websense

Deployment and Installation Center

Websense® TRITON™ Enterprise

v7.7.x

Deployment and Installation Center

Websense TRITON Enterprise version 7.7

June 2012

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc. makes no warranties with respect to this documentation and disclaim any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

1 Deployment and Installation Center

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Gateway Anywhere, v7.7.x	◆ *Planning your deployment*, page 1 ◆ *Installation scenarios*, page 2 ◆ *Upgrade scenarios*, page 2

Use the Deployment and Installation Center to find planning information and installation instructions for Websense Web, Data, and Email Security solutions.

- If you are installing Websense security solutions for the first time, start with the topics under *Planning your deployment*, page 1.
- When your planning is complete, select your installation path under *Installation scenarios*, page 2.
- If you are upgrading from a previous version, see *Upgrade scenarios*, page 2.

Planning your deployment

For general requirements and considerations for all Websense security solutions, see:

- *System requirements for this version*, page 2
- *Preparing for installation*, page 14

For planning guidelines specific to your solution, see:

- *Web Security Deployment Recommendations*, page 23
    - *Deploying Web Security for a distributed enterprise*, page 65
- *Content Gateway Deployment*, page 83
- *Planning Data Security Deployment*, page 103
- *Email Security Gateway Deployment*, page 163

Installation scenarios

- *Installation overview: Web Filter and Web Security*, page 193
- *Installation overview: Web Security Gateway*, page 197
- *Installation overview: Web Security Gateway Anywhere*, page 200
- *Installing Data Security Solutions*, page 303
- *Installing appliance-based Websense solutions*, page 247
- *Installation Overview: TRITON Enterprise*, page 175

For supplemental information for all Websense security solutions, see:

- *Installing components via the Custom option*, page 383
- *Obtaining Microsoft SQL Server*, page 21

Upgrade scenarios

- *Upgrading Websense Security Solutions to v7.7.x*, page 567

System requirements for this version

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Gateway Anywhere, v7.7.x	◆ *TRITON management server requirements*, page 2 ◆ *Reporting database requirements*, page 5 ◆ *Requirements for Web Security solutions*, page 6 ◆ *Email Security Gateway requirements*, page 8 ◆ *Data Security requirements*, page 9

TRITON management server requirements

The machine that hosts core management components for all Websense security solutions is referred to as the **TRITON management server**. This machine hosts the TRITON Unified Security Center (TRITON console), which includes:

- The infrastructure uniting all management components

- A settings database, holding administrator account information and other data shared by all management components
- One or more management modules, used to access configuration, policy management, and reporting tools for a Websense security solution. Available modules include:
  - TRITON - Web Security
  - TRITON - Data Security
  - TRITON - Email Security

Additional components may also reside on the TRITON management server.

Typically, the TRITON management server is a Windows Server 2008 R2 machine. If only the Web Security management module (TRITON - Web Security) is used, the TRITON management server can also be hosted on:

- Windows Server 2008 32-bit
- A V-Series appliance (recommended for evaluations only)

	Windows Server 2008 R2 (Standard and Enterprise)	Windows Server 2008 (Standard and Enterprise) 32-bit	V-Series Appliance
Data Security	✓		
Web Security	✓	✓	✓
Email Security	✓		

Hardware requirements

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

With local reporting database

TRITON console modules	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 Data Security	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space
TRITON - Email Security and Data Security	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space
All TRITON modules (Web Security, Data Security, and Email Security)	8 CPU cores (2.5 GHz), 16 GB RAM, 240 GB Disk Space

Notes:

- Data Security allows for either local or remote installation of the forensics repository. If the repository is hosted remotely, deduct 90GB from the Data Security disk space requirements.
- It is strongly recommended you allocate more than the minimum listed disk space 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 reporting database

TRITON console modules	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 Data Security	4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space
TRITON - Email Security and Data Security	4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space
TRITON - Web Security, Data Security, and 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.

TRITON console browser support

Use any of the following Web browsers to access the TRITON Unified Security Center.

Browser	Versions
Microsoft Internet Explorer	8* and 9
Mozilla Firefox	4.x through 13.x
Google Chrome	13 and later
* For Internet Explorer 8 only, do not use compatibility mode.	

Virtualization systems

All TRITON Unified Security Center components are supported on these virtualization systems:

- Hyper-V over Windows Server 2008 R2
- VMware over Windows Server 2008 R2

Note that this support is for the TRITON console only. Other components (used for filtering, analysis, reporting, or enforcement) may have additional requirements that are not supported by these virtualization environments.

Directory services for administrator authentication

If you allow users to log on to the TRITON console using their network accounts, the following directory services can be used to authenticate administrator logons:

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

Reporting database requirements

For all Websense security solutions, Microsoft SQL Server is used to host the reporting database.

- The TRITON Unified Installer can be used to install Microsoft SQL Server 2008 R2 Express on the TRITON management server machine.
  - This configuration is best for evaluations and small deployments.

- Only use the version of SQL Server 2008 R2 Express included in the Websense software installer.

- Larger organizations are advised to use a Standard or Enterprise version of Microsoft SQL Server. Note that these SQL Server versions cannot reside on the TRITON management server.

Supported Database Engines	Data Security	Web Security	Email Security
SQL Server 2005 SP4*		✓	
SQL Server 2008**	✓	✓	✓
SQL Server 2008 R2 Express	✓	✓	✓
SQL Server 2008 R2***	✓	✓	✓

*All editions except Web, Express, and Compact; 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: SQL Server clustering may be used with all supported standard and enterprise versions of Microsoft SQL Server for failover or high availability.

Requirements for Web Security solutions

Software components

Do **not** install Web Security components on a domain controller machine.

Most Web Security components can run on any of the following operating systems:

- Windows Server 2008 (32-bit) and 2008 R2
- Red Hat Enterprise Linux 5 and 6

The following components are Windows-only (not supported on Linux):

- Linking Service
- Log Server
- DC Agent
- Real-Time Monitor

Websense Content Gateway is Linux only, supported on:

- Red Hat Enterprise Linux 5 and 6
- The corresponding CentOS version (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

See *System requirements for Websense Content Gateway*, page 226, for more information.

Components not available on Websense appliances

The following Web Security components do not run on Websense appliances. If used, they must be installed off-appliance.

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

Client OS

The logon application (LogonApp.exe), Remote Filtering Client, and Web Endpoint are supported 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)
- Windows Server 2003
- Windows Server 2008 and 2008 R2

In addition, for Web Endpoint, the following Web browsers fully support the endpoint client 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.

Integrations

Websense Web Security may be integrated with the following products.

Product	Versions
Microsoft Forefront TMG	2008 or later
Cisco PIX Firewall	v5.3 or later

Product	Versions
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 NGX, NGX 65, UTM-1 (VPN-1) Edge
Citrix XenApp	5.0 or 6.0

Directory Services

Directory	Versions
Microsoft Active Directory (native or mixed mode)	2008 R2, 2008, 2003
Novell eDirectory	v8.5.1 or later
Oracle Directory Services Enterprise Edition	11g
Sun Java System Directory	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

Email Security Gateway requirements

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

- **TRITON - Email Security**, which runs on the TRITON management server (see *TRITON management server requirements*, page 2).
- Email Security **Log Server**, which runs on a Windows Server 2008 or 2008 R2 machine.

Data Security requirements

Operating system

Data Security Component	Supported Operating Systems	32-bit	64-bit
Management server	Windows Server 2008 Standard or Enterprise, R2		✓
Supplemental servers	Windows Server 2003 Standard or Enterprise, R2 SP2	✓	
	Windows Server 2008 Standard or Enterprise, R2		✓
Crawler agent	Windows Server 2003 Standard or Enterprise, R2 SP2	✓	
	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, CentOS 5.7**		
Mobile Agent	CentOS 5.5, CentOS 5.7**		
Data Endpoint client	Windows 7	✓	✓

Data Security Component	Supported Operating Systems	32-bit	64-bit
	v7.7.3 and beyond: Windows 8 (non-Windows Store apps only)	✓	✓
	Windows Vista	✓	✓
	Windows XP	✓	✓
	Windows Server 2003	✓	✓
	Windows Server 2008	✓	✓
	v7.7.3 and beyond: Windows Server 2012 (non-Windows Store apps only)	✓	✓
	v7.7.2: Mac OS X 10.6.7 - 10.7.4. v7.7.3 and beyond: Mac OS X 10.6.7 - 10.8	✓	✓
	Red Hat Enterprise Linux/CentOS 4.8 with stock kernel 2.6.9-89	✓	✓
	Red Hat Enterprise Linux/CentOS 5.1 with stock kernel 2.6.18-53****	✓	✓
	Red Hat Enterprise Linux/CentOS 5.5 with stock kernel 2.6.18-194****	✓	✓

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.

****The Linux endpoint requires FUSE support to enable USB detection. If you are running CentOS 5.1, FUSE support is configured upon installation. If you are running CentOS 5.5, FUSE support is built into the kernel. If you have upgraded from CentOS 5.1 to CentOS 5.5, you may not have FUSE support in your running kernel. If this is the case, please install the relevant FUSE packages before running the endpoint installer.

Data Security Server hardware requirements

Server hardware	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	4 GB	8 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, 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 host 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 your deployment includes more than one Data Security Server, use a domain account (preferred), or the use same local user name and password on each machine.
  - Be sure to set the system time accurately on 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
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)

Preparing for installation

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Gateway Anywhere, v7.7.x ◆ V-Series Appliances, v7.7.x	◆ *All Websense security solutions*, page 14 ◆ *TRITON Unified Security Center*, page 16 ◆ *Web security*, page 17 ◆ *Data Security*, page 20

All Websense security solutions

Before installing any Websense security solution, make a note of the following:

Windows-specific considerations

- Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- In addition to the space required by the Websense installer itself, further disk space is required on the Windows installation drive (typically C) to accommodate temporary files extracted as part of the installation process.

  For information on minimum disk space requirements, see *Hardware requirements*, page 3.
- NET Framework version 2.0 or higher is required to run the Windows installer. If .NET 2.0 is not already installed, it is available from www.microsoft.com.

Note

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

Getting the Websense software installers

The Websense Windows installer is used to install TRITON Unified Security Center; Web Security, Data Security, and Email Security components; and SQL Server 2008 R2 Express.

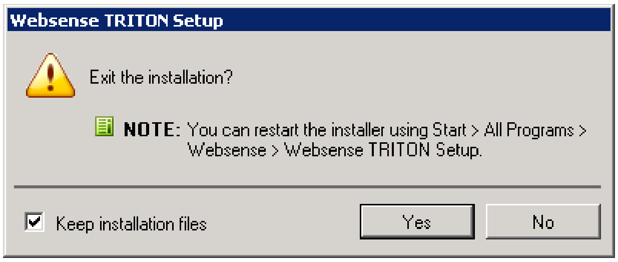
There are also Linux installers for installing Web Security components and Content Gateway.

The installers are also used to upgrade most prior-version components.

Download the installers from mywebsense.com.

- The Windows installer is named **WebsenseTRITON77Setup.exe**. Double-click it to start the installation process.

  If you have previously run the Websense installer on a machine, and you selected the **Keep installation files** option, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to restart the installer without extracting all of the files a second time.

  Websense TRITON Setup

  Exit the installation?

  NOTE: You can restart the installer using Start > All Programs > Websense > Websense TRITON Setup.

  ☑ Keep installation files

  Note that the files occupy approximately 2 GB of disk space.

- The Web Security Linux installer is **WebsenseWeb77Setup_Lnx.tar.gz**.
- The Content Gateway installer is **WebsenseCG77_Lnx.tar.gz**.

Domain Admin 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 admin 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).

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 724.

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 Websense security solutions*, page 14), before installing the TRITON Unified Security Center, note the following:

- Do not install the TRITON Unified Security Center on a domain controller machine.
- If you want to run Microsoft SQL Server on the TRITON management server, use the Websense installer to install SQL Server 2008 R2 Express.

  If you are using a remote installation of SQL Server, you can use any of the supported versions (see *System requirements for this version*, page 2).

SQL Server 2008 R2 Express

The following third-party components are required to install Microsoft SQL Server 2008 R2 Express. Although the Websense installer will install these components automatically if they are not found, it is a best practice to install the components first, before running the Websense installer.

- .NET Framework 3.5 SP1

> ✓ **Note**
> Because the installer requires .NET 2.0, both .NET 2.0 and 3.5 SP1 are required if you are installing SQL Server Express.

- Windows Installer 4.5

- Windows PowerShell 1.0

  PowerShell is available from Microsoft (www.microsoft.com).

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 to run 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 Websense security solutions*, page 14), 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.

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 TRITON Infrastructure. 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 *Websense TRITON Enterprise default ports*, page 712, 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 is positioned to be able to monitor and respond to client Internet requests.

In standalone installations (which do not include Content Gateway or a third-party integration product), if you install Network Agent on a machine that cannot monitor client requests, basic HTTP filtering 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.

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.

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.

SELinux

Before installing, if SELinux is enabled, disable it or set it to *permissive*.

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 *Websense TRITON Enterprise default ports*, page 712.

> **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*.

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>
   ```

   Here, <host> is the name you are assigning this machine.
2. Also update the HOSTNAME entry in the **/etc/sysconfig/network** file:

   ```
   HOSTNAME=<host>
   ```
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 (the IPv4 loopback address). And do not delete the third line in the file, the on that begins ::1 (the IPv6 loopback address).

```
<IP address>    <FQDN>                       <host>
127.0.0.1       localhost.localdomain        localhost
::1             localhost6.localdomain6      localhost6
```

Here, <FQDN> is the fully-qualified domain name of this machine (i.e., <host>.<subdomains>.<top-level domain>)—for example, myhost.example.com—and <host> is the name assigned to the machine.

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.

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 or servers 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 724). Please contact Websense Technical Support for more information on enhancing performance.

Obtaining Microsoft SQL Server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

Prior to installing Websense components, Microsoft SQL Server must be installed and running on a machine in your network.

- See *System requirements for this version*, page 2, for supported versions of SQL Server.
- Note that full versions of Microsoft SQL Server are not included in your Websense subscription, and must be obtained separately. 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:

- Use the Websense installer to install it. Do not download and install it from any other source.
- This is the only Express edition of SQL Server you can use with Websense version 7.7.x 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 full versions of 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 180, 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 417.

2 Web Security Deployment Recommendations

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

Deploying Web Security core components

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

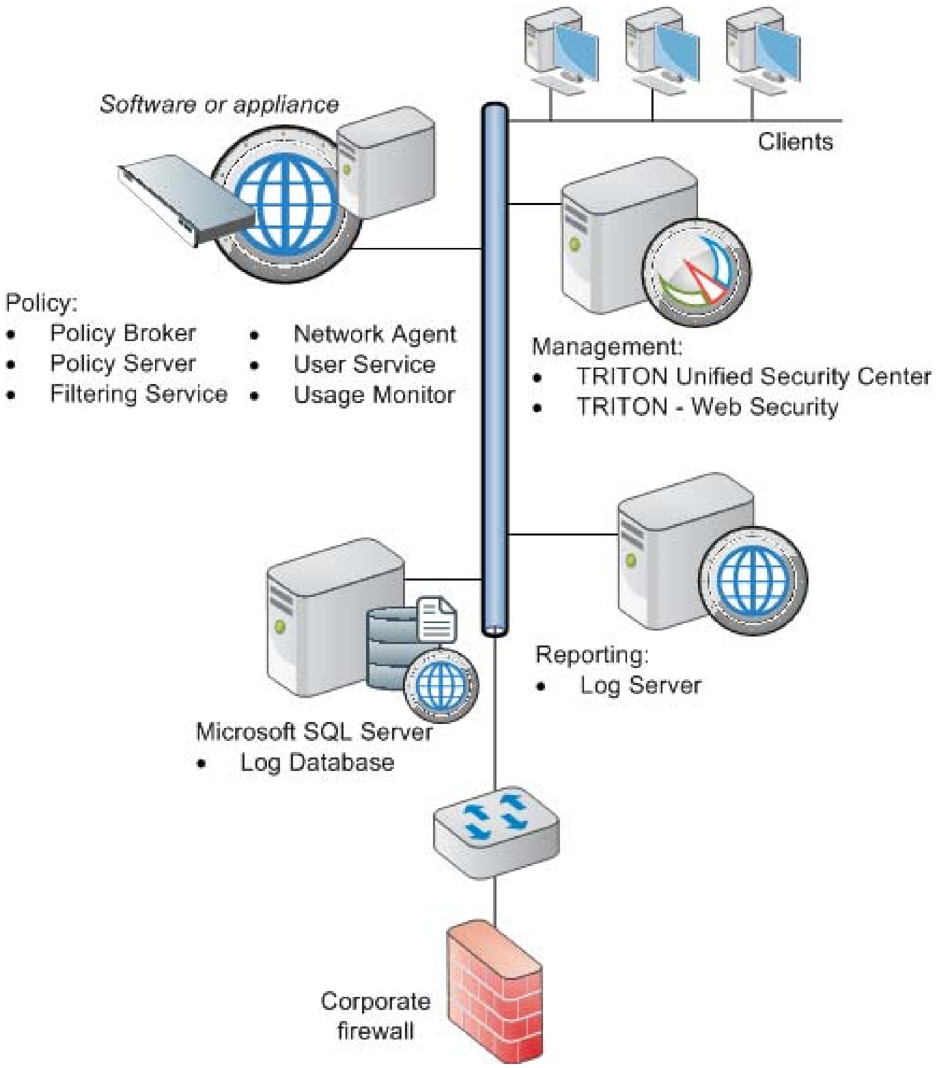
Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Core policy components*, page 26 ◆ *Core management components*, page 28 ◆ *Core reporting components*, page 29

This section of the Deployment and Installation Center describes the core components required by all Websense Web Security solutions, and explains how they are typically distributed.

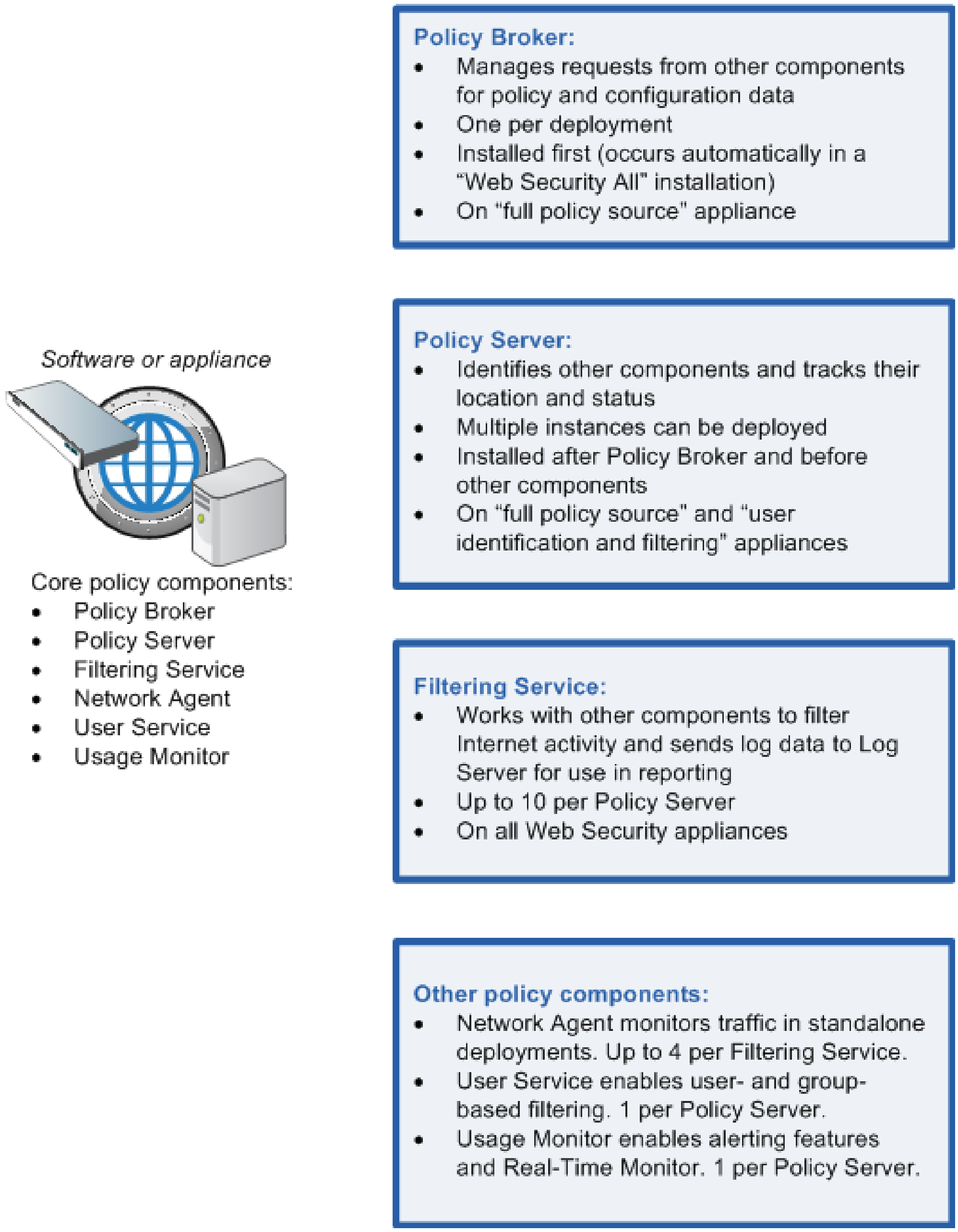
For information about how a deployment can be extended beyond the core components, see *Extending your Web Security deployment*, page 31, and *Deploying transparent identification agents*, page 48.

- If you have a Web Security Gateway solution, also see *Content Gateway Deployment*, page 83.

- Additional information for distributed enterprise deployments is available in *Deploying Web Security for a distributed enterprise*, page 65.



Core policy components



Software or appliance

Core policy components:

- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- User Service
- Usage Monitor

Policy Broker:

- Manages requests from other components for policy and configuration data
- One per deployment
- Installed first (occurs automatically in a "Web Security All" installation)
- On "full policy source" appliance

Policy Server:

- Identifies other components and tracks their location and status
- Multiple instances can be deployed
- Installed after Policy Broker and before other components
- On "full policy source" and "user identification and filtering" appliances

Filtering Service:

- Works with other components to filter Internet activity and sends log data to Log Server for use in reporting
- Up to 10 per Policy Server
- On all Web Security appliances

Other policy components:

- Network Agent monitors traffic in standalone deployments. Up to 4 per Filtering Service.
- User Service enables user- and group-based filtering. 1 per Policy Server.
- Usage Monitor enables alerting features and Real-Time Monitor. 1 per Policy Server.

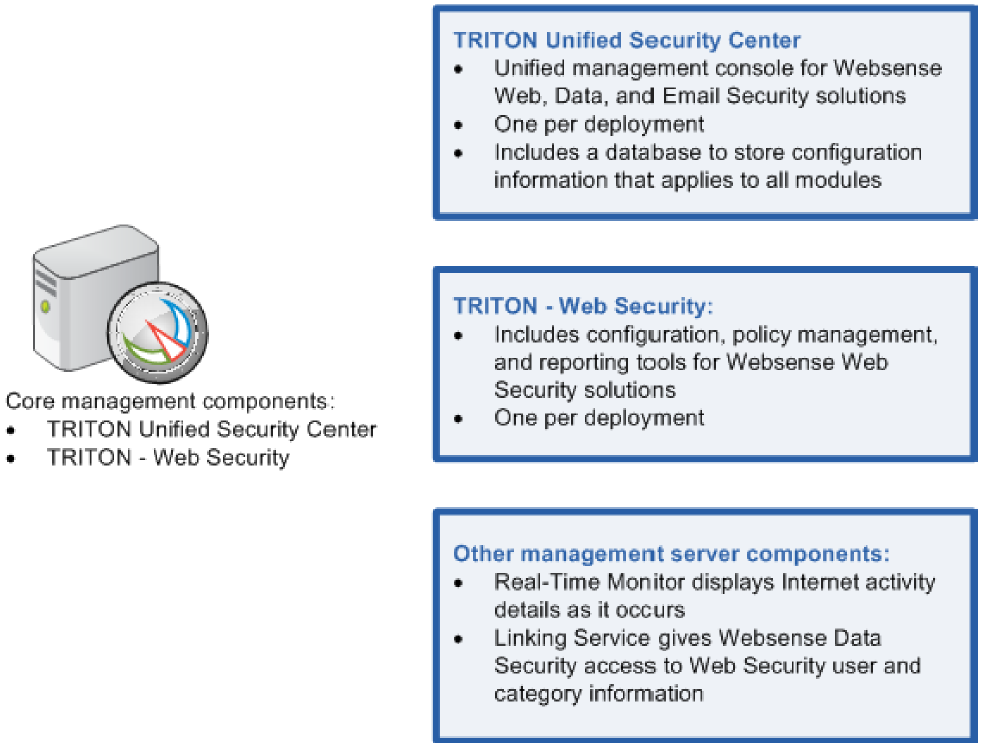
To ensure effective filtering, Websense Web Security core management components must be installed so that:

- All components can communicate with a central installation of Policy Broker.
  - There can be only one Policy Broker instance per deployment.
  - In software installations, Policy Broker can run on Windows or Linux.
  - With Websense appliances, Policy Broker is present on the **full policy source** appliance only.

    - Most components must be able to communicate with Policy Broker on port **55880**. (The exceptions are all optional components: transparent identification agents, State Server, Multiplexer, Linking Service, and Directory Agent.)

- There is a central instance of Policy Server.
    - In software installations, the central Policy Server instance runs on the Policy Broker machine.
    - With Websense appliances, Policy Server is present on the **full policy source** appliance.
    - Additional instances of Policy Server can be deployed on Windows or Linux machines, or on **user identification and filtering** appliances.
    - Most components must be able to communicate with Policy Server on ports **55806** and **40000**. (The exceptions are Remote Filtering Server and State Server.)
- At least one instance of Filtering Service communicates with the central Policy Server.
    - In software installations, Filtering Service can run on the same machine as Policy Broker and Policy Server.
    - With Websense appliances, a Filtering Service instance is present on the **full policy source** appliance.
    - Additional instances of Filtering Service can be deployed on Windows or Linux machines, or on either **user identification and filtering** (includes Policy Server) or **filtering only** (must point to a remote Policy Server) appliances.
- Filtering Service is configured to receive HTTP(S) requests from one of the following:
    - Content Gateway (Websense Web Security Gateway or Gateway Anywhere deployments).
    - Network Agent (Websense Web Filter or Web Security standalone deployments).
    - An integrated third-party firewall, proxy server, or caching application (Websense Web Filter or Web Security integrated deployments).

Core management components



Core management components:

- TRITON Unified Security Center
- TRITON - Web Security

TRITON Unified Security Center

- Unified management console for Websense Web, Data, and Email Security solutions
- One per deployment
- Includes a database to store configuration information that applies to all modules

TRITON - Web Security:

- Includes configuration, policy management, and reporting tools for Websense Web Security solutions
- One per deployment

Other management server components:

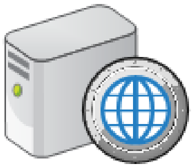
- Real-Time Monitor displays Internet activity details as it occurs
- Linking Service gives Websense Data Security access to Web Security user and category information

The TRITON Unified Security Center (TRITON console) is the centralized management console for Websense Web, data, and email security solutions. The TRITON console includes global administrator settings and appliance connection data, as well as 3 management modules: Web Security, Data Security, and Email Security.

TRITON - Web Security is the console used to perform product configuration, policy management, and reporting tasks for Websense Web Security solutions.

- Install all TRITON Unified Security Center components on a single Windows server (sometimes called the TRITON management server).
    - For evaluation and demonstration purposes, TRITON - Web Security is available on Websense appliances.
    - As a best practice, use a separate, Windows-based TRITON management server for production environments.
- TRITON - Web Security must be able to communicate with:
    - Policy Broker on port 55880
    - Policy Server on ports 40000, 55806, 55817, 55818, and 55824
    - Filtering Service on port 55807
    - Log Server on ports 55812 and 55805
    - User Service on port 55815

Core reporting components

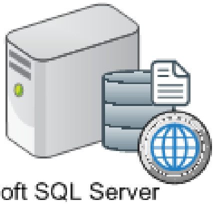


Reporting:

- Log Server

Log Server

- Receives log data and stores it in the Log Database
- Enables investigative reports, presentation reports, and Web Security Dashboard charts
- One per Policy Server
- Multiple Log Server instances can send data to a central Log Server, which sends the data to the Log Database



Microsoft SQL Server

- Log Database

Log Database

- Requires a supported Microsoft SQL Server installation
- Stores Internet activity log data for use in reports
- One per deployment

Web Security Log Server receives information about Internet activity from Filtering Service and processes it into the Log Database.

- Install Log Server on a dedicated Windows server.
  - Log Server does not run on Websense appliances.
  - Because collecting and processing log records is resource-intensive, Log Server should typically not run on the same machine other resource-sensitive components, like the TRITON console or Filtering Service.
- The Log Database resides on a supported Microsoft SQL Server machine.
  - Do not run Log Server on the SQL Server machine.
  - By default, Log Server communicates with SQL Server on the default ODBC port (1433). A custom port can be specified during installation. See *Using a custom port to connect to the Log Database*, page 35.
- The TRITON console machine must be able to communicate with Log Server and the Log Database.

Understanding Web Security standalone and integrated modes

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

Websense Web Filter and Web Security may either be installed as a **standalone** solution, or be **integrated** with a third-party proxy, cache, or firewall product (for example, Check Point Firewall-1 NGX, Cisco ASA, or Microsoft Forefront TMG).

- In a standalone deployment, **Websense Network Agent** monitors Internet activity from all users and forwards both HTTP(S) requests and requests made via other protocols to Websense Filtering Service to determine whether to permit or block the request.

  For information about using Network Agent to enable a standalone deployment, see *Standalone deployment guidelines for Network Agent*, page 53.

- In an integrated deployment, the **third-party product** (integration product) forwards HTTP(S) requests, and sometimes also FTP requests, to Websense Filtering Service to determine whether to permit or block the request.

  For information about integrating Web Filter or Web Security with a third-party product, see:

  - *Integrating Web Security with Check Point*, page 445
  - *Integrating Web Security with Cisco*, page 481
  - *Integrating Web Security with Citrix*, page 513
  - *Integrating Web Security using ICAP Service*, page 557
  - *Integrating Web Security with Microsoft Products*, page 535
  - *Installing Web Security for Universal Integrations*, page 563

Websense Web Security Gateway and Gateway Anywhere solutions include **Websense Content Gateway**, a high-performance Web proxy that provides real-time threat analysis and Web site classification. With Web Security Gateway solutions, Content Gateway forwards HTTP(S) and FTP requests to Websense Filtering Service to determine whether to permit or block the request.

For information about deploying Content Gateway with Web Security Gateway or Gateway Anywhere, see *Content Gateway Deployment*, page 83.

Extending your Web Security deployment

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	

In large, high-traffic, or geographically distributed organizations, you can deploy multiple groups of policy components, each with its own **Websense Policy Server** instance, to:

- Provide load-balancing capabilities.
- Improve filtering responsiveness in locations far away from the central Web Security installation.
- Manage high amounts of traffic.

All Policy Server instances connect to the same, central Policy Broker. Except in very rare circumstances, all Policy Server instances also connect to the same, central instance of TRITON - Web Security.

Each Policy Server instance can support:

- Up to 10 Filtering Service instances (see *Filtering Services per Policy Server*, page 32)
    - Each Filtering Service can support up to 4 Network Agent instances (see *Network Agents per Filtering Service*, page 33)
- 1 User Service
- 1 Usage Monitor
- 1 Web Security Log Server
- 1 State Server (see *Policy Server, Filtering Service, and State Server*, page 33)
- 1 Multiplexer (see *Policy Server, Filtering Service, and Multiplexer*, page 34)
- 1 Directory Agent (Websense Web Security Gateway Anywhere only; see *Directory Agent*, page 47)

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 Policy Server to Filtering Service connection*, page 32.

If Filtering Service and Policy Server become disconnected, all Internet requests are either blocked or permitted, as configured on the Settings > General > Account page TRITON - Web Security. For more information, see Configuring your account information 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 Policy Server to Filtering Service 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>
   ```

   Use the IP address or hostname of the Filtering Service machine.

On 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.

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.

Network Agent communicates with Filtering Service on port 15868.

Policy Server, Filtering Service, and State Server

If your deployment includes multiple instances of Filtering Service that might handle a request from the same user, an optional component, **Websense State Server**, can be installed to enable proper application of time-based filtering actions. For example, users can be granted quota time, which gives them access to sites in selected categories for a limited (configurable) time period.

When State Server is installed, its associated Filtering Service instances share timing information, so users receive the correct allotment of access to time-restricted categories.

- State Server is typically installed on a Policy Server machine, and only one State Server instance is required per **logical deployment**.

A logical deployment is any group of Policy Server and Filtering Service instances that might handle requests from the same set of users.

- State Server can be enabled via the command-line interface on **full policy source** or **user identification and filtering** appliances.
- All Filtering Service instances that communicate with the same State Server instance must share the same time zone, and the time on all machines must be in synch.
- State Server communicates with Filtering Service on port 55828.
- Each Filtering Service instance can communicate with only one State Server.
- All Filtering Service instances associated with the same Policy Server must communicate with the same State Server.
- Multiple Policy Server instances can share a single State Server.

In a geographically dispersed organization, where each location has its own Policy Server and Filtering Service instances, deploy one State Server instance (on the Policy Server machine or V-Series appliance) at each location.

In an organization where all requests are filtered through a central location, only one State Server instance is needed.

Policy Server, Filtering Service, and Multiplexer

Websense Web Security solutions can be configured to pass logging data (the same information processed by Log Server) to a third-party Security and Information and Event Management (SIEM) product.

When SIEM integration is enabled, **Websense Multiplexer** collects log data from Filtering Service and passes it to both Log Server and the integrated SIEM product. (When SIEM integration is disabled, Filtering Service sends log data directly to Log Server, with no intermediary.)

- Multiplexer is typically installed on the Policy Server machine.
    - When Policy Server resides on a V-Series Appliance, always enable Multiplexer on the appliance. Do not attempt to connect an off-appliance Multiplexer instance to the on-appliance Policy Server.
    - With software (non-appliance) installations of Policy Server, it does not matter whether Multiplexer is on the same machine or a different machine.
- Install one Muliplexer per Policy Server.
- Multiplexer can be enabled via the command-line utility on **full policy source** or **user identification and filtering** appliances.

Multiplexer communicates with the following components:

- Policy Server on ports 40000, 55806, and 56010
- Filtering Service on port 55805 (inbound)
- Log Server on port 55805 (outbound)
- SIEM integration (port varies; 514 for TCP and 515 for UDP)

Additional reporting considerations

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Using a custom port to connect to the Log Database*, page 35 ◆ *Using SSL to connect to the Log Database*, page 35 ◆ *Using BCP for log record insertion with SQL Server 2008*, page 36 ◆ *Configuring distributed logging*, page 37

When you install Web Security reporting components, you can configure how those components communicate with the SQL Server database (Log Database). Port and encryption settings selected during installation can be changed after installation, if needed.

In addition, if you are planning to deploy reporting components for a large or geographically distributed organization, and need to use a single, centralized database for reporting, see *Configuring distributed logging*, page 37, for configuration options.

Using a custom port to connect to the Log Database

During TRITON Infrastructure and Websense Log Server installation, you can specify which port to use for Microsoft SQL Server communication. By default, the standard ODBC port (1433) is used.

If you want to use another port, keep in mind that SQL Server typically assigns:

- A fixed port to the default instance (MSSQLSERVER)
- A dynamic port to each named instance

Use the SQL Server Configuration Manager to configure the port used by each SQL Server instance. See your Microsoft documentation for assistance.

Using SSL to connect to the Log Database

During TRITON Infrastructure and Websense Log Server installation, you are given the option to connect to Microsoft SQL Server using an SSL-encrypted connection.

In determining whether to configure reporting and management components to use SSL encryption for Log Database communication, keep in mind that:

- BCP (bulk copy program) cannot be used to add records to the Log Database.
- Log Database connections are slower, which may affect reporting performance.
- If you are running TRITON - Web Security on a V-Series appliance (typically done only for evaluations), the connection from the management console to the database cannot be encrypted.

  If SSL is required, no data can be displayed in the Web Security Dashboard or other reporting tools.

Before enabling SSL encryption during Websense software installation, configure Microsoft SQL Server encryption settings.

1. Launch **SQL Server Configuration Manager** (for example, Start > All Programs > Microsoft SQL Server 2008 > Configuration Tools > SQL Server Configuration Manager).
2. Right-click the **SQL Native Client x.x Configuration** entry used in your SQL Server installation, then select **Properties**.

   Two parameters are listed:

   - **Force Protocol Encryption**: The default setting (No) means that encrypted connections are accepted but not required. This setting is typically best for use with Websense security solutions.

     If this is set to yes, only encrypted connections are accepted.
   - **Trust Server Certificate**: The default setting (No) means that only certificates issued by a Certificate Authority (CA) are accepted for encrypting connections to the database. This requires that a CA-signed certificate be deployed to the SQL Server, Log Server, and TRITON management server machines before Websense components can use a secure connection to connect to the database.

     When this parameter is set to **Yes**, self-signed SSL certificates may be used to encrypt the connection to the database. In this case, the certificate is generated by the SQL Server machine and shared by all components needing to connect to the database.

If you enable SSL encryption during installation, Force Protocol Encryption is set to **Yes**, and Trust Server Certificate is set to **No**, CA-signed certificates must be installed on the TRITON management server and Log Server machines before the component installation will succeed.

Using BCP for log record insertion with SQL Server 2008

The Web Security Log Database can use either of 2 methods to insert log records into the Log Database (reporting database):

- **ODBC** (Open Database Connectivity inserts records into the database individually, using a database driver to manage data between Log Server and Log Database.

- **BCP** (Bulk Copy Program) inserts records into the Log Database in groups called batches. This option is recommended because it offers better efficiency than ODBC insertion.

Before you can use BCP for log record insertion with SQL Server 2008, 2 Microsoft component must be installed on the Log Server machine:

- **Microsoft SQL Server 2008 Native Client** is installed by the TRITON Unified Installer, when you install Web Security Log Server on the machine.
- **Microsoft SQL Server 2008 Command Line Utilities** are available as a free download from Microsoft:

  http://www.microsoft.com/en-us/download/details.aspx?id=16177

After you install the SQL Server 2008 Command Line Utilities, perform the following configuration steps to ensure that Log Server can access the BCP utility:

1. Locate the **bcp.exe** file installed with the SQL Server 2008 Command Line Utilities and make a note of the path to the file. The default location is:

   ```
   C:\Program Files\Microsoft SQL
   Server\100\Tools\Binn\bcp.exe
   ```

2. Navigate to the Websense **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin\) and open **LogServer.ini** in a text editor.
3. Locate the **BCPExePath** parameter, and set its value to the path noted in step 1. For example:

   ```
   BCPExePath=C:\Program Files\Microsoft SQL
   Server\100\Tools\Binn\bcp.exe
   ```

4. Save and close the **LogServer.ini** file.
5. Use the Windows Services dialog box (Start > Administrative Tools > Services) to restart the **Websense Log Server** service.
6. Use the **Settings > Reporting > Log Server** page in TRITON - Web Security to configure Log Server to use BCP for log record insertion.

Configuring distributed logging

If you have a large or distributed environment that requires multiple Log Server instances, you can configure each Log Server to record data to a separate Log Database. If you do not need a central repository of reporting data that can be used to generate organization-wide reports, this may be the most efficient deployment option.

If you, however, you need a single Log Database in order to store all reporting data in a central location, you have 2 options:

- Configure all Log Server instances to independently record their data in the same Log Database.
- Configure distributed Log Server instances to pass their data to a central Log Server, which then records all log records from all instances into the Log Database.

The first option does not require special configuration steps. You need only ensure that each Log Server instance points to the same database (both database engine IP address or hostname and database instance name).

The second option requires more planning and configuration detail, as outlined in the sections that follow.

Note that centralized log processing is not as fast as local logging. Expect a delay of 4 or 5 minutes before the files from remote Log Servers appear in the cache processing directory on the central Log Server.

Part 1: Prepare for centralized logging

1. Identify or create a domain user account to use for running each Log Server service. For example:

   ```
   mydomain\WebsenseLogServer
   ```

   This ensures that permissions are consistent for all instances, and facilitates communication between distributed Log Server instances and the central instance.
2. Identify which Log Server instance will serve as the central Log Server and note its hostname or IP address.

   All remote Log Server instances must be able to communicate with the central Log Server machine.
3. Create a shared folder on the central Log Server machine for all Log Server instances to access:
   a. Create the folder. For example:

      ```
      C:\Program Files (x86)\Websense\Web
      Security\bin\logscache\
      ```

   b. Right-click the new folder and select **Properties**. On the **Sharing** tab, select **Share this folder** and provide the information requested.

      Optionally, also restrict access to the folder to the domain user account assigned to all Log Server instances.

   The shared folder is available within the network via its UNC file path (\\<*host_name*>\<*folder_name*>). For example:

   ```
   \\logserver01\logscache
   ```
4. On the remote Log Server machines, create a mapped drive for the cache folder created in step 3:
   a. Log on to each Log Server machine as the domain user assigned to all Log Server instances.
   b. Open Windows Explorer and go to **Tools > Map Network Drive**.
   c. Select a drive letter for the mapped drive, browse to the shared folder created in step 3, and then click **Finish**.
   d. Make sure that you can copy a small text file from the remote Log Server machine to the shared drive.

Part 2: Configure the central Log Server

1. Go to the central Log Server machine and use the Windows Services dialog box (Start > Administrative Tools > Services) to stop **Websense Log Server** service.
2. Navigate to the Websense **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin, by default) and open the **LogServer.ini** file in a text editor.
3. Search for the phrase “Centralized LogServer,” then make the following changes:

   ```
   [CacheFileWatcher]
   Active=true
   TimeInterval=180
   FilePath=<path_to_shared_cache_folder>
   ```

   - Set the **Active** parameter to **true** to configure the central Log Server to process cache files from remote Log Server instances.
   - Optionally, edit the **TimeInterval** value to determine how frequently (in seconds) the central Log Server checks the cache directory for new files to process.
   - Set the **FilePath** parameter to the shared directory you created in Part 1 of this procedure (in the example above, the value is C:\Program Files (x86)\Websense\Web Security\bin\logscache\).
4. Next, search for **[Visits]** section of the file to change the **UsingVisits** parameter to **false**. (This can also be configured via the Settings > Reporting > Log Server page in TRITON - Web Security.) The section looks like this:

   ```
   [Visits]
   VisitTime=10
   UsingVisits=false
   VisitSortTimeDelay=30
   ```

   This ensures that visits processing (if enabled) is performed only once, by the remote Log Server instances.

   > **Note**
   >
   > When centralized logging is used, log record consolidation is automatically disabled on remote Log Server instances (regardless of the setting in LogServer.ini or TRITON - Web Security). To use log record consolidation, enable it for the **central** Log Server.

5. Save and close the file.
6. To configure this Log Server instance to run as the domain user created in Part 1 of this procedure:
   a. In the Windows Services dialog box, right-click **Websense Log Server** and select **Properties**.
   b. Select the **Log On** tab, then, under “Log on as,” click **This account**.
   c. Browse to the domain user created for this purpose, then enter and confirm the account password.

   d. When you are finished, click **OK** to return to the main Services window.

7. To start Log Server, right-click **Websense Log Server** again, then select **Start**.

Part 3: Configure remote Log Server instances

1. Go to a remote Log Server machine and use the Windows Services dialog box to stop the **Websense Log Server** service.
2. Navigate to the Websense **bin** directory, then open the **LogServer.ini** file for that instance in a text editor.
3. Search for the phrase "Remote LogServer" and make the following changes:

```
[LogFile]
MoveCacheFile=TRUE
MoveCacheFilePath=C:\Program
Files\Websense\bin\CacheProcessing
ProcessCacheFile=FALSE

[UserGroups]
ProcessGroups=FALSE
ProcessUserFullName=FALSE

;Distributed Logging Remote LogServer

[CacheLogging]
Active=true
TimeInterval=180
MinFileSize=1048576
MaxFileSize=5242880
CacheFileProcessingPath=C:\Program
Files\Websense\bin\CacheProcessing
CacheFileOutputPath=<UNC_path_to_mapped_drive>
```

   - Set the **Active** parameter to **true** to configure the remote Log Server to place cache files in the "CacheFileProcessingPath" directory and forward them to the central Log Server.
   - Optionally, change the **TimeInterval** value to determine how often (in seconds) the remote Log Server closes the current cache file and creates a new one.
   - You can also edit the **MinFileSize** and **MaxFileSize** (in bytes) for each cache file. The default minimum is 1 MB; the default maximum is 5 MB.
   - Set **CacheFileProcessingPath** to a local directory on the remote Log Server machine. Cache files are created on the local machine before being sent to the mapped drive on for processing by the central Log Server.
   - Set **CacheFileOutputPath** to the UNC file path of the shared folder on the central Log Server machine.

4. If you want to record visits (rather than hits), and have turned off visits processing for the central Log Server service, make sure visits are enabled in the **[Visits]** section of the INI file for the remote Log Server instance.

```
[Visits]
VisitTime=10
```

```
UsingVisits=true
VisitSortTimeDelay=30
```

✓ **Note**

When centralized logging is used, log record consolidation is automatically disabled on remote Log Server instances (regardless of the setting in LogServer.ini or TRITON - Web Security). To use log record consolidation, enable it for the **central** Log Server.

5. Save and close the file.
6. To configure this Log Server instance to run as the domain user created in Part 1 of this procedure:
    a. In the Windows Services dialog box, right-click **Websense Log Server** and select **Properties**.
    b. Select the **Log On** tab, then, under “Log on as,” click **This account**.
    c. Browse to the domain user created for this purpose, then enter and confirm the account password.
    d. When you are finished, click **OK** to return to the main Services window.
7. To start Log Server, right-click **Websense Log Server** again, then select **Start**.

Repeat the process for each remote Log Server machine.

Web Security required external resources

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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

- **TCP/IP**

  Websense software provides filtering in TCP/IP-based networks only.

- **DNS server**

  A DNS server is used to resolve requested URLs to an IP address. Network Agent, Content Gateway, or your third-party 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 for this version*, page 2, 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.

- **Microsoft SQL Server**

  A supported version of Microsoft SQL Server is required to host the Log Database, which stores reporting data for Websense Web Security solutions. See *System requirements for this version*, page 2, for supported SQL Server versions.

  - SQL Server Standard or Enterprise 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).
  - SQL Server Express, a free, limited-performance database engine, is 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).

Maximizing Web Security system performance

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x	◆ *Network Agent*, page 43 ◆ *HTTP request logging*, page 43 ◆ *Microsoft SQL Server (Log Database)*, page 43 ◆ *Log Database sizing considerations*, page 44

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

Network Agent

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 deploy additional Network Agent instances and divide network monitoring between them.

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.

- Network Agent must have bidirectional visibility into the network segment 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.

HTTP request logging

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.

Microsoft SQL Server (Log Database)

Under high load, Microsoft SQL Server operations are resource intensive, and can be a performance bottleneck for Websense software reporting. For best results:

- Do not install Web Security Log Server on the database engine machine.

- Provide adequate disk space to accommodate the growth of the Log Database. You can monitor growth and sizing information on the Settings > Reporting > Log Database page in TRITON - Web Security.
- 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.

SQL Server clustering is supported for failover or high availability.

Consult your Microsoft documentation for detailed information about optimizing Microsoft SQL Server performance.

Log Database sizing considerations

Log Database disk space requirements vary, based on:

- Network size
- Volume of Internet activity
- How long data must be available for use in reporting
- Logging settings

It is important to host the database engine and Log Database on hardware that matches or exceeds the requirements for expected load and for historical data retention.

Depending on the volume of Internet traffic in your network, and how much data your organization is required to store (based on organizational policy or compliance regulations, for example), the Log Database can become very large.

To help determine an effective logging and reporting strategy for your organization, consider:

- When is the network traffic busiest?

  Schedule resource intensive database and reporting jobs at lower-volume times to improve logging and reporting performance during peak periods.

  See the TRITON - Web Security Help for information about scheduling database jobs, investigative reports, and presentation reports.
- How long should log data be kept to support historical reporting?

  Automatically delete partitions and trend data (stored in the catalog database) after they reach this age to reduce the amount of disk space required for the Log Database.

  See the TRITON - Web Security Help for information about managing Log Database partitions.
- How much detail is really needed in reports?

  To decrease Log Database size, consider:

  - logging visits instead of hits (see *Logging visits (default) vs. logging hits*, page 45)
  - disabling full URL logging (see *Logging full URLs*, page 45)

- enabling consolidation (see *Consolidation*, page 45)
- only logging non-HTTP protocol traffic for selected protocols (see *Protocol logging*, page 46)
- only logging HTTP and HTTPS traffic in selected categories (see *Selective category logging*, page 46)

All of these logging settings can be customized in TRITON - Web Security. Tune your logging settings to achieve the appropriate balance of size savings and report detail for your organization.

Logging visits (default) vs. logging hits

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.

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.

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.

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. You can specify whether or not to log a specific protocol in each protocol filter that you create.

Selective category logging

By default, requests for URLs in all categories are logged. If your organization does not want to report on Internet requests for some categories, you can disable logging for those categories to help reduce Log Database size.

Deploying Web Security hybrid filtering components

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway Anywhere, v7.7.x	◆ *Sync Service*, page 46 ◆ *Directory Agent*, page 47

Websense Web Security Gateway Anywhere offers the ability to combine on-premises and hybrid (in-the-cloud or security-as-a-service) Web security solutions to manage Internet activity for your organization.

Two on-premises components are used to hybrid Web security functionality:

- Websense Sync Service
- Websense Directory Agent

Sync Service

Websense Sync Service is required to send policy updates and user and group information from the on-premises deployment to the hybrid (cloud-based) service. Sync Service also retrieves reporting data from the hybrid service and passes it to Log Server so that it can be used in reports.

- There can be only one Sync Service instance in your deployment.
- Sync Service can be installed on the Log Server machine.
- If you have a distributed logging deployment (multiple Log Server instances pointing to a central Log Server), configure Sync Service to communicate with the central Log Server.

Sync Service must be able to communicate with:

- The hybrid service on port 443
- Log Server on port 55805 (outbound)
- Directory Agent on port 55832 (inbound)
- TRITON - Web Security on port 55832 (inbound)
- Policy Broker on port 55880 (outbound)
- Policy Server on port 55830 (inbound) and ports 55806 and 40000 (outbound)

Directory Agent

Websense Directory Agent is required to enable user, group, and domain (OU) based filtering through the hybrid service.

Directory Agent collects user, group, and OU information from a supported directory service and passes it to Sync Service in LDIF format. Sync Service then forwards the information to the hybrid service.

- Typically, only one Directory Agent instance is required in a deployment.
- Directory Agent can be installed on the same machine as other Websense components, including Sync Service and User Service.
- With Websense appliances, Directory Agent is installed on the **full policy source** or **user directory and filtering** appliance.
- When Directory Agent is installed, it must connect to a Policy Server instance that has an associated **User Service** instance.
    - Directory Agent must communicate with the same directory service as User Service.
    - If you have multiple User Service instances connected to different directory services, you can also have multiple Directory Agent instances, each associated with a different Policy Server.
    - All Directory Agent instances must connect to a single Sync Service. (A deployment can have only one Sync Service instance.)

      Use TRITON - Web Security to configure the Sync Service connection manually for all supplemental Directory Agent instances. See "Directory Agent and User Service" in the TRITON - Web Security Help for configuration steps.

Directory Agent must be able to communicate with:

- Your supported LDAP-based directory service (Windows Active Directory in Native Mode, Oracle Directory Server, or Novell eDirectory)

  If your organization uses Windows Active Directory in mixed mode, user and group data cannot be collected and sent to the hybrid service.
- Websense Sync Service on port 55832
- Policy Server on ports 55806 and 40000

Once configured, Directory Agent collects user and group data from your directory service and sends it to Sync Service in LDIF format. At scheduled intervals, Sync Service sends the user and group information collected by Directory Agent to the hybrid service. Sync Service compresses large files before sending them.

Deploying transparent identification agents

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x	◆ *Combining transparent identification agents*, page 49

Use Websense transparent identification agents to identify users without prompting them for a user name and password in:

- Standalone Web Security deployments
- Integrated deployments in which the integration product does not send user information to Filtering Service

There are 4 transparent identification agents:

- **DC Agent** is used with a Windows Active Directory. The agent:
  - Works by identifying domain controllers in the network, and then querying those domain controllers for user logon sessions
  - Can also be configured to poll client machines to verify logon status
  - Runs on a Windows server and can be installed in any domain in the network

    Note

    Some DC Agent features require local and domain administrator privileges.

  - May use NetBIOS port 139 for automatic domain detection. If NetBIOS port 139 is blocked in your network, deploy a DC Agent instance for each virtually or physically remote domain.
  - Communicates with Filtering Service on port 30600
- **Logon Agent** identifies users as they log on to Windows domains. The agent:
  - Runs on a Linux or Windows server
  - Requires a Windows-only client application (the Logon Application, or LogonApp.exe) to be run on client machines
  - Communicates with Filtering Service on port 30602
- **eDirectory Agent** is used with Novell eDirectory. The agent:

    - Runs on a Linux or Windows server
    - Uses Novell eDirectory authentication to map users to IP addresses
    - Communicates with Filtering Service on port 30700
- **RADIUS Agent** can be used in conjunction with either Windows- or LDAP-based directory services. The agent:
    - Runs on a Linux or Windows server
    - Works with a RADIUS server and client to identify users logging on from remote locations
    - Communicates with Filtering Service on port 30800

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 **Logon Agent** is required for each Filtering Service instance.
- One **eDirectory Agent** is required for each eDirectory Server.
- 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 49.

See *Installing Web Security components*, page 392, for transparent identification agent installation instructions. See the TRITON - Web Security Help for configuration information.

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. 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.
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.

Combination	Same machine?	Same network?	Configuration required
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. 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. 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.

Hardware recommendations for standalone Web Security deployments

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

In standalone deployments, Network Agent (rather than Content Gateway or a third-party integration product) monitors network traffic and enables filtering of all protocols, including HTTP, HTTPS, and FTP.

In a standalone deployment, one or more Network Agent instances:

- 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

The table below provides hardware recommendations for standalone deployments, based on network size. System needs vary depending on the volume of Internet traffic. The table does not include information for the TRITON management server (see *System requirements for this version*, page 2).

The following baseline is used to create the recommendations:

- 1 - 500 users = 1 - 100 requests per second (rps)
- 500 - 2,500 users = 100 - 500 rps
- 2,500 - 10,000 users = 500 - 2,250 rps

Important

- 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.

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

Network Size	Filtering Components	Reporting (Windows)
1 - 500 users	**Windows** or **Linux** • Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater • 4 GB RAM • 10 GB free disk space (Free space must equal at least 20% of total disk space.)	**Windows** • Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater • 4 GB RAM • 100 GB free disk space • Microsoft SQL Server 2008 or 2005, or SQL Server 2008 R2 Express required for Log Database
500 - 2,500 users	**Windows** or **Linux** • Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater • 4 GB RAM • 10 GB free disk space (Free space must equal at least 20% of total disk space.)	**Windows** • Quad-Core Intel Xeon 5420 or better processor, 2.5 GHz or greater • 4 GB RAM • 100 GB free disk space • Microsoft SQL Server 2008 or 2005, or SQL Server 2008 R2 Express required for Log Database

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

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.

For networks with 2,500-10,000 users, at least two Network Agent instances, running on separate machines, are required. 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.

Standalone deployment guidelines for Network Agent

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x	- *Network Agent with multiple NICs*, page 54 - *NAT and Network Agent*, page 55

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

As with integrated proxies, firewalls, and network appliances, Network Agent can be configured to monitor HTTP requests, query Filtering Service to determine whether to permit or block each request, and then log the results of the query. Network Agent can also be configured to monitor, filter, and log non-HTTP requests (including requests that do not originate from an Internet browser).

When Network Agent is used, it must be installed:

- Inside the corporate firewall
- Where it can see all Internet requests for the machines it is assigned to monitor

Network Agent monitors and manages only the traffic that passes through the network device (typically a switch) to which it is attached. Multiple Network Agent instances may be needed, depending on:

- network size
- volume of Internet requests
- network configuration

While a 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.

For more information, see:

- *Network Agent with multiple NICs*, page 54
- *NAT and Network Agent*, page 55
- *Positioning Network Agent in the network*, page 55

Network Agent with 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**.
- 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 information on configuring multiple NICs, see the Network Agent Quick Start.

NAT and Network Agent

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.

Positioning Network Agent in the network

Collection: Deployment and Installation Center | Product: Web Security | Version: 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x	

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

If the Network Agent machine connects to a switch:

- Configure the switch 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.

> ✓ **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.

- Optionally, 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.

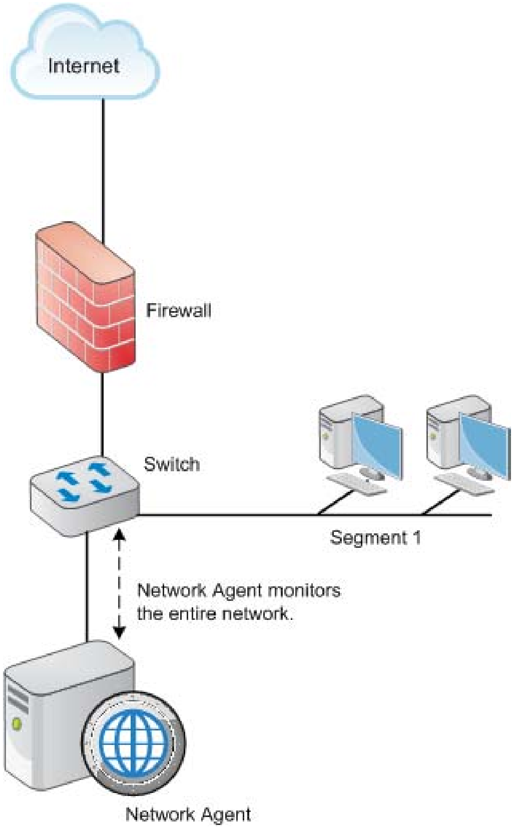
Network Agent can also be installed on a dedicated machine, connected to an unmanaged, unswitched hub located between an external router and the network.

To ensure that Network Agent is able to monitor the expected traffic, it must both be positioned properly and configured in TRITON - Web Security. See Network Agent configuration in the TRITON - Web Security Help for instructions.

Locating Network Agent in a 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 Web Security deployment, installed in a central location to see both HTTP and non-HTTP traffic.



Locating Network Agent in a multiple-segment network

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:

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

Multiple Network Agent instances may be needed 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.

If multiple Network Agent instances are installed:

- Ensure that the instances are deployed so that, together, they monitor the entire network. Partial deployment results in incomplete filtering and loss of log data in network segments not visible to Network Agent.
- Each Network Agent instance must monitor a non-overlapping set of IP addresses. 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 instance is determined by the NIC settings for the agent, configured in TRITON - Web Security. 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.

Central Network Agent placement

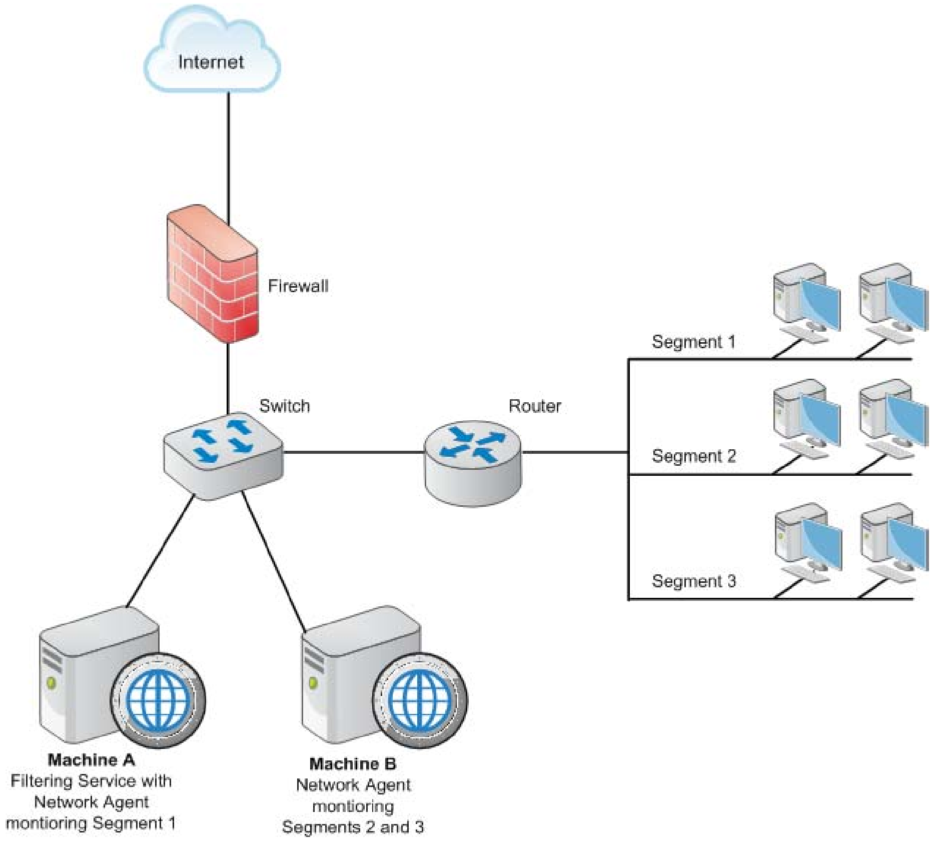
A network with multiple segments can be filtered from a single location. Install Filtering Service where it can receive Internet requests from each Network Agent and any integration product.

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.

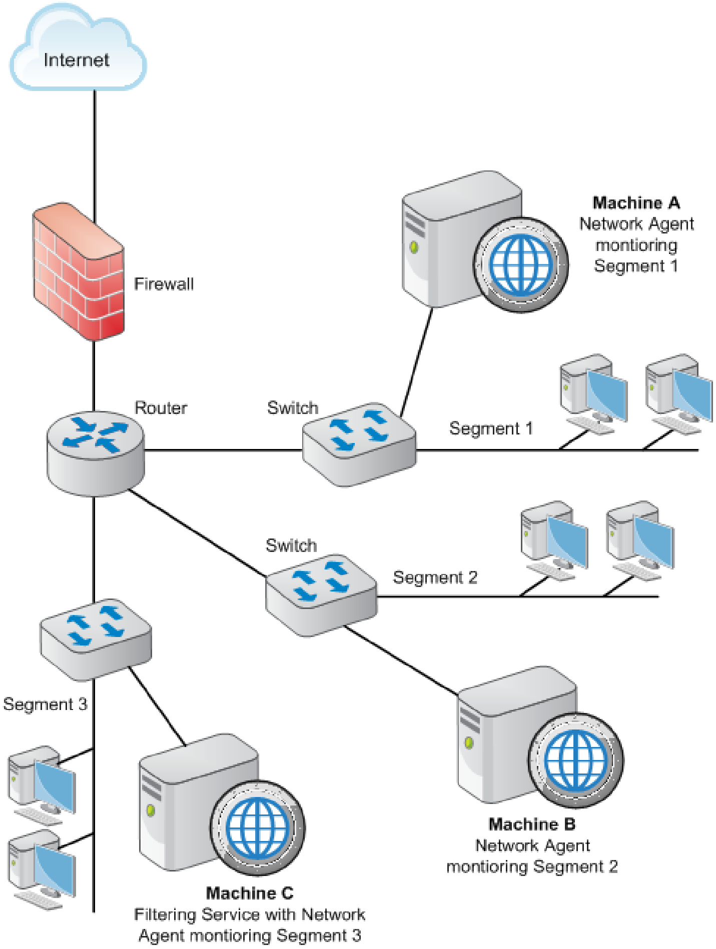


Distributed Network Agent placement

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 each Network Agent instance and any integration product.
- Each Network Agent (machines A, B and C) is connected to the network segment it monitors via the switch’s span or mirror port.

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.



Network Agent on a 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.

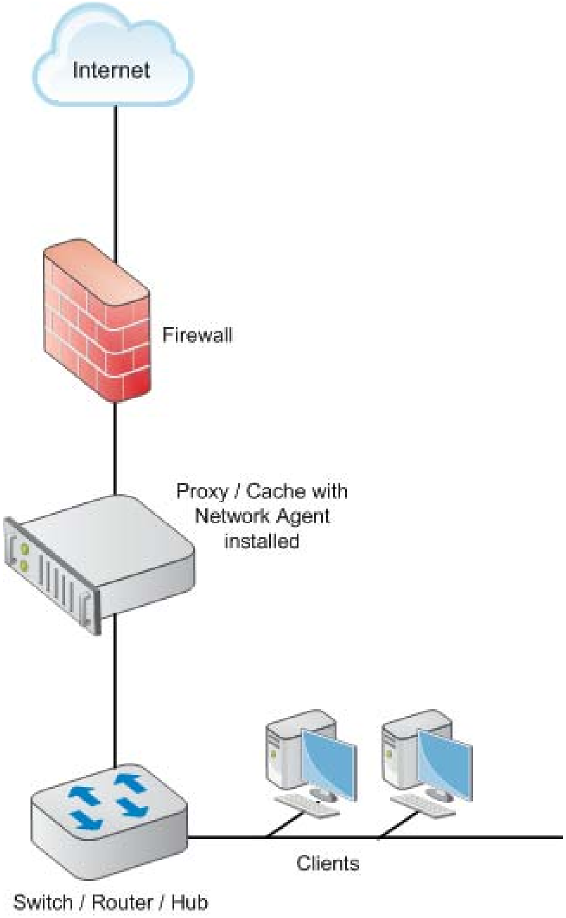
Do not install Network Agent on a firewall. Also, if your network includes a software installation of Content Gateway, do not install Network Agent on the Content Gateway machine. (Content Gateway and Network Agent can reside on the same V-Series appliance.)

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



Deploying Remote Filtering Server and Client

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

With all Web Security solutions, you have the option to use remote filtering software to manage Internet activity for machines that reside or travel outside your network.

- **Remote Filtering Client** is installed on each remote machine.
- The client software communicates with **Remote Filtering Server**, which acts as a proxy to Websense Filtering Service.

Communication between the components 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.

When you install remote filtering components:

- Install Remote Filtering Server on a dedicated machine that can communicate with the Filtering Service machine.

  As a best practice, install Remote Filtering Server in the DMZ outside the firewall protecting the rest of the corporate network. This is strongly recommended.
- Do **not** install 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.

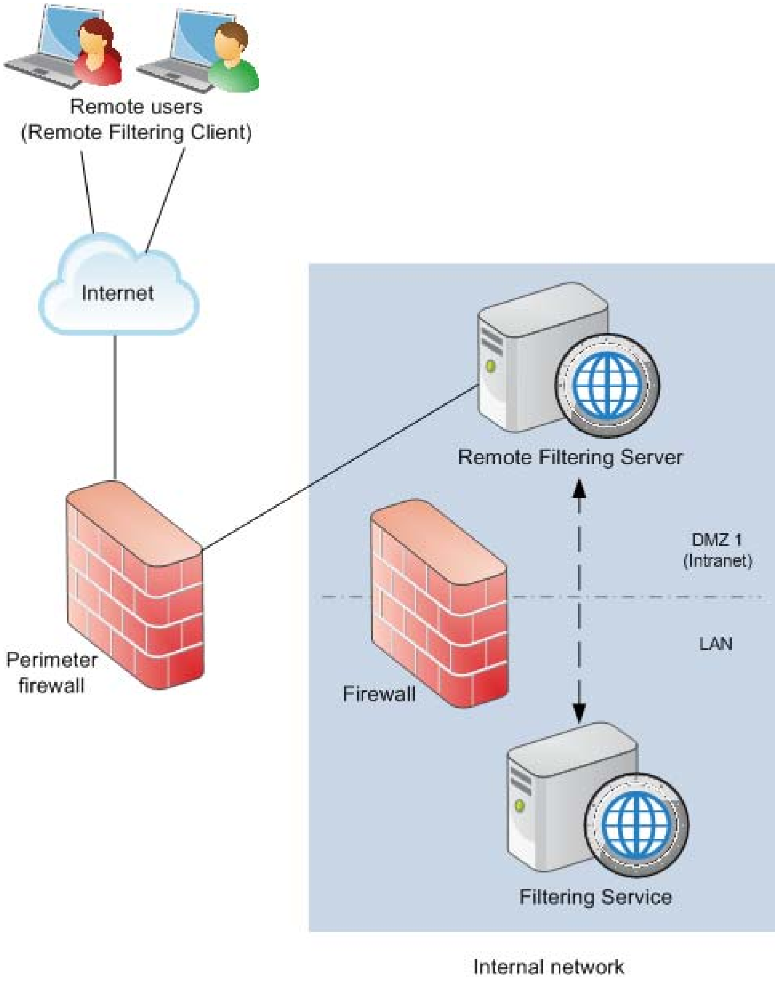
Remote Filtering Client system recommendations:

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

- 512 MB RAM

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

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.



Using the TRITON management server as policy source for filtering-only appliances

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- V10000, V10000 G2, and V5000 G2, v7.7.x

It is possible to deploy Web Security components so that the central Policy Broker and Policy Server are installed on the TRITON management server, and Websense filtering only appliances use that machine as the full policy source.

If you choose this deployment option, it is important to install your components in the following order.

1. Install Policy Broker, Policy Server, and (if you are installing Web Security Gateway Anywhere) Linking Service on the machine that will become the TRITON management server. See *Installing Web Security components*, page 392.
2. Set up the appliance to run in **filtering only** mode, specifying the Policy Broker machine (the future TRITON management server) as the policy source.
3. Create a TRITON management server with either the Web Security module only or the Web and Data Security modules of the TRITON Unified Security Center. See *Creating a TRITON Management Server*, page 180.
4. Install off-appliance components as necessary. See *Installing Web Security components*, page 392.

3 Deploying Web Security for a distributed enterprise

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

Distributed enterprise networks may have many remote locations, ranging from dozens to thousands of small sites. 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.

- 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.

Websense Web Security Gateway Anywhere is a hybrid solution, allowing a combination of on-premises and in-the-cloud filtering.

For more information, see:

- *Web Security basic distributed enterprise topology*, page 66
- *Web Security filtering remote sites*, page 70

- *Web Security distributed enterprise deployment models*, page 74
- *Web Security distributed deployments and secure VPN connections*, page 81

Web Security basic distributed enterprise topology

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

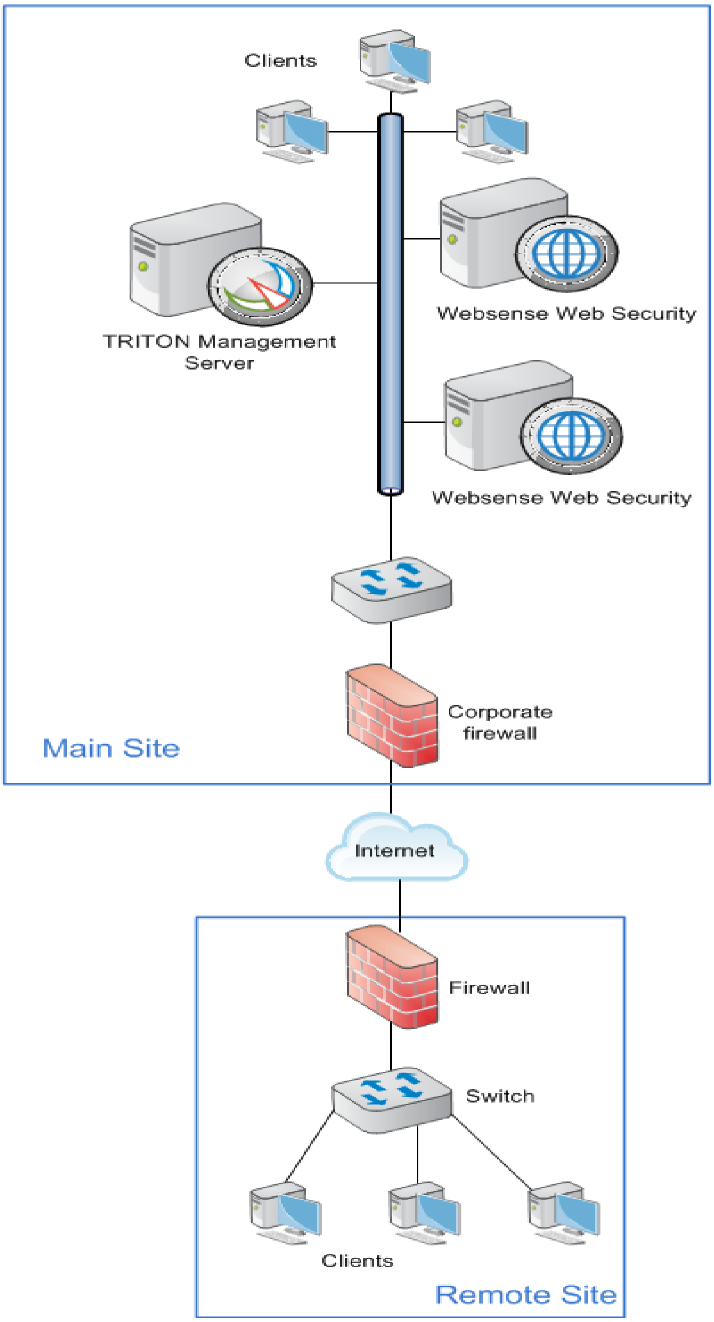
Applies to:	In this topic
- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	- *Web Security and Web Security Gateway*, page 66 - *Websense Web Security Gateway Anywhere*, page 69

Web Security and Web Security Gateway

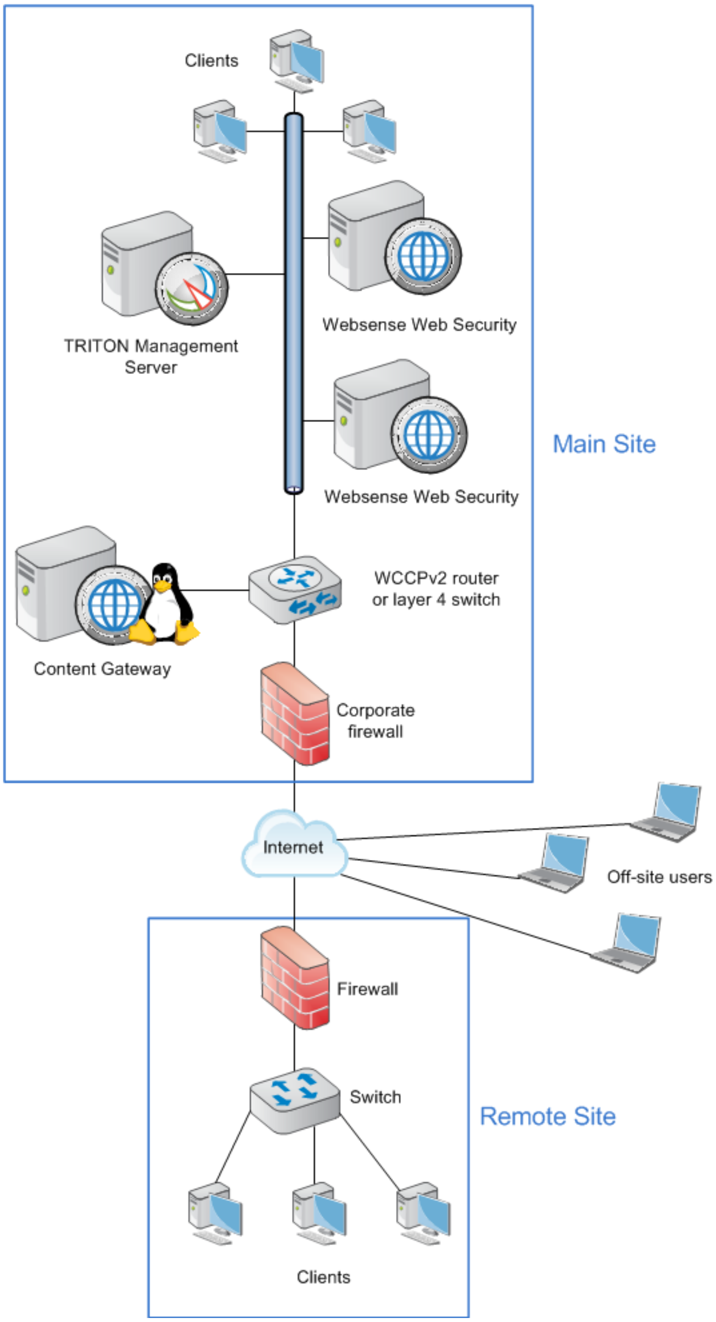
To reduce network infrastructure costs, each remote-site firewall in a decentralized network is connected directly to the Internet, rather than to a corporate WAN.

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.

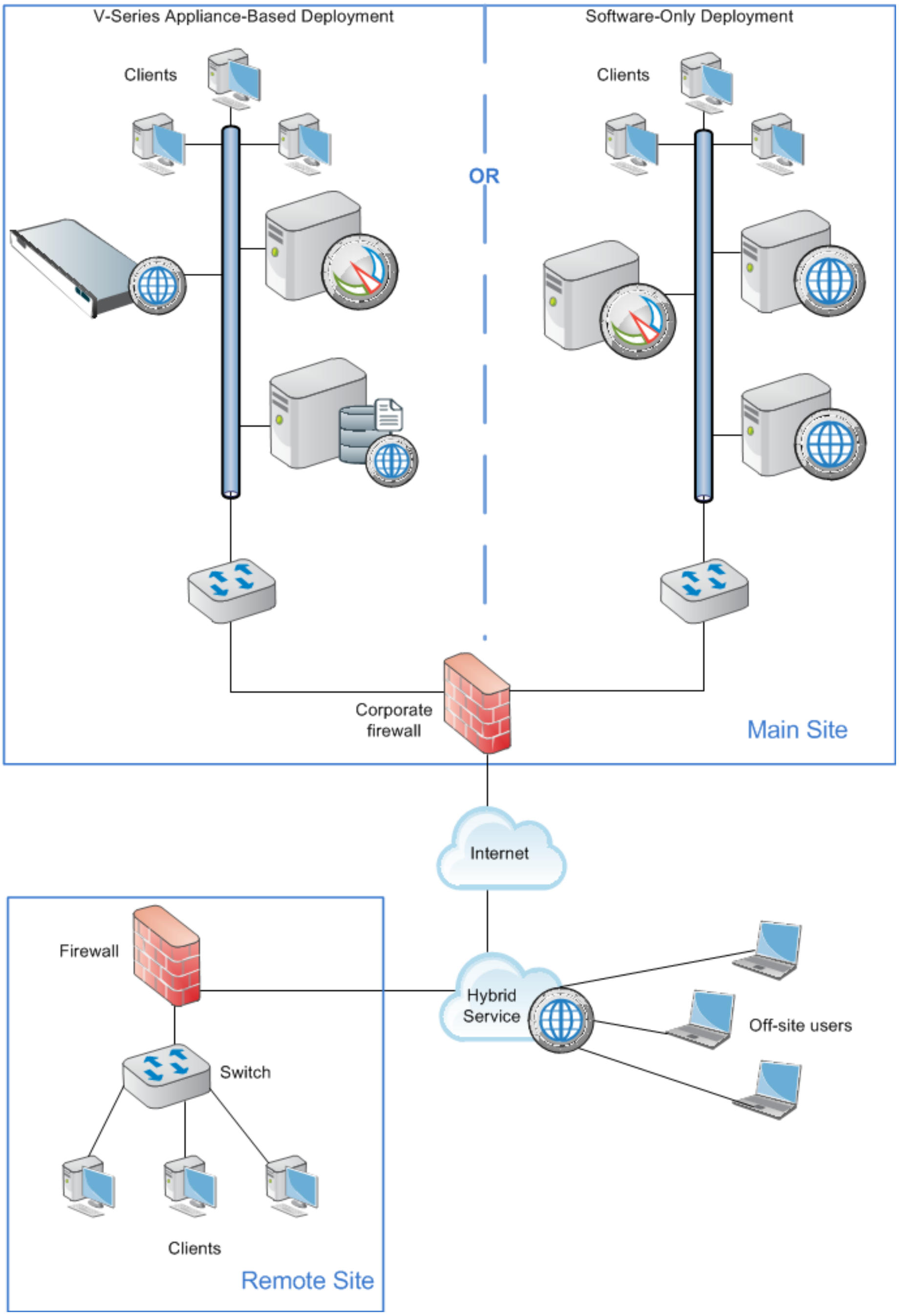


Optionally, off-site users (remote users outside the corporate or remote-site network) can be filtered using Websense remote filtering software. This requires that Remote Filtering Server (not depicted) be deployed in the main site network and Remote Filtering Client be installed on each off-site machine. See *Deploying Remote Filtering Server and Client*, page 62.

The above two illustrations show a high-level scheme only. Details about how Websense filtering components might be distributed across separate machines, Content Gateway deployment, Network Agent placement, use of an integration product, and so forth are not included.

Websense Web Security Gateway Anywhere

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



Web Security Gateway Anywhere software is installed at the main site. This may include:

- One or more Websense V-Series appliances running core filtering components, plus additional servers running reporting, management, and interoperability components.
- One or more Windows or Linux servers running core filtering and interoperability components, plus Windows servers running reporting and management components.

Either Websense remote filtering software or the hybrid service can be used to manage Internet activity for remote sites or off-site machines.

See the TRITON - Web Security Help for more information about configuring the hybrid service for off-site users.

Web Security filtering remote sites

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Websense Web Security or Web Security Gateway*, page 70 ◆ *Websense Web Security Gateway Anywhere*, page 72

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.

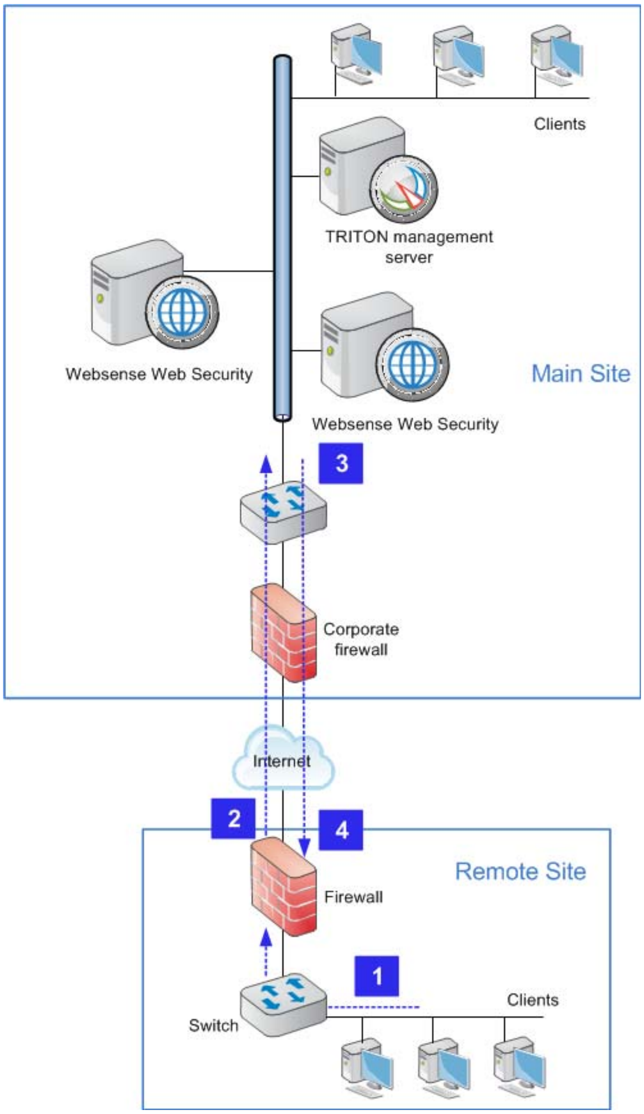
Websense, Inc., has tested this configuration in cooperation with several of its integration partners. A full list of supported integration products can be found at:

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

Centralized filtering Provides distributed enterprises with Websense filtering for each remote site. It also:

- 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 the basic sequence of events involved in filtering a client machine at a remote site.



1. A user requests a Web page.

2. The request is directed through the local firewall to Web Security software at the main site via the Internet.
3. Web Security software responds via the Internet, either permitting or blocking the request.
4. The user is given access to the site or sees a block page.

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

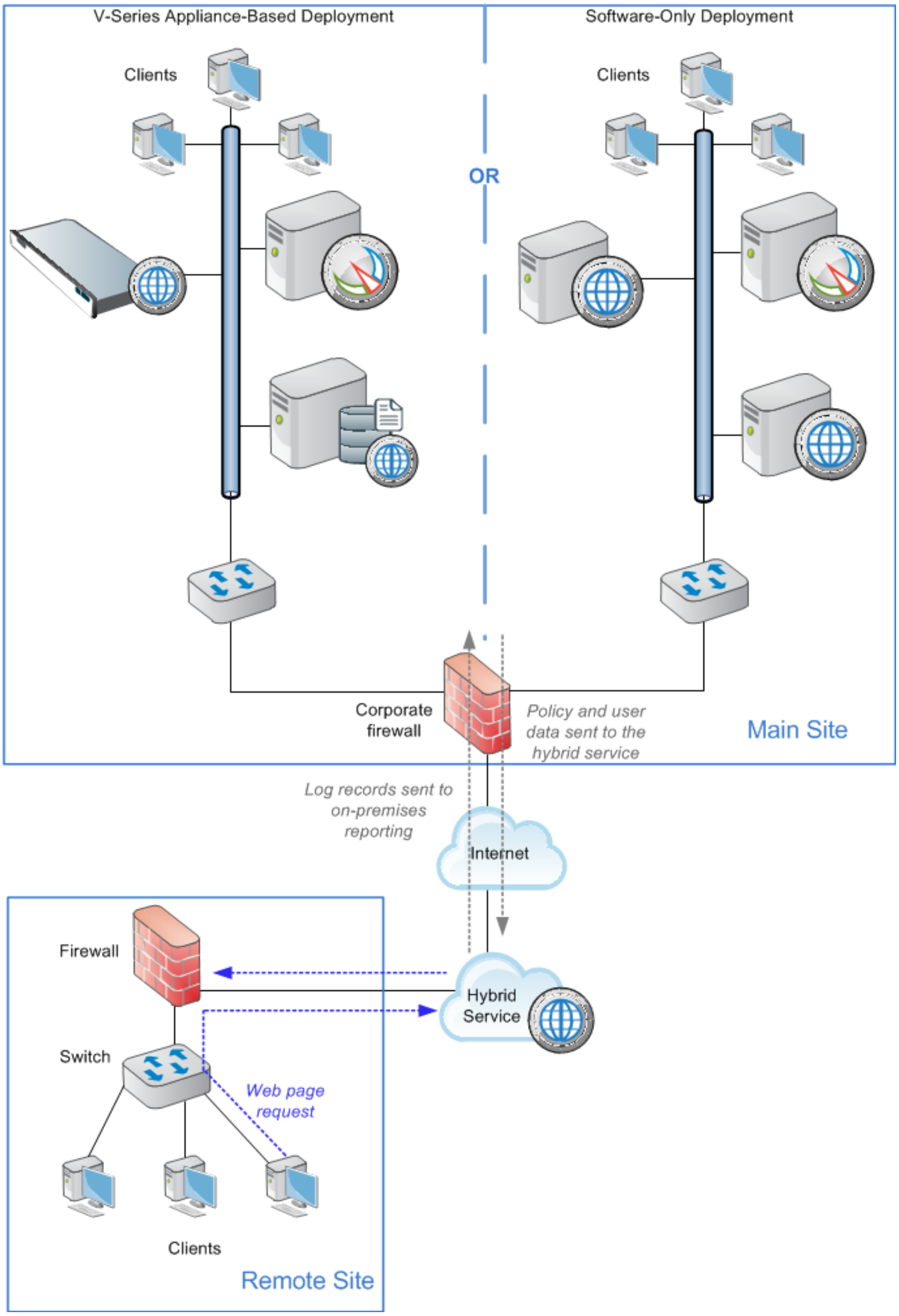
Off-site user machines (like laptops used by travelers) may be filtered using Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 62.

Websense Web Security Gateway Anywhere

In a Web Security Gateway Anywhere deployment, remote sites can be filtered either by the hybrid service or by Websense security solutions installed at the main site.

Using the hybrid service may address network latency issues, because remote sites and off-site users are filtered by the nearest Websense hybrid service cluster.

The following illustration shows how remote-site filtering works via the hybrid service. 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 may be filtered by the hybrid service, or using Websense remove filtering software. See *Deploying Remote Filtering Server and Client*, page 62.

Web Security distributed enterprise deployment models

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	**In this topic**
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Sites in a region*, page 74 ◆ *Expanding sites in a region*, page 76 ◆ *National or worldwide offices*, page 78

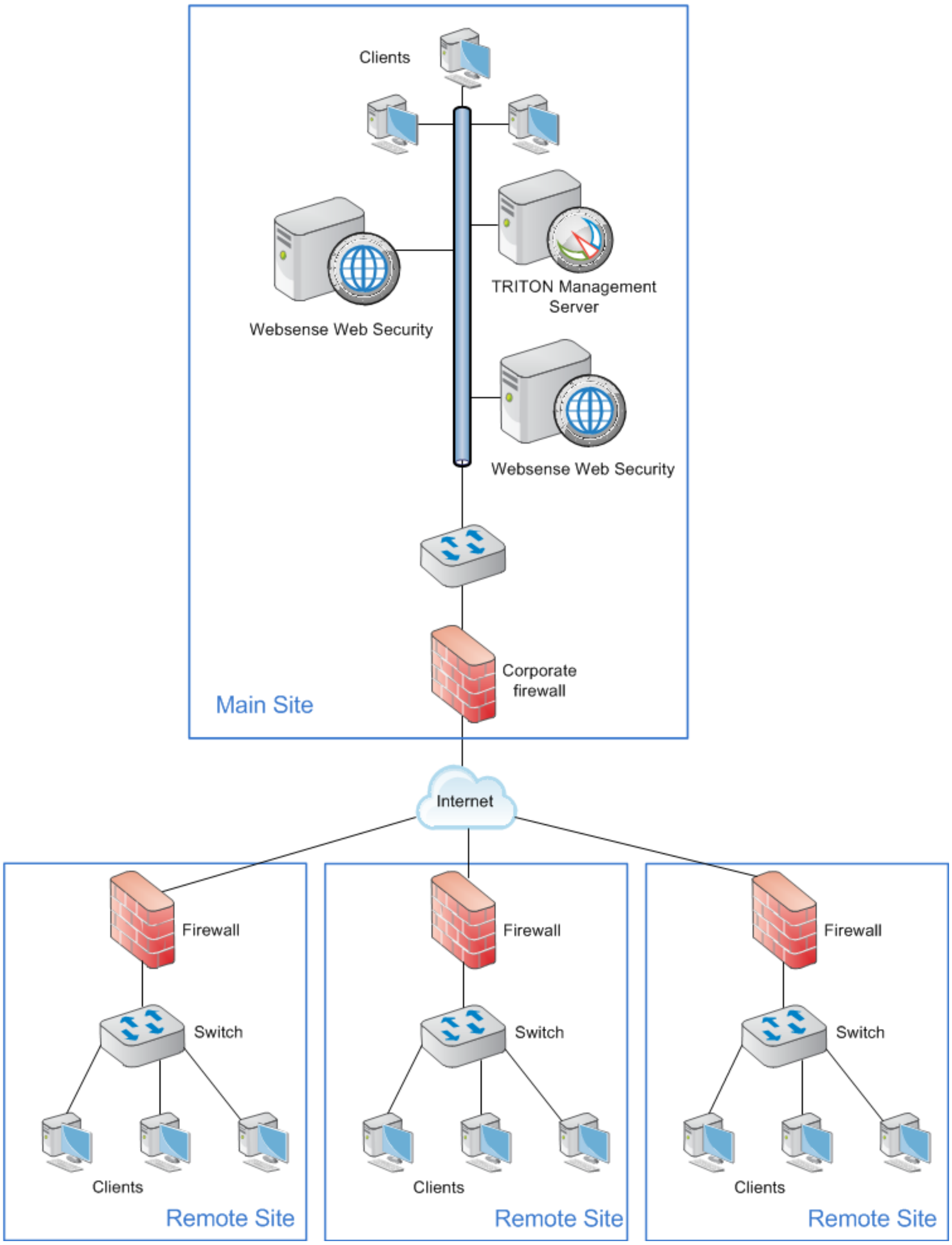
Deployment scenarios vary with different enterprise configurations. For example, an organization with 50 remote sites, all located in the same general region, deploys Websense software differently than a company with remote sites spread throughout the world. This section discusses 3 basic example models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

- *Sites in a region*, page 74: Remote sites located within one region
- *Expanding sites in a region*, page 76: Remote sites located within one region, with a growing number of employees or sites (or both)
- *National or worldwide offices*, page 78: 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 70. 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 software. See *Deploying Remote Filtering Server and Client*, page 62.

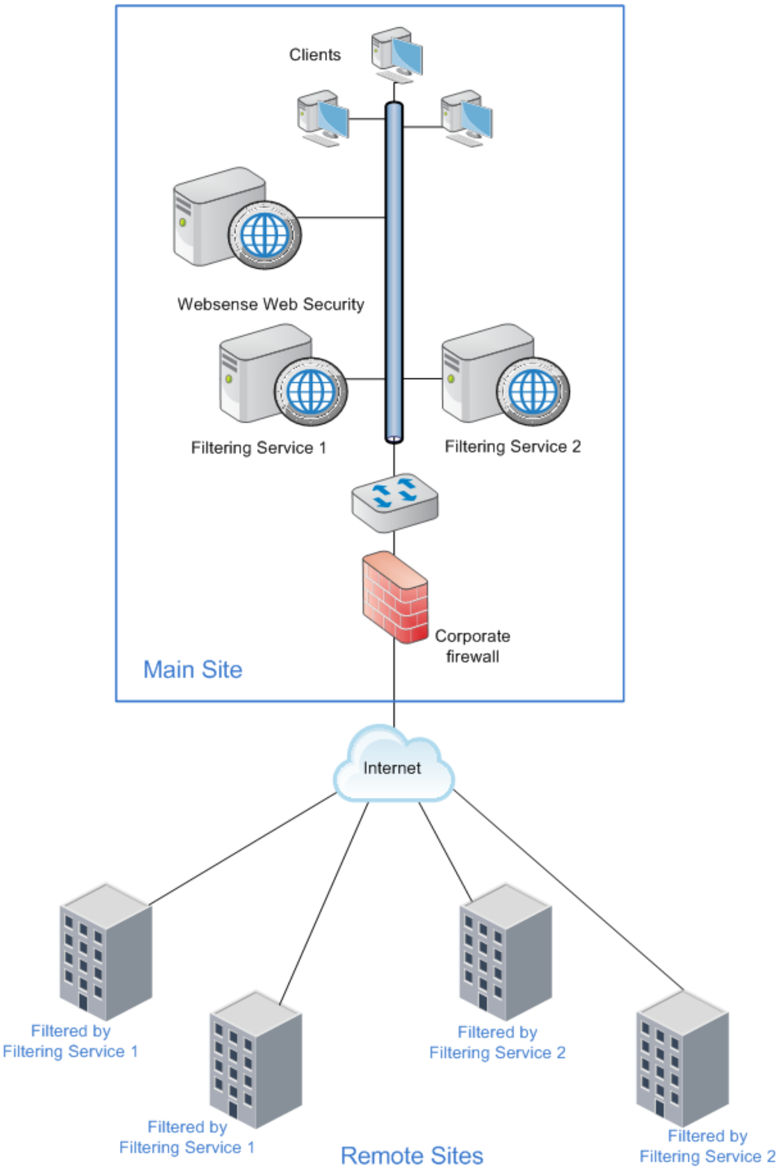
Expanding sites in a region

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.


Clients
Websense Web Security
Filtering Service 1
Filtering Service 2
Corporate firewall
Main Site
Internet
Filtered by Filtering Service 1
Filtered by Filtering Service 1
Filtered by Filtering Service 2
Filtered by Filtering Service 2
Remote Sites

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

Off-site users, not shown in the preceding illustration, can be filtered by Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 62.

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.

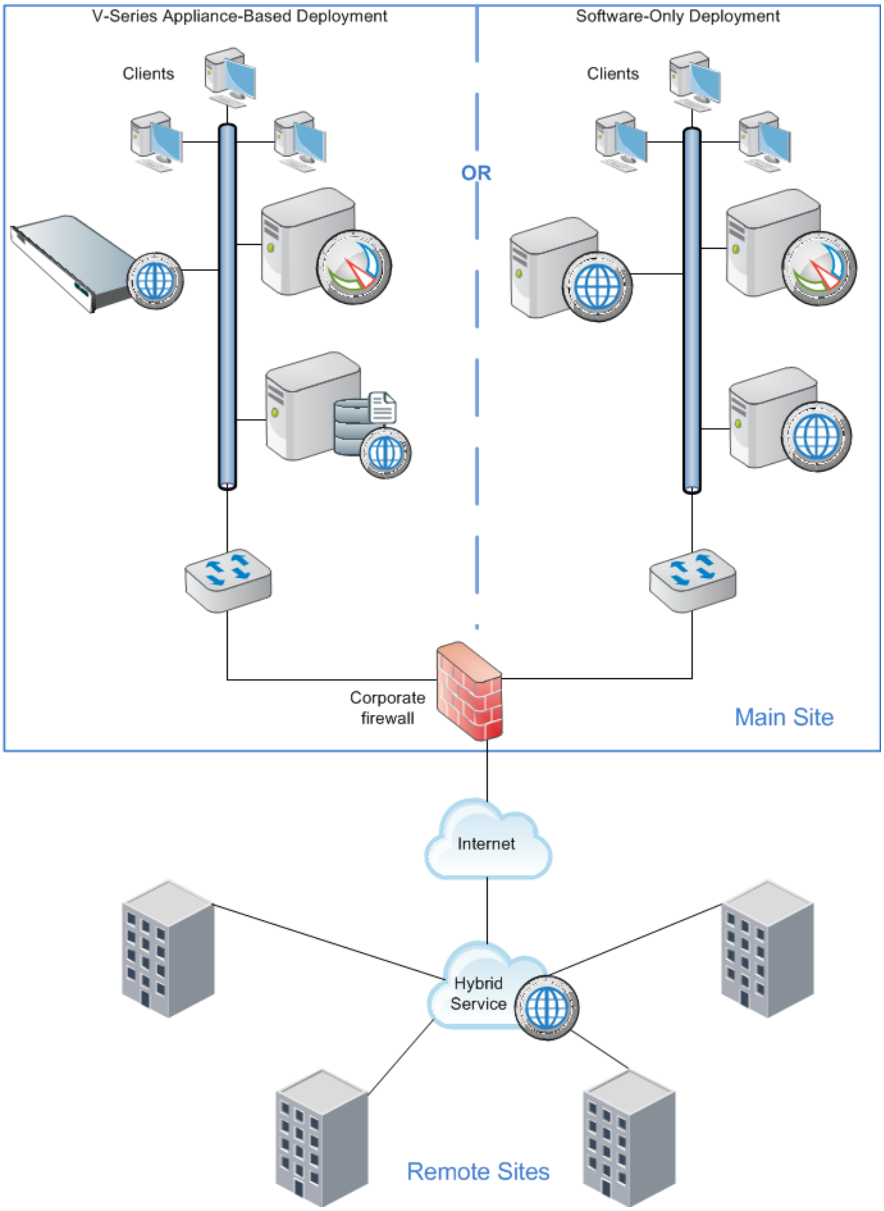
Given the significant number of variables, large organizations should contact a Websense partner or Websense Sales Engineering to plan a rollout strategy before deployment.

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

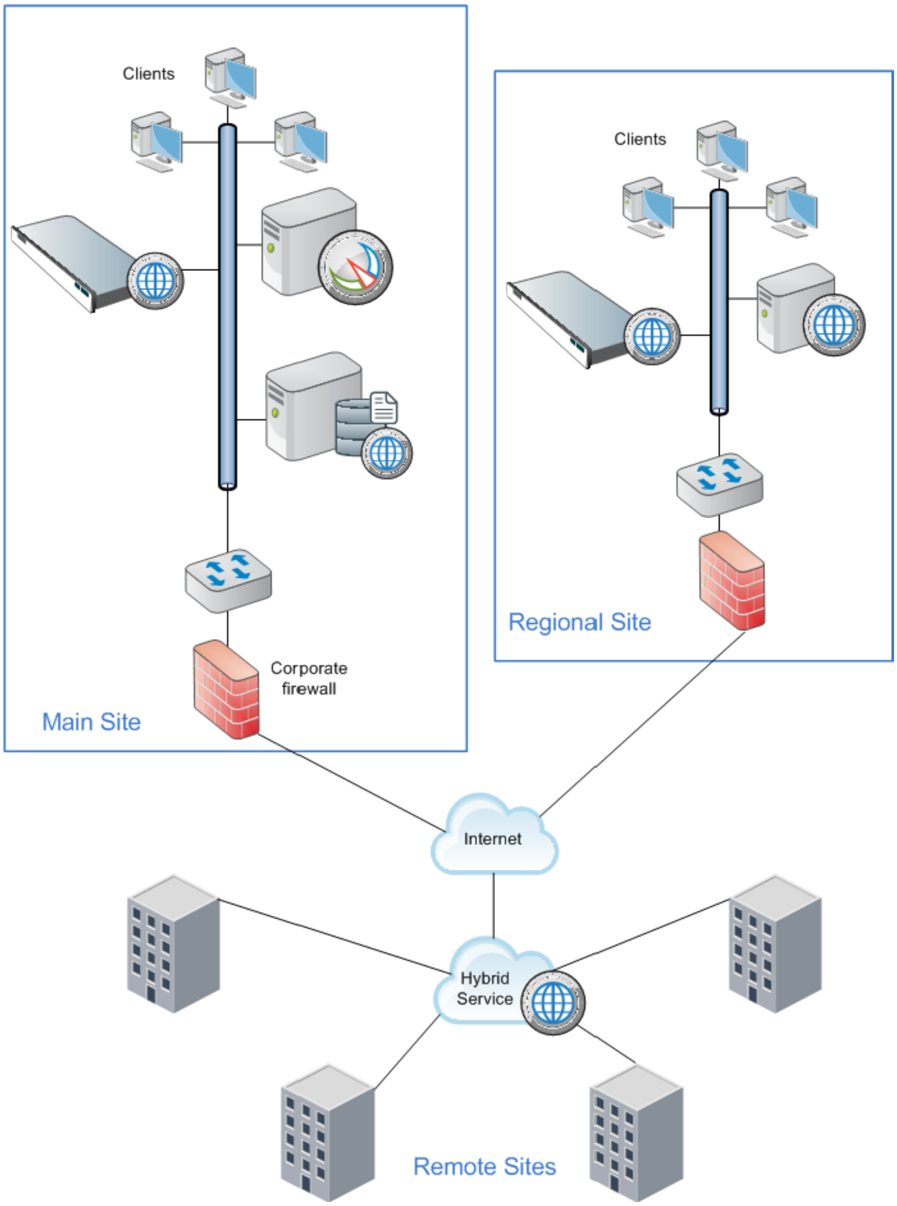
An organization with one main site (such as headquarters office or main campus) and multiple, geographically dispersed remote or branch sites can deploy Websense software at the main site (with main-site users filtered by the on-premises components) and have all remote sites filtered through the hybrid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



Off-site users, not shown in the above illustration, may either be managed by the hybrid service, or with Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 62.

