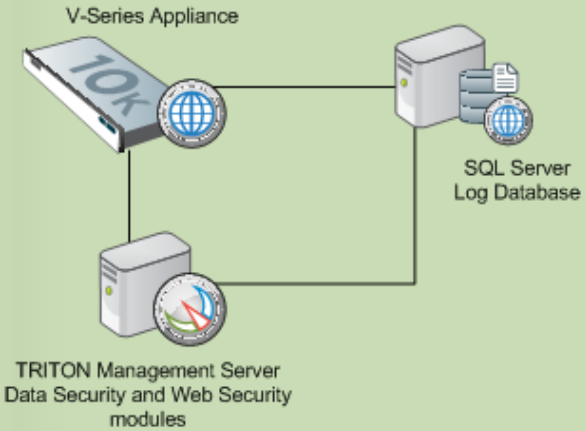
**NOTE:** Protector on site A performs its own analysis. It does not balance the load with the management server. No analysis is performed on the ISA Server

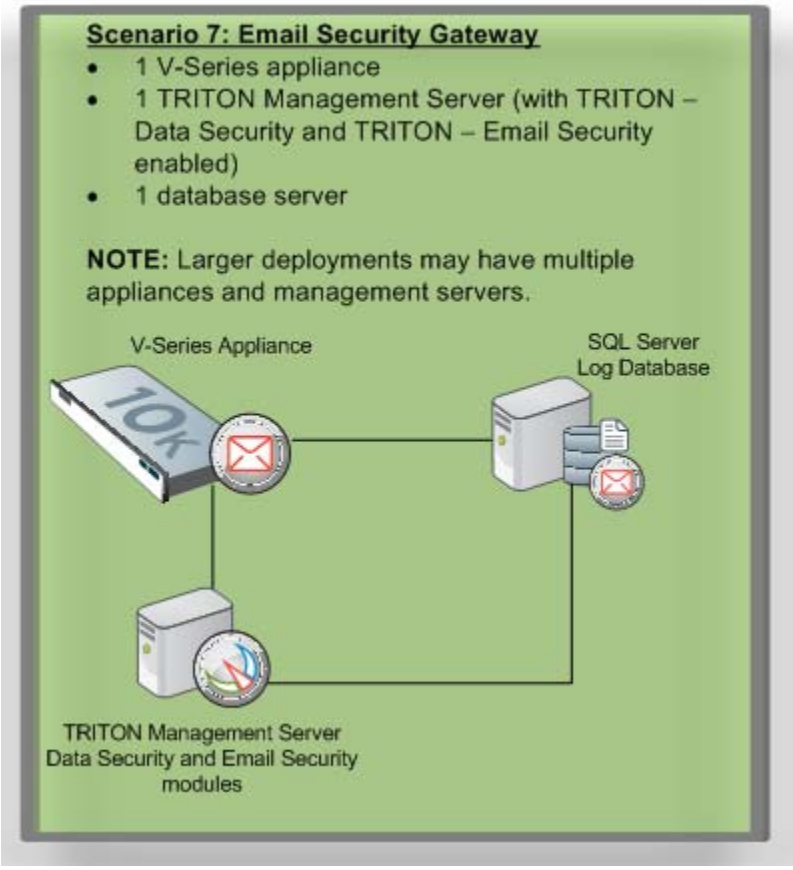



**Scenario 6: Web Security Gateway Anywhere**

- 1 V-Series appliance
- 1 TRITON Management Server (with TRITON – Data Security and TRITON – Web Security enabled)
- 1 database server

**NOTE:** Larger deployments may have multiple appliances and management servers.




Scenario 7: Email Security Gateway
1 V-Series appliance
1 TRITON Management Server (with TRITON – Data Security and TRITON – Email Security enabled)
1 database server
NOTE: Larger deployments may have multiple appliances and management servers.
V-Series Appliance
10K
SQL Server
Log Database
TRITON Management Server
Data Security and Email Security modules

## Websense Web Security Gateway Anywhere

Depending on your enterprise needs and requirements, a deployment can be subject to a variety of different combinations of components that make up Websense Data Security.

| Topology | Small organization | Large org/Enterprise |
|---|---|---|
| • Monitoring or blocking for DLP over Web channels:<br>  • HTTP<br>  • HTTPS<br>  • FTP<br>  • FTP-over-HTTP | • 1 TRITON Management Server with Web Security and Data Security modules enabled<br>• 1 V-Series appliance<br>• 1 Windows server for Microsoft SQL Server and Log Database | **Scenario 1:**<br>• 1 TRITON Management Server with Web Security and Data Security modules enabled<br>• 1 Data Security Server<br>• Multiple V-Series appliances<br>• 1 Windows server for Microsoft SQL Server and Log Database<br>Larger organization with significant amount of traffic or multiple geographic locations. This will require load balancing between policy engines. |
| • Monitoring or blocking for DLP over Web channels:<br>  • HTTP<br>  • HTTPS<br>  • FTP<br>  • FTP-over-HTTP<br>• Monitoring or blocking of SMTP traffic | • 1 TRITON Management Server with SMTP agent and Web Security and Data Security modules enabled<br>• 1 Protector<br>• 1 V-Series appliance<br>• 1 Windows server for Microsoft SQL Server and Log Database | **Scenario 2:**<br>• 1 TRITON Management Server with Web Security and Data Security modules enabled<br>• 1 Data Security Server<br>• 1 Protector<br>• Multiple V-Series appliances<br>• 1 Windows server for Microsoft SQL Server and Log Database |

# Websense Email Security Gateway

| Topology | Small organization | Large org/Enterprise |
|---|---|---|
| • Monitoring or blocking for DLP over email channels:<br>  • SMTP | • 1 TRITON Management Server with Email Security and Data Security modules enabled<br>• 1 V-Series appliance<br>• 1 Windows server for Microsoft SQL Server and Log Database | • 1 TRITON Management Server with Email Security and Data Security modules enabled<br>• 1 Data Security Server<br>• Multiple V-Series appliances<br>• 1 Windows server for Microsoft SQL Server and Log Database<br>Larger organization with significant amount of traffic or multiple geographic locations. This will require load balancing between policy engines. |
| • Monitoring or blocking for DLP over email channels:<br>  • SMTP<br>• Monitoring for:<br>  • Web / FTP<br>  • IM<br>• User-defined protocols<br>• Destination awareness | • 1 TRITON Management Server with Email Security and Data Security modules enabled<br>• 1 Protector<br>• 1 V-Series appliance<br>• 1 Windows server for Microsoft SQL Server and Log Database | • 1 TRITON Management Server with Email Security and Data Security modules enabled<br>• 1 Data Security Server<br>• 1 Protector<br>• Multiple V-Series appliances<br>• 1 Windows server for Microsoft SQL Server and Log Database |

# Websense Data Monitor

| Topology | Small organization | Large org/Enterprise |
|---|---|---|
| • Monitoring for:<br>  • Mail<br>  • Web / FTP<br>  • IM<br>• User-defined protocols<br>• Destination awareness | • 1 Data Security Management Server<br>• 1 protector<br>Small-to-medium business with one or more egress points (connected to the same protector) to monitor traffic. This scenario is tailored to organizations that are keen on monitoring traffic rather than enforcing traffic | **Scenario 1:**<br>• 1 Data Security Management Server<br>• 1 Data Security Server<br>• 1 protector - load balancing with the Data Security server<br>Larger organization with significant amount of traffic. In most cases, they will also plan to move to enforcement. This will require both load balancing between policy engines and building a load-balanced SMTP Agents environment (to avoid single points of failure). Note that Protector MTA can be used in those cases in which SMTP Agent is not supported on the operating system. |
| | | **Scenario 2:**<br>• 1 Data Security Management Server<br>• 1 Data Security Server<br>• 2 protectors - one for each site<br>Organization having multiple geographical locations for monitoring traffic |
| | | **Scenario 3:**<br>• 1 Data Security Management Server<br>• 2 Data Security Servers - one for each site<br>• 2 protectors - one for each site<br>Organization having multiple geographical locations for monitoring traffic with low latency between sites. Local policy engine is placed close to protector to avoid occupying bandwidth when sending transactions to analysis. Both protectors will do load balancing with the local policy engine. |

## Websense Data Protect

| Topology | Small organization | Large org/Enterprise |
|---|---|---|
| The Data Protect module includes:<br>**Data Protection:**<br>• HTTP and SMTP blocking<br>• Policy enforcement for all channels<br>• Destination policy controls<br>**Data Monitoring:**<br>• Monitoring for:<br>  • Mail<br>  • Web / FTP<br>  • IM<br>• User-defined protocols<br>• Destination awareness | • 1 Data Security Management Server<br>• 1 protector | • 1 Data Security Management Server<br>• X Data Security Servers and Y protectors depending on traffic volume.<br>The protect mode is very similar to the monitor mode; therefore, the same topologies mentioned in the monitor table apply here. |

## Websense Data Endpoint

| Topology | Small organization | Large org/Enterprise |
|---|---|---|
| • Local discovery<br>• Removable media & CD/DVD security<br>• Application controls for copy/paste, print, print screen, file access<br>• Endpoint Web channels (HTTP/ HTTPS)<br>• Endpoint LAN control | • 1 Management Server<br>• Endpoint clients | • 1 Data Security Management Server<br>• 1 Data Security Server for every additional 30,000 endpoint clients |

## Websense Data Discover

| Topology | Small organization | Large org/Enterprise |
|---|---|---|
| • Network and file discovery for data in file folders, SharePoint sites, databases, and Exchange servers<br>• Automated remediation for data at rest | • 1 Data Security Management Server<br>• 1 Data Security Server | • 1 Data Security Management Server<br>• Websense Technical Support will assess the number of Data Security servers with discovery and fingerprinting crawlers needed. |

# Planning a phased approach

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

Next, you need to consider the tactics you can employ in protecting your data, how to configure policies, manage incidents and control access.

To assess how to protect your data from compromise, we recommend using Planning Data Security Deployment in a multi-phased approach. Listed below is just one approach of many.

## Phase 1: Monitoring

Start by monitoring data (auditing without blocking). The following steps usually constitute this phase (you may skip some of the steps if they are not relevant):

- Step A: Enable regulatory compliance, regional and industry-related predefined policies:
  - This supplies a solid first stage of DLP (data loss prevention) deployment
  - It will give you a good picture of what information is being sent out, by whom, to where and how
- Step B: Request custom policies from Websense:
  - Moving forward, you may identify that your enterprise has unique needs in terms of data identification that are not covered by predefined policies; for example, you may want to protect coupons that are issued or catalog numbers.
  - To request a policy, please apply to Websense technical support. We will escalate your request and engage the research team. The usual turnaround is approximately 3 weeks (the research team will generally provide an estimated time to completion within 3 days of reviewing the request).
- Step C: Fingerprint data (can be also part of Phase 2):
  - Data fingerprinting allows accurate and efficient data identification
  - Database fingerprinting (PreciseID database technology):
    - PreciseID database fingerprinting allows accurate and efficient detection of fingerprinted records coming from various sources:
    - Database tables
    - Database views
    - CSV files
  - Content policies can be flexibly defined on top of data sources. Detection rules can be configured as combinations of columns and thresholds for a given number of matches.
  - Database fingerprinting can be used in conjunction with PreciseID patterns. While patterns identify a full range of data (for example, all credit cards), database fingerprinting can narrow down the detection only to credit cards of your enterprise customers. You may want to set higher severity on PreciseID database policies than on PreciseID patterns.
  - Files, directory, and SharePoint fingerprinting (PreciseID files technology)
    - PreciseID files technology allows identification of unstructured data (free text)
    - The data that we identify can already be in a different format (e.g., after PDF conversion), different context (excerpt of confidential document that was fingerprinted), and so on
    - Advanced and efficient algorithms allow detecting fingerprints even on endpoints that have limited resources

## Phase 2: Monitoring with notifications

At this stage, we recommend enabling email notifications to various people in the organization when a policy breach is discovered. The options are:

- Global security administrator (can be CISO)

- Data owners (specified for each policy)
- Senders (people that actually leak the information)—some enterprises prefer to use this option to educate users and watch the expected decrease in the amount of incidents over time in the Trends report.
- Managers—direct managers of people that leak information (based on data in the directory server).

## Phase 3: Policy tuning

(Phase 3 can be ongoing, in parallel to Phases 1 and 2.) Make sure that you keep the amount of incidents manageable and that all incidents are relevant. The options are:

- Disable policies that do not bring value to your enterprise
- Make sure the selected channels are relevant for application of policies
- Identify incidents that are authorized transactions and make appropriate changes in the authorization for specific policies (e.g., allowing sending specific information from certain sources to certain destinations)
- Change thresholds to avoid too many incidents from some policies

Phase 3 is also good for making sure that you assign proper incident managers for various types of incidents, and that you create policy category groups in Data Security Manager and assign them to relevant incident managers.

## Phase 4: Enforcing

This phase should begin after all the policies were successfully tuned and business owners, data owners and incident managers are trained and ready to handle the incidents:

- You can start with the SMTP channel only and then gradually move to HTTP enforcement as well. Or you could enforce FTP through ICAP and/or Websense Content Gateway integrations.
- Continue monitoring incidents and identify whether certain policies can be moved back to auditing only. (Consider this efficiency if you release the email regardless of incidents.)
- Encryption: As part of SMTP enforcement, you may want to integrate with encryption gateways. Websense can automatically route certain email transactions to be encrypted based on email content and/or policy definitions (actions).

## Phase 5: Discovery

Again, this phase can start earlier, in parallel with other phases.

Establish discovery tasks on sensitive corporate servers, databases, Exchange servers, and SharePoint sites that are widely accessed to ensure you know what sensitive information is located where, and who is allowed to access it.

## Phase 6: Endpoint deployments

As explained with other phases, this phase can also be instituted earlier in the security process.

Make sure you are controlling data in use (removable media, clipboard operations, file access) by deploying Websense Data Endpoint in your enterprise:

- It will allow controlling data in use even if users are disconnected from network
- You may decide to install it in stealth (invisible) mode

Local discovery will assist you in getting to the files that network discovery wouldn't reach. (Essentially, local discovery is looking at the drives on a local machine, like a laptop, which can be disconnected from the network.)

# 33 Choosing and Deploying Data Security Agents

## Applies to

- Data Security v7.6
- Data Security v7.6.3

## Choosing and deploying Data Security agents

Websense Data Security monitors and protects data by using a series of *agents* that are deployed according to your organization's needs.

These agents are installed on the relevant servers (ISA agent on the ISA server, printer agent on the print server, etc.) to enable Data Security to access the data necessary to analyze the traffic from these servers. Agents, such as the Data Endpoint, enable administrators to analyze content within a user's working environment (PC, laptop, etc.) and block or monitor policy breaches.

This chapter is designed to help you decide which agents to deploy and to instruct you on how to deploy them.

Below is a summary of the Data Security agents.

| Agent | Description |
|---|---|
| Protector | The protector is a standard part of Websense Data Security deployments. It is a soft appliance with a policy engine and a fingerprint repository, and it supports analysis of SMTP, HTTP, HTTPS, FTP, plain text, and IM traffic (chat and file transfer). The protector is also an integration point for third-party solutions that support ICAP (when Websense Content Gateway is not used for this purpose).<br>**Note:** For HTTPS traffic, you must use one or more of the following:<br>• The Websense Content Gateway (WCG) with DLP enabled<br>• The ISA/TMG agent<br>• The Data Endpoint<br>• A third-party ICAP-compliant HTTP/S proxy<br>See *Protector*, page 476 for more information. |
| SMTP agent | SMTP is the protocol used for sending email to recipients outside the organization. The SMTP agent monitors SMTP traffic. It receives all outbound email from the mail server and forwards it to the Data Security policy engine. It then receives the analyzed email back from the policy engine, and blocks or forwards it to the mail gateway as directed<br>See *SMTP agent*, page 504 for more information. |
| ISA/TMG agent | The ISA agent receives Web (HTTP) connections from a Microsoft ISA or Forefront TMG Server network (for HTTPS) and forwards them to the Data Security policy engine. It then receives the analyzed information back from the policy engine and forwards it to the recipients on the Web.<br>See *Microsoft ISA/TMG agent*, page 506 for more information. |
| Endpoint agent | Data Endpoint monitors all data activity on endpoint machines and reports on data at rest on those machines. With the endpoint agent, you can monitor application operations such as cut, copy, paste, and print screen and block users for copying files, or even parts of files, to endpoint devices such as thumb drives. The endpoint agent can also monitor or block print operations.<br>See *Installing and Deploying Websense Endpoint Clients*, page 741 for more information. |
| Printer agent | The printer agent is installed on a Microsoft print server. It monitors data that is sent to network printers through optical character recognition (OCR) technology.<br>See *Printer agent*, page 508 for more information. |
| Policy engine (Web Content Gateway) | This module is embedded in the Websense Content Gateway. It is not active until registered with a TRITON management server, at which point Content Gateway can communicate with it internally. It is required for Websense Web Security Gateway and Web Security Gateway Anywhere deployments.<br>See *Websense Content Gateway*, page 357 for more information. |

| Agent | Description |
|---|---|
| Policy engine (Email Security Gateway) | This module is part of an Email Security Gateway appliance. It is not active until registered with a TRITON management server, at which point Email Security Gateway can communicate with it internally. It is required for Websense Email Security Gateway and Email Security Gateway Anywhere deployments.<br>See *Email Security Gateway (V10000 G2)*, page 585 or *Email Security Gateway (V5000 G2)*, page 575 for more information. |
| Mobile agent | The mobile agent monitors and blocks activities on mobile devices that perform synchronization operations with the Exchange server. With the mobile agent, you can monitor and block data transmitted in email messages, calendar events, and tasks. It is on a Websense appliance, or you can install it on your own hardware. The mobile agent supports ActiveSync, which is a wireless communication protocol used to push resources, such as email, from applications to mobile devices.<br>See *Mobile agent*, page 489 for more information. |
| Integration agent | The Integration agent allows third-party products to send data to Websense Data Security for analysis. It is embedded in third-party installers and communicates with Data Security via a C-based API.<br>See *Integration agent*, page 512 for more information. |
| Crawler | The crawler is the name of the agent that performs discovery and fingerprinting scans. The crawler is installed automatically on the TRITON Management Server and other Data Security servers. If you want to improve scanning performance in high transaction volume environments, you can install it stand-alone on another server as well.<br>See *The crawler*, page 514 for more information. |

**Important**

Data Security agents and machines with a policy engine (such as a Data Security Server or Websense Content Gateway machine) must have direct connection to the TRITON management server. When deployed in a DMZ or behind a firewall, the relevant ports must be allowed.

Each agent supports different actions—permit, block, encrypt—and each is installed using the standard TRITON installer. Note that the various agent options become available only when you are performing the installation on a required server. For example, if you are running the installation wizard on an ISA Server, the ISA agent is shown as an option in the wizard.

For information about troubleshooting Data Security agents, see *Troubleshooting Data Security agent deployment*, page 515.

# Protector

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

The protector is an essential component of Websense Data Security, providing monitoring and blocking capabilities, preventing data loss and leaks of sensitive information. Using PreciseID technology, the protector can be configured to accurately monitor sensitive information-in-transit on any port.



## When to use the protector

The protector works in tandem with the Data Security server. The Data Security server provides advanced analysis capabilities, while the protector sits on the network, intercepts traffic and can either monitor or block the traffic, as needed. The protector supports analysis of SMTP, HTTP, FTP, plain text, IM traffic (e.g., Yahoo, MSN, chat, and file transfer). The protector is also an integration point for third-party solutions that support ICAP.

The protector fits into your existing network with minimum configuration and necessitates no network infrastructure changes.

If you want to monitor SMTP traffic, the protector is your best choice. You configure a span port to be connected to the protector. This span contains your SMTP traffic.

If you want email blocking capabilities, you can use either the protector's explicit MTA mode or the SMTP agent (see below).

We do not recommend that you use both options for the same traffic, although some companies prefer monitoring one point and enforcing policies on another, due to differences in network traffic content and load.

If you want to monitor or transparently block HTTP traffic, you can use the protector to do so, or you can integrate Data Security with Websense Content Gateway or another Web proxy.

If you want to monitor FTP, plain text, or IM traffic, you should use the protector. Note that the protector cannot block traffic on these channels. You can block FTP using Websense Content Gateway (as a DLP agent) or other Web proxy that buffers FTP and supports ICAP.

The first decision that needs to be made when installing a protector is its location on the network. You can deploy the protector in *SPAN/mirror port* mode or in *inline* mode.

## Deploying the protector

Most data-loss detection devices can be connected off the network, enabling them to sniff network traffic and monitor breaches. This monitoring method is useful because it does not interfere with traffic; however, it also does not enable the loss-prevention system to prevent (block) data losses—only to note and report them. In addition to monitoring mode, you can connect the Websense Protector to the network directly in the path of the traffic, enabling traffic to be blocked, quarantined and even terminated before it reaches its destination.

The following table depicts the available modes according to the selected topology.

| Topology Service | SPAN/Mirror Port | Inline/Bridge |
|---|---|---|
| **HTTP** | Monitoring | Monitoring bridge<br>Active (blocking) bridge |
| **SMTP** | Monitoring passive<br>Mail Transfer Agent (MTA) | Monitoring bridge<br>Mail Transfer Agent (MTA) |
| **All Others** | Monitoring | Monitoring |
| **ICAP** | Monitoring<br>Blocking | Monitoring<br>Blocking |

**Note**

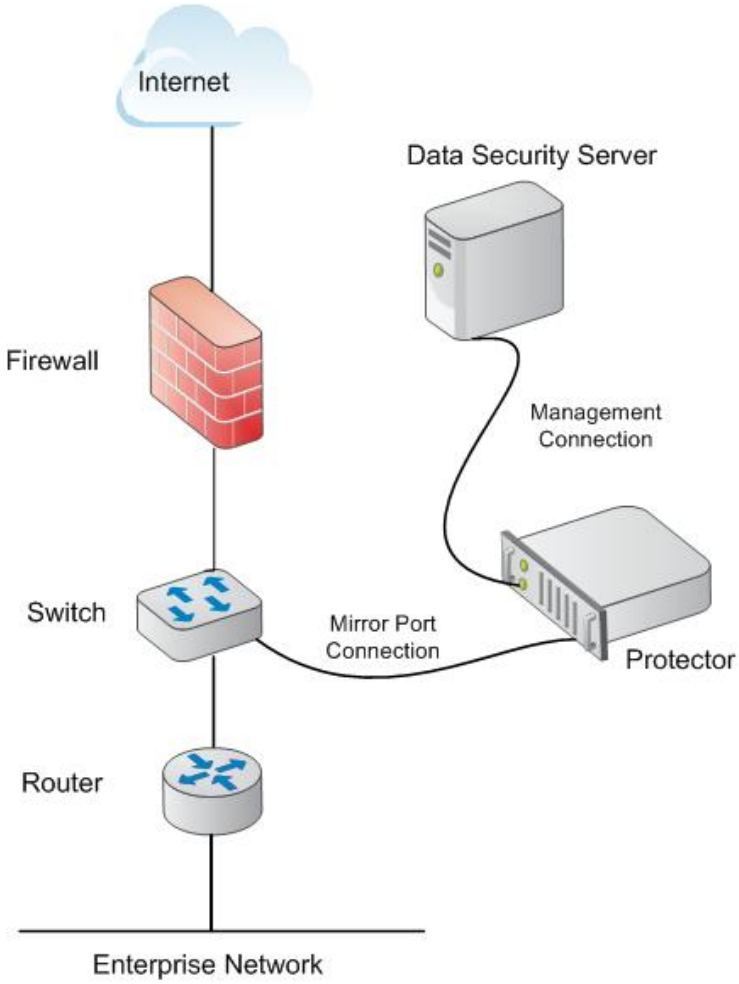
In both inline/bridge and SPAN/mirror port topology, Websense Data Security can be integrated with Web proxies. Blocking and monitoring modes are both available.

## Deploying in SPAN/mirror port configuration

In SPAN/mirror port mode, the protector is connected off the network via the SPAN/mirror port of a switch, which enables the protector to sniff traffic and receive a copy for monitoring purposes, or via a SPAN/mirror device. In SPAN/mirror port mode, traffic is monitored and analyzed, but cannot be blocked. Note that the protector can also be connected to a TAP device.

The following diagram depicts the Websense device connected to the network via a mirror port on a switch, transparently monitoring network traffic.

- Connect the protector to the mirror port of a switch on your network's path.
- Connect the protector to the Data Security server.




## Deploying in inline configuration

In inline/bridge mode, configure the protector as a layer-2 switch directly in the path of your organization's traffic. In this configuration, the data security device functions passively, monitoring the traffic (as in monitoring mode), or actively, blocking traffic as necessary.

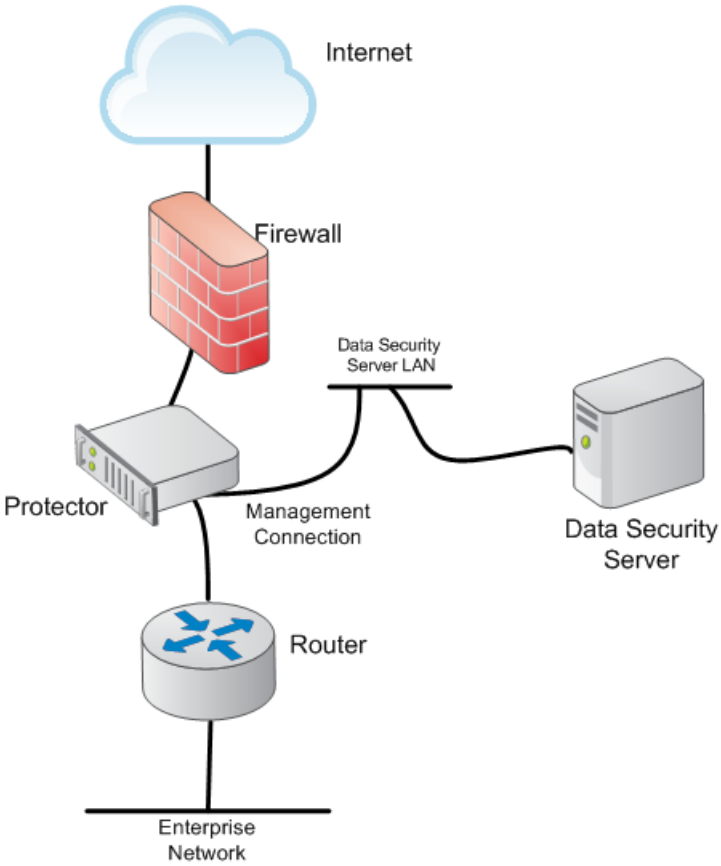
When using the Websense Protector in inline mode, the hardware and software failsafe mechanism is available only when using the certified bypass-server adapter NIC.

The following Silicom network cards (NIC SKUs) are supported by the Websense Protector:

- PEG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI Express Bypass Server Adapter
- PEG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI Express Bypass Server Adapter
- PXG4BPi - Intel-based Quad-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter
- PXG2BPi - Intel-based Dual-Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter

The inline/bridge network setup is the same, regardless of whether the protector is activated in blocking or monitoring mode.

- The following figure depicts a sample setup for the Websense device in inline/ bridge topology.
- Connect the eth0 interface of the protector and the Data Security server to the LAN for management purposes, or use the port set while running the installation wizard.
- Connect the protector to the outgoing connection and to your organization's internal network.




The 2 most common inline (bridge) topologies include:

- HTTP in active (blocking) mode
- HTTP and SMTP in monitoring mode

If you are planning to use one of these modes, when executing the Data Security Protector wizard, make sure the time, date and time zone are precise, and map eth0 to verify it is located on the main board. Connect eth0 of the protector to the LAN.

In inline network configuration, the protector can monitor or block traffic. Monitoring bridge mode monitors traffic. SMTP MTA and HTTP Active Bridge modes have both monitoring and blocking options.

### Inline monitoring

In inline monitoring mode, the protector actually sits in the data path on the network—however, data is monitored and not blocked. This mode is particularly useful during the setup phase, when testing the protector to make sure configuration is accurate and network-appropriate, before enabling blocking capabilities on the network.

### Inline blocking

In inline blocking mode (also known as active bridge mode), the protector sits in the data path on the network. All traffic that traverses the protector is analyzed either locally by the policy engine resident on the protector, or by a Data Security server if load balancing is set up.

The policy engine applies all policies as necessary before determining whether traffic is forwarded to its original destination. If data is detected that is supposed to be blocked, it is quarantined by the protector and does not reach its destinations. All traffic that does not match a policy and is not considered suspicious by the policy engine is forwarded by the protector to its original destination.

The protector communicates with the Data Security server for management purposes as well as for fingerprinting and deployment updates.

## Installing the protector

Installing the Data Security protector comprises 3 basic steps:

1. *Configuring the network*, page 481
2. *Installing the protector software*, page 482
3. Configure the protector in the TRITON Unified Security Center. See *Final step: Verification*, page 487.

### Configuring the network

The following preparatory steps must be taken for the protector to be integrated into your network.

Make sure that firewalls or other access control devices on your network do not block ports used by the protector to communicate with the Data Security server (see*Default ports*, page 927).

When installing the protector device in the network, both incoming and outgoing traffic (in the monitored segment) must be visible.

In some cases, incoming traffic from the Internet and outgoing traffic to the Internet are on separate links. In this case, the mirror port must be configured to send traffic from both links to the protector. The protector needs to have access to the Data Security Management Server and vice versa.

## Installing the protector software

You access the installation wizard for your protector through a command line interpreter (CLI). To install the protector software, do the following:

1. If you have purchased the Websense V5000 G2 Data Security Appliance (v7.6.3 and later), follow the instructions on its quick start poster to rack, cable, and power on the appliance.
2. If you are using your own hardware:
   a. Use either a direct terminal or connect via serial port to access the command line.

      For serial port connection, configure your terminal application, such as HyperTerminal or TeraTerm, as follows:

      - 19200 baud
      - 8 data bits
      - no parity
      - 1 stop bit
      - no flow control

   b. The protector software is provided on an ISO image. Download the image, **WebsenseDataSecurityProtector76x.iso**, from MyWebsense and burn it to a CD.

   c. Place the CD in the protector's CD drive and restart the machine.

   d. An installer page appears. If you are using a regular keyboard and screen, type **kvm** and press **Enter**. If you are using a serial console, press **Enter**. The machine is automatically restarted.
3. You are prompted to enter a user name and password. Enter *admin* for both.

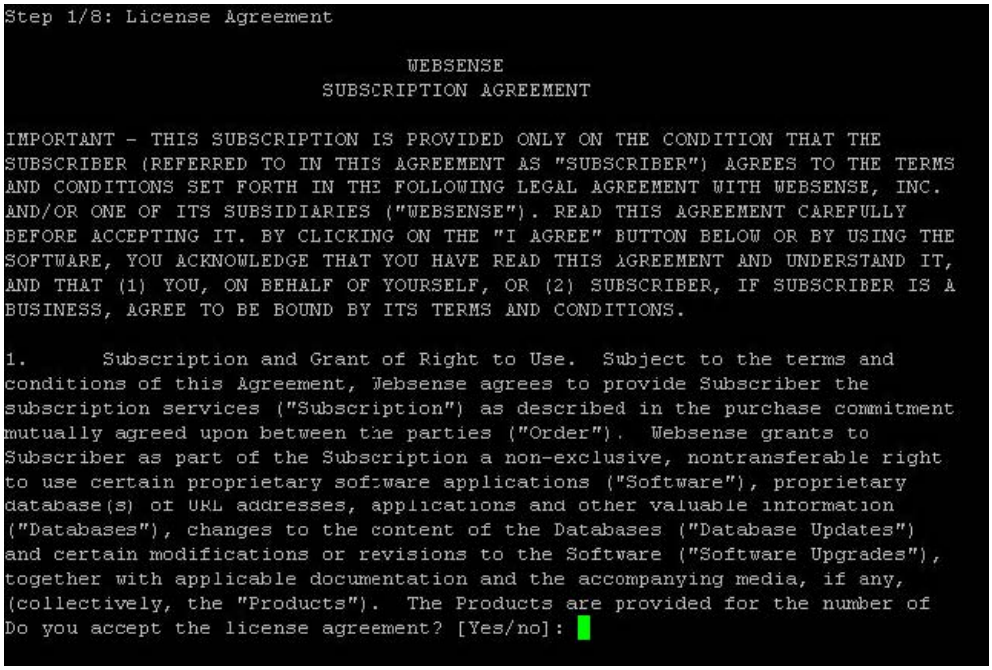
   When the protector CLI opens for the first time, logging in as admin automatically opens the installation wizard. On subsequent attempts, type "wizard" at the command prompt to access the wizard.
4. You have the option to install the Websense protector software or mobile agent software. Type **P** for Protector. Choose this mode whether you are deploying the protector inline or in a SPAN/mirror port configuration. For more information on deploying the protector inline, see *Deploying in inline configuration*, page 478. For more information on deploying the protector in a SPAN/mirror port configuration, see *Deploying in SPAN/mirror port configuration*, page 478.
5. Follow the instructions given by the wizard to configure basic settings.

   When the wizard requires data entry, it prompts you. In some cases, a default setting is provided (shown within brackets [ ]). If the default setting is acceptable, press <**Enter**> to keep the default value.

### STEP 1: Accept license agreement

Each time the installation wizard opens, the end-user license agreement appears. Use the page-down/ scroll /space keys to read/scroll to the end of the agreement. Carefully

read the license agreement, and when prompted, type **yes** to accept the license agreement.




### STEP 2: Select the hardware to install and confirm hardware requirements

Data Security checks to see if your hardware meets the following requirements:

- 2 GB RAM
- 4 CPU
- CPU with more than 2MB of cache
- CPU speed of 8000 bogomips
- Partition "/opt/websense/data" should have at least 45 GB

If your requirements are substandard, you're asked if you want to continue.

### STEP 3: Set administrator password

1. Type in and confirm a new password for the "admin" account. For security reasons, it is best practice to change the default password.

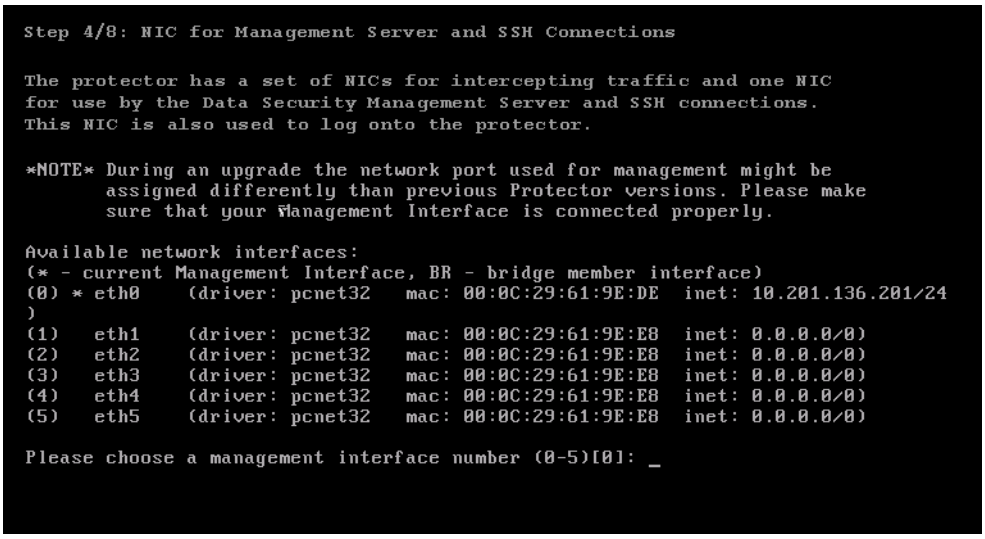
2. Type in and confirm a new Root ("root") Password (mandatory). The root account provides full access to the device and should be used carefully.


### STEP 4: Set the NIC for management server and SSH connections

A list of available network interfaces (NICs) appears. In this step, choose the NIC for use by the Data Security Management Server, SSH connections, and logging onto the protector (eth0 by default). All other NICs will be used for intercepting traffic.

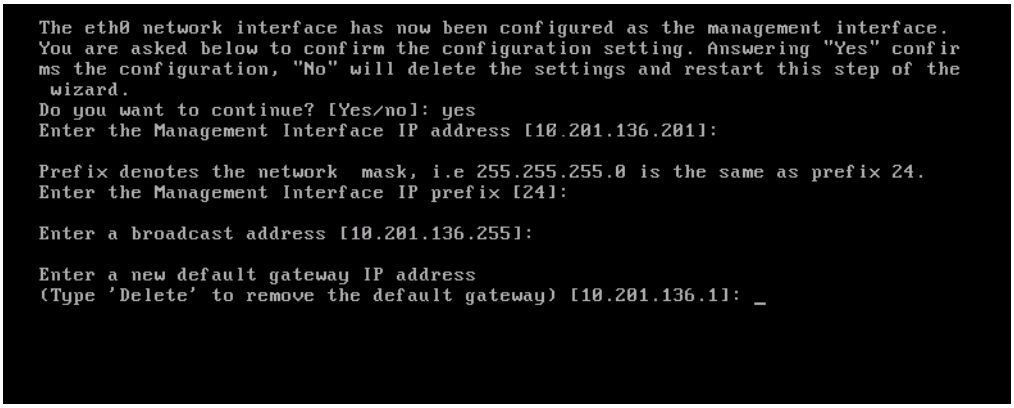
To help you identify which NIC to use, the wizard can simulate traffic for 0-60 seconds and cause LEDs to blink on that port. This does not work for all hardware and drivers.

1. Enter a number 0-60 to indicate how long (in seconds) you'd like traffic simulated or press **Enter** to skip this step.
2. When prompted, choose the NIC index number of the management NIC or accept the default interface.



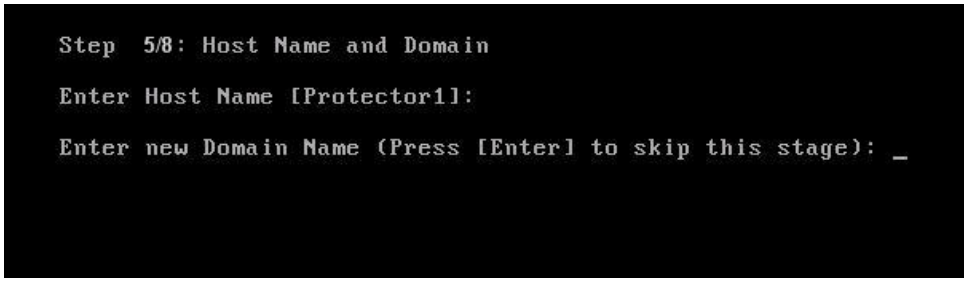

3. Type the IP address of the NIC you've chosen. The default is 192.168.1.1.
4. Type the IP prefix of this NIC. This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 24 (255.255.255.0).
5. Type a broadcast address for the NIC. The installation wizard will provide a calculated value, which is normally the desired one.

6. Type the IP address of the default gateway to be used to access the network. If the IP address of the Data Security server is not on the same subnet as the protector, a default gateway is required to tell the protector how to communicate with the Data Security server.




### STEP 5: Define the host name and domain name

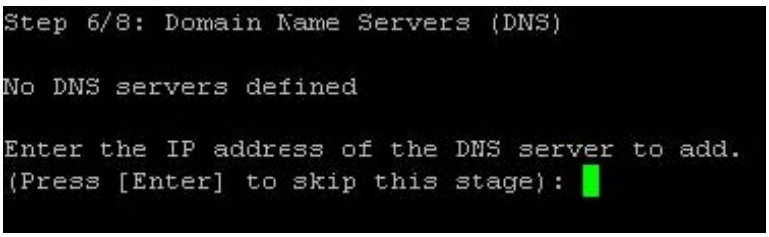
1. Type the host name to be used to identify this protector. The host name should be unique.




2. Optionally, type the domain name of the network into which the protector was added. The domain name set here will be used by the Data Security server when defining the protector's parameters.

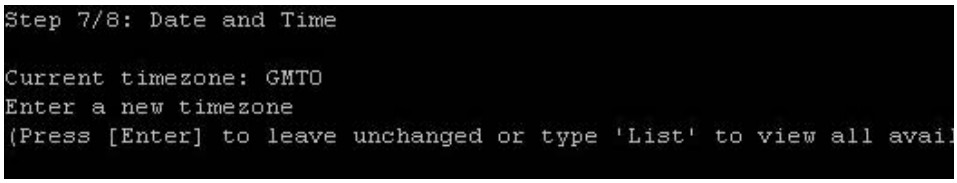
### STEP 6: Define the domain name server

Optionally, type the IP address of the domain name server (DNS) that will service this protector. A DNS will allow access to other network resources using their names instead of their IP addresses.



### STEP 7: Set the date, time and time zone

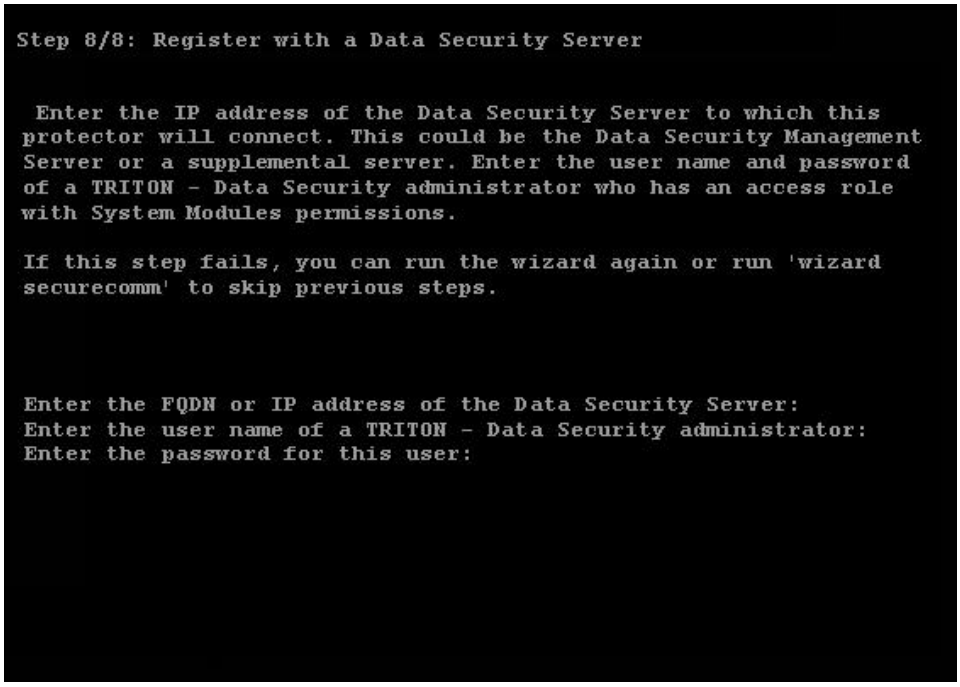
1. Type the current time zone (to view a list of all timezones, type **list**).
2. Type the current date in the following format: dd-mm-yyyy.
3. Type the current time in the following format: HH:MM:SS. Note that this is a 24-hour clock.




### STEP 8: Register with a Data Security Server

In this step, a secure channel will be created connecting the protector to a Data Security Server. This can be the Data Security Management Server or a supplemental server, depending on your set up.

1. Type the IP address or FQDN of the Data Security Server. Note that this must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.



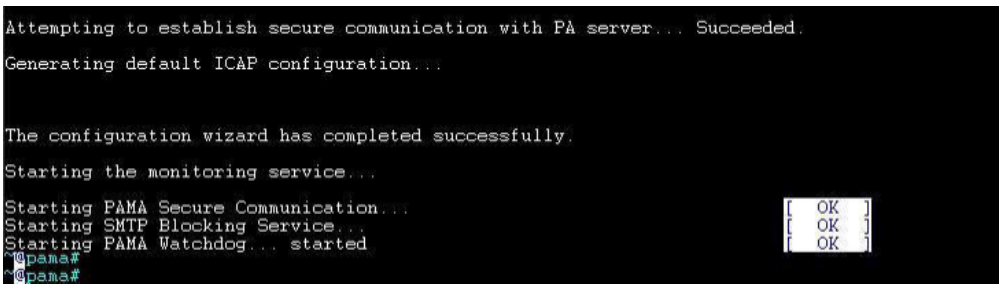

2. Type the user name and password for a TRITON - Data Security administrator that has privileges to manage system modules.

### Final step: Verification

In the Data Security module of TRITON Unified Security Center, verify that the Websense Protector is no longer pending and that the icon displays its active status. Refresh the browser.

Click **Deploy**.

In the protector command-line interface, the following appears:




The protector is now ready to be configured. See *Initial Configuration*, page 763 for instructions.

## Configuring the protector

To begin monitoring the network for sensitive information loss, you must perform some configuration in the TRITON - Data Security user interface. See the TRITON Unified Security Center Help system for instructions on logging on.

Once logged on, navigate to **Settings > Deployment > System Modules** and double-click the installed protector.

- Define the channels that the Websense Protector will monitor.
- Supply additional configuration parameters needed by the Websense Data Security Server to define policies for unauthorized traffic.

When you are done, make sure the protector does not have the status **Disabled** or **Pending**. You can view its status by looking at the System Modules page.

For more configuration information, see “Configuring the protector” in the TRITON - Data Security Help system.

For instructions on configuring the protector for SMTP in monitoring bridge mode or MTA mode, see *Using the protector*, page 521.

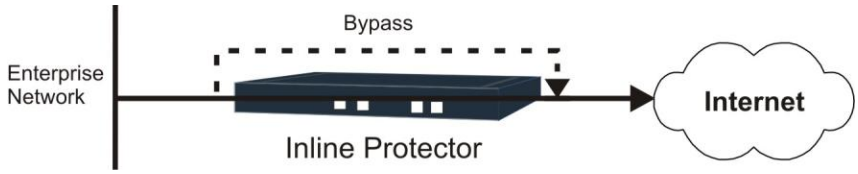
### Setting up Bypass mode

**Bypass** can be used in the event that the Bypass Server Adapter NIC was ordered with the protector; it enables transparent failover in the event of protector failure. When Bypass is enabled, if the protector malfunctions or is powered off, traffic will

transparently pass through the protector to the external network. (Bypass mode is relevant only to the inline/bridge network topology.)

> **Important**
> Only certified Bypass Server Adapter NIC cards are tested and guaranteed to properly bypass the protector in the unlikely event of product failure.

When a certified Bypass Server Adapter NIC dual or quad network card is available on the protector, it's possible to enable the protector's bypass mode. Bypass is a failsafe mechanism that shorts the protector in the unlikely event of device failure, enabling all network traffic to pass transparently through the protector to the network.




You configure bypass mode in the TRITON - Data Security user interface. Select **Settings** > **Configuration** > **System Modules**. Select the protector, then navigate to the Networking tab and select **Enable bypass mode**. Refer to the TRITON - Data Security Help system for more details.

By default, **Bypass Mode** is enabled. This means that when either a software or hardware problem occurs that causes the protector to malfunction, the protector will automatically be bypassed and the (unanalyzed) traffic will continue to pass to the outside network. If Bypass is disabled, when a malfunction occurs **all** traffic will be blocked and won't reach its intended destination.

### Manual bypass

To force the protector into bypass mode, causing all traffic to pass transparently through the protector, do the following:

1. Log onto TRITON - Data Security.
2. Select **Settings > Deployment > System Modules**.
3. Select the protector to bypass.
4. In the Edit Protector dialog, select the **Networking** tab.
5. Under Network Interfaces, click **Edit**.
6. Select the check box labeled, **Enable bypass mode**.
7. Select **Force bypass**.
8. Click **OK** twice.
9. Click **Deploy**.

If you are experiencing network problems, you can verify that problems are not within the Data Security software, by setting Manual Bypass to On and noting if problems persist.

# Mobile agent

## Applies to

- Data Security v7.6.3 and beyond

## In this topic



## Overview

The mobile agent is a Linux-based appliance that lets you secure the type of email content that is synchronized to users' mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks.

The mobile agent analyzes content when users synchronize their mobile devices to your organization's Exchange server. If content or data being pushed to their device breaches the organization's mobile DLP policy, it is quarantined or permitted accordingly.

## Deploying the mobile agent

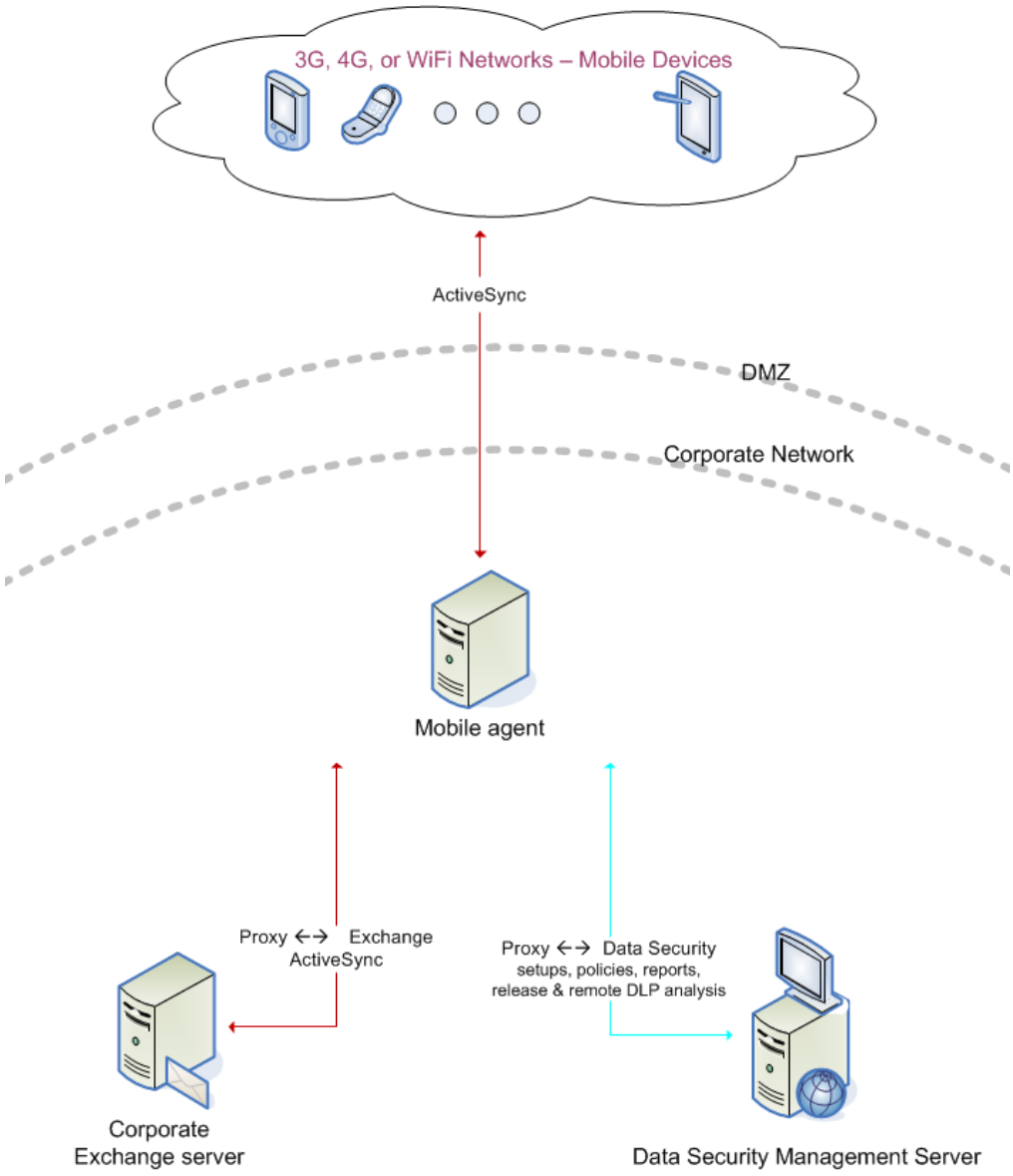
In your network, the appliance connects to the Data Security Management Server and to your Microsoft Exchange agent to provide this function. DLP analysis is done on the appliance or on other Data Security servers (rather than on the management server) to optimize performance and balance the load.

Outside your DMZ, the mobile agent connects to any Microsoft ActiveSync-compatible mobile device over 3G and wireless networks, such as i-pads, Android mobile phones, and i-phones. (ActiveSync is a wireless communication protocol used to push resources, such as email, from applications to mobile devices.)

Unlike the protector, the mobile agent appliance acts as a reverse proxy, because it retrieves resources, such as email, from the Exchange server on behalf of the mobile device.

The following diagram illustrates the system architecture of a typical mobile agent deployment. Depending on your network and security requirements, you can also go

through an edge device, such as a Microsoft ISA Server, that acts as a reverse proxy to the mobile agent.




For system requirements, see *Mobile Agent hardware requirements*, page 53.

For the default port numbers used by the mobile agent, see *Default ports*, page 927. If you have a security policy in place, exclude these ports from that policy so the mobile agent can operate properly. You can lock down or harden your security systems once these ports are open.

Deploying the Data Security mobile agent comprises the following basic steps:

1. *Installing the mobile agent software*, page 491
2. *Configuring the mobile agent*, page 501
3. *Configuring a mobile DLP policy*, page 503

## Installing the mobile agent software

The mobile agent must be installed on hardware that meets the requirements described in *Mobile Agent hardware requirements*, page 53. Websense appliances meet these requirements, or you can host the agent on your own Linux-based hardware.

> **Note**
> For best performance, make sure that the mobile agent is located in close proximity to the back-end server.

You access the installation wizard for your mobile agent through a putty Command Line Interface (CLI).

To install the mobile agent, do the following:

1. If you have purchased the Websense V5000 G2 Data Security Appliance (v7.6.3 and later), follow the instructions on its quick start poster to rack, cable, and power on the appliance.

   If you are using your own hardware:

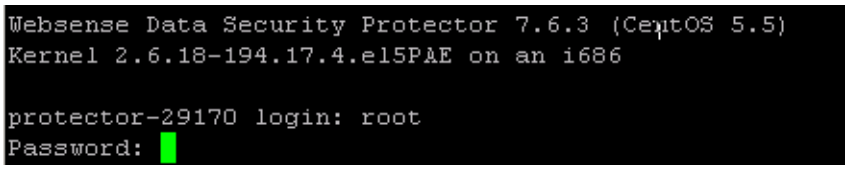
   a. Use either a direct terminal or connect via serial port to access the command line. For serial port connection, configure your terminal application, such as HyperTerminal or TeraTerm, as follows:
      - 19200 baud
      - 8 data bits
      - no parity
      - 1 stop bit
      - no flow control

   b. The mobile agent software is provided on an ISO image. Download the image, **WebsenseDataSecurityProtector76x.iso**, from MyWebsense and burn it to a CD.

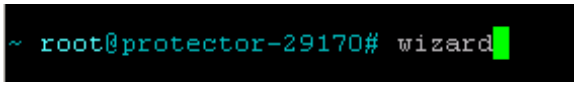
   c. Place the CD in the protector's CD drive and restart the machine.

   d. An installer page appears. If you are using a regular keyboard and screen, type **kvm** and press **Enter**. If you are using a serial console, press **Enter**. The machine is automatically restarted.

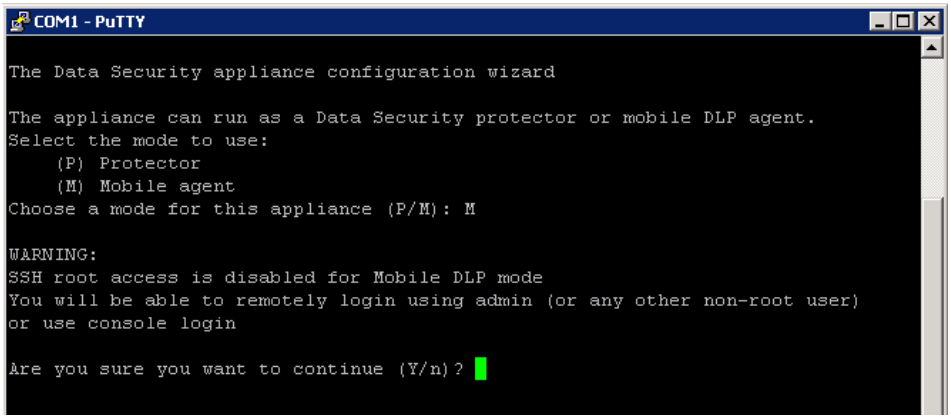
2. You're prompted to enter a user name and password. Enter *root* for user name and *admin* for password.



3. To access the wizard, type “wizard” at the command prompt, and press **Enter**.




4. You have the option to install the Websense protector software or mobile agent software. Type **M** for Mobile agent.




5. Follow the instructions given by the wizard to configure basic settings.

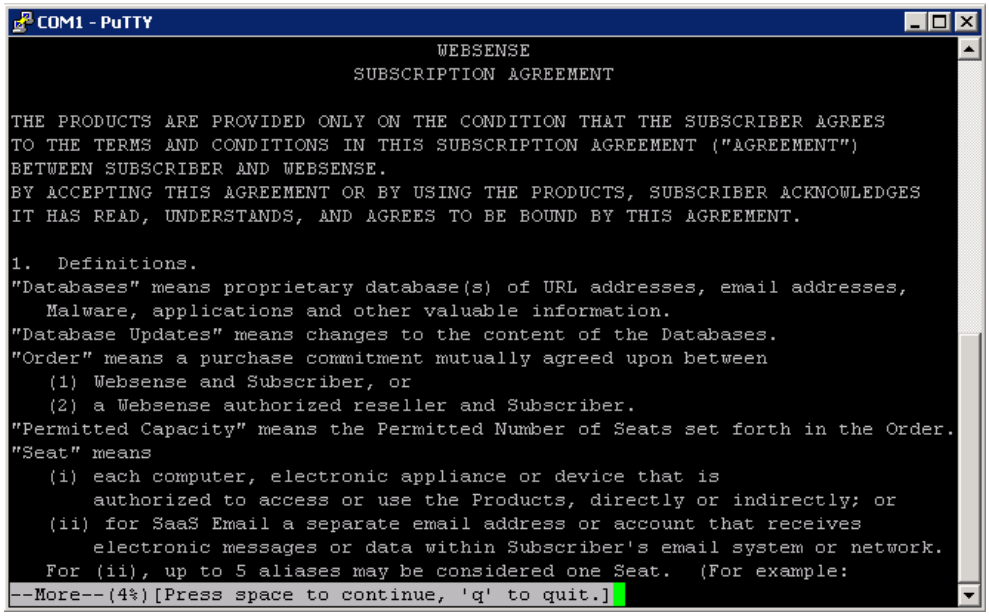
   When the wizard requires data entry, it prompts you. In some cases, a default setting is provided:

   - **Capital letter:** Shows the default value, such as Yes/no for a yes/No prompt.
   - **Square brackets ([ ]):** Shows the current value and is usually followed by text, such as: Press [Enter] to leave as is.

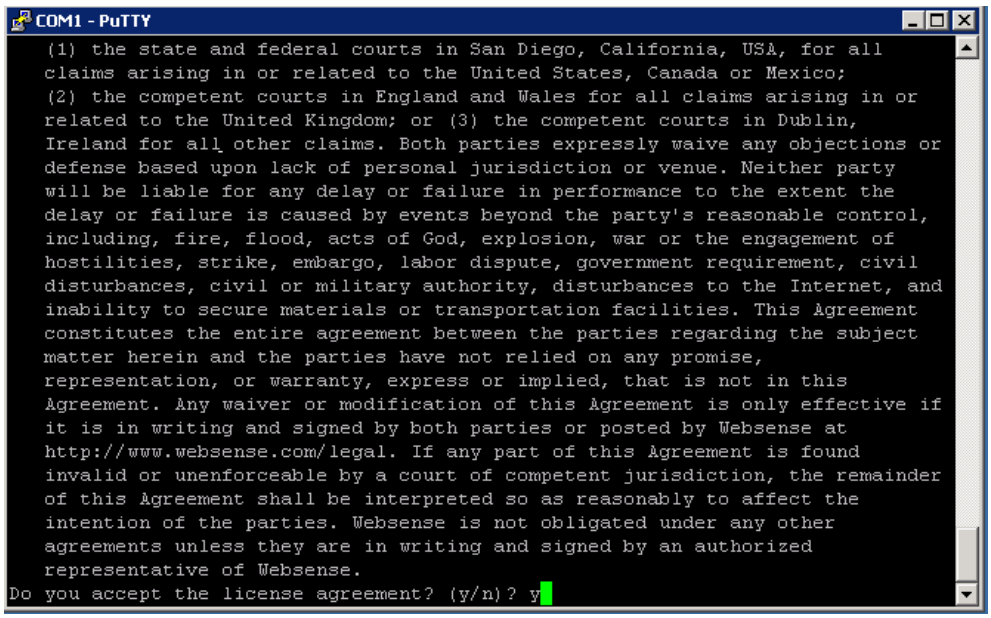
   If the default setting is acceptable, press **<Enter>** to keep the default value.

### STEP 1: Accept license agreement

Each time the installation wizard opens, the end-user license agreement appears. Use the page-down/ scroll / space keys to read/scroll to the end of the agreement.

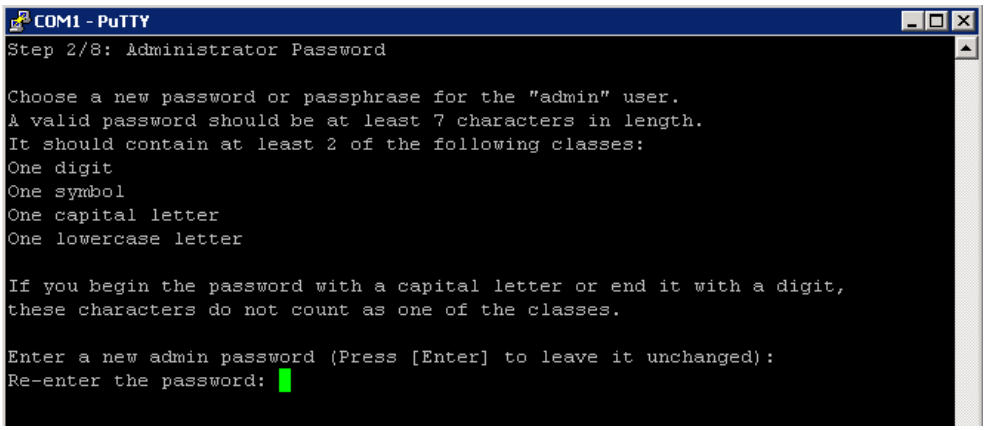



Carefully read the license agreement and when prompted, type **yes** to accept the license agreement.



### STEP 2: Set administrator password

Type in and confirm a new password for the “admin” account. For security reasons, it is best practice to change the default password.




**Important**

A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

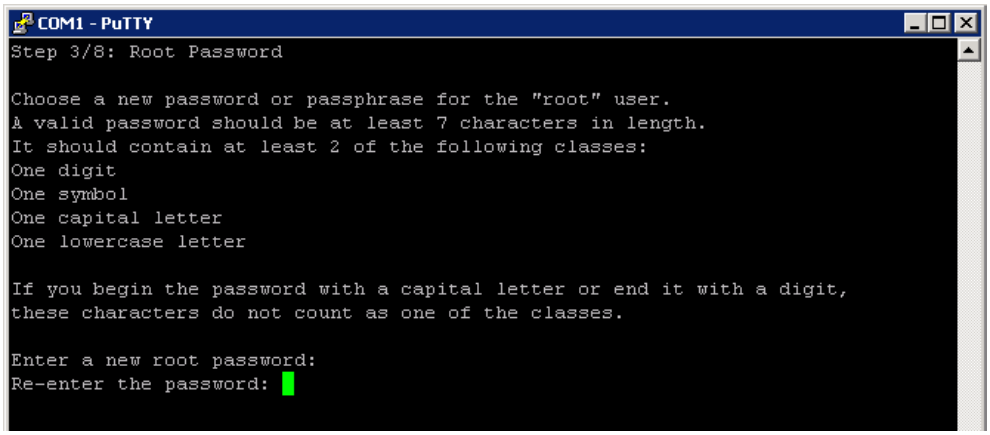
- One digit
- One symbol
- One capital letter
- One lowercase letter

If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

The Operating System (OS) prompts you to change (refresh) your password every 90 days.

### STEP 3: Set root password

Type in and confirm a new password for the root user. The root account provides full access to the device and should be used carefully.




**Important**

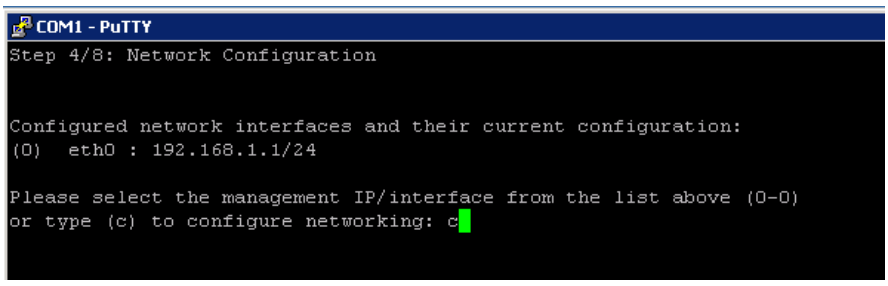
A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

- One digit
- One symbol
- One capital letter
- One lowercase letter

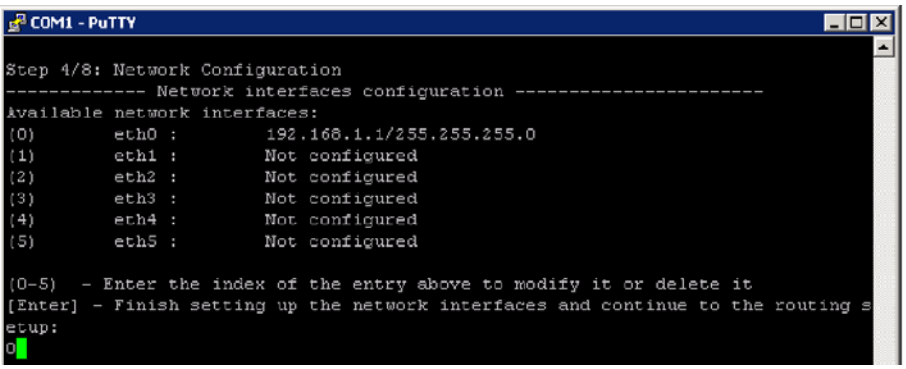
If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

### STEP 4: Network configuration

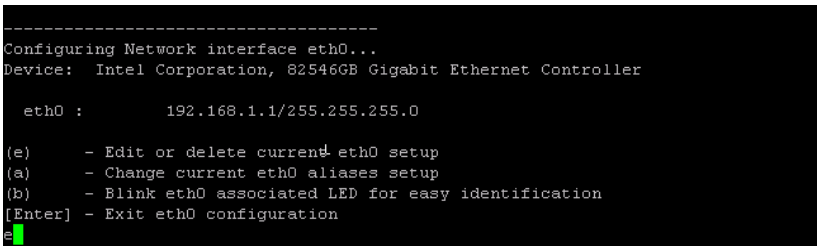
1. Select the network interface (NIC) from the list of available NICs (eth0 by default), or for advanced configuration, type **c**.



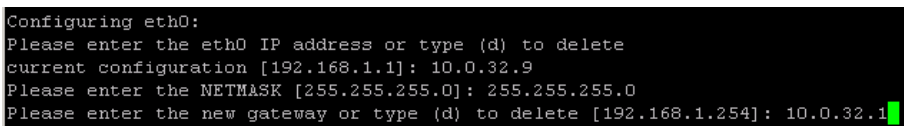
2. To configure your NIC, choose the NIC index number from the list of NICs that display on the wizard.



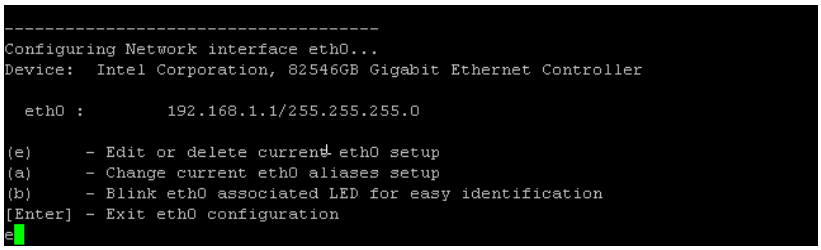

3. To configure the NIC that you selected, do one of the following:
   a. Type **e** to configure the NIC that you selected. You are prompted to define details for the NIC, such as IP address, network address, and gateway (only for the first NIC that you define). You do not need to specify the gateway for subsequent NICs that you want to define.
   b. Type **a** to change the current NIC alias address setup.
   c. Type **b** for LEDs to blink on that port.
   d. Type **Enter** to exit and continue setting other NICs, if required.




4. To define the properties for the NIC:
   a. Type the IP address.
   b. Type the network prefix. This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 255.255.255.0 for eth0.
   c. Type the IP address for the default gateway to be used to access the network. This configuration is only for the first NIC that you configured.

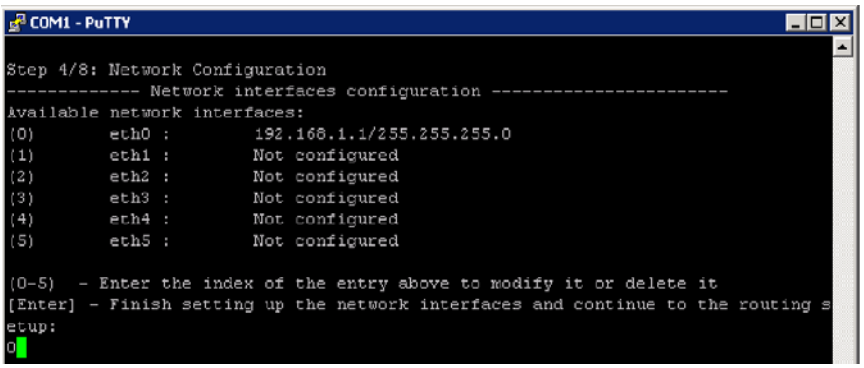


d. After you have configured your NIC, you can redefine it (change the IP address, network prefix, or gateway) or remove it (type **e**, then **d**) if necessary.



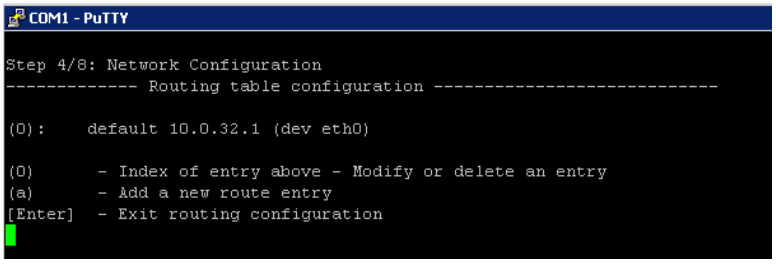

> **Note**
> If you type **Enter**, a list of available NICs display, allowing you to define other NICs.

e. Type a NIC index number to configure another NIC (or reconfigure the same NIC), or type **Enter** to finish setting up the NICs and continue to the routing setup.




f. Type one of the following options:

- **Enter**: Accept the routing configuration.
- **Index**: Modify or delete a routing entry index.
- **a**: Add a routing entry.



**Note**

If the IP address of the Data Security server is not on the same subnet as the one specified for the mobile management NIC, a gateway is required to tell the mobile agent how to communicate with the Data Security server.

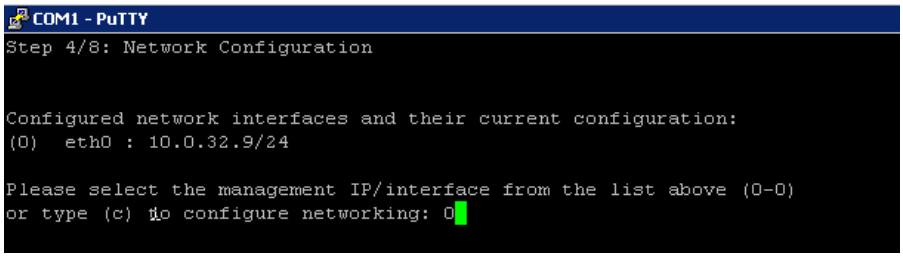
g. To store these network definitions, type **Y**.


**Note**

After you finish routing the configuration, you are prompted to store the network configuration.

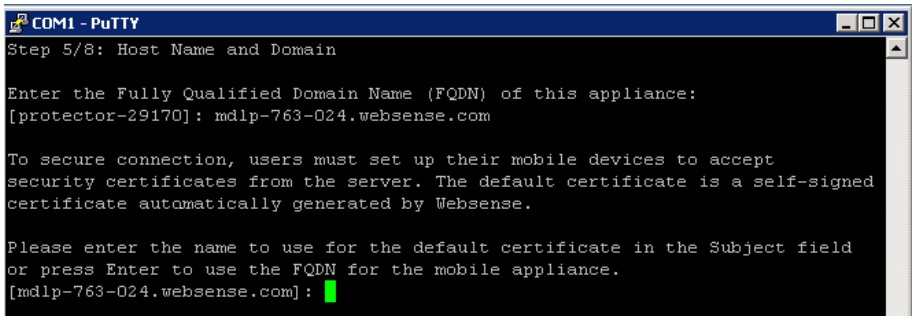
- If you type **n**, the network configuration is not saved, and you are prompted to configure the network again.
- If you type **y**, the details for the network configuration are saved and the network service is reloaded with the new parameters. The new parameters, such as IP address, network prefix, and gateway for the NIC display on the wizard.

5. Type the index number of the Management NIC you have chosen, or type **c** to define the network parameters. This NIC can be used for other purposes, such as SSH connections, access points for mobile devices, and Exchange communications.



### STEP 5: Define the host name

1. Type the Fully Qualified Domain Name (FQDN) for the mobile appliance.

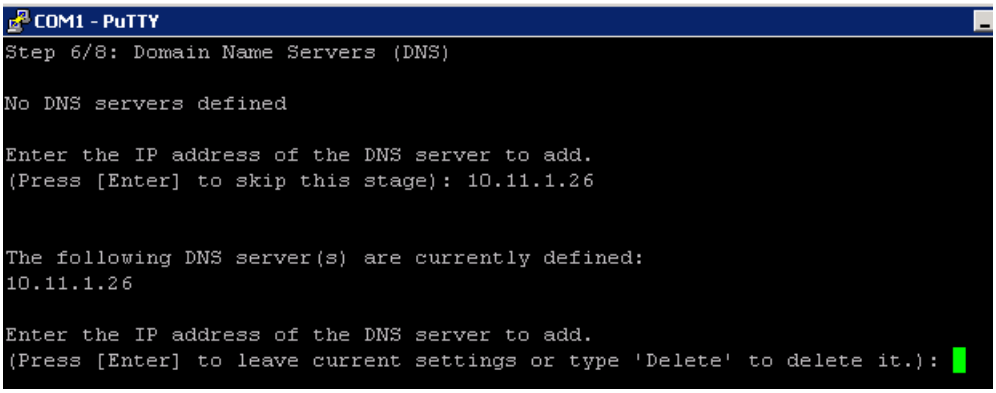



2. Type the name to use for the default security certificate in the **Subject** field.

   This can be used to secure the connections between mobile devices and the mobile agent using the default certificate. The default certificate is a self-signed certificate automatically generated by Websense.

### STEP 6: Define the domain name server

Optionally, in the wizard, type the IP address of the Domain Name Server (DNS) that will service this mobile agent. A DNS will allow access to other network resources using their names instead of their IP addresses.



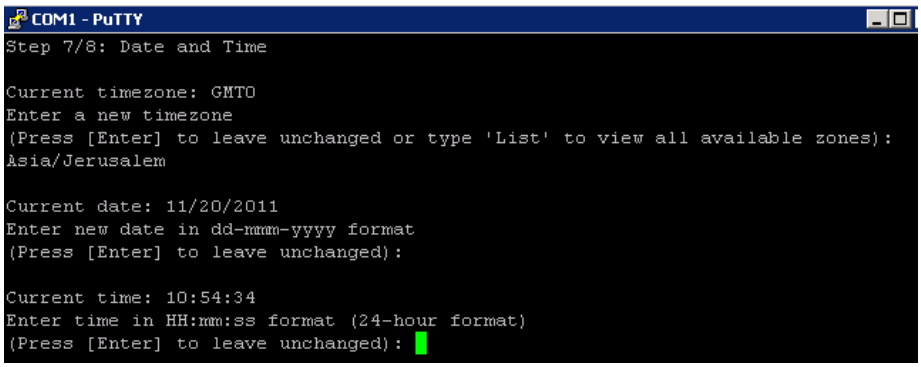

**Important**

Type the IP address of the DNS server if you identify the back-end Exchange server by its host name (using the Data Security GUI) instead of by its IP address.

### STEP 7: Set the date, time and time zone

1. Type the current time zone (to view a list of all time zones, type **list**).
2. Type the current date in the following format: dd-mm-yyyy.

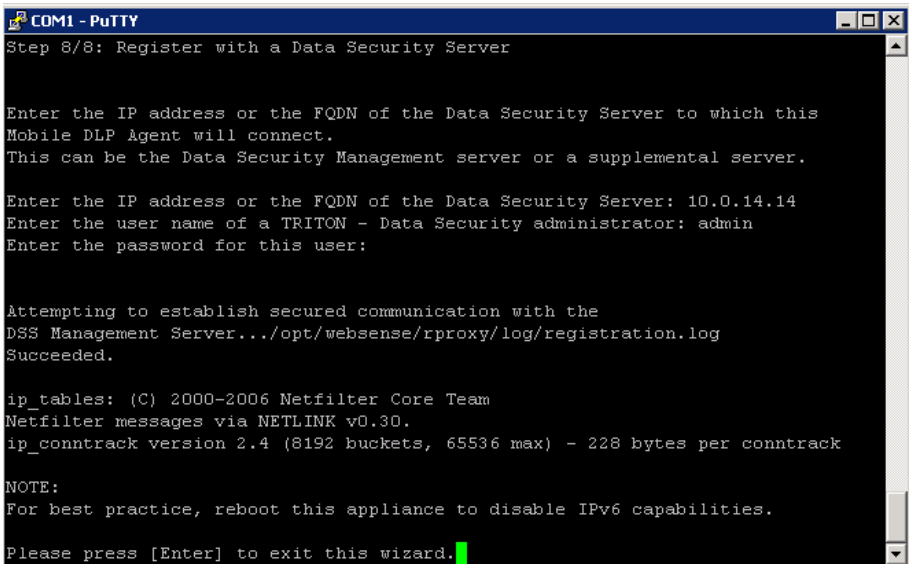
3. Type the current time in the following format: HH:MM:SS. Note that this is a 24-hour clock.




## STEP 8: Register with a Data Security Server

In this step, a secure channel will be created connecting the mobile agent to a Data Security Server. This can be the Data Security Management Server or a supplemental server, depending on your set up.

1. Type the IP address or FQDN of the Data Security Server. Note that this must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.




2. Type the user name and password for a TRITON - Data Security administrator that has privileges to manage system modules.

3. Type **Enter** to exit the wizard. A message displays stating that the configuration was successful.


### Step 9: Reboot the mobile agent appliance

For best practice, reboot the mobile agent appliance. You can reboot later if desired. This completes the IPv6 disabling process that the wizard starts.

### Final step: Verification

In the Data Security module of TRITON Unified Security Center, verify that the Websense mobile agent is no longer pending and that the icon displays its active status. Refresh the browser.

Click **Deploy**.

The mobile agent is now ready to be configured. See *Configuring the mobile agent*, page 501 for instructions.

> **Note**
> If you reboot, make sure that the mobile agent appliance is on before you configure the mobile agent.

## Configuring the mobile agent

1. Log on to TRITON - Data Security.
2. Navigate to **Settings > Deployment > System Modules**.
3. Verify that the mobile agent is available on the **System Modules** page.
4. Double-click **Mobile agent**.
5. Click the **Connection** tab, then define the connections: **Exchange** and **Mobile Devices.** For more information, see the TRITON - Data Security Help.
   a. For **Exchange Connection**, supply the domain and name or IP address of the Exchange server. Ensure a port number is specified.
      - If you select the**Use secure connection (SSL)** check box, the port number defaults to 443.

- If you do not select the **Use secure connection (SSL)** check box, the port number defaults to 80.

> **Important**
> If the Exchange server is specified by name, make sure local resolving is properly configured to resolve this name. In addition, if an edge-like device is used (for example, ISA), ensure there are no loops through the device.

b. For **Mobile Devices Connection**, supply the following information: IP address of the mobile agent and port number. To use all IP addresses, select **All IP addresses** from the **IP address** drop-down list.

> **Note**
> The IP address of the mobile agent was defined during the installation of the mobile device, when configuring the network settings.

6. Optionally, if you secure connections between mobile devices and the mobile agent, you can use one of 2 certificate options:
   - **Self-signed certificate** (default option)
     - A self-signed certificate is signed by Websense.
   - **Custom certificate**
     - A custom certificate is officially signed by a Certificate Authority (CA).

     a. Click **Browse** to locate and upload your public certificate.

     b. Click **Browse** to locate and upload your private key.

     c. Optionally, select the **Add chained certificate** check box, and click **Browse** to locate and upload your chained certificate.

     For more information, see the TRITON - Data Security Help.

7. Click the **Analysis** tab and then select a mode:**Blocking** or **Monitoring**. Click the **Analysis** tab, then configure the **Mode**.

   **Note**

   When you select Blocking mode, it is best practice to:

   - Select the **Allow on fail** option (the default option is **Block on fail**). Selecting **Allow on fail** enables failed messages to be received on the mobile device. If you do not select **Allow on fail**, these messages will be dropped and are not tracked nor released.
   - Define the sender's email address, outgoing mail server, and port to **Notify Users of Breach**. To do so, navigate to **Settings > System > Alerts > Email Properties**.

   For more information, see TRITON - Data Security Help.

8. Navigate to **Main > Resources > Notifications** and select the mobile policy violation template. Add sender details, then use the**Outgoing mail server** field to define a next hop relay for outbound mail. If you do not, the mobile agent may not send block notifications.
9. Click **Deploy**.

   Wait for the agent to fully deploy. This may take a few minutes.

   **Tip**

   You can also configure the mobile agent for high-availability. High-availability enables mobile devices to run seamlessly and continuously in the event of a system outage (such as hardware or software failure).

   For more information about configuring the mobile agent for high-availability, refer to the document Mobile DLP agent using cluster solutions.

## Configuring a mobile DLP policy

To begin analysis, configure the mobile DLP policy or create a custom policy. To configure the mobile DLP policy, Navigate to **Main > DLP Policies > Mobile DLP Policy**. See TRITON - Data Security Help for more configuration information.

To create a custom policy, navigate to **Main > DLP Policies > Manage Policies**. Select **Mobile Email** on the **Destination** tab for each rule to support Mobile events.

# SMTP agent

## Applies to

- Data Security v7.6.x

## In this topic



## SMTP agent

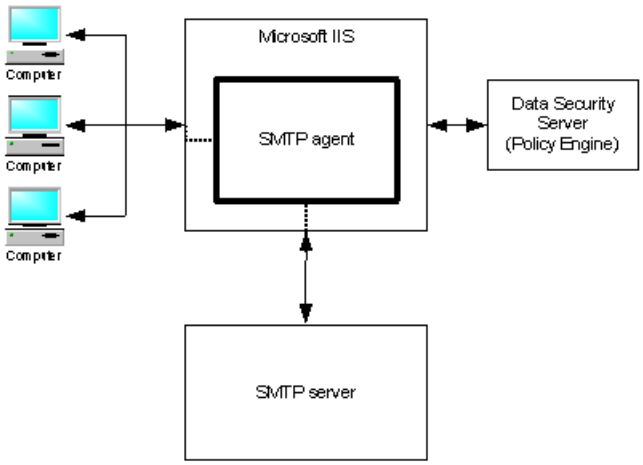
The Websense Data Security SMTP agent is installed on a Data Security server or on another Windows server equipped with Microsoft Internet Information Services (IIS) v6.

The server must be running on the following operating system environments:

- Windows Server 2003 (32-bit)
  - Standard or Enterprise R2
  - Standard or Enterprise R2 SP2
- Windows Server 2003 (64-bit)
  - Standard or Enterprise R2

It receives all outbound email from the mail server and forwards it to a Websense Data Security Policy Engine. The SMTP agent then receives the analyzed email back from the policy engine. Depending on the analysis, SMTP agent blocks the email or forwards it to the mail gateway. When installed on the Data Security Management server or supplemental Data Security server, the SMTP agent uses the local policy engine of those servers to analyze email, unless load balancing has been configured, in

which case it uses the specified policy engine. The SMTP agent supports permit, block, and encrypt actions.




Websense recommends you use the SMTP agent whenever you want the ability to block SMTP traffic in a production environment. (If you need only monitor SMTP traffic, the protector may be a better choice for you.)

To use the SMTP agent, you need to configure your corporate email server to route email to it. (The agent becomes a MTA, accepting responsibility for delivery of mail.)

When the agent is installed on a Data Security server, the SMTP traffic is analyzed by the local policy engine. When it is installed as a stand-alone agent, email messages that are sent to the agent are sent to a Data Security server for analysis (whichever server the SMTP agent is registered with). You can configure Websense Data Security to block or quarantine flagged messages.

If an SMTP email transaction was blocked or quarantined, the administrator responsible for handling this incident can release this incident to those recipients originally blocked from receiving the content.

The SMTP agent is usually not the final server in the chain of custody before the email leaves the enterprise. Email is more frequently passed along to another MTA that provides additional processing (anti-virus scanning, for example).

If you have multiple mail servers, you can deploy multiple SMTP agents or you can have one SMTP agent and configure load balancing between the SMTP agent and the outgoing mail server. If this is not built into your SMTP server, you can use an external load balancer to achieve this.

Install the 32-bit SMTP agent using the Websense installer. See *Installing Data Security Components*, page 692 for more information.

## Installing the 64-bit SMTP agent

A separate 64-bit version of the Websense Data Security Installer is used to install 64-bit SMTP agent.

1. Download **WebsenseDataSecurity760-x64.msi** from www.mywebsense.com to the machine on which you want to install SMTP agent.
2. Launch **WebsenseDataSecurity760-x64.msi**.

   The installer operates identically to the Websense Data Security Installer launched by the Websense installer. The only difference being that the 64-bit installer only installs SMTP or TMG agent.
3. Follow the instructions in *Installing Data Security Components*, page 692 to complete the installation.

   When following those instructions, skip the steps involving the download and launching of the Websense installer. Begin from the point where the Websense Data Security Installer appears.

# Microsoft ISA/TMG agent

## Applies to

- Data Security v7.6.x

## In this topic



## Microsoft ISA/TMG agent

The ISA/TMG agent receives all Web connections from a Microsoft ISA Server or Forefront TMG network and forwards them to the Data Security policy engine. It then receives the analyzed information back from the policy engine and forwards it to the recipients on the Web.

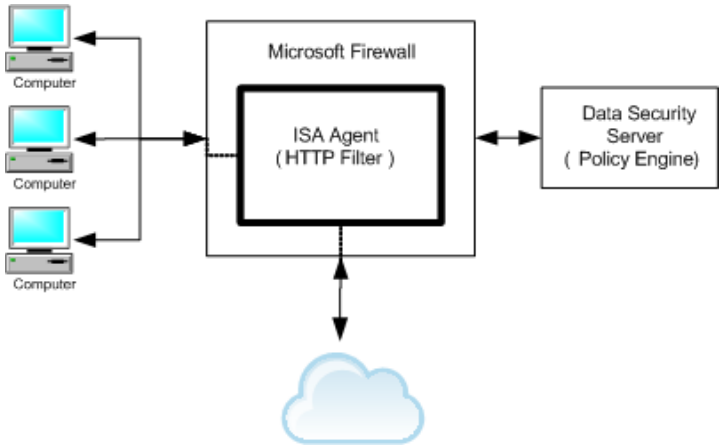
Microsoft ISA 2004 and 2006 are supported on the following operating system environments:

- Windows Server 2003 (32-bit)
  - Standard or Enterprise
  - Standard or Enterprise R2
  - Standard or Enterprise R2 SP2
- Windows Server 2003 (64-bit)
  - Standard or Enterprise R2

Forefront TMG is also supported, on Windows Server 2008 R2 platforms (64-bit). Note that Forefront TMG supports analysis of HTTPS traffic as well as HTTP.

