websense

Deployment and Installation Center

Websense® TRITON® Enterprise

v7.8.x

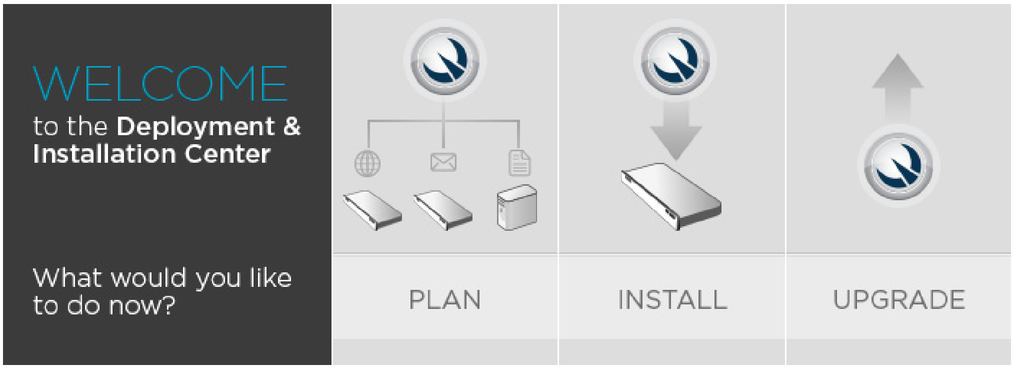
Deployment and Installation Center

Websense TRITON Enterprise version 7.8

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

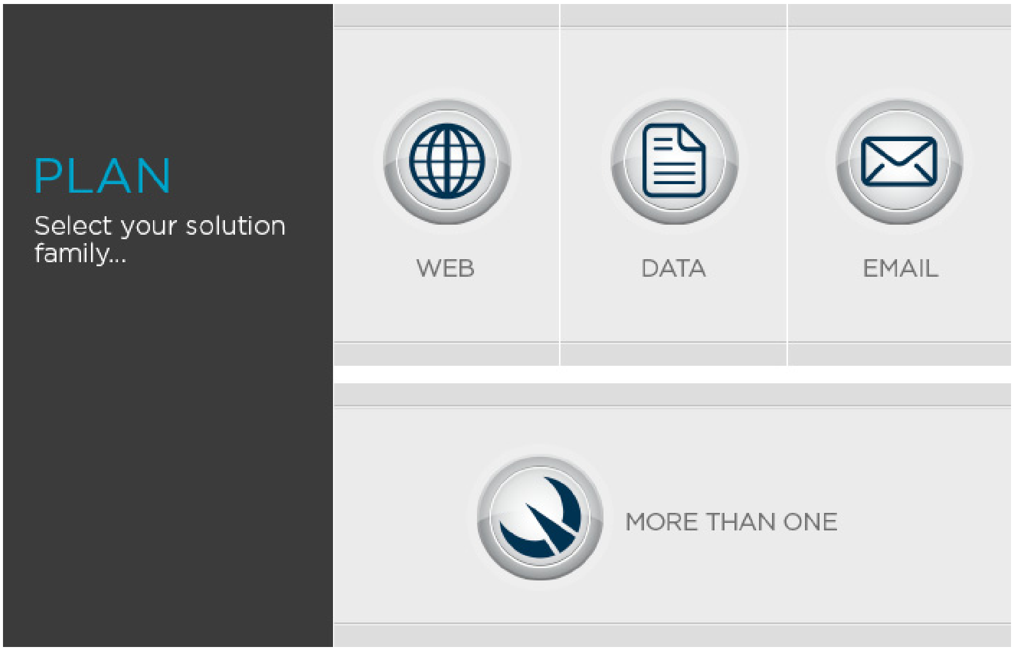
1 Deployment and Installation Center


WELCOME
to the Deployment & Installation Center
What would you like to do now?
PLAN
INSTALL
UPGRADE

Click an image to select an option.

Planning your deployment

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

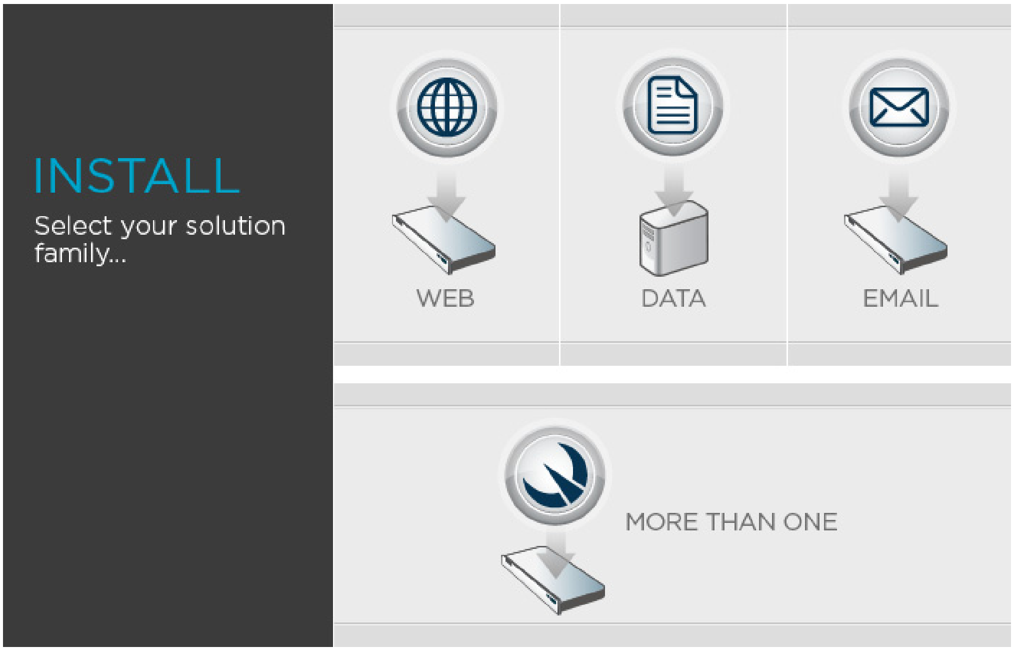


PLAN

Select your solution family...

Installing your security solution

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x



Upgrading your security solution

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Click the link next to your Websense security solution for upgrade instructions.

System requirements for this version

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.8.x	◆ *TRITON management server requirements*, page 5 ◆ *Reporting database requirements*, page 7 ◆ *Requirements for Web Security solutions*, page 8 ◆ *Email Security Gateway requirements*, page 10 ◆ *Data Security requirements*, page 11

TRITON management server requirements

The **TRITON management server** must be one of the following 64-bit machines:

- Windows Server 2008 Standard or Enterprise R2
- Windows Server 2012 Standard Edition
- Windows Server 2012 Standard or Enterprise R2

It hosts the TRITON Unified Security Center (TRITON console), which includes:

- The infrastructure uniting all management components
- A settings database for administrator account information and other shared data
- One or more management modules (Web Security manager, Data Security manager, Email Security manager), used to configure and report on a Websense security solution.

Additional components may also reside on the TRITON management server.

Hardware requirements

The recommended hardware requirements for a TRITON management server vary depending on whether Microsoft SQL Server 2008 R2 Express (used only for evaluations or very small deployments) is installed on the machine.

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 that you allocate more than the minimum listed disk space to allow for scaling with use. The “recommended” option allows for scaling as reporting data accumulates.
- If you install the Websense product on a drive other than the main Windows drive (typically C), it must have at least 3 GB free to accommodate the TRITON installer.

With remote (standard or enterprise) reporting database

Management modules	Recommended	Minimum
Web Security	4 CPU cores (2.5 GHz), 8 GB RAM, 150 GB Disk Space	4 CPU cores (2.5 GHz), 4 GB RAM, 70 GB Disk Space
Data Security	--	4 CPU cores (2.5 GHz), 8 GB RAM, 140 GB Disk Space
Web Security and Data Security	8 CPU cores (2.5 GHz), 12 GB RAM, 300 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space
Email Security and Data Security	8 CPU cores (2.5 GHz), 12 GB RAM, 300 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space
Web Security, Data Security, and Email Security	8 CPU cores (2.5 GHz), 16 GB RAM, 500 GB Disk Space	8 CPU cores (2.5 GHz), 16 GB RAM, 146 GB Disk Space

With local (express) reporting database

Management modules	Recommended	Minimum
Web Security	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space	4 CPU cores (2.5 GHz), 4 GB RAM, 100 GB Disk Space
Data Security	--	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space
Web Security and Data Security	8 CPU cores (2.5 GHz), 12 GB RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space
Email Security and Data Security	8 CPU cores (2.5 GHz), 12 GB RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space
Web Security, Data Security, and Email Security	8 CPU cores (2.5 GHz), 16 GB RAM, 600 GB Disk Space	8 CPU cores (2.5 GHz), 16 GB RAM, 240 GB Disk Space

TRITON console browser support

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

Browser	Versions
Microsoft Internet Explorer*	8, 9, 10, and 11
Mozilla Firefox	4.4 through 30

Browser	Versions
Google Chrome	13 through 35
* Do not use Compatibility View.	

Virtualization systems

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

- Hyper-V over Windows Server 2008 R2 or Windows Server 2012
- VMware over Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2

Note that this support is for the TRITON console only. Other components (used for enforcement, analysis, or reporting) 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
- Lotus Notes
- Generic LDAP directories
- Novell eDirectory
- Oracle Directory Services

Reporting database requirements

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

- For evaluations and small deployments, the TRITON Unified Installer can be used to install Microsoft SQL Server 2008 R2 Express on the TRITON management server machine.

  Use only the version of SQL Server 2008 R2 Express included in the TRITON Unified Installer.
- Larger organizations are advised to use Microsoft SQL Server Standard, Business Intelligence, or Enterprise. These SQL Server editions cannot reside on the TRITON management server.

  SQL Server clustering may be used with all supported standard and enterprise versions of Microsoft SQL Server for failover or high availability.

The supported database engines for Websense Web Security, Data Security, and Email Security solutions are:

- SQL Server 2008 SP3 (or the latest service pack from Microsoft)

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

- SQL Server 2008 R2 Express SP2 (installed by the TRITON Unified Installer)
- SQL Server 2008 R2 SP2 (or the latest service pack from Microsoft)

  All editions except Web and Compact; all service packs; not IA64
- SQL Server 2012 SP1 (or the latest service pack from Microsoft)

  Standard, Business Intelligence, and Enterprise editions

Requirements for Web Security solutions

Software components

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

The following components are Windows-only, running on Windows Server 2008 R2 or R2 SP1, or Windows Server 2012 or 2012 R2 Standard Edition:

- TRITON Unified Security Center (including the Web Security manager)
- Linking Service
- Log Server
- DC Agent
- Real-Time Monitor

Websense Content Gateway is Linux only, certified on:

- Red Hat Enterprise Linux 6.3, 6.4 and 6.5 (64-bit)

  See *System requirements for Websense Content Gateway*, page 168, for a list of supported Red Hat and CentOS versions, and additional information.

All other Web Security components can run on any of the following 64-bit operating systems:

- Windows Server 2008 R2 or R2 SP1
- Windows Server 2012 or 2012 R2 Standard Edition
- Red Hat Enterprise Linux 6

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.

- TRITON Unified Security Center (incl. Web Security manager)
- Log Server
- Sync Service
- Real-Time Monitor
- Linking Service
- Remote Filtering Server

- DC Agent
- Logon Agent
- eDirectory 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 7 with Service Pack 1 (32-bit and 64-bit)
- Windows Vista with Service Pack 1 or higher (32-bit and 64-bit)
- Windows 8
- Windows 8.1 (v7.8.2 and beyond) and Windows 8.1, Update 1 (v7.8.4 and beyond), (LogonApp.exe only, 7.8.3 and later)
- Windows Server 2003
- Windows Server 2008 and 2008 R2
- Mac OSX 10.8 (64-bit)
- Mac OSX 10.9.2 (64-bit) (7.8.3 and later)

In addition, for Web Endpoint, the following web browsers support the endpoint client on both 32-bit and 64-bit Windows operating systems and the 64-bit Mac operating system:

- Internet Explorer 7 to 11 on Windows
- Firefox 3.x to 30 on Windows and Mac
- Safari 5.x on Windows
- Safari 5.x, 6.x, 7.x on Mac
- Google Chrome from 15 to 36 on Windows and Mac
- Opera 11 to 21 on Windows and Opera 11 to 20 on Mac

Full support means that the browser supports all installation methods, and both policy enforcement and proxy manipulation.

Integrations

Websense Web Security may be integrated with the following third-party products.

Product	Versions
Microsoft Forefront TMG	2008 or later
Cisco ASA	v8.0 or later
Cisco Router	IOS v15 or later
Citrix Presentation Server	4.5
Citrix XenApp	5.0, 6.0, or 6.5

In addition, products that can be configured to use ICAP can be integrated via the Websense ICAP Service.

Directory services for user identification

Websense Web Security solutions can use the following directory services for user identification and authentication:

Directory	Versions
Microsoft Active Directory (native or mixed mode)	2012, 2008 R2, 2008
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:

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

Virtualization systems

Windows-based Web Security components that can run on the following virtualization systems:

- Hyper-V over Windows Server 2008 R2 or Windows Server 2012
- VMware over Windows Server 2008 R2 or Windows Server 2012

Email Security Gateway requirements

Email Security Gateway is exclusively appliance-based (V10000 G2/G3, V5000 G2, or X10G), except for the following components:

- **Email Security manager**, which runs on the TRITON management server (see *TRITON management server requirements*, page 5).
- Email Security **Log Server**, which runs on a Windows Server 2008 R2 or 2012 machine.

You can also deploy Email Security Gateway on a virtual appliance. Obtain the image file from the MyWebsense Downloads page. You must have an ESXi VMware platform version 4.0 or later. The Windows components listed above are required along with a virtual appliance deployment.

Data Security requirements

Operating system

Data Security Component	Supported Operating Systems	32-bit	64-bit
Management server	Windows Server 2008 Standard or Enterprise, R2 or R2 SP1		✓
	Windows Server 2012 Standard Edition		✓
	Windows Server 2012 Standard or Enterprise R2		✓
Supplemental servers	Windows Server 2003 Standard or Enterprise, R2 SP2 (v7.8.1 only)	✓	
	Windows Server 2008 Standard or Enterprise, R2 or R2 SP1		✓
	Windows Server 2012 Standard Edition		✓
Crawler agent	Windows Server 2003 Standard or Enterprise, R2 SP2 (v7.8.1 only)	✓	
	Windows Server 2008 Standard or Enterprise, R2 or R2 SP1		✓
SMTP Agent (v7.8.1 and 7.8.2 only)	Windows Server 2003 Standard or Enterprise, R2	✓	✓
	Windows Server 2003 Standard or Enterprise, R2 SP2	✓	✓
ISA Agent (ISA Server 2004/2006) (v7.8.1 and 7.8.2 only)	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 or R2 SP1		✓

Data Security Component	Supported Operating Systems	32-bit	64-bit
Printer agent (v7.8.1 and 7.8.2 only)	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 with Service Pack 1	✓	✓
	Citrix XenDesktop VDI v5.6 and v7.1 running Windows 7 (v7.8.2 and beyond)	✓	✓
	VMware View Horizon VDI v5.2 running Windows 7 (v7.8.3 and beyond)	✓	✓
	Windows 8 Windows 8.1 (v7.8.2 and beyond) and Windows 8.1, Update 1 (v7.8.4 and beyond)	✓	✓
	Windows Vista with Service Pack 1 or higher	✓	✓
	Windows XP with Service Pack 2 or higher	✓	✓
	Citrix XenDesktop VDI v5.6 and v7.1 running Windows XP (v7.8.2 and beyond)	✓	✓
	Windows Server 2003 with Service Pack 2	✓	✓
	Windows Server 2008 with Service Pack 2	✓	✓
	Windows Server 2008 R2 with Service Pack 1		✓
	Citrix XenDesktop VDI v7.1 running Windows Server 2008 R2 (v7.8.2 and beyond)		✓
	VMware View Horizon VDI v5.2 running Windows Server 2008 (v7.8.3 and beyond)		✓
	Windows Server 2012 R2		✓

Data Security Component	Supported Operating Systems	32-bit	64-bit
	Mac OS X 10.7, 10.8 Mac OS X 10.9 (v7.8.2 and beyond)		✓
	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 hostname 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. You can purchase them from a number of computer retailers.

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 850 MB free hard disk space (250 MB for installation, 600 MB for operation)
- At least 512 MB RAM on Windows XP
- At least 1GB RAM on Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2012 Standard Edition

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)

Mac

- At least 1 GB RAM
- At least 500 MB free hard disk space (375 MB for installation, 125 MB for operation)

Preparing for installation

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.8.x ◆ V-Series Appliances, v7.8.x	◆ *All Websense TRITON solutions*, page 16 ◆ *TRITON Unified Security Center*, page 18 ◆ *Web Security*, page 19 ◆ *Data Security*, page 23

All Websense TRITON solutions

Before installing any Websense TRITON solution, make sure that you have completed all of the preparations noted below:

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, roughly 2 GB of 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 disk space requirements, see *Hardware requirements*, page 5.
- The TRITON Unified Installer requires the following versions of .NET Framework, depending on your operating system version:
  - Windows Server 2008 R2: Use version 2.0 or higher. If .NET 2.0 is not already installed, it is available from www.microsoft.com.
  - Windows Server 2012: Version 3.5 is required. If .NET 3.5 is not already installed, it can be added via Server Manager.

Note that .NET Framework 3.5 must be installed before adding any language packs to the operating system (as noted in the following article from Microsoft: http://download.microsoft.com/download/D/1/0/D105DCF6-AC6C-439D-8046-50C5777F3E2F/microsoft-.net-3.5-deployment-considerations.docx).

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

Getting the Websense software installers

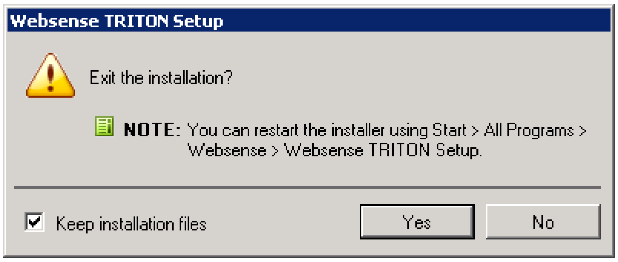
The TRITON Unified Installer is used to install or upgrade the TRITON management server, Web Security solutions, Data Security solutions, Email Security management and reporting components, and SQL Server 2008 R2 Express on supported Windows servers.

There are separate installers for installing Web Security components and Content Gateway on supported Linux servers.

Download the Windows and Linux installers from mywebsense.com.

- The TRITON Unified Installer executable is named **WebsenseTRITON784Setup.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, you can 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

  - Windows Server 2012: Go to the **Start** screen and click the **Websense TRITON Setup** icon.
  - Windows Server 2008 R2: Go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.

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

- The Web Security Linux installer is **WebsenseWeb784Setup_Lnx.tar.gz**.
- The Content Gateway installer is **WebsenseCG784_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 perform the installation, 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, log in as a domain user to run the TRITON Unified 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 451.

No underscores in FQDN

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 inconsistent with Internet Engineering Task Force (IETF) standards.

Note

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

Disable UAC and DEP

Before beginning the installation process, disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.

TRITON Unified Security Center

In addition to the other general preparation actions described in this section:

- 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 4).

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

  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, log in to the machine as a domain user to run the Websense installer. This ensures that Service Broker, installed as part of SQL Server 2008 R2 Express, can authenticate itself against a domain (required).

Web Security

In addition to the general preparation actions (above), Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere components have the following additional requirements.

Filtering Service Internet access

To download the Websense Master Database and enable policy enforcement, 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 439, for more information about ports used by Websense components.

Computer Browser Service

To run User Service or DC Agent on a supported Windows server, the Computer Browser Service must be running.

- On most machines, the service is disabled by default.
- If the service is stopped, the installer will attempt to enable and start it. If this fails, the component installs and starts, but users are not identified until you enable and start the Computer Browser service.

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 policy enforcement 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 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 439.

> **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

If, during the installation, you receive an error regarding the **/etc/hosts** file, use the following information to correct the problem. For versions prior to 7.8.2, use this information to edit your **/etc/hosts** file prior to running the installer.

When installing to a Linux machine, the **hosts** file (by default, in /etc) should contain 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 451). 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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.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 4, for supported versions of SQL Server.
- Note that Standard and Enterprise 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 TRITON Unified Installer to install SQL Server 2008 R2 Express, a free-of-charge, limited performance version of SQL Server 2008 R2. If you choose this option:

- Use the TRITON Unified installer to install SQL Server Express. Do not download and install it from any other source.

  This is the only Express edition of SQL Server you can use with Websense TRITON version 7.8.x solutions.
- Keep in mind that the performance limitations of SQL Server Express make it more appropriate for evaluation environments or small organizations than for larger deployments.

SQL Server 2008 R2 Express can be installed either on the TRITON management server or on a separate machine. For larger enterprises, run the TRITON Unified Security Center and a Standard or Enterprise edition of SQL Server on separate physical machines.

Note

See Administering Websense Databases for more information about selecting a database platform.

To install SQL Server 2008 R2 Express on the TRITON management server, select it when prompted during TRITON Infrastructure installation.

To install SQL Server 2008 Express R2 on any other machine, run the TRITON Unified Installer in custom installation mode and select SQL Server Express. See *Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)*, page 264.

Installing the reporting database in a custom folder with SQL Server 2012

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

Starting with Microsoft SQL Server 2012, the database engine service must have access permissions for the folder where database files are stored. This affects the:

- Web Security Log Database
- Data Security Incident and Configuration Database
- Email Security Log Database

If you want to store your reporting database or databases in any folder other than the SQL Server default folder (C:\Program Files\Microsoft SQL Server), you must:

1. Create the custom folder.
2. Grant the database engine service full permissions to the custom folder.
3. Install your TRITON management server and (for Web or Email Security) Log Server components.

If you do not grant the database engine service the necessary permissions, the installer will not be able to create the reporting database or databases, and some components may fail to install, or be installed incorrectly.

To grant the proper permissions to the database engine service:

1. In Windows Explorer, right-click the custom folder that you created to hold the reporting database or databases and select **Properties**.
2. On the Security tab, click **Edit**, then **Add**.
3. Make sure the hostname of the SQL Server machine appears in the “From this location” field of the Select Users... dialog box.

   If the correct host is not selected, click **Locations**, then select SQL Server host machine and click **OK**.
4. In the Enter the object names... text box, enter the SID of the SQL Server service:
   - The default instance SID is **NT SERVICE\MSSQLSERVER**.
   - Use the format **NT SERVICE\MSSQL$InstanceName** for a named instance.
5. Click **Check Names** to validate the SID.

   If the validation fails:

   a. Click **OK** in the pop-up box to open the Multiple Names Found dialog box.

   b. Select the correct SID, then click **OK**.

   c. Click **OK** again to return to the Permissions dialog box.
6. In the Group or user names list, select the SID you just added, then mark the **Allow** check box under Full control in the Permissions list.
7. Click **Apply**, and then click **OK** twice to exit.

2 Deployment Planning for TRITON Solutions

Deployment and Installation Center | Web, Data, and Email Security Solutions | v7.8.x

Plan TRITON® Enterprise Solutions

If you have a combination of Websense TRITON solutions, or if you have Websense TRITON Enterprise, which combines TRITON Web Security Gateway, Data Security, and Email Security Gateway solutions, use the articles below to plan your deployment:

Web Security

Web Security Deployment Recommendations, page 33

Data Security

Planning Data Security Deployment, page 117

Email Security

Email Security Gateway Deployment, page 119

TRITON Enterprise

TRITON Enterprise deployment overview, page 28

The deployment overview provides a high-level deployment diagram and component summary to help contextualize the detailed, module-specific information provided in the deployment planning articles and guides.

TRITON Enterprise deployment overview

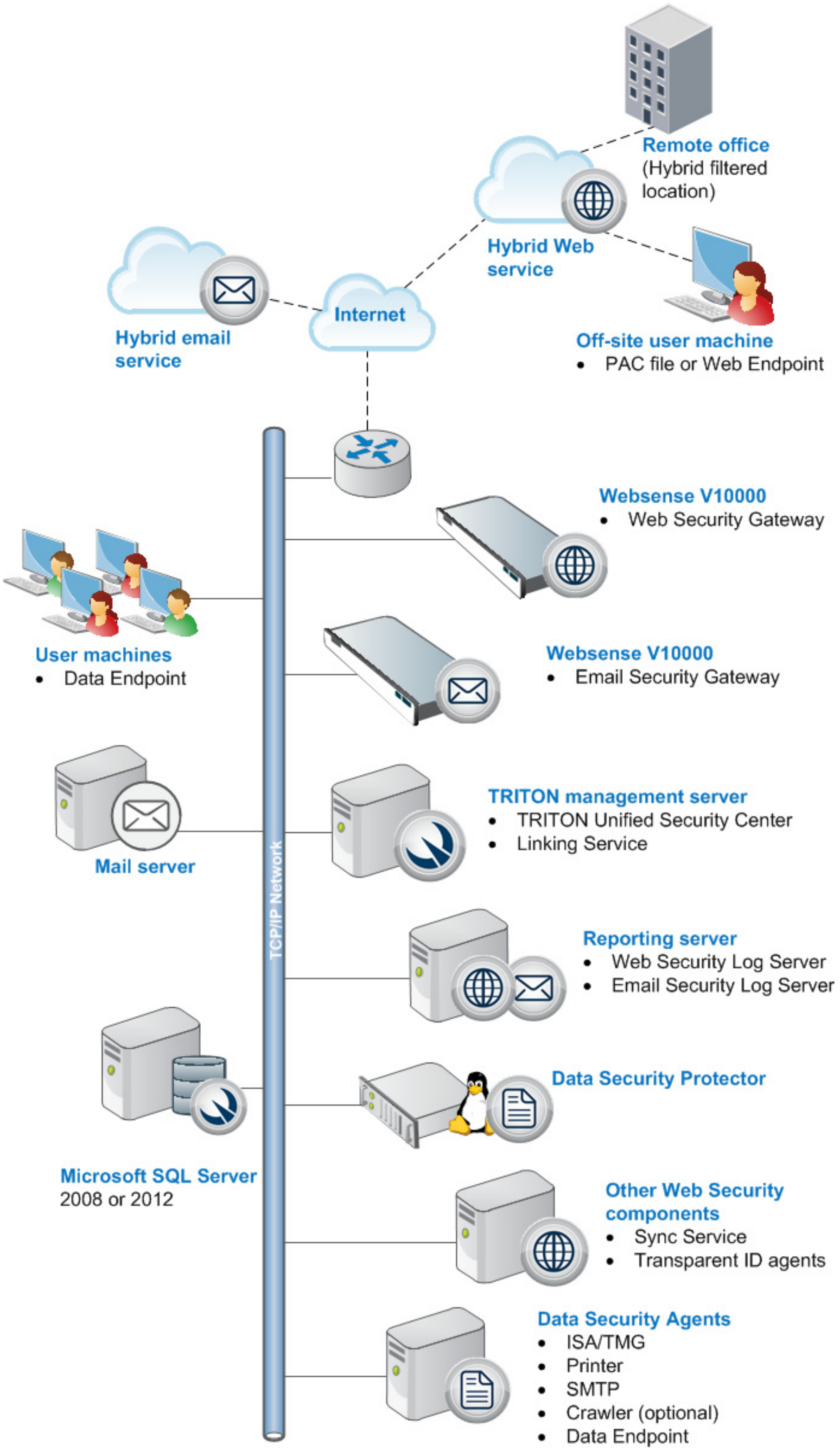
Deployment and Installation Center | Web, Data, and Email Security Solutions | v7.8.x

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

- The TRITON Unified Security Center, the management interface for Web, Email, and Data Security, resides on a Windows server.
- Web Security Gateway Anywhere may be deployed on Websense appliances, dedicated Windows or Linux servers, or a combination of platforms.
- Data Security runs on Windows servers, optional Protector appliances, and elsewhere in the network.
- Email Security Gateway Anywhere enforcement components reside only on Websense appliances. Management and reporting components reside on Windows servers.

High-level deployment diagram

The diagram shows an appliance-based deployment:



Remote office and off-site users

You can use the hybrid web service to provide security for small remote offices. This is accomplished by designating a remote office as a hybrid filtered location.

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

- To direct user requests to the hybrid service, you can install a PAC file or Websense Web Endpoint on the user's machine. Web requests from that machine are then directed to the hybrid service for policy enforcement.
- To use remote filtering software, an optional component, Remote Filtering Server, is installed in your network DMZ, and Remote Filtering Client is installed on user machines. Web requests from the machine are sent to Remote Filtering Server, which connects to Filtering Service for policy enforcement. 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 hybrid web service can 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 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 server on which the 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.

The Data Security Management Server and, typically, Crawler also reside on the TRITON management server machine to provide 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

Remote Filtering Server, 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 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 229, 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 TRITON logging and reporting data. Quarantined email messages are also stored here.

When Websense TRITON 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.

3 Web Security Deployment Recommendations

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Plan Web Security Solutions

This collection of articles explains the requirements, dependencies, and special considerations for deploying the components that make up Websense Web Security solutions.

- Review the *High-level deployment diagrams*, page 34, for Web Security solutions.

  For more distributed networks, find additional diagrams in *Deploying Web Security for a distributed enterprise*, page 77.
- Understand the key components that make up a successful deployment:
  - *Deploying Web Security core components*, page 38
  - (Web Security Gateway and Gateway Anywhere) *Content Gateway Deployment*, page 95
  - (Web Security Gateway Anywhere) *Deploying hybrid Web Security components*, page 43
  - (Web Filter and Web Security) *Understanding Web Security standalone and integrated modes*, page 45
- Find general requirements and considerations:
  - *System requirements for this version*, page 4
  - *Web Security required external resources*, page 58
  - *Maximizing Web Security system performance*, page 59
- Learn how to extend your deployment and add optional user identification and remote policy enforcement components.
  - *Extending your Web Security deployment*, page 49
  - *Additional reporting considerations*, page 53
  - *Deploying transparent identification agents*, page 63
  - *Deployment guidelines for Network Agent*, page 66
  - *Deploying Remote Filtering Server and Client*, page 73

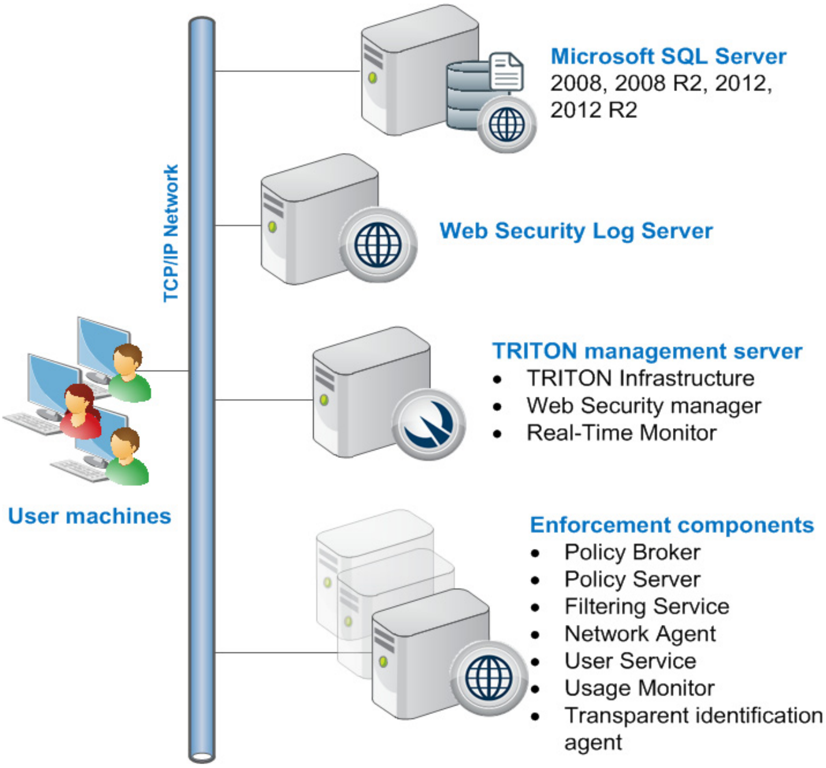
High-level deployment diagrams

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *Web Filter and Web Security deployment diagram* ◆ *Web Security Gateway deployment diagram* ◆ *Web Security Gateway Anywhere deployment diagram*

Web Filter and Web Security deployment diagram

The illustration below shows components distributed across multiple servers in a typical deployment.



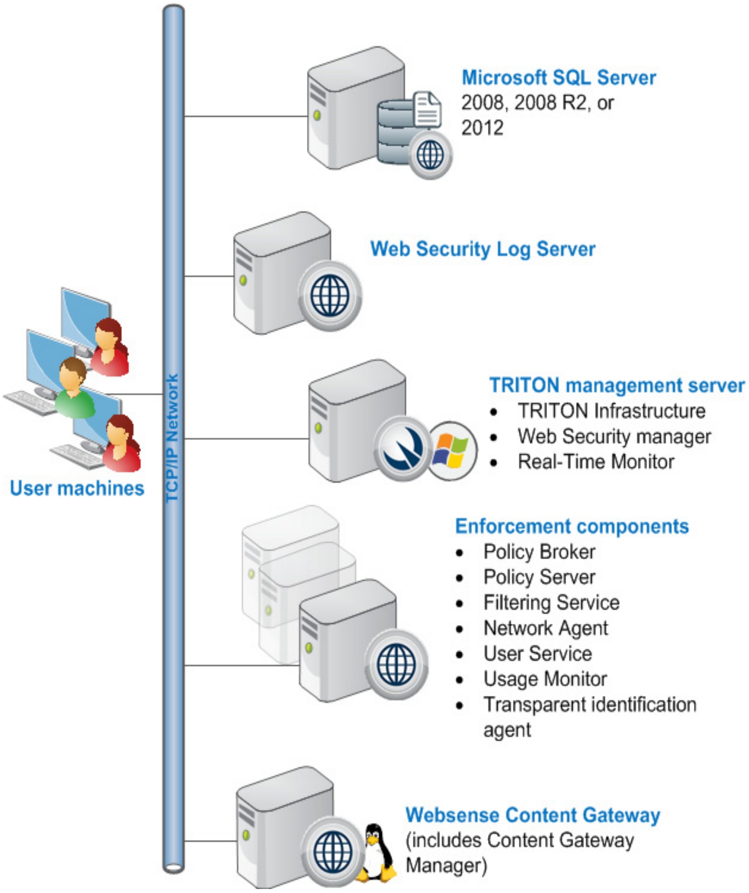
All of the enforcement components, except for the optional transparent identification agents, may reside on a Windows or Linux server, or a Websense appliance.

For evaluation or very small (low traffic) deployments, all Websense components, plus an instance of SQL Server 2008 R2 Express (installed by the TRITON Unified Installer) may reside on a single Windows server.

For more information about the core components that make up a deployment, see *Deploying Web Security core components*, page 38.

Web Security Gateway deployment diagram

This illustration shows a basic software-based deployment of Web Security Gateway. Note that the 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).



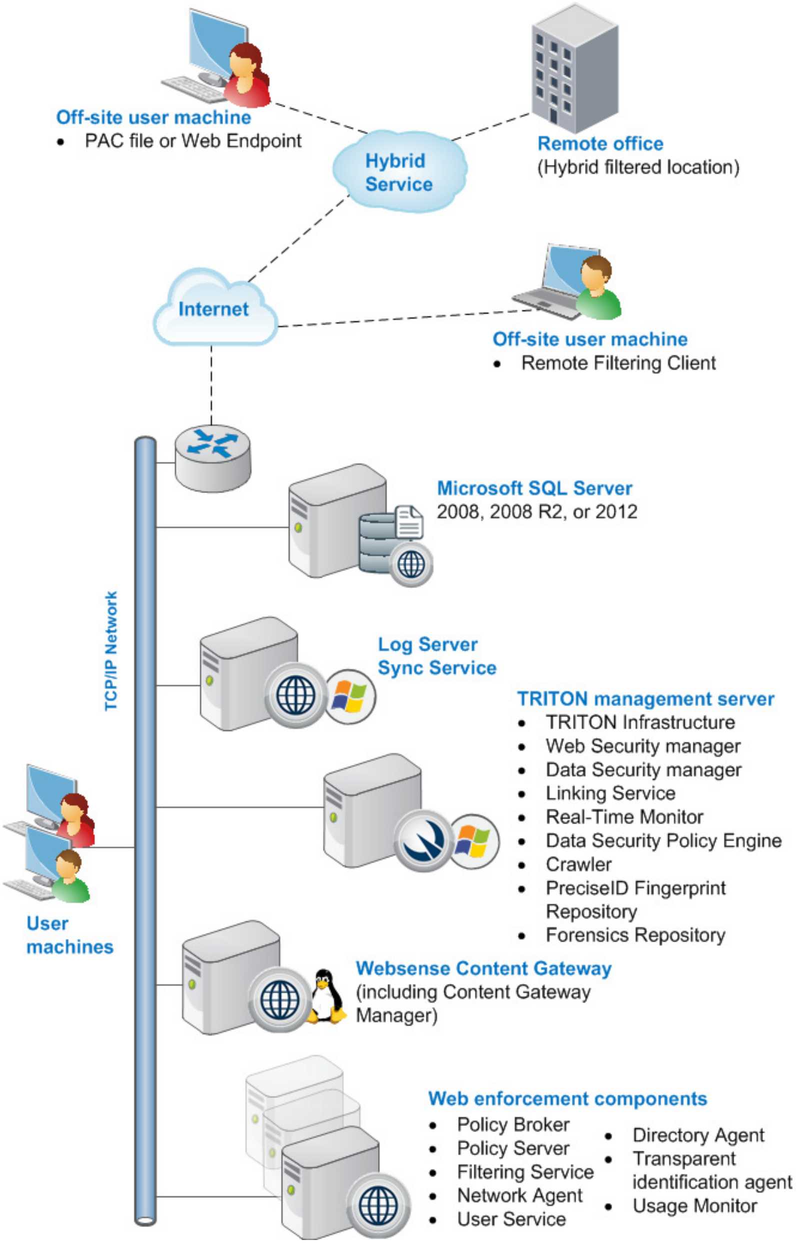
Content Gateway and the enforcement components, except for the optional transparent identification agents, may also reside on a Websense appliance.

For more information about the core components that make up a deployment, see:

- *Deploying Web Security core components*, page 38
- *Content Gateway Deployment*, page 95

Web Security Gateway Anywhere deployment diagram

This 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).



Content Gateway and the enforcement components, except for the optional transparent identification agents, may also reside on a Websense appliance.