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. Though the illustration shows a V-Series appliance deployment, this can also be accomplished with software-only deployments.



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 *Extending your Web Security deployment*, page 31, 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 **full policy source**. See the appliance Getting Started Guide and the 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 above illustration, may either be managed by the hybrid service, or with Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 62.

Web Security distributed deployments and secure VPN connections

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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 48. For information about installing RADIUS Agent, see *Installing Web Security components*, page 392.

4 Content Gateway Deployment

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Gateway Anywhere, v7.7.x

Content Gateway is a high-performance Web proxy that provides real-time threat analysis and Web site classification to protect network computers from malicious Web content and attacks, while facilitating employee access to Web assets and dynamic Web content.

Content Gateway offers:

- On-demand, real-time categorization of Web sites
- HTTP/S and FTP content analysis for malware and malicious threats
- Enterprise Web caching capabilities

Websense Content Gateway is a required add-on module with Websense Web Security Gateway (Anywhere).

Standard deployments include:

- On-premises with Web Security Gateway
- On-premises with Web Security Gateway Anywhere, which provides support for distributed enterprises with one or more branch offices and multiple remote users

Content Gateway can be located on Websense V-Series appliances or as software running on general purpose servers.

Content Gateway can also improve network efficiency and performance by caching frequently accessed Web pages at the edge of the network.

The following topics discuss deployment of Content Gateway:

- *Content Gateway deployment issues*, page 84
- *Content Gateway explicit and transparent proxy deployments*, page 88
- *Special Content Gateway deployment scenarios*, page 93
- *Chaining Content Gateway with other proxies*, page 99

For information about deploying Web Security Gateway software, see *Installation overview: Web Security Gateway*, page 197.

For information about Content Gateway operation, see Content Gateway Manager Help.

Content Gateway deployment issues

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway and Gateway Anywhere, v7.7.x	◆ *Proxy deployment options*, page 84 ◆ *User authentication*, page 85 ◆ *HTTPS content inspection*, page 87 ◆ *Handling special cases*, page 87

Planning to deploy Websense Content Gateway as a proxy in your network should include physical requirements, such as:

- data center location and space
- power and cooling requirements for hardware
- required rack space
- connectivity to existing or extended network topology

Also consider:

- Content Gateway system requirements (hardware and operating system)
- Advantages and disadvantages of proxy network configuration options
- User authentication and identification options
- How to configure and use 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, typically a Web browser, is configured to send a request for Internet content directly to Content Gateway.

In a transparent proxy deployment, a client request for Web content is intercepted (usually by a router) and sent to the proxy. The client is unaware that it is communicating with a proxy.

Both options have advantages and disadvantages. See *Content Gateway explicit and transparent proxy deployments*, page 88 for more information.

Management clustering

A Websense Content Gateway deployment can scale from a single node to multiple nodes to form a management cluster. With management clustering, all the nodes in the cluster share configuration information. A configuration change on one node is automatically propagated all other nodes.

When SSL Manager is enabled to perform HTTPS content inspection, SSL 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 Help for information about configuring Content Gateway clusters.

IP spoofing

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 in transparent proxy deployments only. 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 ports 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 Help.

User authentication

User authentication is the process of verifying a user via a username and password. Several types of user authentication are supported by 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

Content Gateway can be configured for *transparent user authentication* -- with Integrated Windows® Authentication (IWA) or Legacy NTLM -- in which users are not prompted for credentials. Alternatively, Content Gateway can be configured for *prompted* (or *manual) authentication*, in which users are required to enter a username and password to obtain network access.

✓ **Note**

Not all Web browsers support both transparent and prompted authentication modes.

See the v7.7 Websense Content Gateway Release Notes 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 that 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 user 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 96 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 Help for detailed information about configuring these proxy user 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 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 Content Gateway with HTTPS (SSL Manager) enabled, HTTPS data can be decrypted, inspected, 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, you can specify categories of Web sites, individual Web sites, and clients for which decryption and inspection are always bypassed. See *SSL Decryption Bypass* in TRITON - Web Security Help for more information.

Handling special cases

Any 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 Help.

See, also: Web sites that have difficulty transiting Content Gateway.

Content Gateway explicit and transparent proxy deployments

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway and Gateway Anywhere, v7.7.x	◆ *Explicit proxy deployment*, page 88 ◆ *Transparent proxy deployment*, page 89

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 Content Gateway
- *Transparent proxy deployment*, where user requests are automatically redirected to a 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 Content Gateway, see *Explicit Proxy, Transparent Proxy, and ARM* in the Content Gateway Manager Help.

Explicit proxy deployment

Use of 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* in Content Gateway Manager Help for a sample PAC file and more information about how to implement these options. See also: PAC file best practices.

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 and ARM* in Content Gateway Manager 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 and ARM* in Content Gateway Manager 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 and ARM* in Content Gateway Manager 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.

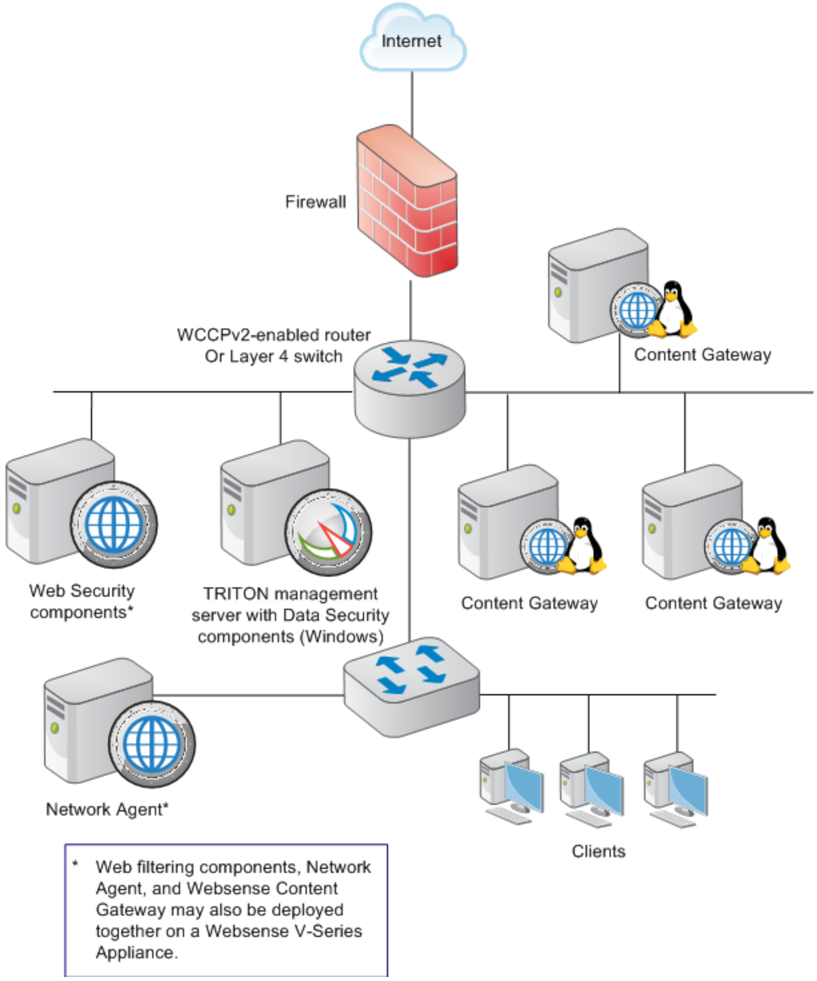
A router may also use Layer 2 (L2), which does not use GRE. Websense recommends the use of L2 if the router supports it. With L2 redirection, Content Gateway must be on the same subnet as the WCCP device (that is, Layer 2 adjacent).

! **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.



* Web filtering components, Network Agent, and Websense Content Gateway may also be deployed together on a Websense V-Series Appliance.

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 user 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Gateway Anywhere, v7.7.x

In this topic

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 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

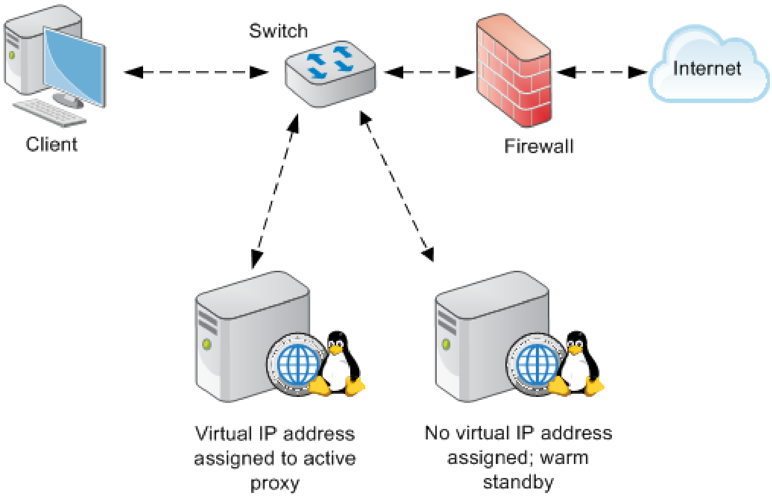
As previously mentioned for the explicit proxy deployment, clients are specifically configured to send requests directly to a proxy. The configuration can be accomplished manually, or via a PAC file or a WPAD server.

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.


Switch
Client
Firewall
Internet
Virtual IP address assigned to active proxy
No virtual IP address assigned; warm standby

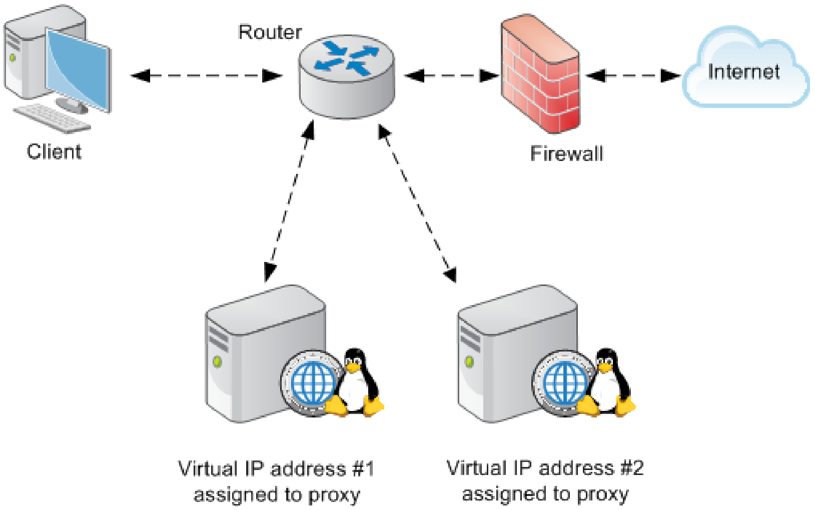
Active/Active

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.

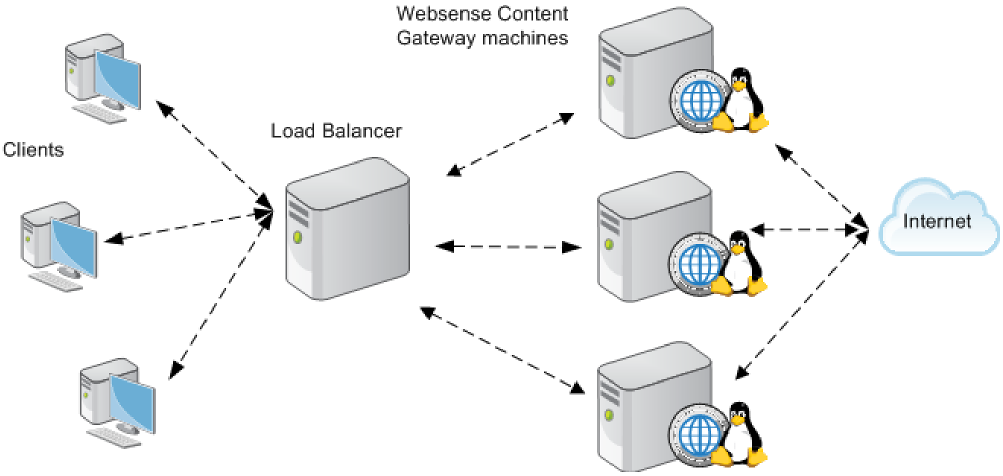
As with the active/standby configuration, an available proxy can assume a failed proxy’s load. Below is an example.


Router
Client
Firewall
Internet
Virtual IP address #1 assigned to proxy
Virtual IP address #2 assigned to proxy

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.



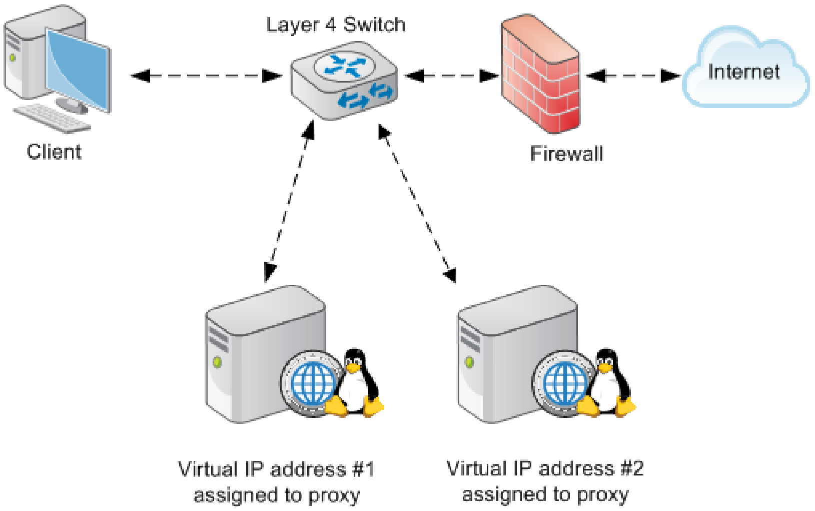
Using transparent proxy

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.



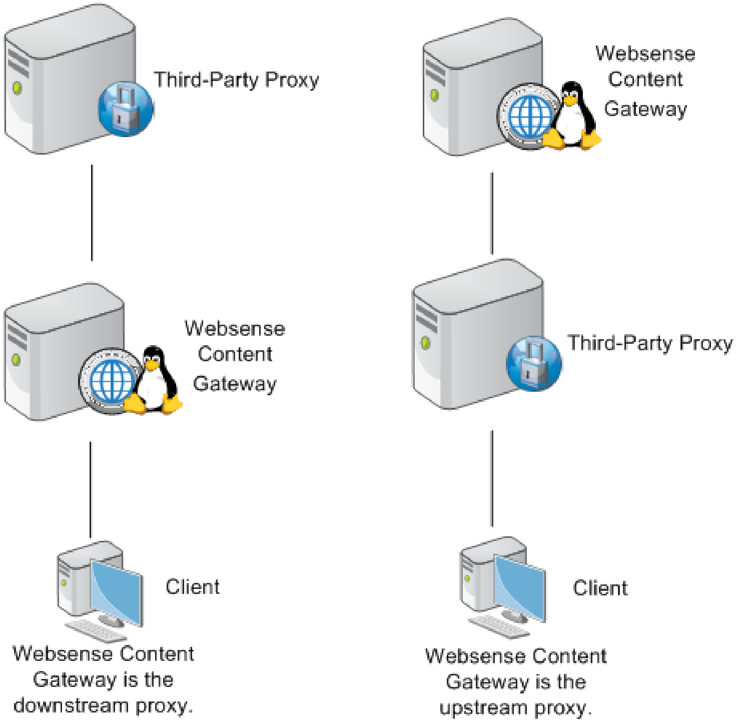
Using a WCCPv2-enabled router

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 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.


Third-Party Proxy
Websense Content Gateway
Client
Websense Content Gateway is the downstream proxy.
Websense Content Gateway
Third-Party Proxy
Client
Websense Content Gateway is the upstream proxy.

See *Chaining Content Gateway with other proxies*, page 99, for specific instructions on using Blue Coat® ProxySG® or Microsoft ISA/TMG 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 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. 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 48, and *Installing Web Security components*, page 392.

Websense Content Gateway is upstream

When 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. 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 Content Gateway's 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 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 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 Content Gateway. See *Deploying transparent identification agents*, page 48, and *Installing Web Security components*, page 392.

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/ TMG server, see *Chaining Content Gateway with other proxies*, page 99.

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, Content Gateway can act either as a parent or child cache, either to other 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 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 SSL 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.

Chaining Content Gateway with other proxies

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway and Gateway Anywhere, v7.7.x	◆ *Blue Coat ProxySG*, page 100 ◆ *Microsoft Internet Security and Acceleration (ISA) server and Forefront Threat Management Gateway (TMG)*, page 101

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 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**)

   Also place the following files in the ISA or TMG installation directory:

   - msvcp100.dll

- msvcr100.dll

2. Register the plug-in with the system. Open a Windows command prompt and change directory to the Microsoft ISA or Forefront TMG installation directory.

   From the command prompt, type:

   ```
   regsvr32 Websense-AuthForward.dll
   ```

3. 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
```

5 Planning Data Security Deployment

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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:

Deciding what data to protect

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Geographical*, page 104 ◆ *Industry*, page 104 ◆ *Sector*, page 104 ◆ *General*, page 104

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Corporate file servers and shared drives*, page 105 ◆ *In-house databases*, page 106

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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.

Define Product Name Variable 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Allocating disk space*, page 109 ◆ *Modifying the disk space setting*, page 110 ◆ *Distributing resources*, page 111

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 112 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.

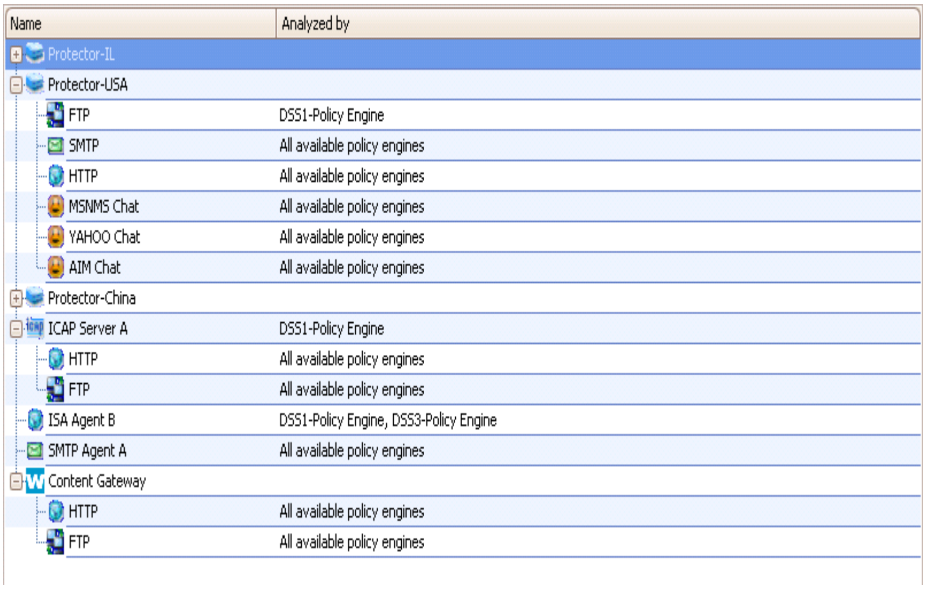
Load balancing enables you to manage how each module sends its data to specified policy engines for analysis. This lets you distribute the load, but more important, it ensures that your vital email and HTTP performance is never harmed. For example, you can designate 1-2 dedicated servers to analyze inline 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.



Name	Analyzed by
Protector-IL	
Protector-USA	
FTP	DSS1-Policy Engine
SMTP	All available policy engines
HTTP	All available policy engines
MSNMS Chat	All available policy engines
YAHOO Chat	All available policy engines
AIM Chat	All available policy engines
Protector-China	
ICAP Server A	DSS1-Policy Engine
HTTP	All available policy engines
FTP	All available policy engines
ISA Agent B	DSS1-Policy Engine, DSS3-Policy Engine
SMTP Agent A	All available policy engines
Content Gateway	
HTTP	All available policy engines
FTP	All available policy engines

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.

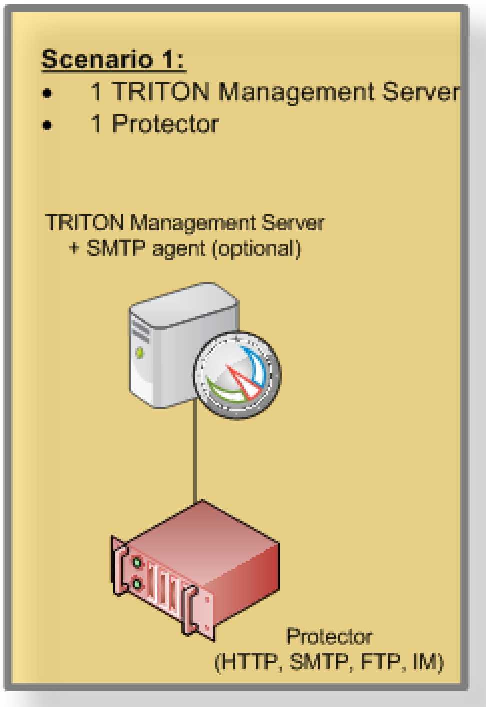
Most common deployments

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x ◆ Web Security Gateway, v7.7.x ◆ Web Security Gateway Anywhere, v7.7.x ◆ Email Security Gateway, v7.7.x	◆ *Websense Web Security Gateway Anywhere*, page 117 ◆ *Websense Email Security Gateway*, page 118 ◆ *Websense Data Monitor*, page 119 ◆ *Websense Data Protect*, page 120 ◆ *Websense Data Endpoint*, page 120 ◆ *Websense Data Discover*, page 121

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.

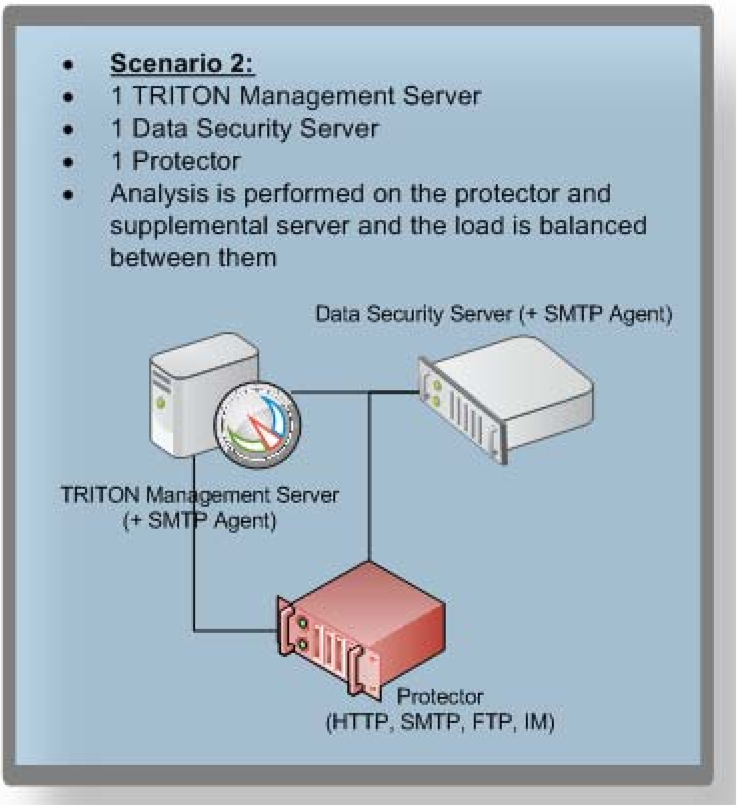


Scenario 1:

- 1 TRITON Management Server
- 1 Protector

TRITON Management Server
+ SMTP agent (optional)

Protector
(HTTP, SMTP, FTP, IM)

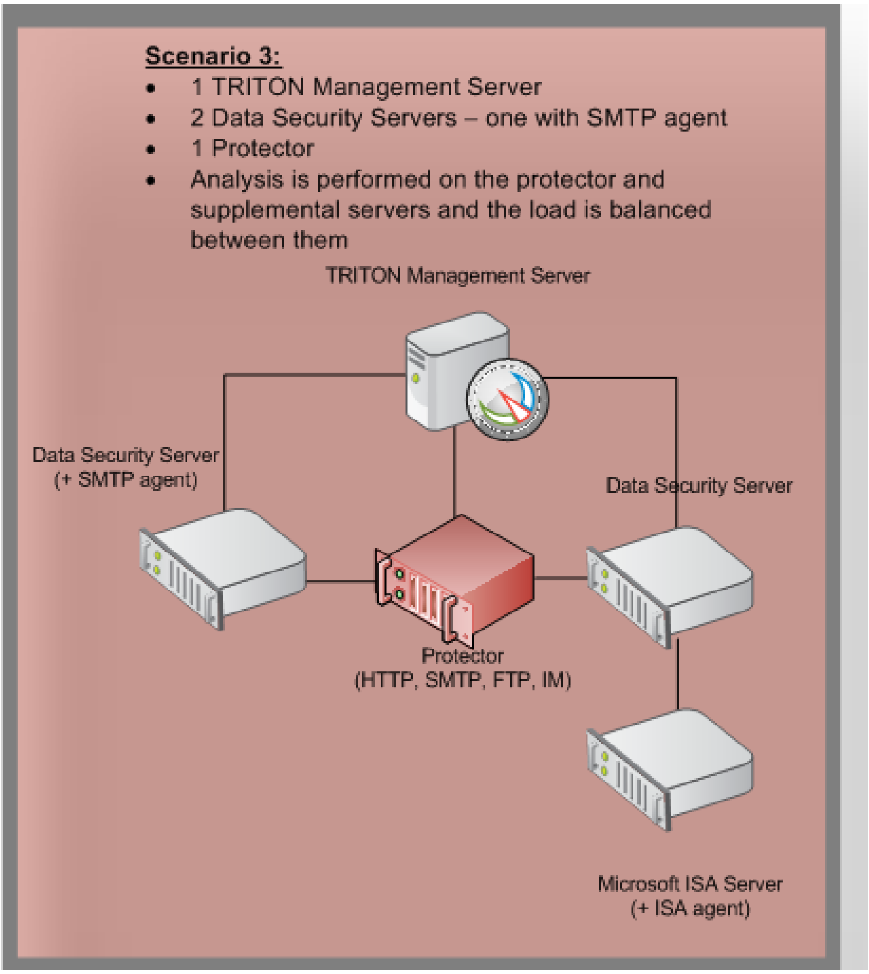


- **Scenario 2:**
- 1 TRITON Management Server
- 1 Data Security Server
- 1 Protector
- Analysis is performed on the protector and supplemental server and the load is balanced between them

Data Security Server (+ SMTP Agent)

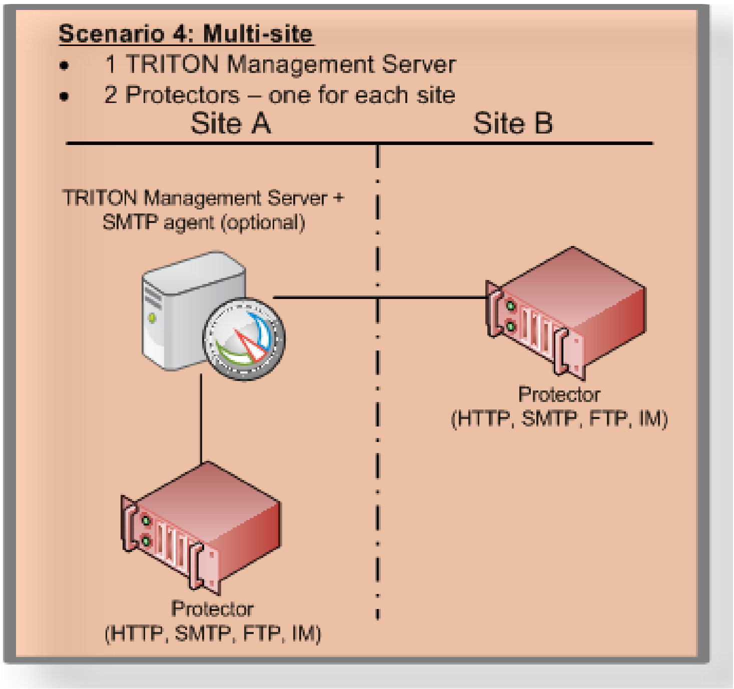
TRITON Management Server
(+ SMTP Agent)

Protector
(HTTP, SMTP, FTP, IM)



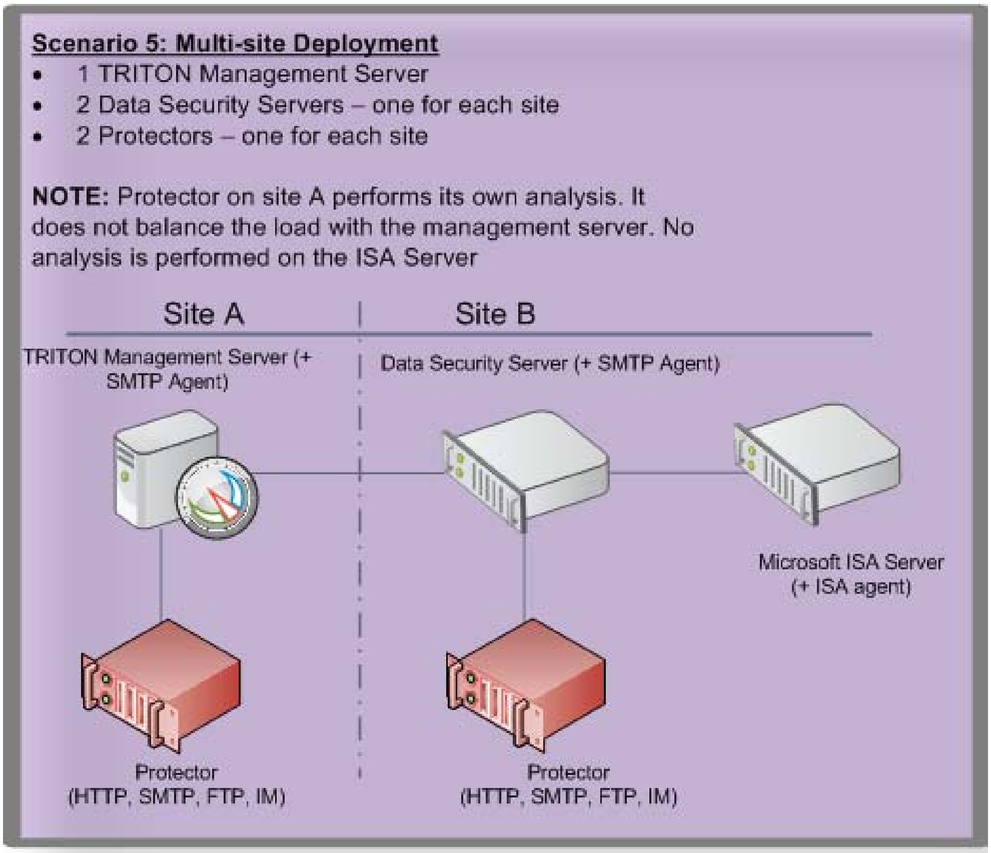
Scenario 3:

- 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



Scenario 4: Multi-site

- 1 TRITON Management Server
- 2 Protectors – one for each site

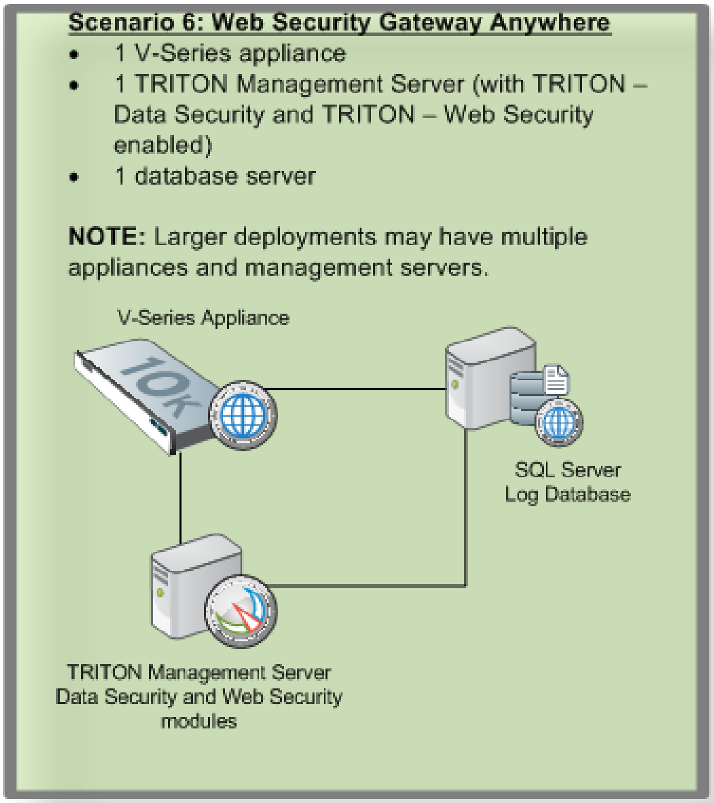


Scenario 5: Multi-site Deployment

- 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

Site A
Site B
TRITON Management Server (+ SMTP Agent)
Data Security Server (+ SMTP Agent)
Microsoft ISA Server (+ ISA agent)
Protector (HTTP, SMTP, FTP, IM)
Protector (HTTP, SMTP, FTP, IM)

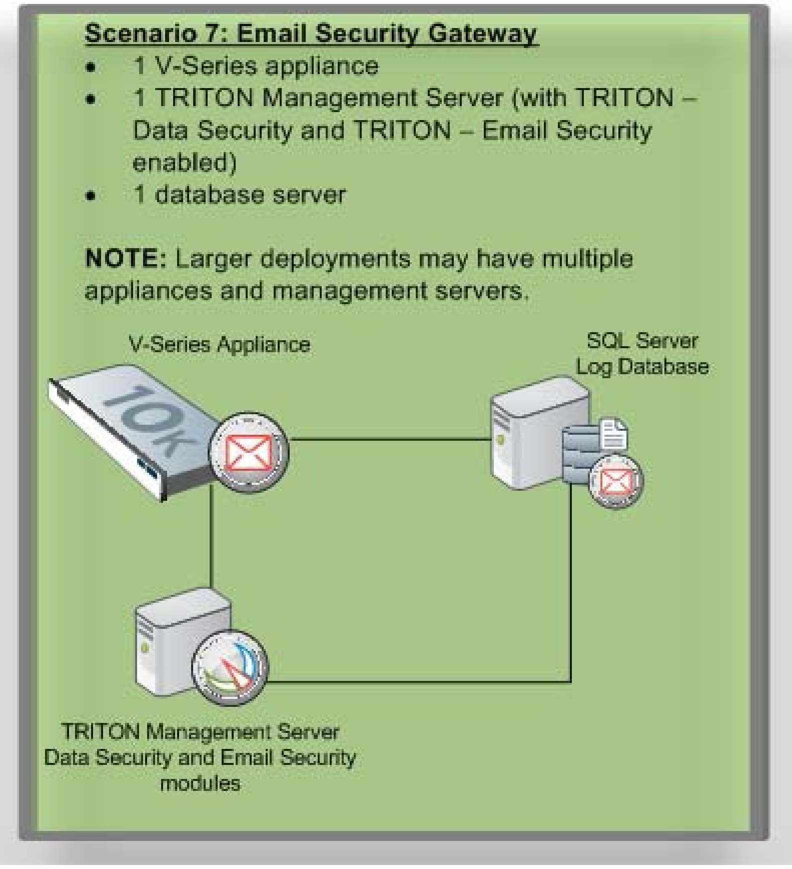


Scenario 6: Web Security Gateway Anywhere

- 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.

V-Series Appliance
10k
SQL Server Log Database
TRITON Management Server Data Security and Web Security modules



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.

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: - HTTP - HTTPS - FTP - FTP-over-HTTP	- 1 TRITON Management Server with Web Security and Data Security modules enabled - 1 V-Series appliance - 1 Windows server for Microsoft SQL Server and Log Database	**Scenario 1:** - 1 TRITON Management Server with Web Security and Data Security modules enabled - 1 Data Security Server - Multiple V-Series appliances - 1 Windows server for Microsoft SQL Server and Log Database 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: - HTTP - HTTPS - FTP - FTP-over-HTTP - Monitoring or blocking of SMTP traffic	- 1 TRITON Management Server with SMTP agent and Web Security and Data Security modules enabled - 1 Protector - 1 V-Series appliance - 1 Windows server for Microsoft SQL Server and Log Database	**Scenario 2:** - 1 TRITON Management Server with Web Security and Data Security modules enabled - 1 Data Security Server - 1 Protector - Multiple V-Series appliances - 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: - SMTP	- 1 TRITON Management Server with Email Security and Data Security modules enabled - 1 V-Series appliance - 1 Windows server for Microsoft SQL Server and Log Database	- 1 TRITON Management Server with Email Security and Data Security modules enabled - 1 Data Security Server - Multiple V-Series appliances - 1 Windows server for Microsoft SQL Server and Log Database 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: - SMTP - Monitoring for: - Web / FTP - IM - User-defined protocols - Destination awareness	- 1 TRITON Management Server with Email Security and Data Security modules enabled - 1 Protector - 1 V-Series appliance - 1 Windows server for Microsoft SQL Server and Log Database	- 1 TRITON Management Server with Email Security and Data Security modules enabled - 1 Data Security Server - 1 Protector - Multiple V-Series appliances - 1 Windows server for Microsoft SQL Server and Log Database

Websense Data Monitor

Topology	Small organization	Large org/Enterprise
- Monitoring for: - Mail - Web / FTP - IM - User-defined protocols - Destination awareness	- 1 Data Security Management Server - 1 protector 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:** - 1 Data Security Management Server - 1 Data Security Server - 1 protector - load balancing with the Data Security server 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: - 1 Data Security Management Server - 1 Data Security Server - 2 protectors - one for each site Organization having multiple geographical locations for monitoring traffic
		Scenario 3: - 1 Data Security Management Server - 2 Data Security Servers - one for each site - 2 protectors - one for each site 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: **Data Protection:** - HTTP and SMTP blocking - Policy enforcement for all channels - Destination policy controls **Data Monitoring:** - Monitoring for: • Mail • Web / FTP • IM - User-defined protocols - Destination awareness	- 1 Data Security Management Server - 1 protector	- 1 Data Security Management Server - X Data Security Servers and Y protectors depending on traffic volume. 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 - Removable media & CD/DVD security - Application controls for copy/paste, print, print screen, file access - Endpoint Web channels (HTTP/ HTTPS) - Endpoint LAN control	- 1 Management Server - Endpoint clients	- 1 Data Security Management Server - 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 • Automated remediation for data at rest	• 1 Data Security Management Server • 1 Data Security Server	• 1 Data Security Management Server • Websense Technical Support will assess the number of Data Security servers with discovery and fingerprinting crawlers needed.

Planning a phased approach

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Phase 1: Monitoring*, page 121 ◆ *Phase 2: Monitoring with notifications*, page 122 ◆ *Phase 3: Policy tuning*, page 123 ◆ *Phase 4: Enforcing*, page 123 ◆ *Phase 5: Discovery*, page 123 ◆ *Phase 6: Endpoint deployments*, page 123

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 Define Product Name Variable 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.)

6 Integrating Data Security with Existing Infrastructure

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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*, page 125
- *Working with Web proxies*, page 130
- *Working with shared drives*, page 144
- *Working with user directory servers*, page 149
- *Working with Exchange servers*, page 151
- *Working with IBM Lotus Domino and Lotus Notes*, page 153

Working with existing email infrastructure

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	**In this topic:**
◆ Data Security, v7.7.x	◆ *Using the SMTP agent*, page 126 ◆ *Using the protector*, page 126

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 *Installing appliance-based Websense solutions*, page 247.

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 413. 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 or names 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.

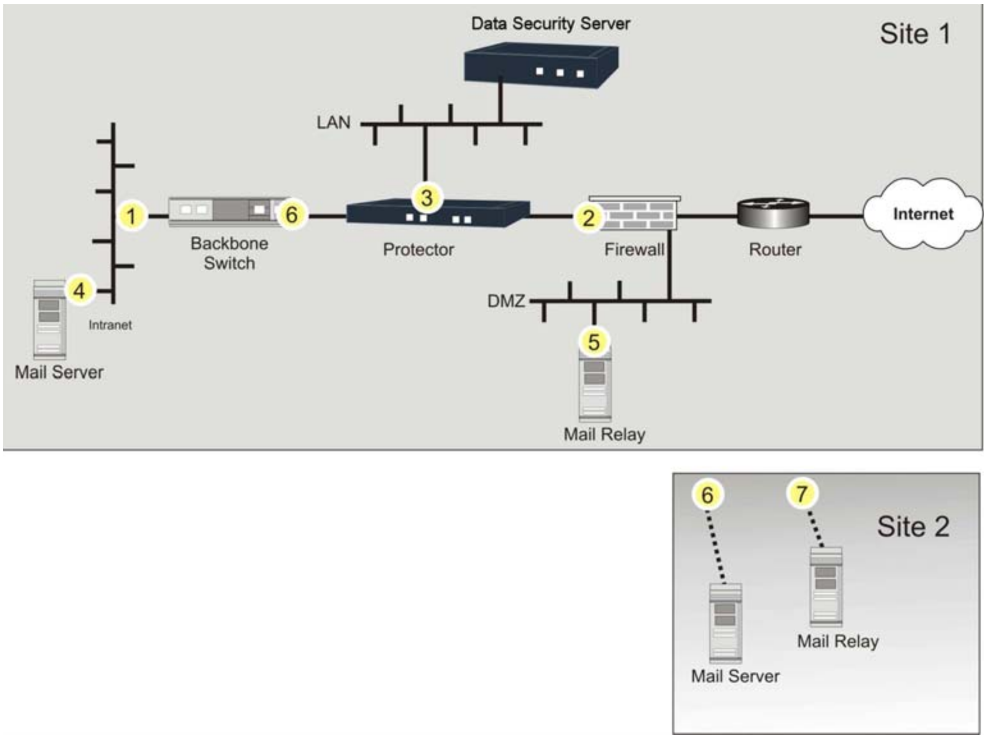
In explicit MTA mode, the protector acts as an MTA for your SMTP traffic and operates in protect mode. Protect mode allows you to block transactions that breach policy.

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 325.

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 413. During installation make sure the time, date and time zone 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 413. 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Blue Coat Web proxy*, page 131 ◆ *Squid open source Web proxy*, page 142 ◆ *ICAP server error and response codes*, page 143

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.

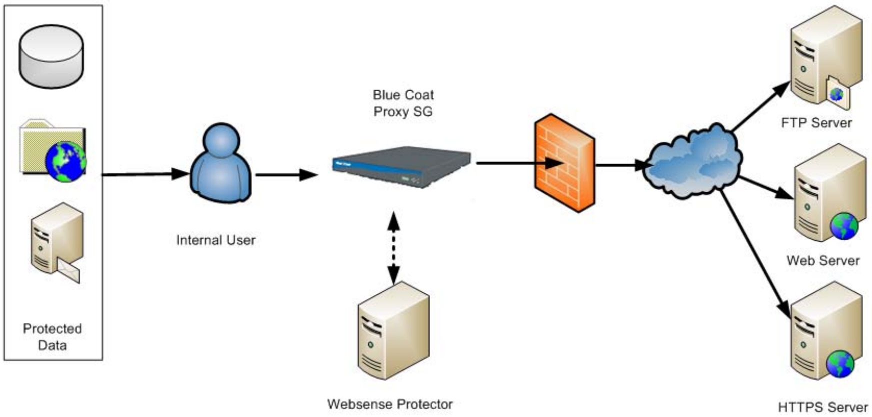
Limitations

- 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:



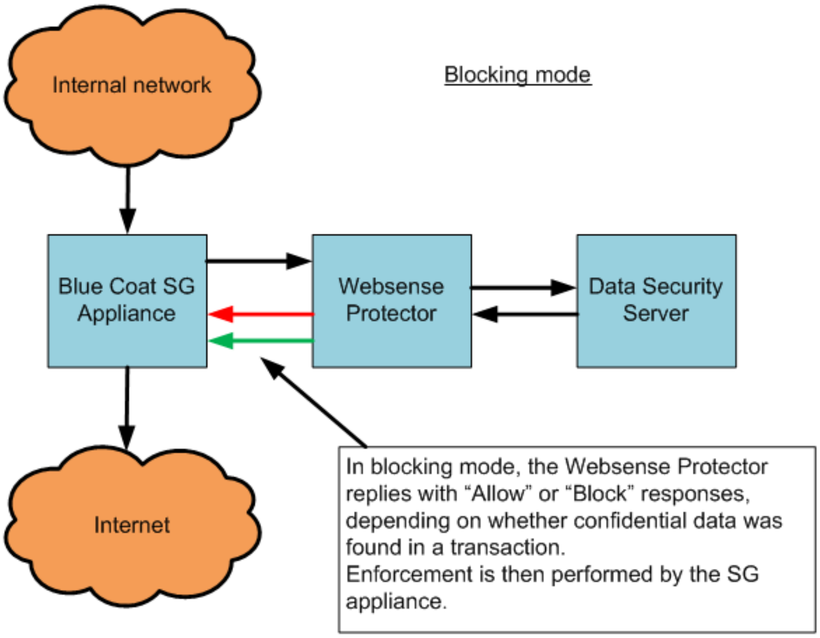
The deployment solution can be used in 2 modes:

- Monitoring mode
- Enforcement mode

You can change the mode as required.

Enforcement mode

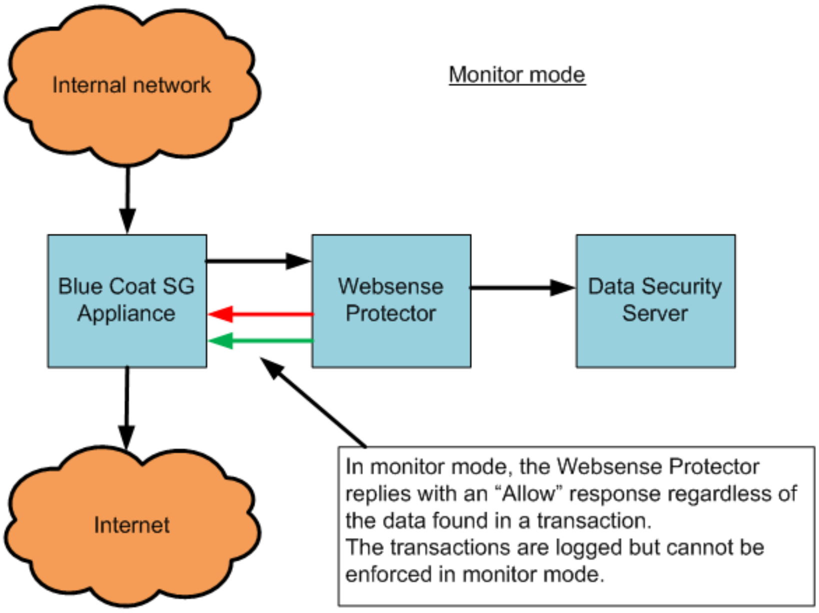
In this mode, the Blue Coat SG appliance requires Websense Data Security to authorize each transaction before allowing the transactions to be posted or uploaded to their intended destination. This is the recommended mode of operation for the solution as it provides the most security.



In blocking mode, the Websense Protector replies with “Allow” or “Block” responses, depending on whether confidential data was found in a transaction.
Enforcement is then performed by the SG appliance.

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.



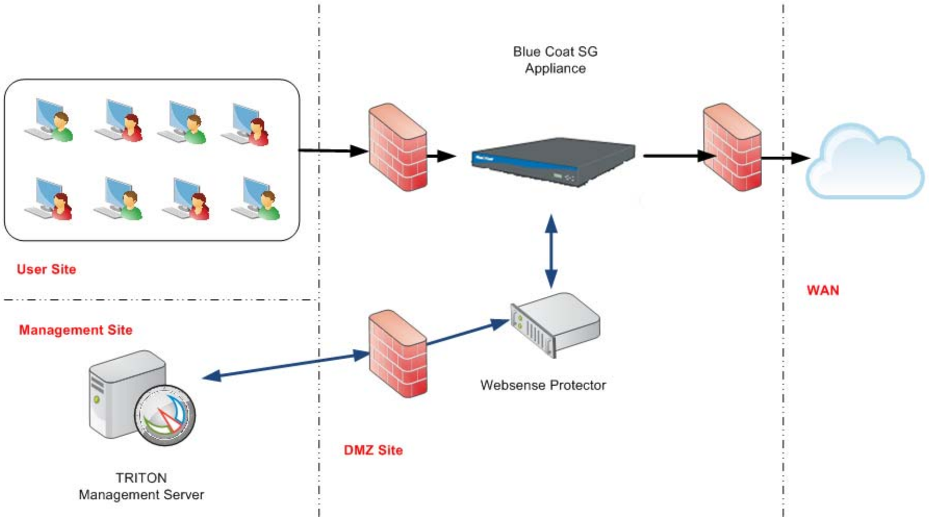
In monitor mode, the Websense Protector replies with an “Allow” response regardless of the data found in a transaction.
The transactions are logged but cannot be enforced in monitor mode.

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 *Installing Data Security Solutions*, page 303, 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

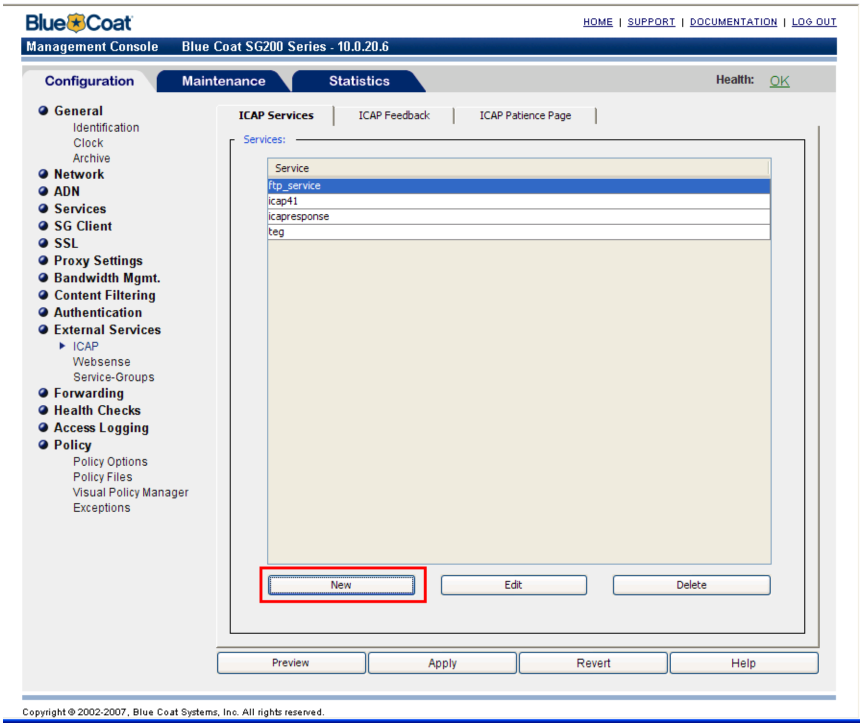
This section describes how to configure the Proxy SG to communicate with the Websense ICAP server on the protector.

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:

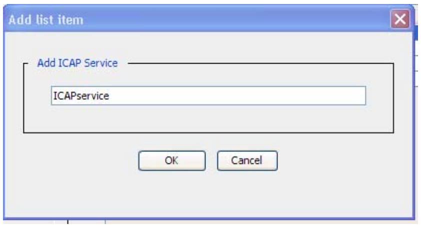
1. Select **Configuration > External Services > ICAP**.
2. To add a new service:

a. Click **New**.



The Add list item window appears.

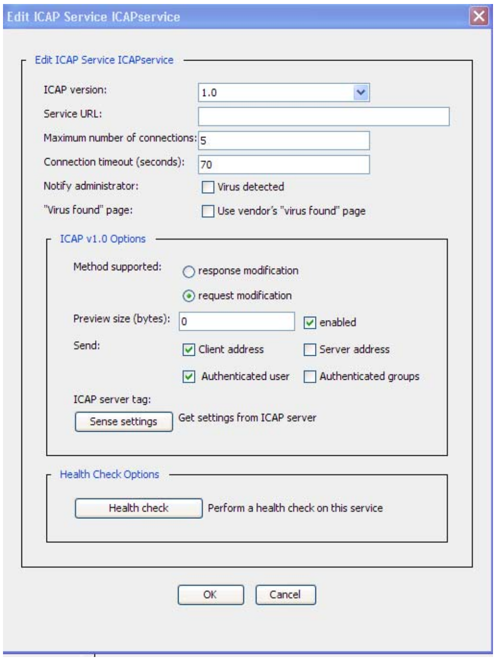
b. In the **Add ICAP Service** field, enter an alphanumeric name.



ICAPservice

c. Click **OK**.

3. In the **Services** list, select the new ICAP service name and click **Edit**. The following screen appears:



Edit ICAP Service ICAPservice

Edit ICAP Service ICAPservice

ICAP version: 1.0

Service URL:

Maximum number of connections: 5

Connection timeout (seconds): 70

Notify administrator: □ Virus detected

"Virus found" page: □ Use vendor's "virus found" page

ICAP v1.0 Options

Method supported: ○ response modification ● request modification

Preview size (bytes): 0 ☑ enabled

Send: ☑ Client address □ Server address ☑ Authenticated user □ Authenticated groups

ICAP server tag:

Sense settings Get settings from ICAP server

Health Check Options

Health check Perform a health check on this service

OK Cancel

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. 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

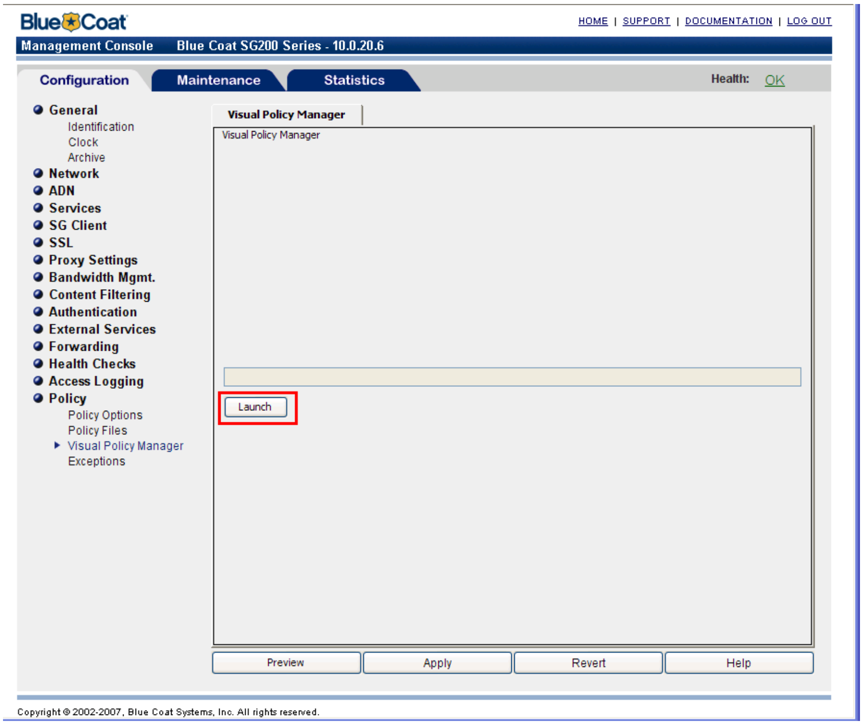
This section describes how to configure the Proxy SG policy to redirect traffic across the ICAP service.

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.

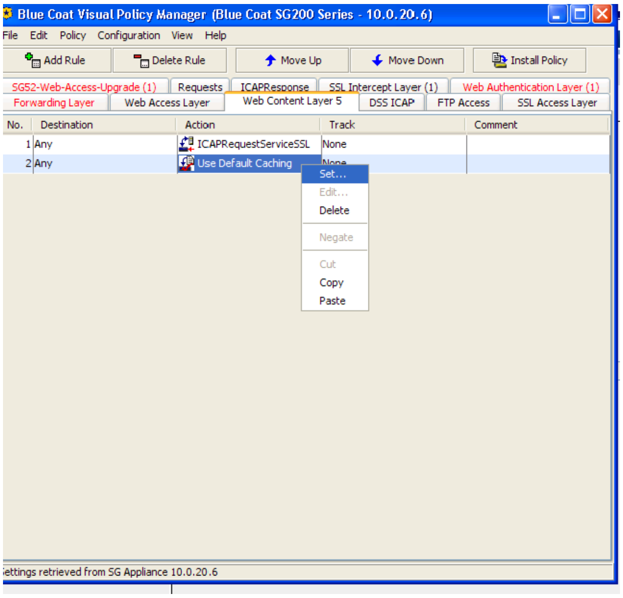
To configure the Proxy SG ICAP policies:

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**.

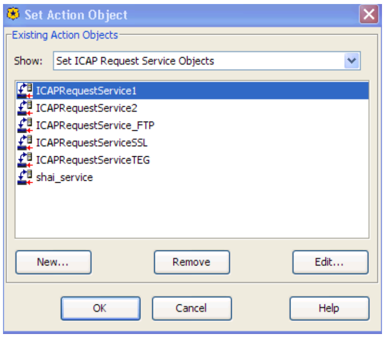
6. Right click the **Action** option and select **Set** from the menu.



No.	Destination	Action	Track	Comment
1	Any	ICAPRequestServiceSSL	None	
2	Any	Use Default Caching	None	

ettings retrieved from SG Appliance 10.0.20.6

7. Under **Show**, select **Set ICAP Request Service Objects**.



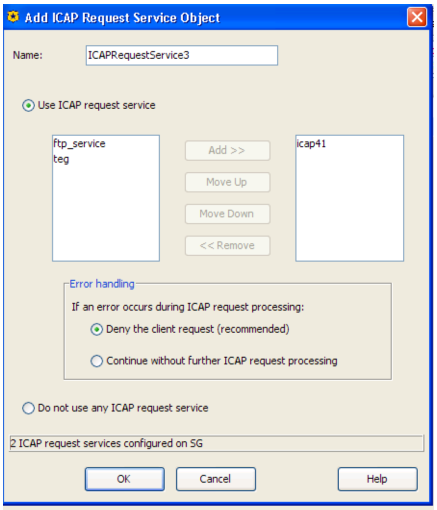
Show: Set ICAP Request Service Objects

ICAPRequestService1
ICAPRequestService2
ICAPRequestService_FTP
ICAPRequestServiceSSL
ICAPRequestServiceTEG
shai_service

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**.



Add ICAP Request Service Object

Name: ICAPRequestService3

● Use ICAP request service

ftp_service
teg

icap41

Error handling

If an error occurs during ICAP request processing:

● Deny the client request (recommended)

○ Continue without further ICAP request processing

○ Do not use any ICAP request service

2 ICAP request services configured on SG

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

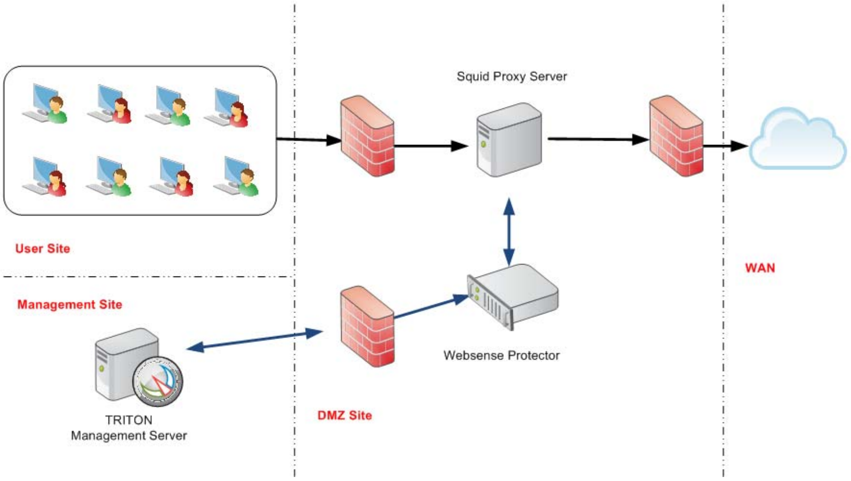
Squid provides protocol support for HTTP, HTTPS, and FTP. It integrates with Websense Data Security over ICAP, which is supported in Squid-3.0 and later.

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 *Installing Data Security Solutions*, page 303, 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

Response Condition	Websense Block Decision	Control Exceeds Size Limit	Error Condition
="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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Performing discovery on Novell file systems*, page 144 ◆ *Performing discovery on Windows NFS shares*, page 146

Discovery is the act of determining where sensitive content is located in your enterprise. If you have shared drives, whether 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 file systems

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.

Preparing the Novell server

1. Create a user account in Novell eDirectory (NDS). This user will be used by the Websense Data Security crawler 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.

Preparing 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 **Add Network Task** > **File System Task**.
    c. On the **Networks** page, click **Edit** to select the Novell server’s IP address.
    d. Click **Advanced**, and add the Novell access port number 524.
    e. On the **Scanned Folders** page, use the Data Security service account for authentication.
    f. Set up all other options as you require.

Performing discovery on Windows NFS shares

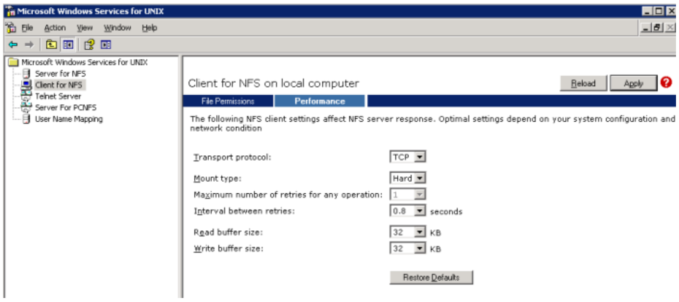
If you want to perform data discovery on Windows file shares, you need to install NFS client on your Data Security server. If you have more than one Data Security server, install NFS client on the one with the crawler you will use to perform discovery.

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.



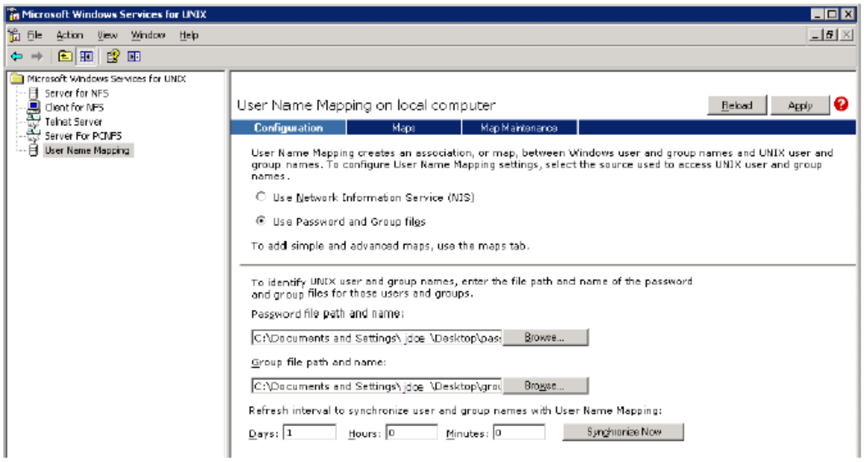
Client for NFS on local computer

The following NFS client settings affect NFS server response. Optimal settings depend on your system configuration and network condition

Transport protocol: TCP
Mount type: Hard
Maximum number of retries for any operation: 1
Interval between retries: 0.8 seconds
Read buffer size: 32 KB
Write buffer size: 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.



User Name Mapping on local computer

User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the source used to access UNIX user and group names.

○ Use Network Information Service (NIS)

● Use Password and Group files

To add simple and advanced maps, use the maps tab.

To identify UNIX user and group names, enter the file path and name of the password and group files for those users and groups.

Password file path and name: C:\Documents and Settings\ jdoe \Desktop\pas

Group file path and name: C:\Documents and Settings\ jdoe \Desktop\grou

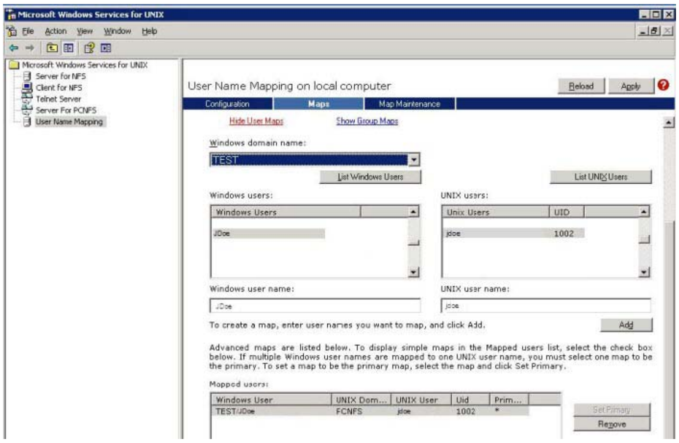
Refresh interval to synchronize user and group names with User Name Mapping:

Days: 1 Hours: 0 Minutes: 0

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.



User Name Mapping on local computer

Windows domain name: TEST

Windows users:

Windows Users
JDoe

UNIX users:

Unix Users	UID
jdoe	1002

Windows user name: JDoe

UNIX user name: jdoe

To create a map, enter user names you want to map, and click Add.

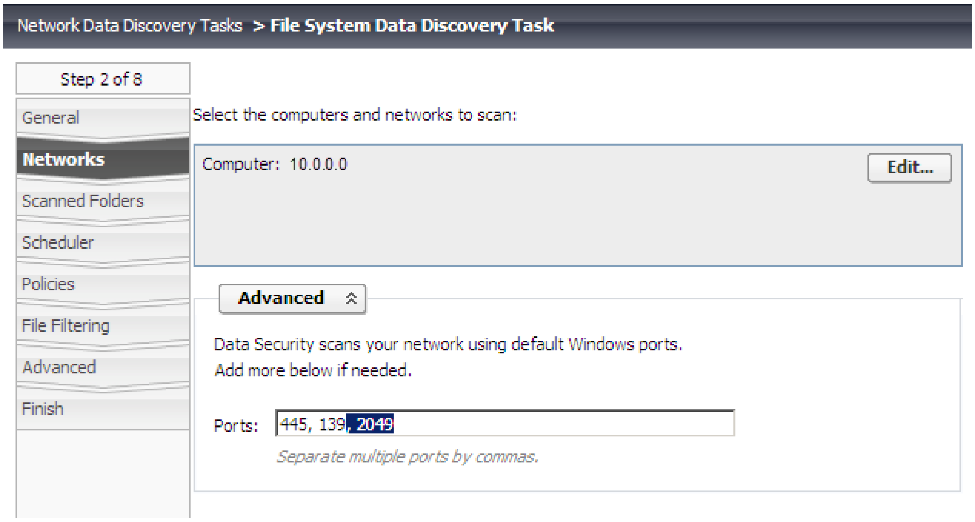
Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
TEST/JDoe	FCNFS	jdoe	1002	*

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.



Network Data Discovery Tasks > File System Data Discovery Task

Step 2 of 8

Select the computers and networks to scan:

Computer: 10.0.0.0

Data Security scans your network using default Windows ports.
Add more below if needed.

Ports: 445, 139, 2049

Separate multiple ports by commas.

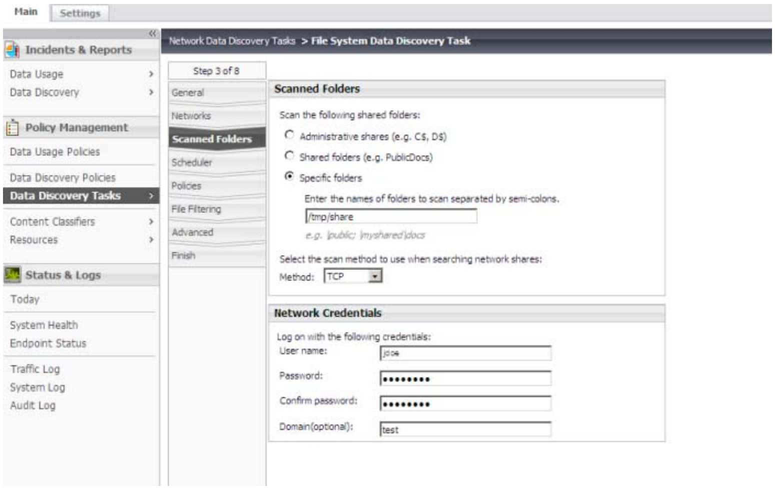
18. On the Scanned Folders screen, specify the shared to be scanned and the user name and password of the Windows user mapped to the UNIX user name.

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: • **Administrative shares** - Select this if you want to scan administrative share drives such as C$. • **Shared folders** - Select this if you want to scan shared folders such as PublicDocs. • **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: • **TCP** - Select TCP if you want to scan the share drives using transmission control protocol. • **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.

Field	Description
Password	Enter a password for this administrator.
Domain	Optionally, enter the domain name of the network.



Network Data Discovery Tasks > File System Data Discovery Task

Scanned Folders

Scan the following shared folders:

○ Administrative shares (e.g. C$, D$)

○ Shared folders (e.g. PublicDocs)

● Specific folders

Enter the names of folders to scan separated by semi-colons.

/tmp/share

e.g. \public; \myshared\docs

Select the scan method to use when searching network shares:

Method: TCP

Network Credentials

Log on with the following credentials:

User name: jdoe

Password: ••••••••

Confirm password: ••••••••

Domain(optional): test

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Configuring user directory server settings*, page 150 ◆ *Importing user data*, page 151 ◆ *Rearranging servers*, page 151

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.
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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

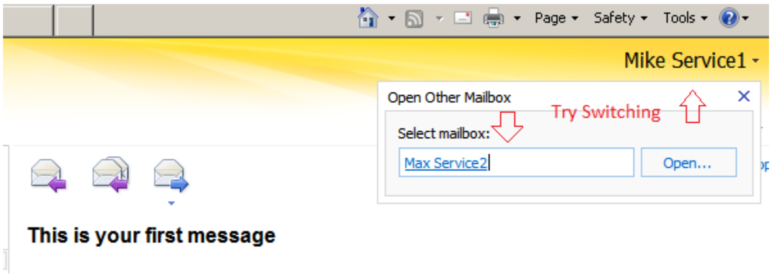
Applies to:	**In this topic:**
◆ Data Security, v7.7.x	

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

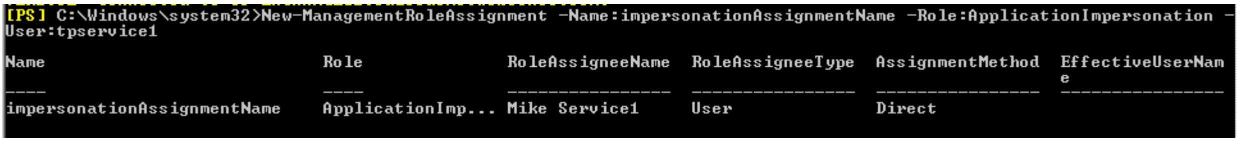
   The service account should now be able to access Exchange via Outlook Web App (OWA) and move between the mailboxes intended to be scanned during the discovery. Try switching between mailboxes as shown below:



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
```



```
[PS] C:\Windows\system32>New-ManagementRoleAssignment -Name:impersonationAssignmentName -Role:ApplicationImpersonation -
User:tpservice1

Name                        Role              RoleAssigneeName  RoleAssigneeType  AssignmentMethod  EffectiveUserNam
                                                                                                    e
----                        ----              ----------------  ----------------  ----------------  ----------------
impersonationAssignmentName ApplicationImp... Mike Service1     User              Direct
```

   For more information on Exchange impersonation, see 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	

With Data Security, you can fingerprint and perform discovery on documents stored in an IBM Lotus Domino Data Management System (DMS). Data Security supports IBM Lotus Domino (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. NSF repositories contain documents and email messages, but Data Security performs discovery only on documents.

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 the TRITON - 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 the TRITON - 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 the TRITON - 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 the TRITON - 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**.

7 Scaling Data Security

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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?

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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.

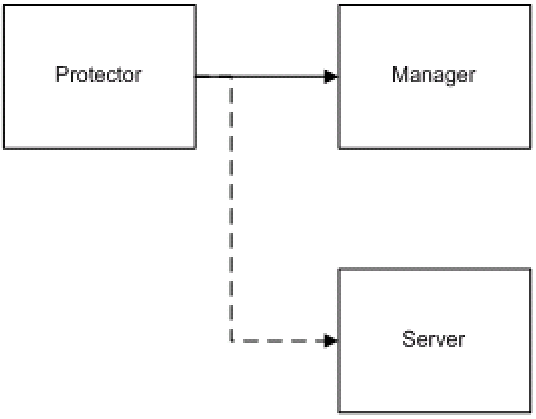
- **The number of transactions grows**

  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.)

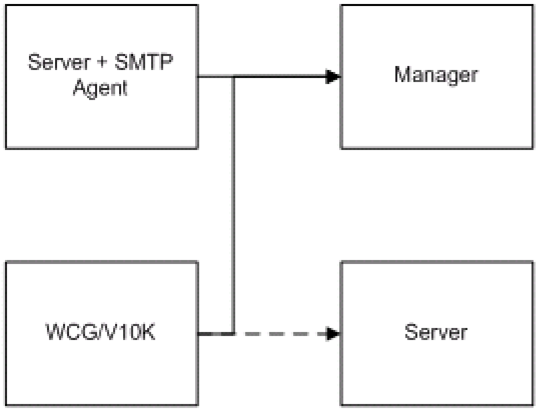
  For more users, add an extra Data Security server and balance the load between the protector and the extra server.



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 112, 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 109.)

  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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

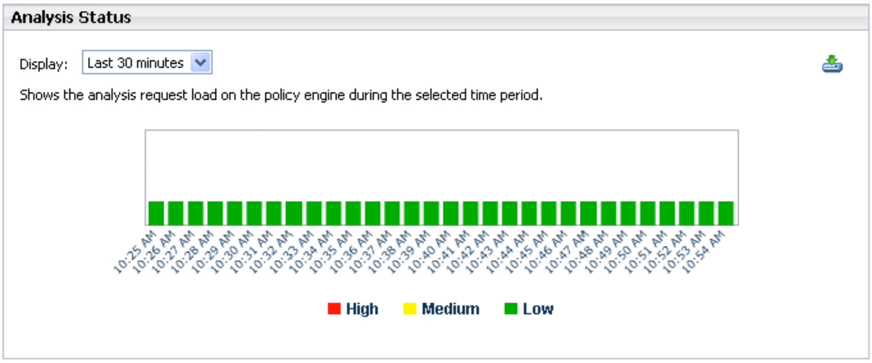
Policy engines analyze transactions sent from various agents and protectors. The protector monitors network traffic and sends transactions to policy engines for analysis. The CPU load on the protector is much lighter than on a policy engine;

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.



Analysis Status

Display: Last 30 minutes

Shows the analysis request load on the policy engine during the selected time period.

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.

8 Email Security Gateway Deployment

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.7.x

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 (TRITON Console).

Each email message is analyzed by a robust set of virus, spam, and URL filters to prevent infected email from entering a network. Custom content filters allow Email Security to analyze messages based on administrator-specified message attribute conditions. Inbound, outbound, and internal email policies can be applied to user-defined sets of senders and recipients.

A Websense Email Security Gateway Anywhere deployment adds support for a hybrid service pre-filtering capability "in the cloud," which analyzes the characteristics of incoming email against a Websense database of known spam and viruses.

Integration with TRITON - Data Security provides valuable data loss prevention (DLP) features to protect an organization's sensitive data. Policies configured in the Data Security module can detect the presence of company data and block the transmission of that data via email. 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. Dashboard status charts (**Main** > **Today** and **Main** > **History**) are based on data collected by the Email Security logging and reporting functions.

A Personal Email Manager facility allows authorized end users to release email messages that Email Security policy has blocked but that may be safe to deliver. End users can maintain personal Always Block and Always Permit lists of email addresses to simplify message delivery. User account management capabilities allow multiple email account control and the delegation of email account management to other individuals.

Email Security Gateway system requirements and deployment options are discussed in the following topics:

- *System requirements*, page 164
- *Single-appliance deployments*, page 166
- *Multiple-appliance deployments*, page 169

The sample diagrams in this guide show V-Series appliances running in Email Security only mode. See the following topics to view diagrams of an appliance running in dual Email Security Gateway/Web Security mode:

- *Web Security and Email Security Gateway (Anywhere)*, page 254
- *Web Security Gateway (Anywhere) and Email Security Gateway (Anywhere)*

See the following topics for Email Security Gateway installation information:

- *Installation steps for appliance-based solutions*, page 263
- *Installing TRITON - Email Security*, page 190

See the following topics for Email Security Gateway product upgrade information:

- *Upgrading Email Security Gateway to v7.7*, page 669
- *Upgrading the TRITON management server*, page 573

System requirements

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.7.x

To view complete hardware, software, and Web browser requirements for TRITON - Email Security, see *System requirements for this version*, page 2,

Every Email Security Gateway deployment includes the following components at a minimum:

In the DMZ

- Websense V-Series appliance (V10000 G2 or V5000 G2), which includes the core Email Security functions and the Personal Email Manager end-user facility

  Email traffic volume in your network may determine which type of appliance you use and how many appliances your deployment needs.

In the internal LAN

- TRITON Unified Security Center management server with both Email Security and Data Security modules installed on a Windows Server® 2008 R2 machine
- Email Security Log Server
- Email Security Log Database (Microsoft® SQL Server® 2008, 2008 R2, or 2008 Express R2)
- Mail exchange server
- End-user machines

✓ **Note**

All Email Security Gateway components must be synchronized by date and time for proper system communication.

The network DMZ 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.

Websense V-Series appliances

The Websense V10000 G2 appliance provides the majority of Email Security Gateway functions. Incoming email flows from the email hybrid service (if enabled) to the Websense appliance and to the mail server. The Websense appliance also provides the Personal Email Manager facility for end users to manage quarantined email. Email Security Gateway can be installed and deployed on a dual-mode V10000 G2 appliance with either Web Security or Web Security Gateway.

The Websense V5000 G2 appliance also provides the majority of Email Security Gateway functions and includes the Personal Email Manager end-user facility. The V5000 appliance can also be configured in dual mode with Web Security and Email Security Gateway.

TRITON management server

The TRITON management server hosts the TRITON Unified Security Center (TRITON Console). This machine includes TRITON Infrastructure and any installed TRITON Console management modules. In an Email Security Gateway deployment, the TRITON management server includes both the Email Security Gateway and Data Security modules.

Email Security Log Server

The TRITON management server often includes the Email Security Log Server component. The log server passes information to the SQL Server reporting database (Email Security Log Database) for use in generating dashboard charts and reports.

During installation, a user configures certain aspects of log server operation, including how log server interacts with Email Security Gateway. These settings can be changed when needed via the Email Security Log Server Configuration utility. Other details about log server operation are configured in this utility as well. The utility is installed on the same machine as log server.

Email Security Log Database (Microsoft SQL Server)

Microsoft SQL Server handles the system and message log database and stores some Email Security configuration settings. SQL Server may be installed on the TRITON management server (SQL Server Express R2 only) or on a dedicated server. For optimal performance, Websense recommends that a full SQL Server (2008 or 2008 R2) be installed on a separate machine. For information about database systems in Websense products, see Administering Websense Databases.

Personal Email Manager

The Email Security appliance is the portal for Personal Email Manager end users who are authorized to manage their own blocked mail. Personal Email Manager end-user options are configured in the Email Security management server interface (**Settings > Personal Email**). A Personal Email Manager administrators can determine:

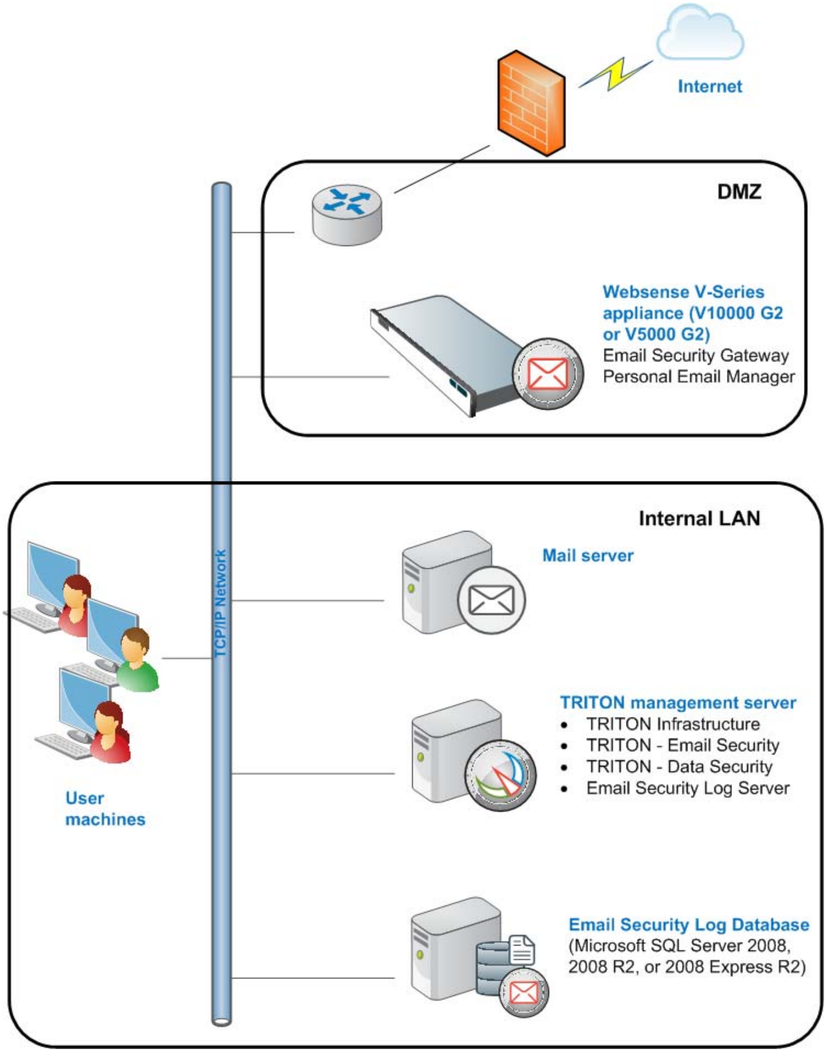
- Which end users can access the Personal Email Manager utility
- What the blocked email notification message contains
- Which end users are allowed to manage personal Always Block and Always Permit lists
- Whether a user can manage multiple email accounts
- Whether a user can delegate email account management responsibilities to another individual (for end users in an LDAP-based user directory, this function can be enabled on the **Add** or **Edit User Directory** page)

Single-appliance deployments

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:	In this topic
- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x	- *Email Security Gateway single appliance*, page 167 - *Email Security Gateway Anywhere single appliance*, page 168

Email Security Gateway single appliance


Internet
DMZ
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway
Personal Email Manager
Internal LAN
TCP/IP Network
Mail server
User machines
TRITON management server
• TRITON Infrastructure
• TRITON - Email Security
• TRITON - Data Security
• Email Security Log Server
Email Security Log Database
(Microsoft SQL Server 2008, 2008 R2, or 2008 Express R2)

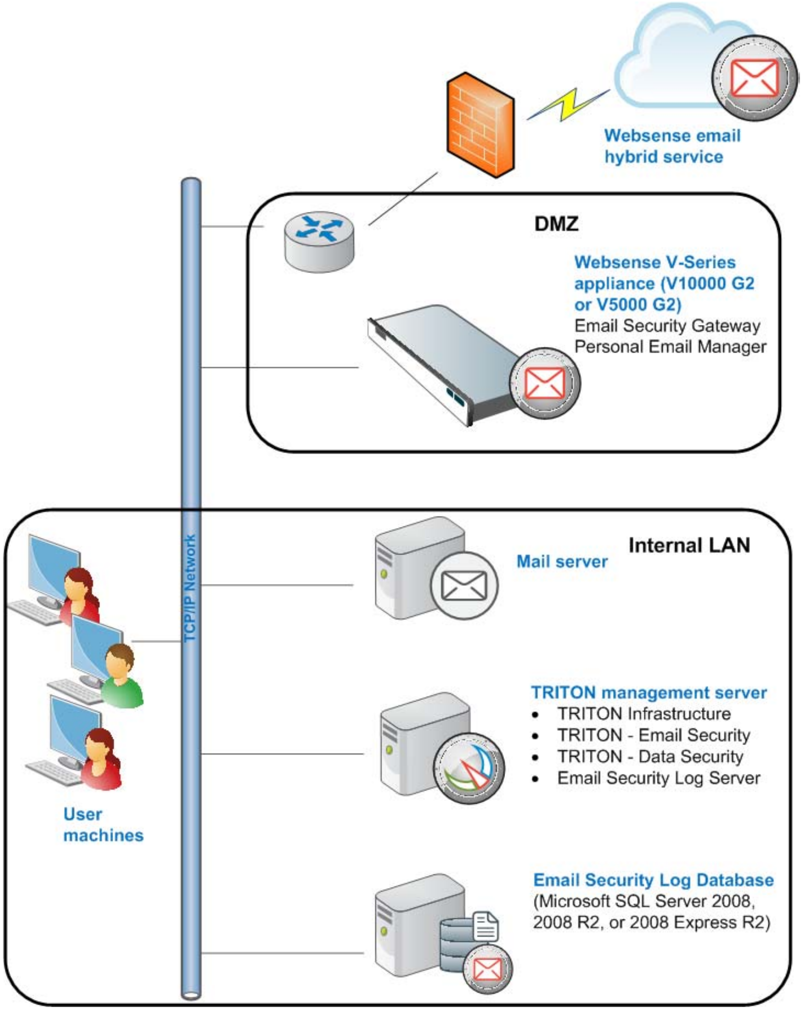
A simple Email Security Gateway deployment uses a single V-Series appliance (either a V10000 G2 or V5000 G2 machine). In this installation, all email analysis occurs in the Email Security Gateway on-premises component using a robust collection of spam, virus, and URL filtering tools (**Main** > **Policy Management** > **Filters**). The Personal Email Manager facility on the appliance allows end users to manage blocked messages.

Data Security data loss prevention (DLP) policies analyze email to ensure acceptable usage policies are enforced and sensitive company data is not lost. DLP policies are enabled in the Email Security module (**Main** > **Policy Management** > **Policies**) but are configured in the Data Security module.

See the *TRITON - Data Security Help* for details about DLP policy settings. See the following *TRITON - Email Security Help* topics for information about Email Security filter and policy tools:

- Creating and configuring email filters
- Creating and configuring email policies

Email Security Gateway Anywhere single appliance


Websense email hybrid service
DMZ
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway
Personal Email Manager
TCP/IP Network
Internal LAN
Mail server
User machines
TRITON management server
• TRITON Infrastructure
• TRITON - Email Security
• TRITON - Data Security
• Email Security Log Server
Email Security Log Database
(Microsoft SQL Server 2008, 2008 R2, or 2008 Express R2)

A simple Email Security Gateway Anywhere deployment uses a single V-Series appliance (either a V10000 G2 or V5000 G2 machine). Websense Email Security Gateway Anywhere offers a comprehensive email security solution that combines the on-premises functions described earlier with hybrid (in-the-cloud) email analysis to manage an organization’s email traffic.

The hybrid service provides an extra layer of email analysis, stopping spam, virus, phishing, and other malware before they reach the network, potentially reducing email bandwidth and storage requirements. The hybrid service can be used to send outbound email to an encryption server before delivery to its recipient.

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
- Comparing the characteristics of inbound email against a Websense database of known spam and viruses, and blocking 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. This function can enhance Email Security system performance.

The Email Security Gateway Anywhere subscription must include the email hybrid service, and the hybrid service must be enabled and properly registered before hybrid service analysis can begin. Register for the hybrid service in the Email Security Gateway management interface (**Settings** > **Hybrid Service** > **Hybrid Configuration**).

The Hybrid Service Log contains records of the email messages that are blocked by the hybrid service. After the hybrid service is registered and enabled, users can view the log at **Main** > **Status** > **Logs** by clicking the Hybrid Service tab.

See the *TRITON* - *Email Security Help* for details on all hybrid service options:

- Registering the email hybrid service
- Configuring the Hybrid Service Log
- Viewing the Hybrid Service Log

Multiple-appliance deployments

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:	**In this topic**
- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x	- *Email Security Gateway Anywhere appliance cluster*, page 170 - *Multiple standalone appliances*, page 172

Multiple V-Series appliance deployments can be implemented when message volume warrants having greater processing capacity. When the deployed appliances are all in standalone mode, the appliances can be a mix of either V10000 G2 or V5000 G2 machines. In an appliance cluster, however, all the machines must be either V10000 G2 or V5000 G2 machines. A cluster cannot contain a mix of appliance platforms.

Email Security Gateway Anywhere appliance cluster

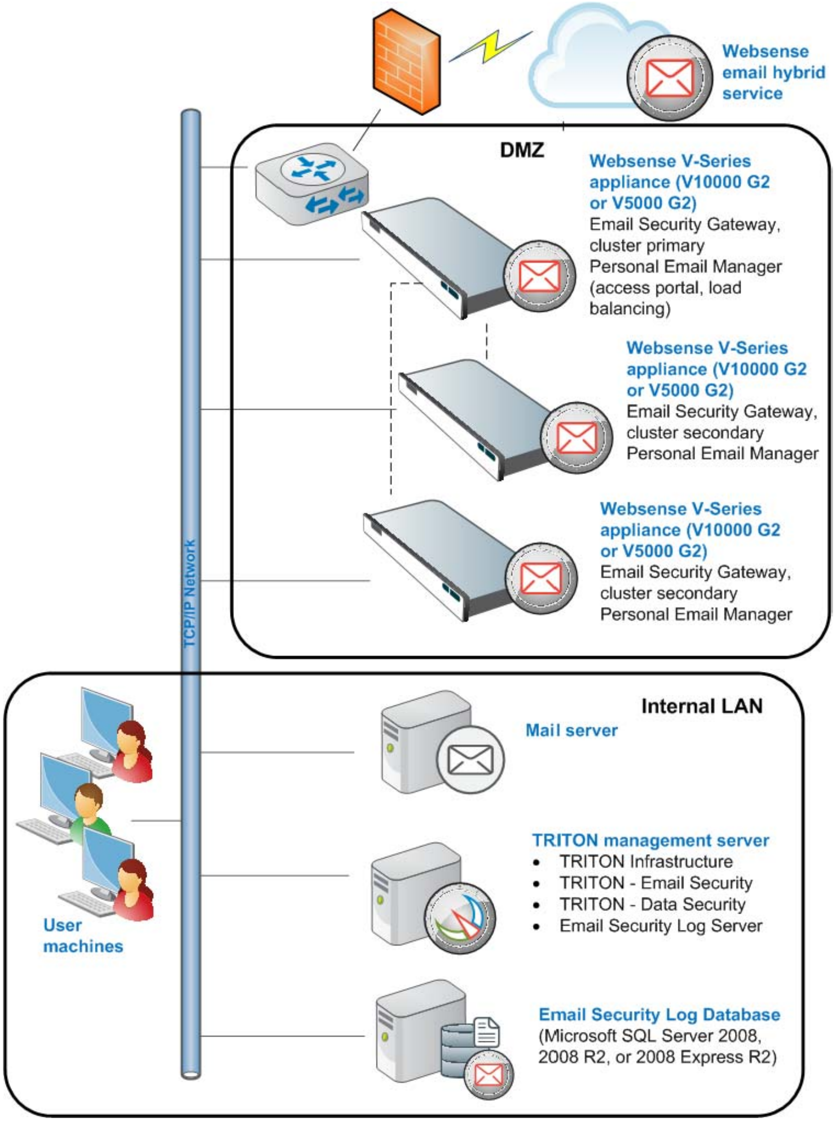
Multiple V-Series appliances are configured in Email Security Gateway as a cluster for this deployment scenario. Appliances in a cluster must all be either V10000 G2 machines or V5000 G2 machines. A cluster cannot contain a mix of different appliance platforms.

This Email Security Gateway Anywhere environment includes the Email Security hybrid service "in the cloud" filtering. See *Email Security Gateway Anywhere single appliance*, page 168, for information about the email hybrid service.

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.

Personal Email Manager traffic load balancing may be accomplished via cluster configuration. After a cluster is created, designate the Personal Email Manager access point in **Settings > Personal Email > Notification Message**, in the Personal Email Manager Portal section. Personal Email Manager traffic is routed to this designated IP address. This appliance then passes the traffic on to other appliances in the cluster via the round robin forwarding mechanism.

To create a cluster, add an appliance to the Email Security appliances list on the **Settings > General > Email Appliances** page, then configure these appliances in a cluster on the **Settings** > **General** > **Cluster Mode** page. See the TRITON - Email Security Help for details.


Websense email hybrid service
DMZ
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway, cluster primary
Personal Email Manager (access portal, load balancing)
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway, cluster secondary
Personal Email Manager
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway, cluster secondary
Personal Email Manager
TCP/IP Network
Internal LAN
Mail server
User machines
TRITON management server
TRITON Infrastructure
TRITON - Email Security
TRITON - Data Security
Email Security Log Server
Email Security Log Database
(Microsoft SQL Server 2008, 2008 R2, or 2008 Express R2)

A primary appliance in a cluster may have up to 7 secondary (or 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 security mode (Email Security only mode or dual Email Security/Web Security mode). The Email Security Gateway management server (TRITON Console) and all cluster appliance versions must all match for cluster communication to work properly.

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 before cluster creation.

Multiple standalone appliances

A multiple standalone appliance deployment might be useful if each appliance must have different configuration settings. Two standalone scenarios are described in this section:

- *Using DNS round robin*, page 172
- *Using domain-based routing*, page 173

These Email Security Gateway Anywhere environments include the Email Security hybrid service “in the cloud” filtering. See *Email Security Gateway Anywhere single appliance*, page 168, for information about the email hybrid service.

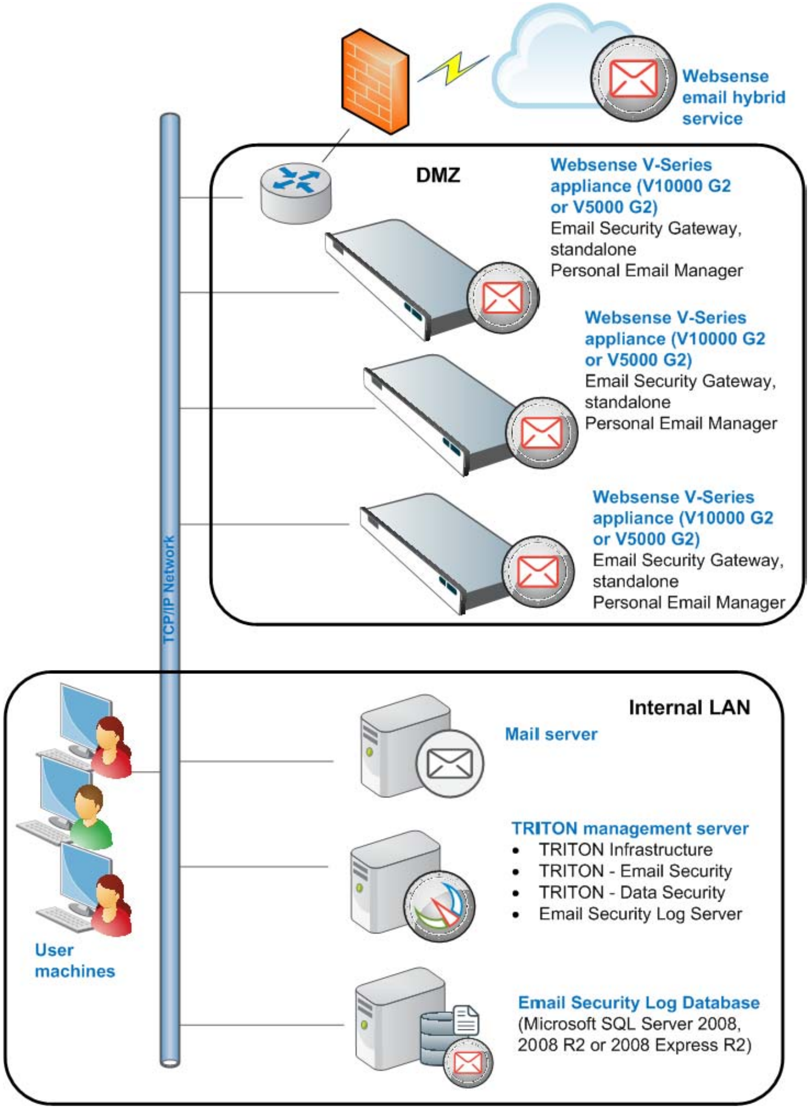
Using DNS round robin

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 > Hybrid Service > 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.


Websense email hybrid service
DMZ
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway, standalone
Personal Email Manager
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway, standalone
Personal Email Manager
Websense V-Series appliance (V10000 G2 or V5000 G2)
Email Security Gateway, standalone
Personal Email Manager
TCP/IP Network
Internal LAN
Mail server
TRITON management server
• TRITON Infrastructure
• TRITON - Email Security
• TRITON - Data Security
• Email Security Log Server
User machines
Email Security Log Database
(Microsoft SQL Server 2008, 2008 R2 or 2008 Express R2)

Using 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** > **Users** > **Domain Groups** > **Add Domain Groups** page. See the *TRITON* - *Email Security Help* for information about adding or editing domain groups:

- Managing domain groups
- Configuring delivery routes

To set up a domain-based delivery route on the **Settings** > **Inbound/Outbound** > **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 **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 selected domain group appears in the Domain details box.

   If you want to add a new domain group to the list, navigate to **Settings** > **Users** > **Domain Groups** and click **Add**.

   If you want to edit your selected domain group, click **Edit** to open the Edit Domain Group page.

Important

The Protected Domain group defined in the **Settings** > **Users** > **Domain Groups** page should not be used to configure Email Security Gateway delivery routes if you need to define domain-based delivery routes via multiple SMTP servers.

Create domain groups that contain subsets of the Protected Domain group for mail routing purposes.

5. Select the **SMTP server IP address** delivery option and enter the following information:
   a. Enter the SMTP server IP address or host name and port.
   b. Mark the check box to enable MX lookup.
   c. 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.

9 Installation Overview: TRITON Enterprise

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.7.x	◆ *Deployment*, page 175 ◆ *Installation*, page 179 ◆ *Initial configuration*, page 180

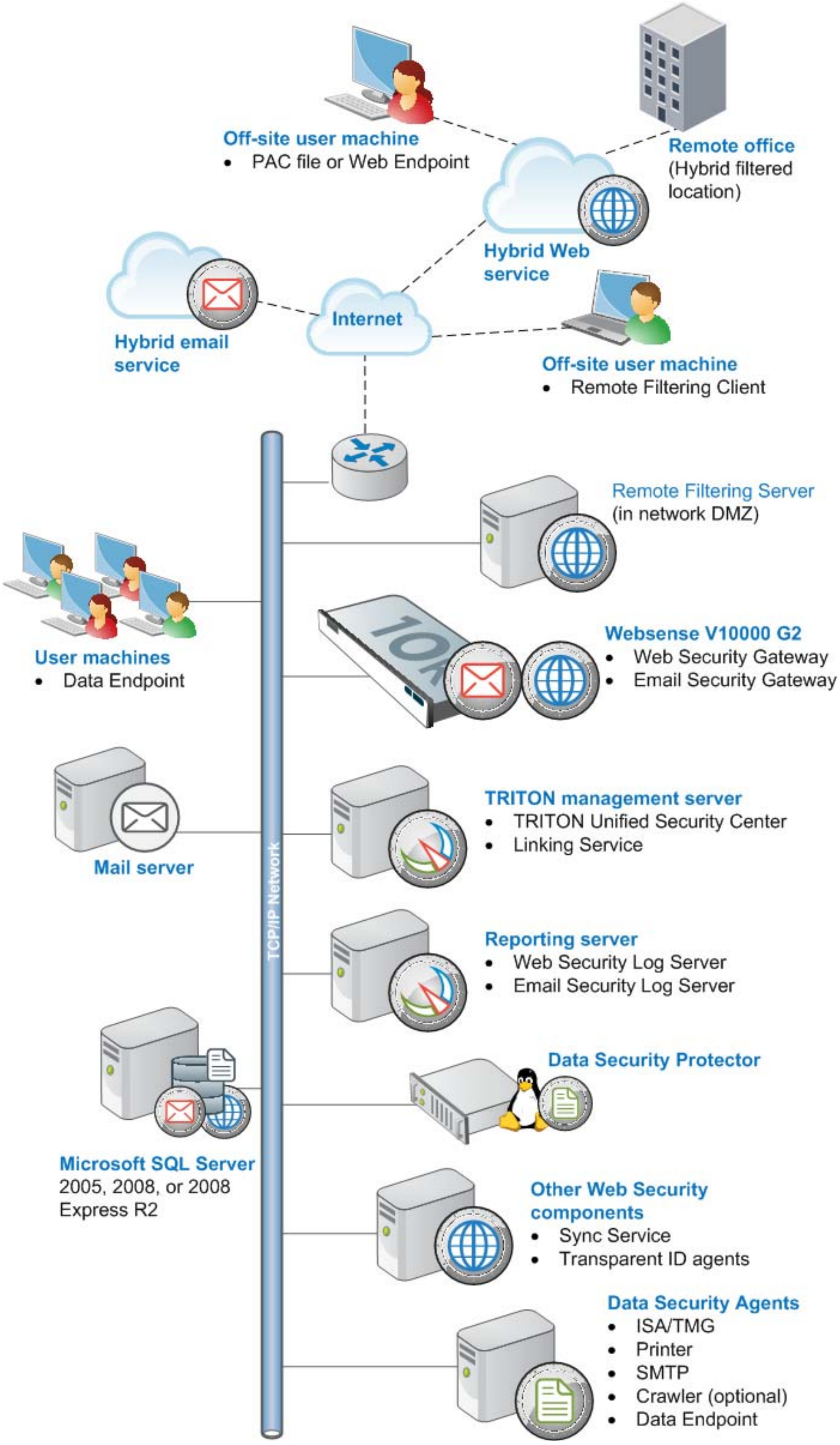
This section provides an overview of TRITON Enterprise deployment and installation activities.