The ISA/TMG agent supports the permit and block actions, and it receives authentication information from the client on its way to the proxy to identify users.

If you are using the ISA agent on an ISA array, be sure to install it on every member of the array; otherwise the configuration will be out of sync and ISA may become non-functional.




Install ISA agent using the Websense installer. See *Installing Data Security Components*, page 692 for more information.

## Installing the TMG agent

A separate 64-bit version of the Websense Data Security Installer is used to install TMG agent.

1. Download **WebsenseDataSecurity760-x64.msi** from www.mywebsense.com to the machine on which you want to install TMG agent.
2. Launch **WebsenseDataSecurity760-x64.msi**.

   The installer operates identically to the Websense Data Security Installer launched by the Websense installer. The only difference being that the 64-bit installer only installs SMTP or TMG agent.
3. Follow the instructions in *Installing Data Security Components*, page 692 to complete the installation.

   When following those instructions, skip the steps involving the download and launching of the Websense installer. Begin from the point where the Websense Data Security Installer appears.

# Printer agent

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

The Data Security printer agent is required when you want to monitor what is printed on your organization's network printers.

The printer agent supports the following Windows Server 2003 32-bit environments:

- Standard or Enterprise
- Standard or Enterprise R2
- Standard or Enterprise R2 SP2

In addition, it also supports permit and block actions.

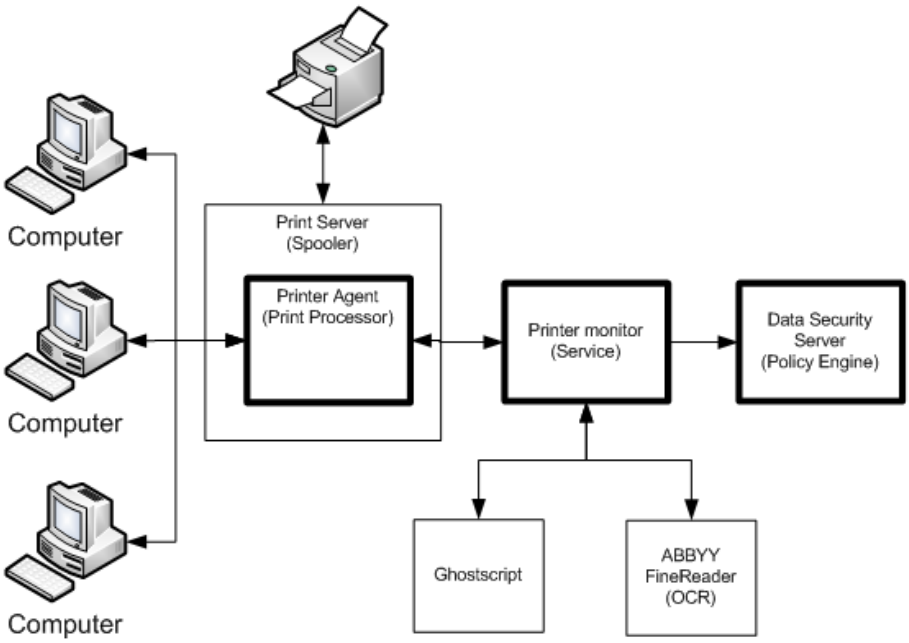
When a user on the network prints a file, it is routed to the Microsoft Windows printer spooler service, where the printer agent intercepts it and sends it to the Data Security policy engine. After analysis of the content, the Data Security system enforces the policy as necessary: either auditing, monitoring or blocking the print job from being printed, in which case the sender (the user who printed the document) receives a notification that the print job was blocked.

The printer agent is capable of identifying the user that submitted the print job, because these credentials are included in the print job.

Websense Data Security generates forensics reports that list the blocked print files along with other blocked transmissions.

You install the printer agent on a Windows print server. It includes optical character recognition (OCR) capabilities. The OCR service (ABBYY FineReader) is required in printer agent installations for better analysis in different printer drivers. Installation without the OCR service is limited and should be performed only after receiving verification from Websense Technical Support that your organization's specific printer driver is supported.

The OCR service enables the recognition and prevention of "corporate-defined" confidential content being printed. The OCR service is required not only to support certain sources, but is also a must when certain printer drivers are used, for example, PCL 6. As a general rule, only standard formats, such as extended meta file (EMF), printer control language (PCL), text (TXT), and postscript (PS) can be received by the printer agent. Nonstandard formats are not supported.




The printer agent is installed using a separate printer agent package (**WebsenseDataSecurityPrinterAgent.zip**) See *Installing the printer agent*, page 509 for instructions.

## Installing the printer agent

There are 2 prerequisites for installing the Data Security printer agent:

- The computer where you're installing the agent must be inside a domain.
- The computer where you're installing the agent must have at least one printer already installed.

If these 2 conditions are not met, the installer doesn't show the option to install the printer agent.

To install the printer agent:

1. Download **WebsenseDataSecurityPrinterAgent.zip** package from www.mywebsense.com.

2. Extract the package to the print spooler machine.

   **Important**
   The package must be extracted to the print spooler machine. Installation must take place on the machine itself for Printer agent to function properly.

3. In the extracted content, open the folder **ABBYY\ABBYY FineReader Engine 8.1**.
4. There should be a subfolder named **Administrator's Guide** (note the apostrophe).

   During extraction, that folder's name can become corrupted. If this has happened, rename the folder to **Administrator's Guide**. Note that in such cases, only the name of the folder is corrupted, the contents are not.
5. Make sure the **DSS-7.6.0-x86.msi** installer is in the same folder as the **ABBYY** and **gs** folders.
6. Run the **DSS-7.6.0-x86.msi** to install Printer agent.

   See *Installing Data Security Components*, page 692 for instructions. Note that those instructions assume you have reached the Websense Data Security installer by launching the general Websense installer. Skip the portions mentioning the Websense installer and follow the instructions relating to the Data Security installer.

## Detecting the printer driver

If you are having difficulty with the recognition and configuring of your printers with the printer agent, you can export the printer registration file to send to Websense Technical Support for analysis. This file indicates printer names and drivers.

**To export printer registration files:**

1. Click **Start > Run** and in the Run dialog, type **regedit**.
2. Click **OK** in the Run dialog. The Registry Editor screen is displayed.
3. In the Registry Editor screen, navigate to the following directory: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers
4. Right-click the Printers folder and select **Export**.
5. Select the desired directory to save the exported (*.reg) file.
6. Click **Save**.
7. Send the exported (*.reg) file to your local Websense technical support representative.

### Alternative detection of printer driver

Alternatively, users may access the following registry key on the print server to detect the printer driver:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Pr
inters\ {Printer Name}\
```

In the registry key, open the printer driver entry and view the string value.

To access the above registry key, refer to *Detecting the printer driver*, steps 1 to 3 above.

## ABBYY FineReader configuration settings for non-English text

If your printers are used for non-English text, you need to make minor modifications to the following ABBYY FineReader configuration files:

- **ExportToTXT-Accurate.ini**
- **ExportToTXT-Fast.ini**

To modify the ABBYY FineReader configuration files:

1. Using Windows Explorer, navigate to the following directory:

   ```
   C:\Program Files\Websense\Data Security\ABBYY\Profiles
   ```

2. Locate the following 2 files: **ExportToTXT-Accurate.ini** and **ExportToTXT-Fast.ini**.
3. Open each of the above **.ini** files in a text-editing application.
4. Locate the [RecognizerParams] section. If it does not exist, create a new section with this name.
5. Add a parameter to the [RecognizerParams] section as follows:

   ```
   [RecognizerParams]
   TextLanguage = English,French
   ```

6. Save the *.ini files.

## Printer agent performance

The printer agent has different demand levels, depending on whether it is in Monitoring or Blocking mode, and whether the OCR service is activated or deactivated.

Monitoring mode operates in an asynchronous manner and therefore, does not introduce analysis time overhead to the printing time.

In Blocking mode, the OCR processing adds up to 3 seconds per page depending on the CPU power of the printer server. You can select Blocking or Monitoring in the Edit Printer Agent window, accessed through **Settings > Deployment > System Modules.** Select the printer agent on the System Modules screen.

Select **Monitoring** if you want to monitor traffic through the print server but not block it.

Select **Blocking** if you want to block actions that breach policy.

# Integration agent

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

The integration agent allows third-party products to send data to Websense Data Security for analysis.

Third parties can package the integration agent inside their own installer using simple, 'industry standard' methods that are completely transparent to end users.

When the third-party product is installed on a users system, it needs to register the integration agent with the Data Security Management Server. This can be done transparently through the installation process or using a command-line utility.

The integration agent works on the following operating systems:

- Windows Server, 32-bit
- Redhat Enterprise Linux

TRITON - Data Security treats third-party products that use the integration agent as it does any other agent.

It supports all relevant views and capabilities, including:

- Incident Management and Reporting
- Quarantine and Release of emails
- Traffic log view
- Load balancing capabilities

The Integration agent does not support discovery transactions.

For information on configuring the integration agent, see “Configuring the integration agent” in the TRITON - Data Security Help system.

# Installing the integration agent

## Installed components

When you embed the integration agent in your product installer, 3 Data Security components are installed on the end-user machine:

- **PEInterface.dll** - A DLL the that interacts with the Data Security policy engine on the management server.
- **ConnectorsAPIClient.exe** - Client software that connects the API in the third-party product with Websense Data Security.
- **registerAgent.bat** (or .vbs) - A script that performs registration with the Data Security Management Server.

## Installation package format

On Windows, the installation package for the integration agent is provided in 2 major formats:

- **MSM file**. The installer that uses the MSM can choose (by setting properties) whether or not to register the product with the Data Security Management Server during installation. The MSM contains a 'custom action' that validates Data Security user names and passwords and can be called by the third-party installer.
- **MSI file**. This file embeds the MSM file. Some parties prefer to work with an MSI, and others can use it as a reference implementation. The MSI installation wizard presents 4 interactive dialogs:
  - **Installation-dir** - installation directory.
  - **Registered Channels** - The DLP channels to use: HTTP, SMTP, Printer, Discovery.
  - **Local IP Address** - which of the static IP addresses currently assigned to the machine should be used for registration.
  - **Data Security Management Server details** - IP address or host name, user name, password.

On Linux, the package is in the form of a relocateable RPM.

# Registering the integration agent

Every instance of the integration agent needs to be registered after being installed. (This is a one time operation.) In other words, every time the third-party product is installed on an end-user machine, that instance of the agent needs to be registered.

The registration operation can be done during the installation by the installer, or using a command-line utility provided with the agent.

The command-line utility should receive the following input arguments:

- **Protocols** - a non-empty list of supported protocols (out of HTTP, SMTP, Printer, Discovery).

- **Data Security Management Server details** - IP address or host name, user name, password.
- **Local IP Address (optional)** - In case this is not supplied, use any of the static addresses of the machine, and print it to the standard output.
- **Search IP Address (optional)** - used for re-registration after IP change. In case this is not supplied, use the address in the**registerAgent.conf** file. If that file does not exist, use the given local IP address.

A successful operation registers the machine with the Data Security Management Server as having the desired protocols and generates certificate files in the same directory that the tool is located. The tool also stored a configuration file (**registerAgent.conf**) with the IP address used for registration.

On failure, the script returns a meaningful exit code and prints an error message to standard output

## Using the Websense Data Security API

Third parties that subscribe to the integration agent use a C-based API to send data to Websense Data Security for analysis and receive dispositions in return.

The API can be used to configure analysis operations on a transaction-by-transaction basis on the following variables:

- Channel/Protocol - Upon installation the third-party product can declare its ability to intercept various protocols, and assign each transaction to a protocol.
- Blocking/Monitoring mode - each transaction can work in a different mode.
- Timeout - can be different per transaction.

For documentation on the Data Security API, consult with your Websense Sales representative.

# The crawler

## Applies to

- Data Security v7.6.x

## In this topic

## Overview

The crawler is the name of the discovery and fingerprinting agent. It is selected by default when you install the Data Security Management Server or supplemental Data Security servers.

You can deploy additional crawlers in your network if you desire. When you set up a fingerprint task, you indicate which crawler should perform the scan. Websense recommends that you use the crawler that is located closest to the data you are scanning.

You can view the status of your crawlers in the TRITON - Data Security user interface. Go to **Settings > Deployment > System Modules**, select the crawler and click on the **Edit** button.

## Installing the crawler agent

To install the crawler agent, use the Websense installer. See *Installing Data Security Components*, page 692 for instructions. To complete the process, you must deploy the agent in the TRITON - Data Security user interface.

For information on configure the crawler, see "Configuring the crawler" in the TRITON - Data Security Help system.

# Troubleshooting Data Security agent deployment

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

Though the installation and deployment of agents is normally a series of clear-cut steps, occasionally, some problems can arise. Below are how to resolve common problem scenarios.

## Initial registration fails

- Make sure you can ping the Data Security agents by IP and by host name from the TRITON Management Server.
  - On Windows, run the following command (in a Command Prompt) to check for block ports:

    netstat 1 -na | find "SYN"

    Each line displayed in response to the command is a blocked port. This command is one-way. Run it on both the agent machine and the TRITON Management Server.
- Check the service log on the TRITON Management Server (and remote policy engines).
- Check /opt/websense/neti/log on the protector.
- Make sure no duplicate certificates are installed on the agents' servers; if there are duplications, delete all of them and re-register the agent. Also, make sure the system date/time of the agent machine and the TRITON Management Server are the same. The following certificates are expected:

  **Certificate > My User Account > Trusted Root Certification Authorities > Certificates > ws-ilp-ca**

  **Certificates > Computer > Personal Certificates ><servername>(issued by ws-ilp-ca)**

  **Certificates > Computer > Trusted Root Certification Authorities > Certificates > ws-ilp-ca**
- Make sure the FQDN value of the agent states the full server name for the agent's server.

  Protector — if domain name is configured, the FQDN is: protectorname.domain.name

  Agents and Data Security server — check "My Computer" properties and copy the computer name value from there.

## Deploy settings fails

- Make sure you can ping the agents by IP and by host name from the TRITON Management Server.
- Check the service log on the TRITON Management Server (and remote policy engines).
- Check the plat.log on the protector.

## Subscription errors

- Restart the Websense TRITON - Data Security service on the TRITON Management Server.
- Check dlp-all.log.

## Network connectivity problems

In complex networks, network connectivity may require routes added to the inline protector.

Although routes can be added with the built in kernel route command, it is strongly recommended that the /opt/websense/neti/bin/route command is used instead. If the kernel route (/sbin/route) is used, the added routes will be lost after rebooting.

/opt/websense/neti/bin/route writes the routes to a file /opt/pa/conf/route so that on subsequent reboots the route information is re-submitted to the protector.
Usage:

```
route: Add/delete routing information
```

Usage:

```
route [list]
route add {destination network | destination ip} {via
{ip}|dev {device}}
route del {destination network | destination ip} {via
{ip}|dev {device}}

network=ip/prefix
```

Example:

```
~@protector7# /opt/websense/neti/bin/route add 192.168.1.0/
24 via 10.212.254.254 dev br0
~@protector7# /opt/websense/neti/bin/route list
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.1.0 10.212.254.254 255.255.255.0 UG 0 0 0 br0
10.212.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
10.212.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br0
0.0.0.0 10.212.254.254 0.0.0.0 UG 0 0 0 eth0
```

# 34 Integrating Data Security with Existing Infrastructure

## Applies to

- Data Security v7.6.x

## Integrating Data Security with existing infrastructure

Websense Data Security is an integral piece of your network architecture, and can be combined with your existing systems to ensure seamless Web and email protection. See the following for information about integrating Websense Data Security with existing systems.



## Working with existing email infrastructure

### Applies to

- Data Security v7.6.x

### In this topic

## Overview

You can configure Websense Data Security within your existing email infrastructure to block and quarantine email that contravenes your policies.

You can do this by connecting Websense Email Security Gateway, the SMTP agent, or the Websense protector to the network directly in the path of the traffic, enabling traffic to be not only monitored, but also blocked, quarantined, or even terminated before it reaches its destination.

This section describes the SMTP agent and protector. For information on using Email Security Gateway, see *Email Security Gateway (V10000 G2)*, page 585 or *Email Security Gateway (V5000 G2)*, page 575.

## Using the SMTP agent

If you want the option to block email that breaches policy, the SMTP agent is the easiest deployment option to configure, monitor, and debug in a production email environment. Do the following to set up the SMTP agent within your email infrastructure for this purpose:

1. Run the Websense installer as described in *Installing Data Security Components*, page 692. You can install the SMTP agent on a TRITON Management Server, supplemental Data Security server, or as a stand-alone agent on another Windows server machine equipped with Microsoft IIS.
2. To configure the SMTP agent, in TRITON - Data Security, select **Settings** > **Deployment** > **System Modules**. Select the SMTP agent.
3. Complete the fields as follows:
   - In the **General** tab:
     - Set the **Mode** to **Blocking**.
     - Specify the action to take when an unspecified error occurs.
   - In the **SMTP Filter** tab:
     - Select the **Enable filtering on the following internal email domains** check box.
     - Enter the domain name(s) to monitor and click **Add**.
   - In the **Encryption & Bypass** tab:
     - If you want encrypted or flagged email to bypass analysis, select the **Enable redirection gateway** check box, then enter the redirection gateway IP and port. Specify the encryption and/or bypass flags to use.
   - In the **Advanced** tab:
     - Specify the footer to add to analyzed email, if any.
   - Click **OK** to save all the above settings.
4. Select **Main** > **Policy Management** > **DLP Policies**. Select the policy rule that you wish to use for email management and click **Edit**.
5. Complete the fields as follows:

- Select **Destinations**, and check the **Network Email** box.
- Select **Severity & Action**, then select an action plan that includes notifications.

6. Click **Deploy** to activate the settings.
7. Configure your corporate email server to route email to the SMTP agent. (The agent becomes a MTA.)

## Using the protector

There are 2 different SMTP modes:

- Monitoring mode (sometimes referred to as passive mode)
- Explicit Mail Transfer Agent (MTA) mode

In monitoring mode, the protector monitors and analyzes SMTP traffic, but does not enable policies to block transactions. It is important that not all networks have permission to send email via the protector's SMTP service, otherwise the protector can be used as a mail relay. To avoid this, you should limit the networks that send email via the protector.

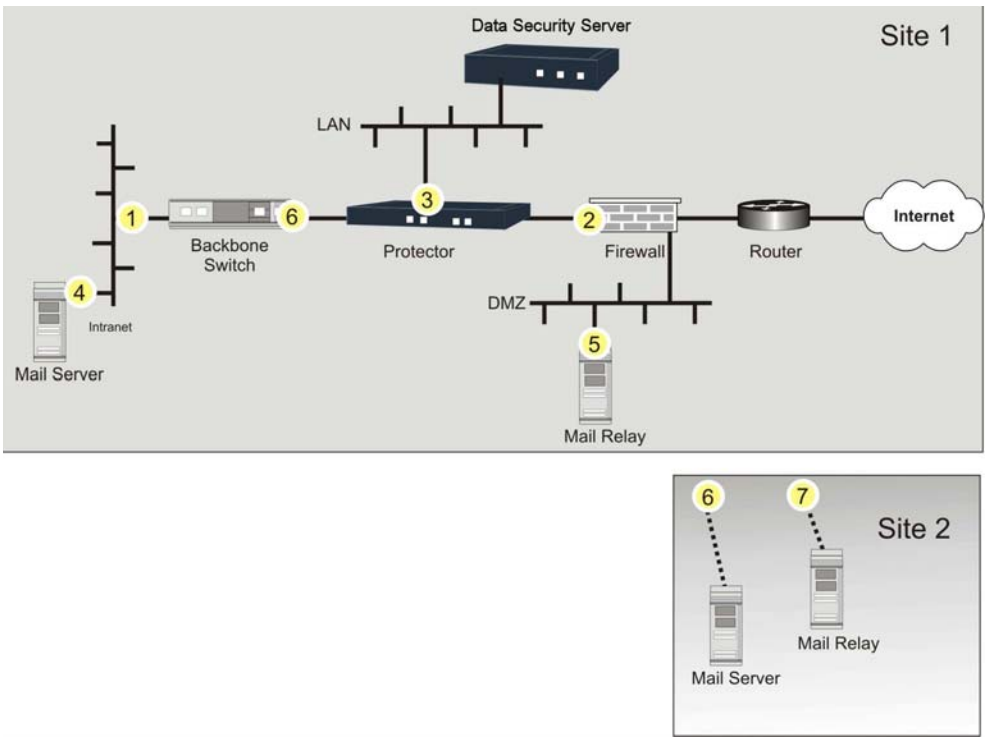
In explicit MTA mode, the protector acts as an MTA for your SMTP traffic and operates in protect mode. Protect mode allows you to block transactions that breach policy.

This section contains the basic steps required to configure Data Security for these 2 topologies.

For more information on deploying the protector inline, see *Deploying the protector*, page 477.

## Pre-installation checklist

The figure below shows a common topology in which the protector is installed inline. The checklist in this section refers to the numbers in this figure.




Before installation, check the following:

- Verify that the required hardware is available - check the latest release notes for the list of certified hardware.
- If inline mode is selected, verify that the protector contains a certified Silicom Network card (either Dual or Quad).
- Have the following ready before installation:
  - Valid IP addresses for the Data Security server and the protector management port in the Data Security LAN
- Make sure the following IP addresses are known prior to installation - they are required in order to complete the procedure:
  - The complete list of internal networks (IP ranges and subnet masks) [1]

    If there is more than one site, the internal networks list should include the networks of all sites.
  - A list of the mail server's IP addresses (in all sites) [4] [6]
  - The IP addresses of the mail relay, if one exists [5] [7]
  - The IP address of the outbound gateway for the protector - this will typically be the internal leg of the firewall [2]

- The IP address of the inbound gateway for the protector - this will typically be the external leg of the backbone switch or router [6]
- The HELO string the protector will use when identifying itself. This is relevant for the SMTP channel only.
- If customized notifications will be displayed when content is blocked, these should be prepared beforehand.

## Setting up SMTP in monitoring mode

1. Power up the protector.
2. Run the Websense installer as described in *Installing Data Security Components*, page 692. During installation make sure the time, date and timezone are precise, and map eth0 to verify it is located on the main board.
3. Connect eth0 of the protector to the LAN.
4. To configure the protector, in TRITON - Data Security, select **Settings** > **Deployment** > **System Modules**. Select the protector.
5. Complete the fields as follows:
   - In the **General** tab:
     - Select **Enabled**.
   - In the **Networking** tab:
     - Set **Default gateway** to the outbound gateway.
     - Set **Interface** to br0.
     - For the **Connection mode**, select Inline (Bridge).
     - In the **Network Interfaces** list, select br0 and click **Edit**. Select **Enable bypass mode** to allow traffic in case of Data Security Server software/ hardware failure. Click **OK**.
   - In the **Local Networks** tab:
     - Select **Include specific networks.** Add all the internal networks for all sites. This list is used to identify the direction of the traffic.The mail servers and mail relays should be considered part of the internal network.
   - In the **Services** tab
     - Select the **SMTP** service**.** On the **General** tab, set the **Mode** to **Monitoring bridge.** On the **Traffic Filter** tab, set the **Direction** to **Outbound.** Click **OK**.
     - Select the **HTTP** service. On the **General** tab, set the **Mode** to **Monitoring bridge.** On the **Traffic Filter** tab, set the **Direction** to **Outbound**. On the**HTTP Filter** tab, select**Exclude destination domains** if required. Click **OK**.
   - Click **OK** to save all the above settings, and click **Deploy** to activate the settings.
6. Connect the protector to the outgoing connection and to the organization’s internal network. This should be done last, after the protector is fully configured.

## Setting up SMTP in MTA modes

### Starting the protector

1. Power up the protector.
2. Run the Websense installer as described in *Installing Data Security Components*, page 692. Make sure the time, date and time zone are precise, and verify that eth0 (or whatever port you specified during installation) is mapped and located on the main board.
3. Connect eth0 or the designated port of the protector to the LAN.

### Configuring the protector

1. In TRITON - Data Security, select **Settings** > **Deployment** > **System Modules**. Select the protector.
2. In the **General** tab:
   - Select **Enabled**.
3. In the **Local Networks** tab:
   - Select **Include specific networks.** Add all the internal networks for all sites. This list is used to identify the direction of the traffic.The mail servers and mail relays should be considered part of the internal network.
4. In the **Services** tab:
   - Select the **SMTP** service**.**
   - On the **General** tab, set the **Mode** to **Mail Transfer Agent (MTA).**
   - On the **Mail Transfer Agent (MTA)** tab:
     - Set the **Operation Mode** to **Blocking** and select the behavior desired when an unspecified error occurs during analysis.
     - Set the **SMTP HELO name**. This is required.
     - Set the next hop MTA if required (for example, the company mail relay).
     - Set the addresses of all networks that are permitted to relay email messages through the protector. This is required, as it is important that not all networks have permission to send email via the protector's SMTP service, otherwise the protector can be used as a mail relay. This list should include the addresses any previous hops, such as your mail server.
5. Click **OK** to save all the above settings for the protector.
6. Select **Main** > **Policy Management** > **DLP Policies**. Select the policy rule that you wish to use for email management and click **Edit**.
7. Complete the fields as follows:
   - Select **Destinations**, and check the **Network Email** box.

- Select **Severity & Action**, then select an action plan that includes notifications.

> **Note**
> For more information about action plans, see the section "Action Plans" in TRITON - Data Security Help.

- Click **OK** to save all the above settings.

8. Click **Deploy** to activate the settings.

### Connecting the protector

1. Connect the protector to the outgoing connection and to the organization's internal network. This should be done last, after the protector is fully configured.
2. If a next hop server exists (for example, a company mail relay) you must add the protector's IP address to its allowed relay list.
3. (Optional) Set your mail server's next hop (smart host) to be the protector's IP address.

# Working with Web proxies

## Applies to

- Data Security v7.6.x

## In this topic

# Overview

If you want Websense Data Security to work with a Web proxy to monitor HTTP, HTTPS, and FTP traffic, we recommend that you use the Websense Content Gateway Web proxy. Websense Content Gateway includes a Data Security policy engine on box and streamlines communication with the TRITON Management Server.

If you have Websense Web Security Gateway or Web Security Gateway Anywhere, the Content Gateway proxy is included in the solution.

Websense Data Security also supports the following Web proxies:

- Blue Coat
- Squid open source

These proxies integrate with Websense Data Security over ICAP, an industry-standard protocol designed for off-loading specialized tasks from proxies.

# Blue Coat Web proxy

Blue Coat provides protocol support for HTTP, HTTPS, and FTP.

The integration solution described in this section is the recommended one. Other configurations can be implemented, but should be tested prior to deployment.

## Limitations

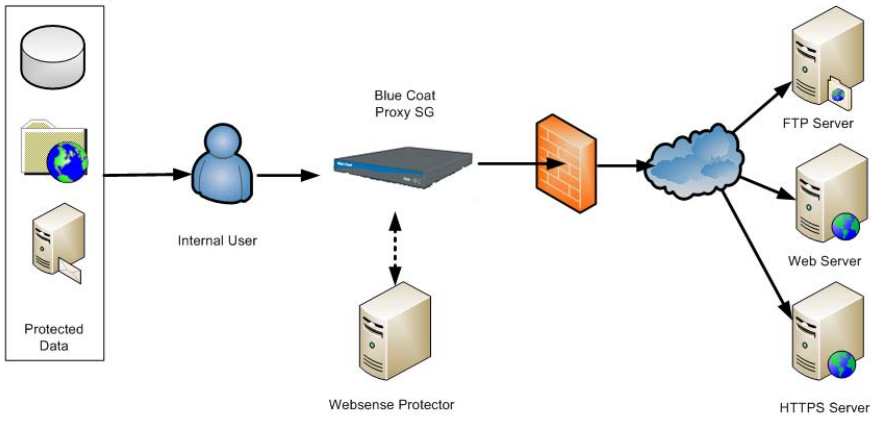
- The solution does not support FTP GET method for request modification.
- The solution does not support HTTP GET method for request modification.
- The solution is limited to scan files of 10MB. The system is capable of generating an error if a file exceeds that size.
- In the described deployment caching is not in effect (Blue Coat SG does not cache PUTs and POSTs). However, you should exercise care if a response mode configuration is used.

## Deployment

This deployment recommendation describes a forward proxy: a Blue Coat SG appliance connected to a Websense protector using ICAP. The Blue Coat SG appliance serves as a proxy for all HTTP, HTTPS, and FTP transactions. It is configured with rules that route data to the Websense ICAP server.

The Websense protector receives all traffic directed to it from the Blue Coat appliance for scanning,

The following diagram outlines the recommended deployment:




The deployment solution can be used in 2 modes:

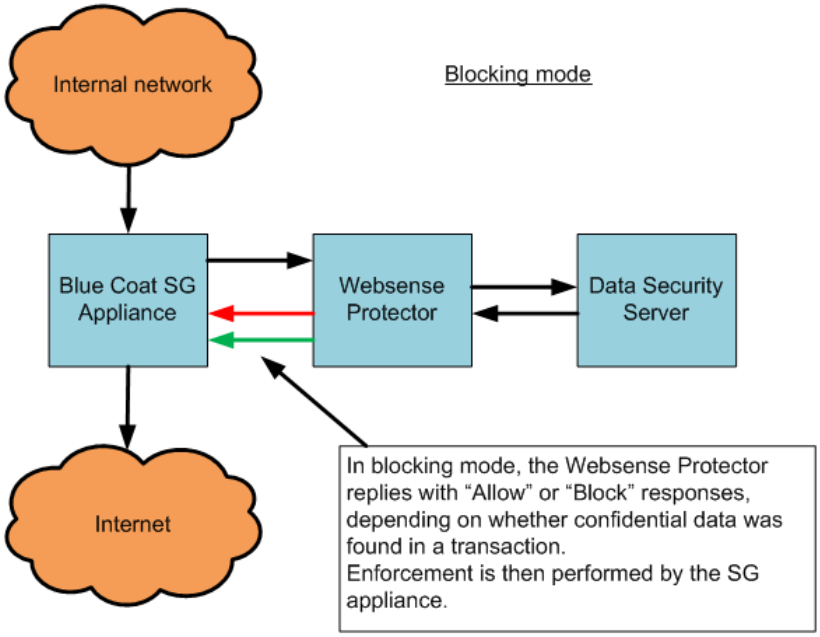
- Monitoring mode
- Enforcement mode

You can change the mode as required.

### Enforcement mode

In this mode, the Blue Coat SG appliance requires Websense Data Security to authorize each transaction before allowing the transactions to be posted or uploaded to

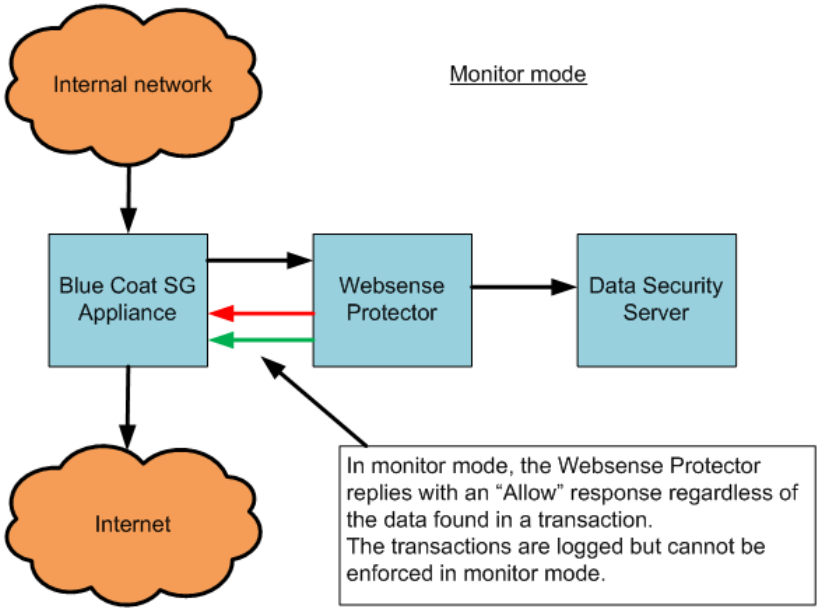
their intended destination. This is the recommended mode of operation for the solution as it provides the most security.




### Monitoring mode

In this mode, the transactions that are redirected by the Blue Coat SG appliance are analyzed by Websense Data Security, which can then generate audits for confidential information usage as well as generate notifications for administrators and information

owners. However, in monitoring mode, the Websense ICAP server universally responds to all redirected transactions with Allow.

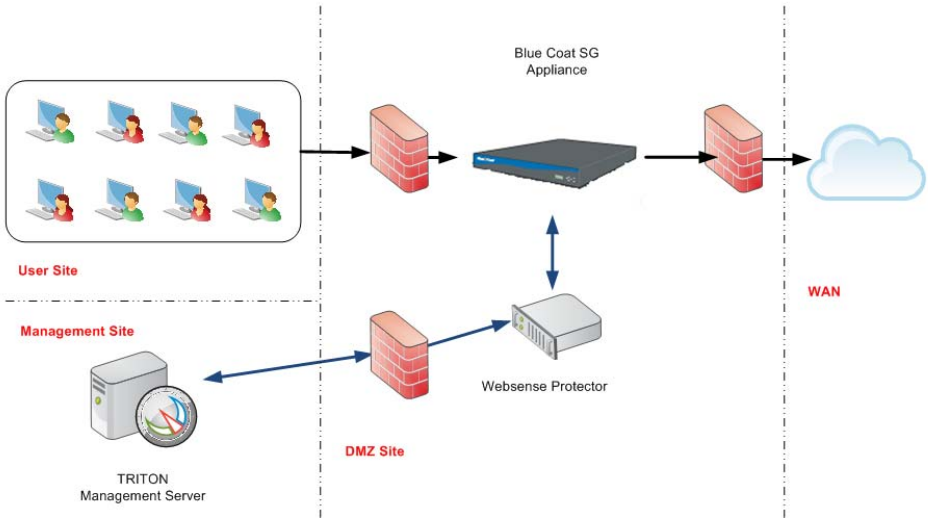



## Network integration

The solution consists of 3 components:

- Websense protector
- Websense TRITON Management Server
- Blue Coat SG appliance

The Websense - Blue Coat ICAP integration component resides on the protector, and acts as a relay between the Blue Coat SG appliances and the TRITON Management Server as shown below:




## Configuring the Blue Coat integration

### System setup

Refer to *Data Security*, page 435 for instructions on installing Websense Data Security. Refer to relevant Blue Coat documentation for more information on installing the Blue Coat appliance.

After connecting the systems, follow instructions to configure network parameters and other properties.

### Configuring Blue Coat

The Blue Coat Proxy SG can be configured with its basic information. You will need several pieces of information to configure the Proxy SG:

1. IP address and netmask of the main interface
2. Default gateway IP address
3. DNS server IP address
4. Console user name and password
5. Enable password
6. IP address and netmask of the ICAP interface

Items 1-5 enable you to set up the initial configuration of the Proxy SG by following the steps configure the Proxy SG with a direct serial port connection in your Blue Coat installation guide.

Once you have completed those steps, you can configure the second interface on the Proxy SG for use with the Websense ICAP server.

First, log on to the Proxy SG management console following the instructions in the Blue Coat installation guide. Then configure Adapter #1 with the IP address and netmask of the ICAP interface using the steps in the Adapters section of your Blue Coat configuration guide. (Adapter #0 is configured during the serial port configuration)

**HTTPS forward proxy configuration**

To enable ILP scanning of HTTPS posted documents, the Proxy SG must be configured for HTTPS forward proxy.

To configure the HTTPS forward proxy, follow the steps in these sections of your Blue Coat configuration guide:

1. Setting up the SSL proxy in transparent proxy mode
2. Creating an issuer keyring for SSL interception
3. Downloading an issuer certificate

You can find this guide in the Documentation section of your Blue Coat account (https://bto.bluecoat.com).

### Configuring the protector for ICAP

You configure the ICAP support on the protector in TRITON - Data Security.

1. Open TRITON - Data Security, and go to **Settings > System Modules**.
2. Under the protector you want to configure, select the ICAP server.

For more information, see the section “Configuring ICAP” in TRITON - Data Security Help.

### Configuring the ICAP service on Blue Coat

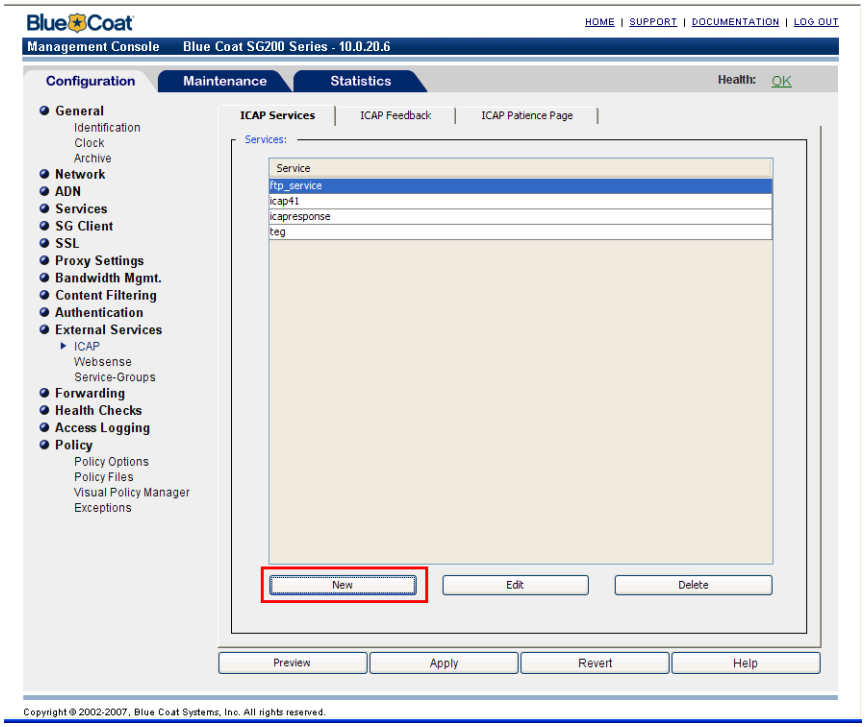
This section describes how to configure the Proxy SG to communicate with the Websense ICAP server on the protector.

This procedure assumes the Proxy SG is operating minimally with initial configurations, and you are logged on to the Blue Coat Management Console. If you have multiple protectors with ICAP servers, you must create a unique Proxy SG service for each one.

To configure the Proxy SG ICAP service:

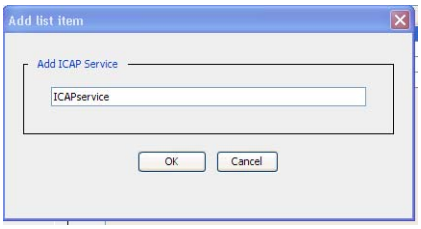
1. Select **Configuration > External Services > ICAP**.
2. To add a new service:

a. Click **New**.



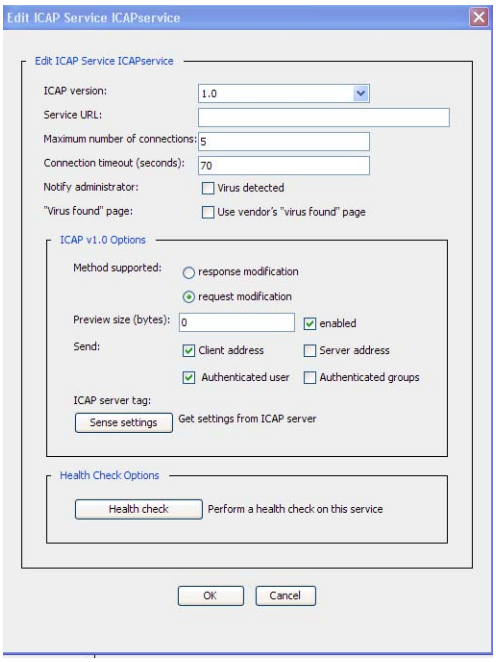

The Add list item window appears.

b. In the **Add ICAP Service** field, enter an alphanumeric name.




c. Click **OK**.

3. In the **Services** list, select the new ICAP service name and click **Edit**. The following screen appears:




4. On the Edit ICAP Service window, configure the following options.

| Field | Description |
|---|---|
| Service URL | This includes the URL schema, the ICAP server host name or IP address, and the ICAP port number. For example, icap://10.1.1.1:87.<br>You can distinguish between encapsulated protocols using different service URLs. |
| Maximum number of connections | The maximum number of connections at any time between the Proxy SG and the ICAP server. This can be any number between 1 and 65535. The default is 5. |
| Connection timeout | The number of seconds the Proxy SG waits for replies from the ICAP server. This can be any number between 60 and 65535. The default timeout is 70 seconds. |
| Notify administrator | Check the **Virus detected** box to send an email to the administrator if the virus scan detects a match. The notification is also sent to the Event Log and the Event Log email list. |
| Method supported | Select **request modification** for this service. Also select **Client address** and/or **Authenticated user**. |
| Send | Optionally, check one or more of these options to specify what is sent to the ICAP server. |
| Sense settings | Optionally, click this to automatically configure the ICAP service using the ICAP server parameters. |

5. Click **OK**.
6. Click **Apply**.

## Policy setup

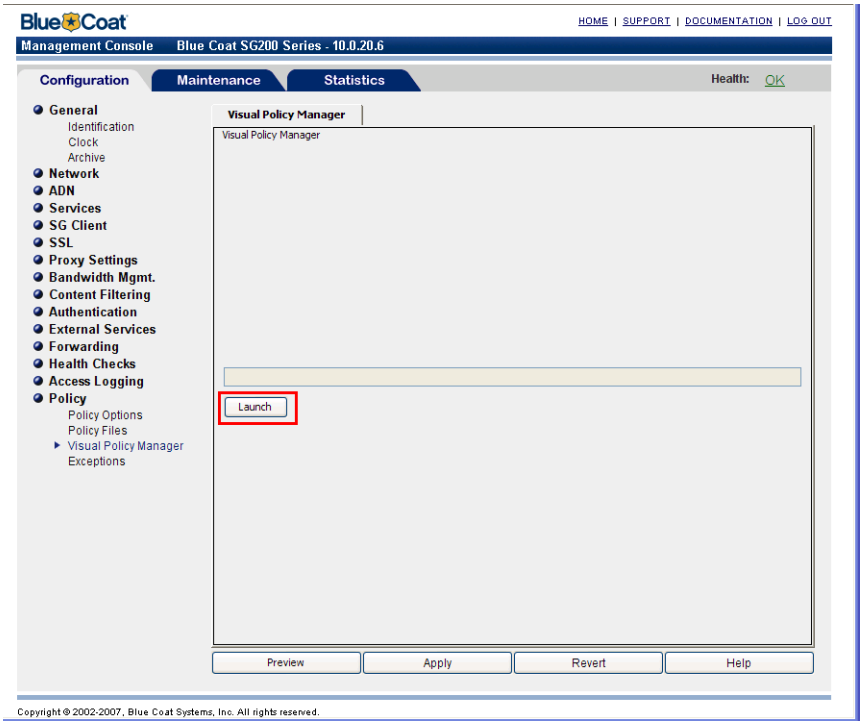
This section describes how to configure the Proxy SG policy to redirect traffic across the ICAP service.

For full details of managing Data Security policies, refer to “Creating Custom Policies” in TRITON - Data Security Help.

The procedure in this section assumes the Proxy SG is operating with initial configurations and ICAP configuration, and you are logged on to the Blue Coat Management Console.

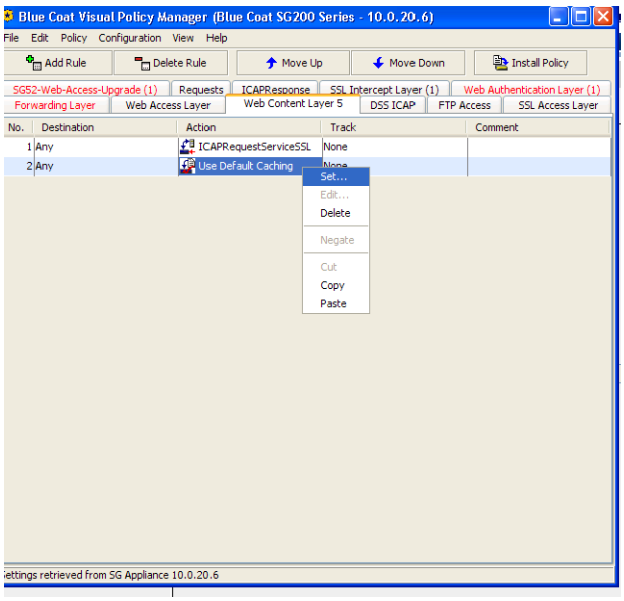
To configure the Proxy SG ICAP policies:

1. Select **Configuration > Policy >Visual Policy Manager**.
2. Click **Launch**.

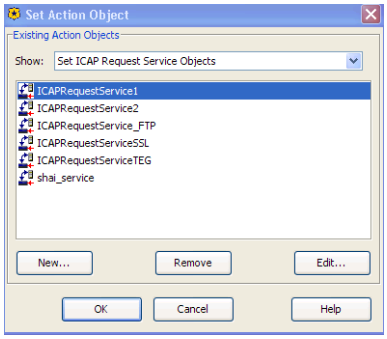



3. In the Visual Policy Manager, select **Add a policy**.
4. Add a content layer.
   a. Click the Web Content Layer tab.
   b. Click Add Rule.
5. Enter a policy name, and click **OK**.

6. Right click the **Action** option and select **Set** from the menu.

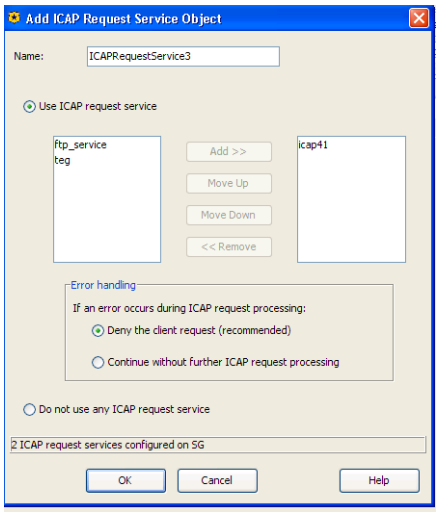



7. Under **Show**, select **Set ICAP Request Service Objects**.




8. Click **New > Set ICAP Request Service.**
9. Enter a name for the ICAP request service.

10. Select **Use ICAP request service**, choose a service from the drop-down list, and click **Add**.




11. Click **OK** twice.
12. Click **Install policy**.

## Configuring HTTPS policies

To configure an HTTPS policy, follow the steps in these sections of your Blue Coat configuration guide:

1. Using the SSL intercept layer
2. Using the SSL access layer

You can find this guide in the Documentation section of your Blue Coat account (https://bto.bluecoat.com).

## Recommended Blue Coat filtering rules

The table below lists filters that should be applied to the Blue Coat policy layer before the data is sent to the protector's ICAP server.

| Protocol | Filter | Condition |
|---|---|---|
| HTTP | GET | Allow always |
| HTTP | POST < 10MB | ICAP REQMOD |
| HTTP | POST > 10MB | Block/Allow always |
| HTTP | PUT < 10MB | ICAP REQMOD |
| HTTP | PUT > 10MB | Block/Allow always |
| HTTPS | GET | Allow always |
| HTTPS | POST < 10MB | ICAP REQMOD |
| HTTPS | POST > 10MB | Block/Allow always |

| Protocol | Filter | Condition |
|---|---|---|
| HTTPS | PUT < 10MB | ICAP REQMOD |
| HTTPS | PUT > 10MB | Block/Allow always |
| FTP | PUT < 10MB | ICAP REQMOD |
| FTP | PUT > 10MB | Block/Allow always |

# Squid open source Web proxy

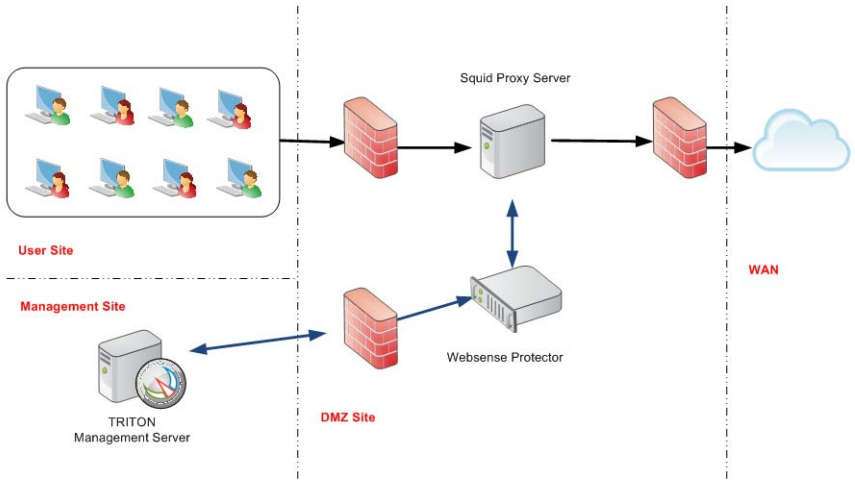
Squid provides protocol support for HTTP, HTTPS, and FTP. It integrates with Websense Data Security over ICAP, which is supported in Squid-3.0 and later.

## Deployment

This deployment recommendation describes a forward proxy: a Squid Web proxy server connected to a Websense protector using ICAP. Squid serves as a proxy for all HTTP, HTTPS, and FTP transactions. It is configured with rules that route data to the Websense ICAP server.

The Websense protector receives all traffic directed to it from the Squid server for scanning,

The following diagram outlines the recommended deployment:




The deployment solution can be used in 2 modes:

- Monitoring mode
- Enforcement mode

You can change the mode as required.

## System setup

Refer to *Data Security*, page 435 for instructions on installing Websense Data Security, and refer to the relevant Squid documentation for more information on installing the Squid Web proxy.

After connecting the systems, follow instructions to configure network parameters and other properties.

## Configuring Squid for ICAP

Set up your Squid proxy to send requests to the ICAP server that is part of the Websense protector.

This example is for Squid-3.1:

```
icap_service service_req reqmod_precache 1
icap://<protector_IP>:1344/reqmod
adaptation_access service_req allow all
```

This example is for Squid-3.0:

```
icap_service service_req reqmod_precache 1
icap://<protector_IP>:1344/reqmod
icap_class class_req service_req
icap_access class_req allow all
```

For full ICAP configuration details for Squid, see http://wiki.squid-cache.org/Features/ICAP?highlight=%28faqlisted.yes%29.

## Configuring the protector for ICAP

You configure the ICAP support on the protector in TRITON - Data Security.

1. Open TRITON - Data Security, and go to **Settings > System Modules**.
2. Under the protector you want to configure, select the ICAP server.

For more information, see the section “Configuring ICAP” in TRITON - Data Security Help.

## ICAP server error and response codes

| Response Condition | Websense Block Decision | Control Exceeds Size Limit | Error Condition |
|---|---|---|---|
| **Condition** | “pana_response” | “huge_content” | “pana_error” |
| **Error Code** | 500 | 500 | 512 |
| **=“X-Response-Info”** | PA-block | | PA-error |
| **=“X-Response-Desc”** | Websense blocked | | |
| **Plain URL** | /usr/local/spicer/etc/blockmessageexample.plain | | |
| **Markup URL** | /usr/local/spicer/etc/block-messageexample.markup | | |

# Working with shared drives

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

Discovery is the act of determining where sensitive content is located in your enterprise. If you have shared drives, for example on Windows or Novell, you can create a data discovery task that describes where and when to perform discovery on these drives, including specific network locations to scan.

## Performing discovery on Novell or NFS shares

This section describes the steps required for Websense Data Security to be able to scan files and folders on Novell file servers.

The following definitions are used in this section:

- **NDS - Novell Directory Services** - Using NDS, a network administrator can set up and control a database of users and manage them using a directory with an easy-to-use graphical user interface (GUI). Users at remote locations can be added, updated, and managed centrally. Applications can be distributed electronically and maintained centrally. The concept is similar to Microsoft's Active Directory.
- **Novell Client for Windows** - a client software used so that Windows machines can authenticate through NDS and access shared resources on Novell servers.

## Configuring data discovery on the Data Security server

First, prepare the Novell server as follows:

1. Create a user account in Novell eDirectory (NDS). This user will be used by the Websense Data Security Discovery agent to authenticate with Novell eDirectory and access files and folders.

   The user account must have the same logon name and password as the Websense Data Security service account.
2. Make sure the newly created user has at least "Read" permissions on all files and folders that you wish to run discovery on.

Next, prepare the Data Security server:

1. Download the latest Novell Client for Windows from the Novell Web site: http://www.novell.com/products/clients/
2. Run setupnw.exe and select **Custom Installation**.
3. Make sure **Novell Distributed Print Services** is not checked and click **Next**.
4. Make sure **NetIdentity Agent** and **NMAS** are checked and click **Next**.
5. Select IP and IPX protocols and click **Next**.
6. Select eDirectory and click **Next**.
7. Wait for the installation to complete, then reboot the server.
8. After the reboot, the Novell logon window should appear instead of the regular Windows logon.
9. Log on to Windows and Novell using the Data Security service account (it should be the same user for both platforms as stated above).

   Under the eDirectory tab, you must select the tree and its relevant context for the folders you are about to run discovery on.
10. Right-click the Novell icon in the task bar and select **Properties**.
11. Click **Cancel**.
12. Ensure the files you are about to run discovery on are accessible from Windows by UNC (for example, \\NovelFileSrv\vol1\Data).
13. Right-click the Novell icon in the task bar and select **Novell Connections**.
14. On all connections, click **Detach** until no connections remain.
15. Open TRITON - Data Security, and create a new data discovery task as follows:

a. Select **Main > Policy Management > Discovery Policies**.
b. Select **Network Discovery Tasks**.
c. Click **New**, and select **File System Task** from the drop-down list.
d. On the **Networks** page, click **Edit** to select the Novell server's IP address.
e. Click **Advanced**, and add the Novell access port number 524.
f. On the **Scanned Folders** page, use the Data Security service account for authentication.
g. Set up all other options as you require.

## Performing discovery on Windows NFS shares

If you want to perform data discovery on Windows file shares, you need to install NFS client on your Data Security server. If you have more than one Data Security server, install NFS client on the one with the crawler you will use to perform discovery.

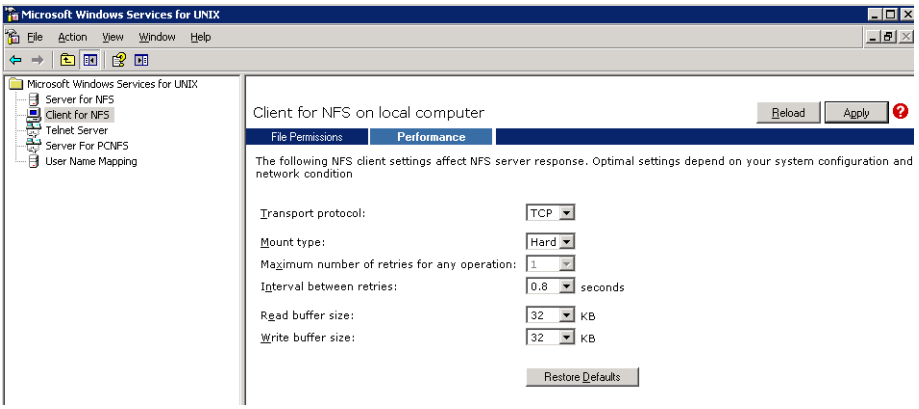
Do not install Data Security on the same machine as the NFS server.

### Windows Server 2003

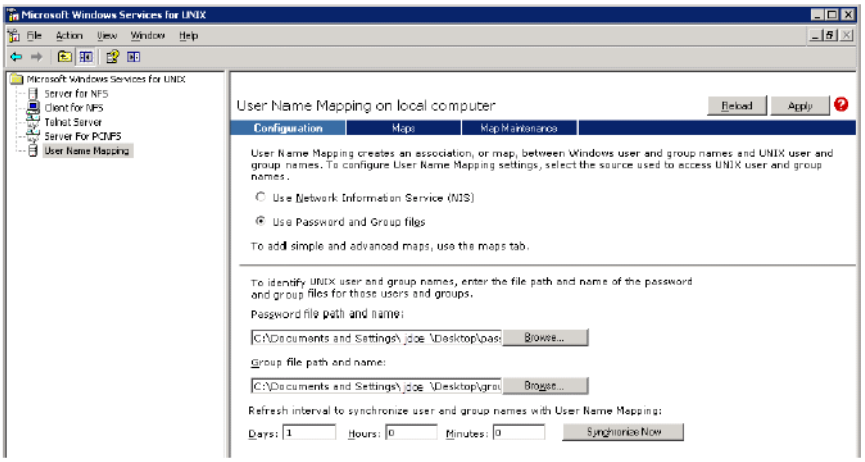
1. On the Data Security server you will use to perform discovery, install the NFS client from the "Windows Services for Unix" package. You can download the package from Microsoft's Technet.
2. During installation, select the following:
   - Utilities
   - NFS > Client for NFS
   - Authentication tools for NFS

   All others features must be disabled.
3. After installation has completed, select **Start > Programs > Windows Services for UNIX > Services for UNIX Administration**.
4. Navigate to Client for NFS and set the file permissions to All, Read, Write and Execute.
5. Under Performance, change the transport protocol from UDP to TCP and the Mount type from Soft to Hard.

6. Ensure that the buffer size is at the maximum of 32 KB.



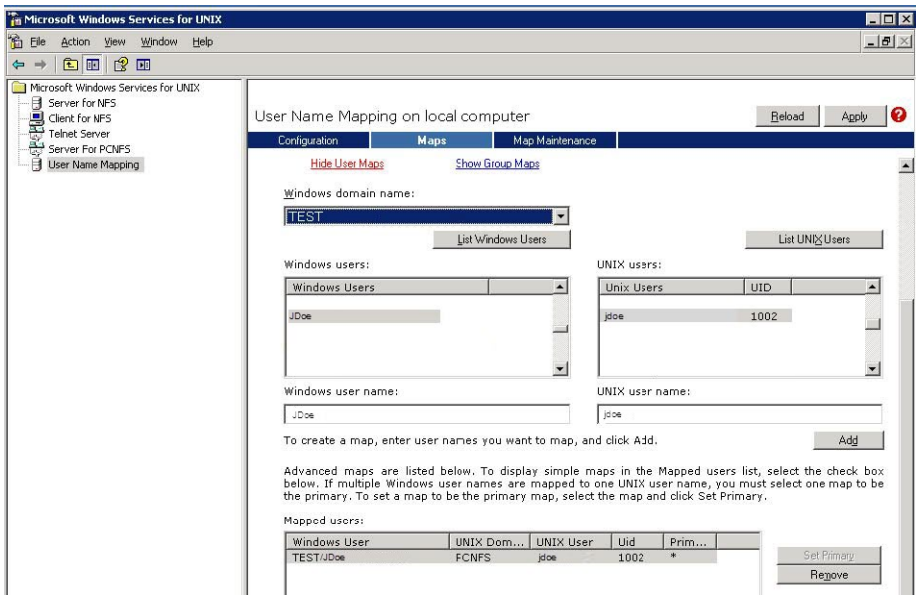

7. Click **Apply** when done.
8. Navigate to User Name Mapping.
9. On the Configuration tab specify whether the user name to be mapped will be imported from a Network Information Service (NIS) or from password/group files (/etc/passwd and /etc/group). For NIS mapping, enter the IP address or host name of the NIS server and the NIS domain name. Files are used in the example below.



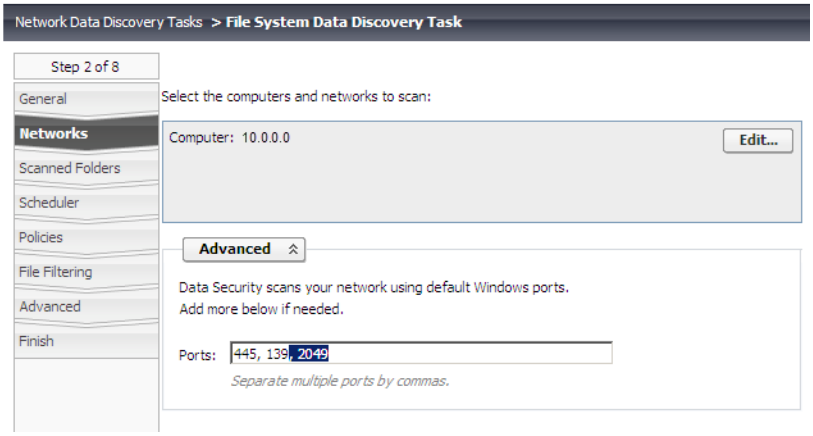

> **Note**
> If you select User Password and Group Files, you only need to add the users and groups that need to be mapped.

10. On the Maps tab, select the machine or domain for the user account that will be specified in the discovery task and click **List Windows Users**.
11. Click **List UNIX Users** and specify an account that has access to the NFS share.

12. Select a user name from each list box, then click **Add** to map the names.



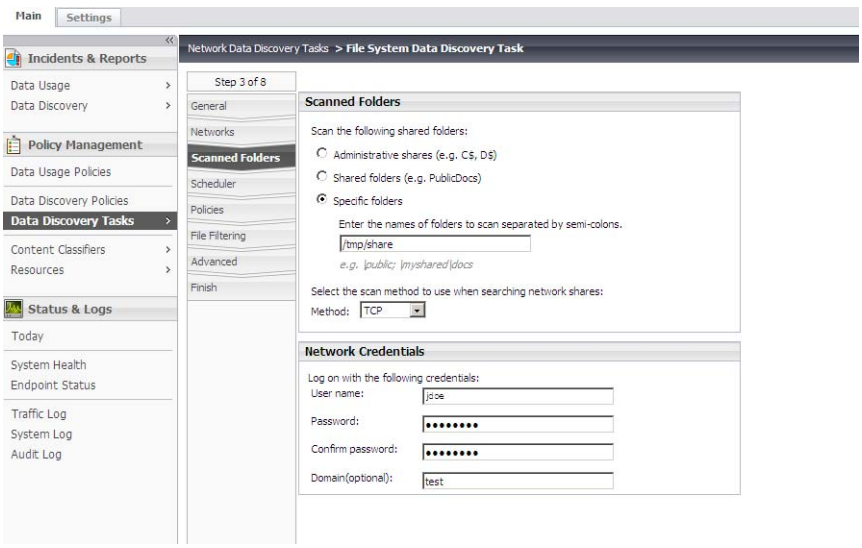

13. Log onto the TRITON Console, and select the Data Security tab.
14. Create a data discovery policy in TRITON - Data Security. (See the section "Creating a data discovery policy" in TRITON - Data Security Help for instructions.)
15. Create a file system task. Select **Main > Policy Management > Discovery Policies, and then select Add Network Task > File System Task**.
16. On the General screen, add a name and description for the discovery task and select the crawler to perform the discovery (the one where you installed the NFS client).
17. On the Networks screen, click **Advanced** and add port 2049 to the existing list of scanned ports.



18. On the Scanned Folders screen, specify the shared to be scanned and the user name and password of the Windows user mapped to the UNIX user name.

> **Note**
> Network discovery has a limit of 255 characters for the path and file name. Files contained in paths that have more than 255 characters are not scanned.

| Field | Description |
|---|---|
| Shared folders | Select the shared folders you want to scan:<br>• **Administrative shares** - Select this if you want to scan administrative share drives such as C$.<br>• **Shared folders** - Select this if you want to scan shared folders such as PublicDocs.<br>• **Specific folders** - Select this if you want to scan specific folders, then enter the name(s) of the folder(s) to scan, separated by semi-colons. |
| Method | Select the method to use when scanning network shares:<br>• **TCP** - Select TCP if you want to scan the share drives using transmission control protocol.<br>• **ICMP** - Select ICMP if you want to scan the share drives using Internet control message protocol. |
| User name | Enter the user name of an administrator with network access. |
| Password | Enter a password for this administrator. |
| Domain | Optionally, enter the domain name of the network. |




19. Deploy your changes.

For more information on the wizard for creating file system discovery tasks, see the section "File System tasks" in TRITON - Data Security Help.

# Working with user directory servers

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

If you have one or more user directory servers, such as Microsoft Active Directory or Lotus Domino, you should integrate your servers into Websense Data Security configuration. Once you have set up server details and imported users and groups using TRITON - Data Security, you can base your administrator login authentication on user directory credentials, resolve user details during analysis, and enhance the details displayed with the incident.

## Configuring user directory server settings

You set up your user directory server settings as part of your initial Websense Data Security configuration:

1. Open TRITON - Data Security.
2. Select **Settings** > **General** > **System**.
3. Select **User Directories**.
4. Click **New** in the toolbar.
5. In the Add User Directory Server dialog box, complete the following fields:

| Field | Description |
|---|---|
| Name | Enter a name for the user directory server. |
| Enabled | Click **Enabled** to enable this server as your user directory server. |
| Type | Select the type of directory from the drop-down list: Active Directory, Lotus, Sun, or another. |

| Field | Description |
|---|---|
| **Connection Settings** | |
| IP address or host name | Enter the IP address or host name of the user directory server. |
| Port | Enter the port number of the user directory server. |
| User distinguished name | Enter a user name that has access to the directory server. |
| Password | Enter the password for this user name. |
| Use SSL encryption | Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption. |
| Follow referrals | Select **Follow referrals** if you want Websense Data Security to follow server referrals should they exist. A server referral is when one server refers to another for programs or data. |
| Test Connection | Click this button to test your connection to the user-directory server. |
| **Directory usage** | |
| Get user attributes | Select this box if you want to retrieve user information from the directory server. |
| Attributes to retrieve | Enter the user attributes that you want TRITON - Data Security to collect for all users (comma separated). |
| Sample email address | Enter a valid email address with which you can perform a test. |
| Test Attributes | Click **Test Attributes** to retrieve user information on the email address you supplied. Mouse over the information icon to check the user information imported. |

6. Click **OK** to save your changes.

The server is listed on the User Directories page.

## Importing user data

By default, Websense Data Security imports data from user directory servers daily at 3.00am. You can change the import time as follows:

1. In TRITON - Data Security, select **Settings > General > System**.
2. Select **User Directories**.
3. Click the **Import daily at** link.
4. Set a new time and click **OK**.

Once you have set up a user directory server, you can start an import at any time in addition to the daily schedule:

1. On the User Directories page, select the server and click **Import Now**.
2. Click **Yes** to continue.

To view user directory entries once they have been imported, go to **Main** > **Policy Management** > **Resources** and select **User Directory Entries**.

## Rearranging servers

Once you have set up a user directory server in TRITON - Data Security, the server is listed on the User Directories page. If you have set up and enabled more than one server, users are imported from user directories in the order listed on this page. If a user is in more than one directory, the first directory record takes precedence.

To rearrange your servers in the order you want them:

1. Click **Rearrange Servers**.
2. Select a server, and use the arrow buttons to move it up or down the list.
3. Click **OK** when done.

# Working with Exchange servers

## Applies to

- Data Security v7.6.x

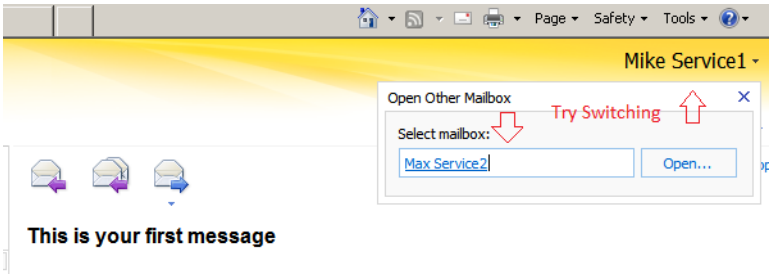
## Overview

With Data Security, you can perform discovery on Microsoft Exchange servers. Before you begin, there are a number of steps you need to take.

### Exchange 2010

1. Define a service account for Exchange discovery scanning.
2. Grant the account one of the following roles. This is necessary so that Data Security can discover messages and display results.
    - Exchange Full Administrator
    - Exchange Administrator
    - Exchange View Only Administrator

The service account should now be able to accesse Exchange via Outlook Web App (OWA) and move between the mailboxes intended to be scanned during the discovery. Try switching between mailboxes as shown below:




3. Configure Exchange impersonation. Exchange impersonation needs to be enabled for the service account used for the discovery
   a. Open the Exchange Management Shell.
   b. Run the **New-ManagementRoleAssignment** cmdlet to add the permission to impersonate to the specified user.

      For example, to enable a service account to impersonate all other users in an organization, enter the following:

      ```
      New-ManagementRoleAssignment -
      Name:impersonationAssignmentName -
      Role:ApplicationImpersonation -User:ServiceAccount
      ```


For more information on Exchange impersonation, see http://msdn.microsoft.com/en-us/library/bb204095.

4. Configure an Exchange discovery task.
   a. Log onto the TRITON Console and select the Data Security tab.
   b. Select **Main > Policy Management > Discovery Policies > Add Network Task > Exchange Task**.
   c. Complete the wizard as explained in the TRITON - Data Security Help.

# Working with IBM Lotus Domino and Lotus Notes

## Applies to

- Data Security v7.6.3 and beyond

## In this topic



## Overview

Starting with v7.6.3, you can fingerprint and perform discovery on documents stored in an IBM Lotus Domino Data Management System (DMS). Data Security supports IBM Lotus Domino and IBM Lotus Notes (Basic and Standard Editions) v7.x and 8.x on Windows Server 2003 or Windows Server 2008R2.

Domino environments normally consist of one or more servers working together with data stored in Notes Storage Format (NSF) files. There are usually many NSFs on any given Domino server. Each entry in the NSF may have a title, one or more body fields, and attachments. For example:

- An NSF for email might have the fields: subject, to, from, bcc, body, and attachment.
- An NSF for inventory management might have the fields: catalog number, title, description, and expiration date.

These sections describe how to integrate your system with Data Security.

### Before you begin

Before you begin, make sure that you:

1. Install Lotus Notes on the machine where you will install the Data Security crawler. This can be the machine where you plan to install the Data Security server software; or it can be a stand-alone machine where you plan to install the crawler agent.

   **Important**
   The crawler you will use for Domino fingerprinting and discovery must be on the same machine as Lotus Notes.

   Be sure that the installation is done for "Anyone who uses this computer."
2. Log on to Lotus Notes and supply a user.id file and password.
3. Connect to the Lotus Domino server from the Lotus Notes client. This should be done by the user who will be installing the crawler. For best practice, do not run Lotus Notes on this machine again after the crawler is installed.

## Getting started

To integrate Data Security with your Domino Server:

1. Run the Data Security installation wizard on a machine with the Lotus Notes client. For best practice, do not run the Lotus Notes client on the machine on which the Data Security crawler is installed.
2. During installation, the installer detects the Notes client and displays the Lotus Domino Connections page. On this page:
   a. Select the check box labeled **Use this machine to scan Lotus Domino servers**.
   b. In the **User ID file** field, browse to one of the authorized users, then navigate to the user's **user.id** file.

   > **Note**
   > Select a user that has permission to access all folders and Notes Storage Format (NSF) files of interest, otherwise certain items may not be scanned.

   c. In the **Password** field, enter the password for the authorized user.

   > **Note**
   > If you need to update the **User ID** and **Password** fields, run the installation wizard and select **Modify.**

## Lotus Domino discovery

Lotus Domino discovery treats a document (body and attachments) as one unit. This way, a breach is reported even if the sensitive content is scattered in different parts of the document that individually would not cause an incident.

To perform discovery on documents:

1. Log on to TRITON - Data Security, and create a discovery policy.

   To do so:

   a. Navigate to **Main > Policy Management > Discovery Policies**.
   b. Select **Locate regulatory & compliance data** or **Create custom policy**.
   c. Complete the steps in the wizard as described in theTRITON - Data Security Help. You can choose dictionary, RegEx, fingerprinting, or other classifiers as needed.
2. Create a Lotus Domino discovery task.

   To do so:

   a. Navigate to **Main > Policy Management > Discovery Policies**.
   b. Select **Add network task > Lotus Domino Task**.

c. Complete the steps in the wizard as described in theTRITON - Data Security Help.

3. To deploy the policy and task to the Lotus Domino server, click **Deploy**. The Domino server will be crawled for your sensitive data at the next scheduled time. Incidents are reported under **Main > Reporting > Discovery**.

## Lotus Domino fingerprinting

Lotus Domino fingerprinting treats the body of a document and each of its attachments as a separate item. This enables the system to show the full path down to the item inside a document that caused a breach.

To fingerprint documents:

1. Log on to TRITON - Data Security, and create a Lotus Domino fingerprinting classifier.

   To do so:

   a. Navigate to **Main > Policy Management > Content Classifiers > File Fingerprinting**.

   b. Select **New > Lotus Domino Fingerprinting**.

   c. Complete the steps in the wizard as described in theTRITON - Data Security Help.

2. Create a Data Loss Prevention (DLP) policy using the following classifier:

   a. Navigate to **Main > Policy Management > DLP Policies**.

   b. Select **Create custom policy**.

   c. Complete the steps in the wizard as described in theTRITON - Data Security Help. Be sure to select the fingerprinting classifier on the **Condition** page.

3. To deploy the policy and classifier to the Lotus Domino server, click**Deploy**. The data on your Domino server will be fingerprinted at the next scheduled time. Incidents are reported under **Main > Reporting > Data Loss Prevention**.

# 35 Scaling Data Security

## Applies to

- Data Security v7.6.x

## Scaling Data Security

As your network (and the security needs of your network) grows, Websense Data Security can grow with it. Our software is architected for scalability, even for networks with massive traffic and complex topologies. The sections below address network growth issues such as recognizing when system loads demand system expansion, single and multi-site configuration and how to deal with the growth of the various information repositories.


- *When does your system need to grow?*, page 553
- *Adding modules to your deployment*, page 557


## When does your system need to grow?

### Applies to

- Data Security v7.6.x

### When does your system need to grow?

There are numerous triggers that might prompt your system expansion. Among them:

- **Performance issues**

  You may or may not be aware of performance issues affecting your system. If you are experiencing slow discovery or fingerprinting scans, for example, this could be an indication of an overworked crawler. You may benefit from an additional crawler or Data Security server. If user are experiencing slow Web or email transactions, you may benefit from an additional policy engine. Even if you are

not aware of performance issues, your system resources may not be fully optimized.

To see how your system is performing, open TRITON - Data Security and select **Main > Status > System Health.** You can expand each module and view statistics on the load, the number of transactions, the latency, and more.

Before adding modules, try balancing the load between your existing Data Security servers (policy engines). To do this, go to **Settings > Deployment > System Modules**, and click **Load Balancing**. Select a service and indicate which policy engine you'd like to assign to that service.

**Note**

Websense recommends that you do not distribute the load to the TRITON Management Server.

- **The number of users grows**

  In a typical small organization (1–500 users), you might only need a TRITON Management Server and a protector to monitor traffic. A larger organization (500–2,500 users) might have a TRITON Management Server, a supplemental Data Security server, and a protector, with load balancing between the protector and supplemental server. (You cannot balance the load with the management server.)

  As your number of users grows, so does your need for a Data Security server.

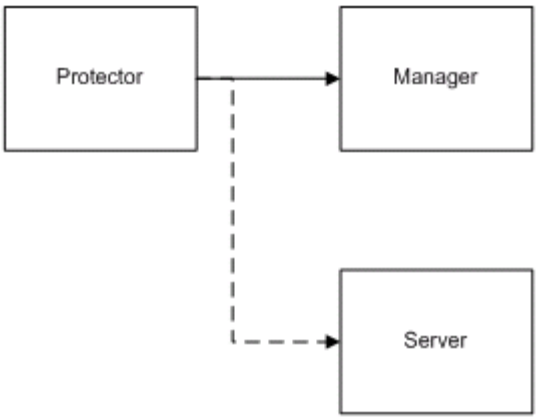
- **The number of transactions grows**

  This is the most important requirement for determining your Data Security needs. Typically the number of transactions grows as your number of users grows.

  *In monitoring mode*, Websense recommends having 1 protector per 20,000 users. This calculation assumes:

  - The protector is monitoring HTTP and SMTP
  - There are 9 busy hours per day
  - There are approximately 20 million transactions per day with a ratio of 15:1 HTTP:SMTP. (HTTP includes GETs and POSTs.)

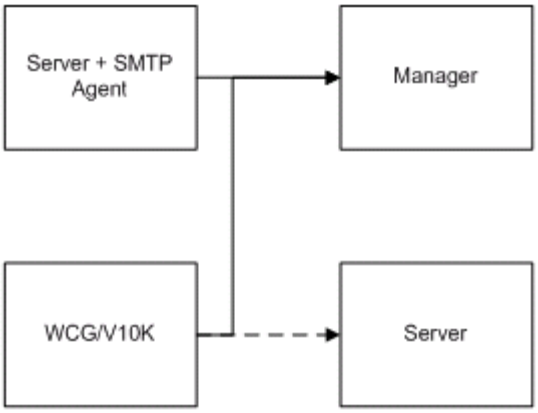
  For more users, add an extra Data Security server and balance the load between the protector and the extra server.

  In *blocking* mode, Websense recommends 1 TRITON Management Server, 1 SMTP agent, and 1 V-Series appliance with Websense Content Gateway software. This calculation assumes:

  - There are 9 busy hours per day
  - There are approximately 15 million transactions per day with a ratio of 15:1 HTTP:SMTP. (HTTP includes GETs and POSTs.)

For more users, add an extra Data Security server.




Note that your transaction volume can grow even if your user base does not. If you anticipate adding a significant amount of traffic, you'd benefit from adding one or more Data Security servers.

- **The number of endpoints grows**

  If you subscribe to the Data Endpoint and you are adding endpoints to the system, you may need additional servers. A general rule of thumb is to add 1 Data Security server for every 30,000 endpoint clients.

- **Moving your deployment from monitor to protect**

  Enforcement requires more resources, particularly because load-balancing must be enforced between policy engines and SMTP agents. If you are moving from monitor to protect, you may benefit from an additional Data Security server.

- **Moving from a single-site to multi-site configuration**

  Websense Data Security supports multi-site, distributed deployments. You can have a local policy engine on the protector, for example, and distributed (primary and secondary) fingerprint repositories. You can have a management server in one location and one or more supplemental Data Security servers in other locations.

  You can utilize the crawlers on the Data Security servers alone to do your fingerprint and discovery scans, or you can install the crawler agent on additional servers to improve performance. These are just a few of the possibilities, and of course, all are scalable.

  See *Most common deployments*, page 459 for distributions our customers commonly use.

  Regardless, organizations having multiple geographical locations need a protector for each site. If you have multiple geographical locations with low latency between sites, you may need 2 protectors and 2 supplemental Data Security servers.

- **Adding branch offices**

  Each branch office requires a protector. If you are adding or acquiring a branch office, you should add a protector.

- **Adding HTTP, SMTP and FTP egress points**

  If you are adding egress points to your network structure, you need to protectors to monitor or protect those egress points.

- **The network grows (in GB)**

  If you are performing network discovery, your network size greatly affects your requirements, as does the frequency of full versus differential scans. If your network is growing, you may require an additional crawler or Data Security server.

- **Repositories such as forensics, fingerprint, policy database are reaching their maximum**

  The Data Security software has some default settings for the disk-space requirements of its fingerprint and forensic repositories, but you can modify all of the values. Businesses with larger transaction volumes and numbers of users can adjust values significantly upward. (See *Allocating disk space*, page 457.)

  At some point, however, you may want to add another server to accommodate these repositories and increase your disk space. The forensics repository can get very large. It has a default setting of 40 GB. The archive has a default setting of 50 GB.

# Adding modules to your deployment

## Applies to

- Data Security v7.6.x

## In this topic



## Overview

If network and security requirements dictate that you need to add new agents or other modules to your deployment, go to the machine where you want to install them and run the Data Security installation wizard.

When you install the module, you are asked to provide the FQDN of the TRITON management server and the credentials for a TRITON administrator with Data Security system modules permissions. When you do, the module is automatically registered with the management server.

If you accept the default configuration, all you have to do is click **Deploy** in TRITON - Data Security (on the management server) to complete the process. If you want to

customize the configurations, go into the System Modules screen and click the module to edit.

Only a management user with system modules permissions can install new network elements.

For information on adding and configuring modules, see**Managing System Modules > Adding modules** in the TRITON - Data Security Help.

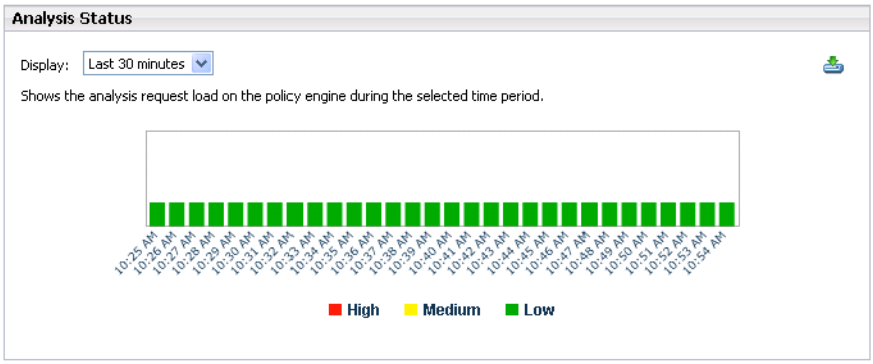
# Value of additional policy engines

Policy engines analyze transactions sent from various agents and protectors. The protector monitors network traffic and sends transactions to policy engines for analysis. The CPU load on the protector is much lighter than on a policy engine; therefore, when scaling up, you should add more policy engines (not protectors) and load-balance the analysis between them.

## Assessing the need for additional policy engines

Check the number of transactions analyzed by the policy engine by selecting **Main > Status > System Health** and clicking on a policy engine.

View the "Analysis status" chart for the policy engine.




If there is red on the chart, this indicates a heavy load on the policy engine during the designated period.

If you are in monitoring mode, a few red bars may not be an issue. The system will process these incidents during a less busy period.

If you are in blocking mode, even one hour of red is undesirable. If you see this, you should perform load balancing and/or add a new Data Security server.

## Optimizing

- Try to avoid analysis of incoming traffic. If incoming is a must, try to limit it to certain domains.
- Never scan all networks; establish limits.

- Check the top policies and see if there are any false positives or unwanted/not needed policies a week or two after first deployment.
- If possible, make sure no spam SMTP mail is undergoing analysis.

# 36 Data Security Protector CLI

## Applies to

- Data Security v7.6.x

## In this topic

- *Configuring NTP support*, page 573

# Overview

A command-line interpreter (also known as a command-line shell) is a computer program that reads lines of text entered by a user and interprets them in the context of a given operating system or programming language.

Command-line interpreters allow users to issue various commands in a very efficient way. This requires the user to know the names of the commands and their parameters, and the syntax of the language that is interpreted.

This chapter describes the command line interpreter (CLI) for the Linux-based Data Security Protector.

The CLI can be used after initial installation to modify the settings configured by the wizard as well as configure other protector parameters. Log in using the **admin** or **root** user (other users can also be defined). Note that **admin** users are limited and not all Linux shell commands are available to them.

# Accessing the CLI

Access the CLI through a direct terminal or via a serial port console.

If using a serial port console, configure your terminal application, such as HyperTerminal or TeraTerm, as follows:

19200 baud, 8 data bits, no parity, 1 stop bit, no flow control.

In addition, the protector allows access via SSH connection.

Connect to port 22 with the SSH tool of your choice and use the credentials you set to access the protector CLI. It is impossible to access the protector using SSH before running the wizard for the first time, as it has irrelevant default network settings.

# Command-line reference

Following are general guidelines to using the CLI.

- For **admin** users, use the help command to view a list of all available commands
- All commands can be run with the **help** option to view detailed help about that command. For example: **iface help**
- The CLI shell implements auto-complete for command names using the TAB key. For example, typing **i**+TAB will display: **iface info** (all the commands that start with **i**)

- The CLI shell implements command history. Use the up/down arrows to view/run/modify previously entered commands, sequentially.

Some commands' output may exceed the height of the screen. Use your terminal software to scroll back and view all output.

- All commands and their arguments are case sensitive.
- Abbreviations are not accepted in the CLI; it is necessary to type the entire word. The TAB button can be used to complete partially typed commands.
- Some command output may exceed the length of the screen. Once the screen is full, the CLI will prompt –**`more-`**. Use the spacebar to display the next screen.

## Exit the command line interface

Syntax `exit`

Description Exits the user from the Websense Protector CLI and returns to the login prompt or to a wrapper shell environment.

Parameters N/A

Default N/A

Example
```
Websense1# exit
Websense1 login:
```

## Show CLI help messages

Syntax `help ?`

Description This command displays all available commands with a small description for each. The list of available commands depends on the user's profile. All commands support the help argument. When used, the command displays a help message relevant to that command.

Parameters N/A

Default N/A

Example
```
Websense1# dns help
dns: Configure or show DNS server(s) Usage: dns
[list | delall] dns [{add | del} <ipaddr>]
```

## Accessing the basic configuration wizard

Syntax `wizard`

Description Opens the Websense Protector Installation Wizard. The user can also run `wizard securecomm` to go directly to the registration stage of the Wizard, where Data Security Manager details are entered.

Parameters N/A

Default N/A

Example
```
Websense1# wizard
Websense1# wizard securecomm
```

## Rebooting the protector

Syntax `reboot`

Description Reboots the protector. The protector is shut down and restarted immediately after the command is executed.

Parameters N/A

Default N/A

Example