For more information about the core components that make up a deployment, see:

- *Deploying Web Security core components*, page 38

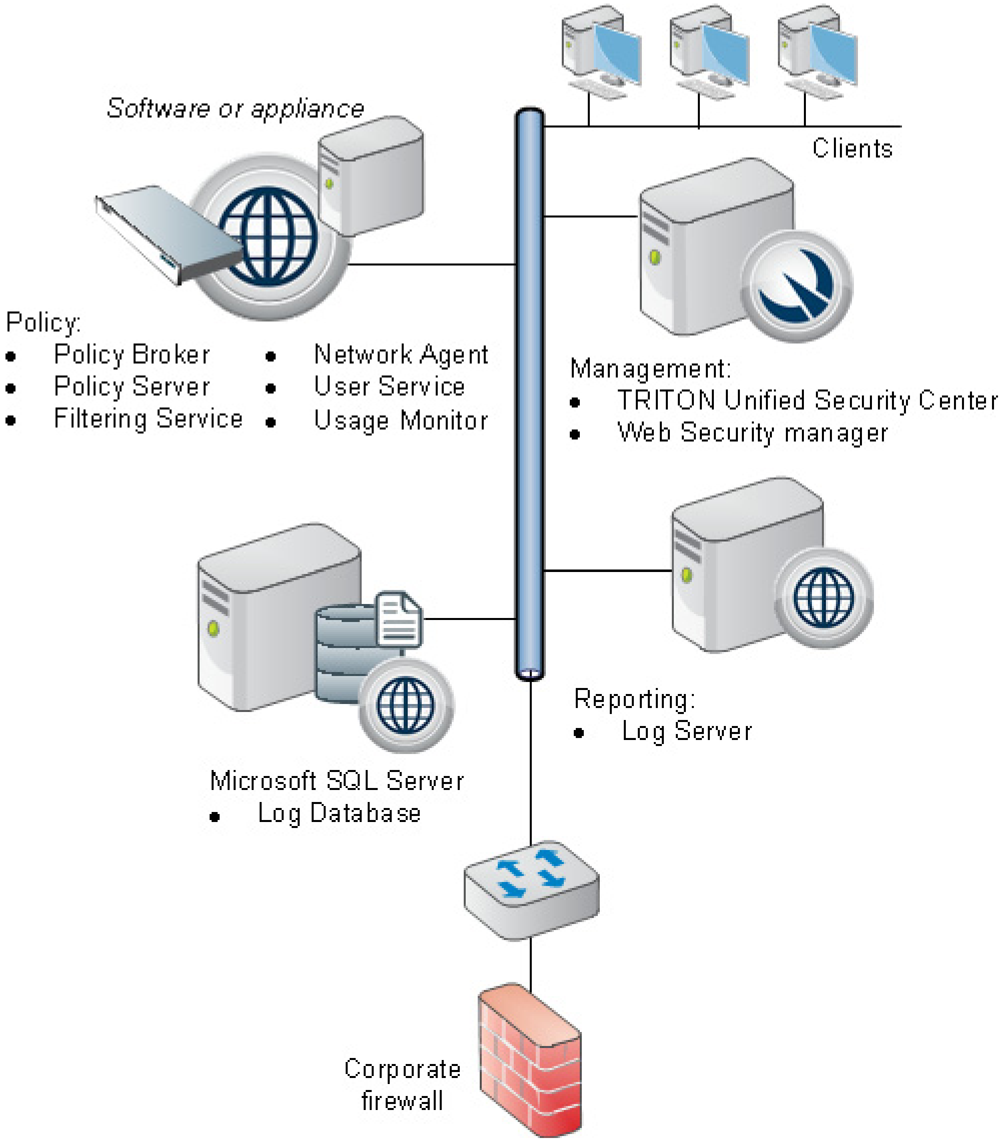
- *Content Gateway Deployment*, page 95
- *Deploying hybrid Web Security components*, page 43

Deploying Web Security core components

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *Core policy components* ◆ *Core management components* ◆ *Core reporting components*

Websense Web Security solutions are made up of core policy, management, and reporting components, shown in the diagram below and described in detail in the sections that follow.



Core policy components

Policy Broker:

- Manages requests from other components for policy and configuration data
- Can be deployed standalone (one per deployment) or replicated (one primary with one or more replicas)
- Sole instance (standalone) or primary (replicated) installed before other components
- On "full policy source" appliance (standalone only)

Software or appliance

Core policy components:

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

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 manage 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:

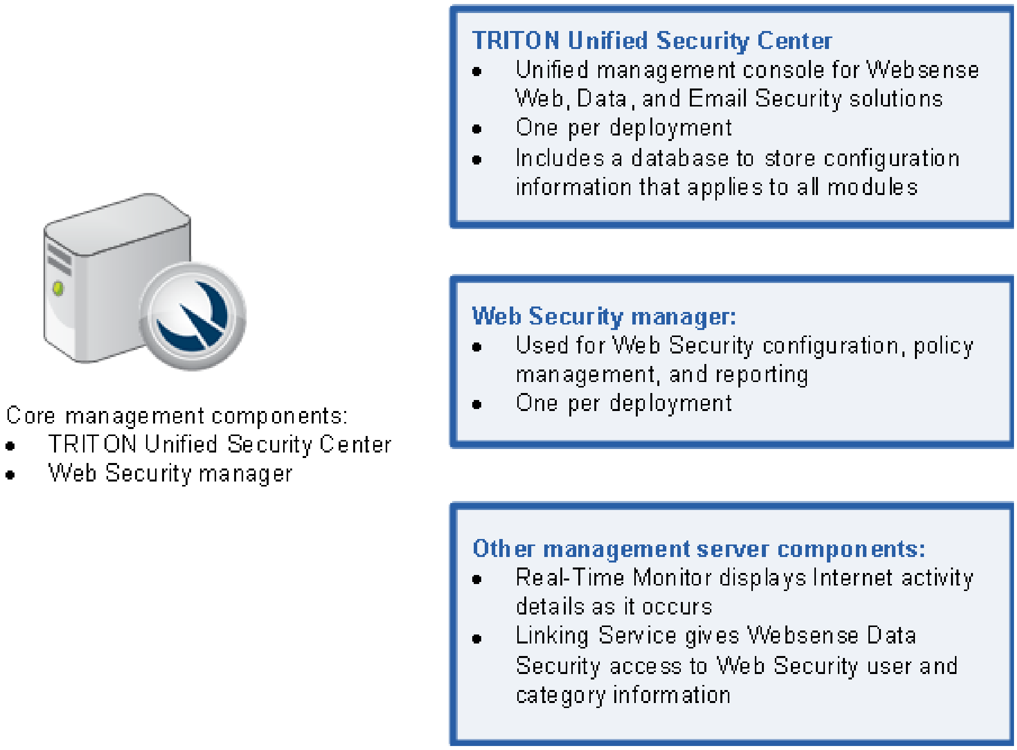
- Network Agent monitors traffic in standalone deployments. Up to 4 per Filtering Service.
- User Service enables user- and group-based filtering. 1 per Policy Server.
- Usage Monitor enables alerting features and Real-Time Monitor. 1 per Policy Server.

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

- All components can communicate with an instance of Policy Broker.
    - In Policy Broker standalone mode (software or appliance), there is only one Policy Broker instance for the entire deployment.

    - In Policy Broker replicated mode (software only), there is one primary Policy Broker (to which configuration updates are written) and one or more Policy Broker replicas (with a read-only copy of the configuration data).
    - In software installations, Policy Broker can run on Windows or Linux.
    - With Websense appliances, the standalone 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 standalone or primary 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, or on a separate machine.
    - 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 (see *Understanding Web Security standalone and integrated modes*, page 45):
    - 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
- Web Security manager

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

Web Security manager:

- Used for Web Security configuration, policy management, and reporting
- One per deployment

Other management server components:

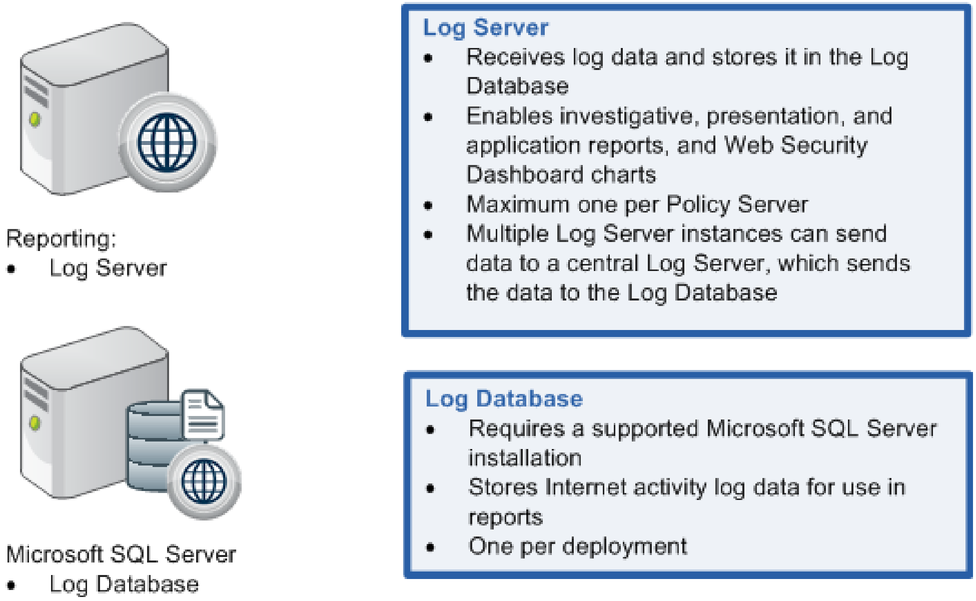
- Real-Time Monitor displays Internet activity details as it occurs
- Linking Service gives Websense Data Security access to Web Security user and category information

The TRITON Unified Security Center (TRITON console) is the centralized management console for Websense TRITON Enterprise 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.

The Web Security manager 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).
- The Web Security manager 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



Log Server

- Receives log data and stores it in the Log Database
- Enables investigative, presentation, and application reports, and Web Security Dashboard charts
- Maximum one per Policy Server
- Multiple Log Server instances can send data to a central Log Server, which sends the data to the 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.
  - You may have one Log Server instance for the entire deployment, or multiple Log Server instances (see *Additional reporting considerations*, page 53), but you can never have more than one Log Server per Policy Server.
- 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 53.
- The TRITON management server machine must be able to communicate with Log Server and the Log Database.

Deploying hybrid Web Security components

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Security Gateway Anywhere, v7.8.x	◆ *Sync Service*, page 43 ◆ *Directory Agent*, page 43

Websense Web Security Gateway Anywhere offers the ability to combine on-premises and hybrid (cloud or security-as-a-service) policy enforcement.

Two on-premises components are used to enable 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 service (in the cloud). 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 either the central Log Server or a remote Log Server. If you are using a version prior to 7.8.2, Sync Service must be configured 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 55885 (outbound)
- Directory Agent on port 55832 (inbound)
- Web Security manager 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 policy enforcement 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. Deployments with multiple Policy Servers, however, would require multiple Directory Agent instances.
- 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 the Web Security manager to configure the Sync Service connection manually for all supplemental Directory Agent instances. See “Directory Agent and User Service” in the 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.

Understanding Web Security standalone and integrated modes

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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, 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. See:
  - *Hardware recommendations for standalone Web Filter or Web Security deployments*, page 47
  - *Deployment guidelines for Network Agent*, page 66
- 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 Cisco*, page 269
  - *Integrating Web Security with Citrix*, page 293
  - *Integrating Web Security using ICAP Service*, page 333
  - *Integrating Web Security with Microsoft Products*, page 311
  - *Installing Web Security for Universal Integrations*, page 339

Websense Web Security Gateway and Gateway Anywhere solutions include **Websense Content Gateway**, a high-performance web proxy that provides real-time threat analysis and website classification. With these solutions, Content Gateway forwards HTTP(S) and FTP requests to Websense Filtering Service to determine whether to permit or block the request. See *Content Gateway Deployment*, page 95.

✓ **Note**

Content Gateway can be combined with F5 BIG-IP Local Traffic Manager, giving greater flexibility to your security gateway infrastructure. You can configure an integrated environment for explicit and transparent proxy in combination with a Websense appliance. For more information, see the F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway Configuration Guide.

Hardware recommendations for standalone Web Filter or Web Security deployments

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

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

- 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 4).

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.

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

Network Size	Enforcement 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 2012, 2008, or 2008 R2, 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 2012, 2008, or 2008 R2, or SQL Server 2008 R2 Express required for Log Database
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 2012, 2008, or 2008 R2 for Log Database

To run both policy enforcement and reporting components 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 whose requests are monitored and managed. See *Extending your Web Security deployment*, page 49.

Extending your Web Security deployment

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *Filtering Services per Policy Server* ◆ *Network Agents per Filtering Service* ◆ *Policy Server, Filtering Service, and State Server* ◆ *Policy Server, Filtering Service, and Multiplexer*

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 responsiveness in locations far away from the central Web Security installation.
- Manage high amounts of traffic.

When Policy Broker is installed in standalone mode, all Policy Server instances connect to the same, central Policy Broker. When Policy Broker is installed in replicated mode, you can configure how each Policy Server determines which Policy Broker instance to use.

Each Policy Server instance can support:

- Up to 10 Filtering Service instances (see *Filtering Services per Policy Server*, page 50)
  - Each Filtering Service can support up to 4 Network Agent instances (see *Network Agents per Filtering Service*, page 51)
- 1 User Service
- 1 Usage Monitor
- 1 Web Security Log Server
- 1 State Server (see *Policy Server, Filtering Service, and State Server*, page 51)
- 1 Multiplexer (see *Policy Server, Filtering Service, and Multiplexer*, page 52)

- 1 Directory Agent (Websense Web Security Gateway Anywhere only; see *Directory Agent*, page 43)

For high-level diagrams of larger Web Security deployments, see *Deploying Web Security for a distributed enterprise*, page 77.

Filtering Services per Policy Server

As a best practice, deploy no more than 10 Filtering Service instances per Policy Server. A Policy Server instance may be able to handle more, depending on the load. If the number of Filtering Service instances exceeds the Policy Server's capacity, however, 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 50.

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

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, deploy no more than 4 Network Agent instances 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, policy enforcement 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 policy actions. (Quota time, for example, is a time-based action that can be used to give users access to websites in selected categories for a configurable time period.)

When State Server is installed, all of 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 managed 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 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *Using a custom port to connect to the Log Database* ◆ *Using SSL to connect to the Log Database* ◆ *Configuring distributed logging*

When you install Web Security reporting components, you can configure how those components communicate with the Microsoft 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 54, 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 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.

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 (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 the Web Security manager.) 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 the Web Security manager). 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=FALSE
   MoveCacheFilePath=C:\Program
   Files\Websense\bin\CacheProcessing
   ProcessCacheFile=TRUE

   [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 the Web Security manager). 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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x

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

- **TCP/IP**

  Websense software provides policy enforcement 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 policy enforcement 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 4, for supported directory services.

  For information on configuring Websense software to communicate with a supported directory service, see the 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. Minimize network latency for efficient Filtering Service performance. Excessive delays under high load circumstances can impact Filtering Service and may cause lapses in policy enforcement.

- **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 4, 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 bundled into the TRITON Unified Installer, is best-suited to evaluation or proof of concept deployments. It can also be used by 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 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x	◆ *Network Agent* ◆ *HTTP request logging* ◆ *Microsoft SQL Server (Log Database)* ◆ *Log Database sizing considerations*

Adjust Websense components to improve policy enforcement 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 Filtering Service, which uses the data to manage 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. 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 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 the Web Security manager.
- 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 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 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 62)
  - disabling full URL logging (see *Logging full URLs*, page 62)

- enabling consolidation (see *Consolidation*, page 62)
- only logging non-HTTP protocol traffic for selected protocols (see *Protocol logging*, page 63)
- only logging HTTP and HTTPS traffic in selected categories (see *Selective category logging*, page 63)

All of these logging settings can be customized in the Web Security manager. 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 transparent identification agents

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x	◆ *Combining transparent identification agents*

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

- Standalone Web Filter or Web Security deployments
- Integrated deployments in which the integration product does not send user information to Filtering Service
- Web Security Gateway or Gateway Anywhere deployments, as an alternative or supplement to transparent or explicit proxy authentication

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

> **Note**
> 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.

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 65.

See *Installing Web Security components*, page 239, for transparent identification agent installation instructions. See the 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.

Combination	Same machine?	Same network?	Configuration required
DC Agent + eDirectory Agent	No	No	Communication with both a Windows directory service and Novel eDirectory is not supported in the same deployment. However, both agents can be installed, with only one agent active.
DC Agent + Logon Agent	Yes	Yes	Configure each agent to use a unique port to communicate with Filtering Service. By default, DC Agent uses port 30600; Logon Agent uses port 30602.
RADIUS Agent + Logon Agent	Yes	Yes	Configure all agents to communicate with Filtering Service.
eDirectory Agent + Logon Agent	No	No	Communication with both Novell eDirectory and a Windows- or LDAP-based directory service in the same deployment is not supported. However, both agents can be installed, with only one agent active.
RADIUS Agent + eDirectory Agent	Yes	Yes	Configure each agent to use a unique port to communicate with Filtering Service. By default, eDirectory Agent uses port 30700; RADIUS Agent uses port 30800. When adding agents to the Web Security manager, use an IP address to identify one, and a machine name to identify the other.
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.

Deployment guidelines for Network Agent

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, and Web Security Gateway (Anywhere) v7.8.x	◆ *NAT and Network Agent* ◆ *Network Agent NIC configuration*

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

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.

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.

Network Agent NIC configuration

Network Agent must be able to see all outgoing and incoming Internet traffic on the network segment that it is assigned to monitor. Do not install multiple instances of Network Agent on the same machine.

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.

- You have the option to use a switch that supports bidirectional spanning. This allows Network Agent to use a single network interface card (NIC) to both monitor traffic and send block pages.

  If the switch does not support bidirectional spanning, the Network Agent machine must have at least 2 NICs: one for monitoring and one for blocking.

  - 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.

Network Agent can also connect to an unmanaged, unswitched hub located between an external router and the network.

If the machine running Network Agent has multiple NICs:

- Each NIC can be configured to monitor or block Internet requests, or both.
- The blocking or inject NIC (used to serve block pages) **must have an IP address** (cannot be set for stealth mode).
- A NIC configured only to monitor (but not block) does not need an IP address (can be set for stealth mode).
- 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:

- 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.

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 positioning Network Agent in your network, see:

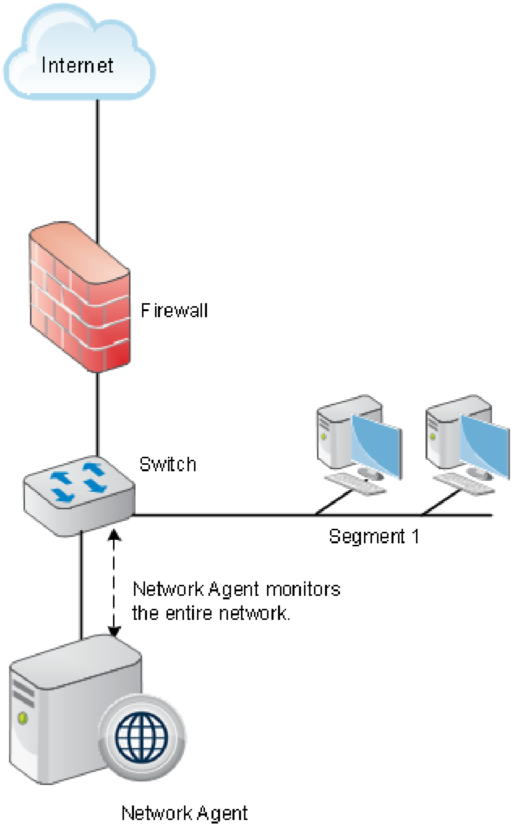
- *Locating Network Agent in a single-segment network*, page 68
- *Locating Network Agent in a multiple-segment network*, page 69
- *Network Agent on a gateway*, page 72

Locating Network Agent in a single-segment network

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

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



Locating Network Agent in a multiple-segment network

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

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 policy enforcement 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 policy enforcement.

  The network segment or IP address range monitored by each Network Agent instance is determined by the NIC settings for the agent, configured in the Web Security manager. See the 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

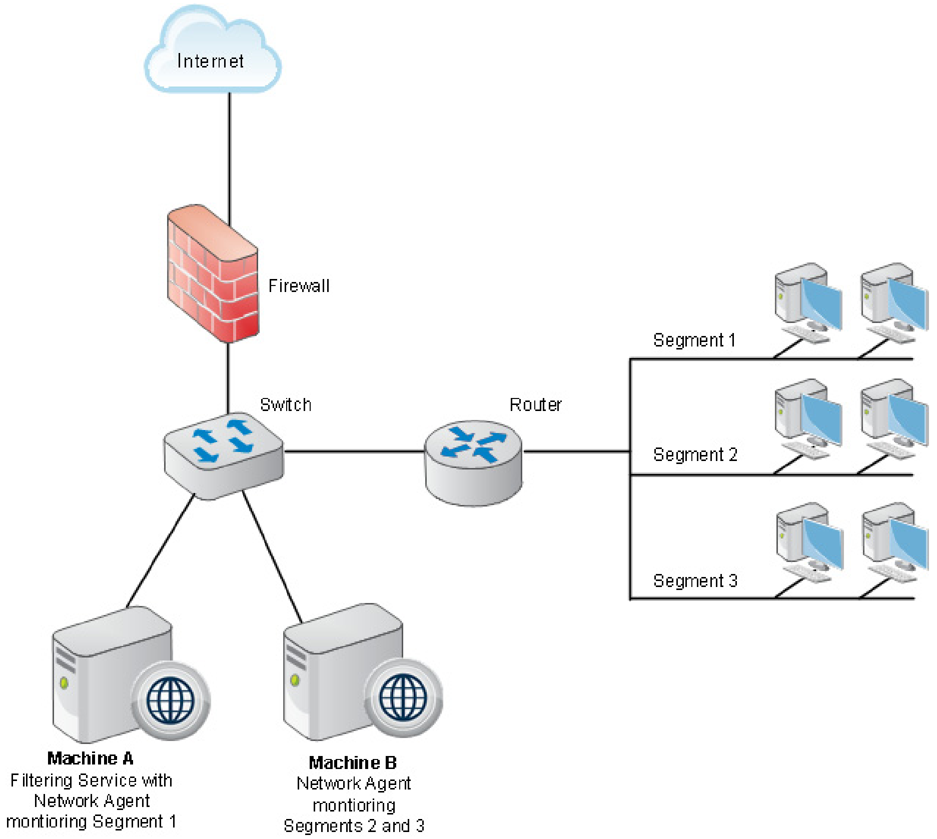
A network with multiple segments can be managed from a single location. Install Filtering Service where it can receive Internet requests from each Network Agent and any integration product.

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.

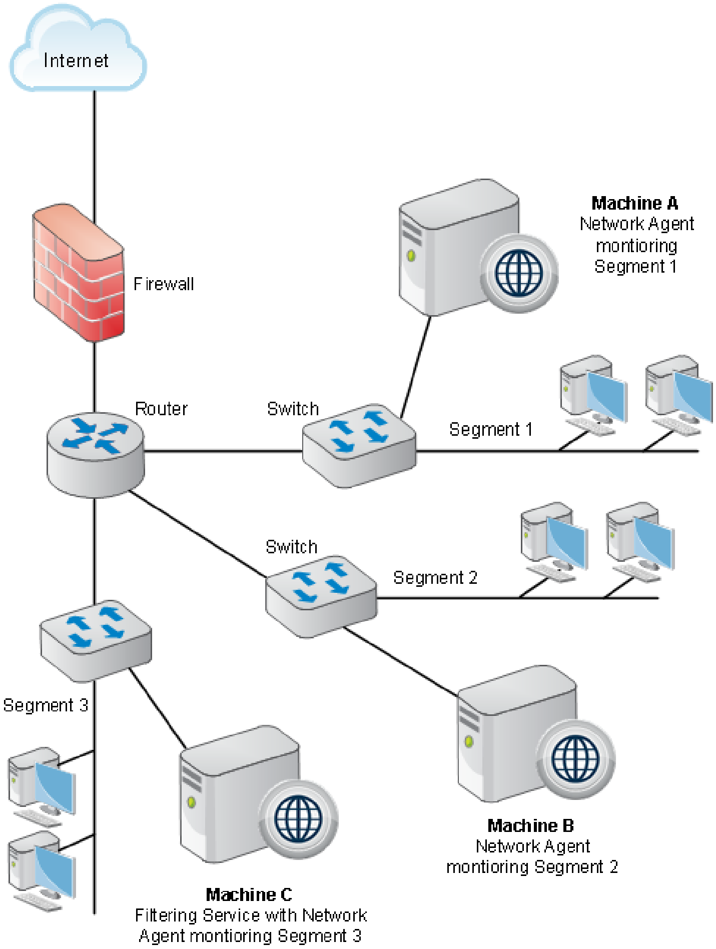


Distributed Network Agent placement

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

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

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.

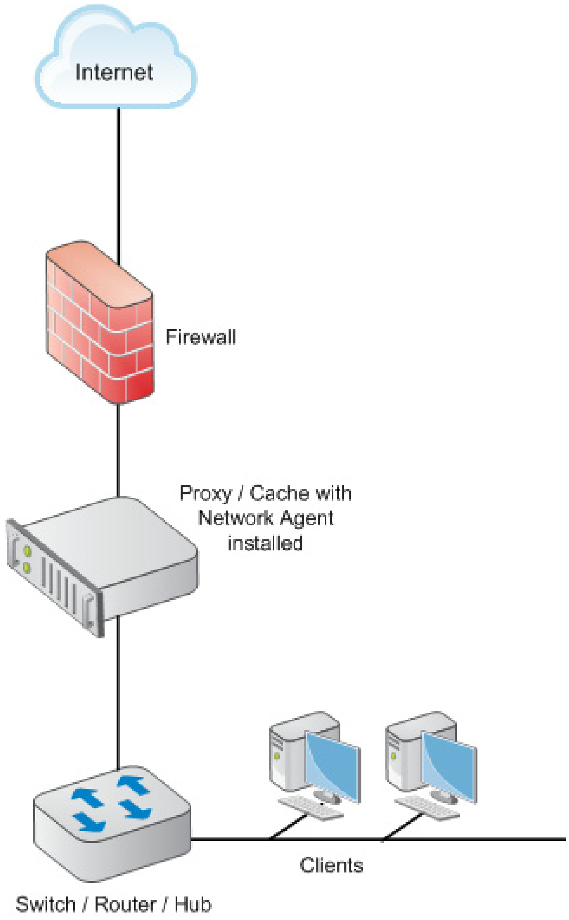
Do not install Network Agent on a firewall. Also, if your network includes a software installation of Content Gateway, do not install Network Agent on the Content Gateway machine. (Content Gateway and Network Agent can reside on the same V-Series appliance.)

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 7.8.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.

When you install remote filtering components:

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

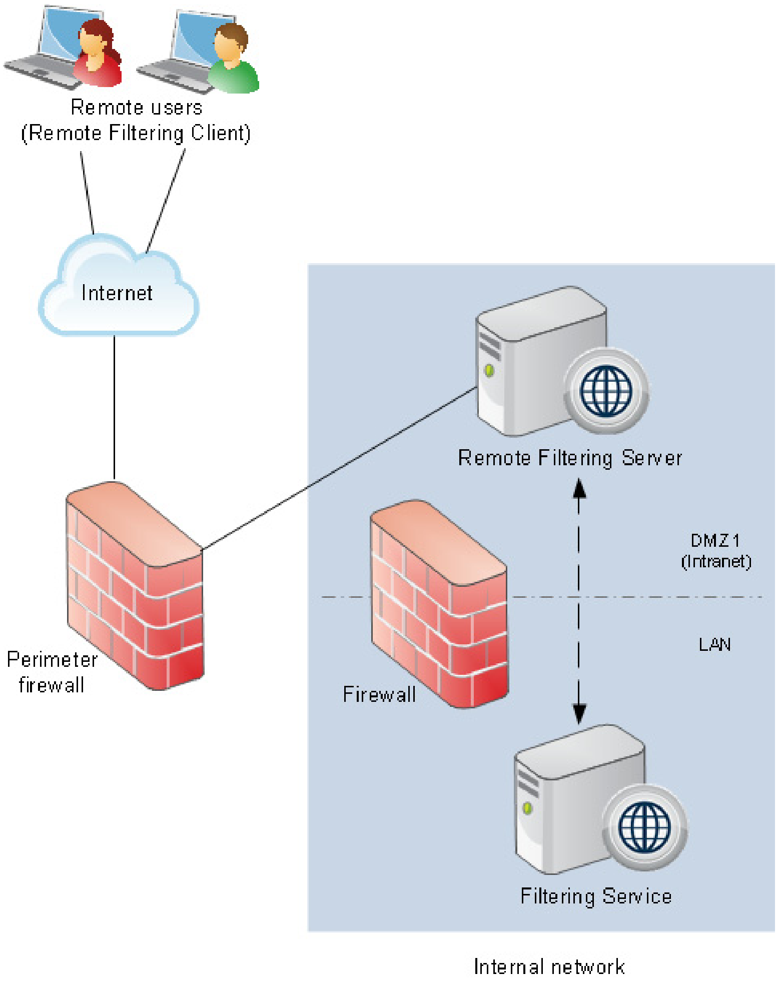
  As a best practice, install Remote Filtering Server in the DMZ outside the firewall protecting the rest of the corporate network. This is strongly recommended.
- Do **not** install Remote Filtering Server on the same machine as Filtering Service or Network Agent.
- Each Filtering Service instance can 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.



4 Deploying Web Security for a distributed enterprise

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x

Distributed enterprise networks may have many remote locations, ranging from dozens to thousands of small sites. The remote locations have Internet access, but may have no dedicated IT staff.

The challenge is to apply consistent, cost-effective web security 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 requests are sent directly to the Internet and are not first routed through a central corporate network.
- Internet access must be managed to permit only appropriate content.
- Cost or maintenance considerations prohibit deploying a dedicated web security server at each site.

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

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

For more information, see:

- *Web Security basic distributed enterprise topology*, page 78
- *Web Security for remote users or locations*, page 82
- *Web Security distributed enterprise deployment models*, page 86
- *Web Security distributed deployments and secure VPN connections*, page 93

Web Security basic distributed enterprise topology

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

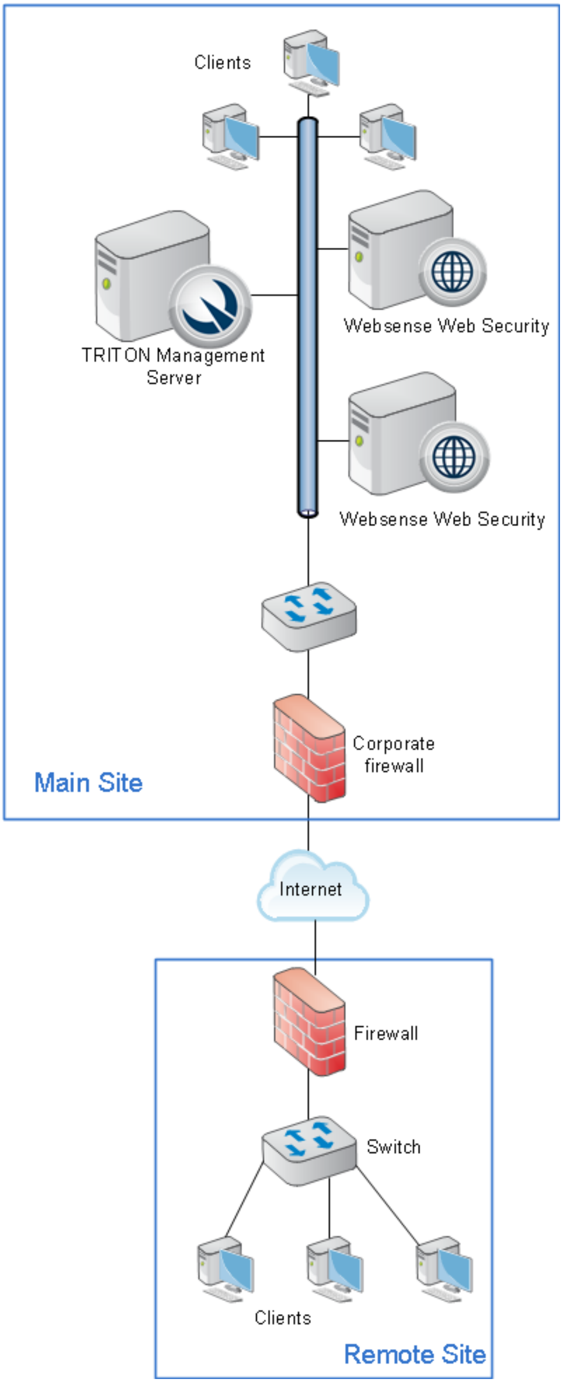
Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *Web Security and Web Security Gateway*, page 78 ◆ *Websense Web Security Gateway Anywhere*, page 81

Web Security and Web Security Gateway

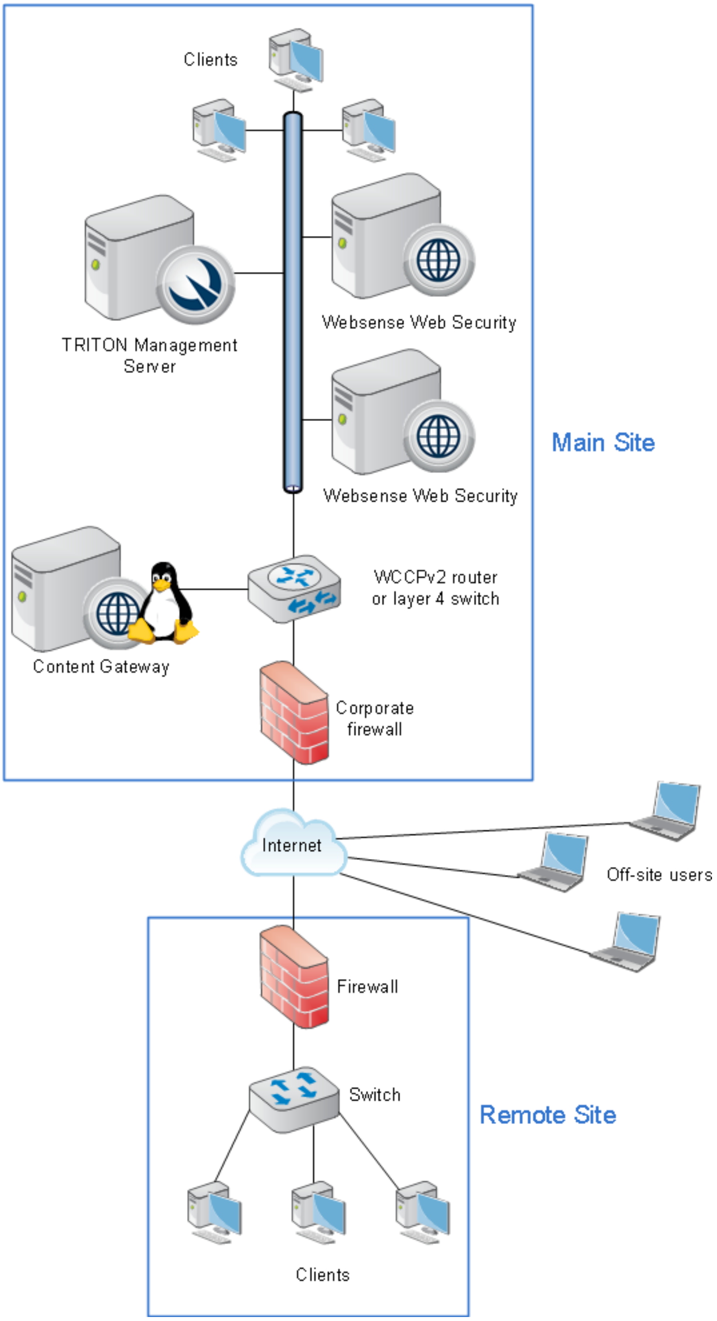
To reduce network infrastructure costs, each remote-site firewall in a decentralized network is connected directly to the Internet, rather than to a corporate WAN.

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



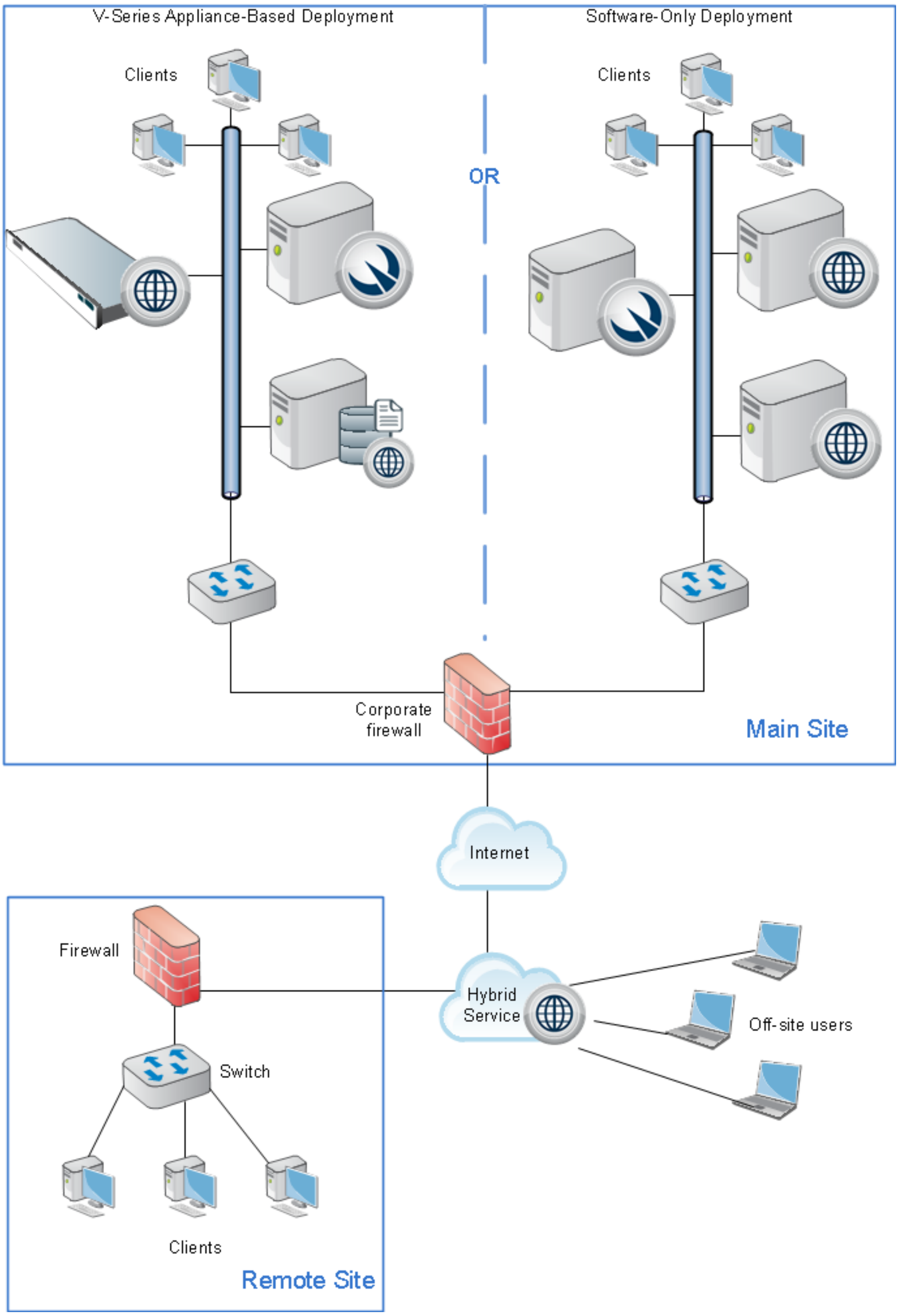
Websense Web Security Gateway adds Websense Content Gateway to the deployment, as shown below.



Optionally, off-site users (remote users outside the corporate or remote-site network) can have requests managed by 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 73.

Websense Web Security Gateway Anywhere

With Web Security Gateway Anywhere, remote site and off-site users can have their Internet requests managed by the hybrid service rather than by the Web Security 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 policy components, plus additional servers running reporting, management, and interoperability components.
- One or more Windows or Linux servers running core policy 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 Web Security Help for more information about configuring the hybrid service for off-site users.