Deployment

Websense TRITON Enterprise includes Web Security Gateway Anywhere, Data Security, and Email Security Gateway Anywhere.

- Core Email Security Gateway Anywhere components can reside only on Websense appliances.
- Web Security Gateway Anywhere may be deployed on Websense appliances, dedicated Windows and Linux servers, or a combination of both.
- Data Security is located on Windows servers and elsewhere in the network.
- The TRITON management interface for Web, Email, and Data Security, resides on a separate Windows server.

The following illustration is a high-level diagram of a basic V10000 G2-based deployment of TRITON Enterprise.



Remote office and off-site users

You can use the hybrid Web service to provide Web security for small remote offices. This is accomplished by designating a remote office as a hybrid filtered location. See *Initial configuration*, page 180, for more information.

Either the hybrid service or Websense remote filtering software can provide Web filtering for off-site users (e.g., telecommuters or traveling personnel).

- To use the hybrid service, a PAC file or 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 remote filtering software, Remote Filtering Server is installed in your network and Remote Filtering Client is installed on user machines. See *Deploying Remote Filtering Server and Client*.

Hybrid services

If your subscription includes Web Security Gateway Anywhere and Email Security Gateway Anywhere:

- The cloud-based (SaaS) hybrid Web service can be used to provide Internet security for remote offices and off-site users.
- The cloud-based email hybrid service provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach your network and possibly reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

Websense Appliances

Websense V-Series appliances may be used to deploy core Web and Email Security Gateway functionality.

- The Content Gateway proxy on the appliance manages Web traffic.
- Incoming email flows from the email hybrid 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.

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.

Components that may not be installed on Websense appliances

TRITON management server

The TRITON management server is the Windows machine on which *TRITON Unified Security Center* (TRITON Console) is installed. The TRITON Console is the management and reporting interface for Websense Web, Data, and Email Security solutions.

Data Security Management Server and, typically, *Crawler* also reside on the TRITON management server machine to providing key Data Security functions, including Web and email DLP (data loss prevention) features.

Linking Service also usually resides on the management server.

Web Security and Email Security Log Server

A separate Windows machine hosts Web Security Log Server and Email Security Log Server. These services receive information about Web Security and Email Security activity and process it into their respective Log Database.

Optional Web Security components

Sync Service and transparent identification agents (*DC Agent*, *Logon Agent*, *eDirectory Agent*, and *RADIUS Agent*) may not reside on V-Series appliances.

Also, you can install additional instances of several Web Security filtering components on Windows or Linux servers, if needed.

Data Security Agents

Microsoft ISA/TMG agent, *Printer agent*, *SMTP agent*, *Crawler*, and *Data Endpoint* are installed on appropriate machines.

See *Installing Data Security Solutions*, page 303 for installation instructions.

Data Endpoint (User Machine)

The *Data Endpoint* can be installed on any machine.

Third-party components

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 messages are also stored here.

When Websense components are installed, SQL Server must be installed and running, typically on its own machine as shown in the diagram above. SQL Server Express (installed using the TRITON Unified Installer) may be used in small deployments or evaluation environments.

Mail server

Your internal mail server.

Deployment details by TRITON Enterprise module

Web Security Gateway Anywhere

- *Web Security Deployment Recommendations*, page 23
- *Deploying Web Security for a distributed enterprise*, page 65

Data Security

- *Planning Data Security Deployment*, page 103
- *Installing TRITON - Data Security*, page 187
- *Installing Data Security Components*, page 315
- *Integrating Data Security with Existing Infrastructure*, page 125
- *Scaling Data Security*, page 157

Email Security Gateway

- *Email Security Gateway Deployment*, page 163

Installation

To install Websense TRITON Enterprise components:

1. Make sure that Microsoft SQL Server is installed and running in your network. See *Obtaining Microsoft SQL Server*, page 21.
2. Install and run the firstboot script on your V-Series appliances. See *Installation steps for appliance-based solutions*, page 263.
3. Install Web and Email Security Log Server. See:
   - *Installing Web Security components*, page 392

     If you plan to enable hybrid Web Security, note that *Sync Service* is typically installed with Web Security Log Server.
   - *Installing Email Security components*, page 414
4. Install TRITON management and core Data Security components on a Windows Server 2008 R2 machine. See *Creating a TRITON Management Server*, page 180.

   On the **Installation Type** screen, select all three modules (**Web Security**, **Data Security**, and **Email Security**) under TRITON Unified Security Center.

5. Install additional components (such as Web Security transparent identification agents or Data Security agents) as needed. See:
   - *Installing Web Security components*, page 392
   - *Installing Data Security components*, page 413
   - *Installing Email Security components*, page 414

Initial configuration

General

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675

Web Security Gateway Anywhere

- *Web Security initial configuration*, page 677
- *Additional configuration for Web Security Gateway Anywhere*, page 679
- *Content Gateway initial configuration*, page 684

Data Security

- *Data Security initial configuration*, page 682

Email Security

- *Email Security Gateway Deployment*, page 163

Creating a TRITON Management Server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway (Anywhere), v7.7.x	◆ *Installing TRITON Unified Security Center*, page 181

The TRITON management server is the machine that hosts the TRITON Unified Security Center, the management and reporting console for Websense Web Security, Data Security, and Email Security solutions.

- *Installing TRITON Unified Security Center*, page 181
- *Installing TRITON - Web Security*, page 185
- *Installing TRITON - Data Security*, page 187
- *Installing TRITON - Email Security*, page 190

Additional, optional components can also run on the machine.

The TRITON management server is “created” by installing these components on a suitable machine (see *System requirements for this version*, page 2).

Important

To enable more than one TRITON module (Web Security, Data Security, Email Security), the TRITON Console must be installed on Windows Server 2008 R2. Because TRITON - Email Security requires TRITON - Data Security, it must always be installed on Windows Server 2008 R2.

Typically, there is only one TRITON management server in a deployment. It serves as the central point for management, configuration, and reporting.

Before you being the installation process, review the information in *Preparing for installation*, page 14. Perform any necessary preparation steps, e.g., disabling firewall and antivirus software.

Installing TRITON Unified Security Center

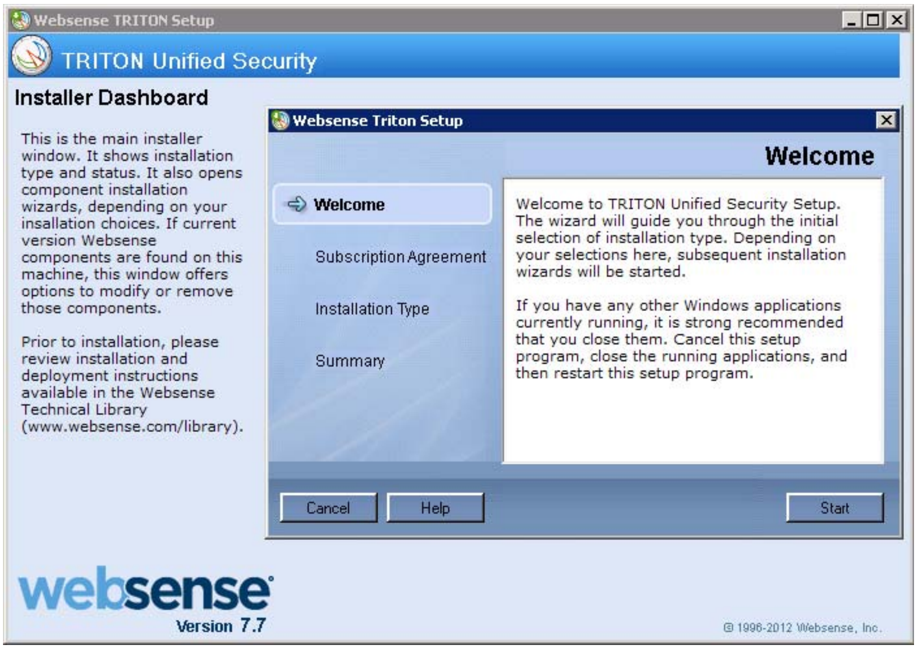
1. Download or copy the TRITON unified installer (the Windows installer) to this machine.

   See *Preparing for installation*, page 14.

2. Double-click the downloaded installer to launch the Websense TRITON Setup program.

   A progress dialog box appears, as files are extracted.

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



This is the main installer window. It shows installation type and status. It also opens component installation wizards, depending on your insallation choices. If current version Websense components are found on this machine, this window offers options to modify or remove those components.

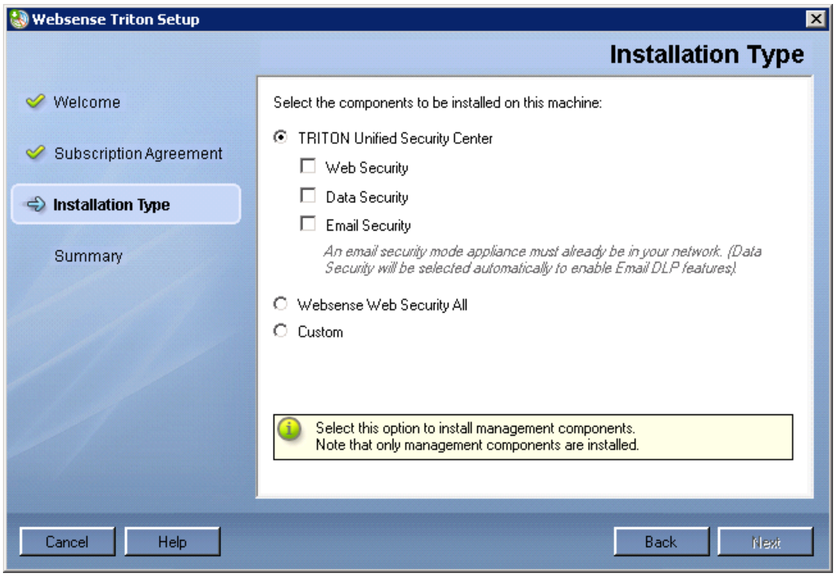
Prior to installation, please review installation and deployment instructions available in the Websense Technical Library (www.websense.com/library).

Welcome to TRITON Unified Security Setup. The wizard will guide you through the initial selection of installation type. Depending on your selections here, subsequent installation wizards will be started.

If you have any other Windows applications currently running, it is strong recommended that you close them. Cancel this setup program, close the running applications, and then restart this setup program.

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).



Select the components to be installed on this machine:

● TRITON Unified Security Center

□ Web Security

□ Data Security

□ Email Security

An email security mode appliance must already be in your network. (Data Security will be selected automatically to enable Email DLP features)

○ Websense Web Security All

○ Custom

Select this option to install management components.
Note that only management components are installed.

Note

The TRITON Unified Security Center modules are management consoles. Selecting them does not install other security or filtering components. 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, Web Security, and 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 Anywhere and Email Security Gateway, install all 3 modules.			

Important

To install the Web Security module of the TRITON Unified Security Center, Policy Broker and Policy Server must be already installed and running (see *Installing components via the Custom option*, page 383). You will need to provide the Policy Server IP address during TRITON - Web Security installation.

In a Websense-appliance-based deployment, Policy Broker and Policy Server run on the **full policy source** appliance.

When you select **Email Security**, **Data Security** is also selected. The Data Security module is required for email DLP (data loss prevention) features, included with Email Security Gateway (Anywhere).

Important

To install the Email Security module of the TRITON Unified Security Center, an Email Security Gateway appliance must already be running. You will need to provide the appliance C interface IP address during TRITON - Email Security installation.

The appliance E1 (and E2, if used) interface must also be configured in the Appliance Manager before the 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*, page 386.

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 component installers launch in the order shown here.

   - *Installing TRITON - Web Security*
   - *Installing TRITON - Data Security*
   - *Installing TRITON - Email Security*

Installing TRITON - Web Security

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x
- Data Security, v7.7.x
- Email Security Gateway (Anywhere), v7.7.x

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 392.

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 180.

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* (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* may be installed on the TRITON management server.
- *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 a Web Security solution and Data Security.
- *Real-Time Monitor* is optional. It is typically installed on the TRITON management server, but can be located elsewhere. 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 TRITON - Data Security

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x
- Data Security, v7.7.x
- Email Security Gateway (Anywhere), v7.7.x

Follow these instructions to install Data Security management components on the TRITON management server. This includes:

- A Data Security policy engine
- Primary fingerprint repository
- Forensics repository
- Endpoint 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 180.
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 install only 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. 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.

   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. Make sure the account used to run SQL has write access to this 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 7.7.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
```

8. In the **Installation Confirmation** screen, click **Install** to begin installation of Data Security components.
9. 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.
10. The **Installation** progress screen appears. Wait for the installation to complete.
11. When the **Installation Complete** screen appears, click **Finish** to close the Data Security installer.
12. 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.

For information on installing other Data Security components, such as the protector, mobile agent, printer agent, SMTP agent, TMG agent, or endpoint client, see *Installing Data Security Components*, page 315.

Installing TRITON - Email Security

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x
- Data Security, v7.7.x
- Email Security Gateway (Anywhere), v7.7.x

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.

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 180.
2. Once the Email Security Installer is launched, the **Introduction** screen appears, click **Next** to begin Email 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 must already be installed and running in your network (see *System requirements for this version*, page 2, for supported versions of SQL Server). 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 install log server on a different machine, deselect the Email Security Log Server option here (in the **Select Components** screen) and complete Email Security installation. Then run TRITON Unified Security Setup on the machine on which you want to install Email Security Log Server. Perform a custom installation of Email Security components (see *Installing Email Security components*, page 414).

4. On the **Email Security Database** screen, specify the IP address or IP address and instance name (format: IP address\instance) for the Email Security database.

   You may specify whether the connection to the database should be encrypted.

   Please note the following issues associated with using this encryption feature:

   - You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.
   - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
   - The connection from the Email Security module on the TRITON Console to the V-Series appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.

   Designate the login type for the database, either Windows authentication or **sa** account.

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. 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. However, 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 **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 product installation).
- Firewall is blocking communication to the appliance on port 6671. Make sure any local firewall allows outbound communication on port 6671.
- Appliance E interface has not been correctly configured in the Appliance Manager.

7. 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.

8. On the **Pre-Installation Summary** screen, review the components to be installed. If they are correct, click **Install**.

   Click **Back** to return to any screen on which you want to modify settings.

9. The **Installing Websense Email Security** screen appears, as components are being installed.
10. Wait until the **Installation Complete** screen appears, and then click **Done**.
11. TRITON Unified Security Setup closes. Installation is complete.

10 Installing Web Security solutions

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

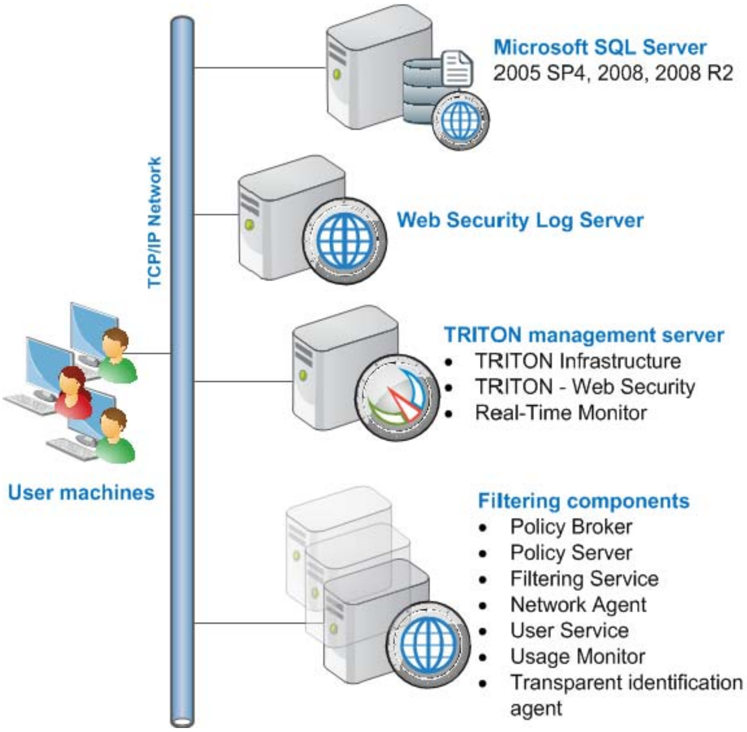
Installation overview: Web Filter and Web Security

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	**In this topic**
◆ Web Filter and Web Security, v7.7.x	◆ *Deployment planning information for Web Filter and Web Security*, page 195 ◆ *Supplemental information for integrated Web Security deployments*, page 195 ◆ *Web Security All installation*, page 195 ◆ *Distributed Web Security installation*, page 195 ◆ *Initial configuration*, page 196

There are 2 main deployment options for Websense Web Filter and Web Security:

1. For evaluation, or for very small (or low traffic) deployments, install all components on one server, using the **Web Security All** installation option.
2. For most production environments, install components distributed across multiple servers, as shown in the high-level illustration below.



Websense Web Security and Web Filter can run in either standalone or integrated mode:

- In standalone mode, Websense Network Agent monitors Internet activity and works with Websense Filtering Service to permit or block requests.
- In integrated mode, a supported third-party proxy, firewall, or caching product communicates with Websense Filtering Service to evaluate whether the Internet requests passing through it should be blocked or permitted.

A Microsoft SQL Server database is used to store Websense reporting data.

- In most deployments, SQL Server Standard or Enterprise must be already installed and running on its own machine.
- For evaluation, or for very small (or low traffic) networks, the Websense installer can be used to install SQL Server 2008 R2 Express. SQL Server Express can run on the TRITON management server, or on its own machine.

The TRITON management server hosts the Web-based management console (the TRITON Unified Security Center), including both infrastructure and TRITON - Web Security components. The TRITON Unified Security Center (TRITON console) is used to configure, manage, and report on your Websense software.

Deployment planning information for Web Filter and Web Security

- *System requirements for this version*, page 2
- *Web Security Deployment Recommendations*, page 23
- *Deploying Web Security for a distributed enterprise*, page 65

Supplemental information for integrated Web Security deployments

- *Integrating Web Security with Check Point*, page 445
- *Integrating Web Security with Cisco*, page 481
- *Integrating Web Security with Citrix*, page 513
- *Integrating Web Security using ICAP Service*, page 557
- *Integrating Web Security with Microsoft Products*, page 535
- *Installing Web Security for Universal Integrations*, page 563

Web Security All installation

An all-in-one Websense Web Security installation may be used for evaluation purposes, or in very small (or low traffic) networks. For most production environments, it is preferable to distribute Web Security components across multiple servers.

To perform a Web Security All installation, see:

1. *Preparing for installation*, page 14
2. *Obtaining Microsoft SQL Server*, page 21
3. *Installing via the Web Security All option*, page 204

Distributed Web Security installation

A standard Websense Web Filter or Web Security installation involves placing components on 3 or more machines.

To perform a standard installation:

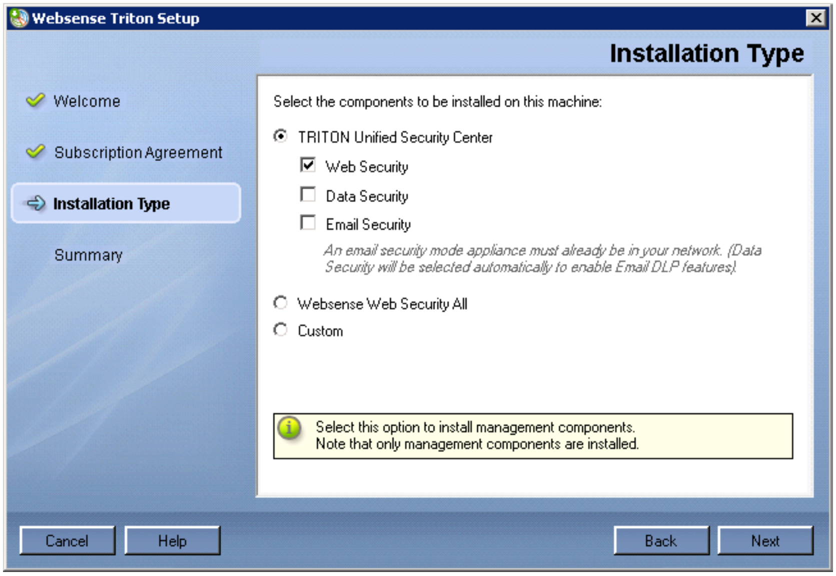
1. Verify that all prerequisites are met (see *Preparing for installation*, page 14).
2. Make sure that Microsoft SQL Server is installed in your network (see *Obtaining Microsoft SQL Server*, page 21).
3. Install filtering components on one or more machines.
   - For Windows, see *Installing Web Security components*, page 392.
   - For Linux, see *Installing Web Security Components on Linux*, page 209.

- For V-Series appliances, see *Installing appliance-based Websense solutions*, page 247.

  Important: Install Policy Broker, Policy Server, and Filtering Service or the full policy source appliance before installing other components.

4. Install Websense Log Server to enable reporting (see *Installing Web Security components*, page 392).
5. Install TRITON management server components (see *Creating a TRITON Management Server*, page 180).

   Important: When you reach the **Installation Type** screen, select only **Web Security** under TRITON Unified Security Center.



Select the components to be installed on this machine:

● TRITON Unified Security Center

☑ Web Security

□ Data Security

□ Email Security

An email security mode appliance must already be in your network. (Data Security will be selected automatically to enable Email DLP features.)

○ Websense Web Security All

○ Custom

Select this option to install management components.
Note that only management components are installed.

Initial configuration

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675
- *Web Security initial configuration*, page 677
- *Using BCP for log record insertion with SQL Server 2008*, page 36

Installation overview: Web Security Gateway

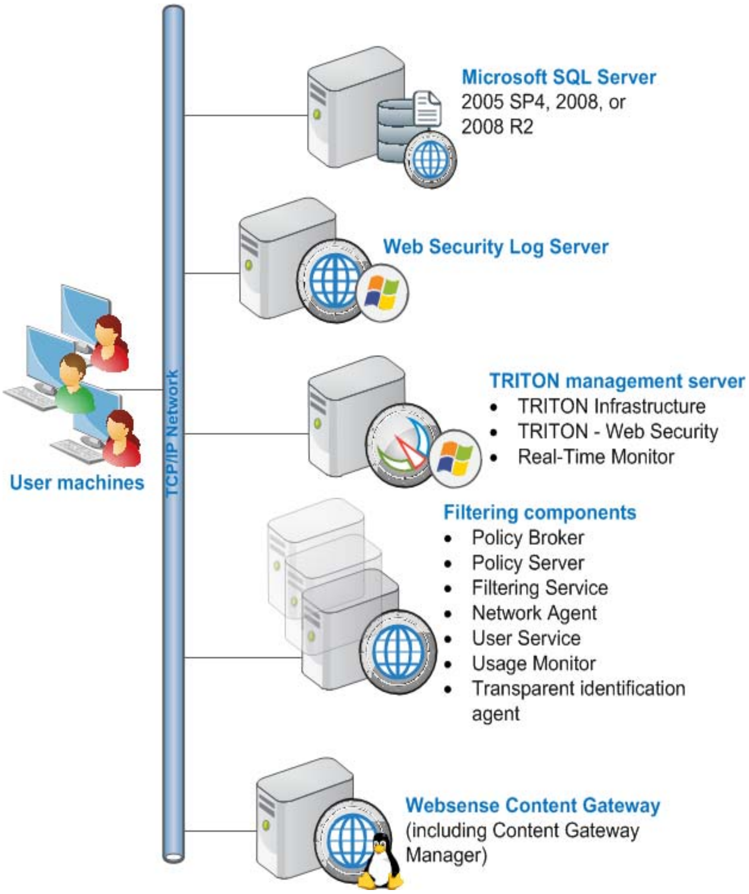
Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway v7.7.x	

This section contains information and about installing Websense Web Security Gateway software components. If your deployment also includes one or more V-Series appliances, additionally refer to *Installing appliance-based Websense solutions*, page 247.

Websense Web Security Gateway is highly-distributable, providing the flexibility to scale a deployment to suit your needs. 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 Web Security Gateway reporting data. When you install Websense Log Server (the main reporting component), SQL Server must be installed and running. (In very small deployments, or for evaluation, SQL Server Express, installed using the Websense installer, may be used.)

The TRITON management server hosts the Web-based management console (the TRITON Unified Security Center), including both infrastructure and TRITON - Web Security components. The TRITON Unified Security Center (TRITON console) is used to configure, manage, and report on your Websense software.

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. It resides on a Linux server or a V-Series appliance. Content Gateway Manager—the management console for Content Gateway—runs on the Content Gateway machine, but can be accessed from the TRITON console.

Deployment

- *Deploying Web Security core components*, page 24
- *Extending your Web Security deployment*, page 31
- *Web Security required external resources*, page 41
- *Maximizing Web Security system performance*, page 42
- *Deploying transparent identification agents*, page 48
- *Hardware recommendations for standalone Web Security deployments*, page 51
- *Deploying Remote Filtering Server and Client*, page 62
- *Deploying Web Security for a distributed enterprise*, page 65

Installation

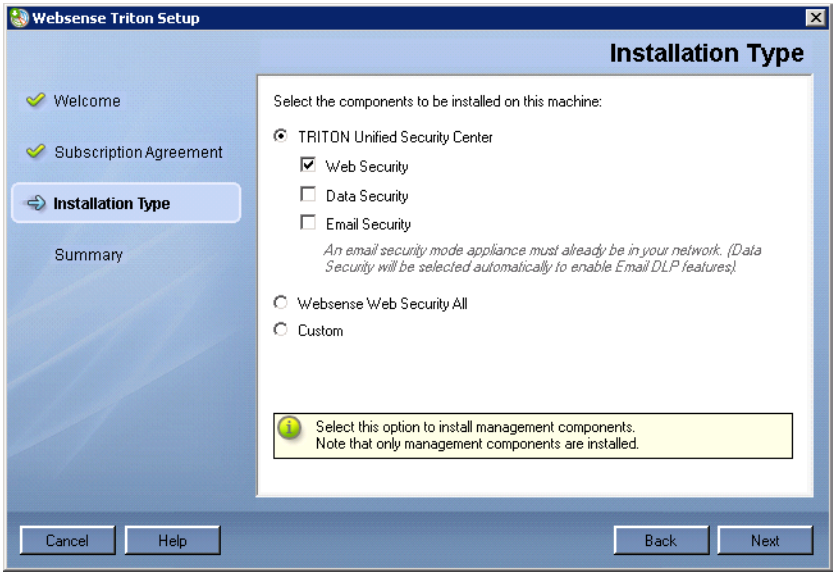
Complete the following main steps (the links go to detailed procedures or information for each step).

1. *Preparing for installation*, page 14
2. *Obtaining Microsoft SQL Server*, page 21
3. Installing filtering components on one or more machines
   - For Windows, see *Installing Web Security components*, page 392.
   - For Linux, see *Installing Web Security Components on Linux*, page 209.
   - For V-Series appliances, see *Installing appliance-based Websense solutions*, page 247.

   Important: Install Policy Broker, Policy Server, and Filtering Service or the full policy source appliance before installing other components.

   During Filtering Service software installation (if applicable), be sure to specify that Filtering Service will be integrated with Websense Content Gateway.
4. *Installing Websense Content Gateway,* page 219
5. *Creating a TRITON Management Server*, page 180

Important: When you reach the **Installation Type** screen, select only **Web Security** under TRITON Unified Security Center.



Select the components to be installed on this machine:

- ● TRITON Unified Security Center
  - ☑ Web Security
  - □ Data Security
  - □ Email Security

  An email security mode appliance must already be in your network. (Data Security will be selected automatically to enable Email DLP features)
- ○ Websense Web Security All
- ○ Custom

Select this option to install management components.
Note that only management components are installed.

Initial configuration

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675
- *Web Security initial configuration*, page 677
- *Using BCP for log record insertion with SQL Server 2008*, page 36
- *Content Gateway initial configuration*, page 684

Installation overview: Web Security Gateway Anywhere

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway Anywhere v7.7.x	◆ *Deployment*, page 203 ◆ *Installation*, page 203 ◆ *Initial configuration*, page 204

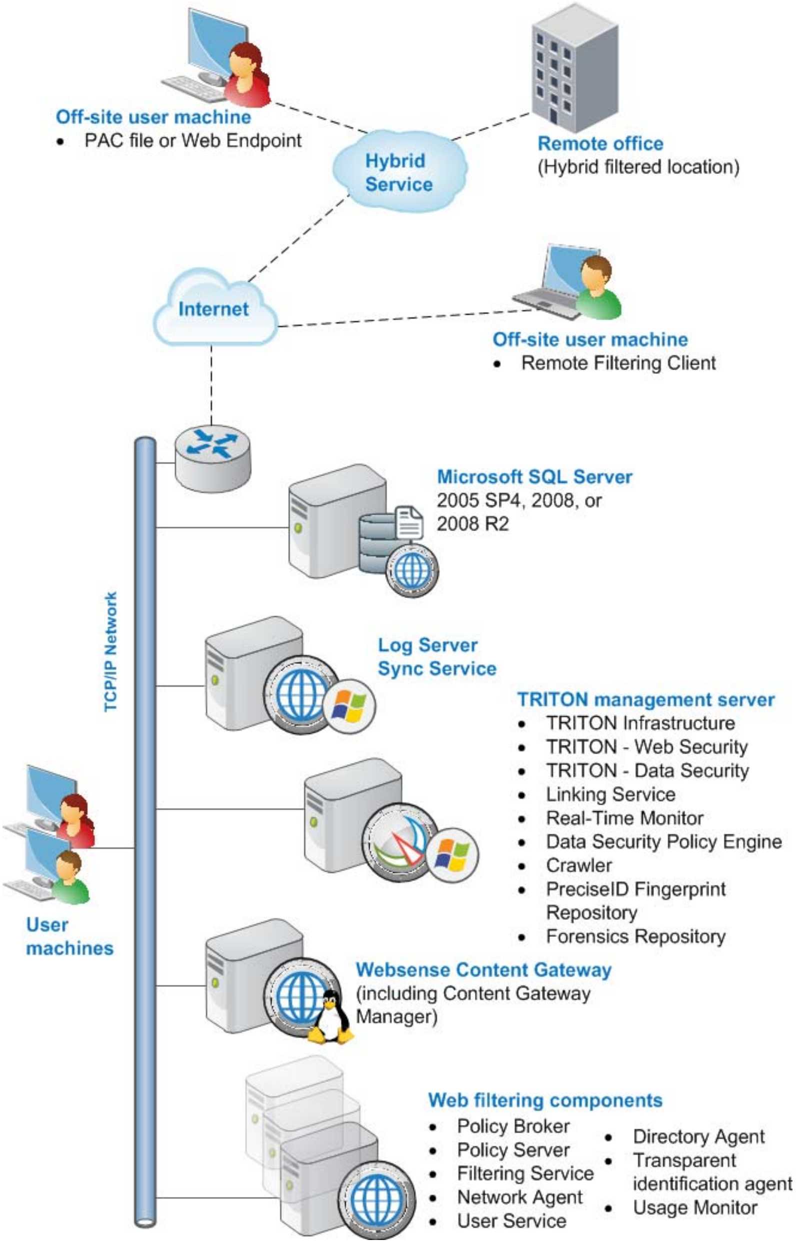
Web Security Gateway Anywhere is a hybrid on-premises and in-the-cloud Web filtering solution. Users inside your corporate network are filtered by on-premises Websense components. Small, remote offices and off-site users can be filtered by Websense hybrid service clusters located across the globe.

In addition, Web Security Gateway Anywhere protects you from data loss over the Web, providing security for outbound content. 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 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.

If your deployment includes one or more V-Series appliances, additionally refer to *Installing appliance-based Websense solutions*, page 247.

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 Web Security and Data Security reporting data. When installing reporting components, SQL Server must be installed and running. (In very small deployments, or for evaluation, SQL Server Express, installed using the Websense installer, may be used.)

The TRITON management server hosts the Web-based management console (the TRITON Unified Security Center), and its Web Security and Data Security modules. It also hosts several additional Data Security components and Linking Service, used to share Web Security category and user information with Data Security.

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. It resides on a Linux server or a V-Series appliance. Content Gateway Manager—the management console for Content Gateway—runs on the Content Gateway machine, but can be accessed from the TRITON console.

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 All Websense Modules*, page 675, for more information.

Off-site users (e.g., telecommuters or traveling personnel) can be filtered using the Websense hybrid service, remote filtering software, or a combination of both solutions.

Deployment

- *System requirements for this version*, page 2
- *Deploying Web Security core components*, page 24
- *Extending your Web Security deployment*, page 31
- *Web Security required external resources*, page 41
- *Deploying transparent identification agents*, page 48
- *Maximizing Web Security system performance*, page 42
- *Deploying Remote Filtering Server and Client*, page 62
- *Deploying Web Security for a distributed enterprise*, page 65

Installation

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

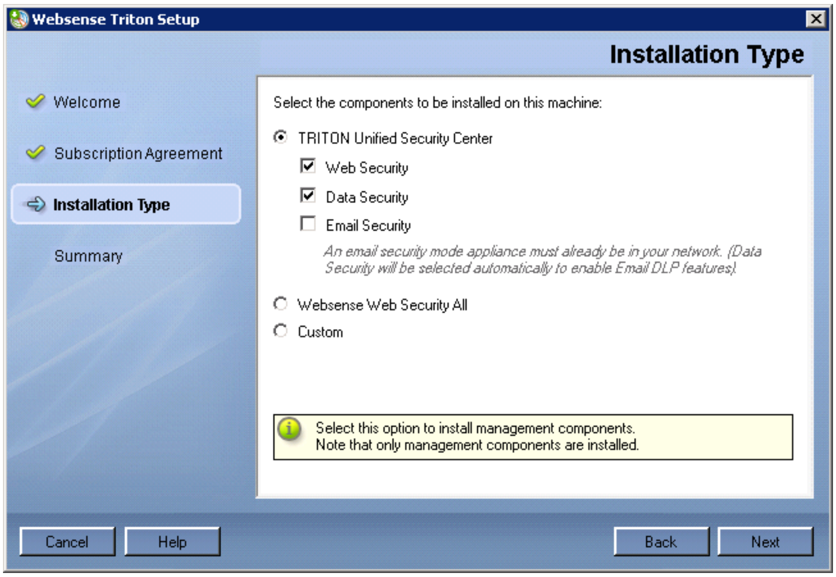
1. *Preparing for installation*, page 14
2. *Obtaining Microsoft SQL Server*, page 21
3. Installing filtering components on one or more machines
   - For Windows, see *Installing Web Security components*, page 392.
   - For Linux, see *Installing Web Security Components on Linux*, page 209.
   - For V-Series appliances, see *Installing appliance-based Websense solutions*, page 247.

   Important: Install Policy Broker, Policy Server, and Filtering Service or the full policy source appliance before installing other components.

   During Filtering Service software installation (if applicable), be sure to specify that Filtering Service will be integrated with Websense Content Gateway.

4. *Installing Websense Content Gateway*, page 231
5. *Creating a TRITON Management Server*, page 180

   Important: When you reach the **Installation Type** screen, select both **Web Security** and **Data Security** under TRITON Unified Security Center.



Installation Type

Select the components to be installed on this machine:

● TRITON Unified Security Center

☑ Web Security

☑ Data Security

□ Email Security

An email security mode appliance must already be in your network. (Data Security will be selected automatically to enable Email DLP features)

○ Websense Web Security All

○ Custom

Select this option to install management components.
Note that only management components are installed.

Initial configuration

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675
- *Web Security initial configuration*, page 677
- *Using BCP for log record insertion with SQL Server 2008*, page 36
- *Content Gateway initial configuration*, page 684
- *Additional configuration for Web Security Gateway Anywhere*, page 679

Installing via the Web Security All option

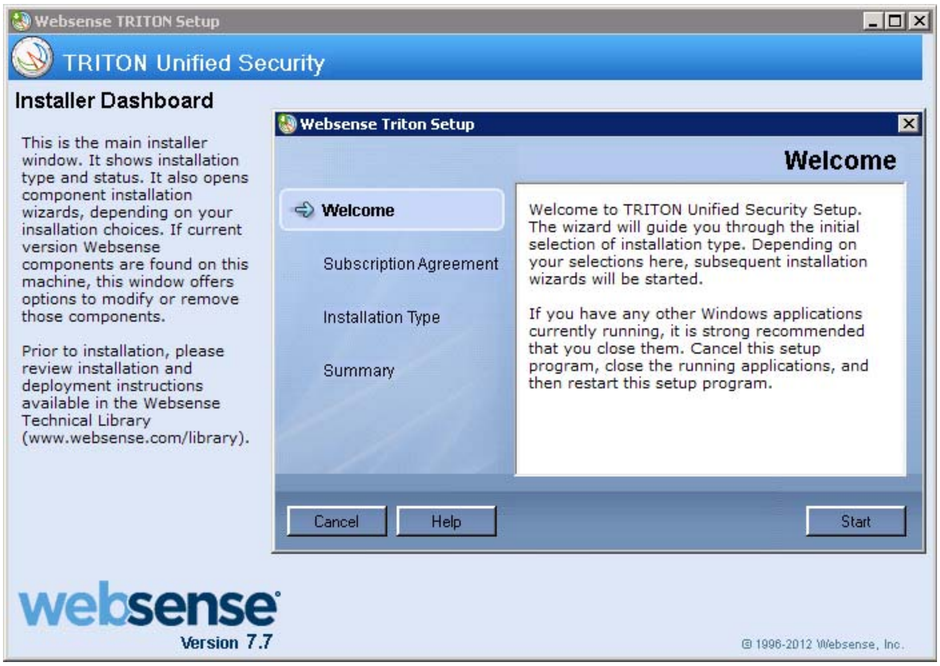
Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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 *Getting the Websense software installers*, page 14).
2. Double-click the downloaded installer to launch the Websense installer. A progress dialog box appears, as files are extracted. Once files have been extracted, there may be a pause of several seconds before the Welcome screen is displayed.
3. On the **Welcome** screen, click **Start**.



This is the main installer window. It shows installation type and status. It also opens component installation wizards, depending on your insallation choices. If current version Websense components are found on this machine, this window offers options to modify or remove those components.

Prior to installation, please review installation and deployment instructions available in the Websense Technical Library (www.websense.com/library).

Welcome to TRITON Unified Security Setup. The wizard will guide you through the initial selection of installation type. Depending on your selections here, subsequent installation wizards will be started.

If you have any other Windows applications currently running, it is strong recommended that you close them. Cancel this setup program, close the running applications, and then restart this setup program.

The Installer Dashboard remains on screen throughout the installation 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*, page 386.
8. When you click **Finish** in TRITON Infrastructure Setup.

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

   See *Active Directory Screen*, page 400, for instructions.
10. If you are using Active Directory, the **Computer Browser** screen may appear.

    See *Computer Browser Screen*, page 400, for instructions.
11. On the **Integration Option** screen, indicate whether to install your Web Security software in standalone or integrated mode.

    See *Integration Option Screen*, page 401, for instructions.

12. If you selected “Integrated with another application or device” in the previous step, on the **Select Integration** screen, select the product you want to integrate with.

    See *Select Integration Screen* for instructions

13. If the **Multiple Network Interfaces** screen appears, select the NIC that Websense components should use to communicate with Websense components on other machines.

    See *Multiple Network Interfaces Screen* for instructions.

14. On the **Network Card Selection** screen, select the network interface card (NIC) that Network Agent should use to monitor Internet activity.

    See *Network Card Selection Screen* for instructions.

15. On the **Log Database Location** screen, specify a location (directory path) for the Websense Log Database.

    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 **Do not install Web Security Gateway Anywhere Components** for Web Security and Web Filter installations.

19. On the **Transparent User Identification** screen, select whether to use Websense transparent identification agents to identify users and then click **Next**.

    Transparent user identification agents allow 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.

    - Select **Use DC Agent to identify users logging on to Windows domains** to install Websense DC Agent on this machine. DC Agent polls domain controllers for information about user logon sessions, and can also poll user machines directly to verify the logged-on user.
    - Select **Use Logon Agent to identify users logging on to local machines** to install Websense Logon Agent on this machine. Logon Agent provides the highest level of user identification accuracy by identifying users as they log on to Windows domains.

Logon Agent works with a logon application that runs via logon script on client machines. For instructions on configuring domain controllers and client machines to use Logon Agent, see the Using Logon Agent for Transparent User Identification technical paper.

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

- Select **Use both DC Agent and Logon Agent** to use both of the agents that work with Windows Active Directory. When both agents are installed, DC Agent information is used as a backup in the unlikely event that Logon Agent is unable to identify a user.
- Select **Use eDirectory Agent to identify users logging on via Novell eDirectory Server** to install Websense eDirectory Agent on this machine. eDirectory Agent queries the Novell 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.

- Select **Do not install a transparent identification agent now** if:
  - Websense software will be integrated with a product that provides user authentication.

> **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.

  - You plan to run the transparent identification agent on one or more other machines.
  - You do not want different filtering policies applied to users or groups.
  - You want all users to be prompted for logon information when they open a browser to access the Internet.

20. On the **Directory Service Access** screen, supply a local and domain administrator account with directory service access permissions.

    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. On the **Installation Complete** screen, click **Done**.

11 Installing Web Security Components on Linux

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Custom installation*, page 210 ◆ *Filtering installation on Linux*, page 210

This section provides instructions for running the Web Security Linux installer to install Websense Web Security components on supported Linux platforms.

Note, however, that the following components can reside only on a Windows machine:

- TRITON Unified Security Center (including the TRITON Infrastructure, TRITON - Web Security, TRITON - Data Security, and TRITON - Email Security modules)

  Note that there is one exception: TRITON - Web Security can run on a V-Series appliance when no other TRITON modules are used.
- Web Security Log Server
- Real-Time Monitor
- DC Agent
- Linking Service
- Unified Endpoint Package Builder
- Citrix Integration Service
- Microsoft Forefront TMG ISAPI plug-in

For more information, see *System requirements for this version*, page 2.

On Linux, there are two types of Web security installation:

- **Custom**: Select which components you want installed on this machine. See *Custom installation*, page 210.
- **Filtering**: Install all Linux-compatible Web security components on this machine. See *Filtering installation on Linux*, page 210.

Filtering installation on Linux

A filtering installation installs all Linux-compatible Web security components, with the exception of Remote Filtering Server, which should be installed by itself on a machine in the network DMZ.

No management and reporting components (e.g., the TRITON console, Log Server) can be installed as part of the Linux installation. 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 14
2. *Starting the Web Security Linux installer*, page 210
3. *Installing all Web security filtering components on Linux*, page 212

Custom installation

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

1. *Preparing for installation*, page 14
2. *Starting the Web Security Linux installer*, page 210
3. *Installing Web Security components on Linux*, page 215

Starting the Web Security Linux installer

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

1. Log on to the installation machine with full 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. The installer package is called:

   ```
   WebsenseWeb77Setup_Lnx.tar.gz
   ```

Place the installer 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 WebsenseWeb77Setup_Lnx.tar.gz
   tar xvf WebsenseWeb77Setup_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. Launch 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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 210 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 210
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 **Network Card Selection** screen appears, see *Network Card Selection Screen* for instructions.
7. If the **Multiple Network Cards** screen appears, see *Multiple Network Interfaces Screen* for instructions.
8. 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.
9. 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.

10. 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.

    It is possible to run multiple instances of the same transparent identification agent, or certain combinations of different transparent identification agents, in a network. For information about multiple instances or combinations of transparent identification agents, see *Combining transparent identification agents*, page 49.

    - **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.

      See the Using Logon Agent for Transparent User Identification technical paper.

      > ✓ **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 Content Gateway or 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.

11. 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.
12. 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.
13. On the **Pre-Installation Summary** screen, verify the information shown.

    The summary shows the installation path and size, and the components to be installed.
14. 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.

15. On the **Installation Complete** screen, click **Done**.

Installing Web Security components on Linux

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Pre-installation steps*, page 215 ◆ *Install Web Security components on Linux*, page 215

Pre-installation steps

Because Web Security uses a 32-bit installer, if you are installing Web Security components on Red Hat Linux 6.2 64-bit, you must install compatibility modules.

1. On the installation machine, set up a Yum repository for the 32-bit compatibility libraries.
   a. Mount the Red Hat Enterprise Linux installation DVD to the folder /mnt/cdrom.
   b. Create a file named **RH62-Media.repo** in the /etc/yum.repos.d folder.
   c. Add following content to **RH62-Media.repo** and save the file.

```
[RH62-Media]
name=RedHat-$releasever - Media
baseurl=file:///mnt/cdrom
gpgcheck=0
enabled=1
```

   d. Run the following command:

```
# yum clean all
```

2. Install the required library packages:

```
yum install libuuid.i686
yum install compat-libcap1-1.10-1.i686
yum install gdbm.i686
yum install libidn.i686
yum install libXtst-1.0.99.2-3.el6.i686
```

Install Web Security components on Linux

These steps assume you have already downloaded and started the Web Security Linux installer. If not, see *Starting the Web Security Linux installer*, page 210.

1. The first step depends on whether there are other Web Security components already installed on the machine:
   - 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**.
   - 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**.
2. 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*
   - *Usage Monitor*
   - *User Service*
   - *Logon Agent*
   - *eDirectory Agent*
   - *RADIUS Agent*
   - *State Server*
   - *Multiplexer*
   - *Filtering Plug-in*
   - *Remote Filtering Server*
   - *Sync Service*
   - *Directory Agent*

3. 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, Logon Agent, eDirectory Agent, RADIUS Agent, State Server, Multiplexer, Remote Filtering Server, Sync Service, or Directory Agent)
   - *Policy Broker Connection Screen* (Policy Server, Sync Service, or Directory Agent).
   - *Multiple Network Interfaces Screen* (if multiple NICs detected)
   - *Integration Option Screen* (Filtering Service)
   - *Select Integration Screen* (Filtering Service, to be integrated with Content Gateway or a third-party product)
   - *Network Agent and Firewall Screen* (Filtering Service and Network Agent; Filtering Service to be integrated with a Check Point product)
   - *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)

4. 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.

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

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

6. 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.

7. On the **Installation Complete** screen, click **Done**.

12 Installing Websense Content Gateway

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway and Web Security Gateway Anywhere, v7.7.x	◆ *Deployment* ◆ *Installation* ◆ *Online Help*

Websense Content Gateway (Content Gateway) is a Linux-based, high-performance Web proxy and cache that provides real-time content analysis and Web site classification to protect clients from malicious Web content while enabling access to safe content.

Content Gateway offers:

- Categorization of dynamic Web sites
- Categorization of new and unclassified sites
- HTTPS content analysis
- Enterprise proxy caching capabilities

> ✓ **Note**
>
> In a Websense-appliance-based deployment, when Web Security Gateway (Anywhere) is configured, Content Gateway is already installed.

In a software-based deployment, Content Gateway is a required part of Websense Web Security Gateway and Web Security Gateway Anywhere. Content Gateway must be installed on a Linux machine. The machine should be dedicated to running Content Gateway.

Websense Web Security Gateway and Web Security Gateway Anywhere subscribers get the following features, in addition to the standard Websense Web Security features:

- Security analysis that inspects incoming Web pages to immediately block malicious content, such as phishing, malware, and viruses.

- Advanced file analysis that applies both advanced detection techniques and traditional antivirus scanning to discover and block infected and malicious files users are attempting to download.

See the TRITON - Web Security Help and read the section titled 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 *Installation overview: Web Security Gateway Anywhere*, page 200.

Content Gateway can be used as an explicit or transparent proxy.

- In an explicit proxy deployment, client applications, typically browsers, must be configured to send requests 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, the content on HTTPS 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 to inspect HTTPS and FTP traffic, you must enable the SSL Manager feature. See Content Gateway Manager Help for information on SSL Manager.

Deployment

- *Proxy deployment options*, page 84
- *User authentication*, page 85
- *HTTPS content inspection*, page 87
- *Handling special cases*, page 87
- *Explicit proxy deployment*, page 88
- *Transparent proxy deployment*, page 89
- *Chaining Content Gateway with other proxies*, page 99

Installation

These installation instructions are for installing Content Gateway software on a server.

> **Note**
> In a 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*
2. *Preparing to install Websense Content Gateway*
3. *Installing Websense Content Gateway*

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 system. 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere, v7.7.x

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:

- *Installation overview: Web Security Gateway*, page 197
- *Installing via the Web Security All option*, page 204
- *Installation overview: Web Security Gateway Anywhere*, page 200

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 addresses or addresses of Policy Server and Filtering Service. You will need them when installing Content Gateway.

> ✓ **Note**
>
> Be sure hostname 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	**In this topic**
- Web Security Gateway and Web Security Gateway Anywhere, v7.7.x	- *Downloading the installer* - *Internet connectivity* - *Security of the Content Gateway machine* - *Explicit or Transparent Proxy* - *System requirements for Websense Content Gateway* - *Hostname and DNS configuration for Content Gateway* - *Preparing a cache disk for use by Websense Content Gateway* - *Preparing for a clustered deployment of Websense Content Gateway*

Before installing Websense Content Gateway (Content Gateway) on a machine, perform the following tasks and consider the following issues.

Downloading the installer

1. Download the **WebsenseCG77Setup_Lnx.tar.gz** installer tar archive, from mywebsense.com to a temporary directory.

   For version 7.7.3 the name is: **WebsenseCG773Setup_Lnx.tar.gz**

2. Create a directory for the tar archive, and then move the archive to the new directory. For example:

   ```
   mkdir wcg_v77
   ```

   ```
   mv <installer tar archive> wcg_v77
   ```

3. Change to the directory you created in Step 2.

   ```
   cd wcg_v77
   ```

4. Unpack the tar archive:

   ```
   tar -xvzf <installer tar archive>
   ```

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 analytic database updates cannot be performed until Internet connectivity is available.

Security of the Content Gateway machine

Consider these security issues prior to installing Content Gateway:

- *Physical security*
- *Root permissions*
- *Ports*

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

For a list of default ports, see Content Gateway ports. They must be open to support the full set of Websense Web Security Gateway features.

> ✓ **Note**
>
> If you customized any ports that Websense software uses for communication, replace the default port with the custom port you implemented.

Restrict inbound traffic to as few 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.

IPTables Firewall

If your server is running the Linux IPTables firewall, you must configure the rules in a way that enables Content Gateway to operate effectively. See the IPTables for Content Gateway article in the Websense Technical Library.

Explicit or Transparent Proxy

Content Gateway can be used as an explicit or transparent proxy. This section contains the following topics:

- *Explicit proxy*
- *Configuring client browsers for explicit proxy*
- *Configuring Internet Explorer 8.0 and later for explicit proxy*
- *Configuring Firefox 5.x for explicit proxy*

Explicit proxy

Explicit proxy deployment requires directly pointing client Web browsers (And other client applications) to Content Gateway for HTTP, and optionally, HTTPS and FTP traffic. This is accomplished by a using a PAC file, WPAD, or by having the user edit browser settings to point to Content Gateway.

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 by setting and propagating browser configuration in your organization through Group Policy, a Windows Server feature. 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. The default port for FTP is 2121.

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 8.0 and later for explicit proxy

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 5.x for explicit proxy

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 proxy 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 a multiple-proxy (cluster) deployment, a WCCP v2-enabled router also supports load distribution among proxies.

See 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).

System requirements for Websense Content Gateway

- *Hardware*
- *Software*
- *Preparing a cache disk for use by Websense Content Gateway*

Hardware

CPU	Quad-core running at 2.8 GHz or faster
Memory:	
If RHEL 6, 64-bit	6 GB
If RHEL 5, 32-bit	4 GB
Disk space	2 disks: • 100 GB for the operating system, Websense Content Gateway, and temporary data. • 147 GB for caching If caching will not be used, this disk is not required. The caching disk: – Should be at least 2 GB and no more than 147 GB – Must be a raw disk, not a mounted file system – Must be dedicated – Must *not* be part of a software RAID – Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64 MB of write-through cache
Network Interfaces	2

To support transparent proxy deployments

Router

Must support WCCP v2.

A Cisco router must run IOS 12.2 or later.

Client machines, the destination Web server, and Content Gateway must reside on different subnets.

—or—

Layer 4 switch

You may use a Layer 4 switch rather than a router.

To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later).

Websense Content Gateway must be Layer 2 adjacent to the switch.

The switch must be able to rewrite the destination MAC address of frames traversing the switch.

The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Software

Content Gateway version 7.7.3 is certified on all of the Red Hat Enterprise Linux versions that 7.7.0 is certified on, plus:

- Update 3, 64-bit, Basic Server

Content Gateway version 7.7.0 is certified on:

- Red Hat Enterprise Linux, 6 series, updates 0, 1, and 2, 64-bit, Basic Server
- Red Hat Enterprise Linux, 5 series, updates 3, 4 and 5, base or Advanced Platform, 32-bit only
- The corresponding CentOS versions (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers).

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.

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
```

For more information on installing on Red Hat Enterprise Linux, see *Requirements for Red Hat Enterprise Linux*.

Websense Web filtering components

Versions must match. When version 7.7.0 is used, TRITON – Web Security must be version 7.7.0. When version 7.7.3 is used, TRITON – Web Security must be version 7.7.3.

Important

Websense filtering software must be installed prior to Content Gateway. When the filtering software is installed, Websense Content Gateway must be specified as the integration product. See *Installation overview: Web Security Gateway*, page 197, *Installing via the Web Security All option*, page 204, or *Installation overview: Web Security Gateway Anywhere*, page 200,.

Integration with Websense Data Security

The version must match other installed components.

- Version 7.7.0 or 7.7.3 (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 Content Gateway.
- Any version can be used via the ICAP interface. See Content Gateway Manager Help for configuration instructions.

Web browsers

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 8 and 9
- Mozilla Firefox 5 and later
- Google Chrome 13 and later

Note

The browser restrictions mentioned above apply only to the Content Gateway Manager and not to client browsers proxied by Content Gateway.

Hostname and DNS configuration for Content Gateway

Configure a hostname for the 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 <hostname>
   ```

   where <*hostname*> 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=<hostname>
   ```

   where <*hostname*> 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 and third lines (the ones that begin with “127.0.0.1” and “::1”, respectively).

   ```
   xxx.xxx.xxx.xxx   <FQDN>    <hostname>
   127.0.0.1       localhost.localdomain   localhost
   ::1             localhost6.localdomain6 localhost6
   ```

   <*FQDN*> is the fully-qualified domain name of this machine (i.e., <*hostname*>.<*subdomain(s)*>.<*top-level domain*>).
   For example: myhost.example.com

   <*hostname*> is the same name specified in Step 1.

   Do **not** reverse the order of the FQDN and hostname.

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.

Note

If a multicast group IP address has not already been defined, 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere, v7.7.x

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 **WebsenseCG77Setup_Lnx.tar.gz** tar archive, from mywebsense.com to a temporary directory. If installing version 7.7.3, download **WebsenseCG773Setup_Lnx.tar.gz**.

   a. Create a directory for the tar archive, and then move the archive to the new directory. For example:

   ```
   mkdir wcg_v77
   mv <installer tar archive> wcg_v77
   ```

   b. Change to the directory you created in Step a.

   ```
   cd wcg_v77
   ```

   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 Content Gateway. Do not install or run 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 installs Content Gateway in /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 4
   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.

✓ **Note**

See also *Installer gives NetworkManager or avahi-daemon error*.

6. Read the subscription agreement. At the 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 will masked characters be shown—but the characters are being accepted. After typing a password, press **Enter**. Then repeat to confirm it.

8. Enter an email address where 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). The address must be IPv4. 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:

```
Websense Content Gateway uses 11 ports on your server:
```

```
----------------------------------------------
'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
```

```
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:

    ```
    Websense Content Gateway Clustering Information
    ------------------------------------------------
    '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] >
    ```

    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 cluster network interface:
    >
    Enter a multicast group address for cluster <cluster_name>.
    Address must be between 224.0.1.27 - 224.0.1.254:
    [<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:

> **Note**
>
> If you choose to not enable raw disk cache now, cache disks may be added after Content Gateway has been installed. For instructions, see Content Gateway Manager Help.

```
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 has the ability to send usage
statistics, information about scanned content and activated
product features to Websense Inc. for the purpose of
improving the accuracy of scanning, filtering and
categorization.

Would you like to allow this communication with Websense,
Inc. ? [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.

    > **Note**
    >
    > The subscription key is shared automatically with Content Gateway if it has already been specified in TRITON –Web Security.
    >
    > If you receive an email from Content Gateway (to the address you specified during installation) with "WCG license download failed" in the subject line, this alert does not mean a problem occurred with the installation. The alert indicates that your deployment may require you to manually enter the subscription key in Content Gateway Manager.
    >
    > See the Getting Started section of the Content Gateway Manager Help for information on entering your subscription key.

19. When installation is complete, reboot the 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
    - Analytics Server

Requirements for Red Hat Enterprise Linux

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway and Web Security Gateway Anywhere, v7.7.x	◆ *Required libraries in Red Hat Enterprise Linux 6* ◆ *Installing on Red Hat Enterprise Linux 6, update 1 and higher* ◆ *Red Hat Enterprise Linux Update 5.x*

Required libraries in Red Hat Enterprise Linux 6

Required libraries:

apr.i686
apr-util.i686
audit-libs.i686
bzip2-libs.i686
compat-db43.i686
compat-expat1.i686
compat-openldap.i686
compat-readline5.i686
cracklib.i686
cyrus-sasl-lib.i686
db4.i686
expat.i686
ftp.x86_64
gdbm.i686
glibc.i686
keyutils-libs.i686
krb5-libs.i686
libattr.i686
libcap.i686
libcom_err.i686
libcurl.i686
libgcc.i686
libicu.i686
libidn.i686
libselinux.i686
libssh2.i686
libstdc++.i686
libtalloc.i686
libtdb.i686
libuuid.i686
libxml2.i686
nc.x86_64
ncurses-devel.i686
ncurses-libs.i686
nspr.i686
nss.i686
nss-softokn.i686
nss-softokn-freebl.i686
nss-util.i686
openldap.i686
openssl.i686
openssl098e.i686
pam.i686
popt.i686
readline.i686
readline-devel.i686
samba-winbind-clients.i686
sqlite.i686
tcl.x86_64
tcp_wrappers-libs.i686
zlib.i686

During Content Gateway installation, the installer will list missing packages and then exit the installer.

To install the missing packages, the operating system must have a repository of available libraries. The Media repository on the Red Hat Enterprise Linux install DVD is an acceptable source of packages.

After the repository is setup, all of the required dependencies can be automatically resolved by running:

```
yum install wcg_deps-1-0.noarch.rpm
```

The above RPM is included in the Content Gateway install tree, at the same level as wcg_install.sh.

Installing on Red Hat Enterprise Linux 6, update 1 and higher

biosdevname

Red Hat Enterprise Linux 6, update 1 introduces **biosdevname**.

biosdevname is not supported by Content Gateway version 7.7.x and lower.

What is biosdevname? The Red Hat Enterprise Linux update 6.1 release notes state:

> ... biosdevname [is an] optional convention for naming network interfaces. biosdevname assigns names to network interfaces based on their physical location. ... biosdevname is disabled by default, except for a limited set of Dell systems.

biosdevname is designed to replace the older, inconsistent “eth#” naming scheme. The new standard will be very helpful when it is fully adopted, however it is not yet fully adopted.

The presence of a single Ethernet device absent the SMIBIOS Slot # and biosdevname field causes the Red Hat Enterprise Linux 6.1 installer and 'udev' to fall back to the preferred eth# device naming for all interfaces.

Important

To ensure interface name consistency among hardware platforms and Red Hat Enterprise Linux 6.0, 6.1, and higher, Content Gateway version 7.7.x requires “eth#” names. If any non-“eth#” names exist, the Content Gateway installer exits and provides a link to instructions for modifying system startup files.

Upgrading from Red Hat Enterprise Linux 6.0 to 6.1 and higher poses no risk. There was no biosdevname support in Update 6.0 and device names are not altered by the upgrade to 6.1 or higher.

Disabling biosdevname

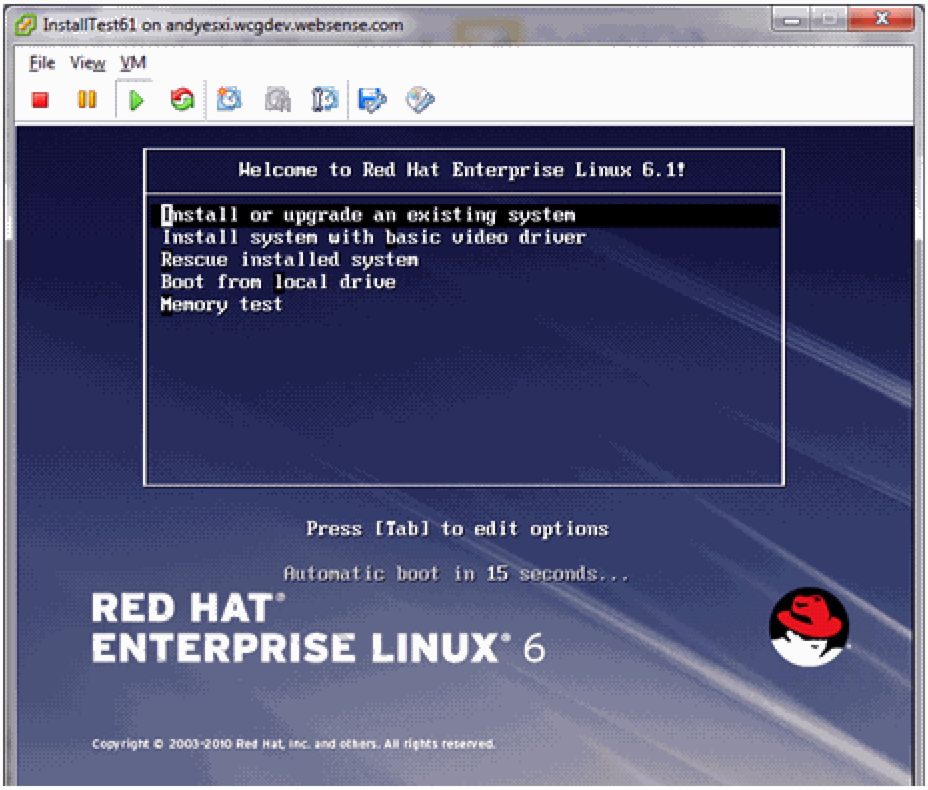
If while installing Content Gateway the installer finds non-eth# interface names, the installer quits and provides a link to instructions for modifying system startup files.

There are 2 ways to disable biosdevname:

1. During operating system installation.
2. Post-operating system installation through modification of several system files and other activities.

The easiest way to disable biosdevname is to do it during operating system installation. This is the recommend method.

Disabling biosdevname during operating system installation:

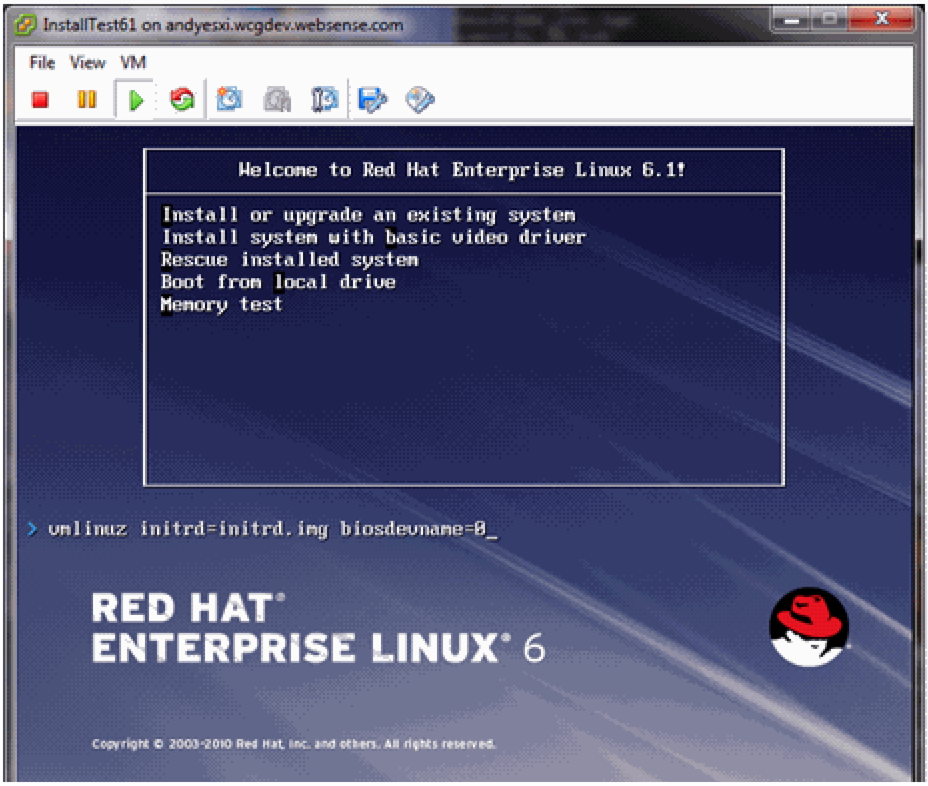


InstallTest61 on andyesxi.wcgdev.websense.com
File View VM

```
Welcome to Red Hat Enterprise Linux 6.1!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test

Press [Tab] to edit options

Automatic boot in 15 seconds...
```

RED HAT®
ENTERPRISE LINUX® 6
Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

When the installer starts, press [TAB] and alter the boot line to add “biosdevname=0” as follows:


InstallTest61 on andyesxi.wcgdev.websense.com
File View VM

```
Welcome to Red Hat Enterprise Linux 6.1!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test

> vmlinuz initrd=initrd.img biosdevname=0_
```

RED HAT®
ENTERPRISE LINUX® 6
Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

Proceed through the rest of the installer as usual.

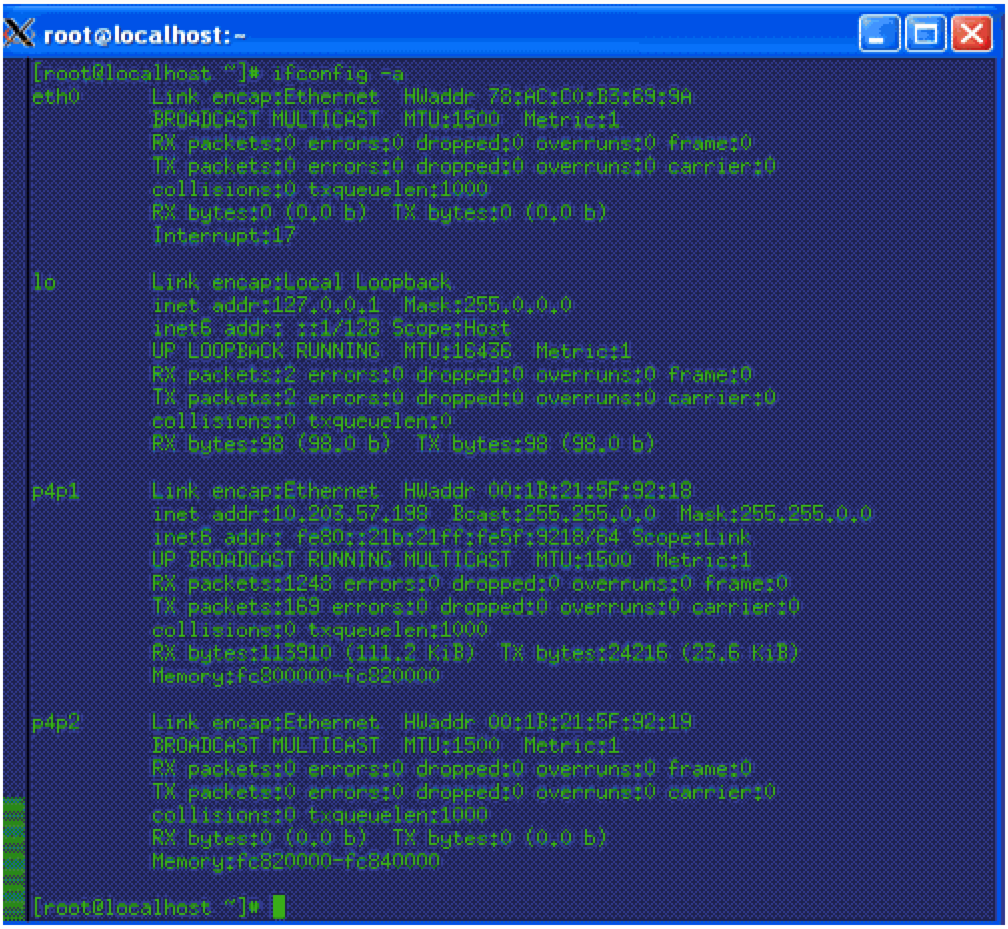
Disabling biosdevname after operating system installation:

Log on to the operating system and verify that non-eth# names are present.

```
ifconfig -a
```

If only “eth#” and “lo” names are present, you are done. No other actions are required.

If there are names like “emb#” or “p#p#” perform the following steps.



```
[root@localhost ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 78:AC:C0:B3:69:9A
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:98 (98.0 b)  TX bytes:98 (98.0 b)

p4p1      Link encap:Ethernet  HWaddr 00:1B:21:5F:92:18
          inet addr:10.203.57.198  Bcast:255.255.0.0  Mask:255.255.0.0
          inet6 addr: fe80::21b:21ff:fe5f:9218/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1248 errors:0 dropped:0 overruns:0 frame:0
          TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:113910 (111.2 KiB)  TX bytes:24216 (23.6 KiB)
          Memory:fc800000-fc820000

p4p2      Link encap:Ethernet  HWaddr 00:1B:21:5F:92:19
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:fc820000-fc840000

[root@localhost ~]#
```

1. Log in as root.
2. cd /etc/sysconfig/network-scripts
3. Rename all “ifcfg-<ifname>” files except “ifcfg-lo” so that they are named “ifcfg-eth#”.
    a. Start by renaming “ifcfg-em1” to “ifcfg-eth0” and continue with the rest of the “ifcfg-em#” files.
    b. When the above are done, rename the “ifcfg-p#p#” files.

       If there are multiple “ifcfg-p#p1” interfaces, rename all of them in the order of the lowest “ifcfg-p#” first. For example, if the initial set of interfaces presented by “`ifconfig -a” is:

       em1 em2 em3 em4 p1p1 p1p2 p2p1 p2p2

       em1 -> eth0

       em2 -> eth1

       em3 -> eth2

       em4 -> eth3

       p1p1 -> eth4

       p1p2 -> eth5

p2p1 -> eth6

p2p2 -> eth7

c. Make the “ifcfg-eth#” files linear so that if you have 6 interfaces you have eth0 through eth5.

4. Edit all the ifcfg-eth# files.
   a. Update the DEVICE= sections to refer to the new name: “eth#”
   b. Update the NAME= sections to refer to the new name: “System eth#”
5. Remove the old udev device mapping file if it exists:

   ```
   rm -f /etc/udev/rules.d/70-persistent-net.rules
   ```
6. Modify the “grub.conf” file to disable biosdevname for the kernel you boot.
   a. Edit /boot/grub/grub.conf
   b. Add the following to the end of your “kernel /vmlinuz” line:

      ```
      biosdevname=0
      ```
7. Reboot.
8. Reconfigure the interfaces as required.

Installer gives NetworkManager or avahi-daemon error

Warning

Content Gateway is supported on Red Hat Enterprise Linux 6, Basic Server (no GUI).

It is **not** supported on Red Hat Enterprise Linux 6 with a GUI.

When Red Hat Enterprise Linux 6 is installed with a GUI, the Content Gateway installer recognizes systems running NetworkManager or avahi-daemon processes and emits an error similar to:

```
Error: The avahi-daemon service is enabled on this system
and must be disabled before Websense Content Gateway v7.7
can be installed.

Please disable the avahi-daemon service with the following
commands and restart the Websense Content Gateway
installation.

    chkconfig --levels 2345 avahi-daemon off

    service avahi-daemon stop
```

To continue, the conflicting NetworkManager and avahi-daemon processes must be stopped.

1. To disable the avahi-daemon service:

   ```
   chkconfig --levels 2345 avahi-daemon off
   service avahi-daemon stop
   ```

2. To restart the installer:

   ```
   ./wch_install.sh
   ```

Red Hat Enterprise Linux Update 5.x

- 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 must be set to disabled or permissive

13 Installing appliance-based Websense solutions

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

This topic provides an overview of V-Series appliance-based Websense solutions, along with a description of solution components and procedures for installing and configuring the appliance. The following sections are included:

- *Websense appliance-based solutions*
- *Summary of appliance solution components*
- *Installation steps for appliance-based solutions*

Websense appliance-based solutions

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

This section provides a brief overview of the following Websense appliance-based solutions:

- *Web Security*

- *Web Security Gateway or Web Security Gateway Anywhere*
- *Email Security Gateway or Email Security Gateway Anywhere*
- *Web Security and Email Security Gateway (Anywhere)*
- *Web Security Gateway (Anywhere) and Email Security Gateway (Anywhere)*

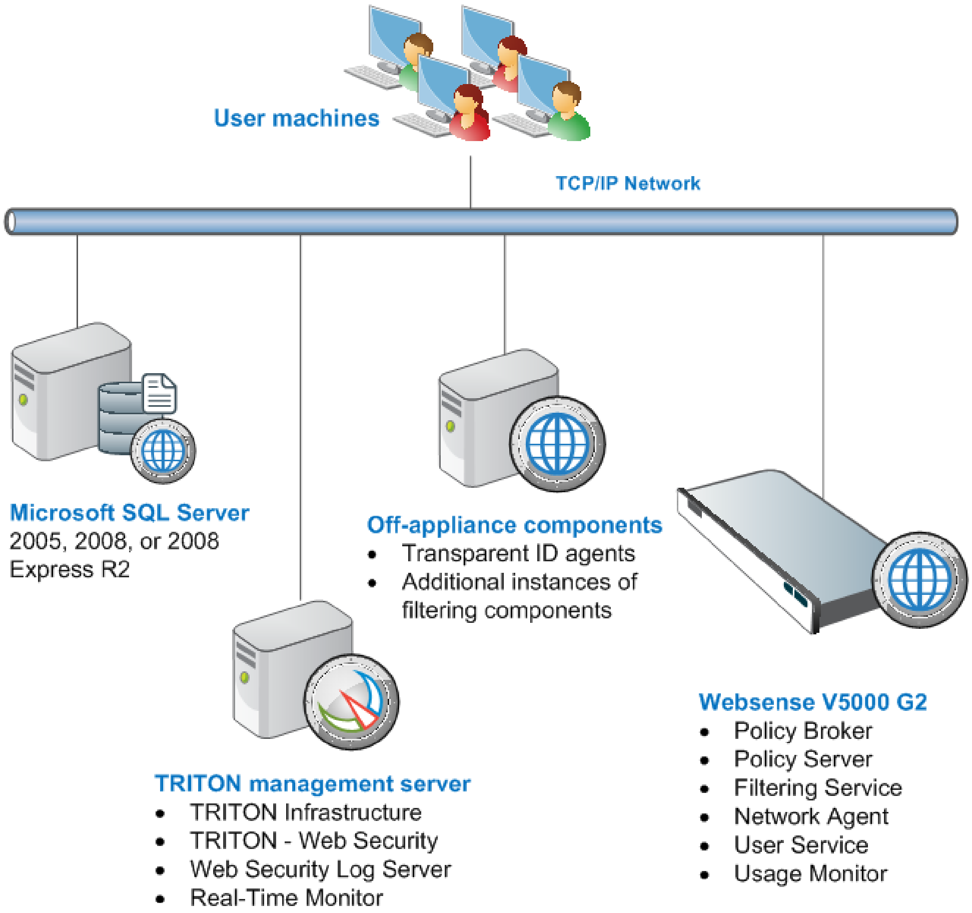
Web Security

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- V5000 G2 v7.7.x

The following illustration provides a high-level overview of a basic single-appliance deployment of Websense Web Security. 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).



For descriptions of the diagram components, see *Summary of appliance solution components*, page 260.

For Web Security appliance installation instructions, see *Installation steps for appliance-based solutions*, page 263.

For information about a software-based Web Security installation, see *Installation overview: Web Filter and Web Security*, page 193.

Deployment

- *System requirements for this version*, page 2
- *Deploying Web Security core components*, page 24
- *Extending your Web Security deployment*, page 31
- *Web Security required external resources*, page 41
- *Deploying transparent identification agents*, page 48
- *Maximizing Web Security system performance*, page 42
- *Deploying Remote Filtering Server and Client*, page 62
- *Deploying Web Security for a distributed enterprise*, page 65

Initial configuration

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675
- *Web Security initial configuration*, page 677

Web Security Gateway or Web Security Gateway Anywhere

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

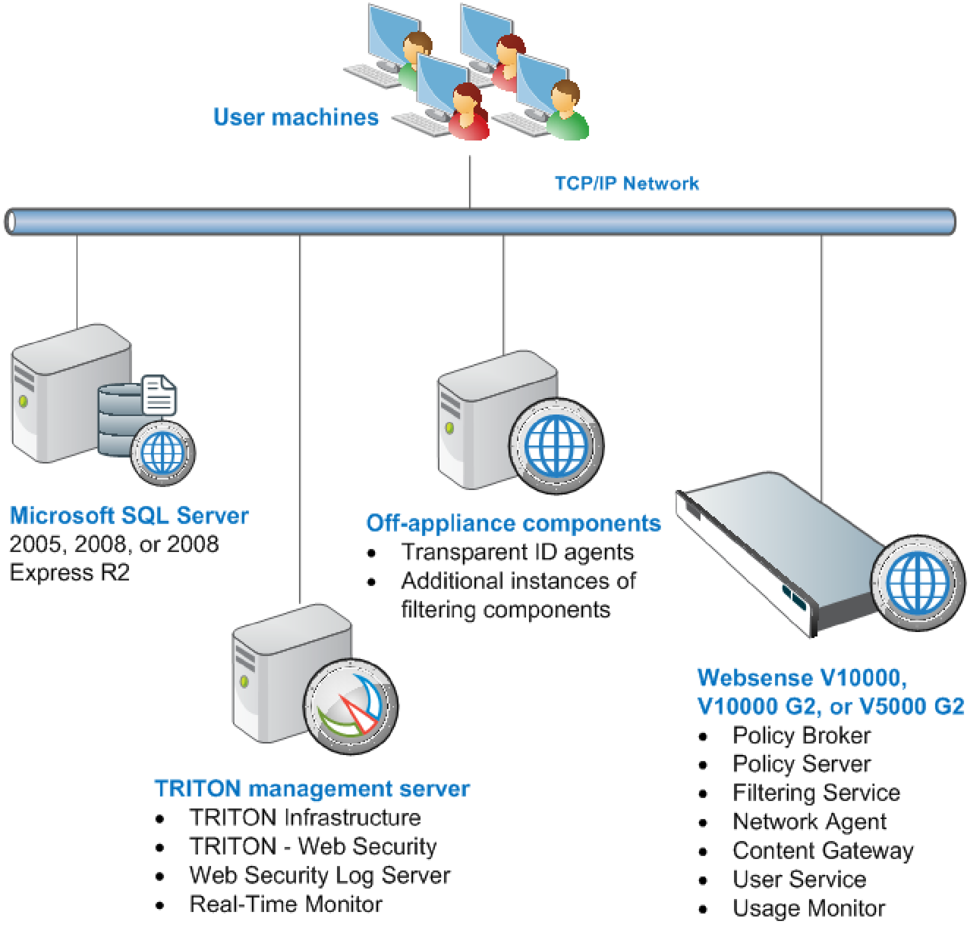
Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

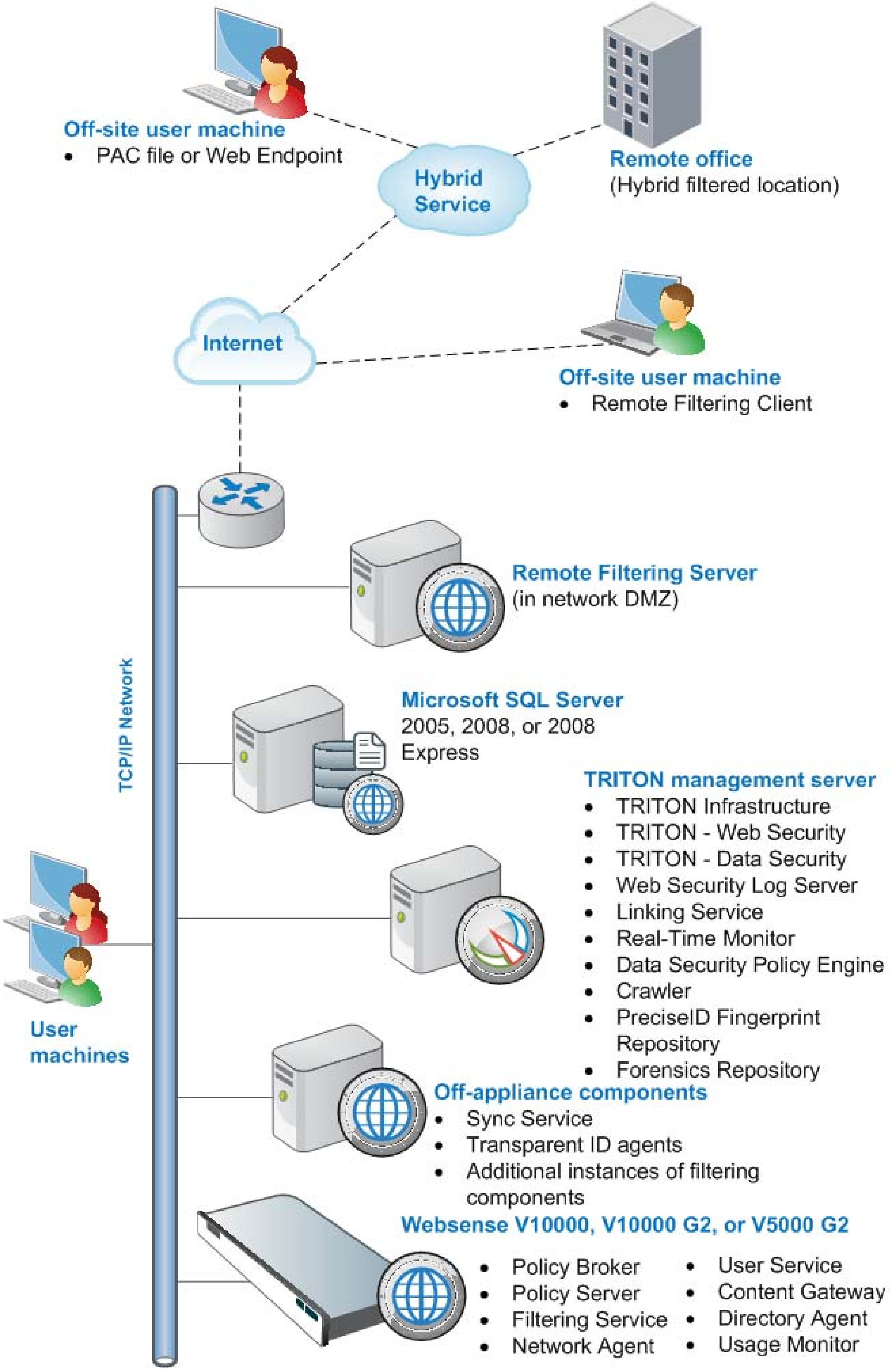
The following illustrations provide a high-level overview of a basic single-appliance deployment of Websense Web Security Gateway and Web Security Gateway Anywhere. In Web Security Gateway Anywhere deployments, both the Web Security and Data Security modules of the TRITON Unified Security Center are enabled.

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

Web Security Gateway:



Web Security Gateway Anywhere:



For descriptions of the diagram components, see *Summary of appliance solution components*, page 260.

For Web Security Gateway appliance installation instructions, see *Installation steps for appliance-based solutions*, page 263.

For information about a software-based Web Security installation, see *Installation overview: Web Security Gateway*, page 197.

Deployment

- *System requirements for this version*, page 2
- *Deploying Web Security core components*, page 24
- *Extending your Web Security deployment*, page 31
- *Web Security required external resources*, page 41
- *Deploying transparent identification agents*, page 48
- *Maximizing Web Security system performance*, page 42
- *Deploying Remote Filtering Server and Client*, page 62
- *Deploying Web Security for a distributed enterprise*, page 65

Initial configuration

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675
- *Web Security initial configuration*, page 677

Web Security Gateway only:

- *Deploying Web Security for a distributed enterprise*, page 65
- *Content Gateway initial configuration*, page 684

Web Security Gateway Anywhere only:

- *Confirm Content Gateway registration with Data Security*, page 680
- *Configuring the Content Gateway policy engine*, page 681
- *Verifying Web and data security linking*, page 681

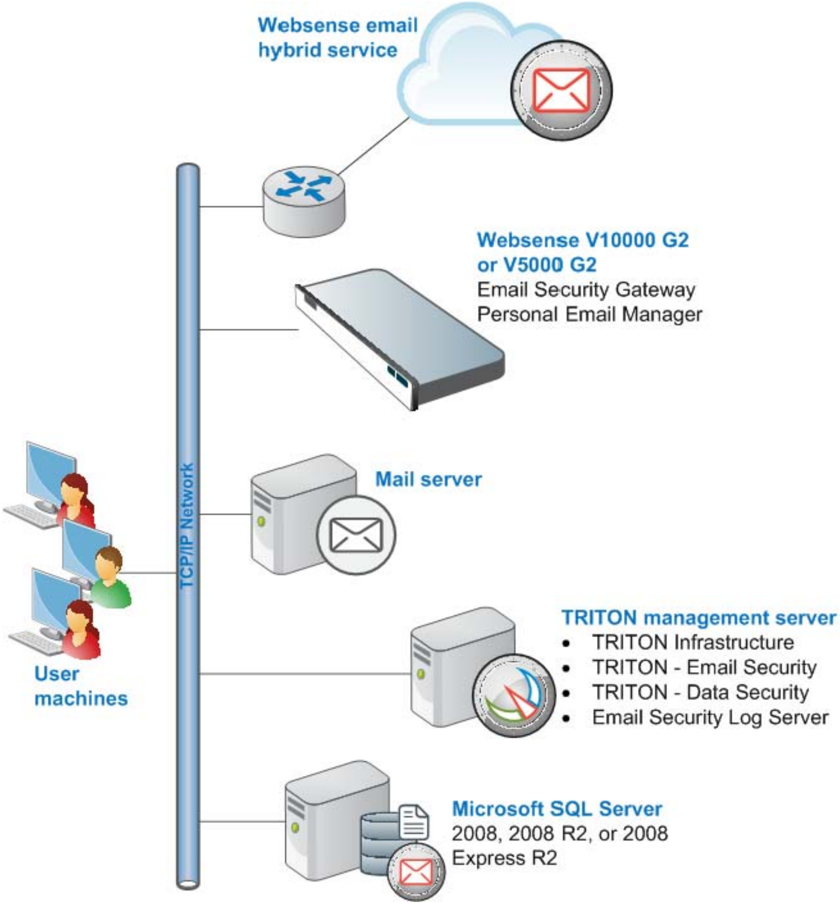
Email Security Gateway or Email Security Gateway Anywhere

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000 G2, V5000 G2 v7.7.x

The following illustration is a high-level diagram of a basic appliance-based deployment of Email Security Gateway Anywhere, which includes the email hybrid service. 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).



For descriptions of the diagram components, see *Summary of appliance solution components*, page 260.

For Email Security Gateway appliance installation instructions, see *Installation steps for appliance-based solutions*, page 263.

Deployment

- *System requirements*, page 164
- *Single-appliance deployments*, page 166
- *Multiple-appliance deployments*, page 169

Initial configuration

- *Email Security Gateway initial configuration*, page 683

Web Security and Email Security Gateway (Anywhere)

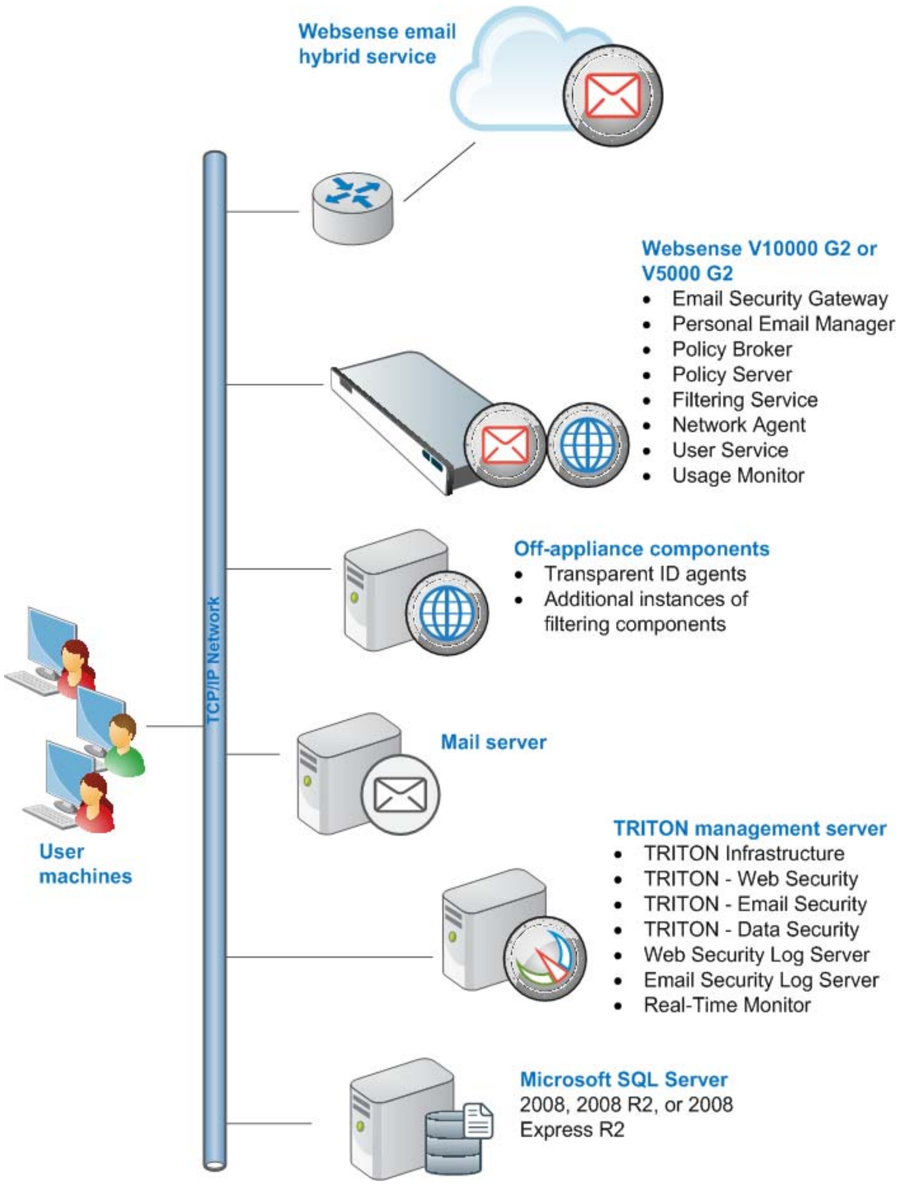
Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000 G2 and V5000 G2 v7.7.x

The following illustration provides a high-level overview of a basic appliance-based deployment of Web Security and Email Security Gateway Anywhere, which includes the email hybrid service. This deployment is supported on either a Websense V10000 G2 or V5000 G2 appliance.

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).



For descriptions of the diagram components, see *Summary of appliance solution components*, page 260.

For Web Security and Email Security Gateway appliance installation instructions, see *Installation steps for appliance-based solutions*, page 263.

Deployment

Web Security

- *System requirements for this version*, page 2

- *Deploying Web Security core components*, page 24
- *Extending your Web Security deployment*, page 31
- *Web Security required external resources*, page 41
- *Deploying transparent identification agents*, page 48
- *Maximizing Web Security system performance*, page 42
- *Deploying Remote Filtering Server and Client*, page 62
- *Deploying Web Security for a distributed enterprise*, page 65

Email Security

- *System requirements*, page 164
- *Single-appliance deployments*, page 166
- *Multiple-appliance deployments*, page 169

Initial configuration

Web Security

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675
- *Web Security initial configuration*, page 677

Email Security

- *Email Security Gateway initial configuration*, page 683

Web Security Gateway (Anywhere) and Email Security Gateway (Anywhere)

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

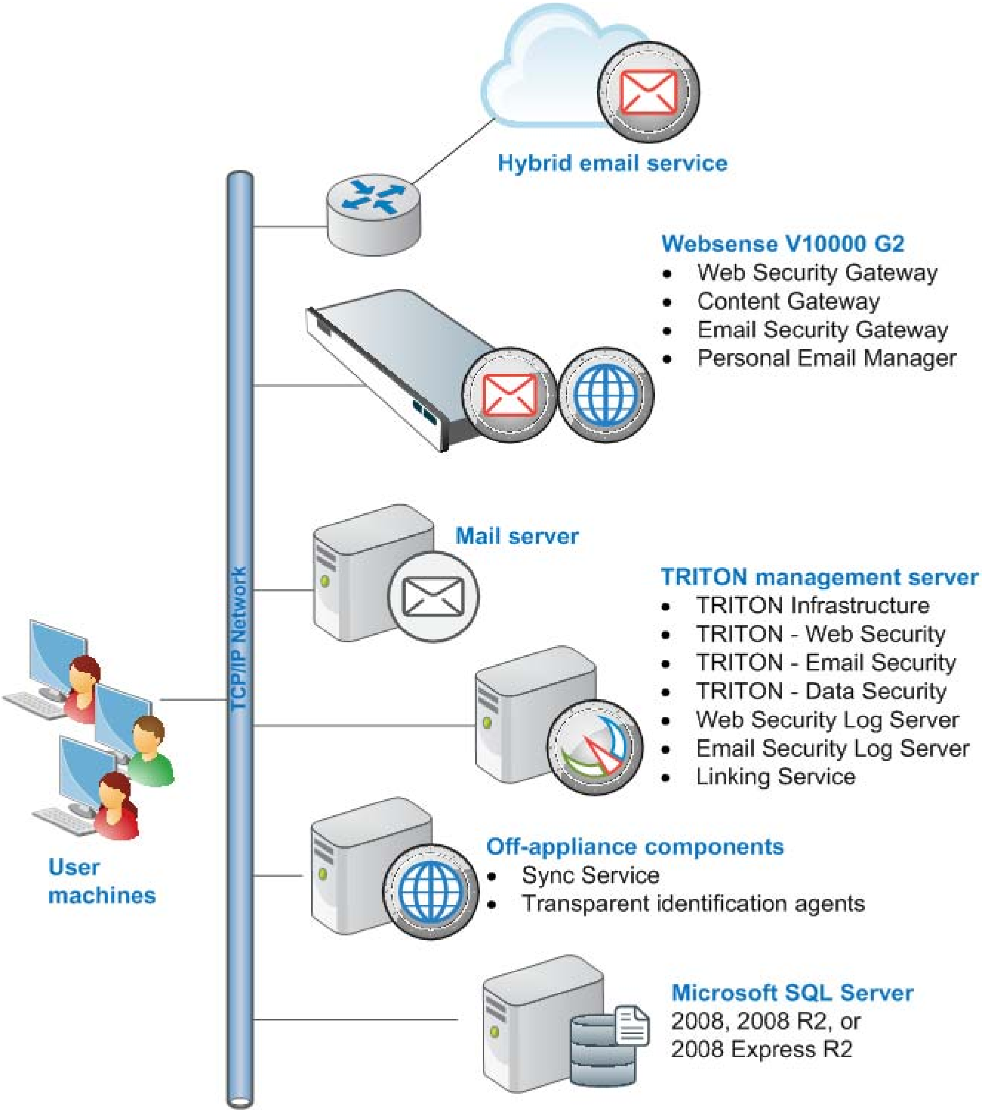
Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000 G2 v7.7.x

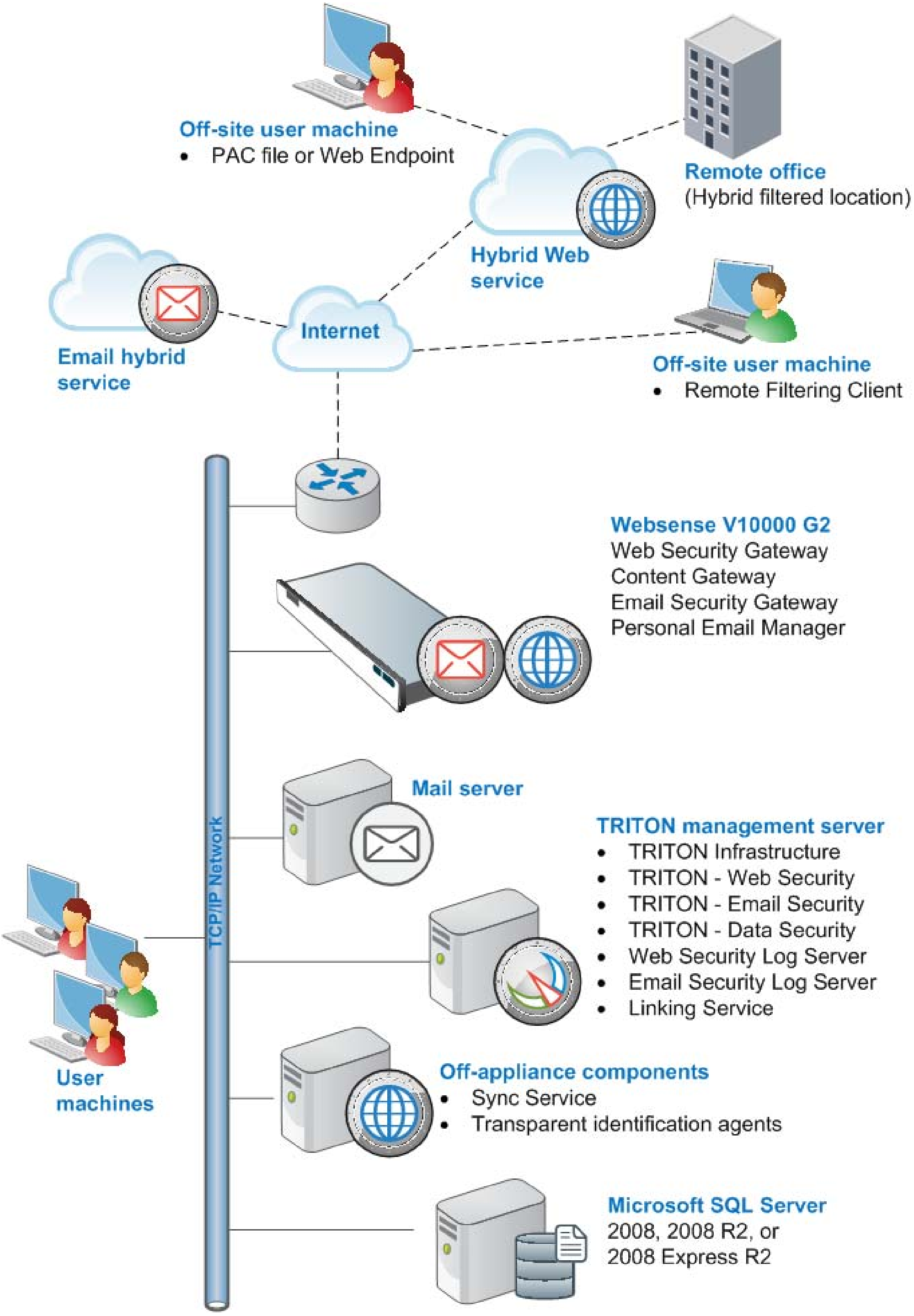
The following illustrations provide a high-level overview of a basic appliance-based deployment of Web Security Gateway (Anywhere) and Email Security Gateway (Anywhere). This deployment is supported only on a Websense V10000 G2 appliance.

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).

Web Security Gateway with Email Security Gateway Anywhere:



Web Security Gateway Anywhere with Email Security Gateway Anywhere:



For descriptions of the diagram components, see *Summary of appliance solution components*, page 260.

For appliance installation instructions, see *Installation steps for appliance-based solutions*, page 263.

Deployment

Web Security Gateway (Anywhere)

- *Deploying Web Security core components*, page 24
- *Extending your Web Security deployment*, page 31
- *Web Security required external resources*, page 41
- *Deploying transparent identification agents*, page 48
- *Maximizing Web Security system performance*, page 42
- *Deploying Remote Filtering Server and Client*, page 62
- *Deploying Web Security for a distributed enterprise*, page 65

Email Security Gateway (Anywhere)

- *System requirements*, page 164
- *Single-appliance deployments*, page 166
- *Multiple-appliance deployments*, page 169

Initial configuration

General

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675

Web Security Gateway and Gateway Anywhere

- *Web Security initial configuration*, page 677
- *Content Gateway initial configuration*, page 684
- *Deploying Web Security for a distributed enterprise*, page 65

Web Security Gateway Anywhere only

- *Confirm Content Gateway registration with Data Security*, page 680
- *Configuring the Content Gateway policy engine*, page 681
- *Verifying Web and data security linking*, page 681

Email Security Gateway (Anywhere)

- *Email Security Gateway initial configuration*, page 683

Summary of appliance solution components

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.7.x ◆ V10000, V10000 G2, and V5000 G2, v7.7.x	◆ *V-Series appliances*, page 260 ◆ *Content Gateway*, page 261 ◆ *Personal Email Manager*, page 261 ◆ *Off-appliance components*, page 262

This topic presents a brief description of the components used in Websense appliance-based solutions. For detailed information about Web Security components like Policy Broker, Policy Server, and transparent identification agents, see *Web Security components*, page 729.