```
Websense1# reboot
```

## Turning off the protector

| | |
|---|---|
| Syntax | `shutdown` |
| Description | Shuts down the protector. The protector is shut down and powered off immediately after the command is executed. |
| Parameters | N/A |
| Default | N/A |
| Example | `Websense1# shutdown` |

## Showing the Websense Protector version

| | |
|---|---|
| Syntax | `version` |
| Description | Displays the protector version information. |
| Parameters | N/A |
| Default | N/A |
| Example | `Websense1# version`<br>`This is Websense Content Protector 7.5.1.009,`<br>`Policy Engine 7.5.1.9 (Appliance 7.5.1.009)` |

## Setting or showing the system date

| | |
|---|---|
| Syntax | `date [-d] [dd-mmm-yyyy]` |
| Description | Sets or displays the date of the protector. By default, the command displays the current date. Otherwise, the argument is used to set the date of the protector.<br>`date` is also a native Linux command. **`Root`** users can access the CLI command by running it with its full path: `/opt/websense/neti/bin/date`. |
| Parameters | If the the **`–d`** option is given, the date is displayed or set using an all digit format (**`mm/dd/yyyy`**, for example: 02/21/2006). Otherwise, a **`dd-mmm-yyy`** format is used. **`dd`** is the day of the month [01 to 31]<br>**`mmm`** is the month in abbreviated 3-letter format [Jan, Feb, Mar, etc.]<br>**`yyyy`** is the year [2006, 2007] |
| Default | N/A |
| Example | `Websense1# date`<br>`21-Feb-2006` |

## Setting or showing the system time

| | |
|---|---|
| Syntax | `time -h [HH[:MM[:SS]]]` |

| | |
|---|---|
| Description | Sets or displays the time in the protector. By default, the command displays the current time.<br>`time` is also a native Linux command. **`Root`** users can access the CLI command by running it with its full path: `/opt/websense/neti/bin/time`. |
| Parameters | **-u** sets the time in UTC<br>**-h** displays a short usage message **HH:MM:SS HH** is the hour [00 to 24]<br>**MM** is the minutes [00 to 59]<br>**SS** is the seconds [00 to 59] |
| Default N/A | In the event that minutes and/or seconds are not entered, they are considered 00. |
| Example | `Websense1# time`<br>`17:55:03` |

## Modify or show system timezone

| | |
|---|---|
| Syntax | `timezone [list, show, set timezone]` |
| Description | Shows or sets the protector timezone. |
| Parameters | **list:** displays a complete list of time zones that can be set in the Websense Protector **show:** displays the time zone set in the Websense Protector (default option) **set** *timezone:* sets the time zone. The **set** command must be followed by the name of the time zone to be selected, as listed using the **list** command. Note that the names of the time zones are case-sensitive. |
| Default | When no argument is given, **show** is assumed. |
| Example | `Websense1# timezone set US/Hawaii` |

## Viewing protector information

| | |
|---|---|
| Syntax | `info { cpu \| memory \| network \| diag \| uptime \| hardware \| features} info stats [reset]` |
| Description | Displays information about the Websense protector.<br>**Root** users must access the CLI command by running it with its full path: `/opt/websense/neti/bin/info`. |
| Parameters | **cpu**: displays the protector's CPU usage information.<br>**memory**: displays the protector memory usage information.<br>**network**: displays the protector's network settings including hostname, domain name, IP address and routing table.<br>**diag**: creates a diagnostic file to be used by Websense technical services.<br>**uptime**: displays the amount of time the protector has been up and operational.<br>**features**: lists all the possible features available on this protector and what they can do (monitor or block)<br>**hardware:** displays hardware information including which network cards are installed.<br>**stats**: displays traffic statistis for each protocol being monitored; this is useful to verify the operational status of the Protector.<br>**stats reset**: resets all statistics counters to zero. |
| Default N/A | |
| Example | `Websense1# info cpu`<br>`Processor 1: 1.3% loaded (98.7% idle) Websense1# info memory`<br>`Free physical memory 8.7%` |

## Collecting statistics

| | |
|---|---|
| Syntax | `debug stats [-d] [-i` ***interval*** `\| -n` ***count*****]** |

| | |
|---|---|
| Description | This command allows a user to collect statistics about network behavior over time. It does so by running **info stats** at specified intervals for a given number of times. The collected statistics are saved in a CSV file for easy manipulation and analysis in spreadsheet tools such as Microsoft Excel. The resulting file is saved as **opt/pa/log/collect_stats.csv.gz** |
| Parameters | **-d:** delete previously recorded statistics information file, if one exists<br>**interval:** the interval in seconds between two runs that take a snapshot of the statistics.<br>**count:** how many times the statistics snapshot should be taken. |
| Default | The default interval is every 60 seconds. The default number is 1440 (which is the equivalent of 24 hours of statistics when the default interval of 60 is selected). |
| Example | `Websense# debug stats` |

## Configure or show the DNS server(s)

| | |
|---|---|
| Syntax | `dns [list \| delall] dns [{add \| del}] ip addr]` |
| Description | Lists, adds, or deletes DNS servers. |
| Parameters | **list:** displays a list of DNS servers in the protector<br>**delall:** deletes all DNS servers set in the protector<br>**add:** adds a DNS server specified by its IP address to the protector<br>**del:** deletes the DNS server denoted by the specified IP address |
| Default | N/A |
| Example | `Websense1# dns add 192.168.15.3` |

## Configure or show the default domain name(s)

| | |
|---|---|
| Syntax | `domain [list \| delall] domain [{add (-m) \| del} <domain>]` |
| Description | Lists, adds, or deletes default domain names in the protector. |
| Parameters | **list:** displays a list of configured default domain names in the protector<br>**delall:** deletes all default domain names set in the protector<br>**add:** adds a default domain name specified by *domain* to the protector<br>Use the **-m** switch to set a domain as main. The main domain is the domain that the protector is actually is a member of. Without the –m switch a 'search domain' is created. For the protector to resolve a domain this domain is searched as well. There may be many 'search domains' but only one main domain.<br>**del:** deletes the default domain name denoted by *domain* from the protector |
| Default | N/A |
| Example | `Websense1# domain add example.com` |

## Configure or show the default gateway

| | |
|---|---|
| Syntax | `gateway` ***ipaddr***<br>`gateway [list \| delete]` |
| Description | By default, displays the current defined gateway. Using the parameters, it is possible to set or delete the default gateway of the protector. |
| Parameters | **ipaddr:** when given, the ipaddr is used as a default gateway for the protector.<br>**list:** shows the configured default gateway.<br>**delete:** deletes the defined default gateway.<br>Please note that if this command is run from a remote SSH session, the session may terminate. |
| Default | N/A |
| Example | `Websense1# gateway 192.168.10.254` |

## Configure or show the host name

| | |
|---|---|
| Syntax | `hostname [name]` |
| Description | Displays the current host name. The parameter can also set a unique name by which to identify the protector. |
| Parameters | **name:** if given, the host name is set to the name given. Otherwise, the host name is displayed. |
| Default | N/A |
| Example | `Websense1# hostname 1Tokyo` |

## Configure or show interface information

| | |
|---|---|
| Syntax | `iface [list]`<br>`iface ifname [ip ipaddr] [prefix prefix] [bcast bcastaddr] [speed speed] [duplex duplex] [mgmt] [enable\|disable] [descr description]` |
| Description | Configures and displays the protector's network interface information. When invoked without arguments or with the **list** option, the command displays a list of all available interfaces in the system. When invoked with only an interface name, the command shows detailed information about that interface. Any other invocation method configures the interface denoted in **ifname**.<br>**Note:** When using this command to configure the management interface, we recommend you use a console connection to the protector (and not a remote SSH connection). Using the latter may terminate the session to the protector. In addition, if the IP address is changed, it may be required to re-establish secure communication with the Websense Data Security Server (by re-running the configuration wizard). |
| Parameters | **ip**: the IP address denoted by *ipaddr* is assigned to the interface. This option is valid only for the management interface. When setting **ip**, the **prefix** and **bcast** options must also be set<br>**prefix:** network mask of the interface. For example: 24 (will assign 255.255.255.0 mask to the interface)<br>**bcast:** broadcast address of the interface. For example: for an interface with the IP address 192.168.1.1/24, the broadcast address is usually 192.168.1.255.<br>**speed:** interface link speed. Available speeds: auto, 10, 100, 1000<br>**duplex:** interface link duplex. Available duplex options: auto, half, full<br>**mgmt:** sets the interface as the management interface of the protector. The previously defined management interface can no longer be used for management purposes.<br>**enable, disable:** enables or disables the interface (default is enable)<br>**descr:** assigns a short description for the interface. Note that if the description contains spaces, it must be enclosed within quotation marks (""). |
| Default | eth0 |
| Example | `Websense1# iface eth0 ip 10.100.16.20 prefix 24 bcast 10.100.16.255 mgmt enable` |

## Add or delete routing information

Syntax
```
route list
route add {destination network | destination ip}
{via ip | dev device}
route del {destination network | destination ip}
{via ip | dev device}
```

Description Adds or deletes route entries in the protector. When adding or deleting routes to networks, use the x.x.x.x/prefix format. For example: 192.168.1.0/24.

Parameters **list:** displays the routing table of the Protector
**add:** adds a route to a network or IP
**del:** deletes a route to a network or IP

Default N/A

Example
```
Websense1# route add 100.20.32.0/24 via
10.16.10.10
Websense1# route add 172.16.1.0/24 dev eth0
```

## Manage users

Syntax
```
user add {username} profile {profile} pwd
{password}
user del {username}
user mod {username} [profile {profile}] [pwd {new
password}]
user list
```

Description The **user** command allows you to define additional users who can access the system. Each user has a profile that defines the operations available to users. Available profiles:
**admin:** all commands are allowed
**netadmin:** only networking related commands are allowed
**policyadmin:** only the policy command is allowed

The list of commands each profile can run cannot be changed.

Parameters **add:** add a user with the given profile and password
**del:** delete a user
**mod:** modify a user's profile and/or password
**list:** display a list of all defined users and their profiles

Default N/A

Example
```
Websense1# user add Jonny profile netadmin pwd
123qwe
```

## Filtering monitored networks

You can use the Websense Management Interface to define which networks are monitored by the protector.

This CLI command enables advanced filtering of monitored networks.

> **Note**
> Websense recommends that you test the filter using a tcpdump command before setting the filter to ensure that the filter expression is recognized by the protector.

| | |
|---|---|
| Syntax | `filter [show \| set rule \| delete]` |
| Parameters | **show:** displays the current active filters - monitored networks<br>**set:** defines a list of monitored networks<br>**delete:** deletes previously set filter rules |
| Default | N/A |
| Example | `Websense1# filter set "tcp and host 10.0.0.1"`<br>Sets the protector to monitor all TCP traffic to/from 10.0.0.1 and ignore all other hosts in the network. If VLAN is used, it should be listed first in the filter (**vlan and tcp**, not **tcp and vlan**). |

# Configuring NTP support

The protector includes an NTP package which contains a NTPD service and a set of related utilities.The service is turned off by default. Enabling the NTP service is simple, but requires very customer-dependent configuration settings. Thus, the following procedure is a general description of the steps that should be executed in order to enable the service.

The NTP service requires **`root`** user permissions.

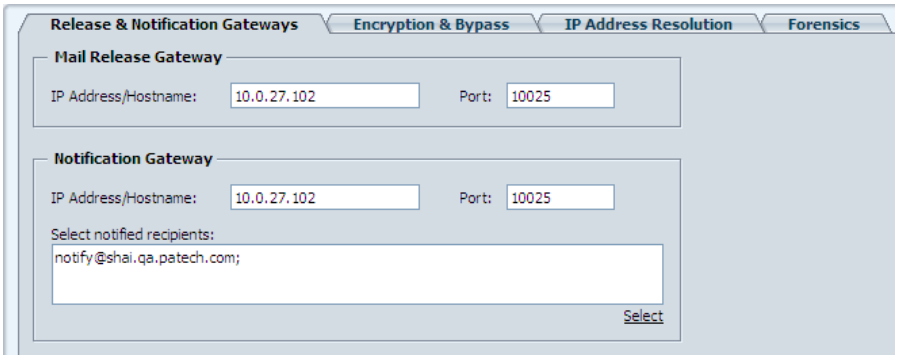
For further NTP configuration details, refer to: http://en.linuxreviews.org/NTP_-_Howto_make_the_clock_show_the_correct_time, or http://doc.ntp.org/4.2.2/**,** and many other sites on the Web.

## Configuration

1. Decide and define the NTP server(s) to be used.
2. Firewall configurations (considering the bullet above): NTP port is UDP 123.
3. Edit the relevant configuration files (/etc/ntp.conf, etc`).

## Execution

1. Perform an initial time synchronization. This can be done manually via the protector's Wizard, or by using the 'ntpdate' utility.




2. From the command line, type `chkconfig ntpd on|off` to start/not start the service each time the protector machine is started.
3. Type `service ntpd start|stop|restart` to explicitly start/stop/restart the service.
4. Type `ntpq -p` to verify the synchronization is correct.

# 37 Email Security Gateway (V5000 G2)

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V5000 G2 v7.6

## In this topic



## Overview

This section of the Websense Technical Library contains information and instructions for deploying Websense Email Security Gateway or Websense Email Security Gateway Anywhere based on a Websense V5000 G2 appliance. For a V10000-G2-based deployment see *Email Security Gateway (V10000 G2)*, page 585.

### Websense hybrid email service

If your subscription includes Email Security Gateway Anywhere, you can enable the Websense hybrid email service. This is an in-the-cloud service that provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach the network and considerably reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

### Websense V5000 G2

The Websense V5000 G2 appliance provides the majority of Email Security Gateway functions. Incoming email flows from the hybrid email service (if enabled) to the Websense appliance and to your mail server.

The Websense appliance also provides the Personal Email Manager facility for end users to manage quarantined email.

### Mail server

This is your internal mail server; not provided by Websense, Inc.

### TRITON management server

A separate *TRITON management server* is required. *TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and any or all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security). In the case of an Email Security Gateway deployment, the Data Security and Email Security modules are required. Email Security Log Server may also be installed on this machine (note that this component may be installed on another machine; it is not required to be located on the TRITON management server).

The Data Security module of the TRITON Unified Security Center works with the Websense appliance to provide email DLP (data loss prevention) features.

### Microsoft SQL Server

Microsoft SQL Server, running on a Windows server in your network, is used to store Websense logging and reporting data. Quarantined email are also stored here.

SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running. SQL Server Express (installed using the Websense installer) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

## Deployment


- *Email Security Gateway system requirements*, page 596
- *Email Security Gateway single-appliance deployments*, page 597
- *Email Security Gateway multiple-appliance deployments*, page 600

# Installation

Complete the following procedures in the order in which they are listed.

1. *Obtaining SQL Server*
2. *Setting up the appliance*
3. *Installing Email Security Log Server*
4. *Creating a TRITON Management Server*
   - The above link goes to general instructions for creating a TRITON management server. As you follow them, choose to install both the*Applies to* and *TRITON - Data Security* modules of TRITON Unified Security Center: when you reach the **Installation Type** screen, select **Email Security (requires Data Security)** under TRITON Unified Security Center. Data Security will automatically be selected along with Email Security, because it is required for Email DLP (data loss prevention) features.

# Initial configuration

The first time you access TRITON - Email Security, you are prompted for your subscription key. Then, you are asked if you want to use the First-Time Configuration Wizard. This wizard guides you through the process of entering essential configuration settings. It is strongly recommended you use this wizard. See the TRITON - Email Security Help for more information.

**Important**

The Configuration Wizard is offered only once, at initial start up of TRITON - Email Security. If you choose to not use the Wizard it will no longer be available. All settings configured in the Wizard can be configured in TRITON - Email Security individually. The Wizard is simply offers a more convenient way to enter essential settings.

See the *Getting Started* section of the TRITON - Email Security Help for information on initial configuration. Be sure to complete the procedures for:

- Domain based route
- Trusted inbound mail
- Data Security
- Email Security Log Server
- Notification

If your subscription includes Email Security Gateway Anywhere, configure the hybrid email service. See the “Registering for the hybrid service” topic in the TRITON - Email Security Help.

# Setting up the appliance

## Applies to

- Email Security Gateway v7.6
- V5000 G2 v7.6

## In this topic



## Overview

> **Note**
> If you have already completed the appliance set up steps provided in the *Websense V-Series Getting Started* guide, skip to *Installing Email Security Log Server*, page 583.

The Quick Start poster, which comes in the shipping box with your appliance, shows you all items included in each Websense appliance shipping box. The 2-page Quick Start explains how to set up the hardware and shows how to connect the cables to the appliance and to your network.

Interface C, P1, and P2 (if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet once the appliance is operational. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that C, and P1 or P2 (if used), are able to access the download servers at **download.websense.com**.
- Make sure that this address is permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the C, P1, and P2 interfaces can access.

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance.

See the next section.

# Perform initial command-line configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for the network interface labeled C and a few other general items. You can run the script again if you want to examine your settings or change settings. You can also change settings through the Appliance Manager (user interface) after firstboot has been executed.

Gather the following information before running the script. Some of this information may have been written down on the Quick Start during hardware setup.

| | |
|---|---|
| Hostname | |
| IP address for network interface C | |
| Subnet mask for network interface C | |
| Default gateway for network interface C (IP address) *Optional*<br><br>**Note:** If you do not provide access to the Internet for interface C, configure:<br>• P1 to download antispam and antivirus database updates from Websense (Email Security mode)<br>Configuring these interfaces to access the Internet for database downloads is done through the Appliance Manager and through the TRITON Unified Security Center. See the Appliance Manager Help for information about configuring the interfaces. See the TRTION - Email Security Help for information about configuring database downloads. | |
| Primary DNS server for network interface C (IP address) | |
| Secondary DNS server for network interface C (IP address) *Optional* | |
| Tertiary DNS server for network interface C (IP address) *Optional* | |
| Unified password (8 to 15 characters, at least 1 letter and 1 number)<br>This password is for initial access to the Appliance Manager. | |

When you have gathered the necessary information, run the initial command line configuration, as follows.

1. Access the appliance through a USB keyboard and monitor or a serial port connection.

   **Note**

   To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

   - 9600 bits per second
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```

4. At the first prompt, select **Email Security only** mode.
5. Follow the on-screen instructions to provide the information collected above.

After the activation script has been completed successfully, access the Appliance Manager. Open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

## Configure the appliance

The Appliance Manager is the Web-based configuration interface for the appliance. Through it you can view system status, configure network and communication settings, and perform general appliance administration tasks.

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces P1 and (optionally) P2.

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

| | |
|---|---|
| Primary NTP server<br>*Optional*<br>Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C. | Domain: |
| Secondary NTP server<br>*Optional* | Domain: |

| | |
|---|---|
| Tertiary NTP server<br>*Optional* | Domain: |
| IP address for network interface P1 | IP address: |
| Subnet mask for network interface P1 | Subnet mask: |
| Default gateway for network interface P1 and P2 (if used)<br>If you use both P1 and P2, the default gateway is automatically assigned to P2 (which is bound to eth1). | IP address: |
| Primary DNS server for network interface P1 and P2 (if used) | IP address: |
| Secondary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| IP address for network interface P2<br>*Required only if P2 is enabled* | IP address: |
| Subnet mask for network interface P2<br>*Required only if P2 is enabled* | Subnet mask: |

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to configure basic system and network interface settings. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   `https://<IP address>:9447/appmng`

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance (see *Perform initial command-line configuration*)
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration** > **System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:

- **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
- **Manually set time and date**: select this option to enter a system time and date yourself.

c. Click **Save** in the Time and Date area.

5. In the left navigation pane, click **Configuration > Network Interfaces**.
6. Under **Websense Email Security Gateway Interfaces (P1 and P2)**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' requests (inbound traffic) and communicate with the Internet (outbound traffic).

   To configure the P interfaces:

   a. Select whether **P1 only** or both **P1 and P2** are used.

      If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

      If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

   b. Click **Save** in the **Websense Email Security Gateway Interfaces (P1 and P2)** area when you are done.

   When only P1 is used, it handles both inbound and outbound traffic.

   Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic.

   See the Appliance Manager Help for more information about configuring Email Security interfaces.

7. Configure routes if necessary:

   a. In the left navigation pane, click **Configuration > Routing**.

   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

   c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

   d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

   **Note**

   An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

   See the Appliance Manager Help for more information about static and module routes.

8. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

# Installing Email Security Log Server

## Applies to

- Email Security Gateway v7.6
- V5000 G2 v7.6

## Installing Email Security Log Server

Email Security Log Server, which logs email security data to the Websense email security database, must run off-appliance (i.e., on a separate machine).

To install Email Security Log Server, perform a custom installation on the machine on which you want to install. See *Installing Email Security Components* for instructions. Note that you can choose to install Email Security Log Server during TRITON Unified Security Center installation on the same machine. If you want to do this, it is not necessary to perform a custom installation on another machine. Be sure to select Email Security Log Server when completing the procedures for creating a TRITON management server.

# 38 Email Security Gateway (V10000 G2)

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## In this topic



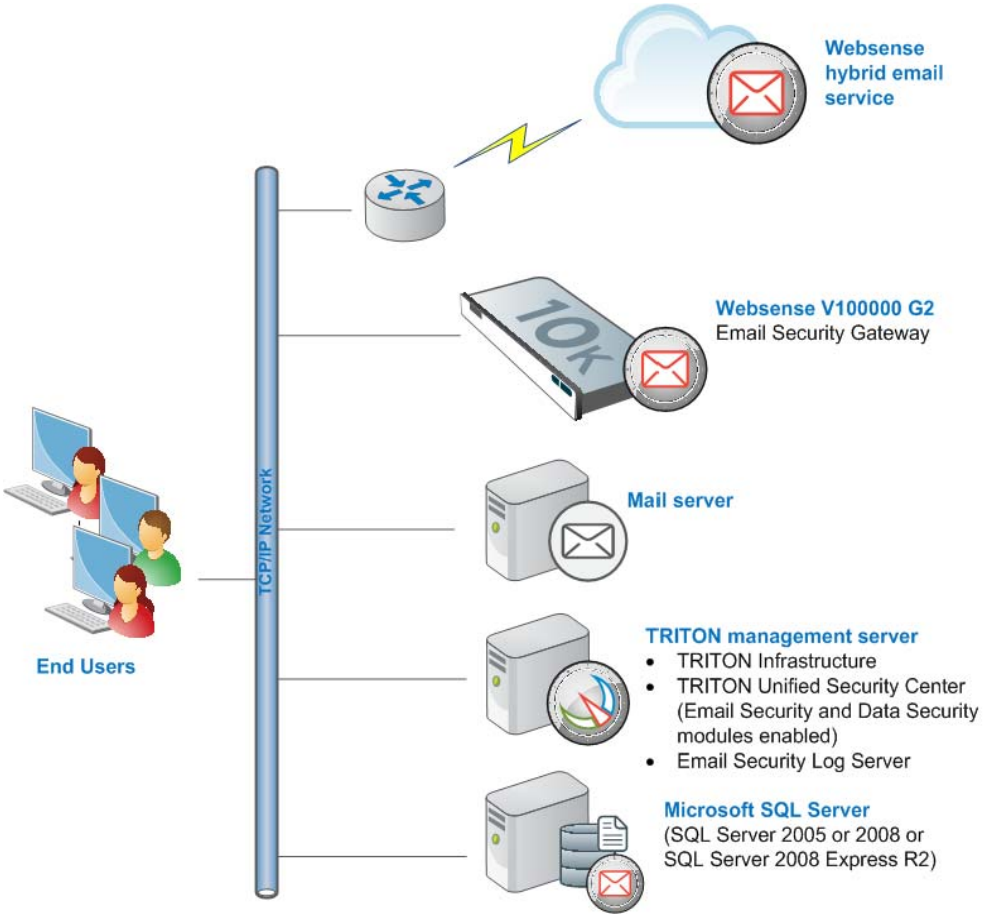
## Overview

This section contains information and instructions for installing Websense Email Security Gateway or Websense Email Security Gateway Anywhere based on a Websense V10000 G2 appliance. For a V5000-G2-based deployment see *Email Security Gateway (V5000 G2)*, page 575.

Note that this section applies to a deployment in which the appliance is configured to *Email Security only* mode. If you are deploying a V10000 G2 in *Web and Email Security* mode, see *Web and Email Security Gateway (V10000 G2)*, page 607 or *Web Security Gateway Anywhere and Email Security Gateway (V10000 G2)*, page 621.

The following illustration is a high-level diagram of a basic appliance-based deployment of Email Security Gateway. Note that this illustration is intended to show

the general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).




### Websense hybrid email service

If your subscription includes Email Security Gateway Anywhere, you can enable the Websense hybrid email service. This is an in-the-cloud service that provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach the network and considerably reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

### Websense V10000 G2

The Websense V10000 G2 appliance provides the majority of Email Security Gateway functions. Incoming email flows from the hybrid email service (if enabled) to the Websense appliance and to your mail server.

The Websense appliance also provides the Personal Email Manager facility for end users to manage quarantined email.

### Mail server

This is your internal mail server; not provided by Websense, Inc.

### TRITON management server

A separate *TRITON management server* is required. *TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and any or all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security). In the case of an Email Security Gateway deployment, the Data Security and Email Security modules are required. Email Security Log Server may also be installed on this machine (note that this component may be installed on another machine; it is not required to be located on the TRITON management server). Multiple instances of Email Security Log Server can be used in a deployment.

The Data Security module of the TRITON Unified Security Center works with the Websense appliance to provide email DLP (data loss prevention) features.

### Microsoft SQL Server

Microsoft SQL Server, running on a Windows server in your network, is used to store Websense logging, reporting, and some configuration data. Quarantined email are also stored here.

SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using TRITON Unified Security Setup) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

## Deployment


- *Email Security Gateway system requirements*, page 596
- *Email Security Gateway single-appliance deployments*, page 597
- *Email Security Gateway multiple-appliance deployments*, page 600


## Installation

Complete the following procedures in the order in which they are listed.

1. *Obtaining SQL Server*
2. *Setting up the appliance*
3. *Installing Email Security Log Server*
4. *Creating a TRITON Management Server*

   The above link goes to general instructions for creating a TRITON management server. As you follow those instructions, choose to install both the *TRITON -*

*Email Security* and *TRITON - Data Security* modules of TRITON Unified Security Center: when you reach the **Installation Type** screen, select **Email Security (requires Data Security)** under TRITON Unified Security Center. Data Security will automatically be selected along with Email Security, because it is required for Email DLP (data loss prevention) features.

# Initial configuration

The first time you access TRITON - Email Security, you are prompted for your subscription key. Then, you are asked if you want to use the First-Time Configuration Wizard. This wizard guides you through the process of entering essential configuration settings. It is strongly recommended you use this wizard. See the TRITON - Email Security Help for more information.

**Important**

The Configuration Wizard is offered only once, at initial start up of TRITON - Email Security. If you choose to not use the Wizard it will no longer be available. All settings configured in the Wizard can be configured in TRITON - Email Security individually. The Wizard is simply offers a more convenient way to enter essential settings.

See the *Getting Started* section of the TRITON - Email Security Help for information on initial configuration. Be sure to complete the procedures for:

- Domain based route
- Trusted inbound mail
- Data Security
- Email Security Log Server
- Notification

If your subscription includes Email Security Gateway Anywhere, configure the hybrid email service. See the “Registering for the hybrid service” topic in the TRITON - Email Security Help.

# Setting up the appliance

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## In this topic



## Overview

> **Note**
> If you have already completed the appliance set up steps provided in the *Websense V-Series Getting Started* guide, skip to

The Quick Start poster, which comes in the shipping box with your appliance, shows you all items included in each Websense appliance shipping box. The 2-page Quick Start explains how to set up the hardware and shows how to connect the cables to the appliance and to your network.

Network interfaces C, E1, and E2 (if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet once the appliance is operational. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that C, and E1 or E2 (if used), are able to access the download servers at **download.websense.com**.
- Make sure that this address is permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the C, E1, and E2 interfaces can access.

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance.

Continue on to the next section to complete the initial configuration.

## Perform initial command-line configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for the network interface labeled C and a few other general items. You can run the script again if you want to examine your settings or change settings. You

can also change settings through the Appliance Manager (user interface) after firstboot has been executed.

Gather the following information before running the script. Some of this information may have been written down on the Quick Start during hardware setup.

| | |
|---|---|
| Hostname | |
| IP address for network interface C | |
| Subnet mask for network interface C | |
| Default gateway for network interface C (IP address) *Optional*<br><br>NOTE: If you do not provide access to the Internet for interface C, configure:<br>• E1 or P1 to download antispam and antivirus database updates from Websense (Email Security mode)<br>Configuring these interfaces to access the Internet for database downloads is done through the Appliance Manager and through the TRITON Unified Security Center. See the Appliance Manager Help for information about configuring the interfaces. See the TRTION - Email Security Help for information about configuring database downloads. | |
| Primary DNS server for network interface C (IP address) | |
| Secondary DNS server for network interface C (IP address) *Optional* | |
| Tertiary DNS server for network interface C (IP address) *Optional* | |
| Unified password (8 to 15 characters, at least 1 letter and 1 number)<br>This password is for the Appliance Manager. | |

When you have gathered the necessary information, run the initial command line configuration, as follows.

1. Access the appliance through a USB keyboard and monitor or a serial port connection.

   **Note**

   To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

   - 9600 bits per second
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```
4. At the first prompt, select **Email Security only** mode.
5. Follow the on-screen instructions to provide the information collected above.

After the activation script has been completed successfully, access the Appliance Manager. Open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

## Configure the appliance

The Appliance Manager is the Web-based configuration interface for the appliance. Through it you can view system status, configure network and communication settings, and perform general appliance administration tasks.

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces E1, E2, P1, and P2 (E2, P1, and P2 are optional). Interfaces P1 and P2 can be bonded to E1 and E2, respectively, either for load balancing or active/standby.

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

| | |
|---|---|
| Primary NTP server<br>*Optional*<br>Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C. | Domain: |
| Secondary NTP server, (domain) *Optional* | Domain: |
| Tertiary NTP server, (domain) *Optional* | Domain: |
| IP address for network interface E1 | IP address: |
| Subnet mask for network interface E1 | Subnet mask: |
| Default gateway for network interface E1 and E2 (if used)<br>If you use both E1 and E2, the default gateway and DNS configuration are shared by both. | IP address: |

| | |
|---|---|
| Primary DNS server for network interface E1 and E2 (if used) | IP address: |
| Secondary DNS server for network interface E1 and E2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface E1 and E2 (if used)<br>*Optional* | IP address: |
| IP address for network interface E2<br>*Required only if E2 is enabled* | IP address: |
| Subnet mask for network interface E2<br>*Required only if E2 is enabled* | IP address: |
| Bond expansion interface P1 to E1? Yes or No<br>*Optional* | If Yes, choose one: Active/standby or Load balancing |
| Bond expansion interface P2 to E2? Yes or No<br>*Optional* | If Yes, choose one: Active/standby or Load balancing |

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to configure basic system and network interface settings. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   `https://<IP address>:9447/appmng`

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance (see *Perform initial command-line configuration*).

   For information about supported browsers, see *System Requirements*, page 41.
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration** > **System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.
   c. Click **Save** in the Time and Date area.

5. In the left navigation pane, click **Configuration** > **Network Interfaces**.
6. Under **Websense Email Security Gateway Interfaces (E1 and E2)**, configure the E1 and E2 (optional) interfaces.

   The E interfaces are used to accept users' requests (inbound traffic) and communicate with the Internet (outbound traffic).

   To configure the E interfaces:

   a. Select whether **E1 only** or both **E1 and E2** are used.

      If you choose E1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **E1**.

      If you choose E1 and E2, enter configuration information under both **E1** and **E2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both E1 and E2.

   b. Click **Save** in the **Websense Email Security Gateway Interfaces (E1 and E2)** area when you are done.

   When only E1 is used, it handles both inbound and outbound traffic.

   Alternatively, you could use both E1 and E2 such that E1 handles inbound traffic and E2 handles outbound traffic.

   See the Appliance Manager Help for more information about configuring E1 and E2.
7. Under **Expansion Interfaces (P1 and P2)**, choose whether to bond to P1 and P2 to E1 and E2.

   Interfaces P1 and P2 can be cabled to your network and then bonded through software configuration to E1 and E2. If you choose to bond the interfaces, P1 must be bonded to E1 and P2 to E2. No other pairing is possible.

   You can choose to bond or not bond E1 and E2 independently. You do not have to bond both. Also, you can choose different bonding modes for E1 and E2 (e.g., E1/P1 could be **Active/Standby** while E2/P2 could be **Load balancing**).

   Make sure all interfaces are cabled properly before configuring bonding.

   To bond P1 to E1:

   a. Under **P1**, select the check box for **Bond to E1 interface**.
   b. Under P1/E1 bonding mode, select:
      - **Active/Standby**: Select this for failover. E1 is active, and P1 is in standby mode. Only if the primary interface fails would its bonded interface (P1) become active.
      - **Load balancing**: Select this for load balancing. If your switch or router supports load balancing, then traffic to and from the primary interface is balanced between the primary interface (E1) and its bonded interface (P1).
   c. Click **Save** in the **Expansion Interfaces (P1 and P2)** area.

   To bond P2 to E2:

   Follow the instruction above for bonding E1 to P1, substituting E2 in place of E1 and P2 in place of P1. Make sure E2 is enabled. Otherwise the **P2** options will be inactive. (See Step 6 for instructions on activating E2.)
8. Configure routes if necessary:

a. In the left navigation pane, click **Configuration** > **Routing**.
b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.
c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.
d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

See the Appliance Manager Help for more information about static and module routes.

9. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

# Installing Email Security Log Server

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## Installing email Security Log Server

Email Security Log Server, which logs email security data to the Websense email security database, must run off-appliance (i.e., on a separate machine).

To install Email Security Log Server, perform a custom installation on the machine on which you want to install. See *Installing Email Security Components* for instructions. Note that you can choose to install Email Security Log Server during TRITON Unified Security Center installation on the same machine. If you want to do this, it is not necessary to perform a custom installation on another machine. Be sure to select Email Security Log Server when completing the procedures for creating a TRITON management server.

# 39 Websense Email Security Gateway Deployment

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Websense Email Security Gateway deployment

Websense® Email Security Gateway provides maximum protection for email systems to prevent malicious threats from entering an organization's network. Email Security provides comprehensive on-premises security hosted on a Websense V-Series appliance (V10000 G2 and V5000 G2). Email Security management functions reside on a separate Windows server in the TRITON™ Unified Security Center.

Each email message is scanned by a robust set of antivirus and antispam filters to prevent infected email from entering a network. Inbound, outbound, and internal email policies can be applied to specified sets of senders and recipients. Websense Email Security Gateway Anywhere adds support for a hybrid service pre-filtering capability "in the cloud," which scans incoming email against a database of known spam and viruses.

Integration with Websense Data Security provides valuable protection for an organization's most sensitive data. Policies configured in the Data Security module can detect the presence of company data and block the release of that data. Data Security can also determine whether a message should be encrypted and pass the message to an encryption server.

Logging and reporting capabilities allow an organization to view system and message status and generate reports of system and email traffic activity. The Email Security Log Database is either installed on the TRITON management server or hosted on a remote Microsoft® SQL Server®.

A Personal Email Manager facility allows authorized end users to manage email messages that Email Security policy has blocked but that may be safe to deliver. End users can maintain individual Always Block and Always Permit lists of email addresses to simplify message delivery.

System requirements and deployment options are discussed in the following topics:

# Email Security Gateway system requirements

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Email Security Gateway system requirements

Every Email Security Gateway deployment includes the following components at a minimum:

**DMZ**

- Websense V-Series appliance (V10000 G2 or V5000 G2)

  Email traffic volume in your network may determine which type of appliance you use.

**Internal LAN**

- TRITON Unified Security Center management server
- Email Security Log Database
- Mail exchange server
- End-user clients

> **Note**
> All these Email Security Gateway components must be located and installed in the same time zone for proper system communication.

The DMZ in the network contains the devices that have direct contact with the Internet. This zone is a buffer between the Internet and the internal LAN. In our examples, the V-Series appliance and any router, switch, or load balancer adjacent to the firewall are located in the DMZ.

The TRITON management server includes Email Security and Data Security management functionality, along with the Email Security Log Server.

> **Note**
>
> Using the Microsoft Bulk Copy Program (BCP) utility can result in faster database record insertion. BCP inserts records into the database in batches, as opposed to using ODBC, which inserts records individually.
>
> BCP is available only if the SQL Server Client Tools are installed on the Email Security Log Server machine before Log Server is installed.
>
> Configure BCP in the Email Security Log Server Configuration wizard.
>
> Use of the BCP utility is recommended for efficient database performance efficiency.

Microsoft SQL Server handles the message database and stores Email Security configuration settings. SQL Server may be installed on the TRITON management server or on a dedicated server. For optimal performance, Websense recommends that SQL Server be installed on a separate, dedicated machine. For information about database systems in Websense products, see Administering Websense Databases.

The Email Security appliance is the portal for Personal Email Manager end users who are authorized to manage their own blocked mail. The Personal Email Manager end user options are configured in the Email Security management server interface, where administrators determine which end users can access the utility and what the blocked email notification message contains. An Email Security administrator can also designate the end users who are allowed to manage personal Always Block and Always Permit lists.

In the samples in this guide, the V-Series appliances are all running in Email Security only mode. See *Web and Email Security Gateway (V10000 G2)* to view a sample diagram with an appliance running in dual Email Security Gateway/Web Security Gateway mode.

See *System Requirements* to view the hardware and system operating requirements for Email Security Gateway components.

# Email Security Gateway single-appliance deployments

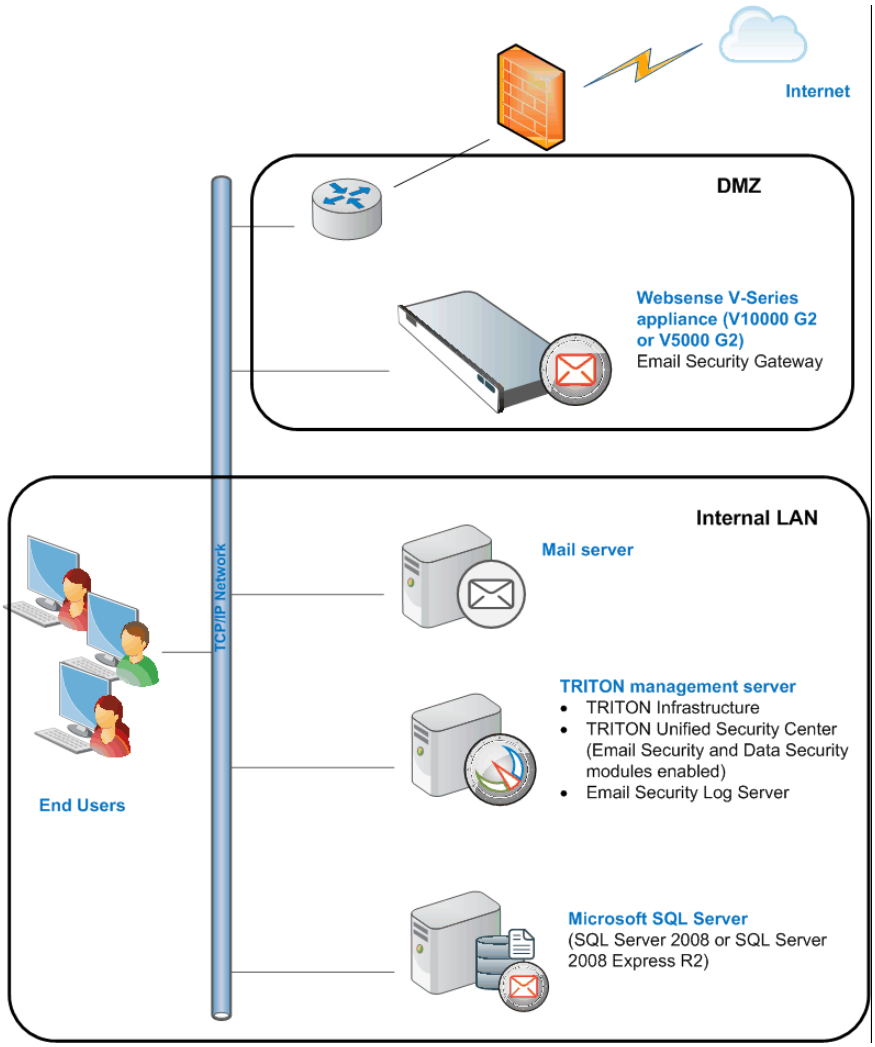
## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## In this topic



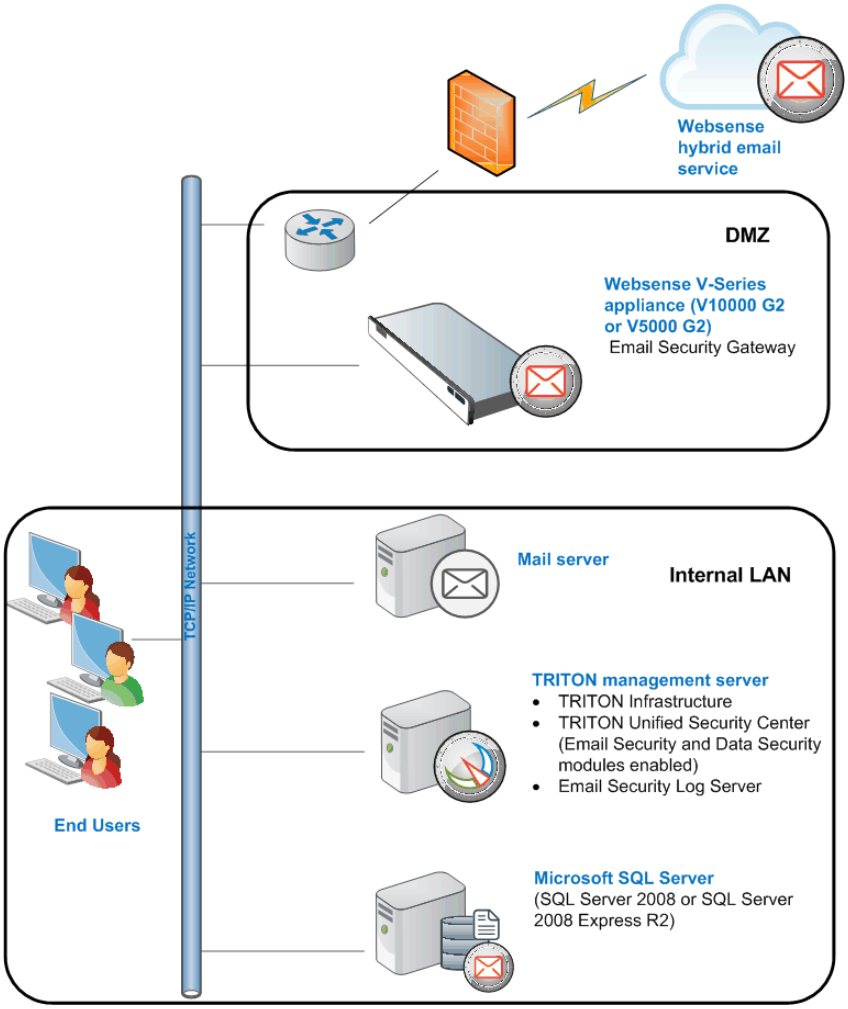
## Single appliance




This simple deployment uses a single V-Series appliance, which can be either a V10000 G2 or V5000 G2 machine.

In this Email Security Gateway installation, all spam and virus filtering occurs in Email Security Gateway using the product's collection of antispam and antivirus engines and tools. Data Security data loss prevention (DLP) policies filter mail for acceptable usage and sensitive company data. See the *TRITON - Email Security Help* for information about Email Security filtering tools.

# Single appliance with hybrid service




This deployment uses a single V-Series appliance, which can be either a V10000 G2 or V5000 G2 machine.

This Email Security Gateway Anywhere environment includes the Email Security hybrid service “in the cloud” filtering. Register for the hybrid service in the Email Security Gateway management interface (**Settings > General > Hybrid Configuration**). See the *TRITON - Email Security Help* for details.

The hybrid service prevents malicious email traffic from entering a company’s network by:

- Dropping a connection request based on the reputation of the IP address of the request
- Scanning inbound email against a database of known spam and viruses, and dropping any message that matches a database entry

The hybrid service may also share spam and virus detection information by writing extended headers in the mail it sends to Email Security Gateway. The additional header information includes a spam/virus detection "score," which Email Security then uses to determine message disposition.

# Email Security Gateway multiple-appliance deployments

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## In this topic



## Overview

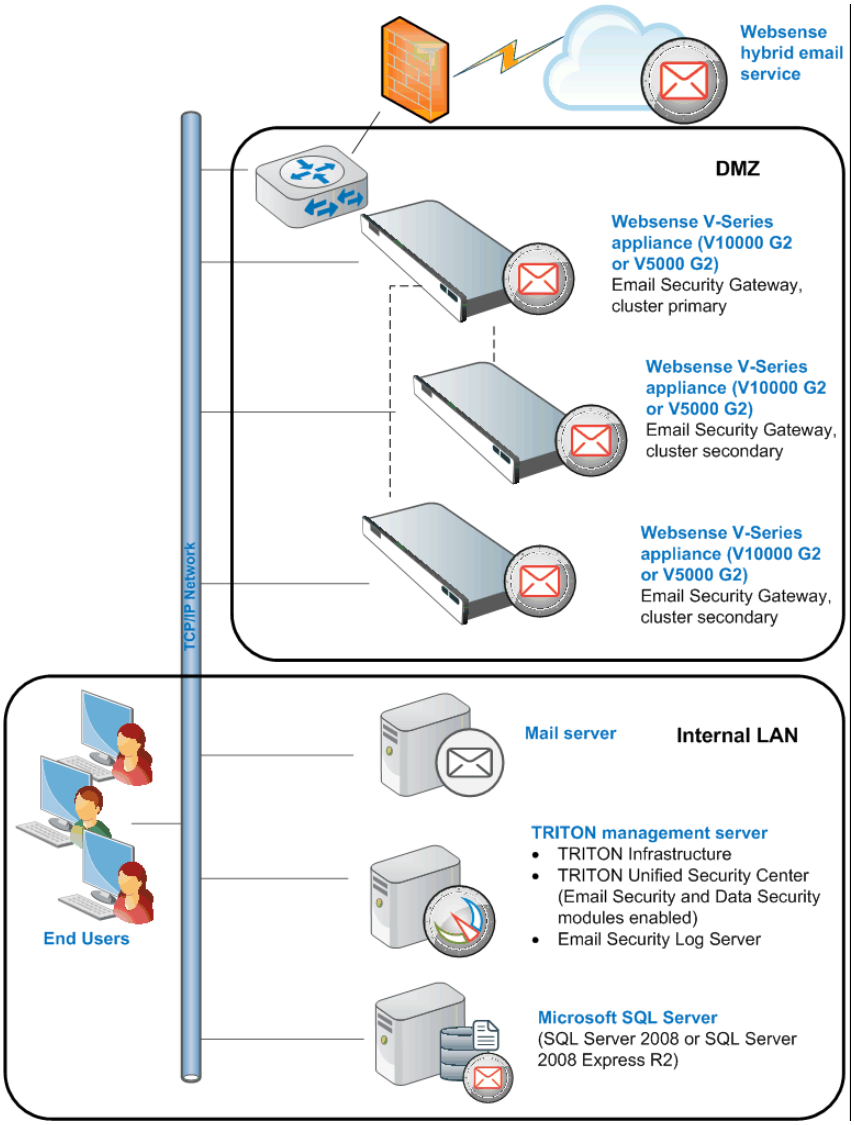
Multiple V-Series appliance deployments can be implemented when message traffic volume warrants having greater processing capacity. When the deployed appliances are all in standalone mode, the appliances can be either V10000 G2 or V5000 G2 machines. In an appliance cluster, however, all the machines must be V10000 G2 or V5000 G2 machines. The cluster cannot contain a mix of appliance platforms.

## Email Security Gateway appliance cluster

Multiple V-Series appliances are configured in Email Security Gateway as a cluster for this deployment. Appliances in a cluster must be either all V10000 G2 machines or all V5000 G2 machines. A cluster cannot contain a mix of different appliance platforms.

You may want to use a third-party load balancer with an appliance cluster, to distribute email traffic among your appliances. Appliances in a cluster all have the same configuration settings, which can streamline a load balancing implementation.

Add an appliance to the Email Security appliances list on the **Settings > General > Email Appliances** page. Configure available appliances in a cluster on the **Settings > General > Cluster Mode** page. See the *TRITON - Email Security Help* for details.




A primary appliance in a cluster may have up to 7 secondary (auxiliary) appliances. Configuration settings for any cluster appliance are managed only on the primary appliance Email Appliances page (**Settings > General > Email Appliances**).

Cluster appliances must all be running in the same deployment mode (Email Security only mode or dual Email Security/Web Security mode). The Email Security Gateway management server and cluster appliance versions must all match for cluster communication to succeed.

In order to protect the messages stored in Email Security queues, appliances added to a cluster must have the same message queue configuration as the other cluster appliances. For example, an administrator-created queue on appliance B must be configured on primary cluster appliance A before appliance B is added to the cluster. Message queue records may be lost if this step is not performed.

This Email Security Gateway Anywhere environment includes the Email Security hybrid service “in the cloud” filtering. Register for the hybrid service in the Email Security Gateway management interface (**Settings > General > Hybrid Configuration**). See the *TRITON - Email Security Help* for details.

The hybrid service prevents malicious email traffic from entering a company’s network by:

- Dropping a connection request based on the reputation of the IP address of the request
- Scanning inbound email against a database of known spam and viruses, and dropping any message that matches a database entry

The hybrid service may also share spam and virus detection information by writing extended headers in the mail it sends to Email Security Gateway. The additional header information includes a spam/virus detection “score,” which Email Security then uses to determine message disposition.

## Multiple standalone appliances with load balancing

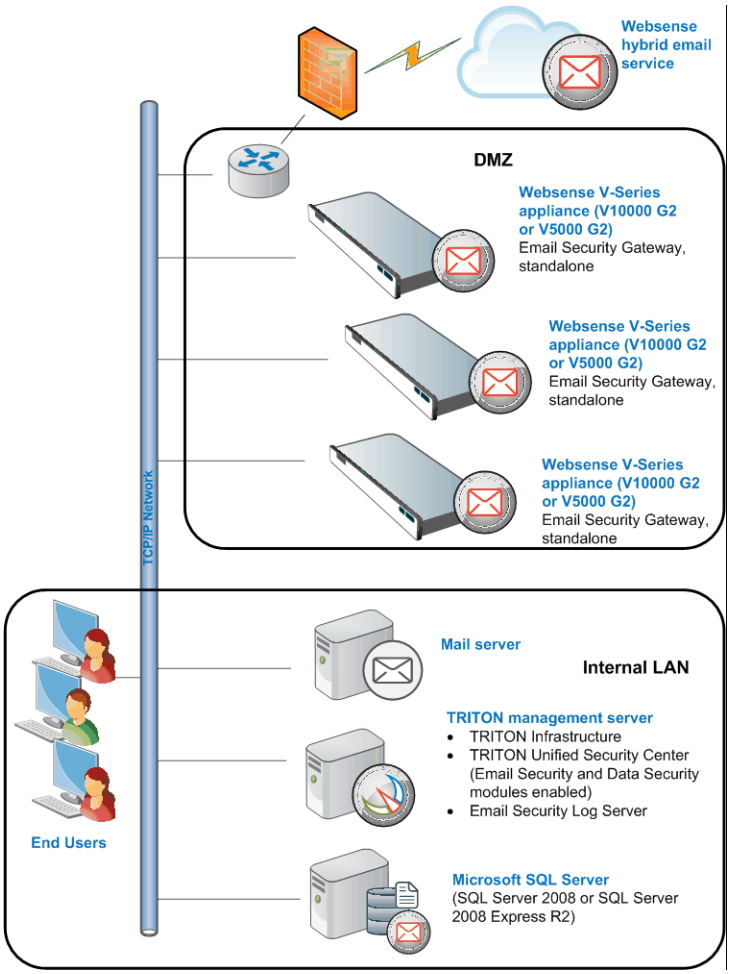
A multiple standalone appliance deployment might be useful if each appliance must have different configuration settings.

Email traffic distribution among multiple standalone appliances can be accomplished by using the domain name system (DNS) round robin method for distributing load.

With Email Security hybrid service configured and running, set up the round robin system as follows:

1. Enter the SMTP server domain in the Delivery Route page of the hybrid service configuration wizard used for registering Email Security Gateway with the hybrid service (**Settings > General > Hybrid Configuration**).
2. Register the IP addresses of the appliances you want subject to the round robin method in the SMTP domain.

If hybrid service is not enabled, you need to modify your MX records to allow round robin load balancing. Ask your DNS manager (usually your Internet service provider) to replace your current MX records with new ones for load balancing that have a preference value equal to your current records.




This Email Security Gateway Anywhere environment includes the Email Security hybrid service "in the cloud" filtering. Register for the hybrid service in the Email Security Gateway management interface (**Settings > General > Hybrid Configuration**). See the *TRITON - Email Security Help* for details.

The hybrid service prevents malicious email traffic from entering a company's network by:

- Dropping a connection request based on the reputation of the IP address of the request
- Scanning inbound email against a database of known spam and viruses, and dropping any message that matches a database entry

The hybrid service may also share spam and virus detection information by writing extended headers in the mail it sends to Email Security Gateway. The additional

header information includes a spam/virus detection "score," which Email Security then uses to determine message disposition.

## Multiple standalone appliances with domain-based routing

You can configure domain-based delivery routes so that messages sent to recipients in specified domains are delivered to a particular appliance.

Configure the domain groups for which you want to define delivery routes in the **Settings > General > Domain Groups > Add Domain Groups** page. See the *TRITON - Email Security Help* for information about adding or editing domain groups.

To set up a domain-based delivery route on the **Settings > Receive/Send > Mail Routing** page:

1. Click **Add** in the Domain-based Routes section to open the Add Domain-based Route page.
2. Enter a name for your route in the **Route name** field.
3. Select an order number from the **Route order** drop-down list to determine the route's scanning order.
4. Select a destination domain from the pre-defined domains in the **Domain group** drop-down list. Default is Protected Domain. Information about the domain group appears in the Domain details box.

   If you want to add a new domain group to the list, navigate to**Settings > General > Domain Groups** and click **Add**.

   If you want to edit your selected domain group, click **Edit** to open the Edit Domain Group page.
5. Select the **SMTP server IP address** option.
6. Enter the SMTP server IP address or host name and port. Mark the check box to enable MX lookup. Click the right arrow to add the SMTP server information to the SMTP Server List. Mail for that domain group is delivered to the specified SMTP server for routing to the domain address.

This Email Security Gateway Anywhere environment includes the Email Security hybrid service "in the cloud" filtering. Register for the hybrid service in the Email Security Gateway management interface (**Settings > General > Hybrid Configuration**). See the *TRITON - Email Security Help* for details.

The hybrid service prevents malicious email traffic from entering a company's network by:

- Dropping a connection request based on the reputation of the IP address of the request
- Scanning inbound email against a database of known spam and viruses, and dropping any message that matches a database entry

The hybrid service may also share spam and virus detection information by writing extended headers in the mail it sends to Email Security Gateway. The additional

header information includes a spam/virus detection “score,” which Email Security then uses to determine message disposition.

# 40 Web and Email Security Gateway (V10000 G2)

## Applies to

- Web Security Gateway v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## In this topic

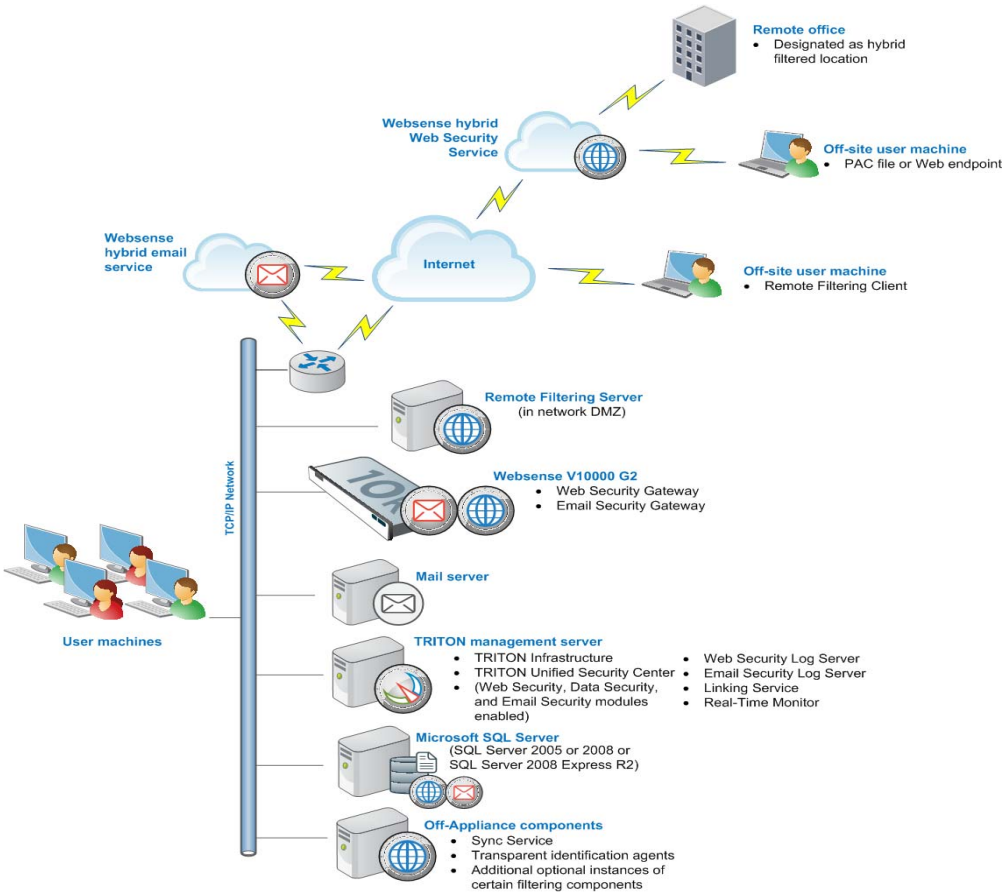


## Overview

This section contains information and instructions for deploying Websense Web Security Gateway and Email Security Gateway (Anywhere) based on a Websense V10000 G2 appliance running in *Web and Email Security* mode.

The following illustration is a high-level diagram of a basic appliance-based deployment of Web and Email Security Gateway. Note that this illustration is intended

to show the general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).




### Websense hybrid email service

If your subscription includes Email Security Gateway Anywhere, you can enable the Websense hybrid email service. This is an in-the-cloud service that provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach the network and considerably reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

### Off-site user machine

Off-site users (e.g., telecommuters or traveling personnel) can be filtered using Websense Remote Filtering. Remote Filtering Client must be installed on this machine. It works with Remote Filtering Server (see below).

### Remote Filtering Server

Websense Remote Filtering is accomplished using a Remote Filtering Server and Remote Filtering Client. Websense*Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction

with *Remote Filtering Client*, to filter off-site users that are outside the corporate network.

### Websense V10000 G2

The Websense V10000 G2 appliance provides the majority of Web and Email Security Gateway functions. Web traffic is directed through the Websense appliance for filtering.

Incoming email flows from the hybrid email service (if enabled) to the Websense appliance and to your mail server. The Websense appliance also provides the Personal Email Manager facility for end users to manage quarantined email.

### Mail server

This is your internal mail server; not provided by Websense, Inc.

### TRITON management server

A separate *TRITON management server* is required. *TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security).

The Data Security module of the TRITON Unified Security Center works with the Websense appliance to provide email DLP (data loss prevention) features.

Web Security Log Server, Email Security Log Server, and Real-Time Monitor may also be installed on this machine (note that these components may be installed on another machine; it is not required to be located on the TRITON management server).

### Microsoft SQL Server

Microsoft SQL Server, running on a Windows server in your network, is used to store Websense logging and reporting data. Quarantined email are also stored here.

SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using TRITON Unified Security Setup) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

### Off-Appliance Components

If you want to use a Websense transparent identification agent, it must be installed on an off-appliance machine. Also, you can install additional instances of certain Web Security filtering components on off-appliance machines.

# Deployment

### Web Security Gateway

- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Web Security Distributed Enterprise Deployments*, page 147

### Email Security Gateway

- *Email Security Gateway system requirements*, page 596
- *Email Security Gateway single-appliance deployments*, page 597
- *Email Security Gateway multiple-appliance deployments*, page 600

# Installation

Complete the following procedures in the order in which they are listed.

1. *Obtaining SQL Server*, page 67
2. *Setting up the appliance*, page 611
3. *Installing off-appliance or optional components*, page 619
4. *Initial configuration*, page 610

   The link above goes to general instructions for creating a TRITON management server. As you follow those instructions, choose to install all three modules of the TRITON Unified Security Center. This is done in the**Installation Type** screen of TRITON Unified Security Setup. When you reach that screen, select **Web Security**, **Data Security**, and **Email Security** (under TRITON Unified Security Center).

# Initial configuration

### General

- *Ports*, page 765
- *Antivirus configuration*, page 765
- *Disable Enhanced Security Configuration in Internet Explorer*, page 765
- *Accessing the TRITON Unified Security Center*, page 765

# Setting up the appliance

## Applies to

- Web Security Gateway v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## In this topic

# Overview

> **Note**
> If you have already completed the appliance set up steps provided in the *Websense V-Series Getting Started* guide, skip to *Installing off-appliance or optional components*, page 619 now.

The Quick Start poster, which comes in the shipping box with your appliance, shows you all items included in each Websense appliance shipping box. The 2-page Quick Start explains how to set up the hardware and shows how to connect the cables to the appliance and to your network.

Network interfaces C, P1, E1, and E2 (if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C, P1, E1, and E2 (if used) are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C, P1, E1, and E2 (if used) interfaces can access.

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance.

# Perform initial command-line configuration

1. Access the appliance through a USB keyboard and monitor or a serial port

| | |
|---|---|
| Hostname | |
| IP address for network interface C | |
| Subnet mask for network interface C | |
| Default gateway for network interface C (IP address) *Optional*<br><br>NOTE: If you do not provide access to the Internet for interface C, configure:<br>• P1 or P2 to download Master URL database updates from Websense<br>• E1 or P1 to download antispam and antivirus database updates from Websense<br>Configuring these interfaces to access the Internet for database downloads is done through the Appliance Manager and through the TRITON Unified Security Center. See the Appliance Manager Help for information about configuring the interfaces. See the TRTION - Web Security and - Email Security Help for information about configuring database downloads. | |
| Primary DNS server for network interface C (IP address) | |
| Secondary DNS server for network interface C (IP address) *Optional* | |
| Tertiary DNS server for network interface C (IP address) *Optional* | |
| Unified password (8 to 15 characters, at least 1 letter and 1 number)<br>This password is for the following:<br>• Appliance Manager<br>• Content Gateway Manager | |

connection.

> **Note**
> To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:
>
> - 9600 bits per second
> - 8 data bits
> - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```
4. At the first prompt, select **Web and Email Security** mode.
5. Follow the on-screen instructions to provide the information you gathered prior to running the firstboot script.

After the activation script has been completed successfully, use the **Logon Portal** to access the Appliance Manager. To reach the**Logon Portal**, open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

## Configure the appliance

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces P1, P2, N, E1, and E2 (P2, N, and E2 are optional).

While the E1/E2 and P1/P2 interfaces can be bonded to each other if the V10000 G2 runs in either *Web Security only* or *Email Security only* modes, they cannot be bonded when the appliance is in *Web and Email Security* mode.

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway. For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCPv2 router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see **Configure** > **Networking** > **WCCP**, **General** tab).

| | |
|---|---|
| Primary NTP server<br>*Optional*<br>Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C. | Domain: |
| Secondary NTP server<br>*Optional* | Domain: |
| Tertiary NTP server<br>*Optional* | Domain: |
| IP address for network interface P1 | IP address: |

| | |
|---|---|
| Subnet mask for network interface P1 | Subnet mask: |
| Default gateway for network interface P1and P2 (if used)<br>If you use both P1 and P2, the default gateway is automatically assigned to P2 (which is bound to eth1). To ensure that outbound packets can reach the Internet, do not locate the IP addresses of P1 and P2 in the same subnet. | IP address: |
| Primary DNS server for network interface P1 and P2 (if used) | IP address: |
| Secondary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| IP address for network interface P2<br>*Required only if P2 is enabled* | IP address: |
| Subnet mask for network interface P2<br>*Required only if P2 is enabled* | Subnet mask: |
| Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic | Choose (C or N): |
| If interface N transports blocking information, N must be connected to a bidirectional span port | Verify interface N setup. |
| IP address for network interface N | IP address: |
| Subnet mask for network interface N | Subnet mask: |
| Default gateway for network interface N<br>*Required only if network interface N carries blocking information* | IP address: |
| Primary DNS server for network interface N | IP address: |
| Secondary DNS server for network interface N<br>*Optional* | IP address: |
| Tertiary DNS server for network interface N<br>*Optional* | IP address: |
| IP address for network interface E1 | IP address: |
| Subnet mask for network interface E1 | Subnet mask: |

| | |
|---|---|
| Default gateway for network interface E1and E2 (if used).<br>If you use both E1 and E2, the default gateway and DNS configuration are shared by both. | IP address: |
| Primary DNS server for network interface E1 and E2 (if used) | IP address: |
| Secondary DNS server for network interface E1 and E2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface E1 and E2 (if used)<br>*Optional* | IP address: |

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to enable default proxy caching, and Web and email filtering. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance (see *Perform initial command-line configuration*, page 613).

   For information about supported browsers, see the Websense Technical Library (www.websense.com/library).
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration > System**.
4. Under **Time and Date**:
   a. Set the time zone.
   b. Set the time and date:
      - **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
      - **Manually set time and date**: select this option to enter a system time and date yourself.
   c. Click **Save** in the Time and Date area.
5. In the left navigation pane, click **Configuration > Network Interfaces**.
6. Under **Websense Content Gateway Interfaces**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

To configure the P interfaces:

a. Select **P1 only** or **P1 and P2**.

   If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

   If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

b. Click **Save** in the **Websense Content Gateway Interfaces** area when you are done.

> **Important**
>
> When you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.
>
> For example, suppose you are using transparent proxy, and the P1 interface is connected to the WCCPv2 router. In this case, you must configure Websense Content Gateway to use eth0 for WCCPv2 communications (in Content Manager, see **Configure** > **Networking** > **WCCP**, **General** tab).

When only P1 is used, it handles both inbound and outbound traffic for the proxy module (i.e., Content Gateway).

Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2 on the **Configuration** > **Routing** page. For example, you might set outbound traffic to go through P2.

Additionally, you can use P1 as a communication channel for multiple Content Gateway servers in a cluster. In this scenario, P1 should not be used for outbound traffic. For additional information on clusters, see the Content Gateway Manager Help.

7. Under **Network Agent Interface (N)**, configure the N interface.

   The N interface is used by the Network Agent module. It must be connected to a span (or mirror) port on a switch allowing it to monitor the Internet requests going through the switch. (Note: be sure to configure the switch so the span port is monitoring all the ports carrying the traffic of interest; see your switch manufacturer's documentation for configuration instructions). For non-HTTP/ HTTPS protocols, the N interface can also be used to send block information to enforce policy.

   > **Note**
   >
   > The appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

   To configure the N interface:

a. Under **Send blocking information for non-HTTP/HTTPS traffic via**, select whether non-HTTP/HTTPS blocking information is sent via the C or N interface.

b. Enter IP address, subnet mask, default gateway (only if you select interface N for sending blocking information), and DNS IP addresses for the N interface.

c. Click **Save** in the **Network Agent Interface (N)** area.

8. Under **Websense Email Security Gateway Interfaces (E1 and E2)**, configure the E1 and E2 (optional) interfaces.

   The E interfaces are used to accept users' requests (inbound traffic) and communicate with the Internet (outbound traffic).

   To configure the E interfaces:

   a. Select whether **E1 only** or both **E1 and E2** are used.

      If you choose E1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **E1**.

      If you choose E1 and E2, enter configuration information under both **E1** and **E2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both E1 and E2.

   b. Click **Save** in the **Websense Email Security Gateway Interfaces (E1 and E2)** area when you are done.

   When only E1 is used, it handles both inbound and outbound traffic.

   Alternatively, you could use both E1 and E2 such that E1 handles inbound traffic and E2 handles outbound traffic.

   See the Appliance Manager Help for more information about configuring E1 and E2.

9. Configure routes if necessary:

   a. In the left navigation pane, click **Configuration** > **Routing**.

   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

   c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

   d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

   > **Note**
   > An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

   See the Appliance Manager Help for more information about static and module routes.

10. Select the policy mode of this appliance:

a. In the left navigation pane, click **Configuration** > **Web Security Components**.

b. Specify the role of this appliance with respect to Websense Web Security policy information.

- Choose **Full policy source** if Websense Policy Broker and Policy Database for your deployment will run on the appliance being configured. (Only one appliance in the network runs these two components, as well as the other filtering components.) Policy Server must also be run on the*full policy source* appliance; Policy Server can run in multiple locations.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

- Choose **User directory and filtering** if the appliance currently being configured is *not* the location of the policy information, but will run Policy Server and User Service. Then, enter the **IP address** of the server that is used as the full policy source—a machine running Policy Broker. (If the full policy source is another appliance, enter the IP address of its C network interface.)
- Choose **Filtering only** if the appliance being configured will not run any policy components. (There are some disadvantages to this reduced role, as explained in the Appliance Manager help system.) Then, enter the **IP address** of the server that is used as the policy source—a machine running Policy Server. The policy source can also be another appliance in *full policy source* or *user directory and filtering* mode. In this case, enter the IP address of the appliance's C network interface.

11. Click **Save**.
12. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

# Installing off-appliance or optional components

## Applies to

- Web Security Gateway v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

# Installing off-appliance or optional components

The following Websense components must run off-appliance (i.e., on a separate machine):

- *Web Security Log Server* (when creating a TRITON management server, Web Security Log Server can be installed on that machine at the same time).
- *Email Security Log Server* (when creating a TRITON management server, Email Security Log Server can be installed on that machine at the same time)
- Transparent identification agents:
  - *DC Agent*
  - *Logon Agent*
  - *eDirectory Agent*
  - *RADIUS Agent*
- *Remote Filtering Server*

Also, additional instances of Web security filtering components may be installed on machines in your network to provide additional functions or distribute processing load. For example, you can install additional Websense *Network Agent* instances on a machines in your network.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

To install off-appliance components, perform a custom installation on the target machine. See *Deployment* for instructions.

# 41 Web Security Gateway Anywhere and Email Security Gateway (V10000 G2)

## Applies to

- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## In this topic

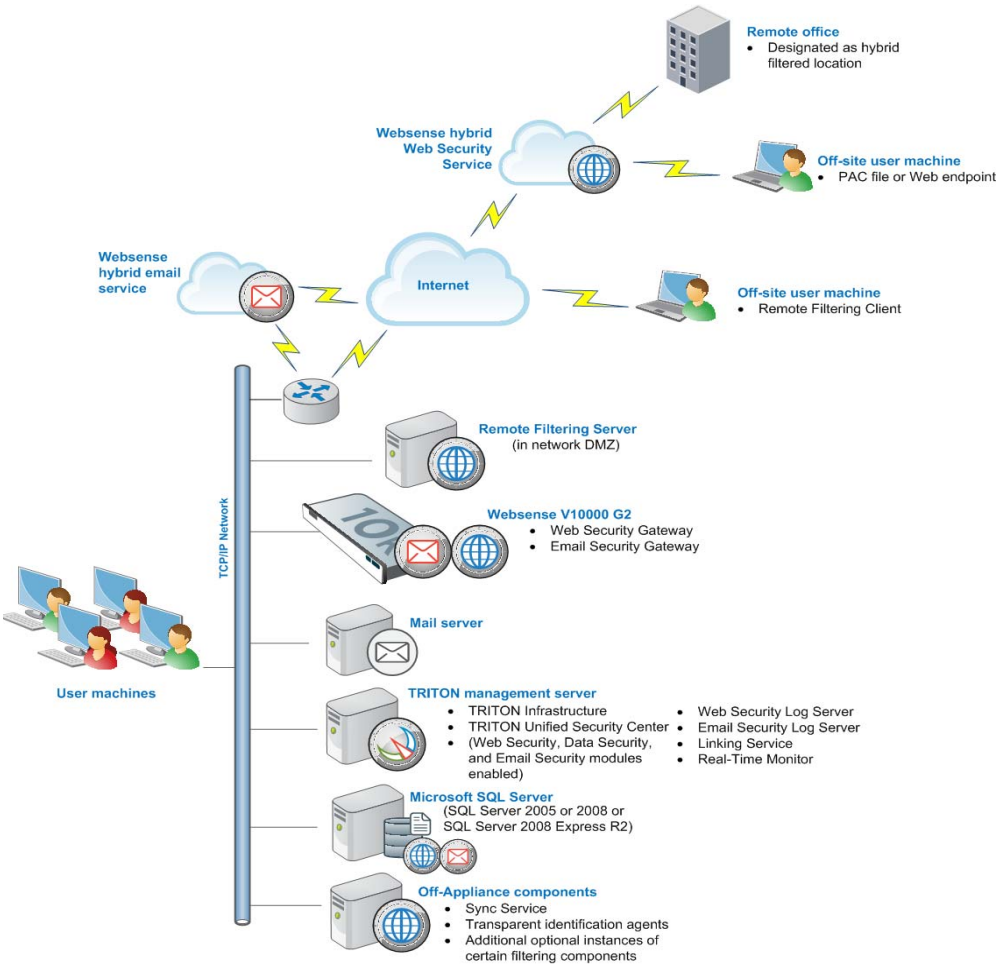


## Overview

This section contains information and instructions for deploying Websense Web Security Gateway Anywhere and Email Security Gateway (Anywhere) based on a Websense V10000 G2 appliance running in *Web and Email Security* mode.

The following illustration is a high-level diagram of a basic appliance-based deployment of Web and Email Security Gateway. Note that this illustration is intended

to show the general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).




## Remote office and off-site users

The Websense hybrid Web Security service can provide Web filtering for small remote offices. This is accomplished by designating a remote office as a hybrid filtered location. See *Initial Configuration* for more information.

Either the hybrid service or Websense Remote Filtering can provide Web filtering for off-site users (e.g., telecommuters or traveling personnel). To use the hybrid service, a PAC file or the Websense Web endpoint is installed on the user's machine. This directs Web browsing to be filtered through the hybrid service according to policies in place.

To use Websense Remote Filtering, Remote Filtering Client must be installed on the off-site machine. It works with Remote Filtering Server (see below).

## Websense hybrid Web Security service

Provides in-the-cloud Web filtering for remote offices and off-site users.

### Websense hybrid email service

If your subscription includes Email Security Gateway Anywhere, you can enable the Websense hybrid email service. This is an in-the-cloud service that provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach the network and considerably reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

### Remote Filtering Server

Websense Remote Filtering is accomplished using a Remote Filtering Server and Remote Filtering Client. Websense*Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users that are outside the corporate network.

### Websense V10000 G2

The Websense V10000 G2 appliance provides the majority of Web and Email Security Gateway functions. Web traffic is directed through the Websense appliance for filtering.

Incoming email flows from the hybrid email service (if enabled) to the Websense appliance and to your mail server. The Websense appliance also provides the Personal Email Manager facility for end users to manage quarantined email.

### Mail server

This is your internal mail server; not provided by Websense, Inc.

### TRITON management server

A separate *TRITON management server* is required. *TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security).

The Data Security module of the TRITON Unified Security Center works with the Websense appliance to provide Web and email DLP (data loss prevention) features.

*Linking Service* is typically installed on this machine. Real-Time Monitor, Web Security Log Server, and Email Security Log Server may also be installed on this machine (note that these components may be installed on another machines; they are not required to be located on the TRITON management server).

### Microsoft SQL Server

Microsoft SQL Server, running on a Windows server in your network, is used to store Websense logging and reporting data. Quarantined email are also stored here.

SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using TRITON Unified Security Setup) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

### Off-Appliance Components

*Sync Service* and Transparent identification agents (*DC Agent*, *Logon Agent*, *eDirectory Agent*, and *RADIUS Agent*) must be installed on a separate machine from the appliance. Also, you can install additional instances of some Web Security filtering components on off-appliance machines.

## Deployment

**Web Security Gateway Anywhere**

- *TRITON management server as policy source for filtering-only appliance*, page 433
- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Web Security Distributed Enterprise Deployments*, page 147

**Email Security Gateway**

- *Email Security Gateway system requirements*, page 596
- *Email Security Gateway single-appliance deployments*, page 597
- *Email Security Gateway multiple-appliance deployments*, page 600

## Installation

Complete the following procedures.

1. *Obtaining SQL Server*
2. *Setting up the appliance*, page 626
3. *Installing off-appliance or optional components*, page 634
4. *Creating a TRITON Management Server*, page 645

The link above goes to general instructions for creating a TRITON management server. As you follow those instructions, choose to install all three modules of the TRITON Unified Security Center. This is done in the**Installation Type** screen of TRITON Unified Security Setup. When you reach that screen, select **Web Security**, **Data Security**, and **Email Security** (under TRITON Unified Security Center).

# Initial configuration

### General

- *Ports*, page 765
- *Antivirus configuration*, page 765
- *Disable Enhanced Security Configuration in Internet Explorer*, page 765
- *Accessing the TRITON Unified Security Center*, page 765
- *Entering subscription key*, page 766
- *SQL Server 2008 R2 Express*, page 766

### Web Security Gateway Anywhere

- *Getting Started Help*, page 767
- *Windows Server 2008*, page 767
- *Logon script for Logon Agent*, page 768
- *Messenger Service for Network Agent block messages*, page 769
- *Administrator privileges for User Service, DC Agent, or Logon Agent*, page 769
- *Configuring Transparent Identification*, page 769
- *Network Agent and multiple NICs*, page 769
- *Remote Filtering*, page 769
- *Identifying Filtering Service by IP address*, page 769
- *Web Security Distributed Enterprise Deployments*, page 147
- *Starting Content Gateway Manager*, page 779
- *Entering a subscription key for Content Gateway*, page 780
- *Enabling SSL Manager in Content Gateway*, page 781
- *Enabling WCCP for Content Gateway*, page 781
- *Registering Websense Content Gateway with Data Security*, page 771
- *Configuring the Content Gateway policy engine*, page 773
- *Verifying Web and data security linking*, page 774
- *Configure filtering for remote offices and off-site users*, page 774

### Email Security Gateway

- *Email Security Gateway initial configuration*, page 777

# Setting up the appliance

## Applies to

- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## In this topic



## Overview

> **Note**
> If you have already completed the appliance set up steps provided in the *Websense V-Series Getting Started* guide, skip to *Installing off-appliance or optional components*, page 634 now.

The Quick Start poster, which comes in the shipping box with your appliance, shows you all items included in each Websense appliance shipping box. The 2-page Quick Start explains how to set up the hardware and shows how to connect the cables to the appliance and to your network.

Network interfaces C, P1, E1, and E2 (if used) must be able to access a DNS server. These interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C, P1, E1, and E2 (if used) are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C, P1, E1, and E2 (if used) interfaces can access.

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits

- no parity

The activation script, called firstboot, runs when you start the appliance.

See *Perform initial command-line configuration*.

## Perform initial command-line configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for the network interface labeled C and a few other general items. You can run the script again if you want to examine your settings or change settings. You can also change settings through the Appliance Manager (user interface) after firstboot has been executed.

Gather the following information before running the script. Some of this information may have been written down on the Quick Start during hardware setup.

| | |
|---|---|
| Hostname | |
| IP address for network interface C | |
| Subnet mask for network interface C | |
| Default gateway for network interface C (IP address) *Optional*<br><br>NOTE: If you do not provide access to the Internet for interface C, configure:<br>• P1 or P2 to download Master URL database updates from Websense<br>• E1 or P1 to download antispam and antivirus database updates from Websense<br>Configuring these interfaces to access the Internet for database downloads is done through the Appliance Manager and through the TRITON Unified Security Center. See the Appliance Manager Help for information about configuring the interfaces. See the TRTION - Web Security and - Email Security Help for information about configuring database downloads. | |
| Primary DNS server for network interface C (IP address) | |
| Secondary DNS server for network interface C (IP address) *Optional* | |
| Tertiary DNS server for network interface C (IP address) *Optional* | |
| Unified password (8 to 15 characters, at least 1 letter and 1 number)<br>This password is for the following:<br>• Appliance Manager<br>• Content Gateway Manager | |

When you have gathered the necessary information, run the initial command line configuration, as follows.

1. Access the appliance through a USB keyboard and monitor or a serial port connection.

   **Note**

   To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

   - 9600 bits per second
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```

4. At the first prompt, select **Web and Email Security** mode.
5. Follow the on-screen instructions to provide the information you gathered prior to running the firstboot script.

After the activation script has been completed successfully, use the **Logon Portal** to access the Appliance Manager. To reach the**Logon Portal**, open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

## Configure the appliance

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces P1, P2, N, E1, and E2 (P2, N, and E2 are optional).

While the E1/E2 and P1/P2 interfaces can be bonded to each other if the V10000 G2 runs in either *Web Security only* or *Email Security only* modes, they cannot be bonded when the appliance is in *Web and Email Security* mode.

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway. For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCPv2 router. In this case, you must configure Websense Content

Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see **Configure** > **Networking** > **WCCP**, **General** tab).

| | |
|---|---|
| Primary NTP server<br>*Optional*<br>Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C. | Domain: |
| Secondary NTP server<br>*Optional* | Domain: |
| Tertiary NTP server<br>*Optional* | Domain: |
| IP address for network interface P1 | IP address: |
| Subnet mask for network interface P1 | Subnet mask: |
| Default gateway for network interface P1and P2 (if used)<br>If you use both P1 and P2, the default gateway is automatically assigned to P2 (which is bound to eth1). To ensure that outbound packets can reach the Internet, do not locate the IP addresses of P1 and P2 in the same subnet. | IP address: |
| Primary DNS server for network interface P1 and P2 (if used) | IP address: |
| Secondary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface P1 and P2 (if used)<br>*Optional* | IP address: |
| IP address for network interface P2<br>*Required only if P2 is enabled* | IP address: |
| Subnet mask for network interface P2<br>*Required only if P2 is enabled* | Subnet mask: |
| Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic | Choose (C or N): |
| If interface N transports blocking information, N must be connected to a bidirectional span port | Verify interface N setup. |
| IP address for network interface N | IP address: |
| Subnet mask for network interface N | Subnet mask: |

| | |
|---|---|
| Default gateway for network interface N<br>*Required only if network interface N carries blocking information* | IP address: |
| Primary DNS server for network interface N | IP address: |
| Secondary DNS server for network interface N<br>*Optional* | IP address: |
| Tertiary DNS server for network interface N<br>*Optional* | IP address: |
| IP address for network interface E1 | IP address: |
| Subnet mask for network interface E1 | Subnet mask: |
| Default gateway for network interface E1and E2 (if used).<br>If you use both E1 and E2, the default gateway and DNS configuration are shared by both. | IP address: |
| Primary DNS server for network interface E1 and E2 (if used) | IP address: |
| Secondary DNS server for network interface E1 and E2 (if used)<br>*Optional* | IP address: |
| Tertiary DNS server for network interface E1 and E2 (if used)<br>*Optional* | IP address: |

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to enable default proxy caching, and Web and email filtering. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance (see *Perform initial command-line configuration*, page 627).

   For information about supported browsers, see the Websense Technical Library (www.websense.com/library).
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration > System**.
4. Under **Time and Date**:
   a. Set the time zone.

b. Set the time and date:

- **Automatically synchronize with an NTP server**: select this option to use a Network Time Protocol server. Specify up to three NTP servers. Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.
- **Manually set time and date**: select this option to enter a system time and date yourself.

c. Click **Save** in the Time and Date area.

5. In the left navigation pane, click **Configuration > Network Interfaces**.
6. Under **Websense Content Gateway Interfaces**, configure the P1 and P2 (optional) interfaces.

   The P interfaces are used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

   To configure the P interfaces:

   a. Select **P1 only** or **P1 and P2**.

      If you choose P1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **P1**.

      If you choose P1 and P2, enter configuration information under both **P1** and **P2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both P1 and P2.

   b. Click **Save** in the **Websense Content Gateway Interfaces** area when you are done.

**Important**

When you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.

For example, suppose you are using transparent proxy, and the P1 interface is connected to the WCCPv2 router. In this case, you must configure Websense Content Gateway to use eth0 for WCCPv2 communications (in Content Manager, see **Configure > Networking > WCCP**, **General** tab).

When only P1 is used, it handles both inbound and outbound traffic for the proxy module (i.e., Content Gateway).

Alternatively, you could use both P1 and P2 such that P1 handles inbound traffic and P2 handles outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2 on the **Configuration > Routing** page. For example, you might set outbound traffic to go through P2.

Additionally, you can use P1 as a communication channel for multiple Content Gateway servers in a cluster. In this scenario, P1 should not be used for outbound

traffic. For additional information on clusters, see the Content Gateway Manager Help.

7. Under **Network Agent Interface (N)**, configure the N interface.

   The N interface is used by the Network Agent module. It must be connected to a span (or mirror) port on a switch allowing it to monitor the Internet requests going through the switch. (Note: be sure to configure the switch so the span port is monitoring all the ports carrying the traffic of interest; see your switch manufacturer's documentation for configuration instructions). For non-HTTP/HTTPS protocols, the N interface can also be used to send block information to enforce policy.

   > **Note**
   > The appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

   To configure the N interface:

   a. Under **Send blocking information for non-HTTP/HTTPS traffic via**, select whether non-HTTP/HTTPS blocking information is sent via the C or N interface.

   b. Enter IP address, subnet mask, default gateway (only if you select interface N for sending blocking information), and DNS IP addresses for the N interface.

   c. Click **Save** in the **Network Agent Interface (N)** area.

8. Under **Websense Email Security Gateway Interfaces (E1 and E2)**, configure the E1 and E2 (optional) interfaces.

   The E interfaces are used to accept users' requests (inbound traffic) and communicate with the Internet (outbound traffic).

   To configure the E interfaces:

   a. Select whether **E1 only** or both **E1 and E2** are used.

      If you choose E1 only, enter configuration information (IP address, subnet mask, default gateway, DNS IP addresses) under **E1**.

      If you choose E1 and E2, enter configuration information under both **E1** and **E2**. Note that default gateway and DNS configuration (under **Shared Setting**) are shared between both E1 and E2.

   b. Click **Save** in the **Websense Email Security Gateway Interfaces (E1 and E2)** area when you are done.

   When only E1 is used, it handles both inbound and outbound traffic.

   Alternatively, you could use both E1 and E2 such that E1 handles inbound traffic and E2 handles outbound traffic.

   See the Appliance Manager Help for more information about configuring E1 and E2.

9. Configure routes if necessary:

   a. In the left navigation pane, click **Configuration > Routing**.

   b. Under Static Routes, use the **Add/Import** button to specify customized, static routes.

c. Under Module Routes, use the **Add** button to specify non-management Web Security or Email Security traffic through the C interface.

d. For either static or module routes, use the **Delete** button to remove existing routes, if necessary.

> **Note**
> An existing route cannot be edited. If you want to edit a route, delete it and then use the **Add/Import** (static) or **Add** (module) button to specify the route with the changes you want.

See the Appliance Manager Help for more information about static and module routes.

10. Select the policy mode of this appliance:

    a. In the left navigation pane, click **Configuration** > **Web Security Components**.

    b. Specify the role of this appliance with respect to Websense Web Security policy information.

    - Choose **Full policy source** if Websense Policy Broker and Policy Database for your deployment will run on the appliance being configured. (Only one appliance in the network runs these two components, as well as the other filtering components.) Policy Server must also be run on the*full policy source* appliance; Policy Server can run in multiple locations.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

    - Choose **User directory and filtering** if the appliance currently being configured is *not* the location of the policy information, but will run Policy Server and User Service. Then, enter the **IP address** of the server that is used as the full policy source—a machine running Policy Broker. (If the full policy source is another appliance, enter the IP address of its C network interface.)
    - Choose **Filtering only** if the appliance being configured will not run any policy components. (There are some disadvantages to this reduced role, as explained in the Appliance Manager help system.) Then, enter the **IP address** of the server that is used as the policy source—a machine running Policy Server. The policy source can also be another appliance in *full policy source* or *user directory and filtering* mode. In this case, enter the IP address of the appliance's C network interface.

11. Click **Save**.

12. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

# Installing off-appliance or optional components

## Applies to

- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 G2

## Installing off-appliance or optional components

The following Websense components must run off-appliance (i.e., on a separate machine):

- *Web Security Log Server* (when creating a TRITON management server, Web Security Log Server can be installed on that machine at the same time).
- *Email Security Log Server* (when creating a TRITON management server, Email Security Log Server can be installed on that machine at the same time).
- *Real-Time Monitor*
- *Sync Service*
- Transparent identification agents:
  - *DC Agent*
  - *Logon Agent*
  - *eDirectory Agent*
  - *RADIUS Agent*
- *Remote Filtering Server*

Also, additional instances of Web security filtering components may be installed on machines in your network to provide additional functions or distribute processing load. For example, you can install additional Websense *Network Agent* instances on a machines in your network.

**Note**

If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

To install off-appliance components, perform a custom installation on the target machine. See *Deployment* for instructions.

# 42 TRITON Enterprise (V10000 G2)

## Applies to

- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- Data Security v7.6
- V10000 G2 v7.6

## In this topic

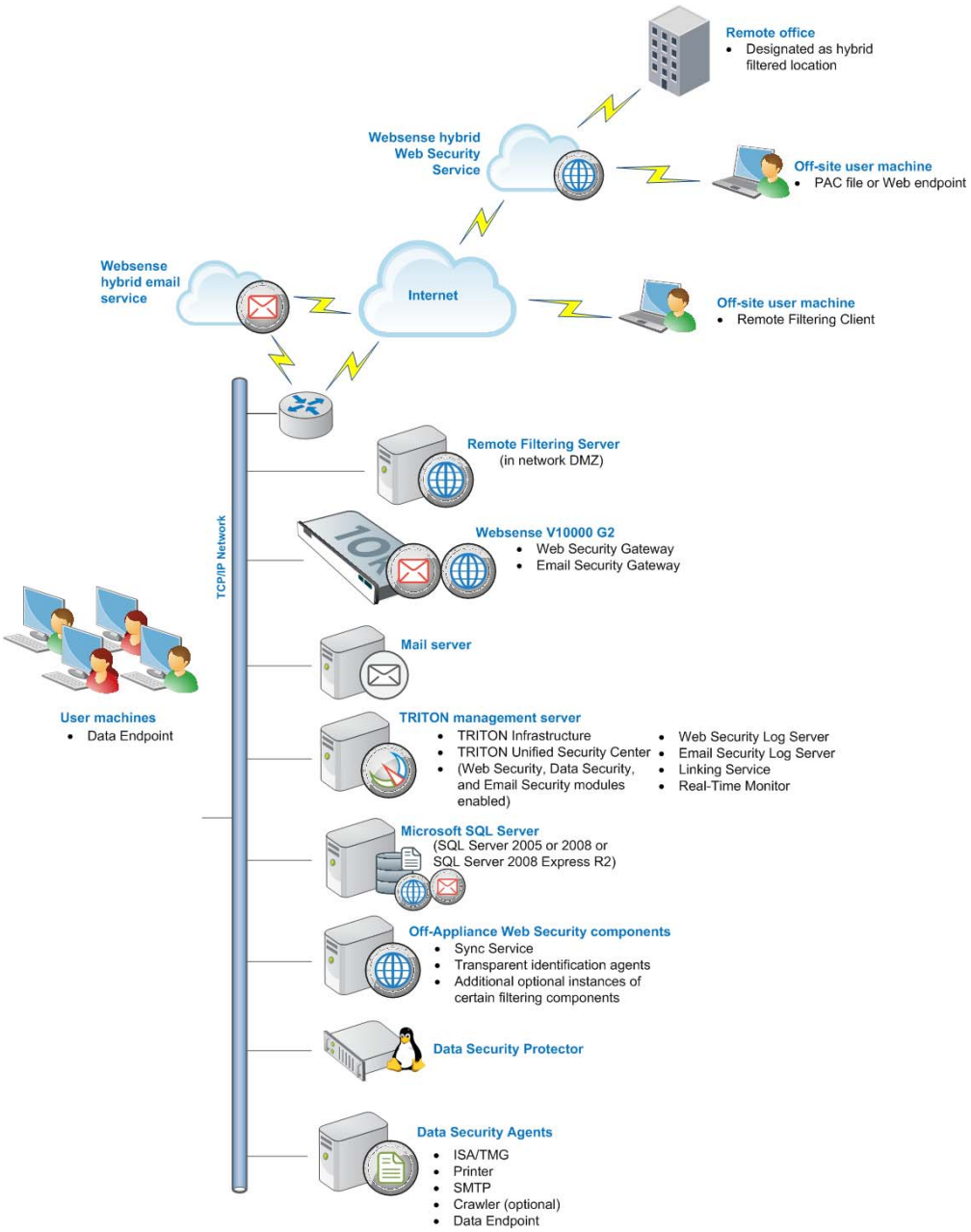


## Overview

This section contains information and instructions for deploying Websense TRITON Enterprise (i.e., Websense Web Security Gateway Anywhere, Data Security, and Email Security Gateway). The Web Security and Email Security portions are based on a Websense V10000 G2 appliance running in *Web and Email Security* mode.

The following illustration is a high-level diagram of a basic V10000-G2-based deployment of TRITON Enterprise. Note that this illustration is intended to show the

general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).




### Remote office and off-site users

The Websense hybrid Web Security service can provide Web filtering for small remote offices. This is accomplished by designating a remote office as a hybrid filtered location. See *Initial Configuration* for more information.