Web Security for remote users or locations

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *Websense Web Security or Web Security Gateway*, page 82 ◆ *Websense Web Security Gateway Anywhere*, page 84

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.

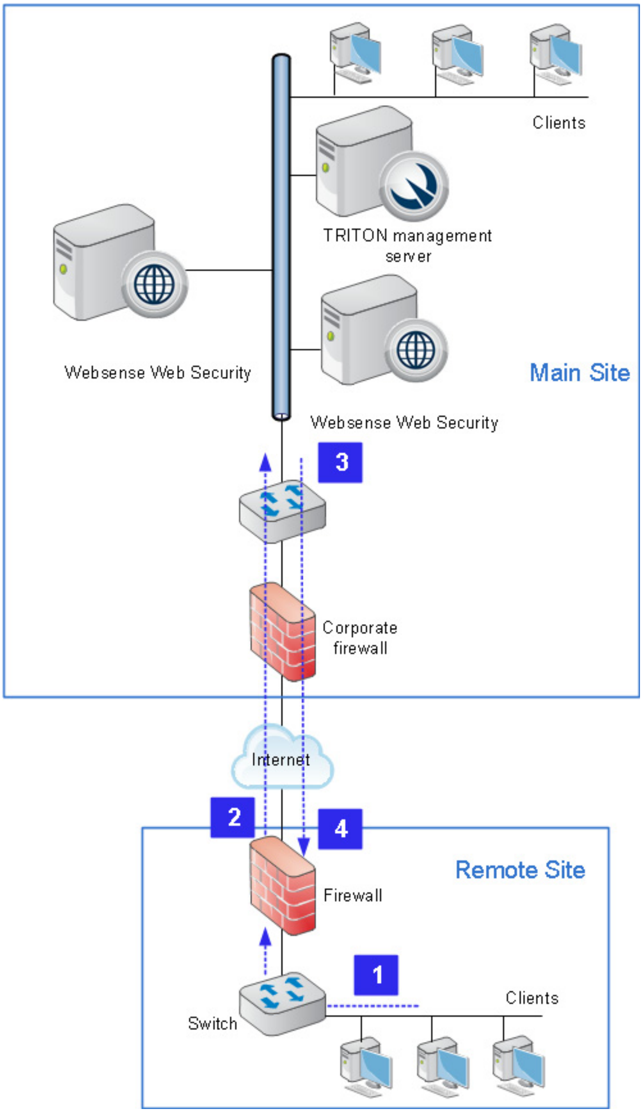
Policy enforcement is performed by the Websense components at the main site. Remote sites must be equipped with a firewall that can be integrated with Websense software (configured to check with Websense software to permit or block Web requests), or an instance of Websense Network Agent must be deployed at the remote site.

Websense, Inc., has tested this configuration in cooperation with several of its integration partners. The Partners page at websense.com links to pages that list our Security Alliance and Vendor Alliance partners.

This configuration provides distributed enterprises with Websense policy enforcement for each remote site. It also:

- Provides uniform Internet access policies at each location.
- Eliminates the cost of additional hardware to host Websense software at each remote site.
- Allows the enterprise to centrally configure, administer, and maintain a limited number of Websense Web Security machines.

The following illustration shows the basic sequence of events involved in responding to a web request from 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.

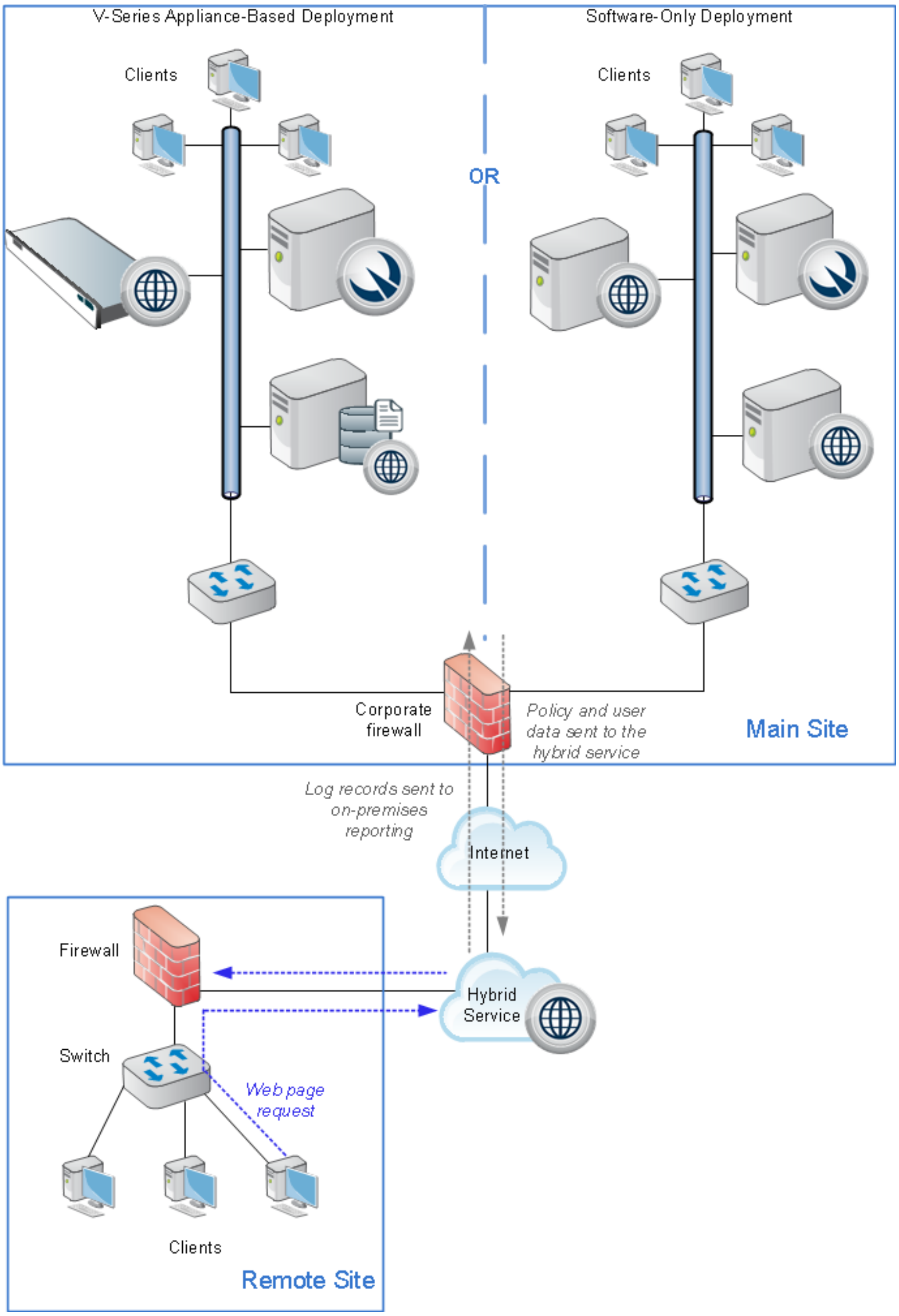
Off-site user machines (like laptops used by travelers) may be managed using Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 73.

Websense Web Security Gateway Anywhere

In a Web Security Gateway Anywhere deployment, Internet requests from remote sites can be managed 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 requests from remote sites and off-site users are managed by the nearest Websense hybrid service cluster.

The following illustration shows how remote-site Internet management works via the hybrid service. A user's web request 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 policy enforcement, 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.

Requests from off-site users may be managed by the hybrid service, or using Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 73.

Web Security distributed enterprise deployment models

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *Sites in a region*, page 86 ◆ *Expanding sites in a region*, page 88 ◆ *National or worldwide offices*, page 90

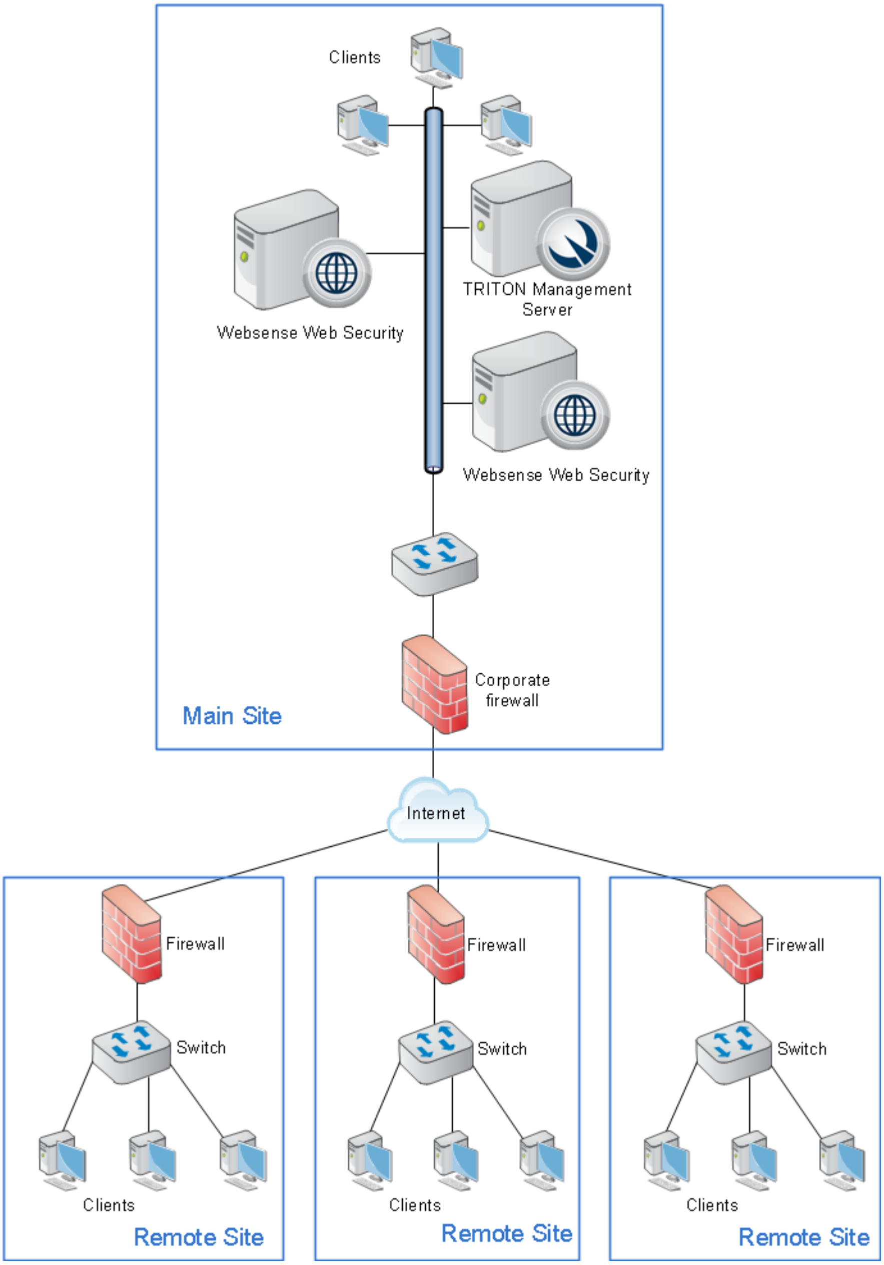
Deployment scenarios vary with different enterprise configurations. For example, an organization with 50 remote sites, all located in the same general region, deploys Websense software differently than a company with remote sites spread throughout the world. This section discusses 3 basic example models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

- *Sites in a region*, page 86: Remote sites located within one region
- *Expanding sites in a region*, page 88: Remote sites located within one region, with a growing number of employees or sites (or both)
- *National or worldwide offices*, page 90: 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 policy enforcement for all clients.



Each remote site would be managed as shown in the illustration under *Websense Web Security or Web Security Gateway*, page 82. The site at 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 handled using Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 73.

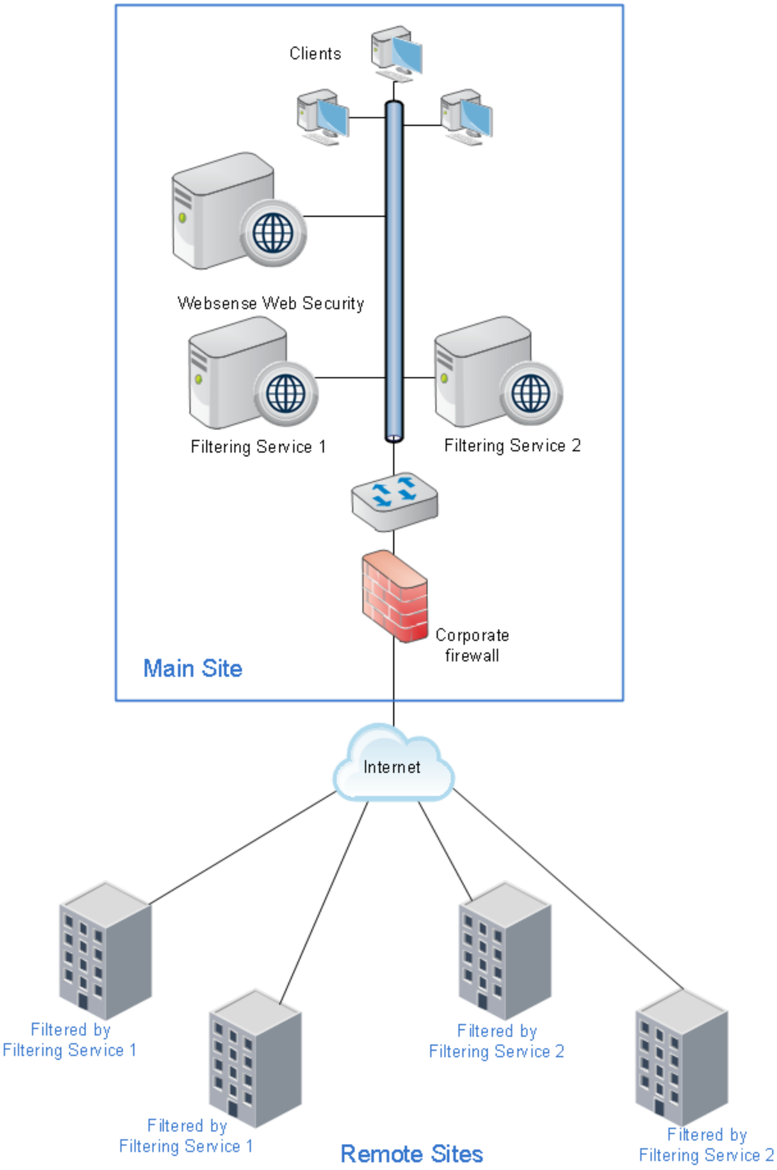
Expanding sites in a region

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 have their requests handled by Websense remote filtering software. See *Deploying Remote Filtering Server and Client*, page 73.

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.

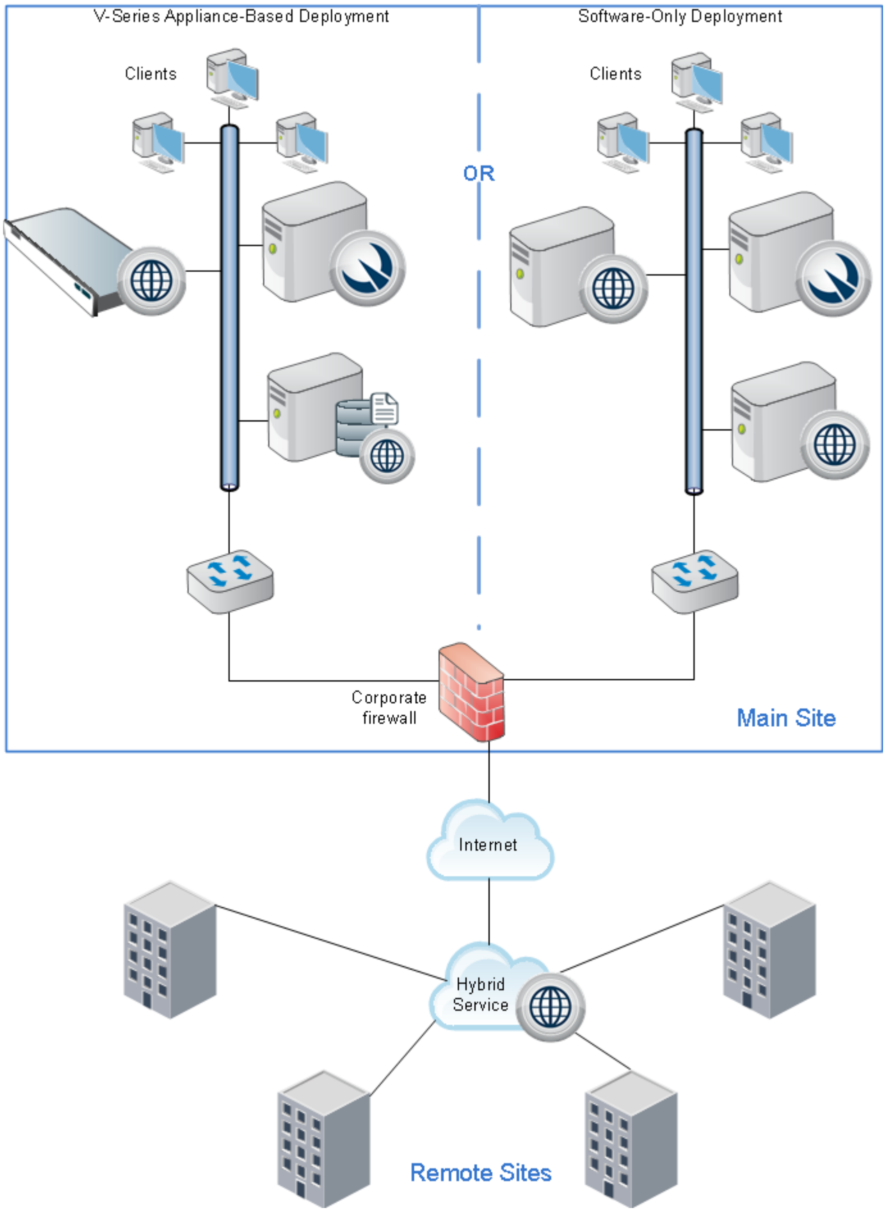
Given the significant number of variables, large organizations should contact a Websense partner or Websense Sales Engineering to plan a rollout strategy before deployment.

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

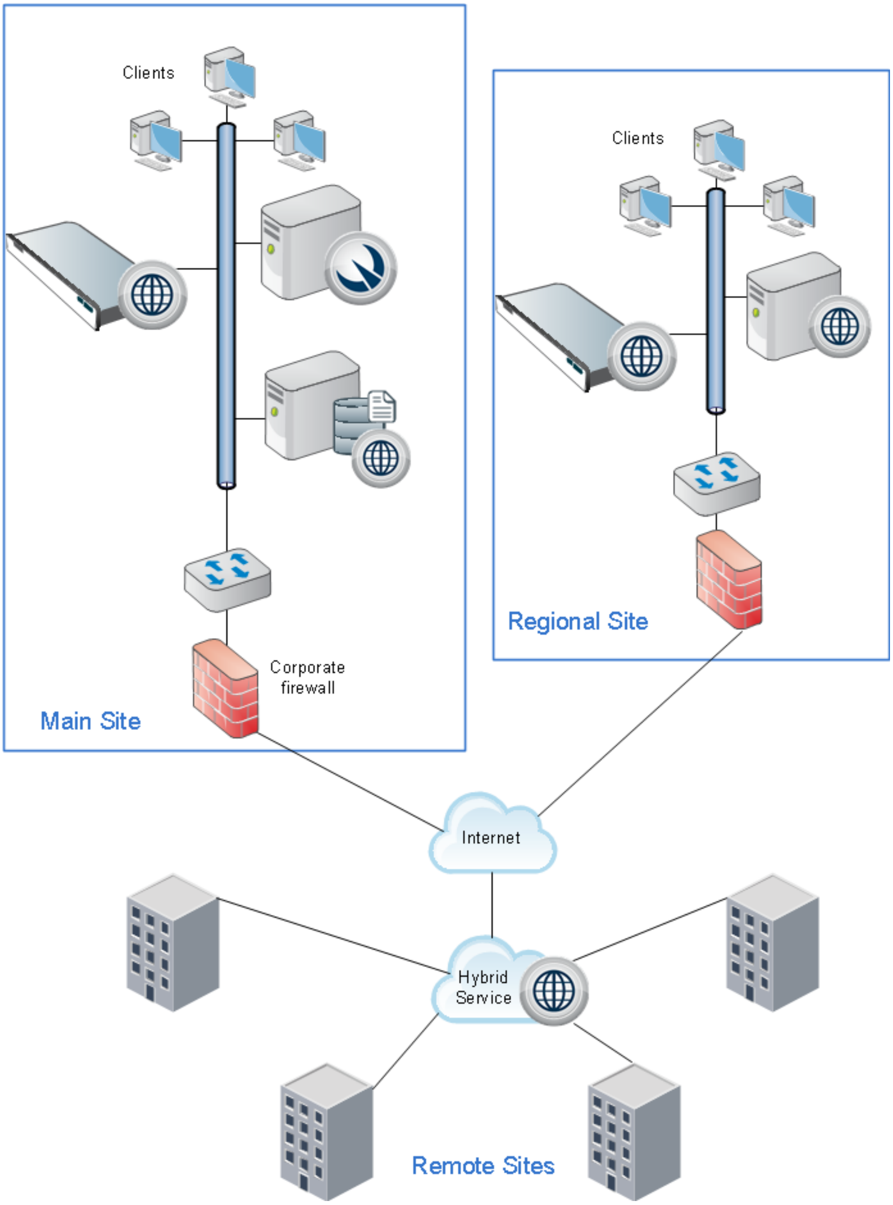
An organization with one main site (such as headquarters office or main campus) and multiple, geographically dispersed remote or branch sites can deploy Websense software at the main site (with policy enforcement for main-site users managed by the on-premises components) and have all remote sites managed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



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 73.

Multiple large sites

Organizations with multiple large sites (such as main headquarters and regional headquarters) can deploy on-premises Web Security software at the larger sites while managing 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 49, and the 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 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 73.

Web Security distributed deployments and secure VPN connections

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 63. For information about installing RADIUS Agent, see *Installing Web Security components*, page 240.

5 Content Gateway Deployment

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Security Gateway and Gateway Anywhere, v7.8.x

Content Gateway is a high-performance web proxy that provides real-time threat analysis and website 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 websites
- HTTP/S and FTP content analysis for malware and malicious threats
- Enterprise web caching capabilities

Content Gateway is a required component of Websense Web Security Gateway and 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 appliances or as software running on dedicated 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 96
- *Content Gateway explicit and transparent proxy deployments*, page 101
- *Special Content Gateway deployment scenarios*, page 106
- *Chaining Content Gateway with other proxies*, page 112

For information about deploying Web Security Gateway software, see *Web Security Deployment Recommendations*, page 33.

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

✓ **Note**

Content Gateway can be combined with F5 BIG-IP Local Traffic Manager, giving greater flexibility to your security gateway infrastructure. You can configure an integrated environment for explicit and transparent proxy in combination with a Websense appliance. For more information, see the F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway Configuration Guide.

Content Gateway deployment issues

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Security Gateway and Gateway Anywhere, v7.8.x	◆ *Proxy deployment options*, page 97 ◆ *User authentication*, page 98 ◆ *HTTPS content inspection*, page 100 ◆ *Handling special cases*, page 101

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 requests for Internet content directly to Content Gateway.

In a transparent proxy deployment, client requests for Internet content are 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 101 for more information.

Management clustering

A Content Gateway deployment can scale from a single node to multiple nodes to form a management cluster. With management clustering, all nodes in the cluster share configuration information. A configuration change on one node is automatically propagated all other nodes. Transparent proxy deployments with WCCP can disable cluster synchronization of WCCP configuration settings.

See *Clusters* in Content Gateway Manager Help for information about configuring Content Gateway clusters.

IP spoofing

By default, when communicating with origin servers Content Gateway proxies client requests substituting its own IP address. This is standard forward proxy operation.

With transparent proxy deployments, and, beginning with version 7.8.3, explicit proxy deployments, Content Gateway supports IP spoofing.

IP spoofing configures the proxy to use:

- The IP address of the client when communicating with the origin server (basic IP spoofing), or
- A specified IP address when communicating with the origin server (range-based IP spoofing)

IP spoofing is sometimes used to support upstream activities that require the client IP address or a specific IP address. It also results in origin servers seeing the client or specified IP address instead of the proxy IP address (although the proxy IP address can be a specified IP address).

IP spoofing:

- Prior to 7.8.3, is supported for transparent proxy deployments only
- When enabled, is supported and applied to both HTTP and HTTPS traffic; it cannot be configured to apply to only one protocol
- Is applied to HTTPS requests whether SSL support is enabled or not

- Relies on the ARM, which is always enabled
- Is not supported with edge devices such as a Cisco ASA or PIX firewall; When this is attempted, requests made by Content Gateway using the client IP address are looped back to Content Gateway
- Does not support IPv6.

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.

For complete information, see IP Spoofing in 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. Web Security solutions offer 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 v7.8 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 109, 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 **rule-based authentication**. Rule-based authentication uses an ordered list of rules to support multiple realm, multiple domain, and other authentication requirements. When a request is processed, the rule list is traversed top to bottom, and the first match is applied.

Authentication rules specify:

1. How to match a user.

   By:

   - IP address
   - Inbound proxy port (explicit proxy only)
   - User-Agent value
   - A combination of the above

2. The domain or ordered list of domains to authenticate against.

   With a list of domains, the first successful authentication is cached and used in subsequent authentications. If IP address caching is configured, the IP address is cached. If Cookie Mode is configured, the cookie (user) is cached.

Rule-based authentication is designed to meet several special requirements:

- **Multiple realm networks** in which domains do not share trust relationships and therefore require that each domain's members be authenticated by a domain controller within their domain. In this environment rules are created that specify:
  - Members of the realm (untrusted domain) by IP address or proxy port
  - The realm (domain) they belong to
- **Authentication when domain membership is unknown:** Some organizations do not always know what domain a user belongs to. For example, this can happen when organizations acquire new businesses and directory services are not mapped or consolidated. The unknown domain membership problem can be handled in rule-based authentication by creating a rule for IP address lists or ranges that specifies an ordered list of domains to attempt to authenticate against. The first successful authentication is remembered and used in later authentications. If

authentication is not successful or the browser times out, no authentication is performed.

- **Authentication based on User-Agent value:** One or more User-Agent values can be specified in an authentication rule. Often this is a list of browsers. When the User-Agent value matches a rule, authentication is performed against the specified domain(s). If the User-Agent value doesn't match any rule and no rule matches based on other values, no authentication is performed (this is always true in rule-based authentication; if no rule matches, no authentication is performed).

See Content Gateway user authentication in Content Gateway Manager Help for detailed information.

Web Security user identification

You can configure user identification in the Web Security manager rather than use user authentication on the proxy. Methods of user identification include Websense transparent identification agents such as Logon Agent or DC Agent, which identify users transparently. Prompted authentication can also be configured in the Web Security manager. See **User Identification** in the Web Security Help for more information.

HTTPS content inspection

When you use Content Gateway SSL support, HTTPS traffic is decrypted, inspected, and 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 support 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, or Policy Based Routing.

✓ **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 websites, individual websites, and clients for which decryption and inspection are bypassed. See SSL Decryption Bypass in Web Security Help.

Handling special cases

Any Content Gateway deployment must be able to handle web requests and web 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 Static bypass rules 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 7.8.x

Applies to:	**In this topic**
◆ Web Security Gateway and Gateway Anywhere, v7.8.x	◆ *Explicit proxy deployment*, page 101 ◆ *Transparent proxy deployment*, page 102

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 transparently 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 when troubleshooting.

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 object (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 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.

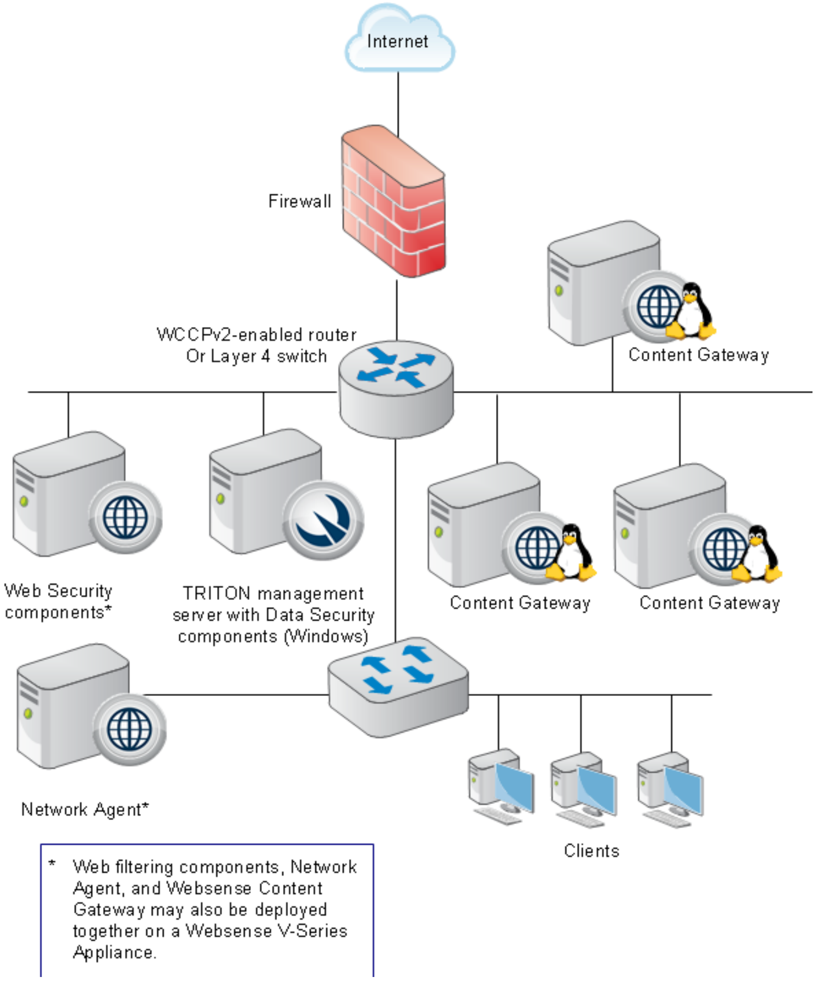
WCCP is a protocol used to route client request traffic to a specific proxy. A WCCP-enabled router can distribute client requests based on the proxy server's IP address, routing traffic to the proxy most likely to contain the requested information.

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).

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 7.8.x

Applies to:	In this topic
◆ Web Security Gateway and Gateway Anywhere, v7.8.x	

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.

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

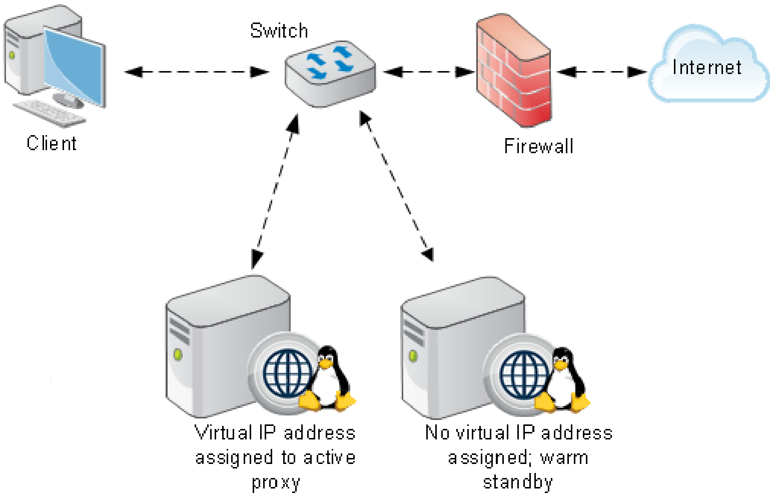
As previously mentioned for the explicit proxy deployment, clients are specifically configured to send requests directly to a proxy. The configuration can be accomplished manually, or via a PAC file or a WPAD server.

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

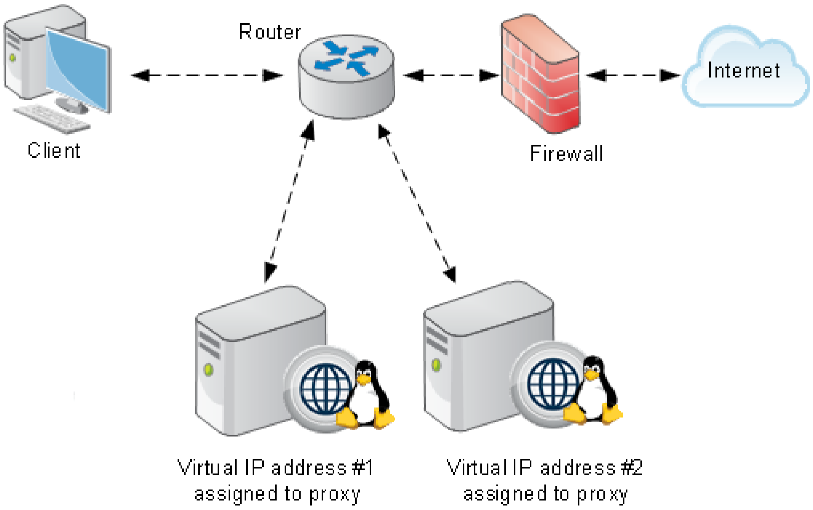
Active/Active

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.

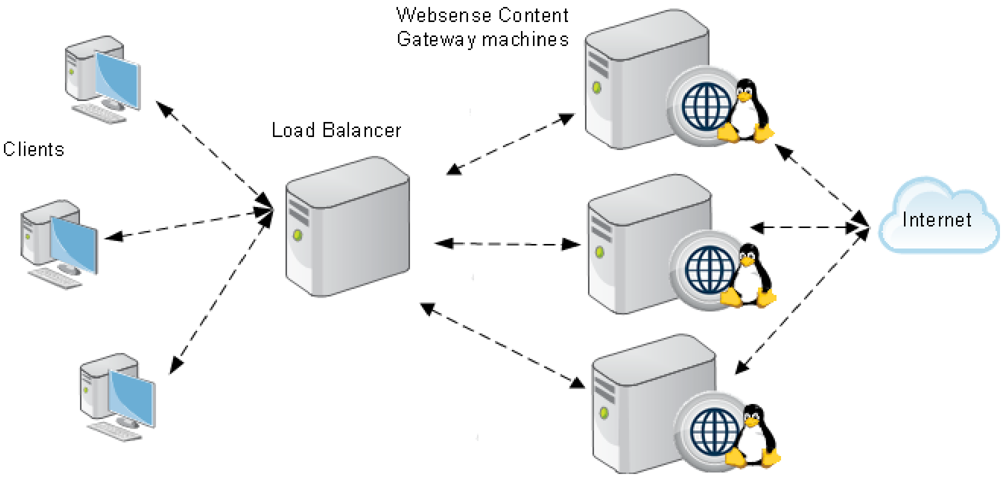


With load balancing

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.

Integrated Windows Authentication is supported with a load balancer beginning with v7.8.2. Follow the specific steps outlined in Content Gateway Help to successfully configure IWA with a load balancer.



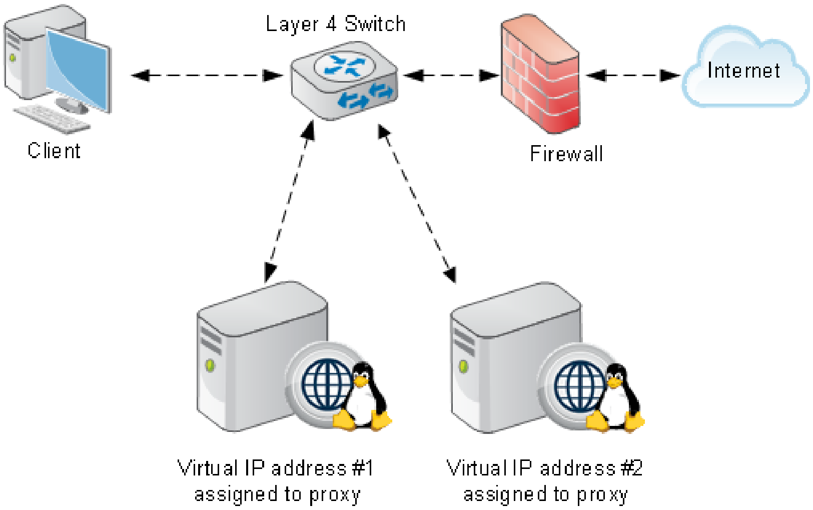
Using transparent proxy

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.


Layer 4 Switch
Client
Firewall
Internet
Virtual IP address #1 assigned to proxy
Virtual IP address #2 assigned to proxy

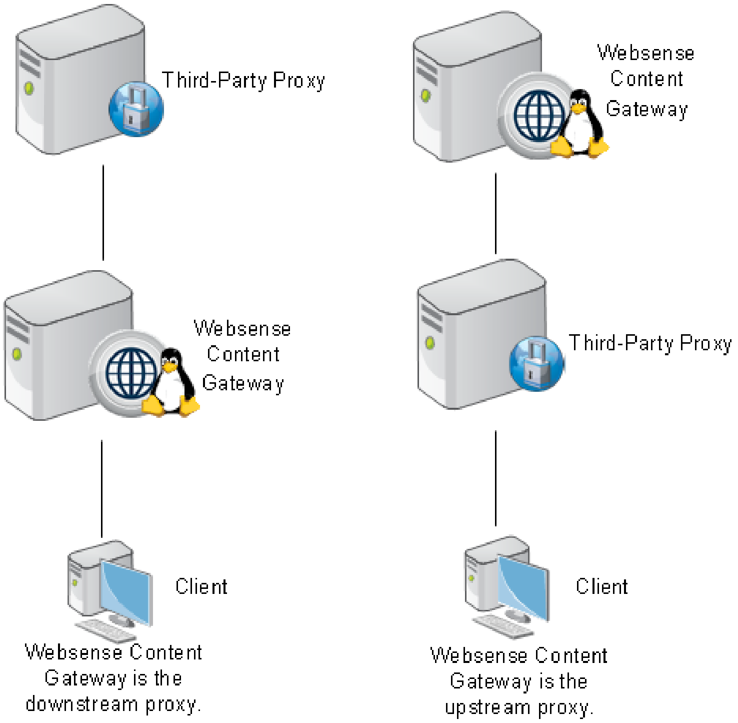
Using a WCCPv2-enabled router

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 112, for specific instructions on using Blue Coat® ProxySG® or Microsoft® Forefront® Threat Management Gateway 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 63, and *Installing Web Security components*, page 239.

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 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 on the Content Gateway Configure page (**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 63, and *Installing Web Security components*, page 239.

Websense Content Gateway can be configured to read authentication from the following proxies in the downstream position:

Blue Coat ProxySG	210 and later
Microsoft Forefront TMG	MBE and later

For detailed configuration instructions for Blue Coat ProxySG and Microsoft TMG server, see *Chaining Content Gateway with other proxies*, page 112.

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 *Hierarchical Caching* in Content Gateway Manager Help.

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 7.8.x

Applies to:	In this topic
◆ Web Security Gateway and Gateway Anywhere, v7.8.x	◆ *In a proxy chain*, page 109 ◆ *Microsoft Forefront Threat Management Gateway (TMG)*, page 114

Blue Coat ProxySG

You can configure the Blue Coat proxy to send X-Forwarded-For and X-Authenticated-User headers for 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 Forefront Threat Management Gateway (TMG)

Microsoft Forefront TMG can be used as a downstream proxy from 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 Forefront TMG.