V-Series appliances

Websense Web Security and Email Security solutions are supported on the following V-Series appliances:

- *Websense V10000*
- *Websense V10000 G2*
- *Websense V5000 G2*

Websense V10000

The Websense V10000 appliance provides the majority of Web Security Gateway functions. Web traffic is directed through the Websense appliance for filtering.

Only the Web Security Gateway module is supported on the V10000 appliance. Web Security and Email Security Gateway modules are not supported.

> **Note**
> V10000 appliances must upgraded to version 7.7.x with the V-Series upgrade patch. There is not a v7.7 recovery (ISO) image for V10000.

Websense V10000 G2

The Websense V10000 G2 appliance provides the majority of Web Security, Web Security Gateway, and Email Security Gateway functions.

For Web Security deployments, Web traffic is directed through the Websense appliance for filtering.

For Email Security deployments, incoming email flows from the email hybrid 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.

Websense V5000 G2

The Websense V5000 G2 appliance provides the majority of Web Security, Web Security Gateway, and Email Security Gateway functions. The V5000 appliance can also be configured in dual mode with Web Security and Email Security Gateway. A Web Security Gateway and Email Security Gateway dual-mode deployment is supported only on a V10000 G2 appliance.

For Web Security deployments, Web traffic is directed through the Websense appliance for filtering.

For Email Security deployments, incoming email flows from the email hybrid 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.

Content Gateway

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.

Personal Email Manager

Personal Email Manager is a tool that allows an end user to manage email that has been blocked by Websense Email Security Gateway. Occasionally Email Security may block email that is safe and that should be delivered.

Personal Email Manager notifies an end user of blocked email and provides the means to manage it, either by permitting mail delivery or blocking a message from reaching a user’s inbox.

Off-appliance components

The following Websense software and third-party components do not run on V-Series appliances.

Microsoft SQL Server

Websense reporting databases are hosted by Microsoft SQL Server. The reporting databases store Websense logging, reporting, and (for some modules) configuration data. With Email Security Gateway, quarantined email messages are stored here as well.

- SQL Server is not included as part of a Websense subscription.
- In most cases, when you install Websense components, SQL Server must already be installed and running on a separate machine.

  In very small deployments, or for evaluation, the TRITON Unified Installer can be used to install SQL Server 2008 R2 Express, either on the TRITON management server or on a separate Windows machine.

TRITON management server

The TRITON management server is the machine that hosts the TRITON Unified Security Center (TRITON console), the management and reporting console for Websense Web Security, Email Security, and Data Security.

This machine manages your entire Websense deployment. It includes TRITON Infrastructure and the TRITON console management modules that you select. The 3 TRITON management modules are:

- TRITON - Web Security
- TRITON - Data Security
- TRITON - Email Security

In an Email Security Gateway deployment, the TRITON management server includes both TRITON - Email Security and TRITON - Data Security, as well as additional Data Security components. TRITON - Data Security is used to configure email DLP (data loss prevention) features.

In a Web Security Gateway Anywhere deployment, the TRITON management server also includes TRITON - Data Security and other Data Security components in order to enable Web DLP functionality.

Additional, optional components can also run on this machine. See *TRITON management server*, page 731, for more information.

In Web Security deployments, Real-Time Monitor is automatically installed on the TRITON management server. In Web Security Gateway Anywhere deployments, Linking Service is also typically installed on this machine.

Reporting components

Both Web Security and Email Security solutions use a component called **Log Server** to pass information to the SQL Server reporting database (Log Database) for use in generating reports.

Web Security Log Server and *Email Security Log Server* are Windows-only components.

Other off-appliance Web Security components

The following Web Security components, if used, must be installed off the appliance:

- Transparent identification agents (*DC Agent*, *Logon Agent*, *eDirectory Agent*, and *RADIUS Agent*).
- Remote filtering software, made up of *Remote Filtering Server* (typically installed on its own machine in the network DMZ) and *Remote Filtering Client* (which runs on user machines). Remote filtering software can be used to filter users that are outside the corporate network (e.g., traveling personnel or telecommuters).
- (Web Security Gateway Anywhere) *Sync Service*, used to send policy and user information to the hybrid service, and to return hybrid filtering reporting data to Log Server. Typically installed on the Log Server machine.

Installation steps for appliance-based solutions

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security, v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x
- V10000, V10000 G2, and V5000 G2, v7.7.x

✓ **Note**

V10000 appliances must upgraded to version 7.7 with the V-Series upgrade patch. See *Web Security or Web and Data Security upgrade outline*, page 580.

Complete the following procedures in the order in which they are listed.

1. Make sure that Microsoft SQL Server is installed and running in your network (see *Obtaining Microsoft SQL Server*, page 21).

If you intend to use SQL Server 2008 R2 Express (installed using the TRITON Unified installer), skip this step. You will install the database engine with TRITON management server components.

2. Install and configure your V-Series appliance or appliances. See *Setting Up Websense V-Series Appliances*, page 265.

> ✓ **Note**
>
> If you have already completed the appliance set up steps as described in the Websense V-Series Getting Started guide, continue with the next step.

3. Install Web Security Log Server, Email Security Log Server, or both. See:
   - *Installing Web Security components*, page 392
   - *Installing Email Security components*, page 414
4. Install TRITON Infrastructure and the management console modules appropriate to your deployment (TRITON - Web Security, TRITON - Data Security, TRITON - Email Security, or a combination of modules).

   See *Creating a TRITON Management Server*, page 180.
5. Install any additional off-appliance Web Security components. See *Installing Web Security components*, page 392.

14 Setting Up Websense V-Series Appliances

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

Setting up a Websense V-Series appliance involves the following tasks.

1. *Set up the appliance hardware*, page 266
2. *Perform initial command-line configuration*, page 270
3. *Configure the appliance*, page 274
4. *Install off-appliance or optional components*, page 298

✓ **Note**

The following sections duplicate the setup and configuration instructions in the V-Series Getting Started guide. If you have already performed those activities, continue with step 3 of *Installation steps for appliance-based solutions*, page 263.

Set up the appliance hardware

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000 G2 and V5000 G2 v7.7.x

The Quick Start poster, which is packaged in the appliance shipping box, shows you all items included in each Websense appliance shipment. The 2-page Quick Start poster explains how to set up the hardware and shows how to connect cables to the appliance and to your network.

- Access V5000 G2 poster
- Access V10000 G2 poster

Review the sections that apply to your Websense appliance model.

- *V10000 G2 hardware setup*
- *V5000 G2 hardware setup*
- *Serial port activation*

V10000 G2 hardware setup

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000 G2, v7.7.x

The appliance's network interfaces must be able to access a DNS server and the Internet, as described below. This information varies slightly depending on the security mode you choose for the appliance.

- *V10000 G2 Web mode with Web Security Gateway*
- *V10000 G2 Email mode*
- *V10000 G2: Web and Email mode with Web Security Gateway*
- *V10000 G2: Web and Email mode with Web Security (no Web gateway)*

V10000 G2 Web mode with Web Security Gateway

Network interface C must be able to access a DNS server. This interface typically has continuous access to the Internet. Essential databases are downloaded from Websense servers through interface C (or optionally through P1).

- Ensure that interface C is 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. This change must be made in the TRITON - Web Security console. 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 interface can access.

V10000 G2 Email mode

Network interface 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 E1 (and E2, if used) are able to access the download servers at **download.websense.com**.
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the E1 (and E2) interfaces can access.
- Network interface E1 (and E2, if used) must be able to access the mail server.

V10000 G2: Web and Email mode with Web Security Gateway

Network interfaces C and 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 and E1 (and E2, if used) are able to access the download servers at **download.websense.com**. (Note that some sites configure the P1 proxy interface instead of the C interface to download the Websense Master Database as well as other security updates. This change must be made in the TRITON - Web Security console. In that situation, interface C does not require Internet access.)
- Make sure the above addresses are permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C and E1 (and E2, if used) interfaces can access.
- Network interface E1 (and E2, if used) must be able to access the mail server.

V10000 G2: Web and Email mode with Web Security (no Web gateway)

Network interfaces C and 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 and E1 (and E2, if used) are able to access the download servers at **download.websense.com**.
- Make sure the above addresses are permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C and E1 (and E2, if used) interfaces can access.
- Network interface E1 (and E2, if used) must be able to access the mail server.
- Network interface N must be connected to a mirror port on a router or switch.
- If interface N is used to send blocking information, then it must be connected to a *bi-directional* mirror port. Through the bi-directional mirror port, interface N not only monitors all client traffic but also sends blocking information if needed.

V5000 G2 hardware setup

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V5000 G2 v7.7.x

The appliance’s network interfaces must be able to access a DNS server and the Internet, as described below. This information varies slightly depending on the security mode you choose for the appliance.

- *V5000 G2: Web mode with Web Security Gateway*
- *V5000 G2: Web mode with Web Security (no Web gateway)*
- *V5000 G2: Web and Email mode with Web Security (no Web gateway)*
- *V5000 G2: Email mode*

V5000 G2: Web mode with Web Security Gateway

Network interface C must be able to access a DNS server. This interface typically has continuous access to the Internet. Essential databases are downloaded from Websense servers through interface C.

- Ensure that interface C is 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. This change must be made in the TRITON - Web Security console. In that situation, interface C does not require Internet access.)

- Make sure the above addresses are permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C interface can access.

V5000 G2: Web mode with Web Security (no Web gateway)

Network interface C must be able to access a DNS server. Interface C must have continuous access to the Internet. Essential databases are downloaded from Websense servers through this interface.

- Ensure that interface C is able to access the download servers at **download.websense.com**.
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C interface can access.
- Network interface N must be connected to a mirror port on a router or switch.
- If interface N is used to send blocking information, then it must be connected to a *bi-directional* mirror port. Through the bi-directional mirror port, interface N not only monitors all client traffic but also sends blocking information if needed.

V5000 G2: Web and Email mode with Web Security (no Web gateway)

Interfaces C and 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 (and P2, if used) are able to access the download servers at **download.websense.com**.
- Make sure the above addresses are permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C and P1 (and P2, if used) interfaces can access.
- Network interface P1 (and P2, if used) must be able to access the mail server.
- Network interface N must be connected to a mirror port on a router or switch.
- If interface N is used to send blocking information, then it must be connected to a *bi-directional* mirror port. Through the bi-directional mirror port, interface N not only monitors all client traffic but also sends blocking information if needed.

V5000 G2: Email mode

Interface 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 P1 (and P2, if used) is able to access the download servers at **download.websense.com**.

- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the P1 and P2 interfaces can access.
- Network interface P1 (and P2, if used) must be able to access the mail server.

Serial port activation

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 baud rate
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance.

See *Perform initial command-line configuration*.

After firstboot is run and the command-line shell is exited, accessing the appliance command-line shell requires the admin credentials (‘admin’ and the password you set during firstboot).

Perform initial command-line configuration

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

Setting up a Websense V-Series appliance involves the following tasks. This topic covers **Step 2**:

1. *Set up the appliance hardware*, page 266
2. *Perform initial command-line configuration*, page 270
   - *Gather the data*
   - *Run firstboot*
3. *Configure the appliance*, page 274
   - *Network interface configuration*
   - *Routing configuration*
   - *Alerting*
   - *Configuring Web Security components*
4. *Install off-appliance or optional components*, page 298

The first time you start a Websense appliance and connect via the serial console, a brief script (**firstboot**) prompts you to:

- select the security mode for the appliance
- supply settings for the network interface labeled C
- enter a few other general items, such as hostname and password

You are given the opportunity to review and change these settings before you exit the **firstboot** script. After you approve the settings, the appliance mode is configured.

Later, if you want to change settings (except the security mode), you can do so through the Appliance Manager user interface.

To change the security mode, re-image the appliance with the recovery DVD shipped with your appliance, or download the recovery image for your appliance from the Websense Downloads site. Then run the **firstboot** script again.

Gather the data

Gather the following information before running the script. Some of this information may have been written down on the Quick Start poster during hardware setup.

Security mode	Choose one: Web Email Web and Email
Which Web Security subscription? (if prompted in Web mode)	Choose one: Websense Web Security Web Security Gateway Web Security Gateway Anywhere

Hostname (example: appliance.domain.com) 1 - 60 characters long. The first character must be a letter. Allowed: letters, numbers, dashes, or periods. The name cannot end with a period. If this is a Web Security Gateway appliance and Content Gateway will be configured to perform Integrated Windows Authentication, the hostname cannot exceed 11 characters (excluding the domain name). For more information, see the section titled Integrated Windows Authentication in Content Gateway Manager Help.	
IP address for network interface C	
Subnet mask for network interface C	
Default gateway for network interface C (IP address) *Optional* NOTE: If you do not provide access to the Internet for interface C, use the TRITON - Web Security console to configure P1 to download Master URL Database updates from Websense (Web mode with Web Security Gateway). Configure E1 or P1* to download antispam and antivirus database updates from Websense (Email mode). 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 TRITON - Web Security and - Email Security Help for information about configuring database downloads. * On a V5000 G2, use P1; there is no E1 interface.	
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) This password is for the following, depending on the security mode of the appliance: Web mode • Appliance Manager • TRITON - Web Security • Content Gateway Manager (for sites using Web Security Gateway / Anywhere) Email mode • Appliance Manager Web and Email mode • Appliance Manager • Content Gateway Manager (for sites using Web Security Gateway / Anywhere)	
Integration method for this appliance (for sites using Web Security). Choose one: • Standalone (Network Agent only) • Microsoft TMG • Cisco PIX • Cisco ASA • Citrix	Choose your third-party integration product (if any).
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Websense to help improve the accuracy of filtering and categorization.

Run firstboot

Run the initial command-line configuration script (**firstboot**) 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 baud rate
- 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.

   To rerun the script manually, enter the following command:

   ```
   firstboot
   ```
4. At the first prompt, select a security mode:
   - **Web**: On model V10000 G2, this mode provides Web Security Gateway. On model V5000 G2, Web mode provides either Web Security or Web Security Gateway, at your choice.
   - **Email**: provides Email Security Gateway features.
   - **Web and Email**: provides Email Security Gateway features and either Web Security Gateway (V10000 G2) or Web Security (V10000 G2 or V5000 G2).
5. Follow the on-screen instructions to provide the information collected above.

After the activation script has been completed successfully, access Appliance Manager by opening a supported browser and entering this URL in the address bar:

```
https://<IP-address-of-interface-C>:9447/appmng/
```

You are now ready to move to this step: *Configure the appliance*

Note that all Websense consoles support the following browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox versions 5 and later
- Google Chrome 13 and later

✓ **Note**

If you use Internet Explorer, ensure that Enhanced Security Configuration is switched off.

If you use Internet Explorer 8, note that Compatibility View is not supported.

Configure the appliance

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

Setting up a Websense V-Series appliance involves the following tasks. This topic covers **Step 3**:

1. *Set up the appliance hardware*
2. *Perform initial command-line configuration*
3. *Configure the appliance*
   - *Network interface configuration*
   - *Routing configuration*
   - *Alerting*
   - *Configuring Web Security components*
4. *Install off-appliance or optional components*

The V-Series Appliance Manager is a Web-based interface for the appliance. Use it to view system status, configure network and communication settings, and perform general appliance administration.

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 (some interfaces are optional in some modes). Note that on a V5000 G2, there are no E1 and E2 interfaces.

System Configuration

Access the Appliance Manager through a supported browser.

> **Important**
>
> If any Websense services are running in your network, stop all Websense services before changing the time. Then, reset the time **and** make certain that the time is consistent across all servers running Websense services. Finally, restart Websense services.
>
> If you do not stop the services first, client updates and policy changes entered after the time reset are not saved.

See the embedded Appliance Manager Help for detailed instructions on any field, or for information about other available settings.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP-address-of-C-interface>:9447/appmng
   ```

   (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**:
   - Use the **Time zone** list to select the time zone to be used on this system.

GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.

- Use the **Time and date** radio buttons to indicate how you want to set the date.

  Time is set and displayed using 24-hour notation.

  - To synchronize with an Internet Network Time Protocol (NTP) server (www.ntp.org.), select the **Automatically synchronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional.

    Important

    If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

    If interface C on this appliance is not connected to the Internet, then you must provide a way for interface C to reach an NTP server. One solution is to install an NTP server on the local network where interface C can reach it.

  - To set the time yourself, select the **Manually set** option and change the value in the Date and Time fields. Use the format indicated below the entry field.

5. Create or edit a unique **appliance description** to help you identify and manage the system, particularly when there will be multiple appliances deployed.

   The description is displayed in the appliance list in the TRITON Unified Security Center when the appliance is added there.

6. Click **OK**.

   In each section that allows changes, **OK** saves and applies the new values. **Cancel** discards changes and restores entry field values to their current settings.

7. Proceed to *Network interface configuration*.

Network interface configuration

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

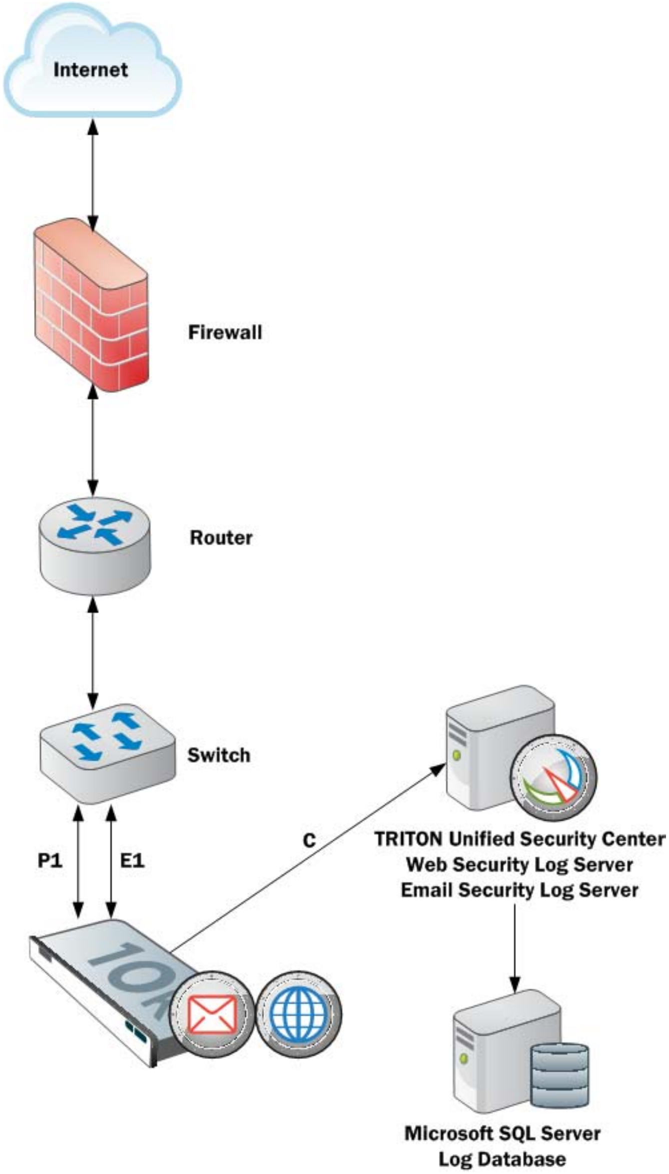
Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

Use the **Configuration > Network Interfaces IPv4** and **IPv6** pages to specify the IP address, subnet mask, default gateway, and DNS addresses for each network interface on the appliance.

- *Appliance Controller Interface (C)*
- *Websense Content Gateway Interfaces (P1 and P2)*
- *Network Agent Interface (N)*
- *Email Security Gateway Interfaces (E1 and E2, or P1 and P2)*

- *Interface bonding*



Appliances with Web Security Gateway (Anywhere) support IPv6 addresses for C, P1, P2, and N.

Appliances with Email Security Gateway **do not** support IPv6 addresses for E1 and E2.

For more information about IPv6 support, see Appliance Manager Help.

Click **OK** to save and apply new values in each section.

Appliance Controller Interface (C)

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

The Appliance Controller interface (C), already assigned during **firstboot**:

- Communicates with all Websense management interfaces
- Communicates with the Websense Data Security server
- Provides inter-appliance communication
- Transports (optionally) non-HTTP and non-HTTPS protocol enforcement
- Handles Websense Master Database downloads via the Internet (unless your site uses P1 for database downloads).

Important

Changing the C interface IP address significantly impacts the deployment and may require reinstallation of some components.

If your appliance is in production and you need to change the C interface IP address, see the embedded Appliance Manager Help system for guidance.

Guidelines for configuring network interface C

IP address (C interface)	Required. This interface typically requires continual access to the Internet, though some sites use P1 for all communication with the Internet. If you change the IP address of the C interface, the update process may take about 10 minutes. After the IP address is changed, you are redirected to a logon page. Enter your user name and password. The **Status** > **General** page will show that the services are starting up. Wait for all required services to start (optional services include: Directory Agent, State Server, Multiplexer, and TRITON - Web Security manager).
Subnet mask (C)	Required.

Default gateway (C)	Optional. IP address of the router that allows traffic to be routed outside of the subnet.
Primary DNS (C)	Required. IP address of the domain name server.
Secondary DNS (C)	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS (C)	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Websense Content Gateway Interfaces (P1 and P2)

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

The Websense Content Gateway Interfaces (P1 and P2) handle traffic directed to and from the Websense Content Gateway proxy module.

- Both the P1 and P2 proxy interfaces can be used to accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic). In other words, both interfaces can be configured to handle traffic into and out of the proxy module.
- A typical configuration is to use P1 for both inbound and outbound traffic; P2 is not used.
- Another option is to configure P1 to accept users' Internet requests (inbound only). In this case, P2 is configured to communicate with Web servers (outbound).

Important

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 the General tab of the **Configure** > **Networking** > **WCCP** page).

Guidelines for configuring network interfaces P1 and P2

General guideline	If you use both P1 and P2, and configure them in the same subnet, the default gateway is automatically bonded on P2. Ensure that outbound packets can reach the Internet.
IP address (P1 or P2 interface)	Required.
Subnet mask	Required.
Default gateway	Required. The gateway must be in the same subnet as the IP address of the interface (P1 or P2) used for communicating with the Internet (outbound traffic). If you use both P1 and P2, they must be located in the same subnet. The default gateway is automatically assigned to P2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Network Agent Interface (N)

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

Network Agent is a software component used to filter protocols other than HTTP and HTTPS. It provides bandwidth optimization data and enhanced logging detail.

Network Agent continually monitors overall network usage, including bytes transferred over the network. The agent sends usage summaries to other Websense software at predefined intervals.

Network Agent is typically configured to see both inbound and outbound traffic in your network. The agent distinguishes between:

- Requests sent from internal machines to internal machines (hits to an intranet server, for example)

- Requests sent from internal machines to external machines such as Web servers (user Internet requests, for example)

You choose whether blocking information for non-HTTP protocols is routed through interface C or interface N.

Guidelines for configuring network interface N

Select an interface to use to send blocking information for non-HTTP and HTTPS traffic	• Select **Interface C** only if you want to use interface C to send blocking information. • Select **Interface N** if network interface N is connected to a bidirectional span port, and you want to use N to transport blocking information. Blocking NIC settings configured in TRITON - Web Security do not override the settings you enter in this pane. The settings in Appliance Manager take precedence.
IP address of interface N	Optional, unless interface N is selected to transport blocking information (above), in which case it's required. Network Agent should be able to see the outbound and inbound traffic in your network. Network Agent ignores ports 80, 443, 8070, and 8080.
Subnet mask	Required if interface N is selected. Otherwise the subnet mask has a fixed value of 255.255.255.255.
Default gateway	Required if Interface N is checked. Otherwise, the field is disabled.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Network Agent can instead be installed on a different server in the network.

Email Security Gateway Interfaces (E1 and E2, or P1 and P2)

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000 G2 and V5000 G2 v7.7.x

Websense Email Security Gateway Interfaces handle traffic into and out of the Websense Email Security Gateway module. It is important that you set up interfaces

E1, E2, and C correctly before deploying off-appliance components. TRITON Unified Security Center installation cannot complete unless these interfaces are correctly configured.

> **Note**
>
> The names of the interfaces vary depending on the model of V-Series appliance.
>
> - On V10000 G2, E1 and E2 are used.
> - On V5000 G2, P1 and P2 are used.

- Both the E1 and E2 interfaces can be used to accept inbound traffic and send outbound traffic. On V5000 G2, use P1 and P2.
- A typical configuration is to use E1 (P1) for both inbound and outbound traffic; E2 (P2) is not used.
- Another option is to configure E1 (P1) to accept inbound and E2 (P2) to send outbound traffic.
- When you need to support a large volume of outbound traffic, you can configure virtual interfaces on E1 or E2 (P1 or P2).

> **Important**
>
> On the V10000 G2, if you use the E2 interface, the E1 interface is bound to eth0, and the E2 interface is bound to eth1. Keep this in mind when you configure Websense Email Security Gateway.
>
> On the V5000 G2, 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 Email Security Gateway.

Guidelines for configuring network interfaces E1 and E2

Please note the following important guidelines for configuring the E1 and E2 interfaces for Email Security:

- If you use both the E1 and E2 interfaces, it is recommended that you do not configure them in the same subnet.
- Using both E1 and E2 and locating them in the same subnet can disrupt (or even stop) mail flow, depending on your network topology. In this situation, you should examine your routing table and adjust it manually if necessary to allow network traffic to flow smoothly.

- The gateway must be in the same subnet as the IP address of the interface (E1 or E2) used for communicating with the Internet (outbound traffic). Ensure that all outbound packets can reach the Internet.

IP address (E1 or E2 interface)	Required. E1 is used by default to connect to SQL Server for reporting. If E1 does not have a valid IP address or does not have DNS access, then Email Security Gateway cannot resolve the SQL Server hostname and cannot create a connection with SQL Server. Off-box installation of the management console is then blocked. On a V5000 G2, substitute P1 for E1.
Subnet mask	Required.
Default gateway	Required. The gateway must be in the same subnet as the IP address of the interface (E1 or E2) used for communicating with the Internet (outbound traffic). If you use both E1 and E2, and you locate them in the same subnet, then the default gateway is automatically assigned to E2 (which is bound to eth1). Ensure that outbound packets can reach the Internet.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

Email Security virtual interfaces

Multiple virtual IP addresses can be configured on E1 or E2.

- Virtual IP addresses are used for outbound traffic only.
- Virtual IP addresses are bound to the specified physical interface.
- Virtual IP addresses must be in the same subnet as the specified physical interface.
- A maximum of 10 virtual IP addresses can be specified for each physical interface (E1 and E2).

Multiple virtual interfaces can be helpful to support multiple domains or a large volume of outbound traffic.

To add virtual IP addresses to E1 or E2:

1. Go to **Configuration > Network Interfaces > Virtual Interfaces** and click **Add**.
2. Select E1 or E2. If E2 has not been configured, it is not offered.
3. In the Virtual IP address entry field enter one IPv4 address per line.

4. Click **Add Interfaces**.

If you are not configuring interface bonding at this time, proceed next to *Routing configuration*.

Interface bonding

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.7.x ◆ V10000 and V10000 G2, v7.7.x	◆ *V10000/V10000 G2 with Websense Web Security only*, page 285 ◆ *V10000 G2 with Websense Email Security Gateway only*, page 286

V10000 appliances (Websense Web Security only) and V10000 G2 appliances that run one module only—Websense Web Security **or** Websense Email Security Gateway—can bond interfaces for failover or load balancing. Configuration details are provided below.

Interface bonding is not supported on V5000 G2 appliances.

Important
Do not bond interfaces that have different speeds or duplex modes. Doing so can result in performance problems.

V10000/V10000 G2 with Websense Web Security only

Interfaces E1 and E2 can be cabled to your network and then bonded through software settings to a Websense Content Gateway interface, with E1 optionally bonded to P1, and E2 optionally bonded to P2. No other pairing is possible.

Interface bonding provides these alternatives:

- Active/Standby mode: P1 (or P2) is active, and E1 (or E2) is in standby mode. Only if the primary interface fails would its bonded interface (E1 or E2) become active.
- Load balancing: If the switch or router that is directly connected to the V10000/V10000 G2 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be balanced between the primary interface and its bonded interface (E1 or E2).

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.

If you do bond an interface (P1 or P2), choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both.

Ensure that all interfaces are cabled properly before bonding. Do not bond interfaces that have different speeds or duplex modes. Doing so can result in performance problems.

V10000 G2 with Websense Email Security Gateway only

Interfaces P1 and P2 can be cabled to your network and then bonded through software settings to a Websense Email Security Gateway interface, with P1 optionally bonded to E1, and P2 optionally bonded to E2. No other pairing is possible.

Interface bonding provides these alternatives:

- Active/Standby mode: E1 (or E2) is active, and P1 (or P2) is in standby mode. Only if the primary interface fails would its bonded interface (P1 or P2) become active.
- Load balancing: If the switch or router that is directly connected to the V10000 G2 supports load balancing (etherchannel, trunk group, or similar), then traffic to and from the primary interface can be balanced between the primary interface and its bonded interface (P1 or P2).

You can choose to bond or not bond each Websense Email Security Gateway interface (E1 and E2) independently. You do not have to bond at all.

If you do bond an interface (E1 or E2), choose one mode for that bonding (either active/standby or load balancing). You do not have to choose the same bonding mode for both.

Ensure that all interfaces are cabled properly before bonding. Do not bond interfaces that have different speeds or duplex modes. Doing so can result in performance problems.

Routing configuration

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.7.x ◆ V10000, V10000 G2, and V5000 G2, v7.7.x	◆ *Configuring static routes*, page 287 ◆ *Configuring module routes*, page 289

Use the **Configuration** > **Routing** page to specify:

- Static routes from subnets and client computers through any active appliance interface, except N. If IPv6 is enabled, static IPv6 routes can also be added and imported.
- Module routes from appliance modules through appliance interface C to subnets. IPv6 module routes are **not** supported.

Configuring static routes

- Static routes can be specified for any active interface on the appliance, except N, which is dedicated to Network Agent and cannot be routed.
- The same route cannot be added for 2 different interfaces on the same module. If attempted, the appliance displays an error.
- Static routes that are defined for an interface that is later made inactive remain in the routing table, and are displayed in gray to indicate that the routes are inactive.
- Static routes that become invalid because the IP address of the interface changes are disabled and displayed in red.
- Static routes can be added and deleted, but not modified. To modify a route, delete it and add a new route specifying the new values.
- When a static route is added, imported, or deleted, the services associated with the module that manage the specified interface must be restarted. For example, if static routes are added to interface P1, when the additions are complete, all Content Gateway services must be restarted.
- The static route table has a maximum limit of 5000 entries.

Adding static routes

Static routes can be added one at a time, or many at a time using an import file.

When a static route is added, data entered in each field is validated by the appliance, and an error message is displayed if there is an inconsistency in the route.

To add static routes:

1. Go to the **Configuration > Routing** page, select the IPv4 or IPv6 tab, and click **Add/Import** under **Static Routes**.
2. **To manually add a single route**, select the **Add individual route** radio button, enter values for all fields, and then click **Add Route**.

Destination Network	Required. Specify the subnet IP address for which traffic will be routed.
Subnet Mask (IPv4) or Subnet prefix length (IPv6)	Required. The subnet mask or prefix for the network where the clients reside (such as 255.255.0.0, or 64)
Gateway	Required. IP address providing access from the proxy subnet to the client subnet. This address must be on the same subnet as the appliance.
Interface	Required. The appliance interface to be used for the static route. Only active interfaces are offered in the drop down list.

3. **To add multiple routes using an import list file**:
   a. Prepare the import file. See **Import file specifications**, below.
   b. Select the **Import route file** radio button.
   c. Specify the full path and file name, or **Browse** to locate the file. Click **Import Route** to import the routes specified in the file.

      The appliance reads the file, validates each route, and reports errors for lines that are invalid.

      Duplicate route entries are ignored; duplicate entries are not created.

      If the number of routes in the file, combined with the number of existing routes exceeds the 5000 route table limit, the import fails. No routes are added and an error message displays.

Import file specifications:

1. The file must be a plain text file. (Most routers export route tables to a plain text file.)
2. The file can contain comment lines. Comment lines begin with “#”.
3. A line that defines a route must include the following 4 fields in the order shown. Each field must be separated by a space.

   For IPv4:

   ```
   destination netmask default-gateway interface
   ```

   Destination is a subnet address or host IP address.

Netmask determines the proper value of *destination*.

Default-gateway is the next hop.

Interface is the appliance interface through which traffic is routed. The specified interface must be enabled. If it is disabled, the appliance reports an error and does not add the route.

For IPv6:

```
destination prefix-length default-gateway interface
```

Destination is a subnet address or host IP address.

Prefix-length determines the proper value of *destination*.

Default-gateway is the next hop.

Interface is the appliance interface through which traffic is routed. The specified interface must be enabled. If it is disabled, the appliance reports an error and does not add the route.

Exporting the route table

To export the route table to a text file, click **Export Table**. Use the Browse dialog to specify a location and name for the file.

All routes in the table, whether enabled or disabled, are exported.

The file is formatted as described above for import files.

Configuring module routes

In some deployments it is necessary or desirable to route some Web Security or Email Security traffic through the appliance C interface (typically Web and email traffic is routed through separate, dedicated interfaces (P1/P2, E1/E2) and C is reserved for management traffic). However, some sites might want to route authentication (or other) traffic through the C interface. This is accomplished by defining module routes on the **Configuration** > **Routing** page.

The module route table has a maximum limit of 5000 entries.

Adding a module route

1. In the Module Route section of the **Configuration** > **Routing** page, click **Add**.

2. Specify a value for each field and click **Add Route**.

Module	Required. Select a module from the drop down list. The list displays only modules installed on the appliance. The Network Agent module may be installed, but will not appear in the list.
Destination subnet	Required. Specify the subnet IP address for which traffic will be routed.
Subnet mask	Required. The subnet mask for the destination subnet.

✓ **Note**

It is the responsibility of the administrator to verify that the endpoint is available on the subnet.

Alerting

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.7.x ◆ V10000, V10000 G2, and V5000 G2, v7.7.x	◆ *Enable SNMP polling (monitoring)*, page 290 ◆ *Enable SNMP traps*, page 291 ◆ *Enable specific alerts*, page 292

Use the **Configuration** > **Alerting** page to enable and configure SNMP alerting.

There are 2 methods of SNMP alerting that you can enable on the **Setup** tab:

- Allow your SNMP manager to poll the appliance for standard SNMP counters (see *Enable SNMP polling (monitoring)*).
- Configure the appliance to send SNMP traps for selected events to your SNMP manager (see *Enable SNMP traps*).

  After enabling the SNMP trap server on the appliance, use the **Alerts** tab to configure which events cause a trap to be sent. See *Enable specific alerts*, page 292.

Enable SNMP polling (monitoring)

1. Under Monitoring Server, click **On**.

2. Select the **SNMP version** (v1, v2c, or v3) used in your network.
   - With SNMP v1 and v2c, a suffix (-wcg, -wws, -na, or -esg) is appended to the community name to indicate the originating module for the counter.
   - With SNMP v3, you can specify the context name (WCG, WWS, NA, or ESG) to poll counters for each module.
3. If you selected v1 or v2c, provide the **Community name** for the appliance, and then click **OK**.

   You have completed your SNMP monitoring configuration.
4. If you selected v3, select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.
5. If you selected a security level that includes authentication, also enter the **Password** for the selected user name, then select the **Authentication protocol** (MD5 or SHA).
6. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter and confirm the **Encryption key** used for encryption.
7. Click **OK** to implement your changes.

Enable SNMP traps

Before enabling the appliance to send SNMP traps, download the **appliance MIB file** using the link in the Trap Server section of the **Configuration > Alerting** page. The MIB file must be installed in your SNMP manager before it can interpret traps sent by the appliance.

When you are ready for the appliance to start sending SNMP traps:

1. Under Trap Server, click **On**, and then select the SNMP version (v1, v2c, or v3) used in your network.
2. For SNMP v1 or v2c, provide the following information:
   - The **Community name** to associate with traps sent by the appliance
   - The IP address and port used by your SNMP manager.
3. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **OK** to apply and save your changes. See *Enable specific alerts*, page 292, to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the community name, IP address, and port, and make sure that the network allows communication between the appliance C interface and the SNMP manager.
4. For SNMP v3, enter the **Engine ID** and **IP address** of your SNMP manager, as well as the **Port** used for SNMP communication.
5. Select the **Security level** (None, Authentication only, or Authentication and Encryption) used in your network, and the **User name** to associate with SNMP communication.

6. If you selected a security level that includes authentication, also enter and confirm the **Password** for the selected user name, then select the **Authentication protocol** (MD5 or SHA).
7. If you selected authentication and encryption, select the **Encryption protocol** (DES or AES), and then enter the **Privacy password** used for encryption.
8. To verify your configuration, click **Send Test Trap**. If the test trap succeeds, click **OK** to implement your changes. See *Enable specific alerts*, page 292, to configure which events cause a trap to be sent.

   If there is a problem sending the test trap, verify the community name, IP address, and port, and make sure that the network allows communication between the appliance and the SNMP manager.

Enable specific alerts

The appliance can send traps for each of its modules: Appliance Controller, Websense Content Gateway, Websense Web Security, Network Agent, and Email Security Gateway. The Alerts tab of the **Configuration > Alerting** page lists the alerts associated with only the modules that you have enabled.

A table for each module lists:

- The hardware or software **Event** that triggers the alert (for example, a network interface link going down or coming up, or a Websense service stopping).
- The **Threshold**, if applicable, that defines the alert condition (for example, CPU usage exceeding 90%, or free disk space reaching less than 10% of the total disk size).
- The **Type** of alert (system resource or operational event).
- Whether or not an SNMP trap is sent when the event occurs or the threshold is reached.

To enable all alerts for a module, select the check box next to **SNMP** in the table header. All check boxes in the column are selected.

Otherwise, mark the check box next to an event name to enable SNMP alerts for that event. To disable alerts for an event, clear the associated check box.

Time-based thresholds: Most of the events that have a configurable threshold also have a configurable time-based threshold, specified in minutes. When the time-based threshold is set and both thresholds are exceeded, an alert is sent. To enable time-based thresholds, select the **Enable time-based thresholds** check box at the top of the page. The time-based threshold is enabled on every event for which it is configurable.

Event-cleared alerts: In addition to generating event condition alerts, you can configure alerts to be sent when conditions return below the threshold. These are called **event-cleared alerts**. To enable event-cleared alerts, select the **Generate event-cleared alerts** check box at the top of the page.

The following events do not generate event-cleared alerts:

- Hostname change
- IP address change
- Scheduled backup failure
- SNMP authentication failure

When you have finished configuring alerts, click **OK** to implement the changes.

Proceed next to *Configuring Web Security components*.

Configuring Web Security components

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ V10000, V10000 G2, and V5000 G2, v7.7.x	◆ *What is a policy source?*, page 294 ◆ *What if an appliance is not the policy source?*, page 295 ◆ *User directory with V-Series appliances*, page 296 ◆ *Redundancy*, page 297

Use the **Configuration > Web Security Components** page to specify which Web Security components are active on the appliance, and where the appliance gets Web Security global configuration and filtering policy information. Also define the TRITON - Web Security location.

- Under **Policy Source**, select which Web Security configuration is used on this appliance: **Full policy source** (default; see *What is a policy source?*), **User directory and filtering**, or **Filtering only** (see *What if an appliance is not the policy source?*). If this is a Full policy source appliance, it acts as both the Policy Broker and a Policy Server. There can be only 1 Full policy source appliance in your network.
- If this is a User directory and filtering appliance, it also acts as a Policy Server. Enter the IP address of the Policy Broker appliance or server.
- If this is a Filtering only appliance, enter the IP address of a Policy Server. It does not have to be the IP address of the Policy Broker machine.

1. Click **OK** to save and apply your changes.

2. If this is a Web Security only (or Web Security Gateway only) appliance running as a Full policy source, under **Web Security Components** > **TRITON - Web Security**, specify whether to use the TRITON instance installed **On** the appliance, or whether to use an **Off**-appliance instance.

> ✓ **Note**
>
> When you upgrade from an earlier version of the appliance, your previous settings are preserved. If you do not have an off-appliance management console location already established, the system uses TRITON - Web Security on the policy source appliance by default.

   - If you are using Websense Data Security or Email Security Gateway in conjunction with Websense Web Security Gateway, the TRITON Unified Security Center must be installed on a Windows Server 2008 R2 64-bit machine.
   - Generally, the on-appliance installation of TRITON - Web Security is intended for evaluations and small deployments. Most production sites are advised to download the TRITON installer from mywebsense.com and install the TRITON console on a separate Windows server.

3. If you are moving from using an off-appliance TRITON - Web Security instance to using the on-appliance instance, make sure you have backed up your original TRITON console. Then expand **Import Configuration** and browse to the location of your backup file.

   This allows you to move much of your existing configuration and policy information to the appliance, rather than having to recreate your settings.

   As always, be sure to verify the configuration in the new TRITON console, as some settings may not be preserved during migration.

4. Click **OK** to save and apply your changes.

What is a policy source?

Every Websense Web Security deployment must include a single **policy source**. This is an appliance or other server that hosts 2 components: Websense Policy Broker and Websense Policy Database. All other Websense appliances or other servers point to this machine and receive regular updates from it. This appliance (or other server) is called the **policy source**.

- When a Web Security only appliance (or Web Security Gateway only appliance) is configured as a policy source, all available Web Security components run on that appliance, including.
  - Filtering Service
  - Policy Database
  - Policy Broker
  - Policy Server

  - User Service
  - Directory Agent (required only for hybrid service)
  - State Server (optional)
  - Multiplexer (optional)
  - Usage Monitor
  - Control Service
  - TRITON - Web Security (optional)
    - Reports Information Service
    - Investigative Reports Scheduler
    - Manager Web Server
    - Reporting Web Server
    - Central Access
    - Unified Security Center
    - Settings Database
  - Websense Content Gateway module (only with Web Security Gateway)
  - Network Agent module (required for Web Security; optional for Web Security Gateway)

  Windows-only services, like Log Server, and optional services, like transparent identification agents, still run on other machines.

- When a policy source appliance runs in **Web and Email Security** mode (hosting Websense Web Security Gateway and Email Security Gateway), the TRITON services are disabled by default.
- A non-appliance policy source is a server hosting **Policy Broker**. The Policy Database is automatically created and run on the Policy Broker machine. This machine typically also includes a Policy Server instance, and may include additional Websense software components.

The Policy Database holds all filtering policies (including client definitions, filters, and filter components) for all appliances and all domains in the network. It also holds global configuration information that applies to the entire deployment.

What if an appliance is not the policy source?

A Websense V-Series appliance that is not serving as the policy source can be designated to run either **User directory and filtering** or **Filtering only**.

- A **User directory and filtering** appliance is a lightweight version of the policy source machine. It runs:
  - Policy Server
  - User Service
  - Usage Monitor
  - Filtering Service
  - Control Service

    - Directory Agent
    - Websense Content Gateway module (if Web Security Gateway is used)
    - Network Agent module (required for Web Security; optional for Web Security Gateway)

  Having User Service and Policy Server on remote appliances means that you are able to obtain local network user names. Latency between User Service and Policy Server is eliminated, because both run on the same appliance.

  Whenever you make a policy change, that change is immediately updated on the policy source appliance. The change is pushed out to user directory and filtering appliances within 30 seconds.

  These appliances can continue filtering for as long as 14 days if their connection with the policy source machine is interrupted. So even if a network connection is poor or is lost, filtering continues as expected.

  A **User directory and filtering** appliance is configured to point to the full policy source for updates.

- A **Filtering only** appliance does not run Policy Server. It runs only:
    - Filtering Service
    - Control Service
    - Websense Content Gateway module (if Web Security Gateway is used)
    - Network Agent module (required for Web Security; optional for Web Security Gateway)

  A **Filtering only** appliance is configured to point to a Policy Server. This works best when the appliance is close to the Policy server and on the same network.

  These appliances require a continual connection to the centralized Policy Server, not only to stay current, but also to continue filtering. If the connection to the Policy Server becomes unavailable for any reason, filtering on a **Filtering only** appliance can continue for up to 3 hours.

  If the Policy Server machine is on a remote network, with a WAN connection, it can be difficult to obtain user name/IP address maps for the local users.

User directory with V-Series appliances

If your organization relies on user identification or authentication, each appliance that is running Websense User Service must be configured to talk to a user directory. Multiple appliances can talk to the same user directory, or to different user directories.

Preparing for a hybrid configuration

In Web Security Gateway Anywhere environments, some users may be filtered by the hybrid (SaaS) service. In this situation, an interoperability component on the appliance called **Directory Agent** is required to enable user-, group-, and domain- (OU) based filtering.

Directory Agent must be able to communicate with:

- A supported LDAP-based directory service:

    - Windows Active Directory® (Mixed Mode)
    - Windows Active Directory (Native Mode®)
    - Oracle (Sun Java™) System Directory
    - Novell eDirectory
- Websense **Sync Service**

After deployment, use TRITON - Web Security to configure User Service and Directory Agent.

- User Service configuration is performed on the Settings > General > Directory Services page.
- Directory Agent configuration is performed on the Settings > Hybrid Configuration > Shared User Data page.
    - You can have multiple Directory Agent instances.
    - Each Directory Agent must use a unique, non-overlapping root context.
    - Each Directory Agent instance must be associated with a different Policy Server.
    - All Directory Agent instances must connect to a single Sync Service. (A deployment can have only one Sync Service instance.)
    - You must configure the Sync Service connection manually for all supplemental Directory Agent instances (these are the Directory Agents running on User Directory and filtering, and Filtering only appliances). Communication is configured automatically for the Directory Agent instance that connects to the same Policy Server as Sync Service. See the TRITON - Web Security Help for details.

You can configure Directory Agent to use a different root context than User Service, and to process its directory data differently than User Service. Also, with Windows Active Directory, if User Service is configured to communicate with multiple global catalog servers, Directory Agent can communicate with all of them.

Redundancy

Internet usage filtering requires interaction between several Websense software components:

- User requests for Internet access are proxied by Content Gateway.
- User requests for Internet access may also be monitored by Network Agent.
- The requests are sent to Websense Filtering Service for processing.
- Filtering Service communicates with Policy Server and Policy Broker to apply the appropriate policy in response to the request.

In some networks, additional machines may be used to deploy additional instances of Content Gateway, Filtering Service, Network Agent, or other components. For example, in a large, segmented network, you may need a separate Network Agent for each segment. Or, you might deploy the Remote Filtering Server on a separate computer, to enable filtering of laptops and other computers that are outside the organization's network.

Check the Websense Deployment and Installation Center for component distribution options. Contact your Websense Sales Engineer, or your authorized Websense reseller, for assistance in planning a more complex deployment.

Install off-appliance or optional components

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

Setting up a Websense V-Series appliance involves the following tasks. This topic covers **Step 4**:

1. *Set up the appliance hardware*
2. *Perform initial command-line configuration*
3. *Configure the appliance*
    - *Network interface configuration*
    - *Routing configuration*
    - *Alerting*
    - *Configuring Web Security components*
4. *Install off-appliance or optional components*

After the appliance has been configured, install the off-appliance components you want. Follow the links for your deployment in *Installation steps for appliance-based solutions*, page 263

Note

Before deploying off-appliance components, be sure to use Appliance Manager to configure the appliance interfaces that you plan to use [C, P1, P2 (optional), E1, and E2 (optional)].

At sites using **Email Security Gateway**, E1 is used by default to connect to SQL Server for reporting. If E1 does not have a valid IP address or does not have DNS access, then Email Security Gateway cannot resolve the SQL Server hostname and cannot create a connection with SQL Server. In that situation, off-box installation of the management console is blocked. [On a V5000 G2, substitute P1 for E1.]

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.

Note

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 machines in your network.

Creating a TRITON management server

Important

The appliance must be set up and configured before you create a TRITON management server. If you have not done so already, complete the following procedures before creating a TRITON management server:

- *Set up the appliance hardware*, page 266
- *Perform initial command-line configuration*, page 270
- *Configure the appliance*, page 274

The machine on which **TRITON Unified Security Center** is installed is referred to as the **TRITON management server**. To install TRITON management server, follow the link in *Installation steps for appliance-based solutions*, page 263.

Restoring to Factory Image

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security v7.7.x
- Web Security Gateway and Web Security Gateway Anywhere v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere v7.7.x
- V10000, V10000 G2, and V5000 G2 v7.7.x

USB Image

Beginning with v7.7.3, V-Series appliances no longer ship with a recovery DVD. The recovery image is available to download and install from a USB flash drive. The recovery image can be downloaded from MyWebsense. Once the image is downloaded, it must be burned to a USB flash drive. For instructions on how to create the USB drive image, please see the article in the Websense Technical Library.

DVD Image

Prior to the release of v7.7.3, the V10000, V10000 G2, and V5000 G2 shipped with a recovery DVD that can be used to restore the appliance to its factory image. This recovery procedure should be used only if you need to roll back your installation to a previous version. You can use the DVD (after saving a Full configuration backup) to re-image the appliance and then recover your custom appliance and module settings.

> **Important**
>
> Use the original recovery DVD that came with your appliance. If you have misplaced it, you can download a DVD image from MyWebsense. It is important you use an image that is associated with the manufacture date of your appliance. The MyWebsense Downloads page will indicate the appliance manufacture date appropriate for each image.

Note that all Websense components running off the appliance must be stopped before you reset to factory image.

1. Stop all Websense components that are running off the appliance. For example, stop Web Security or Email Security Log Servers, Sync Service, Linking Service, transparent ID agents, and TRITON Unified Security Center.
2. If possible, back up any information you want preserved.
   a. Using a Web browser, log onto the Appliance Manager:

      ```
      https://<C interface IP address>:9447/appmng/
      ```

   b. Go to **Administration > Backup Utility**, and create a Full Configuration backup. See online Help for assistance. Save this backup file to another machine.
3. Go to the machine rack and insert the recovery disk into the appliance DVD drive.
4. Reboot the appliance. (An alternative is to turn off the power, and then turn it on again.)
5. Watch the terminal screen closely after the reboot starts. When a list of function keys appears at the upper right during reboot, press **F11.** Then select one of the following:
   - **Boot from SATA Optical** drive (V10000 G2)
   - **Boot from Embedded SATA 1 TEAC DVD-ROM DV-28SW** drive (V5000 G2)
   - **Boot from Primary CDROM: TEAC DVD-ROM DV-28SW** drive (V5000 G2R2)
6. When asked whether you want to continue, enter **yes**.

   Restoring the image can take 20 minutes or more. When the DVD is ejected, be sure to remove it from the drive.
7. Press any key to view the subscription agreement.
8. Enter **yes** to accept the subscription agreement, and then enter **yes** to begin firstboot.

   This begins the **firstboot** script.
9. Follow the on-screen instructions at the terminal and provide the necessary information.

   See *Perform initial command-line configuration* for details about what information is requested.

Restore backed-up configuration

1. Restore the backed up configuration via the Appliance Manager.
    a. Using a Web browser, log onto the Appliance Manager

    ```
    https://<C interface IP address>:9447/appmng
    ```

    b. Go to **Administration > Backup Utility**.

    c. Choose **Restore**.
2. Select **Full Appliance Configuration** restore mode and click **Run Restore Wizard**.
3. In the Restore Wizard:
    a. File Location: Select **Another location (browse for file)**. Then click **Next**.

    b. Select File: **Browse** to the backup file (*.bak file) to select it. Then click **Next**.

    c. Confirm: Verify backup file details and then click **Restore Now**.

    The appliance will be rebooted automatically after the restore is complete. Appliance and software module settings are restored.
4. Ensure that the appliance time and date are synchronized with other servers.
5. Restart the components that run off the appliance.
6. On occasion, a manual download of the Websense Web Security Master Database should be initiated after a recovery. Do this in the TRITON Unified Security Center (Web Security module) if you receive a warning message about the Master Database.

15 Installing Data Security Solutions

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Deployment*, page 304 ◆ *Installation*, page 306

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.

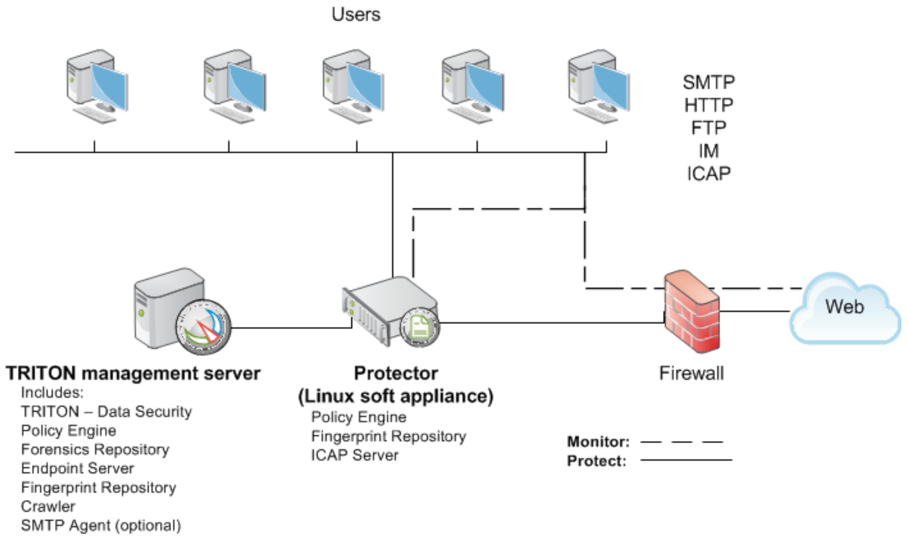
Optionally, the protector works in tandem with the Data Security Management Server. The Data Security Management Server performs discovery (performed by Crawler) and provides advanced analysis capabilities. The protector sits in the network, intercepts and analyzes traffic, and can either monitor or 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.

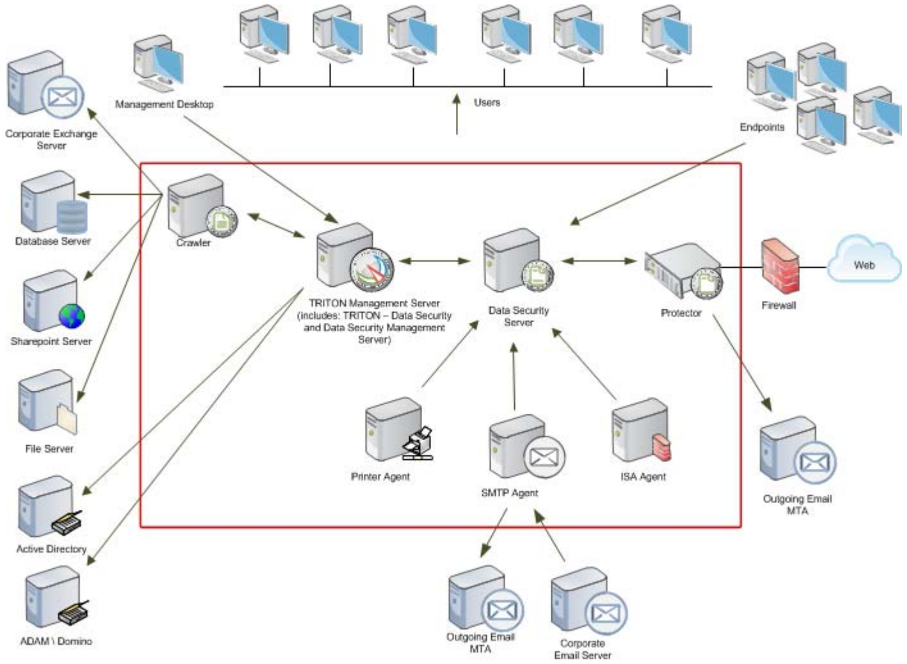
Websense Data Security *agents* are also an integral part of the system. These agents are installed on the relevant servers (the ISA agent on the Microsoft ISA server, printer agent on the print server, etc.) to enable Data Security to access the data necessary to analyze the traffic from these servers. 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.

Deployment

A basic deployment might have 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.

For diagrams of the most common customer deployments, see *Most common deployments*, page 112.

Before you deploy 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 103
2. *Determining where your confidential data resides*, page 105
3. *Determining your information flow*, page 106
4. *Defining the business owners for the data*, page 106
5. *Deciding who will manage incidents*, page 107
6. *Planning access control*, page 107
7. *Analyzing network structure*, page 108
8. *Planning network resources*, page 109
9. *Planning a phased approach*, page 121

For additional deployment information, see:

- *Integrating Data Security with Existing Infrastructure*, page 125
- *Scaling Data Security*, page 157

Installation

For best practice, before installing Websense Data Security, you should obtain and install Microsoft SQL Server (*Obtaining Microsoft SQL Server*, page 21) and read the considerations described in *Preparing for installation*, page 14.

Data Security installation involves 3 basic steps.

1. *Installing TRITON Unified Security Center*, page 181

   This includes the TRITON infrastructure and TRITON Console. 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.
2. *Installing TRITON - Data Security*, page 187. You are automatically prompted to do this when you install the TRITON Unified Security Center with Data Security selected.

   This includes the Data Security Management Server—a policy engine, crawler, fingerprint repository, and when applicable, an SMTP agent, and endpoint server.
3. *Installing Data Security components*, page 413. If desired, you can install one or more optional components for monitoring things like print servers, ISA/TMG servers, endpoint machines. You can also install extra Data Security servers and crawlers for system scaling.

Websense Data Security supports installations over Virtual Machines (VM), but Microsoft SQL Server must be present to support the incident and policy database. See *Installing Data Security on a virtual machine*, page 306 for details.

Installing Data Security on a virtual machine

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 for this version*, page 2, 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. • An additional 55 MB free on the destination drive during installation • 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 • 8GB RAM • 150 GB Disk • 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

✓ **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.

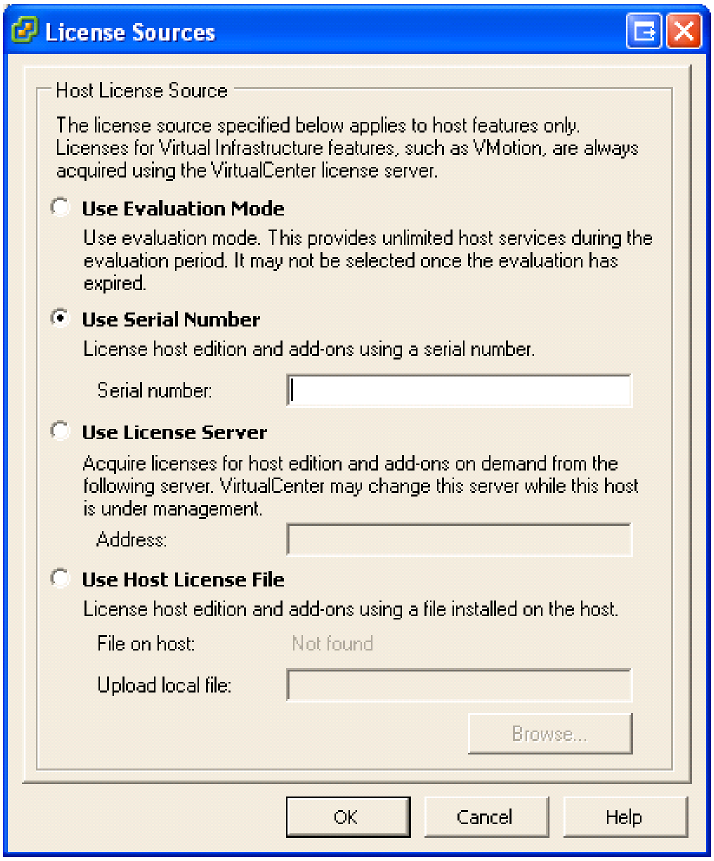
Installing the license and setting the time

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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.



License Sources

Host License Source

The license source specified below applies to host features only. Licenses for Virtual Infrastructure features, such as VMotion, are always acquired using the VirtualCenter license server.

○ **Use Evaluation Mode**

Use evaluation mode. This provides unlimited host services during the evaluation period. It may not be selected once the evaluation has expired.

● **Use Serial Number**

License host edition and add-ons using a serial number.

Serial number:

○ **Use License Server**

Acquire licenses for host edition and add-ons on demand from the following server. VirtualCenter may change this server while this host is under management.

Address:

○ **Use Host License File**

License host edition and add-ons using a file installed on the host.

File on host: Not found

Upload local file:

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

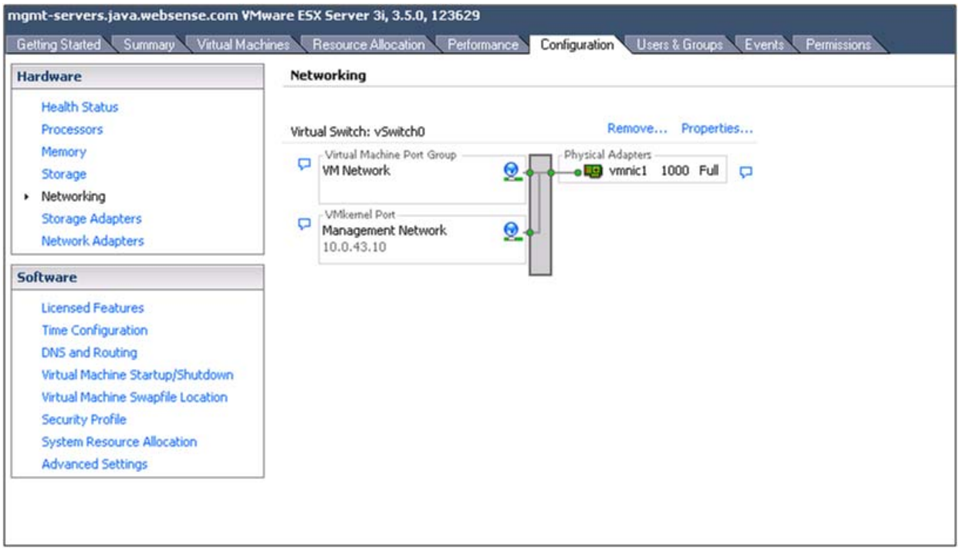
Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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.



mgmt-servers.java.websense.com VMware ESX Server 3i, 3.5.0, 123629

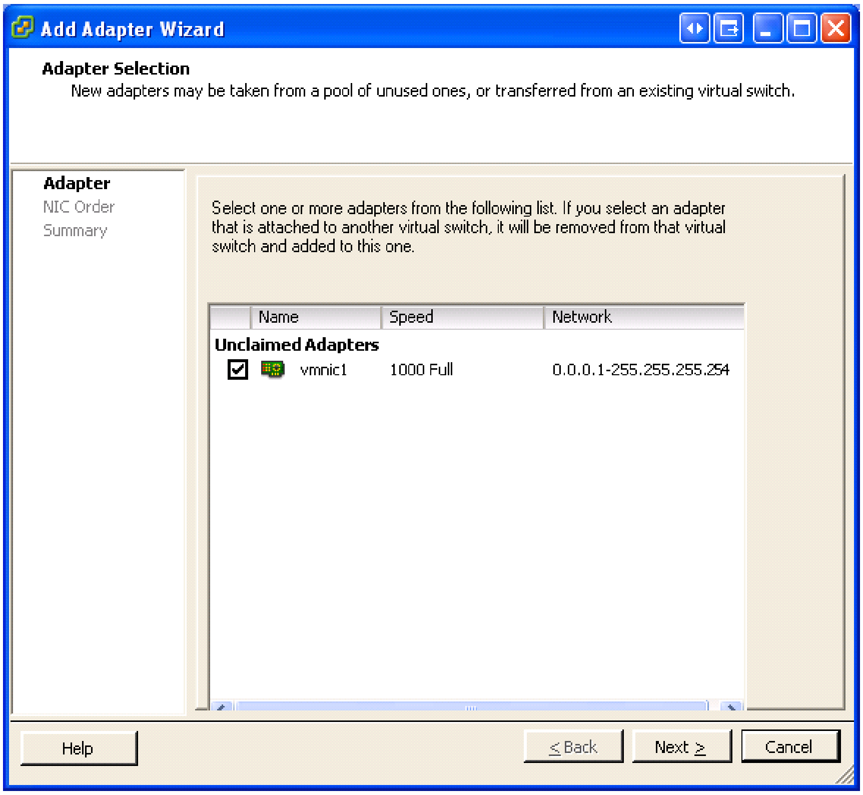
Virtual Switch: vSwitch0

Virtual Machine Port Group: VM Network

Physical Adapters: vmnic1 1000 Full

VMkernel Port: Management Network 10.0.43.10

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.



Add Adapter Wizard

Adapter Selection

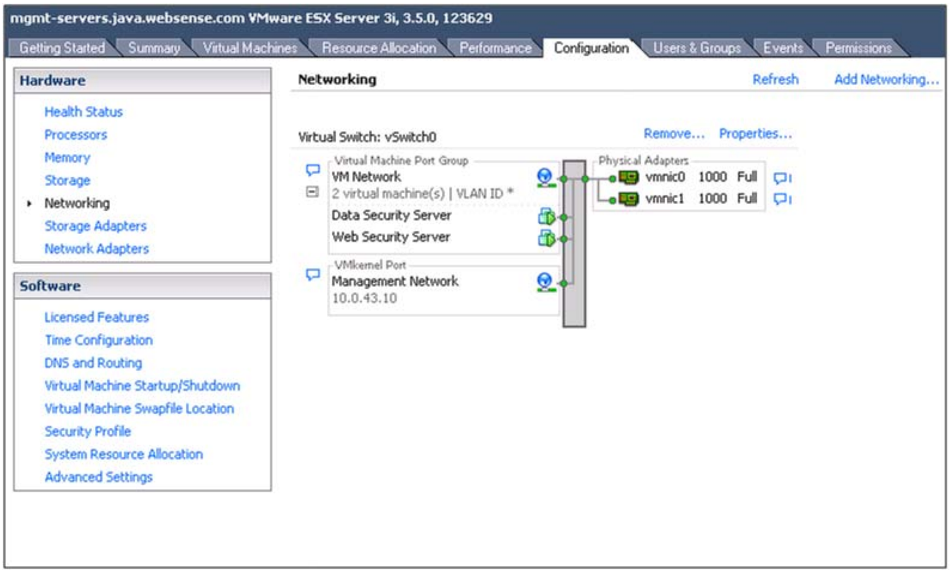
New adapters may be taken from a pool of unused ones, or transferred from an existing virtual switch.

Select one or more adapters from the following list. If you select an adapter that is attached to another virtual switch, it will be removed from that virtual switch and added to this one.

	Name	Speed	Network
Unclaimed Adapters			
☑	vmnic1	1000 Full	0.0.0.1-255.255.255.254

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:



Virtual Switch: vSwitch0

Virtual Machine Port Group
VM Network
2 virtual machine(s) | VLAN ID *
Data Security Server
Web Security Server

VMkernel Port
Management Network
10.0.43.10

Physical Adapters

vmnic0	1000	Full
vmnic1	1000	Full

Creating the Data Security virtual machine

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 Microsoft Windows Server 2008 R2 (64 bit).
6. Click **Next**.
7. Set the number of virtual processors according to the TRITON management server for your deployment, and click **Next**. See *System requirements for this version*, page 2, for more information.
8. Set the virtual machine memory to a minimum of 8 GB, depending on your deployment, and click **Next**. See *System requirements for this version*, page 2, for more information.
9. Accept the defaults on the Network page and the I/O Adapters page, clicking **Next** to continue.
10. Select **Create a new virtual disk** and click **Next**.
11. Set the disk capacity to150 GB.
12. Click **Next** to progress through the Advanced Options page without changing the defaults.
13. 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 180, to install the TRITON management server on your virtual machine.

16 Installing Data Security Components

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Once you've installed Data Security on the TRITON management server (as described in *Creating a TRITON Management Server*, page 180), you can install other Data Security components as needed. In larger deployments, you might install supplemental Data Security servers, crawlers, or policy engines. In some scenarios, you might install the Data Security protector and/or any number of Data Security agents such as the printer agent for monitoring printer output or ISA agent for monitoring data on Microsoft ISA servers.

Data Security 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. The Data Endpoint agent enables administrators to analyze content within a user's working environment (PC, laptop, etc.) and block or monitor policy breaches.

Important

If you plan to install a Data Security component—for example, a supplemental server or agent—TRITON Unified Security Center must already be installed in your network along with the Data Security Management Server software.

Do not install any Data Security component on a domain controller.

- *Installing supplemental Data Security servers*, page 316
- *Installing Data Security agents*, page 321

Installing supplemental Data Security servers

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Operating system support*, page 316 ◆ *Hardware requirements*, page 317 ◆ *Software requirements*, page 317 ◆ *Required ports*, page 318 ◆ *Installation steps*, page 318

Medium to large enterprises may require more than one Data Security server to perform content analysis efficiently. Having multiple Data Security servers allows your organization to grow, improves performance, and allows for custom load balancing.

Supplemental Data Security server installations include:

- A policy engine
- SMTP agent (Windows Server 2003 installations only)
- Secondary fingerprint repository (the primary is on the management server)
- Endpoint server
- Optical Character Recognition (OCR) server
- Crawler

✓ **Notes:**
In production environments, do not install a Data Security server on a Microsoft Exchange, ISA, or print server. These systems require abundant resources.

Operating system support

Supplemental Data Security servers must be running on one of the following operating system environments:

- Windows Server 2003 (32-bit) Standard or Enterprise R2 SP2
- Windows Server 2008 (64-bit) Standard or Enterprise R2

Hardware requirements

Supplemental Data Security servers must meet the following hardware requirements.

Server hardware	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	4 GB	8 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

Software requirements

The following requirements apply to all Data Security servers:

- For optimized performance, 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 host 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 your deployment includes more than one Data Security Server, use a domain account (preferred), or the use same local user name and password on each machine.
  - Be sure to set the system time accurately on the TRITON management server.

Required ports

The following ports must be kept open for supplemental Data Security servers:

Outbound

To	Port	Purpose
Data Security Management Server	17443	Incidents
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Inbound

From	Port	Purpose
Data Security Management Server	8892	Syslog
Data Security Management Server	139	File sharing
Data Security Management Server	445	File sharing
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Installation steps

1. Download the Websense installer (**WebsenseTRITON77Setup.exe**) from mywebsense.com.
2. Launch the installer on the machine where you want to install the supplemental server.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the server software.

   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:.

8. On the **Select Components** screen, select **Data Security Server**.
9. The **Fingerprinting Database** screen appears. To choose a location other than the default shown, use the **Browse** button.
10. The **Virtual SMTP Server** screen appears. This is because an SMTP agent is included with supplemental Data Security server installations.

    In the **Select Virtual Server** list, select the IIS virtual SMTP server that should be bound to the SMTP agent. The 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.

    (See *Preparing a machine for the SMTP agent*, page 357 for instructions on installing Microsoft IIS from Control Panel and configuring inbound and outbound SMTP Virtual Servers.)
11. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
12. In the **Register with the Data Security Server** screen specify the location and log on credentials for the TRITON management server.

    FQDN is the fully-qualified domain name of a machine. The credentials should be for a TRITON - Data Security administrator with System Modules permissions.
13. In the **Local Administrator** screen, supply a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters. If you are installing Data Security v7.7.0, this password cannot exceed 19 characters. If you are installing version 7.7.2 or beyond, password length doesn't matter.
14. If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, 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.

15. 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.

16. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.

17. Log onto TRITON - Data Security and click **Deploy** to fully connect the supplemental server with the management server.

Installing Data Security agents

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Below is a summary of the Data Security agents.

With the exception of the protector, mobile agent, and Data Endpoint, Data Security agents are installed using the Custom option of the standard Websense installer.

Note that the various agents 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 wizard knows this and lists the ISA agent as an option that you can install.

Click the links to learn more about each agent, including where to deploy it, installation prerequisites, installation steps, special considerations, and best practices.

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). Note: For HTTPS traffic, the protector works with a Web proxy such as Websense Content Gateway. See *Protector*, page 324 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 See *SMTP agent*, page 355 for more information.
ISA/TMG agent	The ISA agent receives all Web (HTTP or HTTPS) connections from a Microsoft ISA or Forefront TMG 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. See *Microsoft ISA/TMG agent*, page 362 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. See *Installing and Deploying Websense Endpoint Clients*, page 421 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. See *Printer agent*, page 365 for more information.
Web Content Gateway	A Data Security policy engine is embedded in Websense Content Gateway. No agent installation is required; however, the policy engine is not active until registered with a TRITON management server. See Content Gateway Help for registration instructions.
Email Security Gateway	A Data Security policy engine is embedded in Email Security Gateway. No agent installation is required; however, the policy engine is not active until registered with a TRITON management server. See the TRITON - Email Security Help for registration instructions.

Agent	Description
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. See *Mobile agent*, page 339 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. See *Integration agent*, page 372 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. See *The crawler*, page 375 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.

Protector

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	

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 Active (blocking) bridge
SMTP	Monitoring passive Mail Transfer Agent (MTA)	Monitoring bridge Mail Transfer Agent (MTA)
All Others	Monitoring	Monitoring
ICAP	Monitoring Blocking	Monitoring Blocking

✓ **Note**

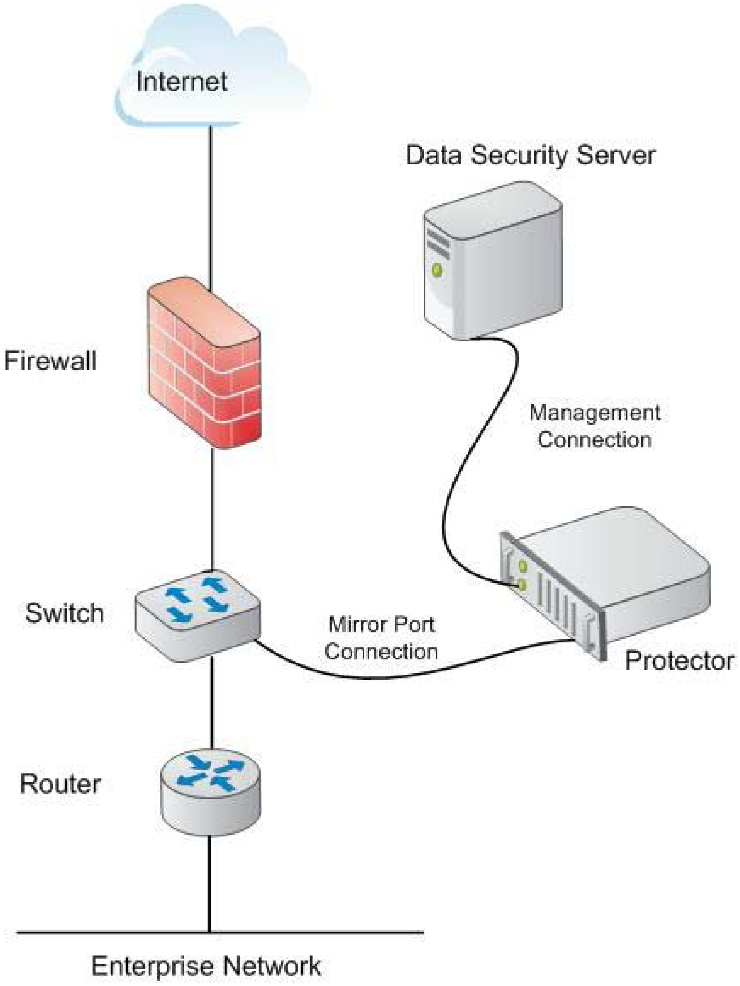
In both inline/bridge and SPAN/mirror port topology, Websense Data Security can be integrated with Web proxies. Blocking and monitoring modes are both available.

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.

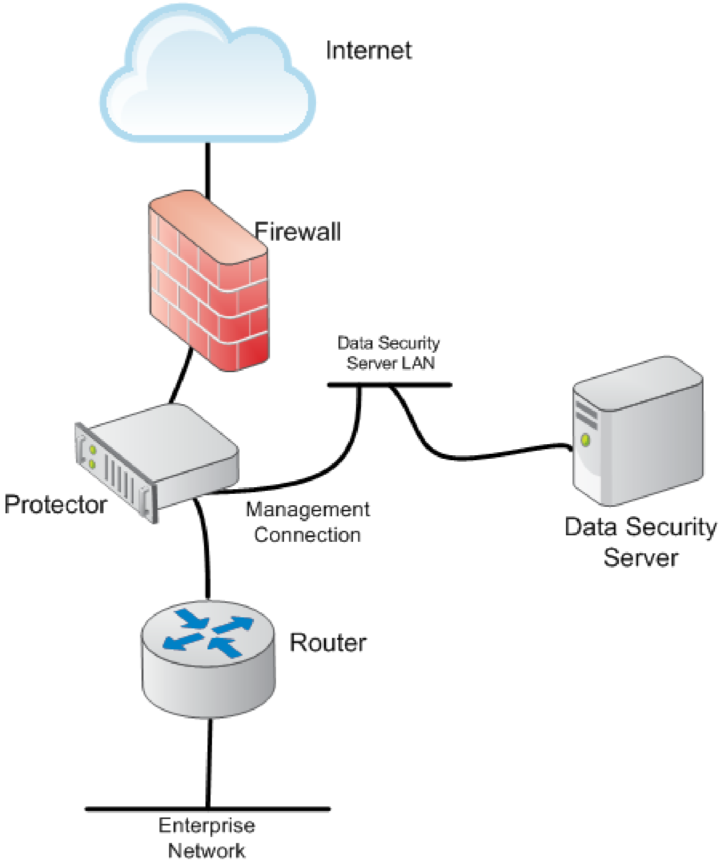
When using the Websense Protector in inline mode, the hardware and software failsafe mechanism is available only when using the certified bypass-server adapter NIC.

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.

Hardware requirements

The protector is a soft appliance. If you are using your own hardware, it must meet the following 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

Protector	Minimum requirements	Recommended
Hardware RAID	1	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.

Required ports

The following ports must be kept open for the protector:

Outbound

To	Port	Purpose
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Next hop MTA	25**	SMTP
Websense Web Security	56992	Linking Service
Other	UDP 123	Inbound/ outbound NTPD (available on the appliance yet disabled by default)

* This range is necessary for load balancing.
** Explicit MTA

Inbound

From	Port	Purpose
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Anywhere (including TRITON - Data Security)	22	SSH access
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Explicit MTA	25**	SMTP
Explicit MTA	10025**	SMTP, mail analysis

* This range is necessary for load balancing.
** Explicit MTA

If you are connecting third-part software such as a Web proxy through ICAP, the ICAP client should keep the following ports open:

Outbound

To	Port	Purpose
Protector	1344	Receiving ICAP traffic

Inbound

None

Installing the protector software

Installing the Data Security protector comprises 3 basic steps:

1. *Configuring the network*, page 331
2. *Installation steps*, page 331
3. Configure the protector in the TRITON Unified Security Center. See *Final step: Verification*, page 336.

Protector installations include:

- A policy engine
- ICAP client - for integration with third-party solutions that support ICAP, such as some Web proxies.
- Secondary fingerprint repository (the primary is on the management server)

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 *Protector*, page 721).

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.

Installation steps

You access the installation wizard for your protector through a command line interpreter (CLI). (See *Data Security Protector CLI*, page 791 for a reference guide.)

To install the protector, do the following:

1. If you have purchased the Websense V5000 G2 Data Security Appliance, 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 protector software is provided on an ISO image. Download the image, **WebsenseDataSecurityProtector77x.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 *admin* for both.

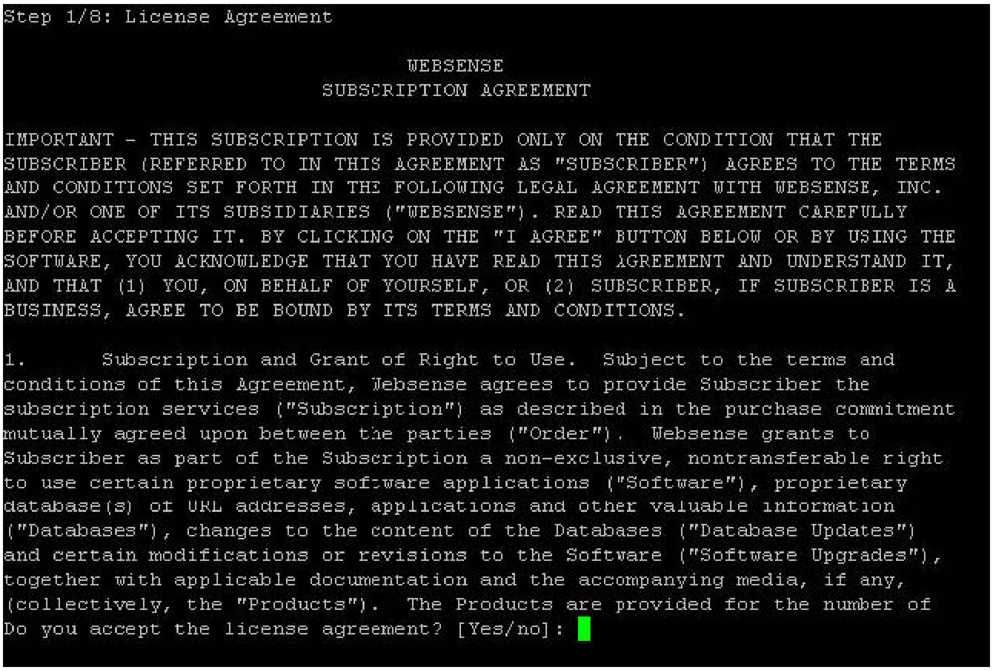
When the protector CLI opens for the first time, logging in as admin automatically opens the installation wizard. On subsequent attempts, type “wizard” at the command prompt to access the wizard.

3. 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 326. For more information on deploying the protector in a SPAN/mirror port configuration, see *Deploying in SPAN/mirror port configuration*, page 325.
4. 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 1/8: License Agreement

                                 WEBSENSE
                          SUBSCRIPTION AGREEMENT

IMPORTANT - THIS SUBSCRIPTION IS PROVIDED ONLY ON THE CONDITION THAT THE
SUBSCRIBER (REFERRED TO IN THIS AGREEMENT AS "SUBSCRIBER") AGREES TO THE TERMS
AND CONDITIONS SET FORTH IN THE FOLLOWING LEGAL AGREEMENT WITH WEBSENSE, INC.
AND/OR ONE OF ITS SUBSIDIARIES ("WEBSENSE"). READ THIS AGREEMENT CAREFULLY
BEFORE ACCEPTING IT. BY CLICKING ON THE "I AGREE" BUTTON BELOW OR BY USING THE
SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND IT,
AND THAT (1) YOU, ON BEHALF OF YOURSELF, OR (2) SUBSCRIBER, IF SUBSCRIBER IS A
BUSINESS, AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1.      Subscription and Grant of Right to Use.  Subject to the terms and
conditions of this Agreement, Websense agrees to provide Subscriber the
subscription services ("Subscription") as described in the purchase commitment
mutually agreed upon between the parties ("Order").  Websense grants to
Subscriber as part of the Subscription a non-exclusive, nontransferable right
to use certain proprietary software applications ("Software"), proprietary
database(s) of URL addresses, applications and other valuable information
("Databases"), changes to the content of the Databases ("Database Updates")
and certain modifications or revisions to the Software ("Software Upgrades"),
together with applicable documentation and the accompanying media, if any,
(collectively, the "Products").  The Products are provided for the number of
Do you accept the license agreement? [Yes/no]:
```

STEP 2: Select the hardware to install and confirm hardware requirements

Data Security checks to see if your hardware meets the following requirements:

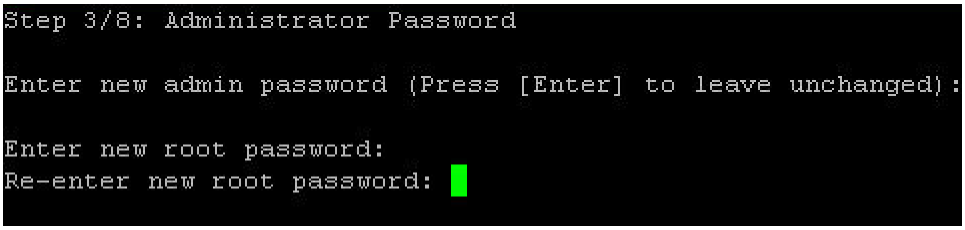
- 2 GB RAM
- 4 CPU

- 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 3/8: Administrator Password

Enter new admin password (Press [Enter] to leave unchanged):

Enter new root password:
Re-enter new root password:
```

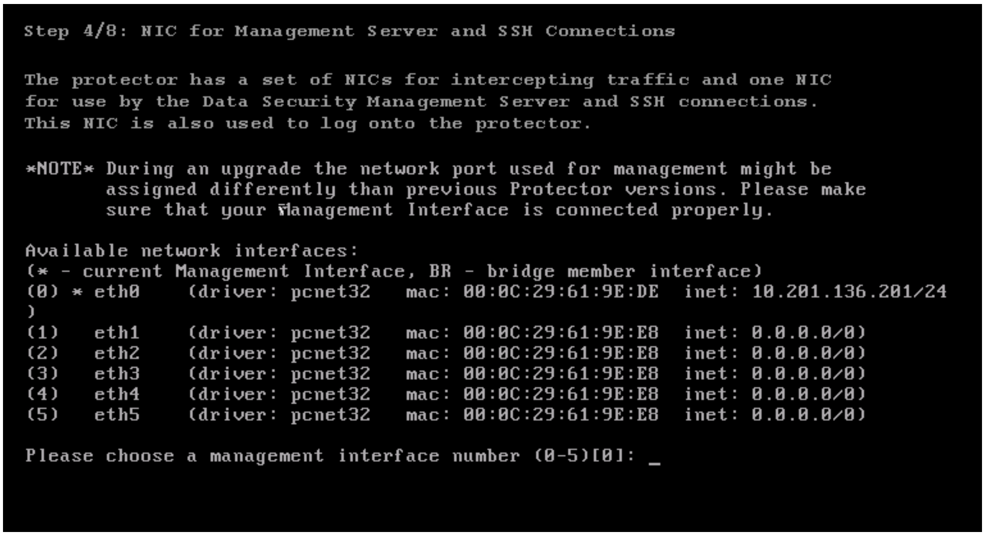
STEP 4: Set the NIC for management server and SSH connections

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.

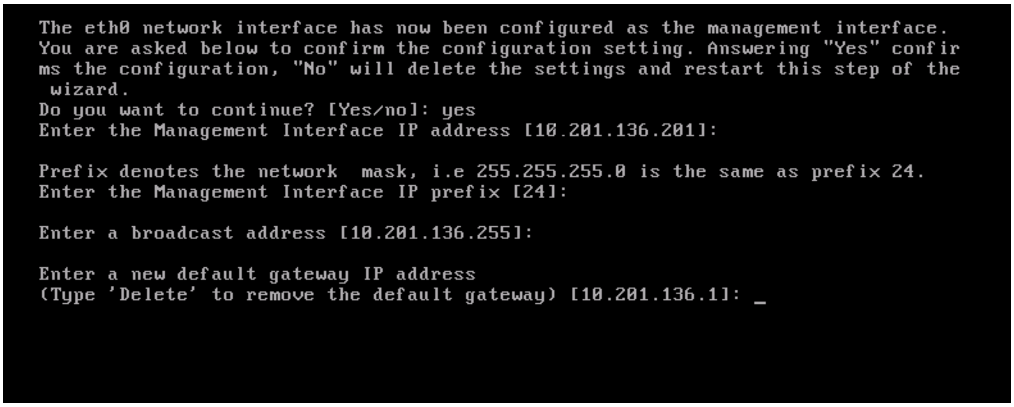
1. Enter a number 0-60 to indicate how long (in seconds) you’d like traffic simulated or press Enter to skip this step.

2. When prompted, choose the NIC index number of the management NIC or accept the default interface.



```
Step 4/8: NIC for Management Server and SSH Connections

The protector has a set of NICs for intercepting traffic and one NIC
for use by the Data Security Management Server and SSH connections.
This NIC is also used to log onto the protector.

*NOTE* During an upgrade the network port used for management might be
       assigned differently than previous Protector versions. Please make
       sure that your Management Interface is connected properly.

Available network interfaces:
(* - current Management Interface, BR - bridge member interface)
(0) * eth0    (driver: pcnet32   mac: 00:0C:29:61:9E:DE  inet: 10.201.136.201/24
)
(1)   eth1    (driver: pcnet32   mac: 00:0C:29:61:9E:E8  inet: 0.0.0.0/0)
(2)   eth2    (driver: pcnet32   mac: 00:0C:29:61:9E:E8  inet: 0.0.0.0/0)
(3)   eth3    (driver: pcnet32   mac: 00:0C:29:61:9E:E8  inet: 0.0.0.0/0)
(4)   eth4    (driver: pcnet32   mac: 00:0C:29:61:9E:E8  inet: 0.0.0.0/0)
(5)   eth5    (driver: pcnet32   mac: 00:0C:29:61:9E:E8  inet: 0.0.0.0/0)

Please choose a management interface number (0-5)[0]: _
```

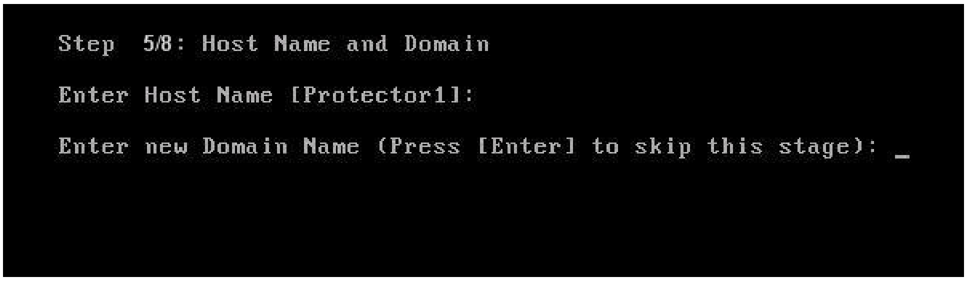
3. Type the IP address of the NIC you’ve chosen. The default is 192.168.1.1.
4. Type the IP prefix of this NIC. This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 24 (255.255.255.0).
5. Type a broadcast address for the NIC. The installation wizard will provide 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.



```
The eth0 network interface has now been configured as the management interface.
You are asked below to confirm the configuration setting. Answering "Yes" confir
ms the configuration, "No" will delete the settings and restart this step of the
 wizard.
Do you want to continue? [Yes/no]: yes
Enter the Management Interface IP address [10.201.136.201]:

Prefix denotes the network  mask, i.e 255.255.255.0 is the same as prefix 24.
Enter the Management Interface IP prefix [24]:

Enter a broadcast address [10.201.136.255]:

Enter a new default gateway IP address
(Type 'Delete' to remove the default gateway) [10.201.136.1]: _
```

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.

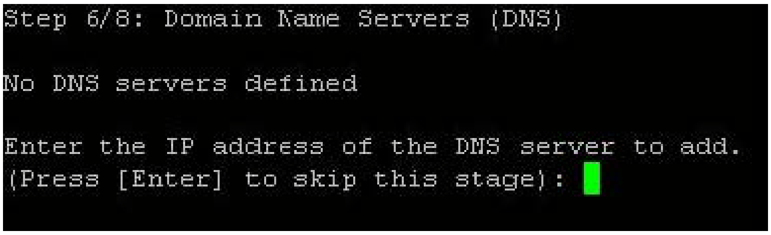


```
Step  5/8: Host Name and Domain

Enter Host Name [Protector1]:

Enter new Domain Name (Press [Enter] to skip this stage): _
```

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

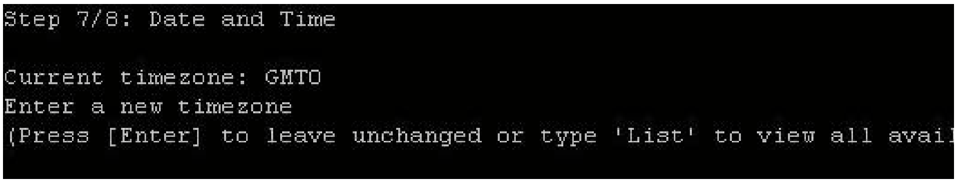
Optionally, type the IP address of the domain name server (DNS) that will service this protector. A DNS will allow access to other network resources using their names instead of their IP addresses.



```
Step 6/8: Domain Name Servers (DNS)

No DNS servers defined

Enter the IP address of the DNS server to add.
(Press [Enter] to skip this stage):
```

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-mmm-yyyy.
3. Type the current time in the following format: HH:MM:SS. Note that this is a 24-hour clock.

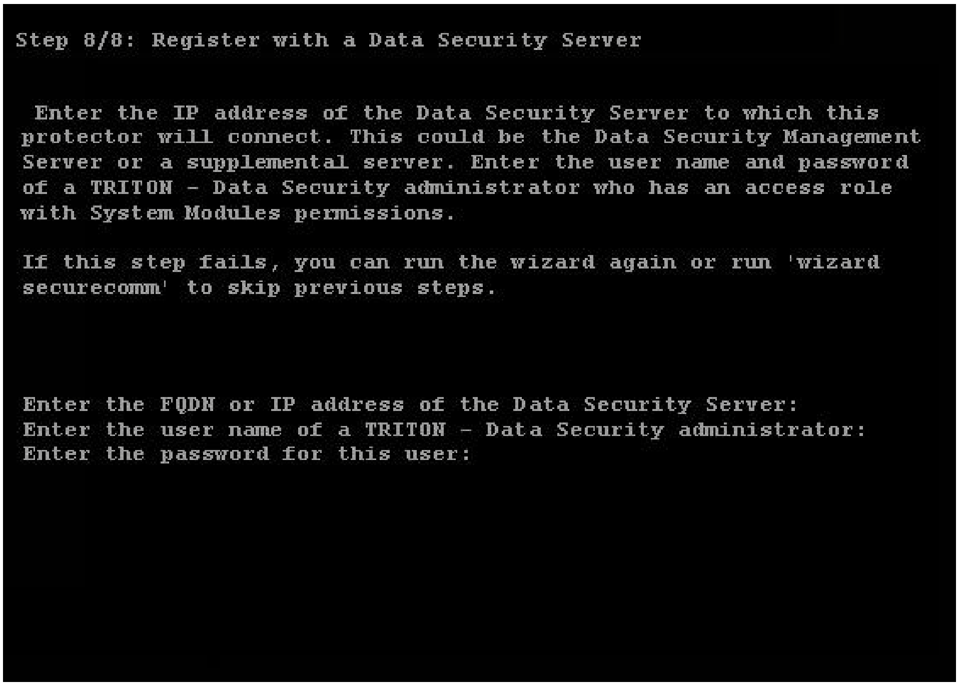


```
Step 7/8: Date and Time

Current timezone: GMT0
Enter a new timezone
(Press [Enter] to leave unchanged or type 'List' to view all avail
```

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.



```
Step 8/8: Register with a Data Security Server


 Enter the IP address of the Data Security Server to which this
protector will connect. This could be the Data Security Management
Server or a supplemental server. Enter the user name and password
of a TRITON - Data Security administrator who has an access role
with System Modules permissions.

If this step fails, you can run the wizard again or run 'wizard
securecomm' to skip previous steps.



Enter the FQDN or IP address of the Data Security Server:
Enter the user name of a TRITON - Data Security administrator:
Enter the password for this user:
```

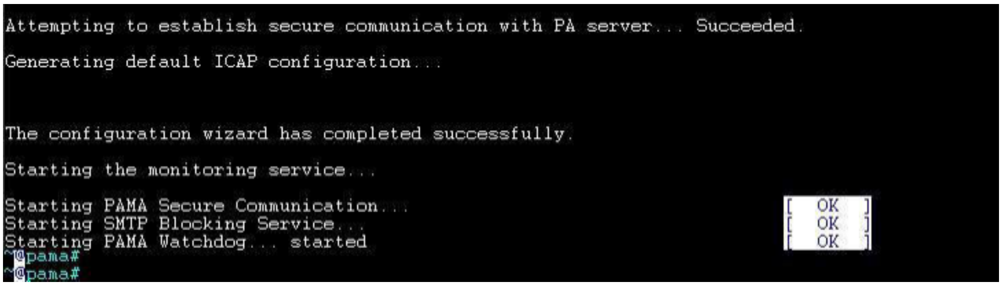
2. Type the user name and password for a TRITON - Data Security administrator that has privileges to manage system modules.

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:



```
Attempting to establish secure communication with PA server... Succeeded.
Generating default ICAP configuration...


The configuration wizard has completed successfully.
Starting the monitoring service...
Starting PAMA Secure Communication...                          [  OK  ]
Starting SMTP Blocking Service...                              [  OK  ]
Starting PAMA Watchdog... started                              [  OK  ]
~@pama#
~@pama#
```

The protector is now ready to be configured. See *Initial Configuration for All Websense Modules*, page 675 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 126.

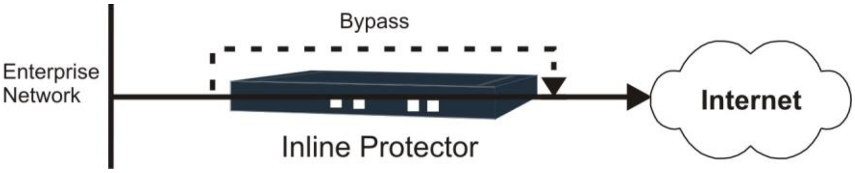
Setting up Bypass mode

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	

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.

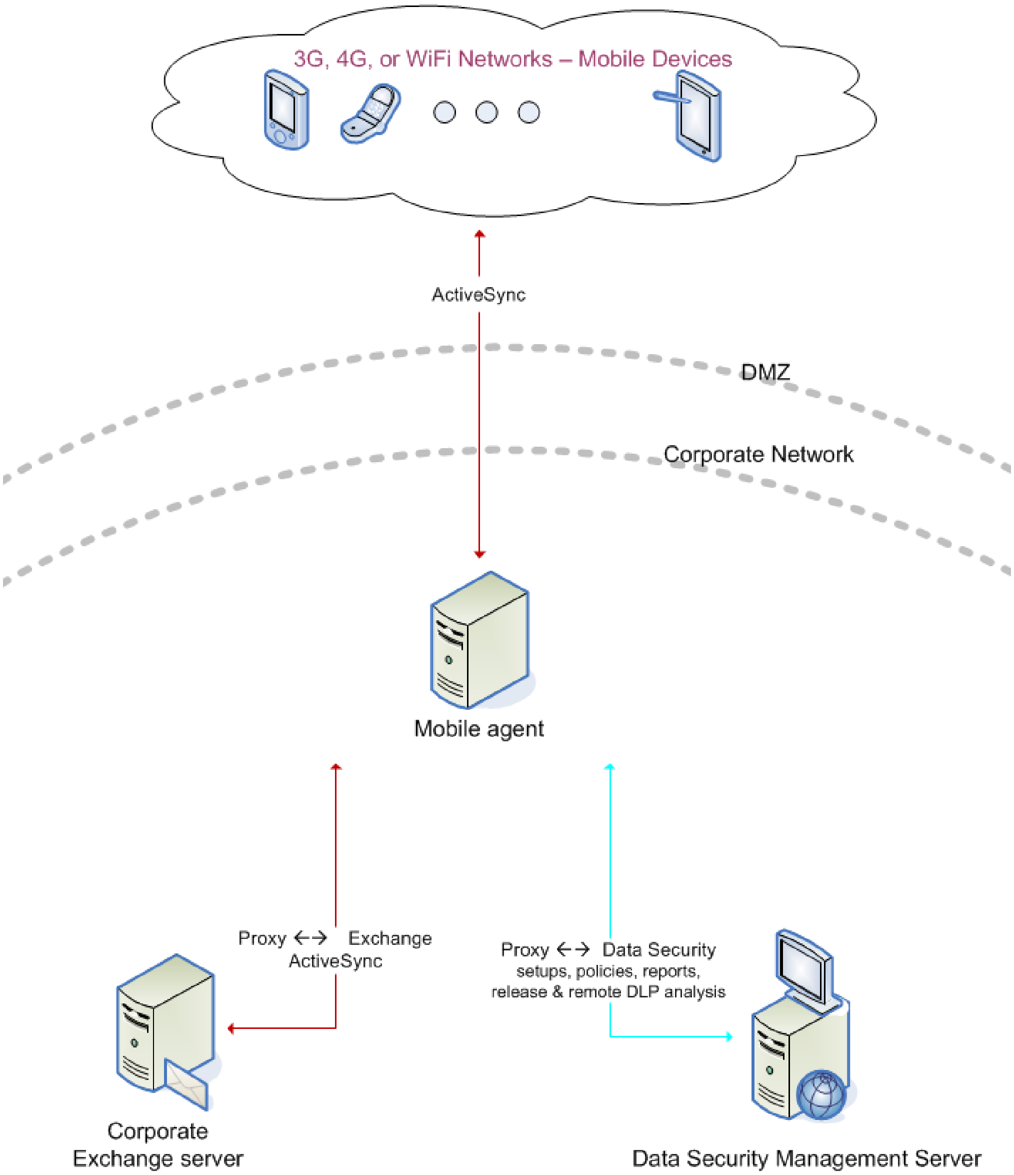
Deploying the mobile agent

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.


3G, 4G, or WiFi Networks – Mobile Devices
ActiveSync
DMZ
Corporate Network
Mobile agent
Proxy ←→ Exchange ActiveSync
Proxy ←→ Data Security setups, policies, reports, release & remote DLP analysis
Corporate Exchange server
Data Security Management Server

For system requirements, see *Mobile Agent hardware requirements*, page 13.

For the default port numbers used by the mobile agent, see *Mobile agent*, page 722. 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 342
2. *Configuring the mobile agent*, page 352
3. *Configuring a mobile DLP policy*, page 354

Mobile agent installations include:

- A policy engine
- Secondary fingerprint repository (the primary is on the management server)

Hardware requirements

The mobile agent is a soft appliance. If you are using your own hardware, it must meet the following 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
Hard drives	2 - 72 GB	4 - 146 GB
Disk space	70 GB	292 GB
Hardware RAID	1	1 + 0
NICs	2	2

Required ports

The following ports must be kept open for the mobile agent:

Outbound

To	Port	Purpose
Data Security Management Server	17443	Syslog, forensics, incidents, mobile status
Data Security Management Server	80	Fingerprint sync
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Microsoft Exchange Server	80/443	ActiveSync (user defined using TRITON - Data Security)
Websense Web Security	56992	Linking Service
Other	UDP 123	Inbound/ outbound NTPD (available on the appliance yet disabled by default)

* This range is necessary for load balancing.

Inbound

From	Port	Purpose
Data Security Management Server	5820	Settings deployment
Mobile Devices	80/443	ActiveSync (user defined using TRITON - Data Security)
Data Security Management Server	8892	Management
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Anywhere (including the Mobile agent)	22	SSH access
Data Security Server	5443	Release quarantined messages
* This range is necessary for load balancing.		

Installing the mobile agent software

The mobile agent must be installed on hardware that meets the requirements described in *Mobile Agent hardware requirements*, page 13. 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, 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:

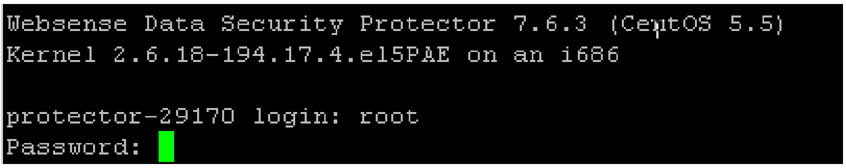
      - 19200 baud
      - 8 data bits
      - no parity
      - 1 stop bit
      - no flow control

   b. The mobile agent software is provided on an ISO image. Download the image, **WebsenseDataSecurityProtector77x.iso**, from MyWebsense and burn it to a CD.

   c. Place the CD in the protector’s CD drive and restart the machine.

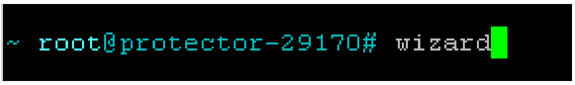
d. An installer page appears. If you are using a regular keyboard and screen, type **kvm** and press **Enter**. If you are using a serial console, press **Enter**. The machine is automatically restarted.

2. You’re prompted to enter a user name and password. Enter *root* for user name and *admin* for password.



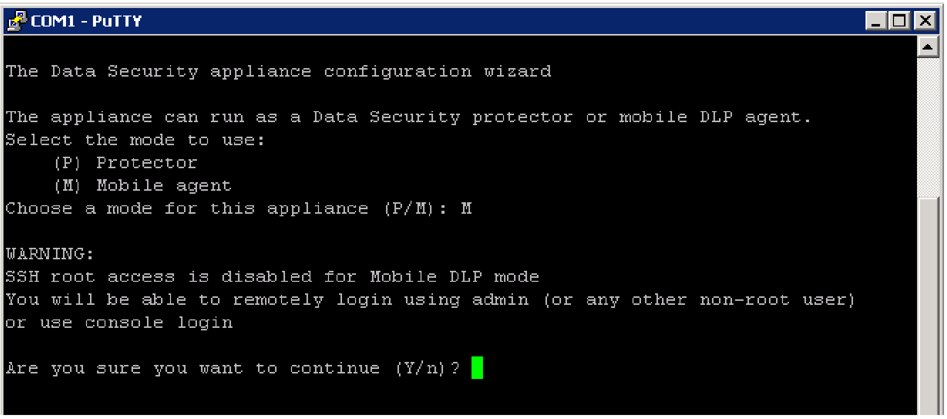
```
Websense Data Security Protector 7.6.3 (CentOS 5.5)
Kernel 2.6.18-194.17.4.el5PAE on an i686

protector-29170 login: root
Password:
```

3. To access the wizard, type “wizard” at the command prompt, and press **Enter**.