Either the hybrid service or Websense Remote Filtering can provide Web filtering for off-site users (e.g., telecommuters or traveling personnel). To use the hybrid service, a PAC file or the Websense Web endpoint is installed on the user's machine. This directs Web browsing to be filtered through the hybrid service according to policies in place.

To use Websense Remote Filtering, Remote Filtering Client must be installed on the off-site machine. It works with Remote Filtering Server (see below).

### Websense hybrid Web Security service

Provides Web filtering for remote offices and off-site users.

### Websense hybrid email service

If your subscription includes Email Security Gateway Anywhere, you can enable the Websense hybrid email service. This is an in-the-cloud service that provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach the network and considerably reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

### Remote Filtering Server

Websense Remote Filtering is accomplished using a Remote Filtering Server and Remote Filtering Client. Websense*Remote Filtering Server* is typically installed on its own machine in the network DMZ. Remote Filtering Server is used, in conjunction with *Remote Filtering Client*, to filter off-site users that are outside the corporate network.

### Websense V10000 G2

The Websense V10000 G2 appliance provides the majority of Web and Email Security Gateway functions. Web traffic is directed through the Websense appliance for filtering.

Incoming email flows from the hybrid email service (if enabled) to the Websense appliance and to your mail server. The Websense appliance also provides the Personal Email Manager facility for end users to manage quarantined email.

### Mail server

This is your internal mail server; not provided by Websense, Inc.

### TRITON management server

A separate *TRITON management server* is required. *TRITON management server* is the term used to refer to the machine on which *TRITON Unified Security Center* is installed. This machine is used to manage your Websense deployment. It includes TRITON Infrastructure and all of the TRITON Unified Security Center modules (Web Security, Data Security, and Email Security).

The Data Security module of the TRITON Unified Security Center works with the Websense appliance to provide Web and email DLP (data loss prevention) features.

Also located on the TRITON management server are Data Security Management Server and, typically, *Crawler* providing key Data Security functions.

*Linking Service* is typically installed on this machine. Real-Time Monitor, Web Security Log Server, and Email Security Log Server may also be installed on this machine (note that these components may be installed on another machines; they are not required to be located on the TRITON management server).

### Microsoft SQL Server

Microsoft SQL Server, running on a Windows server in your network, is used to store Websense logging and reporting data. Quarantined email are also stored here.

SQL Server must be obtained separately; it is not included as part of a Websense subscription. When installing Websense components, SQL Server must be installed and running, typically on its own machine as shown above. SQL Server Express (installed using TRITON Unified Security Setup) may be used in place of SQL Server. However, it is a best practice to use SQL Server Express only in non-production or evaluation environments.

### Off-Appliance Web Security Components

*Sync Service* and Transparent identification agents (*DC Agent*, *Logon Agent*, *eDirectory Agent*, and *RADIUS Agent*) must be installed on a separate machine from the appliance. Also, you can install additional instances of certain Web Security filtering components on off-appliance machines.

### Data Security Protector

The protector is a Linux-based soft-appliance, providing monitoring and blocking capabilities, preventing data loss and leaks of sensitive information. Using PreciseID technology, the protector can be configured to accurately monitor sensitive information-in-transit on any port.

### Data Security Agents

*Microsoft ISA agent*/TMG agent, *Printer agent*, *SMTP agent*, *Crawler*, and *Endpoint agent* are installed on appropriate machines.

### Data Endpoint (User Machine)

The *Endpoint agent* can be installed on any machine.

# Deployment

### Web Security Gateway Anywhere

- *TRITON management server as policy source for filtering-only appliance*, page 433
- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Web Security Distributed Enterprise Deployments*, page 147

### Data Security

- *Planning Data Security Deployment*, page 449
- *Choosing and Deploying Data Security Agents*, page 473
- *Integrating Data Security with Existing Infrastructure*, page 519
- *Scaling Data Security*, page 553
- *Data Security Protector CLI*, page 561

**Email Security Gateway**

- *Email Security Gateway system requirements*, page 596
- *Email Security Gateway single-appliance deployments*, page 597
- *Email Security Gateway multiple-appliance deployments*, page 600

# Installation

Complete the following procedures.

1. *Obtaining SQL Server*, page 67
2. *Setting up the appliance*, page 626
3. *Installing off-appliance or optional Web Security components*, page 642
4. *Creating a TRITON Management Server,* page 645

   The link above goes to general instructions for creating a TRITON management server. As you follow those instructions, choose to install all three modules of the TRITON Unified Security Center. This is done in the**Installation Type** screen of TRITON Unified Security Setup. When you reach that screen, select **Web Security**, **Data Security**, and **Email Security** (under TRITON Unified Security Center).
5. *Installing Data Security Components*, page 692

# Initial configuration

**General**

- *Ports*, page 765
- *Antivirus configuration*, page 765
- *Disable Enhanced Security Configuration in Internet Explorer*, page 765
- *Accessing the TRITON Unified Security Center*, page 765
- *Entering subscription key*, page 766
- *SQL Server 2008 R2 Express*, page 766

**Web Security Gateway Anywhere**

- *Getting Started Help*, page 767
- *Windows Server 2008*, page 767
- *Logon script for Logon Agent*, page 768

# Installing off-appliance or optional Web Security components

## Applies to

- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- Data Security v7.6
- V10000 G2

## Installing off-appliance or optional Web Security components

The following Websense components must run off-appliance (i.e., on a separate machine):

- *Web Security Log Server* (when creating a TRITON management server, Web Security Log Server can be installed on that machine at the same time).
- *Email Security Log Server* (when creating a TRITON management server, Email Security Log Server can be installed on that machine at the same time).
- *Real-Time Monitor*
- *Sync Service*

- Transparent identification agents:
  - *DC Agent*
  - *Logon Agent*
  - *eDirectory Agent*
  - *RADIUS Agent*
- *Remote Filtering Server*

Also, additional instances of Web security filtering components may be installed on machines in your network to provide additional functions or distribute processing load. For example, you can install additional Websense *Network Agent* instances on a machines in your network.

> **Note**
> If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

To install off-appliance components, perform a custom installation on the target machine. See *Deployment* for instructions.

# 43 Creating a TRITON Management Server

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Data Security v7.6

## In this topic



## Overview

*TRITON management server* is the term used to refer to the machine on which TRITON Unified Security Center, along with certain optional components, are installed. It is "created" by installing these components on a suitable machine (see *System Requirements*, page 41).

> **Important**
>
> To enable more than one of its modules (i.e., TRITON - Web Security, - Data Security, and - Email Security), TRITON Unified Security Center must be installed on Windows Server 2008 R2 (64-bit). Note that TRITON - Email Security requires TRITON - Data Security, so it must be installed on Windows Server 2008 R2.

Typically, there is only one TRITON management server in an entire deployment. It serves as the central point for management, configuration, and reporting.

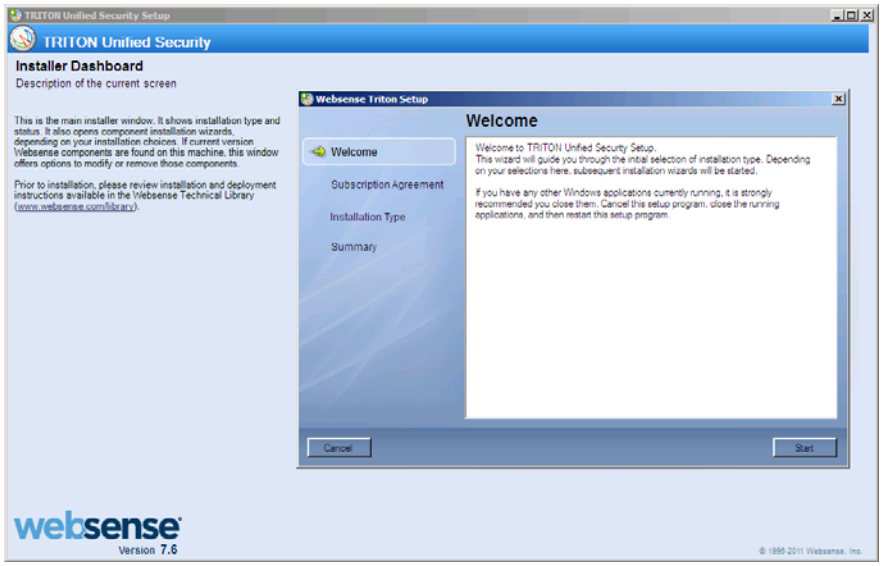
## Preparing for installation

Review the information in *Preparing for Installation*, page 55. Perform any necessary preparation steps, e.g., disabling firewall and antivirus.

## Installing TRITON Unified Security Center

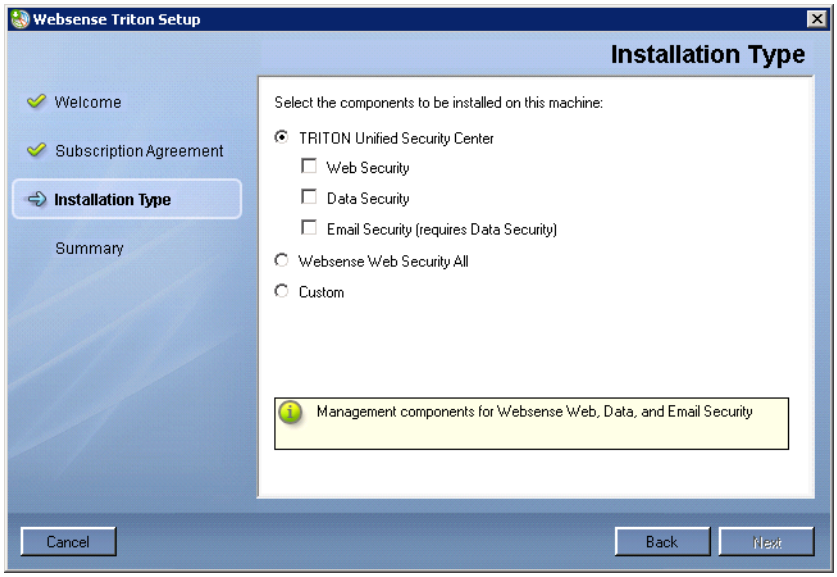
Do not install any Websense components on a domain controller.

1. Download or copy the Websense installer to this machine.
   See *Preparing for Installation*, page 55 for instructions.
2. Double-click the downloaded installer to launch the Websense installer.
   A progress dialog box appears, as files are extracted.
3. On the **Welcome** screen, click **Start**.




4. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.

5. On the **Installation Type** screen, select **TRITON Unified Security Center** and the modules you want to install (Web Security, Data Security, and Email Security).




> **Note**
> The TRITON Unified Security Center modules are management components only. Selecting them does not install components for any other function. Non-management components are installed using the**Websense Web Security All** or **Custom** options.

See the following table for information about which modules you should select for installation.

| Solution | TRITON Unified Security module | | |
|---|---|---|---|
| | Web Security | Data Security | Email Security |
| Web Filter | X | | |
| Web Security | X | | |
| Web Security Gateway | X | | |
| Web Security Gateway Anywhere | X | X | |
| Data Security | | X | |
| Email Security Gateway (Anywhere) | | X | X |
| Note: If your subscription includes a combination of these solutions, install all of the modules required by them. For example, if your subscription includes both Web Security Gateway and Email Security Gateway, then install all three modules. | | | |

**Important**

To install the Web Security module of the TRITON Unified Security Center, *Policy Server* must be already installed and running on a machine in your network. If it is not, cancel this installation and use a custom installation to install it (see *Custom Deployment)*. In a Websense-appliance-based deployment, Policy Server is already installed and enabled on an appliance running in *full policy source* or *user directory and filtering* mode.

When you select **Email Security**, **Data Security** is selected automatically as well because it is required for email DLP (data loss prevention) features.

**Important**

To install the Email Security module of the TRITON Unified Security Center (i.e., TRITON - Email Security) an Email Security Gateway appliance must already be in your network. You will need to provide the appliance's C interface IP address during installation of TRITON - Email Security.

6. On the **Summary** screen, click **Next** to continue the installation.
7. TRITON Infrastructure Setup launches.

   Follow the instructions in *Installing TRITON Infrastructure*.
8. When you click **Finish** in TRITON Infrastructure Setup, component installers for each module selected, in the Module Selection screen (Step 5), will be launched in succession.

   Only the component installers for the modules you have selected will be launched. For example, if you select only Web Security and Data Security, then the Email Security installer will not be launched.
9. Complete the following procedures for the modules you have selected. For each module, a component installer will launch.The components installers launch in the order shown here.
   - *Installing the Web Security module for TRITON Unified Security Center*
   - *Installing the Data Security module for TRITON Unified Security Center*
   - *Installing the Email Security module for TRITON Unified Security Center*

# Installing the Web Security module for TRITON Unified Security Center

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Installing the Web Security module for TRITON Unified Security Center

Follow these instructions to install Web Security management components on a TRITON management server.

**Important**

If you do not plan to install Policy Broker and Policy Server on this machine, they must already be installed and running elsewhere in your deployment. If you have a Web-security-mode appliance running in *full policy source* mode, Policy Broker and Policy Server are already on that appliance. For instructions on installing these components, see *Installing Web Security components*, page 668.

1. It is assumed you have reached this point by starting a TRITON Unified Security Center installation. If not, see *Creating a TRITON Management Server*, page 645.
2. In the **Select Components** screen, select the components you want to install on this machine and then click **Next**.

   The following Web security components are available for installation on a TRITON management server:

   - *TRITON - Web Security* (i.e., the Web Security module in the TRITON Unified Security Center) must be installed. It is selected by default and cannot be deselected. The other components shown are optional for this machine.
   - *Web Security Log Server* is typically installed on the TRITON management server. However, you may install it elsewhere.

- *Sync Service* is required if your subscription includes Websense Web Security Gateway Anywhere. It can be installed on this machine or another machine. It is important to note that in most cases there must be only one instance of Sync Service in your entire deployment. Typically, Sync Service is located on the same machine as Web Security Log Server.
- Select *Linking Service* if your subscription includes both Websense Web Security (any Web Security solution, including Web Security Gateway Anywhere) and Data Security.
- *Real-Time Monitor* is optional. It is typically installed on the TRITON management server, but can be located elsewhere. You should install only one instance of Real-Time Monitor per *Policy Server* instance.
- Select *Policy Broker* and *Policy Server* if these components have not already been installed in your deployment. They are required to install TRITON - Web Security. In a Websense appliance-based deployment, these components are already installed on a Websense appliance running in *full policy source* mode.

**Important**

There must be only one instance of Policy Broker in your entire deployment. There can be multiple instances of Policy Server.

3. The **Policy Server Connection** screen appears. (If you chose to install Policy Broker and Policy Server on this machine, skip this step.)

   See *Policy Server Connection Screen* for instructions.
4. If you selected Sync Service for installation, the **Policy Broker Connection** screen appears. (If you chose to install Policy Broker and Policy Server on this machine, skip this step.)

   See *Policy Broker Connection Screen* for instructions.
5. If you selected Web Security Log Server for installation, the **Log Database Location** screen appears.

   See *Log Database Location Screen* for instructions.
6. If you selected Web Security Log Server for installation, the **Optimize Log Database Size** screen appears.

   See *Optimize Log Database Size Screen* for instructions.
7. If you select Linking Service for installation, the **Filtering Service Communication** screen appears.

   See *Filtering Service Communication Screen* for instructions.
8. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.
9. Click **Next** to start the installation. The **Installing Websense** progress screen is displayed. Wait for installation to complete.
10. On the **Installation Complete** screen, click **Next**.

11. If you have not selected any other TRITON Unified Security Center module, you are returned to the Modify Installation dashboard. Installation is complete.

    If you have chosen to install other modules of the TRITON Unified Security Center, you are returned to the Installer Dashboard and the next component installer is launched.

# Installing the Data Security module for TRITON Unified Security Center

## Applies to

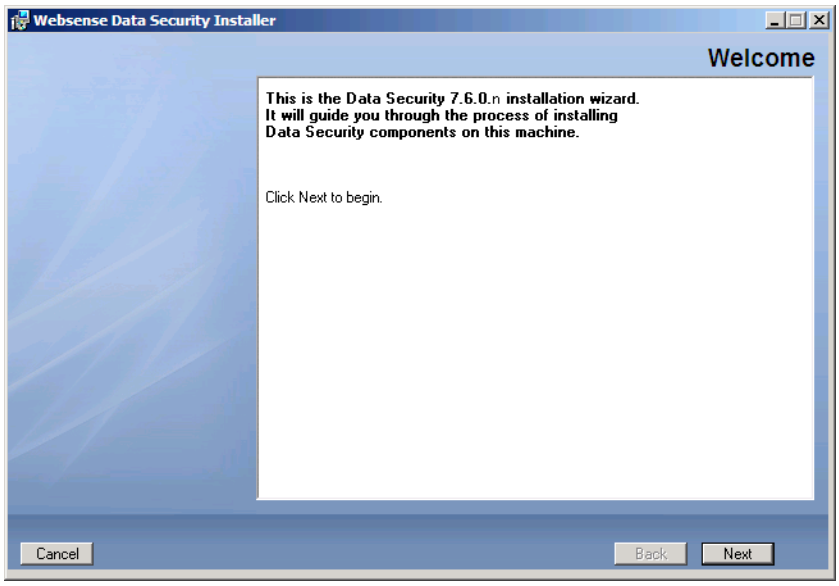
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- V10000 V7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Installing the Data Security module for TRITON Unified Security Center

Follow these instructions to install Data Security management components on a TRITON management server.

1. It is assumed you have reached this point by starting a TRITON Unified Security Center installation. If not, see *Creating a TRITON Management Server*, page 645.

2. Once the Websense Data Security Installer is launched, the **Welcome** screen appears, click **Next** to begin Data Security installation.




> **Note**
> If the .NET 2.0 framework is not found on this machine, the Data Security Installer installs it.

3. In the **Select Components** screen, click **Next** to accept the default selections.

> **Note**
> If there is insufficient RAM on this machine for Data Security Management Server components, a message appears. Click **OK** to dismiss the message. You are allowed to proceed with the installation. However, it is a best practice to only install if you have sufficient RAM.

4. If prompted, click **OK** to indicate that services such as ASP.NET and SMTP will be enabled.

   Required Windows components will be installed. You may need access to the operating system installation disc or image.

5. On the **Fingerprinting Database** screen, accept the default location or use the **Browse** button to specify a different location.

   Note that you can install the Fingerprinting database to a local path only.

6. Use the options on the **Import Data From Previous Version** screen to restore data from a backup of another Data Security Server if necessary.

   Select the **Load data from previous version** check box and then use the **Browse** button to specify the location of the backup data you want restored.

For more information about backups, see the TRITON - Data Security Help.

7. In the **Installation Confirmation** screen, click **Install** to begin installation of Data Security components.
8. If the following message appears, click **Yes** to continue the installation:

   *Data Security needs port 80 free.*
   *In order to proceed with this installation, DSS will free up this port.*
   *Click Yes to proceed OR click No to preserve your settings.*

   Clicking **No** cancels the installation.

   A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.
9. The **Installation** progress screen appears. Wait for the installation to complete.
10. When the **Installation Complete** screen appears, click **Finish** to close the Data Security installer.
11. If no other TRITON Unified Security Center module is chosen for installation, you are returned to the Modify Installation dashboard. Installation is complete.

    Otherwise, you are returned to the Installer Dashboard and the next component installer is launched.

# Installing the Email Security module for TRITON Unified Security Center

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Installing the Email Security module for TRITON Unified Security Center

Follow these instructions to install the Email Security module of the TRITON Unified Security Center. In addition to the Email Security module (also referred to as TRITON - Email Security) you will be given the option to install Email Security Log Server on this machine.server

1. It is assumed you have reached this point by starting a TRITON Unified Security Center installation and selecting the Email Security module. If not, see*Creating a TRITON Management Server*, page 645.
2. Once the Email Security Installer is launched, the **Introduction** screen appears, click **Next** to begin Data Security installation.
3. On the **Select Components** screen, choose whether to install Email Security Log Server on this machine and then click **Next**.

TRITON - Email Security (i.e, the Email Security module of the TRITON Unified Security Center) will be installed automatically. You cannot deselect it.

> **Note**
> If you do not see TRITON - Email Security on this screen, TRITON Infrastructure was not detected by the Email Security Installer. TRITON Infrastructure must be installed already to be able to install TRITON - Email Security.

Email Security Log Server is selected for installation by default. To install Email Security Log Server, SQL Server or SQL Server Express (see *System Requirements*, page 41 for supported versions of SQL Server) must already be installed and running in your network. If you chose to install SQL Server Express during TRITON Infrastructure installation, then it is already installed on this machine.

If you choose to install Email Security Log Server, the Email Security Log Server Configuration utility is also installed. This utility can be accessed by selecting **Start** > **All Programs** > **Websense** > **Email Security** > **Email Security Log Server Configuration**.

You can install Email Security Log Server on another machine; it is not required to be installed on the same machine as TRITON - Email Security. To do so, deselect it here (in the **Select Components** screen). Complete this installation and then run the Websense installer on the machine on which you want to install Email Security Log Server. Choose to perform a custom installation of Email Security components (see *Installing Email Security Components*, page 701).

4. On the **Email Security Gateway** screen specify the Email Security Gateway appliance to be managed by this installation of the TRITON Unified Security Center and then click **Next**.

   Enter the IP address of the **C** interface of the Email Security Gateway appliance. You must specify an IP address only. Do not use a fully-qualified domain name (FQDN).

   When you click **Next**, communication with the specified appliance will be verified. Communication may be unsuccessful if:

   - Subscription key has already been applied to the appliance (typically meaning another installation of TRITON Unified Security Center has been used to manage the appliance). The subscription key must be reset on the appliance.
   - Version of software to be installed does not match the version of the appliance. Verify whether the versions match.
   - Specified appliance is a secondary appliance in a cluster. Specify the primary appliance in the cluster or a non-clustered appliance.
   - The appliance cannot connect to the specified database server (specified during TRITON Infrastructure installation).

- Firewall is blocking communication to the appliance on port 6671. Make sure any local firewall allows outbound communication on port 6671.

5. On the **Email Security Database File Location** screen, specify where Email Security database files should be located and then click **Next**.

   This screen appears only if you chose to install Email Security Log Server in addition to TRITON - Email Security.

   A default location for the Log Database is automatically shown.

   > **Note**
   > Information about the location of the database engine and connection credentials were entered when TRITON Infrastructure was installed on this machine. The Email Security Installer reads this information from configuration files created by TRITON Infrastructure Setup.

   It is a best practice to use the default location. If you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files.

   The path entered here is understood to refer to the machine on which the database engine is located. The path entered must specify a directory that already exists.

6. On the **Installation Folder** screen, specify the location to which you want to install Email Security components and then click **Next**.

   To select a location different than the default, use the **Browse** button.

   Each component (TRITON - Email Security and/or Email Security Log Server) will be installed in its own folder under the parent folder you specify here.

7. On the **Pre-Installation Summary** screen, review the components to be installed. If they are correct, click **Install**.
8. The **Installing Websense Email Security** screen appears, as components are being installed.
9. Wait until the **Installation Complete** screen appears, and then click **Done**. Creating a TRITON Management Server
10. TRITON Unified Security Setup closes. Installation is complete.

# 44 Custom Deployment

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## In this topic



## Overview

This section of the Websense Technical Library discusses custom deployments. *Custom deployments* refers to deployments that do not match the distribution and placement of components as described in the main deployment scenarios (see below). Use the information in this section to plan for and install individual components.

Typically, components are deployed as part of the following deployment scenarios:

- *Web Filter or Web Security (software-based)*, page 69
- *Web Security Gateway (software-based)*, page 161
- *Web Security All*, page 75
- *Web Security Gateway Anywhere (software-based)*, page 351

- *Data Security*, page 435
- *Web Security Gateway (appliance-based)*, page 405
- *Web Security Gateway Anywhere (appliance-based)*, page 419
- *Email Security Gateway (V10000 G2)*, page 585
- *Email Security Gateway (V5000 G2)*, page 575
- *Web and Email Security Gateway (V10000 G2)*, page 607
- *Web Security Gateway Anywhere and Email Security Gateway (V10000 G2)*, page 621
- *TRITON Enterprise (V10000 G2)*, page 637

# Deployment

### General

- *System Requirements*, page 41

### Web Security

- *Network considerations*, page 85
- *Component limits and ratios*, page 87
- *Required external resources*, page 90
- *Deploying transparent identification agents*, page 91
- *Maximizing system performance*, page 94
- *Hardware recommendations for stand-alone deployments of Web Filter or Web Security*, page 98
- *Remote Filtering Server and Client*, page 101
- *Deploying Network Agent*, page 105
- *Integrating Web Security with Content Gateway*, page 126
- *Integrating Web Security with Microsoft ISA Server or Forefront TMG*, page 128
- *Integrating Web Security with Cisco*, page 132
- *Integrating Web Security with Check Point*, page 136
- *Integrating Web Security with Squid Web Proxy Cache*, page 139
- *Integrating Web Security with Citrix*, page 143
- *Other integrations for Web Security*, page 145
- *Web Security Distributed Enterprise Deployments*, page 147

### Data Security

- *Planning Data Security Deployment*, page 449
- *Choosing and Deploying Data Security Agents*, page 473
- *Integrating Data Security with Existing Infrastructure*, page 519
- *Scaling Data Security*, page 553

- *Data Security Protector CLI*, page 561

**Email Security**

- *Email Security Gateway system requirements*, page 596
- *Email Security Gateway single-appliance deployments*, page 597
- *Email Security Gateway multiple-appliance deployments*, page 600

# Installation

**Notes**

- Data Security Protector is installed with a separate installer. See *Protector*, page 476.
- Data Security Endpoint is installed by creating a specialized installation package and distributing it to endpoint machines using SMS. See *Printer agent*, page 508
- Use the WebsenseDataSecurityPrinterAgent.zip package to install Data Security Printer agent. See *Installing the printer agent*, page 509 for more information.
- A separate installer is used to install 64-bit TMG or SMTP Agents. See *Installing the 64-bit SMTP agent*, page 506 or *Installing the TMG agent*, page 507 for more information.

To perform a custom installation, first start a custom installation (see *Starting a custom installation*, page 660). Then see the following instructions for the components you want to install:

- *Installing TRITON Infrastructure*, page 661
- *Installing Web Security components*, page 668
- *Installing Data Security Components*, page 692
- *Installing Email Security Components*, page 701
- *Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)*, page 704

# Initial configuration

**General**

- *Ports*, page 765
- *Antivirus configuration*, page 765
- *Disable Enhanced Security Configuration in Internet Explorer*, page 765

# Starting a custom installation

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Data Security v7.6

## Starting a custom installation

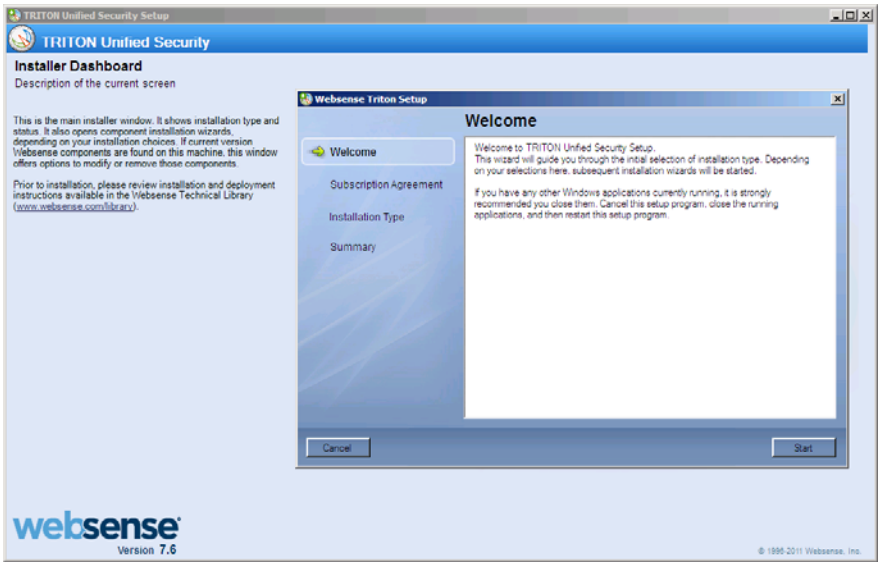
1. Download or copy the Websense installer to this machine.

Download **WebsenseTRITON76Setup.exe** from mywebsense.com.

2. Double-click **WebsenseTRITON76Setup.exe** to launch the Websense installer.

   A progress dialog box appears, as files are extracted.

3. On the **Welcome** screen, click **Start**.




Note the Installer Dashboard stays on-screen during the whole time the Websense installer is run. Various subinstallers and dialog boxes will appear over it.

4. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
5. On the **Installation Type** screen, select **Custom**.
6. On the **Summary** screen, click **Next** to continue the installation.

   If current-version components are already installed on this machine, the links next to a product will be **Modify** and **Remove**, rather than install. Click **Remove** to remove components and **Modify** to add components.

# Installing TRITON Infrastructure

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6

# Installing TRITON Infrastructure

*TRITON Infrastructure* is composed of common user interface, logging, and reporting components required by the TRITON Unified Security Center modules (i.e. TRITON - Web Security, TRITON - Data Security, and TRITON - Email Security).

When installing TRITON Infrastructure, you can choose to also install SQL Server 2008 R2 Express—a free, limited-performance version of SQL Server—to be used for Websense logging data. It is important to note that, as a best practice, SQL Server 2008 R2 Express should be used only in non-production or evaluation environments. A non-limited-performance version of SQL Server should be used in production environments.

1. It is assumed you have already launched the Websense installer done one of the following:
   - Selected the **Custom** installation type, and selected TRITON Infrastructure install. (See *Deployment*, page 658.)
   - Selected the TRITON Unified Security Center installation type. *Installing TRITON Unified Security Center*, page 646.)
   - Started an upgrade of prior-version Web or Data Security components, with TRITON - Web Security or - Data Security installed on this machine. In this case, skip to Step 4 now.
2. On the Custom Installation dashboard, click the **Install** link for TRITON Infrastructure.


If TRITON Infrastructure Setup has been started as part of a TRITON Unified Security Center installation, skip this step.

3. TRITON Infrastructure Setup is launched.
4. On the TRITON Infrastructure Setup **Welcome** screen, click **Next**.

5. On the **Installation Directory** screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.

   **Important**
   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   - To accept the default location (recommended), simply click **Next**. By default the installation directory is C:\Program Files\Websense\ (32-bit machines) or C:\Program Files (x86)\Websense\ (64-bit machines).
   - To specify a different location, use the **Browse** button.

6. On the **SQL Server** screen, specify the location of your database engine and how you want to connect to it.

   The information you enter on this screen will be used by the Web, Data, and Email security component installers as well. The Web, Data, and Email modules of the TRITON Unified Security Center will use the database and credentials you specify here to store and retrieve their data. The Web security component installer will allow you to override this database and credential information, and specify a different database. The Data and Email security component installers will not; they will use what is specified here during TRITON Infrastructure installation.

   - **Install SQL Server Express on this machine**: Select this option to install SQL Server 2008 R2 Express on this machine. TRITON Unified Security Center will use this database engine for Websense logging data.

     The Websense installer will automatically install .NET 3.5 SP1, Powershell 1.0, and Windows Installer 4.5 if not found on the machine. These are required for SQL Server 2008 R2 Express.

     A default database instance, named mssqlserver, will be created. If a database instance named mssqlserver already exists on this machine (for example, if MSDE is installed on this machine), then an instance named TRITONSQL2K8R2X is created instead.

     If you are installing TRITON Infrastructure as part of an upgrade process from prior-version Web Security, you may have to stop Filtering Service now. If .NET 3.5 SP1 is not found on this machine, the installer needs access to windowsupdate.microsoft.com. If Filtering Service blocks this machine from accessing windowsupdate.microsoft.com SQL Server Express cannot be installed.

     If you currently use MSDE for Websense data and want to use that data post-upgrade, back up the Websense databases now. See *Backing up Websense data from MSDE*, page 944 for instructions. Leave the Websense installer running and come back once you have backed up MSDE data.

   - **Use existing SQL Server on another machine**: Select this option to specify the location and connection credentials for a database server located elsewhere in the network.

- **Server Name**: Enter the hostname or IP address of the SQL Server machine. See *System Requirements* to verify your version of SQL Server is supported. To use a SQL Server instance, other than the default, specify it here. Note that the instance you want to use must already exist. Refer to Microsoft documentation for information about creating instances.

After selecting one of the above options (for installing SQL Server Express or using existing SQL Server) specify an authentication method, and user name and password; see below.

- **Authentication**: Select how Websense components on this machine should connect to the database engine. Select **SQL Server Authentication** to connect using a SQL Server account. Select **Windows Authentication** to connect using a Windows trusted connection.
  - **User Name**: If you are installing SQL Server Express on this machine, a user name of *sa* is automatically specified (this is the default system administrator account); enter the password you want for *sa*. This account must be configured to have system administrator rights in SQL Server.

    Otherwise, the currently logged in user that launched the Websense installer is taken as the Windows account to use to connect to SQL Server when Windows authentication is chosen. This account must have certain roles assigned; see *Installing with SQL Server*, page 690.

    You cannot specify a different account in the **SQL Server** screen when installing TRITON Infrastructure. If you want to use a different account, cancel the installation. Log onto the machine as the user you want used for SQL Server Windows authentication and then restart the Websense installer.

    In some organizations, policies are in place where service accounts (i.e., accounts used to run Windows services) cannot be interactive (i.e., used by a user for general login) and interactive accounts cannot be used to run services. In such a case, if possible, allow a service account to be interactive for the duration of installing Websense products. Log onto the machine with the service account, so services are properly installed to run as a service user, and then revoke the interactivity for that account after installation is complete.
  - **Password**: Enter the password for the specified account. If you chose to install SQL Server Express on this machine, confirm the password.

When you click **Next**, connection to the database engine is verified if you chose to use an existing SQL Server installation on another machine. If the connection test is successful, the next installer screen appears.

If the test is unsuccessful, the following message appears:

*Unable to connect to SQL*
*Make sure the SQL Server you specified is currently running. If it is running, verify the access credentials you supplied.*

Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

7. On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Unified Security Center.

   - **IP Address**: Select an IP address for this machine. If this machine has a single network interface card (NIC) then only one address will be listed.

     The IP address selected here is the one to use when accessing the TRITON Unified Security Center (via Web browser). This is also the IP address you should specify to any Websense component needing connection to the TRITON Unified Security Center machine.

     If you chose to install SQL Server 2008 R2 Express, when installing Web Security Log Server or Email Security Log Server on another machine, specify this IP address for the database engine location.

   - **Server/Domain**: Specify the server or domain of the user account to use be used by TRITON Infrastructure and TRITON Unified Security Center. By default, this field is filled with the server/domain of the account you logged into this machine with. If you want to specify a different account, be sure to use the **Browse** button.

   - User Name: Specify the user name of the account to be used by TRITON Unified Security Center. By default, this field is filled with the user name of the account you logged into this machine with. If you want to specify a different account, be sure to use the Browse button.

     **Important**

     Account names must include only ASCII characters– i.e. English-based letters, numbers and some special characters such as # and &.

   - Password: Enter the password for the specified account.

8. On the **admin Account** screen, enter an email address and password for the default administration account for TRITON Unified Security Center, and then click **Next**.

   Administrator accounts in TRITON Unified Security Center must have an email address. System notification and password reset information is sent to this address (only after SMTP configuration is done; see next step).

   It is a best practice to use a strong password as described on-screen.

9. On the **Email Settings** screen, enter information about the SMTP server to be used for system notifications and then click **Next**. Note that this is optional, you can configure these settings after installation in the TRITON Unified Security Center. If you do not want to configure these settings now, clear the **Configure email settings** check box and then click **Next**.

   **Important**

   If you do not configure an SMTP server now and you lose the **admin** account password (set on previous screen) before logging into TRITON Unified Security Center and configuring an SMTP server, the *Forgot my password* link on the login page will not provide password recovery information. SMTP server configuration must be completed before password recovery email can be sent by the system.

   - **IP address or hostname**: IP address or host name of the SMTP server through which email alerts should be sent. In most cases, the default **Port** (25) should be used. If the specified SMTP server is configured to use a different port, enter it here.
   - **Sender email address**: Originator email address appearing in notification email.
   - **Sender name**: Optional descriptive name that can appear in notification email. This is can help recipients identify this as a notification email from the TRITON Unified Security Center.

10. On the **Pre-Installation Summary** screen, verify the information and then click **Next** to begin the installation..

    **Warning**

    If you chose to install SQL Server Express, depending on whether certain Windows prerequisites are installed, your machine may be automatically restarted up to two times during the installation process. Restarts are not required if the prerequisites are already installed.

    **Note**

    When you click **Next**, if you chose to install SQL Server Express on this machine, it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

11. If you chose to install SQL Server Express, .NET Framework 3.5 SP1, PowerShell 1.0, and Windows Installer 4.5 will be installed if not already present. Wait for Windows to configure components.

    a. If the following message appears during this process, click **OK**:

*Setup could not restart the machine. Possible causes are insufficient privileges, or an application rejected the restart. Please restart the machine manually and setup will restart.*

b. A software update installation wizard completion screen may appear for Hotfix for Windows Server 2003 (KB942288-v4). This is for Windows Installer 4.5. The machine must be restarted. Click **Finish** to restart now (do not select **Do not restart now**). Note that it may take approximately 1 minute for the restart to occur. Wait for the restart.

- If you are upgrading prior-version Web Security or Data Security the following message appears after restart. Click **OK**.

  *An older version of Web Security* (or *Data Security*) *is installed on this machine.*
  *press OK to upgrade it or Cancel to exit the installation.*

- If Websense Manager (v7.1) or TRITON - Web Security (v7.5) is installed on this machine, the following message appears. Click **Yes**.

  *Keep TRITON - Web Security on this machine and upgrade it to version 7.6 TRITON Unified Security Center?*

  *Selecting No will launch the current-version uninstaller. Uninstall the current-version TRITON - Web Security. After uninstall, remaining components will be upgraded to version 7.6.*

c. Websense installer starts again. In the TRITON Infrastructure Setup **Welcome** screen, click **Next**.

d. The **Ready to Resume EIP Infra installation** screen appears. Click **Next**.

> **Note**
> When you click **Next**, if you chose to install SQL Server it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

12. If you chose to install SQL Server Express on this machine, SQL Server 2008 R2 Setup is launched. Wait for it to complete.

    The Setup Support Files screen appears and then an Installation Progress screen appears. Wait for these screens to complete automatically. It is not necessary to click or select anything in these screens.

    Note that it may take approximately 10-15 minutes for the SQL Server 2008 R2 Express installation to complete.

13. Next, the **Installation** screen appears. Wait until all files have been installed.

    If the following message appears, check whether port 9443 is already in use on this machine:

    *Error 1920. Server 'Websense TRITON Central Access' (EIPManagerProxy) failed to start. Verify that you have sufficient privileges to start system services.*

    If port 9443 is in use, release it and then click **Retry** to continue installation.

14. On the **Installation Complete** screen, click **Finish**.
15. If you backed up Websense data from MSDE and chose to install SQL Server Express on this machine:

    **Note**

    Depending on the type of installation you are performing, the Websense installer may launch one of the component installers (i.e., for Web, Data, or Email Security) at this point. Leave the Websense and component installers running and perform the steps below. Then return to the component installer to continue the installation process.

    a. Restore the backed up data to SQL Server Express.

    See *Restoring Websense data to SQL Server Express*, page 945 for instructions.

    b. Configure Log Server to use the installation of SQL Server Express.

    See *Configuring 7.5 Log Server to SQL Server Express prior to upgrade to 7.6*, page 949 for instructions.

    This must be done or the Websense installer will be unable to upgrade Log Server to version 7.6. Note that Log Server may be running on a different machine.

# Installing Web Security components

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Installing Web Security components

Complete these steps to install Web security components on a machine. If you are installing components on multiple machines, run the Websense installer and complete these steps on each machine, selecting the particular components you want.

To install Web Security components on a Linux machine, see *Installing Web Security components on Linux*, page 336.

1. It is assumed you have already launched the Websense installer and chosen the Custom installation type. If not, see *Deployment*, page 658.

   If you are adding components, skip to Step 3 now.

2. On the Custom Installation dashboard, click the **Install** link for Web Security.


The Web Security component installer is launched.

3. On the **Select Components** screen, select the components you want to install on this machine.

**Note**

TRITON - Web Security is available in the **Select Components** screen only if TRITON Infrastructure is already installed on this machine. See *Installing TRITON Infrastructure*, page 661 for instructions.

**Important**

In any Web security deployment, the following three components must be installed in this order (and before any other Web security components):

- Policy Broker
- Policy Server
- Filtering Service

If you select all three to be installed at the same time on a machine, they are installed in the correct order. After these three components, all other Web security components can be installed in any order.

**Important**

There must be **only one** instance of Policy Broker in an entire deployment. Note that in an appliance-based deployment a Web Security mode appliance running in *full policy source* mode has Policy Broker already installed and running.

See the following for more information about each component:

- *Policy Broker*
- *Policy Server*
- *Filtering Service*
- *Network Agent*
- *Usage Monitor*
- *TRITON - Web Security*
- *Real-Time Monitor*
- *Web Security Log Server*
- *User Service*
- *DC Agent*
- *eDirectory Agent*
- *RADIUS Agent*
- *Logon Agent*
- *Filtering Plug-in*
- *Remote Filtering Client*
- *Remote Filtering Server*
- *Linking Service*
- *Sync Service*
- *Directory Agent*

4. Depending on the components you have selected, some or all of the following installer screens appear. (In the following list, after a screen name, is the component-selection or machine condition that causes the screen to appear.) Click the screen name for instructions.
   - *Policy Server Connection Screen*, page 673 (Filtering Service, Network Agent, Usage Monitor, TRITON - Web Security, Real-Time Monitor, Web Security Log Server, User Service, DC Agent, eDirectory Agent, RADIUS Agent, Logon Agent, Remote Filtering Client Pack, Remote Filtering Server, Linking Service, Sync Service, or Directory Agent)
   - *Policy Broker Connection Screen*, page 674 (Policy Server, Sync Service, or Directory Agent)
   - *Multiple Network Cards Screen*, page 676 (if multiple NICs detected)
   - *Active Directory Screen*, page 676 (if installing User Service, DC Agent, or Logon Agent on Windows Server 2008)
   - *Computer Browser Screen*, page 677 (if installing User Service, DC Agent, or Logon Agent on Windows Server 2008 and the Computer Browser service is not running)
   - *Integration Option Screen*, page 678 (Filtering Service)
   - *Select Integration Screen*, page 679 (Filtering Service, to be integrated with a third-party product, or Filtering Plug-In)
   - *Network Agent and Firewall Screen*, page 680 (Filtering Service and Network Agent; Filtering Service to be integrated with a Check Point product)
   - *Filtering Plug-In Screen*, page 680 (Filtering Service, to be integrated with Citrix, Microsoft ISA Server, or Squid Web Proxy Cache)

- *Squid Configuration Screen*, page 681 (Filtering Service, to be integrated with Squid Web Proxy Cache, or Filtering Plug-In)
- *Network Card Selection Screen*, page 681 (Network Agent)
- *Database Information Screen*, page 682 (Web Security Log Server)
- *Log Database Location Screen*, page 683 (Web Security Log Server)
- *Optimize Log Database Size Screen*, page 684 (Web Security Log Server)
- *Filtering Feedback Screen*, page 685 (Filtering Service or Network Agent)
- *Directory Service Access Screen*, page 685 (User Service, DC Agent, or Logon Agent)
- *Remote Filtering Communication Screen*, page 686 (Remote Filtering Server)
- *Remote Filtering Pass Phrase Screen*, page 688 (Remote Filtering Server)
- *Filtering Service Information for Remote Filtering Screen*, page 688 (Remote Filtering Server)
- *Filtering Service Communication Screen*, page 675 (Network Agent, a filtering plug-in, or Linking Service)

5. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

   The installation path must be absolute (not relative). The default installation path is:

   - C:\Program Files or Program Files (x86)\Websense\Web Security

   The installer creates this directory if it does not exist.

   > **Important**
   > The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   The installer compares the installation's system requirements with the machine's resources.

   - Insufficient disk space prompts an error message. The installer closes when you click **OK**.
   - Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.

6. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

7. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
8. If you chose to install the ISA Server filtering plug-in, the **Stop Microsoft Firewall Service** screen appears. Do the following:

a. Stop the Microsoft Firewall service and then click **Next**.

> **Note**
> Leave the Websense installer running as you stop the Microsoft Firewall service. Then return to the installer and click **Next** to continue installation.

> **Important**
> In order to correctly install the ISA Server filtering plug-in, the Microsoft Firewall Service must be stopped. Installation of the plug-in files and registration of the plug-in the system registry cannot occur while the Microsoft Firewall Service has certain files locked. Stopping the Microsoft Firewall Service unlocks these files.

To stop the Firewall service, go to the Windows Services console (**Administrative Tools > Services)**. Right-click Microsoft Firewall, and then select **Stop**. When the service has stopped, return to the Websense installer and continue the installation process. The Firewall Service may also be stopped from the ISA Server Management console or Command Prompt (using the command `net stop fwsrv`). See Microsoft's documentation for more information.

> **Important**
> When the Microsoft Firewall service is stopped, ISA Server goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service needs to be stopped for only a few minutes as the ISA Server filtering plug-in is installed and configured.

b. When the following message appears, start the Microsoft Firewall service and then click **OK**:

*The Websense ISAPI Filter has been configured, you can now start the Microsoft Firewall Service*.

To start the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click Microsoft Firewall, and then select **Start**.The Firewall Service may also be started from the ISA Server Management console or Command Prompt (using the command `net start fwsrv`). See Microsoft's documentation for more information.

9. On the **Installation Complete** screen, click **Done**.

Additional configuration may be necessary if integrating Web Filter or Web Security with another product. See:

- *Check Point Integration*, page 285

- *Cisco Integration*, page 193
- *Citrix Integration*, page 167
- *Microsoft ISA Server or Forefront TMG Integration*, page 227
- *Squid Web Proxy Cache Integration*, page 259
- *Universal Integrations*, page 323

## Policy Server Connection Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if any of the following is selected for installation but Policy Server is not:

| | |
|---|---|
| Filtering Service | Logon Agent |
| Network Agent | Remote Filtering Client Pack |
| Usage Monitor | Remote Filtering Server |
| TRITON - Web Security | Linking Service |
| Web Security Log Server | Sync Service |
| User Service | Directory Agent |
| DC Agent | Real-Time Monitor |
| eDirectory Agent | |
| RADIUS Agent | |

It is assumed Policy Server is installed on another machine. Enter the IP address of the machine and the port Policy Server uses to communicate with other Websense components (default is 55806). If this is a Websense-appliance-based deployment, Policy Server is already installed on the Web-security-mode appliance running in *full policy source* mode. In this case, enter the IP address of the appliance's C interface for the Policy Server IP address.

The port used by Policy Server to communicate with other Websense components must be in the range 1024-65535. In a software-based deployment, Policy Server may have been automatically configured to use a port other than the default 55806. When Policy Server is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Policy Server, check the `websense.ini` file—located in `C:\Program Files\Websense\Web Security\bin` (Windows) or

`/opt/Websense/bin` (Linux)—on the Policy Server machine. In this file, look for the **PolicyServerPort** value.

**Important**

Do not modify the `websense.ini` file.

If Policy Server is not installed yet, anywhere in your network, you must install it before installing any of the components listed above. To install it on this machine, click **Previous** and select **Policy Server** in addition to already selected components. To install it on another machine, run this installer on that machine (prior to installing components on this machine).

## Policy Broker Connection Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Policy Server, Sync Service, or Directory Agent is selected for installation, but Policy Broker is not.

In a software-base deployment, enter the IP address of the machine on which Policy Broker is installed and the port Policy Broker uses to communicate with other Websense components (default is 55880). If it is installed on this machine, enter its IP address (actual address, not loopback).

In an appliance-based deployment, Policy Broker is already installed on an appliance running in *full policy source* mode. Enter the IP address of the appliance's C interface and use the default port (55880).

The communication port must be in the range 1024-65535. Policy Broker may have been automatically configured to use a port other than the default 55880 for communication with other Websense components. When Policy Broker is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Policy Broker, check the `BrokerService.cfg` file—located in `C:\Program Files\Websense\Web Security\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Policy Broker machine. In this file, look for the **listen_port** value.

**Important**

Do not modify the `BrokerService.cfg` file.

If Policy Broker is not installed yet, anywhere in your network, you must install it before installing any other Websense Web security component. To install it on this machine, click **Previous** and select **Policy Broker** in addition to already selected components. To install it on another machine, run this installer on that machine.

## Filtering Service Communication Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Network Agent, a filtering plug-in, or Linking Service is selected for installation.

Enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). If Filtering Service is installed on this machine, enter the IP address of this machine (note: actual IP address, not the loopback address, 127.0.0.1).

In an appliance-based deployment, Filtering Service is already installed on a Web-security-mode appliance. Enter the IP address of the appliance's C interface and use the default port (15868). Note that a deployment may contain multiple appliances, each with a Filtering Service running. In that case, enter the C-interface IP address of the appliance with the Filtering Service you want Network Agent, filtering plug-in (i.e., integration product), or Linking Service to use.

The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535. In a software-base deployment, Filtering Service may have been automatically configured to use a port other than the default 15868. When Filtering Service is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Filtering Service, check the `eimserver.ini` file—located in `C:\Program Files\Websense\Web Security\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.

**Important**

Do not modify the `eimserver.ini` file.

If Filtering Service is not installed yet, anywhere in your network, you must install it before installing Network Agent, a filtering plug-in, Linking Service. To install it on this machine, click **Previous** and select **Filtering Service** in addition to already selected components. To install it on another machine, run this installation program on

that machine (prior to installing Network Agent, a filtering plug-in, or Linking Service on this machine).

**Important**

In the case of a filtering plug-in, when installing Filtering Service, be sure to do so as integrated with the integration product.

## Multiple Network Cards Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if multiple network interface cards (NICs) are detected on this machine.

Select the IP address of the NIC to be used by Websense Web Security software on this machine. This is the NIC that will be used to send block pages when a user requests filtered content.

**Important**

The installer cannot determine whether IP addresses are valid. It simply lists the currently configured address of each detected NIC. Be sure to verify that the IP address you select is valid in your network. An incorrect IP address will prevent Websense software on this machine from functioning properly.

You will specify later whether this NIC is also used by Network Agent to monitor Internet traffic and send protocol block messages.

**Note**

If the selected NIC will be used by Network Agent, it must support promiscuous mode.

## Active Directory Screen

### Applies to

- Web Filter v7.6

- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if you are installing User Service, DC Agent, or Logon Agent on Windows Server 2008.

Indicate whether you are using Active Directory to authenticate users in your network and then click **Next**.

## Computer Browser Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if all the following are true:

- Installing User Service, DC Agent, or Logon Agent on Windows Server 2008
- Using Active Directory
- Windows Computer Browser service is not currently running.

Choose whether to start this service and then click **Next**.

The Computer Browser service is a Windows utility that must be set to Automatic and Start in the Windows Services dialog box for Websense components to communicate with Active Directory.

> **Note**
> If you choose to start the Computer Browser service now, make sure the Computer Browser service is enabled on this machine. In most cases, it is disabled by default. The installer will attempt to start the service and configure it to start up automatically from now on. If the service is disabled, the installer will be unable to start it.

If you choose not to have the installer start the service, or if the installer is unable to start it, you must start it manually after installation. If you use Active Directory 2008 to authenticate users, you must also start the Computer Browser service on the Active Directory machine.

If you choose not to have the installer start the service, or if the installer is unable to start it, you must start it manually after installation. If you use Active Directory 2008 to authenticate users, you must also start the Computer Browser service on the Active Directory machine. See *Turning on the Computer Browser service*, page 689.

## Integration Option Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Filtering Service is selected for installation.

Indicate whether this is a stand-alone or integrated installation, and then click **Next**.

- **Stand-alone**: Websense software will not be integrated with a third-party product. Websense Network Agent monitors all Internet requests and sends them to Websense Filtering Service. Network Agent also sends block messages to users attempting to access filtered content.

  > **Note**
  > In a stand-alone environment, Network Agent must be installed (either on this machine or a networked machine).

- **Integrated with another application or device**: Websense software is installed in integrated mode, ready to integrate with a third-party firewall, proxy server, cache, or network appliance, referred to as an *integration product*. Select this option if you want to integrate Websense software with:
  - Websense Content Gateway
  - Check Point
  - Cisco ASA, Content Engine, PIX, or router
  - Citrix
  - Microsoft ISA Server or Forefront TMG
  - Squid Web Proxy Cache
  - Other supported integration (as a "universal" integration)

  The integration product communicates with Websense Filtering Service to determine whether to allow Internet requests. Filtering Service sends block pages, if necessary, to users attempting to access filtered content. In an integrated environment, Websense Network Agent is used only to filter requests on Internet protocols not managed by the integration product (for example, protocols for

instant messaging). Network Agent sends block messages and alerts when necessary.

> **Note**
> In an integrated environment, Network Agent is optional.

## Select Integration Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if you selected **Integrated with another application or device** in the *Integration Option Screen*.

Select your integration product and then click **Next**.

> **Note**
> If your subscription includes Websense Web Security Gateway or Web Security Gateway Anywhere, select **Websense Content Gateway** as the integration product.

If you selected Forefront TMG, the following message appears.

*Integration with Forefront TMG requires a Websense plug-in. Complete this installation process and then install the plug-in on the Forefront TMG machine, using the separate Forefront TMG plug-in installer. For more information, see the Installation Guide Supplement for use with Microsoft ISA Server and Forefront TMG.*

As the message indicates, complete this installation process to install Filtering Service integrated with Forefront TMG (and any other components you have selected). Then, run the separate Websense Forefront TMG installer, on the Forefront TMG machine, to install the filtering plug-in. See *Installing the ISAPI Filter plug-in for Forefront TMG*, page 234.

If you selected Filtering Plug-In for installation, the **Select Integration** screen shows only two options:

- Microsoft Internet Security and Acceleration Server
- Citrix

These are the only integration products requiring a filtering plug-in, on Windows.

If you want to integrate Web Filter or Web Security with Citrix products, see *Citrix Integration*, page 167.

## Network Agent and Firewall Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if you select Check Point as the integration product on the *Select Integration Screen* and you have chosen Network Agent as a component to install (in addition to Filtering Service).

Network Agent should not be installed on the Check Point machine (unless the machine has separate processors or virtual processors to separately support Network Agent and the firewall software). Network Agent uses packet capturing that may conflict with the firewall software. Choosing to not install Network Agent does not affect installation of the other Websense components, they will still be installed.

## Filtering Plug-In Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if you selected Microsft ISA Server or Squid Web Proxy Cache (Linux only) in the *Select Integration Screen*:

Select options as described below and then click **Next**.

If you selected Microsoft ISA Server or Squid Web Proxy Cache, you can choose either or both of the options in the **Filtering Plug-In** screen:

- **Yes, install the plug-in on this machine**: This option installs only the filtering plug-in on this machine. Enter the IP address and port for Websense Filtering Service. If you are integrating with Microsoft Forefront TMG, do **not** select this option. The plug-in for Forefront TMG is installed using a separate installer.See *Installing the ISAPI Filter plug-in for Forefront TMG*, page 234.)
- **Install other selected components**: This option installs all selected Websense components, but not the plug-in. Note: Selecting this option installs Websense

software in integrated mode, ready to integrate with Microsoft ISA Server or Squid Web Proxy Cache (whichever you selected).

> **Note**
> To install both the plug-in and selected Websense components, you must select both of the above options. When you select **Install other selected components**, the Filtering Service **IP address** and **Port** boxes are greyed out because you do not need to specify them; Filtering Service is being installed on this machine.

## Squid Configuration Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This screen appears if you selected Squid Web Proxy Cache as the integration product on the *Select Integration Screen*. It also appears if you selected Filtering Plug-In for installation and chose Squid Web Proxy Cache.

Enter paths to the squid.conf and squid executable files. The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

> **Note**
> The installer will automatically start Squid Web Proxy Cache once installation is complete.

## Network Card Selection Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Network Agent is selected for installation.

Select the network interface card (NIC) to be used by Network Agent and then click **Next**.

> **Note**
> This screen appears even if the machine does not have multiple NICs. In this case, only one NIC is listed.

This is the NIC that Network Agent will use to communicate with other Websense software components. All enabled NICs with an IP address are listed.

> **Note**
> For Network Agent to operate, this machine must be connected to a bi-directional span port (or mirror port) on a switch or hub that processes the network traffic to be monitored.

You may select multiple NICs. After installation, use TRITON - Web Security to configure how Network Agent will use each selected NIC (for more information, see the TRITON - Web Security Help).

On Linux, NICs without an IP address are also listed. Do not choose a NIC without an IP address.

After installation, you can configure Network Agent to use NICs without an IP address to monitor Internet requests. See the TRITON - Web Security Help for more information.

## Database Information Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Web Security Log Server is selected for installation and TRITON Infrastructure is not installed on this machine.

Enter the hostname or IP address of the machine on which a supported database engine is running (see *System Requirements* for supported database system

information). If a supported database engine is detected on this machine, its IP address is already entered by default. To use a database engine on a different machine, enter its IP address instead.

After entering the IP address of the database engine machine, choose how to connect to the database:

- **Trusted connection**: use a Windows account to log into the database. Enter the user name and password of a trusted account with local administration privileges on the database machine.
- **Database account**: use a SQL Server account to log into the database. Enter the user name and password for a SQL Server account that has administrative access to the database. The SQL Server password cannot be blank, or begin or end with a hyphen (-).

> **Note**
> The database engine must be running to install Websense reporting components. The installer will test for a connection to the specified database engine when you click **Next** on the **Database Information** screen. The installer cannot proceed unless a successful connection can be made.

## Log Database Location Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Web Security Log Server is selected for installation.

Accept the default location for the Log Database files, or select a different location. Then, click **Next**.

Note that if TRITON Infrastructure is installed on this machine, the default database location information is taken from TRITON Infrastructure's configuration. Typically, you should accept the default in this case.

If the database engine is on this machine, the default location is the Websense directory (`C:\Program Files\Websense`). If the database engine is on another machine, the default location is `C:\Program Files\Microsoft SQL Server` on that machine.

It is a best practice to use the default location. If you want to create the Log Database files in a different location (or if you already have Log Database files in a different location), enter the path. The path entered here is understood to refer to the machine on which the database engine is located.

**Important**

The directory you specify for the Log Database files must already exist. The installer cannot create a new directory.

You can also specify a particular database instance in this path. The instance must already exist. See Microsoft SQL Server documentation for information about instances and paths to instances.

## Optimize Log Database Size Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Web Security Log Server is selected for installation.

The options on this screen allow you to control the size of the Web Security Log Database, which can grow quite large. Select either or both of the following options and then click **Next**.

**Log Web page visits**: Enable this option to log one record (or a few records) with combined hits and bandwidth data for each Web page requested rather than a record for each separate file included in the Web page request. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities. Deselect this option to log a record of each separate file that is part of a Web page request, including images and advertisements. This results in more precise reports, but creates a much larger database and causes reports to generate more slowly.

**Consolidate requests**: Enable this option to combine Internet requests that share the same value for all of the following elements, within a certain interval of time (1 minute, by default):

- Domain name (for example: www.websense.com)
- Category
- Keyword
- Action (for example: Category Blocked)

- User/workstation

## Filtering Feedback Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Filtering Service or Network Agent is selected for installation.

Select whether you want Websense software to send feedback to Websense, Inc. to improve accuracy and then click **Next**.

Choosing to allow feedback to Websense, Inc. helps improve the accuracy of Websense software for all customers. The feedback consists of any URLs that could not be categorized by Websense software. Such uncategorized URLs are evaluated by Websense, Inc. If warranted, they are investigated in more detail and put into an appropriate category. The Websense Master Database is updated with this information. When your Websense software downloads the updated database, it will be able to categorize those URLs and filter them according to the policies you have set.

**Important**

No information about users or your network is collected. The information is only about the visited URLs themselves. Only uncategorized URLs and the frequency of requests to them are collected. Uncategorized intranet URLs are not included in feedback.

**Note**

You can later choose to enable or disable feedback (the feedback mechanism is known as WebCatcher) using the Log Server Configuration utility (**Start** > **All Programs** > **Websense** > **Web Security** > **Web Security Log Server Configuration**). For more information, see Log Server Configuration Help.

## Directory Service Access Screen

### Applies to

- Web Filter v7.6

- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if User Service, DC Agent, or Logon Agent is selected for installation.

Enter the domain, user name, and password of an account that is a member of the Domain Admins group on the domain controller. This must be the domain controller for the users you wish to apply user- or group-based filtering policies to. User Service uses this account to query the domain controller for user information.

> **Note**
> User information on domain controllers trusted by the domain controller in question will also be accessible.

If you choose not to specify a Domain Admin account now (by leaving the fields blank), you can specify it after installation:

- On Linux, specify a Domain Admin account to be used by User Service. For more information, see *Troubleshooting* > *User Identification* in the TRITON - Web Security Help.
- On Windows, configure the Websense User Service service to **Log on as** a Domain Admin user, using the Windows **Services** dialog box:
  a. Start the Windows **Services** dialog box (typically, **Start** > **Administrative Tools** > **Services**).
  b. Right-click Websense User Service and select **Properties**.
  c. In the service properties dialog box, select the **Log On** tab.
  d. Under **Log on as**, select **This account** and enter the domain\username and password (twice) of the trusted account you specified during installation.
  e. Click **OK**.
  f. A message appears informing you the account you specified has been granted the Log On As A Service right. Click **OK**.
  g. A message appears informing you the new logon name will not take effect until you stop and restart the service. Click **OK**.
  h. Click **OK** to exit the service properties dialog box.
  i. Right-click Websense User Service and select Restart.

## Remote Filtering Communication Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Remote Filtering Server is selected for installation.

The external IP address or host name of the firewall or gateway must be visible from outside the network. If you enter a host name, it must be in the form of a fully-qualified domain name: <*machine name*>.<*domain name*>

> **Important**
> Remember whether you entered an IP address or a host name here. When installing the Remote Filtering Client on user machines, you must enter this address in the same form (IP address or domain name).

> **Note**
> It is a best practice to use IP addresses, rather than host names, unless you are confident of the reliability of your DNS servers. If host names cannot be resolved, Remote Filtering Clients will be unable to connect to the Remote Filtering Server.

The external communication port can be any free port in the range 10-65535 on this machine. This port receives HTTP/HTTPS/FTP requests from external Remote Filtering Client machines (i.e. user machines, running Remote Filtering Client, outside the network). The default is 80. If a Web server is running on this machine, it may be necessary to use a different port.

> **Note**
> The external network firewall or gateway must be configured to route traffic, typically via PAT or NAT, from Remote Filtering Client machines to the internal IP address of this machine.

The internal communication port can be any free port in the range 1024-65535 on this machine. The default is 8800. This is the port to which remote client heartbeats are sent to determine whether a client machine is inside or outside the network. The external network firewall must be configured to block traffic on this port. Only internal network connections should be allowed to this port.

For more information, see the Remote Filtering Software technical paper.

## Remote Filtering Pass Phrase Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Remote Filtering Server is selected for installation.

The pass phrase has a maximum length of 32 characters. This pass phrase is combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

If you want this instance of Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.

The pass phrase must include only ASCII characters but cannot include spaces. Do not use extended ASCII or double-byte characters.

You must use this pass phrase when you install the Remote Filtering Client on user machines that will connect to this Remote Filtering Server.

## Filtering Service Information for Remote Filtering Screen

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Description

This Web Security installer screen appears if Remote Filtering Server is selected for installation.

- **Internal IP address**: Enter the actual IP address of the Filtering Service machine to be used by this instance of Remote Filtering Server.
- **Filtering port and Block page port**: The filtering port is used by Filtering Service to communicate with other Websense components. The block page port is used by Filtering Service to send block pages to client machines. These ports must be in the range 1024-65535. These ports must be open on any firewall between the Remote Filtering Server and Filtering Service.

Filtering Service may have been automatically configured to use ports other than the default 15868 (filtering port) and 15871 (block page port). When Filtering Service is installed, the installation program checks whether these default ports are already in use on that machine. If either is already in use, the port is automatically incremented until a free port is found.

To find the ports used by Filtering Service, check the `eimserver.ini` file—located in `C:\Program Files\Websense\Web Security\bin` (Windows) or */opt/Websense/bin* (Linux)—on the Filtering Service machine. Look for the **WebsenseServerPort** (filtering port) and **BlockMsgServerPort** (block page port) values.

**Important**

Do not modify the `eimserver.ini` file.

- **Translated IP address**: Use this box to provide the translated IP address of Filtering Service if it is behind a network-address-translating device. You must check **A firewall or other network device performs address translation between Remote Filtering Server and Filtering Service** to activate this box.

## Turning on the Computer Browser service

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Turning on the Computer Browser service

The Websense installer offers the option to turn on the Computer Browser service during installation of the following components on Windows Server 2008.

- Websense User Service
- Websense DC Agent
- Websense Logon Agent

If you chose not to have it started, or the installer was not successful, you must turn on the service manually.

In addition, if your network uses Active Directory 2008 to authenticate users, the Windows Computer Browser service must be running on the Active Directory machine. Note that the Windows Firewall must be turned off in order for the Computer Browser service to start.

Perform the following procedure on each machine running an affected component:

1. Make sure that Windows Network File Sharing is enabled.

a. Go to **Start** > **Control Panel** > **Network and Sharing Center**.
b. In the **Sharing and Discovery** section, set **File Sharing** to **On**.

2. Go to **Control Panel** > **Administrative Tools** > **Services**.
3. Double-click **Computer Browser** to open the Properties dialog box.
4. Set the **Startup type** to **Automatic**.
5. Click **Start**.
6. Click **OK** to save your changes and close the Services dialog box.
7. Repeat these steps on each machine running Windows Server 2008 and an affected component.

## Installing with SQL Server

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

### Installing with SQL Server

See *System Requirements*, page 41 for which versions of SQL Server are supported.

1. Install SQL Server according to Microsoft instructions, if needed.
2. Make sure SQL Server is running.
3. Make sure SQL Server Agent is running.

> **Note**
> On SQL Server 2008 Express R2, SQL Service Broker is used instead of SQL Server Agent.

4. Obtain the SQL Server logon ID and password for a SQL Server Administrator, or for an account that has db_creator server role, SQLAgent role, and db_datareader in **msdb**.

   You need this logon ID and password when you install Websense components.
5. Restart the SQL Server machine after installation.

> **Note**
> You must restart the machine after installing Microsoft SQL Server and before installing Websense Web Security Log Server or Email Security Log Server.

6. Make sure the TRITON Unified Security Center machine can recognize and communicate with SQL Server.

If Web Security Log Server or Email Security Log Server are installed on another machine, make sure it can communicate with SQL Server as well.

7. Install the SQL Server client tools on the TRITON Unified Security Center machine. Run the SQL Server installation program, and select **Connectivity Only** when asked what components to install.

   If Web Security Log Server or Email Security Log Server is installed on another machine, install the SQL Server client tools on that machine instead.

8. Restart the machine after installing the connectivity option. See Microsoft SQL Server documentation for details.

### Configuring Microsoft SQL Server user roles

Microsoft SQL Server defines SQL Server Agent roles that govern accessibility of the job framework. The SQL Server Agent jobs are stored in the SQL Server **msdb** database.

To install Websense Log Server successfully, the user account that owns the Websense database must have one of the following membership roles in the **msdb** database and db_datareader :

- SQLAgentUserRole
- SQLAgentReader Role
- SQLAgentOperator Role

The SQL user account must also have **dbcreator** fixed server role privilege.

Use Microsoft SQL Server Management Studio to grant the database user account the necessary permissions to successfully install Log Server.

1. On the SQL Server machine, go to **Start > Programs > Microsoft SQL Server 2005** or **2008 > Microsoft SQL Server Management Studio**.
2. Log into SQL Server as a user with SQL sysadmin right.
3. Select the **Object Explorer** tree, and then go to select **Security > Logins**.
4. Select the login account to be used during the installation.
5. Right-click the login account and select **Properties** for this user.
6. Select **Server Roles**, and then select **dbcreator**.
7. Select **User Mapping** and do the following:
   a. Select **msdb** in database mapping.
   b. Grant membership to one of these roles:
      - SQLAgentUserRole
      - SQLAgentReader Role
      - SQLAgentOperator Role
      - db_datareader
   c. Click **OK** to save your changes.
8. Click **OK** to save your changes.

# Installing Data Security Components

## Applies to

- Data Security v7.6

## Installing Data Security components

**Notes**

- If you are installing version 7.6 Data Security components as part of an upgrade process from a prior-version, start at step Step 3 below.
- To install Printer agent, use the WebsenseDataSecurityPrinterAgent.zip package instead of the Websense installer. See *Installing the printer agent*, page 509 for more information.
- A separate installer is used to install 64-bit TMG or SMTP Agents. See *Installing the 64-bit SMTP agent*, page 506 or *Installing the TMG agent*, page 507 for more information.

1. It is assumed you have already launched the Websense installer and chosen the Custom installation type. If not, see *Deployment*, page 658.

   **Note**

   If you plan to install a Data Security agent (for example, Printer Agent, ISA Agent, and so forth) TRITON Unified Security Center, with the Data Security module enabled, must already be installed in your network. See *Creating a TRITON Management Server*, page 645.

2. On the Custom Installation screen, click the ***Install*** link for **Data Security**.


> **Note**
> To install a Protector, a separate installer is used. See *Installing the protector*, page 481.

3. The Websense Data Security Installer is launched. On the **Welcome** screen, click **Next** to begin Data Security installation.

> **Note**
> If the .NET 2.0 server is not found on this machine, the Data Security Installer installs it. You may need access to the Windows installation disc or image.

4. In the **Destination Folder** screen, specify the folder into which to install Data Security components.

   The default destination is C:\Program Files *or* Program Files (x86)\Websense\Data Security. If you have a larger drive, it is used instead. Large removable drives may be detected by the system as a local drive and used as the default. Do not install on removable media.

> **Important**
> The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

> **Note**
> Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

5. In the **Select Components** screen, select the components you want to install on this machine.

> **Note**
> If there is insufficient RAM on this machine for Data Security Management Server components, a message appears. Click **OK** to dismiss the message. You are allowed to proceed with the installation. However, it is a best practice to only install if you have sufficient RAM.

Not all Data Security components may be available in the **Select Components** screen. Which components are available depends on the operating system of the machine and applications detected by the Data Security Installer. For example, if a print server is found, then Printer Agent will be available for installation.

> **Note**
> A *TRITON management server* already has a Data Security Server installed (if you chose the Data Security module of the *TRITON Unified Security Center*). Install Data Security Server on other machines only if you want secondary Data Security Servers.

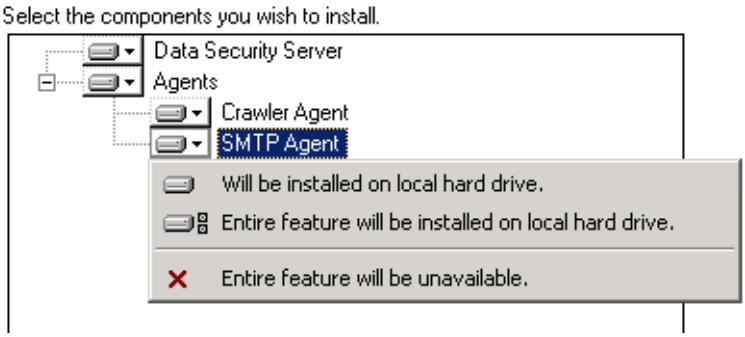
- **Crawler Agent**: scans networks transparently to locate confidential documents and data on endpoints, laptops and servers. It also performs fingerprinting, and scans databases as well as documents.
- **Printer Agent**: enables integration between printer servers and the Data Security Server intercepting print jobs from the printer spooler. Websense recommends you install the printer agent on a dedicated print server.

> **Note**
> To install Printer Agent, you must download and extract WebsenseDataSecurityPrinterAgent.zip prior to running the Websense installer. See *Detecting the printer driver*, page 510.

- **SMTP Agent**: enables integration between the SMTP Server and the Data Security Server enabling analysis of all external email, before forwarding it to the mail gateway.

- **ISA Agent**: receives all Web connections from Microsoft ISA Server and enables the Data Security Server to analyze them. Note that ISA Agent requires 1 GB free disk space on the ISA Server machine. The installer will not allow you to install ISA Agent if available space is less.
- **TMG Agent**: receives all Web connections from Microsoft Forefront TMG and enables the Data Security Server to analyze them.

Use the drop-down menu next to each component to select whether it will be installed.




**Notes:**

- Do not install a Data Security Server on a Microsoft Exchange or ISA Server in a production environment. ISA Server and Exchange Server consume so many system resources, Websense recommends you keep the Data Security Server separate.
- Do not install any Data Security component on a domain controller.
- If you are installing a supplemental Data Security Server, you cannot also install ISA Agent on the same machine.
- It is not a best practice to install the Printer Agent or ISA/TMG Agent on the same machine as a Data Security Server in production environments.

- **Will be installed on local hard drive**: selects the item for installation.
- **Entire feature will be installed on local hard drive**: if an item has sub-items, selecting this option chooses all sub-items for installation.
- **Entire feature will be unavailable**: deselects an item for installation; it will not be installed. If an item has sub-items, all sub-items will be deselected. Deselected items show a red X next to them.

If you have selected Crawler Agent for installation, the following message may appear:

*Data Security Discovery Agent works with a sepcific version of WinPcap.*
*The installation has detected that your WinPcap version is <version>*
*In order to proceed with this installation, WinPcap version 4.0.0.1040 needs to be*

*installed and will replace yours.*
*Click Yes to proceed or Click No to preserve your WinPcap version and deselect the Discovery Agent Feature to continue with the installation.*

"Discovery Agent" refers to Crawler Agent. The particular version of WinPcap mentioned in this message must be in place to install Crawler Agent. Note that after installation of Crawler Agent you can install a different version of WinPcap. Crawler Agent should continue to work properly.

6. Which components are selected for installation determines which remaining installer screens appear. In the remaining steps, follow only the instructions that apply to the components you have selected.
7. Use the options on the **Import Data From Previous Version** screen to restore data from a backup of a previous-version Data Security Server if necessary.

   Select the **Load Data From Backup** check box and then use the **Browse** button to specify the location of the backup data you want restored.

   For more information about backups, see the TRITON - Data Security Help.

   > **Note**
   > If you are upgrading a prior-version of Data Security, select **Load data from previous version** and then use the **Browse** button to specify the location of the data exported when you ran the export script at the beginning of the upgrade process.

8. If your SQL Server database is on a remote machine, you are prompted for the name of a temporary folder. This screen defines where Data Security should store temporary files during archive processing as well as system backup and restore.

   Archiving lets you manage the size of your incident database and optimize performance. Backup lets you safeguard your policies, forensics, configuration, data, fingerprints, encryption keys, and more.

   If you do not plan to archive incidents or perform system backup and restore, you do not need to fill out this screen.

   Before proceeding, create a folder in a location that both the database and TRITON management server can access. (The folder must exist before you click **Next**.) On average, this folder will hold 10 GB of data, so choose a location that can accommodate this.

**v7.6.0 to v7.6.2**

On the **Temporary Archive Folder** screen, complete the fields as follows:

> **Important**
> The **Temporary Archive Folder** screen affects system backup and restore as well as incident archiving.

- **Enable incident archiving**: Check this box if you plan to archive old or aging incidents or perform system backup. This box does not appear when you run the installer in Modify mode and perform a disaster recovery restore operation.
- **SQL Server Access**: Enter the path that the SQL Server should use to access the temporary folder. For best practice, it should be a remote Universal Naming Convention (UNC) path, but local and shared network paths are supported. For example: c:\folder or \\10.2.1.1.\folder.
- **Data Security Management Security Access**: Enter the UNC path that the management server should use to access the temporary folder. For example: \\10.2.1.1.\folder. Enter a user name and password for a user who is authorized to access this location and optionally a domain.

**v7.6.3 and beyond**

On the **Temporary Folder Location** screen, complete the fields as follows:

- **Enable incident archiving and system backup**: Check this box if you plan to archive old or aging incidents and perform system backup or restore. This box does not appear when you run the installer in Modify mode and perform a disaster recovery restore operation.
- **From SQL Server**: Enter the path that the SQL Server should use to access the temporary folder. For best practice, it should be a remote UNC path, but local and shared network paths are supported. For example: c:\folder or \\10.2.1.1.\folder.
- **From TRITON Management Server**: Enter the UNC path the management server should use to access the temporary folder. For example: \\10.2.1.1.\folder. Enter a user name and password for a user who is authorized to access this location.

> **Important**
> For all 7.6.x versions, the account used to access the SQL Server must have BACKUP DATABASE permissions to communicate with the installer. If it does not, an error results when you click **Next**.

To grant this permission, issue the following T-SQL commands on the SQL Server instance:

```
USE master
GRANT BACKUP DATABASE TO <user>
GO
```

After installation of Data Security components, you can revoke this permission:

```
USE master
REVOKE BACKUP DATABASE TO <user>
GO
```

9. Starting with v7.6.3, if a Lotus Notes client is detected on this machine, the**Lotus Domino Connections** screen appears.

   If you plan to perform fingerprinting or discovery on your Domino server, complete the information on this page.

   **Important**

   Before you complete the information on this screen, make sure that you:

   - Create at least one user account with administrator privileges for the Domino environment. (Read permissions are not sufficient.)
   - Be sure that the Lotus Notes installation is done for "Anyone who uses this computer."
   - Connect to the Lotus Domino server from the Lotus Notes client.

   a. On the **Lotus Domino Connections** page, select the check box labeled **Use this machine to scan Lotus Domino servers**.

   b. In the **User ID file** field, browse to one of the authorized administrator users, then navigate to the user's **user.id** file.

   **Note**

   Select a user that has permission to access all folders and Notes Storage Format (NSF) files of interest, otherwise certain items may not be scanned.

   c. In the **Password** field, enter the password for the authorized administrator user.

10. If installing Printer Agent, the **Print Processor Destination(s)** screen appears.

    This screen is for information only; there are no options to select. The displayed list contains the names of all cluster nodes on which the Printer Agent is installed. Make sure that all nodes holding print spooler resources are listed.

11. If installing Printer Agent, the **Optical Character Recognition** screen appears.

    The Optical Character Recognition (OCR) service that is bundled with the Data Security software begins installation of the OCR service. Once the OCR service finishes installation, the OCR screen is displayed.

| Section | Description |
|---|---|
| OCR Analysis Threshold | **Per printed page:**<br>This parameter limits dynamically (according to the number of pages) the total time that the OCR can extract text from the printed job. In case of a timeout, the content analysis will be performed only on the extracted text that took place before the timeout.<br>(Default value: 3 sec.; Range: 1-60 sec.)<br>**No more than *nn* seconds:**<br>This number is a static overall limit to the total time that the OCR can extract text from the printed job. In case of a timeout, the content analysis will be performed only on the extracted text that took place before the timeout.<br>(Default value: 300 sec.; Range: 1-3600 sec.) |
| OCR Accuracy | Running the OCR in accurate mode results in higher latency. Administrators can set the size of jobs that will be executed in the most accurate OCR mode (small jobs do not produce high latency, so it is reasonable to use better accuracy). In most cases, lower OCR quality is sufficient and provides good results.<br>Keep in mind that the average OCR Analysis per printed page limit is ignored for small documents, but the entire print job limit is still adhered to.<br>(Default value: 5 pages) |

    Optionally, you can change the default values defined for the OCR Analysis Threshold and the OCR Accuracy.

12. If installing Data Security Server, the **Fingerprinting Database** screen appears.

    To choose a location other than the default shown, use the **Browse** button.

13. If installing SMTP Agent, the **Virtual SMTP Server** screen appears.

    In the **Select Virtual Server** list, select the IIS virtual SMTP server that should be bound to the Data Security SMTP Agent. SMTP Agent will monitor traffic that goes through this virtual server. If there multiple SMTP servers listed, the SMTP Agent should typically be bound to Inbound.

14. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
15. In the **Register with the Data Security Server** screen specify the location and log on credentials to a Data Security Server.

    FQDN is the fully-qualified domain name of a machine.

If you are installing a secondary Data Security Server, enter the location and log on credentials for the TRITON Unified Security Center machine.

If you are installing an agent, enter the location and log on credentials for the TRITON Unified Security Center machine.

16. In the **Local Administrator** screen, enter a user name and password as instructed on-screen.
17. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.

    Installation may seem to take a long time. Unless a specific error or failure message appears, allow the installer to proceed.

    If the following message appears, click **Yes** to continue the installation:

    *Data Security needs port 80 free.*
    *In order to proceed with this installation, DSS will free up this port.*
    *Click Yes to proceed OR click No to preserve your settings.*

    Clicking **No** cancels the installation.

    A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.
18. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.
19. Additionally, a **Printer Agent Configuration** screen may appear.
    a. Select a printer from the list and click **OK**.

       A red exclamation point indicates that a printer has settings that are incompatible with the printer agent. The printer agent is unable to monitor traffic for printers that are configured with incompatible settings, for example, "Print directly to printer." Hover the mouse over a problematic printer for details in a tooltip.

       You can still select an incompatible printer. If you do, the following message appears:

       *The Websense Printer Agent is unable to monitor traffic when one or more printers are configured with incompatible settings. Do you wish Websense to correct the settings?*

       Click **Yes**. The settings are automatically modified to accommodate the printer agent.

    b. Once installation is complete, the printers you selected appear as policy resources in the TRITON - Data Security module of the TRITON Unified Security Center (navigate to **Main** > **Configuration** > **Resources**). See *Accessing the TRITON Unified Security Center*, page 765.

    c. To complete the process, click Deploy in TRITON - Data Security.
20. Once installation is complete, the **Installation Successful** screen appears to inform you that your installation is complete.

# Installing Email Security Components

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Installing Email Security components

Websense Email Security Gateway is an exclusively appliance-based solution. All components run on the appliance exclusively except for TRITON - Email Security (i.e. the Email Security module of the TRITION Unified Security Center) and Email Security Log Server. These are the only two Email Security components that may be installed using the Websense installer.

1. It is assumed you have already launched the Websense installer, chosen the Custom installation type. If not, see *Deployment*, page 658.
2. On the **Custom Installation** dashboard, click the *Install* link for Email Security.


3. The Email Security component installer is launched.
4. On the **Introduction** screen, click **Next**.
5. If the Email Security Installer detects TRITON Infrastructure on this machine, it operates as if it is part of a TRITON Unified Security Center installation. See *Installing the Email Security module for TRITON Unified Security Center*, page 653 for instructions.

   If TRITON Infrastructure is not detected, then the Email Security Installer operates in custom mode, see the remaining steps below.

6. In the **Select Components** screen specify whether you want to install Email Security Log Server.

   Email Security Log Server is selected for installation by default. To install Email Security Log Server, SQL Server or SQL Server Express (see *System Requirements*, page 41 for supported database systems) must already be installed and running in your network.

   If you choose to install Email Security Log Server, the Email Security Log Server Configuration utility is also installed. This utility can be accessed by selecting **Start** > **All Programs** > **Websense** > **Email Security** > **Email Security Log Server Configuration**.

7. If TRITON Infrastructure is not found already installed on this machine, the **Log Database** screen appears. Specify the location of a database engine and how you want to connect to it.

   - **Log Database IP**: Enter the IP address of the database engine machine. If you want to use a named database instance, enter it the form *<IP address>\<instance name>*. Note that the instance must already exist. See your SQL Server documentation for instructions on creating instances.
     If you chose to install SQL Server Express as part of the installation of the TRITON Unified Security Center, the log database IP address should be that of the TRITON Unified Security Center machine.
   - **Database login type**: Select how Email Security Log Server should connect to the database engine.
     - **Trusted connection**:connect using a Windows trusted connection.
     - **Database account**:connect using a SQL Server account.

     Then enter a user name and password.
     - If using a trusted connection, enter the domain\username of the account to be used. This account must be a trusted local administrator on the database engine machine.
     - If using a database account, enter the name of a SQL Server account. This account must have certain roles assigned; see *Installing with SQL Server*, page 690.

   When you click **Next**, connection to the database engine is verified. If the connection test is successful, the next installer screen appears.

8. On the **Email Security Database File Location** screen, specify where Email Security database files should be located and then click **Next**.

   This screen appears only if you chose to install Email Security Log Server. A default location for the Log Database is automatically shown. It is a best practice to use the default location. If you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files. The path entered here is understood to refer to the machine on which the database engine is located. The path entered must specify a directory that already exists.

   If any Email Security components (e.g., TRITON - Email Security or another instance of Email Security Log Server) have already been installed in your

deployment, the following message appears:

*The Email Security database exists, do you want to remove it?*

This occurs because the database was created upon installation of the other Email Security components. Click **No** to continue using the existing database. In general, you should keep the database if you are sure the database was created only during the course of installing other components in your current deployment.

Clicking **Yes** removes the database..

> **Warning**
> If any Email Security log data has been written to the database it will be lost if you remove the database. If you want to keep this data, back up the esglogdb76 and esglogdb76_*n* databases. See your SQL Server documentation for backup instructions.

> **Warning**
> If you remove the database, any currently quarantined email will no longer be accessible.

9. On the **Installation Folder** screen, specify the location to which you want to install Email Security Log Server and then click **Next**.

   > **Important**
   > The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   To select a location different than the default, use the **Browse** button.

   Email Security Log Server will be installed in its own folder under the parent folder you specify here.

10. On the **Pre-Installation Summary** screen, review the components to be installed. If they are correct, click **Install**.
11. The **Installing Websense Email Security** screen appears, as components are being installed.
12. Wait until the **Installation Complete** screen appears, and then click **Done**.

# Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Installing SQL Server 2008 R2 Express

During TRITON Infrastructure installation, you can choose to install SQL Server 2008 R2 Express along with it. If you are installing TRITON Infrastructure, and you want to install SQL Server 2008 R2 Express on the same machine (i.e., the *TRITON management server*) you should do so during TRITON Infrastructure installation. See *Installing TRITON Infrastructure*, page 661.

This section provides instructions for installing SQL Server 2008 R2 Express without installing TRITON Infrastructure. Typically, this is done to install SQL Server 2008 R2 Express on a machine that is not a TRITON management server.

1. If you will use SQL Server 2008 R2 Express to store and maintain Web Security data, log in to the machine as domain user. Do this prior to starting the Websense installer.
2. It is a best practice to install the Windows prerequisites for installing SQL Server Express beforehand:
   - .NET Framework 3.5 SP1
   - Powershell 1.0
   - Windows Installer 4.5

   **Note**
   The Websense installer will automatically install these if not found on the machine.

   See *SQL Server 2008 R2 Express*, page 59.
3. If you currently use MSDE for Websense data and want to use that data post-upgrade, back up the Websense databases now. See *Backing up Websense data from MSDE*, page 944 for instructions. Leave the Websense installer running and come back once you have backed up MSDE data.

You may have to stop Filtering Service now. If .NET 3.5 SP1 is not found on this machine, the installer needs access to windowsupdate.microsoft.com. If Filtering Service blocks this machine from accessing windowsupdate.microsoft.com SQL Server Express cannot be installed.

4. It is assumed you have already launched the the Websense installer and chosen the Custom installation type. If not, see *Custom Installation*.

   You may also be following these instructions as part of upgrading (Web Security) Log Server to version 7.6. If so, skip this step. Also note that instead of the Custom Installation dashboard, you may be in the **Modify Installation** dashboard. The steps to complete remain the same.

5. On the **Custom Installation** dashboard, click the *Install* link for SQL Server Express.
6. On the **Welcome** screen, click **Start** to begin the installation wizard.
7. On the **Configuration** screen, selection options as described below and then click **Next**.
   - Use the **Browse** button to specify a different folder if you do not want to install to the default location shown.
   - If you want to create a named instance, instead of using the default SQL Server instance, select **Named instance** and then enter an instance name. Note the following about instance names:

     **Note**

     If MSDE is currently installed on this machine, you must install SQL Server Express to a named instance. It is a best practice to name the instance TRITONSQL2K8R2X. Other upgrade instructions regarding moving Websense data from MSDE to SQL Server Express will assume this instance name if both are installed on the same machine. If you choose a different one, substitute the instance name accordingly when following those instructions.

     - Not case sensitive
     - 16 characters or less
     - Only letters, numbers, dollar sign ($), or underscore (_) are allowed
     - First character must be a letter
     - Cannot contain the term *Default* or other reserved keyword (see Microsoft documentation for more information about reserved keywords)
   - Select an authentication mode:
     - **Windows Authentication mode**: select this to use Windows authentication, i.e., trusted connection, to authenticate users.
     - **Mixed Mode (SQL Server authentication and Windows authentication)**: select this to use SQL Server authentication. Enter a password (and re-enter to confirm) for the built-in SA user.

Depending on your selections, the Pre-Installation Summary screen, will show different information than shown in the above illustration.

> **Warning**
> Depending on whether certain Windows prerequisites are installed, your machine may be automatically restarted up to two times during the installation process. Restarts are not required if the prerequisites are already installed.

8. In the **Pre-Installation Summary** screen, click **Next** to begin installation.

   The Setup Support Files screen appears and then an Installation Progress screen appears. Wait for these screens to complete automatically. It is not necessary to click or select anything in these screens.

   Note that it may take approximately 10-15 minutes for the SQL Server 2008 R2 Express installation to complete.

9. Next, the **Installation** screen appears. Wait until all files have been installed.
10. On the **Summary** screen, click **Finish**.
11. If you backed up Websense data from MSDE:
    a. Make sure TCP/IP connection to the database instance is enabled and SQL Server Browser service is running.

       See *SQL Server 2008 R2 Express*, page 766 for instructions.

    b. Restore the backed up data to SQL Server Express.

       See *Restoring Websense data to SQL Server Express*, page 945 for instructions.

    c. Configure Log Server to use the installation of SQL Server Express.

       See *Configuring 7.5 Log Server to SQL Server Express prior to upgrade to 7.6*, page 949 for instructions.

       This must be done or the Websense installer will be unable to upgrade Log Server to version 7.6. Note that Log Server may be running on a different machine.

# 45 Components

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## In this topic



## Overview

This section of the Websense Technical Library contains brief descriptions of Websense components, organized into the following categories.

## TRITON Unified Security Center components

- *TRITON Infrastructure*, page 710

## Web Security

- *Policy Broker*, page 712
- *Policy Server*, page 713
- *Filtering Service*, page 715
- *Network Agent*, page 716
- *Usage Monitor*, page 718
- *TRITON - Web Security*, page 718
- *Web Security Log Server*, page 719
- *User Service*, page 721
- *DC Agent*, page 722
- *eDirectory Agent*, page 723
- *RADIUS Agent*, page 724
- *Logon Agent*, page 724
- *Logon Application*, page 725
- *Filtering Plug-in*, page 726
- *Remote Filtering Client*, page 727
- *Remote Filtering Server*, page 728
- *Linking Service*, page 729
- *Sync Service*, page 730
- *Directory Agent*, page 731
- *Real-Time Monitor*, page 732
- *Websense Content Gateway*, page 733

## Data Security

- *TRITON - Data Security*, page 733
- *Protector*, page 734
- *SMTP agent*, page 734
- *Microsoft ISA agent*, page 735
- *Endpoint agent*, page 735
- *Printer agent*, page 736
- *Integration agent*, page 736
- *Crawler*, page 737

# Email Security Gateway


- *TRITON - Email Security*, page 737
- *Email Security Log Server*, page 738


# TRITON management server

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Description

The term *TRITON management server* refers to the machine on which TRITON Unified Security Center is installed. This includes *TRITON Infrastructure* and any or all of the TRITON modules (Web Security, Data Security, and Email Security).

Typically, *Web Security Log Server* (Web Security deployments) and *Email Security Log Server* (Email Security Gateway deployments) are installed on the TRITON management server. However, this is not required and some organizations may choose to install these components elsewhere.

Optionally, SQL Server 2008 R2 Express may also be installed on the TRITON management server to be used to store Websense log data.

It is a best practice to limit the Websense components on the TRITON management server machine to the following:

- *TRITON Infrastructure*
- *TRITON - Web Security*
- *TRITON - Data Security*
- *TRITON - Email Security*
- *Web Security Log Server* (optional)
- *Email Security Log Server* (optional)
- *SQL Server 2008 R2 Express* (optional)
- *Real-Time Monitor* (optional)

- *Sync Service* (optional)
- *Directory Agent* (optional)

In most cases, if you must install additional components (other than those listed above) on a TRITON management server, you should avoid placing *Filtering Service* or *Network Agent* on the machine.

# TRITON Unified Security Center

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

The TRITON Unified Security Center is the Web browser-based, graphical management application for your entire deployment. It consists of three modules: *TRITON - Web Security*, *TRITON - Data Security*, and *Applies to*. Depending on your subscription, not all of these modules may be enabled.

Note that *TRITON Infrastructure* is required by TRITON Unified Security Center.

## Placement

The TRITON Unified Security Center is typically placed on a dedicated machine, referred to as the *TRITON management server*.

# TRITON Infrastructure

## Applies to

- Web Filter v7.6

- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

TRITON Infrastructure is composed of common user interface, logging, and reporting components required by the TRITON modules (i.e. TRITON - Web Security, TRITON - Data Security, and TRITON - Email Security). It also maintains an internal database of TRITON infrastructure settings.

TRITON Infrastructure is not intended to be installed by itself on a machine. It must be installed in conjunction with at least one of the TRITON modules mentioned above.

TRITON Infrastructure also (optionally) includes SQL Server 2008 R2 Express that may be used for Websense logging data.

## Placement

The TRITON Infrastructure is always installed on a *TRITON management server*.

# SQL Server 2008 R2 Express

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6

- V5000 G2 v7.6

## Description

SQL Server 2008 R2 Express is a free, limited-performance version of SQL Server 2008 R2. In place of one of the supported versions of SQL Server (see *System Requirements*, page 41) you can use SQL Server 2008 R2 Express to store and maintain Websense log and reporting data. Note, however, that due to performance limitations built in by Microsoft, SQL Server 2008 R2 Express may not be suitable for all organizations; see Administering Websense Databases for more information.

## Placement

SQL Server 2008 R2 Express can be installed on the *TRITON management server* or on a separate machine.

## Special Considerations

Only use the *Websense installer* to install SQL Server 2008 R2 Express for use with Websense solutions. Do not use an installer obtained elsewhere.

# Policy Broker

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

Policy Broker manages policy and configuration information required by other Websense Web security components. The Policy Database is installed with Policy Broker to store this information.

## Placement

In a Websense appliance-based deployment, Policy Broker is already installed on the appliance designated as *policy source*.

## Special Considerations

During a custom installation, Policy Broker is listed as a component you can install only if it is not found on the current machine. It might, however, be installed already on another machine. If it has been installed on another machine (or is running on a *policy source* appliance), do **not** install it on this machine.

**Important**

There can be only one instance of Policy Broker in the entire deployment. Policy Broker must be installed first, before any other Websense Web security component. If you select other components to install along with Policy Broker, they will be installed in the proper order.

**Note**

If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

# Policy Server

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

Policy Server identifies and tracks the location and status of other Websense Web security components in a deployment. It also:

- Logs event messages for Websense components.
- Stores configuration information specific to a single Policy Server instance.
- Communicates configuration data to *Filtering Service* for use in filtering Internet requests.

Policy and most configuration settings are shared between Policy Servers that share a Policy Database.

## Placement

In a Websense appliance-based deployment, Policy Server is already installed on the appliance designated as *policy source*.

In a software-based deployment, Policy Server is typically installed on the same machine as *Filtering Service*. Large or distributed environments can include multiple Policy Servers. Each Policy Server may communicate with up to 10 Filtering Services
See *Filtering Services per Policy Server*, page 88.

## Special Considerations

During a custom installation, to install Policy Server, Policy Broker must already be installed either on the same machine or another machine in the network. If *Policy Broker* is not installed already, you may choose to install both it and Policy Server at the same time.

**Important**

There can be only one instance of Policy Broker in the entire deployment. If Policy Broker is already installed on another machine, specify its location when asked by the installer. Do not install another instance of Policy Broker on this machine.

**Note**

If Policy Broker runs on an appliance, only on-appliance instances of Policy Server can communicate with Policy Broker. In this case, Policy Server cannot be installed off-appliance. If Policy Broker is installed off-appliance, however, both on-appliance and off-appliance instances of Policy Server can communicate with it.

In a very large network, or a network with a large volume of Internet traffic, you may need multiple Policy Server instances, on separate machines. All instances must connect to the same Policy Broker.

If multiple Policy Servers are installed, each must be installed before the other Web security components with which it communicates.

When you install Web security components on a machine separate from Policy Server, the installer asks for the Policy Server location and port number. The default port is 55806. The same port must be entered for each component that connects to this Policy Server.

# Filtering Service

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

Filtering Service works with Network Agent or an integration product to provide Internet filtering. When a user requests a site, Filtering Service receives the request and determines which policy applies.

- Filtering Service must be running for Internet requests to be filtered and logged.
- Each Filtering Service instance downloads its own copy of the Websense Master Database.

## Placement

In a Websense appliance-based deployment, Filtering Service is already installed on any Web security-mode appliance.

In a software-based deployment, Filtering Service is typically installed on the same machine as Policy Server. Large or distributed environments may include multiple Filtering Service instances.

## Special Considerations

During a custom installation, to install Filtering Service, *Policy Server* must already be installed either on this machine or another machine in the network. If Policy Server is not installed already, you can select it to be installed at the same time as Filtering Service. Typically, Policy Server is installed on the same machine as Filtering Service.

**Note**

The following three components must be installed in this order (and before any other components):

1. Policy Broker
2. Policy Server
3. Filtering Service

If you select all three to be installed at the same time, they are installed in the correct order. After these three components, all other Websense components can be installed in any order.

Depending on the size of the network or volume of Internet traffic, multiple Filtering Service instances may be needed. It is a best practice to have a maximum of ten Filtering Services per Policy Server.

Filtering Service must be installed before *Network Agent*, *Filtering Plug-in*, and *Linking Service*.

# Network Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

Network Agent works with Filtering Service to enable protocol management, bandwidth-based filtering, and reporting on bytes transferred.

- In a stand-alone software deployment (i.e. Filtering Service is not integrated with a third party gateway, firewall, or routing device), enables HTTP and non-HTTP filtering
- In an integrated software deployment, enables filtering for protocols not managed by your integration product and provides enhanced logging information

## Placement

In a Websense appliance-based deployment, Network Agent is already installed on any Web security-mode appliance.

In a software-based deployment, Network Agent must be installed on a machine that can see the Internet requests **from** the internal network as well as the Internet response **to** those requests. By connecting to a span or mirror port on a router or switch, Network Agent can monitor all Internet requests.

**Important**

Do **not** install Network Agent on a machine:

- Running Microsoft ISA Server.
- Running a firewall. Network Agent uses packet capturing that may conflict with the firewall software. The only exception is a blade server or appliance with separate processors or virtual processors to separately support Network Agent and the firewall software.

In busy networks, filtering performance improves if Network Agent is installed on a separate machine from Policy Broker, Policy Server, and Filtering Service.

To share load, multiple Network Agents can be installed on separate machines, with each one monitoring a separate IP-address range. The ranges combine to cover the entire network, but must not overlap. Overlapping ranges result in double logging of Internet activity. If the entire network is not covered by instances of Network Agent, some machines are not filtered and their Internet traffic not logged.

IP-address ranges for Network Agent are configured in the TRITON - Web Security module of the *TRITON Unified Security Center* after installation. See the Network Configuration topic in the TRITON - Web Security Help for instructions.

**Important**

If you install Network Agent on a machine that cannot monitor the targeted traffic, Websense features such as protocol management and Bandwidth Optimizer cannot perform as expected.

### Special Considerations

During a custom installation, Network Agent can be installed at the same time as Policy Server and Filtering Service. If Network Agent is installed on a separate machine, Filtering Service and Policy Server must be running before you install Network Agent. The installation cannot proceed if Policy Server and Filtering Service cannot be located.

If you use multiple instances of Network Agent, it is a best practice to have no more than 4 Network Agents per Filtering Service.

## Usage Monitor

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

### Description

Usage Monitor tracks users' Internet activity and sends alerts when Internet activity for particular URL categories or protocols reaches configured threshold limits. Alerts can be sent via email or on-screen display, or an SNMP alert can be sent to an SNMP Trap Server. Each Policy Server should have a separate Usage Monitor.

How alerts are sent is configured in the TRITON - Web Security module of TRITON Unified Security Center.See the TRITON - Web Security Help for more information.

## TRITON - Web Security

### Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 v7.6

- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

TRITON - Web Security is a module of the *TRITON Unified Security Center*. It is used to configure and manage the Web security features of a deployment.Use TRITON - Web Security to define and customize Internet access policies, add or remove filtering clients, configure Websense software components, generate reports, and more.

## Placement

In either Websense appliance-based or software-based deployments, TRITON - Web Security is installed, as part of the TRITON Unified Security Center.

On a Web security-mode appliance, TRITON Unified Security Center is pre-installed. However, this is typically disabled in favor of running TRITON Unified Security Center on a separate *TRITON management server*. An on-appliance TRITON Unified Security Center is typically used only for small or evaluation deployments.

**Important**

An on-appliance TRITON Unified Security Center has only the TRITON - Web Security module enabled, even if your subscription includes Data Security or Email Security. To enable the Data Security or Email Security modules, TRITON Unified Security Center must be located off the appliance, on a separate server (and the on-appliance TRITON Unified Security Center must be disabled; see Migrating TRITON - Web Security from or to an appliance).

# Web Security Log Server

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

Web Security Log Server logs Internet request data, including:

- Source of request
- Category or protocol associated with the request
- Whether the request was permitted or blocked
- Whether keyword blocking, file type blocking, quota allocations, bandwidth levels, or password protection were applied

Web Security Log Server can log to only one Web Security Log Database at a time, and only one Web Security Log Server can be installed for each Policy Server.

Web Security Log Server is a Windows-only component. It is not supported on Linux.

## Placement

Typically, Web Security Log Server is installed on the *TRITON management server*.

In a software-based deployment, it is a best practice to not install Web Security Log Server on the same machine as Filtering Service or Network Agent—filtering or logging performance may be affected if they are on the same machine.

In a Websense appliance-based deployment, Web Security Log Server must be installed on a separate, Windows machine—typically on the TRITON management server.

Environments with a high volume of Internet activity should place Web Security Log Server on a dedicated machine. Web Security Log Server processing can consume considerable system resources.

## Special Considerations

To be able to install Web Security Log Server, a supported database engine (see *System Requirements*, page 41) must be running.

> **Note**
> Web Security Log Server must be installed before you can see charts on the Status > Today and Status > History pages, or run presentation or investigative reports, in the TRITON - Web Security module of TRITON Unified Security Center.

If you install Web Security Log Server on a machine separate from TRITON Unified Security Center, stop and restart the **Websense TRITON - Web Security** and

**Websense Web Reporting Tools** services after installation. These services are on the *TRITON management server*.

**Important**

When Web Security Log Server is not installed on the TRITON management server, you **must** stop and restart the services mentioned above on the TRITON management server before creating scheduled jobs in presentation reports. You will be unable to create scheduled jobs until the services are restarted.

# User Service

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

User Service communicates with an LDAP or NTLM-based directory service to apply filtering policies based on users, groups, domains, and organizational units.

A deployment can have only one User Service per Policy Server.

The directory service is not a Websense product or component.

## Placement

In a Websense appliance-based deployment, User Service is already installed on any Web security-mode appliance.

In a software-based deployment, User Service is generally installed on the same machine as *Policy Server*.

## Special Considerations

When installing User Service (as part of a custom installation), log on with local administrator (Windows) or root (Linux) privileges before launching the installer. This ensures that User Service has the permissions it needs to enable user-based filtering. Administrator privileges can also be configured after installation. See the *Troubleshooting > User Identification* topic in the TRITON - Web Security Help for instructions.

During a custom installation, if you are installing User Service on a machine on which Policy Server is not installed, the installer asks you to identify the Policy Server machine. There must be only one User Service for each Policy Server.

After installation, follow the instructions in the *User Identification* section of the TRITON - Web Security Help to configure how Websense software identifies directory clients (users, groups, etc.).

**Note**

If User Service is installed on a Linux machine **and** Network Agent is used for protocol filtering, be sure to install the Samba client (v2.2.8a or later) on the User Service machine so that protocol block messages can be displayed on Windows computers.

# DC Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

DC Agent is a Websense transparent identification agent used in networks that authenticate users with a Windows directory service. It mainly does the following:

- Offers transparent user identification for users in a Windows-based directory service.
- Polls domain controllers in the network to transparently identify users.

- Communicates with User Service to provide up-to-date user logon session information to Websense software for use in filtering.

> **Note**
> DC Agent can be installed only on a Windows machine.

## Placement

In a Websense appliance-based deployment, DC Agent must be installed on a separate, Windows machine. It does not run on an appliance.

In a large network, you can install multiple DC Agents to provide ample space for files that are continually populated with user information.

Do not install DC Agent on the same machine as eDirectory Agent, because this can cause conflicts. Also, do not use DC Agent in a network in which eDirectory Agent is used.

If Websense software is integrated with a third-party product (firewall, proxy server, cache, or network appliance) providing user authentication, a transparent identification agent may not be necessary

# eDirectory Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

eDirectory Agent works with Novell® eDirectory™ to identify users transparently so that Websense software can filter them according to policies assigned to users or groups. eDirectory Agent gathers user logon session information from Novell eDirectory, which authenticates users logging on to the network. It then associates each authenticated user with an IP address and works with *User Service* to supply the information to *Filtering Service*.

## Placement

In a Websense appliance-based deployment, eDirectory Agent must be installed on a separate machine. It does not run on an appliance.

Do not install eDirectory Agent on the same machine as *DC Agent* or *Logon Agent*, because this can cause conflicts. Also, do not use eDirectory Agent in a network in which DC Agent or Logon Agent is used.

If Websense software is integrated with a third-party product (firewall, proxy server, cache, or network appliance) providing user authentication, a transparent identification agent may not be necessary.

# RADIUS Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

RADIUS Agent enables Websense software to provide user and group filtering by transparently identifying users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection. The agent can be used in conjunction with either Windows- or LDAP-based directory services.

# Logon Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

Logon Agent is a Websense transparent identification agent that detects users as they log on to Windows domains in your network. It is for use with Windows-based client machines on a network that uses Active Directory or Windows NT Directory. Logon Agent:

- Provides unsurpassed accuracy in transparent user identification in Linux and Windows networks.
- Does not rely on a directory service or other intermediary when capturing user logon sessions.
- Detects user logon sessions as they occur.

Logon Agent communicates with Logon Application on client machines to ensure that individual user logon sessions are captured and processed directly by Websense software.

## Placement

In a Websense appliance-based deployment, Logon Agent must be installed on a separate Windows machine. It does not run on an appliance.

Do not install Logon Agent on the same machine as eDirectory Agent, because this can cause conflicts. Also, do not use Logon Agent in a network in which eDirectory Agent is used.

## Special Considerations

To use Logon Agent, you must modify the Group Policy on domain controllers so it launches a *Logon Application* (**LogonApp.exe**) as part of the logon script. Client machines must use NTLM (v1 or v2) when authenticating users (NTLMv1 only, in the case of Windows Server 2008; see note below). For instructions on configuring domain controllers and client machines to use Logon Agent, see*Creating and running the script for Logon Agent*, page 782.

Logon Agent can be run with DC Agent if some of the users in your network are not being authenticated properly. If DC Agent is unable to identify certain users (for example, if it is unable to communicate with a domain controller due to network bandwidth or security restrictions), they would still be identified by Logon Agent at log on.

# Logon Application

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

Logon Application works with *Logon Agent*. It runs from a logon script on a domain controller to capture logon sessions as users log on to, or log off of, Windows domains in the network. Logon Application, `LogonApp.exe`, runs as a process on client Windows machines. Upon log on, Logon Application identifies the user and sends the information to Logon Agent.

## Placement

Logon Application runs as a process on client user machines. It is not installed directly, but rather it is pushed out via Group Policy in Windows domains when employing Logon Agent for user identification.

## Special Considerations

Logon Application runs only in conjunction with Logon Agent. The Group Policy on domain controllers must be modified so it launches Logon Application (**LogonApp.exe**) as part of the logon script. Client machines must use NTLM (v1 or v2) when authenticating users.

# Filtering Plug-in

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

Websense software can integrate with a third-party firewall, proxy, router, or similar product (referred to as an *integration product*). For certain integration products, a Websense filtering plug-in may be required to enable communication between Filtering Service and the integration product.

A filtering plug-in is required for Websense software to integrate with the following integration products:

- Microsoft ISA Server
- Microsoft Forefront TMG (see Note below)
- Citrix Presentation Server or XenApp
- Squid Web Proxy Cache

All other supported integration products (see *System Requirements*, page 41) do not require a filtering plug-in.

> **Note**
> The filtering plug-in for Microsoft Forefront TMG is installed using a separate installer. See*Installing the ISAPI Filter plug-in for Forefront TMG*, page 234.

## Placement

A filtering plug-in is installed on the integration product machine itself. Select this component only if running the Websense installer on the integration product machine.

## Special Considerations

*Filtering Service* must already be installed in order to install a filtering plug-in. If deploying the Citrix endpoint to a Citrix machine, Filtering Service should be installed on a different machine. If installing on an ISA Server or Squid Web Proxy Cache machine, Filtering Service may be installed on a different machine or the same machine. Note that for Forefront TMG, Filtering Service should be on a different machine.

# Remote Filtering Client

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

Remote Filtering Client allows filtering on client machines when they are outside the network. It can be deployed to Windows machines only.

Remote Filtering Client:

- Resides on client machines outside the network firewall.
- Identifies the machines as clients to be filtered.
- Communicates with *Remote Filtering Server*, installed inside the organization's firewall.

## Placement

Deploy the Remote Filtering Client to machines you want filtered when they are outside your network.

## Special Considerations

The Remote Filtering Client is deployed by copying an MSI installer package to user machines or using a third-party deployment tool. See the Remote Filtering Software technical paper for instructions.

The Remote Filtering Client is obtained by installing the Remote Filtering Client Pack on a Windows machine. Run the Websense installer in custom mode to install the Remote Filtering Client Pack.This places an MSI installer package in the following location on the installation machine: C:\Program Files\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\NO_MSI\CPMClient.msi). This package is used to deploy the Remote Filtering Client to user machines.

**Note**

If installing *Remote Filtering Server* on a Windows machine, install Remote Filtering Client Pack along with it. However, do not deploy the Remote Filtering Client on the machine. Simply install the Remote Filtering Client pack so you can deploy it from the Remote Filtering Server machine.

Before deploying the Remote Filtering Client on Windows Vista machines, make sure User Account Control (UAC) is disabled and that you are logged on to the machine as a local administrator.

# Remote Filtering Server

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

Remote Filtering Server provides Web filtering for machines such as laptops that are located outside the network firewall. A remote computer must be running the *Remote Filtering Client* to be filtered by the Remote Filtering Server.

Remote Filtering Server acts as a proxy that accepts requests from Remote Filtering Client and submits them for filtering. It communicates with *Filtering Service* to provide Internet access management of remote machines.

## Placement

In a Websense appliance-based deployment, Remote Filtering Server must be installed on a separate machine. It is not installed on an appliance.

Remote Filtering Server should be installed on a separate, dedicated machine. Ideally, it should be installed behind the outermost network firewall, but in the DMZ outside the firewall that protects the rest of the network.

## Special Considerations

Run the Websense installer (Windows) or the Web Security Linux installer in custom mode to install Remote Filtering Server on a machine. During installation, Remote Filtering Server connects to ports 40000, 15868, 15871, 55880, and 55806 on the machine or machines running Policy Server, Policy Broker, and Filtering Service. Also, Policy Server uses port 55825 to communicate with the Remote Filtering machine. If a firewall is installed between Remote Filtering Server and these other components, open these ports on the firewall. After installation is complete, ports 15868, 15871, 55880 must remain open.

Remote Filtering Server may be installed on a Windows or Linux machine. If this is a Windows machine, install Remote Filtering Client Pack (see *Remote Filtering Client*) along with Remote Filtering Server. This installs an MSI installer package that can be used to deploy the Remote Filtering Client to target user machines.

**Important**

Deploy the Remote Filtering Client to user machines but do not deploy it to the machine on which you are installing Remote Filtering Server.

See Remote Filtering Software technical paper for more information about installing, configuring, and using remote filtering.

# Linking Service

## Applies to

- Web Security Gateway Anywhere v7.6
- Data Security v7.6

## Description

Linking Service allows Web security and data security components to interoperate in the following ways:

- Allows Websense Data Security to access user information (collected by *User Service*) and URL categorization details from Websense Web Security.
- Enables shared administrative access to the TRITON - Web Security and TRITON - Data Security modules of the TRITON Unified Security Center.

Linking Service is required if your subscription includes Websense Web Security Gateway Anywhere.

## Placement

In a Websense appliance-based deployment, Linking Service must be installed on a separate Windows machine. It is not installed on an appliance.

Typically, Linking Service is installed on the *TRITON management server*.

## Special Considerations

Unless you are installing Linking Service at the same time as these components, make sure *Filtering Service*, *User Service*, and any transparent identification agents (*DC Agent*, *Logon Agent*, or *RADIUS Agent*) are already installed and running in your deployment.

# Sync Service

## Applies to

- Web Security Gateway Anywhere v7.6

## Description

In Websense Web Security Gateway Anywhere deployments, Sync Service:

- Sends policy updates and user and group information to the hybrid service.
- Receives reporting data from the hybrid service.

## Placement

In a Websense appliance-based deployment, Sync Service must be installed on a separate machine. It is not already installed on an appliance.

Typically, Sync Service is installed on the *TRITON management server* if *Web Security Log Server* is installed there as well. Otherwise, Sync Service is typically installed wherever Web Security Log Server is installed.

**Important**

There must be only one instance of Sync Service in an entire deployment of Websense Web Security Gateway Anywhere.

**Note**

If you have a distributed logging deployment (e.g., central office with Web Security Log Server and Log Database; branch offices with their own instances of Web Security Log Server that send data to the central office) be sure to install Sync Service so it communicates with the central Web Security Log Server instance and not one of the branch instances. Hybrid logging data cannot be passed to the central Web Security Log Server instance by branch instances.

## Special Considerations

To install Sync Service in a software-based deployment, Policy Server must already be installed on the same machine or a networked machine.

In a Websense appliance-based deployment, Policy Server is already installed and running on a Web security-mode appliance running in *full policy source* or *user directory and filtering* mode. During installation of Sync Service, when asked for the location of Policy Server, enter the IP address of the C interface on the appropriate appliance in your deployment.

# Directory Agent

## Applies to

- Web Security Gateway Anywhere v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

## Description

In Websense Web Security Gateway Anywhere deployments, Directory Agent collects user and group information from a configured directory service for use in filtering by the hybrid service.

## Placement

In a Websense appliance-based deployment, Directory Agent is already installed on a Web security-mode appliance running in *full policy source* or *user directory and filtering* mode. Typically, only one instance of Directory Agent should be installed in an entire deployment.

## Special Considerations

When installing Directory Agent, *Policy Server* must already be installed on the same machine or a networked machine.

While typically only one instance of Directory Agent should be operating in a deployment, it is possible to install multiple Directory Agent instances. But specific configuration is necessary for them to operate properly. For more information see the TRITON - Web Security Help.

# Real-Time Monitor

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Description

Real-Time Monitor provides a real-time running display of the browsing behavior of end users in your deployment, for troubleshooting and action verification. Once installed, it is accessible in the *TRITON - Web Security* module of the TRITON Unified Security Center.

## Placement

In a Websense appliance-based deployment, Real-Time Monitor must be installed on a separate Windows machine. It is not installed on and does not run on an appliance.

Typically, Real-Time Monitor is installed on the *TRITON management server*.

### Special Considerations

When installing Real-Time Monitor, *Usage Monitor* must already be installed on the same machine or a networked machine.

In a Websense appliance-based deployment, Usage Monitor is already installed on a Web security-mode appliance running in *full policy source* or *user directory and filtering* mode. During installation, when asked for the location of*Policy Server*, enter the IP address of the C interface on the appropriate appliance. Policy Server keeps track of the instance of Usage Monitor that will be used by Real-Time Monitor.

There should be only one instance of Real-Time Monitor per Policy Server.

## Websense Content Gateway

### Applies to

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- V10000 v7.6
- V10000 G2 v7.6
- V5000 G2 v7.6

### Overview

Content Gateway is a Web proxy and cache that passes HTTP(S) traffic to Websense software for filtering. Content Gateway Manager—the Web-browser-based management UI for Content Gateway—runs on the Content Gateway machine, but is typically accessed from within TRITON Unified Security Center.

In an appliance-based deployment of Web Security Gateway or Web Security Gateway Anywhere, Content Gateway runs on any Web-Security-mode appliance.

In software-based deployments, Content Gateway is installed on a Linux machine.

## TRITON - Data Security

### Applies to

- Web Security Gateway Anywhere v7.6

- Data Security v7.6
- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

### Description

The TRITON - Data Security module (also referred to as simply *Data Security module*) of the *TRITON Unified Security Center* used to manage the Data Security features of your deployment.

## Protector

### Applies to

- Data Security v7.6

### Description

The protector is an essential component of Websense Data Security, providing monitoring and blocking capabilities, preventing data loss and leaks of sensitive information. The protector can be configured to accurately monitor sensitive information-in-transit on any port.

See *Protector*, page 476 for more information.

## SMTP agent

### Applies to

- Data Security v7.6

### Description

You can install the SMTP agent on a Data Security Management Server, supplemental Data Security server, or as a stand-alone agent on another Windows server machine equipped with Microsoft IIS. See *System Requirements*, page 41 for supported operating systems.

**Important**

Prior to installing SMTP agent, be sure to prepare for installation as described in *Preparing a machine for SMTP agent*, page 64.

It receives all outbound email from the mail server and forwards it to a Websense Data Security Policy Engine. The SMTP agent then receives the analyzed email back from the policy engine and forwards it to the mail gateway. When installed on the Data Security Management server or supplemental Data Security server, the SMTP agent uses the local policy engine of those servers to analyze email, unless load balancing has been configured, in which case it uses the specified policy engine. The SMTP agent supports permit, block, and encrypt actions.

See *SMTP agent*, page 504 for more information.

# Microsoft ISA agent

## Applies to

- Data Security v7.6

## Description

The ISA agent receives all Web connections from a Microsoft ISA Server network and forwards them to the Data Security policy engine. It then receives the analyzed information back from the policy engine and forwards it to the recipients on the Web. Microsoft ISA 2004 and 2006 are supported on Windows Server 2003 standard R2 edition (32- or 64-bit). Forefront TMG is also supported, on Windows Server 2008 R2 platforms (64-bit).

See *Microsoft ISA/TMG agent*, page 506 for more information.

# Endpoint agent

## Applies to

- Data Security v7.6

## Description

The Websense Data Security Endpoint is a comprehensive, secure, and easy-to-use endpoint data loss prevention solution. The Data Security Endpoint monitors real-time traffic and applies customized security policies over application and storage interfaces, as well as for data discovery.

The Data Security Endpoint allows security administrators to either block or monitor and log files that present a policy breach. The data endpoint creates forensic monitoring that allows administrators to create policies that don’t restrict device usage, but allow full visibility of content traffic.

You can monitor user activity inside endpoint applications, such as the cut, copy, paste, print, and print screen operations. You can also monitor endpoint Web activities and Microsoft Outlook email, and know when users are copying data to external drives and endpoint devices.

Working with data endpoints entails configuring endpoint profiles via TRITON - Data Security. The configuration settings defined in TRITON - Data Security regulate the behavior of the endpoint agents. The endpoint agents analyze content within a user's working environment (PC, laptop and variants) and block or monitor policy breaches as defined by the endpoint profiles.

See *Printer agent*, page 508 for more information.

# Printer agent

## Applies to

- Data Security v7.6

## Description

The Data Security printer agent is required when you want to monitor what is printed on your organization's network printers.

The printer agent supports 32-bit Windows Server 2003 standard and R2 environments, and it supports permit and block actions.

When a user on the network prints a file, it is routed to the Microsoft Windows printer spooler service, where the printer agent intercepts it and sends it to the Data Security policy engine. After analysis of the content, the Data Security system enforces the policy as necessary: either auditing, monitoring or blocking the print job from being printed, in which case the sender (the user who printed the document) receives a notification that the print job was blocked.

See *Printer agent*, page 508 for more information.

# Integration agent

## Applies to

- Data Security v7.6

### Description

The Integration agent allows third-party products to send data to Websense Data Security for analysis. It is embedded in third-party installers and communicates with Data Security via a C-based API.

Third parties can package the integration agent inside their own installer using simple, 'industry standard' methods that are completely transparent to end users.

When the third-party product is installed on a users system, it needs to register the integration agent with the Data Security Management Server. This can be done transparently through the installation process or using a command-line utility.

See *Integration agent*, page 512 for more information.

## Crawler

### Applies to

- Data Security v7.6

### Description

The crawler is the name of the discovery and fingerprinting agent. It is selected by default when you install the Data Security Management Server or supplemental Data Security servers.

You can deploy additional crawlers in your network if you desire. When you set up a fingerprint task, you indicate which crawler should perform the scan. Websense recommends you use the crawler that is located closest in proximity to the data you are scanning.

You can view the status of your crawlers in the TRITON - Data Security user interface. Go to **Settings > Deployment > System Modules**, select the crawler and click on the **Edit** button.

## TRITON - Email Security

### Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Description

The TRITON - Email Security module of the*TRITON Unified Security Center* is used to configure and manage the email security features of your deployment.

TRITON - Email Security and Email Security Log Server are typically installed together, which helps to minimize the impact of report processing on Internet filtering.

## Placement

In either Websense-appliance-based or software-based deployments, TRITON - Email Security is installed, as part of the *TRITON Unified Security Center*, on a separate *TRITON management server*.

## Service Name

Websense components run as services. The service name of TRITON - Email Security is listed below.

| Windows | Linux |
|---|---|
| Websense TRITON - Email Security | n/a |

# Email Security Log Server

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Description

Email Security Log Server logs email security data to the Websense Log Database. Email Security Log Server is a Windows-only component. It is not supported on Linux.

## Placement

Typically, Email Security Log Server is installed on the *TRITON management server*.

In a Websense appliance-based deployment, Email Security Log Server must be installed on a separate, Windows machine—typically on the TRITON management server.

## Special Considerations

To be able to install Email Security Log Server, a supported database engine (see *System Requirements*) must be running. If you install Email Security on a machine separate from TRITON Unified Security Center, stop and restart the **Websense TRITON - Email Security** service after installation. This service is on the *TRITON management server*.

## Service Name

Websense components run as services. The following is the service name for Email Security Log Server.

| Windows | Linux |
|---|---|
| Email Security Log Server | n/a |

# 46 Installing and Deploying Websense Endpoint Clients

## Applies to

- Data Security v7.6.3 and beyond
- Web Security v7.6.2 and beyond
- Web Security Gateway v7.6.2 and beyond
- Web Security Gateway Anywhere v7.6.2 and beyond

## In this topic



## Overview

Websense, Inc., offers solutions for securing client workstations, laptops, and other **endpoint devices** from data loss and inbound Web threats when the devices are outside the corporate network.

The solutions are **endpoint client** software applications that run on the endpoint devices to block, monitor, and log transactions (like Internet requests) according to the organization's security and acceptable use policies. Administrators can create policies that provide full visibility into inbound and outbound traffic, but that don't restrict use of the device.

For Web security, the endpoint clients are:

- Remote Filtering Client (see *When to use the Remote Filtering Client*, page 742)
- Websense Web Endpoint (see *When to use Web Endpoint*, page 742)

And for data loss prevention (DLP):

- Websense Data Endpoint (see *When to use Data Endpoint*, page 743)

Websense endpoint solutions include both server and client components. See *System Requirements*, page 41, for information about the hardware and operating systems supported by endpoint components.

## When to use the Remote Filtering Client

Websense Web Filter, Web Security, and Web Security Gateway (Anywhere) customers can use remote filtering software to monitor and filter Internet activity for endpoint devices (client machines) outside the network.

**Important**

In Web Security Gateway Anywhere deployments, Remote Filtering Client cannot be used for clients filtered by the hybrid service.

Remote filtering software has 2 components: Remote Filtering Client and Remote Filtering Server.

- Remote Filtering Client is installed on each endpoint device (client machine).
- Remote Filtering Service resides inside the network, and acts as a proxy to Websense Filtering Service.

Remote Filtering Client routes Internet requests to Remote Filtering Server, which forwards it to Filtering Service. The request is then evaluated to determine whether or not to permit the site.

By default, the remote filtering components monitor all HTTP, HTTPS, and FTP traffic and apply a user-based policy or the Default policy.

All communication between the client and server is authenticated and encrypted.

**Warning**

Remote Filtering Client **cannot** be installed on machines running Remote Filtering Server. That combination eventually causes filtering to fail.

## When to use Web Endpoint

In Websense Web Security Gateway Anywhere deployments, Websense Web Endpoint can be used to secure client machines filtered by the hybrid service.

Web Endpoint provides transparent authentication, enforces the use of hybrid filtering policies, and passes authentication details to the hybrid service. It is designed for

organizations that want to take advantage of in-the-cloud (security-as-a-service) Web filtering.

With Web Endpoint installed, Web traffic is routed via the hybrid proxies to control user access to Web content, according to the applicable filtering policies. Web Endpoint has 2 operation modes:

- **Web scanning and filtering.** The endpoint client redirects HTTP and HTTPS traffic to the hybrid service with an encrypted token that identifies the user, enabling the correct policy to be applied and reporting data to be correctly logged. No password or other security information is included.

  The endpoint client can be used with both full-tunnel and split-tunnel VPNs, ensuring that all Web traffic is scanned and filtered.
- **Proxy manipulation.** For supported browsers, the endpoint client manipulates proxy settings in real-time. For example, if the endpoint detects it is at a hotspot, but the user has not finished registration, it removes its proxy settings until the gateway has successfully opened.

You can enable Web Endpoint for some or all machines filtered by the hybrid service.

## When to use Data Endpoint

Data Endpoint is designed for organizations concerned about data loss originated at the endpoint, whether malicious or inadvertent. For example, if you want to prevent employees from taking sensitive data home on their laptops and printing it, posting to the Web, copy and pasting it, etc., you would benefit from this endpoint solution.

Websense Data Endpoint is a comprehensive, secure and easy-to-use endpoint data loss prevention (DLP) solution. It monitors real-time traffic and applies customized DLP policies over application and storage interfaces. You can also apply discovery policies to endpoints to determine what sensitive data they hold.

You can monitor user activity inside endpoint applications, such as the cut, copy, paste, print, and print screen operations. You can also monitor endpoint Web activities and know when users are copying data to external drives and endpoint devices.

## Endpoint solution system requirements

*System Requirements*, page 41, provides the operating system requirements for endpoint server and client components.

- Find Web security requirements under “Web Security and Web Security Gateway,” in the “Software deployments,” “Client OS,” and “Web endpoint” sections.
- Find data security requirements under “Data Security,” in the “Operating system” and “Data Endpoint hardware requirements” sections.

# Deploying Websense endpoints

## Applies to

- Data Security v7.6.3 and beyond
- Web Security v7.6.2 and beyond
- Web Security Gateway v7.6.2 and beyond
- Web Security Gateway Anywhere v7.6.2 and beyond

## In this topic



Endpoint software is configured and packaged before it is distributed to endpoint devices (client machines).

If you have both Web and data security solutions, packages are customized according to your needs and created using the Websense Endpoint Package Builder. The package builder can create 32- and 64-bit Windows packages for all 3 types of Websense endpoints, as well as Linux packages for Data Endpoint.

The package builder can be found in the directory where you install Websense Data Security: **C:\Program Files\Websense\Data Security\client\WebsenseEndpointPackageBuilder.exe** by default.

If you do not subscribe to Data Security, you do not need to use the package builder to deploy the Web filtering endpoints. Rather:

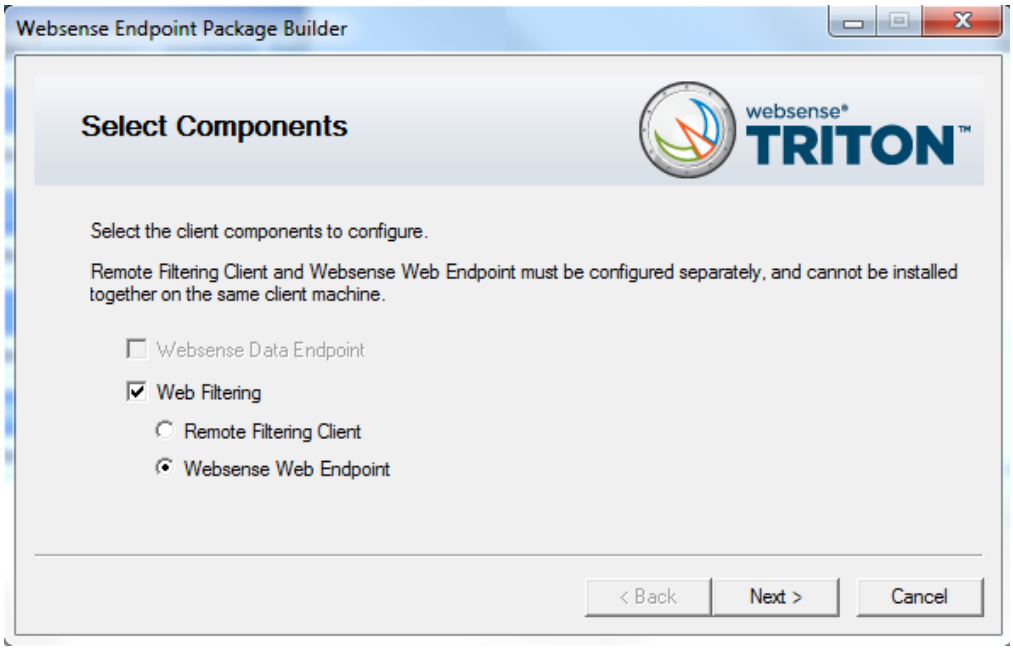
- You can download the Web Endpoint package by logging onto TRITON - Web Security and navigating to the **Settings > Hybrid Configuration > Hybrid User Identification** page.
- You can install the Remote Filtering Client Pack by running the TRITON Unified Installer and selecting the Custom installation option for Web Security.

## Creating installation packages

> **Note**
> If you have existing versions of Data Endpoint or Remote Filtering Client, uninstall them before deploying the new installation packages.

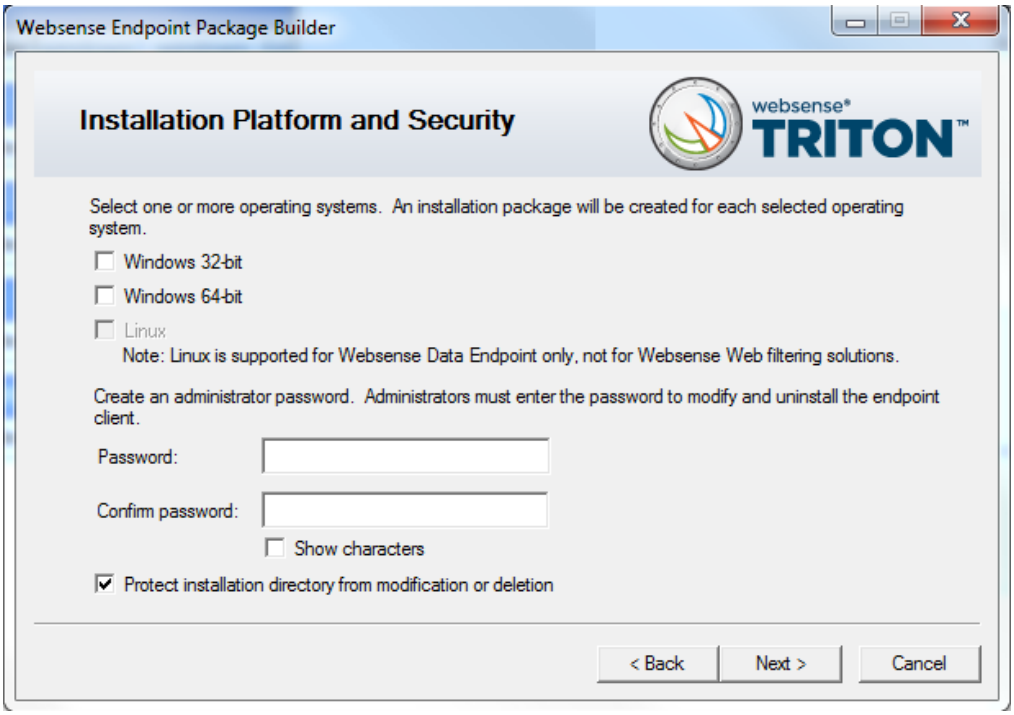
1. Go to **Start** > **Programs** > **Websense** > **Data Security** > **Endpoint Package Builder**.
2. Click **Next**, and then accept the terms of the subscription agreement.

3. The Select Components screen appears:




Select one or more endpoint solutions to install. You can create packages for both Websense Data Endpoint and one Web filtering solution, but cannot select both Web filtering solutions.

4. The Installation Platform and Security screen appears:



a. Select the operating systems used by the endpoint devices that you will be protecting:
   - Windows 32-bit
   - Windows 64-bit
   - Linux (applies to Data Endpoint only)

b. For security purposes, anyone who tries to modify or uninstall endpoint software is prompted for a password. Enter a password that administrators can use for this purpose.

   For Data Endpoint, once the endpoint client contacts the endpoint server, this password is overwritten with the password specified by a TRITON administrator. Administrators can set this password on the General tab under **Settings > General > System > Endpoint**.

   If no password is specified, every user is able to uninstall the endpoint software from their computer.

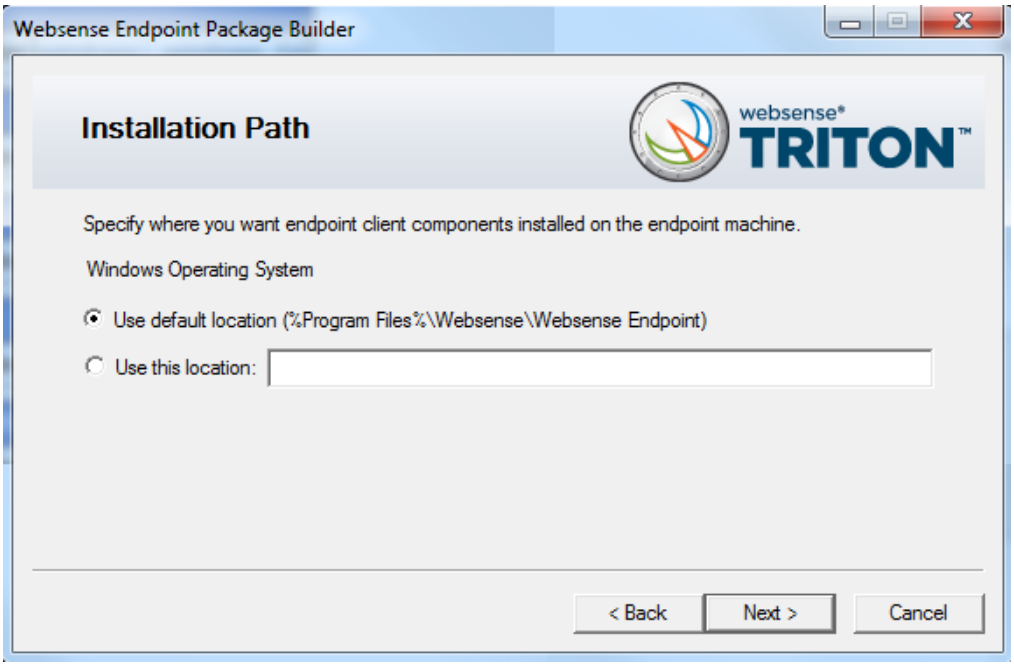
   Click **Show characters** to display the password characters while you type.

c. Sometimes when users cannot modify or uninstall the endpoint software, they try to delete the directory where the software is installed.

   Click **Protect installation directory from modification or deletion** if you do not want users to be able to perform these functions.

d. Click **Next** when you're done.

5. The Installation Path screen appears:



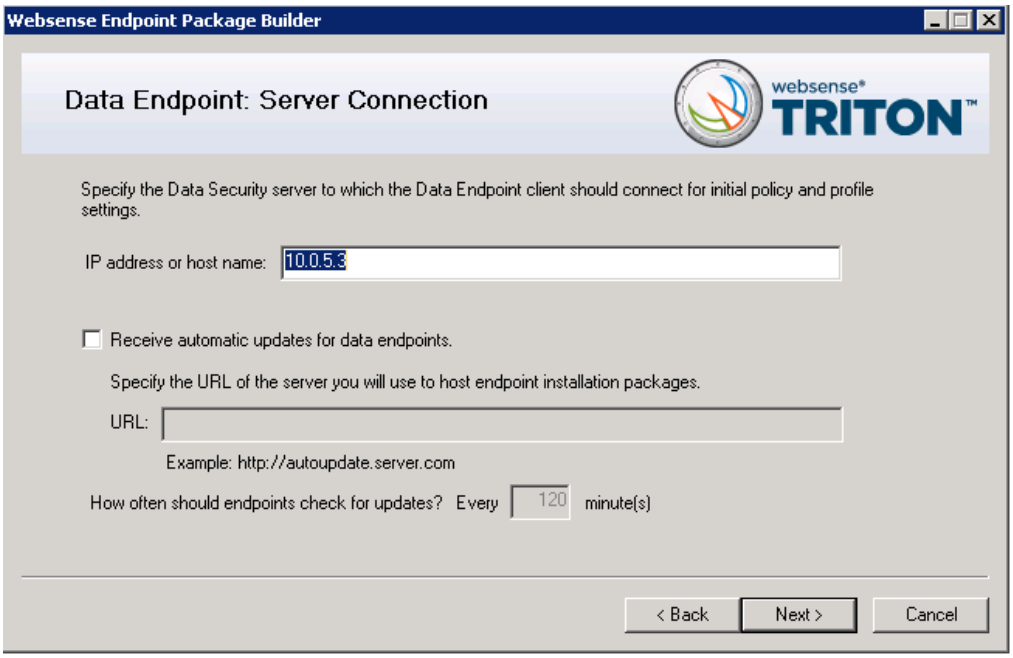

Specify the directory where you want endpoint software installed on each endpoint device. The endpoint software must be installed in a directory path that contains only English characters.

- **Use default location**: The endpoint software is installed in a default directory: \Program Files\Websense\Websense Endpoint (*Windows*) or /opt/websense/LinuxEndpoint (*Linux*).
- **Use this location**: Manually specify the installation path for the endpoint software. Environment variables are supported.

6. Click **Next**. The screens that appear next depend on the endpoint clients you chose. See:
   - *Websense Data Endpoint*, page 747
   - *Websense Web Endpoint*, page 749
   - *Remote Filtering Client*, page 750

## Websense Data Endpoint

1. If you chose Websense Data Endpoint, the Server Connection screen appears:




**IP address or host name**: Provide the IP address or host name of the Data Security server that endpoint machines should use to retrieve initial profile and policy information. (Once configured, endpoints retrieve policy and profile updates from the endpoint server defined in their profiles.)

**Receive automatic updates for data endpoints**: When new versions of Data Endpoint are released, you may upgrade the software on each endpoint—this can be done via GPO or SMS—or you can configure automatic updates on this screen.

To automate endpoint software updates:

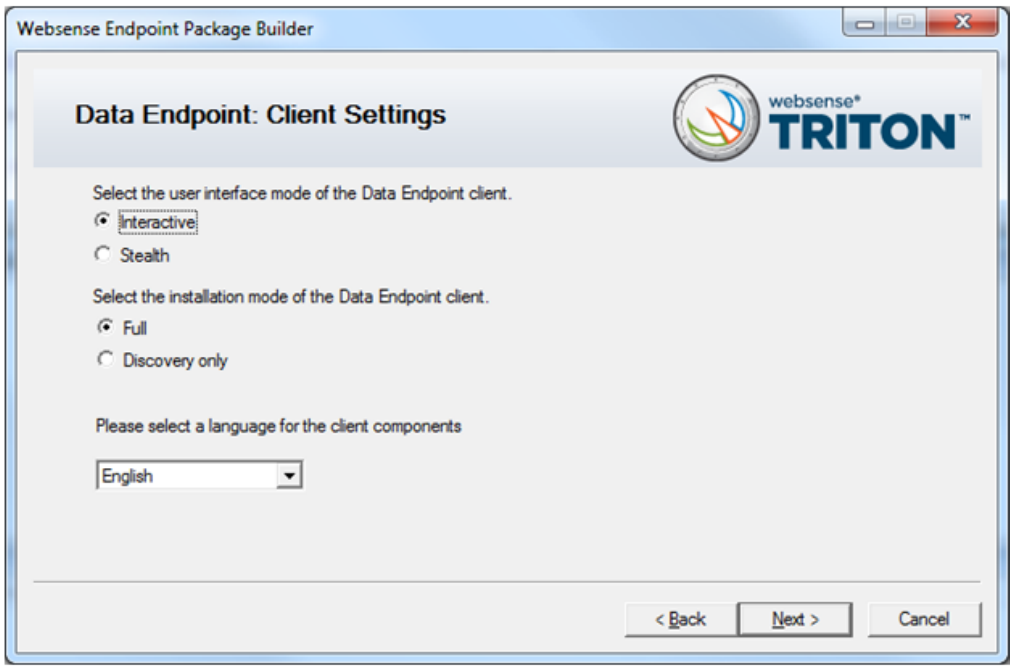
a. Prepare a server with the latest updates on it (see "Automatic Updates for Websense data endpoints" for details).

b. Select **Receive automatic updates for data endpoints**.

c. Specify the URL of the server you created. (It cannot be secure http (https).)

d. Indicate how often you want endpoint machines to check for updates.

2. Click **Next** and the Client Settings screen appears:




Complete the fields as follows:

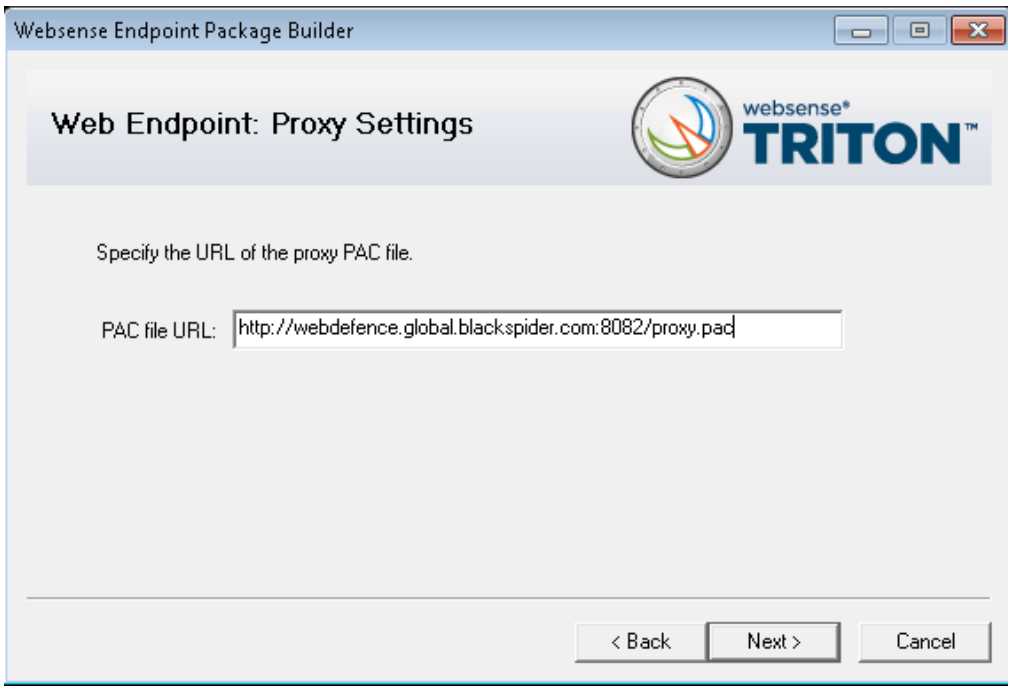
| | |
|---|---|
| User interface mode | Select from the following 2 options:<br>• **Interactive**: A user interface is displayed on all endpoint machines. Users know when files have been contained and have the option to save them to an authorized location.<br>• **Stealth**: The Websense Data Endpoint user interface is not displayed to the user.<br>Note that reinstallation is required to switch user interface modes. |
| Installation Mode | Applies to Windows only. Select from the following 2 options:<br>• **Full**: Installs the endpoint with full policy monitoring and blocking capabilities upon a policy breach. All incidents are reported in the TRITON Console.<br>Endpoints that are installed in Full Mode require a reboot.<br>• **Discovery Only**: Configures the endpoint to run discovery analysis but not DLP. Discovery Only installation does not require a reboot. |

| | |
|---|---|
| Installation Language | Select the default local language for the client user interface and the messages that are displayed to the user.<br>**Note:** The language used for displaying messages (English, Russian and German) can be changed via TRITON - Data Security, but the language displayed in the user interface (buttons, captions, fields, etc.) can only be set during packaging. |

3. Click **Next**. If you chose no other endpoints, skip to*Global settings*, page 754, for instructions. Otherwise, move to *Websense Web Endpoint*, page 749, or *Remote Filtering Client*, page 750.

## Websense Web Endpoint

1. If you chose Websense Web Endpoint, the Proxy Settings screen appears:

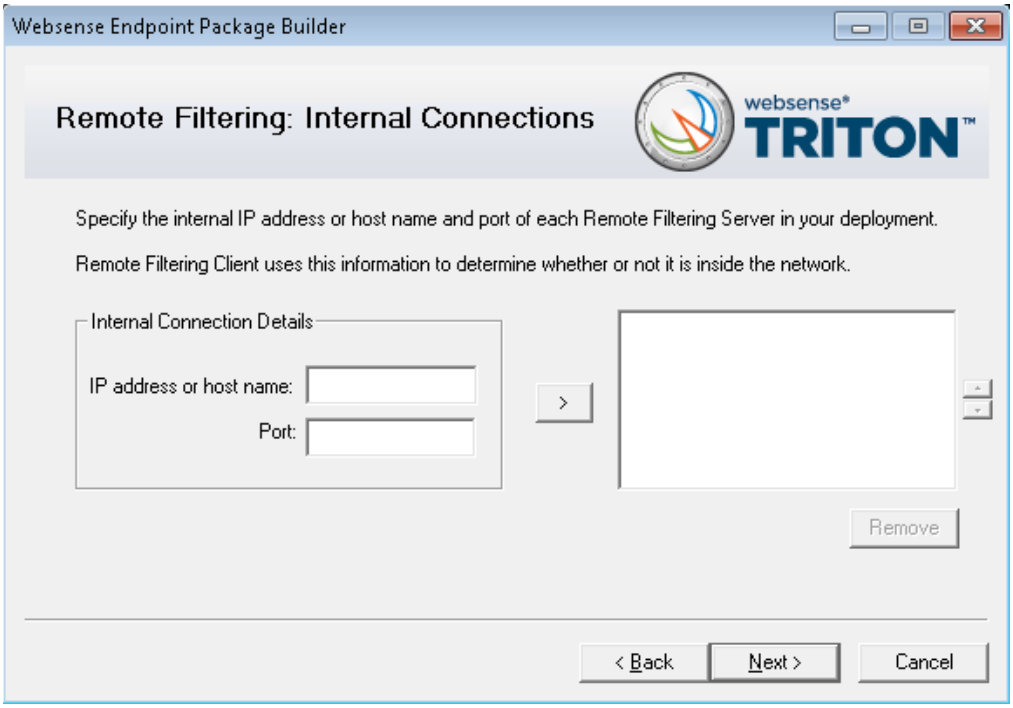



Specify the URL for the proxy PAC file. This file defines how Web browsers chooses an appropriate proxy for fetching a given URL. The standard proxy PAC file URL for hybrid filtering is:

2. http://hybrid-web.global.blackspider.com:8082/proxy.pacClick **Next**, and the Save Installation Package screen appears. See *Global settings*, page 754 for instructions on configuring this screen.

## Remote Filtering Client

1. If you chose Remote Filtering Client, the Internal Connections screen appears:



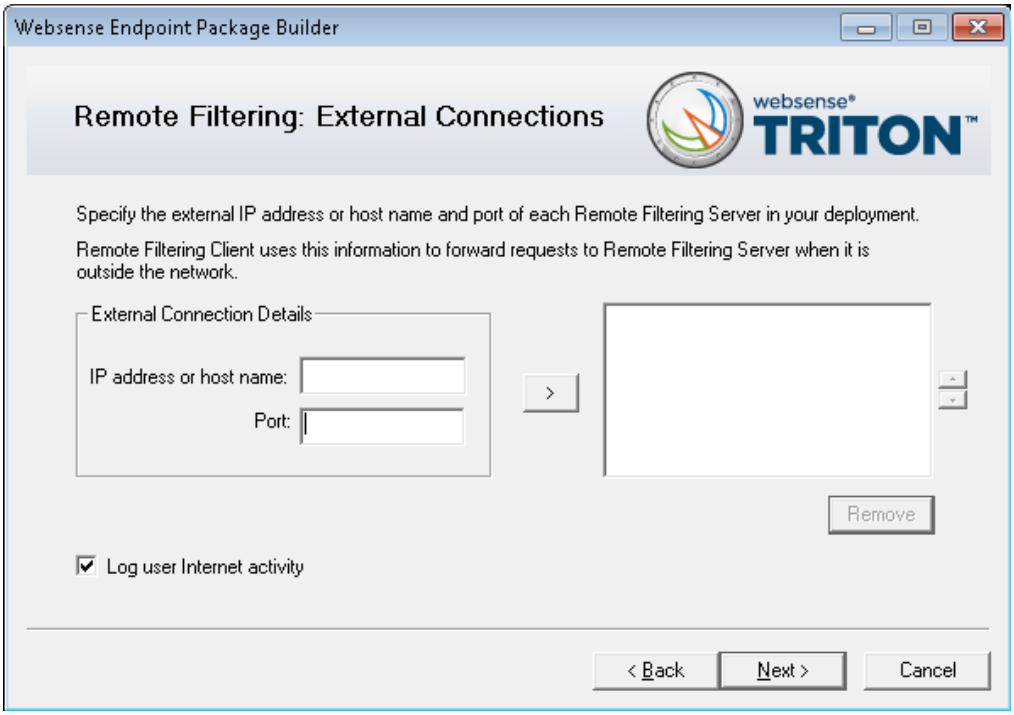

Enter connection information for the Remote Filtering Server to which this client should attempt to connect first.

**IP address or host name**: Internal IP address or FQDN for the primary Remote Filtering Server machine.

**Port**: Internal communication port on the primary Remote Filtering Server that can be accessed only from inside the network firewall. This must be the same port entered in the Internal Communication Port field when this Remote Filtering Server was installed.

> **Note**
> If Remote Filtering Client is on a laptop that is used both inside and outside the network firewall, this allows Websense software to determine where the machine is located and filters it appropriately.

2. Click **Next** and the External Connections screen appears:

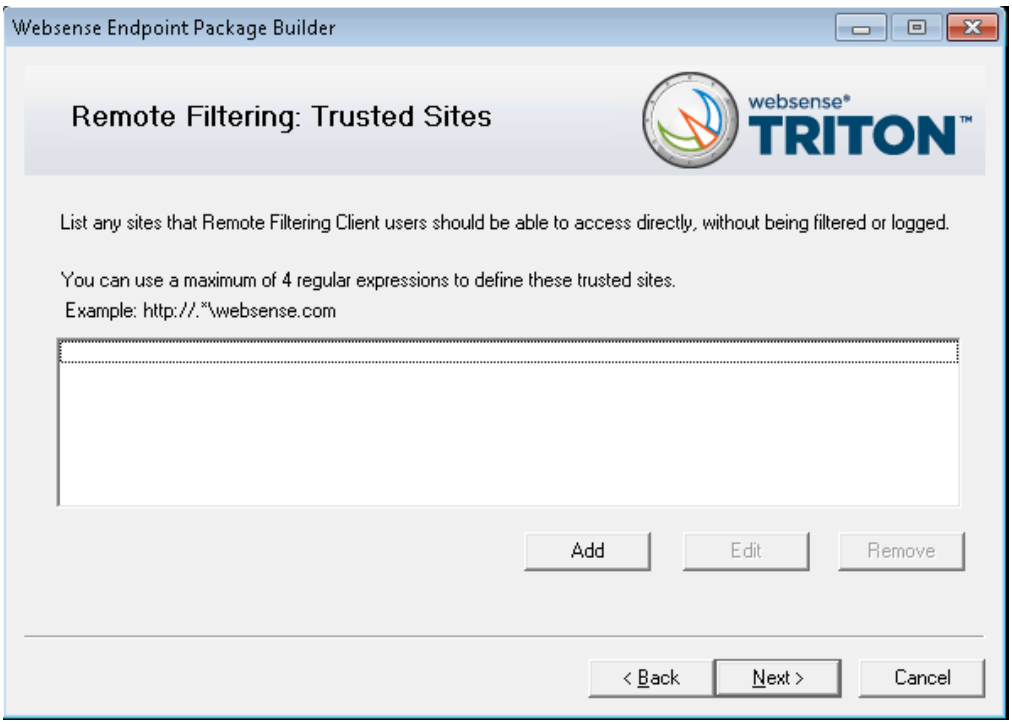



**IP address or host name**: Externally visible IP address or fully qualified domain name (FQDN) of the primary Remote Filtering Server machine.

> **Important**
> You must use the same address format (either IP address or FQDN) as when you installed this Remote Filtering Server.

**Port**: Externally accessible port used to communicate with the primary Remote Filtering Server. This must match the external port number entered when installing the primary Remote Filtering Server.

3. Click **Next** and the Trusted Sites screen appears:




On this screen, you can specify URLs or domains that should not be filtered.

a. Click **Add**.

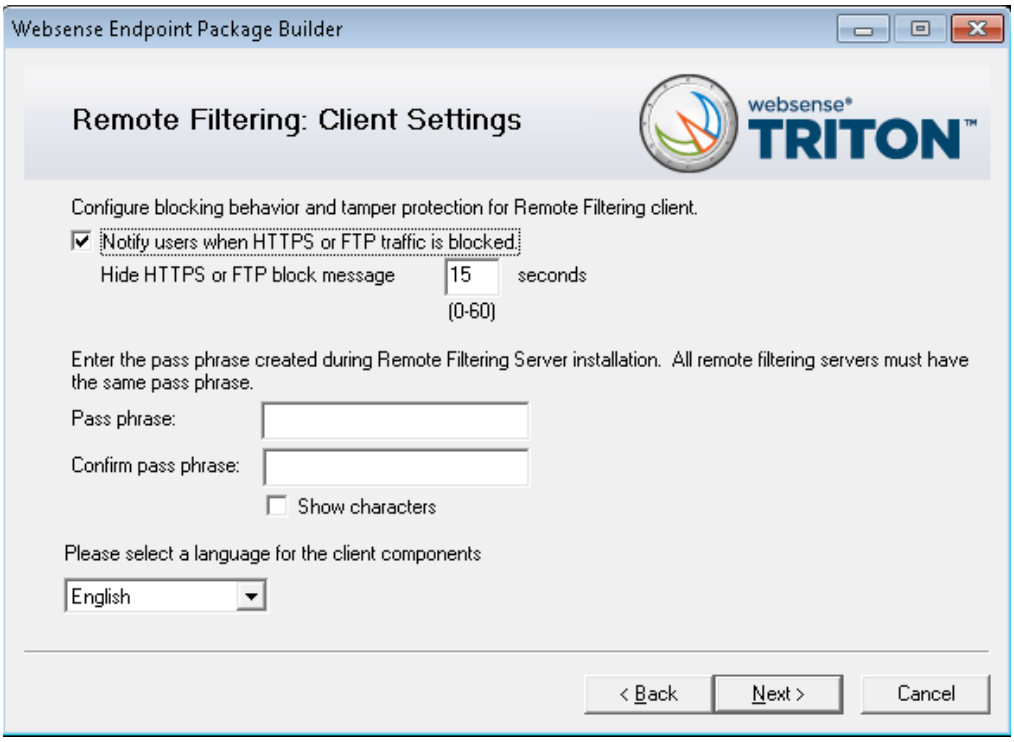
b. In the dialog box that appears, enter a URL or a regular expression specifying a set of URLs. Any regular expression adhering to ISO/IEC TR 19768 (within the character-number limit) is valid.

c. Click **OK**.

To edit a URL or regular expression, select it and then click **Edit**.

To remove a URL or regular expression, select it and then click **Remove**.

4. Click **Next** and the Client Settings screen appears:



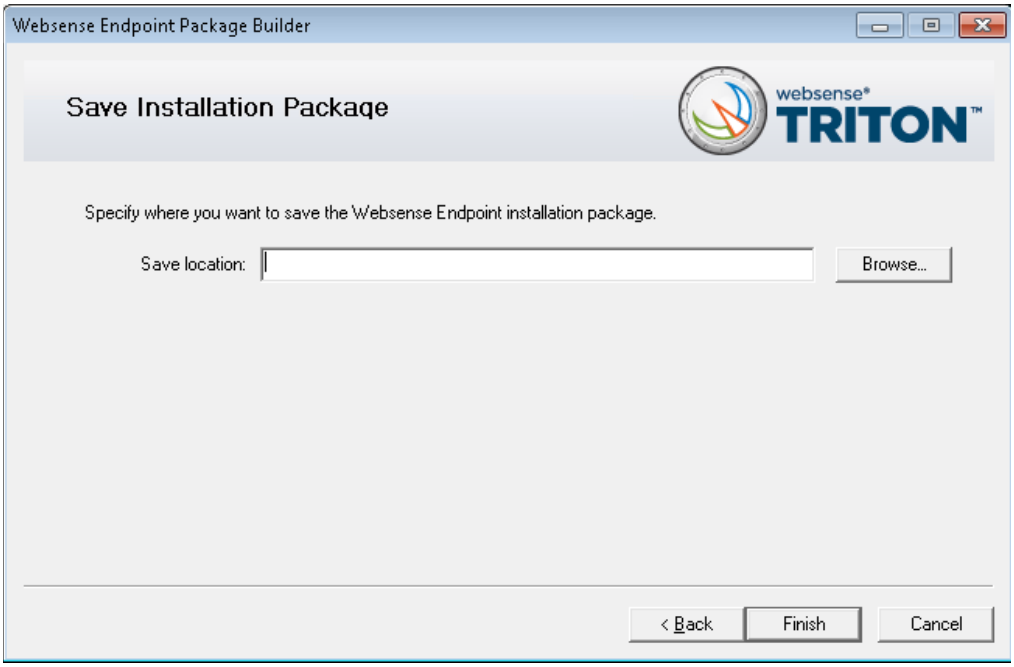

Complete the fields as follows:

| | |
|---|---|
| Notify users when HTTPS or FTP traffic is blocked | For HTTP traffic, custom block pages are shown inside users' browser windows when traffic is blocked.<br>Select this option if you want users to receive a pop-up message for blocked HTTPS or FTP traffic. If you enable this option, specify the time the pop-up message should remain visible to the user. |
| Pass phrase | Enter and confirm your pass phrase.<br>The pass phrase you enter must be the same one used when you installed the Remote Filtering Server. This pass phrase is used to connect the Remote Filtering Client with the server. |
| Language | Select the default local language for the client user interface and the messages that are displayed to the user. |

5. Click **Next**, and the Save Installation Package screen appears. See *Global settings*, page 754 for instructions on configuring this screen.

### Global settings

1. When you're done configuring your endpoint selections, the Save Installation Package screen appears:




   In the Save location field, provide the directory path where you want the endpoint packages to be stored before they are deployed to client machines. Either manually enter a path or click **Browse** to find the location.

2. Click **Finish**.

   You'll see a system message if the package is created successfully. If the creation of the package fails, you'll see an error message. If this happens, contact Websense Technical Support for assistance.

3. Click **OK**.

   Once the packaging tool has finished, the packages are created in the designated path. Refer to *Deployment options*, page 754, for instructions on distributing the package to the endpoint devices.

## Deployment options

There are 3 ways to distribute the endpoint software:

- *Manually on each endpoint machine*
- *Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS)*
- *Automatically*

> **Important**
> At the completion of any deployment, you must restart the endpoint to complete the installation.

1. *Manually on each endpoint machine*. Windows packages contain a single executable file: **WebesenseEndpoint_32bit.exe** or **WebesenseEndpoint_64bit.exe**. This file is a self-extracting archive.

   Linux packages (Data Endpoint only) contain 2 installers with the same functionality:

   - **LinuxEndpoint_SFX_installer_el4** - should be used with Red Hat Enterprise Linux version 4.x.
   - **LinuxEndpoint_SFX_installer_el5** - should be used with Red Hat Enterprise Linux version 5.x.

     To install Data Endpoint software on a Linux computer, copy the correct installer to the machine and run it as root. No reboot is necessary. The endpoint software starts automatically.

2. *Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS)* for Windows environments that use these Microsoft tools to manage the computers in their networks. See "Creating and distributing Websense endpoints using SCCM or SMS" for details.

3. *Automatically* (applies to updates only).

   For information on deploying Web Endpoint updates automatically, see *Enabling automatic updates for Web Endpoint*, page 756.

   To deploy Data Endpoint updates automatically, you must create an update server that hosts endpoint installation packages. See "Automatic Updates for Websense data endpoints" for details.

   You must also select **Receive automatic updates for data endpoints** on the Websense Endpoint Package Builder "Server Connections" screen. On this same screen, specify the URL of the server you created and indicate how often you want endpoint machines to check for updates (every 2 hours by default).

   When configured properly, your update server pushes software updates out to endpoint machines and installs the packages in the background silently.

> **Note**
> If you want to change the components installed on a data endpoint with components of the same version (for example, switch from a data and web endpoint combination to a data only endpoint), you must use the package builder to generate a new package and use one of the other deployment options to deploy it. You cannot use the auto-update feature to update endpoints with the same version.

You can confirm that the Web Endpoint or Data Endpoint is installed and running on a machine as follows:

- For Web Endpoint, go to **Start > Control Panel > Administrative Tools > Services**. Check that **Websense SaaS Service** is present in the Services list, and is started.
- When the Data Endpoint is installed in interactive mode, an icon ) appears on the endpoint machine's task bar. Click the icon for status information. (No icon shows in stealth mode.)

For information on endpoint software system requirements, see *Endpoint solution system requirements*, page 743.

If you plan to deploy multiple endpoint solutions (data and Web) on the same machine, see *Multiple agent limitations*, page 758, before proceeding.

## Enabling automatic updates for Web Endpoint

Once you have deployed your endpoint package to end users, Web Endpoint can be updated for some or all of your hybrid filtering users directly from the hybrid service. If you use the Data Endpoint auto-update feature for endpoints with both data and Web capabilities, however, endpoints receive updates from your auto-update server instead.

To enable automatic Web Endpoint updates to client machines:

1. Go to the **Settings > Hybrid Configuration > Hybrid User Identification** page in TRITON - Web Security.
2. Mark **Enable installation and update of Web Endpoint on client machines**.

   This defines whether automatic updates are deployed to the client machines that you specify. If you uncheck this option at a later date, no further automatic updates occur. However, the installed endpoint software continues to run until it is uninstalled from the client machines.
3. Mark **Automatically update endpoint installations when a new version is released**.
4. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

> **Note**
> At the completion of an endpoint update, you must restart the endpoint for the updates to take effect.

Note that while a Web Endpoint update is taking place (which can take several minutes), end users are unable to browse, but are shown a Web page explaining that the update is occurring. This page continues to retry the requested Web page every 10 seconds until the endpoint software has finished updating. The request is then submitted, and either the page or a block page is displayed.

# Uninstalling endpoint software

## Applies to

- Data Security v7.6.3 and beyond
- Web Security v7.6.2 and beyond
- Web Security Gateway v7.6.2 and beyond
- Web Security Gateway Anywhere v7.6.2 and beyond

## In this topic



You can uninstall endpoint software 2 ways:

- Locally on each endpoint agent via **Control Panel** > **Add/Remove Programs** (Windows) or the **ep-uninstall** script (Linux). Add/Remove Programs launches **uninstall.exe** in the endpoint installation folder.

  **Note**
  If you configured an administrative password, you must supply it to uninstall the software.

- Remotely through a deployment server (SMS).

  **Note**
  In this mode, if you configured an administrative password, you must deploy the following command. (Type it on a single line with no returns.)

  Web or Data Endpoint:

  ```
  msiexec /x {product_code} XPSWD=password /qn
  ```

  Remote Filtering Client:

  ```
  msiexec /x {product_code} XPSWDRF=password /qn
  ```

  In these examples, *product_code* is a unique identifier (GUID) that can be found in the **setup.ini** file of each installation package, and *password* is the administrator password that you entered when creating the installation package.

## Local uninstall

### Windows

1. Go to **Start > Control Panel > Add/Remove Programs**.
2. The Add/Remove Programs screen is displayed.
3. Scroll down the list of installed programs, select **Websense Endpoint** and click **Remove**.
4. Click **Yes** in the confirmation message asking if you sure you want to delete the Websense Endpoint.
5. You may be prompted to provide an administrative password, if you defined one. If so, enter the password in the field provided and click **OK**.
6. You'll see a system message indicating you must restart your system. Click **Yes** to restart or **No** to restart your system later. Once the computer has been restarted, the configuration changes apply.

### Linux (Data Endpoint only)

Run the **ep-uninstall** script (located by default at /opt/websense/LinuxEndpoint/ep-uninstall). You may be prompted for an administrative password, if one was defined by your system administrator.

## Remote uninstall

You can uninstall endpoint software remotely by using distribution systems. If you used an SMS distribution system to create packages for installation, those packages can be reused, with a slight modification, for uninstalling the software. If a package was not created for deployment of the endpoint software, a new one needs to be created for uninstalling.

To uninstall with package:

1. Follow the procedure for Creating and distributing Websense endpoints using SCCM or SMS.
2. In step 1, select **Per-system uninstall**.
3. Complete the remaining procedures.
4. After deploying the package, the Websense Endpoint will be uninstalled from the defined list of computers.

# Multiple agent limitations

## Applies to

- Data Security v7.6.3 and beyond

- Web Security v7.6.2 and beyond
- Web Security Gateway v7.6.2 and beyond
- Web Security Gateway Anywhere v7.6.2 and beyond

## In this topic



Some Websense endpoint clients can run together on the same machine. For example, Data Endpoint can be installed with Web Endpoint or Remote Filtering Client.

Endpoint software can also be installed with third-party agents, such as an antivirus agent.

There are limitations in all multi-agent deployments to be aware of.

## Multiple Websense endpoints

With the Websense Endpoint Package Builder, you can create packages for multiple agents (Web and data) and, depending on the agent, multiple operating systems (Windows and Linux). You can deploy these packages to the same or different endpoint (client) machines.

For example, you can deploy Web Endpoint and Data Endpoint on the same Windows machine; or you can deploy Remote Filtering Client and Data Endpoint on the same machine.

You cannot deploy Web Endpoint and Remote Filtering Client on the same machine. The package builder does not let you create packages for both. Likewise, you cannot deploy multiple agents on Linux machines. Only Data Endpoint supports Linux.

Here are some other restrictions to consider:

- If you are deploying Web and data endpoints on the same machine, you must deploy them at the same time.
- If you are deploying Web and data endpoints on the same machine, the Web Endpoint must be v7.6.2 or later and the Data Endpoint must be v7.6.3 or later. If you generate both endpoints using the Websense Endpoint Package Builder, you do not need to worry about version mismatch.
- Starting with v7.6.3, the packages created by the Websense Endpoint Package Builder are backwards compatible with previous endpoint versions.
- If you are using the v7.6.3 unified endpoint package builder to generate Remote Filtering Client installation packages, v7.6.2 Remote Filtering Clients are created. The package builder creates only the installation file, however, and does not include the configuration tool used to edit the Remote Filtering Client settings.

  To update configuration settings for a v7.6.2 Remote Filtering Client created using the v7.6.3 unified endpoint package builder, log on to MyWebsense, and click **Downloads**. Next, select **Websense Data Security Suite** as the product and

**7.6.3** as the version. The Websense Remote Filtering Client Configuration Tool appears as a download option.

To use the configuration tool:

1. Download the ZIP file.
2. Extract the 2 self-extracting executables from the ZIP file. As the file names indicate, one is used to configure Windows 32-bit clients, and the other is used to configure Windows 64-bit clients.
3. Run the appropriate self-extracting executable on any Windows machine to unpack the Remote Filtering Client configuration tool.
4. Go to http://www.websense.com/content/support/library/web/v76/remote_filtering/rfcl_config_util.aspx, and follow the instructions provided under "Configure an installation profile" to change your Remote Filtering Client configuration.

## Third-party agents

By default, Windows XP and Windows Server 2003 limit the number of concurrent agents in a system. As a result, a fatal (BSOD) error may occur when users try to access files via DFS (Distributed File System) and Websense endpoint software is installed with more than 2 other agents.

To overcome this limitation, update client operating systems to Windows XP SP3 or Windows Server 2003 SP2 and follow the procedures below.

For further details, please refer to: http://support.microsoft.com/kb/906866.

On all relevant endpoint (client) machines:

1. Make a backup copy of your Windows registry before you continue. See support.microsoft.com for details.
2. Click **Start** > **Run** and type **regedit**, then click **OK**.
3. Locate and then click the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Mup\
   Parameters
   ```

4. In the right pane, right-click **DfsIrpStackSize**, then click **Modify**.

   **Note**

   If the DfsIrpStackSize registry entry does not exist, you must create it. To do this, follow steps:

   a. On the **Edit** menu, point to **New**, then click **DWORD Value**.

   b. Type **DfsIrpStackSize**, then press **ENTER**.

5. In the Base box, click **Decimal**, then type **10** in the Value data box and click **OK**.
6. Exit the Registry Editor.

7. Restart the computer.

# Configuring endpoint software

## Applies to

- Data Security v7.6.3 and beyond
- Web Security v7.6.2 and beyond

Data Endpoint is configured in the TRITON console. For information, see:

- Configuring Endpoint Deployment

If you are deploying Remote Filtering Client or Web Endpoint using the package builder and GPO or SMS, there are no client settings to configure in the TRITON console.

# 47 Initial Configuration

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Data Security v7.6
- Email Security Gateway v7.6

## In this topic

# Overview

This section of the Technical Library contains information about initial configuration tasks to perform after installation or issues to be aware of.

# Initial configuration (all deployments)

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6
- Email Security Gateway v7.6
- Data Security v7.6

## In this topic

- *Entering subscription key*, page 766
- *SMTP server configuration*, page 766
- *SQL Server 2008 R2 Express*, page 766

## Ports

Websense software components use certain ports by default to communicate with each other and the Internet. After installation, be sure to configure any firewall protecting the machine to allow communication on the ports used by the components you have installed. See *Default ports*, page 927.

## Antivirus configuration

To avoid interference with the performance of Websense components, exclude certain Websense folders and files from antivirus scans. See *Excluding Websense Files from Antivirus Scans*, page 939.

## Disable Enhanced Security Configuration in Internet Explorer

When using Internet Explorer, disable Enhanced Security Configuration to view all features in the TRITON Unified Security Center.

### Windows Server 2008

1. Open the Server Manager.
2. Under **Server Summary**, in the Security Information section, click**Configure IE ESC**.
3. In the **Internet Explorer Enhanced Security Configuration** dialog box, under **Administrators**, select the **Off** radio button, and then click **OK**.

### Windows Server 2003

1. Open Windows Add or Remove Programs.
2. In Windows Add or Remove Programs, select **Add/Remove Windows Components** (in left pane).
3. In the Windows Components Wizard, select **Internet Explorer Enhanced Security Configuration**.
4. Click **Next**.
5. Click **Finish**.

## Accessing the TRITON Unified Security Center

Using a supported browser (see *System Requirements*, page 41), go to https://<IP address>:9443/triton. Where <IP address> is the IP address of the machine on which TRITON Unified Security Center is installed. If using the TRITON Unified Security

Center installed on a Websense appliance (Web Security Gateway only) then use the IP address of the appliance's C interface.

Use the default *admin* account (password set during installation) to log on for the first time.

## Entering subscription key

Enter your subscription key(s) as described below.

### Web Security

At initial startup TRITON - Web Security prompts for a subscription key. The key you enter will automatically be applied to Content Gateway as well. See the TRITON - Web Security Help for more information.

### Data Security

At initial startup TRITON - Data Security starts at the subscription key page. See the *Initial Setup* section of the TRITON - Data Security Help for more information.

### Email Security

In TRITON - Email Security, enter the subscription key on the **Settings > General > Subscription** page. See the TRITON - Email Security Help for more information.

## SMTP server configuration

It is recommended you specify an SMTP server to be used for system alert and password reset email. See the TRITON Unified Security Help for more information.

## SQL Server 2008 R2 Express

If you installed SQL Server 2008 R2 Express, verify that SQL Server Browser service is running and TCP/IP is enabled.

1. Launch SQL Server Configuration Manager (**Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **Configuration Tools** > **SQL Server Configuration Manager**).
2. In the tree pane, select **SQL Server Service**.
3. In the properties pane, make sure SQL Server Browser is running and start mode is automatic.

   Right-click to start the service or change its start mode.
4. In the tree pane, select **SQL Server Network Configuration** > **Protocols for <*instance name*>**, where <*instance name*> is the default instance or TRITONSQL2K8R2X (or other instance name you specified).
5. In the properties pane, make sure TCP/IP is enabled.