The **Websense-AuthForward.TMG_Plugin-64.zip** file is available on the MyWebsense Downloads page.

1. Log on to your MyWebsense account.
2. Select the **Downloads** tab.
3. Select Websense Web Security Gateway from the **Product** drop-down list.
4. In the list, expand **TMG 64-bit plugin...** to see the download details. Click the **download** link to start the download.

Install a plug-in:

1. Unzip the package and copy the following files to the Forefront TMG installation directory:
   - Websense-AuthForward.dll
   - msvcp110.dll
   - msvcr110.dll
2. Register the plug-in with the system. Open a Windows command prompt and change directory to the Forefront TMG installation directory.

   From the command prompt, type:

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

3. Verify the plug-in was registered in the Forefront TMG management user interface (**Start > Programs > Microsoft Forefront TMG > Microsoft Forefront TMG Management**). In the System section, select **Add-ins**, then click the **Web-filter** tab. The **WsAuthForward** plug-in should be listed.

To uninstall the plug-in, in Forefront TMG installation directory run the following command in a Windows command prompt.

```
regsvr32 /u Websense-AuthForward.dll
```

6 Planning Data Security Deployment

Deployment and Installation Center | Data Security Solutions | Version 7.8.x

Plan Data Security Solutions

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.

The Data Security Deployment Guide guide helps you plan your deployment, integrate it with existing infrastructure such as shared drives, user directory servers, and Exchange servers, and design for scalability.

7 Email Security Gateway Deployment

Deployment and Installation Center | Email Security Solutions | Version 7.8.x

Plan Email Security Solutions

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 appliance (V10000 G2, V10000 G3, V5000 G2, or X10G). Email Security management functions reside on a separate Windows server in the TRITON® Unified Security Center (TRITON console).

Email Security Gateway may also be deployed on a virtual appliance using a VMware platform (ESXi v4.0 or later). The appliance image is available for download from MyWebsense in an open virtualization format (OVF) package. A TRITON manager installed on a separate Windows machine is required for Email Security Gateway administration functions in this deployment. A virtual appliance may not be clustered with a V- or X-Series appliance. See the virtual appliance Quick Start Guide for deployment and configuration information.

Each email message is processed by a robust set of analytics to prevent malicious threats from entering a network. Custom content filters allow Email Security to analyze messages based on administrator-specified message attribute conditions. Commercial bulk email analysis can determine whether a message has been sent from a third-party bulk email management company or directly from a business. 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 threats.

Enhance your security by adding Websense ThreatScope, a set of cloud-based functions, to your Email Security Gateway Anywhere subscription:

- URL sandboxing
- File sandboxing
- Phishing detection

URL sandboxing provides real-time analysis of uncategorized URLs that are embedded in Email Security Gateway inbound mail. File sandboxing inspects email attachment file types that commonly contain security threats (including .exe, .pdf, .xls, .xlsx, .doc, .docx, .ppt, .pptx, and archive files). Phishing detection and education provides cloud-based analysis of an inbound message for phishing email characteristics. Options for handling suspected phishing mail include blocking the delivery or replacing the mail with a phishing education message. See Email Security Gateway Help for details.

Integration with Data Security provides valuable data loss protection (DLP) features to protect an organization's most sensitive data and facilitate message encryption. Policies configured in the Data Security manager 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.

If your network includes Websense Web Security, you can also use its URL analysis function. Email Security Gateway queries the Websense URL category master database and determines the risk level of a URL found in an email message.

Logging and reporting capabilities allow an organization to view system and message status and generate reports of system and email traffic activity.

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 121
- *Single-appliance deployments*, page 123
- *Multiple-appliance deployments*, page 126

The sample diagrams in this guide show Websense appliances running in Email Security only mode. See Installing Web Security and Email Security appliance-based solutions to view diagrams of an appliance running in dual Email Security Gateway/Web Security mode.

See the following topics for Email Security Gateway installation information:

- Installing Email Security appliance-based solutions
- Installing Email Security management components
- X-Series Chassis Getting Started Guide
- Using the X-Series Command Line Interface (CLI)

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

- Upgrading Email Security Gateway Solutions

- Upgrading the TRITON management server

System requirements

Deployment and Installation Center | Email Security Solutions | Version 7.8.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.8.x

To view complete hardware, software, and Web browser requirements for Email Security Gateway, see System requirements for this version.

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

In the DMZ

- Websense appliance (V10000 G2, V10000 G3, V5000 G2, or X10G), 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 or 2012 machine
- Email Security Log Server
- Email Security Log Database (Microsoft® SQL Server® 2008, 2008 R2, 2012, 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 appliance and any router, switch, or load balancer adjacent to the firewall are located in the DMZ.

Websense appliances

The Websense V10000 G2, V10000 G3, or X10G 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 or V10000 G3 appliance with either Web Security or Web Security Gateway.

Email Security Gateway can occupy individual blade servers on an X10G appliance. The X-Series chassis may include a combination of Email Security and Web Security blade servers.

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.

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, although this component can also be installed on a separate machine. The log server passes information to the SQL Server reporting database (Email Security Log Database) for use in generating dashboard charts and reports, messages, and Message Log data.

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 or on a dedicated server. For optimal performance, Websense recommends that a full SQL Server (2008, 2008 R2, or 2012) be installed on a separate machine. (SQL Server Express, which can be installed as part of the TRITON console installation, is recommended only for evaluation purposes.) 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 administrator can determine:

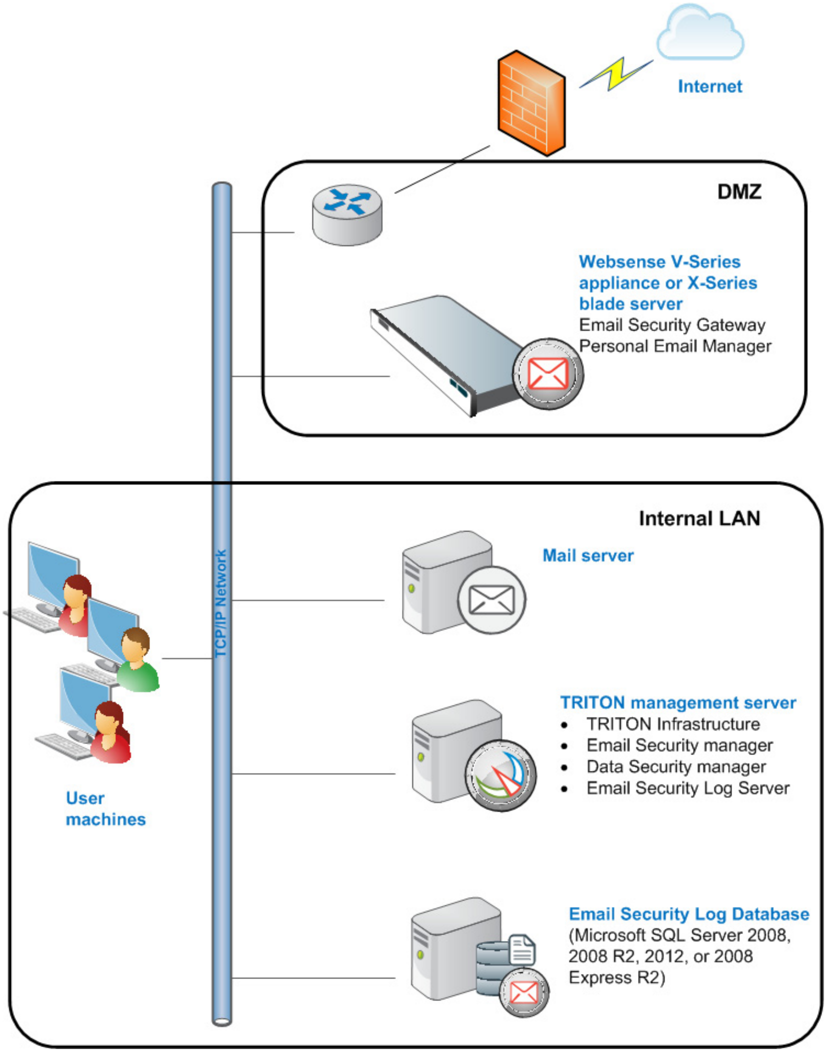
- Which end users can access the Personal Email Manager utility and which actions, if any, those users are allowed to perform on blocked messages
- What the blocked email notification message contains
- Which end users are allowed to manage personal Always Block and Always Permit lists
- Whether a user can manage multiple email accounts
- Whether a user can delegate email account management responsibilities to another individual

Single-appliance deployments

Deployment and Installation Center | Email Security Solutions | Version 7.8.x

Applies to:	In this topic
• Email Security Gateway and Email Security Gateway Anywhere, v7.8.x	• *Email Security Gateway single appliance* • *Email Security Gateway Anywhere single appliance*

Email Security Gateway single appliance



A simple Email Security Gateway deployment uses a single V-Series appliance (V10000 G2, V10000 G3, or V5000 G2) or a single X10G blade server. In this installation, all email analysis occurs in the Email Security Gateway on-premises component using a robust collection of threat detection tools (**Main** > **Policy Management** > **Filters**). The Personal Email Manager facility on the appliance allows end users to manage blocked messages.

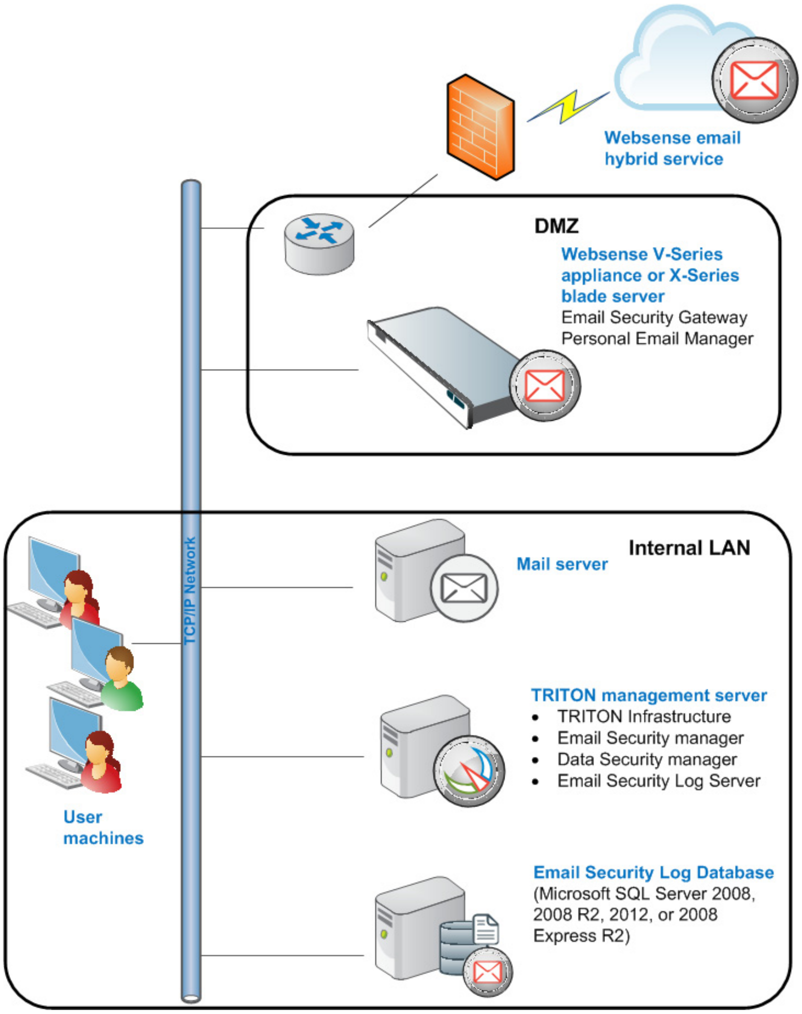
In this scenario, Email Security Log Server is installed on the same machine as the TRITON console. It can be installed on a separate machine if desired.

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

See the *Data Security Manager Help* for details about DLP policy settings. See the following *Email Security Manager 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



A simple Email Security Gateway Anywhere deployment uses a single V-Series appliance (V10000 G2, V10000 G3, or V5000 G2) or a single X10G blade server. 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, virus, and commercial bulk email detection information by writing extended headers in the mail it sends to Email Security Gateway. The additional header information includes a threat 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 *Email Security Manager 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 7.8.x

Applies to:	In this topic
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x	- *Email Security Gateway Anywhere appliance cluster* - *Multiple standalone appliances*

Multiple 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 V10000 G2, V10000 G3, or V5000 G2 machines. An appliance cluster usually cannot contain a mix of appliance platforms. However, a V10000 G2 appliance may be deployed in a cluster with a V10000 G3 appliance. Contact Websense Technical Support for more information.

An X-Series modular chassis may include multiple blade servers running Email Security Gateway.

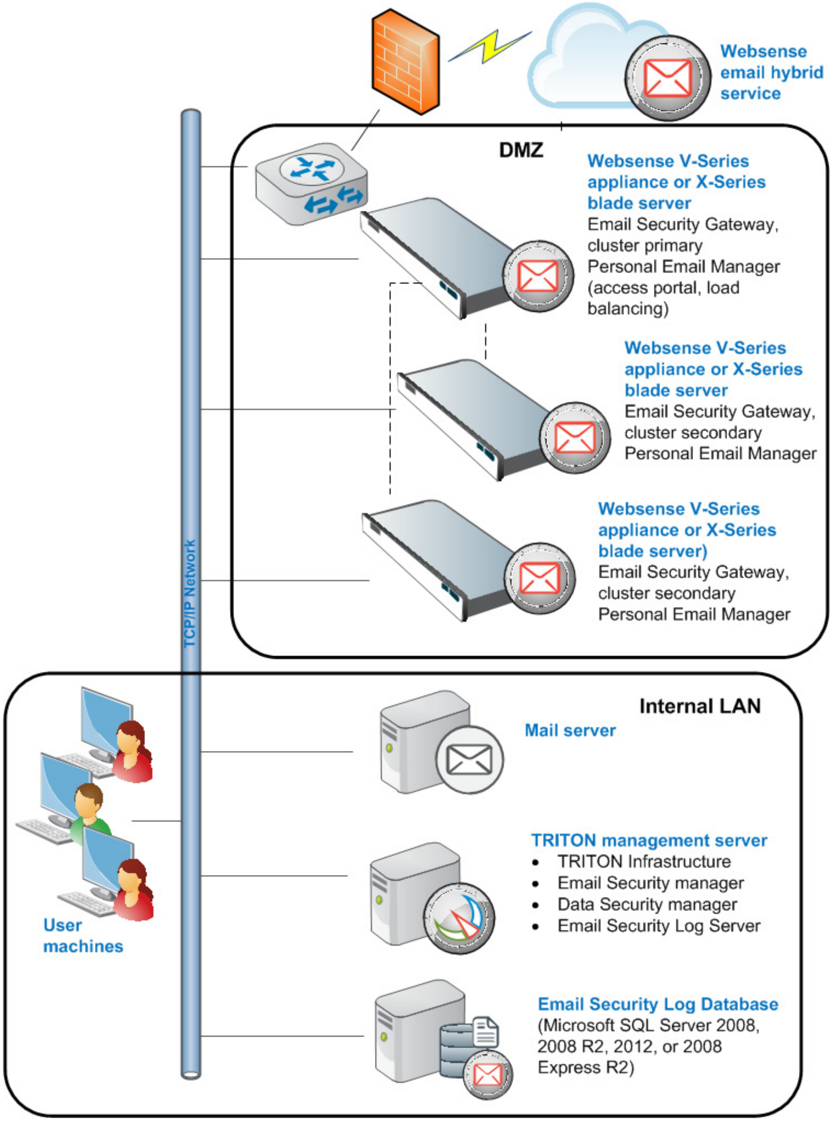
Email Security Gateway Anywhere appliance cluster

Multiple V-Series appliances are configured in Email Security Gateway Anywhere as a cluster for this deployment scenario. You may also consider multiple X10G blade servers for this scenario. This Email Security Gateway Anywhere environment includes the Email Security hybrid service "in the cloud" filtering. See *Email Security Gateway Anywhere single appliance*, page 125, for information about the email hybrid service.

You may want to use a third-party load balancer with a V-Series 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 [Email Security Gateway Manager Help]() for details.


Websense email hybrid service
DMZ
Websense V-Series appliance or X-Series blade server
Email Security Gateway, cluster primary
Personal Email Manager (access portal, load balancing)
Websense V-Series appliance or X-Series blade server
Email Security Gateway, cluster secondary
Personal Email Manager
Websense V-Series appliance or X-Series blade server)
Email Security Gateway, cluster secondary
Personal Email Manager
TCP/IP Network
Internal LAN
Mail server
User machines
TRITON management server
TRITON Infrastructure
Email Security manager
Data Security manager
Email Security Log Server
Email Security Log Database
(Microsoft SQL Server 2008, 2008 R2, 2012, 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.

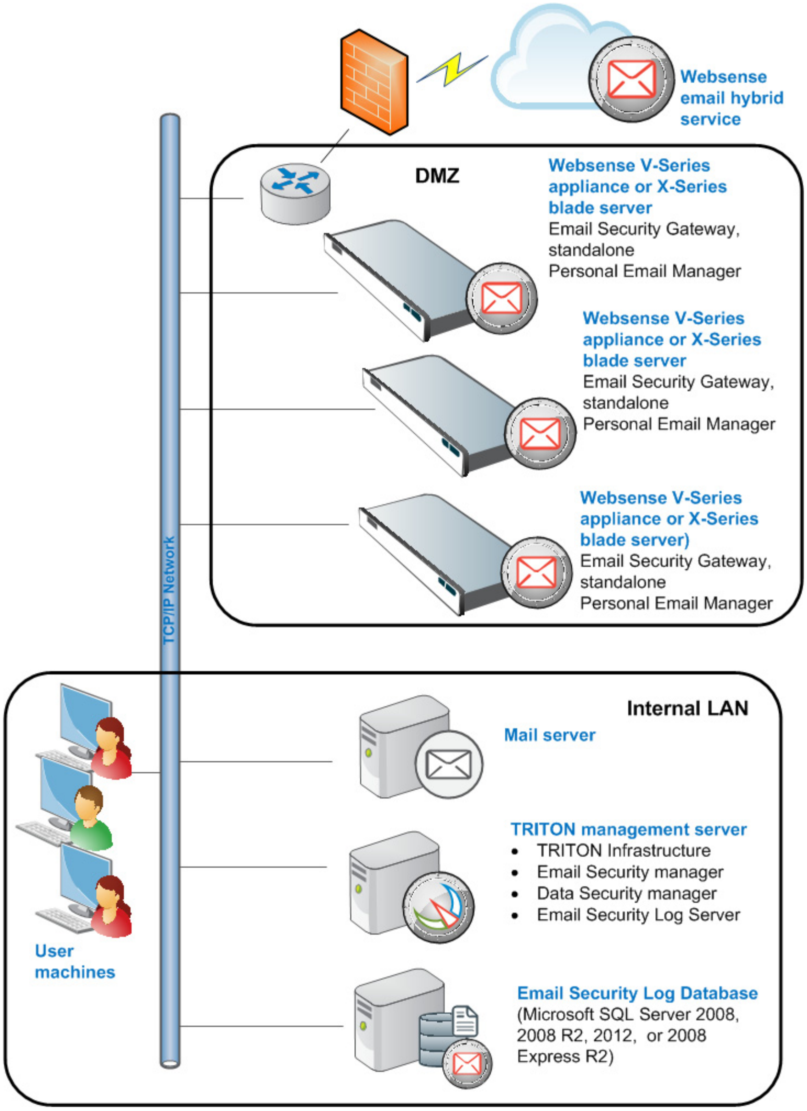
Message queue records may be lost if this step is not performed before cluster creation.

Multiple standalone appliances

A multiple standalone V-Series appliance or X-Series blade server deployment might be useful if each appliance must have different configuration settings. Two standalone scenarios are described in this section:

- *Using domain-based routing*, page 130
- *Using DNS round robin*, page 131

These Email Security Gateway Anywhere environments include the Email Security hybrid service "in the cloud" filtering. See *Email Security Gateway Anywhere single appliance*, page 125, for information about the email hybrid service.


Websense email hybrid service
DMZ
Websense V-Series appliance or X-Series blade server
Email Security Gateway, standalone
Personal Email Manager
Websense V-Series appliance or X-Series blade server
Email Security Gateway, standalone
Personal Email Manager
Websense V-Series appliance or X-Series blade server)
Email Security Gateway, standalone
Personal Email Manager
TCP/IP Network
Internal LAN
Mail server
TRITON management server
• TRITON Infrastructure
• Email Security manager
• Data Security manager
• Email Security Log Server
User machines
Email Security Log Database
(Microsoft SQL Server 2008, 2008 R2, 2012, 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. Configuring a delivery preference for each SMTP server facilitates message routing.

Configure the domain groups for which you want to define delivery routes in the **Settings > Users > Domain Groups > Add Domain Groups** page. See the *Email Security Gateway Manager 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 to open the SMTP Server List:
   a. Click **Add** to open the Add SMTP Server dialog box.
   b. Enter the SMTP server IP address or host name and port.

c. Mark the **Enable MX lookup** check box to enable the MX lookup function.

> **Important**
>
> If you entered an IP address in the previous step, the MX lookup option is not available.
>
> If you entered a host name in the previous step, this option is available.
>
> ◆ Mark the **Enable MX lookup** check box for message delivery based on the host name MX record.
>
> ◆ If you do not mark this check box, message delivery is based on the host name A record.

d. Enter a preference number for this server (from 1 - 65535; default value is 5).

If a single route has multiple defined server addresses, Email Security attempts to deliver mail in order of server preference. When multiple routes have the same preference, round robin delivery is used.

You may enter no more than 16 addresses in the SMTP Server List.

6. Select any desired security delivery options.

a. Select **Use Transport Layer Security (TLS)** if you want email traffic to use opportunistic TLS protocol.

b. Select **Require authentication** when you want users to supply credentials. Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method when you want users to authenticate.

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.

8 Installing TRITON Enterprise

Deployment and Installation Center | Web, Data, and Email Security Solutions 7.8.x

Install TRITON® Enterprise Solutions

If you have more than one Websense TRITON security solution, use the sections below to find the appropriate set of installation instructions.

Websense TRITON Enterprise

If you are combining a web, data, and email solution, see the Websense TRITON Enterprise Installation Guide. This document guides you through:

- Preparing for a TRITON Enterprise deployment
- Installing the Web Security policy source and the TRITON management server
- Installing further recommended Web Security, Data Security, and Email Security Gateway components
- Initial web, data, and email configuration

After completing those steps, see Installing Data Security Servers and Agents for instructions on installing additional components, like the protector and agents.

Web Security and Data Security

If you are combining a Web Security and a Data Security solution, in most cases, the best process is to first complete the steps in Installation Instructions: Web Security Gateway Anywhere. This document guides you through installation of:

- All Web Security Gateway Anywhere components
- Data Security Management Server components (which reside on the TRITON management server)

After completing those steps, see Installing Data Security Servers and Agents for instructions on installing additional components, like the protector and agents.

Web Security and Email Security

If you are combining a Web Security and an Email Security Gateway solution, in most cases, the best process is to follow the steps in the Websense TRITON Enterprise Installation Guide. This document guides you through installation of:

- All Web Security Gateway Anywhere components
- All Email Security Gateway Anywhere components
- Data Security Management Server components (which enable the Web DLP features of Web Security Gateway Anywhere, if purchased, and the Email DLP features of Email Security Gateway)

Email Security and Data Security

If you are combining an Email Security Gateway and a Data Security solution, in most cases, the best process is to follow the steps in the Email Security Gateway installation guide. This document guides you through installation of:

- All Email Security Gateway Anywhere components
- Data Security Management Server components (which reside on the TRITON management server)

After completing those steps, see Installing Data Security Servers and Agents for instructions on installing additional components, like the protector and agents.

Creating a TRITON Management Server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:	In this topic
- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x - Data Security, v7.8.x - Email Security Gateway (Anywhere), v7.8.x	- *Installing the TRITON Unified Security Center*, page 135

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

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 4).

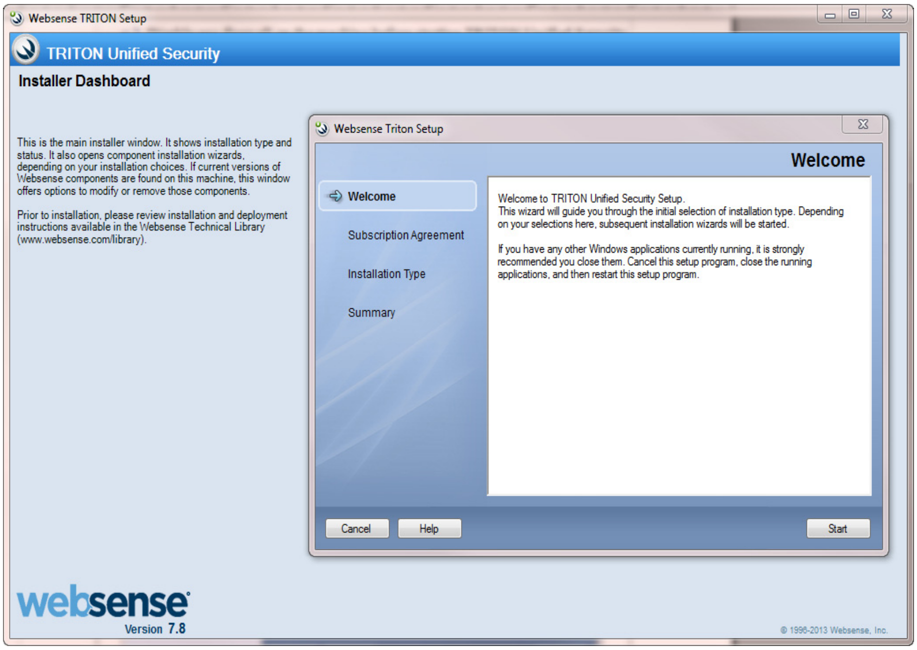
Typically, there is only one TRITON management server in a deployment. It serves as the central point for management, configuration, and reporting.

Installing the TRITON Unified Security Center

1. Double-click the installer file to launch the Websense TRITON Setup program.

   A progress dialog box appears, as files are extracted.

2. 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 installation choices. If current versions of Websense components are found on this machine, this window offers options to modify or remove those components.

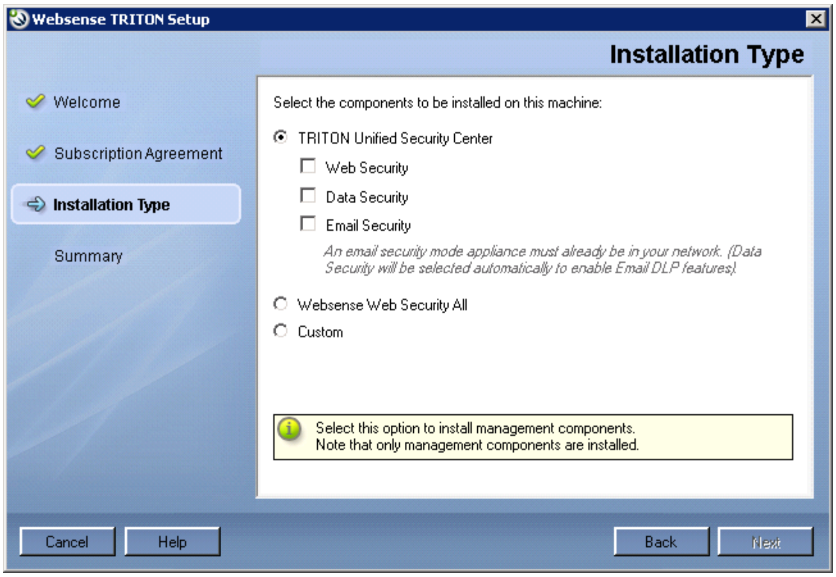
Prior to installation, please review installation and deployment instructions available in the Websense Technical Library (www.websense.com/library).

Welcome to TRITON Unified Security Setup.
This 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 strongly recommended you close them. Cancel this setup program, close the running applications, and then restart this setup program.

3. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.

4. On the **Installation Type** screen, select **TRITON Unified Security Center** and the modules you want to install (Web Security, Data Security, and Email Security).



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.

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, an instance of Policy Broker and Policy Server must be already installed and running (see *Installing components via the Custom option*, page 231). You are prompted for the Policy Server IP address during console installation.

In appliance-based deployments, Policy Broker and Policy Server reside 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 console installation.

The appliance E1 (and E2, if used) interface must also be configured in the Appliance manager before you install Email Security management components.

5. On the **Summary** screen, click **Next** to continue the installation.
6. TRITON Infrastructure Setup launches.

   Follow the instructions in *Installing TRITON Infrastructure*, page 234.

7. When you click **Finish** in TRITON Infrastructure Setup, component installers for each module selected in the Module Selection screen (Step 4), are launched in succession.

   Only the component installers for the modules you have selected are launched. For example, if you select only Web Security and Data Security, the Email Security installer is not launched.

8. 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 Web Security management components*
   - *Installing Data Security management components*
   - *Installing Email Security management components*

Installing Web Security management components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- ◆ Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x
- ◆ Data Security, v7.8.x
- ◆ Email Security Gateway (Anywhere), v7.8.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 **full policy source** Web Security appliance, Policy Broker and Policy Server reside there. For instructions on installing these components, see *Installing Web Security components*, page 240.

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 134.
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:
   - Web Security manager (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.

✓ **Note**

Although Sync Service and the Web Security Log Server may be installed on the TRITON management server, they consume considerable system resources. For TRITON Enterprise deployments, it is recommended to install these components on another machine.

- Select Linking Service if your subscription includes both a Web Security solution and Data Security.

Important

Filtering Service must be installed in your network before you install Linking Service. In an appliance-based deployment, Filtering Service is installed on all Web Security appliances (full policy source, user directory and filtering, and filtering only). In a software-based deployment, it is recommended that you install Filtering Service with Policy Broker and Policy Server on another separate machine from the TRITON management server, as Filtering Service can consume considerable system resources and may have a performance impact on the TRITON management server. Large or distributed environments may include multiple Filtering Service instances.

You can return to the TRITON management server at a later time and install Linking Service if required.

- Real-Time Monitor is installed by default on the TRITON management server. Because one Real-Time Monitor instance can monitor multiple Policy Servers, additional instances are not usually required. If you install additional instances, you may have a maximum of one per Policy Server.
- Select Policy Broker and Policy Server if these components have not already been installed in your deployment. They are required to install the Web Security manager. If you have a **full policy source** appliance, these components are already installed.

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 Data Security management components

Deployment and Installation Center | Data Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x
- Data Security, v7.8.x
- Email Security Gateway (Anywhere), v7.8.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 134.
2. When the Websense Data Security Installer is launched, a **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. 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**
>
> 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
```

7. In the **Installation Confirmation** screen, click **Install** to begin installation of Data Security components.
8. If the following message appears, click **Yes** to continue the installation:

   Data Security needs port 80 free.
   In order to proceed with this installation, DSS will free up this port.
   Click Yes to proceed OR click No to preserve your settings.

   Clicking **No** cancels the installation.

   A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.
9. The **Installation** progress screen appears. Wait for the installation to complete.
10. When the **Installation Complete** screen appears, click **Finish** to close the Data Security installer.
11. If no other TRITON Unified Security Center module is chosen for installation, you are returned to the Modify Installation dashboard. Installation is complete.

    Otherwise, you are returned to the Installer Dashboard and the next component installer is launched.

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 Agents and Servers.

Installing Email Security management components

Deployment and Installation Center | Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x
- Data Security, v7.8.x
- Email Security Gateway (Anywhere), v7.8.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 Email Security manager), 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 134.
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**.

   Email Security manager (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 the Email Security module on this screen, TRITON Infrastructure was not detected by the Email Security Installer. TRITON Infrastructure must be installed already to be able to install Email Security management components.

   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 4, 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 the TRITON console. 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 260).

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 SQL authentication.

5. On the **Email Security Database File Location** screen, specify where Email Security database files should be located and then click **Next**.

   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 can specify a directory that already exists, or you can create a new directory via the browse function.

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** or **E** (E1 or E2) 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). Resolve this issue in 1 of the following ways:
    - Reset the subscription key on the appliance.
    - If the **Appliance network communication** popup message appears, click **OK** and enter your subscription key in the appropriate entry field.
- 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 (Email Security manager 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 your settings for 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.

9 Installing Web Security solutions

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Install Web Security Solutions

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x

For a PDF with start-to-finish instructions for a typical installation, see:

- Installation Instructions: Web Security Gateway Anywhere
- Installation Instructions: Web Security Gateway
- Installation Instructions: Web Security or Web Filter

To perform a simple, one-machine installation of a Web Security solution on a supported Windows server (for example, for evaluation), see *Installing via the Web Security All option*.

Installing via the Web Security All option

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x

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

1. Download or copy the TRITON Unified Installer (the Windows installer) to this machine. The installer is available from mywebsense.com, and the installer file is **WebsenseTRITON784Setup.exe**.
2. Double-click the installer file to launch the Websense TRITON Setup program. 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**.

   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. On the TRITON Infrastructure Setup Welcome screen, click **Next**.
8. On the Installation Directory screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.
   - To accept the default location (recommended), simply click **Next**.
   - To specify a different location, click **Browse**.

   Important

   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.
9. On the SQL Server screen, select **Use existing SQL Server on another machine**, then specify the location and connection credentials for a database server located elsewhere in the network.
   a. Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any, and the **Port** to use for SQL Server communication.

      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.
   b. Specify whether to use **SQL Server Authentication** (a SQL Server account) or **Windows Authentication** (a Windows trusted connection), then provide the **User Name** or **Account** and its **Password**.

      If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web Security manager. See Configuring Websense Apache services to use a trusted connection.
   c. Click **Next**. The installer verifies the connection to the database engine. 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.

10. 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.

      Administrators will use this address to access the TRITON console (via a web browser), and Websense component on other machines will use the address to connect to the TRITON management server.

    - Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and TRITON Unified Security Center. The 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.

11. 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 on screen.

12. 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.

13. On the Pre-Installation Summary screen, verify the information and then click **Next** to begin the installation.
14. The Installation screen appears, showing installation progress. Wait until all files have been installed.

    If the following message appears, check to see if 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.
15. On the Installation Complete screen, click **Finish**.

    You are returned to the Installer Dashboard and, after a few seconds, the Web Security component installer launches.
16. If the **Multiple Network Interfaces** screen appears, select the NIC that Websense components should use to communicate with Websense components on other machines, then click **Next**. (Prior to 7.8.2, this screen appears later in this sequence.)
17. On the **Policy Broker Replication** screen, indicate which Policy Broker mode to use. If you are not sure about which Policy Broker mode to choose, see Managing Policy Broker Replication.
18. On the **Active Directory** screen, specify whether your network uses Windows Active Directory, then click **Next**.
19. If you are using Active Directory, the **Computer Browser** screen may appear. Click **Next** to have the installer attempt to start the service.

    If the installer is unable to start the service, you must start it after installation.
20. On the **Integration Option** screen, indicate whether to install your Web Security software in standalone or integrated mode, then click **Next**.
    - If you have Web Security Gateway or Gateway Anywhere, select the **integrated** option.
    - If you aren't sure what to select, see *Understanding Web Security standalone and integrated modes*, page 45.
21. 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, then click **Next**.
22. On the **Network Card Selection** screen, select the network interface card (NIC) that Network Agent should use to monitor Internet activity, then click **Next**.

    For more information, see *Deployment guidelines for Network Agent*, page 66.
23. If the machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components. Follow the on-screen prompts to complete this process.

24. On the **Log Database Location** screen, specify a location (directory path) for the Websense Log Database, then click **Next**.
25. On the **Optimize Log Database Size** screen, select options for optimizing the size of log database records, then click **Next**.
    - When **Log Web page visits** is selected (default), one record (or a few records) is created with combined hits and bandwidth data for each web page requested, rather than a record for each separate file included in the request. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities.
    - When **Consolidate requests** is selected, Internet requests that share the same value for domain name, category, keyword, action (like permit or block) and user/IP address, within a certain interval of time (1 minute, by default), are combined.
26. On the **Filtering Feedback** screen, choose whether to send categorization feedback to Websense, Inc., then click **Next**.
27. On the **Web Security Gateway Anywhere Components** screen, indicate whether to install Sync Service and Directory Agent, then click **Next**. These services are only used if you have a Web Security Gateway Anywhere key.
28. 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 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 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.

29. On the **Directory Service Access** screen, supply a local and domain administrator account with directory service access permissions.
30. 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 policies on these remote users without prompting for logon information.
31. On the **Pre-Installation Summary** screen, verify the information shown.

    The summary shows the installation path and size, and the components to be installed.
32. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
33. On the **Installation Complete** screen, click **Done**.

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

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- V10000 G3, V10000 G2, and V5000 G2, v7.8.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 and Policy Server on the machine that will become the TRITON management server. See *Installing Web Security components*, page 240.
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. Install management components (including the Web Security or the Web Security and Data Security modules of the TRITON console) on the Policy Broker machine to create the TRITON management server.

   If you are installing Web Security Gateway Anywhere, also install Linking Service on the management server machine.

   See *Creating a TRITON Management Server*, page 134.

Install reporting and other off-appliance components as necessary. See *Installing Web Security components*, page 240.

10 Installing Web Security Components on Linux

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x

Use the Web Security Linux installer to install supported components on a Linux machine.

Complete installation instructions for installing Web Security solutions (which include steps for Linux, Windows, and appliance installations) are available here:

- Installation Instructions: Web Security Gateway Anywhere
- Installation Instructions: Web Security Gateway
- Installation Instructions: Web Security or Web Filter

If you want to install all Linux-compatible Web Security components (except for Remote Filtering Server) on this machine, you can instead use the following instructions:

1. *Starting the Web Security Linux installer*, page 155
2. *Using the Filtering option to install Web Security components on Linux*, page 157

(Remote Filtering Server is not included because it resides by itself on a machine in the network DMZ.)

Starting the Web Security Linux installer

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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:

   ```
   WebsenseWeb78Setup_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 WebsenseWeb78Setup_Lnx.tar.gz
   tar xvf WebsenseWeb78Setup_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.

Using the Filtering option to install Web Security components on Linux

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 155, 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.
4. On the Integration Option screen, indicate whether this is a stand-alone or integrated installation, and then click **Next**.

    See *Understanding Web Security standalone and integrated modes*, page 45, for more information.
5. If you chose **Integrated with another application or device** (on the Integration Option screen), the **Select Integration** screen appears. Select your integration, then click **Next**.
6. If the **Multiple Network Cards** screen appears, 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 blocked 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.

7. On the **Network Card Selection** screen, select the NIC that Network Agent should use to communicate with other Web Security components, then click **Next**.

   The list may include NICs that do not have an IP address are also listed. Do **not** choose a NIC without an IP address.

8. On the **Filtering Feedback** screen, select whether you want Websense software to send feedback to Websense, Inc. to improve accuracy. Then click **Next**.

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 if you do not have a Web Security Gateway Anywhere subscription, or if you want to install Sync Service and Directory Agent on another machine.

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 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 65.

    - **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 to apply policies to users or groups, and do not want user and group information to appear in reports.
  - 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 (/opt/Websense), or click **Choose** to specify another path, and then click **Next**.

    The installation path must be absolute (not relative).

    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**.