```
~ root@protector-29170# wizard
```

4. You have the option to install the Websense protector software or mobile agent software. Type **M** for Mobile agent.



```
The Data Security appliance configuration wizard

The appliance can run as a Data Security protector or mobile DLP agent.
Select the mode to use:
    (P) Protector
    (M) Mobile agent
Choose a mode for this appliance (P/M): M

WARNING:
SSH root access is disabled for Mobile DLP mode
You will be able to remotely login using admin (or any other non-root user)
or use console login

Are you sure you want to continue (Y/n)?
```

5. Follow the instructions given by the wizard to configure basic settings.

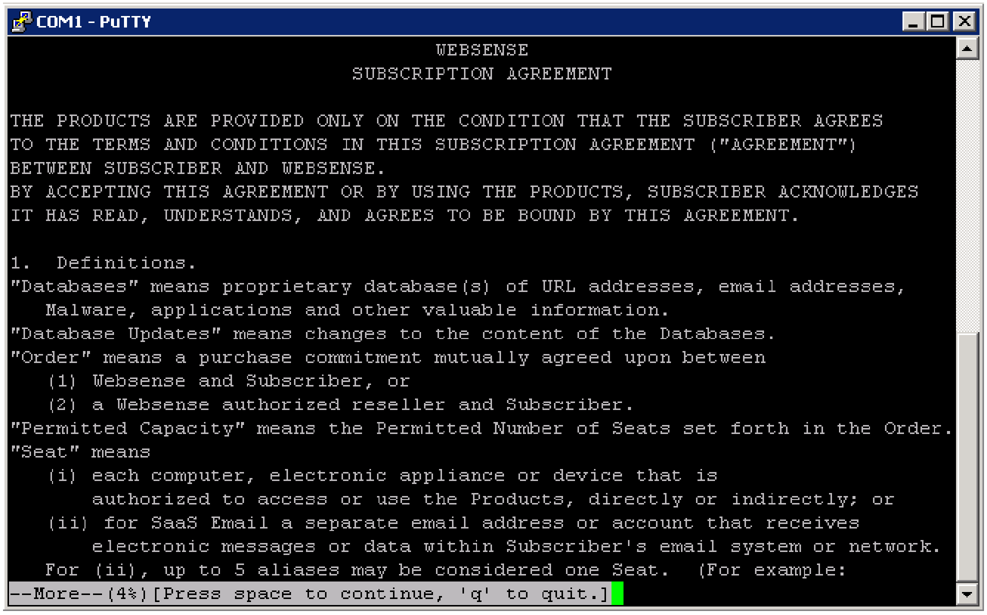
When the wizard requires data entry, it prompts you. In some cases, a default setting is provided:

- 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.

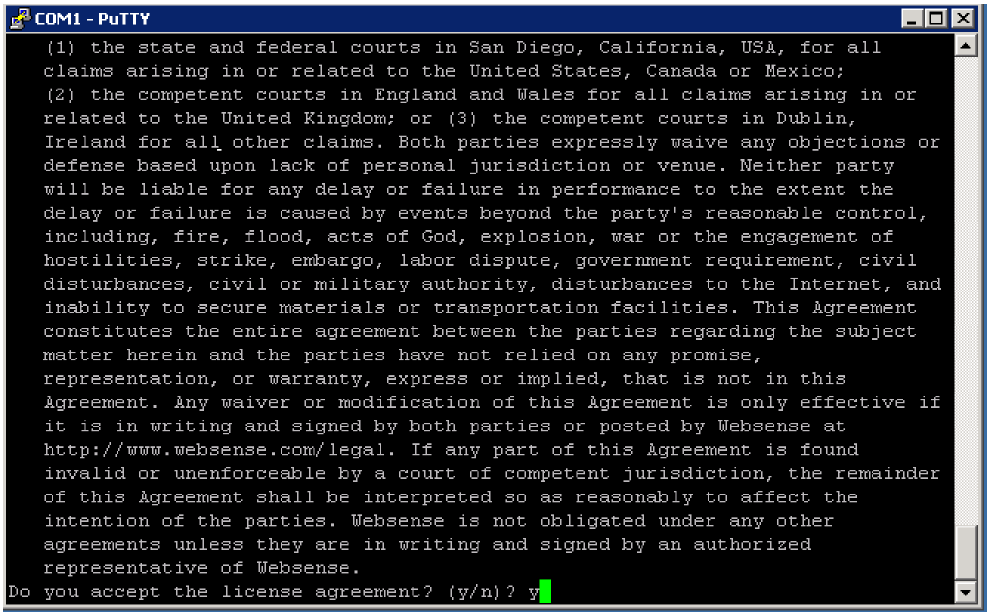
STEP 1: Accept license agreement

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.



```
                                    WEBSENSE
                             SUBSCRIPTION AGREEMENT

THE PRODUCTS ARE PROVIDED ONLY ON THE CONDITION THAT THE SUBSCRIBER AGREES
TO THE TERMS AND CONDITIONS IN THIS SUBSCRIPTION AGREEMENT ("AGREEMENT")
BETWEEN SUBSCRIBER AND WEBSENSE.
BY ACCEPTING THIS AGREEMENT OR BY USING THE PRODUCTS, SUBSCRIBER ACKNOWLEDGES
IT HAS READ, UNDERSTANDS, AND AGREES TO BE BOUND BY THIS AGREEMENT.

1.  Definitions.
"Databases" means proprietary database(s) of URL addresses, email addresses,
   Malware, applications and other valuable information.
"Database Updates" means changes to the content of the Databases.
"Order" means a purchase commitment mutually agreed upon between
   (1) Websense and Subscriber, or
   (2) a Websense authorized reseller and Subscriber.
"Permitted Capacity" means the Permitted Number of Seats set forth in the Order.
"Seat" means
   (i) each computer, electronic appliance or device that is
       authorized to access or use the Products, directly or indirectly; or
   (ii) for SaaS Email a separate email address or account that receives
       electronic messages or data within Subscriber's email system or network.
   For (ii), up to 5 aliases may be considered one Seat.  (For example:
--More--(4%)[Press space to continue, 'q' to quit.]
```

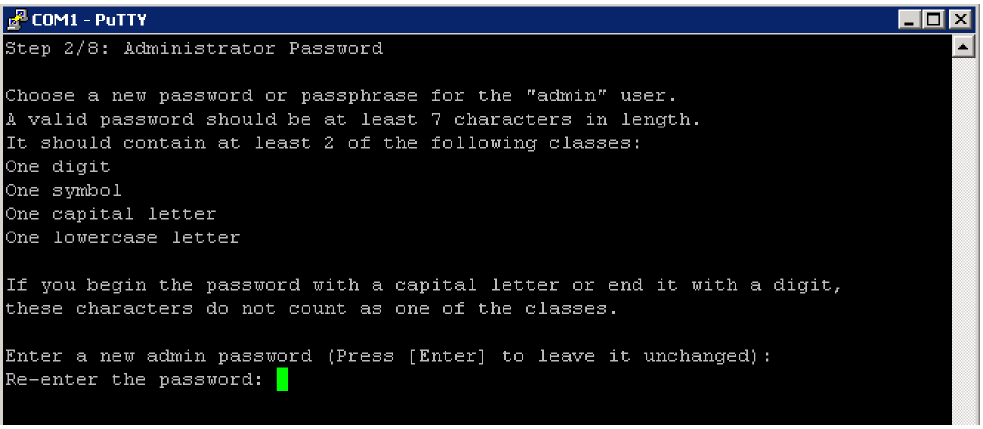
Carefully read the license agreement and when prompted, type yes to accept the license agreement.



```
   (1) the state and federal courts in San Diego, California, USA, for all
   claims arising in or related to the United States, Canada or Mexico;
   (2) the competent courts in England and Wales for all claims arising in or
   related to the United Kingdom; or (3) the competent courts in Dublin,
   Ireland for all other claims. Both parties expressly waive any objections or
   defense based upon lack of personal jurisdiction or venue. Neither party
   will be liable for any delay or failure in performance to the extent the
   delay or failure is caused by events beyond the party's reasonable control,
   including, fire, flood, acts of God, explosion, war or the engagement of
   hostilities, strike, embargo, labor dispute, government requirement, civil
   disturbances, civil or military authority, disturbances to the Internet, and
   inability to secure materials or transportation facilities. This Agreement
   constitutes the entire agreement between the parties regarding the subject
   matter herein and the parties have not relied on any promise,
   representation, or warranty, express or implied, that is not in this
   Agreement. Any waiver or modification of this Agreement is only effective if
   it is in writing and signed by both parties or posted by Websense at
   http://www.websense.com/legal. If any part of this Agreement is found
   invalid or unenforceable by a court of competent jurisdiction, the remainder
   of this Agreement shall be interpreted so as reasonably to affect the
   intention of the parties. Websense is not obligated under any other
   agreements unless they are in writing and signed by an authorized
   representative of Websense.
Do you accept the license agreement? (y/n)? y
```

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.



```
Step 2/8: Administrator Password

Choose a new password or passphrase for the "admin" user.
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 the classes.

Enter a new admin password (Press [Enter] to leave it unchanged):
Re-enter the password:
```

Important

A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

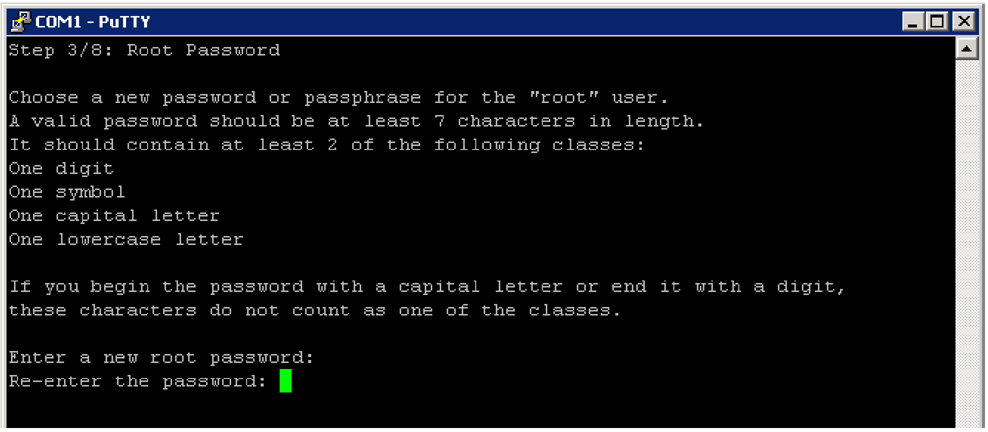
- One digit
- One symbol
- One capital letter
- One lowercase letter

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.



```
Step 3/8: Root Password

Choose a new password or passphrase for the "root" user.
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 the classes.

Enter a new root password:
Re-enter the password:
```

Important

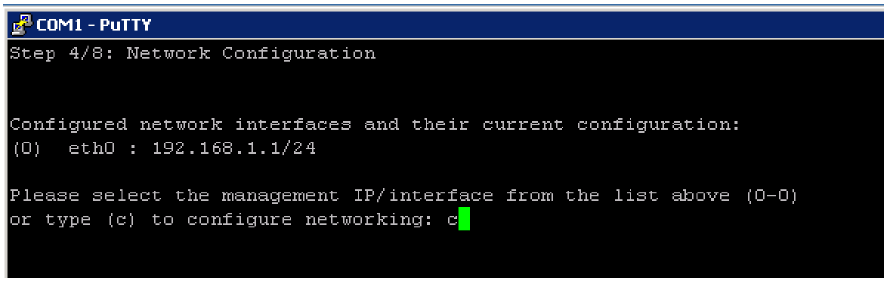
A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:

- 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.

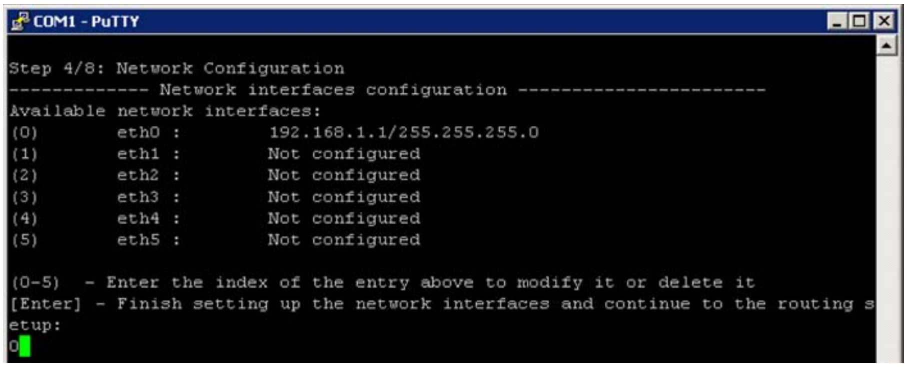
STEP 4: Network configuration

1. Select the network interface (NIC) from the list of available NICs (eth0 by default), or for advanced configuration, type c.



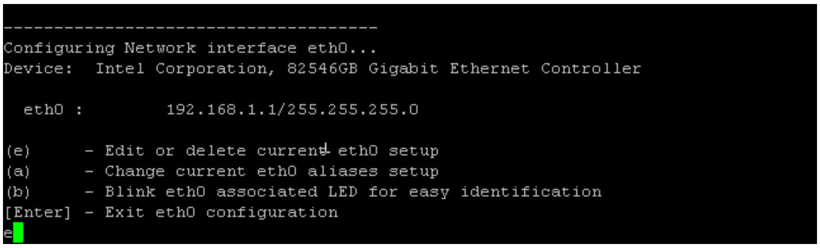
```
Step 4/8: Network Configuration


Configured network interfaces and their current configuration:
(0)  eth0 : 192.168.1.1/24

Please select the management IP/interface from the list above (0-0)
or type (c) to configure networking: c
```

2. To configure your NIC, choose the NIC index number from the list of NICs that display on the wizard.



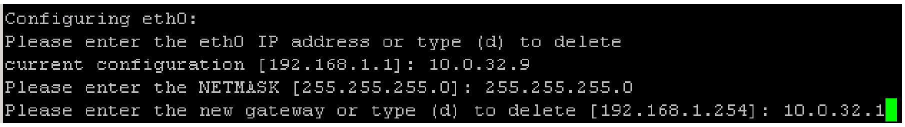
```
Step 4/8: Network Configuration
------------ Network interfaces configuration -----------------------
Available network interfaces:
(0)       eth0 :        192.168.1.1/255.255.255.0
(1)       eth1 :        Not configured
(2)       eth2 :        Not configured
(3)       eth3 :        Not configured
(4)       eth4 :        Not configured
(5)       eth5 :        Not configured

(0-5)  - Enter the index of the entry above to modify it or delete it
[Enter] - Finish setting up the network interfaces and continue to the routing s
etup:
0
```

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.



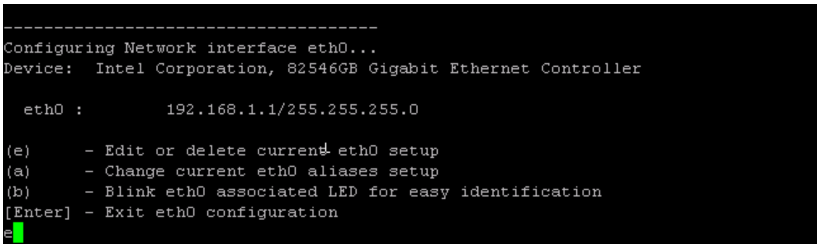
```
-----------------------------------
Configuring Network interface eth0...
Device:  Intel Corporation, 82546GB Gigabit Ethernet Controller

  eth0 :        192.168.1.1/255.255.255.0

(e)      - Edit or delete current eth0 setup
(a)      - Change current eth0 aliases setup
(b)      - Blink eth0 associated LED for easy identification
[Enter] - Exit eth0 configuration
e
```

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.



```
Configuring eth0:
Please enter the eth0 IP address or type (d) to delete
current configuration [192.168.1.1]: 10.0.32.9
Please enter the NETMASK [255.255.255.0]: 255.255.255.0
Please enter the new gateway or type (d) to delete [192.168.1.254]: 10.0.32.1
```

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.

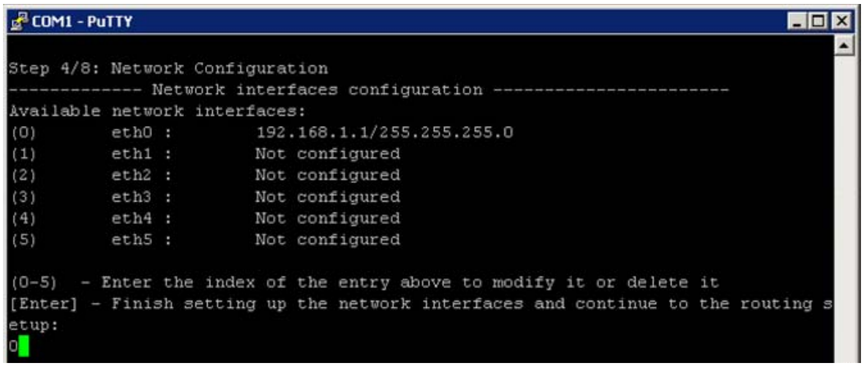


```
------------------------------------
Configuring Network interface eth0...
Device:  Intel Corporation, 82546GB Gigabit Ethernet Controller

  eth0 :        192.168.1.1/255.255.255.0

(e)      - Edit or delete current eth0 setup
(a)      - Change current eth0 aliases setup
(b)      - Blink eth0 associated LED for easy identification
[Enter] - Exit eth0 configuration
e
```

Note

If you type **Enter**, a list of available NICs display, allowing you to define other NICs.

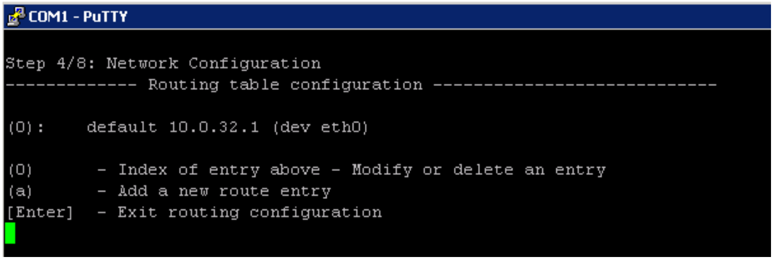
e. Type a NIC index number to configure another NIC (or reconfigure the same NIC), or type Enter to finish setting up the NICs and continue to the routing setup.



```
Step 4/8: Network Configuration
------------- Network interfaces configuration -----------------------
Available network interfaces:
(0)       eth0 :        192.168.1.1/255.255.255.0
(1)       eth1 :        Not configured
(2)       eth2 :        Not configured
(3)       eth3 :        Not configured
(4)       eth4 :        Not configured
(5)       eth5 :        Not configured

(0-5)   - Enter the index of the entry above to modify it or delete it
[Enter] - Finish setting up the network interfaces and continue to the routing s
etup:
0
```

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.

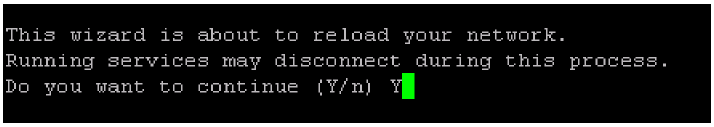


```
Step 4/8: Network Configuration
------------- Routing table configuration ----------------------------

(0):    default 10.0.32.1 (dev eth0)

(0)       - Index of entry above - Modify or delete an entry
(a)       - Add a new route entry
[Enter]   - Exit routing configuration
```

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.



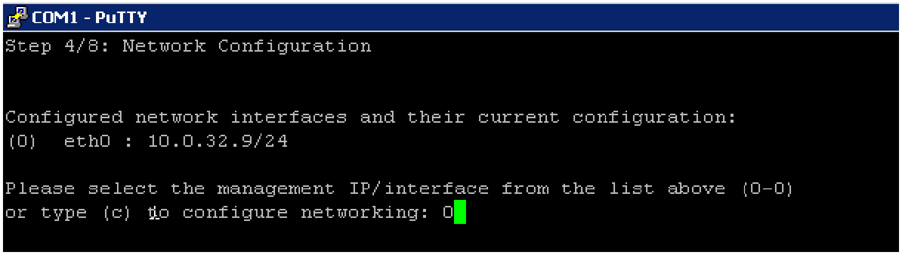
```
This wizard is about to reload your network.
Running services may disconnect during this process.
Do you want to continue (Y/n) Y
```

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.

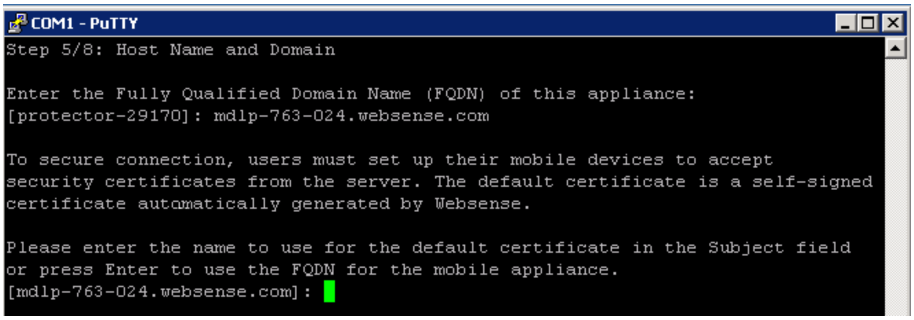
5. Type the index number of the Management NIC you have chosen, or type c to define the network parameters. This NIC can be used for other purposes, such as SSH connections, access points for mobile devices, and Exchange communications.



```
Step 4/8: Network Configuration


Configured network interfaces and their current configuration:
(0)   eth0 : 10.0.32.9/24

Please select the management IP/interface from the list above (0-0)
or type (c) to configure networking: 0
```

STEP 5: Define the host name

1. Type the Fully Qualified Domain Name (FQDN) for the mobile appliance.



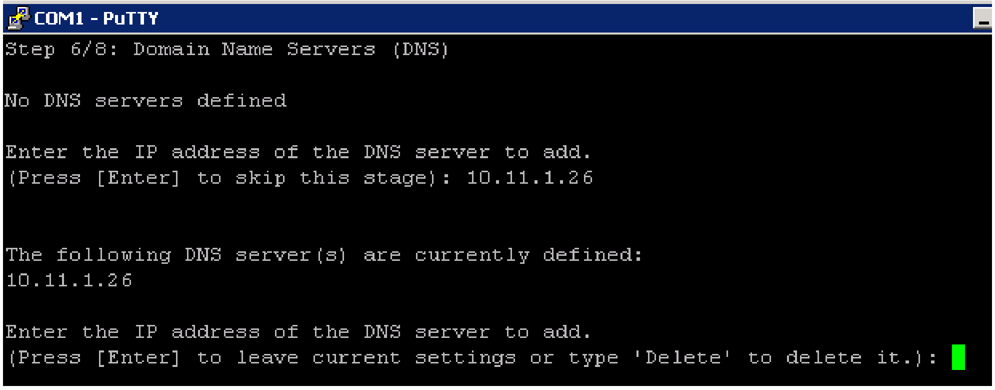
```
Step 5/8: Host Name and Domain

Enter the Fully Qualified Domain Name (FQDN) of this appliance:
[protector-29170]: mdlp-763-024.websense.com

To secure connection, users must set up their mobile devices to accept
security certificates from the server. The default certificate is a self-signed
certificate automatically generated by Websense.

Please enter the name to use for the default certificate in the Subject field
or press Enter to use the FQDN for the mobile appliance.
[mdlp-763-024.websense.com]:
```

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.



```
Step 6/8: Domain Name Servers (DNS)

No DNS servers defined

Enter the IP address of the DNS server to add.
(Press [Enter] to skip this stage): 10.11.1.26


The following DNS server(s) are currently defined:
10.11.1.26

Enter the IP address of the DNS server to add.
(Press [Enter] to leave current settings or type 'Delete' to delete it.):
```

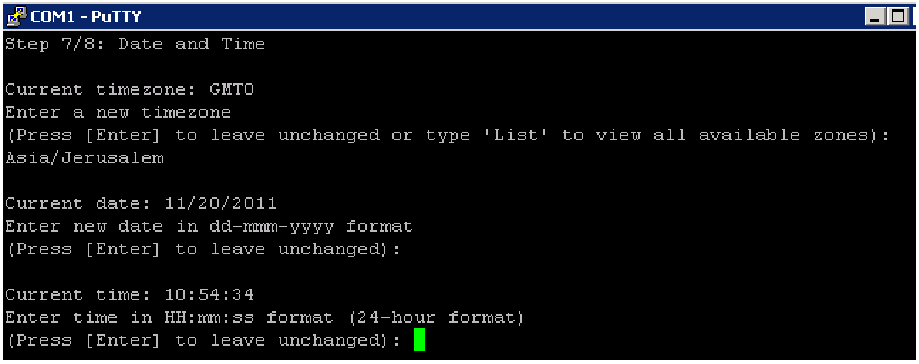
Important

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.

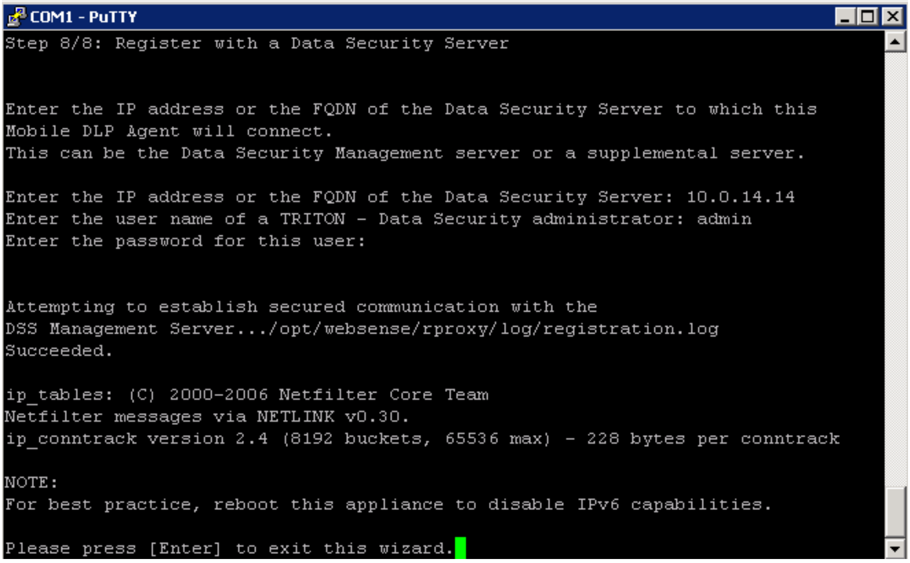


```
Step 7/8: Date and Time

Current timezone: GMT0
Enter a new timezone
(Press [Enter] to leave unchanged or type 'List' to view all available zones):
Asia/Jerusalem

Current date: 11/20/2011
Enter new date in dd-mmm-yyyy format
(Press [Enter] to leave unchanged):

Current time: 10:54:34
Enter time in HH:mm:ss format (24-hour format)
(Press [Enter] to leave unchanged):
```

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.

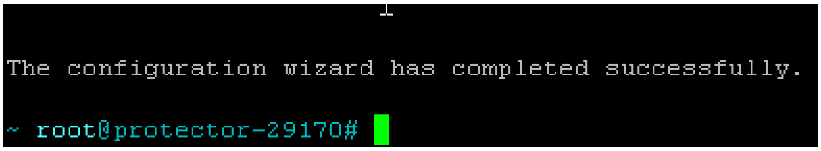
1. Type the IP address or FQDN of the Data Security Server. Note that this must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.



```
Step 8/8: Register with a Data Security Server


Enter the IP address or the FQDN of the Data Security Server to which this
Mobile DLP Agent will connect.
This can be the Data Security Management server or a supplemental server.

Enter the IP address or the FQDN of the Data Security Server: 10.0.14.14
Enter the user name of a TRITON - Data Security administrator: admin
Enter the password for this user:


Attempting to establish secured communication with the
DSS Management Server.../opt/websense/rproxy/log/registration.log
Succeeded.

ip_tables: (C) 2000-2006 Netfilter Core Team
Netfilter messages via NETLINK v0.30.
ip_conntrack version 2.4 (8192 buckets, 65536 max) - 228 bytes per conntrack

NOTE:
For best practice, reboot this appliance to disable IPv6 capabilities.

Please press [Enter] to exit this wizard.
```

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.



```
The configuration wizard has completed successfully.

~ root@protector-29170#
```

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 352 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.

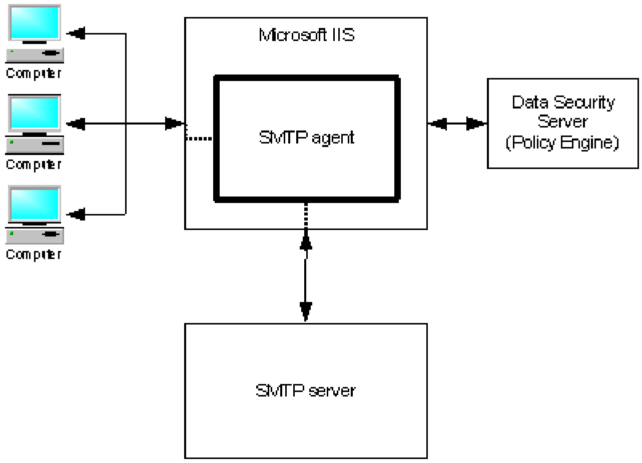
SMTP agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Operating system support*, page 356 ◆ *Required ports*, page 356 ◆ *Preparing a machine for the SMTP agent*, page 357 ◆ *Installing the SMTP agent*, page 358 ◆ *Testing the SMTP agent*, page 359

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.

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.

Operating system support

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

Required ports

The following ports must be kept open for the SMTP agent:

Outbound

To	Port	Purpose
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Next hop MTA	25**	SMTP for inbound/outbound traffic

* This range is necessary for load balancing.
** This is default. Other port can be configured.

Inbound

From	Port	Purpose

Previous MTA	25*	SMTP for inbound/outbound traffic
* This is default. Other port can be configured.		

Preparing a machine for the 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.
    a. In Windows control panel, select **Add/Remove programs > Windows Components**.
    b. Select **Application Server**, and then click **Details**.
    c. Select **Internet Information Services (IIS)**, and then click **Details**.
    d. Select **SMTP Service**, and then click **Details**.
    e. Click **OK** 3 times to close the windows.
    f. Click **Next** to configure and install the components.
2. Configure the SMTP Service.
    a. In IIS Manager, right-click the Default SMTP Virtual Server and rename it to “Inbound”.
    b. Right-click the Inbound server and select **Properties**.
    c. Select the Messages tab, and then deselect all message “Limits”. (These should be enforced by the mail server.)
    d. Select the Delivery tab, and then click **Outbound Connections**.
    e. Set the TCP port to 10025 and click **OK**.
    f. Click **Advanced** and 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.
3. Add a new SMTP Virtual Server in IIS Manager.
    a. Right-click the server name, select **New > SMTP Virtual Server**.
    b. Using the resulting wizard, configure the following 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.

Installing the SMTP agent

1. If your IIS machine has a 32-bit operating system, download the Websense installer (**WebsenseTRITON77Setup.exe**) from mywebsense.com.

   On 64-bit machines, download **WebsenseDataSecurityAgents770-x64.msi** instead.
2. Launch the installer.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

   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:.

8. On the **Select Components** screen, select **SMTP agent** and then **Entire feature will be installed on local hard drive**. If this is a stand-alone server, deselect all other options, including Data Security Server.
9. The **Virtual SMTP Server** screen appears.

   In the **Select Virtual Server** list, select the IIS virtual SMTP server that should be bound to the SMTP agent. The 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.

   (See *Preparing a machine for the SMTP agent*, page 357, for instructions on installing Microsoft IIS from Control Panel and configuring inbound and outbound SMTP Virtual Servers.)
10. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.

11. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server.

    FQDN is the fully-qualified domain name of a machine.

12. 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.

13. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.

14. Once installation is complete, the **Installation Successful** screen appears to inform you that your installation is complete.

Before cutting over the live mail flow, be sure to test relaying through all mail servers as described in *Testing the SMTP agent*, page 359. The easiest way to test your installation is using Outlook Express installed on the same machine as the SMTP agent.

For information on configuring the SMTP agent for your existing email infrastructure, see *Using the SMTP agent*, page 126.

Testing the SMTP agent

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).

Microsoft ISA/TMG agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

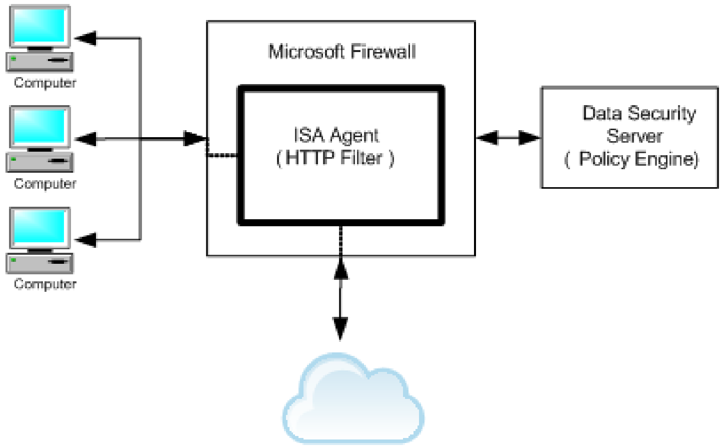
Applies to:	In this topic:
◆ Data Security, v7.7.x	

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.

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. It supports both HTTPS and HTTP traffic.

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

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.



Operating system support

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).

Required ports

The following ports must be kept open for the ISA/TMG agent:

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communications
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Internet gateway	80	For HTTP connections

* This range is necessary for load balancing.

Inbound

None

Installing the ISA/TMG agent

For best practice, do not install the ISA agent on the same machine as a supplemental Data Security Server in a production environment.

1. If your ISA or TMG Server machine has a 32-bit operating system, download the Websense installer (**WebsenseTRITON77Setup.exe**) from mywebsense.com.

   On 64-bit machines, download **WebsenseDataSecurityAgents770-x64.msi** instead.
2. Launch the installer.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

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:.

8. On the **Select Components** screen, select **ISA or TMG agent** and then **Entire feature will be installed on local hard drive**.
9. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
10. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server.

    FQDN is the fully-qualified domain name of a machine.
11. 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.
12. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.
13. Once installation is complete, the **Installation Successful** screen appears to inform you that your installation is complete.

To ensure that the ISA/TMG agent is properly installed and enabled in ISA/TMG, navigate to Web Filters in the ISA/TMG Management Console.

Printer agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	

The Data Security printer agent is required when you want to monitor what is printed on your organization's network printers.

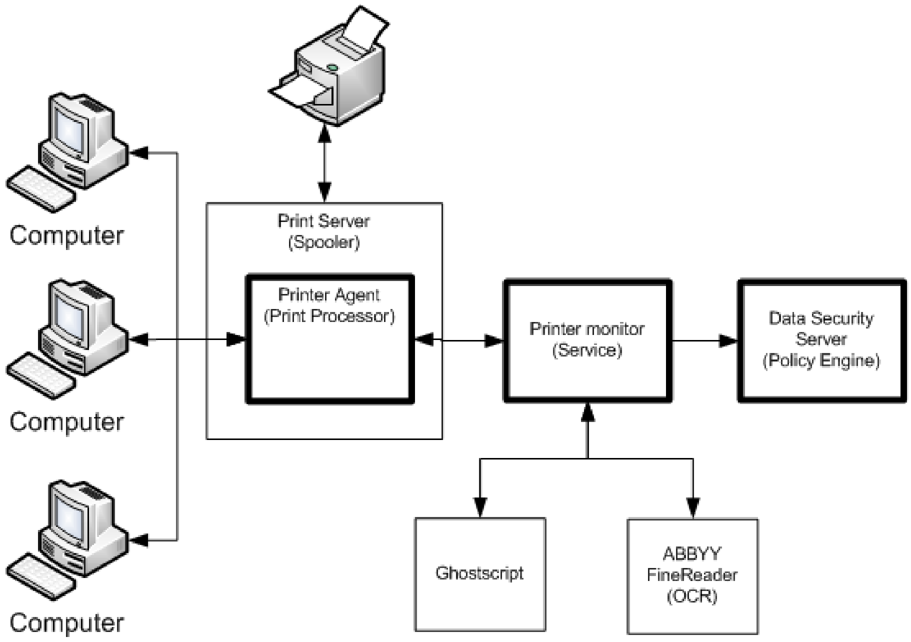
The printer agent supports permit and block actions.

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 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.


Computer
Computer
Computer
Print Server (Spooler)
Printer Agent (Print Processor)
Printer monitor (Service)
Data Security Server (Policy Engine)
Ghostscript
ABBYY FineReader (OCR)

The printer agent is installed using a separate printer agent package (WebsenseDataSecurityPrinterAgent.zip) See *Installing the printer agent*, page 367 for instructions.

Operating system support

The printer agent supports the following Windows Server 2003 32-bit environments:

- Standard or Enterprise
- Standard or Enterprise R2
- Standard or Enterprise R2 SP2

Required ports

The following ports must be kept open for the printer agent:

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communications

Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Management Server	17443	Incidents
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
* This range is necessary for load balancing.		
Inbound		
None		

Prerequisites

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.
- For best practice, do not install the printer agent on the same machine as a supplemental Data Security Server in a production environment.

If these 2 conditions are not met, the installer doesn't show the option to install the printer agent.

Installing the printer agent

1. Download and extract **WebsenseDataSecurityPrinterAgent.zip** from mywebsense.com on the print server machine.
2. Launch the Data Security installer, **DSS-7.7.0.60-x86.msi**, on the print spooler machine. Your version and build number may vary.
3. On the **Welcome** screen, click **Next** to begin the installation.
4. In the **Destination Folder** screen, specify the folder into which to install the agent.

   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. On the **Select Components** screen, select **Printer Agent** and then **Entire feature will be installed on local hard drive**.
6. When prompted, click **Setup** to extract a software installer for GPL Ghostscript. Ghostscript is an interpreter for .ps and .pdf description languages. This software is required for the printer agent.
7. Accept the defaults in the Ghostscript wizard, then click **Install**.
8. The **Optical Character Recognition** screen appears.

Section	Description
OCR Analysis Threshold	**Per printed page:** 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. (Default value: 3 sec.; Range: 1-60 sec.) **No more than *nn* seconds:** 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. (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. 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. (Default value: 5 pages)

Optionally, you can change the default values defined for the OCR Analysis Threshold and the OCR Accuracy.

9. The **Fingerprinting Database** screen appears. To choose a location other than the default shown, use the **Browse** button.
10. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.

11. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server.

    FQDN is the fully-qualified domain name of a machine.

12. In the **Local Administrator** screen, enter a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters. If you are installing Data Security v7.7.0, this password cannot exceed 19 characters. If you are installing version 7.7.2 or beyond, password length doesn't matter.

13. n 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.

14. A **Configure Printer Agent** screen appears.

    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?*

    b. Click **Yes**. The settings are automatically modified to accommodate the printer agent.

15. 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.

16. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.

    The printers you selected appear as policy resources in TRITON - Data Security. To view them, log onto the TRITON Console and navigate to **Main** > **Configuration** > **Resources**.

17. To complete the process, click **Deploy** in TRITON - Data Security.

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.

Configuration settings for non-English text

If your printers are used for non-English text, you need to make minor modifications to the following configuration files:

- ExportToTXT-Accurate.ini
- ExportToTXT-Fast.ini

To modify the 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Installing the integration agent*, page 372 ◆ *Registering the integration agent*, page 373 ◆ *Using the Websense Data Security API*, page 374

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 relocatable 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Operating system support*, page 375 ◆ *Required ports*, page 375 ◆ *Installing the crawler agent*, page 376

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 **Edit**.

Operating system support

Supplemental Data Security servers must be running on one of the following operating system environments:

- Windows Server 2003 (32-bit) Standard or Enterprise R2 SP2
- Windows Server 2008 (64-bit) Standard or Enterprise R2

Required ports

The following ports must be kept open for the crawler:

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communication
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Salesforce server	80 or 8080	Salesforce discovery

* This range is necessary for load balancing.

Inbound

From	Port	Purpose
Data Security Management Server	9797*	Crawler listening

* This is only for the standalone crawler agent.

Installing the crawler agent

1. Download the Websense installer (**WebsenseTRITON77Setup.exe**) from mywebsense.com.
2. Launch the installer.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.
7. In the **Destination Folder** screen, specify the folder into which to install the agent.

   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:.

8. On the **Select Components** screen, select **Crawler agent** and then **Entire feature will be installed on local hard drive**. If this is a stand-alone installation, deselect all other options, including Data Security Server.
9. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.

   The following message may appear:

   > *Data Security Discovery Agent works with a specific 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 the crawler agent. The particular version of WinPcap mentioned in this message must be in place to install Crawler Agent. Note that after installation of the crawler agent you can install a different version of WinPcap. The crawler agent should continue to work properly.

10. In the **Register with the Data Security Server** screen specify the path and log on credentials for the Data Security server to which this agent will connect. This could be the TRITON management server or a secondary Data Security server.

    FQDN is the fully-qualified domain name of a machine.

11. In the **Local Administrator** screen, enter a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters. If you are installing Data Security v7.7.0, this password cannot exceed 19 characters. If you are installing version 7.7.2 or beyond, password length doesn't matter.

12. If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, 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.

13. 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.

14. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.

15. Once installation is complete, the **Installation Successful** screen appears to inform you that your installation is complete.

For information on configure the crawler, see “Configuring the crawler” in the TRITON - Data Security Help system.

Troubleshooting Data Security agent installation

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Initial registration fails*, page 379 ◆ *Deploy settings fails*, page 380 ◆ *Subscription errors*, page 380 ◆ *Network connectivity problems*, page 380

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 logs on the TRITON Management Server (and remote policy engines).
  - %dss_home%/logs/mgmtd.log
  - %dss_home%/tomcat/logs/dlp/dlp-all.log
- Check logs on the protector. These reside in the /opt/websense/neti/log directory. In particular, check:
  - /opt/websense/neti/log/registration.log
- 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 logs on the TRITON Management Server (and remote policy engines).
  - %dss_home%/tomcat/logs/dlp/dlp-all.log
  - %dss_home%/tomcat/logs/dlp/deployment-trace.log
- Check the plat.log on the protector.

Subscription errors

- Restart the Websense TRITON - Data Security service on the TRITON Management Server.
- Check %dss_home%/tomcat/logs/dlp/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
```

17 Installing components via the Custom option

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Gateway Anywhere v7.7.x	◆ *Deployment*, page 383 ◆ *Installation*, page 384 ◆ *Initial configuration*, page 385

Websense software components can be deployed in a variety of configurations. In many cases, additional instances of individual components can be added as your network grows or traffic patterns change.

Use the custom installation instructions provided in this section in conjunction with the information provided about common installation scenarios (listed below).

- *Installation overview: Web Filter and Web Security*, page 193
- *Installation overview: Web Security Gateway*, page 197
- *Installation overview: Web Security Gateway Anywhere*, page 200
- *Installing appliance-based Websense solutions*, page 247
- *Installing Data Security Solutions*, page 303
- *Installation Overview: TRITON Enterprise*, page 175

Deployment

General

- *System requirements for this version*, page 2

Web Security

- *Web Security Deployment Recommendations*, page 23
- *Deploying Web Security for a distributed enterprise*, page 65
- *Integrating Web Security with Check Point*, page 445
- *Integrating Web Security with Cisco*, page 481
- *Integrating Web Security with Citrix*, page 513
- *Integrating Web Security using ICAP Service*, page 557
- *Integrating Web Security with Microsoft Products*, page 535
- *Installing Web Security for Universal Integrations*, page 563

Data Security

- *Planning Data Security Deployment*, page 103
- *Installing TRITON - Data Security*, page 187
- *Installing Data Security Components*, page 315
- *Integrating Data Security with Existing Infrastructure*, page 125
- *Scaling Data Security*, page 157

Email Security

- *Email Security Gateway Deployment*, page 163

Installation

To perform a custom installation, first start a custom installation (see *Starting a custom installation*, page 385). Then see the following instructions for the components you want to install:

- *Installing TRITON Infrastructure*, page 386
- *Installing Web Security components*, page 392
- *Installing Data Security components*, page 413
- *Installing Email Security components*, page 414
- *Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)*, page 417

Initial configuration

General

- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Initial Configuration for All Websense Modules*, page 675

Web Security Gateway Anywhere

- *Web Security initial configuration*, page 677
- *Content Gateway initial configuration*, page 684
- *Additional configuration for Web Security Gateway Anywhere*, page 679

Data Security

- *Data Security initial configuration*, page 682

Starting a custom installation

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

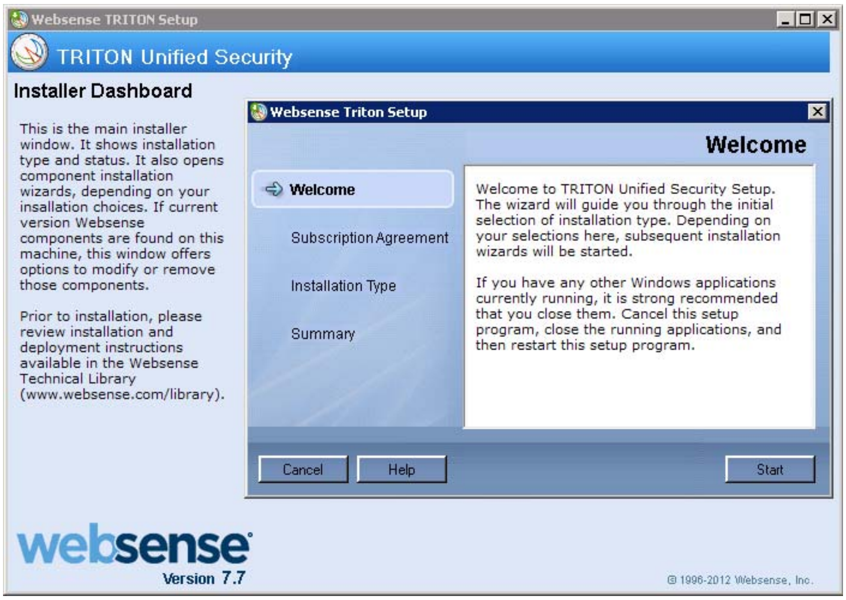
- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

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

   You can download **WebsenseTRITON77Setup.exe** from mywebsense.com.
2. Double-click **WebsenseTRITON77Setup.exe** to launch the installer.

   A progress dialog box appears, as files are extracted.

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



This is the main installer window. It shows installation type and status. It also opens component installation wizards, depending on your insallation choices. If current version Websense components are found on this machine, this window offers options to modify or remove those components.

Prior to installation, please review installation and deployment instructions available in the Websense Technical Library (www.websense.com/library).

Welcome to TRITON Unified Security Setup. The wizard will guide you through the initial selection of installation type. Depending on your selections here, subsequent installation wizards will be started.

If you have any other Windows applications currently running, it is strong recommended that you close them. Cancel this setup program, close the running applications, and then restart this setup program.

The Installer Dashboard stays on-screen during installation. Various subinstallers and dialog boxes are displayed over it.

4. On the **Subscription Agreement** screen, select **I accept this agreement**, 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

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

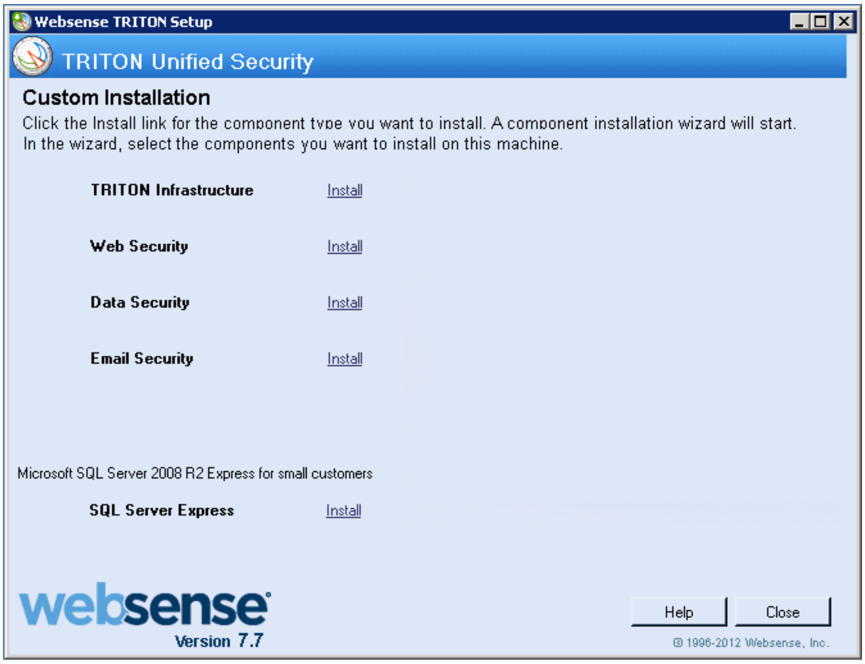
Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

TRITON Infrastructure is composed of common user interface, logging, and reporting components required by the TRITON Unified Security Center modules (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 383.)
   - Selected the TRITON Unified Security Center installation type. (See *Installing TRITON Unified Security Center*, page 181.)
   - 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 3 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.)



Custom Installation

Click the Install link for the component type you want to install. A component installation wizard will start.
In the wizard, select the components you want to install on this machine.

TRITON Infrastructure Install

Web Security Install

Data Security Install

Email Security Install

Microsoft SQL Server 2008 R2 Express for small customers

SQL Server Express Install

TRITON Infrastructure Setup is launched.

3. On the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
4. 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**.
- To specify a different location, click **Browse**.

5. On the **SQL Server** screen, specify the location of your database engine and the type of authentication to use for the connection. Also specify whether to encrypt communication with the database.

   The information entered here is also used by the Web, Data, and Email Security component installers, by default. The Web Security component installer can be used to specify a different database; the Data and Email Security component installers cannot.

   - Select **Use existing SQL Server on this machine** if the Websense installer has already been used to install SQL Server 2008 R2 Express on this machine.
   - Select **Install SQL Server Express on this machine** to install SQL Server 2008 R2 Express on this machine.

     When this option is selected, .NET 3.5 SP1, Powershell 1.0, and Windows Installer 4.5 are installed automatically if they are not found on the machine. These are required for SQL Server 2008 R2 Express.

     A default database instance named **mssqlserver** is created, by default. If a database instance with the default name already exists on this machine, an instance named TRITONSQL2K8R2X is created instead.

     If .NET 3.5 SP1 is not found on the machine, the installer needs access to windowsupdate.microsoft.com. If anything blocks this machine from accessing the site, 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 before installing SQL Server 2008 R2 Express (see *Backing up the MSDE Log Database*, page 764). Leave the Websense installer running and come back once you have backed up MSDE data.

     In some cases, you are prompted to reboot the machine after installing SQL Server Express. If you do, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to restart the installer.
   - Select **Use existing SQL Server on another machine** to specify the location and connection credentials for a database server located elsewhere in the network.

     Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any.

     - If you are using a named instance, the instance must already exist.
     - If you are using SQL Server clustering, enter the virtual IP address of the cluster.

     Also provide the **Port** used to connect to the database (1433, by default).

     See *System requirements for this version*, page 2, to verify your version of SQL Server is supported.

   After selecting one of the above options, specify an authentication method and account information:

- Select the **Authentication** method to use for database connections: **SQL Server Authentication** (to use a SQL Server account) or **Windows Authentication** (to use a Windows trusted connection).

  Next, provide the **User Name** or **Account** and its **Password**. This account must be configured to have system administrator rights in SQL Server. If you are using SQL Server Express, **sa** (the default system administrator account) is automatically specified (this is the default system administrator account).

  For more information about permissions required for the connection account, see *Installing with SQL Server*, page 411.

  If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in TRITON - Web Security and its reporting tools. See *Using a batch file for Apache SSL certificate file operations*, page 727.

When you click **Next**, connection to the database engine is verified. 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.

6. On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Unified Security Center.

   - Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.

     Use the IP address selected to access the TRITON Unified Security Center (via Web browser). Also specify this IP address to any Websense component that needs to connect to the TRITON management server.

     If you chose to install SQL Server 2008 R2 Express, if you install Web Security or Email Security Log Server on another machine, specify this IP address for the database engine location.

   - Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and TRITON Unified Security Center. The server/host name cannot exceed 15 characters.

   - Specify the **User name** of the account to be used by TRITON Unified Security Center.

   - Enter the **Password** for the specified account. If you are installing Data Security v7.7.0, this password must not exceed 19 characters. If you are installing version 7.7.2 or beyond, password length doesn’t matter.

7. On the **Administrator Account** screen, enter an email address and password for the default TRITON console administration account: **admin**. When you are finished, click **Next**.

   System notification and password reset information is sent to the email address specified (once SMTP configuration is done; see next step).

It is a best practice to use a strong password as described onscreen.

8. On the **Email Settings** screen, enter information about the SMTP server to be used for system notifications and then click **Next**. You can also configure these settings after installation in the TRITON console.

> **Important**
>
> If you do not configure an SMTP server now and you lose the **admin** account password (set on previous screen) before the setup is done in the TRITON console, the “Forgot my password” link on the logon page does not provide password recovery information. SMTP server configuration must be completed before password recovery email can be sent.

- **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.

9. 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.

10. 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 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 7.7 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 7.7.

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.

11. 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.

12. 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.

13. On the **Installation Complete** screen, click **Finish**.

14. 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 764, for instructions.

    b. Configure Log Server to use the installation of SQL Server Express.

       See *Configuring 7.5 Log Server to connect to SQL Server Express prior to upgrade to 7.7*, page 768, for instructions.

       This must be done or the Websense installer will be unable to upgrade Log Server to version 7.7. Note that Log Server may be running on a different machine.

Installing Web Security components

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

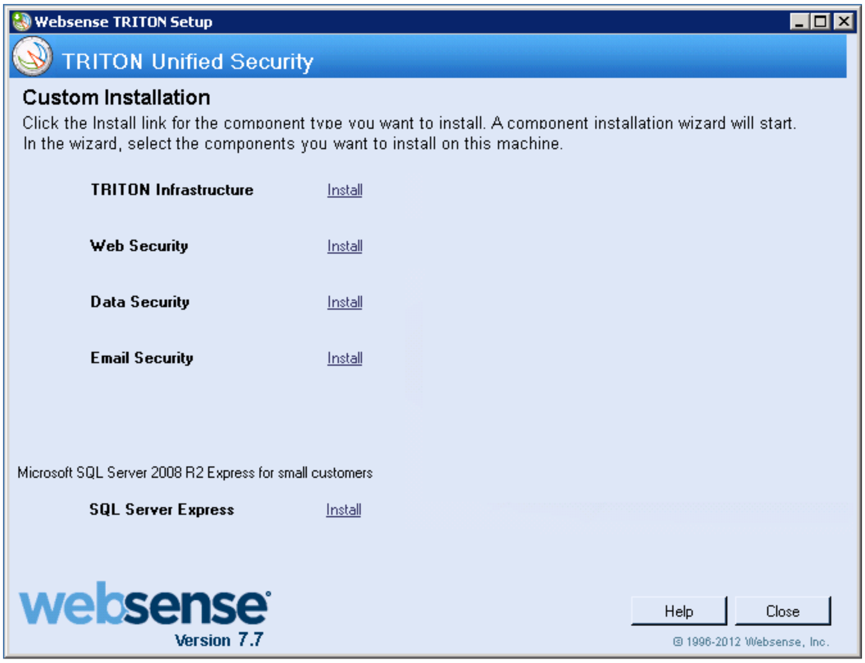
Complete these steps to install one or more Web Security software components on Windows. (To install Web Security components on a Linux machine, see *Installing Web Security Components on Linux*, page 209.)

If you are distributing components across multiple machines, run the installer and complete the installation steps on each machine.

These instructions assume that you have already launched the installer and selected **Custom**. (For instructions on performing these steps, see *Deployment*, page 383.)

If you are adding components, skip to Step 2.

1. On the Custom Installation dashboard, click the Web Security **Install** link.



Websense TRITON Setup

TRITON Unified Security

Custom Installation

Click the Install link for the component type you want to install. A component installation wizard will start.
In the wizard, select the components you want to install on this machine.

TRITON Infrastructure	Install
Web Security	Install
Data Security	Install
Email Security	Install

Microsoft SQL Server 2008 R2 Express for small customers

SQL Server Express	Install

The Web Security component installer is launched.

2. Use the **Select Components** screen to identify the component or components to install on this machine. As you make your selection, remember that:
   - Policy Broker, Policy Server, and Filtering Service must be installed in the order listed, and before any other Web Security components. (If you select all 3 at the same time, they are installed in the correct order.)
   - TRITON - Web Security is available only when TRITON Infrastructure is already installed on the machine (see *Installing TRITON Infrastructure*, page 386).
   - 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*
- *Logon Agent*
- *eDirectory Agent*
- *RADIUS Agent*
- *State Server*
- *Multiplexer*
- *Filtering Plug-in*
- *Remote Filtering Client*
- *Remote Filtering Server*
- *Linking Service*
- *Sync Service*
- *Directory Agent*

3. Depending on the components selected, some or all of the following installer screens appear. (The parenthetical information below indicates which components or machine conditions cause the screen to appear.)

   Click the screen name for instructions.

   - *Policy Server Connection Screen*, page 396 (Filtering Service, Network Agent, Usage Monitor, TRITON - Web Security, Real-Time Monitor, Web Security Log Server, User Service, DC Agent, Logon Agent, eDirectory Agent, RADIUS Agent, State Server, Multiplexer, Remote Filtering Client Pack, Remote Filtering Server, Linking Service, Sync Service, or Directory Agent)
   - *Policy Broker Connection Screen*, page 397 (Policy Server, Sync Service, or Directory Agent)
   - *Multiple Network Interfaces Screen*, page 399 (if multiple NICs detected)
   - *Active Directory Screen*, page 400 (if installing User Service, DC Agent, or Logon Agent on Windows Server 2008)
   - *Computer Browser Screen*, page 400 (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 401 (Filtering Service)
   - *Select Integration Screen*, page 402 (Filtering Service, to be integrated with a third-party product, or Filtering Plug-In)
   - *Network Agent and Firewall Screen*, page 403 (Filtering Service and Network Agent; Filtering Service to be integrated with a Check Point product)
   - *Network Card Selection Screen*, page 403 (Network Agent)
   - *Database Information Screen*, page 404 (Web Security Log Server)
   - *Log Database Location Screen*, page 405 (Web Security Log Server)
   - *Optimize Log Database Size Screen*, page 405 (Web Security Log Server)
   - *Filtering Feedback Screen*, page 406 (Filtering Service or Network Agent)
   - *Directory Service Access Screen*, page 407 (User Service, DC Agent, or Logon Agent)

- *Remote Filtering Communication Screen*, page 408 (Remote Filtering Server)
- *Remote Filtering Pass Phrase Screen*, page 409 (Remote Filtering Server)
- *Filtering Service Information for Remote Filtering Screen*, page 409 (Remote Filtering Server)
- *Filtering Service Communication Screen*, page 398 (Network Agent, a filtering plug-in, or Linking Service)

4. 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.

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

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

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

7. On the **Installation Complete** screen, click **Done**.

   Additional configuration may be necessary if you are integrating Web Security with another product. See:

   - *Integrating Web Security with Check Point*, page 445
   - *Integrating Web Security with Cisco*, page 481
   - *Integrating Web Security with Citrix*, page 513
   - *Integrating Web Security with Microsoft Products*, page 535
   - *Installing Web Security for Universal Integrations*, page 563

Policy Server Connection Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if any of the following is selected for installation, but Policy Server is neither selected nor already installed on the machine:

Windows only

- TRITON - Web Security
- Log Server
- DC Agent
- Real-Time Monitor
- Remote Filtering Client Pack
- Linking Service

Windows or Linux

- Filtering Service
- Network Agent
- Usage Monitor
- User Service
- Logon Agent
- eDirectory Agent
- RADIUS Agent
- State Server
- Multiplexer
- Remote Filtering Server
- Sync Service
- Directory Agent

Enter the IP address of the Policy Server machine and the Policy Server communication port (default is 55806).

- The Policy Server communication port must be in the range 1024-65535.
- During installation, Policy Server may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Server instances.) To verify the port:
  1. Navigate to the Websense **bin** directory on the Policy Server machine (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/, by default).
  2. Open the **websense.ini** file in a text editor.
  3. Locate the **PolicyServerPort** value.
  4. When you are finished, close the file without saving. Do **not** modify the file.

If your deployment includes Websense V-Series Appliances:

- Policy Server is installed on the **full policy source** appliance and any **user directory and filtering** appliances.
- If Policy Server is running on any appliance, enter the IP address of the appliance’s C interface.

  Note that when Policy Server resides on an appliance, you must enable the on-appliance Multiplexer or Directory Agent, rather than connecting an off-appliance (software-based) instance of the service to the on-appliance Policy Server.

If Policy Server is not currently installed anywhere in your network, you must install it before any of the components listed above.

- To install Policy Server on this machine, click **Previous**, then add **Policy Server** to the components selected for installation.
- To install Policy Server on another machine, run the TRITON Unified Installer or Web Security Linux Installer on that machine first, before continuing to attempt installation on the current machine.

Policy Broker Connection Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if Policy Server, Sync Service, or Directory Agent is selected for installation, but Policy Broker is not.

Enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

- If Policy Broker is installed on this machine, enter its actual IP address (not the loopback address).
- In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.
- The Policy Broker communication port must be in the range 1024-65535. During installation, Policy Broker may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Broker instances.) To verify the port:
  1. Navigate to the Websense **bin** directory on the Policy Server machine (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/, by default).
  2. Open the **BrokerService.cfg** file in a text editor.
  3. Locate the **listen_port** value.
  4. When you are finished, close the file without saving. Do **not** modify the file.

If Policy Broker is not installed anywhere in your network, you must install it before **any other** Web Security component.

- To install Policy Broker on this machine, click **Previous**, then add **Policy Broker** to the components selected for installation.
- To install Policy Broker on another machine, run the TRITON Unified Installer or Web Security Linux Installer on that machine first, before continuing to attempt installation on the current machine.

Filtering Service Communication Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if Network Agent, a filtering plug-in, or Linking Service (Windows only) is selected for installation.

Enter the IP address of the Filtering Service machine and the port Filtering Service uses to communicate with Network Agent, Content Gateway, or third-party integration products (default is 15868).

- If Filtering Service is installed on this machine, enter its actual IP address (not the loopback address).
- In an appliance-based deployment, Filtering Service is installed on all Web Security appliances (full policy source, user directory and filtering, and filtering only).
  - Enter the IP address of the appliance's C interface and use the default port (15868).
  - If you have multiple appliances, be sure to select the one you want Network Agent, the filtering plug-in, or Linking Service to use.
- The Filtering Service communication port must be in the range 1024-65535. During installation, Filtering Service may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Filtering Service instances.) To verify the port:
  1. Navigate to the Websense **bin** directory on the Policy Server machine (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/, by default).
  2. Open the **eimserver.ini** file in a text editor.
  3. Locate the **WebsenseServerPort** value.
  4. When you are finished, close the file without saving. Do **not** modify the file.

If Filtering Service is not installed anywhere in your network, you must install it before installing Network Agent, a filtering plug-in, or Linking Service.

- To install Filtering Service on this machine, click **Previous**, then add **Filtering Service** to the components selected for installation.

- To install Filtering Service on another machine, run the TRITON Unified Installer or Web Security Linux Installer on that machine first, before continuing to attempt installation on the current machine.

Important

Make sure to select the correct integration mode for the Filtering Service instance (standalone or integrated with a supported product).

Multiple Network Interfaces Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if multiple network interface cards (NICs) are detected on this machine.

Select the IP address of the NIC that Web Security components should use for communication. This NIC will also 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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 410.

Integration Option Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if Filtering Service is selected for installation.

Indicate whether this is a standalone or integrated installation, then click **Next**.

- **Stand-alone**: Websense Network Agent is responsible for monitoring all Internet requests and sending them to Filtering Service for evaluation. Network Agent also sends block messages to users attempting to access filtered content.

  ✓ **Note**
  To enable standalone Web Security, Network Agent must be installed in your network.

- **Integrated with another application or device**: Content Gateway or a third-party firewall, proxy server, cache, or network appliance (integration product) is responsible for monitoring Internet requests and sending them to Filtering Service for evaluation. Supported integration options include:
  - Websense Content Gateway
  - Check Point
  - Cisco ASA, Content Engine, PIX, or router
  - Citrix
  - Websense ICAP Server
  - Microsoft Forefront TMG
  - Other supported integration (as a “universal” integration)

  In an integrated environment, Filtering Service sends block pages, if necessary, to users attempting to access filtered content. 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.

If you select the integrated option, the next screen prompts you to identify which integration product you are using.

Select Integration Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This 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**.

- If you are installing Web Security Gateway or Gateway Anywhere, select **Websense Content Gateway** as the integration product.
- If you selected Forefront TMG, a message is displayed, explaining that the integration requires a Websense plug-in that must be installed with a separate installer.

  As the message indicates, complete this installation process to install Filtering Service 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 539.

(Windows only) If you selected Filtering Plug-In for installation, the **Select Integration** screen shows only one option: Citrix. No other filtering plug-ins can be installed using this installer.

If you want to integrate Web Filter or Web Security with Citrix products, see *Integrating Web Security with Citrix*, page 513.

Network Agent and Firewall Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This installer screen appears if you select Check Point as the integration product on the *Select Integration Screen* and include Network Agent as a component to install.

Do not install Network Agent 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.

Network Card Selection Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if Network Agent is selected for installation, even if the machine only has one network interface card (NIC).

Select the NIC that Network Agent should use to communicate with other Web Security components, then click **Next**.

- All enabled NICs with an IP address are listed.
- 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 *Network Agent and stealth mode NICs*, page 685.

✓ **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).

Database Information Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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 this version*, page 2, 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.

If you are using SQL Server clustering, enter the virtual IP address of the cluster.

After entering the IP address of the database engine machine, choose how to connect to the database:

- Select **Trusted connection** to use a Windows account to connect to the database. Enter the user name and password of a trusted account with local administration privileges on the database machine. Note that the trusted account you specify here should be the same as that with which you logged onto this machine before starting the Websense installer.

  If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in TRITON - Web Security and its reporting tools. See *Using a batch file for Apache SSL certificate file operations*, page 727
- Select **Database account** to use a SQL Server account to connect to 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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 (x86)\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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if Filtering Service or Network Agent is selected for installation.

Indicate whether you want Websense software to send feedback to Websense, Inc., then click **Next**.

Sending feedback helps improve the accuracy of Websense software for all customers. Information is sent about security URLs and any URLs that could not be categorized. Uncategorized URLs are evaluated and, if warranted, added to a Master Database category.

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 to enable or disable feedback (WebCatcher) on the **Settings** > **General** > **Account** page in TRITON - Web Security.

Directory Service Access Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if User Service, DC Agent (Windows only), 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 whose directory includes the users to whom you plan to apply user- or group-based policies.
- 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 the TRITON - Web Security Help.
- On Windows, configure the Websense User Service service to **Log on as** a Domain Admin user:
  a. Open the Windows Services dialog box (**Start** > **Administrative Tools** > **Services**).
  b. Right-click **Websense User Service** and select **Properties**, then click the **Log On** tab.
  c. Under **Log on as**, select **This account** and enter the domain\username and password (twice) of the trusted account you specified during installation.

d. Click **OK**.

e. A message appears informing you the account you specified has been granted the Log On As A Service right. Click **OK**.

f. A message appears informing you the new logon name will not take effect until you stop and restart the service. Click **OK**.

g. Click **OK** to exit the service properties dialog box.

h. Right-click **Websense User Service** and select **Restart**.

Remote Filtering Communication Screen

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

This screen appears if Remote Filtering Server is selected for installation.

The external IP address or hostname of the firewall or gateway must be visible from outside the network. If you enter a hostname, it must be in the form of a fully-qualified domain name:

```
machine_name.domain_name
```

- Remember whether you entered an IP address or a hostname here. When installing Remote Filtering Client on user machines, you must enter this address in the same form (IP address or name).
- It is a best practice to use IP addresses, rather than hostnames, unless you are confident of the reliability of your DNS servers. If hostnames cannot be resolved, Remote Filtering Clients cannot connect to 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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). To find the ports used by Filtering Service:

1. Navigate to the Websense **bin** directory on the Policy Server machine (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/, by default).
2. Open the **eimserver.ini** file in a text editor.
3. Locate the **WebsenseServerPort** (filtering port) and **BlockMsgServerPort** (block page port) values.
4. When you are finished, close the file without saving. Do **not** modify the 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

See *System requirements for this version*, page 2, 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**
> If you are using 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**. For Email Security Gateway/Anywhere, the server role must be sysadmin.

   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. The Email Security Gateway/Anywhere user account must have **sysadmin** 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

You use the same Websense installer to install most Data Security components as you do to install the TRITON Unified Security Center and TRITON infrastructure.

If you plan to install a Data Security component, the TRITON components must already be installed in your network along with the Data Security Management Server software. See *Creating a TRITON Management Server*, page 180.

To install an additional Data Security component:

1. Launch the Websense installer on the appropriate machine.
2. Choose the Custom installation type.
3. Click the **Install** link for Data Security.
4. Select the agent to install when prompted to select a component.

Not all Data Security components may show in the **Select Components** screen. The components that are offered depends on the operating system of the machine and applications detected by the installer. For example, if a print server is found, then the Printer Agent option appears. If ISA Server is found, the ISA agent is offered.

Possible options include:

- **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.
- **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/TMG Agent**: receives all Web connections from Microsoft ISA Server or Forefront TMG 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.

For instructions on installing each agent, refer to the chapter, *Installing Data Security Components*, page 315. Each agent has prerequisites and best practices that must be followed.

This chapter also describes how to install Linux-based components such as the protector and mobile agent.

Installing Email Security components

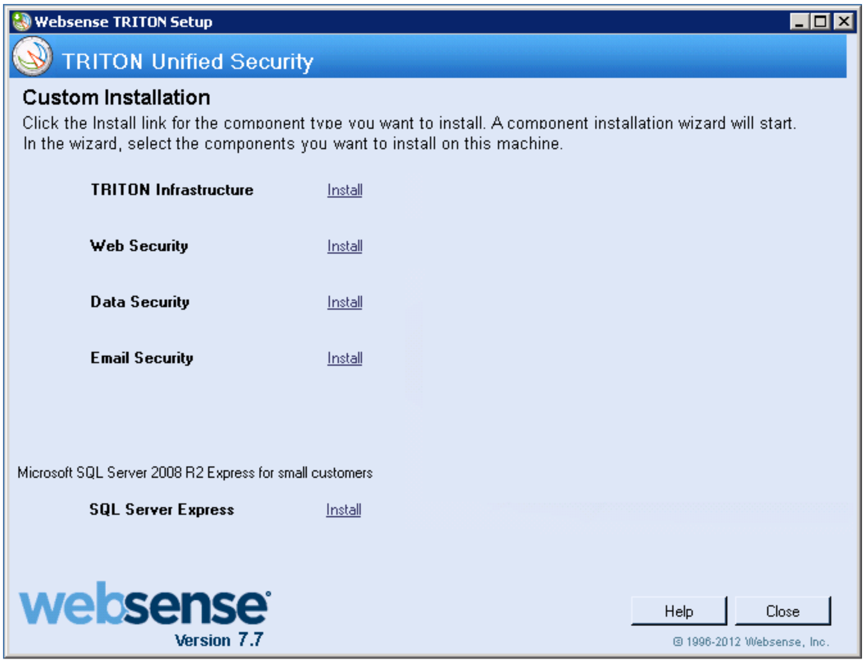
Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Gateway Anywhere, v7.7.x

Websense Email Security Gateway is an appliance-based solution. All components run on the appliance except TRITON - Email Security (i.e., the Email Security module of the TRITON 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 and chosen the Custom installation type. If not, see *Deployment*, page 383.
2. On the **Custom Installation** dashboard, click the **Install** link for Email Security.



Custom Installation

Click the Install link for the component type you want to install. A component installation wizard will start. In the wizard, select the components you want to install on this machine.

TRITON Infrastructure	Install
Web Security	Install
Data Security	Install
Email Security	Install

Microsoft SQL Server 2008 R2 Express for small customers

SQL Server Express	Install

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 TRITON - Email Security*, page 190, for instructions.

   If TRITON Infrastructure is not detected, then the Email Security Installer operates in custom mode.
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 must already be installed and running in your network. (See *System requirements for this version*, page 2, for supported database systems.)

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 **Email Security 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.

   - You may specify whether the connection to the database should be encrypted.

     Please note the following issues associated with using this encryption feature:

     - You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.
     - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
     - The connection from the Email Security module on the TRITON Console to the V-Series appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.

   - **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 411.

   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. 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. However, 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)

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

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 386.

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 16.

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 the MSDE Log Database*, page 764, 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 *Starting a 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 *Initial Configuration for All Websense Modules*, page 675, for instructions.

    b. Restore the backed up data to SQL Server Express.

       See *Restoring Websense data to SQL Server Express*, page 764, for instructions.

    c. Configure Log Server to use the installation of SQL Server Express.

       See *Configuring 7.5 Log Server to connect to SQL Server Express prior to upgrade to 7.7*, page 768, for instructions.

       This must be done or the Websense installer will be unable to upgrade Log Server to version 7.7. Note that Log Server may be running on a different machine.

18 Installing and Deploying Websense Endpoint Clients

Deployment and Installation Center | Web and Data Security Solutions | Version 7.7.x

Applies to:	In this topic
- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x - Data Security, v7.7.x	- *When to use Web Endpoint*, page 422 - *When to use the Remote Filtering Client*, page 422 - *When to use Data Endpoint*, page 423 - *Endpoint solution system requirements*, page 423

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 422)
- Websense Web Endpoint (see *When to use Web Endpoint*, page 422)

And for data loss prevention (DLP):

- Websense Data Endpoint (see *When to use Data Endpoint*, page 423)

Websense endpoint solutions include both server and client components. See *System requirements for this version*, page 2, for information about the hardware requirements and supported operating systems for endpoint components.

When to use the Remote Filtering Client

Remote filtering software can be used with any Web Security solution to manage Internet activity for endpoint devices (client machines) outside the network.

Remote filtering software has 2 components: Remote Filtering Client and Remote Filtering Server.

- Remote Filtering Client is installed on each endpoint device (client machine).

> **Warning**
>
> Remote Filtering Client **cannot** be installed on machines running Remote Filtering Server. That combination eventually causes filtering to fail.

> **Important**
>
> In Web Security Gateway Anywhere deployments, Remote Filtering Client cannot be used on machines filtered by the hybrid service.

- Remote Filtering Server resides inside the network, and acts as a proxy to Websense Filtering Service.

Internet requests from clients using remote filtering software are processed as follows:

1. Remote Filtering Client routes Internet requests to Remote Filtering Server.
2. Remote Filtering Server forward the requests to Websense Filtering Service.
3. Filtering Service determines whether to block or permit the request.
4. Filtering Service sends the block or permit response to Remote Filtering Server.
5. Remote Filtering Server responds to Remote Filtering Client.

All communication between the client and server is authenticated and encrypted.

By default, the remote filtering software manages all HTTP, HTTPS, and FTP requests from machines where Remote Filtering Client is installed.

Remote filtering software can apply a user, group, or OU policy to a request, or the Default policy. (IP-address-based policies, applied to the computer or network, cannot be applied to machines when they are outside the network.)

When to use Web Endpoint

In Websense Web Security Gateway Anywhere deployments, Websense Web Endpoint can be used to secure client machines whose Internet activity is managed by the hybrid service. Web Endpoint provides transparent authentication and enforces the use of hybrid Web security policies.

Web Endpoint routes Internet requests to the hybrid service so that the appropriate Web security policy can be applied.

Web Endpoint has 2 operation modes:

- In **Web scanning and filtering** mode, 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.
- In **proxy manipulation** mode, 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 for this version, page 2, 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

Deployment and Installation Center | Web and Data Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x	◆ *Creating installation packages*, page 425 ◆ *Deployment options*, page 436

There are different methods for configuring and packaging endpoint client software depending on which endpoint client or combination of clients you are using:

- When Web Endpoint is installed by itself on client machines, use the endpoint package provided on the **Settings** > **Hybrid Configuration** > **Hybrid User Identification** page in TRITON - Web Security.
  - Different endpoint packages are available for 32-bit and 64-bit clients; select the appropriate package (or combination of packages) from the list provided.
  - When you select an endpoint package, a GPO command is displayed on the page. Use the command provided if you intend to deploy the Web Endpoint MSI package to client machines via GPO.

  See the TRITON - Web Security Help for more information about downloading and deploying Web Endpoint.
- When Web Endpoint is installed with Data Endpoint, use the Websense Endpoint Package Builder (see below) to create a combined installation package for both the Web and Data Endpoints.

  The combined installation package (a single executable file) is used to deploy both endpoint clients to user machines.
- When Remote Filtering Client or Data Endpoint is installed alone, or when the two endpoint clients are installed together, use the Websense Endpoint Package Builder (see below) to create an installation package.

The Endpoint Package Builder is a Windows utility that can be used to create 32- and 64-bit Windows packages for Remote Filtering Client, Web Endpoint, and Data Endpoint. It can also be use to create Linux packages for Data Endpoint.

- The utility can run on any Windows machine to create or configure Remote Filtering Client installation packages.
- The utility must run on a machine with Data Security components installed to create or configure Data Endpoint packages.

The package builder can be found in the following directories:

- If Web Security is installed:

  `C:\Program Files` *or* `Program Files (x86)\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\`

- If Data Security is installed:

  `C:\Program Files` *or* `Program Files (x86)\Websense\Data Security\client\`

Creating installation packages

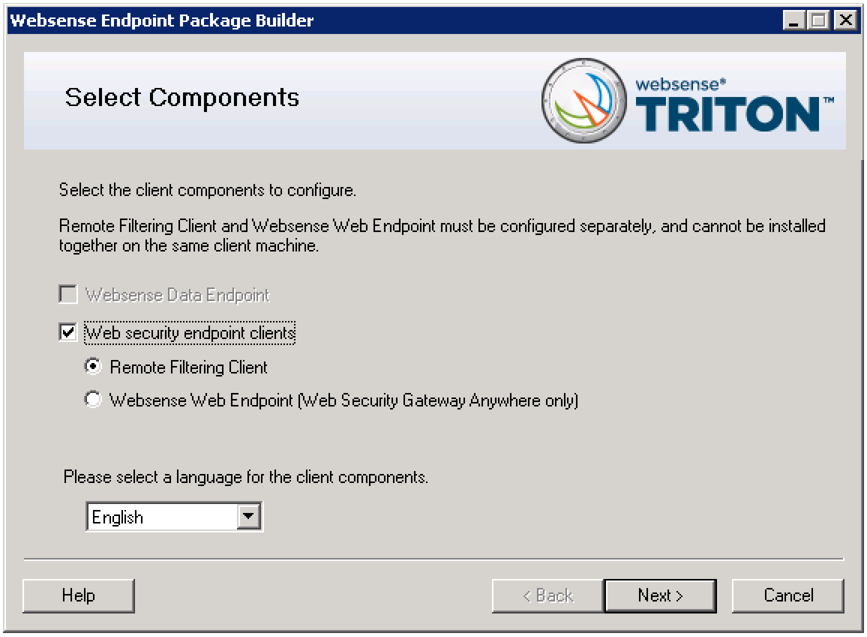
> ✓ **Note**
>
> If you existing versions of Data Endpoint or Remote Filtering Client are running on client machines, uninstall them before deploying the new installation packages.

1. To launch the Websense Endpoint Package Builder:
   - On any Windows server that includes Web Security components, navigate to **C:\Program Files** *or* **Program Files (x86)\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack** and double-click **WECfg.exe**.

     If you don't want to run the package builder on the server machine, copy the executable to another Windows machine (server or workstation) and run the executable there.
   - On the Data Security Management Server machine, navigate to **Start** > **All Programs** > **Websense** > **Data Security** > **Endpoint Package Builder**.

   The Websense Endpoint Package Builder utility extracts required files and launches.

2. On the **Select Components** screen, select one or more endpoint clients to configure. You can create packages for both Websense Data Endpoint and one Web Security endpoint client, but you cannot select both Remote Filtering Client and Web Endpoint at the same time.



Websense Endpoint Package Builder

Select Components

Select the client components to configure.

Remote Filtering Client and Websense Web Endpoint must be configured separately, and cannot be installed together on the same client machine.

☐ Websense Data Endpoint

☑ Web security endpoint clients

● Remote Filtering Client

○ Websense Web Endpoint (Web Security Gateway Anywhere only)

Please select a language for the client components.

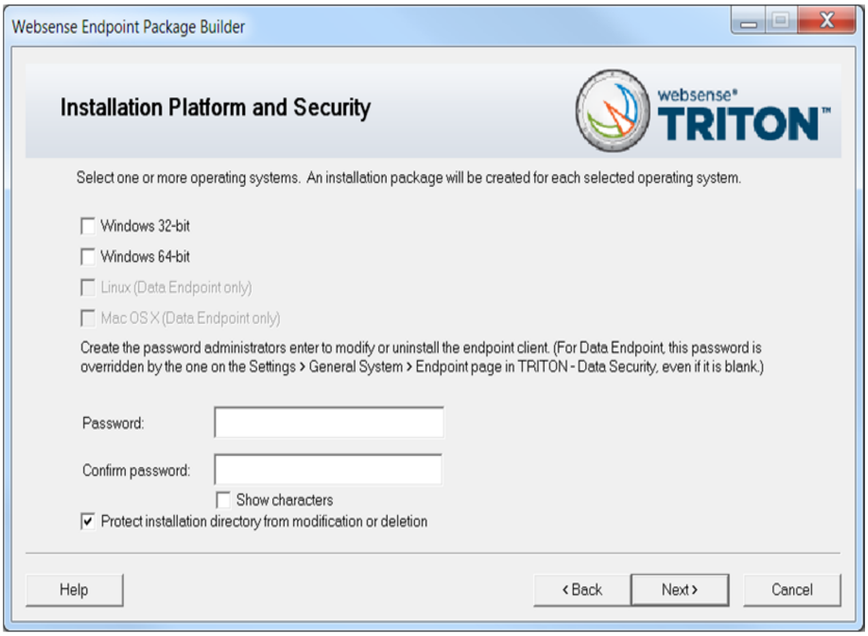
English

Also select a language for the client components.

In the TRITON Console, you can change the language used for displaying messages to Data Endpoint users, but the language displayed in the user interface (buttons, captions, fields, etc.) can only be set during packaging.

Click **Next** when you’re done.

3. On the **Installation Platform and Security** screen, select the operating system or systems for which you want to create an installation package, create the administrator password that will be used to uninstall or modify endpoint client software, and configure anti-tampering settings. When you are finished, click **Next**.



Installation Platform and Security

Select one or more operating systems. An installation package will be created for each selected operating system.

□ Windows 32-bit

□ Windows 64-bit

□ Linux (Data Endpoint only)

□ Mac OS X (Data Endpoint only)

Create the password administrators enter to modify or uninstall the endpoint client. (For Data Endpoint, this password is overridden by the one on the Settings > General System > Endpoint page in TRITON - Data Security, even if it is blank.)

Password:

Confirm password:

□ Show characters

☑ Protect installation directory from modification or deletion

- You can create Windows (32-bit or 64-bit) installation packages for any endpoint client. For Data Endpoint, you can also create a Mac OS X or Linux installation package.
- For security purposes, anyone who tries to modify or uninstall endpoint software is prompted for a password.

  For Web Endpoint and Data Endpoint, once the endpoint client contacts the server, this password is overwritten with the password specified by a TRITON administrator.

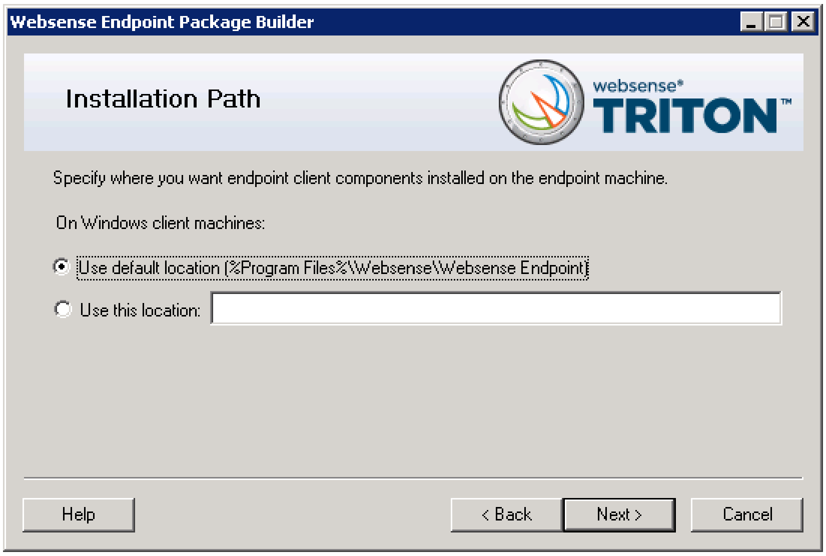
  - Data Endpoint: Administrators can set this password on the General tab under **Settings** > **General** > **System** > **Endpoint**.
  - Web Endpoint: Go to **Settings** > **Hybrid Configuration** > **Hybrid User Identification**, then enter and confirm an anti-tampering password.

  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.
- 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.

4. On the **Installation Path** screen appears, specify the directory to use for installing endpoint software on each endpoint device. The directory path must contain only English characters.



Websense Endpoint Package Builder

Installation Path

Specify where you want endpoint client components installed on the endpoint machine.

On Windows client machines:

● Use default location (%Program Files%\Websense\Websense Endpoint)

○ Use this location:

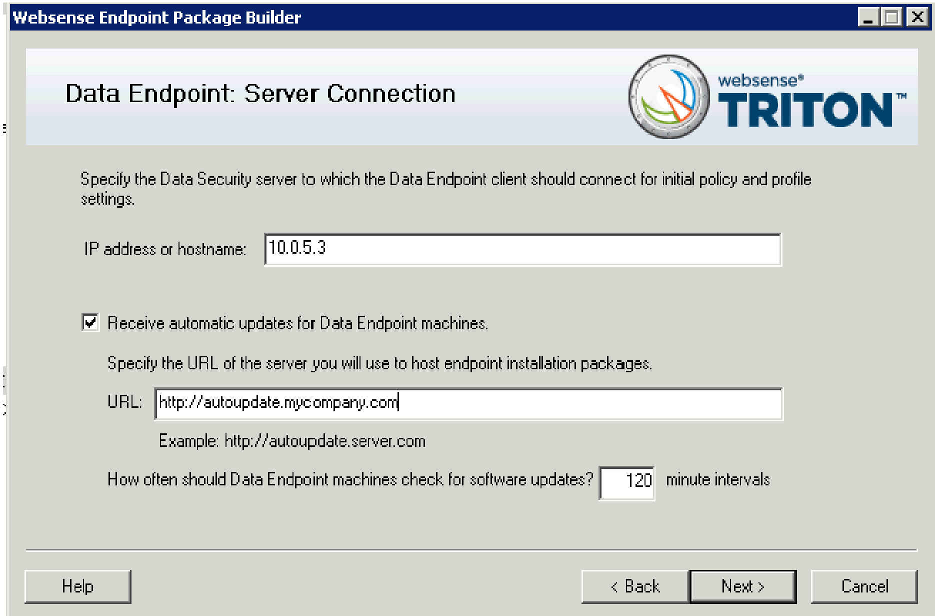
- **Use default location**: The endpoint software is installed in a default directory: \Program Files\Websense\Websense Endpoint (*Windows*) or /opt/websense/LinuxEndpoint (*Linux*).
- **Use this location**: Manually specify the installation path for the endpoint software. Environment variables are supported.

5. Click **Next**. The screens that appear next depend on the endpoint clients you chose. See:

- *Websense Data Endpoint*, page 429
- *Websense Web Endpoint*, page 431
- *Remote Filtering Client*, page 432

Websense Data Endpoint

1. If you chose Websense Data Endpoint, the Server Connection screen appears:



Data Endpoint: Server Connection

Specify the Data Security server to which the Data Endpoint client should connect for initial policy and profile settings.

IP address or hostname: 10.0.5.3

☑ Receive automatic updates for Data Endpoint machines.

Specify the URL of the server you will use to host endpoint installation packages.

URL: http://autoupdate.mycompany.com

Example: http://autoupdate.server.com

How often should Data Endpoint machines check for software updates? 120 minute intervals

IP address or hostname: 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 Endpoint machines: 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:

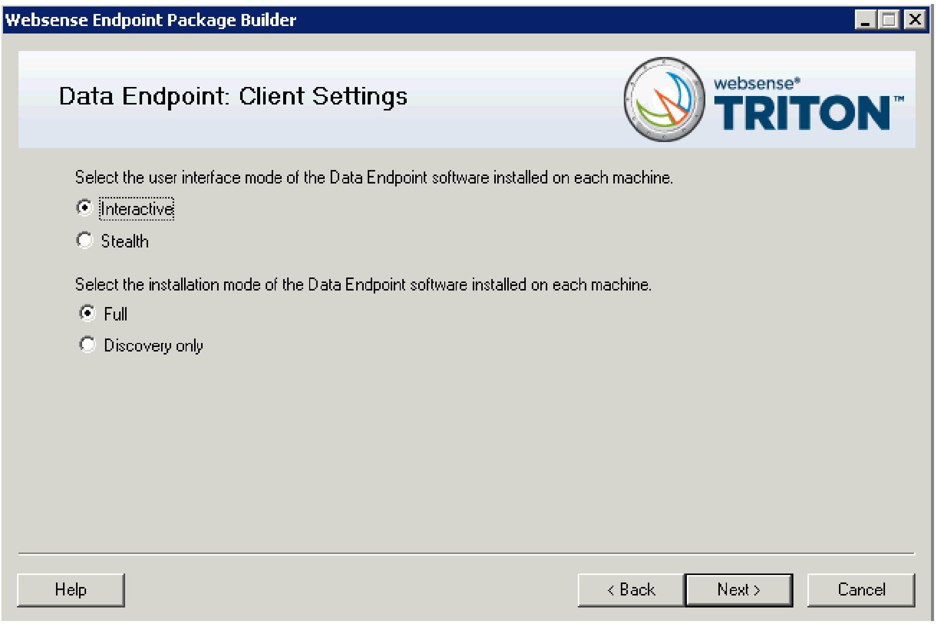
a. Prepare a server with the latest updates on it (see “Automatic Updates for Websense data endpoints” for details).

b. Select **Receive automatic updates for Data Endpoint machines**.

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:



Data Endpoint: Client Settings

Select the user interface mode of the Data Endpoint software installed on each machine.

● Interactive

○ Stealth

Select the installation mode of the Data Endpoint software installed on each machine.

● Full

○ Discovery only

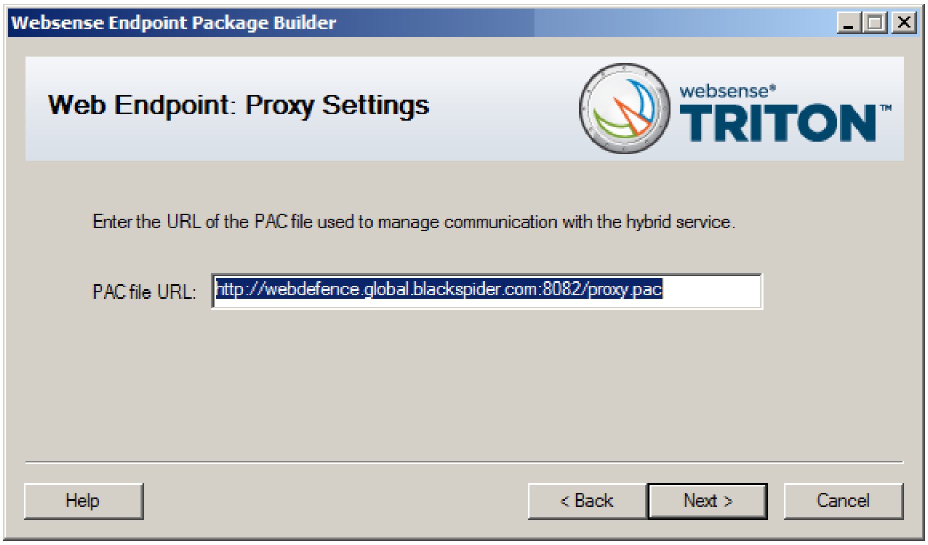
Complete the fields as follows:

User interface mode	Select from the following 2 options: • **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. • **Stealth**: The Websense Data Endpoint user interface is not displayed to the user. Note that reinstallation is required to switch user interface modes.
Installation Mode	Applies to Windows only. Select from the following 2 options: • **Full**: Installs the endpoint with full policy monitoring and blocking capabilities upon a policy breach. All incidents are reported in the TRITON Console. Endpoints that are installed in Full Mode require a reboot. • **Discovery Only**: Configures the endpoint to run discovery analysis but not DLP. Discovery Only installation does not require a reboot.

3. Click **Next**. If you chose no other endpoints, skip to *Global settings*, page 436, for instructions. Otherwise, move to *Websense Web Endpoint*, page 431, or *Remote Filtering Client*, page 432.

Websense Web Endpoint

1. If you chose Websense Web Endpoint, use the **Proxy Settings** screen to specify the URL of the hybrid PAC file.


Websense Endpoint Package Builder
Web Endpoint: Proxy Settings
websense® TRITON™
Help
< Back
Next >
Cancel

Enter the URL of the PAC file used to manage communication with the hybrid service.

PAC file URL: http://webdefence.global.blackspider.com:8082/proxy.pac

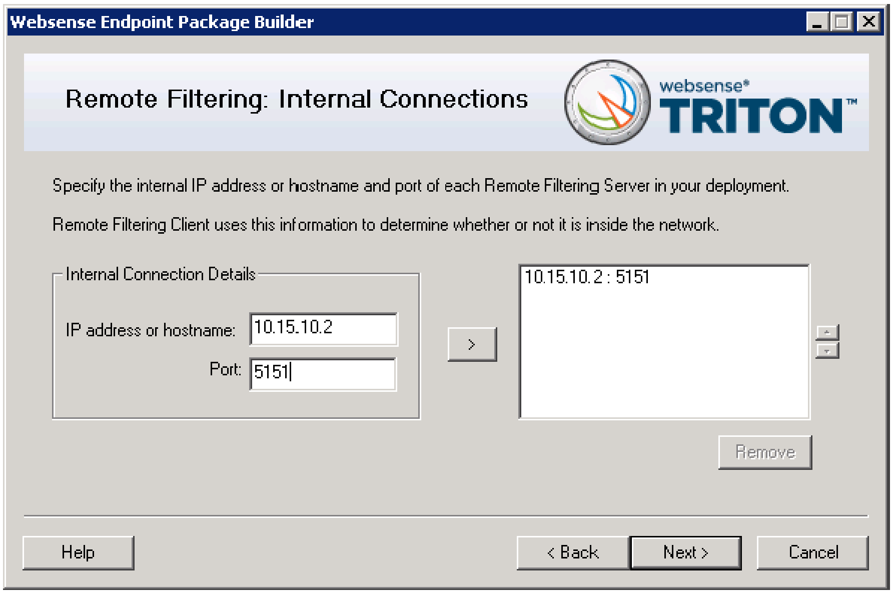
The PAC file defines how Web browsers choose an appropriate proxy for fetching a given URL. The standard proxy PAC file URL for hybrid filtering is:

http://pac.hybrid-web.global.blackspider.com:8082/proxy.pac

2. Click **Next** to continue to the Save Installation Package screen. See *Global settings*, page 436, for configuration instructions.

Remote Filtering Client

1. If you chose Remote Filtering Client, use the **Internal Connections** screen to list internal connection details for each Remote Filtering Server instance to which the clients will attempt to connect. When you are finished, click **Next**.


Websense Endpoint Package Builder
Remote Filtering: Internal Connections
websense®
TRITON™

Specify the internal IP address or hostname and port of each Remote Filtering Server in your deployment.

Remote Filtering Client uses this information to determine whether or not it is inside the network.

Internal Connection Details

IP address or hostname: 10.15.10.2

Port: 5151

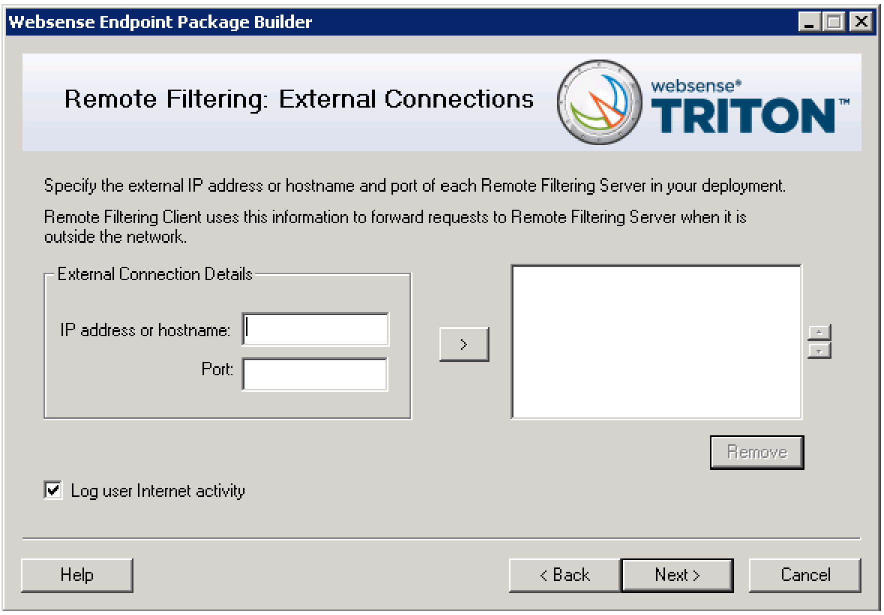
10.15.10.2 : 5151

Remove
Help
< Back
Next >
Cancel

- **IP address or hostname**: Internal IP address or FQDN for the Remote Filtering Server machine.
- **Port**: Internal communication port on the 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.

Because some machines, like laptops, may travel in and out of your organization’s network, Remote Filtering Client uses this internal connection information to determine whether it is within or outside the network. This ensures that the machine is not double filtered (by both internal Web Security components and remote filtering software).

2. On the **External Connections** screen, provide external connection details for each Remote Filtering Server that may handle requests for Remote Filtering Client instances. When you are finished, click **Next**.



Websense Endpoint Package Builder

Remote Filtering: External Connections

Specify the external IP address or hostname and port of each Remote Filtering Server in your deployment.

Remote Filtering Client uses this information to forward requests to Remote Filtering Server when it is outside the network.