If not, right-click TCP/IP and enable it.

# Web Security initial configuration

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Getting Started Help

See the *Getting Started* section of the TRITON - Web Security Help for an overview and initial configuration information.

Also see the New User Quick Start Tutorial (which is offered the first time you log into TRITON - Web Security) for information about basic configuration.

## Windows Server 2008

If you install certain components on Windows Server 2008, or if your network uses Active Directory 2008 to authenticate users, be aware of the issues listed below. In some cases, additional configuration steps are required.

- If you run Websense User Service on Windows Server 2008, and your network uses a Windows NT Directory or Active Directory (Mixed Mode), Websense User Service must run as an account that has administrative privileges on the directory.

This means that the User Service machine must be joined to the domain before performing the installation.

See the Troubleshooting section of the TRITON - Web Security Help for instructions on checking and changing the User Service account. Look for the topic on changing DC Agent, Logon Agent, and User Service permissions.

- If you run Websense User Service, DC Agent, or Logon Agent on Windows Server 2008, the Windows Computer Browser service on that machine must be running.
- If Websense User Service is installed on Windows Server 2008, protocol block messages and popup usage alerts cannot be displayed at client machines.
- If your network uses Active Directory 2008 to authenticate users, the Windows Computer Browser service on that machine must be running.
- If you run Websense User Service on Windows Server 2008, Network Agent cannot send protocol block messages to users. The protocol requests are blocked, but no message is displayed.

  In addition, usage alert popup messages cannot be displayed to users. The alerts are generated, and other notification methods function normally.
- All Websense tools and utilities installed on Windows Server 2008, and text editors used to modify Websense configuration files (such as websense.ini),**must** be run as the local administrator. Otherwise, you may be prevented from running the tool or the changes you make may not be implemented.

  1. Open Windows Explorer to the bin subdirectory in the Websense installation directory (the default installation directory is C:\Program Files or Program Files (x86)\Websense\Web Security).
  2. Right-click the relevant executable file, and then click **Properties**. Following is a list of files for which this should be done.
     - **wsbackup.exe** for Websense Backup and Restore
     - **logserverconfig.exe** for the Log Server Configuration utility
     - executable for any text editor used to modify a Websense configuration file (such as websense.ini)
  3. In the **Compatibility** tab, under **Privilege Level**, select **Run this program as an administrator**. Then, click **OK**.

## Logon script for Logon Agent

If you installed Websense Logon Agent, you must create a logon script for clients that identifies them to Websense software when they log on to a Windows domain. The Websense Logon application, **LogonApp.exe**, provides a user name and IP address to the Logon Agent each time a Windows client connects to a Windows Active Directory or a Windows NT directory service. See *Creating and running the script for Logon Agent*, page 782.

## Messenger Service for Network Agent block messages

All Windows computers being filtered must have the Messenger Service enabled to receive protocol block messages from Network Agent. See the *Protocol Block Messages* topic in TRITON - Web Security Help for instructions.

## Administrator privileges for User Service, DC Agent, or Logon Agent

If you were unable to grant User Service, DC Agent, or Logon Agent administrator privileges during installation, do so now to ensure that they will function correctly. For instructions, see the *Troubleshooting* > *User Identification* topic on changing User Service, DC Agent, and Logon Agent service permissions in TRITON - Web Security Help.

## Configuring Transparent Identification

If you installed DC Agent, eDirectory Agent, Logon Agent After installation, follow the instructions in User Identification topic of the TRITON - Web Security Help to configure Websense software to use DC Agent to identify users without prompting them for logon information.

## Testing Network Agent

If you installed Network Agent, use the Network Traffic Detector to test whether Network Agent can see the Internet activity that you want it to monitor. See the *Network Configuration* topic in TRITON - Web Security Help for instructions.

## Network Agent and multiple NICs

If you installed Network Agent on a machine with multiple NICs, you can configure the agent to use more than one NIC to monitor and block requests. See the *Network Configuration* topic in TRITON - Web Security Help for more information. To configure a stealth mode NIC for monitoring, see *Configuring a stealth mode NIC*, page 788.

## Remote Filtering

If you installed the optional Remote Filtering components, some configuration is required. For instructions, see the Remote Filtering Software technical paper.

## Identifying Filtering Service by IP address

When Websense software blocks an Internet request, the browser is redirected to a block page hosted by Filtering Service. The block page URL takes the form:

```
http://<FilteringServiceNameorIPAddress>:<MessagePort>/cgi-
bin/blockpage.cgi?ws-session=#########
```

If Filtering Service is installed on a machine with multiple NICs, and Filtering Service is identified by machine host name rather than IP address, users could receive a blank page rather than a block page.

- If you have an internal domain name server (DNS), enter the Filtering Service machine's IP address as a resource record in your DNS. See your DNS documentation for instructions.
- If you do not have an internal DNS:
  1. On the Filtering Service machine, go to the Websense bin directory (by default, **C:\Program Files\Websense\bin** or **opt/Websense/bin**).
  2. Make a backup copy of **eimserver.ini** in another directory.
  3. Open the original **eimserver.ini** file in a text editor.
  4. In the **[WebsenseServer]** section, enter the following command:

     ```
     BlockMsgServerName=<IP address>
     ```

     Here, <**IP address**> is the IP address of the Filtering Service machine.

     **Important**

     **Do not** use the loopback address 127.0.0.1.

  5. Save the file.
  6. Restart the Filtering Service. See *Starting or Stopping Web Security Services*, page 923.

# Web Security Gateway Anywhere initial configuration

## Applies to

- Web Security Gateway Anywhere v7.6

## In this topic

## Overview

In addition to the items under *Web Security initial configuration*, page 767, perform these procedures if your subscription includes Web Security Gateway Anywhere.

## Registering Websense Content Gateway with Data Security

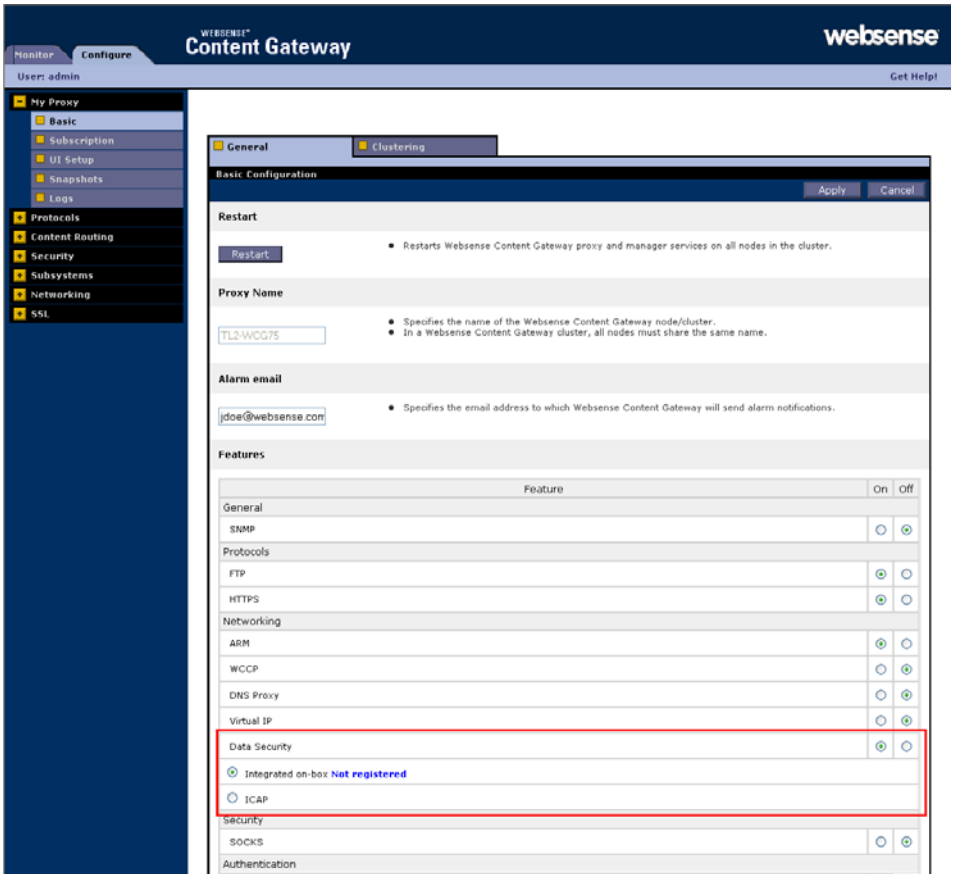
1. Ensure that the Content Gateway and Data Security Management Server systems are running and accessible, and that their system clocks are synchronized.
2. Ensure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Host name alone is not sufficient.
3. If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface ("C" on a V-Series appliance) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.
4. Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a V-Series appliance). This is the NIC used by the Data Security Management Server during the registration process.

   After registration, the IP address can move to another network interface.
5. Open Content Gateway Manager: in *TRITON - Web Security*, on the **Settings** tab, select **General** > **Content Gateway Access**. Then click the IP address of the Content Gateway machine.

   Alternatively, using a supported Web browser, go to: https://<wcg_IP_or_hostname>:8081

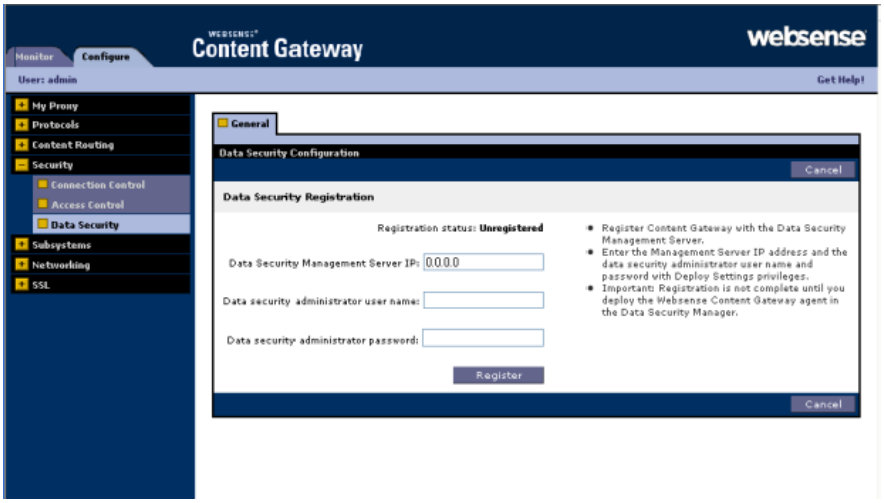
   where <wcg_IP_or_hostname> is the IP address or hostname of the machine on which Content Gateway is running. If Content Gateway is running on an appliance, use the IP address of the appliance's C interface.
6. Select **Configure > My Proxy > Basic > General**.
7. On the General tab, under **Networking**, enable **Data Security** (by selecting the **On** radio button to the right).

8. Select **Integrated on-box** and then click the **Apply** button (either at the top or bottom of the screen).




A registration status link, **Not registered**, displays.

9. Click the **Not registered** link. This opens the **Configure > Security > Data Security** registration screen.




10. Enter the IP address of the **Data Security Management Server**.

11. Enter a user name and password for a Data Security administrator with Deploy Settings privileges.
12. Click **Register**. You are reminded to synchronize the system time between the proxy machine and the Data Security Management Server.
13. If registration succeeds, a Data Security Configuration page displays. Set the following configuration options.
    a. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Data Security for analysis and policy enforcement.
    b. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement.

    These options can be accessed whenever Data Security is registered by going to the **Configure** > **Security** > **Data Security** > **General** page.
14. Click **Apply**.
15. Restart Content Gateway.

Data Security and the proxy communicate over ports 4636, 4575, and 4622.

## Configuring the Content Gateway policy engine

When you register the Websense Content Gateway policy engine with the Data Security Management Server, a Content Gateway module appears in the TRITON - Data Security System Modules screen.

By default, this agent is configured to monitor Web traffic, not block it, and for a default violation message to appear when an incident is triggered. If this is acceptable, you do not need to make changes to the Content Gateway configuration. Simply deploy the new settings.

If you want to block Web traffic that breaches policy and customize the violation message, do the following:

1. From the TRITON - Data Security user interface, select **Settings** > **Deployment** > **System Modules**.
2. Select the Content Gateway module in the tree view (click the module name itself, not the plus sign next to it).

   It will be listed as **Content Gateway on** <*FQDN*> **(**<*PE_version*>**)**, where <*FQDN*> is the fully-qualified domain name of the Content Gateway machine and <*PE_version*> is the version of the Content Gateway policy engine.
3. Select the **HTTP/HTTPS** tab and configure the blocking behavior you want.

   Select **Help** > **Explain This Page** for instructions for each option.
4. Select the **FTP** tab and configure the blocking behavior you want.

   Select **Help** > **Explain This Page** for instructions for each option.
5. Click **Save** to save your changes.
6. Click **Deploy** to deploy your settings.

**Important**
Even if you do not change the default configuration, you must click **Deploy** to finalize your Content Gateway deployment process.

## Verifying Web and data security linking

When *Linking Service* is installed, it automatically configures linking between Web and Data Security to allow Data Security access to user identification and URL categorization data.

1. Log into the *TRITON Unified Security Center*.
2. In *TRITON - Data Security*, select **Settings** (under General) > **System** > **URL Categories & User Names**.
3. Verify settings and test the connection.

   Select **Help** > **Explain This Page** for detailed information about the settings on this screen.
4. Click **OK** to save any changes.
5. Click **Deploy** to deploy your settings.

## Configure filtering for remote offices and off-site users

See the "Identification of hybrid filtering users" topic in the TRITON - Web Security Help.

# Data Security initial configuration

**Note**
TRITON - Data Security may not be available immediately after installation. It takes a few minutes to initialize the system after it is first installed.

## Applies to

- Data Security v7.6

## In this topic

- *General Setup*, page 777

# SMTP Agent

If you installed this agent, you must deploy the it in the TRITON - Data Security. The easiest way to test your installation is using Outlook Express installed on the same machine as the SMTP agent.

See “Configuring the SMTP agent” in the TRITON - Data Security Help system.

Before cutting over the live mail flow, be sure to test relaying through all mail servers as described in *Testing*, page 775.

For information on configuring the SMTP agent for your existing email infrastructure, see *Using the SMTP agent*, page 520. For more information on configuring this agent, see “Configuring the SMTP agent” in the TRITON - Data Security Help system.

## Testing

1. Test relay access from the mail server to the Data Security MTA:

   Send a test message from the central mail server to the SMTP agent MTA through telnet:

   From the mail server, open a command line and execute the following commands:

   ```
   telnet [DSS MTA ip/hostname] 25
   HELO me
   MAIL FROM:[email_address@local.domain]
   RCPT TO:[your_address@websense.com]
   DATA
   Subject: testing DSS MTA
   .
   quit
   ```

   Once you type the period and press enter you should get a "250 Ok:" message from the Data Security MTA. If you get any message other than 250 OK do a Google search for that SMTP message.

   If you get a 250 OK, but do not receive your message in your corp address, continue to step 2.

2. Test relay access from Data Security MTA Inbound to Outbound:

   Send a test message from the SMTP agent server to its own Inbound SMTP Virtual Server through telnet:

   From the SMTP agent server, open a command line and execute the following commands:

   ```
   telnet localhost 25
   HELO me
   MAIL FROM:[email_address@local.domain]
   RCPT TO:[your_address@websense.com]
   DATA
   Subject: testing DSS MTA
   .
   quit
   ```

Once you type the period and press enter you should get a "250 Ok:" message from the SMTP Virtual Server. If you get any message other than 250 OK do a Google search for that SMTP message. If you get a 250 OK, but do not receive your message in your corp address, check the Badmail/Queue directories for the inbound SMTP Virtual Server (C:\Inetpub\mailroot by default). If the folders are empty, continue to step 3.

3. Test relay access from Data Security MTA to its own Outbound server:

   Send a test message from the SMTP Agent server to its own Outbound SMTP Virtual Server through telnet:

   From the SMTP agent server, open a command line and execute the following commands:

   ```
   telnet localhost 10025
   HELO me
   MAIL FROM:[email_address@local.domain]
   RCPT TO:[your_address@websense.com]
   DATA
   Subject: testing DSS MTA
   .
   quit
   ```

   Once you type the period and press enter you should get a "250 Ok:" message from the SMTP Virtual Server. If you get any message other than 250 OK do a Google search for that SMTP message. If you get a 250 OK, but do not receive your message in your corp address, check the Badmail/Queue directories for the Outbound SMTP Virtual Server (C:\Inetpub\outbound by default). If the folders are empty, continue to step four.

4. Test relay access from Data Security MTA to the next hop MTA:

   Send a test message from the SMTP Agent server to the next hop MTA through telnet:

   From the SMTP agent server, open a command line and execute the following commands:

   ```
   telnet [next hop MTA/smarthost IP/hostname] 25
   HELO me
   MAIL FROM:[email_address@local.domain]
   RCPT TO:[your_address@websense.com]
   DATA
   Subject: testing DSS MTA
   .
   quit
   ```

   Once you type the period and press enter you should get a "250 Ok:" message from the next hop MTA. If you get any message other than 250 OK do a Google search for that SMTP message. If you get a 250 OK, but do not receive your message in your corp address, then there is some issue beyond the DSS MTA mail flow (i.e. delivery from next hop MTA to destination domain mail servers).

## ISA Agent

If you installed this agent, you must deploy the it in TRITON - Data Security. To ensure that the ISA agent is properly installed and enabled in ISA, navigate to Web Filters in the ISA Management Console.

See “Configuring the ISA agent” in the TRITON - Data Security Help system.

## Crawler Agent

If you installed this agent, you must deploy it in TRITON - Data Security. See “Configuring the crawler” in the TRITON - Data Security Help system.

## General Setup

See the *Initial Setup* section of the TRITON - Data Security Help for information on the following topics:

- Defining general system settings
  - Connection to directory services
  - System alerts
- Setting up notifications
  - Notifications when policy breaches occur
- Configuring Web attributes
  - Web DLP policies
  - Policies for particular Web sites
  - Policy owners
- Configuring outbound and inbound attributes
  - Email policies
- Creating a regulatory and compliance policy
- Configuring system modules
  - Viewing Data Security modules
  - Configuring the protector
- Deploying your settings

# Email Security Gateway initial configuration

## Applies to

- Email Security Gateway v7.6
- Email Security Gateway Anywhere v7.6

## Email Security Gateway initial configuration

The first time you access TRITON - Email Security, you are prompted for your subscription key. Then, you are asked if you want to use the First-Time Configuration Wizard. This wizard guides you through the process of entering essential configuration settings. It is strongly recommended you use this wizard. See the TRITON - Email Security Help for more information.

**Important**

The Configuration Wizard is offered only once, at initial start up of TRITON - Email Security. If you choose to not use the Wizard it will no longer be available. All settings configured in the Wizard can be configured in TRITON - Email Security individually. The Wizard is simply offers a more convenient way to enter essential settings.

See the *Getting Started* section of the TRITON - Email Security Help for information on initial configuration. Be sure to complete the procedures for:

- Domain based route
- Trusted inbound mail
- Data Security
- Email Security Log Server
- Notification

If your subscription includes Email Security Gateway Anywhere, configure the hybrid email service. See the “Registering for the hybrid service” topic in the TRITON - Email Security Help.

# Content Gateway initial configuration

## Applies to

- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic

- *Enabling WCCP for Content Gateway*

## Overview

This section lists some initial tasks to perform after installing Websense Content Gateway. These are basic configuration tasks to bring Content Gateway to an initial, operable state. See the Content Gateway Manager Help for full configuration and management instructions.

Not all of these tasks may apply to you. Perform only those tasks that apply to your deployment.

## Starting Content Gateway Manager

Content Gateway Manager is the management user interface to Websense Content Gateway.

Content Gateway Manager supports the browsers listed in *System Requirements*, page 41. Use of another browser version may result in unexpected behavior. Java and JavaScript must be enabled in your browser. See your browser documentation for information on enabling Java and JavaScript.

There are 3 ways to access Content Gateway Manager:

- From the Content Gateway button in TRITON - Web Security
- By entering the IP address and port of the Content Gateway host system
- When Content Gateway is a module on a V-Series appliance, by opening the V-Series Logon portal and clicking the Content Gateway button.

### To access Content Gateway Manager directly

1. Open your Web browser.
2. Open a Web browser supported by Content Gateway Manager and enter the following URL:

   `https://<IP address>:8081`

   where `<IP address>` is the IP address of the Content Gateway machine. Note: 8081 is the default port.

   If the browser warns you about the site's security certificate, choose to proceed to the site anyway:

   - Internet Explorer: Click **Continue to this website (not recommended)**.

- Firefox: Scroll to the bottom of the invalid certificate message and click **Or you can add an exception**. Next, click **Add Exception** > **Get Certificate**. Select **Permanently store this exception**. Then click **Confirm Security Exception**.

> **Note**
> A pending alarm may be indicated on the screen. Clicking it will display more information. If it is a "WCG license download failed" alarm, you may clear it. This condition is resolved by entering a subscription key, which you will do in the next few steps.

For more information on using HTTPS to start Content Gateway Manager, see the *Using SSL for secure administration* topic in the Content Gateway Manager Help.

3. Enter the user name (**admin**) and password for the Content Gateway Manager default administrator user.

   The password was set up during installation.

4. If you are using Internet Explorer, install the Content Gateway Manager's security certificate:
   a. Next to the address bar, click **Certificate Error**.
   b. Click **View certificates**.
   c. Click **Install Certificate**.
   d. In the Certificate Import Wizard, click **Next** on the welcome dialog box. Select **Automatically select the certificate store based on the type of certificate** and click **Next**. On the last dialog box, click **Finish**.
   e. You are asked if you want to install the certificate. Click **Yes**.
   f. An *Import was successful* message appears. Click **Yes**.
   g. You are returned to the Certificate dialog box. Click **OK**.

5. Content Gateway Manager opens to the **Monitor > My Proxy > Summary** page. This page provides information on the features of your subscription and details of your Content Gateway system. See the Content Gateway Manager Help for more information.

## Entering a subscription key for Content Gateway

If Content Gateway is installed as part of Websense Web Security Gateway or Web Security Gateway Anywhere, the subscription key is automatically applied to Content Gateway when you enter it in TRITON - Web Security. See *Entering subscription key*, page 766 for more information.

If Content Gateway is deployed with only Websense Data Security, complete the following steps to enter a subscription key.

1. Start Content Gateway Manager.
2. For instructions, see *Starting Content Gateway Manager*, page 779.

3. Click the **Configure** tab on the upper left of the screen.
4. Enter your Websense subscription key:
   a. Click **My Proxy > Subscription > Subscription Management**.
   b. Enter your Websense subscription key and click **Apply**.
   c. Click **Basic** > **General** and then the **Restart** button to restart Content Gateway.

## Enabling SSL Manager in Content Gateway

In Content Gateway Manager:

1. Click **Configure > My Proxy > Basic > General**.
2. If it is not already enabled, set **HTTPS** to **On**. Then click **Apply** and the **Restart** button.
3. Confirm the ports listed on **Configure > Protocols > HTTPS > General**.
4. Add the Content Gateway Manager root security certificate:
   a. In the left navigation pane, click **SSL > Certificates > Add Root CA**.
   b. Click **Browse**.
   c. Select /**home/Websense/content_gateway_ca.cer** and click **Open**.
   d. Click **Add Certificate Authority**.

   "Issuer successfully imported!" appears.
5. Configure SSL Manager by providing information on the**Configure > SSL** pages in Content Gateway Manager.

   To get the benefit of SSL certificate verification, a very important element of SSL security, go to **Configure > SSL > Validation > General** and select **Enable the certificate verification engine**. This option is disabled by default. Review and select verification engine options. Be aware that certificates fail verification for a variety of reasons. You need to anticipate these failures and become familiar with the bypass options for when you want to proceed to a site anyway. For more information, see *Working with Encrypted Data* in the Content Gateway Manager Help.

## Enabling WCCP for Content Gateway

If you are supporting transparent proxy through WCCPv2-enabled routers, enable WCCP in Content Gateway Manager, and configure WCCP settings. See the Content Gateway Manager Help for details.

# Creating and running the script for Logon Agent

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## In this topic



## Overview

If you installed Websense Logon Agent, you must create a logon script for clients that identifies them to Websense software when they log on to a Windows domain. The Websense Logon application, **LogonApp.exe**, provides a user name and IP address to the Logon Agent each time a Windows client connects to a Windows Active Directory or a Windows NT directory service.

During Logon Agent installation, the logon application and script files are placed in the Websense **bin** directory (by default, C:\Program Files or Program Files (x86)\Websense\Web Security\bin on Windows or /opt/Websense/bin on Linux).

- **LogonApp.exe** (Windows only): The Websense executable that communicates user information to the Logon Agent.
- **Logon.bat**: The batch file containing sample logon and logout scripts.
- **LogonApp_ReadMe.txt**: A summary of the procedures for creating and running the Websense logon script and optional logout script.

## Prerequisites for running the logon script

Logon Agent requires running the logon application on Windows machines.

- If the logon script runs the logon application in persistent mode, configure your Active Directory server **not** to run scripts synchronously.
- Be sure that all computers can connect to the shared drive on the domain controller containing **logon.bat** and **LogonApp.exe**. You must copy both of these files from the machine running Logon Agent to both the **logon** and **logout** directories on the domain controller.

To determine if a Windows machine has access to the domain controller, run the following command from a command prompt:

```
net view /domain:<domain name>
```

- The TCP/IP NetBIOS Helper Service must be running on each Windows 2000, Windows XP, Windows Vista, Windows Server 2003, and Windows NT client machine that is identified by Logon Agent.
- The logon application on client machines must use NTLM authentication to communicate with Logon Agent. By default, Windows Vista machines use NTLMv2.

  To change this setting globally, for all machines in the network, modify the default domain Group Policy Object (GPO) to require use of NTLM authentication:

  1. On the domain controller machine, go to Start > Run, and then enter **mmc**.
  2. In the Microsoft Management Console, go to **File > Add/Remove Snap-In**, and then click **Add**.
  3. Select **Group Policy Management Editor**, and then click **Add**.
  4. Select the default GPO (for example, Default domain policy), and then click **Finish**.
  5. Click **Close** and then **OK** to close the open dialog boxes.
  6. In the navigation pane of the Console window, expand the Computer Configuration > Policy > Windows Settings > Security Settings > Local Policies node, and then select **Security Options**.
  7. In the content pane, select **Network Security: LAN Manager authentication level**, and change the setting to **Send NTLM response only**.
  8. Save and close the Console file.

  To change this setting on individual Windows Vista machines, change the default setting for **Network security: LAN Manager authentication level** as follows:

  1. Open the Windows **Local Security Settings** window. See the Windows online Help for assistance.
  2. Go to **Security Settings > Local Policy > Security Options**, and double-click **Network security: LAN Manager authentication level**.
  3. In the Properties dialog box that appears, select **Send NTLM response only**.

## Websense user map and persistent mode

When Logon Agent identifies a user, the user name and IP address are stored in a user map. The length of time this information is stored without reverification depends on whether the logon application is running in *persistent* mode or *non-persistent* mode. If LogonApp.exe is running in persistent mode, the update time interval is configured in TRITON - Web Security.

In non-persistent mode, user map information is created at logon and is not updated. The use of non-persistent mode creates less traffic between Websense software and the clients in your network.

In Active Directory, you can use a logout script to clear the logon information from the Websense user map before the interval defined in TRITON - Web Security. See *Task 1: Prepare the scripts*, page 784, for more information.

For detailed information about configuring Logon Agent in TRITON - Web Security, see the User Identification topic in TRITON - Web Security Help.

## Deployment tasks

- *Task 1: Prepare the scripts*

  Edit the parameters in the sample script file (Logon.bat) to suit your network.

- *Task 2: Configure the scripts to run*

  You can run your logon script from a Windows Active Directory or Windows NT directory service using group policies.

  The Websense executable and logon batch file must be moved to a shared drive on the domain controller that is visible to all clients. If you use Active Directory, you also can create and deploy an optional logout batch file on the shared drive.

- *Task 3: Configure Logon Agent in TRITON - Web Security*

  After the logon scripts and application have been deployed, configure Logon Agent in TRITON - Web Security.

### Task 1: Prepare the scripts

A batch file, called **Logon.bat**, is installed with Logon Agent in the Websense **bin** directory (by default, C:\Program Files or Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin).

This file contains instructions for using the scripting parameters, and two sample scripts: a logon script that runs the logon application (LogonApp.exe), and a logout script. The logout script removes user information from the Websense user map when the user logs out. Only Active Directory can use both types of scripts.

#### Script parameters

Construct a logon or logout script using the samples provided and the parameters in the table below.

The required portion of the logon script is:

```
LogonApp.exe http://<server>:<port>
```

This command runs LogonApp.exe in persistent mode (the default).

> **Note**
> You can edit the sample, or create a new batch file containing a single command.

| Parameter | Description |
|---|---|
| <*server*> | IP address or name of the Websense Logon Agent machine. This entry must match the machine address or name entered in TRITON - Web Security in Task 3. |
| <*port*> | The port number used by Logon Agent (default 15880). |
| /NOPERSIST | Causes the logon application to send user information to the Logon Agent at logon only. The user name and IP address are communicated to the server at logon and remain in the Websense user map until the user's data is automatically cleared at a predefined time interval. The default user entry expiration is 24 hours, and can be changed in TRITON - Web Security.<br>If the NOPERSIST parameter is omitted, LogonApp.exe operates in persistent mode, residing in memory on the domain server and updating the Logon Agent with the user names and IP addresses at predefined intervals. The default interval is 15 minutes, and can be changed in TRITON - Web Security. |
| /COPY | Copies the logon application to the**%USERPROFILE%\Local Settings\Temp** directory on users' machines, where it is run by the logon script from local memory. This optional parameter helps to prevent your logon script from hanging.<br>COPY can be used only in persistent mode. |
| /VERBOSE | Debugging parameter that must be used only at the direction of Technical Support. |
| /LOGOUT | Used only in an optional logout script, this parameter removes the user's logon information from the Websense user map when the user logs off. If you use Active Directory, this parameter can clear the logon information from the user map before the interval defined for Logon Agent has elapsed.<br>Use this optional parameter in a logout script in a different batch file than the one containing the logon script. See the *Examples* below. |

## Examples

The sample logon script sends user information to the Logon Agent at logon only. The information is not updated during the user's session (NOPERSIST). The information is sent to port 15880 on the server identified by IP address 10.2.2.95.

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST
```

With Active Directory you have the option to clear the logon information for each user as soon as the user logs out. (This option is not available with Windows NTLM.) Create a companion logout script in a different batch file, and place it into a different directory than the logon script.

Copy the logon batch file and rename it **Logout.bat**. Edit the script to read:

```
LogonApp.exe http://10.2.2.95:15880 /NOPERSIST /LOGOUT
```

## Task 2: Configure the scripts to run

You can configure your logon script to run with a group policy on Active Directory or on Windows NT Directory. The logout script only runs with Active Directory.

> **Note**
> The following procedures are specific to Microsoft operating systems and are provided here as a courtesy. Websense, Inc., cannot be responsible for changes to these procedures or to the operating systems that employ them. For more information, see the links provided.

### Active Directory

If your network uses Windows 98 client machines, go to the Microsoft Web site for assistance.

1. Make sure your environment meets the conditions described in *Prerequisites for running the logon script*, page 782.
2. On the Active Directory machine, go to the Windows Control Panel and select **Administrative Tools > Active Directory Users and Computers**.
3. Right-click the domain, and then select **Properties**.
4. On the **Group Policy** tab, click **New** and create a policy called **Websense Logon Script**.
5. Double-click the new policy or click **Edit**.
6. In the tree structure displayed, expand **User Configuration**.
7. Go to **Windows Settings** > **Scripts (Logon/Logoff)**.
8. In the right pane, double-click **Logon**.
9. Click **Show Files** to open this policy's logon script folder in Windows Explorer.
10. Copy two files into this folder:
    - **Logon.bat**, your edited logon batch file
    - **LogonApp.exe**, the application
11. Close the Explorer window.
12. Click **Add** in the Logon Properties dialog box.
13. Enter **Logon.bat** in the **Script Name** field or browse for the file.
14. Leave the **Script Parameters** field empty.
15. Click **OK** twice to accept the changes.
16. (Optional) If you have prepared a logout script, repeat Step 6 through Step 15. Choose **Logoff** at Step 8, and use your logout batch file when you are prompted to copy or name the batch file.
17. Close the Group Policy Object Editor dialog box.
18. Click **OK** in the domain Properties dialog box to apply the script.

19. Repeat this procedure on each domain controller in your network, as needed.

> **Note**
>
> You can determine if your script is running as intended by configuring your Websense software for manual authentication. If transparent authentication with Logon Agent fails for any reason, users are prompted for a user name and password when opening a browser. Ask your users to notify you if this problem occurs.
>
> To enable manual authentication, see the *User Identification* topic in the TRITON - Web Security Help.

For additional information about deploying logon scripts to users and groups in Active Directory, go to the Microsoft TechNet site (technet2.microsoft.com/), and search for the exact phrase: *Logon Scripts How To*.

### Windows NT directory or Active Directory (mixed mode)

1. Make sure your environment meets the conditions described in *Prerequisites for running the logon script*, page 782.
2. Copy the **Logon.bat** and **LogonApp.exe** files from the Websense installation directory on the Logon Agent machine (by default, C:\Program Files or Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin) to the **netlogon** share directory on the domain controller machine.

   ```
   C:\WINNT\system32\Repl\Import\Scripts
   ```

   Depending on your configuration, you may need to copy these files to other domain controllers in the network to run the script for all your users.
3. In the Control Panel of the domain controller, select **Administrative Tools > User Manager for Domains**.
4. Select the users for whom the script must be run, and double-click to edit the user properties.
5. Click **Profile**.
6. Enter the path to the logon batch file in the **User Profile Path** field (see Step 2).
7. Enter **Logon.bat** in the **Logon Script Name** field.
8. Click **OK**.

9. Repeat this procedure on each domain controller in your network, as needed.

> **Note**
> You can determine if your script is running as intended by configuring your Websense software to use manual authentication when transparent identification fails. If transparent authentication with Logon Agent fails for any reason, users are prompted for a user name and password when opening a browser. Ask your users to notify you if this problem occurs.
>
> To enable manual authentication, see the *User Identification* topic in the TRITON - Web Security Help.

### Task 3: Configure Logon Agent in TRITON - Web Security

After the logon/logout scripts and the logon application have been deployed and configured on the domain controllers, you must enable authentication in TRITON - Web Security. See the *User Identification* > *Logon Agent* topic in the TRITON - Web Security Help for instructions.

# Configuring a stealth mode NIC

## Applies to

- Web Filter v7.6
- Web Security v7.6
- Web Security Gateway v7.6
- Web Security Gateway Anywhere v7.6

## Configuring a stealth mode NIC

Websense software can inspect all packets with a monitoring NIC (network interface card) that has been configured for *stealth mode*. A NIC in stealth mode has no IP address and cannot be used for communication. Security and network performance are improved with this configuration. Removing the IP address prevents connections to the NIC from outside resources and stops unwanted broadcasts.

If Network Agent is configured to use a stealth-mode NIC, the installation machine must have multiple NICs. If Network Agent is installed on a separate machine, a second, TCP/IP-capable interface (i.e., it is not in stealth mode) must be configured to communicate with Websense software for filtering and logging.

During installation, stealth-mode interfaces do not display as a choice for Websense communications. Make sure you know the configuration of all the interfaces in the machine before attempting an installation.

**Important**

On Linux, stealth mode NICs appear together with TCP/IP-capable interfaces and must not be selected for communication.

Stealth mode for the Network Agent interface is supported on Windows and Linux.

## Windows

Configure a NIC for stealth mode as follows.

1. Go to **Start > Settings > Network and Dial-up Connection** to display a list of all the interfaces active in the machine.
2. Select the interface you want to configure.
3. Select **File** > **Properties**.

   A dialog box displays the NIC connection properties.
4. Clear the **Internet Protocol (TCP/IP)** checkbox.
5. Click **OK**.

## Linux

To configure a NIC for stealth mode in Linux, disable the Address Resolution Protocol (ARP), which breaks the link between the IP address and the MAC address of the interface. Run the following commands, replacing <*interface*> with the NIC's name, for example, **`eth0`**.

- To configure a NIC for stealth mode, run this command:

  `ifconfig <interface> -arp up`
- To return the NIC to normal mode, run this command:

  `ifconfig <interface> arp up`

**Important**

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Linux system configuration file, **/etc/sysconfig/network-scripts/ifcfg-<adapter name>**.

# 48 Adding or Modifying Components

## Applies to

- Web Filter 7.6.x
- Web Security 7.6.x
- Web Security Gateway 7.6.x
- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Overview

Websense components are added or modified using the Websense installer. When run on a machine that has current-version components installed, the Websense installer displays the **Modify Installation** dashboard.

For each type of component found (i.e., TRITON Infrastructure, Web Security, Data Security, and Email Security), the **Modify Installation** dashboard shows *Modify* and *Remove* links.

Clicking a *Modify* link starts a separate installer that is used to add or modify components of each type. For instructions, see:

- *Modifying TRITON Infrastructure*, page 792
- *Adding Web Security components*, page 794
- *Adding or modifying Data Security components*, page 796
- *Adding Email Security components*, page 801

Instead of *Modify* and *Remove* links, an *Install* link appears when no components of a particular type are found on this machine. Clicking *Install* starts a custom installation. For instructions, see:

- *Installing TRITON Infrastructure*, page 661
- *Installing Web Security components*, page 668
- *Installing Data Security Components*, page 692
- *Installing Email Security Components*, page 701

# Modifying TRITON Infrastructure

## Applies to

- Web Filter 7.6.x
- Web Security 7.6.x
- Web Security Gateway 7.6.x
- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Modifying TRITON Infrastructure

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.

2. In **Modify Installation** dashboard, click the **Modify** link for TRITON Infrastructure.


3. On the TRITON Infrastructure Setup **Welcome** screen, click **Modify**.
4. Proceed through the TRITON Infrastructure Setup screens. Current settings are shown. If you do not want to make any changes on a screen, simply click **Next**.

   For instructions on a screen see *Installing TRITON Infrastructure*, page 661.

5. To restore TRITON data backed up from another machine, use the **Restore Data From Backup** screen:
   a. Select **Use backup** data.
   b. Use **Browse** to locate the backup files.

      **Note**
      If the backup is located on another machine, map a network drive to its location. Otherwise, you will be unable to select it in when you click **Browse**.

      If the backup is from a Websense appliance, use a utility like 7-Zip to extract and unpack the contents of the appliance TRITON backup file to a temporary directory on this machine. When the process is complete, you should have a directory called **EIP_bak** that contains, among other files, **EIP.db** and **httpd-data.txt**, as well as **apache** and **tomcat** folders.
   c. Select **Merge administrators into existing installations (do not overwrite)** if you want to merge administrator accounts from the backup into the current system (see *Upgrading or Merging Administrators*, page 917 for more information).
   d. Click **Next**.

      If the following message appears, click **Yes** to proceed:

*The backup located at <path> is from the same release but from a different build (n). Proceed?*

Build differences do not affect restoration of the backup. Click **Yes** to continue with restoring the backup.

6. Click **Finish** at the **Installation Complete** screen.

# Adding Web Security components

## Applies to

- Web Filter 7.6.x
- Web Security 7.6.x
- Web Security Gateway 7.6.x
- Web Security Gateway Anywhere 7.6.x

**Note**

You cannot directly add Web Security components to a machine on which a filtering plug-in only is installed. See *Adding components to a filtering plug-in only machine*, page 795.

**Important**

Do not add other Web Security components to a Remote Filtering Server machine.

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.

2. In **Modify Installation** dashboard, click the **Modify** link for Web Security.


The Web Security component installer is started.

3. On the **Add Components** screen, select **Install additional components on this machine** and click **Next**.
4. On the **Select Components** screen, select the components you want to add and proceed as you would when performing a custom installation of Web Security components. See *Installing Web Security components*, page 668 for instruction.
5. When you are done adding Web Security components, you are returned to the **Modify Installation** dashboard.

# Adding components to a filtering plug-in only machine

## Applies to

- Web Filter 7.6.x
- Web Security 7.6.x

## Adding components to a filtering plug-in only machine

The following integration products require a Websense Web Security filtering plug-in:

- Microsoft ISA Server
- Citrix Presentation Server or XenApp
- Squid Web Proxy Cache

If you installed only the filtering plug-in on an integration product machine, you cannot directly add other Web Security components to it. The add component process

requires certain additional Websense files to be present. During the original installation of the filtering plug-in, these additional files were not installed to minimize the installation size on the machine.

> **Note**
> No other Websense components, other than Citrix Integration Service (i.e. the filtering plug-in) should be installed on a Citrix machine. Do not add components to it.

To add components to a machine on which a filtering plug-in is installed as the only Websense component, uninstall the plug-in (see *Removing Components*, page 805) and then run the Websense installer again to install the components you want. Be sure to select the filtering plug-in as one of the components to install when re-running the installer.

> **Note**
> Do not install Websense Network Agent on an ISA Server machine, unless ISA Server is used as a proxy only and not firewall.

# Adding or modifying Data Security components

## Applies to

- Web Filter 7.6.x
- Web Security 7.6.x
- Web Security Gateway 7.6.x
- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Adding or modifying Data Security components

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.

2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.


3. From the installation wizard, select **Modify**.

   This enables you to review the Data Security installation screens, making modifications as necessary. To add components, select them on the **Select Components** screen.

   Also, refer to the following sections for the most common Data Security modify procedures:

   - *Recreating Data Security certificates*, page 797
   - *Repairing Data Security components*, page 798
   - *Changing the Data Security privileged account*, page 799
   - *Changing the domain of a Data Security Server*, page 800

# Recreating Data Security certificates

## Applies to

- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Recreating Data Security certificates

From the Modify menu, you can also re-certify the server. In the initial authentication, the Data Security Management Server trades certificates with the other servers and endpoints in the network.

> **Important**
> When you perform the following procedure, endpoints that are configured to use HTTPS lose connection with the servers. To keep endpoints operational until you can re-install them, change the endpoint profile to allow HTTP before performing the procedure.

To re-run the security communication between Data Security components:

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. From the installation wizard, select **Modify**.
4. On the Recreate Certificate Authority screen, select the **Recreate Certificate Authority** check box.
5. Complete the installation wizard as prompted.

After recreating certificates, you must re-register all agents and servers (see *Re-registering Websense Data Security components*, page 968 for instructions), and repeat the Reestablish Connection process for each agent and server.

Endpoints also need to be reinstalled, or they will not be able to communicate with the servers via HTTPS. Create a new endpoint package using the package-building tool, and use SMS or a similar mechanism to install the new package on these endpoints. See *Deploying Websense endpoints*, page 744 for information on creating and installing an endpoint package.

# Repairing Data Security components

## Applies to

- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Repairing Data Security components

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. From the installation wizard, select **Repair**.
4. Complete the installation wizard as prompted.

This restores the installation configuration to its last successful state. This can be used to recover from various corruption scenarios, such as binary files getting deleted, registries getting corrupted, etc.

# Changing the Data Security privileged account

## Applies to

- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Changing the Data Security privileged account

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This is starts the installer without having to re-extract files.
   - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. From the installation wizard, select **Modify**.
4. In the Local Administrator dialog, select the new Websense Data Security privileged account to be used. Make sure the user is a member of the Administrator's local group.
5. Complete the installation wizard as prompted.

# Changing the domain of a Data Security Server

## Applies to

- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Changing the domain of a Data Security Server

It is a best practice to perform this task during off hours, or to route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.).

1. Stop the protector:
   a. Login to the protector as root.
   b. Execute “service pama stop”.

# To join a Data Security Server to a domain

## Applies to

- Web Security Gateway Anywhere 7.6.x
- Data Security 7.6.x
- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## To join a Data Security Server to a domain

1. In the TRITON - Data Security module of the TRITON Unified Security Center, add the Websense privileged account user from the domain to the local Administrators group. Add the user itself and not the domain group of which it is a member.
2. Log on with the Websense service account from the domain.
3. Restart the machine.
4. From **Start > Settings > Control Panel > Add/Remove Programs**, select **Websense Data Security** and click **Change/Remove**.
5. Perform the steps described in the procedure, *Changing the host name of the Data Security Management Server*, page 965.

6. Re-register all Websense Data Security policy engine servers, agents and protectors (See *Re-registering Websense Data Security components*, page 968).
7. Click **Deploy** in TRITON - Data Security.
8. In your PreciseID fingerprint classifiers, change the server to the correct name.
9. Run breach tests on all the channels to verify that the Websense Data Security infrastructure is functioning well. Make sure you get events in both the Event Viewer and Incidents Management.

# Adding Email Security components

## Applies to

- Email Security Gateway 7.6.x
- Email Security Gateway Anywhere 7.6.x

## Adding Email Security components

Only two Email Security Gateway components may be added on a machine: TRITON - Email Security and Email Security Log Server. All other Email Security Gateway components run on a Websense appliance and are managed through the Appliance Manager.

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) navigate to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This starts the installer without having to re-extract files.
   - Double-click the installer executable.

2. In **Modify Installation** dashboard, click the **Modify** link for Email Security.


The Email Security installer starts.

3. On the **Introduction** screen, click **Next**.
4. On the **Select Components** screen, select components to add and then click **Next**.

> **Note**
> If TRITON Infrastructure is currently installed on this machine, Email Security components automatically use the database engine and database login credentials entered when TRITON Infrastructure was installed. The Email Security Installer reads this information from configuration files created by TRITON Infrastructure Setup.

5. If TRITON Infrastructure is not found already installed on this machine, the **Log Database** screen appears. Specify the location of a database engine and how you want to connect to it.
   - **Log Database IP**: Enter the IP address of the database engine machine. If you want to use a named database instance, enter it the form *<IP address>\<instance name>*. Note that the instance must already exist. See your SQL Server documentation for instructions on creating instances.
     If you chose to install SQL Server Express as part of the installation of the TRITON Unified Security Center, the log database IP address should be that of the TRITON Unified Security Center machine.
   - **Database login type**: Select how Email Security Log Server should connect to the database engine.
     - **Trusted connection**:connect using a Windows trusted connection.
     - **Database account**:connect using a SQL Server account.

     Then enter a user name and password.

- If using a trusted connection, enter the domain\username of the account to be used. This account must be a trusted local administrator on the database engine machine.
- If using a database account, enter the name of a SQL Server account. This account must have certain roles assigned; see *Installing with SQL Server*, page 690.

When you click **Next**, connection to the database engine is verified. If the connection test is successful, the next installer screen appears.

6. On the **Email Security Database File Location** screen, specify where Email Security database files should be located and then click **Next**.

   This screen appears only if you chose to install Email Security Log Server.

   A default location for the Log Database is automatically shown.

   It is a best practice to use the default location. If you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files.

   The path entered here is understood to refer to the machine on which the database engine is located. The path entered must specify a directory that already exists.

7. On the **Pre-Installation Summary** screen, click **Install**.
8. The **Installing Websense Email Security** screen appears, as components are being installed.
9. Wait until the **Installation Complete** screen appears, and then click **Done**.

# 49 Removing Components

## Applies to

- Web Filter 7.6
- Web Security 7.6
- Web Security Gateway 7.6
- Web Security Gateway Anywhere 7.6
- Data Security 7.6
- Email Security Gateway 7.6
- Email Security Gateway Anywhere 7.6

## Overview

Websense components are removed using the Websense installer. When run on a machine that has current-version components installed, the Websense installer displays the **Modify Installation** dashboard.

For each type of component found (i.e., TRITON Infrastructure, Web Security, Data Security, and Email Security), the **Modify Installation** dashboard shows *Modify* and *Remove* links.

Clicking a *Remove* link starts a separate uninstaller that is used to remove components of each type. See the following sections for instructions:

- *Removing TRITON Infrastructure*, page 806
- *Removing Web Security components*, page 808
- *Removing Data Security components*, page 816
- *Removing Email Security components*, page 818

# Removing TRITON Infrastructure

## Applies to

- Web Filter 7.6
- Web Security 7.6
- Web Security Gateway 7.6
- Web Security Gateway Anywhere 7.6
- Data Security 7.6
- Email Security Gateway 7.6
- Email Security Gateway Anywhere 7.6

## In this topic



## Overview

Typically, *TRITON Infrastructure* should be removed only after removing any TRITON Unified Security Center modules (i.e. TRITON - Web Security, - Data Security, and - Email Security) from the same machine. It is possible to remove TRITON Infrastructure before removing TRITON Unified Security Center modules, but the modules will be rendered inoperable.

For instructions on removing TRITON Unified Security Center modules, see:

- TRITON - Web Security: *Removing Web Security components*, page 808
- TRITON - Data Security: *Removing Data Security components*, page 816
- TRITON - Email Security: *Removing Email Security components*, page 818

## To remove TRITON Infrastructure

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This starts the installer without having to re-extract files.
   - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Remove** link for TRITON Infrastructure.


3. At the **TRITON Infrastructure Uninstall** screen, click **Next**.

   The **Installation** screen appears, showing removal progress.

   The following message may appear if you have TRITON Unified Security Center modules installed on this machine (i.e., TRITON - Web Security, - Data Security, or - Email Security):

   *There are* n *management modules of TRITON Unified Security Center installed which will be inoperable if you remove TRITON Infrastructure.*
   *Do you want to continue with removal of TRITON Infrastructure?*
   *Note: Continuing will not remove the modules, only TRITON Infrastructure. You should remove the modules before removing TRITON Infrastructure.*

   **Warning**
   Removing TRITON Infrastructure will render TRITON Unified Security Center modules inoperable.

   Click **Yes** to proceed with removal of TRITON Infrastructure. Click **No** to cancel.
4. At the **TRITON Infrastructure has been uninstalled** screen, click **Finish**.
5. You are returned to the **Modify Installation** dashboard.

# Removing Web Security components

## Applies to

- Web Filter 7.6
- Web Security 7.6
- Web Security Gateway 7.6
- Web Security Gateway Anywhere 7.6
- Data Security 7.6
- Email Security Gateway 7.6
- Email Security Gateway Anywhere 7.6

## In this topic



## Overview

The Policy Broker and the Policy Server instances associated with the components you want to remove must be running when you remove Web Security components. Policy Server keeps track of the location of the components associated with it. It must be running so it is aware when a component has been removed. Policy Broker and Policy Server may be running on different machines than the one from which you are removing components. In a Websense appliance-based deployment, Policy Broker and Policy Server run on an appliance in*full policy source* mode. If you have an appliance running in *user directory and filtering* mode, then Policy Server is running on it (but not Policy Broker).

Web Security components should be removed in a particular order because of certain dependencies (see *Removal order of Web Security components*, page 813). If you are removing all components on a machine, make sure you move any custom files you want preserved beforehand (see*Preserving custom data before removing Web Security component*, page 814). Also, if your Web Security deployment is integrated with another product, see the following for any integration-specific requirements:

- *Check Point Integration*, page 285
- *Cisco Integration*, page 193
- *Citrix Integration*, page 167
- *Squid Web Proxy Cache Integration*, page 259
- *Universal Integrations*, page 323

Removal instructions are slightly different depending on the operating system:

- *To remove Web Security components (Windows)*, page 809
- *To remove Web Security components (Linux)*, page 811


## To remove Web Security components (Windows)

**Note**
After uninstalling components, you may be prompted to restart the machine.

1. Before removing components:
   - Use the Websense Backup Utility to make a backup of Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
   - If you are removing components from a Windows Server 2008 machine, log in as the built-in administrator, or run the Websense installer with elevated (full administrator) privileges.
2. Log on with **local** administrator privileges.
3. Close all applications (except Websense software; see the next step) and stop any antivirus software.
4. Make sure Websense software is running. The Web Security uninstaller looks for Policy Server during the removal process.

   **Warning**
   Do not remove Web Security components without the associated Policy Server running. Policy Server keeps track of configuration and component locations. If Policy Server is not running, files for the selected components are still removed, but configuration information is not updated for those components. Problems could occur later if you attempt to reinstall these components.

5. Start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This starts the installer without having to re-extract files.
   - Double-click the installer executable.

6. In **Modify Installation** dashboard, click the **Remove** link for Web Security.


7. At the **Remove Components** screen, select the components you want to remove and then click **Next**.

> **Warning**
>
> When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.
>
> Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining Web Security components and requires the reinstallation of those components.

> **Note**
>
> If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, the uninstaller cannot stop Network Agent and an error message is displayed.

If Policy Server is not running, a message indicates removing Web Security components may require communication with Policy Server.

a. Cancel the uninstaller.

b. Restart Policy Server from the Windows Services dialog box.

c. Start the Websense installer again and follow removal instructions again (Step 5).

8. At the **Summary** screen, click **Next**.

   The **Installation** screen appears, showing removal progress.

If you are uninstalling Network Agent after Policy Server has already been removed, expect the process to take several minutes. Network Agent is successfully uninstalled, although no progress notification is displayed.

9. At the **Uninstall Complete** screen, click **Uninstall**.

   **Important**
   Do not click **Cancel** in the Uninstall Complete screen. This renders the uninstallation incomplete. Be sure to click **Uninstall**.

10. You are returned to the **Modify Installation** dashboard.
11. If you stopped your antivirus software, restart it.
12. If you remove an integration plug-in, you may need to restart the integration product. See:
    - *Check Point Integration*, page 285
    - *Cisco Integration*, page 193
    - *Citrix Integration*, page 167
    - *Squid Web Proxy Cache Integration*, page 259
    - *Universal Integrations*, page 323.

## To remove Web Security components (Linux)

**Note**
Before removing components, use the Websense Backup Utility to back up Web Security configuration and initialization files. See the TRITON - Web Security Help for instructions.

1. Log on as **root**.
2. Close all applications (except Websense software; see the next step) and stop any antivirus software.
3. Make sure Websense software is running. The Websense uninstaller looks for Policy Server during the removal process.

   **Warning**
   When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.

   Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining Web Security components and requires the reinstallation of those components.

> **Note**
> If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, the uninstaller cannot stop Network Agent and an error message is displayed.

4. Run the uninstall program from the Websense installation directory (**/opt/Websense** by default):

   ```
   ./uninstall.sh
   ```

   A GUI version is available on English versions of Linux. To run it, enter:

   ```
   ./uninstall.sh -g
   ```

   The installer detects the installed Web Security components and lists them.

   > **Warning**
   > When removing components separately, always remove all other components, then Policy Server, and finally Policy Broker.
   >
   > Do **not** remove Policy Server before any component other than Policy Broker. Removing Policy Server cuts off communication with the remaining components and requires the reinstallation of those components.

5. Select the components you want to remove, and choose **Next**.

   > **Note**
   > If you are removing Filtering Service, all associated Network Agents must have already been removed. If you try to remove Network Agent **after** its associated Filtering Service has been removed, Setup cannot stop Network Agent and an error message is displayed.

   If Policy Server is not running, a message tells you that removing Websense components may require communication with Policy Server

   a. Cancel the uninstaller.
   b. Open a command shell and go to the **Websense** directory (/opt/Websense, by default).
   c. Enter the following command to start Websense services:

      ```
      ./WebsenseAdmin start
      ```

   d. Restart this process at Step 4.

6. A list shows the components selected for removal. Choose **Next**.

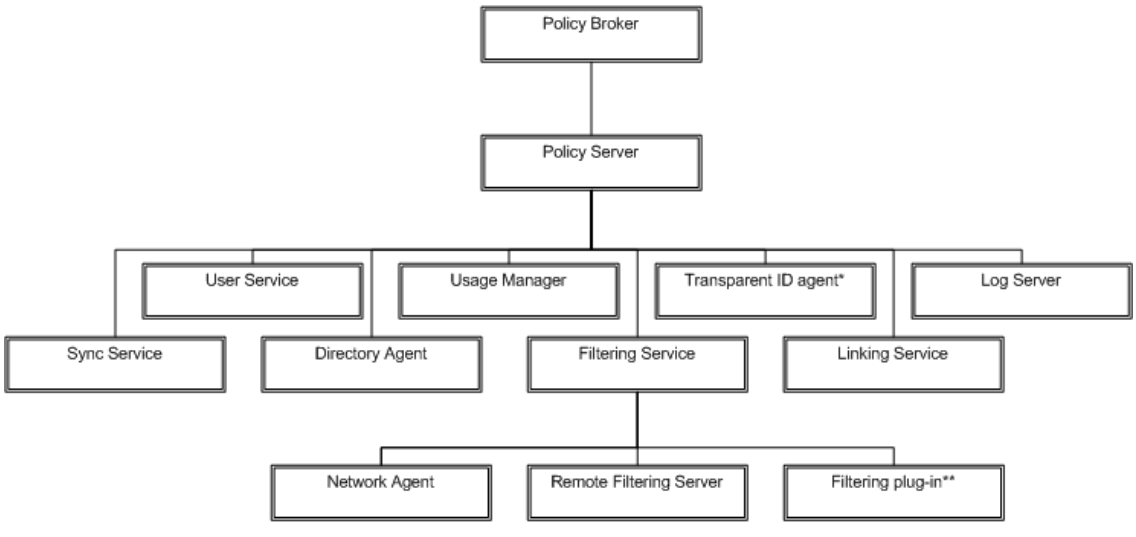
If you are uninstalling Network Agent on a remote machine after removing Policy Server, expect the process to take several minutes. Network Agent is successfully uninstalled, although no progress notification is displayed.

7. A completion message indicates that components have been removed. Exit the installer.
8. If you stopped your antivirus software, restart it.
9. If you remove an integration plug-in, you may need to restart the integration product. See:
   - *Check Point Integration*, page 285
   - *Cisco Integration*, page 193
   - *Citrix Integration*, page 167
   - *Squid Web Proxy Cache Integration*, page 259
   - *Universal Integrations*, page 323.

# Removal order of Web Security components

## Removal order of Web Security components

When removing a particular Web Security component, it is important to remove any dependent components first. Component dependencies are shown in the following diagram (note: not all Web Security components are included; only those with removal dependencies are shown).



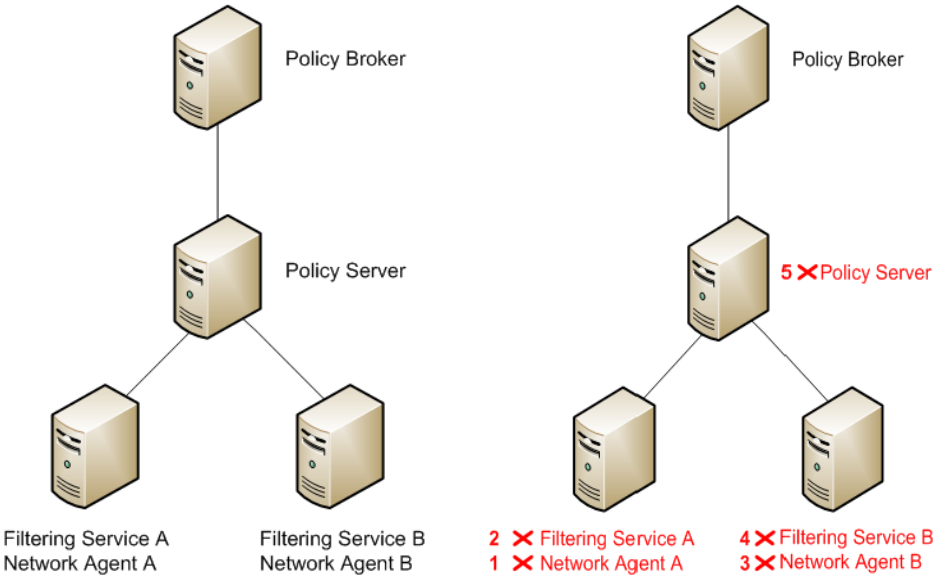

* DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent

** Microsoft ISAPI Filter, Citrix Integration Service, or Squid redirector plug-in

The dependency hierarchy goes from top-down, components below depend on components above. For example, if you want to remove Filtering Service, any associated Network Agent, Remote Filtering Server, and Filtering plug-in instances must be removed first. Likewise, to remove Policy Server, you must first remove any

instances of the components below it in the diagram (which is everything except Policy Broker).

It is important to note that these dependencies apply to distributed components as well. The uninstaller will notify you of dependent components on the same machine. However, it cannot notify you of dependent components on other machines. You must be sure to remove any dependent components on other machines before removing a component on this machine. For example, to remove the Policy Server instance shown below (left-side illustration), you must first remove Network Agent and then Filtering Service on the two machines dependent on the Policy Server. The numbers in the right-side illustration indicate the proper order of removal.




Notice that each Network Agent is removed before its associated Filtering Service, which is required by the component dependencies. Also, it does not matter which Filtering Service and Network Agent pair is removed before the other—just both pairs must be removed prior to removing the Policy Server.

# Preserving custom data before removing Web Security component

## Preserving custom data before removing Web Security component

If you have data or files you created yourself in the Websense\Web Security directory (default: C:\Program Files or Program Files (x86)\Websense\Web Security in Windows; /opt/Websense in Linux) or in sub-directories of the Websense\Web

Security directory, copy them to another location before removing all Web Security components. The uninstallation process may remove these files.

> **Note**
> If you have saved reports you want to retain after uninstalling all components, copy them from the **ReportingOutput** directory (under the Websense\Web Security directory). The report files are of the following types: *.pdf, *.xls, or *.zip (for HTML files).

Files of the following types are not removed by the uninstaller if they are located in the Websense\Web Security directory itself:

- *.zip
- *.mdb
- *.mdf
- *.ndf
- *.ldf
- *.bak

The above file types are protected from removal only in the Websense\Web Security directory itself. They may be removed if they reside in a sub-directory of the Websense directory. There are two sub-directories, however, that are protected from removal. Files in the Websense backup directory (default: C:\Program Files or Program Files (x86)\Websense\Web Security\backup in Windows; /opt/Websense/backup in Linux), if it exists, will not be removed by the uninstaller. Also, if the Log Database files reside in a sub-directory of the Websense directory, they will not be removed.

# Uninstalling Content Gateway

## Applies to

- Web Security Gateway 7.6
- Web Security Gateway Anywhere 7.6

## Uninstalling Content Gateway

To uninstall Websense Content Gateway, use the uninstall script (/root/WCG/Current/wcg_uninstall.sh).

1. Make sure you have root permissions.

   ```
   su root
   ```

2. Change to the /root/WCG/Current directory:

```
cd /root/WCG/Current
```

3. Run the uninstaller:

   ```
   ./wcg_uninstall.sh
   ```

4. Confirm that you want to uninstall the product. You *must* enter **y** or **n**.

   ```
   Are you sure you want to remove Websense Content Gateway
   [y/n]?
   ```

5. When a message indicates that Websense Content Gateway has been uninstalled, reboot the system.

# Removing Data Security components

## Applies to

- Web Security Gateway Anywhere 7.6
- Data Security 7.6.x
- Email Security Gateway 7.6
- Email Security Gateway Anywhere 7.6

## In this topic



## Overview

Data Security components can only be removed altogether. You cannot select particular components on a machine for removal.

**Warning**

Websense Email Security Gateway requires Websense Data Security to be installed. If you are using Email Security Gateway, do not uninstall Data Security or Email Security Gateway will quit working.

For instructions on removing a Data Endpoint, see *To remove a Data Endpoint*, page 817.

## To remove Data Security components

1. If you are uninstalling the printer agent v7.6.x, select **Start > All Programs > Websense > Printer Agent Configuration**, and when the configuration tool launches, select **Remove All**.
2. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) navigate to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This starts the installer without having to re-extract files.
   - Double-click the installer executable.
3. In **Modify Installation** dashboard, click the **Modify** link for Data Security.


4. At the **Welcome** screen, click **Remove**.
5. At the **Data Security Uninstall** screen, click **Uninstall**.

   **Important**
   This removes all Data Security components from this machine.

   The **Installation** screen appears, showing removal progress.
6. At the **Uninstallation Complete** screen, click **Finish**.
7. You are returned to the **Modify Installation** dashboard.
8. Reboot your machine.
9. Delete the Data Security installation directory.

## To remove a Data Endpoint

See *Uninstalling endpoint software*, page 757.

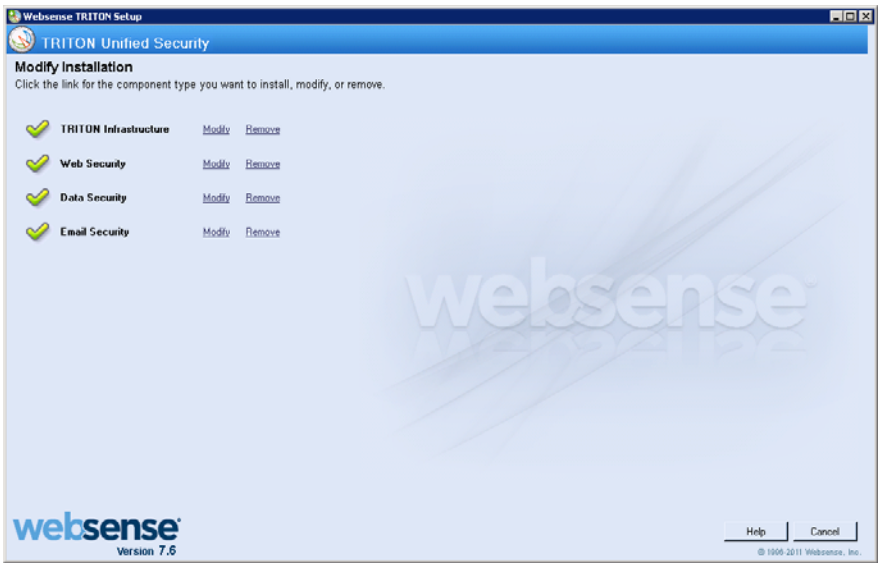
# Removing Email Security components

## Applies to

- Email Security Gateway 7.6
- Email Security Gateway Anywhere 7.6

## To remove Email Security components

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files (see *Keeping installer files*, page 58) navigate to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**. This starts the installer without having to re-extract files.
   - Double-click the installer executable.
2. In **Modify Installation** dashboard, click the *Remove* link for Email Security.




The Email Security uninstaller starts.

3. On the **Uninstall Websense Email Security** screen, click **Next**.
4. On the **Uninstall Options** screen, choose whether you want to uninstall all or specific Email Security Gateway components.

   Note that the icons next to **Complete Uninstall** and **Uninstall Specific Components** are buttons. Click the button for the option you want and then click **Next**.
5. If you chose to remove specific components, the **Choose Components to Remove** screen appears. Select the check box for each component you want to remove and then click **Uninstall**.
6. The **Uninstall Websense Email Security** screen appears, showing removal progress.

The following message may appear:

*The Email Security database exists, do you want to remove it?*

Clicking **Yes** removes the database. Clicking **No** keeps the database and proceeds with removing components.

**Warning**

You will lose current Email Security log data if you remove the database. If you want to keep this data, back up the esglogdb76 and esglogdb76_*n* databases. See your SQL Server documentation for backup instructions.

**Warning**

If you remove the database, any currently quarantined email will no longer be accessible. If you plan to reinstall TRITON - Email Security elsewhere to use with the same Email Security Gateway appliance and want access to currently quarantined email after reinstalling, do not remove the database.

7. On the **Components Removed** screen, click **Done**.

# 50 Upgrading Websense software to the latest v7.6.x

## Applies to

- Web Filter v7.x
- Web Security v7.x
- Web Security Gateway v7.6.x
- Data Security v7.6.x
- Email Security v7.6.x

## In this topic



## Overview

This section of the Websense Technical Library explains how to upgrade to the latest version of Websense software in the v7.6.x series.

- For Web Security, Web Filter, and Web Security Gateway, the latest version is v7.6.7.
- For Email Security Gateway, the latest version is v7.6.7.
- For Data Security, it is v7.6.8.

Components within the same product module must be running at the same version. Make sure that every Websense server has been upgraded.

- For example, all Web security components must be upgraded to v7.6.7.
- All Data security components must be upgraded to v7.6.8.
- All Email security components must be upgraded to v7.6.7.

All direct upgrades to components that run on Windows servers use the same TRITON installer. After backing up your system, download and launch this TRITON installation package for Windows servers: **WebsenseTRITON767Setup.exe**.

For upgrades to Linux components, back up the servers and then download and use **WebsenseWeb767Setup_Lnx.tar.gz.**

## Upgrade paths after backup

- For Web Filter and Web Security (running off the V-Series appliance), you can upgrade to v7.6.7 directly from v7.1.x, 7.5.x, v7.6.x. If you're running an earlier version of Web Security or Web Filter, you should back up your files, upgrade to v7.1, back up files again, and then upgrade to v7.6.7.
- For Content Gateway software at v7.1.x or v7.5.x (not on appliance), back up your files, upgrade to v7.6.0, back up your files again, and then upgrade to v7.6.7.
- For Data Security, you must be at v7.6.0, v7.6.2, or v7.6.3 before upgrading to v7.6.8. See *Upgrading to Data Security 7.6.0* for information on upgrading Data Security from earlier versions, such as v7.1 or v7.5, to v7.6.0.
- For Email Security Gateway you may be running v7.6.0 or v7.6.2 before upgrading to v7.6.7. See *Email Security Gateway (V10000 G2)*, page 585 or *Email Security Gateway (V5000 G2)*, page 575 for information on installing and deploying Email Security v7.6.0.

Considerations for upgrading to v7.6.x:

- Unless instructed otherwise by Websense Technical Support, your system must be functional prior to upgrade.
- For best practice, perform a full backup of your system before performing an upgrade. The WsBackup utility is available on Windows and Linux. The backup Utility saves the essential Websense software files on the machine on which it is run, including any custom policies and block pages. A complete list of the files saved can be found in the Websense Manager Help (v7.1.x) and TRITON - Web Security Help (v7.5 and v7.6).
- The upgrade process on the TRITON manager machine (Windows server) guides you through upgrading all TRITON security modules that you have installed to the latest version. You cannot choose which modules to upgrade. Partial upgrades are not supported. (Each product is moved to the latest version available for that product.)
- With the exception of the TRITON infrastructure, if one of the component's upgrade fails, you can continue to upgrade the rest of the components, or you can exit the process and modify component settings.

  You cannot continue if the infrastructure upgrade fails, and you cannot roll back a component that was upgraded successfully.
- After upgrade, your system has the same configuration settings as before the upgrade. The upgrade process does not allow you to change your configuration or settings. (You can change those after the upgrade, if desired.)

- The upgrade process guides you on the correct upgrade sequence across machines. Where critical, it verifies that the upgrade was performed in the correct order.

For instructions on upgrading all TRITON modules, see *Performing the upgrade*, page 824. In this topic, there are procedures for upgrading:

- *TRITON Infrastructure*, page 825
- *Web Security*, page 826
- *Data Security*, page 827
- *Email Security*, page 827

### Upgrade order for mixed topologies

If you have a mixed topology, upgrade components in the following order:

1. Policy Broker (a Web security component)
2. Other Web Security components
3. TRITON infrastructure (includes Web, Email, and Data Security management components)
4. Other Data Security components

Always upgrade the Web security Policy Broker before the TRITON management server (or at the same time, if they are on the same machine).

If the Policy Broker machine has Data Security components on it, still upgrade the Policy Broker first.

Always upgrade the management server before any other Data Security components. In this way, Data Security policy engines (and thus analysis) continue to function before the policy engines can be upgraded themselves. Note that you cannot deploy new policies to the policy engines until they are upgraded to the same version as the management server.

If you need to upgrade a Data Security policy engine before upgrading the TRITON management server—because the policy engine resides on an appliance that acts as Policy Source—detection of fingerprinted content might not work on the appliance until the management server is upgraded as well.

**Important**

The components running on the machine you are upgrading go down until the upgrade is complete. You should expect a brief period of down time.

**Sample scenario:**

If your current Websense environment includes the following:

- 2 copies of Websense Content Gateway v7.6.0 (software only)

- 1 TRITON management server (including Web, Data, and Email management components, Web Security Policy Broker, and Web and Email Security Log Servers)
- 1 V5000 G2 with Email Security Gateway

Upgrade your system in the following order:

1. TRITON management server (this upgrades the Policy Broker simultaneously)
2. V5000 G2 with Email Security Gateway (MTA)
3. Websense Content Gateway (software)

Note that the Content Gateway proxies will not perform Web filtering after the Policy Broker is upgraded, until the Content Gateway software is upgraded as well.

The Email Security Gateway MTA will continue to function after the management server upgrade, but the logs are cached on the appliance until Email Security Gateway is upgraded as well. For best practice, upgrade Email Security Gateway as soon as possible after the management server, or email traffic must be redirected to another MTA.

The Data Security policy engine embedded in Content Gateway and Email Security Gateway will continue to monitor the old Web and email DLP policies and block/permit accordingly.

# Performing the upgrade

## In this topic



## Getting Started

To upgrade your components on Windows after backing up your files with WSBackup, download and launch the latest TRITON installation package, **WebsenseTRITON767Setup.exe**. Use this same package even if you are upgrading Email Security components to v7.6.7 and Data Security components to 7.6.8.

The latest installer always upgrades your software to the newest version (if not already upgraded).

- Using the latest TRITON installer, you upgrade existing Data Security software to v7.6.8.

- Existing Email Security software upgrades to v7.6.7
- Existing Web Security software upgrades to v7.6.7.
- If you are already on the latest Data and Email security version, the installer upgrades only Web security.

This is the same executable used for scratch installations. To obtain the installer package, visit the Websense Downloads site:

www.websense.com/MyWebsense/Downloads/

The installation package detects if earlier versions of the product are installed, and automatically starts a series of upgrade wizards—one for each of the installed components.

For upgrades to Linux components, back up the files with WSBackup and then download and use **WebsenseWeb767Setup_Lnx.tar.gz.**

## TRITON Infrastructure

The TRITON infrastructure provides basic framework for the TRITON unified console and includes a central settings database and internal services.

The infrastructure upgrade wizard contains the following dialogs. Note that no input is required from you to upgrade the TRITON infrastructure.

| Wizard Page | Fields |
|---|---|
| Welcome | This screen welcomes you to the installation and upgrade wizard.<br>1. Click **Next** to begin the upgrade process. The system checks disk space requirements.<br>2. When prompted, click **Next** to launch the installation wizard. |
| Pre-Installation Summary | This screen shows:<br>• The destination folder for the installation files.<br>• The name of the SQL Server machine and the user name of an authorized database administrator.<br>• The IP address of the TRITON management server and administrator credentials.<br>Click **Next** to accept the properties. |

| Wizard Page | Fields |
|---|---|
| Installation | This screen shows the progress of the installation. The system stops processes, copies new files, updates component registration, removes unused files, and more. |
| Summary | When installation of this module is complete, this screen summarizes your system settings. This screen shows:<br>• The destination folder for the installation files.<br>• The name of the SQL Server machine and the user name of an authorized database administrator.<br>• The IP address of the TRITON management server and administrator credentials.<br>Click **Finish** to complete the upgrade for this module. |

## Web Security

The Web Security upgrade wizard contains the following dialogs. Note that no input is required from you.

| Wizard Page | Fields |
|---|---|
| Introduction | This screen welcomes you to the Web Security upgrade wizard. Click **Next** to continue. |
| Pre-Installation Summary | This screen informs you that a previous version of Web Security or Web Filter has been detected.<br>1. Click **Next** to start the upgrade.<br>The installer proceeds to stop all Websense software services. This can take up to 10 minutes. When complete, it tells you which components will be upgraded.<br>2. Click **Install** to continue.<br>The installer proceeds to back up critical files. |
| Installation | This screen shows that the installation is progressing.<br>When complete, the installer configures your Web Security software. This can take up to 10 minutes. |
| Installation Complete | You're notified when installation of this module is complete. Click **Done** to exit the installer. |

## Data Security

The Data Security upgrade wizard contains the following dialogs. Note that no input is required from you.

| Wizard Page | Fields |
|---|---|
| Welcome | This screen welcomes you to the installation and upgrade wizard for Data Security.<br>The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard. |
| Select Components | This screen shows the components that will be upgraded (those that are currently installed). The system then determines the disk space required for these components. Click **Next** to continue. |
| Temporary File Location | If you are using a remote SQL Server database, this screen shows where temporary files will be stored during archive processing or system backup or restore. |
| Installation Confirmation | Verify your system settings and click **Install** to continue the upgrade. |
| Installation | This screen shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more. |
| Summary | When installation of this module is complete, this screen summarizes your system settings.<br>1. Click **Done** and you're prompted to update your predefined policies and content classifiers.<br>2. Click **OK** to install the updates. You're shown the status of the updates, the items being updated, and details such as how many policies are updated, deleted, or added.<br>3. Click **Close** when the updates are complete. |

## Email Security

The Email Security upgrade wizard is used to upgrade the components that are installed off of the V-Series appliance: the management component (TRITON - Email Security), and the Email Security Log Server. It contains the following dialogs. Note that no input is required from you.

| Wizard Page | Fields |
|---|---|
| Introduction | This screen welcomes you to the Email Security upgrade wizard. Click **Next** to continue. |
| Select Components | This screen shows the components that will be upgraded (those that are currently installed). Click **Next** to continue. |

| Wizard Page | Fields |
|---|---|
| Configuration | This page shows the IP address of the database engine configured to manage the Email Security Log Database and the logon type. If you have changed the database since your previous installation, modify the settings here. |
| Pre-Installation Summary | This screen shows:<br>• The components to be installed<br>• The pre-existing and new version numbers<br>• The destination folder for the installation files<br>• The required and available disk space<br>Click **Install** to begin the upgrade. |
| Installation | This screen shows that the installation is progressing.<br>The management component, TRITON - Email Security, is upgraded on the TRITON management server.<br>The Email Security Log Server is upgraded on machines where it is found.<br>When complete, the installer configures your Email Security software. This can take up to 10 minutes. |
| Summary | You're notified when installation of this module is complete. Click **Done** to exit the installer. |

For Email Security appliances, there is a patch upgrade available for v7.6.7. A patch exists for dual appliances (Web and Email Security) and for Web Security (only) appliances, as well.

# 51 Upgrading Web Security or Web Filter to 7.6.0

## Applies to

- Web Filter v7.1, v7.5, v7.6.0
- Web Security v7.1, v7.5, v7.6.0
- Web Security Gateway v7.1, v7.5, v7.6.0

## Overview

This section of the Websense Technical Library describes how to upgrade software-based (not running on a Websense appliance) Web Security components to v7.6.0. For information on how to upgrade to v7.6.2, refer to*Upgrading Websense software to the latest v7.6.x*, page 821.

Perform an upgrade by running the Websense installer on a machine with previous-version Websense components installed. The installer detects the presence of the components and upgrades them (with the exception of Remote Filtering Client) to the current version. For instructions on upgrading Remote Filtering Client, see Remote Filtering Software technical paper.

> **Note**
> Technical papers and documents mentioned in this article are available in the Websense Technical Library: www.websense.com/library.

Versions 7.1.x and 7.5.x of Websense Web Security or Websense Web Filter may be directly upgraded to version 7.6.

**Important**

Sites upgrading from version 7.1.1 should study the section titled *Backing up files* to see a list of variables that are returned to their default values during an upgrade from version 7.1.1 to version 7.6. Before you upgrade from version 7.1.1, please make a note of any custom values you have given these few variables, so that you can reset them after the upgrade.

New features for version 7.6 are described in the *Release Notes* for Websense Web Security and Websense Web Filter, Version 7.6. Information specific to this release is also available in the Upgrading User Quick Start tutorial, accessible from within TRITON - Web Security once it is installed.

See the following topics:


- *Versions supported for upgrade*, page 830
- *Preparing for the upgrade*, page 832
- *Upgrade instructions (Windows)*, page 842
- *Upgrade instructions (Linux)*, page 846
- *Adding Web Security components during upgrade*, page 849
- *Changing IP addresses of Web Security components after upgrade*, page 850
- *New security certificate*, page 850


For information about upgrading Websense software when integrated with a third-party product, see:


- *Check Point Integration*, page 285
- *Cisco Integration*, page 193
- *Citrix Integration*, page 167
- *Squid Web Proxy Cache Integration*, page 259
- *Universal Integrations*, page 323


# Versions supported for upgrade

## Applies to

- Web Filter v7.1, v7.5, v7.6
- Web Security v7.1, v7.5, v7.6
- Web Security Gateway v7.1, v7.5, v7.6

## In this topic



## Overview

Direct upgrades to version 7.6 are supported from version 7.1 or higher of Websense Web security components. Configuration and policy settings are preserved (with a few exceptions for sites *Upgrading from v7.1.1*.).

Upgrades from versions prior to 7.1 require intermediate upgrades:

- version 5.5 > version 6.1 > version 6.3.2 > version 7.1 > version 7.6

> **Important**
> After upgrading from version 6.3.2 to 7.1, reboot the machine before upgrading it to version 7.6.

Configuration and policy settings are preserved across the intermediate upgrades. To perform an intermediate upgrade, download the installer package for the intermediate version from the Websense Downloads site:

www.websense.com/MyWebsense/Downloads/

> **Important**
> When performing intermediate upgrades, be sure to read the Websense Web Security and Websense Web Filter *Installation Guide* and its upgrade supplement for each upgrade version. They contain important information specific to upgrading between particular versions that may not be found in this version of the upgrade supplement.

## Upgrading versions prior to 5.5

Perform a fresh installation rather than upgrade Websense software that is prior to version 5.5. Uninstall the prior version (be sure to remove all components from all machines in the network) and then install version 7.6. For uninstallation instructions, see the installation guide for your version available here (http://www.websense.com/applications/docsarchive).

If you have a complicated policy configuration, contact Websense Technical Support for assistance.

# Preparing for the upgrade

## Applies to

- Web Filter v7.1, v7.5, v7.6
- Web Security v7.1, v7.5, v7.6
- Web Security Gateway v7.1, v7.5, v7.6

## In this topic



## Overview

This section describes important tasks to perform or issues to consider before upgrading Websense software.

## System requirements

Before upgrading Websense Web Security components, make sure the installation machine meets the system recommendations in *System Requirements*, page 41, including hardware specifications, operating system, browser, and database engine.

## Preparing for installation

See *Preparing for Installation*, page 55 for important information about preparing to use the Websense installer, which is used to upgrade components on Windows.

On Linux, the Web Security installer for linux is used to upgrade components.

**Important**

As part of the upgrade process, the Websense installer can install SQL Server 2008 R2 Express (which replaces MSDE as the no-cost, reduced-performance version of SQL Server supported by Websense solutions). If you intend to install SQL Server 2008 R2 Express, be sure to install the following prior to starting the upgrade:

- .NET Framework 3.5 SP1
- Windows Installer 4.5

## Deciding location of Web Security Manager

**Note**

In this section, the *Web Security manager* refers to both v7.5 TRITON - Web Security and v7.1 Websense Manager.

In version 7.6, management of a Websense deployment is concentrated on one machine, the TRITON management server. All management interfaces (i.e., TRITON - Web Security, - Data Security, and - Email Security) and components run on this machine.

When upgrading Web Security components to version 7.6, you must decide what to do with the current installation of the Web Security manager. You can choose to leave it in its current location and upgrade it in place. TRITON Infrastructure will be installed and then the Web Security manager upgraded. Together these components form a TRITON Unified Security Center.

You can choose to move it to a different machine. To do this, uninstall the Web Security manager from its current location. Then install TRITON Unified Security Center (including v7.6 TRITON - Web Security) on a different machine.*Upgrade instructions (Windows)*, page 842 guide you through this process.

Note that if the Web Security manager is installed on Linux, it will be disabled by the installer during upgrade. For version 7.6, management functions run only on Windows.

It is important to note that TRITON Unified Security Center can run with **only** its Web Security management module (i.e., TRITON - Web Security) enabled if running on a Windows Server 2003 machine. If you want to enable other management modules (e.g., TRITON - Data Security or - Email Security), TRITON Unified Security Center must run on a Windows Server 2008 R2 machine. If the Web Security manager is currently running on a Windows Server 2003 machine, you must uninstall it. Then, install TRITON Unified Security Center on a Windows Server 2008 R2 machine. Note that if your subscription includes Web Security Gateway Anywhere, you must run the TRITON Unified Security Center on a Windows Server 2008 R2 machine because both TRITON - Web Security and - Data Security modules are required.

If necessary, obtain a machine meeting the operating system and hardware requirements stated in *System Requirements*, page 41 prior to beginning the upgrade process.

When the upgrade process is started the prior-version Web Security manager will be detected if present and the installer will ask what you want to do with it.

## Websense administrator accounts

Make sure Websense administrator accounts authenticated by a directory service have an email address specified in the directory service. In version 7.6, an email address is required for each administrator account (except group accounts). See *Upgrading or Merging Administrators*, page 917 for more information.

## Backing up files

Before upgrading to a new version of Websense Web Security components, it is a best practice to perform a full system backup. This makes it possible to restore the current production system with minimum downtime, if necessary.

### Upgrading from v7.1.x or v7.5

Use the Websense Backup Utility on each machine that contains Websense Web Security components:

1. Stop Websense services. See *Starting or Stopping Web Security Services*, page 923.
2. Do one of the following:
   - *Windows*: Open a command window (Run > cmd) and navigate to the Websense **bin** directory (C:\Program Files\Websense\bin, by default).
   - *Linux*: Navigate to the Websense installation directory (/opt/Websense/bin, by default).
3. Use the following command to run the Backup Utility:
   - *Windows*:

```
wsbackup -b -d <directory>
```

- *Linux*:

```
./wsbackup -b -d <directory>
```

For these commands, <*directory*> is the path where the backup file will be stored.

The Backup Utility saves the essential Websense software files on the machine on which it is run, including any custom block pages. A complete list of the files saved can be found in the Websense Manager (v7.1.x) or TRITON - Web Security (v7.5) Help.

Repeat this process on **all** machines on which Websense Web Security components are installed, and make sure that the files are stored in a safe and accessible location.

4. Start the Websense services. The Websense services must be running when you start the upgrade.

## Upgrading from v7.1.1

Sites upgrading to version 7.6 from Websense Web Filter or Web Security version 7.1.1 should run the backup utility described above and should also carefully read the following list. This is a short list of configuration variables affected by the upgrade from v7.1.1.

These variables are returned to their default values during an upgrade from version 7.1.1 to version 7.6. They must be reset to your custom values.

Before you upgrade from version 7.1.1, please make a note of any custom values you may have given these variables or settings, so that you can reset them after the upgrade.

### Windows-specific variables and settings that assume default values

- If you customized the charts displayed on the Today page in Websense Manager, or changed the values of the Time or Bandwidth Estimate options, you must re-do these customizations on the Today page in the TRITON console for Web Security.
- If you have set up Active Directory on the **Settings** > **General** > **Directory Services** page, you need to re-enter the information after the upgrade.
- If you customized the name of the folder used to output scheduled presentation reports, your customized folder name does not persist after the upgrade to v7.6. Check the name of this folder inside the file **mng.xml** in this path: C:\Program Files\Websense\tomcat\conf\Catalina\. The filename is the value for the parameter: **reportsOutput**.
- Reporting preferences on the page **Settings** > **Reporting** > **Preferences** do not persist after an upgrade to v7.6.This includes the **SMTP server IP address** or name, the **email recipients** for scheduled reports, and the **Allow self-reporting** check box. Note the values before the upgrade and reset them afterwards.
- Note the Active Directory values configured in Websense Manager on the **Settings** > **Directory Service** page. You need to specify these again after the upgrade.

- Navigate to the **Manage Custom LDAP Groups** page, and note any custom groups you have set up, based on attributes defined in your directory service. This option is available only if you have configured Websense software to communicate with an LDAP-based directory service. After the upgrade to v7.6, custom LDAP groups created by delegated administrators need to be re-created.
- If you specified a non-standard port on which Network Agent monitors HTTP traffic, the setting does not persist after an upgrade to v7.6. This paragraph explains how to check this setting. Navigate to the **Settings > Network Agent > Local Settings** page to see the settings for a selected instance of Network Agent. The IP address of the selected Network Agent instance appears in the title bar of the content pane, and is highlighted in the left navigation pane. Use the **Network Interface Cards** list to see the configuration for the individual NICs. Click on a NIC in the **Name** column to view (and then make note of) custom details. If HTTP requests in your network are passed through a non-standard port, click **Advanced Network Agent Settings** to see the ports that Network Agent monitors. By default the Ports used for HTTP traffic are 8080, 80.
- If you customized the HTTPS port value for Websense Manager, the custom value does not persist after upgrade. To check the value, or to reset the value after the upgrade:
  - On the machine where the TRITON Unified Security Center runs, use the Windows Services dialog box (Start > Administrative Tools > Services) to stop the Websense TRITON - Web Security service.
  - In a text editor, open the file **server.xml** from the folder C:\Program Files\Websense\Web Security\tomcat\conf.
  - Change the value of the HTTPS port to the desired port.
- After upgrade, you must manually set the version number to 7.6 (in place of 7.1.1) in the container \EIMServer\Global\Version\ in the file **config.xml**. This file is located by default in the directory C:\Program Files\Websense\Web Security\bin\.

### Linux-specific variable that assumes default value

The value of DNSLookup in the file **eimserver.ini** should be noted before upgrade and restored afterwards.

This file is located by default in the directory /opt/Websense/bin/.

### Variables on both Windows and Linux that assume default value

- During the process of upgrading from v7.1.1, the parameter redirect_children, in the **squid.conf** file located by default in the /etc/squid directory, is reset to default.
- The value of all parameters in the file **mng.xml**, such as **connectionsMaxActive,** should be noted before upgrade and then restored to the custom value after the upgrade.This file is located by default in the directory:

> **Warning**
> Do not simply replace the mng.xml file with the pre-upgrade version of the file. That will corrupt the installation. Instead, open the post-upgrade mng.xml file and edit parameters to pre-upgrade values individually.

- Windows:
  C:\Program Files\Websense\tomcat\conf\Catalina\localhost\ (v7.1.1)
  C:\Program Files\Websense\Web Security \tomcat\conf\Catalina\localhost\ (v7.6)
- Linux: /opt/Websense/tomcat/conf/Catalina/localhost/

### Upgrading from v5.x and v6.x

Before starting the multiple-step process required to upgrade a v5.x or v6.x system, be sure to back up (at a minimum) the following files:

1. Stop all Websense services. See "Stopping and starting Websense services" in the Websense Enterprise and Websense Web Security Suite *Installation Guide*.
2. Make a backup copy of the following files (located by default in the C:\Program Files\Websense\bin or /opt/Websense/bin directory).
   - config.xml
   - websense.ini
   - eimserver.ini
3. If you have created custom block pages, make a backup copy of the files in the **Websense\BlockPages\en\Custom** (Windows) or **Websense/BlockPages/en/Custom** (Linux) directory.
4. Save the backup copies to another location.
5. Start the Websense services. The Websense services must be running when you start the upgrade.

## Preparing SQL Server for upgrade

It is important that you back up your current Websense databases and stop any active SQL Server Agent jobs prior to upgrading. After upgrade, reactivate the jobs to resume normal database operations.

**Warning**

Having active database operations taking place during upgrade can leave the Websense log database in an inconsistent state after upgrade. It is important to stop Log Server and currently active SQL Server Agent jobs prior to upgrading Web Security or Web Filter.

1. Back up Websense databases.

   Refer to Microsoft documentation for instructions on backing up databases. The Websense Web Security databases are named wslogdb70, wslogdb70_1, wslogdb70_2, and so on. wslogdb70 is referred to as the *catalog database*. wslogdb70_*n* are *database partitions*.
2. On the machine running Websense Log Server, stop Websense Log Server:

   Use the Microsoft Services console to stop Websense Log Server.

3. Disable all currently active Websense SQL Server Agent jobs:
   a. Log in to the Microsoft SQL Server Management Studio.
   b. In the Object Explorer, expand **SQL Server Agent** > **Jobs**.
   c. Right-click and disable the following jobs:
      - Websense_ETL_Job_wslogdb70
      - Websense_IBT_DRIVER_wslogdb70
      - Websense_Mantenance_Job_wslogdb70

   Disabling the jobs prevents them from executing at the next scheduled time. Make sure all jobs have completed any current operation before proceeding with upgrade.
4. Perform the upgrade of Web Security or Web Filter.
5. After upgrade, enable the disabled jobs to resume normal database operations.

## Changes to integration products

The Websense v7.6 filtering plug-in for Citrix Presentation Server has been redesigned. Earlier Citrix plug-ins *must be removed* before you upgrade Websense components, then reinstalled after the upgrade is complete.

- *Citrix Integration*, page 167

If you plan to modify or upgrade other integration products, it is a best practice to make the change before upgrading Websense software. For more information, see:

- *Check Point Integration*, page 285
- *Cisco Integration*, page 193
- *Squid Web Proxy Cache Integration*, page 259
- *Universal Integrations*, page 323

## Websense Master Database updated

The Websense Master Database is removed when you upgrade. Websense Filtering Service downloads a new Master Database after the upgrade is completed.

## All traffic permitted or blocked during upgrade

If Websense Web Filter or Web Security is integrated with another product or device all traffic is either unfiltered and permitted, or completely blocked during the upgrade, depending on how your integration product is configured to respond when Websense filtering is unavailable.

When you upgrade a stand-alone installation of Web Filter or Web Security, filtering stops when Websense services are stopped. Users have unfiltered access to the Internet until the Websense services are restarted.

## Relocating components

If you want to move any Websense component in your deployment to a different machine, it is a best practice to do so before upgrading.

Remove the component and then install it on the new machine,**using the installer for the component version**. See the Websense Web Security and Websense Web Filter *Installation Guide,* for your version, for instructions.

**Important**

When moving components, make sure the associated Websense Policy Server is running. Policy Server keeps track of the location of components in a deployment. See the *Installation Guide*, for your version, for more information.

Once components are distributed to their final locations, run the new version installer on each machine to upgrade the components to the new version. See *Upgrade instructions (Windows)*, page 842.

## Log Server using trusted connection

If you are upgrading Websense Log Server and it uses a Windows trusted connection to access the Log Database, you must log on to this machine with the same trusted account before running the Websense installer to perform the upgrade.

Use the Windows **Services** dialog box to find which account is used by Log Server:

a. Start the Windows **Services** dialog box (typically, **Start** > **Administrative Tools** > **Services**).

b. View the **Log On As** column entry for Websense Log Server. This is the account you should use.

## Functioning deployments only

The upgrade process is designed for a properly functioning deployment of Websense software. Upgrading does not repair a non-functional system.

## Version 6.x Audit Log

If you must perform an intermediate upgrade (see *Versions supported for upgrade*, page 830) from version 6.3.2 to 7.1, be aware that the Audit Log for the version 6.3.2 installation will not carry across to version 7.1. To preserve your 6.x Audit Log, use Websense Manager to export the log to a tab-separated text file prior to upgrading. Then, move the exported file to a directory that will not be affected by the upgrade

(i.e., outside the Websense installation directory: C:\Program Files\Websense or /opt/Websense, by default).

> **Note**
> If you upgraded to version 7.1 without exporting the 6.x Audit Log, you may still be able to retrieve it. Search the Websense Knowledge Base (www.websense.com/support) for the terms *Upgrading from v6.x does not preserve the audit log*.

## Previous version configuration files

Do not install version 7.5 Websense software on a separate machine and then copy a previous version's configuration files to that machine.

## Non-English language versions

This version is available in English only.

## Upgrading distributed components

To upgrade Websense software, run the Websense installer on each machine running Websense components. Distributed components must be upgraded in a particular order. Start with the machine running Policy Broker.

### Upgrade order

If Web Security components are distributed across multiple machines, they must be upgraded in the following order due to dependencies between them.

1. Policy Broker
2. Policy Server
3. User Service
4. Filtering Service
5. Network Agent
6. Transparent identification agents
7. Filtering plug-in (on integration product machine)
8. Log Server
9. Websense Manager or TRITON - Web Security

If multiple components are installed on a machine, the installer upgrades them in the proper order.

## Upgrading a filtering plug-in

If your Websense software is integrated with a third-party product requiring a Websense filtering plug-in (Microsoft ISA Server or Forefront TMG, Citrix Presentation Server, or Squid Web Proxy Cache), the plug-in must be upgraded as well.

Before performing the upgrade, make sure your version of integration product is supported by the new version of Websense software. See *System Requirements*, page 41.

Run the Websense installer on the integration product machine. The installer detects Websense integration-specific components and upgrades them.

**Warning**

The Websense v7.6 filtering plug-in for Citrix Presentation Server has been redesigned. Earlier Citrix plug-ins must be removed before you upgrade Websense components, then reinstalled after the upgrade is complete.

**Important**

The filtering plug-in for Microsoft Forefront TMG is upgraded by the separate Forefront TMG plug-in installer. See *Installing the ISAPI Filter plug-in for Forefront TMG*, page 234.

**Note**

If you are changing your integrated firewall, proxy server, caching application, or network appliance, modify that product before upgrading Websense software.

## Websense services must be running

Websense services must be running when the upgrade process begins. The installer stops and starts these services during the upgrade.

If these services have been running uninterrupted for several months, the installer may not be able to stop them before the upgrade process times out.

To ensure the success of the upgrade, manually stop and start all the Websense services before beginning the upgrade. See *Starting or Stopping Web Security Services*, page 923 for instructions.

**Important**

In the Windows Services dialog box, if you have set the **Recovery** properties of any of the Websense services to restart the service on failure, you must change this setting to **Take No Action** before upgrading.

## Matching locales

When upgrading Websense Filtering Service installed on a machine separate from Websense Manager (v7.1) or TRITON - Web Security (v7.5), you must upgrade Filtering Service in the same locale environment (language and character set) as Websense Manager/TRITON - Web Security.

- Before upgrading Filtering Service on Windows, open **Control Panel** > **Regional Options**, and change the locale to match that of the Websense Manager/TRITON - Web Security machine.
- When upgrading on Linux, log on to the Filtering Service machine with the locale appropriate to Websense Manager/TRITON - Web Security.

After the upgrade is complete, Websense services can be restarted with any locale setting.

# Upgrade instructions (Windows)

## Applies to

- Web Filter v7.1, v7.5, v7.6
- Web Security v7.1, v7.5, v7.6
- Web Security Gateway v7.1, v7.5, v7.6

## Upgrade instructions

The version 7.6 Websense installer is also used for upgrades. After it starts, the installer detects when older version components are installed. The installer also detects which Websense components are installed and need to be upgraded, and

checks the version of the database management system to ensure it is compatible with the new version of Websense software.

**Warning**

If you are using the Websense filtering plug-in for Citrix Presentation Server, you must remove it before beginning this upgrade procedure, then reinstall it after the upgrade is complete. Use the Citrix endpoint package to do so, not the v7.6 Websense installer.

**Important**

Filtering and logging services are not available while running the upgrade. To reduce the impact on network users, run the upgrade after hours, or during a quiet time on the network.

Perform the following procedure on each machine running Websense Web Security components.

1. If you performed an intermediate upgrade from version 6.3.2 to 7.1, and you have not done so yet, reboot the machine before upgrading from version 7.1 to 7.6.
2. Close all instances of Websense Manager (v7.1) or TRITON - Web Security (v7.5).

   **Important**

   If Websense components are installed on multiple machines, see *Upgrade order*, page 840 for important information about the required upgrade sequence. All components that interact in a deployment must be upgraded to the same version.

3. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

   If you are upgrading User Service, DC Agent, or Logon Agent, this ensures that those components have administrator privileges on the domain.

   **Important**

   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account. See *Log Server using trusted connection*, page 839.

4. Perform a full system backup. See *Backing up files*, page 834.
5. Stop Log Server and disable SQL Server Agent jobs.

See *Preparing SQL Server for upgrade*, page 837.

6. Close all applications and stop any antivirus software.

   **Warning**
   Be sure to close the Windows Event Viewer, or the upgrade may fail.

7. Configure current Web Security network administrators to be authenticated against a version 7.6-supported directory service if necessary. See *Upgrading or Merging Administrators*, page 917 for more information.

   **Note**
   In version 7.6, the **WebsenseAdministrator** account is replaced by an **admin** account. See *Upgrading or Merging Administrators*, page 917 for more information.

8. Download the Websense installer. See *Websense installer*, page 57 for instructions.
9. Double-click **WebsenseTRITON76Setup.exe** to launch the Websense installer.

   A progress dialog box appears, as files are extracted.

10. The installer detects Web Security components from an earlier version and asks how you want to proceed:

    *An older version of Web Security is installed on this machine. Press OK to upgrade it or Cancel to exit the installation.*

    Click **OK** to proceed.

11. If Websense Manager (v7.1) or TRITON - Web Security (v7.5) is installed on this machine:

    The following message appears:

    *Keep TRITON - Web Security on this machine and upgrade it to version 7.6 TRITON Unified Security Center?*

    *Selecting No will launch the current-version uninstaller. Uninstall the current-version TRITON - Web Security. After uninstall, remaining components will be upgraded to version 7.6.*

    See *Deciding location of Web Security Manager*, page 833 for more information.

    - If you click **Yes**:

      The **Installer Dashboard** appears and then TRITON Infrastructure Setup starts. See *Installing TRITON Infrastructure* for instructions. Return to these instructions once TRITON Infrastructure installation is complete.

    - If you click **No**:

The current version Web Security uninstaller is started automatically. See the Websense Technical Library (www.websense.com/library) for uninstallation instructions for your version. Be sure to select only Websense Manager (v7.1) or TRITON - Web Security (v7.5) for removal. After unistallation, the v7.6 Web Security component installer is started automatically.

12. On the (Websense Web Security/Web Filter v7.6 Installer) **Introduction** screen, click Next.

    Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

13. On the **Websense Upgrade** screen, select **Start the upgrade** and then click Next.

    **Important**

    Be sure to close all instances of TRITON - Web Security (v7.5) or Websense Manager (v7.1), on all machines, before clicking **Next**.

    If the **Database Information** screen appears, stating Log Server is found on this machine and it is configured to connect to MSDE, you must install SQL Server 2008 R2 Express (SQL Server Express) and then configure Log Server to connect to it before Log Server can be upgraded. Click **Cancel**, and then **Quit**. You are returned to the **Modify Installation Dashboard**. Install SQL Server Express either on this machine or another machine. It is possible to install SQL Server Express on the same machine currently running MSDE. See *Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)*, page 704 for instructions.

    Once SQL Server Express has been installed (and, optionally, MSDE data restored or attached to it). Run the Websense installer again on this machine (the one running Log Server) to upgrade components.

14. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

    The **Pre-Upgrade Summary** screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the Windows Service dialog box to stop the services. See *Starting or Stopping Web Security Services*, page 923 for instructions. Once you have manually stopped the services, return to the installer.

15. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Install**.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.

16. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.

17. Reboot the machine.

    **Important**
    The machine must be rebooted to complete the upgrade process.

18. If you stopped your antivirus software, restart it.
19. Re-enable SQL Server Agent jobs if you disabled them prior to upgrade.

    See *Preparing SQL Server for upgrade*, page 837.
20. If you have an integration product installed, additional upgrade steps may be necessary. See:
    - *Check Point Integration*, page 285
    - *Cisco Integration*, page 193
    - *Citrix Integration*, page 167
    - *Squid Web Proxy Cache Integration*, page 259
    - *Universal Integrations*, page 323
21. Repeat the upgrade procedure on each machine running Web Security components, in the recommended order (see *Upgrade order*, page 840).

    All components that interact must be upgraded to the same version.

    If you have complete installations in separate locations that do not interact, they do not have to run the same Websense software version.

# Upgrade instructions (Linux)

## Applies to

- Web Filter v7.1, v7.5, v7.6
- Web Security v7.1, v7.5, v7.6
- Web Security Gateway v7.1, v7.5, v7.6

## Upgrade instructions

The version 7.6 Web Security Linux installer is used for upgrades. After it starts, the installer detects when older version components are installed. The installer also detects which Websense components are installed and need to be upgraded.

**Important**

Filtering and logging services are not available while running the upgrade. To reduce the impact on network users, run the upgrade after hours, or during a quiet time on the network.

Perform the following procedure on each machine running Websense Web Security components.

**Important**

If Websense components are installed on multiple machines, see *Upgrade order*, page 840 for important information about the required upgrade sequence. All components that interact in a deployment must be upgraded to the same version.

1. Close all instances of Websense Manager (v7.1) or TRITON - Web Security (v7.5).
2. Log on the installation machine with administrator privileges (typically, as **root**)

   If you are upgrading User Service or Logon Agent, this ensures that those components have administrator privileges.
3. Perform a full system backup. See *Backing up files*, page 834.
4. Close all applications and stop any antivirus software.
5. Check the **etc/hosts** file. If there is no host name for the machine, add one.

   See the *Hostname*, page 63 for instructions.
6. Create a setup directory for the installer files, such as **/root/Websense_setup**.

**Important**

If your Websense services have been running uninterrupted for several months, the installer may have difficulty stopping them.

To prevent the upgrade process from timing out and failing, stop the services manually and start them again before beginning the upgrade. For instructions, see *Starting or Stopping Web Security Services*, page 923.

7. Download and start the Web Security Linux installer. See *Starting the Web Security Linux installer*, page 330 for instructions.

   **Important**

   If Websense components are installed on multiple machines, see *Upgrade order*, page 840 for important information about the required upgrade sequence. All components that interact in a deployment must be upgraded to the same version.

8. On the **Introduction** screen, click Next.

   **Note**

   These instructions refer to installer screens. In the command-line Linux installer, prompts are displayed that correspond to each screen. Instructions for a screen also apply to the corresponding command-line prompt. The main difference is how options are selected. Rather than clicking items in a screen, you will enter menu-item numbers or characters.

9. On the **Subscription Agreement** screen, click **I accept the terms of the Subscription Agreement** and click Next.
10. If Websense Manager (v7.1) or TRITON - Web Security (v7.5) is installed on this machine, the **TRITON - Web Security Disabled after Upgrade** screen appears. Click **Next** to proceed.

    In version 7.6, TRITON - Web Security must run on a Windows machine as part of the TRITON Unified Security Center.
11. On the **Websense Upgrade** screen, select **Start the upgrade** and then click Next.

    **Important**

    Be sure to close all instances of TRITON - Web Security (v7.5) or Websense Manager (v7.1), on all machines, before clicking **Next**.

12. When you click **Next**, a *Stopping All Services* progress message appears. Wait for Websense services to be stopped.

    The **Pre-Upgrade Summary** screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. Use the `WebsenseAdmin` command. See *Starting or Stopping Web Security Services*, page 923 for instructions. Once you have manually stopped the services, return to the installer.

13. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Install**.

    **Note**
    TRITON - Web Security may appear in the list of components to be upgraded. However, it will not be upgraded. It will be disabled.

    Critical files are backed up and install properties initialized. And then the **Installing Websense** screen appears.

14. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
15. Reboot the machine.

    **Important**
    The machine must be rebooted to complete the upgrade process.

16. If you stopped your antivirus software, restart it.
17. If you have an integration product installed, additional upgrade steps may be necessary. See:
    - *Check Point Integration*, page 285
    - *Cisco Integration*, page 193
    - *Citrix Integration*, page 167
    - *Squid Web Proxy Cache Integration*, page 259
    - *Universal Integrations*, page 323
18. Repeat the upgrade procedure on each machine running Web Security components, in the recommended order (see *Upgrade order*, page 840).

    All components that interact must be upgraded to the same version.

    If you have complete installations in separate locations that do not interact, they do not have to run the same Websense software version.
19. After all components have been upgraded, see*Initial Configuration*, page 763. Be sure to reset specific custom values if you are *Upgrading from v7.1.1*.

# Adding Web Security components during upgrade

## Applies to

- Web Filter v7.1, v7.5, v7.6
- Web Security v7.1, v7.5, v7.6
- Web Security Gateway v7.1, v7.5, v7.6

### Adding Web Security components during upgrade

To add components to a machine on which Websense components are already installed, first upgrade the pre-existing components (see *Upgrade instructions (Windows)*, page 842 or *Upgrade instructions (Linux)*, page 846). The first time you run the Websense installer, it will upgrade the existing components. After upgrading, run the Websense installer again on the same machine. This time, the installer will ask if you want to add components. See *Adding or Modifying Components*, page 791.

## Changing IP addresses of Web Security components after upgrade

### Applies to

- Web Filter v7.1, v7.5, v7.6
- Web Security v7.1, v7.5, v7.6
- Web Security Gateway v7.1, v7.5, v7.6

### Changing IP addresses of Web Security components after upgrade

If the IP address changes for a machine running Policy Server or Policy Broker after upgrade, certain configuration files must be updated. See the instructions for changing the Policy Server IP address under the *Websense Server Administration* topic in the TRITON - Web Security Help. Use the same procedure if you change the IP address of Policy Broker (more instances of the IP address will be found in the files being updated).

Websense Web Security software handles IP address changes in the background for most other components, without any interruption to filtering.

In some cases, Websense services need to be restarted or configurations updated after changing an IP address.

Network Agent settings can be updated in TRITON - Web Security. See the TRITON - Web Security Help for more information.

## New security certificate

### Applies to

- Web Filter v7.1, v7.5, v7.6

- Web Security v7.1, v7.5, v7.6
- Web Security Gateway v7.1, v7.5, v7.6

## New security certificate

After upgrade, you must install or permanently accept a new security certificate issued by Websense, Inc. to avoid seeing a certificate error when you first launch TRITON Unified Security Center. The prior-version certificate (accepted when accessing TRITON - Web Security or - Data Security) is no longer valid.

An SSL connection is used for secure, browser-based communication with TRITON Unified Security Center. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch TRITON Unified Security Center from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser. See the *Websense Knowledge Base* for instructions.

# 52 Upgrading Websense Content Gateway to 7.6.0

## Applies to

- Content Gateway v7.5, v7.6.0
- Web Security Gateway v7.5, v7.6.0

## In this topic



## Overview

This section of the Websense Technical Library covers upgrading software-based Websense Content Gateway installations (i.e., not running on a Websense appliance).

Perform an upgrade by running the Content Gateway installer on a machine with a previous version of Content Gateway installed. The installer detects the presence of Content Gateway and upgrades it to the current version.

**Important**
The installation location of Content Gateway is made uniform in 7.6. The default location, /opt/WCG, is the actual location of every 7.6 installation post-upgrade. The upgrade process detects installations in other locations and moves the installation to /opt/WCG.

**Important:**
In 7.6, in **explicit proxy deployments**, when HTTPS (SSL Manager) is enabled, PAC files and browsers must be configured to send HTTPS traffic to Content Gateway on port 8080. The **ipnat.config** rule that was used in previous releases to redirect traffic from 8070 to 8080 has been removed.

**Note**
Technical papers and documents mentioned in this article are available Websense Technical Library: www.websense.com/library.

## Versions supported for upgrade

Direct upgrades to version 7.6 are supported from version 7.5 and higher of Content Gateway.

Upgrades from versions prior to 7.5 require intermediate upgrades:

- version 7.0 > version 7.1 > version 7.5 > version 7.6

**Important**
The upgrade from version 7.1 to 7.5 requires a Red Hat Enterprise Linux operating system version upgrade followed by a fresh install of 7.5.

Follow the upgrade procedures documented with each intermediate version. To perform an intermediate upgrade, download the installer package for the intermediate version from the Websense Downloads site:

www.websense.com/MyWebsense/Downloads/

**Important**

When performing intermediate upgrades, be sure to read the Websense Content Gateway Installation Guide and its upgrade supplement for each upgrade version. They contain important information specific to upgrading between particular versions that may not be found in this version of the upgrade supplement.

## Upgrading from version 7.5.3

Due to the timing of Content Gateway releases 7.5.3 and 7.6.0, a small number of 7.5.3 corrections could not be included in 7.6.0. These include:

- Hotix 1 - NTLM: prompt for credentials when user is outside configured domain
- Portions of hotfix 6 - proxy chaining; LDAP authentication; mobile users
- Hotfixes after hotfix 6 (none as of commercial release of 7.6)

# Preparing for the upgrade



## System requirements

Before upgrading Content Gateway, make sure the installation machine meets the system recommendations in *System requirements for Websense Content Gateway*, page 366, including hardware specifications, operating system, and browser.

## Preparing for installation

Summary:

- Read the Websense Content Gateway v7.6 Release Notes **and** these upgrade instructions
- Upgrade TRITON Unified Security Center and TRITON - Web Security before upgrading Content Gateway. See *Upgrading Web Security or Web Filter to 7.6.0*, page 829.
- If upgrading Red Hat Enterprise Linux, upgrade the operating system before upgrading Content Gateway. The Content Gateway installer installs a version of ARM that is compatible with the current Red Hat kernel version.

- If configured, disable Virtual IP failover and leave it disabled until all members of the cluster are upgraded and clustering has been re-enabled.
- If configured, disable clustering and leave clustering disabled until all members of the cluster are upgraded. All cluster members must run the same version of Content Gateway and should, therefore, be upgraded at the same time. When all nodes are upgraded, re-enable clustering and restart Content Gateway (restarting any node causes all nodes to restart).

## Deprecated in 7.6

These features are deprecated in version 7.6:

- WCCP v1.
- Full clustering. See the entry for Full clustering in *Configuration settings not preserved*, below
- FTP caching. If FTP caching was enabled in your 7.5 configuration, it is disabled during upgrade. The configuration option is removed from 7.6 Content Gateway Manager.
- ARM Security. If ARM Security was enabled in your 7.5 configuration, it is disabled during upgrade. The configuration option is removed from 7.6 Content Gateway Manager.
- Congestion Control. If Congestion Control was enabled in your 7.5 configuration, it is disabled during upgrade. The configuration option is removed from 7.6 Content Gateway Manager.
- ICP Peering. If ICP Peering was enabled in your 7.5 configuration, it is disabled during upgrade. The configuration option is removed from 7.6 Content Gateway Manager.

## Configuration settings not preserved

The following configuration settings are **not** preserved and must be reconfigured post-upgrade:

- Proxy user authentication and access control filter (filter.config) configuration settings are not retained. These include:
  - LDAP, RADIUS, NTLM, and multiple realm rules
  - All filtering rules (filter.config)

  Multiple authentication methods with multiple authentication realms is expanded in version 7.6 and made more powerful with the addition of Integrated Windows Authentication. Multiple authentication realm rules used in 7.5 deployments must be recreated after upgrading to 7.6. Also, if NTLM was configured in 7.5, consider moving to Integrated Windows Authentication.

  Before upgrading, be prepared to reconfigure user authentication options and proxy filtering rules (often used to bypass authentication). It is recommended that a copy of your 7.5 filter.config file be copied to a safe location for future reference.

### New features to configure after upgrade

You may want to configure these new and enhanced features post-upgrade (for more information, see the Release Notes):

- Explicit proxy deployments can configure multiple inbound ports.
- Transparent proxy deployments with WCCP have more configuration options.
- Integrated Windows Authentication (with Kerberos) provides more robust proxy user authentication with Windows Active Directory. If NTLM was a user authentication method in version 7.5, consider moving to Integrated Windows Authentication.
- Multiple Realm Authentication is enhanced and now supports multiple authentication rules for multiple authentication realms.
- Full clustering is deprecated in version 7.6. Multiple installations of Content Gateway can no longer form a single logical cache. During upgrade, Full clusters are automatically converted to Managed clusters (no reconfiguration is necessary). Managed clusters share configuration settings among nodes.
- For deployments that use SSL Manager, SSL clustering is added to share SSL Manager settings among nodes in a cluster. It is configured separately from Managed clustering.

## Upgrading distributed components

Websense Content Gateway is the Web proxy component of Websense Web Security Gateway and Websense Web Security Gateway Anywhere. Websense Web Security components must be upgraded prior to upgrading Content Gateway. To upgrade Websense Web Security, run the Websense installer on each machine running Websense Web Security components. Distributed components must be upgraded in a particular order. See Websense Web Security and Websense Web Filter <BN-BookName>Installation Guide.

# Upgrading Websense Content Gateway

Complete these steps to upgrade Content Gateway on a server in a software-base deployment.

In a Websense-appliance-based deployment, Content Gateway is upgraded when the 7.6 patch is applied.

Before you begin, be sure to read *Preparing to install Websense Content Gateway*, page 361.

**Warning**

*Before you begin*, ensure that **/tmp** has enough free space to hold the existing Content Gateway log files. During the upgrade procedure, the installer temporarily copies log files located in **/opt/WCG/logs** to **/tmp**. If the **/tmp** partition does not have enough available space and becomes full, the upgrade will fail.

If you determine that **/tmp** does not have enough space, manually move the contents of **/opt/WCG/logs** to a partition that has enough space and then delete the log files in **/opt/WCG/logs**. Run the installer to perform the upgrade. When the upgrade is complete, move the log files from the temporary location back to **/opt/WCG/logs** and delete the files in the temporary location.

For step-by-step instructions, see the Knowledge Base article titled *Upgrading can fail if the /tmp partition becomes full*.

**Also:** Snapshots saved in**/opt/WCG/config/snapshots** are not saved during the upgrade procedure. To preserve your snapshots, manually copy them to a temporary location and copy them back after the upgrade is complete.

**Note: /opt/WCG** is the version 7.6 installation location.

**Important**

If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for:

```
/opt/WCG/config/internal/no_cop
```

If the file exists, remove it and restart Content Gateway:

```
/opt/WCG/WCGAdmin start
```

1. To upgrade to Websense Content Gateway version 7.6, start by downloading the installer. Go to: www.websense.com/MyWebsense/Downloads/

2. Disable any currently running firewall on this machine for the duration of the Content Gateway upgrade. Bring the firewall back up after upgrade is complete, opening ports used by Content Gateway.

   For example, if you are running IPTables:

   a. At a command prompt, enter **service iptables status** to determine if the firewall is running.

b. If the firewall is running, enter **service iptables stop**.

c. After upgrade, restart the firewall. In the firewall, be sure to open the ports used by Content Gateway on this machine. See *Ports*, page 362 for more information.

3. Unpack the Content Gateway installer tar archive:

   ```
   tar -xvzf <installer tar archive>
   ```

   > **Important**
   > If SELinux is enabled, set it to permissive, or disable it before installing Content Gateway. Do not install or run Content Gateway with SELinux enabled.

4. Make sure you have root permissions:

   ```
   su root
   ```

5. In the directory where you unpacked the tar archive, begin the upgrade, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

   The installer will upgrade and, if necessary, move Content Gateway to **/opt/WCG**. It is installed as **root**.

   > **Note**
   > Up to the point that you are prompted to confirm your desire to upgrade, you can quit the installer by pressing CTRL+C. If you change your mind after you choose to continue, do **not** use CTRL+C to stop the process. Instead, allow the installation to complete and then uninstall it.

6. If your system does not meet the minimum recommended requirements, you receive a warning. For example:

   ```
   Warning: Websense Content Gateway requires at least 2
   gigabytes of RAM.

   Do you wish to continue [y/n]?
   ```

   Enter **n** to quit the installer, and return to the system prompt.

   Enter **y** to continue the upgrade. If you choose to run Content Gateway after receiving this warning, performance may be affected.

7. Read the subscription agreement. At the following prompt, enter **y** to continue the upgrade or **n** to cancel.

   ```
   Do you accept the above agreement [y/n]? y
   ```

8. When asked, choose to replace the existing version of Content Gateway with the 7.6 version.

   ```
   WCG version 7.5.0-nnnn was found.
   Do you want to replace it with version 7.6.0-nnnn [y/n]? y
   ```

9. Existing settings and logs are copied to backup files and stored. For example:

   ```
   Stopping Websense Content Gateway processes...done

   Copying settings from /opt/WCG to /root/WCG/OldVersions/
   7.5.0-1143-20110322-131541/...done

   Copying SSL Manager settings to /root/WCG/OldVersions/7.5.0-
   1143-20110322-131541/...done

   Moving log files from /opt/WCG/logs to /tmp/wcg_tmp/logs/
   ...done
   ```

10. You can either re-use the installation selections you entered during the last install, or provide new answers to all installation prompts:

    ```
    Previous install configuration </root/WCG/Current/
    WCGinstall.cfg> found.

    Use current installation selections [y/n]?
    ```

    Enter **y** to use previous installation selections.

    Enter **n** to revert to Websense default values, and receive all installation questions and answer them again.

11. The following message appears if Content Gateway is currently configured to use WCCP v1. Press ENTER to proceed.

    ```
    WCCP will be disabled as WCCP v1 is obsolete.> ENTER
    ```

    Only WCCP v2 is supported by Content Gateway 7.6. See Content Gateway Manager Help for information about configuring WCCP v2.

12. If you answered **y** at Step 10, then you can also leave proxy settings at their current values or revert to Websense default values.

    ```
    Restore settings after install [y/n]?
    ```

    Enter **y** to keep the proxy settings as they are.

    Enter **n** to restore Websense default settings for the proxy.

13. The previously installed version of Websense Content Gateway is removed, and the settings and selections you chose to retain are re-used. Wait.

    ```
    *COMPLETED* Websense Content Gateway 7.6.0-1166
    installation.
    A log file of this installation process has been written to
    /root/WCG/Current/WCGinstall.log
    ```

```
For full operating information, see the Websense Content
Gateway Help system.


Follow these steps to start the Websense Content Gateway
management interface (Content Gateway Manager):
------------------------------------------------------------
1. Start a browser.
2. Enter the IP address of the Websense Content Gateway
server, followed by a colon and the management interface
port (8081 for this installation). For example: https://
11.222.33.44:8081.
3. Log on using username admin and the password you chose
earlier.


A copy of the CA public key used by the Manager is located in
/root/WCG/.
```

14. The upgrade is now complete, and the proxy software is running.

    If you chose to revert to Websense default proxy settings, be sure to configure any custom options.

15. If you answered **n** at Step 10, the current version of Websense Content Gateway is removed, and a fresh install of 7.6 begins. See *Installing Websense Content Gateway*, page 372, for a detailed description of the installation procedure.

16. Check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

    All services should be running. These include:

    Content Cop

    Websense Content Gateway

    Content Gateway Manager

    Websense Download Service

    Analytics Server

    **Important**

    If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for:

    ```
    /opt/WCG/config/internal/no_cop
    ```

    If the file exists, remove it and restart Content Gateway:

    ```
    /opt/WCG/WCGAdmin start
    ```

17. Perform the post-installation steps described in *Post upgrade activities*, page 862, and in *Initial Configuration*, page 763.

# Post upgrade activities

In version 7.6, when using Content Gateway with TRITON - Web Security it is not necessary to enter a subscription key. The key is automatically fetched from TRITON - Web Security.

1. If at the start of the upgrade process you manually moved your existing log files to a temporary location, move them back to **/opt/WCG/logs** and delete the files in the temporary location.

2. If at the start of the upgrade procedure you manually moved your existing snapshot files to a temporary location, copy them back to **/opt/WCG/config/snapshots** and delete them from the temporary location.

3. Register Content Gateway nodes in TRITON - Web Security on the **Settings > Content Gateway Access** page. Registered nodes add a link to the Content Gateway Manager logon portal and provide a visual system health indicator, a green check mark or a red X icon.

4. Configure Content Gateway system alerts in TRITON - Web Security. Select Content Gateway system alerts are now sent to TRITON - Web Security (in addition to Content Gateway Manager). To configure which alerts are sent, in TRITON - Web Security go to the **Settings > Alerts > System** page.

5. If WCCP v2 was your version 7.5 transparent proxy deployment, it is highly recommended that you familiarize yourself with the new features and review your configuration. See Transparent interception with WCCP v2 devices in Content Gateway Manager Help. WCCP v1 is deprecated.

6. If Content Gateway user authentication was used, it must be reconfigured. This includes LDAP, RADIUS, NTLM, and multiple realm rules. For an overview of 7.6 features, see Proxy user authentication.

   If NTLM authentication was configured, consider moving to Integrated Windows Authentication. See Integrated Windows Authentication.

   If multiple realm authentication rules were used in 7.5, you will have to become acquainted with the new feature and recreate your rules. See Multiple realm authentication.

7. If access control filtering rules (filter.config) were defined, they must be recreated. It will be helpful to work from the file you saved before upgrading, but filtering rules should be recreated in the filter.config rule editor in Content Gateway Manager. See Filtering Rules.

# 53 Upgrading Websense Content Gateway to v7.6.2

## Applies to

- Content Gateway v7.6.0, v7.6.2
- Web Security Gateway v7.6.0, v7.6.2

## In this topic



## Overview

This section of the Websense Technical Library covers upgrading software-based Websense Content Gateway installations (i.e., not running on a Websense appliance).

Perform an upgrade by running the Content Gateway installer on a machine with a previous version of Content Gateway installed. The installer detects the presence of Content Gateway and upgrades it to the current version.

**Important**
The installation location of Content Gateway is made uniform in 7.6.2. The default location, /opt/WCG, is the actual location of every 7.6.2 installation post-upgrade. The upgrade process detects installations in other locations and moves the installation to /opt/WCG.

**Important:**
In 7.6.2, in **explicit proxy deployments**, when HTTPS (SSL Manager) is enabled, PAC files and browsers must be configured to send HTTPS traffic to Content Gateway on port 8080. The **ipnat.config** rule that was used in previous releases to redirect traffic from 8070 to 8080 has been removed.

**Note**
Technical papers and documents mentioned in this article are available Websense Technical Library: www.websense.com/library.

## Versions supported for upgrade

Direct upgrades to version 7.6.2 are supported from version 7.6.0 and higher of Content Gateway.

Upgrades from versions prior to 7.6.2 require intermediate upgrades:

- version 7.0 > version 7.1 > version 7.5.x > version 7.6.0 > version 7.6.2

Follow the upgrade procedures documented with each intermediate version. To perform an intermediate upgrade, download the installer package for the intermediate version from the Websense Downloads site:

www.websense.com/MyWebsense/Downloads/

**Important**

When performing intermediate upgrades, be sure to read the Websense Content Gateway Installation Guide and its upgrade supplement for each upgrade version. They contain important information specific to upgrading between particular versions that may not be found in this version of the upgrade supplement.

# Preparing for the upgrade



## System requirements

Before upgrading Content Gateway, make sure the installation machine meets the system recommendations in *System requirements for Websense Content Gateway*, page 366, including hardware specifications, operating system, and browser.

## Preparing for installation

Summary:

- Read the Websense Content Gateway v7.6.2 Release Notes **and** these upgrade instructions
- Upgrade TRITON Unified Security Center and TRITON - Web Security before upgrading Content Gateway. See Upgrade Websense Software to v7.6.3.
- If upgrading Red Hat Enterprise Linux, upgrade the operating system before upgrading Content Gateway. The Content Gateway installer installs a version of ARM that is compatible with the current Red Hat kernel version.
- If configured, disable Virtual IP failover and leave it disabled until all members of the cluster are upgraded and clustering has been re-enabled.
- If configured, disable clustering and leave clustering disabled until all members of the cluster are upgraded. All cluster members must run the same version of Content Gateway and should, therefore, be upgraded at the same time. When all nodes are upgraded, re-enable clustering and restart Content Gateway (restarting any node causes all nodes to restart).

### New features to configure after upgrade

You may want to configure these new and enhanced features post-upgrade (for more information, see the Release Notes):

- Users can now specify domain names for all NTLM authentication attempts.
- LDAP authentication on the proxy is now compatible with passwords containing special characters.

## Upgrading distributed components

Websense Content Gateway is the Web proxy component of Websense Web Security Gateway and Websense Web Security Gateway Anywhere. Websense Web Security components must be upgraded prior to upgrading Content Gateway. To upgrade Websense Web Security, run the Websense installer on each machine running Websense Web Security components. Distributed components must be upgraded in a particular order. See Websense Web Security and Websense Web Filter Installation Guide.

# Upgrading Websense Content Gateway

Complete these steps to upgrade Content Gateway on a server in a software-based deployment.

In a Websense-appliance-based deployment, Content Gateway is upgraded when the 7.6.2 patch is applied.

Before you begin, be sure to read the Websense Content Gateway Release Notes.

**Warning**

Snapshots saved in **/opt/WCG/config/snapshots** are not saved during the upgrade procedure. To preserve your snapshots, manually copy them to a temporary location and copy them back after the upgrade is complete.

**Note: /opt/WCG** is the version 7.6.2 installation location.

**Important**

If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for:

```
/opt/WCG/config/internal/no_cop
```

If the file exists, remove it and restart Content Gateway:

```
/opt/WCG/WCGAdmin start
```

1. To upgrade to Websense Content Gateway version 7.6.2, start by downloading the installer. Go to: www.websense.com/MyWebsense/Downloads/

2. Disable any currently running firewall on this machine for the duration of the Content Gateway upgrade. Bring the firewall back up after upgrade is complete, opening ports used by Content Gateway.

   For example, if you are running IPTables:

   a. At a command prompt, enter **service iptables status** to determine if the firewall is running.

   b. If the firewall is running, enter **service iptables stop**.

   c. After upgrade, restart the firewall. In the firewall, be sure to open the ports used by Content Gateway on this machine. See *Ports*, page 362 for more information.

3. Unpack the Content Gateway installer tar archive:

   ```
   tar -xvzf <installer tar archive>
   ```

   **Important**

   If SELinux is enabled, set it to permissive, or disable it before installing Content Gateway. Do not install or run Content Gateway with SELinux enabled.

4. Make sure you have root permissions:

   ```
   su root
   ```

5. In the directory where you unpacked the tar archive, begin the upgrade, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

   The installer will upgrade and, if necessary, move Content Gateway to **/opt/WCG**. It is installed as **root**.

   **Note**

   Up to the point that you are prompted to confirm your desire to upgrade, you can quit the installer by pressing CTRL+C. If you change your mind after you choose to continue, do **not** use CTRL+C to stop the process. Instead, allow the installation to complete and then uninstall it.

6. If your system does not meet the minimum recommended requirements, you receive a warning. For example:

   ```
   Warning: Websense Content Gateway requires at least 2
   gigabytes of RAM.

   Do you wish to continue [y/n]?
   ```

Enter **n** to quit the installer, and return to the system prompt.

Enter **y** to continue the upgrade. If you choose to run Content Gateway after receiving this warning, performance may be affected.

7. Read the subscription agreement. At the following prompt, enter**y** to continue the upgrade or **n** to cancel.

   ```
   Do you accept the above agreement [y/n]? y
   ```

8. When asked, choose to replace the existing version of Content Gateway with the 7.6.2 version.

   ```
   WCG version 7.6.0-nnnn was found.
   Do you want to replace it with version 7.6.2-nnnn [y/n]? y
   ```

9. Existing settings and logs are copied to backup files and stored. For example:

   ```
   Stopping Websense Content Gateway processes...done

   Copying settings from /opt/WCG to /root/WCG/OldVersions/
   7.6.0-1185-20110905-145233/...done

   Copying SSL Manager settings to /root/WCG/OldVersions/7.6.0-
   1185-20110905-145233/...done

   Moving log files from /opt/WCG/logs to /opt/wcg_tmp/logs/
   ...done
   ```

10. You can either re-use the installation selections you entered during the last install, or provide new answers to all installation prompts:

    ```
    Previous install selections </root/WCG/Current/
    WCGinstall.cfg> found.

    Use current installation selections [y/n]?
    ```

    Enter **y** to use previous installation selections.

    Enter **n** to revert to Websense default values, and receive all installation questions and answer them again.

11. If you answered **y** at Step 10, then you can also leave proxy settings at their current values or revert to Websense default values.

    ```
    Restore settings after install [y/n]?
    ```

    Enter **y** to keep the proxy settings as they are.

    Enter **n** to restore Websense default settings for the proxy.

12. The previously installed version of Websense Content Gateway is removed, and the settings and selections you chose to retain are re-used. Wait.

    ```
    *COMPLETED* Websense Content Gateway 7.6.2-1224
    installation.
    A log file of this installation process has been written to
    /root/WCG/Current/WCGinstall.log
    ```

```
For full operating information, see the Websense Content
Gateway Help system.


Follow these steps to start the Websense Content Gateway
management interface (Content Gateway Manager):
------------------------------------------------------------
1. Start a browser.
2. Enter the IP address of the Websense Content Gateway
server, followed by a colon and the management interface
port (8081 for this installation). For example: https://
11.222.33.44:8081.
3. Log on using username admin and the password you chose
earlier.


A copy of the CA public key used by the Manager is located in
/root/WCG/.
```

13. The upgrade is now complete, and the proxy software is running.

    If you chose to revert to Websense default proxy settings, be sure to configure any custom options.

14. If you answered **n** at Step 10, the current version of Websense Content Gateway is removed, and a fresh install of 7.6.2 begins. See the Websense Content Gateway chapter of this document for a detailed description of the installation procedure.

15. Check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

    All services should be running. These include:

    Content Cop

    Websense Content Gateway

    Content Gateway Manager

    Websense Download Service

    Analytics Server

    **Important**

    If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for:

    ```
    /opt/WCG/config/internal/no_cop
    ```

    If the file exists, remove it and restart Content Gateway:

    ```
    /opt/WCG/WCGAdmin start
    ```

16. Perform the post-installation steps described in *Post upgrade activities*, page 870, and in *Initial Configuration*, page 763.

# Post upgrade activities

In version 7.6.2, when using Content Gateway with TRITON - Web Security it is not necessary to enter a subscription key. The key is automatically fetched from TRITON - Web Security.

1. If at the start of the upgrade process you manually moved your existing log files to a temporary location, move them back to **/opt/WCG/logs** and delete the files in the temporary location.

2. If at the start of the upgrade procedure you manually moved your existing snapshot files to a temporary location, copy them back to **/opt/WCG/config/snapshots** and delete them from the temporary location.

3. Register Content Gateway nodes in TRITON - Web Security on the **Settings > Content Gateway Access** page. Registered nodes add a link to the Content Gateway Manager logon portal and provide a visual system health indicator, a green check mark or a red X icon.

4. Configure Content Gateway system alerts in TRITON - Web Security. Select Content Gateway system alerts are now sent to TRITON - Web Security (in addition to Content Gateway Manager). To configure which alerts are sent, in TRITON - Web Security go to the **Settings > Alerts > System** page.

5. If Content Gateway user authentication was used, it must be reconfigured. This includes LDAP, RADIUS, NTLM, and multiple realm rules. For an overview of 7.6.x features, see Proxy user authentication.

   If NTLM authentication was configured, consider moving to Integrated Windows Authentication. See Integrated Windows Authentication.

6. If access control filtering rules (filter.config) were defined, they must be recreated. It will be helpful to work from the file you saved before upgrading, but filtering rules should be recreated in the filter.config rule editor in Content Gateway Manager. See Filtering Rules.

# 54 Upgrading to Websense Web Security Gateway Anywhere to v7.6.0

## Applies to

- Web Security Gateway Anywhere v7.5, v7.6.0

## In this topic



## Versions supported for upgrade

Direct upgrades to version 7.6 are supported from version 7.5 Websense Web Security Gateway Anywhere.

## TRITON Unified Security Center

Version 7.6 centralizes management of all Websense solutions into the TRITON Unified Security Center. TRITON - Web Security and - Data Security are now modules of the TRITON Unified Security Center.

Because both the TRITON - Web Security and - Data Security modules are required for Web Security Gateway Anywhere, TRITON Unified Security Center must be installed on a Windows Server 2008 R2 machine. As part of the upgrade process, you will remove the prior-version TRITON - Web Security, TRITON - Data Security, and Data Security Management Server from their current locations and install them on them the Windows Server 2008 R2 machine as part of the TRITON Unified Security Center.

# Upgrade instructions (software-based)

This section describes how to upgrade a software-based deployment of Web Security Gateway Anywhere from v7.5 to v7.6. For information on how to upgrade Web Security software to v7.6.2, refer to *Upgrading Websense software to the latest v7.6.x*, page 821.

Prior to upgrade, see *Upgrading or Merging Administrators*, page 917 for important information about how administrator accounts are handled by the upgrade process.

1. Configure current Web Security network administrators to be authenticated against a version 7.6-supported directory service if necssary. See *Upgrading or Merging Administrators*, page 917 for more information.
2. Upgrade Web Security components.

   See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.

   **Important**

   When upgrading Web Security components be sure to choose to remove the prior-version TRITON - Web Security from its machine. For version 7.6 both TRITON - Web Security and - Data Security must run on the same Windows Server 2008 R2 machine as part of the TRITON Unified Security Center.

3. On a Windows Server 2008 R2 machine, create a TRITON management server, installing only the Web Security module of the TRITON Unified Security Center. This machine is referred to as the ***unified TRITON management server*** in the steps below. You will "migrate" Data Security Management Server to this machine later in this procedure.

   See *Creating a TRITON Management Server*, page 645. When following those instructions, be sure to do the following:

   - On the **Installation Type** screen: under TRITON Unified Security Center, select only **Web Security**.
   - In the Web Security installer, on the *Policy Server Connection Screen*, be sure to specify the main Policy Server you upgraded in Step 2 above.

   When you have completed the procedure(s) in *Creating a TRITON Management Server*, page 645, return to these instructions.
4. Log in to the TRITON Unified Security Center on the newly-created unfied TRITON management server and assign email addresses to the Web Security local administrator accounts upgraded from the prior-version system. See *Upgrading or Merging Administrators*, page 917 for more information.
5. Upgrade Data Security components.

   See *Upgrading to Data Security 7.6.0*, page 879 for instructions. Upgrade all Data Security components, including Data Security Management Server. This creates a version 7.6 TRITON Unified Security Center, with Data Security module enabled. This machine is referred to as the ***Data Security TRITON management server*** in

remaining steps below. You will back up and then remove components from this machine later in this procedure.

6. On the Data Security TRITON management server (seeStep 5) back up **TRITON** data in the TRITON Unified Security Center running on that machine.

   See the TRITON Unified Security Center Help for instructions.

7. On the Data Security TRITON management server, back up**Data Security** data in the TRITON Unified Security Center running on that machine.

   See the TRITON - Data Security Help for instructions.

8. On the unified TRITON management server (seeStep 3) restore the TRITON data backup from the Data Security machine:

   a. Start the Websense installer.

      See *Starting the Websense installer*, page 57.

   b. In the installer, for TRITON Infrastructure, select the **Modify** link.

   c. Accept the defaults in the installer screens and click **Next**, until you reach the **Restore Data from Backup** screen.

   d. On the **Restore Data from Backup** screen, select **Use backup data** and **Browse** to the location of the TRITON data backup from the Data Security machine.

      **Note**
      If the backup is located on another machine, map a network drive to its location. Otherwise, you will be unable to select it in when you click **Browse**.

   e. Select **Merge administrators into existing installations (do not overwrite)**.

   f. Click **Next**.

      If the following message appears, click **Yes** to proceed:

      *The backup located at <path> is from the same release but from a different build (n). Proceed?*

      Build differences do not affect restoration of the backup. Click **Yes** to continue with restoring the backup.

   g. Proceed through the remaining installer screens, accepting defaults, and click **Finish**.

9. Add Data Security Server to the unified TRITON management server.

   See *Installing Data Security Components*, page 692 for instructions.

10. Restore the Data Security backup you created on the Data Security TRITON management server (in Step 7).

    See *Adding or modifying Data Security components*, page 796for instructions. As you follow those instructions, when you reach the **Restore Data From Backup** screen, be sure to choose to restore the backup you created in Step 7. See the TRITON - Data Security Help for more information.

11. Log into the unified TRITON Unified Security Center. In the Data Security module, click **Deploy**.

See *Accessing the TRITON Unified Security Center*, page 765 for instructions.

12. Remove Data Security components from the Data Security TRITON Unified Security machine.

    See *Removing Data Security components*, page 816 for instructions. Return here when done.

13. Remove TRITON Infrastructure from the Data Security TRITON management server.

    See *Removing TRITON Infrastructure*, page 806 for instructions. Return here when done.

14. Upgrade Content Gateway.

    See *Upgrading Websense Content Gateway to 7.6.0*, page 853.

## Upgrade instructions (appliance-based)

Complete the following steps to upgrade an appliance-based deployment of Web Security Gateway Anywhere from v7.5 to v7.6.

Prior to upgrade, see *Upgrading or Merging Administrators*, page 917 for important information about how administrator accounts are handled by the upgrade process.

1. Configure current Web Security network administrators to be authenticated against a version 7.6-supported directory service if necssary. See *Upgrading or Merging Administrators*, page 917 for more information.
2. If Policy Broker and Policy Server are running off-appliance, upgrade them now.

   See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions. Do not upgrade any other off-appliance components at this point.
3. Upgrade the V-series appliances in your deployment.

   See *Upgrading V-Series Appliance to 7.6*, page 907 for instructions.
4. Upgrade off-appliance Web Security components.

   See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.

   **Important**

   When upgrading Web Security components be sure to choose to remove the prior-version TRITON - Web Security from its machine if it is located off-appliance. For version 7.6 both TRITON - Web Security and - Data Security must run on the same Windows Server 2008 R2 machine as part of the TRITON Unified Security Center.

5. If TRITON - Web Security is running on an appliance, disable it:
   a. Log on to the Appliance Manager (https://<*C interface IP address*>:9447/appmng)
   b. Under **Configuration**, select **Web Security Components**.

c. Under **TRITON - Web Security**, select **Disabled**.

d. Click **Save**.

The disabling process may take several minutes. Wait for it to complete.

e. When the process completes successfully, click the *TRITON Configuration* link that is displayed below the **Disabled** option.

If a certificate error is displayed, click the continue or accept option to start the download.

f. Save the TRITON backup file (**EIP_bak.tgz**) in a convenient location. The file will be used to restore your settings to the unified TRITON management server (which you will create in Step 6).

6. On a Windows Server 2008 R2 machine, create a TRITON management server, installing only the Web Security module of the TRITON Unified Security Center. This machine is referred to as the ***unified TRITON management server*** in the steps below. You will "migrate" Data Security Management Server to this machine later in this procedure.

See *Creating a TRITON Management Server*, page 645 for instructions.
**Important**: Before going to those instructions read the following; they are specific options you should select during the creation of a TRITON management server:

a. In the Websense installer, on the **Installation Type** screen, under TRITON Unified Security Center, select only **Web Security**.

b. In the Web Security installer, on the*Policy Server Connection Screen*, be sure to specify the main Policy Server you upgraded inStep 2 or Step 3 (depending on the location of the main Policy Server) above.

7. Restore the TRITON backup from the appliance:

a. Use a utility like 7-Zip to extract and unpack the contents of the appliance TRITON backup file to a temporary directory on this machine. When the process is complete, you should have a directory called **EIP_bak** that contains, among other files, **EIP.db** and **httpd-data.txt**, as well as **apache** and **tomcat** folders.

b. Start the Websense installer.

See *Starting the Websense installer*, page 57.

c. In the installer, for TRITON Infrastructure, select the **Modify** link.

d. Accept the defaults in the installer screens and click **Next**, until you reach the **Restore Data from Backup** screen.

e. On the **Restore Data from Backup** screen, select **Use backup data** and **Browse** to the location of the TRITON data backup from the Data Security machine.

> **Note**
> If the backup is located on another machine, map a network drive to its location. Otherwise, you will be unable to select it in when you click **Browse**.

f. Select **Merge administrators into existing installations (do not overwrite)**.

g. Click **Next**.

If the following message appears, click **Yes** to proceed:

*The backup located at <path> is from the same release but from a different build (n). Proceed?*

Build differences do not affect restoration of the backup. Click **Yes** to continue with restoring the backup.

h. Proceed through the remaining installer screens, accepting defaults, and click **Finish**.

8. Log in to the TRITON Unified Security Center on the newly-created unfied TRITON management server and assign email addresses to the Web Security local administrator accounts upgraded from the prior-version system. See*Upgrading or Merging Administrators*, page 917 for more information.

9. Upgrade Data Security components.

See *Upgrading to Data Security 7.6.0*, page 879 for instructions. Upgrade all Data Security components, including Data Security Management Server. This creates a version 7.6 TRITON Unified Security Center, with Data Security module enabled. This machine is referred to as the ***Data Security TRITON management server*** in remaining steps below. You will back up and then remove components from this machine later in this procedure.

10. On the Data Security TRITON management server (seeStep 9) back up **TRITON** data in the TRITON Unified Security Center running on that machine.

See the TRITON Unified Security Center Help for instructions.

11. On the Data Security TRITON management server, back up**Data Security** data in the TRITON Unified Security Center running on that machine.

See the TRITON - Data Security Help for instructions.

12. On the unified TRITON management server (seeStep 6) restore the TRITON data backup from the Data Security machine.

See the TRITON Unified Security Center Help for instructions.

13. Add Data Security Server to the unified TRITON management server.

See *Installing Data Security Components*, page 692 for instructions.

14. Restore the Data Security backup you created on the Data Security TRITON management server (in Step 10).

See *Adding or modifying Data Security components*, page 796for instructions. As you follow those instructions, when you reach the **Restore Data From Backup** screen, be sure to choose to restore the backup you created in Step 10. See the TRITON - Data Security Help for more information.

15. Log into the unified TRITON Unified Security Center. In the Data Security module, click **Deploy**.

See *Accessing the TRITON Unified Security Center*, page 765 for instructions.

16. Remove Data Security components from the Data Security TRITON Unified Security machine.

See *Removing Data Security components*, page 816 for instructions. Return here when done.

17. Remove TRITON Infrastructure from the Data Security TRITON management server.

    See *Removing TRITON Infrastructure*, page 806 for instructions. Return here when done.

# Post-Upgrade configuration

## Reregister Data Security Agents with the TRITON management server

Reregister Data Security endpoints and agents (e.g., SMTP, Printer, ISA) with the Data Security Management Server on the unified TRITON management server. See the TRITON - Data Security Help for more information.

## Reregister Content Gateway with Data Security Management Server

Reregister Content Gateway with the Data Security Management Server. See *Registering Websense Content Gateway with Data Security*, page 771.

## Verify administrator accounts

Verify and resolve any issues with TRITON administrator accounts created by the upgrade process (for example, missing email addresses or modified user names). See *Upgrading or Merging Administrators*, page 917 for more information.

## New security certificate

After upgrade, you must install or permanently accept a new security certificate issued by Websense, Inc. to avoid seeing a certificate error when you first launch TRITON Unified Security Center. The prior-version certificate (accepted when accessing TRITON - Web Security or - Data Security) is no longer valid.

An SSL connection is used for secure, browser-based communication with TRITON Unified Security Center. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch TRITON Unified Security Center from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser. See the *Websense Knowledge Base* for instructions.

# 55 Upgrading to Data Security 7.6.0

## Applies to

- Data Security v7.1, v7.5, v7.6
- Web Security Gateway Anywhere v7.5, v7.6

## Upgrading to Data Security v7.6

This section describes how to upgrade a Data Security from v7.1 or v7.5 to v7.6. For information on how to upgrade Data Security software to v7.6.3, refer to *Upgrading Websense software to the latest v7.6.x*, page 821.

Note the following exceptions when you are upgrading Websense Data Security software to v7.6:

- Version 7.6 has a new permission structure. When upgrading, roles are reset to support the new structure.
- Exchange Agent is no longer supported in version 7.6. Upon upgrade, it is removed.
- If the SMTP agent was installed previously on the Data Security Management Server, it will no longer be present if you upgrade the Data Security Management Server to a Windows 2008 R2 machine.

There are also some exceptions specific to your version.

### v7.1 exceptions

When upgrading from Data Security Suite 7.1:

- Only incident data and forensics are upgraded.
- Policies, profiles, and settings from v7.1 are not available post-upgrade and they cannot be restored.
- Fingerprints are deleted.
- The following reporting features are lost:
  - Report filters

  - User preferences
  - Report schedules
- Remediation scripts are lost.
- Customized roles are granted Default Role permissions.
- Safend Agent is not supported in versions 7.5 and 7.6. When upgrading from version 7.1, it is removed.

### v7.5 exceptions

- The Traffic Log screen may display the following actions incorrectly for version 7.5 traffic:
  - Block
  - Encrypt
  - Endpoint confirm allow
  - Endpoint confirm denied
- If you choose to use SQL Server 2008 R2 Express to store Data Security data, only the 4 most recent partitions will be online. All other partitions are archived.

See *Upgrade Notes and Exceptions*, page 902 for full details.

For instructions on upgrading, see the following topics:


- *Upgrading Data Security Management Server*, page 883
- *Upgrading a supplemental Data Security server or standalone agents*, page 895
- *Upgrading a Data Security Protector*, page 898
- *Upgrading Content Gateway with Data Security*, page 900
- *Upgrading Data Security endpoints*, page 901


# Preparing for upgrade of Data Security

## Applies to

- Data Security v7.1, v7.5, v7.6
- Web Security Gateway Anywhere v7.5, v7.6

## In this topic

- *Notes and exceptions*, page 882

## Redirect traffic

Prior to upgrading Data Security (Suite) to version 7.6, it is a best practice to redirect traffic to not be monitored by Data Security (Suite).

- Re-route email traffic so exchange servers send email directly, rather than through Data Security agents or Protectors.
- Bypass any inline Protectors.
- Disable ISA Agent if installed on an ISA Server machine.

If you are running Data Security (Suite) in monitoring only mode, it is not necessary to redirect traffic.

## TRITON management server

In version 7.6, management of a Websense deployment is concentrated on one machine, the TRITON management server. All management interfaces (i.e., TRITON - Web Security, - Data Security, and - Email Security) and components run on this machine.

When upgrading the Data Security Management Server, you must decide whether you want to upgrade the same machine to be the 7.6 TRITON management server. Note that in most cases, TRITON management server must be a Windows Server 2008 R2 machine.

The TRITON management server can be a Windows Server 2003 machine if you plan to enable only one module of the TRITON Unified Security Center (for example, TRITON - Data Security only). If you plan to enable multiple modules (for example both TRITON - Web Security and - Data Security for a deployment of Web Security Gateway Anywhere), the TRITON management server must be a Windows Server 2008 R2 machine.

If necessary, obtain a machine meeting the operating system and hardware requirements stated in *System Requirements*, page 41 prior to beginning the upgrade process.

## SQL Server

Prior to upgrading to Data Security 7.6, Microsoft SQL Server must be installed and operational somewhere in your network. For version 7.6, SQL Server is used, instead of Oracle Database, to store and maintain Data Security data. See *System Requirements*, page 41 for which versions of SQL Server are supported.

Optionally, you can use the Websense installer to install SQL Server 2008 R2 Express (SQL Server Express)—a free, limited-performance edition of SQL Server—to be used for Data Security data.

> **Note**
> Only the supported Express edition of SQL Server (i.e., SQL Server 2008 R2 Express) can be installed on the *TRITON management server*. If using "full" SQL Server, it must run on a separate machine.

If you want to install SQL Server Express on a machine separate from the *TRITON management server*, install it prior to upgrading Data Security. See *Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)*, page 704 for instructions.

If you want to install SQL Server Express on the TRITON management server, it is not necessary to install it before upgrading. Choose to install it during installation of *TRITON Infrastructure*.

> **Note**
> In version 7.1, the Data Security Management Server could be installed on a machine that also had SQL Server 2005 installed. If you want to use SQL Server 2008 R2 Express on the same machine, you must remove SQL Server 2005 prior to upgrading.

## 7.1 license file not valid

A Data Security Suite version 7.1 license file is not valid for use with version 7.6. Prior to upgrading, obtain a version 7.6 license file from Websense, Inc.

## Websense administrator accounts

Make sure Websense administrator accounts authenticated by a directory service have an email address specified in the directory service. In version 7.6, an email address is required for each administrator account (except group accounts). See *Upgrading or Merging Administrators*, page 917 for more information.

## Notes and exceptions

Read *Upgrade Notes and Exceptions*, page 902 for important information about data and configuration that may not be supported or may be moved by the upgrade process.

# Upgrading Data Security Management Server

## Applies to

- Data Security v7.1, v7.5, v7.6
- Web Security Gateway Anywhere v7.5, v7.6

## In this topic



## Overview

Complete these instructions to upgrade a Data Security Management Server from version 7.1 or 7.5 to 7.6.0. Unless otherwise noted, all instructions apply to both version 7.1 and 7.5 Data Security Management Server.

For information on how to upgrade to v7.6.3, refer to *Upgrading Websense software to the latest v7.6.x*, page 821.

You can either upgrade Data Security Management Server "in place," i.e., it is upgraded to version 7.6 on its current machine, or you can upgrade it to another machine (for example, from a Windows Server 2003 machine to a Window Server 2008 R2 machine). There is a procedure below for each case:

- *Upgrade in place*, page 883
- *Upgrade to another machine*, page 889

In version 7.6, Data Security Management Server is part of the *TRITON management server*. These instructions will refer to TRITON management server in place of Data Security Management Server when discussing version 7.6. Additionally, Data Security 7.6 uses Microsoft SQL Server instead of Oracle Database for data storage.

Note that the upgrade process can take a long time because large amounts of data may need to be copied. You can reduce this time by relocating the forensics repository (steps for doing this are included in the procedure below). See *Forensics Repository*, page 903 for more information.

## Upgrade in place

1. Make sure your current Data Security (Suite) deployment has hotfixes applied for its version as follows:
   - Update Data Security Suite 7.1.0 - 7.1.4 to 7.1.5. Versions 7.1.5 or higher can be upgraded directly to 7.6.

- Update Data Security 7.5.x to 7.5.9 prior to upgrade to 7.6.

See *How to get the latest Data Security Suite hotfixes* for more information.

2. Check the System Health screen to make sure your system is functioning properly. If you suspect it is not, please contact Websense Technical Support before proceeding.

3. Perform a full backup of the machine.

   See 7.5 TRITON - Data Security Help or 7.1 DSS Manager Help for more information on backing up Data Security data.

4. If you are upgrading from version 7.1, export system modules to PDF.

   In DSS Manager, select **Configuration** > **System Modules** and then click the PDF icon.

5. Relocate forensics data.

   **Note**
   If your forensics repository is large (more than approximately 3 GB) upgrading Data Security can take a very long time. It is strongly recommended you relocate forensics data prior to using the upgrade export tool and then copy the data back to the appropriate location after upgrading. It is a best practice to relocate forensics a day prior to upgrading Data Security to allow sufficient time to complete this task.

   **Warning**
   If you have archived partitions, you must relocate forensics prior to using the upgrade export tool. Otherwise, the archived partitions will not be available in the upgraded system.

   If you are upgrading from version 7.5:

   Note: in the following steps, the Websense folder is typically C:\Program Files\Websense.

   a. Stop the DSS watchdog service:
      i. Select **Start > Programs > Accessories > Scheduled tasks**.
      ii. Right-click **DSS Watchdog** and select **Properties**.
      iii. De-select **Enabled**.
      iv. Click **OK**.
   b. In the Windows Services console, stop the **Websense DSS Manager** service.

Alternatively, issue the command **`net stop tomcat6`** in a Command Prompt.

c. Rename **Websense\Data Security\forensics_repository\data** to **Websense\Data Security\forensics_repository\oldData**

d. Create a new folder named **Websense\Data Security\forensics_repository\data**

e. Create a new folder named **Websense\Data Security\archive_mng\oldStorage**

f. Move all folders starting with **FR-ARC-** from **Websense\Data Security\archive_mng\storage** to **Websense\Data Security\archive_mng\oldStorage**

g. In the Windows Services console, start the **Websense DSS Manager** service.

Alternatively, issue the command **`net start tomcat6`** in a Command Prompt.

h. Move or copy the following folder to a location outside the Websense folder: **Websense\Data Security\forensics_repository\oldData**

i. Search the **oldData** folder for files with the name **`*.ser`** and delete those files.

j. Move or copy all folders starting with **`FR-ARC-`** from **Websense\Data Security\archive_mng\oldStorage** to a location outside the Websense folder

If you are upgrading from version 7.1:

Note: in the following steps, the Websense folder is typically C:\Program Files\Websense.

k. In the Windows Services console, stop the **Websense DSS Manager** service.

Alternatively, issue the command `net stop tomcat6` in a Command Prompt.

l. Rename **Websense\Data Security Suite\Archive** to **Websense\Data Security Suite\oldArchive**

m. Create a new folder named **Websense\Data Security Suite\Archive.**

n. Share the Archive folder, and give the 'change' and 'write' permissions to both the DSS user and the currently logged-in user (the user that will run the script).

o. In the Windows Services console, start the **Websense DSS Manager** service.

Alternatively, issue the command **`net start tomcat6`** in a Command Prompt.

p. Move or copy **Websense\Data Security Suite\oldArchive** to a location outside the Websense folder

6. Obtain the upgrade export tool zip package and extract it.

Download **WebsenseDataSecurityUpgradeExportTool.zip** from www.mywebsense.com.

7. Copy the upgrade_export_tool folder to a temporary folder on the Data Security Management Server (this folder is referred to as the *export tool folder* in the rest of these instructions).

   Copy to a location outside the Websense folder (typically, C:\Program Files\Websense) for example C:\temp\upgrade_export_tool.

8. Run the export script:

   **Important**

   Data Security Suite 7.1 will not be operational after running the export script.

   Data Security 7.5 will continue to operate, but new data generated after running the export tool will not be imported to Data Security 7.6.

   **Note**

   Prior to running the export script, see *Estimating export data size*, page 902 to estimate the amount of data that will be generated.

   a. Open a Command Prompt.

   b. From the export tool folder, enter the following command:

      ```
      python export.py
      ```

      Note the above command generates export data in %dss_home%/archive_mng/export-data. You can specify a different location by specifying a path in the command:

      ```
      python export.py <path>
      ```

      where <path> is local; it cannot be a network path or a location on a mapped network drive. If you specify <path>, substitute it for %dss_home%/archive/mng/export-data in the remaining steps below.

   c. Wait for the script to complete.

      Depending on the amount of data, this process may take a long time.

      **Important**

      If the script fails during an upgrade from v7.1, do *not* run it again (running it again may corrupt the data). Contact Websense Technical Support before proceeding.

9. Check the following files for any errors:

   - dbexport.log (in export tool folder you created in Step 7, for example C:\temp\upgrade_export_tool)
   - db.log (in export tool folder you created in Step 7, for example C:\temp\upgrade_export_tool)

- %dss_home%/archive/mng/export-data/DataExport.log

If you find errors, contact Websense Technical Support.

10. If you provided an alternate path in step 7b, skip to step 10. Otherwise, move the data exported by the export script to a location outside the Websense folder.

    The exported data is located in %dss_home%/archive_mng/export-data. Move the entire export-data folder to a location outside the Websense folder (typically, C:\Program Files\Websense).

    Note the export-data folder should contain the following. If it does not and you're upgrading from v7.5, try running the script again. If it does not and you're upgrading from v7.1, contact Websense Technical Support.

    When upgrading from 7.1 or 7.5:

    - Certs (folder)
    - DSS_FILES (folder)
    - Forensics_repository (folder)
    - OldPolicyXMLs (folder)
    - Onlinetables (folder)
    - Partitiontables (folder)
    - **Backup.txt** (this file is required when restoring data to the upgraded system)
    - Dataexport.log

    When upgrading from 7.5 the following are also present (in addition to those above):

    - Crawlers (folder)
    - Policies_backup (folder)
    - PreciseID_DB (folder)
    - RunCommands (folder; only present if you had *remediation script* resources)
    - Ep-profile-keys.zip
    - Subscription.xml
    - Wbsn-pairing-map.txt

11. Perform the actions appropriate to your machine, as described in *Preparing for Installation*, page 55.

12. Download and launch the version 7.6 Websense installer (Websense installer).

    A progress dialog box appears, as files are extracted:

13. When the following message appears, click **OK**:

    *An older version of Data Security is installed on this machine. Press OK to upgrade it or Cancel to exit the installation.*

The **Installer Dashboard** appears.

14. TRITON Infrastructure Setup starts. Complete the TRITON Infrastructure Setup wizard. See *Installing TRITON Infrastructure*, page 661 for instructions. Return to this procedure when done.

    TRITON Infrastructure is required for TRITON Unified Security Center. In version 7.6, all management interfaces (i.e., TRITON - Web Security, - Data Security, and - Email Security) are modules of the TRITON Unified Security Center. TRITON Unified Security Center will be installed on this machine and v7.5 TRITON - Data Security upgraded to be its Data Security module.

15. The following message appears. Click **OK** to proceed (Important: do this only if you have already run the export tool. If you have not, cancel the installation and see Step 6).

    *Before installing this version of Data Security, the existing version will be removed. Please make sure that the export-tool of this version has been successfully executed on this machine. Click OK to remove the existing version of Data Security, or Cancel to exit.*

    The prior-version Data Security components are first removed and then replaced with current versions. The prior-version Data Security Installation Wizard is launched. This is used to remove components.

    Note that the **Installer Dashboard** remains on-screen, behind the prior-version installer.

16. Click **Next** in the prior-version installer to begin removing components.

    Components are removed.

17. When the wizard notifies you that**Data Security has been successfully installed**, click **Finish**

    Note the screen mentions installation success, but this simply means the Data Security Installation Wizard has completed its task successfully, which in this case is removing components.

18. You are returned to the Installer Dashboard and the **Websense Data Security Installer** appears.

    This is the current-version installer that will install version 7.6 Data Security components.

19. Install version 7.6 Data Security components. Be sure to select the same components for installation as were previously on this machine. You can install additional components as well.

    See *Installing Data Security Components*, page 692 for instructions. **Important**: When following these instructions, be sure to import the data exported when you ran the export script (in Step 6) on the **Import Data From Previous Version** screen.

20. If you relocated forensics data prior to upgrade (Step 5):

    Upgraded from version 7.5:

    a. Copy the contents of **oldData** (from the location outside the Websense folder) to **Websense\Data Security\forensics_repository\data** (note: copy the contents and not the folder itself).
    b. Copy all content moved from **Websense\Data Security\archive_mng\oldStorage** (step Windows Step j, page 885) to **Websense\Data Security\archive_mng\storage**

    Upgraded from version 7.1:

    - Copy the contents of **oldArchive** (from the location outside the Websense folder) to **Websense\Data Security\forensics_repository** (note: copy the contents and not the folder itself).

21. Oracle is no longer used by Data Security in version 7.6. To conserve system resources, it is a best practice to disable the Oracle service.

    To disable Oracle, in the Windows Services console, disable the **OracleServiceMng** service. Note that this disables the service but does not remove any old data. Disabling Oracle is optional.

## Upgrade to another machine

The following process is different from a fresh install; it describes how to migrate incidents, reports, and more from your existing system to the new one.

1. Make sure your current Data Security (Suite) deployment has hotfixes applied for its version as follows:

   - Update Data Security Suite 7.1.0 - 7.1.4 to 7.1.5. Versions 7.1.5 or higher can be upgraded directly to 7.6.
   - Update Data Security 7.5.x to 7.5.9 prior to upgrade to 7.6.

   See *How to get the latest Data Security Suite hotfixes* for more information.

2. Check the System Health screen to make sure your system is functioning properly. If you suspect it is not, please contact Websense Technical Support before proceeding.

3. Perform a full backup of the machine.

   See 7.5 TRITON - Data Security Help or 7.1 DSS Manager Help for more information on backing up Data Security data.

4. If you are upgrading from version 7.1, export system modules to PDF.

In DSS Manager, select **Configuration** > **System Modules** and then click the PDF icon.

5. Relocate forensics data.

> **Note**
> If your forensics repository is large (more than approximately 3 GB) upgrading Data Security can take a very long time. It is strongly recommended you relocate forensics data prior to using the upgrade export tool and then copy the data back to the appropriate location after upgrading. It is a best practice to relocate forensics a day prior to upgrading Data Security to allow sufficient time to complete this task.

> **Warning**
> If you have archived partitions, you must relocate forensics prior to using the upgrade export tool. Otherwise, the archived partitions will not be available in the upgraded system.

If you are upgrading from version 7.5:

Note: in the following steps, the Websense folder is typically C:\Program Files\Websense.

a. Stop the DSS watchdog service:

   v. Select **Start > Programs > Accessories > Scheduled tasks**.

   vi. Right-click **DSS Watchdog** and select **Properties**.

   vii. De-select **Enabled**.

   viii. Click **OK**.

b. In the Windows Services console, stop the **Websense DSS Manager** service.

   Alternatively, issue the command **`net stop tomcat6`** in a Command Prompt.

c. Rename **Websense\Data Security\forensics_repository\data** to **Websense\Data Security\forensics_repository\oldData**

d. Create a new folder named **Websense\Data Security\forensics_repository\data**

e. Create a new folder named **Websense\Data Security\archive_mng\oldStorage**

f. Move all folders starting with **FR-ARC-** from **Websense\Data Security\archive_mng\storage** to **Websense\Data Security\archive_mng\oldStorage**

g. In the Windows Services console, start the **Websense DSS Manager** service.

   Alternatively, issue the command **`net start tomcat6`** in a Command Prompt.

h. Move or copy the following folder to a location outside the Websense folder: **Websense\Data Security\forensics_repository\oldData**

i. Search the **oldData** folder for files with the name **`*.ser`** and delete those files.

j. Move or copy all folders starting with **`FR-ARC-`** from **Websense\Data Security\archive_mng\oldStorage** to a location outside the Websense folder

If you are upgrading from version 7.1:

Note: in the following steps, the Websense folder is typically C:\Program Files\Websense.

k. Stop the DSS watchdog service:

ix. Select **Start** > **Programs** > **Accessories** > **Scheduled tasks**.

x. Right-click **DSS Watchdog** and select **Properties**.

xi. De-select **Enabled**.

xii. Click **OK**.

l. In the Windows Services console, stop the **Websense DSS Manager** service.

Alternatively, issue the command `net stop tomcat6` in a Command Prompt.

m. Rename **Websense\Data Security Suite\Archive** to **Websense\Data Security Suite\oldArchive**

n. Create a new folder named **Websense\Data Security Suite\Archive**

o. Share the Archive folder, and give the 'change' and 'write' permissions to both the DSS user and the currently logged-in user (the user that will run the script).

p. In the Windows Services console, start the **Websense DSS Manager** service.

Alternatively, issue the command **`net start tomcat6`** in a Command Prompt.

q. Move or copy **Websense\Data Security Suite\oldArchive** to a location outside the Websense folder

6. Obtain the upgrade export tool zip package and extract it.

Download **WebsenseDataSecurityUpgradeExportTool.zip** from www.mywebsense.com.

7. Copy the upgrade_export_tool folder to a temporary folder on the Data Security Management Server (this folder is referred to as the *export tool folder* in the rest of these instructions).

Copy to a location outside the Websense folder (typically, C:\Program Files\Websense) for example C:\temp\upgrade_export_tool.

8. Run the export script:

   **Important**

   Data Security Suite 7.1 will not be operational after running the export script.

   Data Security 7.5 will continue to operate, but new data generated after running the export tool will not be imported to Data Security 7.6.

   **Note**

   Prior to running the export script, see *Estimating export data size*, page 902 to estimate the amount of data that will be generated.

   a. Open a Command Prompt.

   b. From the export tool folder, enter the following command:

      ```
      python export.py
      ```

      Note the above command generates export data in %dss_home%/archive_mng/export-data. You can specify a different location by specifying a path in the command:

      ```
      python export.py <path>
      ```

      where <path> is local; it cannot be a network path or a location on a mapped network drive. If you specify <path>, substitute it for %dss_home%/archive/mng/export-data in the remaining steps below.

   c. Wait for the script to complete.

      Depending on the amount of data, this process may take a long time.

      **Important**

      If the script fails during an upgrade from v7.1, do *not* run it again (running it again may corrupt the data). Contact Websense Technical Support before proceeding.

9. Check the following files for any errors:

   - dbexport.log (in export tool folder you created in Step 7, for example C:\temp\upgrade_export_tool)
   - db.log (in export tool folder you created in Step 7, for example C:\temp\upgrade_export_tool)
   - %dss_home%/archive/mng/export-data/DataExport.log

   If you find errors, contact Websense Technical Support.

10. If you provided an alternate path in step 8b, skip to step 10. Otherwise, move the data exported by the export script to the target machine (i.e., the one to which you want to upgrade Data Security Management Server).

The exported data is located in %dss_home%/archive_mng/export-data.

Note the export-data folder should contain the following (if it does not, try running the export script again; see Step 8).

When upgrading from 7.1 or 7.5:

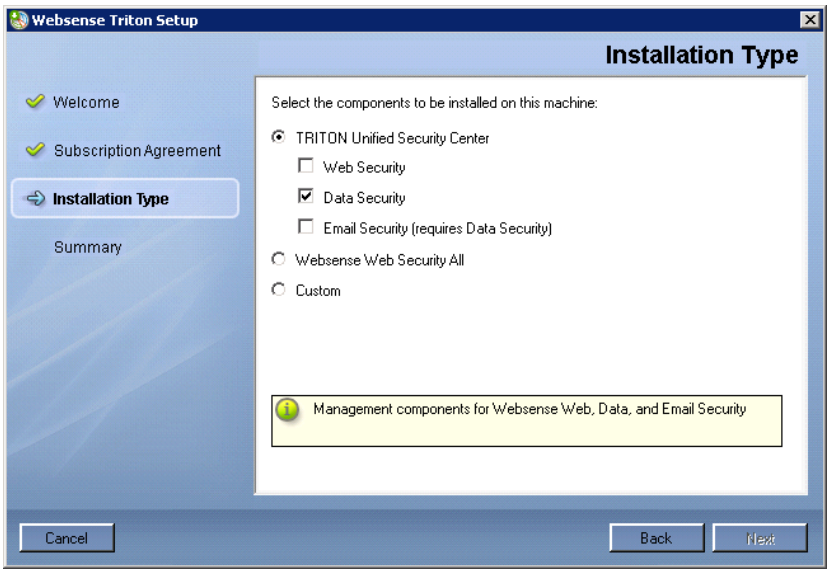
- Certs (folder)
- DSS_FILES (folder)
- Forensics_repository (folder)
- OldPolicyXMLs (folder)
- Onlinetables (folder)
- Partitiontables (folder)
- **Backup.txt** (this file is required when restoring data to the upgraded system)
- Dataexport.log

When upgrading from 7.5 the following are also present (in addition to those above):

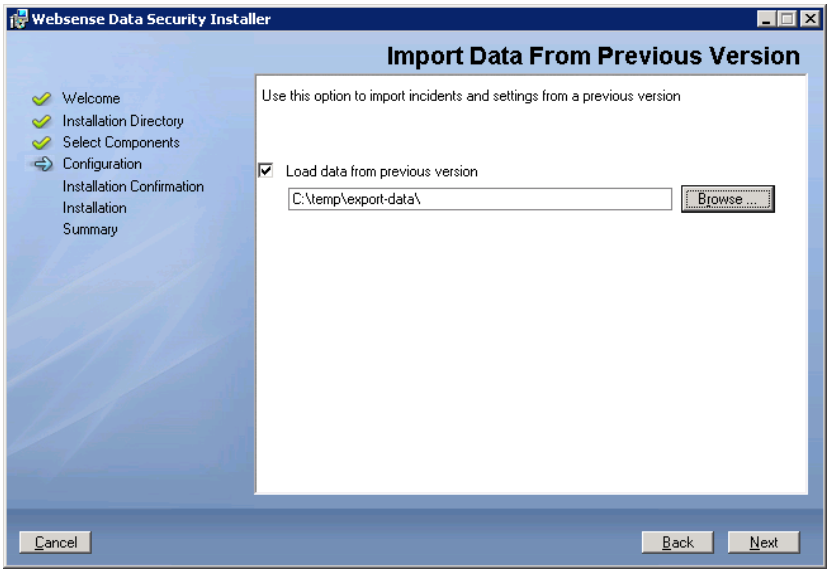
- Crawlers (folder)
- Policies_backup (folder)
- PreciseID_DB (folder)
- RunCommands (folder; only present if you had *remediation script* resources)
- Ep-profile-keys.zip
- Subscription.xml
- Wbsn-pairing-map.txt

11. On the target machine (i.e., the one to which you want to upgrade Data Security Management Server), follow the procedures to create a TRITON management server as directed in *Creating a TRITON Management Server*, page 645. **Important**: when following those procedures, do the following:

a. When you reach the **Installation Type** screen of the Websense installer, be sure to select **Data Security** (under TRITON Unified Security Center). Note that you can install the other modules if you want, but TRITON - Data Security is the only one necessary for a Data Security deployment.




b. When the Data Security installer appears, on the **Import Data From Previous Version** screen, select the **Load Data From Backup** check box and then use the **Browse** button to select the location of the data exported by the export script.




12. Log on to the version 7.6 TRITON Unified Security Center (on the TRITON management server you just created):
    a. Verify system settings, configuration, and modules.
    b. Click **Deploy**.

Note that at this point the system is functional. However, if you relocated forensics data prior to upgrade, it is not present yet. You will restore this data in the next step.

13. If you relocated forensics data prior to upgrade (Step 5):

    Upgraded from version 7.5:

    a. Copy the contents of **oldData** (from the location outside the Websense folder, on the old machine) to **Websense\Data Security\forensics_repository\data** on this machine (note: copy the contents and not the folder itself).
    b. Copy all content moved from **Websense\Data Security\archive_mng\oldStorage** on the old machine (step Windows Step j, page 885) to **Websense\Data Security\archive_mng\storage** on this machine

    Upgraded from version 7.1:

    - Copy the contents of **oldArchive** (from the location outside the Websense folder, on the old machine) to **Websense\Data Security\forensics_repository** on this machine (note: copy the contents and not the folder itself).

# Upgrading a supplemental Data Security server or standalone agents

## Applies to

- Data Security v7.1, v7.5, v7.6
- Web Security Gateway Anywhere v7.5, v7.6

## In this topic



## Overview

Complete these steps to upgrade a supplement Data Security server or standalone agents (e.g. SMTP, Printer, Discovery, ISA/TMG) to v7.6.0.

For best practice, upgrade the management server without changing the operating system version of supplemental machines, then perform system modifications as required.

> **Important**
> If you are upgrading a Data Security server or agent to a new Windows 2008 machine, be sure to keep the original IP address/host name if you want to retain settings and information from the original server. This is especially important on machines where a v7.5 crawler was installed and had a fingerprinting classifier assigned to it. Using the same IP address prevents fingerprints from being lost.

You do not need to delete fingerprint tasks before upgrading Data Security servers.

## Upgrading from version 7.5

1. Perform the actions appropriate to your machine, as described in *Preparing for Installation*, page 55.

2. Download and launch the version 7.6 Websense installer (Websense installer).

   A progress dialog box appears, as files are extracted.

3. The **Installer Dashboard** appears.

   Any version 7.5 Data Security components found on this machine are upgraded to version 7.6.

4. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

   When you upgrade a Data Security server it takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in:

   - Potential false positives and negatives
   - Endpoints not receiving updated profiles
   - File-system discovery starts but immediately indicates "completed with errors"

## Upgrading from version 7.1

1. In the version 7.6 TRITON Unified Security Center (either on the upgraded Data Security Management Server machine or the machine to which you migrated Data Security Management Server during upgrade) go to **Data Security** module > **Settings** > **System Modules** and delete Printer and ISA Agents if they exist

2. Download and launch the version 7.6 Websense installer (Websense installer) on the supplemental Data Security server or standalone agent machine you want to upgrade.

   A progress dialog box appears, as files are extracted.

3. When the following message appears, click **OK**:

   *An older version of Data Security is installed on this machine. Press OK to upgrade it or Cancel to exit the installation.*

   The **Installer Dashboard** appears.

4. The prior-version Data Security components are first removed and then replaced with current versions. The prior-version Data Security Installation Wizard is launched. This is used to remove components.

   Note that the **Installer Dashboard** remains on-screen, behind the prior-version installer.

5. Click **Next** in the prior-version installer to begin removing components.

   Components are removed.

6. When the wizard notifies you that**Data Security has been successfully installed**, click **Finish**

   Note the screen mentions installation success, but this simply means the Data Security Installation Wizard has completed its task successfully, which in this case is removing components.

7. You are returned to the Installer Dashboard and the **Websense Data Security Installer** appears.

   This is the current-version installer that will install version 7.6 Data Security components.

8. Install version 7.6 Data Security components. Be sure to select the same components for installation as were previously on this machine. You can install additional components as well.

9. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

   When you upgrade a Data Security server it takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in:

   - Potential false positives and negatives
   - Endpoints not receiving updated profiles
   - File-system discovery starts but immediately indicates "completed with errors"

10. In the version 7.6 TRITON Unified Security Center (go to **Data Security** module > **Settings** > **System Modules**) modify Printer and/or ISA Agents that have been added, if any, so their settings match the settings in place prior to upgrade.

    Refer to the PDF of exported system module information you created when upgrading the Data Security Management Server.

# Upgrading a Data Security Protector

## Applies to

- Data Security v7.1, v7.5, v7.6

## In this topic



## Overview

**Important**

If you are upgrading your protector to new hardware, be sure to keep the original IP address/host name if you want to retain settings and information from the original machine.

If you assign a new IP, the protector's settings are cleared to default when it registers with the management server. In this case, you should manually delete the protector with the original IP address from the system modules page of TRITON - Data Security.

## Upgrading from version 7.5

Complete the following steps to upgrade a Data Security Protector from version 7.5 to version 7.6.

**Important**

Upgrade the Data Security Management Server **before** upgrading Protectors.

1. Obtain the protector update file (protector-update-7.6.0) and place it in a temporary directory (for example, in /tmp/).

2. Allow read/write/execute by all on the update file, for example:

```
chmod 777 /tmp/protector-update-7.6.0
```

3. Start the upgrade, for example:

   ```
   /tmp/protector-update-7.6.0
   ```

4. When the upgrade script is finished, reboot the machine.

5. If, when upgrading Data Security Management Server, you moved management functions to a different machine (i.e., created a TRITON management server on a different machine), reregister Protector with the new TRITON management server:

   ```
   wizard securecomm
   ```

   > **Note**
   > Even if you did not move management functions to a different machine, reregister Protector if you changed the domain membership or IP address of the Data Security Management Server machine.

6. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

   When you upgrade a Data Security server or protector, it takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in:

   - Potential false positives and negatives
   - Endpoints not receiving updated profiles
   - File-system discovery starts but immediately indicates "completed with errors"

## Upgrading from version 7.1

Complete the following steps to upgrade a Data Security Protector from version 7.1 to version 7.6.

> **Important**
> Upgrade the Data Security Management Server **before** upgrading Protectors.

1. In the version 7.6 TRITON Unified Security Center (either on the upgraded Data Security Management Server machine or the machine to which you migrated Data Security Management Server during upgrade) go to **Data Security** module > **Settings** > **System Modules** and delete Protector.

2. Perform a new installation of version 7.6 Protector on the 7.1 Protector machine.

This must be done because an upgrade from version 7.1 to 7.6 Protector is not supported.

3. In the version 7.6 TRITON Unified Security Center (either on the upgraded Data Security Management Server machine or the machine to which you migrated Data Security Management Server during upgrade) go to **Data Security** module > **Settings** > **System Modules** and modify the settings for the added Protector to match those in place prior to upgrade.

   Refer to the PDF of exported system module information you created when upgrading the Data Security Management Server.

4. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

   When you upgrade a Data Security server or protector, it takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in:

   - Potential false positives and negatives
   - Endpoints not receiving updated profiles
   - File-system discovery starts but immediately indicates "completed with errors"

# Upgrading Content Gateway with Data Security

## Applies to

- Data Security v7.1, v7.5, v7.6
- Web Security Gateway Anywhere v7.5, v7.6

## Upgrading Content Gateway with Data Security

**Important**

Upgrade the Data Security Management Server **before** upgrading agents.

Upgrading Content Gateway 7.1 to 7.6 is not possible. Instead, install Content Gateway 7.6 as a new installation. See *Websense Content Gateway*, page 357.

To upgrade Content Gateway 7.5 to 7.6, see*Upgrading Websense Content Gateway to 7.6.0*, page 853. Once you have upgraded Content Gateway, reregister it with the TRITON management server. See *Registering Websense Content Gateway with Data Security*, page 771.

# Upgrading Data Security endpoints

## Applies to

- Data Security v7.1, v7.5, v7.6
- Web Security Gateway Anywhere v7.5, v7.6

## Upgrading Data Security endpoints

First upgrade the Data Security Management Server and any supplemental Data Security servers. Then upgrade Data Security endpoints. Upgrade endpoints by deploying the 7.6 version of them to their current locations. See *Deploying Websense endpoints*, page 744.

It is possible that some endpoints are not connected to the network or are unavailable for upgrade for some other reason. These endpoints will continue to function and be able to identify breaches and create incidents. They will operate according to the last policy applied to it.

In version 7.6, you can configure prior-version endpoints to operate in monitoring mode until they are updated. In this mode, the endpoints only audit actions and do not block.

**Note**

A prior-version endpoint configured to block printscreen actions will continue to block that action even if you set it to monitoring mode in version 7.6.

Incidents from prior-version endpoints will continue to be accepted by upgraded Data Security Management and supplemental servers.

Data Security Management Server is upgraded to be part of the version 7.6 TRITON Unified Security Center. Note that during upgrade, if there are multiple network interfaces on the machine, you can choose a different IP address than that currently used. If you do so, endpoint clients configured to connect to endpoint servers on this machine will no longer be using the correct IP address. A solution to this situation is create a version 7.6 Data Security supplemental server using the old IP address so endpoint clients can still connect to it and (optionally) remove it after the endpoints have been updated to version 7.6 (connecting to the new IP address).

**Important**

At the completion of any endpoint update, you must restart the endpoint for the updates to take effect.

# Upgrade Notes and Exceptions

## Applies to

- Data Security v7.1, v7.5, v7.6
- Web Security Gateway Anywhere v7.5, v7.6

## In this topic



## Estimating export data size

Use the following guidelines to estimate the amount of data that will be generated by the upgrade export tool (i.e., export.py script).

### Incident metadata

Data in Motion: 1 GB exported data per 350,000 incidents.

Data at Rest: 1 GB exported data per 100,000 incidents.

### Incident forensics

Exported data for forensics is equal to the size of the forensics data itself.

> **Important**
> If current forensics data is more than 3 GB, it should be located outside the Websense folder as directed in the upgrade instructions. Otherwise the upgrade export process can take a very long time.

### Resources and configuration

Total exported data approximately 0.5 GB, broken down as follows:

- 0.2 GB for Resource Repository
- 0.1 for other management data
- 0.2 for predefined policies

### Fingerprint and discovery

This applies only when upgrading from version 7.5.x.

Export data is equal to the sum of the following:

- %dss_home%\DiscoveryJobs
- PreciseID database folder (%dss_home%\PreciseID DB by default)
- Sum of *Endpoint package size* of all *PreciseID File* classifiers (typically, under 1 GB)

## Forensics Repository

Version 7.1 forensics data is moved from  %DSS HOME%/Archive to %DSS HOME%/forensics_respository by the upgrade process.

> **Note**
> When the maximum disk space (by default 50 GB) is reached, the oldest forensics are moved to the archive folder to free space (by default Websense\Archive).

The time it takes to complete the upgrade process for the Data Security Management Server can be reduced if, before upgrading, you move the forensics repository from the default location to a new location on a different machine. Make sure the new location is accessible by the TRITON management server after upgrade.

After upgrading from version 7.1, the version 7.1 forensics repository will exist in addition to the forensics manager. Forensics data can be reached from TRITON - Data Security in the same way as in version 7.1 (not through the forensics manager). There will be a version for each incident which will determine how to get to the forensics.

## Policies

7.1 policies cannot be upgraded to 7.6. Only 7.5 policies will be upgraded.

Once upgraded to version 7.6, you cannot restore prior-version policies to the upgraded system.

## Incident Management and Reports

When upgrading from version 7.1 to v7.6, the following will be lost:

- Report filters
- User preferences
- Report schedules

Note that version 7.1 data for filters and scheduled report tasks will be exported to the following folder: %DSS HOME%\old_7_1_data.

## Remediation Script

When upgrading from version 7.1, Remediation Scripts are lost. You must recreate them in version 7.6.

## Traffic Log screen

After upgrading from version 7.5, the Traffic Log screen may display the following actions incorrectly for version 7.5 traffic:

- Block
- Encrypt
- Endpoint confirm allow
- Endpoint confirm denied

## SQL Server 2008 R2 Express

If you choose to use SQL Server 2008 R2 Express to store Data Security data, only the 4 most recent partitions will be online. All other partitions are archived.

## Roles

Version 7.6 has a new permission structure. When upgrading, 7.1 and 7.5 roles will be reset to support the new structure.

Version 7.1 customized roles will be granted Default Role permissions in version 7.6.

Version 7.1 roles data will be exported to a folder named **old_7_1_data** in the export-data folder (see Step 10, page 887).

## New security certificate

After upgrade, you must install or permanently accept a new security certificate issued by Websense, Inc. to avoid seeing a certificate error when you first launch TRITON Unified Security Center. The prior-version certificate (accepted when accessing TRITON - Web Security or - Data Security) is no longer valid.

An SSL connection is used for secure, browser-based communication with TRITON Unified Security Center. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch TRITON Unified Security Center from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser. See the *Websense Knowledge Base* for instructions.

## Fingerprints from version 7.1.x lost

When upgrading from version 7.1.x to 7.6, fingerprints are deleted.

## Excel Fingerprints from version 7.5.x

When upgrading from version 7.5, incorrect fingerprints of Excel files remain. Prior versions of Data Security had a issue when extracting text out of numeric cells in Excel documents. Only the first (most significant) 15-digits of any numeric cell would be fingerprinted.

Although this issue has been resolved in version 7.6, Excel files fingerprinted in previous versions may not be caught by version 7.6 if they contain many numeric fields with more than 15 digits.

Re-fingerprint the relevant files (delete the document fingerprints and start another fingerprinting scan). This assumes that the fingerprinted files still exist on the file servers (or Sharepoint server) to be re-fingerprinted.

## MMC report

The upgrade export tool generates an HTML report describing settings and policies that existed in 7.1 Data Security Suite Management Console. Use this report as a reference to recreate settings that are not upgraded to version 7.6.

The report is named ExportReport.html and placed in the export-data folder.

## SMTP Agent not supported on Windows 2008 R2

If SMTP agent was installed on the version 7.1/7.5 Data Security Management Server, it will no longer be present if you upgrade the Data Security Management Server to a Windows 2008 R2 machine.

## Exchange Agent deprecated

Exchange Agent is no longer supported in version 7.6. Upon upgrade, it will not be upgraded, but instead removed.

## Safend Agent deprecated

Safend Agent is not supported in versions 7.5 and 7.6. When upgrading from version 7.1 Data Security Suite, Safend Agent is removed.

# 56 Upgrading V-Series Appliance to 7.6

## Applies to

- V5000 and V10000 with Web Security Gateway v7.6
- V5000 and V10000 with Web Security Gateway Anywhere v7.6

## In this topic



## Versions supported for upgrade

The following appliance versions can be directly upgraded to version 7.6:

- 7.5
- 7.5.1
- 7.5.2
- 7.5.3

Prior versions must be upgraded to one of the above versions prior to upgrading to version 7.6.

# Estimated time to complete upgrade

It is estimated that installation of this upgrade takes approximately 100 minutes (one V-Series appliance and one Windows server), which includes:

- 10 minutes to download the upgrade file
- 10 minutes to back up the V-Series files
- 40 to 50 minutes to run the upgrade
- 10 minutes to restart the V-Series and verify that the upgrade was successful
- 5 minutes to download the version 7.6 Websense installer
- 10 to 15 minutes to run the installer to upgrade the off-box components
- 5 minutes to restart the Windows server and verify that the upgrade was successful

# Preparing for the upgrade

Before upgrading, perform the following tasks or be aware of the following issues.

## Back up configuration and settings

Back up your configuration files, log files, and policy databases from the appliance. See the following Solution Center article at www.websense.com/support: "How do I back up and restore the files on my appliance?"

## Download Content Gateway logs

To ensure that you retain a copy of all logs, download the Content Gateway logging directory. Depending on their size, older logs may be removed automatically by the upgrade. Note that policy databases and Websense databases are not affected by the upgrade.

## Service disruption during upgrade

Service may be disrupted for 50 to 60 minutes while the upgrade is being applied to the V-Series appliance and it restarts. Note that service is not disrupted while the off-box components are upgraded.

## Restart required

At completion of the V-Series upgrade, you must restart the appliance.

# Websense administrator accounts

Make sure Websense administrator accounts authenticated by a directory service have an email address specified in the directory service. In version 7.6, an email address is required for each administrator account (except group accounts). See *Upgrading or Merging Administrators*, page 917 for more information.

# Content Gateway changes

Several Content Gateway changes and enhancements require consideration prior to appliance upgrade.

## Configuration settings not preserved

The following Content Gateway configuration settings are **not** preserved and must be reconfigured post-upgrade:

- Proxy user authentication and access control filter (filter.config) configuration settings are not retained. These include:
  - LDAP, RADIUS, NTLM, and multiple realm rules
  - All filtering rules (filter.config)

  Multiple authentication methods with multiple authentication realms is expanded in version 7.6 and made more powerful with the addition of Integrated Windows Authentication. Multiple authentication realm rules used in 7.5 deployments must be recreated after upgrading to 7.6. Also, if NTLM was configured in 7.5, consider moving to Integrated Windows Authentication.

  Before upgrading, be prepared to reconfigure user authentication options and proxy filtering rules (often used to bypass authentication). It is recommended that copy your 7.5 filter.config file to a safe location for future reference.

## New features to configure after upgrade

You may want to configure these new and enhanced features post-upgrade (for more information, see the Content Gateway Release Notes):

- Explicit proxy deployments can configure multiple inbound ports.
- Transparent proxy deployments with WCCP have more configuration options.
- Integrated Windows Authentication (with Kerberos) provides more robust proxy user authentication with Windows Active Directory. If NTLM was a user authentication method in version 7.5, consider moving to Integrated Windows Authentication.
- Multiple Realm Authentication is enhanced and now supports multiple authentication rules for multiple authentication realms.
- **Full clustering is deprecated in version 7.6.** Multiple installations of Content Gateway can no longer form a single logical cache. After upgrade, consider configuring Managed clusters.

- For deployments that use SSL Manager, SSL clustering is added to share SSL Manager settings among nodes in a cluster. It is configured separately from Managed clustering.

For more, see Content Gateway *Post upgrade activities*, page 862.

## admin password

If TRITON - Web Security is running on an appliance, the default **WebsenseAdministrator** user is replaced by a user named **admin** upon upgrade. The **admin** user will have the same password the **WebsenseAdministrator** user had prior to upgrade.

The **admin** user is the new default administrator account for version 7.6. Use it in place of **WebsenseAdministrator**.

## Disable on-appliance TRITON - Web Security if both on- and off-appliance instances used in prior version

If you had both on- and off-appliance instances of TRITON - Web Security running in version 7.5.x, disable the on-appliance instance after upgrading the appliance to version 7.6. To disable the on-appliance TRITON - Data Security:

1. Log on to the Appliance Manager (https://<*C interface IP address*>:9447/appmng)
2. Under **Configuration**, select **Web Security Components**.
3. Under **TRITON - Web Security**, select **Disabled**.
4. Click **Save**.

   The disabling process may take several minutes. Wait for it to complete.
5. When the process completes successfully, a *TRITON Configuration* link appears below the **Disabled** option.

   Use this link if you want to create a backup of TRITON settings that can be restored to the off-appliance TRITON Unified Security Center:

   a. Click the backup file link that is displayed below the Disabled button.

   b. If a certificate error is displayed, click the continue or accept option to start the download.

   c. Save the TRITON backup file (**EIP_bak.tgz**) in a convenient location.

# Upgrade instructions

> **Important**
>
> V-Series appliance services are disrupted (not available) while the patch is applied until the V-Series appliance completes its restart, approximately 50 to 60 minutes. It is best to perform the upgrade at a time when service demand is at a minimum.

1. If you have multiple V-Series appliances, read *Upgrading multiple V-Series appliances*, page 912 **prior** to following this procedure.
2. If your appliances are clustered, see *Upgrading clustered appliances*, page 913.
3. Take all precautions to ensure that power to the V-Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.
4. Back up appliance configuration and settings. See *Back up configuration and settings*, page 908.
5. Restart the appliance (in Appliance Manager: **Status** > **Modules** > **Restart Appliance**).

   See the Appliance Manager Help for more information.
6. Download the upgrade patch:

   Go to MyWebsense.com and select **Downloads** tab. Click *Get Hotfixes & Patches*. Select your appliance model and version.

   > **Important**
   >
   > Upgrade all Websense V-Series appliances to v7.6 **before** upgrading the Websense software on the Windows servers to v7.6. If your deployment uses several appliances, upgrade the primary appliance first (this is the appliance that hosts the policy source), then the secondaries, and finally the off-box components. See *Upgrading multiple V-Series appliances*, below.

7. If clustering is enabled in Content Gateway, you'll need to disable it. Log on to the Content Gateway Manager by pointing the browser to `https://<IP-address-for-interface-C>:8081` and then:
   a. Navigate to **Configure** > **My Proxy** > **Basic** > **Clustering**.
   b. In the **Cluster Type** area, select **Single Node**.
   c. Click **Apply**.
   d. **Restart** Content Gateway.
8. Log on to the V-Series console by pointing a browser to:

   `https://<IP-address-for-interface-C>:9447/appmng/`

The user name is: **admin**.

The password was set on your appliance when **firstboot** was run.

9. Navigate to **Administration > Patch Management**.
10. Click **Browse**, and select the v7.6 upgrade file.
11. Click **Upload**. After a few seconds, the upgrade is listed in the**Uploaded patches** list.
12. Click **Install** to apply the upgrade. It takes 40 to 50 minutes for the upgrade process to complete. During this time proxy services are unavailable to users.
13. When the installation is complete, restart the appliance right away; click **Restart Now** when prompted. Do not cycle the power.
14. When the appliance has restarted, log on to the Appliance Manager console and verify on the **Configuration > General** page that the V-Series version is 7.6.

    In rare cases, when logging in to the Appliance Manager for the first time after upgrade, your browser may show an **HTTP Status - Internal Error** page. If this occurs, cycle the power to the appliance. Once the appliance has restarted, you should be able to log in.
15. If you have multiple appliances, upgrade them all, repeating Step 8 - Step 14 for each.
16. Upgrade all Websense modules running off the appliance (such as **TRITON - Web Security** and **Log Server**).

    See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.
17. To confirm that the Windows components were successfully upgraded, log on to TRITON Unified Security Center.

## Upgrading multiple V-Series appliances

When multiple V-Series appliances are deployed on the same network, it is very important that they be upgraded in the prescribed order.

### Best practice for upgrade sequence if full policy source is on V-Series appliance

Multiple V-Series appliances (1 *full policy source*, 1 or more *user directory and filtering* and/or *filtering only*). Policy Broker and Policy Server run on the primary:

1. Upgrade the *full policy source* V-Series appliance and immediately restart when the upgrade completes.
2. Sequentially apply the upgrade to all *user directory and filtering* appliances. Restart each appliance when the upgrade completes.
3. Sequentially apply the upgrade to all *filtering only* appliances. Restart each appliance when the upgrade completes.
4. After all appliances have been upgraded, upgrade off-box components.

### Best practice for upgrade sequence if full policy source is not on V-

### Series appliance

#### If you have multiple V-Series appliances with full policy source (Policy Broker and Policy Server) located off-appliance

1. Use the version 7.6 Websense installer to upgrade **only** Policy Broker and Policy Server. See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.
2. Apply the v7.6 upgrade to each appliance and immediately restart as each upgrade completes.
3. Use the version 7.6 Websense installer to upgrade remaining off-appliance components. See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.

### If the full policy source appliance is down or unavailable

Best practice is to upgrade the *full policy source* appliance first, then the *user directory and filtering*, then *filtering only* appliances, and finally the off-appliance Websense components.

However, if your site must upgrade a *user directory and filtering* or *filtering only* appliance before the *full policy source* appliance, or if your *full policy source* appliance is unavailable, is being replaced, or is being re-imaged, then set a *user directory and filtering* or *filtering only* appliance (temporarily) to be the full policy source. To do this:

1. On that secondary appliance, in the V-Series console, move to the page **Configuration > Web Security Components**.
2. For **Policy Source**, select **Full policy source**. Save the setting.
3. Upgrade this appliance to version 7.6 and restart it.

After the original *full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *full policy source* machine to point to the original *full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance and restart it.
2. On the previously upgraded secondary appliance, in the V-Series console, move to the page **Configuration > Web Security Components**.
3. For **Policy Source**, select **User directory and filtering** or **Filtering only** and enter the IP address of the primary appliance. Save the setting.
4. Use the version 7.6 Websense installer to upgrade remaining off-appliance components. See *Upgrading Web Security or Web Filter to 7.6.0*, page 829 for instructions.

## Upgrading clustered appliances

Upgrading clustered appliances to version 7.6 requires a service disruption while each node of the cluster is upgraded.

Members of the cluster are upgraded serially, restarted, and then Content Gateway services are stopped until all nodes are upgraded. Then Content Gateway is started on all members of the cluster.

> **Important**
>
> Full clustering is not supported in version 7.6. Prior to upgrading a V-Series appliance, it must be configured to Single Node (i.e., not clustered). After upgrade, you can set the appliance to Management Clustering if you want. However, note that this is a different type of clustering than full clustering. See the Content Gateway Manager Help for more information.

1. Follow the *Upgrade instructions*.
2. After the restart is complete, when all services are available, immediately stop the Content Gateway services.
   a. Log on to the Appliance Manager.
   b. Navigate to **Status** > **Modules**.
   c. In the **Websense Content Gateway** area, click **Stop Services**.
   d. When prompted, click **OK** to continue.

   > **Note**
   > If Virtual IP is enabled, for a short time there will be an IP address conflict. After Content Gateway services are stopped, the conflict goes away.

3. Repeat steps 1 and 2 for every node in the cluster.
4. When all nodes have been upgraded, start the Content Gateway services on each node.
   a. Log on to the Appliance Manager.
   b. Navigate to **Status > Modules**.
   c. In the **Websense Content Gateway** area, click **Start Services**.

# Post-upgrade activities

- Perform the Content Gateway *Post upgrade activities*, page 862.
- *Verify Network Agent settings*, page 915
- *Check Tunneled Protocol Detection and Rich Internet Scanning settings*, page 915

## Verify Network Agent settings

After upgrading a **filtering only** V-Series appliance to version 7.6, use TRITON - Web Security to verify your Network Agent local settings. Go to Settings > Network Agent, highlight the Global option, and select the Network Agent IP address (the IP address of the appliance C interface). Then verify:

- The **Filtering Service IP address**.This is usually the IP address of the C interface.
- The option selected for **If Filtering Service is unavailable** (Permit or Block).
- The **HTTP traffic** and **Configure this Network Agent instance to ignore traffic...** options under Advanced Network Agent Settings.

After caching and saving any changes to these settings, select the **NIC-2** link in the Network Interface Cards table to open the NIC Configuration page. Verify that:

- The **Integrations** section shows the correct logging and filtering settings.
- The **Protocol Management** include the correct filtering and bandwidth measurement settings.

Be sure to cache and save any changes.

## Check Tunneled Protocol Detection and Rich Internet Scanning settings

After upgrading, Tunneled Protocol Detection and Rich Internet Scanning become enabled by default (even if they were disabled prior to upgrade). Due to system resources used by these features, they should be disabled if you do not use them.

# 57 Upgrading or Merging Administrators

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## In this topic



## Overview

This article discusses what happens to Websense administrator accounts when upgrading from prior-version Web Security or Data Security solutions to version 7.6. It also describes what occurs when version 7.6 administrator accounts are restored from a backup to an existing system that already has administrator accounts configured.

For information about which prior versions are supported for upgrade and the upgrade process, see the version 7.6 Upgrade Center.

# admin account

For version 7.6, the default, built-in Global Security Administrator account is named **admin**. This account has access to all administrative and management functions in the TRITON Unified Security Center. The account replaces the Web Security **WebsenseAdministrator** and Data Security **admin** accounts from prior versions.

# Upgrading

## Upgrading Web Security

When upgrading Web Security solutions to 7.6, Websense administrator accounts are upgraded as described here.

### WebsenseAdministrator

This built-in default account is no longer used in version 7.6 TRITON Unified Security Center. Upon upgrade it is replaced by an account named**admin** which is the built-in default Global Security Administrator account in 7.6 TRITON Unified Security Center.

During installation of version 7.6 TRITON Unified Security Center, you are asked for a password to be used for the **admin** account.

If a prior-version Websense appliance is running on-appliance TRITON - Web Security, it is upgraded to version 7.6 TRITON Unified Security Center (Web Security module only). In this case, the **admin** account will be automatically configured to the password of the prior-version **WebsenseAdministrator** account.

### Local accounts

Websense administrator accounts not authenticated against a directory service are referred to as *local* accounts. Local administrator accounts will appear in the upgraded system, however they must be assigned email addresses. In version 7.6, all administrator accounts must have an email address.

Users will still be able to use these accounts to log in to TRITON Unified Security Center. However, no changes in permissions can be made to them until an email address is specified. Also, without an email address, these accounts cannot use the password recovery feature or receive alerts.

### Network accounts

Websense administrator accounts authenticated against a directory service are referred to as *network* accounts. The directory service used to authenticate network administrator accounts prior to upgrade will be used by version 7.6 TRITON Unified Security Center to authenticate network administrator accounts. Like local

administrator accounts, prior-version network administrator accounts do not have email addresses specified. As part of the upgrade process, if the directory service contains an email address for a network administrator account, that address is automatically assigned to it in version 7.6 TRITON Unified Security Center.

**Important**

Prior to upgrade, if you are using Windows NT Directory to authenticate administrator accounts, configure the system to use a directory service supported in version 7.6 (see *Windows NT Directory* below).

### Windows NT Directory

Prior to upgrade, if Windows NT Directory or Windows NT Directory/Active Directory (Mixed Mode) is used to authenticate network administrator accounts, configure the system to use a directory service supported in version 7.6 (see version 7.6 System Requirements). **Do this prior to upgrade**.

This process involves selecting a version 7.6-supported directory service as Logon Directory and then replacing each Windows NT-based or Mixed Mode account with one on the new directory service (see TRITON - Web Security Help for instructions on removing and adding accounts).

If this is not done, the accounts will not be usable in version 7.6. They will still appear as Web Security delegated administrators in version 7.6 TRITON Unified Security Center. However, users will be unable to log in with those accounts. Also, those accounts cannot be removed.

### Other LDAP Directory

If Web Security has Logon Directory set to **Other LDAP Directory**—i.e., is configured to authenticate network administrator accounts against **Other LDAP Directory** instead of **Active Directory (Native Mode)** or **Windows NT Directory/ Active Directory (Mixed Mode)**—upon upgrade, network administrator accounts will be authenticated against **Generic Directory** in version 7.6 TRITON Unified Security Center. This occurs even if a directory service supported by version 7.6 TRITON Unified Security Center was the configured directory service prior to upgrade. Note that this does not happen if **Active Directory (Native Mode)** was the configured Logon Directory prior to upgrade; in that case Active Directory is used post-upgrade.

It is important after upgrade that you verify the configured directory service (log in to the TRITON Unified Security Center and go to **TRITON Settings** > **User Directory**). Make any changes necessary.

## Upgrading Data Security

When upgrading Data Security solutions to 7.6, Websense administrator accounts are upgraded as described here.

### admin

Upon upgrade the prior-version **admin** account is replaced by the version 7.6 **admin** account which is the built-in default Global Security Administrator account in 7.6 TRITON Unified Security Center.

During installation of version 7.6 TRITON Unified Security Center, you are asked for a password to be used for the **admin** account.

### Local accounts

Websense administrator accounts not authenticated against a directory service are referred to as *local* accounts. Local administrator accounts will appear in the upgraded system, however they must be assigned email addresses. In version 7.6, all administrator accounts must have an email address.

Users will still be able to use these accounts to log in to TRITON Unified Security Center. However, no changes in permissions can be made to them until an email address is specified. Also, without an email address, these accounts cannot use the password recovery feature or receive alerts.

### Network accounts

Websense administrator accounts authenticated against a directory service are referred to as *network* accounts. The directory service used to authenticate network administrator accounts prior to upgrade will be used by version 7.6 TRITON Unified Security Center to authenticate network administrator accounts. Like local administrator accounts, prior-version network administrator accounts do not have email addresses specified. As part of the upgrade process, if the directory service contains an email address for a network administrator account, that address is automatically assigned to it in version 7.6 TRITON Unified Security Center.

In version 7.5, Data Security administrator accounts could be authenticated against multiple directory services. Whichever was used as the primary directory service for authentication is used upon upgrade to version 7.6. Version 7.5 administrator accounts authenticated against a non-primary directory service will still appear in version 7.6. However, users will not be able to log in with those accounts until a Data Security Super Administrator configures them to work with the proper directory service.

## Upgrading Web Security Gateway Anywhere

Upgrading Web Security Gateway Anywhere involves both Web Security and Data Security administrator accounts. The application upgrade process for Web Security Gateway Anywhere comprises upgrading the Web Security portion to version 7.6 first and then upgrading (and merging) the Data Security portion.

Web Security administrator accounts are upgraded as described in *Upgrading Web Security*, page 918. It is important that local administrator accounts be assigned email addresses before merging Data Security accounts so proper merging can occur.

Next, Data Security administrator accounts are merged with the upgraded Web Security administrator accounts. Note that if a directory service is not configured prior to the merging of Data Security accounts, the primary directory service used by the incoming Data Security accounts will be used by the version 7.6 system.

# Merging

When a TRITON backup is restored to a TRITON management server, the administrator accounts it contains must be merged with existing accounts.

## Local accounts

TRITON administrator accounts not authenticated against a directory service are referred to as *local* accounts. If an incoming (from backup restore or upgrade merge) local account matches an existing local account on both name and email address, it is merged with the existing account. The permissions currently defined for the existing account are used.

If an incoming account matches an existing local account on either name or email address, but not both, it is rejected.

If an incoming local account's name matches an existing network account, it is imported but has its name modified by appending *@local*. For example, an incoming account with name **user** would be imported into the TRITON Unified Security Center as **user@local**. A Global Security Administrator or the appropriate Security Administrator must verify renamed accounts and resolve them with existing accounts as necessary.

If an existing modified name is already used, then incremented numbers are also included. For example **user@local1**, **user@local2**, and so on.

## Network accounts

TRITON administrator accounts authenticated against a directory service are referred to as *network* accounts. The currently configured directory service is used to resolve incoming accounts. If not directory service is currently configured, then the directory service used by the incoming accounts is used.

Incoming accounts are matched to existing network accounts by LDAP distinguished name. If a match occurs, the account is merged with the existing account. The permissions currently defined for the existing account are used.

If an incoming network account's name matches that of an existing local account, it is imported but has its name modified by appending *@network*. For example, an incoming account with name *user* would be imported into the TRITON Unified Security Center as **user@network**. A Global Security Administrator or the appropriate Security Administrator must verify renamed accounts and resolve them with existing accounts as necessary.

If an existing modified name is already used, then incremented numbers are also included. For example **user@network1**, **user@network2**, and so on.

# 58 Starting or Stopping Web Security Services

## Applies to

- Web Filter 7.6
- Web Security 7.6
- Web Security Gateway 7.6
- Web Security Gateway Anywhere 7.6

## In this topic



## Overview

By default, Websense services are configured to start when the machine starts.

Occasionally, you may need to stop or start a Websense service. For example, Filtering Service must be stopped and started after customizing default block messages.

> **Note**
> When Filtering Service is started, CPU usage can be 90% or more for several minutes while the Websense Master Database is loaded into local memory.

# Manually stopping and starting services (Windows)

Use the Windows Services console to stop and start one or more Websense services:

1. Open the Windows Services console (Start > All Programs > Administrative Tools > Services).
2. Right-click a service name, and then select **Start**, **Stop**, or **Restart**. Restart stops the service, then restarts it again immediately from a single command.

   Refer to *Stopping and starting principal components*, page 925 for the correct order to use when stopping or starting multiple Websense services.

> **Warning**
> Do **not** use the **taskkill** command to stop Websense services. This may corrupt the services.

# Manually stopping and starting services (Linux)

Stop, start, or restart Websense services (daemons) from the command line on a Linux machine.

Restarting stops a daemon, then restarts it immediately from a single command. If Websense components are spread across multiple machines, be sure that Policy Broker and the Policy Database are stopped last and started first. See *Stopping and starting principal components*, page 925 for the preferred stopping and starting order.

There are two scripts to stop and start Websense services:

- WebsenseAdmin: can stop, start, or restart all Websense components together.
- WebsenseDaemonControl: can stop or start individual components.

> **Warning**
> Do **not** use the **kill** command to stop Websense services. This may corrupt the services.

## Stopping, starting, or restarting all services

1. Go to the Websense installation directory (/opt/Websense/, by default).
2. Use the following commands to stop, start, or restart all Websense services in the correct order:
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`
   - `./WebsenseAdmin restart`
3. View the running status of all Websense services with the following command:

```
./WebsenseAdmin status
```

## Stopping or starting individual services

1. Go to the Websense installation directory (/opt/Websense/, by default).
2. Enter the following command: `./WebsenseDaemonControl`.

   A list of installed components is displayed, showing whether each process is running or stopped.
3. Enter the letter associated with a component to start or stop the associated process.

   To refresh the list, enter `R`.
4. When you are finished, enter `Q` or `X` to exit the tool.

# Stopping and starting principal components

When stopping individual components on Windows machines, or when stopping components spread across multiple machines, stop the optional components first, and then the principal components, ending with the following, in the order shown:

1. Websense Network Agent
2. Websense Filtering Service
3. Websense User Service
4. Websense Policy Server
5. Websense Policy Broker
6. Websense Policy Database
7. Websense Control Service

When starting services, reverse this order. It is especially important that you begin with the following services, in the order shown:

1. Websense Control Service
2. Websense Policy Database
3. Websense Policy Broker
4. Websense Policy Server

Also remember that if you are stopping and starting services on the TRITON Unified Security Center machine, you may need to stop or start the following as well:

- Websense Web Reporting Tools
- Websense TRITON - Web Security

# 59 Default ports

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Overview

This article describes the default port numbers used by Websense products and components. It is important to note that these are default port numbers; some of them may have been changed during installation for your particular deployment.

These default port numbers apply to both Websense-appliance-based and software-based deployments.

Port information in this article is divided into the following sections:



## Data Security

The most robust and effective implementation of Data Security depends on certain ports being open to support the mechanics of the software. The table below lists the ports that need to remain open for all of the Data Security software/hardware configurations.

If you have a security policy in place, exclude these ports from that policy so that Data Security can operate properly. If you do not, the policy you have in place may disrupt Data Security functionality.

You can lock down or "harden" your security systems once these ports are open.

**Important**

Data Security agents and machines with a policy engine, such as a Data Security Server or Websense Content Gateway machine, must have direct connection to the Data Security Management Server (on the TRITON management server). When deployed in a DMZ or behind a firewall, the relevant ports must be allowed.

# Human interface device (Administrator Client)

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 19448 | UI browsing |
| TRITON - Data Security | 9443 | UI browsing |
| TRITON - Data Security | 3389 | Remote desktop |
| Protector | 22 | SSH |

## Inbound

(None)

# Data Endpoint Client

## Outbound

| To | Port | Purpose |
|---|---|---|
| Data Security Server | 443* | Connect to Endpoint Server |
| Data Security Server | 80** | Connect to Endpoint Server |

* You can choose between secured and unsecured connections. The default is secured (HTTPS, port 443).
** Optional

## Inbound

(None)

# Data Endpoint Server

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 443 | Retrieve fingerprints and natural language processing scripts |
| TRITON - Data Security | 8891 | Status |
| TRITON - Data Security | 17443 | Incidents |
| Endpoint Client | 80 | |

## Inbound

| From | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 443 | Retrieve fingerprints and natural language processing scripts |
| Endpoint Client | 80 | Incidents |
| Endpoint Client | 17443 | Incidents |
| Supplemental Data Security Server | 17444 | Retrieve fingerprints and natural language processing scripts |

# Printer Agent

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 443 | Secure communications |
| TRITON - Data Security | 8888 | Configuration and deployment |
| TRITON - Data Security | 8889 | Registration - MGMTD |
| TRITON - Data Security | 18404* | Secure content transport |
| TRITON - Data Security | 17443 | |
| Data Security Server | 8888 | Registration - MGMTD |
| Data Security Server | 18404 | Secure content transport |

* Necessary for load balancing with TRITON - Data Security.
** This is the default. Other ports can be configured.

## Inbound

(None)

# ISA Agent

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 443 | Secure communications |
| TRITON - Data Security | 8888 | Configuration and deployment |
| TRITON - Data Security | 8889 | Registration - MGMTD |
| TRITON - Data Security | 18404* | Secure content transport |
| Data Security Server | 8888 | Registration - MGMTD |
| Data Security Server | 18404 | Secure content transport |
| | 80 | |

* Necessary for load balancing with TRITON - Data Security.
** This is the default. Other ports can be configured.

## Inbound

(None)

# SMTP Agent

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 8888 | Configuration and deployment |
| TRITON - Data Security | 18404 | Secure communications |
| TRITON - Data Security | 8889 | Registration |
| Data Security Server | 8888 | Registration |
| Data Security Server | 18404 | Secure content transport |
| Next hop MTA | 25* | SMTP for inbound/outbound traffic |
| | | |
| * This is the default. Other ports can be configured. | | |

## Inbound

| From | Port | Purpose |
|---|---|---|
| Previous MTA | 25* | SMTP for inbound/outbound traffic |
| * This is the default. Other ports can be configured. | | |

# TRITON - Web Security

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 56992 | Linking Service |

## Inbound

| From | Port | Purpose |
|---|---|---|
| TRITON - Data Security, Data Security Server, Protector, Content Gateway | 56992 | Linking Service |

# Discovery and Fingerprint Agent (Crawler)

### Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 8888 | Configuration and deployment |
| TRITON - Data Security | 8889 | Registration |
| TRITON - Data Security | 443 | Secure communication |
| TRITON - Data Security | 5820 | Fingerprinting |
| TRITON - Data Security | 9080 | Resource resolution |
| Data Security Server | 8888 | Registration |
| Data Security Server | 18404 | Secure content transport |
| Data Security Server | 9080 | Resource resolution |
| Salesforce server | 80 or 8080 | Salesforce discovery |

### Inbound

| From | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 9797 | Crawler listening |

## Exchange Server

### Outbound

(None)

### Inbound

| From | Port | Purpose |
|---|---|---|
| Data Security Server - Discovery and Fingerprint Agent | 80 | Exchange discovery |
| Data Security Server - Discovery and Fingerprint Agent | 443 | Exchange discovery |

## File Server

### Outbound

(None)

### Inbound

| From | Port | Purpose |
|---|---|---|
| Discovery and Fingerprint Agent | 139 | File sharing access |
| Discovery and Fingerprint Agent | 445 | File sharing access |

## Sharepoint Server

### Outbound

(None)

### Inbound

| From | Port |
|---|---|
| Discovery and Fingerprint Agent | 80 |
| Discovery and Fingerprint Agent | 443 |

## Database Server

### Outbound

| To | Port | Purpose |
|---|---|---|
| Discovery and Fingerprint Agent | Varies | The port that allows connection to the database (according to database type) |

### Inbound

| From | Port | Purpose |
|---|---|---|
| Discovery and Fingerprint Agent | Varies | The port that allows connection to the database (according to database type) |

## TRITON - Data Security

### Outbound

(None)

### Inbound

| From | Port | Purpose |
|---|---|---|
| Data Security Server, Protector, Content Gateway | 8888 | Registration |
| Data Security Server, Protector, Content Gateway | 17443 | Incidents |
| Data Security Server, Protector, Content Gateway | 139 | File sharing |
| Data Security Server, Protector, Content Gateway | 443 | Secure communication |
| Data Security Server, Protector, Content Gateway | 445 | File sharing |
| Data Security Server, Protector, Content Gateway | 5819-5822 | Fingerprint repository |
| Data Security Server, Protector, Content Gateway | 8453 | User repository |
| Data Security Server, Protector, Content Gateway | 8005 | Tomcat server |
| Data Security Server, Protector, Content Gateway | 8889 | Registration |
| Data Security Server, Protector, Content Gateway | 18303 | Local agents analysis |
| Data Security Server, Protector, Content Gateway | 18404 | Analysis |
| Data Security Server, Protector, Content Gateway | 17444 | Fingerprint distribution |

## Data Security Server

### Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 17443 | Incidents |
| TRITON - Data Security | 18404 | Analysis |

### Inbound

| From | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 8888 | Registration |
| TRITON - Data Security | 8889 | |
| TRITON - Data Security | 8892 | Syslog |
| TRITON - Data Security | 139 | File sharing |
| TRITON - Data Security | 445 | File sharing |

## Content Gateway

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 80 | Fingerprint sync |
| TRITON - Data Security | 5821 | Fingerprint sync |
| TRITON - Data Security | 5819 | Non-default fingerprint detection |
| TRITON - Data Security | 8443 | Registration |
| TRITON - Data Security | 9443 | Syslog |
| TRITON - Data Security | 18303 | Local agents analysis |
| TRITON - Data Security | 8888 | MGMTD |
| TRITON - Data Security | 17444 | Retrieve fingerprints and natural language processing scripts |
| TRITON - Data Security | 8889 | MGMTD |
| Websense Web Security | 56992 | Linking Service |
| Data Security Server | 18404 | Analysis |

## Inbound

(None)

# Protector

## Outbound

| To | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 8888 | Settings deployment |
| TRITON - Data Security | 18303 | Local agents analysis |
| TRITON - Data Security | 5819 | Non-default fingerprint detection |
| TRITON - Data Security | 5821 | Fingerprint sync |
| TRITON - Data Security | 5820 | Fingerprint repository |
| TRITON - Data Security | 17443 | Syslog, forensics, incidents |
| TRITON - Data Security | 17444 | Pull configurations |
| TRITON - Data Security | 80 | Fingerprint sync |
| Data Security Server | 8888 | Settings deployment |
| Data Security Server | 8889 | MGMTD |
| Data Security Server | 8892 | MGMTD |
| Data Security Server | 18404 | Analysis |
| Data Security Server | 9080 | Analysis |
| Next hop MTA | 25* | SMTP |
| TRITON Unified Security Center | 56992 | Linking Service |
| Other | UDP<br>123 | Inbound/<br>outbound NTPD (available on the appliance yet disabled by default) |
| * Explicit MTA | | |

## Inbound

| From | Port | Purpose |
|---|---|---|
| TRITON - Data Security | 8888 | Settings deployment |
| Anywhere (including TRITON - Data Security) | 22 | SSH access |
| Data Security Server | 8888 | Settings deployment |
| Explicit MTA | 25* | SMTP |
| Explicit MTA | 10025* | SMTP, mail analysis |
| * Explicit MTA | | |

# ICAP client

### Outbound

(None)

### Inbound

| To | Port |
|---|---|
| Protector | 1344 |

## Email Security Gateway

The following ports are used on the Email Security Gateway appliance.

| Interface | Port | Direction | Description |
|---|---|---|---|
| C/E1/E2 | 6643 | Inbound | Personal Email Manager load balancing |
| C/E1/E2<br>(C recommended) | 6671 | Inbound | SSL proxy to be accessed by TRITON - Email Security |
| C/E1/E2 | 9449 | Inbound | Personal Email Manager user interface |
| E1/E2 | 8888 | Inbound | Email data loss prevention system health and log data |
| E1/E2 | 9080 | Inbound | Email data loss prevention resource allocation requests |
| E1/E2 | 25 | Inbound | SMTP |
| E1/E2 | 2525 | Inbound | Receipt of messages from Data Security for encryption |

The following ports are used on the appliance for connections to TRITON - Data Security.

| Interface | Port | Direction | Description |
|---|---|---|---|
| E1/E2 | 25 | Outbound | SMTP |
| E1/E2 8888 | | Outbound | Fingerprint status |
| E1/E2 | 5821 | Outbound | Fingerprint repository |
| E1/E2 | 17443 | Outbound | Registration, syslog, forensics, incidents |
| E1/E2 | 17444 | Outbound | Fingerprint download |
| E1/E2 | 18404 | Outbound | Message analysis |

The following ports are used by Email Security Gateway for off-appliance system components.

| Interface | Port | Direction | Description |
|---|---|---|---|
| E1/E2 | 9443 | Inbound | TRITON - Email Security (via TRITON Unified Security Center) |
| E1/E2 | 50800 | Outbound | Email Security Log Server |
| E1/E2 | 1433<br>1434 | Outbound | Email security log database default instance |
| E1/E2 | 443 | Outbound | Hybrid service |
| E1/E2 | 15868 | Outbound | Websense Web Filter |
| E1/E2 | 389<br>636 | Outbound | LDAP server |
| E1/E2 | 80 | Outbound | Database download server |
| E1/E2 | 53 | Outbound | DNS server |
| C | 162 | Outbound | SNMP Trap server |

# 60 Excluding Websense Files from Antivirus Scans

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## In this topic



## Overview

Antivirus scanning can degrade the performance of Websense components. This article lists folders and files that should be excluded from antivirus scans. Refer to your antivirus vendor's documentation for instructions on excluding files from scans.

> **Note**
> During installation of Websense products, disable antivirus software altogether. After installation, be sure to re-enable antivirus software.

## Websense installation folder

On Windows, Websense products are installed in subfolders of the Websense installation folder, by default *:\Program Files or Program Files (x86)\Websense. It is a best practice to exclude this folder and its subfolders from antivirus scans.

## Web security

It is a best practice to exclude the installation directory from antivirus scans. By default this directory is:

- **Windows**: Websense installation folder (see *Websense installation folder* above)
- **Linux**: /opt/Websense/

## Data security

It is a best practice to exclude the following from antivirus scans.

- Websense installation folder (see *Websense installation folder* above)
- *:\Program files\Microsoft SQL Server*.*
- C:\Documents and Settings\<user>\Local Settings\Temp*.*
- %WINDIR%\Temp*.*
- The forensics repository (configurable; defaults to Websense folder)

On non-management servers, such as Data Security analyzers, exclude the following directories from antivirus scanning:

- The folder where Data Security was installed: *:\Program Files or Program Files (x86)\Websense*.* by default.
- *:\Inetpub\mailroot*.* - (typically at the OS folder)
- *:\Inetpub\wwwroot*.* - (typically at the OS folder)
- C:\Documents and Settings\<user>\Local Settings\Temp*.*
- %WINDIR%\Temp*.*

- The forensics repository (configurable; defaults to Websense folder)

> **Note**
> Regarding the default installation folder locations in the list above, you can configure the software to install to other locations.
>
> The FP-Repository folder is usually located inside the installation folder, but can be configured to other locations.
>
> On endpoint installations, excluding the installation folder is sufficient.

The following directories should be excluded from the antivirus software that is deployed to endpoint clients:

- Endpoint processes: DSER.EXE and DSERUI.EXE
- EP adapter processes: EndPointClassifier.exe and kvoop.exe

## Email security

It is a best practice to exclude the Websense installation folder (see *Websense installation folder* above) and any Data Security folders that apply (see *Data security* above).

# 61 Migrating from MSDE to SQL Server 2008 R2 Express

## Applies to

- Web Filter 7.6
- Web Security 7.6
- Web Security Gateway 7.6
- Web Security Gateway Anywhere 7.6

## In this topic



## Overview

MSDE (Microsoft Desktop Engine) was supported by Websense Web security products prior to version 7.6. It is not supported for version 7.6.

This article contains instructions for migrating data from an existing installation of MSDE to SQL Server 2008 R2 Express for use by version 7.6 Websense Web security products.

In general, these procedures should be performed in conjunction with upgrading Web Security to version 7.6 (see *Upgrading Web Security or Web Filter to 7.6.0*, page 829). The instructions for upgrade will refer you to these procedures at appropriate points.

**Important**

Perform these procedures only on a properly operating installation of MSDE. Websense filtering and logging should be operating as normal. Performing this procedure will not fix a corrupted or inoperative installation of MSDE.

**Note**

For more about osql commands mentioned in these instructions, see Microsoft knowledge base article 325003 (http://support.microsoft.com/kb/325003) *How to manage the SQL Server Desktop Engine (MSDE 2000) or SQL Server 2005 Express Edition by using the osql utility*.

## Backing up Websense data from MSDE

It is a best practice to back up Websense data from MSDE and restore the back ups to SQL Server Express if you want to continue using the data on version 7.6 Web Security solutions. Alternatively, you can copy and then attach the data (see *Copying Websense data from MSDE*, page 946) or detach and then attach the data (see *Detaching Websense data from MSDE*, page 947)

1. Create a directory to hold database backups.
2. On the machine running Websense Log Server, stop Websense Log Server:

   Use the Microsoft Services console to stop Websense Log Server.
3. On the MSDE machine, perform a backup of prior-version Web security databases (wslogdb70, wslogdb70_1, and additional partitions if present) by issuing the following commands using the osql utility:

   ```
   osql -U sa -P <password>
   use master
   go
   backup database wslogdb70 to disk = '<path to backup directory>\wslogdb70.bak'
   go
   backup database wslogdb70_1 to disk = '<path to backup directory>\wslogdb70_1.bak'
   go
   ```

   Repeat the last two commands for each additional database partition (e.g. wslogdb70_2, wslogdb70_3, and so on).

# Restoring Websense data to SQL Server Express

Once you have installed SQL Server 2008 R2 Express (see *Obtaining SQL Server*, page 67) you can restore Websense data backed up from MSDE. If you copied or detached Websense data, instead of backing up, see *Attaching Websense data in SQL Server Express*, page 948.

1. Start SQL Server Management Studio (**Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **SQL Server Management Studio**
2. Log in to SQL Server.

   Use the credentials specified during installation of SQL Server Express.
3. In the Object Explorer, right-click **Databases** and select **Restore Database**.
4. In the **Restore Database** dialog box:
   a. Under **Destination for restore**, for **To database** type **wslogdb70**.
   b. Under **Source for restore**, select **From device** and click the browse button (  ).
   c. In the **Specify Backup** dialog box:
      - For **Backup media**, select **File**.
      - Click **Add**.
      - In the **Locate Backup File** dialog box, navigate to and then select the wslogdb70.bak file you created in MSDE.
      - Click **OK**.
   d. Under **Select the backup sets to restore**, select the **Restore** check box for the database that was entered above.
   e. Under **Select a page** (upper left of screen) select **Options** and verify the **Restore As** directory is correct. Also, make sure the currently logged-in user has write permissions for that directory path.

      If you wish to continue accessing the old Websense database files in MSDE, change the **Restore As** column for both the .mdf and .ldf files so they specify a different location. If you restore these files to the default location, you may not be able to do so without overwriting the current versions of those files. If you overwrite the current versions, MSDE will no longer be able to work with them. Note that this applies only to working with old data in MSDE. Version 7.6 Web Security will use SQL Server Express for its data.
   f. Select **OK** to restore.

      If an error appears stating the file cannot be restored over an existing file, click OK. Go to the **Options** page. Choose to restore the files to a different location than currently existing versions. See Step e for instructions.

      If an error appears stating the file is in use by another process, click OK. Go to the **Options** page. Choose to restore the files to a different location than currently existing versions. See Step e for instructions.
   g. Repeat this process for each database partition (e.g., wslogdb70_1.bak, wslogdb70_2.bak, and so on).

5. Review the SQL Server Express error logs. Resolve any issues before continuing.
6. If you are running SQL Server Express on the same machine as MSDE, it is a best practice to disable MSDE services. See *Disabling MSDE services after upgrade*, page 949.

If you prefer to issue T-SQL commands to restore databases, here are sample commands:

```
use master;
go
restore database wslogdb70
from disk ='<path>\<file_name>'
with
move 'wslogdb70' to '<target_path>\wslogdb70.mdf',
move 'wslogdb70_log.ldf' to
'<target_path>\wslogdb70_log.ldf'
go
restore database wslogdb70_1
from disk ='<path>\<file_name>'
with
move 'wslogdb70_1' to '<target_path>\wslogdb70_1.mdf',
move 'wslogdb70_1_log.ldf' to
'<target_path>\wslogdb70_1_log.ldf'
go
```

(*repeat for any other database partitions, e.g., wslogdb70_2, wslogdb70_3, and so on*)

# Copying Websense data from MSDE

It is a best practice to use the a backup-restore method for moving Websense data from MSDE to SQL Server Express (see*Backing up Websense data from MSDE*, page 944). However, you may copy .mdf and .ldf files to move the data instead.

1. Create a directory to hold database backups.
2. On the machine running Websense Log Server, stop Websense Log Server:

   Use the Microsoft Services console to stop Websense Log Server.
3. On the MSDE machine, using the Microsoft Services console, stop the MSSQLSERVER service (this stops MSDE).
4. Copy the following files to the backup directory you created in Step 1:
   - wslogdb70.mdf and wslogdb70.ldf
   - wslogdb70_1.mdf and wslogdb70_1.ldf

- .mdf and .ldf files for any other partitions, e.g., wslogdb70_2.mdf and wslogdb70_2.ldf, wslogdb70_3.mdf and wslogdb70_3.ldf, and so on.

By default, these files are located in either C:\Program Files\Websense (if Log Server is installed on the same machine as MSDE) or C:\Program Files\Microsoft SQL Server (if Log Server is not on the MSDE machine).

After installing SQL Server 2008 R2 Express, attach the data you copied from MSDE. See *Attaching Websense data in SQL Server Express*, page 948.

## Detaching Websense data from MSDE

It is a best practice to use the a backup-restore method for moving Websense data from MSDE to SQL Server Express (see*Backing up Websense data from MSDE*, page 944). However, you may detach and attach database files to move the data instead.

1. Create a directory to hold database backups.
2. On the machine running Websense Log Server, stop and disable Websense Log Server:

   Use the Microsoft Services console to stop Websense Log Server.
3. Detach Websense databases in MSDE.

   For example, using osql to log in to the database, use the following commands:

   ```
   use master
   go
   exec sp_detach_db 'wslogdb70'
   go
   exec sp_detach_db 'wslogdb70_1'
   go
   ```

   (*repeat for any other database partitions, e.g., wslogdb70_2, wslogdb70_3, and so on*)
4. Move the following files to the backup directory you created in Step 1:
   - wslogdb70.mdf and wslogdb70.ldf
   - wslogdb70_1.mdf and wslogdb70_1.ldf
   - .mdf and .ldf files for any other partitions, e.g., wslogdb70_2.mdf and wslogdb70_2.ldf, wslogdb70_3.mdf and wslogdb70_3.ldf, and so on.

   By default, these files are located in either C:\Program Files\Websense (if Log Server is installed on the same machine as MSDE) or C:\Program Files\Microsoft SQL Server (if Log Server is not on the MSDE machine).

After installing SQL Server Express, attach the data you detached from MSDE. See *Attaching Websense data in SQL Server Express*, page 948.

# Attaching Websense data in SQL Server Express

1. Start SQL Server Management Studio (**Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **SQL Server Management Studio**
2. Log in to SQL Server.

   Use the credentials specified during installation of SQL Server Express.
3. In the Object Explorer, right-click **Databases** and select **Attach**.
4. In the **Attach Databases** dialog box, select database files:
   a. Click **Add**.
   b. In the **Locate Database Files** dialog box, navigate to and then select the wslogdb70.mdf file you created in MSDE.
   c. Click **OK**.
   d. Repeat from Step a for each database partition (e.g., wslogdb70_1.mdf, wslogdb70_2.mdf, and so on).

   Under **Databases to attach**, click each line and view the **<*name*> database details** section to verify the information for each database file.
5. Click **OK**.
6. If you are running SQL Server Express on the same machine as MSDE, it is a best practice to disable MSDE services. See *Disabling MSDE services after upgrade*, page 949.

If you prefer to issue T-SQL commands to attach databases, here are sample commands (executed in Query window or sqlcmd command prompt):

```
use master
go
exec sp_attach_db @dbname = N'wslogdb70',
    @filename1 = N'<path>\wslogdb70.mdf',
    @filename2 = N'<path>\wslogdb70_log.ldf';
go
exec sp_attach_db @dbname = N'wslogdb70_1',
    @filename1 = N'<path>\wslogdb70_1.mdf',
    @filename2 = N'<path>\wslogdb70_1_log.ldf';
go
```

(*repeat for all remaining database partitions, e.g., wslogdb70_2, wslogdb70_3, and so on*)

# Configuring 7.5 Log Server to SQL Server Express prior to upgrade to 7.6

MSDE is no longer supported by Websense solutions in verison 7.6. In its place, SQL Server 2008 R2 Express (SQL Server Express) is supported.

When you upgrade a version 7.1 or 7.5 deployment, you can choose to use SQL Server Express in version 7.6. In this case, if Log Server was configured to use MSDE to store Websense data, the data must be migrated and then Log Server configured to use the installation of SQL Server Express prior to upgrading. The Websense installer is unable to upgrade Log Server if it is configured to MSDE.

Complete the following steps to configure Log Server to SQL Server Express.

1. On the Log Server machine, update the ODBC connection to the Log Database:
   a. On the Log Server machine, open the ODBC Data Source Administrator (**Control Panel** > **Administrative Tools** > **Data Sources (ODBC)**).
   b. On the **System DSN** tab, select the Websense database (by default **wslogdb70**), and then click **Configure**.
   c. On the first screen in the Microsoft SQL Server DSN Configuration wizard, for **Server**, select the SQL Server Express instance on the SQL Server Express machine, either default instance (host name of SQL Server Express machine) or TRITONSQL2K8R2X.

      If you named the database instance something other than default or TRITONSQL2K8R2X, then select that instance instead.
   d. Follow the on-screen instructions to update and verify the connection.
2. Refresh the Log Server connection to the database:
   a. Open the Log Server Configuration utility (**Start** > **Programs** > **Websense** > **Utilities** > **Log Server Configuration**) and select the **Database** tab.
   b. Click the **Connection** button.
   c. In the **Machine Data Source** tab, select the appropriate **Data Source Name**, and then click **OK**.
   d. Enter the user name and password for the SQL Server account, and then click **OK**.
   e. Click **Apply** in the Log Server Configuration window to save the change.
   f. Click **Start** on the **Connection** tab to restart the Log Server service.
3. Click **OK** to close Log Server Configuration.

# Disabling MSDE services after upgrade

If SQL Server Express is installed on the same machine as MSDE, it is a best practice to disable MSDE so it does not consume system resources which can affect the performance of SQL Server Express.

Using the Windows Services console to stop the following services:

- MSSQLSERVER
- SQLSERVERAGENT

# 62 Changing the IP Address, Host Name, or Domain of the TRITON Management Server

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## In this topic

# Overview

If you modify the IP address, host name, or domain membership of the *TRITON management server*, you must make configuration changes to the TRITON Unified Security Center to reflect the modification.

**Important**

This article applies to only the management components on a TRITON management server. If you have other Websense components on this machine, additional configuration (not covered in this article) may be necessary for those components to operate properly after changing IP address, host name, or domain membership.

See *Management components* for more information.

Each module of the *TRITON Unified Security Center* must be configured separately. Depending on your subscription, you may not have all modules enabled. In the procedures below, complete the steps for only the modules that are active (see *Management components*).

Which machine attribute you change determines which configuration steps are required. See the following:

- *Changing the IP address of the TRITON management server*, page 955
- *Changing host name or domain of the TRITON management server*, page 957

# Management components

This article applies to only the management components on a TRITON management server. Any other Websense components on this machine may need additional configuration that is not covered in this article.

Management components are (service names shown):

- Websense Data Security Management Server
- Websense Data Security Manager
- Websense Data Security Policy Engine
- Websense Data Security PreciseID Database
- Websense Data Security Web Server
- Websense Data Security Work Scheduler
- Websense Explorer Report Scheduler
- Websense Information Service for Explorer
- Websense Linking Service

- Websense Web Security Log Server
- Websense Reporter Scheduler
- Websense RTM Client
- Websense RTM Database
- Websense RTM Server
- Websense TRITON - Web Security
- Websense TRITON Web Server
- Websense TRITON Reporting Database
- Websense TRITON Settings Database
- Websense TRITON Unified Security Center
- Websense Web Reporting Tools
- Websense Control Service
- Websense TRITON - Email Security
- Websense Email Security Log Server

Note that you may not have all the above components installed on your machine. As long as the components that are installed are listed above, this article applies to you.

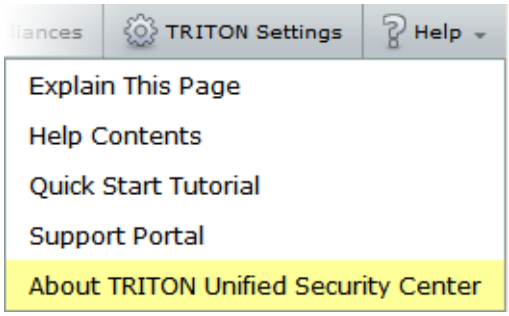
If you have additional components, not listed above, search the Websense knowledge base (at www.websense.com/support) for information about configuring those components after an IP address, host name, or domain membership change. If you need further assistance, please contact Websense Technical Support.

## Determining which TRITON Unified Security Center modules are active

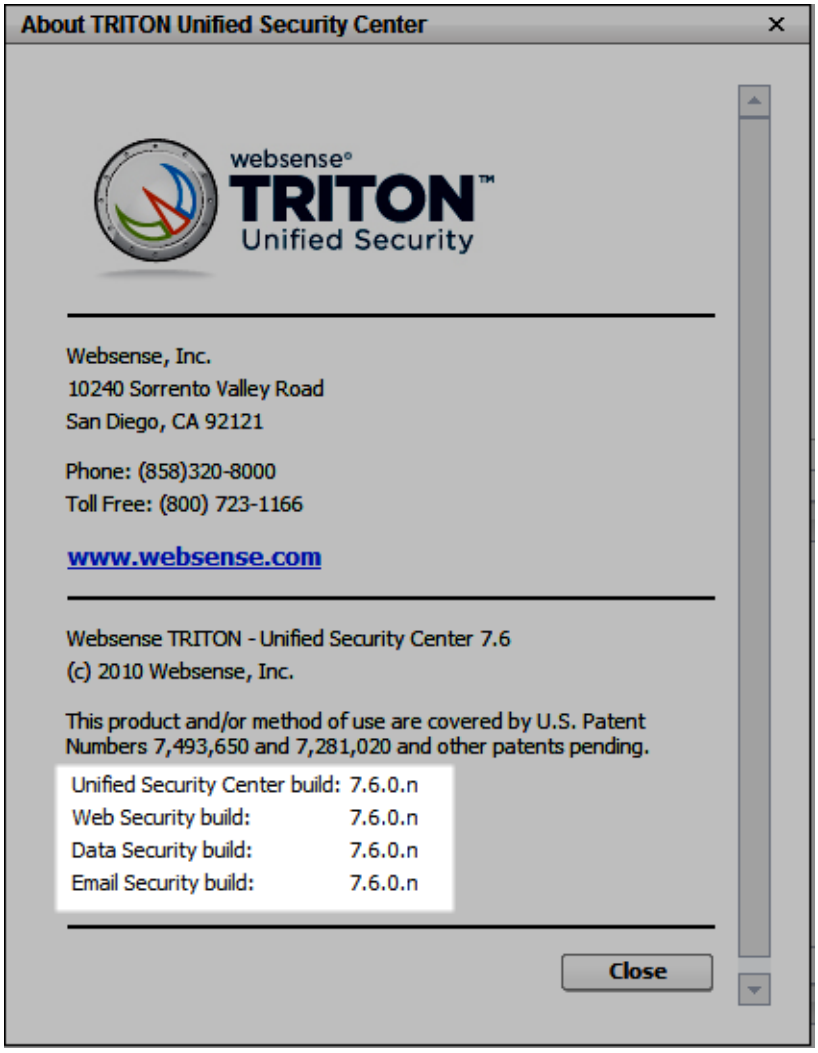
Depending on your subscription, one or more modules in the TRITON Unified Security Center may not be active.

To determine which modules are active:

1. In the TRITON Unified Security Center, go to **Help** > **About TRITON Unified Security Center**.



2. The About TRITON Unified Security Center dialog box lists the modules that are active (highlighted in illustration below).




## Installation folder

By default, the installation folder under which Websense software is installed is:

- **C:\Program Files (x86)\Websense** (on 64-bit Windows)
- **C:\Program Files\Websense** (on 32-bit Windows)

# Changing the IP address of the TRITON management server

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Changing the IP address of the TRITON management server

Complete these steps if you have changed the IP address of the *TRITON management server*.

> **Note**
> You may not be required to complete all steps below. Depending on your subscription, not all TRITON Unified Security Center modules may be active.

1. If you have not done so already, change the IP address of the TRITON management server machine at the operating system level (i.e., in Windows).
2. Update TRITON Infrastructure with the new IP address.

   See *Configuring TRITON Infrastructure to new IP address, host name, or domain*, page 958 for instructions.

   If SQL Server 2008 R2 Express (SQL Server Express) is installed on this machine, it will be automatically configured to the new IP address along with TRITON Infrastructure.
3. (*TRITON - Web Security only*)
   Update the configuration of the TRITON - Web Security module to reflect the new IP address:
   a. Recreate Apache SSL certificates for the TRITON - Web Security module. See *Creating Apache SSL Certificates*, page 973. When following these instructions, be sure to edit the openssl.txt file to reflect the new IP address of the TRITON management server.
   b. Edit the TRITON - Web Security catalina.properties file to reflect the new IP address. See *Configuring Tomcat to a new local IP address*, page 959.

4. (*TRITON - Email Security only*)
   Edit the TRITON - Email Security **catalina.properties** file to reflect the new IP address. See *Configuring Tomcat to a new local IP address*, page 959.
5. (*TRITON - Email Security only*)
   If Email Security Log Server is installed on the TRITON management server machine, update TRITON Unified Security Center with its new IP address. See *Updating the IP address for Email Security Log Server*, page 960.

   > **Note**
   > This is required only for those appliances using the Email Security Log Server located on the TRITON management server machine. If an appliance is using an Email Security Log Server located elsewhere, do not update its IP address on that appliance.

   If you have multiple Email Security Gateway appliances in your deployment, update them as well with the new IP address of Email Security Log Server. To update other appliances, complete the steps again in *Updating the IP address for Email Security Log Server*, page 960 with the following modifications:

   a. After logging into the TRITON Unified Security Center, click **Appliances** in the TRITON Unified Security Center banner.
   b. Click **Manage Appliances** and select the appliance you want to update.
   c. Continue with the rest of the procedure as normal.
   d. Repeat this process for each Email Security Gateway appliance that uses the Email Security Log Server located on the TRITON management server machine.
6. (*TRITON - Email Security only*)
   If the Email Security log database is located on the TRITON management server machine (e.g., SQL Server 2008 R2 Express is installed on the machine and maintains the log database), update the log database location in TRITON Unified Security Center. See *Updating the log database location for Email Security Gateway*, page 961.
7. (*TRITON - Data Security only*)
   Modify the Data Security Management Server installation to reflect the change. See *Changing the IP address of the Data Security Management Server*, page 964.
8. (*TRITON - Web Security only*)
   If Real-Time Monitor is installed on the TRITON management server (i.e., RTM Server, RTM Database, RTM Client services running), restart RTM Server and Client:

   In a Command Prompt execute the following commands.

   ```
   net stop WebsenseRTM
   netstart WebsenseRTM
   net stop WebsenseRtmTomcat
   net start WebsenseRtmTomcat
   ```

9. If your subscription includes Websense Web Security Gateway Anywhere, Email Security Gateway, or Email Security Gateway Anywhere, re-register them with Data Security Management Server (located on the TRITON management server machine). This is required for Web and email DLP (data loss prevention) features.

   For Web Security Gateway Anywhere, see *To enable data loss prevention over Web channels, you must connect the Content Gateway module of your Web security solution to the Data Security Management Server. Follow these steps to establish that connection:*, page 969.

   For Email Security Gateway, see *Re-registering Email Security Gateway with Data Security*, page 962.

# Changing host name or domain of the TRITON management server

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Changing host name or domain of the TRITON management server

Complete these steps if you have changed the host name or domain membership of the *TRITON management server*.

> **Note**
> You may not be required to complete all steps below. Depending on your subscription, only some TRITON Unified Security Center modules may be active.

1. If you have not done so already, change the host name or domain membership of the TRITON management server machine at the operating system level (i.e., in Windows).

   Note that changing the host name or domain membership typically requires a reboot of the machine.

2. Update TRITON Infrastructure with the new host name or domain.

See *Configuring TRITON Infrastructure to new IP address, host name, or domain*, page 958 for instructions.

If SQL Server 2008 R2 Express (SQL Server Express) is installed on this machine, it is **not** automatically ocnfigured to use the new host name or domain along with TRITON Infrastructure. It must be configured separately. See the following Microsoft article for instructions:

http://msdn.microsoft.com/en-us/library/ms143799.aspx

3. (*TRITON - Web Security only*)
   Edit the TRITON - Web Security module's configuration to reflect the new host name. See *Configuring TRITON - Web Security with new host name*, page 963.
4. (*TRITON - Data Security only*)
   Modify the Data Security Management Server installation to reflect the change. See *Changing the domain of a Data Security Server*, page 800.

# Configuring TRITON Infrastructure to new IP address, host name, or domain

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Configuring TRITON Infrastructure to new IP address, host name, or domain

If you change the IP address, host name, or domain of the TRITON management server, TRITON Infrastructure's configuration must be modified to reflect the change.

> **Note**
> If SQL Server 2008 R2 Express is installed on the TRITON management server, completing these steps will not update it to a new IP address, host name, or domain. This must be done separately. See

1. Launch the Websense installer.

If you chose to keep installer files the last time you ran the installer, you can launch it without re-extracting files by going to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.

2. In the installer, for TRITON Infrastructure, select the **Modify** link.
3. Accept the defaults in the installer screens and click **Next**, until you reach the **Server IP Address** screen.
4. If you changed the IP address of the TRITON management server, select the new IP address in the **Server IP Address** screen.
5. If you changed the host name or domain of the TRITON management server, the installer will automatically detect the new settings and configure TRITON Infrastructure.
6. Proceed through the remaining installer screens, accepting defaults, and click **Finish**.

# Configuring Tomcat to a new local IP address

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Configuring Tomcat to a new local IP address

If you have changed the IP address of the TRITON management server, you must complete the following steps to update the Tomcat configuration for the TRITON - Web Security or TRITON - Email Security module.

**Note**

Tomcat configuration for TRITON Infrastructure and TRITON - Data Security is done automatically when configuring to new IP address, host name, or domain. See *Configuring TRITON Infrastructure to new IP address, host name, or domain*, page 958.

> **Warning**
> This procedure involves editing configuration files. Before editing any file make a backup copy of it. This allows you to revert to original, unmodified files if any issues arise.

1. Open the following file in a text editor:
   - TRITON - Web Security:

     <*Installation folder*>\Web Security\tomcat\conf\catalina.properties
   - TRITON - Email Security:

     <*Installation folder*>\Email Security\ESG Manager\tomcat\conf\catalina.properties
2. In the file, edit the following value to reflect the new IP address:
   - TRITON - Web Security:

     java-fw.ip
   - TRITON - Email Security:

     manager_ip
3. Save and close the catalina.properties file.
4. Using the Windows Services console (**Start** > **Control Panel** > **Administrative Tools** > **Services**), restart the service for the module you want to update:
   - Websense TRITON - Web Security
   - Websense TRITON - Email Security

# Updating the IP address for Email Security Log Server

## Applies to

- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Updating the IP address for Email Security Log Server

If the IP address of the machine running Email Security Log Server is changed, you must update TRITON Unified Security Center to use the new address.

1. Log on to the TRITON Unified Security Center and click **Email Security**.
2. In **Settings** > **Log Server**, enter the new IP address in the **Server IP address** field.
3. Click **Save**.

# Updating the log database location for Email Security Gateway

## Applies to

- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Updating the log database location for Email Security Gateway

If the IP address of the Email Security database (i.e., the IP address of the machine running SQL Server or SQL Express) has changed, you must update TRITON Unified Security Center and Email Security Log Server to use the new address.

Even if the Email Security database is located on the same machine as TRITON Unified Security Center or Email Security Log Server, you must complete these steps.

1. Log on to the TRITON Unified Security Center and click **Email Security**.
2. In **Settings** > **Log Database**, enter the new IP address in the **Log database** field.

   If the Email Security database is located on the TRITON management server itself and you are performing this procedure because you changed the IP address of the TRITON management server, you should enter its new IP address here.
3. Click **OK** (in the Log Database Location area of the screen).

   Leave the TRITON Unified Security Center at this screen.You will come back to it later to complete this procedure.
4. On the machine running Email Security Log Server, start the Log Server Configuration utility (**Start** > **Programs** > **Websense** > **Email Security** > **Log Server Configuration**).
5. In the utility, on the **Database** tab, click **Connection**.
6. In the **Select Data Source** dialog box, on the **Machine Data Source** tab, click **New**.

   You will create a new data source connection to the new IP address of the Email Security database.
7. In the **Create New Data Source** wizard that appears, select **System Data Source (Applies to this machine only)** and then click **Next**.
8. In the list of drivers, select **SQL Server** and then click **Next**.
9. In the next dialog box, click **Finish**.
10. In the **Create a New Data Source to SQL Server** wizard, enter a **Name**, **Description**, and the **Server** IP address for the new data source connection. Then click **Next**.

    The server IP address should be the new IP address of the machine on which the Email Security database is located. If the database is located on the TRITON

management server and you are performing this procedure because you have changed the management server's IP address, enter its new IP address here.

11. In the next dialog box, select options as described below.
    a. Select an authentication method for connecting to the database:
       - **With Windows NT authentication using the network login ID**: to use a Windows trusted account.
       - **With SQL Server authentication using a login ID and password entered by the user**: to use a SQL Server account.
    b. Enable **Connect to SQL Server to obtain default settings for the additional configuration options**.
    c. Enter the **Login ID** and **Password** of the *sa* SQL Server account if you selected SQL Server authentication in Step a above).
    d. Click **Next**.
12. In the next dialog box, enable **Change the default database to** and then select **esglogdb76** from the drop-down menu. Then click **Next**.
13. In the next dialog box, accept the default settings and click **Finish**.
14. Click **Test Data Source** to test the connection. Upon test success, click **OK**.
15. Click **OK** again.
16. Click **OK** again.
17. In the SQL Server Login dialog box, enter a **Login ID** (by default, sa) and **Password**. Then click **OK**.

    If you choose to **Use Trusted Connection** (i.e., Windows NT authentication), Login ID and Password are not necessary.
18. In the Log Server Configuration utility, click **Apply** and then **OK** to the warning message about stopping and restarting Log Server.
19. On the **Connection** tab, under **Service Status**, click **Stop**.

    This stops Email Security Log Server.
20. Click the same button (it now is labeled **Start**).

    This starts Email Security Log Server. It is now configured to use the new Email Security database location.
21. Click **OK** to close the Log Server Configuration utility.

# Re-registering Email Security Gateway with Data Security

## Applies to

- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## Re-registering Email Security Gateway with Data Security

If the IP address of the TRITON management server has changed, you must re-register Email Security Gateway with Data Security Management Server (which is located on the TRITON management server).

1. Log on to the TRITON Unified Security Center and click **Email Security**.
2. In **Settings** > **Data Security**, click **Unregister**.
3. (Only if automatic registration is disabled) Enter the new IP address in the **IP address** field.
4. Click **Register**.

# Configuring TRITON - Web Security with new host name

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6

## Configuring TRITON - Web Security with new host name

If the host name of the TRITON management server has changed, you must edit the TRITON - Web Security module's configuration to reflect the change.

**Warning**

This procedure involves editing configuration files. Before editing any file make a backup copy of it. This allows you to revert to original, unmodified files if any issues arise.

1. Open the following file in a text editor:

   <*Installation folder*>\Web Security\apache\conf\httpd.conf
2. In the httpd.conf file, edit the **ServerName** property to reflect the new host name.

   ServerName is specified in the form <*host name*>:<*port*>, for example:

   **ServerName ExampleServer01:18080**. Edit only the <*host name*> portion.
3. Save and close the httpd.conf file.
4. Open the following file in a text editor:

   <*Installation folder*>\Web Security\apache\conf\extra\httpd-ssl.conf
5. In the httpd-ssl.conf file, edit the **ServerName** property to reflect the new host name.

In the httpd-ssl.conf file, ServerName is specified in the same form as in the httpd.conf file mentioned above, <*host name*>:<*port*>. Edit only the <*host name*> portion.

6. Save and close the httpd-ssl.conf file.
7. Using the Windows Services console (**Start** > **Control Panel** > **Administrative Tools** > **Services**), restart the **Websense Web Reporting Tools** service.

# Changing the IP address of the Data Security Management Server

**Important**

If you change both the IP address and host name of a server (or the IP address and domain):

- You must complete the entire process of updating one before starting to change the other (and wait for all endpoints to be updated).
- If any endpoints are not connected to the network when settings are deployed, you must create a new endpoint package using the package-building tool, and use SMS or a similar mechanism to install the new package on these endpoints. See *Deploying Websense endpoints*, page 744 for information on creating and installing an endpoint package.

Websense recommends you perform this task during off hours, or route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.).

1. It is assumed you have already changed the IP address of the TRITON management server machine. If not, see *Changing the IP address of the TRITON management server*, page 955
2. Stop the protector:
   a. Log onto the protector as root.
   b. Execute “service pama stop”.
3. On the TRITON management server, launch the Websense installer.

   If you chose to keep installer files the last time you ran the installer, you can launch it without re-extracting files by going to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.
4. In the installer, for Data Security, select the **Modify** link.
5. Accept the defaults in the installer screens and click **Next**, until you reach the **Server Access** screen. Select the new IP address here.

6. If you changed the host name or domain of the TRITON management server, the installer will automatically detect the new settings and configure TRITON Infrastructure.
7. Proceed through the remaining installer screens, accepting defaults, and click **Finish**.
8. If you have a mail server relaying SMTP traffic to the Websense Data Security Management Server (SMTP agent), change its configuration to relay mail to the new Websense Data Security Management Server IP.
9. In TRITON - Data Security, change the IP address on the following screens, if necessary:
   a. **Settings > Configuration > System** > **Archive Storage**
   b. **Settings > Deployment > System Modules**. Choose the **SMTP Agent** and click the **Encryption & Bypass** tab.
10. Re-register all Websense Data Security stand-alone agents, such as: ISA agent, Exchange agent, and printer agent (See *Re-registering Websense Data Security components*, page 968).
11. Start the protector:
    a. Log onto the protector as root.
    b. Execute “service pama start”.
12. Click **Deploy** in TRITON - Data Security.
13. Since management server IP was changed, all endpoints must be reinstalled with the new IP. See *Deploying Websense endpoints*, page 744 for information on creating and installing an endpoint package.
14. Verify that new events appear in the traffic log, the system log doesn’t display errors, the endpoint status shows that endpoints are synchronized, and that new incidents are written into the data usage incident management screen.

# Changing the host name of the Data Security Management Server

## Applies to

- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

# Changing the host name of the Data Security Management Server

> **Note**
> To change both the IP address and host name of a server, you must complete the entire process of updating one before starting to change the other (and wait for all endpoints to be updated).

Websense recommends you perform this task during off hours, or to route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.).

1. It is assumed you have already changed the host name of the TRITON management server, if not see *Changing host name or domain of the TRITON management server*, page 957.
2. Stop the protector:
   a. Log onto the protector as root.
   b. Execute “service pama stop”.
3. On the TRITON management server, launch the Websense installer.

   If you chose to keep installer files the last time you ran the installer, you can launch it without re-extracting files by going to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.
4. In the installer, for Data Security, select the **Modify** link.
5. Click **Next** in the Installation Wizard until you get to **Local Administrator.**
6. Choose the new server name and the correct user name (in the form “NEWNAME\UserName”).
7. Start the protector:
   a. Log onto the protector as root.
   b. Execute “service pama start”.
8. Click **Next** to finish the modification.
9. (Optional) In TRITON - Data Security, change <New Server Name> in the following places:
   a. Select **Settings > System Modules**.
   b. Click the **Data Security Management Server.**
   c. One at a time, click the **Endpoint Server**, **Policy Engine**, **Forensics Repository**, **SMTP Agent**, **PreciseID Database**, and **Crawler**, and change the server name in the Name field.

10. Click **Deploy** in TRITON - Data Security.

> **Note**
> If any endpoints are not connected to the network when settings are deployed, they will not be updated. In this case, you must create a new endpoint package using the package-building tool, and use SMS or a similar mechanism to install the new package on these endpoints.
>
> See *Deploying Websense endpoints*, page 744 for information on creating and installing an endpoint package.

11. Verify that new events appear in the traffic log, the system log doesn't display errors, the endpoint status shows that endpoints are synchronized, and that new incidents are written into the data usage incident management screen.

# Changing the domain of the Data Security Management Server

## Applies to

- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

## In this topic



## Overview

It is a best practice to perform this task during off hours, or to route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.).

1. Stop the protector:
   a. Login to the protector as root.
   b. Execute "service pama stop".

### To join a Data Security Management Server to a domain

1. Create a Websense mail-enabled user inside the domain.
2. Add the management server machine into the domain - Do not restart the Domain Controller.
3. In TRITON - Data Security, import users from the directory service and add administrator roles privilege to the user that you created.
4. Make sure the DNS entries configured for the network card are pointing to a domain DNS server.
5. Restart the Data Security Management Server.
6. Perform the steps in *Changing the host name of the Data Security Management Server*, page 965.

### To remove a Data Security Management Server from a domain

1. Remove the management server machine from the domain - Do not restart the Domain Controller.
2. Restart the Data Security Management Server.
3. Perform the steps described in *Changing the host name of the Data Security Management Server*, page 965.

## Re-registering Websense Data Security components

### Applies to

- Websense Web Security Gateway Anywhere 7.6
- Websense Data Security 7.6
- Websense Email Security Gateway 7.6
- Websense Email Security Gateway Anywhere 7.6

### In this topic



### Overview

You must re-register all Data Security servers, agents, and protectors when you change the IP address, host name, or domain of the TRITON management server.

Before you start, make sure you know the user name and password of a Data Security administrator who has an access role with System Modules privileges.

## Data Security servers and agents

Go to each Data Security server and machine with a Data Security agent installed and do the following:

1. Launch the Websense installer.
2. In the installer, for Data Security, select the **Modify** link.
3. Accept the defaults in the installer screens and click **Next**, until you reach the **Register with the Data Security Server** screen.
4. In the **Register with the Data Security Server** screen, enter the new IP address of the TRITON management server along with the user name and password of a TRITON administrator.

When the installers finish:

1. Log onto TRITON - Data Security, navigate to **Settings > Deployment > System Modules** and verify that the components appears in the tree view.
2. Click **Deploy**.

## Protector

1. Log onto each protector as root.
2. Run “wizard securecomm”.
3. Enter the Data Security Management Server’s IP address along with the user name and password of a Data Security administrator with System Modules privileges.
4. Log onto TRITON - Data Security, navigate to **Settings > Deployment > System Modules** and verify that the protector appears in the tree view.
5. Click **Deploy**.

## Websense Content Gateway

To enable data loss prevention over Web channels, you must connect the Content Gateway module of your Web security solution to the Data Security Management Server. Follow these steps to establish that connection:

1. Ensure that Content Gateway and Data Security Management Server systems are running and accessible, and that their system clocks are approximately synchronized.
2. Ensure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Host name alone is not sufficient.

3. If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface ("C" on a V-Series appliance) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.
4. Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a V-Series appliance). Data Security Management Server uses the eth0 NIC during the registration process.

   After registration, the IP address can move to another network interface on the same machine; however, that IP address is used for configuration deployment and must be available as long as the 2 modules are registered.
5. From the Content Gateway Manager, select **Configure** > **Basic** > **General**.
6. Make sure Data Security is turned on (the **On** radio button and **Integrated on-box** must be selected). Now click the Not Registered link. This opens the **Configure** > **Security** > **Data Security** registration screen.
7. Enter the IP address of the Data Security Management Server.
8. Enter a user name and password for a Data Security administrator with Manage System Modules privileges.
9. Click **Register**. You are reminded to synchronize the system time between the proxy machine and the Data Security Management Server.
10. If registration succeeds, a Data Security Configuration page displays. Set the following configuration options:
    a. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Data Security for analysis and policy enforcement.
    b. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement.

    These options can be accessed whenever Data Security is registered by going to the **Configure** > **Security** > **Data Security** > **General** page.
11. Click **Apply**.
12. Restart Content Gateway.
13. Deploy the Content Gateway module by clicking **Deploy** in the TRITON - Data Security user interface.

## Troubleshooting the connection

This section contains troubleshooting tips for problems registering the Content Gateway with Data Security.

If you cannot register Websense Content Gateway with the Data Security Management Server (you receive an error in Content Gateway Manager) be sure that you can ping the Data Security Management Server from the proxy machine. (Go to the Linux command line and ping the IP address of the Data Security Management Server.)

If the ping fails, make sure that you have the correct IP address for the Data Security Management Server by going to that machine and running **ipconfig** from the command line.

If the proxy is on a V-Series appliance, try pinging the IPv4 address of the appliance's C interface from the Data Security Management Server.

If the proxy is not on a Websense appliance, try pinging the IPv4 address of the Content Gateway host system eth0 network interface from the Data Security Management Server. The registration process requires that Content Gateway is reachable on eth0. After registration, the IP address may move to another network interface on the system, but that IP address must remain available while the 2 modules are being registered.

If Content Gateway is deployed as a transparent proxy and the communication interface ("C" on a V-Series appliance) is subject to transparent routing, the registration process was likely intercepted by the transparent routing and prevented from completing. Ensure that traffic to and from the communication interface is not subject to transparent routing.

If registration still fails, make sure that neither the proxy machine nor the Data Security Management Server has a machine name with a hyphen in it. This has been known to cause registration problems.

And make sure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Host name alone is not sufficient to register the proxy with the Data Security Management Server.

# 63 Creating Apache SSL Certificates

## Applies to

- Websense Web Filter 7.6
- Websense Web Security 7.6
- Websense Web Security Gateway 7.6
- Websense Web Security Gateway Anywhere 7.6

## In this topic



## Overview

Complete the following procedure to create (or re-create) Apache SSL certificates for the TRITON - Web Security module of *TRITON management server*.

> **Note**
> These are basic instructions for creating certificates. Changing the password on certificates is not included in these steps. Avoid changing passwords if possible.

## Procedure

Perform these steps on the *TRITON management server*.

1. Using the Windows Services console (**Start** > **Control Panel** > **Administrative Tools** > **Services**), stop the following services:

- Websense TRITON - Web Security
- Websense Web Reporting Tools

2. Edit <*Installation folder*>\Web Security\apache\conf\ssl\openssl.txt if necessary.

   If you have changed the IP address of this machine, edit the IP address in the openssl.txt file to match.

> **Note**
> You can create a batch file to automate the tasks in Step 3-Step 8. See *Using a batch file for Apache SSL certificate file operations*. If you choose to create a batch file, execute it and then skip to Step 8.

3. In <*Installation folder*>\Web Security\apache\conf\ssl\automation\ run the following scripts in the following order:
   a. s1_newreq.bat
   b. s2_server_key.bat
   c. s3_server_crt.bat
   d. s4_server_p12.bat
4. Copy:
   <*Installation folder*>\Web Security\apache\conf\ssl\output\server.key to
   <*Installation folder*>\Web Security\apache\conf\ssl\ssl.key\server.key
5. Copy:
   <*Installation folder*>\Web Security\apache\conf\ssl\output\server.crt to
   <*Installation folder*>\Web Security\apache\conf\ssl\ssl.crt\server.crt
6. Copy:
   <*Installation folder*>\Web Security\apache\conf\ssl\output\cakey.pem to
   <*Installation folder*>\Web Security\apache\conf\ssl\private\cakey.pem
7. Copy:
   <*Installation folder*>\Web Security\apache\conf\ssl\output\manager.p12 to
   <*Installation folder*>\Web Security\tomcat\conf\keystore\tomcat\manager.p12
8. Using the Windows Services console, start the following services:
   - Websense TRITON - Web Security
   - Websense Web Reporting Tools

> **Note**
> For more information about Apache SSL go to http://www.apache-ssl.org/#FAQ.

# Using a batch file for Apache SSL certificate file operations

When creating Apache SSL certificates, there are several batch files to execute and files to copy. You can automate the process by creating and running a batch file.

The following is an example batch file you can use to create your own:

```
@echo off
set HOME=<Installation folder>\Web Security
set WORKING_DIR=%HOME%\apache\conf\ssl\automation
call "%WORKING_DIR%\s1_newreq.bat"
call "%WORKING_DIR%\s2_server_key.bat"
call "%WORKING_DIR%\s3_server_crt.bat"
call "%WORKING_DIR%\s4_server_p12.bat"


@echo on
copy "%HOME%\apache\conf\ssl\output\server.key"
"%HOME%\apache\conf\ssl\ssl.key\server.key"
copy "%HOME%\apache\conf\ssl\output\server.crt"
"%HOME%\apache\conf\ssl\ssl.crt\server.cr"
copy "%HOME%\apache\conf\ssl\output\cakey.pem"
"%HOME%\apache\conf\ssl\private\cakey.pem"
copy "%HOME%\apache\conf\ssl\output\manager.p12"
"%HOME%\tomcat\conf\keystore\tomcat\manager.p12"
```