11 Installing Websense Content Gateway

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Security Gateway and Web Security Gateway Anywhere, v7.8.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 website classification to protect clients from malicious content while enabling access to safe content.

Content Gateway offers:

- Categorization of dynamic websites
- Categorization of new and unclassified websites
- Optionally, HTTPS and FTP content analysis, in addition to HTTP
- Enterprise Web proxy caching capabilities

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

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

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, viruses, and more.

- 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.
- Outbound content and file analytic options that mirror inbound analysis. As well as Data Theft Protection options that look for and block custom encrypted files, password files, and files containing sensitive or suspicious data.

See the "Scanning options" section of the Web Security Help.

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.

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 devices in the network that run WCCP or that perform policy-based routing.

If you enable SSL support, the content of 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 SSL support. See Content Gateway Manager Help for a complete description of SSL support.

Deployment

- *Proxy deployment options*, page 97
- *User authentication*, page 98
- *HTTPS content inspection*, page 100
- *Handling special cases*, page 101
- *Explicit proxy deployment*, page 101
- *Transparent proxy deployment*, page 102
- *Chaining Content Gateway with other proxies*, page 112

Installation

These 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 the 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 7.8.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere, v7.8.x

If you are installing Websense Content Gateway (Content Gateway) as part of a software-based deployment of Web Security Gateway or Web Security Gateway Anywhere, you must install the core policy and management components prior to installing Content Gateway. For instructions, see:

- Installation Instructions: Web Security Gateway Anywhere
- Installation Instructions: Web Security Gateway
- *Installing via the Web Security All option*, page 147

During installation of filtering components:

- On the *Integration Option Screen*, be sure to select **Integrated with another application or device**. In the *Select Integration Screen* that follows, select **Websense Content Gateway** as the integration product.
- Note the IP address or addresses of Policy Server and Filtering Service. You will need them when installing Content Gateway.

> **Important**
>
> Ensure that hostname and DNS are configured before installing your Websense products (see *System requirements for Websense Content Gateway*.)
>
> Be sure to 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 7.8.x

Applies to:	In this topic
◆ Web Security Gateway and Web Security Gateway Anywhere, v7.8.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 the host machine, you must perform the following tasks and consider the following issues.

Downloading the installer

1. Download the **WebsenseCG78Setup_Lnx.tar.gz** installer tar archive, from mywebsense.com to a temporary directory.
2. Create a directory for the tar archive, and then move the archive to the new directory. For example:

```
mkdir wcg_v78
mv WebsenseCG78Setup_Lnx.tar.gz ./wcg_v78/
```

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

```
cd wcg_v78
```

4. Unpack the tar archive:

```
tar -xvzf WebsenseCG78Setup_Lnx.tar.gz
```

Internet connectivity

It is recommended that the Content Gateway host 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 the following security issues prior to installing Content Gateway:

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 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 (GPO), a Windows Server feature. For more information about Group Policy, search the Microsoft TechNet website 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.

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 WCCP v2-enabled router or Layer 4 switch. 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 WCCP v2-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:	
Red Hat Enterprise Linux 6 series, 64-bit	6 GB minimum 8 GB recommended
Disk space	2 disks: • 100 GB for the operating system, 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. The latest version is recommended. 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 7.8.x is certified on:

- **Red Hat Enterprise Linux 6 series, 64-bit, Basic Server**
  - Kernel version for 6.5: 2.6.32-431 (not recommended for v7.8.3 Content Gateway)
  - Kernel version for 6.4: 2.6.32-358
  - Kernel version for 6.3: 2.6.32-279
  - Kernel version for 6.2: 2.6.32-220
  - Kernel version for 6.1: 2.6.32-131
  - Kernel version for 6.0: 2.6.32-71
- V-Series appliances

Content Gateway is supported on:

- The corresponding CentOS version (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 Security core policy components

Version 7.8 is required.

Important

Websense core policy components must be installed prior to Content Gateway. When Filtering Service is installed, Content Gateway must be specified as the integration product. See:

- Installation Instructions: Web Security Gateway Anywhere
- Installation Instructions: Web Security Gateway

Integration with Websense Data Security

Version 7.8 is required.

- Any version can be used via the ICAP interface. However, use of the integrated, on-box components is strongly recommended. 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. The Content Gateway manager supports the following web browsers:

- Internet Explorer 8, 9, 10 and 11
- 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.
   - 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 will 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 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 7.8.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere, v7.8.x

Installing Websense Content Gateway

Complete these steps to install Websense Content Gateway on a Linux server in a software-based deployment of Websense Web security software. In a Websense-appliance-based deployment, Content Gateway is already installed on the appliance.

Important

Before you begin, be sure to read and perform the activities described in *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 **WebsenseCG78Setup_Lnx.tar.gz** tar archive, from mywebsense.com to a temporary directory.

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

   ```
   mkdir wcg_v78
   mv WebsenseCG78Setup_Lnx.tar.gz ./wcg_v78/
   ```

   b. Change to the directory you created in Step a.

   ```
   cd wcg_v78
   ```

   c. Unpack the tar archive:

   ```
   tar -xvzf WebsenseCG78Setup_Lnx.tar.gz
   ```

Warning

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 server does not meet the minimum hardware requirements or is missing required operating system packages, you will receive error or warning messages. For example:

```
Error: Websense Content Gateway v7.8.0 on x86_64 requires
several packages that are not present on your system.

Please install the following packages: <list of packages>

If you are connected to a yum repository you can install
these packages with the following command:

yum install <list of packages>

See the Websense Technical Library (www.websense.com/
library) for information about the software requirements
for x86_64 installation.
```

   Install the missing packages and again start the Content Gateway installer.

   Here is an example of a system resource warning:

```
Warning: Websense Content Gateway requires at least 6
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 a minimum requirements 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 or **n** to cancel the installation.

```
Do you accept the above agreement [y/n]? y
```

7. Enter and confirm a password for the Content Gateway 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 – the 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 8 ports on your server:

Port Assignments:

-----------------
'1'  Websense Content Gateway Proxy Port  8080
'2'  Web Interface port                   8081
'3'  Auto config port                     8083
'4'  Process manager port                 8084
'5'  Logging server port                  8085
'6'  Clustering port                      8086
'7'  Reliable service port                8087
'8'  Multicast port                       8088


Enter the port assignment you would like to change:

‘1-8’ - specific port changes
‘X’   - no change
‘H’   - help
[X] >
```

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. As a way of improving the Content Gateway product, you can elect to send Websense, Inc., information about usage statistics, scanned content, and activated product features. **Important:** 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 The 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 the Web Security manager.

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 the Content Gateway manager.

See the Getting Started section of 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 7.8.x

Applies to:	In this topic
◆ Web Security Gateway and Web Security Gateway Anywhere, v7.8.x	◆ *Required libraries in Red Hat Enterprise Linux 6* ◆ *Installing on Red Hat Enterprise Linux 6, update 1 and higher*

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 7.8.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 7.8.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

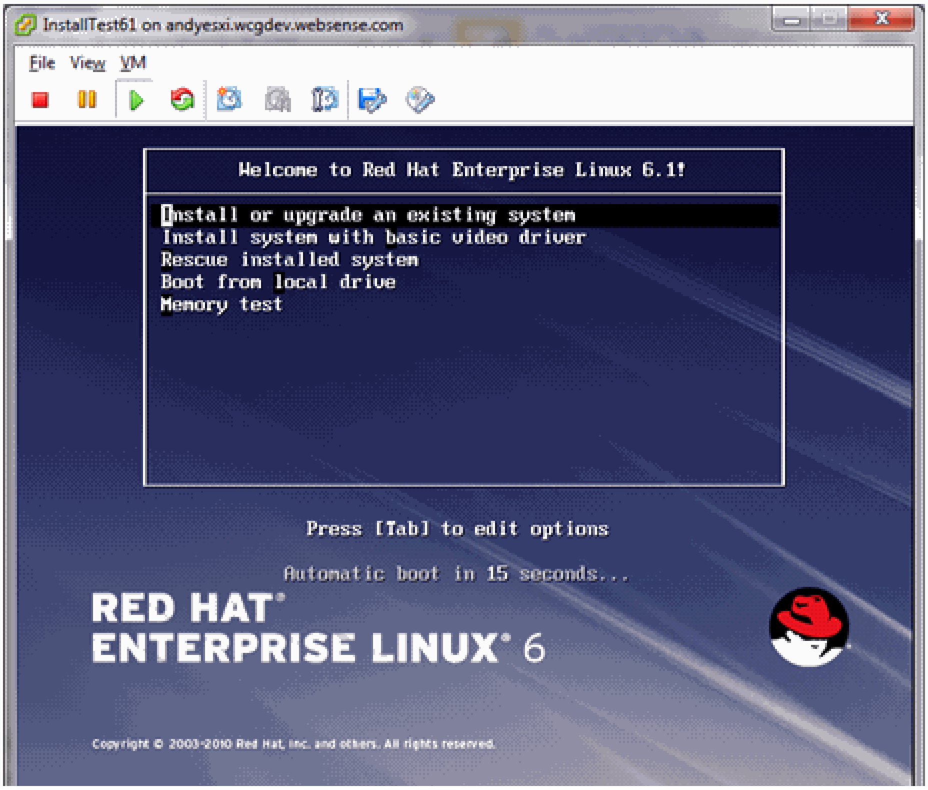
If while installing Content Gateway the installer finds non-eth# interface names, the installer quits and provides a link to instructions for modifying system startup files.

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:

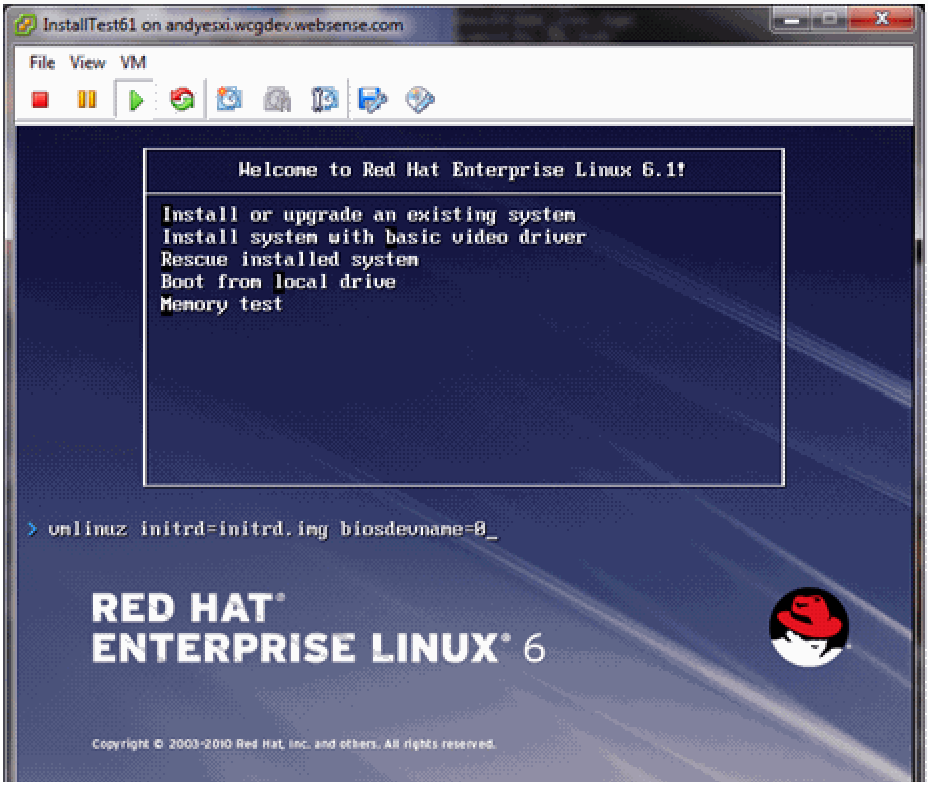


InstallTest61 on andyesxi.wcgdev.websense.com
File View VM

```
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.

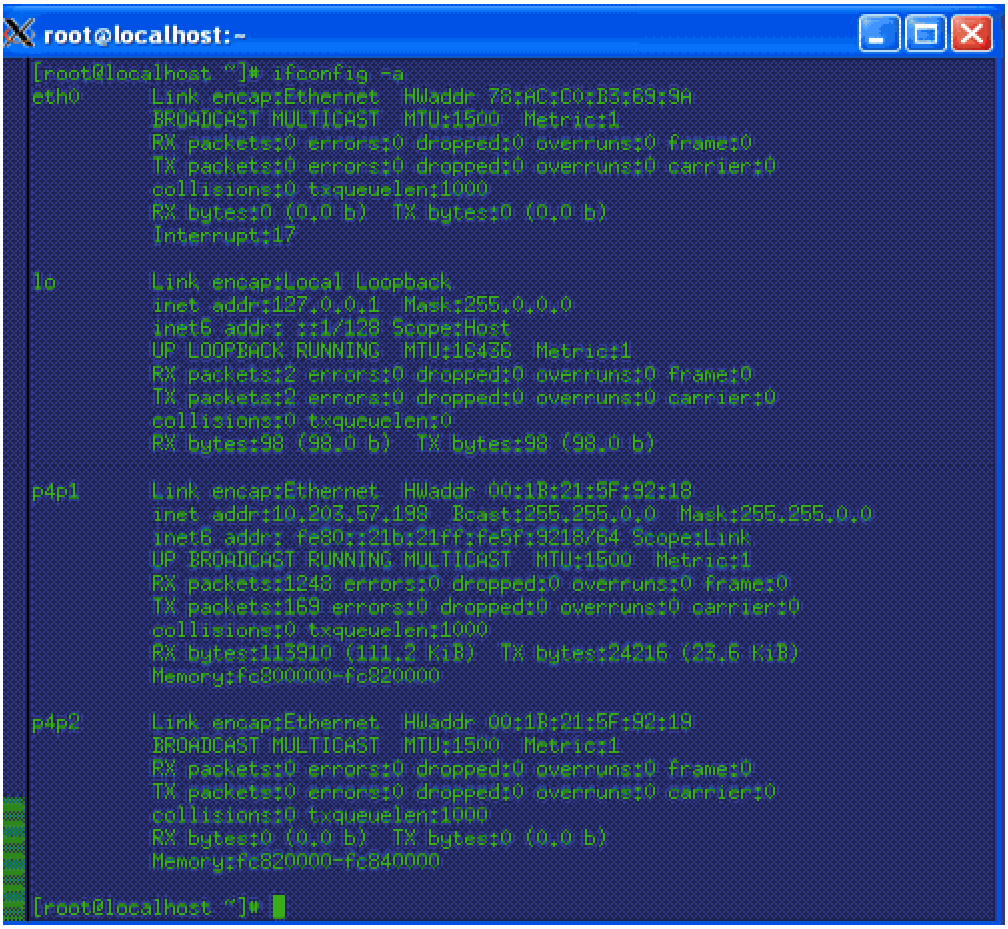
Disabling biosdevname after operating system installation:

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 packeta:2 errora: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

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
```

Warning

Content Gateway is supported on Red Hat Enterprise Linux 6, Basic Server (no GUI) and is ***not*** supported on RHEL 6 with a GUI.

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
```

12 Installing appliance-based Websense solutions

Deployment and Installation Center | Web and Email Security Solutions | Version 7.8.x

Install Email Security Solutions

Websense Email Security Gateway solutions are available only on Websense V-Series appliances:

- Email Security Gateway/Anywhere
- Web and Email Security Gateway/Anywhere (dual-mode appliance)

V-Series appliances can also be components in the following Websense solutions:

- Web Security
- Web Security Gateway/Anywhere

Installation of any Websense appliance-based solution includes the following basic steps:

1. Ensure that Microsoft SQL Server is installed and running in your network.
2. Install and configure your V-Series appliances.
3. Install Websense Log Server (Email or Web)
4. Install TRITON infrastructure, including all appropriate management modules.
5. Install all off-appliance product components.

For detailed appliance-based product installation materials for solutions that include Email Security, see one of the following:

- Installing Email Security appliance-based solutions
- Installing Web Security and Email Security appliance-based solutions

If you are looking for Web Security-only installation instructions for appliances, go to *Installing Web Security solutions*, page 147, and select the PDF for your solution.

13 Setting Up Websense V-Series Appliances

Deployment and Installation Center | Web and Email Security Solutions | Version 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.x

Setting up a Websense V-Series appliance involves the following tasks.

1. *Set up the appliance hardware*, page 191
2. *Perform initial command-line configuration*, page 196
3. *Configure the appliance*, page 200
4. *Install off-appliance or optional components*, page 224

✓ **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 Log Server installation.

Set up the appliance hardware

Deployment and Installation Center | Web and Email Security Solutions | Version 7.8.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.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
- Access V10000 G3 poster

Review the sections that apply to your Websense appliance model.

- *V10000 G2/G3 hardware setup*
- *V5000 G2 hardware setup*
- *Serial port activation*

V10000 G2/G3 hardware setup

Deployment and Installation Center | Web and Email Security Solutions | Version 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2 and V10000 G3 v7.8.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/G3: Web mode with Web Security Gateway*
- *V10000 G2/G3: Email mode*
- *V10000 G2/G3: Web and Email mode with Web Security Gateway*
- *V10000 G2/G3: Web and Email mode with Web Security (no content gateway)*

V10000 G2/G3: 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 Web Security manager. 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/G3: 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) can 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) interface can access.
- Network interface E1 (and E2, if used) must be able to access the mail server.

V10000 G2/G3: Web and Email mode with Web Security Gateway

Network interfaces C, P1, 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, P1, 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 Web Security manager. In that situation, interface C does not require Internet access.)
- Make sure the above address is permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C, P1, 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/G3: Web and Email mode with Web Security (no content 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 address is 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 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V5000 G2 v7.8.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 content gateway)*
- *V5000 G2: Web and Email mode with Web Security (no content 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 Web Security manager. 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.

V5000 G2: Web mode with Web Security (no content 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 content 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 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.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 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.x

Setting up a Websense V-Series appliance involves the following tasks. This topic covers **Step 2**:

1. *Set up the appliance hardware*, page 191
2. *Perform initial command-line configuration*, page 196
   - *Gather the data*
   - *Run firstboot*
3. *Configure the appliance*, page 200
   - *Network interface configuration*
   - *Routing configuration*
   - *Alerting*
   - *Configuring Web Security components*
4. *Install off-appliance or optional components*, page 224

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 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 Web Security manager 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 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 • 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 only [without the content gateway]). Choose one: • Standalone (Network Agent only) • Microsoft TMG • 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 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/G3, 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/G3) or Web Security (V10000 G2/G3 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, 9, 10, and 11
- Mozilla Firefox version 5 and later
- Google Chrome 13 and later

Note

If you use Internet Explorer, ensure that the Enhanced Security Configuration (IE ESC) is turned off.

Compatibility View is not supported.

Configure the appliance

Deployment and Installation Center | Web and Email Security Solutions | Version 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.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.

Before you configure an appliance for use with any Websense Web Security product, it is essential to note that one server in your network must serve as the policy source for all appliances running Websense software.

- Every Web Security deployment must include a policy source machine. This can be an appliance or a Windows or Linux server that hosts at least 2 components: Policy Broker and Policy Database (also hosts Policy Server and may host additional components). All other Websense appliances point to this machine and receive regular updates from it.
- You must set up a Windows or Linux policy source machine first, or configure a policy source appliance first (as described below), then configure your other appliances to point to it and communicate with it.

> **Note**
>
> If Policy Broker runs on a V-Series appliance, then 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.

After completing the initial configuration required by the **firstboot** script, choose your policy source machine (for Web Security) and then 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 7.8.x

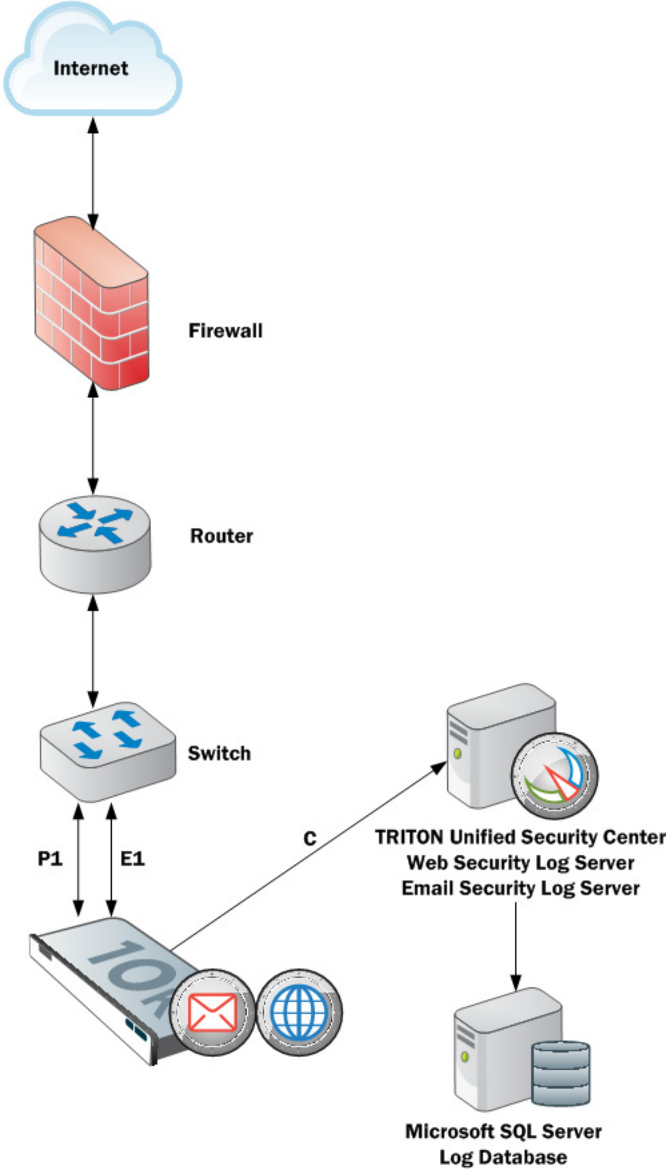
Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.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 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.x

The Appliance Controller interface (C), already assigned during **firstboot**:

- Communicates with all Websense management interfaces
- Communicates with the Websense Data Security management 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, and Multiplexer).
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 7.8.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.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, the default gateway is automatically assigned to P2 (which is bound to eth1). 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). 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 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.x

Network Agent is a software component used to provide security for 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 Web Security manager do not override the settings you enter in this pane. The settings in Appliance manager take precedence.
IP address of interface N	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 7.8.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.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/G3, 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/G3, 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

In the following important guidelines for configuring the E1 and E2 interfaces for Email Security, please note that for a V5000 G2 appliance, you should substitute P1 for E1 and P2 for E2.

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 DNS servers 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 7.8.x

Applies to:	In this topic
◆ Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.8.x ◆ V10000 G2 and V10000 G3, v7.8.x	◆ *V10000 G2/G3 with Websense Web Security Gateway only*, page 212 ◆ *V10000 G2/G3 with Websense Email Security Gateway only*, page 213

V10000 G2/G3 appliances that run one module only—Websense Web Security Gateway **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 G2/G3 with Websense Web Security Gateway 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 G2/G3 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/G3 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/G3 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 7.8.x

Applies to:	In this topic
◆ Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.8.x ◆ V10000 G2, V10000 G3, and V5000 G2, v7.8.x	◆ *Configuring static routes*, page 214 ◆ *Configuring module routes*, page 216

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 this operation is 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 7.8.x

Applies to:	In this topic
- Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x - Email Security Gateway and Email Security Gateway Anywhere, v7.8.x - V10000 G2, V10000 G3, and V5000 G2, v7.8.x	- *Enable SNMP polling (monitoring)*, page 217 - *Enable SNMP traps*, page 218 - *Enable specific alerts*, page 218

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 218.

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 218, 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 218, 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 7.8.x

Applies to:	In this topic
◆ Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ V10000 G2, V10000 G3, and V5000 G2, v7.8.x	◆ *What is a policy source?*, page 220 ◆ *What if an appliance is not the policy source?*, page 222 ◆ *User directory with V-Series appliances*, page 223 ◆ *Redundancy*, page 224

Be sure that you have selected your policy source machine before starting to complete this section. The policy source is the machine where appliances get Web Security global configuration and policy information. If a Windows or Linux server will be the policy source machine in your network, set it up first, so that you can point the V-Series appliances to it.

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. You should also specify the Web Security manager location.

1. 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.
2. The TRITON Unified Security Center (management consoles) must be installed on a Windows Server 2008 R2 or R2 SP1 64-bit or Windows Server 2012 or 2012 R2 Standard Edition machine. Identify this machine here by IP address.
3. Click **OK** to save and apply your changes.

What is a policy source?

Every Websense Web Security deployment must include a policy source. This is an appliance or other server that hosts at least 2 components: Websense Policy Broker and Websense Policy Database (Policy Server must also be present; additional components are often installed). All other Websense appliances or other servers point to this machine and receive regular updates from it.

Websense Policy Broker is the component that controls access to global configuration information and policy data consumed by other components. Policy Broker can be deployed in a standalone configuration or in a replicated configuration.

- A **standalone** configuration has 1 Policy Broker for the entire deployment. All Policy Servers connect to the same Policy Broker. In a standalone deployment, Policy Broker can reside on a Windows or Linux server, or a Websense appliance.
- In a **replicated** configuration, there is 1 primary Policy Broker, to which configuration and policy changes are saved, and one or more **replica** instances, each with its own read-only copy of the configuration and policy data. Each Policy Server can be configured to specify whether it attempts to connect to the primary Policy Broker or a replica instance at startup.

  In a replicated configuration, Policy Broker cannot reside on a Websense appliance. The primary Policy Broker and all replica instances must be hosted by a Windows or Linux server.

When Policy Broker replication is enabled, if the primary Policy Broker machine fails, all components connect to replica Policy Broker instances and continue to run normally, using the read-only configuration and policy data stored by the replica.

When a Websense 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; disabled by default)
- Multiplexer (optional; disabled by default; unavailable when the appliance is Filtering only)
- Usage Monitor
- Control Service
- Websense Content Gateway module (only with Web Security Gateway)
- Network Agent module (optional)

Windows-only services, like the TRITON Unified Security Center, Log Server, and optional services, like transparent identification agents, still run on other machines.

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 (cloud) 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 the Web Security manager 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 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

Web traffic management requires interaction between several Websense software components:

- User requests for Internet access are proxied and analyzed by Content Gateway.
- User requests for Internet access may also be managed by Network Agent.
- The requests are sent to Websense Filtering Service for processing.
- Filtering Service communicates with 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 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.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 plan to use. Follow the links for your deployment in *Installing appliance-based Websense solutions*, page 189

Note

Before deploying off-appliance components, be sure to use the 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 a V-Series appliance:

- Only on-appliance instances of Policy Server can communicate with Policy Broker.
- 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 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 191
- *Perform initial command-line configuration*, page 196
- *Configure the appliance*, page 200

The machine on which **TRITON Unified Security Center** is installed is referred to as the **TRITON management server**. To install TRITON management server, see *Installing appliance-based Websense solutions*, page 189.

Restoring to Factory Image

Deployment and Installation Center | Web and Email Security Solutions | Version 7.8.x

Applies to:

- Web Security v7.8.x
- Web Security Gateway and Web Security Gateway Anywhere v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere v7.8.x
- V10000 G2, V10000 G3, and V5000 G2 v7.8.x

USB Image

The current generation of V-Series appliances does not 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 for restoring older versions

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. After the appliance image is restored, components running off the appliance must be reinstalled.

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/G3)
   - **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. Reinstall 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 Web Security manager if you receive a warning message about the Master Database.

14 Installing Data Security Solutions

Deployment and Installation Center | Data Security Solutions | Version 7.8.x

Install Data Security Solutions

To install Data Security, you perform 2 basic steps.

1. Install the TRITON infrastructure. This includes the TRITON console, settings database, and reporting database.
2. Install Data Security management components. This includes the a policy engine, crawler, fingerprint repository, forensics repository, and endpoint server.

   (Data Security supports installations over Virtual Machines (VM), but Microsoft SQL Server must be present to support the incident and policy database.)

Once you've installed management components, you may choose to install Data Security agents on print servers, TMG servers, or endpoint client machines. You can also install extra Data Security servers and crawlers for system scaling.

See the Data Security Installation Guide for step-by-step instructions.

It includes system requirements, port requirements, installation steps, as well as pre- and post-installation steps for each component when required.

It also covers how to add, modify, and remove components.

15 Installing components via the Custom option

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x ◆ Email Security Gateway and Email Security Gateway Anywhere v7.8.x	◆ *Deployment*, page 231 ◆ *Installation*, page 232 ◆ *Initial configuration*, page 232

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 to adapt the common installation scenarios (listed below) for your deployment.

- Installation Instructions: Web Security Gateway Anywhere
- Installation Instructions: Web Security Gateway
- Installation Instructions: Web Security or Web Filter
- Data Security Installation Guide
- Installing Email Security appliance-based solutions
- Installing Web Security and Email Security appliance-based solutions
- *Installing TRITON Enterprise*, page 133

Deployment

General

- *System requirements for this version*, page 4

Web Security

- *Web Security Deployment Recommendations*, page 33
- *Deploying Web Security for a distributed enterprise*, page 77
- *Integrating Web Security with Cisco*, page 269
- *Integrating Web Security with Citrix*, page 293
- *Integrating Web Security using ICAP Service*, page 333
- *Integrating Web Security with Microsoft Products*, page 311
- *Installing Web Security for Universal Integrations*, page 339

Data Security

- *Planning Data Security Deployment*
- *Integrating Data Security with Existing Infrastructure*
- *Scaling Data Security*

Email Security

- *Email Security Gateway Deployment*, page 119

Installation

To perform a custom installation, first start a custom installation (see *Starting a custom installation (Windows)*, page 233). Then see the following instructions for the components you want to install:

- *Installing TRITON Infrastructure*, page 234
- *Installing Web Security components*, page 240
- *Installing Data Security components*, page 259
- *Installing Email Security components*, page 260
- *Installing SQL Server 2008 R2 Express (without TRITON Infrastructure)*, page 264

Initial configuration

General

- *Websense TRITON Enterprise default ports*, page 439
- *Excluding Websense files from antivirus scans*, page 451
- *Initial Configuration for All Websense Modules*, page 407

Web Security Gateway Anywhere

- *Web Security initial configuration*, page 409
- *Content Gateway initial configuration*, page 416
- *Additional configuration for Web Security Gateway Anywhere*, page 411

Data Security

- *Data Security initial configuration*, page 413

Starting a custom installation (Windows)

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

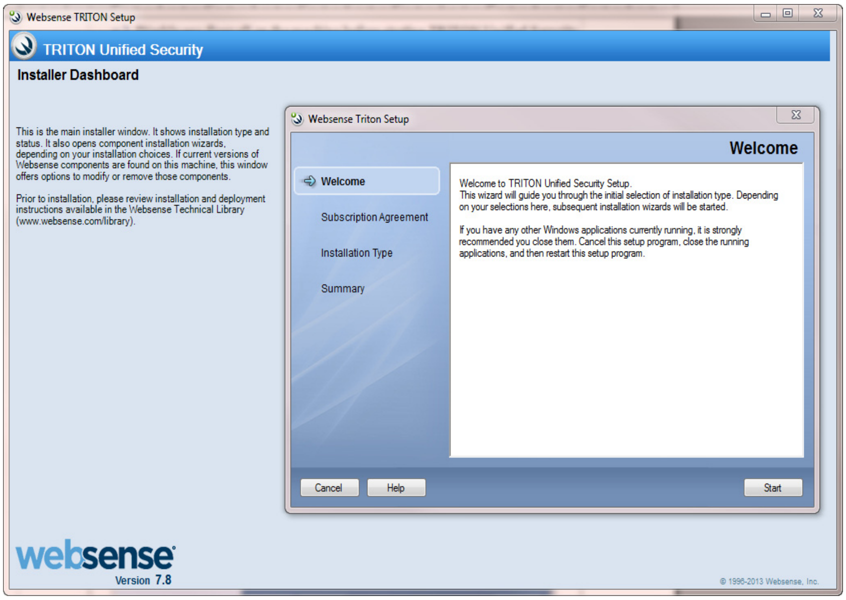
Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

1. Download or copy the TRITON Unified Installer (the Windows installer) to this machine. The installer is available from mywebsense.com, and the installer file is **WebsenseTRITON784Setup.exe**
2. Double-click **WebsenseTRITON784Setup.exe** to launch the installer.

   A progress dialog box appears, as files are extracted. It make take some time to extract all of the installer files and launch the setup program.

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



Installer Dashboard

This is the main installer window. It shows installation type and status. It also opens component installation wizards, depending on your installation choices. If current versions of 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.
This 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 strongly recommended 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 7.8.x

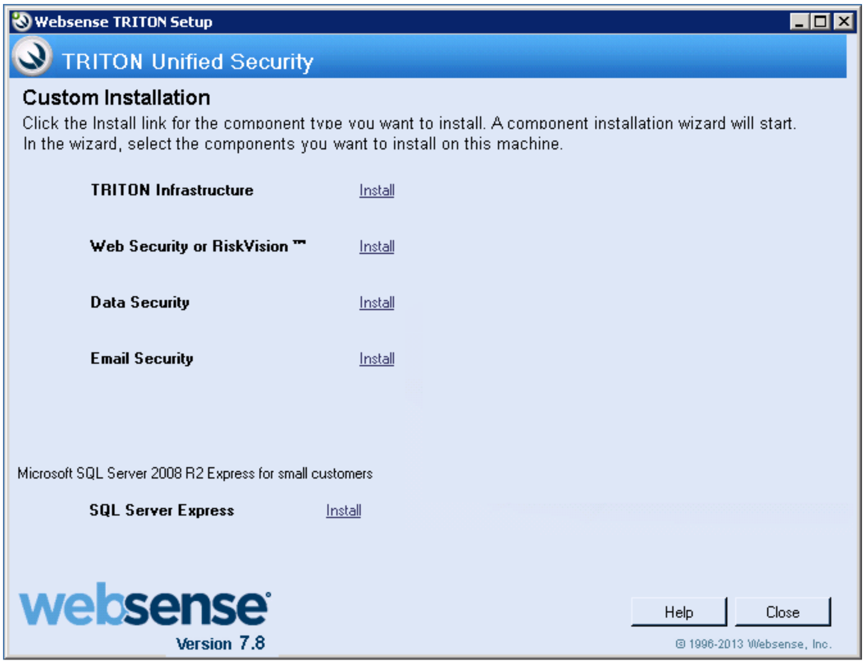
Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

TRITON Infrastructure is composed of common user interface components required by the TRITON Unified Security Center modules (the Web Security, Data Security, and Email Security managers).

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 standard or enterprise version of SQL Server should be used in production environments.

1. It is assumed you have already launched the Websense installer and done one of the following:
   - Selected the **Custom** installation type, and selected TRITON Infrastructure install. (See *Deployment*, page 231.)
   - Selected the TRITON Unified Security Center installation type. (See *Installing the TRITON Unified Security Center*, page 135.)
   - Started an upgrade of prior-version Web or Data Security components, with Web Security or Data Security management components 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.

Microsoft SQL Server 2008 R2 Express for small customers

   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.

     In some cases, you are prompted to reboot the machine after installing SQL Server Express. If you do, to restart the installer:

     - Windows Server 2012: Go to the **Start** screen and click the **Websense TRITON Setup** icon.
     - Windows Server 2008 R2: Go to **Start** > **All Programs** > **Websense** > **Websense TRITON Setup**.
   - 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).

     ✓ **Note**

     If your Email Security Gateway SQL Server installation uses a named instance, port 1433 is opened on the firewall even if you specify a different port. You must manually change this port setting after Email Security Gateway installation.

See *System requirements for this version*, page 4, 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. If you are using Windows authentication with Data Security, Web Security Gateway Anywhere or Email Security Gateway/Anywhere, use an account with the sysadmin role. If you are using SQL Server Express, sa (the default system administrator account) is automatically specified.

  ✓ **Note**

  The system administrator account password cannot contain single or double quotes.

  For more information about permissions required for the connection account, see *Installing with SQL Server*, page 257.

  If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web Security manager. See *Configuring Websense Apache services to use a trusted connection*, page 454.

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.

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 name can help recipients identify the notification as 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. Websense installer starts again. In the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
    c. 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**.

Installing Web Security components

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x

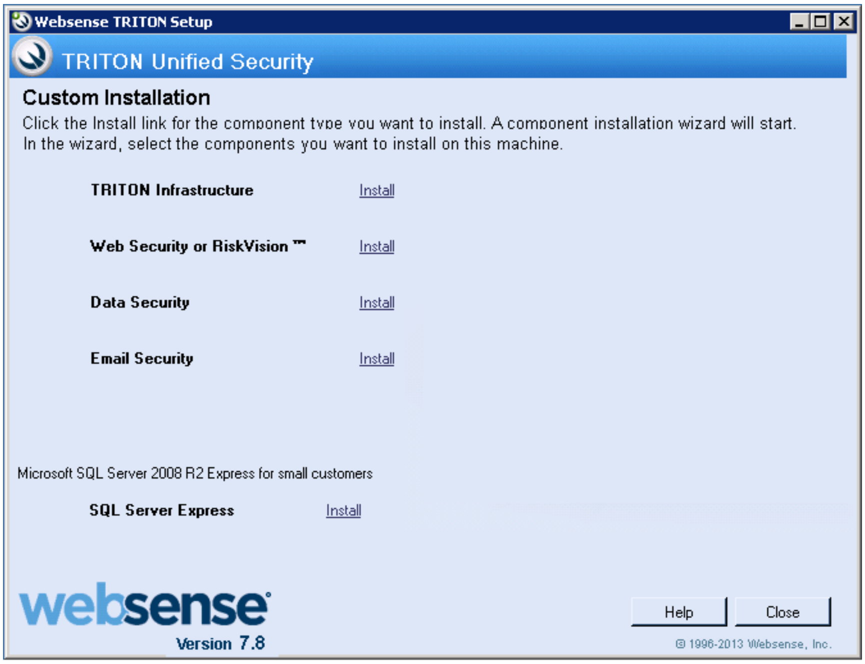
Complete these steps to install one or more Web Security software components on Windows. (To install Web Security components on a Linux machine, see *Installing Web Security Components on Linux*, page 155.)

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 231.)

If you are adding components, skip to Step 2.

1. On the Custom Installation dashboard, click the Web Security **Install** link.



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 or RiskVision ™	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.)

- The Web Security manager is available only when TRITON Infrastructure is already installed on the machine (see *Installing TRITON Infrastructure*, page 234).
- 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. In this scenario, there can be only one Policy Broker for the deployment.

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 243 (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 244 (Policy Server, Sync Service, or Directory Agent)
   - *Multiple Network Interfaces Screen*, page 246 (if multiple NICs detected)
   - *Active Directory Screen*, page 247 (if installing User Service, DC Agent, or Logon Agent on Windows Server 2008)
   - *Computer Browser Screen*, page 247 (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 248 (Filtering Service)
   - *Select Integration Screen*, page 249 (Filtering Service, to be integrated with a third-party product, or Filtering Plug-In)
   - *Network Card Selection Screen*, page 249 (Network Agent)
   - **SQL Server Native Client Tools** (Web Security or Web Security Log Server)

     If the installer appears in the foreground, follow the prompts to install the required tools.
   - *Database Information Screen*, page 250 (Web Security Log Server)
   - *Log Database Location Screen*, page 251 (Web Security Log Server)
   - *Optimize Log Database Size Screen*, page 252 (Web Security Log Server)
   - *Filtering Feedback Screen*, page 252 (Filtering Service or Network Agent)
   - *Directory Service Access Screen*, page 253 (User Service, DC Agent, or Logon Agent)
   - *Remote Filtering Communication Screen*, page 254 (Remote Filtering Server)
   - *Remote Filtering Pass Phrase Screen*, page 255 (Remote Filtering Server)
   - *Filtering Service Information for Remote Filtering Screen*, page 256 (Remote Filtering Server)

- *Filtering Service Communication Screen*, page 245 (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 one of the following:

   C:\Program Files (x86)\Websense\Web Security (on the TRITON management server)

   C:\Program Files\Websense\Web Security (on servers that do not have management components)

   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 Cisco*, page 269
   - *Integrating Web Security with Citrix*, page 293
   - *Integrating Web Security with Microsoft Products*, page 311
   - *Installing Web Security for Universal Integrations*, page 339

Policy Server Connection Screen

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 (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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 (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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 (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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 256.

Integration Option Screen

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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
  - Cisco ASA or routers
  - 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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 Web Security to integrate with Forefront TMG*, page 315.

(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 293.

Network Card Selection Screen

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 417.

> ✓ **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 the Web Security manager to configure how Network Agent will use each selected NIC (for more information, see the Web Security Help).

Database Information Screen

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 4, 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 the Web Security manager. See *Configuring Websense Apache services to use a trusted connection*, page 454.

- 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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 the Web Security manager.

Directory Service Access Screen

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 Web Security Help.

- On Windows, configure the Websense User Service service to **Log on as** a Domain Admin user:
  a. Open the Windows Services tool (**Service Manager > Tools > Services** or **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**, then click **OK** again.
  g. Right-click **Websense User Service** and select **Restart**.

Remote Filtering Communication Screen

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 (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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x

See *System requirements for this version*, page 4, 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, Web Security Gateway Anywhere, and Data Security, the account must have a sysadmin role.

   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 2008** or **2012** > **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**. For Email Security Gateway/ Anywhere, Web Security Gateway Anywhere, and Data Security, also select **sysadmin**.
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

      and also to:
      - db_datareader
   c. Select **wbsn-data-security** in database mapping and mark it as “db_owner”.
   d. Select **wbsn-data-security-temp-archive** in database mapping and mark it as “db_owner”.
   e. 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 7.8.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 134.

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 Installing Data Security Servers and Agents. 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 7.8.x

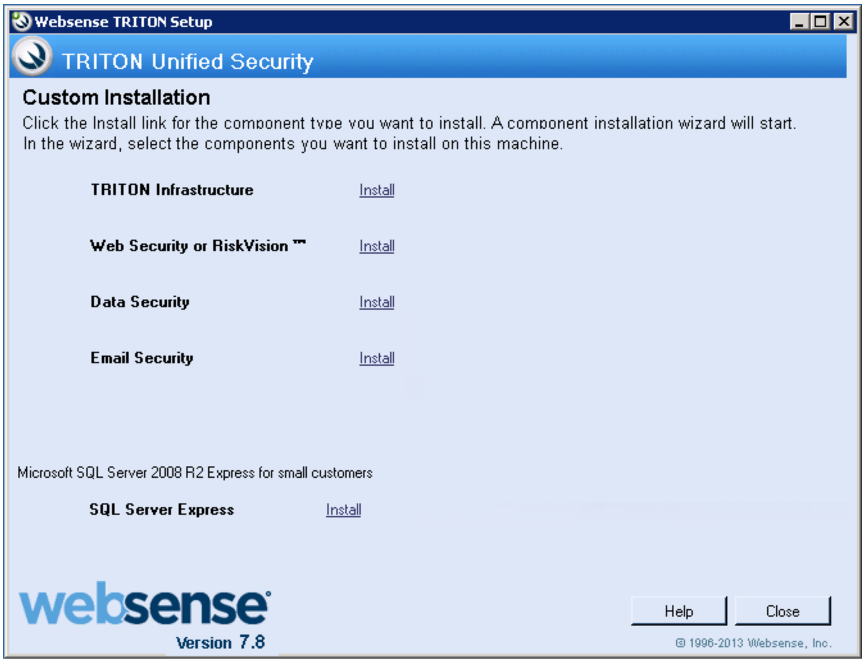
Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

Websense Email Security Gateway is an appliance-based solution. All components run on the appliance except the Email Security manager (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 231.

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 or RiskVision ™ 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 Email Security management components*, page 143, 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 4, 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 in 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 257.

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., Email Security Gateway manager 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

Any Email Security log data that has been written to the database will be lost if you remove the database. If you want to keep this data, back up the esglogdb7x and esglogdb7x_*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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.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 234.

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 19.

   You may have to stop Filtering Service. 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.
3. It is assumed you have already launched the the Websense installer and chosen the Custom installation type. If not, see *Starting a custom installation (Windows)*.
4. On the **Custom Installation** dashboard, click the *Install* link for SQL Server Express.

5. On the **Welcome** screen, click **Start** to begin the installation wizard.
6. 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:
     - 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.

7. 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.
8. Next, the **Installation** screen appears. Wait until all files have been installed.
9. On the **Summary** screen, click **Finish**.

16 Websense Endpoint Clients

Deployment and Installation Center | Web and Data Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x

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
- Websense Web Endpoint

And for data loss prevention (DLP):

- Websense Data Endpoint

You can deploy one of the Web Security solutions along with Data Endpoint, but you cannot deploy all three endpoints at one time. For instructions on installing and deploying the various endpoints, see:

- Installing and Deploying Data Endpoint Clients
- Installing and Deploying Web Endpoint Clients
- Combining Web and Data Endpoint Clients
- Installing and Deploying Remote Filtering Client

17 Integrating Web Security with Cisco

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

Websense Web Filter and Web Security can be integrated with Cisco® Adaptive Security Appliance (ASA) v8.0 and later and Cisco IOS routers v15 and later.

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 log bandwidth data for reporting block Internet requests based on bandwidth consumption.
- 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 application of user-based policies.

  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 273, provides general introductory information.
- *Configuring a Cisco Security Appliance*, page 276, discusses Cisco Adaptive Security Appliance (ASA).
- *Configuring a Cisco IOS Router*, page 284, discusses Cisco IOS router.

Deployment considerations for integration with Cisco products

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Cisco ASA*, page 270 ◆ *Cisco IOS Routers*, page 271

Related topics:

- *Getting started with a Cisco integration*, page 273
- *Configuring a Cisco Security Appliance*, page 276
- *Configuring a Cisco IOS Router*, page 284

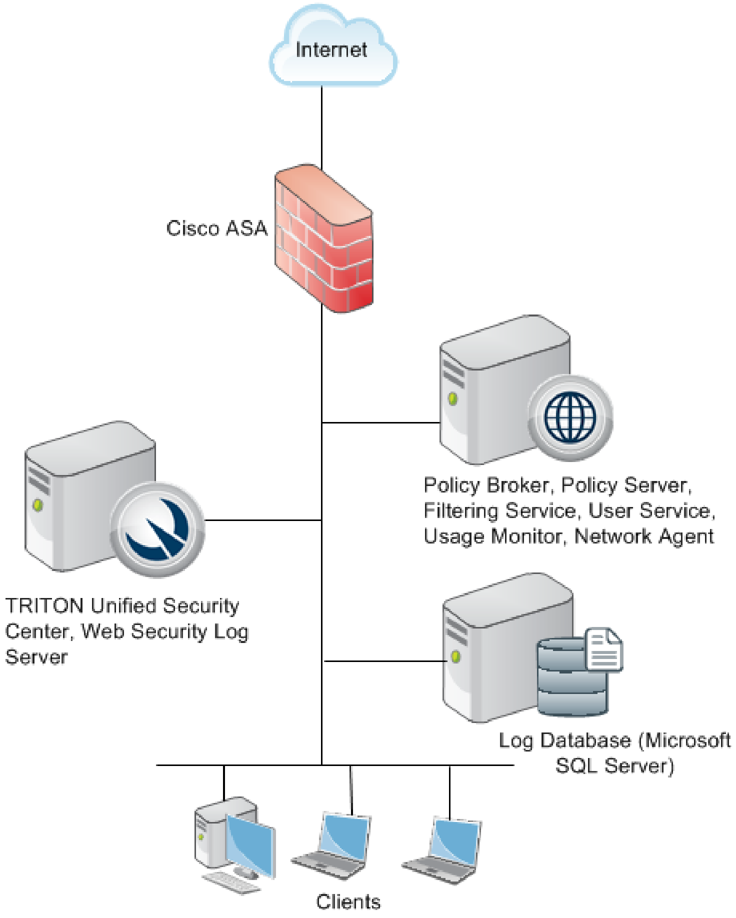
Cisco ASA

A simple and common network topology places Websense policy enforcement components on a single machine, or group of dedicated machines, communicating with a 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 269, for configuration instructions.

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


Internet
Cisco ASA
Policy Broker, Policy Server, Filtering Service, User Service, Usage Monitor, Network Agent
TRITON Unified Security Center, Web Security Log Server
Log Database (Microsoft SQL Server)
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.

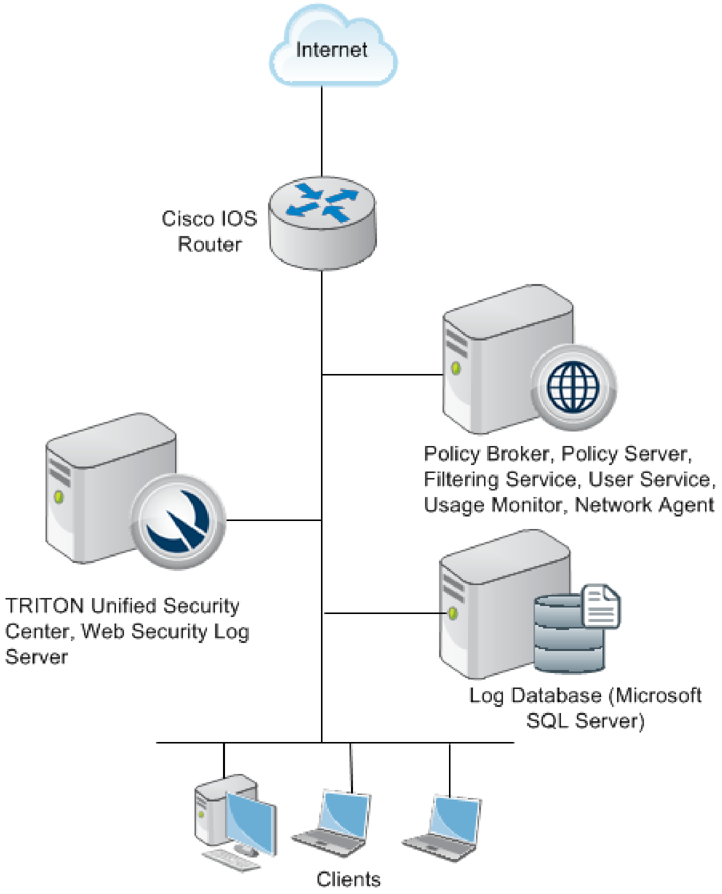
Cisco IOS Routers

In this common configuration, Websense policy enforcement 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 that bypasses the router cannot be managed by the Websense software.


Internet
Cisco IOS Router
Policy Broker, Policy Server, Filtering Service, User Service, Usage Monitor, Network Agent
TRITON Unified Security Center, Web Security Log Server
Log Database (Microsoft SQL Server)
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 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	

Related topics:

- *Deployment considerations for integration with Cisco products*, page 270
- *Configuring a Cisco Security Appliance*, page 276
- *Configuring a Cisco IOS Router*, page 284

How Web Filter and Web Security work with Cisco products

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

When it receives an Internet request, the Cisco product queries Filtering Service to determine if the requested website should be blocked or permitted. Filtering Service determines which policy or exception applies to the request and uses that to determine whether to block or permit the request.

- For HTTP, if the site is blocked, the browser displays a block page instead of the requested site.
- For HTTPS or FTP, if the site is blocked, the user is denied access and receives a blank page.
- If the site is permitted, Filtering Service notifies the Cisco product that the site is not blocked, and the client is allowed to visit the site.

Installing of Web Filter or Web Security

Install Web Filter or Web Security as directed in Installation Instructions: Web Security or Web Filter. 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 Routers**
- Do not install a transparent identification agent if you plan to configure user authentication 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 351, for upgrading instructions.

If you are upgrading your Websense deployment and changing your Cisco product, see *Migrating between integrations after installation*, page 274.

Migrating between integrations after installation

You can change the Cisco integration product (for example, change from ASA 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 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 427, for instructions.
5. Restart the machine (Windows only).
6. Use the Websense installer to reinstall Filtering Service. See *Installing Web Security components*, page 239, 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
  ```