External Connection Details

IP address or hostname:

Port:

☑ Log user Internet activity

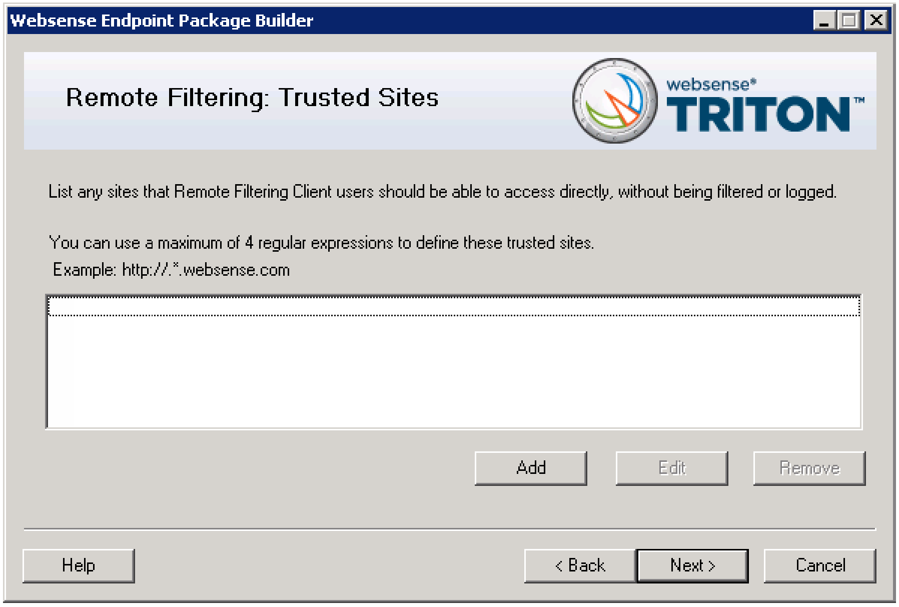
- **IP address or hostname**: Externally visible IP address or fully qualified domain name (FQDN) of the primary Remote Filtering Server machine.

> **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.
- Clear the **Log user Internet activity** check box to avoid recording Internet request data for machines running Remote Filtering Client. By default, Internet activity handled by Remote Filtering Client is logged for use in Web Security reporting tools.

This is the information that Remote Filtering Client uses to pass Internet requests to Remote Filtering Server when the client machine (endpoint device) is outside the network.

3. On the **Trusted Sites** screen, enter any URLs or domains that should be always permitted by Remote Filtering Client. Requests for these URLs or domains are not forwarded to Remote Filtering Server, and are not logged (do not appear in reports). When you are finished, click **Next**.


Websense Endpoint Package Builder
Remote Filtering: Trusted Sites
websense® TRITON™

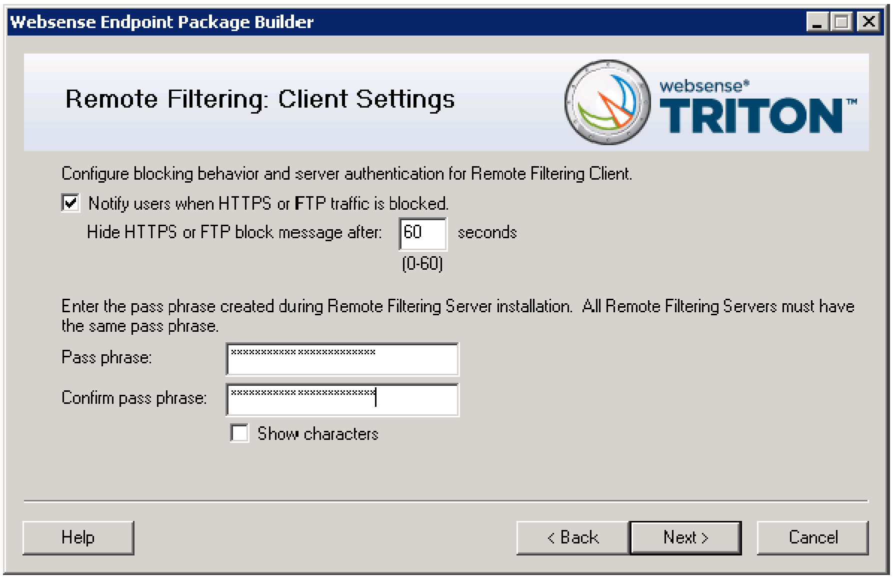
List any sites that Remote Filtering Client users should be able to access directly, without being filtered or logged.

You can use a maximum of 4 regular expressions to define these trusted sites.
Example: http://.*.websense.com

Add
Edit
Remove
Help
< Back
Next >
Cancel

- To define a trusted site, click **Add**, then enter a URL or a regular expression. Any regular expression adhering to ISO/IEC TR 19768 (within the character-number limit) is valid. When you are finished, click **OK**.
- To change an entry, select it, then click **Edit**.
- To delete an entry, select it, then click **Remove**.

4. Use the **Client Settings** screen to configure blocking behavior, the pass phrase used to encrypt communication with Remote Filtering Server, and the display language for client components. When you are finished, click **Next**.



Remote Filtering: Client Settings

Configure blocking behavior and server authentication for Remote Filtering Client.

☑ Notify users when HTTPS or FTP traffic is blocked.

Hide HTTPS or FTP block message after: 60 seconds (0-60)

Enter the pass phrase created during Remote Filtering Server installation. All Remote Filtering Servers must have the same pass phrase.

Pass phrase: ****************************

Confirm pass phrase: ****************************

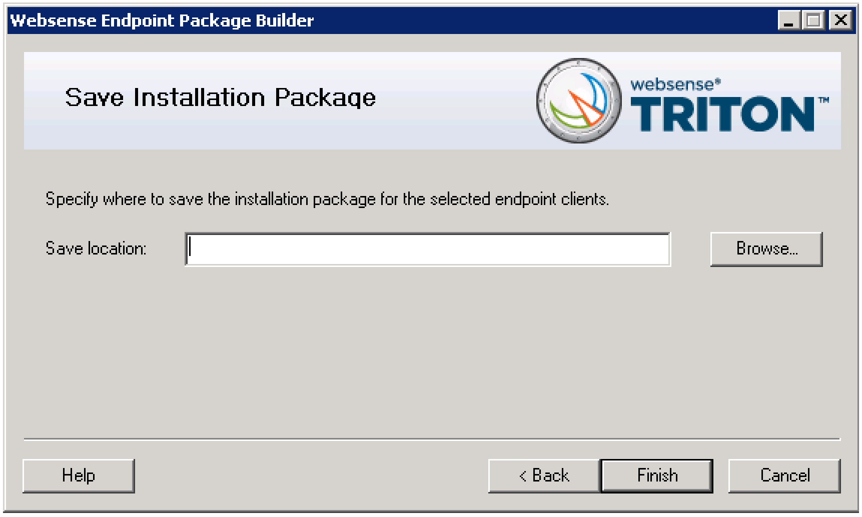
□ Show characters

- Select **Notify users when HTTPS or FTP traffic is blocked** to display a pop-up message on client machines for blocked HTTPS or FTP traffic. If you enable this option, also specify how long the pop-up message remains visible to the user.
- Enter and confirm the **Pass phrase** used to encrypt communication with Remote Filtering Server. This must be the same pass phrase that you created during Remote Filtering Server installation.
- Select the default local language for the client user interface and messages that are displayed to the user.

5. When you click **Next**, the Save Installation Package screen appears. See *Global settings*, page 436, for instructions on configuring this screen.

Global settings

1. When you're done configuring your endpoint selections, use the **Save Installation Package** screen to enter a directory path to use for storing the installation package before it is deployed to client machines.

   Specify where to save the installation package for the selected endpoint clients.

   Save location:

   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 436, for instructions on distributing the package to the endpoint devices.

Deployment options

> **Important**
> After deploying the installation package, you must restart the endpoint software to complete the installation process.

There are a few ways to distribute the endpoint software:

- Manually on each endpoint device

  See *Deploying endpoint clients manually*, page 437.

- Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS) (Windows only)

  See Creating and distributing Websense endpoints using SCCM or SMS for details.

- Using a Microsoft Group Policy Object (GPO) or other third-party deployment tool for Windows.
  - The GPO command for deploying Web Endpoint is displayed on the **Settings > Hybrid Configuration > Hybrid User Identification** page in TRITON - Web Security. Note that the command includes a WSCONTEXT parameter that is required to ensure that your organization's policies are applied to user requests.

    See Manually deploying Web Endpoint for Windows in the TRITON - Web Security Help for details.
  - Instructions for deploying Remote Filtering Client via GPO can be found under Installing with a third-party deployment tool in the Remote Filtering Software technical paper.
  - If you need assistance deploying the Data Endpoint installation package (or any installation package that includes both Data Endpoint and a Web Security endpoint client) via GPO, contact Websense Technical Support.
- Using Remote Desktop (Mac OS X only)

  See Installing Mac endpoints with Remote Desktop for details.

You can also enable Web Endpoint and Data Endpoint automatic updates to ensure that endpoint client software is kept current after the initial deployment. See:

- *Enabling automatic updates for Data Endpoint*, page 438
- *Enabling automatic updates for Web Endpoint*, page 439

To confirm that Web Endpoint or Data Endpoint is installed and running on a machine:

- 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 (W) 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 423.

If you plan to deploy multiple endpoint solutions (data and Web) on the same machine, see *Multiple agent limitations*, page 441, before proceeding.

Deploying endpoint clients manually

Windows

Windows packages contain a single executable file: **WebesenseEndpoint_32bit.exe** or **WebesenseEndpoint_64bit.exe**.

First copy this self-extracting executable file to the client machine, then:

- If the package contains only Data Endpoint, only Remote Filtering Client, or a both Data Endpoint and Remote Filtering Client, double-click it to install the endpoint client.
- If the package contains Data Endpoint and Web Endpoint, the WSCONTEXT argument (used to identify your organization to the hybrid service) must be included in the command string, as follows:

  ```
  WebsenseEndpoint_64bit.exe /v"WSCONTEXT=<token>"
  ```

  Here, <token> is the WSCONTEXT value displayed in the GPO command string on the Settings > Hybrid Configuration > Hybrid User Identification page in TRITON - Web Security.

  All arguments passed via the **/v** parameter must be enclosed in straight quotes, as shown in the example.

If you are upgrading an existing endpoint client on the Windows machine, and the old client has an anti-tampering password, you must provide the old password when you run the new installation package. For example:

```
WebsenseEndpoint_32bit.exe /v"XPSWD=<password>"
```

Here, “<password>” is the anti-tampering password used by the previous-version endpoint client. All arguments passed via the **/v** parameter must be enclosed in straight quotes, as shown in the example.

Note that if you are upgrading Web Endpoint and Data Endpoint together, you must provide both the XPSWD and WSCONTEXT arguments. For example:

```
WebsenseEndpoint_64bit.exe /v"XPSWD=<password>
WSCONTEXT=<token>"
```

Linux

Linux packages (Data Endpoint only) contain 2 installers with the same functionality:

- **LinuxEndpoint_SFX_installer_el4 -** use with Red Hat Enterprise Linux version 4.x.
- **LinuxEndpoint_SFX_installer_el5 -** use 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.

Enabling automatic updates for Data Endpoint

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.

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 any 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

Deployment and Installation Center | Web and Data Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x	◆ *Local uninstall*, page 440 ◆ *Remote uninstall*, page 441

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.

  If you use a deployment server, the uninstall command is:

  - 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.

  To find the **setup.ini** file, use a file compression tool like WinZip or 7-Zip to extract the contents of the installation package executable.

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 SDCCM 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

Deployment and Installation Center | Web and Data Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x	◆ *Multiple Websense endpoints*, page 442 ◆ *Third-party agents*, page 442

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 either Web Endpoint and Data Endpoint or 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 a single package containing 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.
- The packages created by the Websense Endpoint Package Builder are backwards compatible with previous endpoint versions.

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:

a. Go to **Edit > 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.

19 Integrating Web Security with Check Point

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:
◆ Web Filter and Web Security, v7.7.x

This section of the Deployment and Installation Center provides information specific to integrating Websense Web Security solutions with Check Point® products. Refer to *Installation overview: Web Filter and Web Security*, page 193, as your primary source of installation information. Only additional or alternative steps required to integrate with Check Point products are provided in the topics in this section.

This section includes information about:

- *Deployment considerations for integration with Check Point products*, page 445
- *Getting started with a Check Point integration*, page 449
- *Configuring Check Point products to work with Web Security solutions*, page 454
- *Configuring CheckPoint secure communication*, page 468
- *Troubleshooting Check Point integration*, page 477

Deployment considerations for integration with Check Point products

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	**In this topic**
◆ Web Filter and Web Security, v7.7.x	◆ *Simple*, page 446 ◆ *Distributed*, page 448

This section includes a general discussion of 2 common Check Point integration deployment options: simple deployment with unified components, and distributed deployment.

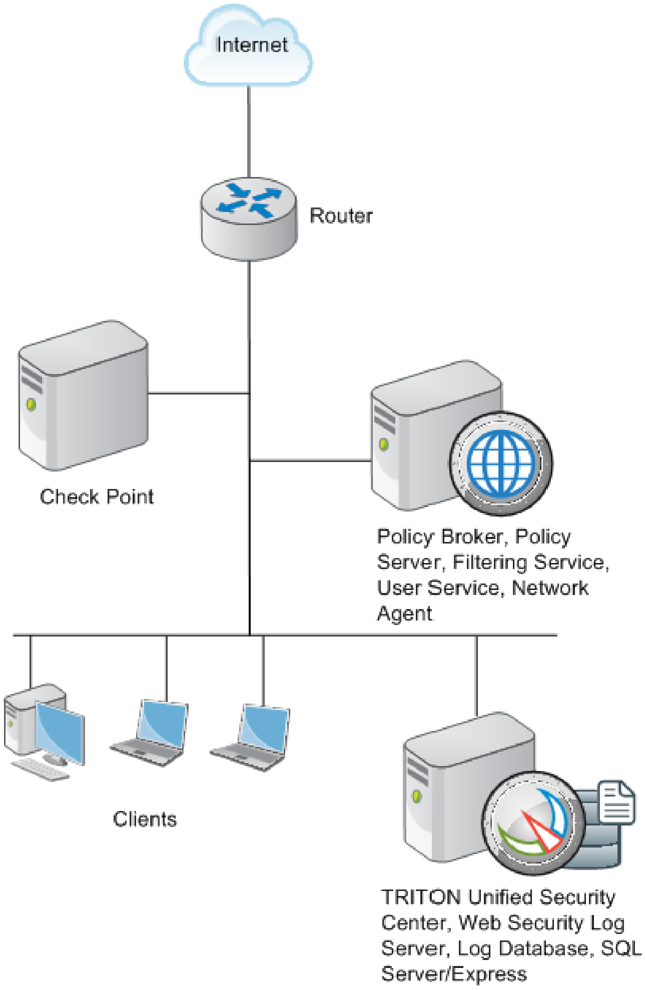
Related topics:

- *Getting started with a Check Point integration*, page 449
- *Configuring Check Point products to work with Web Security solutions*, page 454
- *Configuring CheckPoint secure communication*, page 468

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.

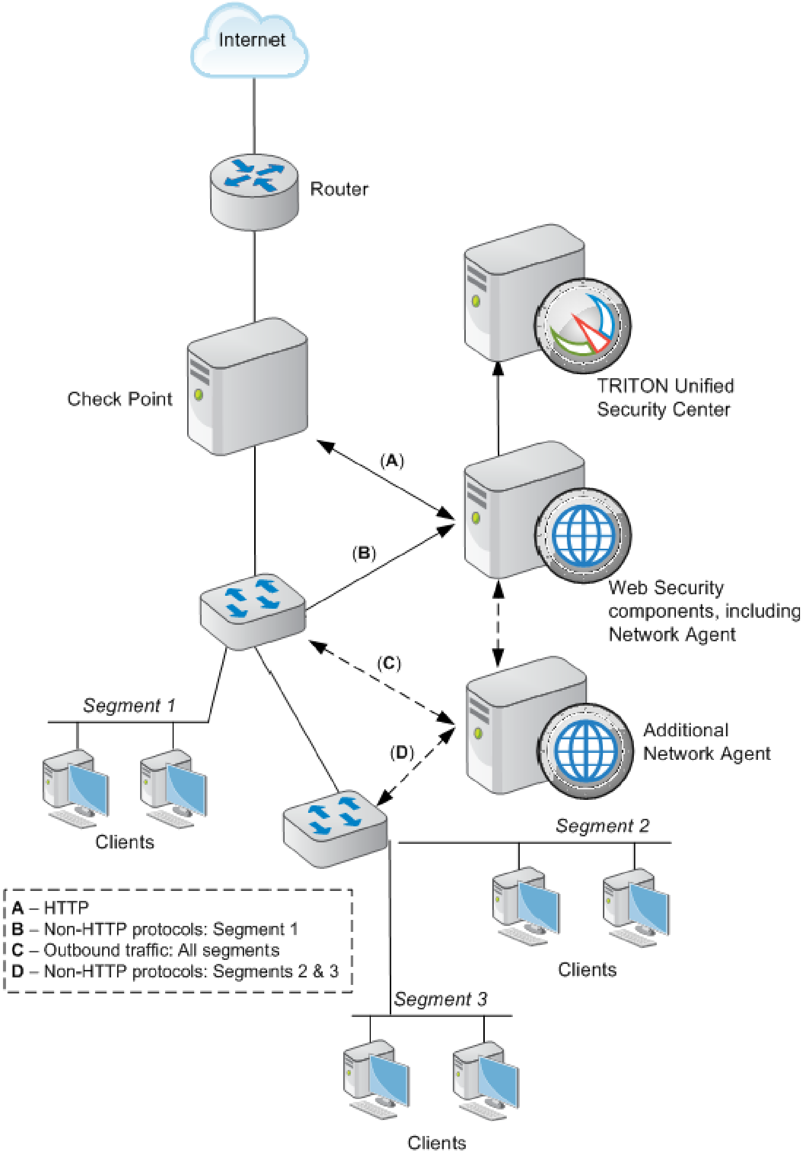
- TRITON Unified Security Center and reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network. HTTP requests are handled by the Check Point appliance, and non-HTTP traffic is managed by Network Agent, which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


Internet
Router
Check Point
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
Clients
TRITON Unified Security Center, Web Security Log Server, Log Database, SQL Server/Express

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.

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.


Internet
Router
Check Point
TRITON Unified Security Center
(A)
(B)
Web Security components, including Network Agent
(C)
Segment 1
(D)
Additional Network Agent
Clients
Segment 2
A – HTTP
B – Non-HTTP protocols: Segment 1
C – Outbound traffic: All segments
D – Non-HTTP protocols: Segments 2 & 3
Clients
Segment 3
Clients

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

Do **not** install Network Agent on the same machine as Check Point software.

Getting started with a Check Point integration

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
- Web Filter and Web Security, v7.7.x	

Websense Web Filter and Web Security are compatible with the following Check Point products:

- Check Point NGX and NGX 65
- Check Point UTM-1 (VPN-1) Edge

Websense Web Filter or Web Security integration with Check Point works as follows:

- **Websense Filtering Service** interacts with the Check Point product and Network Agent to filter Internet requests.

- **Websense 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 is separated from the Enforcement Module, 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.

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 *Configuring Check Point products to work with Web Security solutions*, page 454, 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 464, 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 392, 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 Security solutions*, page 454, for information on configuring the firewall integration with Websense software.

If Filtering Service is installed on a multihomed machine, 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 679, for instructions.

Upgrading Web Filter or Web Security when integrated with Check Point

Before upgrading Websense software, make sure your Check Point product is supported by the new version.

Follow the instructions in *Upgrading Websense Web Security Solutions*, page 579.

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 Security solutions*, page 454.

Migrating between Check Point versions

If you plan to upgrade your Check Point product (from FireWall-1 NG to 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 Websense Web Security Solutions*, page 579, 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 Security solutions*, page 454, for the necessary configuration procedures to ensure that your new version of the Check Point product can communicate with Websense software.

Configuring Check Point products to work with Web Security solutions

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Creating a network object*, page 455 ◆ *Creating an OPSEC application object*, page 456 ◆ *Creating Resource Objects*, page 458 ◆ *Defining rules*, page 461 ◆ *Configuring enhanced UFP performance*, page 464

In addition to defining Websense 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 Websense Web Filter or Web Security 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 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 455.
- Create an OPSEC™ application object for the Websense UFP Server. See *Creating an OPSEC application object*, page 456.
- Create URI resource objects for the dictionary categories that Websense software sends to the Check Point product. See *Creating Resource Objects*, page 458.
  - 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 468.

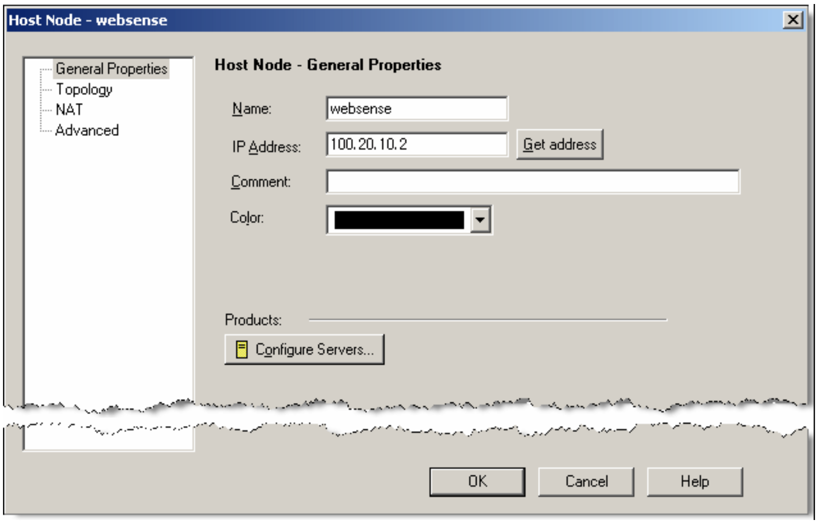
  - To return to clear communication, see *Restoring Clear Communication*, page 475.

- Define rules that govern how the Check Point product behaves when it receives a response from Websense software. See *Defining rules*, page 461.
- Optionally, you can configure the Check Point product for enhanced UFP performance. Make sure that you have configured the Check Point product for Websense content filtering before this procedure. See *Configuring enhanced UFP performance*, page 464.

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.



Name: websense

IP Address: 100.20.10.2

4. Complete the items in the page:

Field	Description
Name	Enter a descriptive name for the network object representing the Filtering Service machine, such as **WebsenseFS** (make a note of this name for later use). 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. 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.

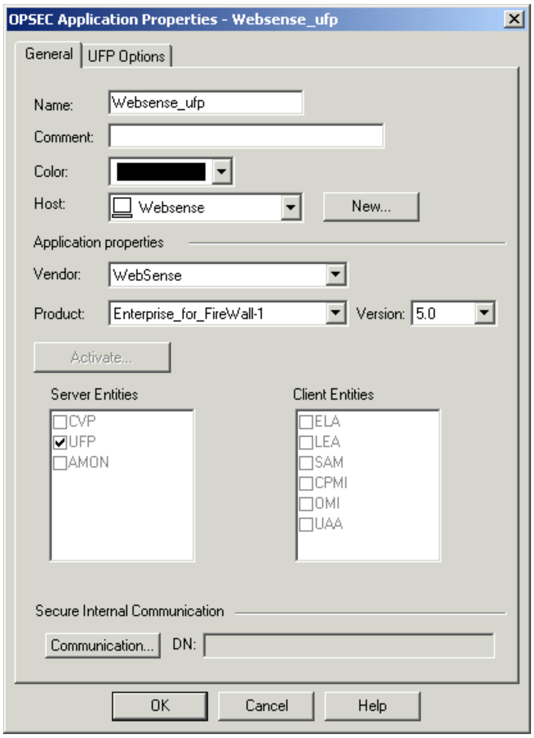
5. Click **OK**.

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:



OPSEC Application Properties - Websense_ufp

Name: Websense_ufp

Comment:

Color: ■

Host: Websense

Application properties

Vendor: WebSense

Product: Enterprise_for_FireWall-1

Version: 5.0

Server Entities

□ CVP
☑ UFP
□ AMON

Client Entities

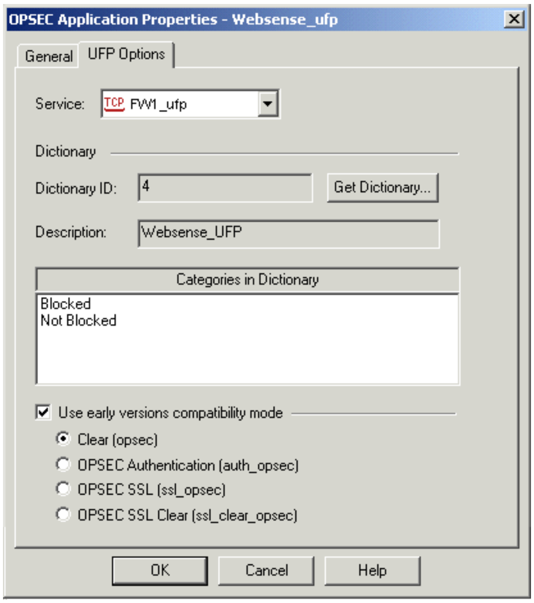
□ ELA
□ LEA
□ SAM
□ CPMI
□ OMI
□ UAA

Secure Internal Communication

DN:

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. If you have not yet created this object, click **New** to create it. See *Creating a network object*, page 455 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.



Service: FW1_ufp

Dictionary ID: 4

Description: Websense_UFP

Categories in Dictionary

Blocked
Not Blocked

☑ Use early versions compatibility mode

● Clear (opsec)
○ OPSEC Authentication (auth_opsec)
○ OPSEC SSL (ssl_opsec)
○ OPSEC SSL Clear (ssl_clear_opsec)

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 468, 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.

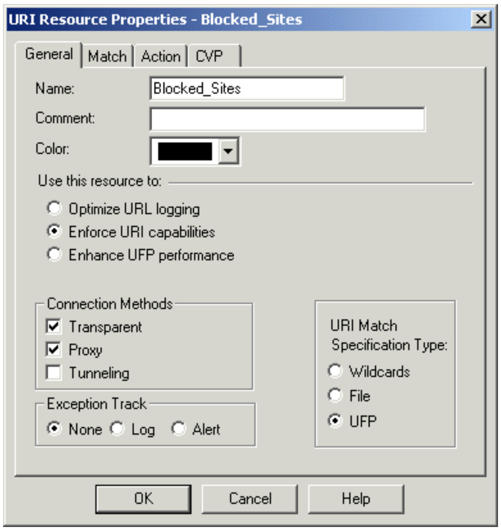
Creating Resource Objects

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.



URI Resource Properties - Blocked_Sites

Name: Blocked_Sites

Comment:

Color: ■

Use this resource to:

○ Optimize URL logging
● Enforce URI capabilities
○ Enhance UFP performance

Connection Methods

☑ Transparent
☑ Proxy
□ Tunneling

Exception Track

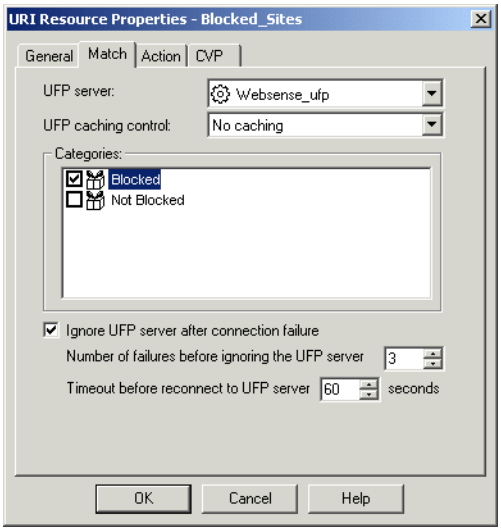
● None ○ Log ○ Alert

URI Match Specification Type:

○ Wildcards
○ File
● UFP

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**. This option enables all other functionality of the URI resource, such as configuring CVP checking on the **CVP** tab. 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 Specificatio n Type	Select **UFP**.

4. Select the **Match** tab, and complete the items in the tab.



UFP server: Websense_ufp

UFP caching control: No caching

Categories:

☑ Blocked

□ Not Blocked

☑ Ignore UFP server after connection failure

Number of failures before ignoring the UFP server 3

Timeout before reconnect to UFP server 60 seconds

Field	Description
UFP server	Select the OPSEC Application object that was created for the Websense UFP Server in *Creating an OPSEC application object*, page 456.
UFP caching control	Select a caching option. **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. 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. • 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 458.

  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.

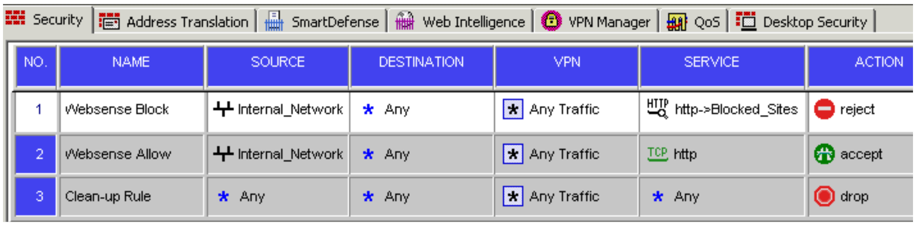
RULE 1: Blocks access to undesirable Web sites. Add the new rule at an appropriate location in the Rule Base:

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 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 458.
Action	Reject
Track	None
Install On	Policy Targets
Time	Any (default)
Comment	(NGX only) Enter a more detailed description of the rule.

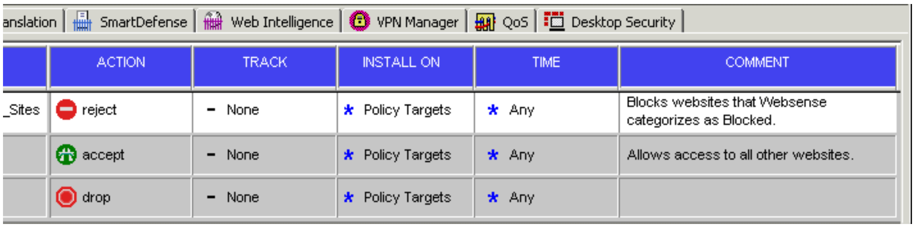
RULE 2: The second rule allows access to all other Web sites. Add the second rule *after* Rule 1.

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.



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION
1	Websense Block	Internal_Network	* Any	Any Traffic	http->Blocked_Sites	reject
2	Websense Allow	Internal_Network	* Any	Any Traffic	http	accept
3	Clean-up Rule	* Any	* Any	Any Traffic	* Any	drop



	ACTION	TRACK	INSTALL ON	TIME	COMMENT
_Sites	reject	- None	* Policy Targets	* Any	Blocks websites that Websense categorizes as Blocked.
	accept	- None	* Policy Targets	* Any	Allows access to all other websites.
	drop	- None	* Policy Targets	* Any	

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 and stopping Web Security services*, page 709, for instructions on stopping and restarting Websense services. See also *Stopping and restarting the UFP Server*, page 473.

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 465.

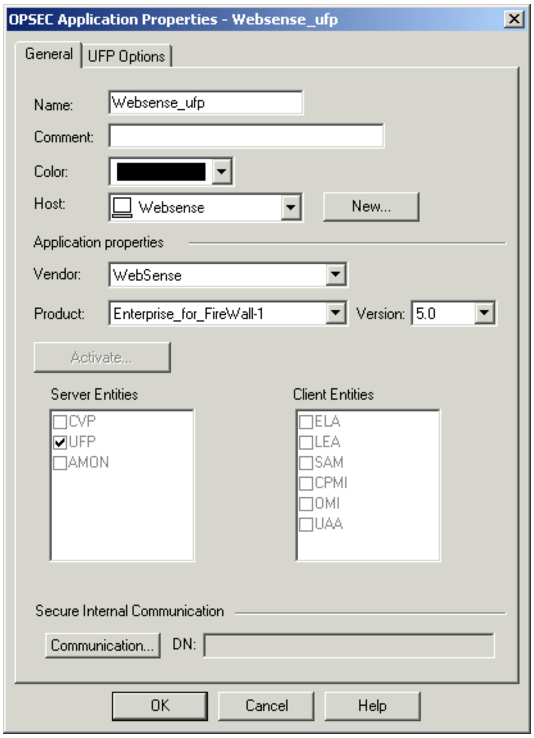
- Configure the URI Resource Object that identifies the Websense dictionary category Blocked for enhanced UFP performance. See *Enhanced UFP performance*, page 466.

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 456.

   The OPSEC Application Properties dialog box for this object appears.



OPSEC Application Properties - Websense_ufp

Name: Websense_ufp

Comment:

Color: ■

Host: Websense

Application properties

Vendor: WebSense

Product: Enterprise_for_FireWall-1

Version: 5.0

Server Entities

□ CVP
☑ UFP
□ AMON

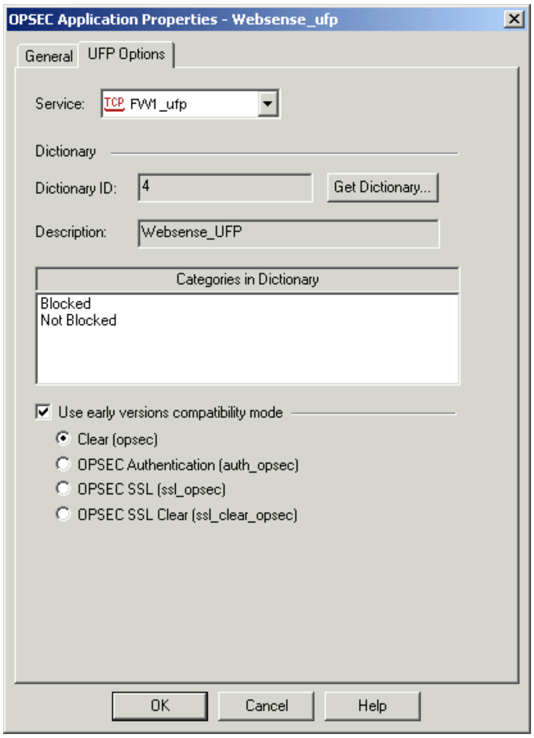
Client Entities

□ ELA
□ LEA
□ SAM
□ CPMI
□ OMI
□ UAA

Secure Internal Communication

DN:

3. Select the **UFP Options** tab.



Service: TCP FW1_ufp

Dictionary

Dictionary ID: 4

Description: Websense_UFP

Categories in Dictionary

Blocked
Not Blocked

☑ Use early versions compatibility mode

● Clear (opsec)
○ OPSEC Authentication (auth_opsec)
○ OPSEC SSL (ssl_opsec)
○ OPSEC SSL Clear (ssl_clear_opsec)

4. Select **Use early versions compatibility mode** (Backwards Compatibility in earlier versions).
5. Select **Clear (opsec)**, then click **OK** and close the Servers and OPSEC Applications dialog box.
6. Select **Policy** > **Install** to install the policy on the firewall. See Check Point product documentation for more information.

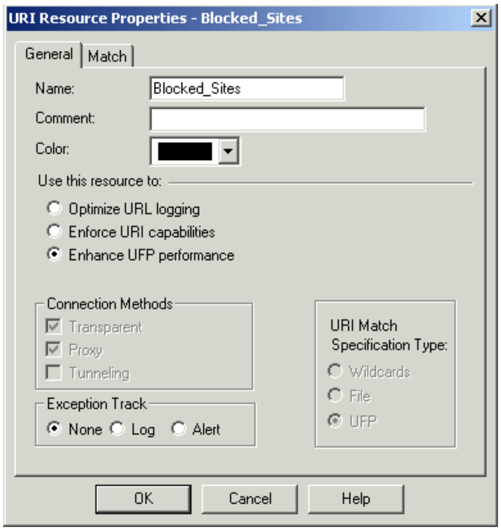
Enhanced UFP performance

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 458.

The URI Resource Properties dialog box for this resource appears.



URI Resource Properties - Blocked_Sites

General | Match

Name: Blocked_Sites

Comment:

Color: ■

Use this resource to:

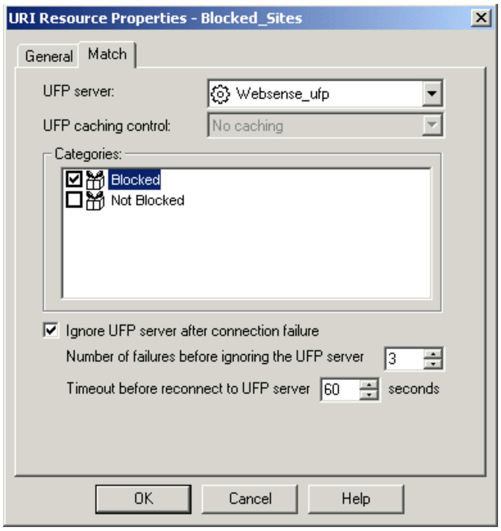
○ Optimize URL logging
○ Enforce URI capabilities
● Enhance UFP performance

Connection Methods
☑ Transparent
☑ Proxy
□ Tunneling

Exception Track
● None ○ Log ○ Alert

URI Match Specification Type:
○ Wildcards
○ File
● UFP

3. In the **General** tab, select **Enhance UFP performance**.
4. Select the **Match** tab.



URI Resource Properties - Blocked_Sites

General | Match

UFP server: Websense_ufp

UFP caching control: No caching

Categories:
☑ Blocked
□ Not Blocked

☑ Ignore UFP server after connection failure

Number of failures before ignoring the UFP server 3

Timeout before reconnect to UFP server 60 seconds

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.

Configuring CheckPoint secure communication

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Establishing Secure Internal Communication*, page 468 ◆ *Restoring Clear Communication*, page 475

ISecure Internal Communication (SIC) may be needed when you integrate a Check Point product with Websense software. Following are instructions for enabling and disabling this communication method.

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 469.
- Configure Websense software to use Secure Internal Communication. See *Configuring Websense software to use SIC*, page 471.
- Update the OPSEC Application object within the Check Point product to receive secure communications from Websense software. See *Updating the OPSEC Application object*, page 473.

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.

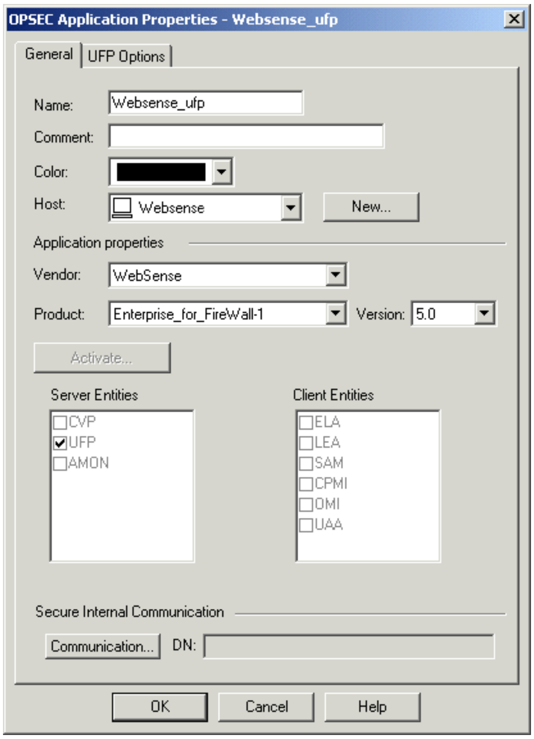
- Both the Check Point product and Websense software must already be installed and running.
- In the Check Point product, create the following objects:
  - An object for the firewall. Consult Check Point product documentation for instructions.
  - Network Objects that represent your network topology (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 456.

> **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 456.

   The OPSEC Application Properties dialog box for this object appears.



OPSEC Application Properties - Websense_ufp

General | UFP Options

Name: Websense_ufp

Comment:

Color: ■

Host: Websense

Application properties

Vendor: WebSense

Product: Enterprise_for_FireWall-1 Version: 5.0

Server Entities: □ CVP ☑ UFP □ AMON

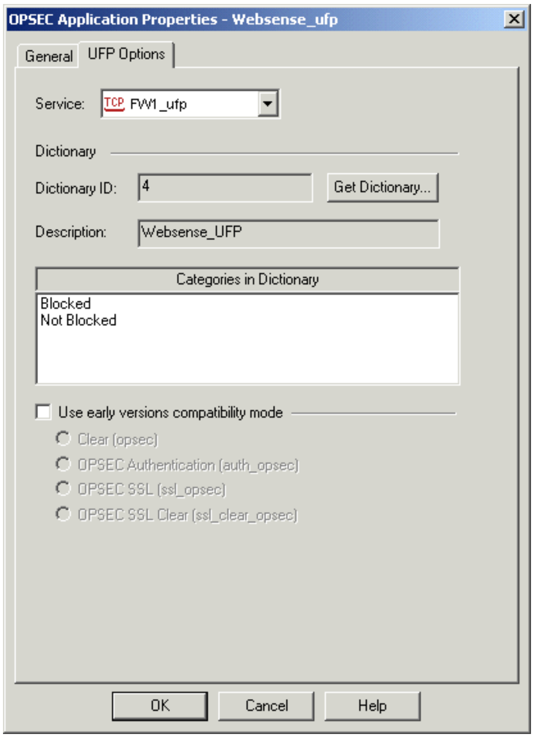
Client Entities: □ ELA □ LEA □ SAM □ CPMI □ OMI □ UAA

Secure Internal Communication

DN:

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.



Service: TCP FW1_ufp

Dictionary ID: 4

Description: Websense_UFP

Categories in Dictionary

Blocked
Not Blocked

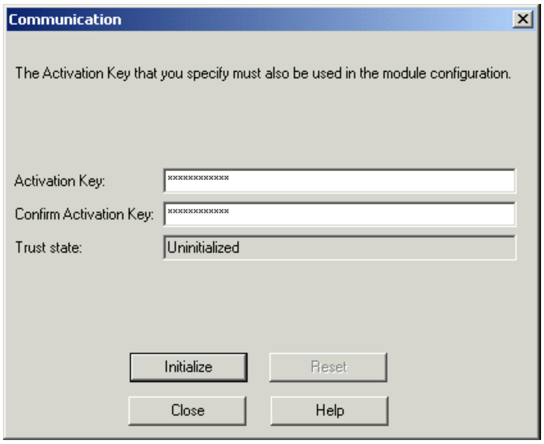
☐ Use early versions compatibility mode

○ Clear (opsec)
○ OPSEC Authentication (auth_opsec)
○ OPSEC SSL (ssl_opsec)
○ OPSEC SSL Clear (ssl_clear_opsec)

   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.



The Activation Key that you specify must also be used in the module configuration.

Activation Key: ************

Confirm Activation Key: ************

Trust state: Uninitialized

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, then click **OK**.
8. Close the **Servers and OPSEC Applications** dialog box.
9. 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 469.
<path>	Path to the output certificate file, **opsec.p12**. This variable must be expressed as a complete path. ◆ If the OPSECDIR variable already exists, the default path is **$OPSECDIR/opsec.p12**. ◆ 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 and stopping Web Security services*, page 709, for instructions on stopping and restarting Websense services. See also *Stopping and restarting the UFP Server*, page 473.

Stopping and restarting the UFP Server

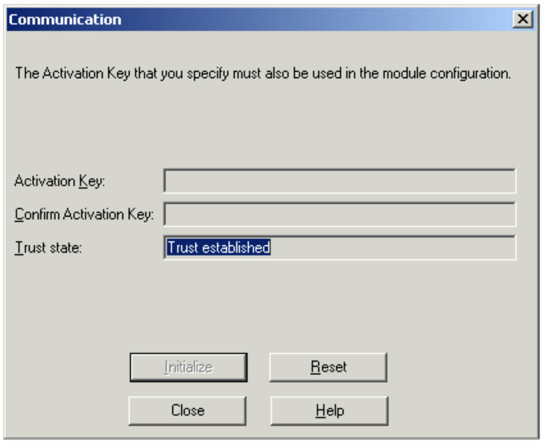
Filtering Service must be running for the Websense UFP Server to function. When the Filtering Service is stopped, the UFP Server is automatically shut down. The UFP Server must be restarted manually. If the UFP Server is started first, it automatically starts the Filtering Service. Stopping or starting 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 456.

   The OPSEC Application Properties dialog box for this object appears.
3. Click **Communication**.
4. Verify that the Trust state field shows **Trust established**.



Communication

The Activation Key that you specify must also be used in the module configuration.

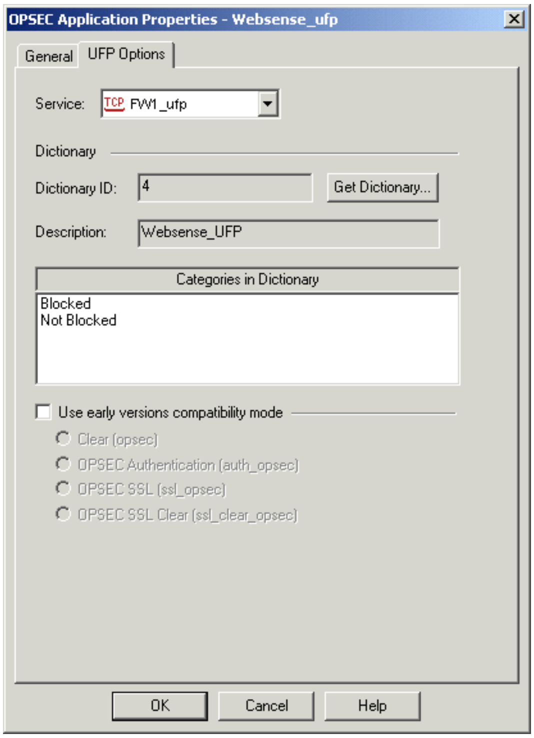
Activation Key:

Confirm Activation Key:

Trust state: Trust established

5. Click **Close** to return to the OPSEC Application Properties dialog box, then click **OK**.
6. Close the Servers and OPSEC Applications dialog box.
7. Select **Policy** > **Install** to install the policy on the firewall. See Check Point product documentation for more information.

8. Open the OPSEC Application object created for the Websense UFP Server again.
9. Go to the **UFP Options** tab of the OPSEC Application Properties dialog box for this object.



Service: TCP FW1_ufp

Dictionary

Dictionary ID: 4

Description: Websense_UFP

Blocked
Not Blocked

☐ Use early versions compatibility mode

○ Clear (opsec)
○ OPSEC Authentication (auth_opsec)
○ OPSEC SSL (ssl_opsec)
○ OPSEC SSL Clear (ssl_clear_opsec)

10. Make sure the **Use early versions compatibility mode** check box is not selected. (This field was called Use backwards compatibility mode in earlier versions.)
11. 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 the TRITON - Web Security Help for more information.

Important

Before continuing, make sure the **Use early versions compatibility mode** check box is *not* selected.

12. Click **OK**.
13. Close the Servers and OPSEC Applications dialog box.
14. 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 458.

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,O=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.

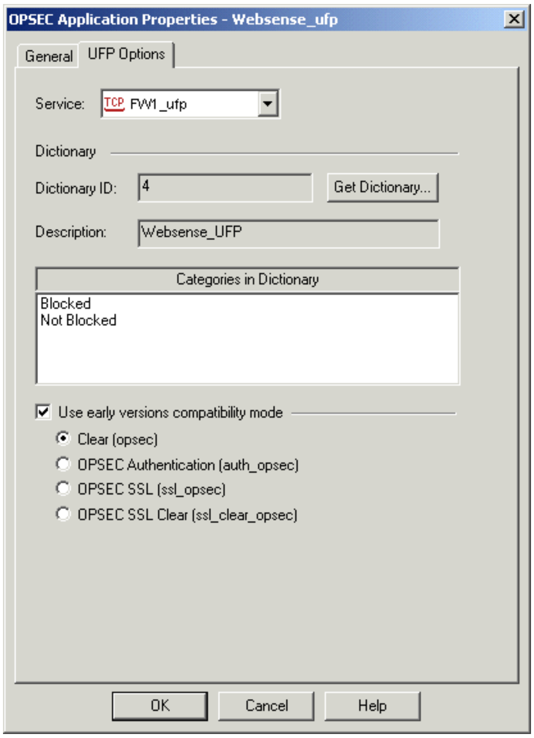
   See *Starting and stopping Web Security services*, page 709, for instructions on stopping and restarting Websense services. See also *Stopping and restarting the UFP Server*, page 473.
6. Open the SmartDashboard, and select **Manage** > **Servers and OPSEC Applications**.
7. Double-click on the OPSEC 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.



OPSEC Application Properties - Websense_ufp

General | UFP Options

Service: TCP FW1_ufp

Dictionary

Dictionary ID: 4

Get Dictionary...

Description: Websense_UFP

Categories in Dictionary
Blocked
Not Blocked

☑ Use early versions compatibility mode

● Clear (opsec)
○ OPSEC Authentication (auth_opsec)
○ OPSEC SSL (ssl_opsec)
○ OPSEC SSL Clear (ssl_clear_opsec)

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.

Troubleshooting Check Point integration

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	

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 451, 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, select **Manage** > **Services**.
  2. Select **FW1_ufp** from the list of services, then click **Edit**.

     The TCP Services Properties dialog box appears.
  3. 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 465), 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

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.

20 Integrating Web Security with Cisco

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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

See *System requirements for this version*, page 2, for a list of Cisco products supported for integration with Websense Web Filter or Web Security.

Integrating with a Cisco product involves the following components:

- **Websense Filtering Service** works with the Cisco product and Network Agent to respond to Internet requests.

  For redundancy, two or more instances of Filtering Service may be used. Only one instance (the primary server) is active at any given time. URL look-up requests are be sent only to the primary server.

- **Websense 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 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.

- If HTTP(S) or FTP authentication is enabled in the Cisco product, **Websense User Service** must be installed in the same domain or root context as authenticated users to get correct user information and provide it to Filtering Service for accurate user-based filtering.

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

To enable the integration, direct Internet requests through your Cisco product, and configure it for use with Websense software.

- *Getting started with a Cisco integration*, page 486, provides general introductory information.
- *Configuring a Cisco Security Appliance*, page 489, discusses Cisco PIX Firewall and Adaptive Security Appliance (ASA).
- *Configuring a Cisco IOS Router*, page 500, discusses Cisco IOS router.
- *Configuring a Cisco Content Engine*, page 507, discusses Cisco Content Engine.

Cisco configuration command conventions

The following conventions are used for commands in this document:

- Angle brackets (< >) 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

Deployment considerations for integration with Cisco products

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Cisco PIX/ASA*, page 483 ◆ *Cisco Content Engine*, page 484 ◆ *Cisco IOS Routers*, page 485

Related topics:

- *Getting started with a Cisco integration*, page 486
- *Configuring a Cisco Security Appliance*, page 489
- *Configuring a Cisco IOS Router*, page 500
- *Configuring a Cisco Content Engine*, page 507

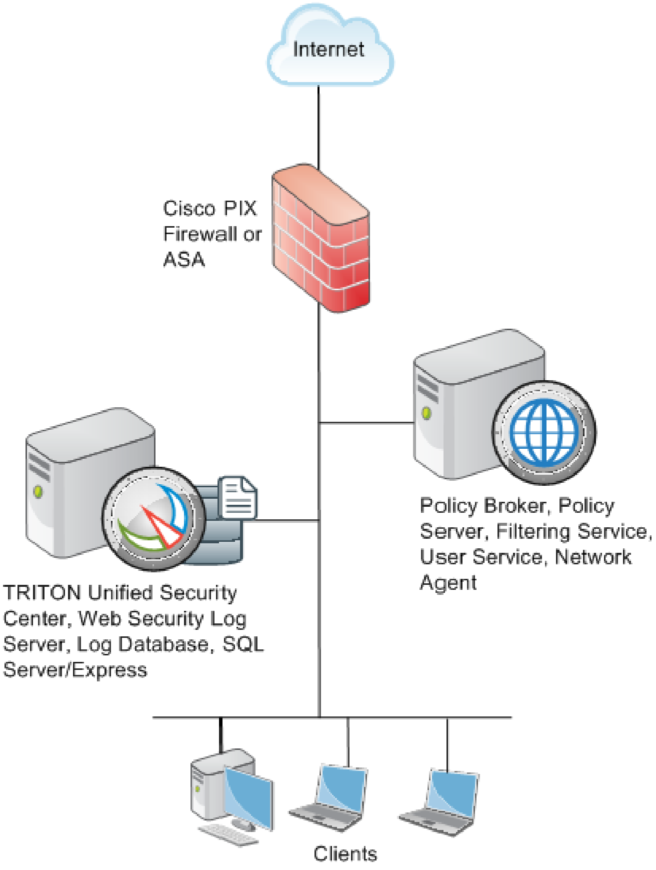
Cisco PIX/ASA

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 *Integrating Web Security with Cisco*, page 481, 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.

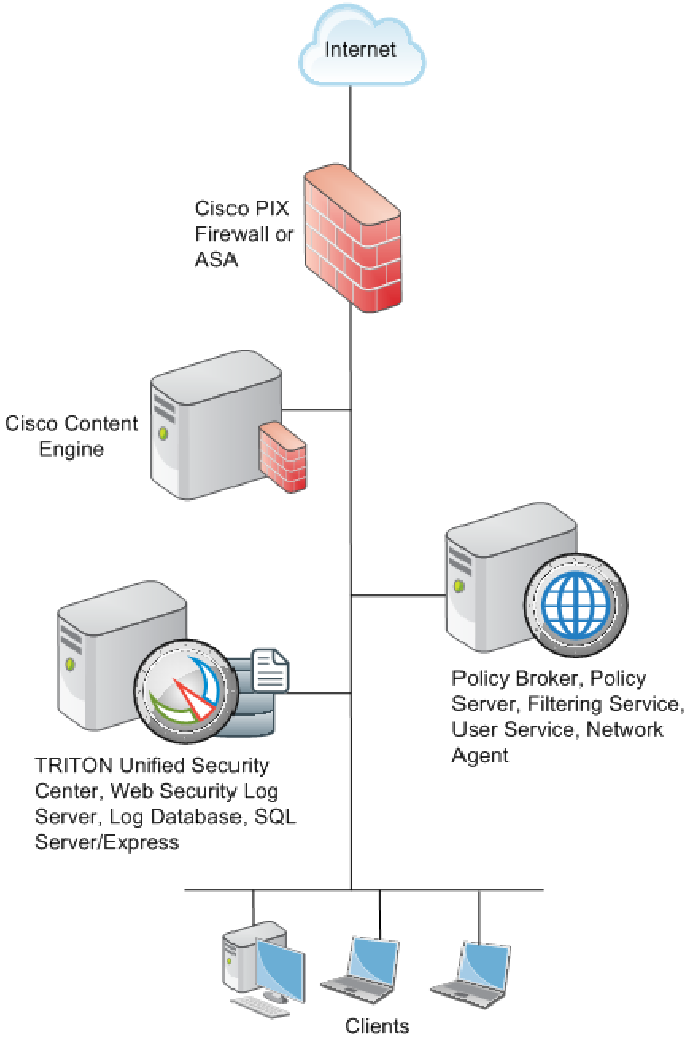

Internet
Cisco PIX Firewall or ASA
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
TRITON Unified Security Center, Web Security Log Server, Log Database, SQL Server/Express
Clients

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.

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.


Internet
Cisco PIX Firewall or ASA
Cisco Content Engine
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
TRITON Unified Security Center, Web Security Log Server, Log Database, SQL Server/Express
Clients

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.

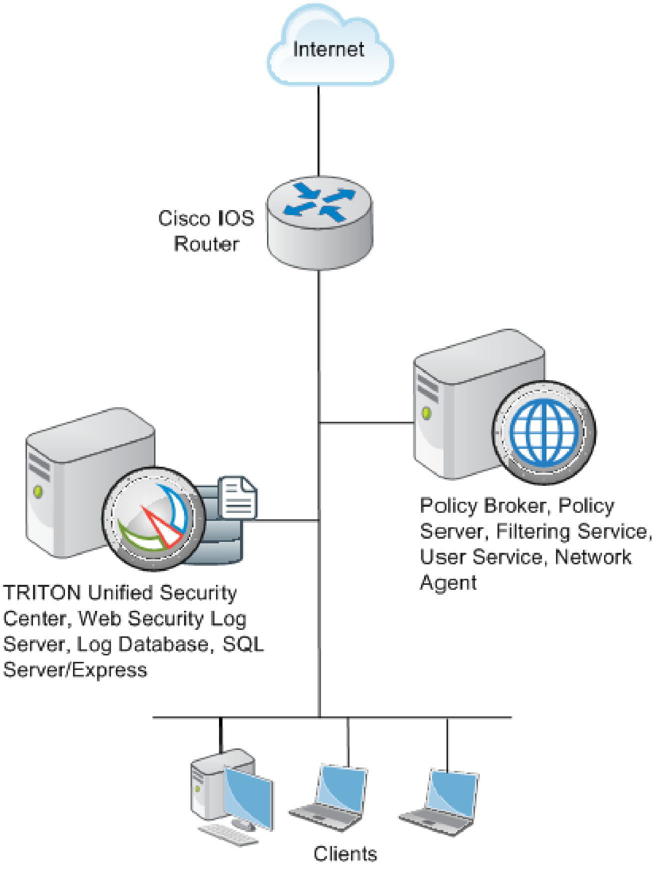
Cisco IOS Routers

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.


Internet
Cisco IOS Router
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
TRITON Unified Security Center, Web Security Log Server, Log Database, SQL Server/Express
Clients

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.

Getting started with a Cisco integration

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *How Websense filtering works with Cisco products*, page 486 ◆ *Installation of Web Filter or Web Security*, page 487 ◆ *Upgrading Websense Web Filter or Web Security*, page 487 ◆ *Migrating between integrations after installation*, page 488 ◆ *Network Agent enhanced logging*, page 489

Related topics:

- *Deployment considerations for integration with Cisco products*, page 482
- *Configuring a Cisco Security Appliance*, page 489
- *Configuring a Cisco IOS Router*, page 500
- *Configuring a Cisco Content Engine*, page 507

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 512.

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 receives 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.

Installation of Web Filter or Web Security

Install Web Filter or Web Security as directed in *Installation overview: Web Filter and Web Security*, page 193. 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 you upgrade Websense software that is already integrated with a Cisco product, no additional Cisco configuration is necessary. See *Upgrading Websense Web Security Solutions*, page 579, for upgrading instructions.

If you are upgrading your Websense deployment and changing your Cisco product, see *Migrating between integrations after installation*, page 488.

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 698, for instructions.
5. Restart the machine (Windows only).
6. Use the Websense installer to reinstall Filtering Service. See *Installing Web Security components*, page 392, 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 and stopping Web Security services*, page 709.
10. Use TRITON - Web Security to identify which Filtering Service instance is associated with each Network Agent.

    a. Use a supported browser (see *System requirements for this version*, page 2) to go to **https://<IP address>:9443/triton**.

    Here, <*IP address*> is the IP address of the machine on which the TRITON console installed.

    b. Click the **Web Security** module, then go to **Settings > Network Agent**.

    c. Click the appropriate IP address in the navigation pane to open the **Local Settings** page for a Network Agent instance.

    d. 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.

e. Log off 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**, where <*IP address*> is the IP address of the machine on which the TRITON console.
2. Select the **Web Security** module, then go to **Settings** > **Network Agent**.
3. Click appropriate IP address in the navigation pane to open the **Local Settings** page for a Network Agent instance.
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.

Configuring a Cisco Security Appliance

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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 configuration command conventions*, page 482
- *Cisco integration configuration procedure*, page 490
- *User-based filtering for Cisco integration*, page 498

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 configuration procedure

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Configuration procedure*, page 490 ◆ *Parameters for the filter commands*, page 497

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. In v7.0 of the Cisco security appliance software, a value for this parameter must be entered. In v6.3.1 and earlier, <*if_name*> defaults to `inside` if not specified. 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. 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. ◆ v7.0(1) and later: Range: 10 - 120; Default: 30 ◆ v6.3: Range: 1 - 30; Default: 5
`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. **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. If this parameter is not specified, it defaults to **5**, which is the recommended setting. If you select the UDP protocol, this option is not available. 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 497.

   Examples:

Command example	Action
`filter url http 0 0 0 0`	Filters every HTTP request to all destinations. 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. 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. 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 497.

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. 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. 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 497.

Examples:

Command example	Action
`filter ftp 21 0 0 0 0`	Filters every FTP request to all destinations. 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. 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. 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:

    - Either enter the command:

      ```
      copy run start
      ```

    - Or enter the commands:

      ```
      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 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. The option to set a custom Web port or port range is only available in v5.3 and higher of Cisco software. **Note:** 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. In Cisco software version 7.0, you must always enter **http**.

<port>	`filter https`
	`filter ftp`
		Defines the port number the security appliance watches for https or ftp requests.
		The standard HTTPS port is **443**.
		The standard FTP port is **21**.

<local_ip>	`filter http`
	`filter https`
	`filter ftp`
		IP address requesting access.
		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`
	`filter https`
	`filter ftp`
		Network mask of the **local_ip** address (the IP address requesting access).
		You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts within the local network.

<foreign_ip>	`filter http`
	`filter https`
	`filter ftp`
		IP address to which access is requested.
		You can use 0.0.0.0 (or in shortened form, 0) to specify all external destinations.

<foreign_mask>	`filter http`
	`filter https`
	`filter ftp`
		Network mask of the **foreign_ip** address (the IP address to which access is requested).
		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.

Parameter	Applies to	Definition

`[allow]`	`filter http`
	`filter https`
	`filter ftp`
		Lets outbound connections pass through the security appliance without filtering when Filtering Service is unavailable.
		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. (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. 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. • Enter **longurl-truncate** to send only the host name or IP address to Filtering Service. • Enter **longurl-deny** to deny the request without sending it to Filtering Service. (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. (Supported in Cisco PIX v6.2 and higher.)

User-based filtering for Cisco integration

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Overview*, page 499 ◆ *Enable protocol filtering*, page 499

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 Deployment and Installation Center 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 machine 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.

Configuring a Cisco IOS Router

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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 configuration command conventions*, page 482
- *Cisco IOS startup configuration*, page 500
- *Cisco IOS configuration commands*, page 502
- *Cisco IOS executable commands*, page 506

Cisco IOS startup configuration

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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. 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. 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. 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 500.

```
no ip urlfilter server vendor websense <ip-address>
```

Cisco IOS configuration commands

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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. The default port number is 15868.
`timeout <secs>`	The amount of time the Cisco IOS router waits for a response from Websense Filtering Service. 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. 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 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- ◆ Web Filter, Web Security, and Web Security Gateway, v7.7.x

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.

Configuring a Cisco Content Engine

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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*, page 508
- *Cisco Content Engine console or telnet session*, page 509
- *Verifying Cisco Content Engine configuration*, page 510
- *Configuring firewalls or routers when integrating with Cisco Content Engine*, page 511
- *Cisco Content Engine and browser access to the Internet*, page 512
- *Cisco Content Engine clusters*, page 512

Cisco Content Engine Web-based interface

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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. The default is 15868.
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. The default is 20.

Field	Description
Allowmode	When allowmode is enabled, the Content Engine allows HTTP traffic if Filtering Services does not respond. 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.

For more information on using the Web-based interface, see Cisco documentation, available at www.cisco.com.

Cisco Content Engine console or telnet session

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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. The default is 15868.
`<seconds>`	The amount of time (0-240) in seconds that the Content Engine waits for a response from Filtering Service. 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway, v7.7.x

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 Master Database download instructions.

Cisco Content Engine and browser access to the Internet

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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.

21 Integrating Web Security with Citrix

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

This section of the Websense Technical Library provides information about integrating Websense Web Filter or Web Security with Citrix® XenApp™.

- To have their Internet activity managed by Websense software, Citrix client computers must access the Internet through a Citrix server.
- Non-Citrix clients in the network can be managed as part of the same Websense deployment. See *Combining Citrix with another integration*, page 530, for more information.

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

- **Websense Citrix Integration Service** must be installed on each Citrix server to allow that server to communicate with Websense Filtering Service.

  Citrix Integration Service works with the following Citrix products:

Product	Operating System
XenApp 6.0	Windows Server 2008 R2
XenApp 5.0	Windows Server 2008 (32- and 64-bit)

- **Websense Filtering Service** interacts with Citrix Integration Service and Network Agent to determine whether to block or permit Internet requests.
- **Websense Network Agent** manages Internet protocols not managed by your Citrix server integration.

  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:

- *Filtering Citrix server users*, page 516
- *Citrix Integration Service installation overview*, page 519
- *Upgrading Citrix Integration Service to 7.7*, page 528
- *Configuring user access on Citrix servers*, page 529
- *Initial Setup of Citrix integration*, page 530

Deployment considerations for integration with Citrix products

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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

For the XenApp versions supported by Websense software, see *System requirements for this version*, page 2.

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 *Integrating Web Security with Citrix*, page 513).
- 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 *Integrating Web Security with Citrix*, page 513, 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

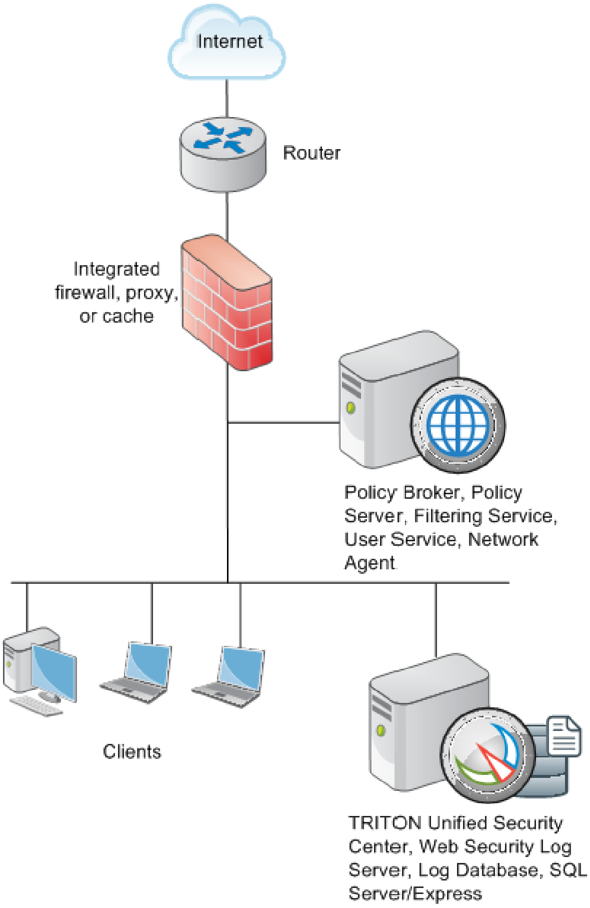
Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

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.


Internet
Router
Integrated firewall, proxy, or cache
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
Clients
TRITON Unified Security Center, Web Security Log Server, Log Database, SQL Server/Express

Other configurations are possible. See your integration product's documentation for other recommendations. See *Installing Web Security for Universal Integrations*, page 563, 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.

Filtering Citrix server users

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Filtering both Citrix and non-Citrix users*, page 518

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

- A recommended maximum of 10 Citrix servers can be connected to one Websense Filtering Service. This number can be configured and depends on the user load.

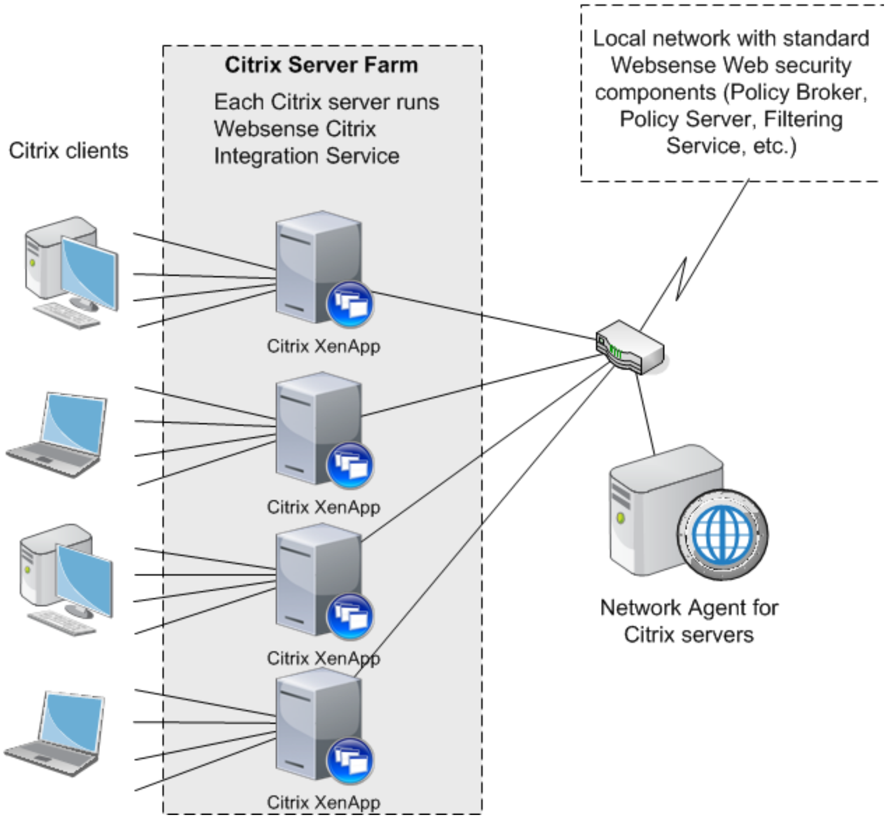
  Multiple Filtering Services are needed if more than 15 Citrix servers are used, with each Citrix server handling about 20 to 30 Citrix users.
- The Filtering Service and Websense Network Agent monitoring Citrix traffic should be installed on a dedicated machine, and not on a Citrix server.
- The Filtering Service and Network Agent instances monitoring Citrix traffic use the same Policy Broker, Policy Server, User Service, and so on as Filtering Service and Network Agent instances used to monitor non-Citrix traffic.
- Separate Filtering Service and Network Agent instances must be used to monitor non-Citrix traffic.
- Do not configure a separate integration product 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 the TRITON - Web Security Help for instructions on configuring IP ranges for Network Agent.

- If you have standalone instances of Filtering Service (not configured to integrate with Citrix or any other integration product), use a dedicated instance of Network Agent 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.

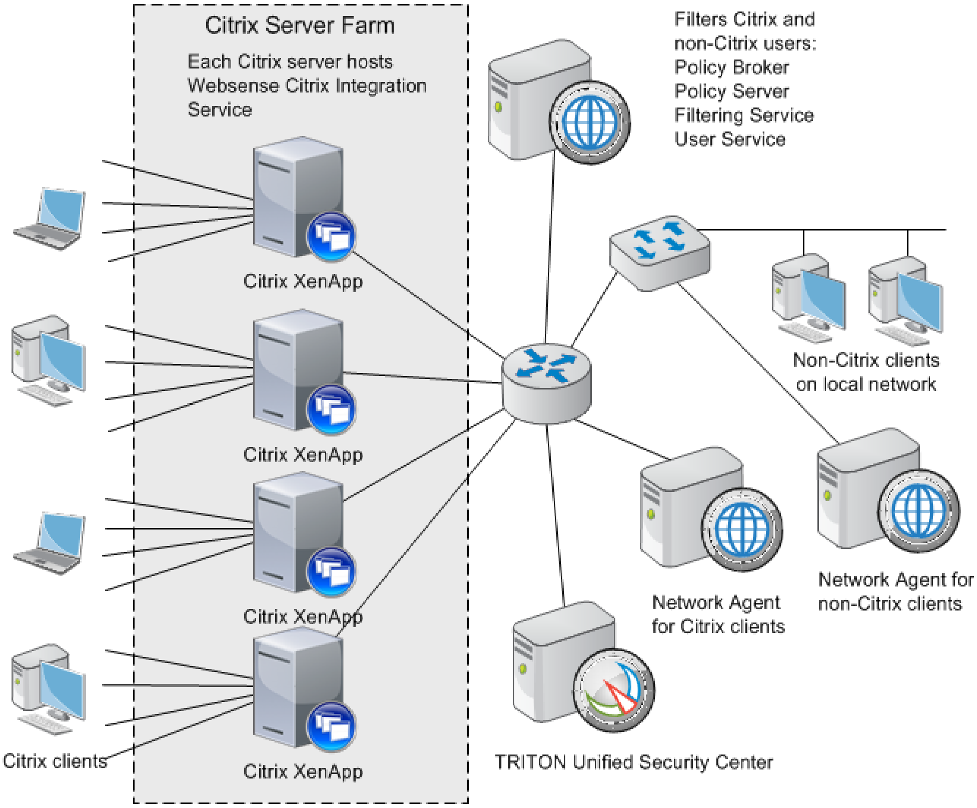
This diagram shows a typical deployment to filter users who access the Internet through a Citrix server. To simplify the diagram, not all individual Websense components are shown.


Citrix Server Farm
Each Citrix server runs Websense Citrix Integration Service
Local network with standard Websense Web security components (Policy Broker, Policy Server, Filtering Service, etc.)
Citrix clients
Citrix XenApp
Citrix XenApp
Citrix XenApp
Citrix XenApp
Network Agent for Citrix servers

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.


Citrix Server Farm
Each Citrix server hosts Websense Citrix Integration Service
Citrix XenApp
Citrix XenApp
Citrix XenApp
Citrix XenApp
Citrix clients
Filters Citrix and non-Citrix users:
Policy Broker
Policy Server
Filtering Service
User Service
Non-Citrix clients on local network
Network Agent for Citrix clients
Network Agent for non-Citrix clients
TRITON Unified Security Center

- To install the Citrix Integration Service on a Citrix Server, see page 520.
- 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 *Install Filtering Service and Network Agent to integrate with Citrix* for instructions.
- To install Websense Web Filter or Web Security for non-Citrix users, refer to the appropriate section of this Deployment and Installation Center for that integration product.
- 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 530.

Citrix Integration Service installation overview

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

There are 5 general steps involved in configuring Websense Web Security solutions to integrate with Citrix:

1. Install one or more instances of Websense Filtering Service to integrate with Citrix.
2. Install a dedicated Websense Network Agent to monitor the Citrix servers.

   To perform the first 2 steps, see *Install Filtering Service and Network Agent to integrate with Citrix*, page 519.
3. Obtain the Citrix configuration package (used to install the Citrix Integration Service configuration utility).

   See *Obtain the Citrix Integration Service configuration package*, page 520.
4. Create and configure a Citrix Integration Service installation package for your deployment.

   See *Configure the Citrix Integration Service installation package*, page 521.
5. Use the installation package to install Citrix Installation Service on your Citrix servers.

   See *Use the installation package to install Citrix Integration Service on a Citrix server*, page 526.

For information about upgrading a prior-version Citrix Integration Service, see *Upgrading Citrix Integration Service to 7.7*, page 528.

If Websense software will manage Internet activity for both Citrix and non-Citrix users, refer to *Combining Citrix with another integration*, page 530, after installing the Websense Citrix Integration Service.

Install Filtering Service and Network Agent to integrate with Citrix

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

Before performing these steps, Websense Policy Broker and Policy Server must already be installed and running in your network. You will be prompted for Policy Server connection information during Filtering Service installation.

1. Install an instance of Websense Filtering Service to integrate with Citrix as follows:
   a. Launch the Websense Unified Installer on a machine other than the Citrix server and select a **Custom** installation.
   b. On the Custom Installation screen, next to Web Security, click **Install** or **Modify**.
   c. Select **Filtering Service** as the component to install.
   d. On the Integration Option screen, select **Integrated with another application or device**.
   e. On the Select Integration screen, select **Citrix**.

   For more detailed custom installation instructions, see *Installing Web Security components*, page 392.

   You can install other Web Security components on this machine as well (for example, Policy Broker, Policy Server, User Service and so forth).

   Important

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

2. Run the installer again on a separate machine to install the instance of Network Agent that will integrate with Citrix.

   When prompted for Filtering Service connection information, enter the IP address of the Filtering Service instance installed in step 1.

To continue with the next step in the integration process, see *Obtain the Citrix Integration Service configuration package*, page 520.

Obtain the Citrix Integration Service configuration package

Applies to:

- Web Filter and Web Security, v7.7.x

Everything you need to configure and install Websense Citrix Integration Service is contained in a self-extracting archive (the Citrix configuration package) containing:

- A configuration utility, used to customize the template installation package for your deployment
- A default installation package to use as a template (consisting of an MSI file, several DLLs, and configuration files)

The Citrix configuration package is included on any Windows machine containing Websense components (for example, the TRITON management server or the Log Server machine). It can be found in the following directory:

> C:\Program Files *or* Program Files (x86)\Websense\Web Security\CitrixPlugin\
> 32-bit *or* 64-bit

Note that there are separate 32-bit and 64-bit configuration packages. Select the appropriate one for the **target** operating system (the Citrix server operating system).

To avoid installing unnecessary files on the Citrix server, copy the Citrix configuration package you want to use (32-bit, 64-bit, or both) from the Windows server to the machine on which you want to configure your custom installation package. The configuration package can run on most Windows operating systems; it does not need to be run on a server.

To continue with the next step in the integration process, see *Configure the Citrix Integration Service installation package*, page 521.

Configure the Citrix Integration Service installation package

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

Extract the contents of the Citrix configuration package and run the configuration utility to create a Citrix Integration Service installation package to deploy to Citrix servers.

1. Double-click the configuration package executable, then click **Extract**. The package name is either:
   - WCISUtil_Win32_*nnnn*.exe (32-bit)
   - WCISUtil_x64_*nnnn*.exe (64-bit)

2. Double-click **Websense Citrix Integration Service Configuration.exe** to start the configuration utility.

> **Important**
>
> The 32- and 64-bit versions of the configuration utility have the same name. Make sure you are launching the correct version.

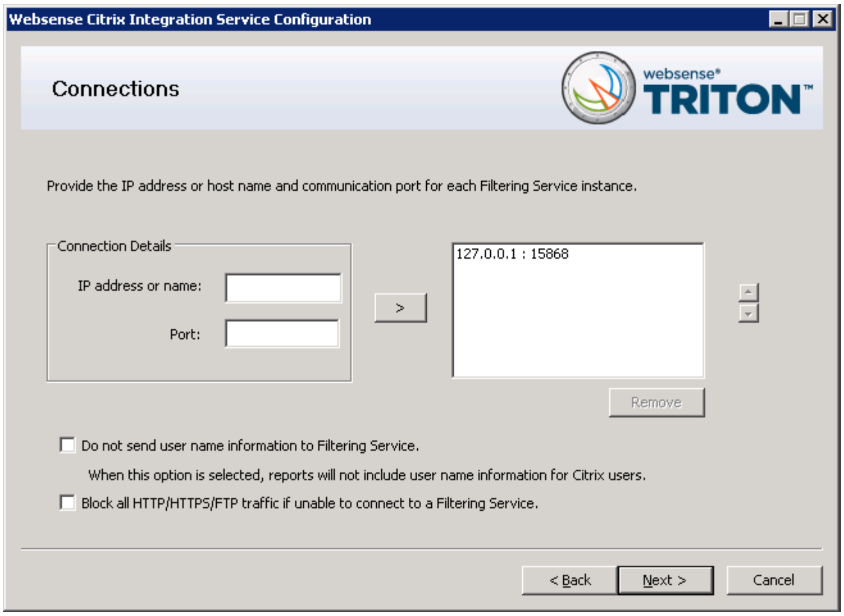
3. In the **Profile Source** screen, click **Browse** and select the folder containing either the default Citrix installation package template or an existing installation package that you want to modify, then click **Next**.

   If the following message appears, make sure all necessary files are present in the folder you specified:

   ```
   The selected installation package does not include all of
   the necessary files.
   ```

   The folder you specify must contain all of the files extracted from the Citrix configuration package in step 1.

4. In the **Connections** screen, configure Filtering Service connection behavior for Citrix Integration Service as described below. When you are finished, click **Next**.



Websense Citrix Integration Service Configuration

Connections

Provide the IP address or host name and communication port for each Filtering Service instance.

Connection Details

IP address or name:

Port:

127.0.0.1 : 15868

□ Do not send user name information to Filtering Service.

When this option is selected, reports will not include user name information for Citrix users.

□ Block all HTTP/HTTPS/FTP traffic if unable to connect to a Filtering Service.

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

      Filtering Service should never be installed on the Citrix server machine itself.

b. Under **Connection Details**, enter the IP address or hostname of a Filtering Service machine, then enter the filtering port (15868 by default).

Note

The Filtering Service port must be in the range 1024-65535. 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.

c. Click the right arrow (>) to add the IP address/hostname and port entry to the list to the right.

d. Repeat the previous 2 steps for each Filtering Service instance you want used by the Citrix server.

When multiple Filtering Service instances are specified, if the first instance is unavailable, Citrix Integration Service attempts communication with the next instance in the list.

If no Filtering Service instances are available, Citrix Integration Service continues to attempt communication in the background every 1 minute. Until communication is established, Citrix Integration Service fails open (permits all requests) or fails closed (blocks all requests) depending on your select in **step f** (below).

Note

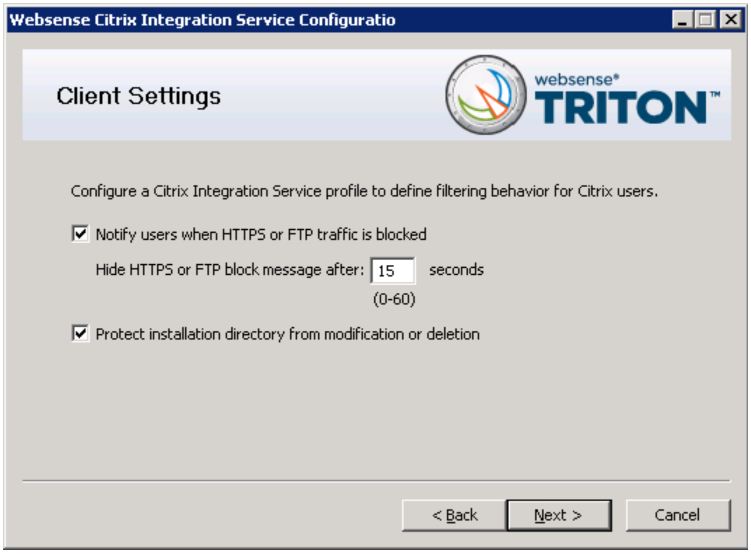
Each Filtering Service instance tracks continue, quota, and password override information independently. If the Citrix Integration Service fails over from one Filtering Service instance to another, usage quotas may be different and override passwords may need to be entered again.

e. Enable or disable the **Do not send user name information to Filtering Service** option. If this option is selected (enabled), user name information for Citrix users is not included in reports.

The setting applies to all Filtering Service instances listed.

f. Enable or disable the **Block all HTTP/HTTPS/FTP traffic if unable to connect to a Filtering Server** option to determine whether Citrix Integration Service blocks or permits all requests when it cannot communicate with Filtering Service.

5. In the **Client Settings** screen, select options as described below. When you are finished, click **Next**.



Client Settings

Configure a Citrix Integration Service profile to define filtering behavior for Citrix users.

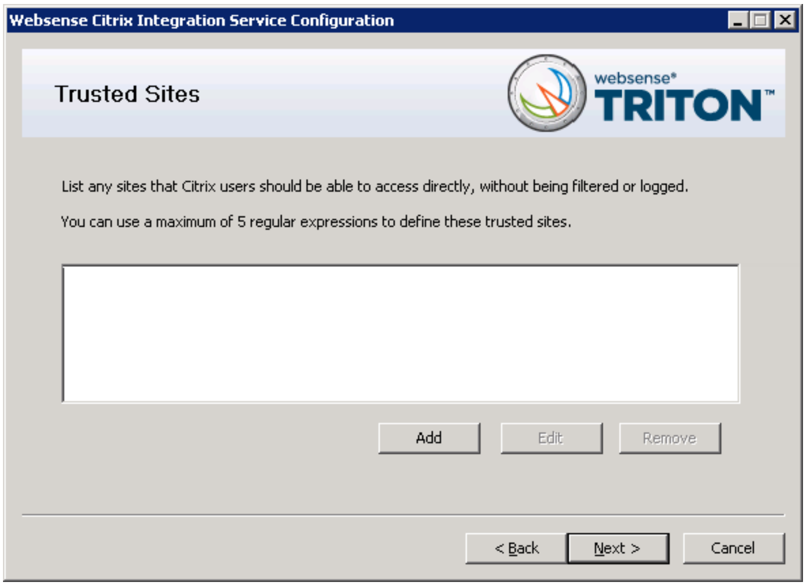
☑ Notify users when HTTPS or FTP traffic is blocked

Hide HTTPS or FTP block message after: 15 seconds (0-60)

☑ Protect installation directory from modification or deletion

- **Notify users when HTTPS or FTP traffic is blocked**: Determine whether users see a browser pop-up message when HTTPS or FTP traffic is blocked. If so, also specify the how long the pop-up message remains visible.
- **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 stopped.

6. On the **Trusted Sites** screen, specify those URLs or domains that should not be filtered as explained below. When you are finished, click **Next**.



Trusted Sites

List any sites that Citrix users should be able to access directly, without being filtered or logged.

You can use a maximum of 5 regular expressions to define these trusted sites.

To add a URL or regular expression, click **Add**, then enter either a URL or a regular expression specifying a set of URLs. Any regular expression adhering to

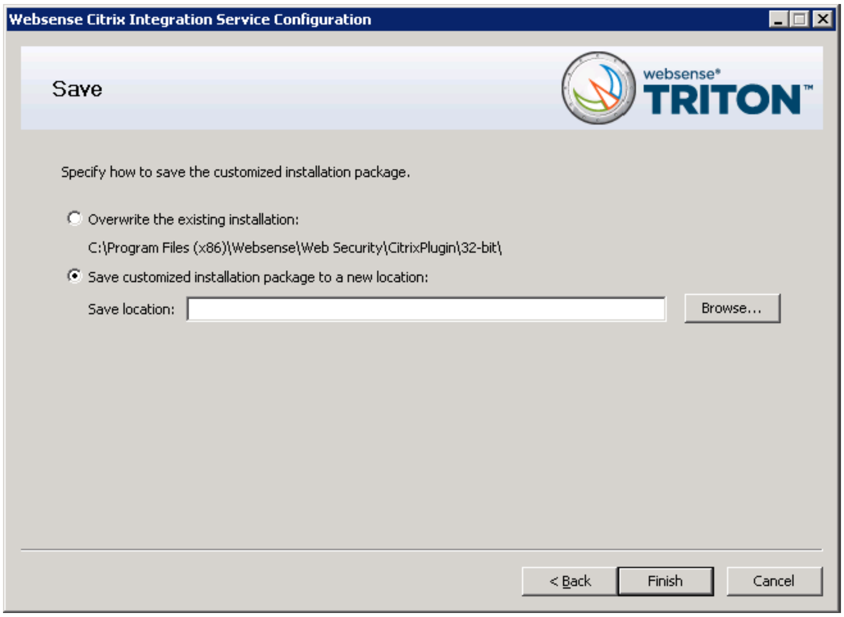
ISO/IEC TR 19768 (within the character-number limit) is valid. When you are finished, click **OK**.

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**.

The URLs you specify here are trusted by any Citrix server on which this Citrix Integration Service is install. It has no bearing on how Filtering Service instances filter requests from non-Citrix users and other Citrix servers that use a different Citrix Integration Service configuration.

7. On the **Save** screen, specify how you want the customized installation package saved. When you are finished, click **Finish**.



Specify how to save the customized installation package.

○ Overwrite the existing installation:

C:\Program Files (x86)\Websense\Web Security\CitrixPlugin\32-bit\

● Save customized installation package to a new location:

Save location:

- Select **Overwrite the existing installation** 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 522.
- Select **Save the customized installation package to a new location** to save the customized installation package to a different location. Click **Browse**, and specify a 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 installation package is now ready for use.

If you have multiple Citrix servers for which you want different customized settings, repeat this procedure, starting at Step 2, page 522, to create an installation package for each. Save each customized installation package to different folders.

To continue to the last step in the integration process, see *Use the installation package to install Citrix Integration Service on a Citrix server*, page 526.

Use the installation package to install Citrix Integration Service on a Citrix server

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

A Citrix installation package includes the following files:

- 0x0409.ini
- CI.cab
- CIClientConfig.hsw
- CIClientMessage.hsw
- DLP.cab
- GClientConfig.hsw
- setup.exe
- Setup.ini
- Websense Citrix Integration Service.msi
- WEP.cab

All of the files must be present to install Citrix Integration Service.

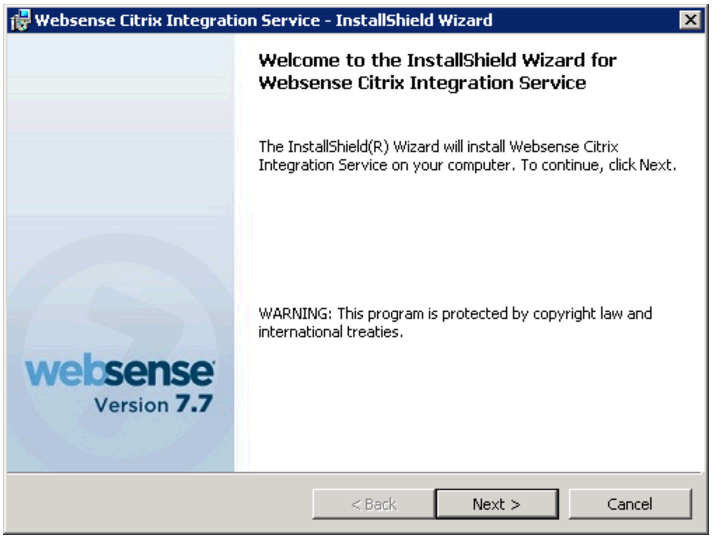
✓ **Note**

If you want to use the same Citrix Integration Service configuration on multiple Citrix servers, use the same Citrix installation package for them. Repeat the procedure, below, on each Citrix server.

1. Log on with **local** administrator privileges to the machine running Citrix 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 configuration 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. It may take a few seconds for the program to begin to run.

When the Welcome screen appears, click **Next**.

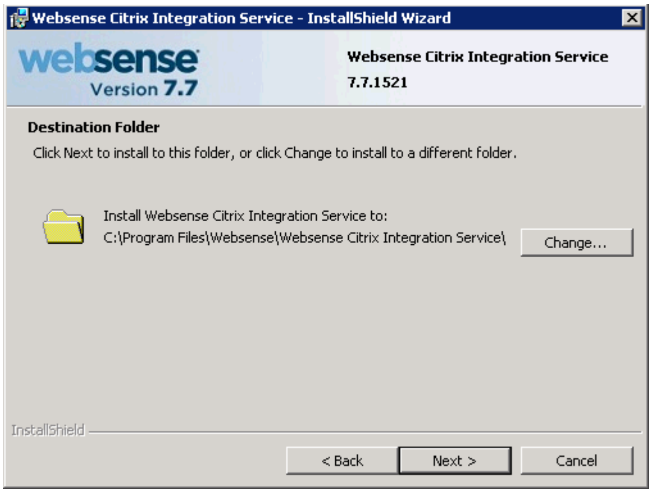


Welcome to the InstallShield Wizard for Websense Citrix Integration Service

The InstallShield(R) Wizard will install Websense Citrix Integration Service on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5. Accept the subscription agreement, then click **Next**.
6. On the **Destination Folder** screen, accept the default location shown or click **Change** to choose a different location, then click **Next**.



Websense Citrix Integration Service 7.7.1521

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Websense Citrix Integration Service to:
C:\Program Files\Websense\Websense Citrix Integration Service\

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 7.7

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

The Websense Citrix Integration Service cannot be upgraded directly from previous versions.

Instead, remove the existing Citrix plug-in or Citrix Integration Service **before** upgrading your Websense software to v7.7. Then, after upgrade, install the v7.7 Citrix Integration Service on the Citrix server.

The steps are as follows:

1. Uninstall the prior-version Citrix Integration Service.

   For removal instructions, see v7.6 *Deployment and Installation Center* or the v7.1 or v7.5 *Installation Guide* for the version to be removed. These materials are available in the Websense Technical Library (www.websense.com/library).
2. Upgrade your Websense Web Security solution to the current version.

   See *Upgrading Websense Security Solutions to v7.7.x*, page 567.

   > ⚠ **Warning**
   >
   > Do **not** run the Websense installer on the Citrix machine to install the Citrix Integration Service. Citrix Integration Service is installed via a Citrix configuration package. See the next step below.

3. Configure and install the current-version Citrix Integration Service. This involves 3 steps:

   a. *Obtain the Citrix Integration Service configuration package*, page 520.

   b. *Configure the Citrix Integration Service installation package*, page 521.

   c. *Use the installation package to install Citrix Integration Service on a Citrix server*, page 526.

Configuring user access on Citrix servers

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

To allow Websense Web Security solutions 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.

Following is an overview of the procedure for configuring user access in Citrix XenApp 5.0. 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	

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 the 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 Security solutions can be set up to filter both Citrix and non-Citrix users. This section provides instructions for configuring Websense software to work with the Citrix integration product.

Deployment scenarios

The corporate network (non-Citrix users) can access the Internet through Websense Network Agent, Content Gateway, or a third-party integration product, such as Cisco® PIX® or Microsoft® Forefront TMG. The component or integration product sends Internet requests to Websense Filtering Service to determine whether to block or permit the request.

Citrix clients access the network through Citrix 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, see *Filtering Citrix server users*, page 516.

Websense filtering is accomplished by installing the Websense Citrix Integration Service on each Citrix server. See *Citrix Integration Service installation overview*, page 519, 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 you have a standalone deployment of Websense Web Filter or Web Security, separate instances of Network Agent are needed for the Citrix and non-Citrix users. See *Standalone Websense Web Filter or Web Security configuration*, page 533, for configuration information.

Configuration

To use a Websense Web Security solution to filter both Citrix users and users accessing the Internet through Network Agent or another integration product, the non-Citrix-related components must be installed and running before the Citrix integration is completed.

1. Install your Web Security solution.
2. Install the Filtering Service and Network Agent to be used for Citrix integration.
3. Configure and iinstall the Websense Citrix Integration Service on each Citrix server.

   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.

   See *Citrix Integration Service installation overview*, page 519, for instructions for steps 2 and 3.
4. Configure the non-Citrix integration product to ensure that requests coming from the Citrix clients are not filtered twice. See *Configuring the non-Citrix integration*, page 531.

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, which determines whether to block or permit the request. Simultaneously, the Citrix server sends the same request to the non-Citrix integration, which must be configured to allow the request to pass through.

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.

Use the Firewall-1 SmartDashboard™ (or Policy Editor in older versions) to 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 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 Forefront TMG (TMG) machine.

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

1. On the 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 software contains the following URL:
>
> **url=http://ms_proxy_intra_array_auth_query/**
>
> Do not delete this URL. It is used by TMG machines in a CARP array for communication. This URL must be ignored to allow filtering and logging to work properly when multiple TMG instances 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=<Citrix_server_hostname>
   ```

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

3. Restart the TMG machine.

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

Standalone Websense Web Filter or Web Security configuration

In a standalone Websense Web Filter or Web Security deployment, 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 and Deploy**.

See the “Network Configuration” topic in the TRITON - Web Security Help for instructions on configuring NIC settings.

22 Integrating Web Security with Microsoft Products

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

This section of the Deployment and Installation Center provides information specific to integrating Websense Web Security solutions with Microsoft® Forefront™ Threat Management Gateway (TMG) 2010 or later.

Refer to *Installation overview: Web Filter and Web Security*, page 193, as your primary source of installation instructions. Only additional or alternate steps required to enable TMG integration are provided here.

An integration with TMG affects the following Websense components:

- **Websense ISAPI Filter plug-in**: This additional Websense component is installed on the machine running TMG. The ISAPI Filter plug-in configures TMG to communicate with Websense Filtering Service.
- **Websense Filtering Service**: Interacts with 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 TMG machine in your network.
- **Websense Network Agent**: Manages Internet protocols that are not handled by TMG. Network Agent also enables bandwidth-based filtering.

If your environment includes an array of TMG machines, install Websense Web Security components on a machine outside the array.

When TMG receives an Internet request from a user, it passes the request to Websense Filtering Service, which determines the category assigned to the URL and checks the policy assigned to the client.

- 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 TMG that the site is not blocked, and the client is given access to the site.

The following topics discuss the various aspects of integrating with TMG:

- *Deployment considerations for integration with Forefront TMG*, page 536
- *Installing Web Security to integrate with Forefront TMG*, page 539
- *Upgrading Web Security when integrated with ISA Server or Forefront TMG*, page 542
- *Removing the ISAPI Filter Plug-In*, page 542
- *Converting to an integration with Forefront TMG*, page 544
- *Forefront TMG initial setup*, page 545
- *User identification and authentication with Forefront TMG*, page 551

Deployment considerations for integration with Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

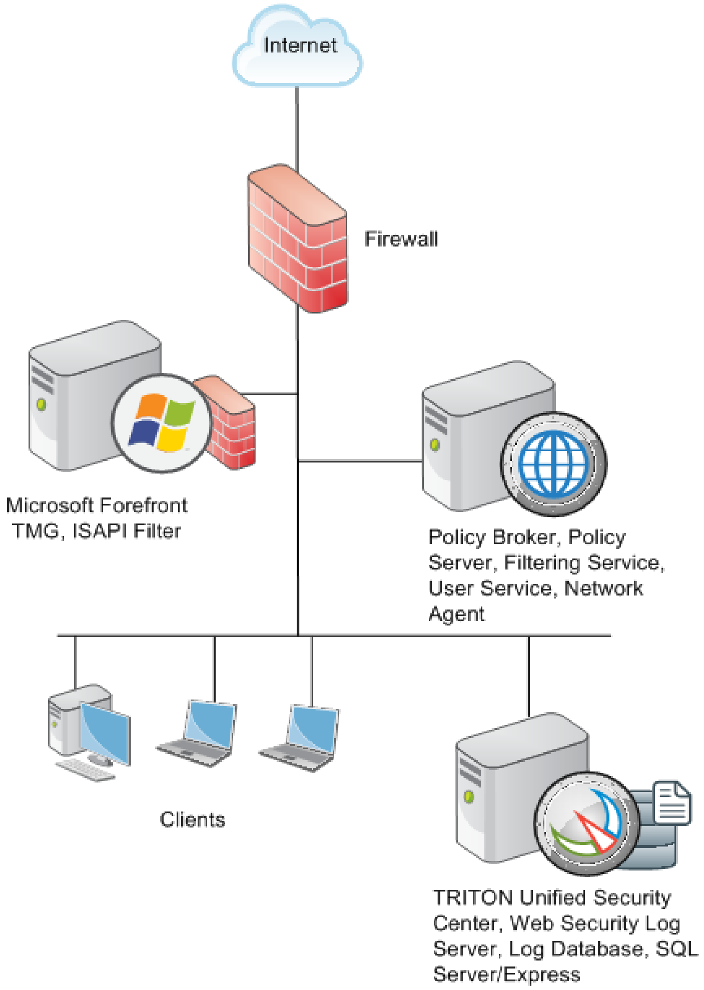
Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Single Microsoft Forefront TMG configuration*, page 536 ◆ *Array configuration*, page 537

Single Microsoft Forefront TMG configuration

The following illustration shows placement of Websense filtering components on 2 dedicated machines, separate from the Microsoft Forefront TMG server.

- The ISAPI Filter must be installed on the TMG machine so that Internet activity information can be communicated to Filtering Service.

- The Filtering Service and TMG machines must be able to communicate over the network.

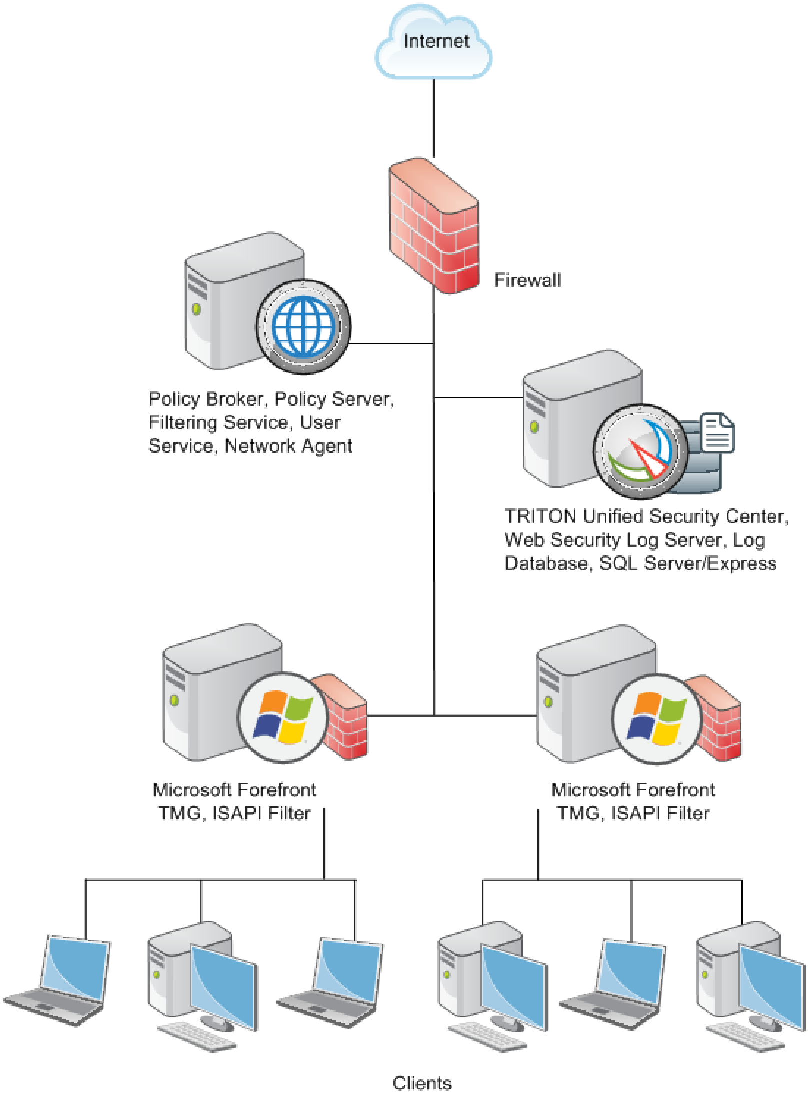

Internet
Firewall
Microsoft Forefront TMG, ISAPI Filter
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
Clients
TRITON Unified Security Center, Web Security Log Server, Log Database, SQL Server/Express

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.

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 Forefront 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.


Internet
Firewall
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
TRITON Unified Security Center, Web Security Log Server, Log Database, SQL Server/Express
Microsoft Forefront TMG, ISAPI Filter
Microsoft Forefront TMG, ISAPI Filter
Clients

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

Installing Web Security to integrate with Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Installing the ISAPI Filter plug-in for Forefront TMG*, page 539

The general process of installing Websense Web Security solutions to integrate with Microsoft Forefront TMG is as follows:

1. Begin by installing Web Security policy, management, and reporting components in your network (not on the TMG machine).
   - See *Installation overview: Web Filter and Web Security*, page 193, for instructions.
   - Websense Filtering Service must already be installed before the ISAPI Filter plug-in is installed on the TMG machine. When installing Filtering Service, specify that it is integrated with TMG.

2. Install the ISAPI Filter plug-in on the TMG machine (as described below).

   The Forefront TMG plug-in installer, rather than the TRITON Unified Installer, is used to install the ISAPI plug-in for Forefront TMG, as described in the next section.

   The only Websense components installed on the Forefront TMG machine are the ISAPI Filter plug-in and Websense Control Service (which manages installation and removal of Websense software components).

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 on the TMG machine.

Websense Filtering Service must be installed and running before you install the ISAPI Filter plug-in. Make sure that Forefront TMG integration was specified during Filtering Service installation.

Important

- The ISAPI Filter plug-in for Forefront TMG is supported on **only** Windows 2008 R2.
- As part of the installation process, you must stop the Microsoft Forefront TMG Firewall service (Firewall service). Because this may stop network traffic, perform the installation during a time when a stoppage will least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.
- Port 55933 (Websense Control Service communication port) must be open locally, for the ISAPI Filter plug-in to be installed successfully.

Before beginning the installation process:

- Download or copy the Forefront TMG plug-in installer to this machine. This installer is available at mywebsense.com.
- Close all applications and stop any antivirus software.

To perform the installation:

1. Start the Forefront TMG plug-in installer. When the Introduction screen displays, click **Next**.
2. On the **Subscription Agreement** screen, after accepting the terms of the agreement, click **Next**.
3. 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.
   - To verify the Filtering Service port, check the **WebsenseServerPort** value in the **eimserver.ini** file, located in the Websense **bin** directory on the Filtering Service machine.
4. On the **Installation Directory** screen, accept the default location and click **Next**.
5. On the **Pre-Installation Summary** screen, verify that **Filtering Plug-in** is the only component selected for installation, then click **Install**.

   An **Installing** progress screen is displayed. Wait for the installation to complete.

6. 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 the Microsoft 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.

7. When the following message appears, start the Firewall service and 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.

   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 the Microsoft documentation for more information.

8. On the **Installation Complete** screen, click **Done**.
9. If you stopped antivirus software on this machine, restart it now.

You can verify successful installation of the ISAPI Filter plug-in by logging into the Forefront TMG management console. Navigate to **System** > **Web Filters** and verify that WsISAFilter is present in the list of Web Filters.

Upgrading Web Security when integrated with ISA Server or Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

- Microsoft ISA Server is not supported in this version. If you are currently running ISA Server, before upgrading your Websense software:
  1. Upgrade your existing ISA Server installation to a supported version of Forefront TMG.
  2. Reinstall your existing Websense Filtering Service to integrate with Forefront TMG.
  3. Install the ISAPI Filter plug-in from your existing version on the Forefront TMG.
- To upgrade to the current version:
  1. Upgrade Websense Web Security components, including Filtering Service.
  2. Run the Forefront TMG plug-in installer on the Forefront TMG machine.

> ✓ **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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

Detailed instructions for removing Websense filtering components are provided in the *Removing components*, page 695. However, additional steps are required when you remove the ISAPI Filter plug-in from an TMG machine.

1. Log on with **local** administrator privileges and navigate to **Start** > **Control Panel** > **Uninstall a program** (under **Programs**).
2. Select **Websense Web Security / Websense Web Filter**, then click **Uninstall/ Change**.

   This launches the Websense uninstaller.
3. On the **Remove Components** screen, select **Filtering Plug-in** and any other components to be removed, and then click **Next**.
4. 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 **Start** > **Programs** > **Administrative Tools** > **Services**. Right-click **Microsoft Forefront TMG Firewall**, 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, 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.
5. 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.
   ```

   - 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**.
6. On the **Websense Software Removed** screen, choose whether you want to restart now or later and then click **Done**.