10. Use the Web Security manager to identify which Filtering Service instance is associated with each Network Agent.

    a. Use a supported browser (see *System requirements for this version*, page 4) to go to **https://<IP address>:9443/triton**.

       Here, <*IP address*> is the IP address of the TRITON management server.

    b. Click the **Web Security** module, then go to **Settings > Network Agent**.

    c. Position the mouse over the **General** option and wait a second or two for a list of IP addresses to appear.

    d. Click an IP address to open the **Local Settings** page for that Network Agent instance.

    e. Under **Filtering Service Definition**, select the IP address for the machine running Filtering Service. During the migration, the setting may have been reset to None.

    f. Log off of the TRITON console.

    For more information, see the information about configuring local settings in the “Network Configuration” section of 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 manage HTTP(S) or FTP requests based on bandwidth consumption:

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 categories and protocols, please refer to the “Bandwidth Optimizer” section of the Web Security Help.

Configuring a Cisco Security Appliance

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:
◆ Web Filter and Web Security, v7.8.x

After Websense Web Filter or Web Security is installed, the Cisco 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 Web Security Help for information about implementing policies.

For information about configuring Websense integration with ASA through a console or telnet session, see:

- *Cisco integration configuration procedure*, page 276
- *User-based policies and Cisco integration*, page 283

For information on configuring your security appliance through the management interface, see the documentation for your Cisco product, available at www.cisco.com.

Cisco integration configuration procedure

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Configuration procedure*, page 276 ◆ *Parameters for the filter commands*, page 282

Configuration procedure

To configure your security appliance to send Internet requests to Websense software for policy enforcement:

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 Websense software URL management.

```
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>)`	(required) The network interface to use for Websense Filtering Service communication. You must type the parentheses ( ) when you enter a value for this parameter.
`vendor websense`	Indicates the URL management 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. Range: 10 - 120; Default: 30
`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**.
    - To review all the filter rules, enter **show running-config filter**.

    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 282.

    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 the Web Security manager to apply policies to individual clients (by IP address, user name, group, or OU).

See the Web Security Help for information about creating and applying 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**.
- To review all the filter rules, enter **show run filter**.
- Enter **exit** to go up a level to run the show command.

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 282.

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 the Web Security manager to apply policies to individual clients (by IP address, user name, group, or OU).

See the Web Security Help for information about creating and applying 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**.
- To review all the filter rules, enter **show run filter**.
- Enter **exit** to go up a level to run the **show** command.

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 282.

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 the Web Security manager to apply policies to individual clients (by IP address, user name, group, or OU).

See the Web Security Help for information about creating and applying 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:

    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.

    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**.
    - 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 manage Internet requests after the Websense Master Database is downloaded and the software is activated within the Cisco security appliance. See the 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.

`<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.

`[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.

Parameter	Applies to	Definition
`[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.
`[proxy-block]`	`filter http`	Enter this parameter to prevent users from connecting to an HTTP proxy server.

User-based policies and Cisco integration

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

If http, https or ftp authentication is enabled on a 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 policy enforcement.

> **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.

If user authentication is not enabled on the Cisco security appliance, manual authentication or transparent identification agents can be used to apply user-based policies. See the Web Security Help for information about configuring manual authentication, or configuring transparent identification agents.

If user authentication information is provided by a Cisco security appliance, it can only be used for HTTP(S) and FTP filtering by default.

To enable Internet protocol management, follow these steps:

1. Log on to the machine on which Filtering Service is installed.

2. Stop use the Windows Services dialog box or /opt/Websense/WebsenseDaemonControl command to stop Filtering Service.
3. Navigate to the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin) and open the **eimserver.ini** file in a text editor.
4. Under [WebsenseServer], add the parameter **CacheWISPUsers=on**.
5. Use the Windows Services dialog box or /opt/Websense/WebsenseDaemonControl command to restart Filtering Service.

Configuring a Cisco IOS Router

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 IOS startup configuration*, page 284
- *Cisco IOS configuration commands*, page 287
- *Cisco IOS executable commands*, page 290

Cisco IOS startup configuration

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 (the primary server) is used at a time. If the primary server becomes unavailable, the system goes to the list of configured 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 285.

```
no ip urlfilter server vendor websense <ip-address>
```

Cisco IOS configuration commands

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

These commands are used to configure the Cisco IOS router to filter HTTP requests through Websense Filtering Service.

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*> server <*IP address:port*>

  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*> server <*IP address:port*>

  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*> server <*IP address:port*>

  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 7.8.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway, v7.8.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.

18 Integrating Web Security with Citrix

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

Websense Web Filter and Web Security can be integrated with Citrix® XenApp™ 5.0, 6.0, and 6.5.

- 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 307, 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.
- **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.

  Although Network Agent can manage protocols other than HTTP, FTP, or SSL used by applications on the Citrix server, it can only apply a computer or network policy, or the Default policy to those requests.

See the following for information about integrating with Citrix products:

- *Managing Internet requests from Citrix server users*, page 294
- *Citrix Integration Service installation overview*, page 297
- *Upgrading the Citrix Integration Service*, page 305
- *Configuring user access on Citrix servers*, page 306
- *Initial Setup of Citrix integration*, page 307

Managing Internet requests from Citrix server users

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Managing Internet requests for both Citrix and non-Citrix users*, page 296

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

- A recommended maximum of 10 Citrix servers can connected to one Websense Filtering Service instance. This number can be configured and depends on the user load.

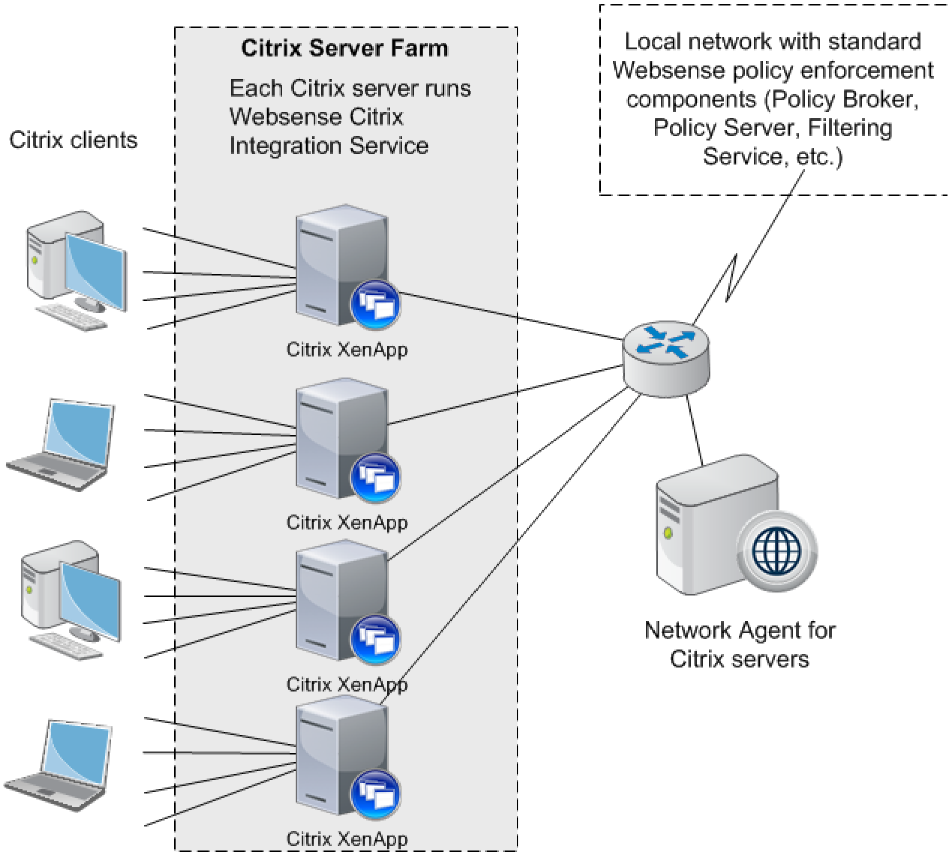
  Multiple Filtering Service instances are needed if more than 15 Citrix servers are used, with each Citrix server handling about 20 to 30 Citrix users.
- The Filtering Service and Network Agent monitoring Citrix traffic should be installed on a dedicated machine, and not on a Citrix server.
- Separate Filtering Service and Network Agent instances must be used to monitor non-Citrix traffic.
- The Filtering Service and Network Agent instances monitoring Citrix traffic use the same Policy Broker, Policy Server, User Service, and other components as the Filtering Service and Network Agent instances 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 manage other protocol traffic from the Citrix servers:

  - Network Agent must be located where it can see all of the traffic between the Citrix servers and 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 Web Security Help for instructions on configuring IP address 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 address or range. Otherwise, the Default policy is applied to all users.

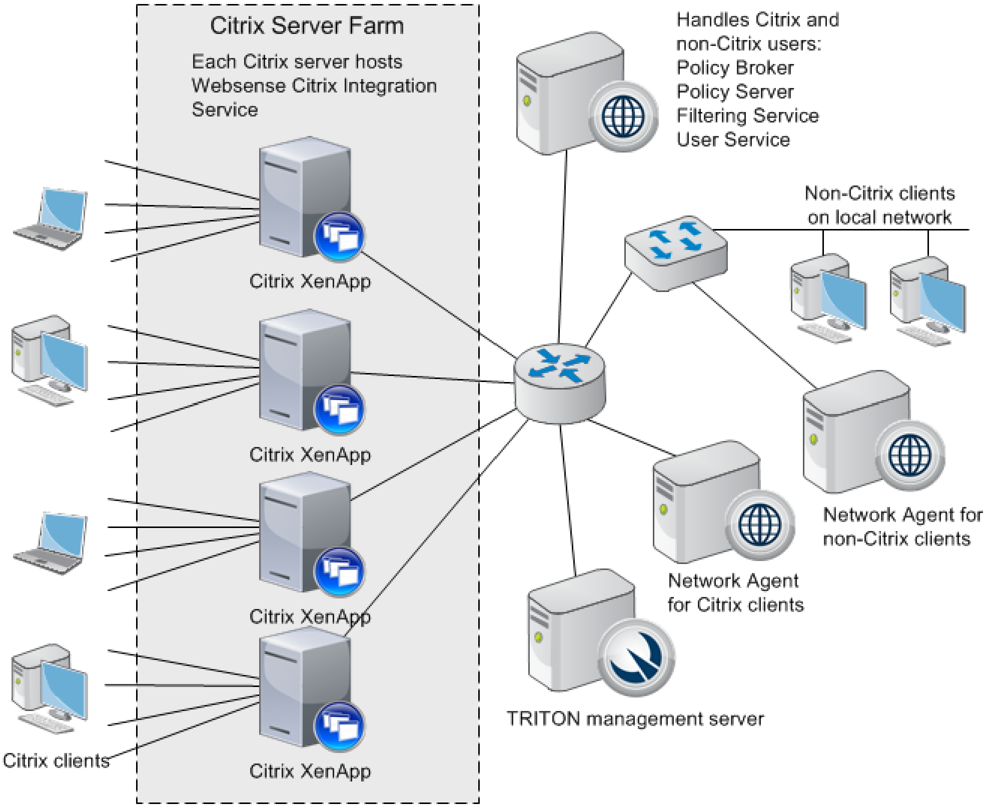
This diagram shows a typical deployment to manage requests from users who access the Internet through a Citrix server. To simplify the diagram, not all Websense components are shown.


Citrix clients
Citrix Server Farm
Each Citrix server runs Websense Citrix Integration Service
Citrix XenApp
Citrix XenApp
Citrix XenApp
Citrix XenApp
Local network with standard Websense policy enforcement components (Policy Broker, Policy Server, Filtering Service, etc.)
Network Agent for Citrix servers

The main Websense policy enforcement 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.

Managing Internet requests for 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
Handles Citrix and non-Citrix users:
Policy Broker
Policy Server
Filtering Service
User Service
Non-Citrix clients on local network
Network Agent for non-Citrix clients
Network Agent for Citrix clients
TRITON management server

- ◆ To install the Citrix Integration Service on a Citrix Server, see *Citrix Integration Service installation overview*, page 297.
- ◆ 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*, page 298, for instructions.
- ◆ To configure the Websense components installed with the non-Citrix integration to communicate with Citrix, refer to the section pertaining to your integration in *Combining Citrix with another integration*, page 307.

Citrix Integration Service installation overview

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 298.
3. Obtain the Citrix configuration package (used to install the Citrix Integration Service configuration utility).

   See *Obtain the Citrix Integration Service configuration package*, page 299.
4. Create and configure a Citrix Integration Service installation package for your deployment.

   See *Configure the Citrix Integration Service installation package*, page 299.
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 304.

For information about upgrading a prior-version Citrix Integration Service, see *Upgrading the Citrix Integration Service*, page 305.

If Websense software will manage Internet activity for both Citrix and non-Citrix users, refer to *Combining Citrix with another integration*, page 307, 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 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 TRITON Unified Installer (Windows) or Web Security Linux 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 239.

    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 (Windows or Linux) 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 299.

Obtain the Citrix Integration Service configuration package

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

Everything you need to configure and install Websense Citrix Integration Service (64-bit only) 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\

Copy the Citrix configuration package (folder) 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 299.

Configure the Citrix Integration Service installation package

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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.

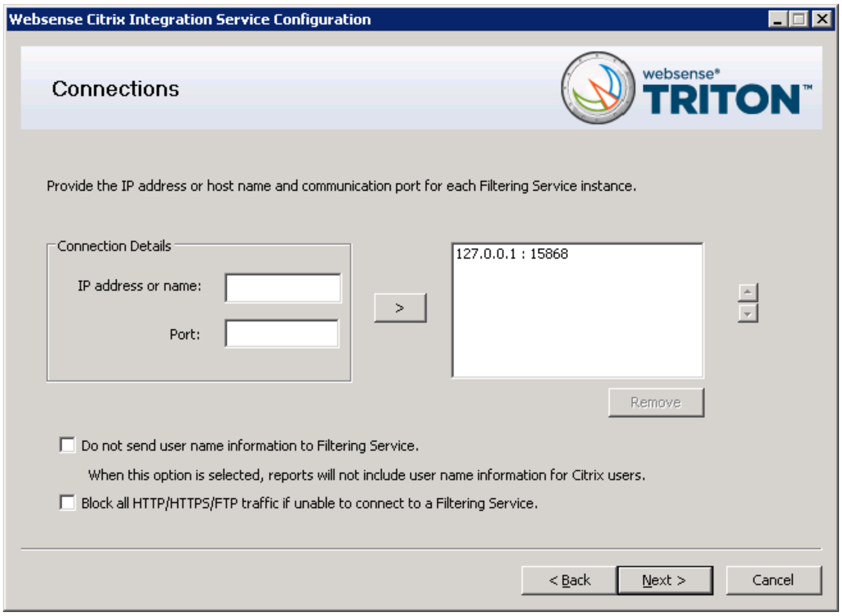
1. Double-click the configuration package executable, then click **Extract**. The package name is WCISUtil_x64_*nnnn*.exe.

2. Double-click **Websense Citrix Integration Service Configuration.exe** to start the configuration utility.
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**.



Provide the IP address or host name and communication port for each Filtering Service instance.

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).

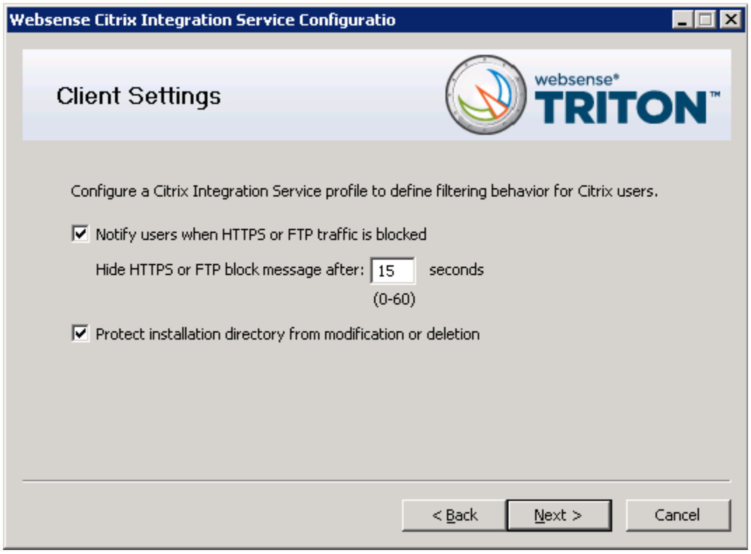
> ✓ **Note**
>
> Each Filtering Service instance tracks continue, quota, and password override information independently. If the Citrix Integration Service fails over from one Filtering Service instance to another, usage quotas may be different and override passwords may need to be entered again.

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**.



Configure a Citrix Integration Service profile to define filtering behavior for Citrix users.

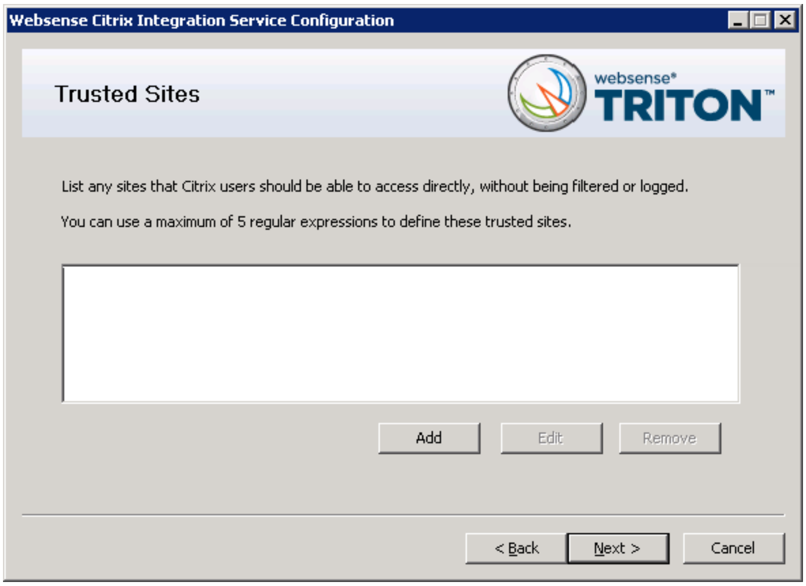
☑ Notify users when HTTPS or FTP traffic is blocked

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 any URLs or domains that should be ignored (not forwarded for policy enforcement). When you are finished, click **Next**.



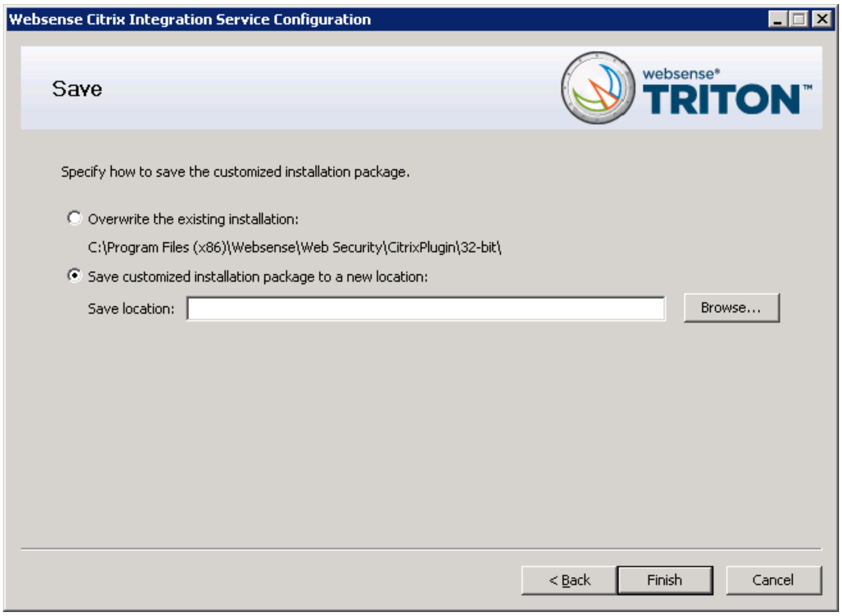
List any sites that Citrix users should be able to access directly, without being filtered or logged.

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**.



Websense Citrix Integration Service Configuration

Save

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 300.
- 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 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 304.

Use the installation package to install Citrix Integration Service on a Citrix server

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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**.
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**.

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 the Citrix Integration Service

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

The Websense Citrix Integration Service can be upgraded to v7.8 directly from v7.7, but not from version 7.6 or earlier.

- If you are upgrading from v7.7, simply create a new Citrix Integration Service installation package and run it on the Citrix server. You do not need to uninstall the previous version of the Citrix Integration Service first.
- If you are upgrading from v7.6 or earlier, remove the current version of the Citrix Integration Service first, then create a v7.8 Citrix Integration Service installation package and run it on the Citrix Server.

The steps are as follows:

1. If you are running v7.6 or earlier, uninstall your current Citrix Integration Service version.
2. Upgrade your Websense Web Security solution to the current version.

   See *Upgrading Websense Web Security Solutions*, page 351.

   > **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 299.

   b. *Configure the Citrix Integration Service installation package*, page 299.

   c. *Use the installation package to install Citrix Integration Service on a Citrix server*, page 304.

Configuring user access on Citrix servers

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 or 6.5.

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 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.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 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 manage 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® ASA 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 *Managing Internet requests from Citrix server users*, page 294.

Websense policy management is enabled by installing the Websense Citrix Integration Service on each Citrix server. See *Citrix Integration Service installation overview*, page 297, 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 309, for configuration information.

Configuration

To use a Websense Web Security solution to manage 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 297, 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 processed twice. See *Configuring the non-Citrix integration*, page 308.

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 processed 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.

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 the Web Security manager and go to **Settings > Network Agent**, then position the mouse over the **Global** menu item.
2. When the lists of IP addresses appears, 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 Web Security Help for instructions on configuring NIC settings.

19 Integrating Web Security with Microsoft Products

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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).

Refer to Installation Instructions: Web Security or Web Filter 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

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

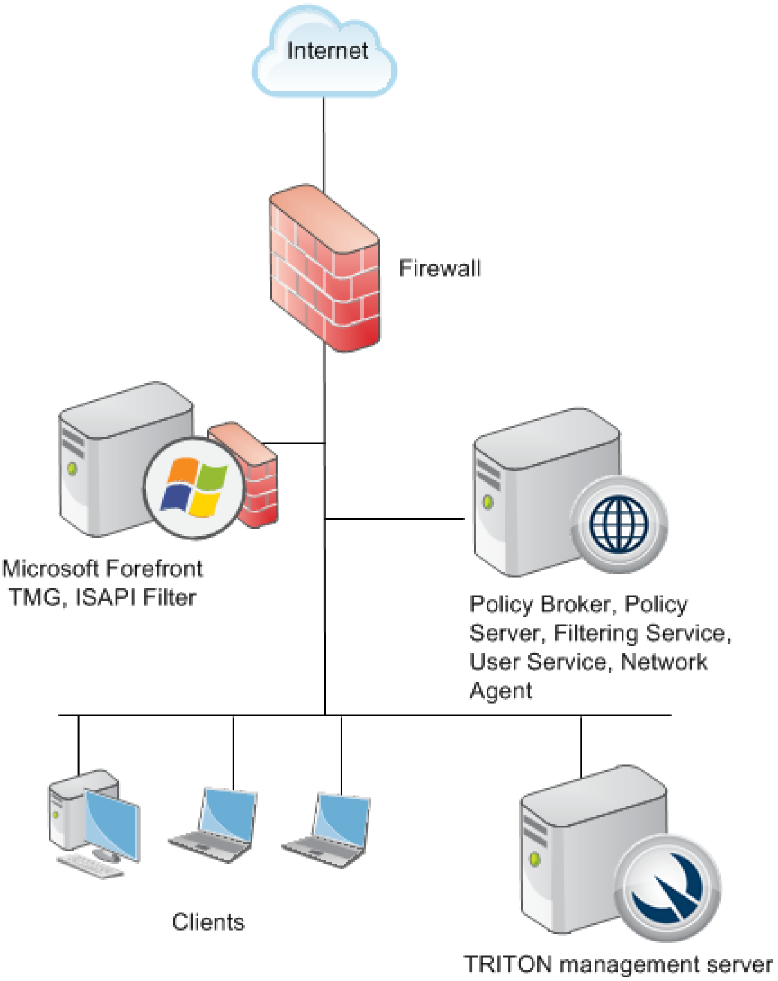
Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Single Microsoft Forefront TMG configuration*, page 312 ◆ *Array configuration*, page 313

Single Microsoft Forefront TMG configuration

The following illustration shows placement of Websense policy enforcement and management 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.

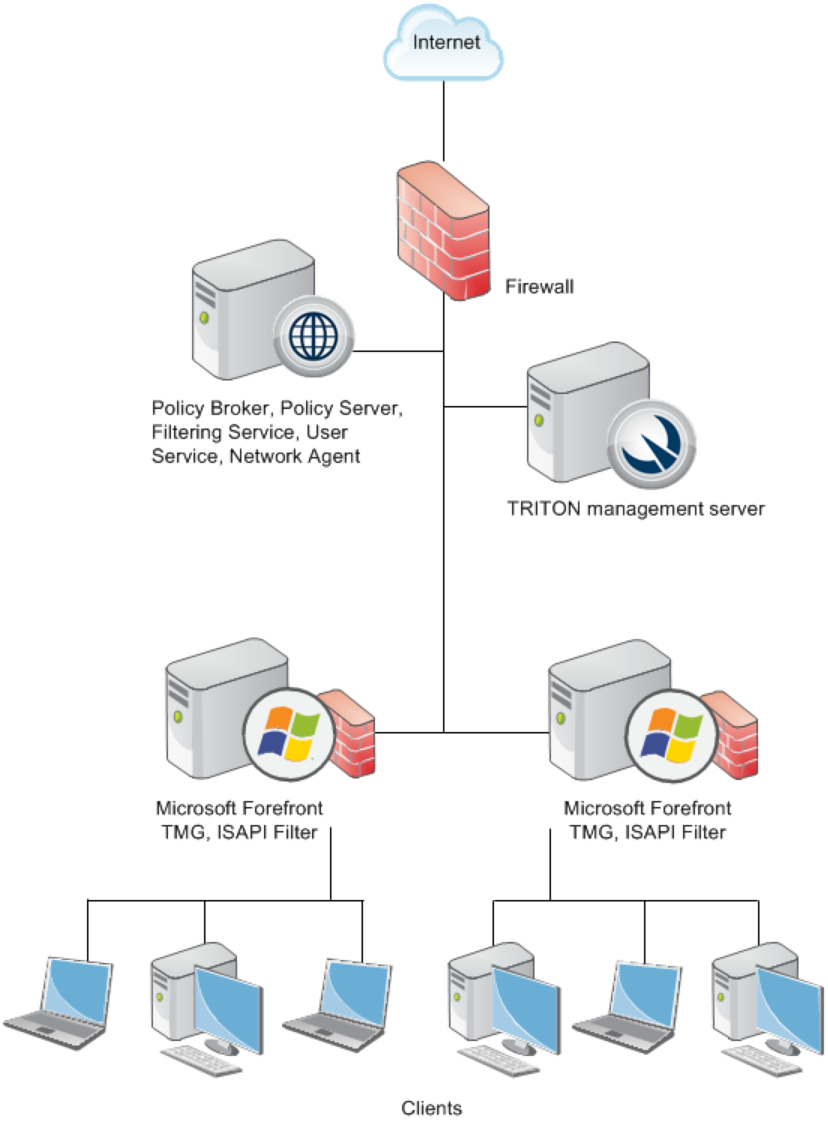

Internet
Firewall
Microsoft Forefront TMG, ISAPI Filter
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent
Clients
TRITON management server

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 management server
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 7.8.x

Applies to:

◆ Web Filter and Web Security, v7.8.x

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).

   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 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).

The TRITON Unified Installer is used to install the Websense ISAPI Filter plug-in for Forefront TMG on the TMG machine.

Important

◆ 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 prompted 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 TRITON Unified Installer to the TMG machine. This installer is available at mywebsense.com.

◆ Close all applications and stop any antivirus software.

To perform the installation:

1. Log on to the TMG machine with domain admin privileges.
2. Right-click **TRITON78xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progess dialog box appears, as files are extracted.

3. On the Welcome screen, click **Start**.
4. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
5. On the Installation Type screen, select **Custom** and then click **Next**.
6. On the Custom Installation screen, click the **Install** link next to Web Security or RiskVision.
7. On the Select Components screen, select **Filtering Plug-in**, then click **Next**.
8. 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.
9. On the **Installation Directory** screen, accept the default location and click **Next**.
10. 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.
11. 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:

a. Go to **Start > Administrative Tools > Services** or **Server Manager > Tools > Services**.

b. 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. Network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

12. 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:

    a. Go to **Start** > **Administrative Tools** > **Services** or **Server Manager** > **Tools** > **Services**.

    b. 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.

13. On the **Installation Complete** screen, click **Done**.
14. 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 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 TRITON Unified 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 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

When you remove the ISAPI Filter plug-in from a Forefront 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:

a. Go to **Start** > **Programs** > **Administrative Tools** > **Services** or **Server Manager** > **Tools** > **Services**.

b. 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:
        a. Go to **Start** > **Administrative Tools** > **Services** or **Server Manager** > **Tools** > **Services**.
        b. Right-click **Microsoft Forefront TMG Firewall**, 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 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

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.

1. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the Web Security Help for instructions.
2. 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 427, for instructions. Be sure to remove **only** Filtering Service.

5. Reinstall Filtering Service to integrate with TMG.

   See *Adding Web Security components*, page 422, 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**.

6. Install the ISAPI Filter plug-in on the TMG machine. For instructions, see *Installing Web Security to integrate with Forefront TMG*, page 315.

7. Enable authentication so that users can be properly identified and their Internet requests can be processed. For instructions, see *User identification and authentication with Forefront TMG*, page 326.

Forefront TMG initial setup

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

- If you installed Web Security Log Server, see *Enabling communication with the Log Database when integrated with Forefront TMG*, page 321.
- Websense software filters HTTP, HTTPS, and FTP requests sent to TMG, but cannot manage traffic tunneled over a SOCKS or WinSOCK proxy server. To use Websense Web Filter or Web Security 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 handle (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 322, 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 324, 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 Web Security Help for instructions.
- If you installed Remote Filtering Server in your Websense deployment, configure TMG to not monitor (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 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.x

When you install Web Security Log Server, TMG must be configured to permit communication with the Log Database. This **must** be completed before Internet 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 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Firewall/Forefront TMG Client*, page 322 ◆ *SecureNAT clients*, page 323 ◆ *Configuring the ISAPI Filter plug-in*, page 323

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 handles Internet requests normally.

However, if the proxy server is disabled, Websense software cannot manage 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 323, for additional configuration steps.

✓ **Note**

If the proxy server is disabled, Websense software manages HTTP only; it cannot manage 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 323, 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.

   Hostnames must be entered in ALL CAPS. Entries that are not in all capital letters are not used.
3. If the TMG machine hosts multiple websites, add the names of all the sites being hosted. For example: **webmail.rcd.com**.

   If only one website 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 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Client computer configuration*, page 325 ◆ *Firewall configuration*, page 325

You can configure the ISAPI Filter plug-in to bypass both policy enforcement and logging for certain traffic, based on the user name, hostname, or URL. This may be used for a small group of websites or users, or for machines in a complex proxy-array or proxy-chaining configuration.

To prevent policy enforcement and logging of this traffic, add the user names, hostnames, and URLs that you do not want Websense software to handle 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 policy enforcement 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 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *TMG clients*, page 326 ◆ *Firewall/Forefront TMG and SecureNAT clients*, page 327 ◆ *Web Proxy clients*, page 327 ◆ *Authentication Methods*, page 328 ◆ *Transparent identification*, page 329

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 Web Security Help for more information.

TMG clients

These TMG clients are supported:

- Firewall/Forefront TMG (see *Firewall/Forefront TMG and SecureNAT clients*, page 327)
- SecureNAT (see *Firewall/Forefront TMG and SecureNAT clients*, page 327)
- Web Proxy (see *Web Proxy clients*, page 327)

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 329, 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 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, 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 329, 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 328, 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 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*

Internet Explorer supports all of these authentication methods. Other 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:

- Apply computer and network policies.
- Enable manual authentication to permit user-based policy enforcement.

  See "Manual Authentication" in the Web Security Help for more information.
- Enable transparent identification to permit user-based policy enforcement.

  See *Transparent identification*, page 329, 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. User information is sent to Websense software, which then applies 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 329) in conjunction with Integrated Windows authentication.

Client Certificate authentication

Client Certificate authentication identifies users requesting information about a website. 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 Instructions: Web Security or Web Filter for instructions on installing individual Websense components. See "User Identification" in the 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 Web Security Help for more information and instructionson activating this feature.

Troubleshooting integration with Forefront TMG

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
- Web Filter and Web Security, v7.8.x	- *SecureNAT clients are not receiving the correct policy*, page 330 - *No policy enforcement occurs after the ISAPI Filter plug-in is installed*, page 330

SecureNAT clients are not receiving the correct policy

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 322.

No policy enforcement occurs after the ISAPI Filter plug-in is installed

If users requests are not being handled properly 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.

20 Integrating Web Security using ICAP Service

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 334.

After installing Websense software, configure your proxy to communicate with Websense ICAP Service (see *Configuring the proxy to communicate with ICAP Service*, page 335).

Websense ICAP service may also require configuration (see *Configuring ICAP Service*, page 336) if the default settings are not appropriate for your environment.

To have Internet requests managed 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 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Converting a standalone installation to use ICAP integration*, page 334

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 335
- *Configuring ICAP Service*, page 336

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 335
   - *Configuring ICAP Service*, page 336

Configuring the proxy to communicate with ICAP Service

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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 336, 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 336, 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 the Web Security manager.

  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 the Web Security manager.
- 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 7.8.x

Applies to:

- Web Filter and Web Security, v7.8.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
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

Parameter	Description	Default Value
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**.

21 Installing Web Security for Universal Integrations

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:	In this topic
◆ Web Filter and Web Security, v7.8.x	◆ *Installation steps for universal integrations*, page 340 ◆ *Migrating to a different integration after installation*, page 340

This document describes integrating Websense Web Security solutions with supported integration products other than those addressed in the following topics:

- *Integrating Web Security with Cisco*, page 269
- *Integrating Web Security with Citrix*, page 293
- *Integrating Web Security using ICAP Service*, page 333
- *Integrating Web Security with Microsoft Products*, page 311

The Partners page at websense.com links to pages that list our Security Alliance and Vendor Alliance partners. Refer to the lists of Websense Technology Partners 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.

Installation steps 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 147.

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 policy enforcement, 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 policy enforcement. 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 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 422.
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 tool (Start > Administrative Tools > Services or Server Manager > 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 **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 the Web Security manager 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 Web Security Help.

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

22 Upgrading TRITON Enterprise

Deployment and Installation Center | Web, Data, and Email Security Solutions | v7.8.x

Upgrade TRITON® Enterprise Solutions

If you have more than one Websense TRITON security solution, use the sections below to find the appropriate set of installation instructions.

Websense TRITON Enterprise modules must be at least version 7.7.0 to upgrade to v7.8.x.

Websense TRITON Enterprise

For step-by-step instructions on upgrading from versions 7.6 and 7.7, see the following guides:

- Upgrading TRITON Enterprise v7.6.x to v7.7.x
- Upgrading TRITON Enterprise v7.7.x to v7.8.x

For an outline of the process, see *Upgrade procedure for solutions that include Web, Email, and Data Security*, page 344.

Web Security and Data Security

If you are combining a Web Security and a Data Security solution, in most cases, the best process is to first complete the steps in Upgrade Instructions: Web Security Gateway Anywhere. This document guides you through upgrading:

- All Web Security Gateway Anywhere components
- Data Security Management Server components (which reside on the TRITON management server)

After completing those steps, see the Data Security instructions for Upgrading from v7.7.x to v7.8.x for instructions on upgrading additional components, like the Protector and agents.

Web Security and Email Security

If you are combining a Web Security and an Email Security Gateway solution, in most cases, the best process is to follow the steps in the Websense TRITON Enterprise Upgrade Guide. This document guides you through upgrading:

- All Web Security Gateway Anywhere components
- All Email Security Gateway Anywhere components
- Data Security Management Server components (which enable the Web DLP features of Web Security Gateway Anywhere, if purchased, and the Email DLP features of Email Security Gateway)

Email Security and Data Security

If you are combining an Email Security Gateway and a Data Security solution, in most cases, the best process is to follow the steps for Upgrading Email Security Gateway v7.7.x to v7.8.x. This document guides you through upgrading:

- All Email Security Gateway Anywhere components
- Data Security Management Server components (which reside on the TRITON management server)

After completing those steps, see the Data Security instructions for Upgrading from v7.7.x to v7.8.x for instructions on upgrading additional components, like the Protector and agents.

Upgrade procedure for solutions that include Web, Email, and Data Security

Deployment and Installation Center | Web, Data, and Email Security Solutions | v7.8.x

This outline 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.)

For complete instructions see:

- Upgrading TRITON Enterprise v7.6.x to v7.7.x
- Upgrading TRITON Enterprise v7.7.x to v7.8.x

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.
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.
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.
4. Upgrade the **TRITON management server**. All modules on the machine are upgraded in the correct order.
5. Upgrade Web Security **Log Server**. All components on the machine are upgraded in the correct order.
6. Upgrade Email Security **Log Server**. All components on the machine are upgraded in the correct order.
7. 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.
8. Upgrade any additional Web Security server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines.
9. Upgrade any additional Data Security server components and agents, including supplemental servers, SMTP agents, ISA/TMG agents, printer agents, protectors, and mobile agents.
10. Upgrade client components, including the logon application (LogonApp.exe), Remote Filtering Client, Web Endpoint, and Data Endpoint.

Upgrading the TRITON management server

Deployment and Installation Center | Web, Data, and Email Security Solutions | v7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x and v7.7.x ◆ Data Security, v7.7.x ◆ Email Security Gateway and Email Security Gateway Anywhere, v7.7.x	◆ *TRITON Infrastructure*, page 346 ◆ *Web Security*, page 347 ◆ *Data Security*, page 348 ◆ *Email Security*, page 348

To upgrade TRITON management server components, use the v7.8.2 TRITON unified installer (Windows only): **WebsenseTRITON782Setup.exe**, available from:

www.websense.com/MyWebsense/Downloads/

Select your **product**, **version** (7.8.2), 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 (such as 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.

Wizard Screen	Fields
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A popup message appears at this stage, warning that you must also upgrade all modules. This popup may be hidden behind the main installer window, so if your installation appears to freeze, locate the hidden popup by moving the main installer window, and click **OK** to proceed with the installation.
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 (https://<IP_address_or_hostname>:9443/triton/).
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. Click **Deploy**.

For information on upgrading other Data Security components, such as supplemental servers, agents, and endpoints, refer to *Upgrading Data Security to v7.8.x*, page 393.

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.

Wizard Screen	Fields
Configuration	This page shows the IP address of the database engine configured to manage the Email Security Log Database and the logon type. If you have changed the database since your previous installation, modify the settings here.
Pre-Installation Summary	This screen shows: ◆ 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.
Installation	This screen shows that the installation is progressing. The Email Security Gateway manager 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.

23 Upgrading Websense Web Security Solutions

Deployment and Installation Center | Web and Data Security Solutions | Version 7.8.x

Upgrade Web Security Solutions

To get started, use the following list to find the upgrade path for your Web Security or Web and Data Security solution:

- Websense Web Filter and Web Security software-only deployments (no V-Series appliances) at versions **7.6.0 - 7.7.x** may be directly upgraded to version 7.8.x.

  If this describes your deployment, jump to either:

  - Upgrade Instructions: Web Filter and Web Security (a start-to finish PDF)
  - *Before upgrading Web Security to v7.8*, page 354, the starting point for online upgrade instructions

- Content Gateway and Data Security components must be upgraded to **v7.7** before you can upgrade to v7.8.x. V-Series appliances must first be upgraded to v7.8.1 before being upgraded to v7.8.2 or v7.8.3.

  As a result, all Websense Web Security Gateway and Gateway Anywhere deployments (software) must be at version **7.7.x** to upgrade directly to version 7.8.x. All Websense Web Security Gateway and Gateway Anywhere deployments on V-Series appliances must be at version 7.7.x, upgrade to version 7.8.1, and then to version 7.8.2 or 7.8.3.

  If all of your components are at v7.7.x, hotfix 94 must be applied to v7.7.x prior to upgrading Content Gateway (software or appliance) to v7.8.x. This retains the default Sync Mode setting and can prevent latency sometimes caused by Async scanning. Go to Select one of the following documents for instructions on installing Hotfix 94 and upgrading to v7.8.x:

  - Upgrade Instructructions: Web Security Gateway (start-to-finish PDF)
  - Upgrade Instructions: Web Security Gateway Anywhere (start-to-finish PDF)

  Otherwise, see *Web Security or Web and Data Security upgrade outline*, page 352, to work through the upgrade process.

- If you are upgrading from a version prior to v7.6.x, jump to *Upgrading from Web Security version 7.5.x or earlier*, page 352.

Policy information and most configuration details are preserved across intermediate upgrades.

Web Security or Web and Data Security upgrade outline

Deployment and Installation Center | Web and Data Security Solutions | Version 7.8.x

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
   - V-Series Appliance
   - Websense Data Security
2. Before beginning the upgrade process, see:
   - *Before upgrading Web Security to v7.8*, page 354
   - Appliance Upgrade Guide
3. When you are ready to start upgrading, see *Upgrading Web Security or Web and Data Security solutions from v7.6 or v7.7*, page 361.

   This procedure includes both software and appliance instructions.
4. After upgrade, see the Upgrading Admin 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 7.5.x or earlier

Deployment and Installation Center | Web Security Solutions | Version 7.5.x and earlier

Applies to:

◆ Web Filter, Web Security, and Web Security Gateway, v7.5.x and earlier

Versions 7.0.x and 7.1.x and earlier must be upgraded to version 7.6 or 7.7 before they can be upgraded to version 7.8.x.

- Websense Content Gateway and V-Series appliances must be at v7.7.x to upgrade to v7.8. (Note that V-Series appliances must first upgrade to v7.8.1 before upgrading to v7.8.2 or 7.8.3.)
- Data Security components (included with Web Security Gateway Anywhere) must be at v7.7.x to upgrade to v7.8.

For example, the path might be:

v7.0 (Web Filter, software-only) > v7.5 > v7.7 > v7.8

v7.1.1 (Web Security Gateway) > 7.6 > v7.7 > v7.8

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
- v7.7 software Upgrade Instructions
- v7.7 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 395, 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 v7.8.x is to perform a fresh installation at the current version. See *Installing Web Security solutions*, page 147.

After upgrading Web Security to v7.6 or v7.7, see the following start-to-finish PDF instructions to upgrade to v7.8:

- Upgrade Instructions: Web Filter and Web Security
- Upgrade Instructructions: Web Security Gateway
- Upgrade Instructions: Web Security Gateway Anywhere

Before upgrading Web Security to v7.8

Deployment and Installation Center | Web Security Solutions | Version 7.6.x - v7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x - v7.8.x	◆ *Restart services before starting the upgrade*, page 356 ◆ *Internet access during the upgrade process*, page 356 ◆ *Find your upgrade procedure*, page 356

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 4.
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 8.
3. Make sure that your integration product (if any) is supported in v7.8. If necessary, upgrade your integration product before beginning the Websense software upgrade.
   - Integration with Squid Web Proxy Cache is not supported in v7.8.x.
   - Integration with CheckPoint products is not supported in v7.8.x.
   - Integration with Microsoft ISA Server is not supported in v7.8.x. For information about integration with Microsoft Forefront TMG, see *Integrating Web Security with Microsoft Products*, page 311.
   - Supported Citrix versions have changed. In addition, the Citrix Integration Service changed substantially in v7.6. See *Integrating Web Security with Citrix*, page 293, before upgrading Websense software.
   - To review current Cisco integration requirements, see *Integrating Web Security with Cisco*, page 269.

- 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 the current version.

  - If you are moving from an on-box integration, next install the current version 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 the Web Security manager, 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 333, 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 339.

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 357.
   - For V-Series Appliance backup instructions, see Using the backup utility in Appliance Manager Help.
   - For TRITON settings, see *Backing up TRITON infrastructure settings*, page 358.

5. Before upgrading Websense Filtering Service, make sure that the Filtering Service machine and the TRITON management server have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.

6. 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 358.

7. 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 tool (**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.

8. If your deployment includes V-Series appliances, see the Appliance Upgrade Guide 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:
  - *Windows*: Navigate to the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin, by default) and enter the following command:

    ```
    WebsenseAdmin restart
    ```

  - *Linux*: Navigate to the **Websense** directory (/opt/Websense/, by default) and enter the following command:

    ```
    ./WebsenseAdmin restart
    ```

- 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 Security or Web and Data Security solutions from v7.6 or v7.7*, page 361.

Backing up Web Security configuration

Deployment and Installation Center | Web Security Solutions | Version v7.6.x - v7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x - v7.8.x

Before upgrading to a new version of any Websense Web Security solution, 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 all Websense services on the machine.
   - *Windows*: Navigate to the Websense **Web Security** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\, by default) and enter the following command:

     ```
     WebsenseAdmin stop
     ```

   - *Linux*: Navigate to the **/opt/Websense/** directory and enter the following command:

     ```
     ./WebsenseAdmin stop
     ```

2. Use the following command to run the Backup Utility:
   - *Windows*: From the Websense **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin), enter the following command:

     ```
     wsbackup -b -d <directory>
     ```

   - *Linux*: From the **/opt/Websense/** directory, enter the following command:

     ```
     ./wsbackup -b -d <directory>
     ```

   For these commands, <*directory*> is the path where the backup file will be stored.

   The Backup Utility saves the essential Websense software files on the machine on which it is run, including any custom block pages. A complete list of the files saved can be found in the 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.

3. Start the Websense services. The Websense services must be running when you start the upgrade.
   - *Windows*: From the Websense **Web Security** directory, enter the following command:

     ```
     WebsenseAdmin start
     ```

   - *Linux*: From the **/opt/Websense/** directory, enter the following command:

     ```
     ./WebsenseAdmin start
     ```

Also back up your TRITON Infrastructure settings. See *Backing up TRITON infrastructure settings*, page 358.

Backing up TRITON infrastructure settings

Deployment and Installation Center | Web Security Solutions | Version 7.6.x - 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x - v7.8.x

Use the TRITON backup utility to back up your TRITON Settings information (administrator accounts, for example).

1. On the TRITON management server machine, go to **Start** > **Administrative Tools** > **Task Scheduler**, then select **Task Scheduler Library**.
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**. By default, the backup files are stored on the C drive.

Preparing the Web Security Log Database for upgrade

Deployment and Installation Center | Web Security Solutions | Version 7.6.x - v7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x - v7.8.x

It is important that you back up your current Websense reporting databases, stop Log Server, and do one of the following before upgrading to ensure the integrity of your reporting data:

- *Microsoft SQL Server Standard or Enterprise*: Stop any active SQL Server Agent jobs. After upgrade, reactivate the jobs to resume normal database operations.

- *SQL Server Express*: Restart the **MSSQLSERVER** service to make sure no Browser Service jobs are running.

> **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.

Step 1: Back up the databases and stop Log Server

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**.

Step 2: Make sure no database jobs are running

If you have Microsoft SQL Server Express, use the Windows Services tool to restart the **MSSQLSERVER** service.

If you have a full version of Microsoft SQL Server:

1. Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).
2. 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_AMT_ETL_wslogdb70
   - Websense_IBT_DRIVER_wslogdb70
   - Websense_Trend_DRIVER_wslogdb70
   - Websense_Maintenance_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.

Step 3: Upgrade and re-enable the jobs

1. Perform the Websense upgrade.

2. After upgrade, if you have a full version of SQL Server, enable the disabled jobs to resume normal database operations.

Web Security upgrade order

Deployment and Installation Center | Web Security Solutions | Version 7.0.x - v7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.8.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 (primary or standalone)

   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. Replica Policy Brokers (when upgrading from v7.8.1)

   Upgrade replica Policy Brokers after the primary has been upgraded and before attempting to upgrade any Policy Servers associated with them. If Policy Server is installed on the same machine, it will be upgraded at the same time.

3. Policy Server

   Runs on all **user directory and filtering** appliances, and may run on other Windows or Linux servers.

4. User Service, Filtering Service, and Directory Agent

   This includes all **filtering only** appliances, and may include other Windows or Linux servers.

5. 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 358.

6. TRITON management server
7. Network Agent, Content Gateway
8. Transparent identification agents, Remote Filtering Server, Filtering plug-in (Citrix XenApp or Microsoft Forefront TMG)

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
- *Websense Endpoint Clients*, page 267

Upgrading Web Security or Web and Data Security solutions from v7.6 or v7.7

Deployment and Installation Center | Web Security Solutions | Version 7.6.0 - v7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.0 - v7.7.x
- Data Security, v7.6.0, v7.6.2 and v7.7.x

This procedure covers the steps required to upgrade any Web Security solution, or Web and Data Security solutions together, from v7.6.0 - v7.7.x to v7.8.

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:
   - *v7.8 Web Security software upgrade instructions (Windows)*, page 362
   - *v7.8 Web Security software upgrade instructions (Linux)*, page 366
   - *Upgrading V-Series Appliances to v7.8.x*, page 391
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:
   - *v7.8 Web Security software upgrade instructions (Windows)*, page 362
   - *v7.8 Web Security software upgrade instructions (Linux)*, page 366
   - *Upgrading V-Series Appliances to v7.8.x*, page 391
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:

- *v7.8 Web Security software upgrade instructions (Windows)*, page 362
- *v7.8 Web Security software upgrade instructions (Linux)*, page 366
- *Upgrading V-Series Appliances to v7.8.x*, page 391

4. Upgrade Websense **Log Server**. All components on the machine are upgraded in the correct order. For instructions, see *v7.8 Web Security software upgrade instructions (Windows)*, page 362.
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:
   - *v7.8 Web Security software upgrade instructions (Windows)*, page 362.
   - *Upgrading Data Security to v7.8.x*, page 393.
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 v7.8.x*, page 371.
   - *v7.8 Web Security software upgrade instructions (Windows)*, page 362
   - *v7.8 Web Security software upgrade instructions (Linux)*, page 366
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:
   - *v7.8 Web Security software upgrade instructions (Windows)*, page 362
   - *v7.8 Web Security software upgrade instructions (Linux)*, page 366
   - *Upgrading Data Security to v7.8.x*, page 393

When you are finished, see:

- *Websense Endpoint Clients*, page 267, 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).

v7.8 Web Security software upgrade instructions (Windows)

Deployment and Installation Center | Web Security Solutions | Version 7.6.x and 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x and v7.7.x

Use the version 7.8 TRITON Unified Installer (**WebsenseTRITON784Setup.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 Security or Web and Data Security solutions from v7.6 or v7.7*, page 361, 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 v7.6 or v7.7, and you have not restarted the upgraded machines, perform a restart before beginning the v7.8 upgrade.
- Perform a full system backup. See *Backing up Web Security configuration*, page 357.

> **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 the TRITON console.
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 358.

4. Close all applications and stop any antivirus software.

> **Warning**
>
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

5. Go to the **Downloads** tab of mywebsense.com to download the TRITON Unified Installer.
   - The installer file is **WebsenseTRITON784Setup.exe**.
   - Installer files occupy approximately 2 GB of disk space.
6. Double-click **WebsenseTRITON784Setup.exe** to launch the installer. A progress dialog box appears, as files are extracted.
7. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
8. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
9. On the **Websense Upgrade** screen, select **Start the upgrade**, then click **Next**.
10. 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 C:\Program Files (x86)\Websense\Web Security\bin\WebsenseAdmin stop command, or the Windows Services dialog box, to stop the services. Once you have manually stopped the services, return to the installer.
11. 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.

    The upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.
12. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
13. Reboot the machine.

> **Important**
>
> The machine must be rebooted to complete the upgrade process.

14. If you stopped your antivirus software, restart it.

15. Re-enable SQL Server Agent jobs if you disabled them prior to upgrade.

    See *Preparing the Web Security Log Database for upgrade*, page 358.

16. If you have an integration product installed, additional upgrade steps may be necessary. See:

    - *Integrating Web Security with Cisco*, page 269
    - *Integrating Web Security with Citrix*, page 293
    - *Integrating Web Security with Microsoft Products*, page 311
    - *Installing Web Security for Universal Integrations*, page 339

17. Repeat the upgrade procedure on each machine running Web Security components, in the recommended order (see *Web Security upgrade order*, page 360).

    All components that interact must be upgraded to the same version.

    If you have complete installations in separate locations that do not interact, they do not have to run the same Websense software version.

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 420.

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.

v7.8 Web Security software upgrade instructions (Linux)

Deployment and Installation Center | Web Security Solutions | Version 7.6.x and 7.7.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6.x and 7.7.x

Use the Linux installer (**WebsenseWeb784Setup_Lnx.tar.gz**) to upgrade existing v7.6 or v7.7 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 357.

If Websense components are installed on multiple machines, see *Web Security upgrade order*, page 360, for important information about the required upgrade sequence.

Important

Upgrade the primary (or standalone) Policy Broker machine first, then any replica Policy Broker machines, 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 the TRITON console.
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 16, 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, use the **/opt/Websense/WebsenseAdmin restart** command to restart the services manually before beginning the upgrade.

6. Download the Web Security Linux installer from the Downloads page at mywebsense.com. The installer file is called **WebsenseWeb784Setup_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 155, 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. 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**.

11. 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 using the **/opt/Websense/WebsenseAdmin stop** command. You can leave the installer running when you do so. Once you have manually stopped the services, return to the installer.
12. 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.
13. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
14. Reboot the machine.

> **Important**
>
> The machine must be rebooted to complete the upgrade process.

15. If you stopped your antivirus software, restart it.

16. If you have an integration product installed, additional upgrade steps may be necessary. See:
    - *Integrating Web Security with Cisco*, page 269
    - *Integrating Web Security with Citrix*, page 293
    - *Integrating Web Security using ICAP Service*, page 333
    - *Integrating Web Security with Microsoft Products*, page 311
    - *Installing Web Security for Universal Integrations*, page 339
17. Repeat the upgrade procedure on each machine running Web Security components, in the recommended order (see *Web Security upgrade order*, page 360).

    All components that interact must be upgraded to the same version.

    If you have complete installations in separate locations that do not interact, they do not have to run the same Websense software version.
18. After all components have been upgraded, see *Initial Configuration for All Websense Modules*, page 407.

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 420.

24 Upgrading Content Gateway to v7.8.x

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

Applies to:	In this topic
◆ Web Security Gateway and Web Security Gateway Anywhere v7.7.x and earlier	◆ *System requirements* ◆ *Versions supported for direct upgrade to v7.8.1* ◆ *Upgrading distributed components* ◆ *Preparing to upgrade* ◆ *Upgrading Websense Content Gateway* ◆ *Post-upgrade activities*

This section provides upgrade instructions for software-based Websense Content Gateway installations.

> ✓ **Note**
> Upgrading Content Gateway on a V-Series appliance is handled by the V-Series upgrade (patch) process. See *Upgrading V-Series Appliances to v7.8.x*.

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.

Versions supported for direct upgrade to v7.8.1

Direct upgrade to Content Gateway v7.8.1 is supported from v7.7.0 and v7.7.3. Upgrades from earlier versions require intermediate upgrades:

- version 7.0/7.1 > version 7.5 > version 7.6 > version 7.7 > version 7.8.x

Important

Follow the upgrade procedures for each intermediate version.

Read the Websense Content Gateway Installation Guide and its upgrade supplement for each version.

See:

- Version 7.5 Content Gateway Installation Guide
- Version 7.6 Content Gateway Installation Guide
- Version 7.7 Content Gateway Installation Guide

To perform an intermediate upgrade, download the installer package for that version from the Websense Downloads site.

System requirements

Before upgrading Content Gateway, make sure the installation machine meets the system requirement outlined 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. **Several Web Security components must be upgraded prior to upgrading Content Gateway.** Distributed components must be upgraded in a particular order. See *Upgrading Websense Web Security Solutions*.

Preparing to upgrade

There are several large and important changes beginning in version 7.8.2. Please read the 7.8.3Release Notes before starting the upgrade.

SSL support

SSL support is rearchitected in version 7.8. Most SSL configuration settings are saved and applied to the upgraded Content Gateway.

During upgrade:

- The v7.7.x SSL SQLite3 database is converted to a new database file.
- The Incident list is retained.

- Dynamic certificates are not retained. All other certificates are retained.
- The Certificate Authority Tree is retained (trusted Root CA tree).
- SSLv2 is no longer enabled by default. If it is enabled prior to upgrade, the setting is retained.
- CRL and OCSP revocation statistics (on Monitor > SSL > CRL Statistics) are retained.
- Customized certificate failure and connect error message pages are not retained.
- SSL **inbound*.log** and **outbound*.log** files are deleted. After upgrade, transaction logging is sent to **extended.log** or **squid.log** when the logging subsystem is configured for “Log Transactions and Errors” or “Log Transactions Only”. Otherwise, logging is sent to **content_gateway.out**.

Before upgrading:

- Consider performing maintenance on the Incident list; remove unwanted entries.
- Note customizations to certificate failure and connect error message pages. The code structure of the pages has changed; you cannot simply reapply (paste) the 7.7.x HTML.

User authentication

The upgrade process converts existing Multiple Realm Authentication rules into equivalent Rule-Based Authentication rules, with some important changes in structure.

Consolidated credential caching

There is one credential cache for both explicit and transparent proxy mode, and one Global Authentication Options page for setting the caching method and Time-To-Live.

During upgrade:

- (For upgrades from 7.7.x to 7.8.x) The credential cache Enabled/Disabled setting for explicit proxy is retained from the Global Authentication Options tab. Caching for transparent proxy traffic is always enabled.
- The Authentication Mode setting (IP address or Cookie mode) is retained from the Transparent Proxy Authentication tab.
- The Cache TTL value is retained from Transparent Proxy Authentication tab unless the value on the Global Authentication Options tab is not the default, in which case the customized value is used. The cache TTL value is in minutes.
- IP addresses and ranges on the Global Authentication Options Multi-user IP Exclusions list are moved to the cookie cache IP address list.
- If cookie caching is enabled in a Multiple Realm rule, the source IP addresses from that rule are copied to cookie cache IP address list.

Integrated Windows Authentication (IWA)

After upgrade, always check and, if necessary, rejoin IWA domains.

- Upgrade to version 7.8.1 should preserve exiting IWA domain joins.
- Upgrade to version 7.8.2 breaks IWA domain joins. Therefore, IWA domains must be rejoined.

> **Important**
>
> If your deployment uses IWA and a load balancer:
>
> - Version 7.8.1 does not support the configuration.
> - Versions 7.8.2 and 7.8.3 support load balancers, however, post-upgrade a special configuration must be applied. Follow the configuration steps described in the v7.8.2 Release Notes or the v7.8.3 Release Notes.

Features to configure after upgrade

You may want to review and configure the following enhanced features post-upgrade.

- Range-based IP spoofing. If you use IP spoofing, see the Help system for information about how range-based IP spoofing can address a boarder range of source IP address requirements when traffic is routed through Content Gateway.
- WCCP configuration synchronization in a cluster. It's now possible to disable WCCP configuration synchronization.

Upgrading Websense Content Gateway

Content Gateway runs on Websense full policy source, user directory and filtering, and filtering only appliances (all of which should already have been upgraded at this point).

Content Gateway is also:

- **Certified** on Red Hat Enterprise Linux, updates 4 and 5
  - Kernel version for 6.5: 2.6.32-431 (not recommended for v7.8.3 Content Gateway)
  - Kernel version for 6.4: 2.6.32-358
- **Supported** on Red Hat Enterprise Linux and CentOS 6, updates 0, 1, 2, 3, 4, and 5
  - Kernel version for 6.3: 2.6.32-279
  - Kernel version for 6.2: 2.6.32-220
  - Kernel version for 6.1: 2.6.32-131
  - Kernel version for 6.0: 2.6.32-71

To display the kernel version installed on your system, enter the command:

```
/bin/uname -r
```

If you have software instances of Content Gateway, make sure the host system meets the following hardware requirements before upgrading:

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum 8 GB recommended
Disk Space	2 disks: ◆ 100 GB for the operating system, Content Gateway, and temporary data. ◆ Max 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

In addition, to support **transparent proxy** deployments:

Router	Must support WCCP v2. A Cisco router must run IOS 12.2 or later. The latest version is recommended. 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).

Next, choose your upgrade procedure:

- For Content Gateway v7.7.x hosted on Red Hat Enterprise Linux **6 series**, see the section “Content Gateway: RHEL 6 upgrade instructions” below.

- For Content Gateway v7.7.x hosted on Red Hat Enterprise Linux **5 series**, see the section “Content Gateway: Upgrade Red Hat Enterprise Linux 5-series to 6-series during the Content Gateway upgrade” below.

Content Gateway: RHEL 6 upgrade instructions

This section describes upgrading Content Gateway v7.7.x to v7.8.x on your pre-existing Red Hat Enterprise Linux 6 host. If you are also upgrading Red Hat Enterprise Linux 5 to Red Hat Enterprise Linux 6, see the section “Content Gateway: Upgrade Red Hat Enterprise Linux 5-series to 6-series during the Content Gateway upgrade” below.

Important

At the beginning of the upgrade procedure, the installer checks to see if the partition that hosts **/opt** has enough space to hold a copy of the existing Content Gateway log files (copied to **/opt/WCG_tmp/logs**). If there’s not enough space, the installer prints an error message and quits.

In this situation, if you want to retain the log files you must copy the contents of **/opt/WCG/logs** to a location that has enough space, and then delete the log files in **/opt/WCG/logs**.

When the upgrade is complete, move the files from the temporary location back to **/opt/WCG/logs** and delete the files in the temporary location.

Note

If you have multiple Content Gateway instances deployed in a cluster, you **do not** have to disable clustering or VIP (if used). As each member of the cluster is upgraded it will rejoin the cluster.

1. If your Web Security Gateway solution is deployed with Data Security, log on to the Content Gateway manager and go to the **Configure** > **My Proxy** > **Basic** page and disable Data Security.

   When the upgrade is complete, return to the **Configure** > **My Proxy** > **Basic** page, enable Data Security, and restart Content Gateway. Then, navigate to the **Configure** > **Security** > **Data Security** page and confirm that automatic registration was successful. If it was not, manually register with Data Security.

2. Log on to the Content Gateway Linux host and acquire root permissions:

   ```
   su root
   ```

3. Disable any currently running firewall on this machine for the duration of the upgrade. Bring the firewall back up after the 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 7.8.x installer from mywebsense.com and save it to a temporary directory. For example, place it in:

   ```
   /tmp/wcg_v78
   ```

5. Unpack the Content Gateway installer tar archive:

   ```
   cd /tmp/wcg_v78
   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. If you intend to upgrade Red Hat Enterprise Linux 6.x to a more recent version, perform the upgrade now. See your Red Hat Enterprise Linux documentation.

7. In the directory where you unpacked the tar archive (for example, /tmp/wcg_78), 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.

8. If your server does not meet the minimum hardware requirements or is missing required operating system packages, you will receive error or warning messages. For example:

   ```
   Error: Websense Content Gateway v7.8.x on x86_64 requires
   several packages that are not present on your system.
   Please install the following packages: <list of packages>
   ```

```
If you are connected to a yum repository you can install
these packages with the following command:
yum install <list of packages>
See the Websense Technical Library (www.websense.com/
library) for information about the software requirements
for x86_64 installation.
```

You may run into this error because 32-bit packages were required for v7.7.x and 64-bit libraries are required for v7.8.x.

To make it easier to install the needed packages, the Content Gateway distribution includes a Linux “rpm” containing the needed packages. To install its contents, ensure that the operating system has access to the Red Hat Linux distribution library (for example the DVD), and enter:

```
yum install wcg_deps-1-0.noarch.rpm
```

Upon successful completion, a list of updated packages is displayed and then the word “Complete!”.

Here is an example of a system resource warning:

```
Warning: Websense Content Gateway requires at least 6
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 upgrade. You should not install or upgrade on a system that does not meet the minimum requirements. If you choose to run Content Gateway after receiving a system resource warning, performance and stability may be affected.

9. Read the subscription agreement. At the prompt, enter **y** to accept the agreement and continue the upgrade, or **n** to cancel.

   ```
   Do you accept the above agreement [y/n]? y
   ```

10. The installer checks for the presence of an existing Content Gateway installation. When asked, choose to replace the existing version with version 7.8.x.

    ```
    WCG version 7.7.n-nnnn was found.
    Do you want to replace it with version 7.8.x-nnnn [y/n]? y
    ```

11. 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/
    7.7.0-1418-PreUpgrade/...done
    Zipping configuration archive...done
    Moving log files from /opt/WCG/logs to /opt/WCG_tmp/logs/
    ...done
    ```

12. You can either re-use the installation selections you entered during the last install, or provide new answers to all installation prompts, such as admin password, admin email address, Policy Server IP address, etc.:

    ```
    Previous installation selections </root/WCG/Current/
    WCGinstall.cfg> found.
    Use previous 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.

13. If you answered **y** at Step 11, then you can also leave proxy settings at their current values or revert to Websense default values (which perform a fresh install!).

    ```
    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.

    Caution: If you answer **n** (no), the current installation of Content Gateway is removed, and a fresh install of 7.8.x begins. See Installing Websense Content Gateway for a detailed description of the installation procedure. This is not an upgrade, but rather a fresh install.

14. The previously installed version of Websense Content Gateway is removed, and the settings and selections you chose to retain are re-used. Details of the upgrade process are output to the screen. Please wait.

    ```
    *COMPLETED* Websense Content Gateway 7.8.x-nnnn
    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 automated portion of 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
```

To finish the upgrade, be sure to perform the post-upgrade instructions at the end of this document.

Content Gateway: Upgrade Red Hat Enterprise Linux 5-series to 6-series during the Content Gateway upgrade

Content Gateway versions 7.7.x run on Red Hat Enterprise Linux 5-series and 6-series.

Content Gateway version 7.8.x runs on 64-bit, Red Hat Enterprise Linux 6-series only.

Use the following procedure to upgrade the host operating system while upgrading Content Gateway. Read it completely before beginning the process.

Important

If you want to retain the existing Content Gateway log files (in **/opt/WCG/logs**), determine their total size, identify a location on your network that has enough space to hold the files, and copy them there.

When the upgrade is complete, copy the files back to /opt/WCG/logs and delete the files from the temporary location.