Converting to an integration with Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Upgrade Websense software and remove Filtering Service*, page 544 ◆ *Reinstall Filtering Service*, page 545 ◆ *Install the Websense ISAPI Filter Plug-In*, page 545

You can convert an existing standalone deployment of Websense Web Security or Web Filter to one that is integrated with TMG, without losing any configuration settings. The conversion process preserves such settings as policies, port numbers, and IP addresses.

The main steps are:

1. Upgrade to the current version of Websense software as a standalone deployment.
2. Restart the installation machine.
3. Uninstall Filtering Service, then reinstall it in integrated mode, selecting Forefront TMG as the integration product. See *Upgrade Websense software and remove Filtering Service*, page 544.
4. Enable authentication so that users can be properly identified and filtered. For instructions, see *User identification and authentication with Forefront TMG*, page 551.

Upgrade Websense software and remove Filtering Service

1. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
2. If you have not done so, upgrade your Websense software to the current version.

   After installing, it is a good idea to run the Backup Utility again to have a baseline for your upgraded software.

3. Make sure Websense software is running. The uninstaller looks for Policy Server during the removal process.

> **Warning**
>
> Do not remove Websense components when the associated Policy Server is stopped. If Policy Server is not running, files for the selected components are removed, but configuration information is not updated. Problems could occur later if you attempt to reinstall these components.

4. Uninstall Filtering Service.

   See *Removing Web Security components*, page 698, for instructions. Be sure to remove **only** Filtering Service.

Reinstall Filtering Service

After Filtering Service is removed, reinstall it to integrate with TMG.

See *Adding Web Security components*, page 690, 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 Forefront Threat Management Gateway**.

Install the Websense ISAPI Filter Plug-In

Next, install the ISAPI Filter plug-in on the TMG machine. This plug-in allows Websense software and TMG to communicate. For instructions, see *Installing the ISAPI Filter plug-in for Forefront TMG*, page 539.

Forefront TMG initial setup

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

- If you installed Web Security Log Server, see *Enabling communication with the Log Database when integrated with Forefront TMG*, page 546.

- Websense software filters HTTP, HTTPS, and FTP requests sent to TMG, but cannot filter traffic tunneled over a SOCKS or WinSOCK proxy server. 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 TMG for each of these protocols.

  For information about disabling a protocol, see the TMG Help from Microsoft.
- Additional configuration of the Websense ISAPI Filter is required if you are using non-Web proxy clients with TMG. These TMG clients include the Firewall/Forefront TMG Client with proxy server disabled, and SecureNAT clients.

  See *Configuring for TMG using non-Web-Proxy clients*, page 547, 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 549, 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 TMG to not monitor (i.e., ignore) the machine on which Remote Filtering Server is installed. If TMG monitors this machine, it could interfere with remote filtering. See your TMG documentation for instructions.

Enabling communication with the Log Database when integrated with Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

When you install Web Security Log Server, TMG must be configured to permit communication with the Log Database. This **must** be completed before filtering activity can be logged.

1. On the TMG machine, open the Forefront TMG management console (**Start** > **Programs** > **Microsoft Forefront TMG** > **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.

Configuring for TMG using non-Web-Proxy clients

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Firewall/Forefront TMG Client*, page 547 ◆ *SecureNAT clients*, page 548 ◆ *Configuring the ISAPI Filter plug-in*, page 548

If you are using non-Web-Proxy clients with 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 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 548, for additional configuration steps.

> **Note**
> If the proxy server is disabled, then Websense software filters HTTP only; it cannot filter HTTPS.

SecureNAT clients

SecureNAT clients require that you configure the default gateway so that all traffic to the Internet is sent through TMG. If you need information about configuring and using SecureNAT clients, see your TMG documentation.

See *Configuring the ISAPI Filter plug-in*, page 548, for additional configuration steps.

Configuring the ISAPI Filter plug-in

If you are using the 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 TMG and to filter only those requests going out to the Internet.

> **Note**
> If you are using the 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 TMG machine, create a file called **ignore.txt** in the Windows **system32** directory.
2. Enter the hostname or IP address of the 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 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 TMG machine.

Configuring the ISAPI Filter plug-in to ignore specific traffic

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Configuring the ISAPI Filter plug-in to ignore specific traffic*, page 549 ◆ *Client computer configuration*, page 550 ◆ *Firewall configuration*, page 550

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 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 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 TMG instances are deployed in an array.

2. Enter each user name, hostname, or URL that you want Websense software to ignore. Enter each item on its own line in the file, using the formats below.

   - **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
```

- **Hostname**: Enter a destination hostname that Websense software should not filter or log user visits to:

  ```
  hostname=<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 TMG service.

Client computer configuration

Internet browsers on client computers should be configured to use TMG to handle HTTP, HTTPS, and FTP requests.

An exception to this configuration is browsers in an TMG environment using Firewall/Forefront TMG Clients or SecureNAT. These browsers must point to the same port, 8080, that 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 TMG.

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.

User identification and authentication with Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *TMG clients*, page 552 ◆ *Firewall/Forefront TMG and SecureNAT clients*, page 552 ◆ *Web Proxy clients*, page 552 ◆ *Authentication Methods*, page 553 ◆ *Transparent identification*, page 555

In order to apply user and group-based policies to Internet requests, Websense Filtering Service must receive information about the user making the request. If no user information is available, Websense software can still apply IP address-based policies, or the Default policy.

To ensure that Filtering Service receives user information, you can:

- Enable authentication within TMG.
- Install a Websense transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent).
- 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.

TMG clients

These TMG clients are supported:

- Firewall/Forefront TMG (see *Firewall/Forefront TMG and SecureNAT clients*, page 552)
- SecureNAT (see *Firewall/Forefront TMG and SecureNAT clients*, page 552)
- Web Proxy (see *Web Proxy clients*, page 552)

The term **clients** in this environment 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 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 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 TMG and use Websense transparent identification. This method allows Websense Filtering Service to obtain user identification from the network's directory services.

  See *Transparent identification*, page 555, 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 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 TMG as a proxy server, Web Proxy clients send Internet requests directly to 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 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 TMG and implementing Websense transparent identification.

  See *Transparent identification*, page 555, for more information.
- If the network uses a mixture of browsers, you can enable one or more of TMG's authentication methods. Some of these methods may require users to authenticate manually for certain older browsers.

  See *Authentication Methods*, page 553, 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 TMG nor a Websense transparent identification agent provides the information.

  See "Manual Authentication" in the TRITON - Web Security Help for more information.

Authentication Methods

TMG provides 4 methods of authentication:

- *Basic authentication*
- *Digest authentication*
- *Integrated Windows authentication* (enabled by default)
- *Client Certificate authentication*

Microsoft Internet Explorer, version 5.0 and later, supports all of these authentication methods. Other Web browsers may support only Basic authentication.

When no authentication method is enabled in TMG, it does not pass Websense software any information about who is making the Internet request. When this 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 555, for more information.

Basic authentication

Basic authentication prompts users to authenticate (log on) each time they open a browser. This authentication allows 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 TMG. The user can authenticate to 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, 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 555) 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, 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 TMG functions.

For more information about TMG authentication and how to configure these authentication methods, see Microsoft’s documentation.

Transparent identification

Websense transparent identification agents (DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent) allow Websense software to apply user and group based policies to Internet requests without prompting users to authenticate in the browser.

- If TMG is not configured to send user information to Filtering Service, you can use a Websense transparent identification agent to identify HTTP and non-HTTP users.
- If TMG provides user information for HTTP(S) requests, you can still use a Websense transparent identification requests to obtain user and group information for other protocol requests, managed by Websense Network Agent.

See *Installation overview: Web Filter and Web Security*, page 193, for instructions on installing individual Websense components. See *User Identification* in the TRITON - Web Security Help for information about configuring transparent identification agents.

Websense software 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. See “Secure Manual Authentication” in the TRITON - Web Security Help for more information and instructions on activating this feature.

Troubleshooting integration with Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *SecureNAT clients are not being filtered*, page 556 ◆ *No filtering occurs after the ISAPI Filter plug-in is installed*, page 556

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 TMG, additional configuration of the Websense ISAPI filter is required. Follow the instructions in *Configuring for TMG using non-Web-Proxy clients*, page 547.

No filtering occurs after the ISAPI Filter plug-in is installed

If users are not being filtered after the Websense ISAPI Filter plug-in has been installed on the Forefront TMG machine, the plug-in may not be able to communicate with Websense Filtering Service.

Verify that the ISAPI Filter plug-in is using the correct Filtering Service information.

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 is 15868.

23 Integrating Web Security using ICAP Service

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

Websense ICAP Service makes it possible to integrate Websense Web Security solutions with third-party proxies and proxy-caches that support communication with ICAP servers.

Integration via ICAP affects the following Websense components:

- **Websense ICAP Service** is installed with Filtering Service. It includes an ICAP server that enables third-party proxies to communicate with Filtering Service.
- **Websense Filtering Service** interacts with ICAP Service and Network Agent to filtering Internet requests passed from the proxy via ICAP.

For installation instructions, see *Installing Web Security to integrate with ICAP Service*, page 558.

After installing Websense software, configure your proxy to communicate with Websense ICAP Service (see *Configuring the proxy to communicate with ICAP Service*, page 559).

The Websense service may also require configuration (see *Configuring ICAP Service*, page 560) if the default settings are not appropriate for your environment.

To be filtered by Websense software, a computer must access the Internet through the integrated proxy.

When the proxy receives an Internet request, it uses ICAP to query Websense ICAP Service to find out if the request should be blocked or permitted. ICAP Service queries Filtering Service, which checks the policy assigned to the client and either serves a block page or notifies the proxy to permit the request.

Installing Web Security to integrate with ICAP Service

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.7.x	◆ *Installation overview*, page 558 ◆ *Converting a standalone installation to use ICAP integration*, page 558

Installation overview

The Websense ICAP Service is installed with Filtering Service.

When running the Websense installer:

- Include Filtering Service as a component to install. If you are using the Web Security All option, Filtering Service is included by default.
- Select **Integrated** as the integration option, then select **ICAP Service** as the integration product.
- Follow the on-screen instructions to complete the installation. Refer to the Web Security installation instructions for more detailed information.

After installation, configure your ICAP integration. See:

- *Configuring the proxy to communicate with ICAP Service*, page 559
- *Configuring ICAP Service*, page 560

Converting a standalone installation to use ICAP integration

You can change a standalone Websense Web Security installation to use ICAP integration without losing configuration settings.

1. Upgrade to the current version (if you are not already using the current version), then restart the Filtering Service machine.
2. Uninstall the existing instance of Filtering Service and Network Agent.
3. Reinstall Filtering Service to integrate with ICAP Service. Also reinstall Network Agent.
    - The components can be reinstalled at the same time if they are on the same machine.
    - If the components are on separate machines, first reinstall Filtering Service, then reinstall Network Agent.
4. Configure your ICAP integration. See:
    - *Configuring the proxy to communicate with ICAP Service*, page 559

- *Configuring ICAP Service*, page 560

Configuring the proxy to communicate with ICAP Service

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

The precise steps required to configure the third-party proxy to communicate with Websense ICAP Service vary from product to product.

For Blue Coat SG Series appliances running SGOS 6.2 or later:

1. Log on to the Management Console and go to **Configuration** > **External Services** > **ICAP**.
2. Create an **ICAP Service** with a name like “WebsenseICAP.”
3. Enter the **Service URL** in the following format:

   ```
   icap://<ICAP_server_address>/<service_name>
   ```

   For example:

   ```
   icap://10.100.57.120/icap
   ```

   See *Configuring ICAP Service*, page 560, for more information about setting or determining the service name.
4. Under ICAP Service Ports, verify that **This service supports plain ICAP connections** is selected, and that the **Plain ICAP port** value is set to **1344** (default).

   See *Configuring ICAP Service*, page 560, for information about changing the ICAP port.
5. Under ICAP v1.0 Options, click **Sense settings** to request settings from Websense ICAP Service.
   - When the settings are retrieved, the **Client address**, **Server address**, and **Authenticated user** boxes should be marked, and **“WEBSENSE”** should appear as the ICAP server tag.
   - If you do not want the proxy to authenticate users and pass user name information to Websense software as part of the ICAP request, deselect the **Authenticated user** check box.
6. Click **OK** to close the Edit window.

Additional configuration steps include:

- Configure a Web Access Layer rule to pass all traffic from any source to any destination to the ICAP server configured above, and specify whether the proxy should fail open (permit all traffic) or fail closed (block all traffic) when the ICAP server is not available.

- Configure a Web Access Layer rule to allow all traffic to the IP address of the Websense Filtering Service machine. This allows client browsers to receive Websense block pages.
- If you want the proxy to authenticate users and pass user name information to Websense software, configure an authentication rule to authenticate users against a supported directory service.

  Note that if you are using Active Directory for user authentication, and use a hostname to identify the Active Directory server, make sure that the hostname resolves to the same IP address for both the third-party proxy and TRITON - Web Security.

  Also, if Active Directory is identified by hostname in the proxy, the hostname is what appears in log records, even if Active Directory is identified by IP address in TRITON - Web Security.
- Optionally configure HealthCheck for the external ICAP server. This causes the Blue Coat appliance to periodically send a URL filter request to the Websense ICAP Service to ensure that it is still running and responding correctly.

Configuring ICAP Service

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter and Web Security, v7.7.x

Websense ICAP Service behavior can be customized by modifying a configuration file called **icap.conf**, located in the Websense **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin, or /opt/Websense/bin/, by default) on the ICAP Service machine.

The **icap.conf** file can include the following parameters. Options marked with an asterisk appear in the file by default. The others can be added to the file if needed.

Parameter	Description	Default Value
WebsenseServer*	IP address of the Filtering Service instance associated with a Websense ICAP Service instance	127.0.0.1
WebsenseServerPort	Filtering Service port used for WISP communication	15868
icapPort*	Websense ICAP Service listening port	1344

Parameter	Description	Default Value
icapServiceName*	Name of the ICAP service. Appears in the URL configured in the ICAP client. For example: `icap://<ip_address>/<name>`	icap
maxConnections*	Maximum number of ICAP server connections, and maximum number of connections from the ICAP server to Filtering Service.	200
optionsTTL*	Sent to the ICAP client in response to an OPTIONS request. The next OPTIONS request is sent after this number of seconds.	3600
serverIPEnabled	Sent to ICAP client in response to OPTIONS request. If TRUE, client should send the X-Server-IP field.	TRUE
failClosed*	If there are errors in the Filtering Service responses, should the request be blocked (fail closed) or permitted (fail open).	TRUE
connectionTimeout*	Number of minutes before a connect times out (expires)	5

To update the ICAP Service configuration:

1. Navigate to the Websense **bin** directory (path noted above) and open **icap.conf** in a text editor.
2. Edit an existing parameter, or add a blank line at the end of the file and enter the parameter that you want to configure.
3. Save and close the file.
4. Restart **Websense ICAP Service**.

24 Installing Web Security for Universal Integrations

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
- Web Filter and Web Security, v7.7.x	

This document describes integrating Websense Web Security solutions with supported integration products other than those addressed in the following topics:

- *Integrating Web Security with Check Point*, page 445
- *Integrating Web Security with Cisco*, page 481
- *Integrating Web Security with Citrix*, page 513
- *Integrating Web Security using ICAP Service*, page 557
- *Integrating Web Security with Microsoft Products*, page 535

Refer to the list of Websense Technology Partners (www.websense.com/global/en/Partners/TAPartners/SecurityEcosystem/) to verify that Websense software supports an integration with your firewall, proxy server, caching application, or network appliance.

Integrating Websense software with another product or device affects the following Websense components:

- **Filtering Service** interacts with your integration product and Network Agent to determine whether Internet requests are blocked or permitted.
- **Network Agent** manages Internet protocols that are not managed by your integration product. It can also detect HTTP network activity (managed by the integration) to enable bandwidth reporting.

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 determines 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 to grant access to the site.

Installing Web Security for universal integrations

This section provides a general overview of the installation process, highlighting the steps important to enabling integration.

For detailed installation instructions, see *Installing Web Security solutions*, page 193.

1. When you install Filtering Service, on the **Integration Option** screen, select **Integrated with another application or device**.
2. On the **Select Integration** screen, select **Other (Universal Integration)**.
3. On the **Transparent User Identification** screen you can choose whether to install a Websense transparent identification agent.
    - If your integration product provides user authentication or identification services, or if you do not intend to use user and group-based filtering, select **None**.
    - To use Websense software for user identification, select the agent or combination of agents appropriate for your deployment.
4. Follow the remaining installer prompts to complete the installation.

After installation is complete:

- 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.
- 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.
- Depending on the integration product you are using, you may also 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.

   If you have uninstalled Filtering Service from a Windows machine, restart the machine to complete the remove process.

5. Close any open applications, and stop any antivirus software, then run the Websense installer again.

6. Add Filtering Service using the procedures for installing individual components. See *Adding Web Security components*, page 690.

7. On the **Integration Option** screen, select **Integrated with another application or device**.

8. On the **Select Integration** screen, select **Other (Universal Integration)**.

9. Follow the installer prompts to complete the installation.

   The installer adds the new integration data, while preserving the previous configuration data.

   On Windows machines, to complete the installation, restart the machine.

10. 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.

11. To identify which Filtering Service instance is associated with each Network Agent:

    a. Log on to TRITON - Web Security and go to **Settings** > **Network Agent**.

    b. Highlight the **General** option, then select a Network Agent IP address to open its **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.

For more information, see the Network Configuration > Local Configuration topic in the TRITON - Web Security Help.

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

25 Upgrading Websense Security Solutions to v7.7.x

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x and earlier

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.7 and earlier
- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.6.x

Click the link next to your Websense security solution for upgrade instructions.

Web Security	- *Upgrading Websense Web Security Solutions*, page 579
Data Security	- *Upgrading Data Security to v7.7.x*, page 627
Email Security	- *Upgrading Email Security Gateway to v7.7*, page 669
Web and Data Security	- *Web Security or Web and Data Security upgrade outline*, page 580
Web and Email Security	- *Upgrading solutions that include Web, Email, and Data Security*, page 568
TRITON Enterprise	- *Upgrading solutions that include Web, Email, and Data Security*, page 568

Upgrading solutions that include Web, Email, and Data Security

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.0 - v7.6.7
- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.6.x

All Websense TRITON Enterprise modules must be at v7.6.0 - v7.6.5 in order to upgrade to v7.7.0. To upgrade to later versions of the Data Security v7.7 series, you must have at least v7.7.0 installed.

Because Email Security Gateway and Gateway Anywhere include Data Security components, the upgrade procedure for Web and Email Security is the same as the upgrade procedure for Websense TRITON Enterprise.

Tip

When you follow a link in this list, right-click the link and open it in a new window or tab. This makes it easier to return to the outline and continue working through the prerequisites.

- *Before upgrading Web, Email, and Data Security*, page 568
- *Upgrade sequence for solutions that include Web, Email, and Data Security*, page 570
- *Upgrade procedure for solutions that include Web, Email, and Data Security*, page 572

Before upgrading Web, Email, and Data Security

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x and earlier

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.0 - v7.6.7
- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.6.x

Several ports have changed in v7.7. You must configure your firewall to open the new ports before upgrading to v7.7.

- The new ports for communicating with the Data Security Management Server for data loss prevention are 17500-17515. Content Gateway, Email Security Gateway, and all Data Security components communicate with this server.
- The ports for communicating with Email Security Gateway have also changed. They are 17700-17714.

You can reconfigure the base port after upgrade using the Modify wizard if desired.

In addition:

> **Tip**
>
> When you follow a link in this list, right-click the link and open it in a new window or tab. This makes it easier to return to the outline and continue working through the prerequisites.

- Unless instructed otherwise by Websense Technical Support, ensure your system is functional prior to upgrade.
- Perform a full backup of your system before upgrading. See:
  - *Backing up TRITON infrastructure settings*, page 588
  - *Backing up Web Security configuration*, page 587
  - How do I back up and restore Websense Content Gateway?
  - *Preparing the Web Security Log Database for upgrade*, page 588
  - *Back up appliance configuration and settings*, page 619
  - How do I back up and restore Data Security software?
- If you are upgrading Data Security to v7.7.0, ensure that the user name and password set for the TRITON Unified Security Center account/Local Administrator account does not exceed 19 characters. Modify these settings if necessary. If you are upgrading it to v7.7.2 or beyond, this is not necessary.
- The upgrade process guides you through upgrading **all** components on the selected machine.
  - You cannot choose which components to upgrade.
  - Partial upgrades are not supported.
- When upgrading the TRITON management server, if upgrade fails for any component **except** TRITON Infrastructure, you can either continue to upgrade the rest of the components or exit the process and modify component settings.
  - You cannot continue if the infrastructure upgrade fails.
  - You cannot roll back a component that was upgraded successfully.
- After upgrade, your system has the same configuration as before the upgrade. The upgrade process does not allow you to change your configuration or settings.

Also see:

- Web Security: *Before upgrading Web Security to v7.7*, page 582
- Appliance: *Preparing for the appliance upgrade*, page 619

Upgrade sequence for solutions that include Web, Email, and Data Security

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x and earlier

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.7 and earlier
- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.6.x

If you have a mixed topology, upgrade components in the following order:

1. The machine hosting Web Security **Policy Broker**
   - This may be a software (Windows or Linux) installation or the **full policy source** appliance.

     If Policy Broker is on an appliance, it *does not matter* whether the appliance is running in Web Security or Web and Email Security mode.
   - If Policy Broker is on the same machine as other Web, Data, or Email Security components, still upgrade the Policy Broker machine first.
   - After Policy Broker is upgraded, Content Gateway instances on other machines do not perform Web filtering until they are also upgraded.
2. Additional instances of Web Security **Policy Server**
   - May be software-based or on **user directory and filtering** appliances.
   - If Policy Server is on an appliance, it *does not matter* whether the appliance is running in Web Security or Web and Email Security mode.
3. Additional instances of Web Security **Filtering Service** or **User Service**
   - Additional instances of Filtering Service may be software-based or on **filtering only** appliances.
   - If Filtering Service is on an appliance, it *does not matter* whether the appliance is running in Web Security or Web and Email Security mode.
4. Web and Email Security **Log Server**

If these components are on separate machines, it does not matter which is upgraded first.

> **Important**
>
> Make sure that no Email Security Log Database or Web Security Log Database jobs are running while the Log Server instances are being upgraded.

5. **TRITON management server** (includes TRITON infrastructure, as well as Web, Email, and Data Security management components)
   - Whenever possible, upgrade the management server before any other Data Security components. This ensures that Data Security policy engines (and thus analysis) continue to function until they are 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 a full policy source appliance—detection of fingerprinted content might not work on the appliance until the management server is upgraded.

     The Data Security policy engine embedded in Content Gateway and Email Security Gateway continues to monitor the old Web and email DLP policies and block/permit accordingly.
6. Any appliances running in **Email Security** mode
   - The Email Security Gateway MTA continues 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.
   - If your appliances are running in Web and Email Security mode, all appliances may already have been upgraded in steps 1-3.
7. Other **Web Security** components (including software-based installations of Content Gateway)
8. Other **Data Security** components

> **Important**
>
> The components running on the machine you are upgrading go down until the upgrade is complete. You should plan for a brief period of down time.

Upgrade procedure for solutions that include Web, Email, and Data Security

This procedure covers the steps required to upgrade either the whole of Websense TRITON Enterprise or a Web and Email Security solution. (Note that Email Security Gateway and Gateway Anywhere always include Data Security components.)

> **Tip**
>
> When you follow a link this procedure, right-click the link and open it in a new window or tab. This makes it easier to return to the outline and continue working through the task.

1. Upgrade Websense **Policy Broker**. All components on the Policy Broker machine (which may be a **full policy source** appliance in either Web Security or Web and Email Security mode) are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
   - *Upgrading V-Series Appliances to v7.7*, page 617
2. Upgrade any instances of Websense **Policy Server** running off the Policy Broker or machine. All components on each Policy Server machine, including **user directory and filtering** appliances, are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
   - *Upgrading V-Series Appliances to v7.7*, page 617
3. Upgrade any additional instances of Websense **Filtering Service** and **User Service**, running on other machines. All components on each machine, including **filtering only** appliances, are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
   - *Upgrading V-Series Appliances to v7.7*, page 617
4. Upgrade Web Security and Email Security **Log Server**. All components on the machine are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - Email Security: *Upgrade instructions*, page 671
5. Upgrade the **TRITON management server**. All modules on the machine are upgraded in the correct order. See *Upgrading the TRITON management server*, page 573.
6. Upgrade any additional software instances of Websense Network Agent and Content Gateway. If these components run on V-Series appliances, this step has already been done. See:

  - *Upgrading Content Gateway to v7.7.x*, page 605
  - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
  - *v7.7 Web Security software upgrade instructions (Linux)*, page 601

7. Upgrade any additional Web Security server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines. See:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
8. Upgrade any additional Data Security server components and agents, including supplemental servers, SMTP agents, ISA/TMG agents, printer agents, protectors, and mobile agents. See:
   - *Upgrading supplemental Data Security servers or standalone agents*, page 628
   - *Upgrading a Data Security protector or mobile agent*, page 629
9. Upgrade client components, including the logon application (LogonApp.exe), Remote Filtering Client, Web Endpoint, and Data Endpoint. See:
   - *Installing and Deploying Websense Endpoint Clients*, page 421
   - *Upgrading Data Security endpoints*, page 630

Upgrading the TRITON management server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.7 and earlier ◆ Data Security, v7.7.x ◆ Email Security Gateway and Gateway Anywhere, v7.6.x	◆ *TRITON Infrastructure*, page 574 ◆ *Web Security*, page 575 ◆ *Data Security*, page 575 ◆ *Email Security*, page 576

To upgrade TRITON management server components, use the v7.7 TRITON unified installer (Windows only): **WebsenseTRITON77Setup.exe**, available from:

www.websense.com/MyWebsense/Downloads/

Select your **product**, **version** (7.7), and **operating system** (Windows), then click **download** next to the installer description.

When you launch the installer, it detects that earlier versions of the product are installed, and automatically starts a series of upgrade wizards—one for each of the modules included on the management server.

✓ **Note**

If TRITON management components run on a virtual machine, restart the server after the upgrade is complete.

TRITON Infrastructure

The TRITON infrastructure provides basic framework for all of the management components that make up TRITON Unified Security Center (TRITON console). This framework includes a central settings database that stores shared configuration (like administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Welcomes you to the installation and upgrade wizard. 1. Click **Next** to begin the upgrade process. The system checks disk space requirements. 2. When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows: • The destination folder for the installation files. • The name of the SQL Server machine and the user name of an authorized database administrator. • The IP address of the TRITON management server and administrator credentials. Click **Next** to accept the properties.
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more.
Summary	When module upgrade is complete, summarizes your system settings, including: • The destination folder for the installation files. • The name of the SQL Server machine and the user name of an authorized database administrator. • The IP address of the TRITON management server and administrator credentials. Click **Finish** to complete the upgrade for this module.

Web Security

The Web Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	Welcomes you to the Web Security upgrade wizard. Click **Next** to continue.
Pre-Installation Summary	Informs you that a previous Web Security software version was detected. 1. Click **Next** to start the upgrade. The installer proceeds to stop all Websense services. This can take up to 10 minutes. When complete, it tells you which components will be upgraded. 2. Click **Install** to continue. The installer to backs up critical files.
Installation	Shows installation progress. When complete, the installer configures your 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 screens.

Wizard Screen	Fields
Welcome	This screen welcomes you to the installation and upgrade wizard for Data Security. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
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. 1. Click **Done** and you're prompted to update your predefined policies and content classifiers. 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. 3. Click **Close** when the updates are complete.

1. Log onto the TRITON Console.

2. Select the Data Security tab.
3. You are prompted to update your policies. Follow the prompts. Websense research teams stay abreast of regulations across many industries and you should keep your policies and classifiers up-to-date. Depending on the number of policies you have, this can take up to an hour. During this time, do not restart the server or any of the services.
4. After your policies are updated, select **Settings** > **Deployment** > **System Modules**.
5. Listed are 2 instances of each Web Content Gateway module that is registered with the system. Delete the older instances. You can identify these by looking at the version number that is displayed.
6. If you are upgrading from v7.6.x to v7.7.0 or v7.7.2 and you use regulatory and compliance attributes in your quick policies, do the following to restore your settings. (You do not need to do this if you are upgrading to v7.7.3).
    a. Select **Main** > **Policy Management** > **DLP Policies**.
    b. One by one, open your quick policies—Web DLP, email DLP, and mobile DLP.
    c. Select the regulatory and compliance attribute. For Web and mobile DLP, this attribute is on the Attributes tab. For email DLP it is on the Outbound and Inbound tabs.
    d. Select the laws to enforce. You wrote these down before starting the upgrade.
7. Click **Deploy**.

For information on upgrading other Data Security components, such as supplemental servers, agents, and endpoints, refer to *Upgrading Data Security to v7.7.x*, page 627.

Email Security

The Email Security upgrade wizard contains the following screens.

Wizard Screen	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.
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: • The components to be installed • The pre-existing and new version numbers • The destination folder for the installation files • The required and available disk space Click **Install** to begin the upgrade.

Wizard Screen	Fields
Installation	This screen shows that the installation is progressing. The management component, TRITON - Email Security, is upgraded on the TRITON management server. The Email Security Log Server is upgraded on machines where it is found. 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.

26 Upgrading Websense Web Security Solutions

Deployment and Installation Center | Web and Data Security Solutions | Version 7.6.x and earlier

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x and earlier ◆ Data Security, v7.6.0, v7.6.2 and v7.6.3	◆ *Determine your Web Security upgrade path*, page 579 ◆ *Web Security or Web and Data Security upgrade outline*, page 580

Determine your Web Security upgrade path

- Websense Web Filter and Web Security software-only deployments (no V-Series appliances) at versions **7.5.x** or v**7.6.0 - 7.6.5** may be directly upgraded to version 7.7.x.

  If this describes your deployment, jump to *Web Security or Web and Data Security upgrade outline*, page 580, to work through the upgrade process.

- Websense Web Security Gateway and Gateway Anywhere deployments (software or appliance) must be at versions **7.6.0 - 7.6.5** to upgrade directly to version 7.7.x.

  If you are at v7.6.0 - v7.6.5, jump to *Web Security or Web and Data Security upgrade outline*, page 580, to work through the upgrade process.

- V-Series appliances, Content Gateway, and Data Security components must be upgraded to v7.6 before you can upgrade to v7.7.x.

  If you have v7.5.x appliances, Content Gateway, or Data Security components, jump to *Upgrading from Web Security Gateway, Web Security Gateway Anywhere, or V-Series Appliance v7.5.x*, page 582.

- If you are upgrading from a version prior to v7.5.x, jump to *Upgrading from Web Security version 7.1.x or earlier*, page 580.

  Policy information and most configuration details are preserved across intermediate upgrades.

Web Security or Web and Data Security upgrade outline

Tip

When you follow a link in this outline, right-click the link and open it in a new window or tab. Close the new window or tab to return to the outline and continue working through the task.

1. Review the Release Notes for your solution and deployment platform. The Release Notes are available from support.websense.com.
   - Websense Web Security
   - Content Gateway
   - TRITON Unified Security Center
   - V-Series Appliance
   - Websense Data Security
2. Before beginning the upgrade process, see:
   - *Before upgrading Web Security to v7.7*, page 582
   - *Preparing for the appliance upgrade*, page 619
3. When you are ready to start upgrading, refer to the instructions for your version:
   - *Upgrading Web Security or Web and Data Security solutions from v7.6*, page 594
   - *Upgrading Web Filter or Web Security software-only deployments from v7.5.x*, page 591

   These procedures include both software and appliance instructions.
4. After upgrade, see the Upgrading User Quick Start tutorial, available either from support.websense.com, or through the Help menu in your management console.

   The tutorial includes a table of terminology changes, directions for finding features or tools in the new management console, and a summary of what was added in each version, beginning with 7.0.

Upgrading from Web Security version 7.1.x or earlier

Deployment and Installation Center | Web Security Solutions | Version 7.1.x and earlier

Applies to:

◆ Web Filter, Web Security, and Web Security Gateway, v7.1.x and earlier

Versions 7.0.x and 7.1.x and earlier must be upgraded to version 7.5 (Web Filter or Web Security software-only deployments) or 7.6 (all other deployments) before they can be upgraded to version 7.7.x.

- Websense Content Gateway and V-Series appliances must be at v7.6.0 - 7.6.5 to upgrade to v7.7.
- Data Security components (included with Web Security Gateway Anywhere) must be at v7.6.x to upgrade to v7.7.

For example, the path might be:

v7.0 (Web Filter, software-only) > v7.5 > v7.7

v7.1.1 (Web Security Gateway) > 7.6 > v7.7

Policy information and most configuration details are preserved across intermediate upgrades.

Follow the upgrade instructions for each intermediate version, available from support.websense.com:

- v7.5 software Upgrade Guide
- v7.5 appliance Upgrade Tips and Upgrade Instructions
- v7.6 software Upgrade Instructions
- v7.6 appliances Upgrade Instructions

Because hardware and operating system support has changed over time, the upgrade process for software (non-appliance) components is likely to require hardware and operating system updates. See *Migrating Web Security to a new operating system*, page 661, for details.

If you are upgrading from a version prior to 7.0, given fundamental changes to software functionality, operating system support, and hardware requirements, the smoothest path to v7.7.x is to perform a fresh installation at the current version. See *Installing Web Security solutions*, page 193.

After upgrading Web Security to v7.5 or v7.6, see the following topics to upgrade to v7.7:

- Software: *Before upgrading Web Security to v7.7*, page 582
- Appliance: *Preparing for the appliance upgrade*, page 619
- *Upgrading Web Filter or Web Security software-only deployments from v7.5.x*, page 591
- *Upgrading Web Security or Web and Data Security solutions from v7.6*, page 594

Upgrading from Web Security Gateway, Web Security Gateway Anywhere, or V-Series Appliance v7.5.x

Deployment and Installation Center | Web Security Solutions | Version 7.5.x

Applies to:
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5.x

If you have v7.5.x Websense Web Security Gateway or Gateway Anywhere, or if your current deployment includes v7.5.x appliances, you must upgrade to **v7.6** before upgrading to v7.7.

Configuration and policy settings are preserved during the intermediate upgrade.

Use the following intermediate upgrade instructions, available from support.websense.com:

- v7.6 software Upgrade Instructions
- v7.6 appliances Upgrade Instructions

The upgrade process for software (non-appliance) components may require system updates. See *Migrating Web Security to a new operating system*, page 661, for details.

After upgrading to v7.6, see the following topics to upgrade to v7.7:

- Software: *Before upgrading Web Security to v7.7*, page 582
- Appliance: *Preparing for the appliance upgrade*, page 619
- *Upgrading Web Security or Web and Data Security solutions from v7.6*, page 594

Before upgrading Web Security to v7.7

Deployment and Installation Center | Web Security Solutions | Version 7.0.x - v7.6.5

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.6.5	◆ *Restart services before starting the upgrade*, page 585 ◆ *Internet access during the upgrade process*, page 585 ◆ *Find your upgrade procedure*, page 585

The upgrade process is designed for a properly functioning deployment of Websense software. Upgrading does not repair a non-functional system.

> **Tip**
>
> When you follow a link in this list, right-click the link and open it in a new window or tab. Close the new window or tab to return to the outline and continue working through the task.

Before upgrading Websense Web Security solutions:

1. Make sure the installation machine meets the hardware and operating system recommendations in *System requirements for this version*, page 2.
2. Verify that third-party components that work with Websense software, including your database engine and directory service, are supported. See *Requirements for Web Security solutions*, page 6.
3. Make sure that your filtering integration product (if any) is supported in v7.7. If necessary, upgrade your integration product before beginning the Websense software upgrade.
   - Integration with Squid Web Proxy Cache is not supported in v7.7.x.
   - Integration with Microsoft ISA Server is not supported in v7.7. For information about integration with Microsoft Forefront TMG, see *Integrating Web Security with Microsoft Products*, page 535.
   - Supported Citrix versions have changed. In addition, the Citrix Integration Service changed substantially in v7.6. See *Integrating Web Security with Citrix*, page 513, before upgrading Websense software.
   - To review current Check Point integration requirements, see *Integrating Web Security with Check Point*, page 445.
   - To review current Cisco integration requirements, see *Integrating Web Security with Cisco*, page 481.
   - Blue Coat no longer supports traditional (on-box or off-box) integration with Websense Web Security solutions. It is still possible, however, to integrate Blue Coat proxies with off-box Websense Web Security via ICAP.

     To make the transition to ICAP integration, first upgrade to v7.7.

     - If you are moving from an on-box integration, next install v7.7 Filtering Service. Be sure to select the integrated option, and specify Websense ICAP Service as the integration product.

       Note that after upgrade, you must recreate your policies in TRITON - Web Security, because you are now using Websense Filtering Service for policy enforcement.
     - If you are transitioning an off-box integration, uninstall Filtering Service, then reinstall it, selecting Websense ICAP Service as the integration product.

       Transitioning off-box integration with Blue Coat does not affect your existing policies.

See *Integrating Web Security using ICAP Service*, page 557, for more information about installing and configuring Websense ICAP Service.

- To review current integration requirements for other products, see *Installing Web Security for Universal Integrations*, page 563.

4. Back up all of your Websense components before starting the upgrade process.
   - For Web Security software backup instructions, see *Backing up Web Security configuration*, page 587.
   - For V-Series Appliance backup instructions, see Using the backup utility in Appliance Manager Help.
   - For v7.6 TRITON settings, see *Backing up TRITON infrastructure settings*, page 588.
5. If you are upgrading from v7.5, there have been changes to the underlying structure of the management console (the TRITON Unified Security Center). See *Placing the Web Security management console (v7.5 only)*, page 586, for help in determining whether you will need to move management components on upgrade.
6. If you are upgrading from v7.5, using delegated administration, and allow administrators to log on using their network accounts:
   - Make sure that your directory service includes an email address for each **user** account defined as a Websense delegated administrator.
   - Group accounts do not need to have an email address assigned in the directory.

   See *Upgrading or merging administrator accounts*, page 759, for more information.
7. Before upgrading Websense Filtering Service, make sure that the Filtering Service machine and the management server (TRITON - Web Security machine) have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.
8. It is important that you back up your current Log Database and stop any active SQL Server Agent jobs prior to upgrading. See *Preparing the Web Security Log Database for upgrade*, page 588.
9. If Websense Log Server uses a Windows trusted connection to access the Log Database, be sure to log on to the Log Server machine using the trusted account to perform the upgrade. To find out which account is used by Log Server:
   a. Launch the Windows Services dialog box (**Start** > **Administrative Tools** > **Services**).
   b. Scroll down to find **Websense Log Server**, then check the **Log On As** column to find the account to use.
10. If your deployment includes V-Series appliances, see *Preparing for the appliance upgrade*, page 619, for additional preparatory steps.

Restart services before starting the upgrade

Websense services must be running before the upgrade process begins. If any service is stopped, start it before initiating the upgrade.

The installer will stop and start Websense services as part of the upgrade process. If the 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 and stopping Web Security services*, page 709, for instructions.
- On Windows machines, if you have configured the **Recovery** properties of any Websense service to restart the service on failure, use the Windows Services dialog box to change this setting to **Take No Action** before upgrading.

Internet access during the upgrade process

When you upgrade a standalone installation, filtering stops when Websense services are stopped. Users have unfiltered access to the Internet until the Websense services are restarted.

If Websense Web Security solutions are integrated with another product or device, all traffic is either permitted or blocked during the upgrade, depending on how your integration product is configured to respond when Websense Filtering Service is unavailable.

The Websense Master Database is removed during the upgrade process. Websense Filtering Service downloads a new Master Database after the upgrade is completed.

Find your upgrade procedure

When you are sure you have complete backups of your existing configuration and are ready to begin the upgrade process, see:

- *Upgrading Web Filter or Web Security software-only deployments from v7.5.x*, page 591
- *Upgrading Web Security or Web and Data Security solutions from v7.6*, page 594

Placing the Web Security management console (v7.5 only)

Deployment and Installation Center | Web Security Solutions | Version 7.5.x

Applies to:

- Web Filter and Web Security, v7.5.x

This topic assumes that you have only Websense Web Filter or Web Security (not Web Security Gateway or Gateway Anywhere). If you have one of the Web Security Gateway solutions, you must upgrade to v7.6 before upgrading to v7.7.

Version 7.7 includes a single management console for system configuration, policy management, and reporting for all Websense security solutions.

- The management console is called the TRITON Unified Security Center (often abbreviated to TRITON console).
- The Web Security module of the TRITON console is called TRITON - Web Security.
- All management components run on the same machine, called the TRITON management server.

When upgrading from v7.5, you can upgrade your management console in place, if it is installed on a Windows Server 2008 32-bit machine or a Windows Server 2008 R2 machine.

When you upgrade in place, a new component, TRITON Infrastructure, is installed first. This is the piece that ties together all management modules, and allows for centralized configuration of administrator accounts and other shared settings.

Once TRITON Infrastructure is installed, the Web Security management console is upgraded.

If your management components are on Linux, or on Windows 2003 or earlier, you must move management components to a different machine.

- If management components are on a Linux operating system supported for other Web Security components, you can remove the existing management components during upgrade of the machine (when prompted by the upgrade process), then later create a TRITON management server on a Windows machine.
- If management components are on an operating system that is not supported in v7.7, you can either:
  - Migrate components to a supported operating system at your existing version, then upgrade to v7.7. See *Migrating Web Security to a new operating system*, page 661.

- If Policy Broker and Policy Broker are running on an operating system supported in v7.7, optionally uninstall management components before upgrade, perform the upgrade, then create a TRITON management server on a supported Windows machine. See *Creating a TRITON Management Server*, page 180.

Backing up Web Security configuration

Deployment and Installation Center | Web Security Solutions | Version v7.0.x - v7.6.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.6.x

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.

Use the Websense Backup Utility on each non-appliance machine that contains Websense Web Security components:

1. Stop Websense services. See *Starting and stopping Web Security services*, page 709.
2. Do one of the following:
   - Windows: Open a command prompt (Run > cmd) and navigate to the Websense **bin** directory. The default location is:

     v7.0 - v7.5: C:\Program Files\Websense\bin

     v7.6: C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin
   - Linux: Navigate to the Websense installation directory (/opt/Websense, by default).
3. Use the following command to run the Backup Utility:
   - Windows:

     ```
     wsbackup -b -d <directory>
     ```
   - Linux:

     ```
     ./WebsenseTools -b -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 TRITON - Web Security Help for your version. (For v7.6, the list is also included in the Backup and Restore FAQ.)

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.

If you are upgrading from v7.6, also back up your TRITON Infrastructure settings. See *Backing up TRITON infrastructure settings*, page 588.

Backing up TRITON infrastructure settings

Deployment and Installation Center | Web Security Solutions | Version 7.6.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x

If you are running v7.6, also use the TRITON backup utility to back up your TRITON Settings information (administrator accounts, for example).

1. On the TRITON management server machine, do one of the following:
   - Windows Server 2008 or 2008 R2: Go to **Start** > **Administrative Tools** > **Task Scheduler**, then select **Task Scheduler Library**.
   - Windows Server 2003: Go to **Start** > **Control Panel** and select **Scheduled Tasks**.
2. If the Triton Backup task is disabled, right-click the task and select **Enable**.
3. Right-click the Triton Backup task and select **Run**.

Preparing the Web Security Log Database for upgrade

Deployment and Installation Center | Web Security Solutions | Version 7.0.x - v7.6.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.6.x

It is important that you back up your current Websense reporting databases and stop any active SQL Server Agent jobs prior to upgrading. After upgrade, reactivate the jobs to resume normal database operations.

> **Warning**
>
> If database operations are active during upgrade, the Websense Log Database may be left in an inconsistent state, rendering it unusable.
>
> When this occurs, it can be difficult to fix.
>
> Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

1. Back up Web Security reporting databases.

   Refer to Microsoft documentation for instructions on backing up databases. The Websense Web Security databases are named wslogdb70 (the catalog database) and wslogdb70_1, wslogdb70_2, and so on (partition databases).
2. On the Log Server machine, use the Windows Services dialog box (Start > Administrative Tools > Services) to stop **Websense Log Server**.
3. Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).
4. To disable all currently active Websense SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:
   - Websense_ETL_Job_wslogdb70
   - Websense_IBT_DRIVER_wslogdb70
   - Websense_Mantenance_Job_wslogdb70

   Disabling the jobs prevents them from executing at the next scheduled time, but does not stop them if a job is in process.

   Make sure all jobs have completed any current operation before proceeding with upgrade.
5. Perform the Websense upgrade.
6. After upgrade, enable the disabled jobs to resume normal database operations.

Web Security upgrade order

Deployment and Installation Center | Web Security Solutions | Version 7.0.x - v7.6.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.6.x

When you upgrade Websense Web Security solutions, the installer or appliance patch automatically upgrades all components on a given machine in the correct order.

As a result, if you have a main server or appliance hosting most of your Web Security components (including Policy Broker), upgrade that machine first, then use the list below to determine the upgrade order for any additional servers or appliances.

If your components are widely distributed, however, ensure that they are upgraded in the correct order, as follows:

1. Policy Broker

   If you are using Websense V-Series appliances, Policy Broker runs on the **full policy source** appliance or server.

   Regardless of the other components running on the machine, always upgrade the Policy Broker machine first. The other components on the machine are upgraded in the correct order.

2. Policy Server

   Runs on all **user directory and filtering** appliances, and may run on other Windows or Linux servers.

3. User Service, Filtering Service, and Directory Agent

   This includes all **filtering only** appliances, and may include other Windows or Linux servers.

4. Log Server and Sync Service

   Make sure that all Log Database jobs are stopped before starting the Log Server upgrade. See *Preparing the Web Security Log Database for upgrade*, page 588.

5. Websense Manager or TRITON - Web Security
6. Network Agent, Content Gateway
7. Transparent identification agents, Remote Filtering Server, Filtering plug-in (Citrix XenApp or Microsoft Forefront TMG)

> **Important**
>
> The Web Security server components must be all be upgraded to the same version. They are not cross-version compatible with one another.

Once all server components have been upgraded, upgrade client components (the logon application, Remote Filtering Client, Web Endpoint) in any order. See:

- Using Logon Agent for Transparent User Identification
- *Installing and Deploying Websense Endpoint Clients*, page 421

Upgrading Web Filter or Web Security software-only deployments from v7.5.x

Deployment and Installation Center | Web Security Solutions | Version 7.5.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.5.x	◆ *Performing the Web Filter or Web Security upgrade from v7.5.x*, page 591 ◆ *All Web Security solutions: new security certificate*, page 593

In v7.7, management components for all Websense solutions are centralized into a single console: the TRITON Unified Security Center, or TRITON console.

Websense Web Filter and Web Security management components can run on:

- Windows Server 2008 (32-bit)
- Windows Server 2008 R2

Prior to upgrade:

- See *Upgrading or merging administrator accounts*, page 759, for important information about how administrator accounts are handled by the upgrade process.
- Update current Web Security network administrators to be authenticated against a version 7.7-supported directory service if necessary. See *Upgrading or merging administrator accounts*, page 759, for more information.

Performing the Web Filter or Web Security upgrade from v7.5.x

Tip

When you follow a link in this procedure, right-click the link and open it in a new window or tab. Close the new window or tab to return to the outline and continue working through the task.

This procedure covers the steps required to upgrade Web Filter or Web Security software-only deployments directly from v7.5.x to v7.7. If your deployment includes V-Series appliances or Content Gateway, you must upgrade to v7.6.x before upgrading to v7.7.

1. Upgrade the server hosting Websense **Policy Broker**. All components on the machine are upgraded in the correct order. For instructions, see:

   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
2. Upgrade any instances of Websense **Policy Server** running off the Policy Broker or machine. All components on each Policy Server machine are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
3. Upgrade any additional instances of Websense **Filtering Service** and **User Service**, running on other machines. All components on each machine are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
4. Upgrade Websense **Log Server**. All components on the machine are upgraded in the correct order. For instructions, see *v7.7 Web Security software upgrade instructions (Windows)*, page 596.
5. Upgrade or create the **TRITON management server**:
   - If your current TRITON - Web Security machine **meets** TRITON Unified Security Center requirements, you can upgrade in place. See *v7.7 Web Security software upgrade instructions (Windows)*, page 596.
   - If your current TRITON - Web Security machine **does not meet** TRITON Unified Security Center requirements, remove TRITON - Web Security from its current location when prompted by the installer.

     Next, create a TRITON management server on a Windows Server 2008 (32-bit) or Windows Server 2008 R2 machine. See *Creating a TRITON Management Server*, page 180.
6. Upgrade any additional Websense Network Agent instances.
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
7. Upgrade any additional server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines. See:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601

When you are finished, proceed to:

- *All Web Security solutions: new security certificate*, page 593, for information about the security certificate used to secure communication with management components.
- *Installing and Deploying Websense Endpoint Clients*, page 421, for information about deploying endpoint clients, including Remote Filtering Client, Web Endpoint, and Data Endpoint.
- Using Logon Agent for Transparent User Identification, for information about deploying the v7.7 logon application (LogonApp.exe).

All Web Security solutions: new security certificate

After upgrade, the first time you launch the management console (TRITON Unified Security Center), the browser displays a certificate error.

This appears because the management console uses a certificate signed by Websense, Inc., and Websense, Inc., is not a recognized certificate authority.

After you install the certificate issued by Websense, Inc., in your browser, communication with the management console is secured, and the certificate warning is not displayed again (in this browser).

To install the TRITON console certificate in Internet Explorer

You can either run an ActiveX control to install the certificate automatically, or you can install the certificate manually.

To install the certificate automatically (requires ActiveX to be enabled in the browser):

1. On the browser warning page, click **Continue to this website (not recommended)**. You must click through the warning once to be able to install the certificate.
2. Click the yellow warning box on the logon screen (where the message **Websense security certificate is required**) appears.
3. In the pop-up box, click the **install the certificate** link.
4. If prompted, provide credentials to allow the certificate to be installed, then click **Yes**.
5. If the browser pops up a yellow security warning bar, click the yellow bar to allow the program that installs the certificate to run.

To install the certificate manually:

1. On the browser warning page, click **Continue to this website (not recommended)**. You must click through the warning once to be able to install the certificate.
2. Click **Certificate Error** on the browser’s address bar (to the right of the management console URL), and then select **View certificate**.
3. In the Certificate dialog box, click **Install Certificate**.
4. Mark the **Place all certificates in the following store** radio button, and then click **Browse**.
5. Select the **Trusted Root Certification Authorities** folder, and then click **OK**.
6. Click **Next**, and then **Finish**.
7. When prompted to install the certificate, click **Yes**, and then click **OK** to close the success message.

Once the certificate is installed, you can launch the TRITON Unified Security Center using this browser without receiving further errors.

To install the TRITON console certificate in Firefox

On the Secure Connection Failed page:

1. Click **Or you can add an exception**.
2. Click **Add Exception**.
3. Make sure that **Permanently store this exception** is selected, and then click **Confirm Security Exception**.

Once the certificate is installed, you can launch the TRITON Unified Security Center using this browser without receiving further errors.

Upgrading Web Security or Web and Data Security solutions from v7.6

Deployment and Installation Center | Web Security Solutions | Version 7.6.0 - v7.6.5

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.0 - v7.6.5
- Data Security, v7.6.0, v7.6.2 and v7.6.3

This procedure covers the steps required to upgrade any Web Security solution, or Web and Data Security solutions together, from v7.6.0 - v7.6.5 to v7.7.

Tip

When you follow a link in this procedure, right-click the link and open it in a new window or tab. Close the new window or tab to return to the outline and continue working through the procedure.

1. Upgrade Websense **Policy Broker**. All components on the Policy Broker machine, which may be a **full policy source** appliance, are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
   - *Upgrading V-Series Appliances to v7.7*, page 617
2. Upgrade any instances of Websense **Policy Server** running off the Policy Broker or machine. All components on each Policy Server machine, including **user directory and filtering** appliances, are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596

- *v7.7 Web Security software upgrade instructions (Linux)*, page 601
- *Upgrading V-Series Appliances to v7.7*, page 617

3. Upgrade any additional instances of Websense **Filtering Service** and **User Service**, running on other machines. All components on each machine, including **filtering only** appliances, are upgraded in the correct order. For instructions, see:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
   - *Upgrading V-Series Appliances to v7.7*, page 617
4. Upgrade Websense **Log Server**. All components on the machine are upgraded in the correct order. For instructions, see *v7.7 Web Security software upgrade instructions (Windows)*, page 596.
5. Upgrade the **TRITON management server**. In Web Security Gateway Anywhere deployments, or deployments that include both Web and Data Security, Data Security components on the machine are detected and automatically upgraded in the correct order. See:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596.
   - *Upgrading Data Security to v7.7.x*, page 627.
6. Upgrade any additional Websense Network Agent instances and, if applicable, Websense Content Gateway. If these components run on V-Series appliances, this step has already been done. See:
   - *Upgrading Content Gateway to v7.7.x*, page 605.
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
7. Upgrade any additional Web Security and, if applicable, Data Security server components, including Protector, transparent identification agents, and Remote Filtering Server, that may be running on other machines. See:
   - *v7.7 Web Security software upgrade instructions (Windows)*, page 596
   - *v7.7 Web Security software upgrade instructions (Linux)*, page 601
   - *Upgrading Data Security to v7.7.x*, page 627

Important

The Web Security server components must be all be upgraded to the same version. They are not cross-version compatible with one another.

When you are finished, see:

- *All Web Security solutions: new security certificate*, page 593, for information about the security certificate used to secure communication with management components.
- *Installing and Deploying Websense Endpoint Clients*, page 421, for information about deploying endpoint clients, including Remote Filtering Client, Web Endpoint, and Data Endpoint.

- Using Logon Agent for Transparent User Identification, for information about deploying the v7.7 logon application (LogonApp.exe).

v7.7 Web Security software upgrade instructions (Windows)

Deployment and Installation Center | Web Security Solutions | Version 7.6.x and 7.5.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x and v7.5.x

Use the version 7.7 TRITON Unified Installer (**WebsenseTRITON77Setup.exe**) to perform the upgrade. The installer detects:

- That older version components are installed
- Which components are installed
- The database engine version

Important

Follow the upgrade order provided in *Upgrading Web Filter or Web Security software-only deployments from v7.5.x*, page 591, or *Upgrading Web Security or Web and Data Security solutions from v7.6*, page 594, to ensure that you are upgrading components in the correct order.

Upgrade the Policy Broker machine first, then any machines running Policy Server. Distributed components on other machines must be upgraded **after** Policy Broker and Policy Server.

Before beginning:

- If you performed an intermediate upgrade to v7.5 or v7.6, and you have not restarted the upgraded machines, perform a restart before beginning the v7.7 upgrade.
- Perform a full system backup. See *Backing up Web Security configuration*, page 587.

Important

Filtering and logging services are not available while you are performing 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. Make sure that no administrators are logged on to TRITON - Web Security.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

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.

3. Stop Log Server and disable SQL Server Agent jobs.

   See *Preparing the Web Security Log Database for upgrade*, page 588.
4. Close all applications and stop any antivirus software.

Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

5. Configure current Web Security network administrators to be authenticated against a version 7.7-supported directory service if necessary. See *Upgrading or merging administrator accounts*, page 759, for more information.

Note

If you are upgrading from v7.5 or earlier, note that the **WebsenseAdministrator** account was replaced by an **admin** account in v7.6. See *Upgrading or merging administrator accounts*, page 759, for more information.

6. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON77Setup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
7. Double-click **WebsenseTRITON77Setup.exe** to launch the installer. A progress dialog box appears, as files are extracted.

8. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.

9. If **v7.5** TRITON - Web Security 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 *Placing the Web Security management console (v7.5 only)*, page 586, for more information.

   - If you click **Yes**:

     The **Installer Dashboard** appears and then TRITON Infrastructure Setup starts. See *Installing TRITON Infrastructure*, page 386, 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 TRITON - Web Security for removal. After the component is removed, the v7.7 Web Security component installer is started automatically.

10. On the installer **Introduction** screen, click **Next**.

    Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

11. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.

Important

Be sure to close all instances of TRITON - Web Security (v7.5) on all machines, before clicking **Next**.

If the **Database Information** screen appears, stating that 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 417, 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.

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 Windows Service dialog box to stop the services. See *Starting and stopping Web Security services*, page 709, 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**.

    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. Re-enable SQL Server Agent jobs if you disabled them prior to upgrade.

    See *Preparing the Web Security Log Database for upgrade*, page 588.

18. If you have an integration product installed, additional upgrade steps may be necessary. See:
    - *Integrating Web Security with Check Point*, page 445
    - *Integrating Web Security with Cisco*, page 481
    - *Integrating Web Security with Citrix*, page 513
    - *Integrating Web Security with Microsoft Products*, page 535
    - *Installing Web Security for Universal Integrations*, page 563
19. Repeat the upgrade procedure on each machine running Web Security components, in the recommended order (see *Web Security upgrade order*, page 589).

    All server components that interact must be upgraded to the same version. They are not cross-version compatible.

    If you have complete installations in separate locations that do not interact, they do not have to run the same Websense software version.

To add additional components to a machine after upgrade, 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 Windows components*, page 688.

New security certificate

After upgrade, the first time you launch the management console (TRITON Unified Security Center), the browser displays a certificate error.

This appears because the management console uses a certificate signed by Websense, Inc., and Websense, Inc., is not a recognized certificate authority.

When you install the certificate issued by Websense, Inc., in your browser, communication with the management console is secured, and the certificate warning is not displayed again (in this browser).

To install the TRITON console certificate in Internet Explorer

You can either run an ActiveX control to install the certificate automatically, or you can install the certificate manually.

To install the certificate automatically (requires ActiveX to be enabled in the browser):

1. On the browser warning page, click **Continue to this website (not recommended)**. You must click through the warning once to be able to install the certificate.
2. Click the yellow warning box on the logon screen (where the message **Websense security certificate is required**) appears.
3. In the pop-up box, click the **install the certificate** link.
4. If prompted, provide credentials to allow the certificate to be installed, then click **Yes**.
5. If the browser pops up a yellow security warning bar, click the yellow bar to allow the program that installs the certificate to run.

To install the certificate manually:

1. On the browser warning page, click **Continue to this website (not recommended)**. You must click through the warning once to be able to install the certificate.
2. Click **Certificate Error** on the browser’s address bar (to the right of the management console URL), and then select **View certificate**.
3. In the Certificate dialog box, click **Install Certificate**.
4. Mark the **Place all certificates in the following store** radio button, and then click **Browse**.
5. Select the **Trusted Root Certification Authorities** folder, and then click **OK**.
6. Click **Next**, and then **Finish**.
7. When prompted to install the certificate, click **Yes**, and then click **OK** to close the success message.

After the certificate is installed, you can launch the TRITON Unified Security Center using this browser without receiving further errors.

To install the TRITON console certificate in Firefox

On the Secure Connection Failed page:

1. Click **Or you can add an exception**.
2. Click **Add Exception**.
3. Make sure that **Permanently store this exception** is selected, and then click **Confirm Security Exception**.

After the certificate is installed, you can launch the TRITON Unified Security Center using this browser without receiving further errors.

v7.7 Web Security software upgrade instructions (Linux)

Deployment and Installation Center | Web Security Solutions | Version 7.6.x and 7.5.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x and 7.5.x

Use the Linux installer (**WebsenseWeb77Setup_Lnx.tar.gz**) to upgrade existing v7.5 or v7.6 components. After the installer starts, it detects which Websense components are installed and need to be upgraded.

Perform a full system backup before starting the upgrade process. See *Backing up Web Security configuration*, page 587.

If Websense components are installed on multiple machines, see *Web Security upgrade order*, page 589, for important information about the required upgrade sequence.

Important

Upgrade the Policy Broker machine first, then any machines running Policy Server.

Distributed components on other machines must be upgraded **after** Policy Broker and Policy Server.

Important

Filtering and logging services are not available while you are performing 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. Make sure no administrators are logged on to TRITON - Web Security.
2. Log on the installation machine with administrator privileges (typically, as **root**).
3. Close all applications and stop any antivirus software.
4. Check the **etc/hosts** file. If there is no host name for the machine, add one.

   See *Preparing for installation*, page 14, for instructions.
5. 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 and stopping Web Security services*, page 709.

6. Download the Web Security Linux installer from the Downloads page at mywebsense.com. The installer file is called **WebsenseWeb77Setup_Lnx.tar.gz**.
7. Uncompress the installer file and use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

   To launch the command-line installer, omit the -g switch:

   ```
   ./install.sh
   ```

   See *Starting the Web Security Linux installer*, page 210, for more detailed instructions.
8. On the Introduction screen, click **Next**.

> **Note**
>
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

9. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
10. If 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 7.7, TRITON - Web Security (the management console) 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 no administrators are logged on to TRITON - Web Security anywhere in the network, 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 and stopping Web Security services*, page 709, 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:
    - *Integrating Web Security with Check Point*, page 445
    - *Integrating Web Security with Cisco*, page 481
    - *Integrating Web Security with Citrix*, page 513
    - *Integrating Web Security using ICAP Service*, page 557
    - *Integrating Web Security with Microsoft Products*, page 535
    - *Installing Web Security for Universal Integrations*, page 563

18. Repeat the upgrade procedure on each machine running Web Security components, in the recommended order (see *Web Security upgrade order*, page 589).

    All server 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 for All Websense Modules*, page 675.

To add additional components to the machine after upgrade, 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 Windows components*, page 688.

27 Upgrading Content Gateway to v7.7.x

Deployment and Installation Center | Web Security Solutions | Version 7.6.x and earlier

Applies to:	**In this topic**
◆ Web Security Gateway and Web Security Gateway Anywhere v7.6.x and earlier	◆ *System requirements* ◆ *Upgrading distributed components* ◆ *Versions supported for upgrade* ◆ *Preparing to upgrade* ◆ *Upgrading Websense Content Gateway* ◆ *Post-upgrade activities*

This section provides upgrade instructions for software-based Websense Content Gateway installations. Upgrading Content Gateway on a V-Series appliance is handled by the V-Series upgrade (patch) process. See *Upgrading V-Series Appliances to v7.7*.

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. See *Versions supported for upgrade*.

> ✓ **Note**
> Technical papers and documents mentioned in this article are available in the Websense Technical Library.

System requirements

Before upgrading Content Gateway, make sure the installation machine meets the system recommendations in *System requirements for Websense Content Gateway*, including hardware specifications, operating system, and browser.

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 *Upgrading Websense Web Security Solutions*.

Versions supported for upgrade

Direct upgrade to Content Gateway version 7.7.x is supported from version 7.6.x and higher. Upgrades from versions **prior** to v7.6.x require intermediate upgrades:

- version 7.0/7.1 > version 7.5 > version 7.6 > version 7.7

Follow the upgrade procedures documented with each intermediate version.

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 versions that may not be found in this version of the upgrade supplement.

For example, 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 v7.5.

See:

- Version 7.5 Content Gateway Installation Guide
- Version 7.6 Content Gateway Installation Guide

To perform an intermediate upgrade, download the installer package for the intermediate version from the Websense Downloads site.

Upgrading from version 7.6.5

Due to the timing of Content Gateway releases 7.6.5 and 7.7.0, an enhancement to the user authentication **Fail Open** feature that was introduced in 7.6.5 was not included in 7.7.0. The enhancement is included in version 7.7.3.

- The Fail Open option is used to allow requests to proceed to Web Security when user authentication fails. For more information, see New in version 7.6.5.

  On upgrade to 7.7.3 the 7.6.x Fail Open setting is retained, as expect.

  The setting of the option on upgrade to 7.7.0 is:

  - 7.6.5 “Disabled” is set to 7.7.0 “Disabled”

- 7.6.5 “Enabled only for critical services failures” is set to 7.7.0 “Enabled”
- 7.6.5 “Enabled for all authentication failures, including incorrect password” is set to 7.7.0 “Enabled”

Preparing to upgrade

- Read the Release Notes for the version you are upgrading to:
  - 7.7.0 Release Notes
  - 7.7.3 Release Notes
- Read the upgrade instructions (this document)
- Upgrade TRITON Unified Security Center and TRITON - Web Security before upgrading Content Gateway. See *Upgrading Websense Web Security Solutions*.
- If you are upgrading Red Hat Enterprise Linux version 5 to version 6, see *Upgrading Red Hat Enterprise Linux during Content Gateway upgrade*.

Configuration settings not preserved

The following configuration settings are **not** preserved and must be reconfigured post-upgrade:

- Integrated Windows Authentication (IWA) Settings.

Note

Make a record of current IWA Settings prior to upgrade to be restored during *Post-upgrade activities*. For more information, see *Integrated Windows Authentication* in Content Gateway Manager Help.

New features to configure after upgrade

You may want to configure the following new and enhanced features post-upgrade.

- With Multiple Realm Authentication rules, the User-Agent and Cookie Mode caching options.

  For more information, see 7.7.3 Release Notes.
- Support for IPv6. To enable, go to Configure > My Proxy > Basic > General.

  For more information, see 7.7.0 Release Notes.

Upgrading Websense Content Gateway

Complete these steps to upgrade Content Gateway on a server in a software-based deployment.

- If you plan to upgrade from Red Hat Enterprise Linux 5 to Red Hat Enterprise Linux 6, see *Upgrading Red Hat Enterprise Linux during Content Gateway upgrade*.
- If you plan to remain on Red Hat Enterprise Linux 5, see *Upgrading from Content Gateway v7.6.x to v7.7.x*.

Important

Upgrade TRITON Unified Security Center and TRITON - Web Security to v7.7 prior to upgrading the operating system or Content Gateway. See *Upgrading Websense Web Security Solutions*.

Upgrading Red Hat Enterprise Linux during Content Gateway upgrade

Version 7.7.0 runs on Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6.0, 6.1, and 6.2, 64-bit, Basic Server. Version 7.7.3 adds support for update 6.3, 64-bit, Basic Server.

Upgrading from a 32-bit to 64-bit operating system creates a change in system architecture that requires a specific upgrade sequence to maintain Content Gateway configuration settings.

Use the following sequence to upgrade Content Gateway 7.6.x on Red Hat Enterprise Linux 5 32-bit, to Content Gateway v7.7.x on Red Hat Enterprise Linux 6 64-bit:

1. Log in or acquire root privileges. All steps should be performed as root.
2. Upgrade to Content Gateway 7.7.x. See *Upgrading from Content Gateway v7.6.x to v7.7.x*.
3. Using a special backup utility, create a backup of Content Gateway v7.7.x and save it in a trusted location on the network:

   ```
   cd ~/WCG/Current/
   ./wcg_config_utililty.sh create WCGbackup
   ```

   This creates a backup, `WCGbackup.tar.gz`, in the current directory.

4. Copy `WCGbackup.tar.gz` to a reliable location on the network where it can easily be retrieved after the operating system upgrade.
5. If you are upgrading Red Hat Enterprise Linux on this machine, uninstall Content Gateway. See Uninstalling Content Gateway. Continue with Step 7.

6. If you want to keep the current machine as a fallback option, power down the computer and disconnect it from the network. Install Red Hat Enterprise Linux on another machine and continue with Step 7.

   ✓ **Note**

   If you want to revert to the original machine, reconnect it to the network and power up. Content Gateway 7.7.x will re-register with TRITON – Web Security.

   If you want to repurpose the machine, do not reconnect it to the network until after you have uninstalled Content Gateway and assigned the machine a new IP address and hostname.

7. Using the same hostname, ethernet interface, and IP address used with Red Hat Enterprise Linux 5, install Red Hat Enterprise Linux 6. Updates 6.0, 6.1, and 6.2 are supported with 7.7.0. Content Gateway 7.7.3 adds support for update 6.3.

   ✓ **Note**

   Content Gateway is designed to run on Red Hat Enterprise Linux, **Basic Server** package. This is the default installation configuration and must be confirmed.

   For more information on installing Red Hat Enterprise Linux 6, see:

   - Red Hat Enterprise Linux 6 Installation Guide
   - *Required libraries in Red Hat Enterprise Linux 6*

8. Install Content Gateway. See *Installing Websense Content Gateway*.
9. Copy `WCGbackup.tar.gz`, that was saved in step 4, to:

   ```
   ~/WCG/Current/
   ```

10. Restore the configuration archive. As root:

   ```
   cd ~/WCG/Current/
   ./wcg_config_utility.sh restore WCGbackup.tar.gz
   ```

Upgrading from Content Gateway v7.6.x to v7.7.x

This section describes how to upgrade Content Gateway version 7.6.x to v7.7.x on your Red Hat Enterprise Linux 5 installation.

✓ **Note**

If you are upgrading to Red Hat Enterprise Linux 6, see *Upgrading Red Hat Enterprise Linux during Content Gateway upgrade*.

Upgrading Content Gateway on a V-Series appliance is handled by the V-Series upgrade (patch) process. See *Upgrading V-Series Appliances to v7.7*.

Before you begin, be sure to read *Preparing to install Websense Content Gateway*.

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*.

Note: /opt/WCG is the version 7.6 installation location.

1. Acquire root permissions:

   ```
   su root
   ```

2. If you are upgrading from versions 7.6.0 only:
   - If configured, disable clustering and leave disabled until all members of the cluster are upgraded.
   - If configured, disable Virtual IP failover and leave it disabled until all members of the cluster are upgraded and re-enabled.

3. 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 *Websense TRITON Enterprise default ports* for more information.

4. Download the Content Gateway version 7.7.x installer from mywebsense.com and save it to a temporary directory. For example:

```
mkdir wcg_v77
mv <installer tar archive> wcg_v77
```

5. Unpack the Content Gateway installer tar archive:

   ```
   cd wcg_v77
   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.

6. In the directory where you unpacked the tar archive, start the installation/upgrade script.

   ```
   ./wcg_install.sh
   ```

   Respond to the prompts.

   Content Gateway is installed and runs as **root**.

   Note

   Up to the point that you are prompted to confirm your intent 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.

7. 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.

8. Read the subscription agreement. At the following prompt, enter **y** to accept the agreement and continue the upgrade, or **n** to cancel.

   ```
   Do you accept the above agreement [y/n]? y
   ```

9. When asked, choose to replace the existing version of Content Gateway with the 7.7.x version.

   ```
   WCG version 7.6.n-nnnn was found.
   Do you want to replace it with version 7.7.x-nnnn [y/n]? y
   ```

10. 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/
    7.6.0-1143-20110322-131541/...done
    ```

```
Copying SSL Manager settings to /root/WCG/OldVersions/
7.6.0-1143-20110322-131541/...done