1. Log on to the Content Gateway v7.7.x host and acquire **root** privileges. All steps must be performed as root.
2. Obtain the Content Gateway v7.8.x gzip installation file, place it on the v7.7.x machine, and use the v7.8.x **wcg_config_utility.sh** script and **configFiles.txt** support file to backup your system.
   a. Download the Content Gateway v7.8.x installer from mywebsense.com. Save it in a convenient location on the network; you'll need it again later. Place a copy in a temporary directory on your Content Gateway server (the Red Hat Enterprise Linux 5-series system). For example, place it in:

      ```
      /tmp/wcg_v78
      ```

   b. Unpack the installer gzip archive:

      ```
      cd /tmp/wcg_v78
      ```

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

c. In /tmp/wcg_v78 unpack **lx86inst.tar**:

```
tar -xvf lx86inst.tar
```

This tar command does not use the 'z' flag because the tar file is not a gzip.

d. Change directory to scripts:

```
cd ./scripts/
```

e. Using **wcg_config_utility.sh** create a backup of Content Gateway v7.7.x and save it to a trusted location on the network:

```
./wcg_config_utililty.sh create WCGbackup
```

This creates **WCGbackup.tar.gz** in the current directory.

3. Copy **WCGbackup.tar.gz** to a reliable location on the network where it can easily be retrieved after the operating system upgrade.
4. If you are upgrading Red Hat Enterprise Linux on this machine, uninstall Content Gateway. See Uninstalling Content Gateway and continue with Step 6.
5. If you want to keep the current machine as a fallback option, power down the computer and disconnect it from the network.

> **Note**
>
> You can only revert to the original machine if the other Web Security components are also reverted to the matching (original) 7.7.x version. When that is the case, you can simply reconnect the Content Gateway host machine to the network and power up. Content Gateway v7.7.x will re-register with 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.

6. Applying the same hostname, ethernet interface, and IP address used with Red Hat Enterprise Linux 5, install Red Hat Enterprise Linux 6. Updates 6.4 and 6.5 are certified with v7.8.x. Updates 6.0, 6.1, 6.2, and 6.3 are supported.

> **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 information on installing Red Hat Enterprise Linux 6, see Red Hat Enterprise Linux 6 Installation Guide.
>
> For a list of required libraries, see Required libraries in Red Hat Enterprise Linux 6.

7. In the directory where you downloaded the **WebsenseCG78Setup_Lnx.tar.gz** 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, 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.

8. 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.

9. 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
   ```

10. 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.

11. 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.

12. 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.

13. 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.

14. 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] >
```

Change a port assignment if it will conflict with another application or process on the machine. Otherwise, leave the default assignments in place. Any new port numbers you assign must be between 1025 and 65535, inclusive.

15. 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.

16. 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>] >
```

17. 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.

18. 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 or disks 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
```

19. 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]
```

20. 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.

21. 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 the Web Security manager.

    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.

22. When installation is complete, reboot the Content Gateway server.
23. 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, and Analytics Server.
24. Copy the **WCGbackup.tar.gz** file, saved in step 3, to:

```
~/WCG/Current/
```

25. Restore the configuration archive. As root:

    ```
    cd ~/WCG/Current/
    ./wcg_config_utility.sh restore WCGbackup.tar.gz
    ```

26. 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
> ```

To finish the upgrade, be sure to perform the steps at the end of this document.

Post-upgrade activities

After you have finished upgrading components, perform the following steps to ensure that your Content Gateway upgrade is complete.

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 the Web Security manager 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.
3. Configure Content Gateway system alerts in the Web Security manager. A subset of Content Gateway system alerts are sent to the Web Security manager (in addition to Content Gateway Manager). To configure which alerts are sent, in the Web Security manager go to the **Settings > Alerts > System** page.
4. If you use SSL support:

   a. If your clients don't yet use a SHA-1 internal Root CA, create and import a SHA-1 Root CA into all affected clients. See Internal Root CA in Content Gateway Help.
   b. Using the notes you compiled prior to upgrade, rebuild your Static Incident list.
   c. Using the notes you compiled prior to upgrade, recreate your customized error message pages. (Not required for upgrades from 7.8.x.)

5. If you use proxy user authentication, review the settings on the **Global Authentication Options** page (**Configure > Security > Access Control > Global Configuration Options**).
6. If you use IWA user authentication, confirm that the AD domain is still joined. Go to **Monitor > Security > Integrated Windows Authentication**. If it is not joined, rejoin the domain. Go to **Configure > Security > Access Control > Integrated Windows Authentication**.
7. If you use Multiple Realm Authentication rules, review the converted Rule-Based Authentication configuration. Go to **Configure > Security > Access Control**.
   a. Check the **Domains** page.
      - IWA domains that were joined before upgrade should still be joined. Select each domain, click **Edit** and give each domain a unique **Domain Identifier**.
      - LDAP and Legacy NTLM domains should be listed. Select each domain, click **Edit** and give each domain a unique domain identifier.
   b. Check each rule.
      - Go to the **Authentication Rules** page and enter the editor.
      - Select each rule and check the configuration.
      - For Multiple Realm Authentication rules that used Cookie Mode Caching, the Source IP address list will have been copied to the cookie list on the Global Authentication Option page.
      - Check that the expected domain is in the **Auth Sequence** list.

   Important: The Rule-Based Authentication feature is very rich and can satisfy many user authentication requirements. To make best use of it, please read Rule-Based Authentication.
8. If you use IWA with a load balancer in v7.7.3 (a custom configuration):
   - IWA with a load balancer is not supported in v7.8.1.
   - IWA with a load balancer is supported in v7.8.2 and v7.8.3. To get the support, upgrade to v7.8.1 and then to v7.8.2 or v7.8.3. Follow the special configuration steps described in the v7.8.2 Release Notes or the v7.8.3 Release Notes.
9. If Web Security Gateway Anywhere and Data Security are deployed together, confirm that Content Gateway has automatically re-registered with Data Security Management Server. If it has not, manually re-register.
   a. Ensure that the Content Gateway and Data Security Management Server system clocks are synchronized to within a few minutes.
   b. In the Content Gateway manager:

- Go to **Configure > My Proxy > Basic**, ensure that **Data Security: Integrated on-box** is enabled, and click **Apply**.
- Next to **Integrated on-box**, click the **Not registered** link. This opens the **Configure > Security > Data Security registration** screen.
- Enter the IP address of the Data Security Management Server.
- Enter a user name and password for logging onto the Data Security manager. The user must be a Data Security administrator with Deploy Settings privileges.
- Click **Register**. If registration is successful, a message confirms the result and prompts you to restart Content Gateway. If registration fails, an error message indicates the cause of failure. Correct the problem and perform the registration process again.

10. If Web Security Gateway Anywhere and Data Security are deployed together and upgraded from v7.7.x to version 7.8.x, you must remove stale entries of Content Gateway instances registered in Data Security system modules:
    a. Log onto the TRITON console.
    b. Select the **Data Security** tab.
    c. Select **Settings > Deployment > System Modules**.
    d. Listed are 2 instances of each Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.
    e. Click **Deploy**.
11. 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**.

25 Upgrading V-Series Appliances to v7.8.x

Deployment and Installation Center | Web and Email Security Solutions | Version 7.8.x

Upgrade Appliances

This information on upgrading your Websense® V-Series™ appliances applies to the following:

- Web Security, Web Security Gateway and Web Security Gateway Anywhere
- Email Security Gateway and Email Security Gateway Anywhere
- V10000 G2, V10000 G3, and V5000 G2

The table below shows supported upgrade paths for versions 7.6.x, 7.7.x, and 7.8.x:

Current Version	End Version (direct upgrade supported)
7.6.0 7.6.1 7.6.2 7.6.5 7.6.7	7.7.0
7.7.0	7.7.3
7.7.0	7.8.1
7.7.3	7.7.4
7.7.3	7.8.1
7.7.4	7.8.1
7.8.1 7.8.2 7.8.3	7.8.4

For step-by-step instructions on the above upgrades, see the Appliance Upgrade Guide.

Note that appliances running versions earlier than v7.6.0 must be upgraded to 7.6.0. Once upgraded to 7.6.0, they can be upgraded directly to 7.7.0. You must upgrade to version 7.7.0 before upgrading to 7.7.3.

You must upgrade to version 7.8.1 before upgrading to 7.8.2 or later. For an overview of the 7.8.1 upgrade process, see the support video, Upgrading a Websense V-Series appliance to v7.8.1.

For high-level flow diagrams for upgrading from v7.7.x to 7.8.x, see:

- Web Security Gateway and Email Security Gateway on V-Series: Upgrade to 7.8.x
- Web Security and Web Security Gateway on V-Series: Upgrade to 7.8.x
- Email Security Gateway on V-Series: Upgrade to 7.8.x

26 Upgrading Data Security to v7.8.x

Deployment and Installation Center | Data Security Solutions | Version 7.8.x

Upgrade Data Security Solutions

You can upgrade to Websense Data Security v7.8.x directly from v7.7.x. 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 7.8.x
7.5.x	Migrate to 7.6.0	Upgrade to 7.7.2	Upgrade to 7.8.x
7.6.x	Upgrade to 7.7.2	Upgrade to 7.8.x	none
7.7.x	Upgrade to 7.8.x	none	none
7.8.0	Upgrade to 7.8.2	none	none

For step-by-step instructions on performing an upgrade, see the following guides. These guides include information on upgrading the management server, supplemental Data Security servers, agents, protectors, and endpoints.

- Upgrading Data Security within the 7.8 Series
- Upgrading from v7.7.x to v7.8.x
- Upgrading from v7.6.x to v7.8.x
- Migrating from v7.5.x to v7.8.x

High-level flow charts are also available for those upgrading from v7.7.x:

- Manager upgrade
- Servers and agents upgrade
- Protector/mobile agent upgrade
- Endpoint upgrade

27 Migrating Web Security to a new operating system

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

If your current Websense Web Security software is running on hardware or software that is no longer supported in v7.8.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: **v7.8.x**.

To prepare for the migration process, continue with *Order of migration and upgrade steps*, page 396.

If your solution includes Websense Content Gateway, also see *Content Gateway: Upgrade Red Hat Enterprise Linux 5-series to 6-series during the Content Gateway upgrade*, page 380, for Content Gateway operating system migration instructions.

Order of migration and upgrade steps

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.8.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. 4. Migrate to Windows 2008 R2. 5. Upgrade to v7.8.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. 4. Migrate to Red Hat Enterprise Linux 6. 5. Upgrade to v7.8.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. 4. Migrate to Windows 2008 R2. 5. Upgrade to v7.8.x on the new platform.
v7.1.x	Red Hat Enterprise Linux 4	1. Migrate to Red Hat Enterprise Linux 5. 2. Upgrade to v7.5.x on the new platform. 3. Upgrade to v7.7.x. 4. Migrate to Red Hat Enterprise Linux 6. 5. Upgrade to v7.8.x on the new platform.
v7.5.x	Windows 2003	1. Migrate to Windows 2008. 2. Upgrade to v7.7.x. 3. Migrate to Windows 2008 R2. 4. Upgrade to v7.8.x.

Current Version	Current Platform	Upgrade Path
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. 3. Migrate to Red Hat Enterprise Linux 6. 4. Upgrade to v7.8.x on the new platform.
v7.6.x	Windows 2003	1. Migrate to Windows 2008 R2. 2. Do one of the following: • If you have Web Security or Web Filter, upgrade directly to v7.8.x. • If you have Web Security Gateway or Gateway Anywhere, upgrade to v7.7.x, then to v7.8.x.
v7.7.x	Red Hat Enterprise Linux 5	1. Migrate to Red Hat Enterprise Linux 6. 2. Upgrade to v7.8.x on the new platform.
v7.7.x	Windows 2008 (32-bit)	1. Migrate to Windows 2008 R2. 2. Upgrade to v7.8.x on the new platform.

For more detailed migration instructions, see:

- *Migrating Web Security management components*, page 397
- *Moving Web Security policy components to a new machine*, page 398
- *Updating the operating system on an existing Web Security machine*, page 400

Migrating Web Security management components

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.8.x

In version 7.8.x, the TRITON management server can reside on either of four 64-bit Windows platforms: Windows Server 2008 R2 or R2 SP1 or Windows Server 2012 or 2012 R2 Standard Edition.

Using the steps that follow:

- Both versions 7.6.x and 7.7.x can be migrated to Windows Server 2008 R2.

- To migrate to Windows Server 2012, first upgrade to v7.8.x on the Windows Server 2008 R2 machine, then use only steps 1-4 of the following procedure to migrate to Windows Server 2012.

To migrate your management server components:

1. Perform a TRITON Infrastructure backup on your current installation, 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 the TRITON components (TRITON Infrastructure and the Web Security module) from their current location.
3. Reinstall TRITON Infrastructure and the Web Security module 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 v7.8.x. See *Upgrading Websense Web Security Solutions*, page 351.

   The upgrade instructions include information about the order in which to upgrade your components.

For migration instructions for additional components, see:

- *Moving Web Security policy components to a new machine*, page 398
- *Updating the operating system on an existing Web Security machine*, page 400

Moving Web Security policy components to a new machine

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - 7.8.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
  - C:\Program Files\Websense\Web Security\bin
  - C:\Program Files (x86)\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*: Navigate to the **Websense\Web Security** directory and enter the following command:

     ```
     WebsenseAdmin stop
     ```

   - *Linux*: Use the **/opt/Websense/WebsenseAdmin stop** command.

5. Do one of the following:

   - If you are moving a v7.7.x Policy Database, 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).

   - If you are moving the Policy Database for v7.6.x or earlier, see the “Restoring Policy Information for versions 7.0.0 through 7.6.x” section of How to back up and restore the v7.x Policy Database for restore instructions.

6. Start the Websense services on the new Policy Broker machine:

   - *Windows*: Navigate to the **Websense\Web Security** directory and enter the following command:

     ```
     WebsenseAdmin start
     ```

   - *Linux*: Use the **/opt/Websense/WebsenseAdmin start** command.

Updating the operating system on an existing Web Security machine

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.0.x - v7.8.x

If the existing Web Security machine meets the hardware specifications for v7.8.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 *or* Program Files (x86)\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 and v7.7*) 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 and v7.7*) 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**.

28 Upgrading Email Security Gateway Solutions

Deployment and Installation Center | Email Security Gateway Solutions | Version 7.8.x

Upgrade Email Security Solutions

The Email Security Gateway v7.8.x upgrade process includes V-Series appliance or virtual appliance components, along with TRITON Unified Security Center and Email Security Log Server Windows components. A virtual appliance upgrade applies only to version 7.8.0 and later.

If you are running Email Security Gateway version 7.8.0 (with appliance version 7.8.1), 7.8.2, or 7.8.3, you can upgrade directly to version 7.8.4. You must perform intermediate upgrades if you are running any other previous version of Email Security Gateway.

The following upgrade paths are available from version 7.6.x:

- 7.6.0 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4
- 7.6.2 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4
- 7.6.7 > 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4

Any version 7.6.x Email Security component that is currently installed on Windows Server 2003 must be migrated to Windows Server 2008 R2 before the upgrade to v7.7.0. Migration to Windows Server 2012 may be performed after an upgrade to v7.8.0.

The following upgrade paths are available from version 7.7.x:

- 7.7.0 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4
- 7.7.3 > 7.8.0 (with V-Series appliance version 7.8.1) > 7.8.4

You should ensure that third-party components are upgraded as well, to work with the new Email Security Gateway version.

We recommend that you perform a system backup in the event your system experiences a power outage during the upgrade process. Recovery procedures are also included in case they are needed.

- *Backup procedures*
- *Recovery procedures*

See the virtual appliance Quick Start Guide for instructions on backing up a virtual appliance.

After preparations are complete, perform the appropriate upgrade procedure:

- Upgrading Email Security Gateway v7.6.x to v7.7.0
- Upgrading Email Security Gateway v7.7.x to v7.8.x

Backup procedures

Deployment and Installation Center | Email Security Gateway Solutions | Version 7.8.x

The backup procedures outlined in the following steps are safeguards against an unexpected interruption of your 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 Email Security Gateway upgrade:

1. Back up the TRITON console settings. See the topic titled Backup and Restore of TRITON Data in TRITON Unified Security Center Help for backup procedures.
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? for backup instructions.
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 Standard and Enterprise versions only)*

   \\SQL Server Agent\\Jobs\\Websense_Maintenance_Job__esglogdb76 *(SQL Server Standard and Enterprise versions only)*

   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 (Email only, or Web and Email on a dual-mode appliance).

   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? for backup procedures.

5. Back up Email Security Gateway manager 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 Email Security Gateway Manager Help for backup details.

6. Upgrade any third-party integration products if necessary for use with Email Security Gateway. See third-party product documentation for appropriate backup and upgrade requirements and procedures.
7. Redirect email traffic out of the system that is being upgraded. If you do not redirect mail traffic, you may lose messages cached during the upgrade process.

> ✓ **Note**
>
> The Personal Email Manager end-user utility is not available until after the V-Series appliance upgrade is complete.

Recovery procedures

Deployment and Installation Center | Email Security Gateway Solutions | Version 7.8.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 *Backup procedures*.)

> ✓ **Note**
>
> Any quarantined or archived messages stored in the appliance local queues may be lost as a result of the recovery process.

Use the following procedure to recover your Email Security Gateway system:

1. Use the recovery DVD or USB drive image to reimage your V-Series appliance to the version from which you were upgrading.
2. Run firstboot.
3. Restore the backup files to your system in the following order, using the restore information for each component referenced in *Backup procedures*:
   a. V-Series appliance
   b. Microsoft SQL Server databases
   c. TRITON Unified Security Center
   d. Data Security manager

e. Email Security Gateway manager

> **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 v7.7.0, you should not upgrade to v7.8 before restoring the v7.7.0 files to Email Security.

4. Verify that your system works as it did before the interrupted upgrade.

You can now initiate the upgrade process.

29 Initial Configuration for All Websense Modules

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.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 439.
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 451.
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.

   In Windows Server 2008 or 2012:

   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**.

   Administrators may also need to restore default settings in their browser in order for the TRITON console to display properly in Internet Explorer. To do this, in Internet Explorer go to **Tools > Internet Options** and select the **Advanced** tab, then click **Reset**. When prompted, click **Reset** again.
4. Use a supported browser (see *System requirements for this version*, page 4) to launch the TRITON 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.

   b. Log on as the default **admin** account, using the password set during installation.

5. Enter your subscription key or keys. At first startup:

   - The Web Security manager prompts for a subscription key in the Initial Setup Checklist.

     If you have a Web Security Gateway solution, the key you enter is automatically applied to Content Gateway, as well.

   - The Data Security manager displays the subscription key page. See the *Initial Setup* section of the Data Security Help for more information.

   - The Email Security manager 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 Email Security Gateway Manager 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 Console 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.

   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 409
- *Data Security initial configuration*, page 413
- *Email Security Gateway initial configuration*, page 414
- *Content Gateway initial configuration*, page 416

Web Security initial configuration

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

In this topic:

Getting started with Web Security solutions

After entering your Web Security subscription key (see *Initial Configuration for All Websense Modules*, page 407), use the Initial Setup Checklist to complete basic setup tasks.

- If you have Web Security Gateway or Gateway Anywhere, also see *Content Gateway initial configuration*, page 416.
- If you have Web Security Gateway Anywhere, also see *Additional configuration for Web Security Gateway Anywhere*, page 411.

Next, you can:

- Configure transparent user identification on the **Settings** > **General** > **User Identification** page (see the “User Identification” topic in the Web Security Help).
  - If you installed Logon Agent, you must create and deploy a client logon script in addition to configuring Logon Agent in the Web Security manager. 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 Web Security Help.
- Enable email or SNMP alerting on the **Settings** > **Alerts** > **Enable Alerts** page (see the “Alerting” topic in the Web Security Help).
- Customize reporting behavior (see the “Reporting Administration” topic in the 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 platforms (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 (x86)\Websense\Web Security\bin\).
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 Web Security Help for more information. To configure a stealth mode NIC for monitoring, see *Network Agent and stealth mode NICs*, page 417.

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.
   - *Windows*: Use the Windows Services tool (Start > Administrative Tools > Services or Server Manager > Tools > Services) to restart **Websense Filtering Service**.

- *Linux*: Use the /opt/Websense/WebsenseDaemonControl command to restart **Filtering Service**.

Additional configuration for Web Security Gateway Anywhere

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applie to:	In this topic:
◆ Web Security Gateway Anywhere, v7.8.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 409, 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 on the Data Security manager System Modules page.

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 Data Security manager, 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 the Data Security manager.
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 7.8.x

> **Note**
>
> The Data Security manager 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 the Data Security manager 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 7.8.x

Applies to:	In this topic:
◆ Email Security Gateway and Email Security Gateway Anywhere v7.8.x	◆ *Email Security Gateway initial configuration*, page 414 ◆ *Email Security Gateway Anywhere initial configuration*, page 415

Email Security Gateway initial configuration

The first time you access Email Security Gateway, 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 Email Security Gateway Manager Help for more information about the wizard.

> **Important**
>
> The configuration wizard is offered only once, at initial start up of Email Security Gateway. If you choose to not use the wizard it will no longer be available. All settings configured in the wizard can be configured in the Email Security Gateway manager individually. The wizard simply offers a more convenient way to enter some initial settings.

See the Getting Started section in Email Security Gateway Manager 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 message analysis database updates

For help with the following Email Security settings, see the Configuring System Settings section in the 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
- Trusted CA certificate importing
- 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 the Email Security Gateway Manager 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 Email Security Gateway Manager Help for details.

Content Gateway initial configuration

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Applies to:

- Web Security Gateway and Web Security Gateway Anywhere v7.8.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 the Web Security manager.

- 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: HTTPS (SSL support), 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 *Web Security user identification*.
- Configure the real-time Scanning Options in the Web Security manager.
- If you enabled content caching during installation, configure content caching.

After the base configuration has been tested, consider these additional activities:

- When HTTPS (SSL support) is used, in the Web Security manager 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 | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere v7.8.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>**.

30 Adding, Modifying, or Removing Components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

The following articles contain instructions for adding, modifying, or removing Websense Web, Data, and Email Security components:

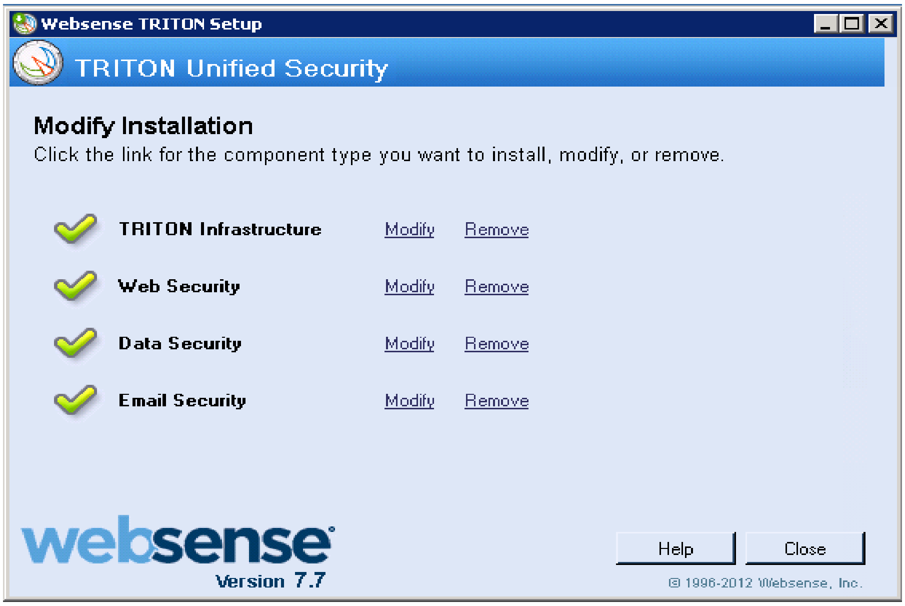
Adding or modifying Windows components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.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.



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 421
- *Adding Web Security components*, page 422
- Adding or modifying Data Security components
- *Adding Email Security components*, page 423

Modifying TRITON Infrastructure

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

1. Start the Websense installer.
   - If you chose to keep installation files after the initial installation, go to the Windows Start screen, or **Start > All Programs > Websense** and select **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 234.
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. 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 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.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 the Windows Start screen, or **Start > All Programs > Websense** and select **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 239, for instructions.
5. When you are done adding Web Security components, you are returned to the **Modify Installation** dashboard.

Adding Email Security components

Deployment and Installation Center | Email Security Solutions | Version 7.8.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

Two Email Security Gateway components may be added on a Windows machine: Email Security Gateway manager 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 the Windows Start screen, or **Start > All Programs > Websense** and select **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 in 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 257.

  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**.

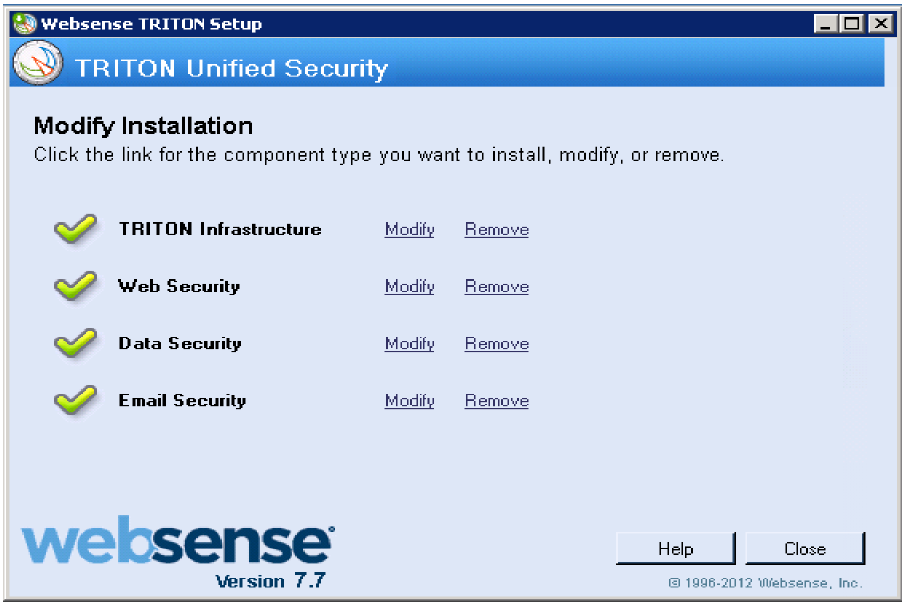
Removing components

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.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.



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 (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 426
- *Removing Web Security components*, page 427
- *Removing Data Security components*, page 435
- *Removing Email Security components*, page 436

Removing TRITON Infrastructure

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x
- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

Remote TRITON Infrastructure only after removing all TRITON Unified Security Center modules (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:

- Web Security: *Removing Web Security components*, page 427
- Data Security: *Removing Data Security components*, page 435
- Email Security: *Removing Email Security components*, page 436

To remove TRITON Infrastructure:

1. Start the Websense installer:
   - If you chose to keep installation files after the initial installation, go to the Windows Start screen, or **Start** > **All Programs** > **Websense** and select **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:

   > *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 7.8.x

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x	◆ *To remove Web Security components (Windows)*, page 428 ◆ *To remove Web Security components (Linux)*, page 430

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 432). 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 433). Also, if your Web Security deployment is integrated with another product, see the following for any integration-specific requirements:

- *Integrating Web Security with Cisco*, page 269
- *Integrating Web Security with Citrix*, page 293
- *Integrating Web Security with Microsoft Products*, page 311
- *Installing Web Security for Universal Integrations*, page 339

Removal instructions are slightly different depending on the operating system:

- *To remove Web Security components (Windows)*, page 428
- *To remove Web Security components (Linux)*, page 430

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 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 the Windows Start screen, or **Start > All Programs > Websense** and select **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 Cisco*, page 269

- *Integrating Web Security with Citrix*, page 293
- *Integrating Web Security with Microsoft Products*, page 311
- *Installing Web Security for Universal Integrations*, page 339.

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 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.

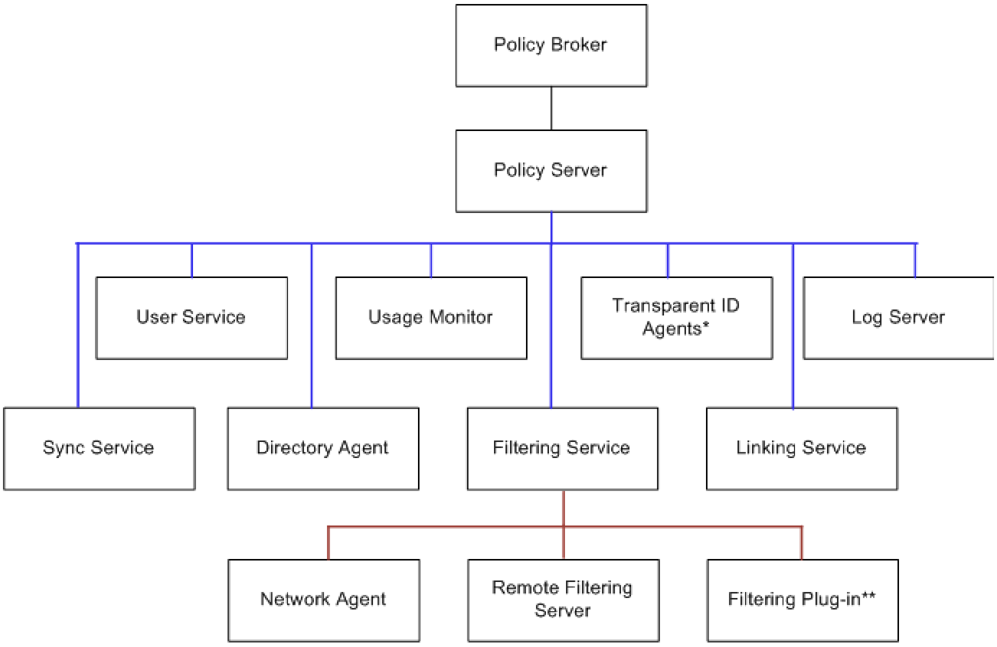
8. If you stopped your antivirus software, restart it.

9. If you remove an integration plug-in, you may need to restart the integration product. See:

   - *Integrating Web Security with Cisco*, page 269
   - *Integrating Web Security with Citrix*, page 293
   - *Integrating Web Security with Microsoft Products*, page 311
   - *Installing Web Security for Universal Integrations*, page 339

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).

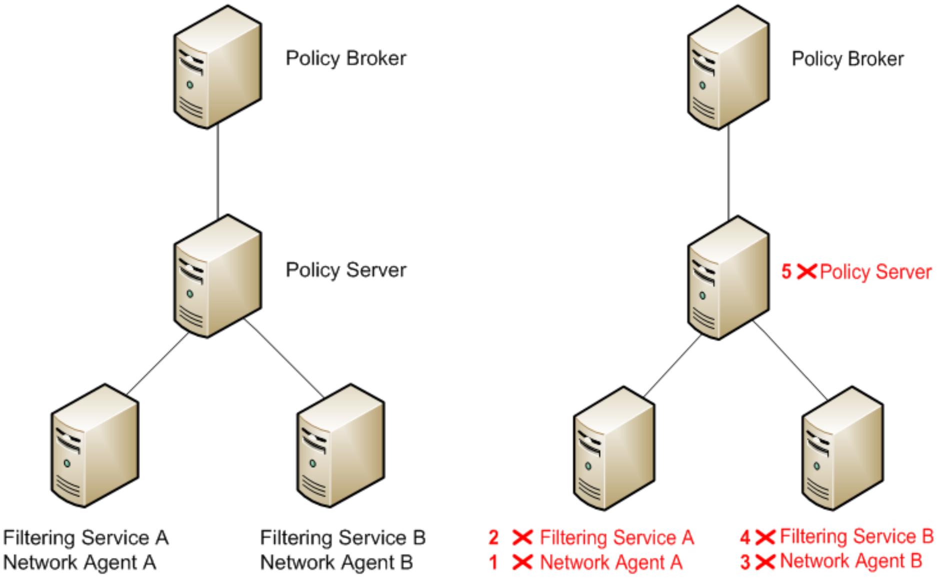


* DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
** Microsoft ISAPI Filter or Citrix Integration Service

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 Web Security installation directory (default: C:\Program Files *or* Program Files (x86)\Websense\Web Security in Windows; /opt/Websense/ in Linux) or its sub-directories, 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 7.8.x

Applies to:

- Web Security Gateway and Gateway Anywhere, v7.8.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 7.8.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 Installing and Deploying Data Endpoint Clients.

To remove Data Security components:

1. Start the Websense installer:
   - If you chose to keep installation files after the initial installation, go to the Windows Start screen, or **Start > All Programs > Websense** and select **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 7.8.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.8.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 the Windows Start screen, or **Start > All Programs > Websense** and select **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 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 Email Security Gateway manager 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 Gateway uninstall process.

31 Quick Reference

Deployment and Installation Center | Web Security Solutions | Version 7.8.x

Use this Deployment and Installation Center Quick Reference to find information about:

- *Websense TRITON Enterprise default ports*, page 439
- *Excluding Websense files from antivirus scans*, page 451
- *Configuring Websense Apache services to use a trusted connection*, page 454

Websense TRITON Enterprise default ports

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.5.x - v7.8.x
- Websense Data Security, v7.8.x
- Websense Email Security Gateway and Email Security Gateway Anywhere, v7.8.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 440
- *Email Security Gateway ports*, page 450

Port information for all solutions is also available in a single Excel spreadsheet.

Data Security ports

Deployment and Installation Center | Data Security Solutions | Version 7.8.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.

Web Security manager

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.
Internet	443	Salesforce fingerprinting

* 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)

Data Security manager

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	17443	Syslog, forensics, incidents, mobile status
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.
Data Security Management Server	80	Fingerprint sync
Data Security Management Server	17443	Syslog, forensics, incidents, mobile status
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.		

FCI 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.
* This range is necessary for load balancing.		
Inbound		
Microsoft FSRM	5985	Microsoft File Server Resource Manager (FSRM)

Email Security Gateway ports

Deployment and Installation Center | Email Security Solutions | Version 7.8.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, Secure Message Delivery end-user portal
C/E1/E2 (C recommended)	6671	Inbound	SSL proxy to be accessed by Email Security manager
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 Websense 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 off-appliance components.

Interface	Port	Direction	Description
C/E1/E2	9443	Inbound	Email Security manager (via TRITON Unified Security Center)
E1/E2	50800	Inbound	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 7.8.x

In this topic:

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 (includes subdirectories) 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 (includes subdirectories) 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 (includes subfolders), by default:

```
*:\Program Files\Websense
```

or

```
*:\Program Files (x86)\Websense
```

Also exclude any Data Security folders that apply (see *Data Security* above).

Configuring Websense Apache services to use a trusted connection

Deployment and Installation Center | Web Security Solutions | Version 7.8.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 tool (**Start** > **Administrative Tools** > **Services** or **Server Manager** > **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**.

Repeat this process (from Step 2) for the **Websense Web Reporting Tools** service.

32 Component Reference

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

In this topic:

For information about Web Security components, see *Deploying Web Security core components*, page 38.

TRITON Unified Security Center components

- *TRITON management server*, page 456
- *TRITON Unified Security Center*, page 457
- *TRITON Infrastructure*, page 457

Data Security components

- *Data Security manager*, page 459
- *Protector*, page 459
- *SMTP agent*, page 459
- *Microsoft ISA/TMG agent*, page 460
- *Data Endpoint*, page 460
- *Printer agent*, page 461
- *Integration agent*, page 461
- *Crawler*, page 462

Email Security Gateway components

- *Email Security manager*, page 462
- *Email Security Log Server*, page 463

TRITON management server

Deployment and Installation Center | Web, Data, and Email Security Solutions | Version 7.8.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x
- Data Security, v7.8.x
- Email Security Gateway (Anywhere), v7.8.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 457), 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:
    - Web Security manager
    - *Data Security manager*
    - *Email Security manager*

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 7.8.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x
- Data Security, v7.8.x
- Email Security Gateway (Anywhere), v7.8.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:

- Web Security manager
- *Data Security manager*
- *Email Security manager*

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 the Appliance manager and Content Gateway manager.

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 7.8.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x
- Data Security, v7.8.x
- Email Security Gateway (Anywhere), v7.8.x

TRITON Infrastructure is composed of common user interface, logging, and reporting components required by the TRITON management modules (the Web Security, Data Security, and Email Security managers). 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 7.8.x

Applies to:

- Web Filter, Web Security, and Web Security Gateway (Anywhere), v7.8.x
- Data Security, v7.8.x
- Email Security Gateway (Anywhere), v7.8.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 of SQL Server, see *System requirements for this version*, page 4.

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.

Websense Content Gateway

Deployment and Installation Center | Web and Data Security Solutions | Version 7.8.x

Applies to:

- Web Security Gateway and Gateway Anywhere, v7.8.x
- Data Security, v7.8.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.

Data Security manager

Deployment and Installation Center | Data Security Solutions | Version 7.8.x

The 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 7.8.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 for more information.

Mobile agent

Deployment and Installation Center | Data Security Solutions | Version 7.8.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 for more information.

SMTP agent

Deployment and Installation Center | Data Security Solutions | Version 7.8.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.

The SMTP agent 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 for more information.

Microsoft ISA/TMG agent

Deployment and Installation Center | Data Security Solutions | Version 7.8.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 for more information.

Data Endpoint

Deployment and Installation Center | Data Security Solutions | Version 7.8.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 the Data Security manager. These settings 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 Installing and Deploying Data Endpoint Clients for more information.

Printer agent

Deployment and Installation Center | Data Security Solutions | Version 7.8.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 for more information.

Microsoft FCI agent

Deployment and Installation Center | Data Security Solutions | Version 7.8.x

The Data Security FCI agent augments the data classification performed using Microsoft File Classification Infrastructure (FCI) on Windows Server 2012 machines. Working in tandem with the Microsoft File Server Resource Manager (FSRM), the agent analyzes data and applies data discovery policies to it, tagging the data when a match is detected. This allows administrators to identify data such as personally identifiable information (PII) or personal health information (PHI) so they can control access to it, perform remediation on it, and more.

See FCI agent for more information.

Integration agent

Deployment and Installation Center | Data Security Solutions | Version 7.8.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 for more information.

Crawler

Deployment and Installation Center | Data Security Solutions | Version 7.8.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 Data Security manager. Go to **Settings > Deployment > System Modules**, select the crawler, and click **Edit**.

See The crawler for more information.

Email Security manager

Deployment and Installation Center | Email Security Solutions | Version 7.8.x

Applies to:

- Email Security Gateway and Email Security Gateway Anywhere, v7.8.x

Description

The Email Security module of the *TRITON Unified Security Center* is used to configure and manage the email security features of your deployment.

Email Security Gateway manager 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. The Email Security Gateway manager 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 the Email Security manager is listed below.

Windows	Linux
Websense TRITON - Email Security	n/a

Email Security Log Server

Deployment and Installation Center | Email Security Solutions | Version 7.8.x

Applies to

- Email Security Gateway and Email Security Gateway Anywhere v7.8.x

Description

Email Security Gateway 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 Gateway 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 Gateway appliance.

Special considerations

To be able to install Email Security Gateway Log Server, a supported database engine (see *System requirements for this version*, page 4) 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 Gateway Log Server.

Windows	Linux
Email Security Log Server	n/a

33 Data Security Protector CLI

Deployment and Installation Center | Data Security Solutions | Version 7.8.x

Applies to:	In this topic:
◆ Data Security, v7.8.x	

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.
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