Moving log files from /opt/WCG/logs to /tmp/wcg_tmp/logs/
...done
```

11. 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.

12. If you answered **y** at Step 11, 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. If you answered **n** at Step 11, the current version of Websense Content Gateway is removed, and a fresh install of 7.7.x begins. See *Installing Websense Content Gateway* for a detailed description of the installation procedure.

14. 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 7.7.0-1200
    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/.
    ```

15. 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.

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
- 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 start Content Gateway:
>
> ```
> /opt/WCG/WCGAdmin start
> ```

17. Refresh the browser cache when logging in to Content Gateway Manager for the first time after upgrade by pressing Shift+F5. The Content Gateway Manager user interface has an updated look and feel for version 7.7 and the old .css files may need to be flushed from your browser cache.
18. Perform the post-installation steps described in *Post-upgrade activities* and in *Initial Configuration for All Websense Modules*.

Post-upgrade activities

In version 7.7.x, 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. 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.
3. 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.
4. If you were using **Integrated Windows Authentication** (IWA), re-enable it and join Content Gateway to the Windows Domain. Configure IWA using the settings you recorded prior to upgrade. See *Configuring Integrated Windows Authentication* in Content Gateway Manager Help.

5. If you upgraded from version 7.6.0 and disabled clustering at the start of the upgrade process, re-enable clustering after all members of the cluster are upgraded and restart Content Gateway (restarting any node causes all nodes to restart).
6. If you upgraded from version 7.6.0 and disabled Virtual IP failover at the start of the upgrade process, re-enable Virtual IP failover after all members of the cluster are upgraded and clustering has been re-enabled.
7. If Web Security Gateway Anywhere and Data Security are deployed together and upgraded to version 7.7, you must remove stale entries of Content Gateway instances registered in Data Security system modules. From the TRITON Console, go to **Data Security** > **Settings** > **Deployment** > **System Modules** and delete instances that display an old version number.
8. If Web Security Gateway Anywhere and Data Security are deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance must be deleted from the list of Data Security system modules or the deployment will fail. Go to the **Data Security** > **Settings** > **Deployment** > **System Modules** page, click on the affected Content Gateway instance to open its **Details** page, click **Delete** and then **Deploy**.
9. Complete support for **GRE Return Method with WCCP** is added in version 7.7.

   If WCCP with GRE is already configured, the existing configuration continues to function as it did in v7.6.x. Note that Content Gateway Manager will produce an alarm suggesting that you update your configuration. Updating the configuration migrates the configuration to the new GRE support infrastructure. You do not have to change your configuration unless you want to add the GRE Return Method.

Important

If you are using WCCP with Cisco ASA, after the upgrade your configuration continues to perform as it did with v7.6.x.

There is no need to change your configuration after upgrade.

In version 7.7.0, should you need to reconfigure Content Gateway to work with your ASA device, set the Forward and Return Method to L2. This forces Content Gateway to negotiate the correct supported method.

In version 7.7.3, should you need to reconfigure Content Gateway to work with your ASA device, access the Service group settings and select **ASA Firewall** from the **Special Device Profile** drop down box instead of individually selecting the GRE forward and return methods. This automatically selects the Packet Forward Method and Packet Return Method and sets some proxy internals.

10. If you use SSL Manager to process HTTPS traffic, the Root CA should be imported into all affected clients.

    In v7.7 (and beginning with v7.6.5), the Content Gateway default Root CA presented to clients is signed with SHA-1. In prior versions, the Root CA was signed with MD5.

    It is strongly recommended that all instances of Content Gateway use the same Root CA, and that for best security the signature algorithm be SHA-1.

    Note

    Client connections may fail (depending on specific browser behavior) if the client sees a certificate generated by an unknown Root CA.

    The best practice is to replace the Websense default Root CA with your organization’s Root CA signed by SHA-1 or stronger. See Internal Root CA in Content Gateway Help.

28 Upgrading V-Series Appliances to v7.7

Deployment and Installation Center | Web and Email Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Security, Web Security Gateway and Web Security Gateway Anywhere, v7.6.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.6.x ◆ V10000, V10000 G2 and V5000 G2, v7.6.x	◆ *Versions supported for upgrade*, page 618 ◆ *Estimates of time to complete upgrade*, page 618 ◆ *Preparing for the appliance upgrade*, page 619 ◆ *Upgrade instructions*, page 622 ◆ *Upgrading multiple V-Series appliances*, page 623 ◆ *Post-upgrade activities*, page 625

Use this information to upgrade existing V-Series appliances in:

- Web and Email mode
    - Web Security and Email Security Gateway (Anywhere)
    - Web Security Gateway (Anywhere) and Email Security Gateway (Anywhere)
- Web only mode
    - Web Security
    - Web Security Gateway (Anywhere)
- Email only mode
    - Email Security Gateway (Anywhere)

In addition to upgrading your appliances, you must also upgrade Websense components installed on other servers.

The order of upgrade is important. Follow the steps prescribed for each solution or combination of solutions.

- *Upgrading Websense Web Security Solutions*, page 579
- *Upgrading Data Security to v7.7.x*, page 627

- *Upgrading Email Security Gateway to v7.7*, page 669
- *Upgrading solutions that include Web, Email, and Data Security*, page 568

Versions supported for upgrade

You can upgrade directly to version 7.7.x from these versions of 7.6:

- 7.6.0, 7.6.1, 7.6.2, 7.6.5

Appliances running earlier versions must be upgraded to one of the above versions before upgrading to version 7.7.x.

✓ **Note**

The upgrade to version 7.7.3 is applied to V-Series appliances via a software patch. Patches are installed via the Appliance Manager under the **Administration** > **Patches/Hotfixes** > **Patches** page. You must be running version 7.7.0 to use the version 7.7.3 patch.

Estimates of time to complete upgrade

The table below provides estimates of the time needed for the 7.7.x patch to be installed on an appliance. The amount of time varies, as indicated. Not all V-Series configurations are shown.

System	Configuration	Elapsed time
V10000 G2	Web security only: Web Security Gateway Full policy source	70 - 90 minutes
V10000 G2 V5000 G2	Web security only: Web Security Gateway User directory and filtering	90 - 110 minutes
V10000 G2	Dual mode: Web Security Gateway and Email Security Gateway	70 - 90 minutes
V10000 G2 V5000 G2	Email security only	20 - 30 minutes

The following provides a basic sample scenario:

Approximate total upgrade time, beginning to end, for all upgrade tasks:

- 1 Dual mode V10000 G2 appliance
- 2 Windows 2008 Server R2 servers: 1 for TRITON console, 1 for Web and Email Log Server

3 hours and 10 minutes

Activity breakout:

- 15 minutes to download the version 7.7 appliance upgrade (patch) file
- 10 minutes to back up the V-Series appliance
- 70 to 90 minutes for the patch to perform the upgrade
- 10 minutes to restart the V-Series and verify that the upgrade was successful
- 20 minutes to download the version 7.7.x Websense TRITON Unified Installer
- 40 to 60 minutes to run the installer to upgrade on the TRITON management server and the Log Server host
- 5 minutes to restart the Windows servers and verify that the upgrade was successful

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied and until the appliance completes a restart. See *Estimates of time to complete upgrade*, page 618.

> ✓ **Note**
>
> Service is not disrupted while the off-box components are upgraded.

At completion of the V-Series upgrade, the appliance must be restarted.

Preparing for the appliance upgrade

Before applying the 7.7.x patch, perform the following tasks and be aware of the following issues.

If you are not already familiar with the preparation required for upgrade of off-appliance components, review those requirements before upgrading your appliances.

- For Web Security solutions, see *Before upgrading Web Security to v7.7*, page 582.
- For Email Security Gateway (Anywhere), see *Preparing for the upgrade*, page 670.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration** > **Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.

4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, save the backup file in another location.

Content Gateway logs

If the appliance hosts Web Security Gateway (Anywhere), during the upgrade, depending on their size, older Content Gateway logs may be automatically removed by the upgrade procedure.

To ensure that all Content Gateway logs are retained, you can download the Content Gateway logging directory.

1. In the Appliance Manager, go to **Administration >Logs**.
2. Select the **Websense Content Gateway** module and then **Download entire log file**.
3. Click **Submit** and specify a location to save the file.

Policy databases and Websense databases are not affected by the upgrade.

Content Gateway Integrated Windows Authentication (IWA) settings

IWA settings are not preserved in the upgrade.

If your deployment uses Content Gateway IWA user authentication, log onto Content Gateway and record the IWA settings, including the name of the domain to which IWA is joined. Keep this record where you can easily retrieve it after upgrade is complete.

Network Agent settings

In the majority of deployments, upgrade preserves all Network Agent settings.

However, when the following conditions are true, the upgrade process does not preserve several Network Agent settings:

- There is a Filtering only appliance that is configured to get policy information from the Policy Broker machine (either the Full policy source appliance or an off-appliance software installation).
- There is an off-appliance Network Agent installation that uses the Filtering Service on the Filtering only appliance, and uses the Policy Server on the Policy Broker machine.

When the above conditions are true and the upgrade is performed, the settings for the off-appliance Network Agent installation are not retained.

In this case, record your Network Agent settings (configured in TRITON - Web Security) before performing the upgrade. Go to the Local Settings page for each Network Agent instance (**Settings > Network Agent** > *agent_IP_address*) and record **all** of its settings.

The following local settings are not preserved.

- Filtering Service IP address

- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

NIC Configuration settings (from the **Settings > Network Agent > NIC Configuration** page for each NIC) are also not preserved:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

Save your record where you can easily access it when the upgrade is complete.

Websense administrator accounts

Make sure Websense administrator accounts authenticated by a directory service have an email address specified in the directory service. In version 7.7, an email address is required for each administrator account (except group accounts).

Content Gateway changes

See the Content Gateway Release Notes for information about enhancements and changes in version 7.7.0.

If you are upgrading to version 7.7.3, see the Content Gateway Release Notes for information about enhancements and changes in version 7.7.3.

SSL Manager

SSL Manager has been enhanced in several ways. See the release notes for more information.

Of particular note, a few Certificate validation options have changed. Users of Certificate validation should review the changes and adjust their settings.

IPv6

Incremental support is added in version 7.7. See the release notes for more information.

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 7.6.x (not recommended), disable the on-appliance instance after upgrading the appliance to version 7.7. To disable the on-appliance TRITON - Web 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 not available while the patch is being applied and until the appliance completes its restart. See *Estimates of time to complete upgrade*, page 618.

It is best to perform the upgrade at a time when service demand is low.

1. If you have multiple V-Series appliances, read *Upgrading multiple V-Series appliances*, page 623, **before** following this procedure.
2. 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.
3. Back up appliance configuration and settings. See *Back up appliance configuration and settings*, page 619.
4. Restart the appliance (in Appliance Manager: **Status** > **Modules** > **Restart Appliance**).
5. To download the upgrade patch, in the Appliance Manager, go to the **Administration > Patches/Hotfixes > Patches** tab. The 7.7.x upgrade patch should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The 7.7 patch should be listed as available.

   Alternatively, the patch can be downloaded from websense.com and uploaded to the appliance.

   a. Go to MyWebsense.com and select the **Downloads** tab. Click **Get Hotfixes & Patches**. Select your appliance model and version.

   b. Log on to the Appliance Manager and navigate to **Administration** > **Patch Management**.

c. Click **Browse**, and select the v7.7.x upgrade file.

d. Click **Upload**. After a few seconds, the upgrade is listed in the **Uploaded patches** list.

This is an efficient method when your deployment has many appliances because the download from Websense occurs only once. Other appliances can upload the patch from the local location.

6. Click **Install** to apply the upgrade.

> **Important**
> When patch installation begins, a dialog box indicates that the patch will take 5 to 10 minutes to apply. This is incorrect. The time is significantly longer. See *Estimates of time to complete upgrade*, page 618.

While the upgrade is being applied, services are **unavailable** to users.

7. When patch installation is complete, restart the appliance right away; click **Restart Now** when prompted. Do not cycle the power.

8. When the appliance has restarted, log on to the Appliance Manager and verify on the **Configuration** > **General** page that the V-Series version is 7.7.x.

   Next go to the **System > Configuration** page and confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.

   In rare cases, when logging onto 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.

9. If you have multiple appliances, upgrade them all. See *Upgrading multiple V-Series appliances*.

10. Upgrade all Websense components running off the appliance (including the TRITON management server, Web and Email Security Log Server, transparent identification agents, and so on).

    See *Upgrading Websense Web Security Solutions*, page 579, and *Upgrading Email Security Gateway to v7.7*, page 669, for instructions.

Upgrading multiple V-Series appliances

When multiple V-Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is an Email mode (only) appliance

Apply the 7.7.x upgrade patch before upgrading the off-appliance components.

Best practice for upgrade sequence if Full policy source is on V-Series

appliance

Follow this sequence whether the Full policy source is a Web mode (only) or Web and Email mode appliance.

Upgrade the **Full policy source** V-Series appliance and immediately restart when the upgrade completes.

1. Sequentially apply the upgrade to all **User directory and filtering** appliances. Restart each appliance when the upgrade completes.
2. Sequentially apply the upgrade to all **Filtering only** appliances.
3. 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 and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Use the version 7.7 Websense installer to upgrade the Policy Broker system. See *Upgrading Websense Web Security Solutions*, page 579, for instructions.
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.
4. Use the version 7.7.x Websense installer to upgrade remaining off-appliance components. See *Upgrading Websense Web Security Solutions*, page 579, 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, navigate to **Configuration > Web Security Components**.
2. For **Policy Source**, select **Full policy source**. Save the setting.
3. Upgrade this appliance to version 7.7.x 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, navigate to **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 7.7.x Websense installer to upgrade remaining off-appliance components. See *Upgrading Websense Web Security Solutions*, page 579, for instructions.

Post-upgrade activities

- If your appliance includes Email Security Gateway (Anywhere), perform the Email Security Gateway *Post-upgrade activities*, page 673.
- If your appliance is a Web Security Policy Server, log onto TRITON console, go to the TRITON - Web Security **Settings** > **General** > **Policy Servers** page and add the appliance. Next go to the TRITON console **Appliances** tab and register the appliance.
- If your appliance includes Web Security Gateway (Anywhere), perform the Content Gateway *Post-upgrade activities*.
- If your appliance uses the Network Agent module, *Verify Network Agent settings*.
- Review the Release Notes for the Websense solutions on your appliances (links provided below). There are several new features that may require some configuration to put into effect.

  Web Security users will be especially interested in the Threats dashboard (no configuration needed). Web Security Gateway (Anywhere) users will be interested in the enhanced outbound scanning options. It is recommended that all of the Scanning Options be reviewed.

  - Web Security Release Notes
  - Content Gateway Release Notes
  - Email Security Gateway Release Notes

Verify Network Agent settings

If you had to record your Network Agent settings prior to upgrade (*Network Agent settings*), restore them after the TRITON console has been upgraded.

Log on to TRITON - Web Security and go to **Settings** > **Network Agent** > **Local Settings**.

Select the IP address of the affected Network Agent installations and check and restore all values, paying particular attention to:

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring

- Ignore Port
- Debug Setting

Also, check the **Settings > Network Agent > NIC Configuration** page for each NIC:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

When your changes are complete, click **OK** and then **Save and Deploy**.

29 Upgrading Data Security to v7.7.x

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

You can upgrade to Websense Data Security v7.7.3 directly from v7.7.0 or v7.7.2. If you have an earlier version, however, there are interim steps to perform. These are shown in the table below.

Your current version	Step 1	Step 2	Step 3
7.1.x	Migrate to 7.6.0	Upgrade to 7.7.2	Upgrade to 7.7.3
7.5.x	Upgrade to 7.6.0	Upgrade to 7.7.2	Upgrade to 7.7.3
7.6.x	Upgrade to 7.7.2	Upgrade to 7.7.3	none
7.7.0	Upgrade to 7.7.3	none	none
7.7.2	Upgrade to 7.7.3	none	none

For instructions on upgrading to any 7.7.x version, see the following topics:

- *Upgrading the Data Security Management Server*, page 628
- *Upgrading supplemental Data Security servers or standalone agents*, page 628
- *Upgrading a Data Security protector or mobile agent*, page 629
- *Upgrading Data Security endpoints*, page 630

For instructions on upgrading to v7.6.0, see:

- *Upgrading Data Security to v7.6.0*, page 633

Upgrading the Data Security Management Server

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

To upgrade your management server, launch the latest TRITON installation package, **WebsenseTRITON77*x*Setup.exe**, where *x* is the version number. This is the same executable used for scratch installations.

> **Important**
>
> The ports for Data Security modules including Web Content Gateway have been consolidated to 17500-17515. The ports for communicating with Email Security Gateway have been consolidated to 17700-17714.
>
> Configure your firewall to open these ports before proceeding.

The installation package detects that earlier versions of the product are installed, and automatically starts a series of upgrade wizards—one for each of the installed components.

- TRITON infrastructure
- Web Security
- Data Security
- Email Security

The Data Security portion of the unified upgrade wizard upgrades all necessary components on the Data Security Management Server. See *Upgrading the TRITON management server*, page 573 for complete instructions on using the upgrade wizard. This section describes important steps to take before you begin the upgrade and after the upgrade is complete.

Upgrading supplemental Data Security servers or standalone agents

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Complete these steps to upgrade a supplemental Data Security server or stand-alone agent (e.g. SMTP, printer, crawler, or ISA/TMG) to v7.7.x.

See *Upgrading Data Security to v7.7.x*, page 627 to see if you can upgrade directly from your version or if you must perform interim upgrade steps.

1. Upgrade the Data Security Management Server. (See *Upgrading the Data Security Management Server*, page 628 for instructions.) This sequence is critical, because if you upgrade supplemental servers or agents first, they stop

communicating with the management server. If you upgrade the management server first, it continues communicating with the components until they are upgraded.

2. If you are upgrading a supplemental server or stand-alone crawler or printer agent to v7.7.0, ensure that the user name and password set for the Local Administrator account does not exceed 19 characters. Modify these settings if necessary. This is not necessary if you are upgrading to v7.7.2 or beyond.
3. Download and run the upgrade installer, **WebsenseTRITON77*x*Setup.exe**, where *x* is the version number.
4. The installation wizard appears.
5. Click **Next** until you complete the wizard.

   Any v7.7.x Data Security components found on this machine are upgraded.
6. After the upgrade has successfully completed, deploy the agents or supplemental servers by logging on to TRITON- Data Security and clicking **Deploy**.
7. 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.
   - File-system discovery starts but immediately indicates "completed with errors".

Upgrading a Data Security protector or mobile agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Do the following to upgrade your protector or mobile agent from version to v7.7.x.

See *Upgrading Data Security to v7.7.x*, page 627 to see if you can upgrade directly from your version or if you must perform interim upgrade steps.

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.

1. Upgrade the TRITON management server as described above. This sequence is critical, because if you upgrade the protector or mobile agent first, it stops communicating with the management server. If you upgrade the management server first, it continues communicating with the components until they are upgraded.
2. Copy the file, protector-update-7.7.*x-yyyy*, into the directory `/tmp` where *x-yyyy* is the latest version and build number.
3. Enter the command:

   ```
   chmod +x /tmp/protector-update-7.7.x-yyyy
   ```
4. If you are upgrading to v7.7.0 from v7.6.8, log on as root and run the following command:

   ```
   rm -r /var/tmp/yum_update_cache
   ```
5. Run the following command:

   ```
   bash ./tmp/protector-update-7.7.x-yyyy
   ```
6. Answer **Y** on the "Are you sure?" question, and complete the wizard, accepting the defaults.
7. Restart the protector or mobile agent machine when the wizard completes.
8. If you have not already, log onto the machine as *root*.
9. Run the following command to re-register the protector or mobile agent with the management server, then follow the prompts in the wizard:

   ```
   wizard securecomm
   ```
10. If you are upgrading to v7.7.0 from v7.6.8, run the following command:

    ```
    rm -r /var/tmp/yum_update_cache
    ```
11. In TRITON - Data Security, click **Deploy**.
12. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

    When you upgrade a 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 false positives and negatives.

Upgrading Data Security endpoints

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

First upgrade the Data Security Management Server and any supplemental Data Security servers. Then upgrade Data Security endpoints.

Windows

After you have updated the Data Security Management Server:

1. Go to the %DSS_Home% directory (by default: **c:\Program Files\Websense\Data Security\client\**) and run **WebsenseEndpointPackageBuilder.exe** to create a new endpoint client package.
2. Choose Windows 32- or 64-bit when prompted.
3. Deploy the v7.7.x package to each endpoint using GPO, SMS, or a similar deployment method. You can install v7.7.x on top of earlier versions without uninstalling and re-installing them.
4. Restart the endpoint after installation is complete.

Linux

After you have updated the Data Security Management Server:

1. Go to the %DSS_Home% directory (by default: **c:\Program Files\Websense\Data Security\client\**) and run **WebsenseEndpointPackageBuilder.exe** to create a new endpoint client package.
2. Choose Linux when prompted.
3. To upgrade Data Endpoint software on a Linux computer, copy the correct installer to the machine and run it as root.
   - **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.

   No reboot is necessary. The endpoint software starts automatically. You can install v7.7.x on top of earlier versions without uninstalling and re-installing them.

See *Deploying Websense endpoints*, page 424 for more information.

30 Upgrading Data Security to v7.6.0

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.1.x, 7.5.x, 7.6.x	◆ *General exceptions*, page 633 ◆ *v7.1 exceptions*, page 633 ◆ *v7.5 exceptions*, page 634

Websense Data Security v7.1 and v7.5 can be upgraded to Data Security 7.6 with some exceptions. For instructions, see the following topics:

- *Preparing for upgrade of Data Security*, page 634
- *Upgrading the Data Security Management Server to v7.6.0*, page 636
- *Upgrading a supplemental Data Security server or standalone agents to v7.6.0*, page 648
- *Upgrading a Data Security protector to v7.6.0*, page 651
- *Upgrading Content Gateway with Data Security*, page 653
- *Upgrading Data Security endpoints*, page 653
- *Upgrade Notes and Exceptions*, page 655

General exceptions

- 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.

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 655, for full details.

Preparing for upgrade of Data Security

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	**In this topic:**
◆ Data Security, v7.1.x, 7.5.x, 7.6.x	◆ *Redirect traffic*, page 635 ◆ *TRITON management server*, page 635 ◆ *SQL Server*, page 635 ◆ *7.1 license file not valid*, page 636 ◆ *Websense administrator accounts*, page 636 ◆ *Notes and exceptions*, page 636

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 (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 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 for this version*, page 2, 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 for this version*, page 2, 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 a “full” version of 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 417, 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 administrator accounts*, page 759, for more information.

Notes and exceptions

Read *Upgrade Notes and Exceptions*, page 655 for important information about data and configuration that may not be supported or may be moved by the upgrade process.

Upgrading the Data Security Management Server to v7.6.0

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.1.x, 7.5.x, 7.6.x	◆ *Upgrade in place*, page 637 ◆ *Upgrade to another machine*, page 642

Complete these instructions to upgrade a Data Security Management Server from version 7.1 or 7.5 to 7.6. Unless otherwise noted, all instructions apply to both version 7.1 and 7.5 Data Security Management Server.

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 637
- *Upgrade to another machine*, page 642

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 656 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.

6. Continue with the appropriate procedure:
   - *Upgrading from version 7.5*, page 638
   - *Upgrading from version 7.1*, page 639

Upgrading from version 7.5

Note: in the following steps, the Websense folder is typically C:\Program Files\Websense.

1. Stop the DSS watchdog service:
   a. Select **Start** > **Programs** > **Accessories** > **Scheduled tasks**.
   b. Right-click **DSS Watchdog** and select **Properties**.
   c. De-select **Enabled**.
   d. Click **OK**.
2. In the Windows Services console, stop the **Websense DSS Manager** service.

   Alternatively, issue the command **net stop tomcat6** in a Command Prompt.
3. Rename **Websense\Data Security\forensics_repository\data** to **Websense\Data Security\forensics_repository\oldData**
4. Create a new folder named **Websense\Data Security\forensics_repository\data**
5. Create a new folder named **Websense\Data Security\archive_mng\oldStorage**
6. Move all folders starting with **FR-ARC-** from **Websense\Data Security\archive_mng\storage** to **Websense\Data Security\archive_mng\oldStorage**.
7. In the Windows Services console, start the **Websense DSS Manager** service.

   Alternatively, issue the command **net start tomcat6** from the Windows Command Prompt.
8. Move or copy the following folder to a location outside the Websense folder:

   Websense\Data Security\forensics_repository\oldData
9. Search the **oldData** folder for files with the name ***.ser** and delete those files.
10. Move or copy all folders starting with **FR-ARC-** from **Websense\Data Security\archive_mng\oldStorage** to a location outside the Websense folder.
11. Continue with *Upgrading from all versions*, page 639.

Upgrading from version 7.1

Note that in the following steps, the Websense folder is typically C:\Program Files\Websense.

1. In the Windows Services console, stop the **Websense DSS Manager** service.

   Alternatively, issue the command **net stop tomcat6** in a Command Prompt.

2. Rename **Websense\Data Security Suite\Archive**
   to **Websense\Data Security Suite\oldArchive**

   Create a new folder named **Websense\Data Security Suite\Archive.**

3. 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).
4. In the Windows Services console, start the **Websense DSS Manager** service.

   Alternatively, issue the command **net start tomcat6** from a Windows Command Prompt.

5. Move or copy **Websense\Data Security Suite\oldArchive** to a location outside the Websense folder.
6. Continue with *Upgrading from all versions*, page 639.

Upgrading from all versions

1. Obtain the upgrade export tool zip package and extract it.
2. Download **WebsenseDataSecurityUpgradeExportTool.zip** from www.mywebsense.com.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.

3. 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 655, 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.

4. Check the following files for any errors:

   - dbexport.log (in export tool folder you created in Step 2, for example C:\temp\upgrade_export_tool)
   - db.log (in export tool folder you created in Step 2, for example C:\temp\upgrade_export_tool)
   - %dss_home%/archive/mng/export-data/DataExport.log

   If you find errors, contact Websense Technical Support.

5. 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

6. Perform the actions appropriate to your machine, as described in *Preparing for installation*, page 14.
7. Download and launch the version 7.6 Websense installer (Websense installer).

   A progress dialog box appears, as files are extracted:
8. 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.
9. TRITON Infrastructure Setup starts. Complete the TRITON Infrastructure Setup wizard. See *Installing TRITON Infrastructure*, page 386, 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.
10. 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 1).

    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.
11. Click **Next** in the prior-version installer to begin removing components.

    Components are removed.
12. 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.

13. 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.

14. 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 413, for instructions. **Important**: When following these instructions, be sure to import the data exported when you ran the export script (in Step 1) on the **Import Data From Previous Version** screen.

15. 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 10, page 638)
       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).

16. 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:

      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. 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**.

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 655 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 2, for example C:\temp\upgrade_export_tool)
   - db.log (in export tool folder you created in Step 2, 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 3).

When upgrading from 7.1 or 7.5:

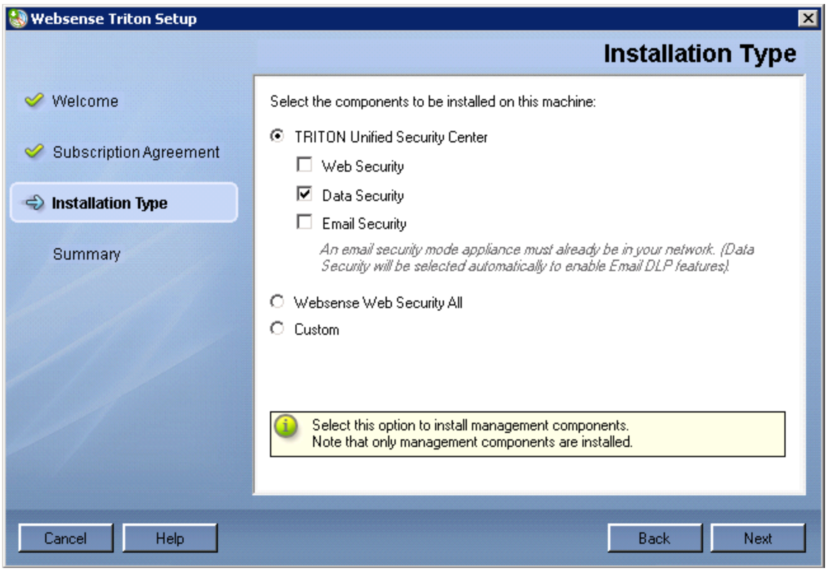
- Certs (folder)
- DSS_FILES (folder)
- Forensics_repository (folder)
- OldPolicyXMLs (folder)
- Onlinetables (folder)
- Partitiontables (folder)
- **Backup.txt** (this file is required when restoring data to the upgraded system)
- Dataexport.log

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 180. **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.



Installation Type

Select the components to be installed on this machine:

● TRITON Unified Security Center

- □ Web Security
- ☑ Data Security
- □ Email Security

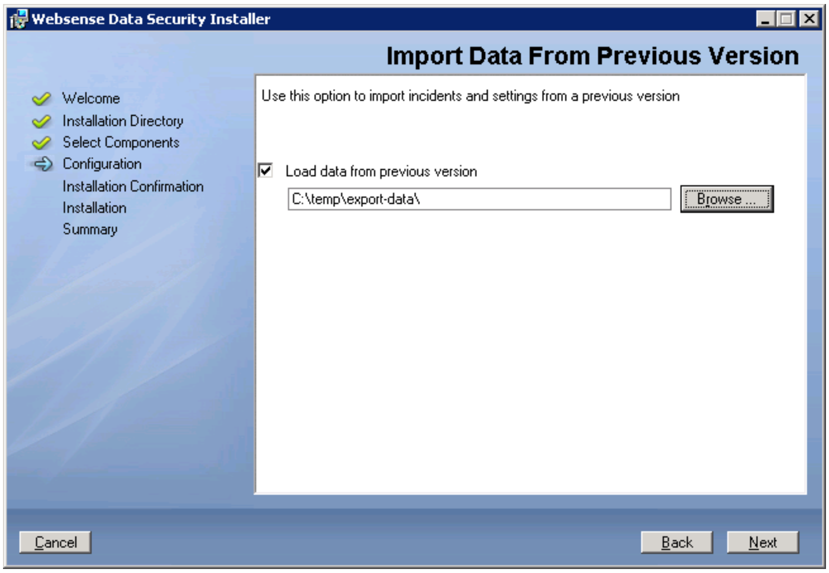
An email security mode appliance must already be in your network. (Data Security will be selected automatically to enable Email DLP features)

○ Websense Web Security All

○ Custom

Select this option to install management components.
Note that only management components are installed.

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.



Import Data From Previous Version

Use this option to import incidents and settings from a previous version

☑ Load data from previous version

C:\temp\export-data\

12. If you meet one or more of the following conditions prior to upgrade, run the SQL script, <name> located in the /<name> directory.

- You have more than one protector
- You have more than one ISA/TMG agent

- You have a Web Content Gateway agent

13. 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.

14. 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 10, page 638)

       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 to v7.6.0

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.1.x, 7.5.x, 7.6.x	◆ *Upgrading from version 7.5*, page 649 ◆ *Upgrading from version 7.1*, page 649

Complete these steps to upgrade a supplement Data Security server or standalone agent (e.g. SMTP, printer, discovery/crawler, 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 14.
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 to v7.6.0

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.1.x, 7.5.x, 7.6.x	◆ *Upgrading from version 7.5*, page 651 ◆ *Upgrading from version 7.1*, page 652

> **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/).Allow read/write/execute by all on the update file, for example:

   ```
   chmod 777 /tmp/protector-update-7.6.0
   ```

2. Start the upgrade, for example:

   ```
   /tmp/protector-update-7.6.0
   ```

3. When the upgrade script is finished, reboot the machine.
4. 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.

5. 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:

- Data Security, v7.1.x, 7.5.x, 7.6.x

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 *Installing Websense Content Gateway*, page 219.

To upgrade Content Gateway 7.5 to 7.6, see *Upgrading Content Gateway to v7.7.x*, page 605. Once you have upgraded Content Gateway, reregister it with the TRITON management server. See *Confirm Content Gateway registration with Data Security*, page 680.

Upgrading Data Security endpoints

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:

- Data Security, v7.1.x, 7.5.x, 7.6.x

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 424.

Important

At the completion of any endpoint update, you must restart the endpoint for the updates to take effect.

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).

Upgrade Notes and Exceptions

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.1.x, 7.5.x, 7.6.x	

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 5, page 640).

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 TRITON - 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.

31 Migrating Web Security to a new operating system

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x, v7.1.x, v7.5.x, and v7.6.x

If your current Websense Web Security software is running on hardware or software that is no longer supported in v7.7.x, the upgrade process also includes an operating system migration.

Depending on your current operating system and hardware, it may be possible to update the operating system in place (on the existing machine). Always back up your Websense software before performing an operating system update.

Whether you update the operating system in place or move to another machine, make sure that the machine meets the hardware requirements for your target Websense software version: **v7.7.x**.

This migration guide provides the steps for migrating core Web Security components from one operating system to another. If your solution includes Websense Content Gateway, see *Upgrading Red Hat Enterprise Linux during Content Gateway upgrade*, page 608, for Content Gateway operating system migration instructions.

To prepare for the migration process, continue with *Order of migration and upgrade steps*, page 661.

Order of migration and upgrade steps

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x, v7.1.x, v7.5.x, and v7.6.x

Depending on your current version, the order of operating system migration and Websense software upgrade steps varies:

Current Version	Current Platform	Upgrade Path
v7.0.x	Windows 2003	1. Upgrade to v7.5.x in place. 2. Migrate to Windows 2008. 3. Upgrade to v7.7.x on the new platform.
v7.0.x	Red Hat Enterprise Linux 3	1. Migrate to Red Hat Enterprise Linux 5. 2. Upgrade to v7.5.x on the new platform. 3. Upgrade to v7.7.x.
v7.1.x	Windows 2003	1. Migrate to Windows 2008. 2. Upgrade to v7.5.x on the new platform. 3. Upgrade to v7.7.x.
v7.1.x	Red Hat Enterprise Linux 4	1. Migrate to Red Hat Enterprise Linux 5. 2. Upgrade to v7.5.x or v7.6.x on the new platform. 3. Upgrade to v7.7.x.
v7.5.x	Windows 2003	1. Migrate to Windows 2008. 2. Upgrade to v7.7.x.
v7.5.x, v7.6.x	Red Hat Enterprise Linux 4	1. Migrate to Red Hat Enterprise Linux 5. 2. Upgrade to v7.7.x on the new platform.
v7.6.x	Windows 2003	1. Migrate to Windows 2008 or 2008 R2. 2. Upgrade to v7.7.x.

For more detailed migration instructions, see:

- *Migrating management components (Websense Manager or TRITON - Web Security)*, page 663
- *Moving Web Security policy components to a new machine*, page 664
- *Updating the operating system on an existing Web Security machine*, page 665

Migrating management components (Websense Manager or TRITON - Web Security)

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x, v7.1.x, v7.5.x, and v7.6.x	◆ *Migrating the v7.6 TRITON management server to a new operating system*, page 663 ◆ *Migrating v7.5.x or earlier Websense Manager or TRITON - Web Security to a new operating system*, page 664

When you migrate management components (Websense Manager in v7.1.x and earlier, or TRITON - Web Security in v7.5.x and later) to a new operating system, keep in mind that:

- In v7.7.x, Web Security management components, when not run in conjunction with Data or Email Security management components, can reside on Windows Server 2008.
- When Web Security management components run together with Data Security, Email Security, or both, all management components must run on the same **Windows Server 2008 R2** machine.

Migrating the v7.6 TRITON management server to a new operating system

To move the v7.6 TRITON management server to a new operating system:

1. Perform a TRITON Infrastructure backup, and store the backup file in a safe location.

   See How do I back up and restore the TRITON infrastructure? in the Websense Technical Library.
2. Uninstall TRITON - Web Security from its current location.
3. Reinstall v7.6 TRITON - Web Security on the new server.

   This makes it possible to preserve your existing global configuration settings, as explained in the next step.
4. Restore your TRITON Infrastructure backup to the new machine to preserve your TRITON Settings configuration.

   See How do I back up and restore the TRITON infrastructure? in the Websense Technical Library.

5. Upgrade your Web Security solution to v7.7.x. See *Upgrading Websense Web Security Solutions*, page 579.

   The upgrade instructions include information about the order in which to upgrade your v7.6.x components.

For migration instructions for additional components, see:

- *Moving Web Security policy components to a new machine*, page 664
- *Updating the operating system on an existing Web Security machine*, page 665

Migrating v7.5.x or earlier Websense Manager or TRITON - Web Security to a new operating system

To move management components to a new operating system, before the final upgrade to v7.7:

1. Uninstall the current version of Websense Manager or TRITON - Web Security.
2. Upgrade your remaining Web Security software components to v7.7.x. See *Upgrading Websense Web Security Solutions*, page 579.
3. Install v7.7.x Websense TRITON Infrastructure and the TRITON - Web Security module on a Windows Server 2008 R2 machine. See *Creating a TRITON Management Server*, page 180.

For migration instructions for additional components, see:

- *Moving Web Security policy components to a new machine*, page 664
- *Updating the operating system on an existing Web Security machine*, page 665

Moving Web Security policy components to a new machine

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x, v7.1.x, v7.5.x, and v7.6.x

When you move the **same Websense software version** to a new machine, use the following procedure to preserve your policies and system configuration.

1. On the original Policy Broker machine (running on the old operating system), navigate to the Websense **bin** directory:
   - Windows: C:\Program Files\Websense\bin *or* C:\Program Files\Websense\Web Security\bin

- Linux: /opt/Websense/bin/

2. Use the following command to back up your existing policy information:

   ```
   PgSetup --save backup.policydb
   ```

   This command backs up only data stored in the Policy Database. It does **not** back up custom block pages or customized configuration files. To preserve customized configuration files or block pages, back those up separately.

3. Copy the backup file resulting from the previous step to the Websense **bin** directory on the new Policy Broker machine.

4. Stop all Websense services on the new Policy Broker machine:

   - Windows: Use the Windows Services dialog box (Start > Administrative Tools > Services) to stop all Websense services, ending with the following, in the order shown:

     a. Websense Policy Server

     b. Websense Policy Broker

     c. Websense Policy Database

   - Linux: Use the **/opt/Websense/WebsenseAdmin stop** command.

5. Use the following command to restore the contents of your Policy Database backup to the new machine without overwriting important token and IP address information:

   ```
   PgSetup --restore backup.policydb --no-clobber
   ```

   The “no-clobber” parameter eliminates the need to update the token value in the config.xml file (a step included in older migration procedures).

6. Start the Websense services on the new Policy Broker machine:

   - Windows: Use the Windows Services dialog box (Start > Administrative Tools > Services) to start all Websense services, starting with the following, in the order shown:

     a. Websense Policy Database

     b. Websense Policy Broker

     c. Websense Policy Server

   - Linux: Run the command from the **/opt/Websense/** directory.

Updating the operating system on an existing Web Security machine

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x, v7.1.x, v7.5.x, and v7.6.x

If the existing Web Security machine meets the hardware specifications for v7.7.x, and you want to update the operating system in place, rather than moving to a new machine, use the following procedure to make sure that your policies and system configuration are preserved.

1. Run the Websense Backup Utility on each machine that includes Web Security components.
   - Windows: Navigate to the Websense **bin** directory (C:\Program Files\Websense\bin or C:\Program Files\Websense\Web Security\bin) and enter the following command:

     ```
     wsbackup -b -d <directory>
     ```
   - Linux: Navigate to the **/opt/Websense/** directory and enter the following command:

     ```
     ./WebsenseTools -b -b -d <directory>
     ```

   Replace <directory> with the destination path for the backup archive.
2. (*v7.6 only*) Run the TRITON infrastructure backup process.
   a. Go to **Start > Administrative Tools > Task Scheduler** and select **Task Scheduler Library**.
   b. If the **Triton Backup** task is disabled, right-click the task and select **Enable**.
   c. Right-click the **Triton Backup** task and select **Run**.

   The file is saved in the **C:\EIPBackup** directory by default.
3. Save the backup file or files in a safe location on another machine or device.
4. Update the operating system on the machine.

Depending on the operating system that you are upgrading, Websense software may continue to run normally, or may be damaged or completely removed from the machine.

If there is a problem with Websense software on the machine:

1. Uninstall and reinstall the affected components, keeping the same Websense software version that existed before the operating system changed.
2. Verify that Websense components are running as expected.
3. Copy the backup file or files created in previous procedure to the Websense machine.
4. Use the Websense Backup Utility to restore your policy and configuration settings from backup.
   - Windows: Navigate to the Websense **bin** directory (C:\Program Files\Websense\bin or C:\Program Files\Websense\Web Security\bin) and enter the following command:

     ```
     wsbackup -r -f <path>\<file>.tar.gz
     ```
   - Linux: Navigate to the **/opt/Websense/** directory and enter the following command:

     ```
     ./WebsenseTools -b -r -f <path>/<file>.tar.gz
     ```

Replace <path> with the location of the file and <file> with the file name. The file name always ends with a .tar.gz extension.

5. (*v7.6 only*) Restore your TRITON infrastructure settings from backup.
   a. Go to **Start > Administrative Tools > Services**.
   b. Right-click the following service and select **Stop**.
      - Websense TRITON Unified Security Center
      - Websense TRITON Web Server
      - Websense TRITON - Web Security
   c. Open the Windows Control Panel and click **Programs**, then **Programs and Features**.
   d. Select **Websense TRITON Infrastructure**, then click **Uninstall/Change**.
   e. When asked if you want to modify, repair, or remove TRITON infrastructure, select **Modify**, then click **Next** until you get to the **Restore Data from Backup** screen.
   f. Mark the **Use backup data** box, then click **Browse** to locate the backup folder.
   g. Click **Next** until the restore process beings.
   h. When the restore process is complete, click **Finish**.
   i. Return to the Services window and click **Refresh**. If any of the services that you stopped has not restarted, right-click it and select **Start**.

32 Upgrading Email Security Gateway to v7.7

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:	In this topic:
- Email Security Gateway and Email Security Gateway Anywhere v7.6.x	- *Versions supported for upgrade*, page 669 - *Preparing for the upgrade*, page 670 - *Upgrade instructions*, page 671 - *Post-upgrade activities*, page 673 - *Recovery procedures*, page 674

These instructions cover the upgrade of a TRITON - Email Security system from v7.6.x to v7.7. The procedure assumes that the system contains an appliance running in Email Security only mode.

If your system includes a dual-mode appliance (with Websense Web Security or Web Security Gateway) or any other Websense product component, you should review the upgrade materials for that product area as well:

- Web Security
- Content Gateway
- Data Security
- V-Series appliances

Versions supported for upgrade

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:
- Email Security Gateway and Email Security Gateway Anywhere v7.6.x

Email Security Gateway versions

The following Email Security Gateway versions can be directly upgraded to version 7.7:

- 7.6.0
- 7.6.2

Windows Server versions

If any Email Security component is currently installed on Windows Server 2003, it must be migrated to Windows Server 2008 R2 before the upgrade. In other words, you need to move the v7.6.x version of the Email Security component installed on Windows 2003 to the new 2008 server and then perform the Email Security Gateway upgrade to v7.7 process.

Preparing for the upgrade

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.6.x

The backup procedures outlined in the following steps are safeguards against an unexpected interruption of your v7.7 upgrade process. A power outage or appliance restart may not allow the upgrade process to finish successfully. You may need to restore your settings databases to their pre-upgrade state in order to re-initiate and complete the upgrade.

Use the following procedure to prepare for your upgrade to Email Security Gateway v7.7:

1. Back up the TRITON Unified Security Center settings. See the topic titled Backup and Restore of TRITON Data in TRITON Unified Security Center Help.
2. Back up the Data Security management server configuration. See the Websense Technical Library topic titled How do I back up and restore Data Security software?
3. Back up your Microsoft SQL Server databases. Ensure that all the files in the following directories are included in your backup:

   \\Database\\esglogdb76

   \\Database\\esglogdb76_*n*

   \\SQL Server Agent\\Jobs\\ Websense_ETL_Job__esglogdb76

   \\SQL Server Agent\\Jobs\\Websense_Maintenance_Job__esglogdb76

   See your Microsoft SQL Server documentation for backup procedure details.

4. Back up Email Security Gateway appliance configuration settings using the appliance back-up procedure.

   ✓ **Note**

   You can perform a full appliance backup or an individual product module backup (just Email, or on a dual-mode appliance, Web and Email).

   As a best practice, we recommend that you perform a full appliance backup rather than an individual module backup.

   See the Websense Technical Library topic titled How do I back up and restore V-Series appliances?

5. Back up Email Security Gateway management server configuration settings using the options on the **Settings** > **General** > **Backup/Restore** screen. Click **Backup** to store your settings locally. You can also specify a remote storage location for your configuration settings and then click **Backup**.

   See the topic titled Backing up and restoring management server settings in TRITON - Email Security Help for details.

6. Upgrade any third-party integration products if necessary for use with Email Security v7.7. See third-party product documentation for appropriate upgrade requirements and procedures.

7. Redirect email traffic out of the system that is being upgraded.

✓ **Note**

The Personal Email Manager end-user utility is not available until after the V-Series appliance upgrade.

Upgrade instructions

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.6.x

Before you begin the upgrade process, you need to configure your firewall to open the following ports:

- Ports 17500 - 17515 (C/E1/E2 interfaces), for outbound traffic to Websense Data Security
- Ports 17700 - 17714 (E1 and E2 interfaces), for inbound communication with Email Security Gateway

See *Email Security Gateway ports*, page 723, for information about all Email Security Gateway default ports, including appliance interface designations and communication direction.

Use the following procedure to perform the upgrade of Email Security Gateway to v7.7:

1. Upgrade Email Security Gateway Log Server if it is installed on a machine other than the one on which the TRITON Console is installed.

    a. Select the **Custom** option on the Installation Type page of the upgrade installer and choose to install the Email Security Log Server only.

    b. Follow the installation wizard instructions.

    The installer does not allow you to change existing configuration settings. Changes must be made after the upgrade.

    The upgrade installer stops the Email Security Gateway Log Server service, updates the Email Security Gateway Log Server, and then restarts the Email Security Gateway Log Server service.

    ✓ **Note**

    The Email Security Gateway management server is not available until after the TRITON Console upgrade.

2. Upgrade all your V-Series appliances. Appliance upgrade is performed using the Appliance Manager patch facility to download the version 7.7 patch and apply it to the appliance. See *Upgrade instructions*, page 622, for the appliance patch upgrade procedure.

    ✓ **Note**

    V-Series appliance services are not available while the patch is being applied and until the appliance completes its restart.

    If your Email Security appliances are configured in a cluster, the primary box should be upgraded first, followed by all its secondary machines, 1 at a time. You do not need to release the appliances from the cluster in order to perform the upgrade.

    Email should not be directed through these machines during the upgrade process.

3. Upgrade the TRITON Console machine. Use the TRITON Enterprise upgrade installer and ensure that TRITON - Email Security is selected for upgrade.

    Follow the installation wizard instructions.

    The installer does not allow you to change configuration settings. Changes must be made after the upgrade.

    The upgrade script stops the Email Security Gateway manager service, updates the Email Security Gateway SQL Server databases, and then restarts the Email Security Gateway manager service.

Post-upgrade activities

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.6.x

Your system should have the same configuration after the upgrade process as it did before the upgrade. Any configuration changes can be made after the upgrade process is finished.

After your upgrade is completed, redirect email traffic through your system to ensure that it performs as expected.

Email hybrid service registration information is retained during the upgrade process, so you do not need to complete the registration again. However, you must repair the registration with Data Security, as described in the next section.

Data Security registration

You must re-register Email Security Gateway with the Data Security module, using the following procedure:

1. In the TRITON - Email Security module, navigate to **Settings** > **General** > **Data Security** and click **Unregister**.
2. In the TRITON - Data Security module, navigate to S**ettings** > **Deployment** > **System Modules**.
3. Click the Email Security Gateway entry.
4. Click **Delete** at the top of the **System Modules** > **Email Security Gateway** page to remove Email Security Gateway registration.
5. When prompted, click **Deploy** to apply the changed Data Security setting.
6. In the TRITON - Email Security module, navigate to **Settings** > **General** > **Data Security**.
7. Register the Email Security appliance with Data Security.
8. Return to the Data Security module and click **Deploy** in the upper right area of the screen.

Recovery procedures

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.6.x

In the event that your upgrade was unexpectedly interrupted (for example, by a power outage or appliance restart), you can use the backup files you created earlier in the process to restore your system to its pre-upgrade state. (See *Preparing for the upgrade*.)

Use the following procedure to recover your Email Security Gateway v7.6.x system:

1. Use the v7.6.0 recovery DVD to reimage your V-Series appliance and run firstboot.
2. If necessary, upgrade from v7.6.0 to v7.6.x.

   Important

   Your backup files should match the version of Email Security to which you are restoring them.

   For example, if your backup files are from v7.6.0, you should not upgrade to v7.6.x before restoring the files to Email Security.

3. Restore the backup files to your system in the following order, using the back up and restore information for each component referenced in *Preparing for the upgrade*:
   a. V-Series appliance
   b. Microsoft SQL Server databases
   c. TRITON Unified Security Center
   d. TRITON - Data Security
   e. TRITON - Email Security manager
4. Verify that your system works as it did before the interrupted upgrade.

You can now initiate the upgrade from v7.6.x to v7.7.

33 Initial Configuration for All Websense Modules

Deployment and Installation Center | Web, Data, and Email Security Solutions | v7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

1. Some of the ports required by Websense components during installation are no longer needed when installation is complete. For information about the ports required for component communication, as well as details about which components need Internet access, see *Websense TRITON Enterprise default ports*, page 712.
2. 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 724.
3. If administrators use Internet Explorer to access the TRITON Unified Security Center (management console), make sure that Enhanced Security Configuration is disabled on their machines.

   For example, in Windows Server 2008:

   a. Open the Server Manager.

   b. Under **Server Summary**, in the Security Information section, click **Configure IE ESC**.

   c. In the **Internet Explorer Enhanced Security Configuration** dialog box, under **Administrators**, select the **Off** radio button, and then click **OK**.
4. Use a supported browser (see *System requirements for this version*, page 2) to launch the TRITON management console and log on using the default account:

   a. Navigate to the following URL:

   ```
   https://<IP_address>:9443/triton/
   ```

   Here, <*IP_address*> is the IP address of the TRITON management server.

   If the TRITON console is installed on a Websense appliance (recommended only for evaluations) use the IP address of the appliance's C interface.

   b. Log on as the default **admin** account, using the password set during installation.

5. Enter your subscription key or keys. At first startup:
   - TRITON - Web Security prompts for a subscription key. If you do not enter the key at the prompt, you can enter it on the **Settings > General > Account** page. See the TRITON - Web Security Help for more information.

     If you have a Web Security Gateway solution, the key you enter is automatically applied to Content Gateway, as well.
   - TRITON - Data Security displays the subscription key page. See the *Initial Setup* section of the TRITON - Data Security Help for more information.
   - TRITON - Email Security prompts for a subscription key. If you do not enter the subscription key in the prompt, you can enter it in the **Settings > General > Subscription** page. See the TRITON - Email Security Help for more information.
6. If you did not provide SMTP server details during installation, use the **TRITON Settings > Notifications** page to specify the SMTP server used to enable administrator password reset functionality and account change notifications. See the TRITON Unified Security Help for more information.
7. If you installed SQL Server 2008 R2 Express, verify that SQL Server Browser service is running and that TCP/IP is enabled.

   a. Launch SQL Server Configuration Manager (**Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **Configuration Tools** > **SQL Server Configuration Manager**).

   b. In the tree pane, select **SQL Server Service**.

   c. 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.

   d. 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).

   e. In the properties pane, make sure TCP/IP is enabled.

      If not, right-click TCP/IP and enable it.

Continue with the initial configuration steps for the Websense security solutions you have installed:

- *Web Security initial configuration*, page 677
- *Data Security initial configuration*, page 682
- *Email Security Gateway initial configuration*, page 683
- *Content Gateway initial configuration*, page 684

Web Security initial configuration

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic:
- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x	- *Getting started with Web Security solutions*, page 677 - *Additional tips for working with Web Security solutions*, page 678 - *Identifying Filtering Service by IP address*, page 679

Getting started with Web Security solutions

After entering your Web Security subscription key (see *Initial Configuration for All Websense Modules*, page 675), perform the following initial steps in TRITON - Web Security (the management console).

For more complete instructions for any step, click **Help** in the TRITON toolbar, then select **Explain This Page**. Alternatively, use the **New User Quick Start** tutorial to run through the initial steps needed to start applying Web Security policies to user requests.

1. If Websense Filtering Service must go through a proxy server or firewall to connect to the Internet, navigate to the **Settings** > **General** > **Database Download** page and provide connection details.

   Filtering Service must be able to connect to the download server to:

   - Verify your subscription.
   - Download the Master Database used to enable Web filtering.

2. On the Main tab, go to the **Policy Management** > **Policies** page and edit the **Default** policy.

   This policy acts as a safety net. It applies to any requests not governed by another policy. Until you define clients and create custom policies, this is the policy that applies to all Internet requests that pass through your Web Security solution.

3. On the Settings tab, go to the **Settings** > **General** > **Directory Services** page and configure the directory service (if any) used in your network. This configuration must be performed before you can apply specific policies to users, groups, and OUs in your network.

4. On the Main tab, go to the **Policy Management** > **Clients** page and define the clients (IP addresses, IP address ranges, users, groups, and OUs) to which you want to apply policies.

5. If you have Web Security Gateway or Gateway Anywhere, also see *Content Gateway initial configuration*, page 684.

6. If you have Web Security Gateway Anywhere, also see *Additional configuration for Web Security Gateway Anywhere*, page 679.

Next, you can:

- Create custom policies and filters on the **Policy Management > Policies** and **Filters** pages. (More information about what filters are, and how they work with policies, is available from the New User Quick Start tutorial or the TRITON - Web Security Help. Both are available from the Help menu in the TRITON console.
- Configure transparent user identification on the **Settings > General > User Identification** page (see the "User Identification" topic in the TRITON - Web Security Help).
  - If you installed Logon Agent, you must create and deploy a client logon script in addition to configuring Logon Agent in TRITON - Web Security. See the Using Logon Agent for Transparent User Identification technical paper for instructions.
  - If you were unable to grant User Service, DC Agent, or Logon Agent administrator privileges during installation, see the "Troubleshooting" > "User Identification" topic on changing User Service, DC Agent, and Logon Agent service permissions in TRITON - Web Security Help.
- Enable email or SNMP alerting on the **Settings > Alerts > Enable Alerts** page (see the "Alerting" topic in the TRITON - Web Security Help).
- Customize reporting behavior (see the "Reporting Administration" topic in the TRITON - Web Security Help).
- Configure optional Remote Filtering components to enable filtering of off-site users. For instructions, see the Remote Filtering Software technical paper.

Additional tips for working with Web Security solutions

- All Websense tools and utilities installed on Windows Server 2008 (such as wsbackup.exe and websenseping.exe), as well as 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. Navigate to the Websense **bin** directory (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.
  3. In the **Compatibility** tab, under **Privilege Level**, select **Run this program as an administrator**. Then, click **OK**.
- 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 *Network Agent and stealth mode NICs*, page 685.

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 hostname 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 Websense Filtering Service. See *Starting and stopping Web Security services*, page 709.

Additional configuration for Web Security Gateway Anywhere

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic:
• Web Security Gateway Anywhere, v7.7.x	• *Confirm Content Gateway registration with Data Security* • *Configuring the Content Gateway policy engine* • *Verifying Web and data security linking*

In addition to the items under *Web Security initial configuration*, page 677, perform these procedures if your subscription includes Web Security Gateway Anywhere.

Confirm Content Gateway registration with Data Security

Content Gateway registers with Data Security automatically. To ensure that registration is successful:

- Synchronize the date and time on the Content Gateway and Data Security Management Server machines to within a few minutes.
- 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.
- 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.

If registration fails an alarm displays in Content Gateway Manager.

1. Verify connectivity between Content Gateway and the Data Security Management Server.
2. In Content Gateway Manager, on the **Configure** > **My Proxy** > **Basic** > **General** page, in the **Networking** section confirm that **Data Security** > **Integrated on-box** is enabled.
3. Restart Content Gateway to initiate another registration attempt.

   Alternatively:

   a. Go to **Configure** > **Security** > **Data Security** and enter the IP address of the **Data Security Management Server**.
   b. Enter a user name and password for a Data Security administrator with Deploy Settings privileges.
   c. Click **Register**.

After Content Gateway has registered with Data Security, in Content Gateway Manager go to **Configure** > **Security** > **Data Security** and set the following options:

1. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Data Security for analysis and policy enforcement.
2. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement. SSL Manager must be enabled on Content Gateway.

   These options can be accessed whenever Data Security is registered by going to the **Configure** > **Security** > **Data Security** > **General** page.
3. Click **Apply** and restart Content Gateway.

Data Security and the proxy communicate over ports 17000-17014.

Configuring the Content Gateway policy engine

When Content Gateway is registered 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 onto TRITON - Data Security.
2. 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.

Data Security initial configuration

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:

- Data Security, v7.7.x

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.

To complete your Data Security installation, log onto TRITON - Data Security and click **Deploy**.

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 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

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:	In this topic:
• Email Security Gateway and Email Security Gateway Anywhere v7.7.x	• *Email Security Gateway initial configuration*, page 683 • *Email Security Gateway Anywhere initial configuration*, page 684

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 some essential configuration settings. It is strongly recommended you use this wizard. See the TRITON - Email Security Help for more information about the wizard.

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 simply offers a more convenient way to enter some initial settings.

See the Getting Started section in TRITON - Email Security Help for information on initial configuration in the following areas:

- First-time Configuration Wizard, for establishing
  - An initial mail route for a protected domain
  - Trusted IP addresses for which some inbound email analysis is not performed
  - Email Security Log Server IP address and port
  - System notification email address
- Websense Data Security registration, to allow the use of email data loss prevention (DLP) policy options
- Master database download scheduling, to manage spam and virus filter updates

For help with the following Email Security settings, see the Configuring System Settings section in TRITON - Email Security Help:

- Administrator management, to modify administrator roles established in the TRITON Unified Security Center

- System settings, to establish system preferences like the SMTP greeting and console language settings
- Appliance management, for administering all the appliances in your network
- User directory creation and management
- Protected domain and trusted IP address lists, to designate all the domains that you want Email Security Gateway to protect and the IP addresses whose mail can bypass some email analysis
- User authentication and recipient validation options
- Transport Layer Security (TLS) certificate handling, to provide an extra layer of security for email communications
- Email Security manager backup and restore functions, to preserve important configuration files, including your appliances list, administrator settings, and report templates
- System alerts, to configure delivery methods for distributing various Email Security system health alerts

Email Security Gateway Anywhere initial configuration

If your subscription includes Email Security Gateway Anywhere, you need to register with the email hybrid service. See the Registering for the hybrid service topic in TRITON - Email Security Help for descriptions of email hybrid service registration.

After you have registered with the hybrid service, you can configure Hybrid Service Log properties and view the Hybrid Service Log. See TRITON - Email Security Help for details.

Content Gateway initial configuration

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.7.x

After Content Gateway is installed, perform these basic configuration activities:

✓ **Note**

The subscription key is **automatically applied** to Content Gateway when you enter it in TRITON - Web Security.

- Log onto Content Gateway Manager and run a basic test (Getting Started)
- If there are multiple instances of Content Gateway, consider configuring a managed cluster.

- Configure protocols to proxy in addition to HTTP: HTTP (SSL Manager), FTP
- Complete your explicit or transparent proxy deployment
  - *Content Gateway explicit and transparent proxy deployments*
  - In Content Gateway Manager Help: Explicit proxy, Transparent proxy
- If proxy user authentication will be used, configure user authentication. Alternatively, configure *TRITON - Web Security user identification*.
- Configure the real-time Scanning Options in TRITON – Web Security.
- If you enabled content caching during installation, configure content caching.

After the base configuration has been tested, consider these additional activities:

- When HTTPS (SSL Manager) is used, in TRITON – Web Security configure categories, clients, and destination servers for SSL decryption bypass
- Create Content Gateway filtering rules to:
  - Deny or allow URL requests
  - Insert custom headers
  - Allow specified applications, or requests to specified Web sites to bypass authentication
  - Keep or strip header information from client requests
  - Prevent specified applications from transiting the proxy
- In explicit proxy deployments, customize the PAC file
- In transparent proxy deployments, use ARM dynamic and static bypass, or use router ACL lists to bypass Content Gateway (see your router documentation)

Network Agent and stealth mode NICs

Deployment and Installation Center | Web Security Solutions | v7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere v7.7.x

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>**.

34 Adding, Modifying, or Removing Components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

The following articles contain instructions for adding, modifying, or removing Websense Web, Data, and Email Security components:

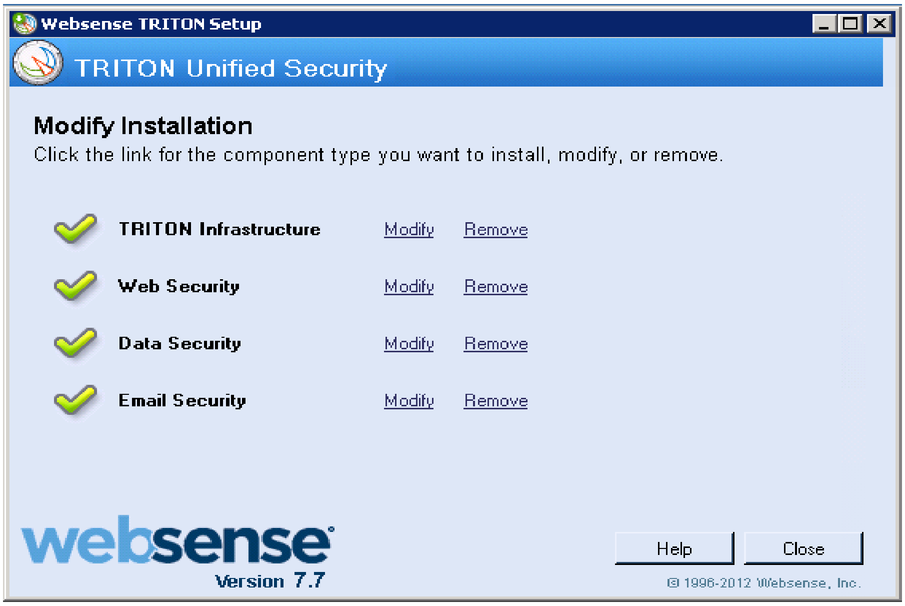
Adding or modifying Windows components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

On Windows machines, Websense components are added or modified using the TRITON Unified Installer. When run on a machine that has current-version components installed, the installer displays the **Modify Installation** dashboard.



Websense TRITON Setup

TRITON Unified Security

Modify Installation

Click the link for the component type you want to install, modify, or remove.

✓	TRITON Infrastructure	Modify	Remove
✓	Web Security	Modify	Remove
✓	Data Security	Modify	Remove
✓	Email Security	Modify	Remove

For each module found on the machine (TRITON Infrastructure, Web Security, Data Security, and Email Security), the Modify Installation dashboard shows **Modify** and **Remove** links. (When no components of a particular type are found, an **Install** link, used to launch a custom installation, is displayed instead.)

Click a **Modify** link to launch the program used to add or modify components of the selected type. See:

- *Modifying TRITON Infrastructure*, page 689
- *Adding Web Security components*, page 690
- *Adding or modifying Data Security components*, page 690
- *Adding Email Security components*, page 693

Modifying TRITON Infrastructure

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

1. Start the Websense installer.
   - If you chose to keep installation files after the initial installation, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, 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 386.
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 administrator accounts*, page 759, 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.
7. If you installed the TRITON management components on a virtual machine, restart the server.

Adding Web Security components

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

> **Important**
> Do not add other Web Security components to a Remote Filtering Server machine.

1. Start the Websense installer:
   - If you chose to keep installation files after the initial installation, go to **Start > All Programs > Websense > Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, 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 392, for instructions.
5. When you are done adding Web Security components, you are returned to the **Modify Installation** dashboard.

Adding or modifying Data Security components

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

1. Start the Websense installer:

- If you chose to keep installation files after the initial installation, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to start the installer without having to re-extract files.
- Otherwise, 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 691
   - *Repairing Data Security components*, page 692
   - *Changing the Data Security privileged account*, page 692
   - *Changing the domain of a Data Security Server*, page 693

Recreating Data Security certificates

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 the last time you ran the installer, 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 Data Security components*, page 787, 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 424, for information on creating and installing an endpoint package.

Repairing Data Security components

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files the last time you ran the installer, 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files the last time you ran the installer, 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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

1. Use TRITON - Data Security to 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 hostname of the Data Security Management Server*, page 784.
6. Re-register all Websense Data Security policy engine servers, agents and protectors (See *Re-registering Data Security components*, page 787).
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

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

Two Email Security Gateway components may be added on a Windows machine: TRITON - Email Security and Email Security Log Server. All other Email Security Gateway components run on a Websense V-Series appliance.

1. Start the Websense installer:
   - If you chose to keep installation files after the initial installation, go to **Start > All Programs > Websense > Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, 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.
   - You may specify whether the connection to the database should be encrypted.

     Please note the following issues associated with using this encryption feature:
     - You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.
     - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
     - The connection from the Email Security module on the TRITON Console to the V-Series appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.

- **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 411.

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. 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.
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**.

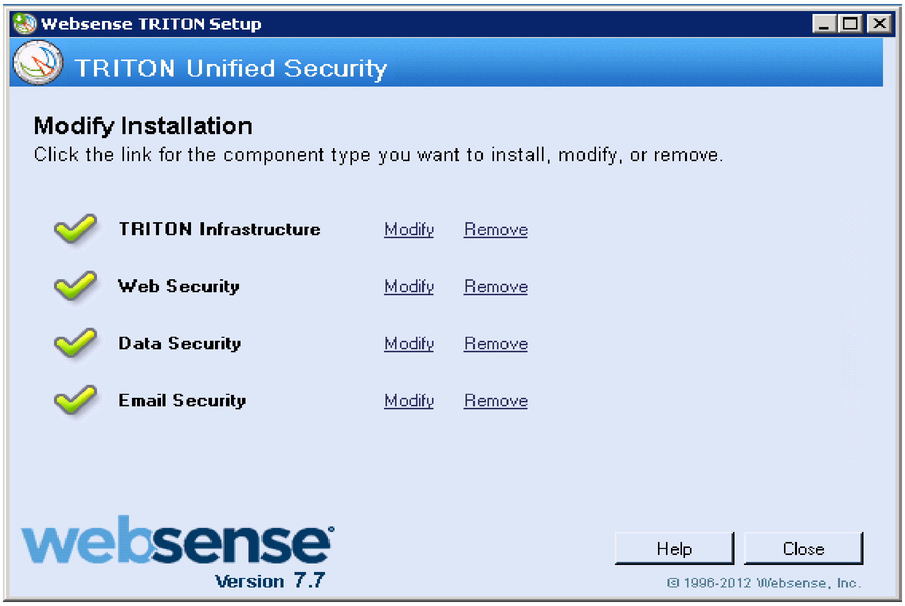
Removing components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- ◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- ◆ Data Security, v7.7.x
- ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

On Windows machines, Websense components are removed using the TRITON Unified Installer. When run on a machine that has current-version components installed, the installer displays the **Modify Installation** dashboard.



Modify Installation

Click the link for the component type you want to install, modify, or remove.

- TRITON Infrastructure Modify Remove
- Web Security Modify Remove
- Data Security Modify Remove
- Email Security Modify Remove

For each module found (TRITON Infrastructure, Web Security, Data Security, and Email Security), the Modify Installation dashboard shows **Modify** and **Remove** links. (When no components of a particular type are found, an **Install** link, used to launch a custom installation, is displayed instead.)

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 696
- *Removing Web Security components*, page 698
- *Removing Data Security components*, page 706
- *Removing Email Security components*, page 706

Removing TRITON Infrastructure

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

Remote TRITON Infrastructure only after removing all TRITON Unified Security Center modules (TRITON - Web Security, Data Security, and Email Security) from the machine. Although it is possible to remove TRITON Infrastructure before removing TRITON Unified Security Center modules, the modules are rendered inoperable.

For instructions on removing TRITON Unified Security Center modules, see:

- TRITON - Web Security: *Removing Web Security components*, page 698
- TRITON - Data Security: *Removing Data Security components*, page 706
- TRITON - Email Security: *Removing Email Security components*, page 706

To remove TRITON Infrastructure:

1. Start the Websense installer:
   - If you chose to keep installation files after the initial installation, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *To remove Web Security components (Windows)*, page 698 ◆ *To remove Web Security components (Linux)*, page 701

Both Policy Broker and the Policy Server instance associated with each set of components you want to remove must be running when you start the removal process.

- Policy Broker may be running on a different machine from the applicable Policy Server instance.
- Policy Broker and Policy Server may be on different machines from the component being removed.
- If you have Websense appliances, Policy Broker and Policy Server run on the **full policy source** appliance.

  Policy Server also runs on **user directory and filtering** appliances.

Web Security components should be removed in a particular order because of certain dependencies (see *Removal order of Web Security components*, page 703). 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 704). Also, if your Web Security deployment is integrated with another product, see the following for any integration-specific requirements:

- *Integrating Web Security with Check Point*, page 445
- *Integrating Web Security with Cisco*, page 481
- *Integrating Web Security with Citrix*, page 513
- *Integrating Web Security with Microsoft Products*, page 535
- *Installing Web Security for Universal Integrations*, page 563

Removal instructions are slightly different depending on the operating system:

- *To remove Web Security components (Windows)*, page 698
- *To remove Web Security components (Linux)*, page 701

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 after the initial installation, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, 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:
    - *Integrating Web Security with Check Point*, page 445
    - *Integrating Web Security with Cisco*, page 481
    - *Integrating Web Security with Citrix*, page 513
    - *Integrating Web Security with Microsoft Products*, page 535
    - *Installing Web Security for Universal Integrations*, page 563.

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.

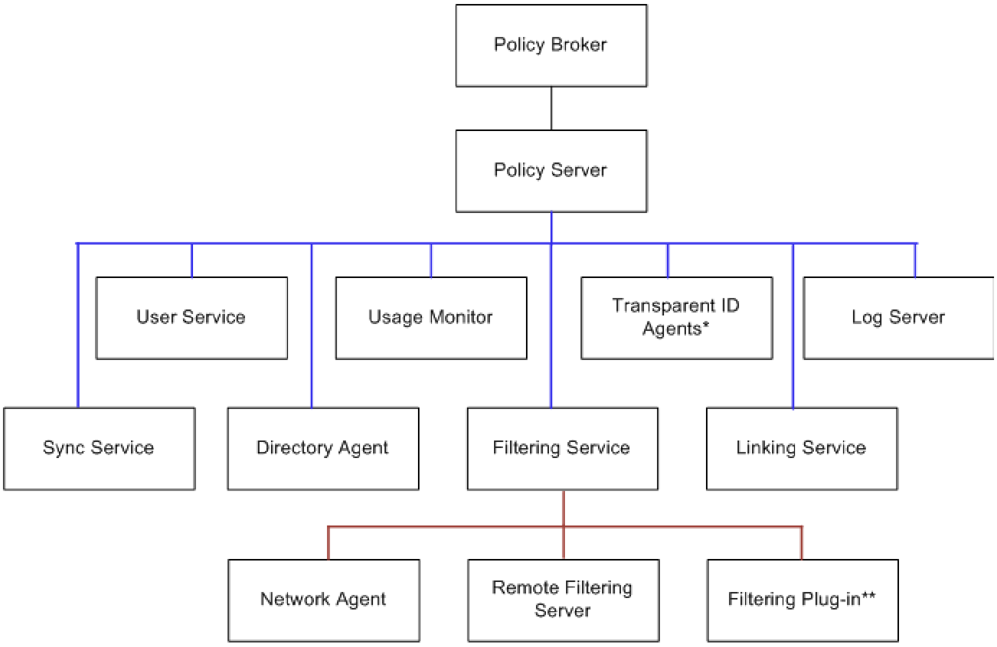
8. If you stopped your antivirus software, restart it.

9. If you remove an integration plug-in, you may need to restart the integration product. See:

   - *Integrating Web Security with Check Point*, page 445
   - *Integrating Web Security with Cisco*, page 481
   - *Integrating Web Security with Citrix*, page 513
   - *Integrating Web Security with Microsoft Products*, page 535
   - *Installing Web Security for Universal Integrations*, page 563

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).

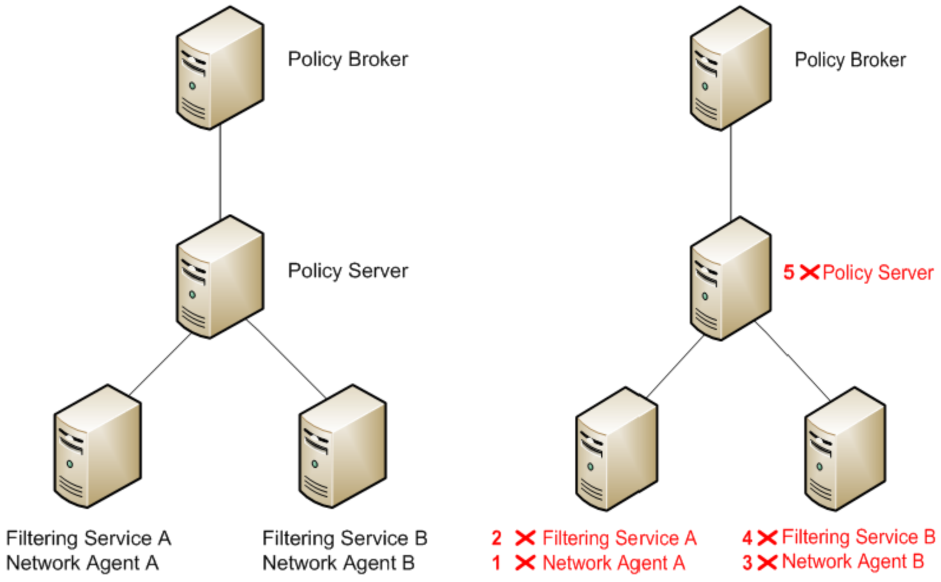


* DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
** Microsoft ISAPI Filter or Citrix Integration Service

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

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 subdirectory, unless either of the following is true:

- They are in the **backup** subdirectory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\backup in Windows; /opt/Websense/backup/ in Linux).
- They are Log Database files.

Removing Content Gateway

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Gateway Anywhere, v7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 *Uninstalling endpoint software*, page 440.

To remove Data Security components:

1. Start the Websense installer:
   - If you chose to keep installation files after the initial installation, go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, double-click the installer executable.
2. In **Modify Installation** dashboard, click the **Modify** link for Data Security.
3. At the **Welcome** screen, click **Remove**.
4. 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.
5. At the **Uninstallation Complete** screen, click **Finish**.
6. You are returned to the **Modify Installation** dashboard.

Removing Email Security components

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

◆ Email Security Gateway and Gateway Anywhere, v7.7.x

1. If you have not done so already, start the Websense installer:
   - If you chose to keep installation files after the initial installation, go to **Start > All Programs > Websense > Websense TRITON Setup** to start the installer without having to re-extract files.
   - Otherwise, 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 **Remove Components** screen, choose whether you want to uninstall all or specific Email Security Gateway components and then click **Next**.
5. The **Summary** screen verifies your uninstall selections. If the summary is not correct, click **Back** and change your selections. If the summary is correct, click **Uninstall**.
6. The **Uninstall TRITON - 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 esglogdb7*x* and esglogdb7*x_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**.
8. You are prompted to restart the machine. A restart is required to complete the Email Security uninstall process.

35 Quick Reference

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Use this Deployment and Installation Center Quick Reference to find information about:

- *Starting and stopping Web Security services*, page 709
- *Websense TRITON Enterprise default ports*, page 712
- *Excluding Websense files from antivirus scans*, page 724
- *Creating Apache SSL certificates*, page 726

Starting and stopping Web Security services

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Manually stopping and starting Web Security services (Windows)*, page 710 ◆ *Manually stopping and starting Web Security services (Linux)*, page 710 ◆ *Stopping and starting principal Web Security components*, page 711

By default, Web Security services are configured to start when the machine starts.

Occasionally, you may need to stop or start an individual 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 Web Security services (Windows)

To stop or start individual services, use the Windows Services dialog box:

1. Go to **Start** > **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.

When stopping and starting individual services, refer to *Stopping and starting principal Web Security components*, page 711, 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.

To stop or start all Web Security services on a machine:

1. Open a Windows Command Prompt and navigate to the Web Security directory (**C:\Program Files (x86)\Websense\Web Security**, by default).
2. Enter one of the following commands:

```
WebsenseAdmin stop
WebsenseAdmin start
```

When you use the **WebsenseAdmin** tool, services are automatically stopped and started in the correct order.

Manually stopping and starting Web Security services (Linux)

Stop, start, or restart services (daemons) from the Linux command line.

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 Web Security components*, page 711, for the preferred stopping and starting order.

There are two scripts to stop and start Websense services:

- Use **WebsenseAdmin** to stop, start, or restart all Web Security components on the machine.
  1. Go to the Websense installation directory (/opt/Websense/, by default).
  2. Use the following commands to stop, start, or restart all Web Security services in the correct order:

     ```
     ./WebsenseAdmin stop
     ./WebsenseAdmin start
     ./WebsenseAdmin restart
     ```

  3. View the running status of all Web Security services with the following command:

     ```
     ./WebsenseAdmin status
     ```

- Use **WebsenseDaemonControl** to stop or start individual components.
  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** exit the tool

> **Warning**
> Do **not** use the **kill** command to stop Websense services. This may corrupt the services.

Stopping and starting principal Web Security components

When stopping individual components, 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

Websense TRITON Enterprise default ports

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Websense Data Security, v7.7.x
- Websense Email Security and Email Security Gateway, v7.7.x

The articles in this collection describe the default port numbers used by Websense product 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:

- Web Security
- *Data Security ports*, page 713
- *Email Security Gateway ports*, page 723

Data Security ports

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

Applies to:

- Data Security, v7.7.x

In this topic

The most robust and effective implementation of Data Security depends on certain ports being open to support the mechanics of the software. The ports for Data Security components are 17500-17515 by default. These ports must be left open for all Data Security software and 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.

The tables in the rest of this section list the inbound and outbound ports required for each Data Security component. (Note that TRITON - Data Security refers to the user interface service. Data Security Management Server refers to the management service, MGMDT.)

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	User interface browsing
TRITON - Data Security	9443	User interface 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 connection. The default is secured (HTTPS, port 443). ** Optional		
Inbound		
None		

Data Endpoint server

Outbound

To	Port	Purpose
Data Security Management Server	443	Retrieve fingerprints and natural language processing scripts
Data Security Management Server	17443	Incidents
Inbound		
From	**Port**	**Purpose**
Data Security Management Server	443	Retrieve fingerprints and natural language processing scripts
Endpoint Client	80	Incidents
Supplemental Data Security Server	17444	Retrieve fingerprints and natural language processing scripts

Printer agent

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communications
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Management Server	17443	Incidents
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
* This range is necessary for load balancing.		
Inbound		
None		

ISA/TMG agent

Outbound

To	Port	Purpose
Data Security Management Server	443	Secure communications

Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Internet gateway	80	For HTTP connections

* This range is necessary for load balancing.

Inbound

None

SMTP agent

Outbound

To	Port	Purpose
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Next hop MTA	25**	SMTP for inbound/outbound traffic

* This range is necessary for load balancing.
** This is default. Other port can be configured.

Inbound

From	Port	Purpose
Previous MTA	25*	SMTP for inbound/outbound traffic

* This is default. Other port can be configured.

TRITON - Web Security

Outbound		
To	**Port**	**Purpose**
Data Security Management Server	56992	Linking Service
Inbound		
From	**Port**	**Purpose**
TRITON - Data Security, Data Security Server, Protector, Web Content Gateway	56992	Linking Service

Crawler agent (discovery and fingerprinting)

Outbound		
To	**Port**	**Purpose**
Data Security Management Server	443	Secure communication
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Salesforce server	80 or 8080	Salesforce discovery
* This range is necessary for load balancing.		
Inbound		
From	**Port**	**Purpose**
Data Security Management Server	9797*	Crawler listening
* This is only for the standalone crawler agent.		

Exchange server

Outbound		
None		
Inbound		
From	**Port**	**Purpose**

Data Security Server, Crawler Agent (Discovery and Fingerprinting)	80	Exchange discovery
Data Security Server, Crawler Agent (Discovery and Fingerprinting)	443	Exchange discovery

File server

Outbound		
None		
Inbound		
From	**Port**	**Purpose**
Crawler Agent (Discovery and Fingerprinting)	139	File sharing access
Crawler Agent (Discovery and Fingerprinting)	445	File sharing access

SharePoint server

Outbound		
None		
Inbound		
From	**Port**	**Purpose**
Crawler Agent (Discovery and Fingerprinting)	80	File sharing access
Crawler Agent (Discovery and Fingerprinting)	443	File sharing access

Database server

Outbound		
To	**Port**	**Purpose**
Crawler Agent (Discovery and Fingerprinting)	Varies	The port that allows connection to the database (according to database type)
Inbound		
From	**Port**	**Purpose**
Crawler Agent (Discovery and Fingerprinting)	Varies	The port that allows connection to the database (according to database type)

TRITON - Data Security

Outbound		
Data Security Server, Protector, Web Content Gateway, Email Security Gateway	17500-17515** and 17700-17715***	Consecutive ports that allow communication with Websense agents and machines.
Inbound		
From	**Port**	**Purpose**
Data Security Server, Protector, Web Content Gateway	17443*	Incidents
Data Security Server, Protector, Web Content Gateway	139	File sharing
Data Security Server, Protector, Web Content Gateway	443	Secure communication
Data Security Server, Protector, Web Content Gateway	445	File sharing
Data Security Server, Protector, Web Content Gateway	8453	User repository
Data Security Server, Protector, Web Content Gateway	8005	Tomcat server
Data Security Server, Protector, Web Content Gateway, Email Security Gateway	17500-17515** and 17700-17715***	Consecutive ports that allow communication with Websense agents and machines.
Data Security Server, Protector, Web Content Gateway	9443*	Access user interface
Data Security Server, Protector, Web Content Gateway	19448*	HTTP access to user interface

* This port should be left open. It is not configurable.
** This range is necessary for load balancing.
***Used when Web Content Gateway and Email Security Gateway are both installed.

Supplemental Data Security server

Outbound

To	Port	Purpose
Data Security Management Server	17443	Incidents
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Inbound

From	Port	Purpose
Data Security Management Server	8892	Syslog
Data Security Management Server	139	File sharing
Data Security Management Server	445	File sharing
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Web Content Gateway

Outbound

To	Port	Purpose
Data Security Management Server	80	Fingerprint sync
Data Security Management Server	9443	Syslog
Websense Web Security	56992	Linking Service
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

* This range is necessary for load balancing.

Inbound

None

Email Security Gateway

The following ports are used on the appliance for outbound connections to TRITON - Data Security.

Outbound

To	Port	Purpose
Data Security Management Server	17500-17515* and 17700-17715**	Settings deployment, fingerprint repository

Data Security Management Server	17443	Syslog, forensics, incidents
Data Security Management Server	17444	Used to pull configuration settings
Data Security Management Server	80	Fingerprint repository sync
Data Security Server	17500-17515* and 17700-17715**	MGMTD

* This range is necessary for load balancing.
**Used when Web Content Gateway and Email Security Gateway are both installed.

Protector

Outbound

To	Port	Purpose
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Next hop MTA	25**	SMTP
Websense Web Security	56992	Linking Service
Other	UDP 123	Inbound/ outbound NTPD (available on the appliance yet disabled by default)

* This range is necessary for load balancing.
** Explicit MTA

Inbound

From	Port	Purpose
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Anywhere (including TRITON - Data Security)	22	SSH access
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Explicit MTA	25**	SMTP

Explicit MTA	10025* *	SMTP, mail analysis
* This range is necessary for load balancing. ** Explicit MTA		

ICAP client

Outbound

To	Port	Purpose
Protector	1344	Receiving ICAP traffic
Inbound		
None		

Mobile agent

Outbound

To	Port	Purpose
Data Security Management Server	17443	Syslog, forensics, incidents, mobile status
Data Security Management Server	80	Fingerprint sync
Data Security Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.
Microsoft Exchange Server	80/443	ActiveSync (user defined using TRITON - Data Security)
Websense Web Security	56992	Linking Service
Other	UDP 123	Inbound/ outbound NTPD (available on the appliance yet disabled by default)
* This range is necessary for load balancing.		

Inbound

From	Port	Purpose
Data Security Management Server	5820	Settings deployment
Mobile Devices	80/443	ActiveSync (user defined using TRITON - Data Security)
Data Security Management Server	8892	Management
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

Anywhere (including the Mobile agent)	22	SSH access
Data Security Server	5443	Release quarantined messages

* This range is necessary for load balancing.

Email Security Gateway ports

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

The following are ports used on the Email Security Gateway appliance.

Interface	Port	Direction	Description
C/E1/E2	9449	Inbound	Personal Email Manager load balancing
C/E1/E2 (C recommended)	6671	Inbound	SSL proxy to be accessed by TRITON - Email Security
C/E1/E2	6643	Inbound	Personal Email Manager user interface
E1/E2	17700*	Inbound	Email data loss prevention system health and log data
E1/E2	25	Inbound	SMTP
E1/E2	2525	Inbound	Receipt of messages from Data Security for encryption

*The port range 17700-17714 must be open for communications with Email Security Gateway.

The following ports are used on the appliance for outbound connections to TRITON - Data Security.

Interface	Port	Direction	Description
C/E1/E2	17500-17515*	Outbound	Fingerprint status
C/E1/E2	17500-17515*	Outbound	Fingerprint repository
C/E1/E2	17443	Outbound	Registration, syslog, forensics, incidents
C/E1/E2	17444	Outbound	Fingerprint download
C/E1/E2	17500-17515*	Outbound	Message analysis
C/E1/E2	80	Outbound	Fingerprint repository synchronization

*This is the default range. The starting location of the range (17500) is configurable.

The following are ports used by Email Security Gateway components off-appliance.

Interface	Port	Direction	Description
C/E1/E2	9443	Inbound	TRITON - Email Security (via TRITON Unified Security Center)
E1/E2	50800	Outbound	Email Security Log Server
E1/E2	1433 1434	Outbound	Email security log database default instance
E1/E2	443	Outbound	Hybrid service
E1/E2	15868	Outbound	Websense Web Filter
E1/E2	389 636	Outbound	LDAP server
E1/E2	80	Outbound	Database download server
E1/E2	53	Outbound	DNS server
C	162	Outbound	SNMP Trap server

Excluding Websense files from antivirus scans

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Email Security Gatewhere Anywhere, v7.7.x	◆ *Web security*, page 725 ◆ *Data security*, page 725 ◆ *Email security*, page 726

Antivirus scanning can degrade the performance of Websense components. This article lists folders and files that should be excluded from antivirus scans.

Please note:

- Websense is not aware of a risk in excluding the files or folders that are mentioned in this section from your antivirus scans. However, it is possible that your system would be safer if you did not exclude them.
- When you scan these files, performance and operating system reliability problems may occur because of file locking.
- Do not exclude any files based on the filename extension. For example, do not exclude all files that have a .dit extension.

- All the files and folders that are described in this section are protected by default permissions to allow only SYSTEM and administrator access, and they contain only operating system components. Excluding an entire folder maybe simpler but may not provide as much protection as excluding specific files based on file names.

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.

Web security

It is a best practice to exclude the Websense installation directory from antivirus scans. By default this directory is:

- **Windows**:

  ```
  *:\Program Files\Websense
  ```

  or

  ```
  *:\Program Files (x86)\Websense
  ```

- **Linux**:

  ```
  /opt/Websense/
  ```

Data security

It is a best practice to exclude the following from antivirus scans.

- The Websense installation folder, which is one of the following:
  - *:\Program Files\Websense
  - *:\Program Files (x86)\Websense
- *:\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. By default, this is one of the following:
  - Program Files\Websense\
  - Program Files (x86)\Websense\*.*

- *:\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**
>
> This document lists the default installation folders. You can configure the software to install to other locations.
>
> The FP-Repository folder is usually located inside the installation folder.

The following directories should be excluded from the antivirus software that is deployed to endpoint clients:

- The endpoint installation folder
- Endpoint processes: wepsvc.exe and dserui.exe
- EndpointClassifier.exe and kvoop.exe

Email security

It is a best practice to exclude the Websense installation folder, by default:

```
*:\Program Files\Websense
```

or

```
*:\Program Files (x86)\Websense
```

Also exclude any Data Security folders that apply (see *Data security* above).

Creating Apache SSL certificates

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x	◆ *Using a batch file for Apache SSL certificate file operations*

Perform the following steps on the TRITON management server to create (or re-create) Apache SSL certificates for TRITON - Web Security.

Note that these are basic instructions for creating certificates. Changing the password on certificates is not included in these steps. Avoid changing passwords if possible.

1. Use the Windows Services dialog box (**Start** > **Administrative Tools** > **Services**) to stop the following services:
   - Websense TRITON - Web Security
   - Websense Web Reporting Tools
2. Review the **Websense\Web Security\apache\conf\ssl\openssl.txt** file to verify that it contains correct information.

   If you have changed the IP address of this machine, for example, 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. Go to the **Websense\Web Security\apache\conf\ssl\automation\** directory and run the following scripts in the order shown:
   a. s1_newreq.bat
   b. s2_server_key.bat
   c. s3_server_crt.bat
   d. s4_server_p12.bat
4. Copy the **Websense\Web Security\apache\conf\ssl\output\server.key** file to:

   ```
   Websense\Web Security\apache\conf\ssl\ssl.key\server.key
   ```
5. Copy the **Websense\Web Security\apache\conf\ssl\output\server.crt** file to:

   ```
   Websense\Web Security\apache\conf\ssl\ssl.crt\server.crt
   ```
6. Copy the **Websense\Web Security\apache\conf\ssl\output\cakey.pem** file to:

   ```
   Websense\Web Security\apache\conf\ssl\private\cakey.pem
   ```
7. Copy the **\Web Security\apache\conf\ssl\output\manager.p12** file to:

   ```
   Websense\Web Security\tomcat\conf\keystore\tomcat\manager
   .p12
   ```
8. Use the Windows Services dialog box to 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_path>\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"
```

Configuring Websense Apache services to use a trusted connection

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

If, during Websense Web Security installation, you chose to use a trusted connection to access the Log Database, you must configure the **Websense TRITON - Web Security** and **Websense Web Reporting Tools** services to log on using the trusted account specified during installation. These services are located on the TRITON management server.

To configure the service to use the trusted account:

1. Go to the TRITON management server machine and open the Windows Services dialog box (**Start** > **Administrative Tools** > **Services**).

2. In the list of services, right-click **Websense TRITON - Web Security** and select **Properties**.
3. In Properties dialog box, select the **Log On** tab.
4. Under **Log on as**, select **This account** and enter the domain\username and password of the trusted account.
5. Click **OK**.
6. Repeat this process (from Step 2) for the **Websense Web Reporting Tools** service.

36 Component Reference

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway (Anywhere), v7.7.x	◆ *TRITON Unified Security Center components*, page 729 ◆ *Web Security components*, page 729 ◆ *Data Security components*, page 730 ◆ *Email Security Gateway components*, page 730

TRITON Unified Security Center components

- *TRITON management server*, page 731
- *TRITON Unified Security Center*, page 731
- *TRITON Infrastructure*, page 732

Web Security components

- *Policy Broker*, page 733
- *Policy Server*, page 734
- *Filtering Service*, page 735
- *Network Agent*, page 736
- *Usage Monitor*, page 738
- *TRITON - Web Security*, page 738
- *Web Security Log Server*, page 739
- *User Service*, page 740
- *DC Agent*, page 741

Data Security components

Email Security Gateway components

TRITON management server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x
- Data Security, v7.7.x
- Email Security Gateway (Anywhere), v7.7.x

The machine that hosts core management components for all Websense security solutions is referred to as the *TRITON management server.* This machine hosts the TRITON Unified Security Center (TRITON console), which includes:

- The infrastructure uniting all management components (see *TRITON Infrastructure*, page 732), including a settings database that holds administrator account information and other data shared by all management components
- One or more management modules, used to access configuration, policy management, and reporting tools for a Websense security solution. Available modules include:
  - *TRITON - Web Security*
  - *TRITON - Data Security*
  - *TRITON - Email Security*

Although additional components may also reside on the TRITON management server, avoid placing Web Security *Filtering Service* or *Network Agent* on the management server machine.

Optionally, in smaller deployments, SQL Server 2008 R2 Express may be installed on the TRITON management server to host the reporting databases.

TRITON Unified Security Center

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x
- Data Security, v7.7.x
- Email Security Gateway (Anywhere), v7.7.x

The TRITON Unified Security Center (TRITON console) is the Web browser-based, graphical management application for your entire deployment. It includes *TRITON Infrastructure* and up to 3 security management modules:

- *TRITON - Web Security*
- *TRITON - Data Security*
- *TRITON - Email Security*

Depending on your subscription, one or more of these modules is enabled.

The TRITON console may also be configured to connect to external management consoles, including Appliance Manager, Content Gateway Manager, and the cloud-based TRITON - Mobile Security console.

The TRITON Unified Security Center is typically placed on a dedicated machine, the *TRITON management server*.

TRITON Infrastructure

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x
- Data Security, v7.7.x
- Email Security Gateway (Anywhere), v7.7.x

TRITON Infrastructure is composed of common user interface, logging, and reporting components required by the TRITON management modules (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 is 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.

TRITON Infrastructure is always installed on a *TRITON management server*.

SQL Server 2008 R2 Express

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x
- Data Security, v7.7.x
- Email Security Gateway (Anywhere), v7.7.x

SQL Server 2008 R2 Express is a free, limited-performance version of SQL Server 2008 R2. In smaller deployments, it can be used to store Websense reporting data.

- Due to performance limitations built in by Microsoft, SQL Server 2008 R2 Express is not suitable for all organizations; see Administering Websense Databases for more information.
- For other supported versions SQL Server, see *System requirements for this version*, page 2.

SQL Server 2008 R2 Express can be installed on the *TRITON management server* or on a separate machine.

Only use the Websense Windows installer to install SQL Server 2008 R2 Express for use with Websense solutions. Do not use an installer obtained elsewhere.

Policy Broker

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Policy Broker manages policy and configuration information required by other Websense Web Security components. The information is stored in the Policy Database, which is installed automatically with Policy Broker.

In a Websense appliance-based deployment, Policy Broker resides on the full policy source appliance.

During a custom installation, if Policy Broker is not found on the current machine, it appears as a component you can install. Before selecting it, however, make sure that it is not already installed on another server or appliance. Do **not** install more than one Policy Broker.

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.

Policy Server

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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.

In a Websense appliance-based deployment, Policy Server is already installed on the full policy source appliance and any user directory and filtering appliances.

In a software-based deployment, Policy Server is typically installed on the same machine as Policy Broker and Filtering Service. Large or distributed environments can include multiple Policy Servers. Each Policy Server may communicate with up to 10 Filtering Service instances.

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.

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 typically 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Filtering Service works with Network Agent, Content Gateway, or a third-party 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.

In a Websense appliance-based deployment, Filtering Service is installed on any Web Security 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.

> ✓ **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 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Network Agent works with Filtering Service to enable protocol management, bandwidth-based filtering, and reporting on bytes transferred.

- In a standalone 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

In a Websense appliance-based deployment, Network Agent is already installed on any Web security-mode V-Series appliance. It may also reside on a dedicated security blade on a X-Series modular chassis.

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 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Usage Monitor tracks users' Internet activity and:

- Passes Internet activity data to Real-Time Monitor.
- Sends alerts when Internet activity for particular URL categories or protocols reaches configured threshold limits.

  Alerts can be sent via email, SNMP trap, or on-screen display. Each Policy Server should have a separate Usage Monitor.

See the TRITON - Web Security Help for more information about alerting and Real-Time Monitor.

TRITON - Web Security

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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.

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Web Security Log Server is a Windows-only component that 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

Each Log Server instance can log to only one Log Database at a time, and only one Log Server can be installed for each Policy Server.

Log Server processing can consume considerable system resources.

In a software-based deployment, do not install 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, Log Server must be installed on a separate Windows machine.

Special considerations

To be able to install Web Security Log Server, a supported database engine (see *Reporting database requirements*, page 5) must be running.

✓ **Note**

Web Security Log Server must be installed before you can see charts on the Status > Dashboard page, or run presentation or investigative reports in TRITON - Web Security.

After installing Log Server, stop and restart the **Websense TRITON - Web Security** and **Websense Web Reporting Tools** services on the management server machine.

Important

When Web Security Log Server is not installed on the TRITON management server, be sure to stop and restart the services mentioned above before creating scheduled jobs in presentation reports. Any scheduled jobs you create before restarting the services cannot be saved properly and will be lost, even if they appear to work for a period of time.

User Service

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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.

In a Websense appliance-based deployment, User Service is already installed on each full policy source and user directory and filtering appliance.

In a software-based deployment, User Service is generally installed on the same machine as *Policy Server*.

Special considerations

When installing User Service, 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 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.
- If you run Websense User Service on Windows Server 2008 or 2008 R2:
  - The Windows Computer Browser service on the User Service machine must be running.

    If your network uses Active Directory 2008 to authenticate users, the Windows Computer Browser service must also be running on the domain controller hosting the directory.
  - Protocol block messages cannot be displayed on client machines.
  - If your network uses a Windows NT Directory or Active Directory (Mixed Mode), 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.

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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.

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.

Special considerations

- 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
- When you run DC Agent on Windows Server 2008 or 2008 R2, the Windows Computer Browser service on that machine must be running.

Logon Agent

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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. Logon Agent:

- Provides unsurpassed accuracy in transparent user identification.
- 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.

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. For instructions on configuring domain controllers and client machines to use Logon Agent, see the Using Logon Agent for Transparent User Identification technical paper.
- 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.
- If you run Logon Agent on Windows Server 2008 or 2008 R2, the Windows Computer Browser service on that machine must be running.

Logon Application

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

The 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. The logon application (LogonApp.exe), runs as a process on client Windows machines. At log on, the logon application identifies the user and sends the information to Logon Agent.

The 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

The logon application runs only in conjunction with Logon Agent. The Group Policy on domain controllers must be modified so it launches **LogonApp.exe** as part of the logon script. Client machines must use NTLM (v1 or v2) when authenticating users.

eDirectory Agent

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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*.

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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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.

State Server

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

State Server enables multiple Filtering Service instances to share timing information. This makes it possible to apply time-based filtering actions (like quota time) in deployments that include multiple Filtering Service instances.

Special considerations

- Install only one State Server instance per **logical deployment**.

  A logical deployment is any group of Policy Server and Filtering Service instances that might handle requests from the same set of users.

  - In a geographically dispersed organization, where each location has its own Policy Server and Filtering Service instances, deploy one State Server instance (on the Policy Server machine or V-Series appliance) at each location.
  - In an organization where all requests are filtered through a central location, only one State Server instance is needed.
- State Server can be enabled via the Command-Line Utility on **full policy source** or **user identification and filtering** appliances.
- All Filtering Service instances that communicate with the same State Server instance must share the same time zone, and the time on all machines must be in synch.
- State Server communicates with Filtering Service on port 55828.
- Each Filtering Service instance can communicate with only one State Server.
- All Filtering Service instances associated with the same Policy Server must communicate with the same State Server.
- Multiple Policy Server instances can share a single State Server.

Multiplexer

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Multiplexer makes it possible for Web Security solutions to pass log data (the same information processed by Log Server) to third-party Security and Information and Event Management (SIEM) products.

Special considerations

- Install one Muliplexer per Policy Server.
- When Policy Server resides on a Websense Appliance, Multiplexer must also be enabled on the appliance.
  - Multiplexer can be enabled via the Command-Line Utility on **full policy source** or **user identification and filtering** appliances.
  - Attempting to connect an off-appliance Multiplexer instance to an on-appliance Policy Server will result in errors.
  - In non-appliance (software-based) deployments, Multiplexer is not required to run on the same machine as Policy Server.

Multiplexer communicates with the following components:

- Policy Server on ports 40000, 55806, and 56010
- Filtering Service on port 55805 (inbound)
- Log Server on port 55805 (outbound)
- SIEM integration (port varies; 514 for TCP and 515 for UDP)

Filtering Plug-in

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Websense software can integrate with a third-party firewall, proxy, router, or similar product (referred to as an integration product). For the integration products, a

Websense filtering plug-in is required to enable communication between Filtering Service and the integration product:

- Microsoft Forefront TMG

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 539.

- Citrix XenApp

All other supported integration products do not require a filtering plug-in.

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. Do not install Filtering Service on the Citrix or Forefront TMG machine.

Remote Filtering Client

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Remote Filtering Client allows filtering on client machines when they are outside the network. The client software:

- Resides on client machines that may be used outside the network firewall.
- Identifies the machines as clients to be filtered.
- Communicates with *Remote Filtering Server*, installed inside the organization’s firewall.

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 executable file to user machines or using a third-party deployment tool. See the Remote Filtering Software technical paper for instructions.

The Remote Filtering Client is configured via the Unified Endpoint Package Builder, which is installed automatically on any Windows machine that includes Websense components (for example, the TRITON management server or the Log Server machine). Find the client pack in the following location: C:\Program Files or Program Files (x86)\Websense\Web Security\DTFAgent\).

✓ **Note**

If you install *Remote Filtering Server* on a Windows machine, the Unified Endpoint Package Builder is automatically installed with it. Do not, however, deploy Remote Filtering Client on 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

Remote Filtering Server provides Web filtering for machines such as laptops that are located outside the network firewall. A remote computer must be running *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.

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. On Windows machines, Remote Filtering Client Pack (see *Remote Filtering Client*) is automatically installed with Remote Filtering Server.

Important

Deploy the Remote Filtering Client to user machines but do not deploy it to the Remote Filtering Server machine.

See Remote Filtering Software technical paper for more information about installing, configuring, and using remote filtering.

Linking Service

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x

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.

Linking Service must be installed on a Windows machine. It is not installed on a Websense 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway Anywhere, v7.7.x

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.

Sync Service is not installed on Websense appliances.

Typically, Sync Service is installed on the *Web Security Log Server* machine.

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 Log Server that send data to the central office) be sure to install Sync Service so it communicates with the central Log Server instance. Branch instances of Log Server cannot send hybrid logging data to the central Log Server.

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 on any full policy source or user directory and filtering appliance. 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

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway Anywhere, v7.7.x

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.

In a Websense appliance-based deployment, Directory Agent is installed (but not enabled, by default) on full policy source and user directory and filtering appliances. Use the Appliance Manager Command-Line Utility to enable the Directory Agent service on an appliance.

Typically, only one instance of Directory Agent is required 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. Specific configuration is necessary for multiple Directory Agent instances to operate properly. For more information, see the TRITON - Web Security Help.

Real-Time Monitor

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.7.x

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.

Real-Time Monitor does not run on Websense appliances. Real-Time Monitor is installed with TRITON - Web Security, by default, 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 full policy source and user directory and filtering appliances. 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.

Install only one instance of Real-Time Monitor per Policy Server.

Websense Content Gateway

Deployment and Installation Center | Web and Data Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway and Gateway Anywhere, v7.7.x
- Data Security, v7.7.x

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

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

The TRITON - Data Security module (also referred to as simply *Data Security module*) of the *TRITON Unified Security Center* is used to manage the Data Security features of your deployment.

Protector

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 324, for more information.

Mobile agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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.

See *Mobile agent*, page 339, for more information.

SMTP agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 *Data Security requirements*, page 9, for supported operating systems.

Important

Prior to installing SMTP agent, be sure to prepare for installation as described in *Preparing a machine for the SMTP agent*, page 357.

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 355, for more information.

Microsoft ISA/TMG agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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.

See *Microsoft ISA/TMG agent*, page 362, for more information.

Data Endpoint

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 *When to use Data Endpoint*, page 423, for more information.

Printer agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

The Data Security printer agent is required when you want to monitor what is printed on your organization's network printers.

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 365, for more information.

Integration agent

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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 372, for more information.

Crawler

Deployment and Installation Center | Data Security Solutions | Version 7.7.x

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.

See *The crawler*, page 375, for more information.

TRITON - Email Security

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

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 email traffic report processing.

Placement

Email Security Gateway is a Websense V-Series appliance-based solution. Most core Email Security functions reside on the appliance. TRITON - Email Security, the management component, 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

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to

- Email Security Gateway and Email Security Gateway Anywhere v7.7.x

Description

Email Security Log Server is the component that receives log records and processes them into the Log Database. Email Security Log Server is a Windows-only component.

Placement

Email Security Log Server must be installed on a separate Windows machine—typically on the TRITON management server. It may not be installed on the Email Security appliance.

Special considerations

To be able to install Email Security Log Server, a supported database engine (see *System requirements for this version*, page 2) must be running.

If you install Email Security Log Server 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

37 Migration Reference

Deployment and Installation Center | Web Security Solutions | Version 7.5.x

Applies to:
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5.x

Use this Deployment and Installation Center Migration Reference to find information about:

- *Upgrading or merging administrator accounts*
- *Migrating from MSDE to SQL Server 2008 R2 Express*

This information applies only to upgrades from v7.5.

- Earlier versions cannot be directly upgraded to v7.7.x.
- Both of these procedures are required for upgrade to 7.6, and do not need to be performed a second time when upgrading from v7.6 to v7.7.

Upgrading or merging administrator accounts

Deployment and Installation Center | Web Security Solutions | Version 7.5.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5.x	◆ *Upgrading Web Security administrator accounts*, page 760 ◆ *Merging administrator accounts*, page 761

This article discusses what happens to Websense administrator accounts:

- During upgrade from v7.5.x to version 7.7

- When version 7.7 administrator accounts are restored from a backup to a system that already has administrator accounts configured

In v7.7 (as in v7.6.x), the default administrator account (with Global Security Administrator permissions) is **admin**. This account has access to all administrative and management functions for all modules of the TRITON Unified Security Center (the Websense management console).

This default account replaces the **WebsenseAdministrator** account from versions 7.5 and earlier.

Upgrading Web Security administrator accounts

When v7.5 Web Security solutions are upgraded to v7.7, administrator accounts are upgraded as described here.

WebsenseAdministrator

On upgrade, the WebsenseAdministrator account is replaced by the **admin** account.

During TRITON Unified Security Center installation, you are prompted to provide a password for the **admin** account.

If a v7.5 Websense appliance is running on-appliance TRITON - Web Security, it is upgraded to version 7.7 TRITON Unified Security Center (Web Security module only). In this case, the **admin** account is automatically configured to use the password assigned to the existing WebsenseAdministrator account.

Local accounts

Websense administrator accounts not authenticated against a directory service are referred to as **local** accounts. Local administrator accounts are brought into the upgraded system, but they must be assigned email addresses.

Administrators can use these accounts to log on to TRITON Unified Security Center, but no permissions changes can be made until the account is associated with an email address. The email address is required for these accounts to access password recovery functionality and 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 continues to be used by the v7.7 TRITON Unified Security Center. As part of the upgrade process, the email address associated with the account in the directory service (if any) is also associated with the account in the TRITON console.

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 7.7 (see version 7.7 System Requirements). **Do this prior to upgrade**.

To do this:

1. Use the Settings > General > Logon Directory page in v7.5 TRITON - Web Security to configure a connection to a v7.7-supported directory service.
2. Replace each existing Windows NT-based or Mixed Mode account with one on the new directory service.

   See the TRITON - Web Security Help for instructions on removing and adding accounts.

If this is not done, the accounts are not usable in version 7.7. The accounts are still listed, but cannot be used to log on to the console. Also, the accounts cannot be removed.

Other LDAP Directory

If **Other LDAP Directory** is selected on the Settings > General > Logon Directory page in v7.5 TRITON - Web Security, the setting is changed on upgrade to **Generic Directory** in the v7.7 TRITON Settings > User Directory page.

This occurs even if the directory service is one specifically supported by the v7.7 TRITON console. (If the directory service is **Active Directory (Native Mode)**, Active Directory is still specified after upgrade.)

After upgrade, log on to the TRITON Unified Security Center and go to **TRITON Settings** > **User Directory** to verify the configured directory service and make any changes necessary.

Merging administrator accounts

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.

Migrating from MSDE to SQL Server 2008 R2 Express

Deployment and Installation Center | Web Security Solutions | Version 7.5.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5.x	

MSDE (Microsoft Desktop Engine) was supported by Websense Web Security products prior to version 7.6. It is not supported for version 7.7.

This article contains instructions for migrating data from an existing installation of MSDE to SQL Server 2008 R2 Express.

In general, these procedures should be performed in conjunction with upgrading Web Security to version 7.7 (see *Upgrading Websense Web Security Solutions*, page 579). 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 the MSDE Log Database

To continue using your existing reporting data in v7.7, back up the v7.5.x MSDE Log Database and restore it to SQL Server Express. Although this is the preferred method, you can alternatively:

- Copy and then attach the data (see *Copying Websense data from MSDE*, page 766).
- Detach and then attach the data (see *Detaching Websense data from MSDE*, page 766).

To back up the data:

1. Create a directory to hold database backups.
2. On the Log Server machine, use the Windows Services dialog box (Start > Administrative Tools > Services) to stop the **Websense Log Server** service.
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 Microsoft SQL Server*, page 21) 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 767.

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**, then click **Add**.

      In the **Locate Backup File** dialog box, navigate to and then select the wslogdb70.bak file you created in MSDE, then 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 769.

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 the MSDE Log Database*, page 764). However, you may copy .mdf and .ldf files to move the data instead.

1. Create a directory to hold database backups.
2. On the Log Server machine, use the Windows Service Control Manager to stop **Websense Log Server**.
3. On the MSDE machine, use the Windows Service Control Manager to 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 767.

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 the MSDE Log Database*, page 764). However, you may detach and attach database files to move the data instead.

1. Create a directory to hold database backups.
2. On the Log Server machine, use the Windows Service Control Manager 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 767.

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 769.

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 connect to SQL Server Express prior to upgrade to 7.7

MSDE is no longer supported by Websense solutions. In its place, SQL Server 2008 R2 Express (SQL Server Express) is supported.

When you upgrade a version 7.5 deployment, you can choose to use SQL Server Express. In this case, if Log Server was configured to use MSDE to store Websense data, you must do the following **before** upgrading:

- The data must be migrated to the new database.
- Log Server must be configured to point to the SQL Server Express installation.

The Websense installer is unable to upgrade Log Server if it is configured to connect to an MSDE database.

Complete the following steps to configure Log Server connect to a SQL Server Express database.

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 (**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 tool to save the change.

   f. Click **Start** on the **Connection** tab to restart the Log Server service.

3. Click **OK** to close the Log Server Configuration tool.

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 Service Control Manager to stop the following services:

- MSSQLSERVER
- SQLSERVERAGENT

38 Changing the TRITON management server IP address, name, or domain

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Gateway Anywhere v7.7.x	◆ *Management components*, page 772 ◆ *Determining which TRITON Unified Security Center modules are active*, page 773

If you modify the IP address, hostname, or domain membership of the TRITON management server, you must make configuration changes to reflect the modification.

Important

This article applies to only the management components on a TRITON management server.

- If Log Server is installed on the machine, remove it before changing the IP address.
- If you have other, non-management components on this machine, additional configuration (not covered in this article) may be necessary.

See *Management components* for more information.

Each module of the TRITON Unified Security Center (TRITON console) 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 774

- *Changing the hostname or domain of the TRITON management server*, page 776

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 include:

- For TRITON infrastructure:
  - Websense TRITON Unified Security Center
  - Websense TRITON Web Server
  - Websense TRITON Settings Database
- For Web Security solutions:
  - Websense Control Service
  - Websense TRITON - Web Security
  - Websense Web Reporting Tools
  - Websense RTM Client
  - Websense RTM Database
  - Websense RTM Server
  - Websense Explorer Report Scheduler
  - Websense Information Service for Explorer
  - Websense Reporter Scheduler
  - Websense Linking Service
  - (not recommended) Websense Log Server
- For Data Security solutions:
  - 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
- For Email Security Gateway and Gateway Anywhere:
  - Websense TRITON - Email Security
  - (not recommended) Websense Email Security Log Server

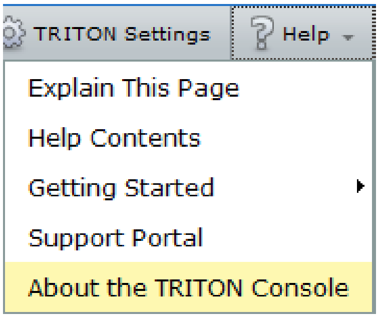
Note that you may not have all the above components installed on your machine. As long as the components that are installed are listed above, this article applies to you.

If you have additional components, not listed above, search the Websense knowledge base (at support.websense.com) for information about configuring those components after an IP address, hostname, or domain membership change. If you need further assistance, please contact Websense Technical Support.

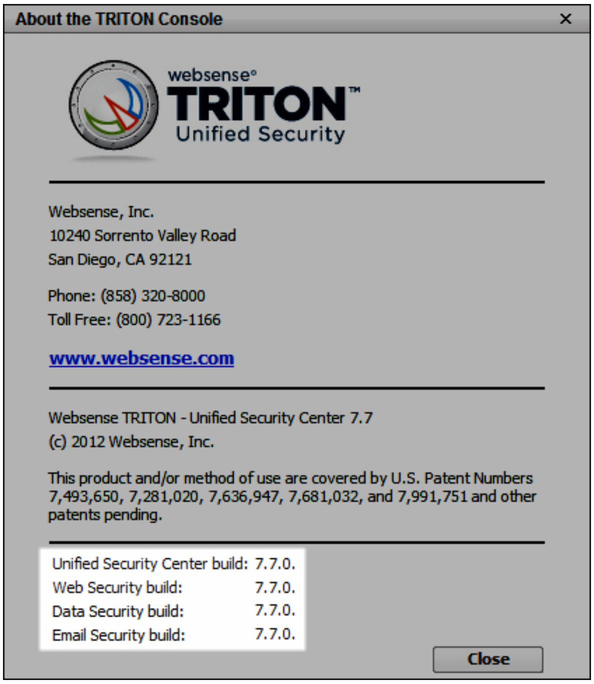
Determining which TRITON Unified Security Center modules are active

To determine which TRITON Unified Security Center modules are active in your deployment:

1. In the TRITON console, go to **Help** > **About the TRITON Console**.



2. The About the TRITON Console dialog box lists the modules that are active (highlighted in illustration below).



Websense, Inc.
10240 Sorrento Valley Road
San Diego, CA 92121

Phone: (858) 320-8000
Toll Free: (800) 723-1166

www.websense.com

Websense TRITON - Unified Security Center 7.7
(c) 2012 Websense, Inc.

This product and/or method of use are covered by U.S. Patent Numbers 7,493,650, 7,281,020, 7,636,947, 7,681,032, and 7,991,751 and other patents pending.

Unified Security Center build:	7.7.0.
Web Security build:	7.7.0.
Data Security build:	7.7.0.
Email Security build:	7.7.0.

Changing the IP address of the TRITON management server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

Before changing the IP address of the TRITON management server, if Web Security Log Server is installed on the management server machine, remove it. The steps below include instructions for reinstalling it after the IP address change is complete.

Complete the following steps **after** changing the IP address of the TRITON management server.

1. Update TRITON Infrastructure with the new IP address.

   See *Configuring TRITON Infrastructure to new IP address, hostname, or domain*, page 777, 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.

2. (*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 TRITON - Web Security. See *Creating Apache SSL certificates*, page 726. 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 use new local IP address*, page 778.

   c. Navigate to the Web Security **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin\, by default) and open the **websense.ini** file in a text editor.

      Update the value of the **LocalServerIP** parameter to the new IP address.

   d. If you want to run Web Security Log Server on the management server (not recommended), and removed it as instructed before changing the IP address of the server, open a Windows command prompt and run the following commands from the C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin\ directory:

      ```
      LogServer.exe -i
      LogServer.exe -r
      ```

e. Log onto TRITON - Web Security and navigate to **Settings** > **Reporting** > **Log Server** page.

f. Verify that correct information appears in the **SQL Server location** field.

   If you change the SQL Server location value, use the Windows Services dialog box to restart **Websense Log Server**.

g. Use the Windows Services dialog box to restart the **Websense RTM Server** and **Websense RTM Client** services.

After changing the Log Server IP address, if alerts appear from old IP address, restart Policy Server to clear the old alert data.

3. (*TRITON - Email Security only*)
   Edit the TRITON - Email Security **catalina.properties** file to reflect the new IP address. See *Configuring Tomcat to a use new local IP address*, page 778.

4. (*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 779.

✓ **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 779 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.

5. (*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 database location in TRITON Unified Security Center. See *Updating the log database location for Email Security Gateway*, page 779.

6. (*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 783.

7. 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 *Re-register Websense Content Gateway*, page 788.

   For Email Security Gateway, see *Re-registering Email Security Gateway with Data Security*, page 781.

Changing the hostname or domain of the TRITON management server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

If SQL Server 2008 Express R2 is installed on the management server, perform the following steps **before** changing the hostname:

1. Log on to SQL Server Management Studio and click **New Query**.
2. In the query window, enter the following commands:

```
Use master;
GO
sp_dropserver '<original_hostname>';
GO
sp_addserver '<new_hostname>', local;
GO
```

   Replace <original_hostname> and <new_hostname> with the actual original and new (planned) names.

3. Close SQL Server Management Server, then use the Windows Services dialog box to restart the **SQL Server (MSSQLSERVER)** service.

After changing the TRITON management server hostname or domain membership, do the following:

1. If you have not done so already, change the hostname or domain membership of the TRITON management server machine at the operating system level (i.e., in Windows).

   Note that changing the hostname or domain membership typically requires a reboot of the machine.

2. Update TRITON Infrastructure with the new hostname or domain.

   See *Configuring TRITON Infrastructure to new IP address, hostname, or domain*, page 777 for instructions.

   If SQL Server 2008 R2 Express (SQL Server Express) is installed on this machine, it is **not** automatically configured to use the new hostname 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 hostname. See *Configuring a new hostname for TRITON - Web Security*, page 782.

4. (*TRITON - Data Security only*)
   Modify the Data Security Management Server installation to reflect the change. See *Changing the domain of the Data Security Management Server*, page 786.

Configuring TRITON Infrastructure to new IP address, hostname, or domain

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

If you change the IP address, hostname, or domain of the TRITON management server, update your TRITON Infrastructure configuration to reflect the change.

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 & Credentials** screen. On that screen:

   - If you changed the IP address of the TRITON management server, select the new address from the **IP address** drop-down list.
   - If you changed the hostname or domain of the TRITON management server, make sure the correct information appears in the **Server or domain** field.

4. Proceed through the remaining installer screens, accepting defaults, and click **Finish**.

Configuring Tomcat to a use new local IP address

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x
- Data Security v7.7.x
- Email Security Gateway and Gateway Anywhere, v7.7.x

If you have changed the IP address of the TRITON management server, you must complete the following steps to update the Tomcat configuration for TRITON -Web Security or TRITON - Email Security.

Note

Tomcat configuration for TRITON Infrastructure and TRITON - Data Security is done automatically when configuring to new IP address, hostname, or domain. See *Configuring TRITON Infrastructure to new IP address, hostname, or domain*, page 777.

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:

     C:\Program Files *or* Program Files (x86)\Websense\Web Security\tomcat\conf\catalina.properties
   - TRITON - Email Security:

     C:\Program Files *or* Program Files (x86)\Websense\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. Use the Windows Services dialog box (**Start** > **Administrative Tools** > **Services**) to 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

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

If the IP address of the machine running Email Security Log Server is changed, you must update TRITON - Email Security to use the new address.

1. Log on to TRITON - Email Security.
2. On the **Settings > Reporting > Log Server** page, enter the new IP address in the **Log Server** field.
3. Click **OK**.

Updating the log database location for Email Security Gateway

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

If the IP address of the Email Security Log Database machine (the IP address of the SQL Server machine) has changed, update TRITON Unified Security Center and Email Security Log Server to use the new address.

Complete these steps even if the Email Security Log Database is located on the same machine as TRITON Unified Security Center or Email Security Log Server.

1. Log on to the TRITON Unified Security Center and click **Email Security**.
2. Go to **Settings > Reporting > Log Database** and 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** > **All Programs** > **Websense** > **Email Security** > **Email Security Log Server Configuration**).

5. In the **Database** tab, click **Connection** to open the **Select Data Source** dialog box.

6. Select the **Machine Data Source** tab and click **New** to open the Create New Data Source dialog box.

   You will create a new data source connection to the new IP address of the Email Security database.

7. 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 **esglogdb7*x*** 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**, then click **OK** once more.

16. 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.

17. In the Email Security Log Server Configuration utility, click **Apply** and then **OK** to the warning message about stopping and restarting Log Server.
18. On the **Connection** tab, under **Service Status**, click **Stop**.

    This stops Email Security Log Server.
19. 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.
20. Click **OK** to close the Email Security Log Server Configuration utility.

Re-registering Email Security Gateway with Data Security

Deployment and Installation Center | Email Security Solutions | Version 7.7.x

Applies to:

- Data Security, v7.7.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.7.x

If the IP address of the TRITON management server has changed, you must re-register Email Security Gateway with Data Security Management Server. Use the following steps:

1. In the TRITON - Email Security module, navigate to **Settings** > **General** > **Data Security** and click **Unregister**.
2. In the TRITON - Data Security module, navigate to S**ettings** > **Deployment** > **System Modules**.
3. Click the Email Security Gateway entry.
4. Click **Delete** at the top of the **System Modules** > **Email Security Gateway** page to remove Email Security Gateway registration.
5. When prompted, click **Deploy** to apply the changed Data Security setting.
6. In the TRITON - Email Security module, navigate to **Settings** > **General** > **Data Security**.
7. Register the Email Security appliance with Data Security.
8. Return to the Data Security module and click **Deploy** in the upper right area of the screen.

Configuring a new hostname for TRITON - Web Security

Deployment and Installation Center | Web Security Solutions | Version 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.x

If the hostname of the TRITON management server has changed, edit your TRITON - Web Security 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. Navigate to the **C:\Program Files or Program Files (x86)\Websense\Web Security\apache\conf\** directory and open the **httpd.conf** file in a text editor.
2. In the **httpd.conf** file, edit the **ServerName** property to reflect the new hostname.

   ServerName is specified in the form <*hostname*>:<*port*>, for example:

   ```
   ServerName my-hostname01:18080
   ```

   Edit only the hostname value.
3. Save and close the **httpd.conf** file.
4. Navigate to the **C:\Program Files or Program Files (x86)\Websense\Web Security\apache\conf\extra\** directory and open the **httpd-ssl.conf** file in a text editor.
5. In the **httpd-ssl.conf** file, edit the **ServerName** property to reflect the new hostname. This entry uses the same format shown in step 2.

   Edit only the hostname value.
6. Save and close the **httpd-ssl.conf** file.
7. Use the Windows Services dialog box (**Start** > **Administrative Tools** > **Services**) to restart the **Websense Web Reporting Tools** service.

Changing the IP address of the Data Security Management Server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway Anywhere, 7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, 7.7.x

Perform this task during off hours, or route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.) while you are performing the task.

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 774.

Important

If you change both the IP address and hostname 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 424, for information on creating and installing an endpoint package.

1. Stop the protector:
   a. Log onto the protector as **root**.
   b. Execute **service pama stop**.
2. 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**.
3. In the installer, for Data Security, select the **Modify** link.
4. Accept the defaults in the installer screens, and then click **Next** until you reach the **Server Access** screen. Select the new IP address here.

5. If you changed the hostname 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**.
7. 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.
8. 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.
9. Re-register all Websense Data Security stand-alone agents, such as: ISA agent, Exchange agent, and printer agent (See *Re-registering Data Security components*, page 787).
10. Start the protector:
    a. Log onto the protector as **root**.
    b. Execute **service pama start**.
11. Click **Deploy** in TRITON - Data Security.
12. Since management server IP was changed, all endpoints must be reinstalled with the new IP. See *Deploying Websense endpoints*, page 424, for information on creating and installing an endpoint package.
13. 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 hostname of the Data Security Management Server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:

- Web Security Gateway Anywhere, 7.7.x
- Data Security, v7.7.x
- Email Security Gateway and Gateway Anywhere, 7.7.x

Perform this task during off hours, or route traffic around the Websense Data Security infrastructure (disabling connectors, ICAP, etc.) while you are performing the task.

It is assumed you have already changed the hostname of the TRITON management server, if not see *Changing the hostname or domain of the TRITON management server*, page 776.

> ✓ **Note**
>
> To change both the IP address and hostname 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).

1. Stop the protector:
   a. Log onto the protector as **root**.
   b. Execute **service pama stop**.
2. 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**.
3. In the installer, for Data Security, select the **Modify** link.
4. Click **Next** in the Installation Wizard until you get to **Local Administrator.**
5. Choose the new server name and the correct user name (in the form “NEWNAME\UserName”).
6. Start the protector:
   a. Log onto the protector as **root**.
   b. Execute **service pama start**.
7. Click **Next** to finish the modification.
8. (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.

9. 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 *Installing and Deploying Websense Endpoint Clients*, page 421, for information on creating and installing an endpoint package.

10. 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

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Data Security, v7.7.x ◆ Web Security Gateway Anywhere 7.7.x ◆ Email Security Gateway 7.7.x ◆ Email Security Gateway Anywhere 7.7.x	◆ *To join a Data Security Management Server to a domain*, page 786 ◆ *To remove a Data Security Management Server from a domain*, page 787

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 hostname of the Data Security Management Server*, page 784.

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 hostname of the Data Security Management Server*, page 784.

Re-registering Data Security components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.7.x

Applies to:	In this topic:
◆ Web Security Gateway Anywhere, 7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Gateway Anywhere, 7.7.x	◆ *Re-register Data Security servers and agents*, page 787 ◆ *Re-register Protector*, page 788 ◆ *Re-register Websense Content Gateway*, page 788

You must re-register all Data Security servers, agents, and protectors when you change the IP address, hostname, 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.

Re-register 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 and go to **Settings** > **Deployment** > **System Modules**.
2. Verify that the components appears in the tree view.
3. Click **Deploy**.

Re-register 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 and go to **Settings** > **Deployment** > **System Modules**.
5. Verify that the protector appears in the tree view.
6. Click **Deploy**.

Re-register 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. Hostname 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 between Content Gateway and 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. Hostname alone is not sufficient to register the proxy with the Data Security Management Server.

39 Data Security Protector CLI

Applies to:	In this topic:
◆ Data Security, v7.7.x	◆ *Overview*, page 791 ◆ *Accessing the CLI*, page 791 ◆ *Command-line reference*, page 792 ◆ *Configuring NTP support*, page 802

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
This is Websense Content Protector 7.5.1.009,
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.

`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 **-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-yyyy** format is used. **dd** is the day of the month [01 to 31] **mmm** is the month in abbreviated 3-letter format [Jan, Feb, Mar, etc.] **yyyy** is the year [2006, 2007]

Default N/A

Example

```
Websense1# date
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.

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
-h displays a short usage message **HH:MM:SS HH** is the hour [00 to 24]
MM is the minutes [00 to 59]
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
17:55:03
```

Modify or show system time zone

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.

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.
memory: displays the protector memory usage information.
network: displays the protector's network settings including hostname, domain name, IP address and routing table.
diag: creates a diagnostic file to be used by Websense technical services.
uptime: displays the amount of time the protector has been up and operational.
features: lists all the possible features available on this protector and what they can do (monitor or block)
hardware: displays hardware information including which network cards are installed.
stats: displays traffic statistics for each protocol being monitored; this is useful to verify the operational status of the Protector.
stats reset: resets all statistics counters to zero.

Default

N/A

Example

```
Websense1# info cpu
Processor 1: 1.3% loaded (98.7% idle) Websense1#
info memory
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
interval: the interval in seconds between two runs that take a snapshot of the statistics.
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
delall: deletes all DNS servers set in the protector
add: adds a DNS server specified by its IP address to the protector
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
delall: deletes all default domain names set in the protector
add: adds a default domain name specified by *domain* to the protector

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.

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***

```
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.
list: shows the configured default gateway.
delete: deletes the defined default gateway.

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]
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**.

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
prefix: network mask of the interface. For example: 24 (will assign 255.255.255.0 mask to the interface)
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.
speed: interface link speed. Available speeds: auto, 10, 100, 1000
duplex: interface link duplex. Available duplex options: auto, half, full
mgmt: sets the interface as the management interface of the protector. The previously defined management interface can no longer be used for management purposes.
enable, disable: enables or disables the interface (default is enable)
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 **set:** defines a list of monitored networks **delete:** deletes previously set filter rules
Default	N/A
Example	`Websense1# filter set "tcp and host 10.0.0.1"` 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.

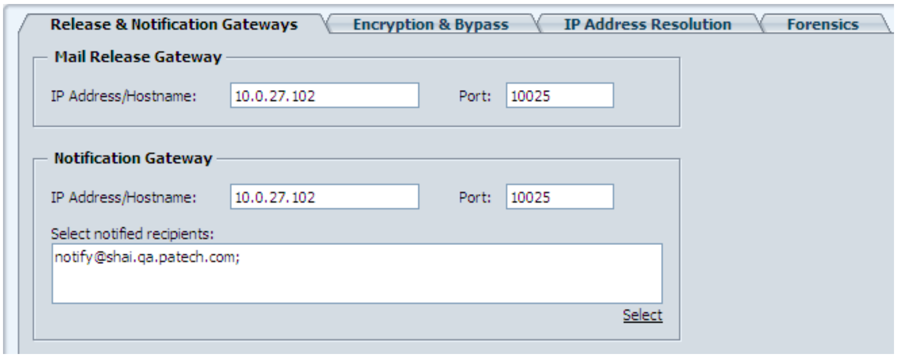
For further NTP configuration details, refer to: http://en.linuxreviews.org/NTP_-_Howto_make_the_clock_show_the_correct_time, or http://doc.ntp.org/4.2.2/**,** and many other sites on the Web.

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.



Mail Release Gateway

IP Address/Hostname: 10.0.27.102 Port: 10025

Notification Gateway

IP Address/Hostname: 10.0.27.102 Port: 10025

Select notified recipients:
notify@shai.qa.patech.com;

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.

Index