websense
ESSENTIAL INFORMATION PROTECTION™

Installation Guide

Websense® Content Gateway
Websense Web Security Gateway

v7.5

Installation Guide for Websense Content Gateway / Websense Web Security Gateway

Contents

1 Prerequisites and Preparation

Websense Content Gateway runs with either Websense Web Security or Websense Web Filter to provide the advantages of a proxy cache, improving bandwidth usage and network performance by storing requested Web pages and, while a stored page is considered fresh, serving that Web page to the requesting client.

In addition, Websense Content Gateway can scan for content categorization. This feature examines the content on Web pages that are not included in the Websense Master Database and on pages that Websense has determined to have rapidly changing content. After this examination, Websense Content Gateway returns a recommended category to Websense filtering software, which then permits or blocks the Web page depending on the policy in effect.

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

- Security scanning, which inspects incoming Web pages to immediately block malicious code, such as phishing, malware, and viruses.
- Advanced file scanning, which offers both traditional antivirus scanning and advanced detection techniques for discovering and blocking infected and malicious files users are attempting to download.
- Content stripping, which removes active content (code written in selected scripting languages) from incoming Web pages.

See the TRITON - Web Security Help for information on the scanning options.

When installed as part of Websense Web Security Gateway Anywhere, Websense Content Gateway also works with Websense Data Security Management Server to prevent data loss over Web channels. For more information, see the *Websense Web Security Gateway Anywhere Getting Started Guide*.

Websense Content Gateway can behave as an explicit or transparent proxy.

- In an explicit proxy deployment, client browsers must be configured to point to Websense Content Gateway.
- In a transparent proxy deployment, client requests are intercepted and redirected to Websense Content Gateway by an external network device (required).

If you enable SSL Manager, in addition to filtering HTTPS URLs, the content on those pages is decrypted, examined for security issues, and, if appropriate, re-encrypted and forwarded to the destination.

When you run Websense Content Gateway with Websense Data Security, which inspects HTTPS and FTP traffic, you must enable the SSL Manager feature. See the Content Gateway Manager Help for information on SSL Manager.

Pre-installation considerations

Before you install Websense Content Gateway, consider:

- System security. Your network can carry sensitive data. SSL Manager lets you have data decrypted and then re-encrypted on the way to its destination. Consider locking down your system as much as possible to prevent others from seeing your data. See *Security*, page 7.
- Network configuration. Websense Content Gateway can run as an explicit proxy (where browsers point to Websense Content Gateway), or a transparent proxy (where traffic is redirected through a WCCP-enabled router or a Layer 4 switch in your network and the ARM, Adaptive Redirection Module, feature of Websense Content Gateway). See *Network configuration*, page 16 and see the Content Gateway Manager Help for information on the ARM.

  Websense Content Gateway can proxy HTTP, HTTPS, FTP, and other protocols. To transparently proxy protocols other than HTTP through a WCCP-enabled router, the router must use WCCP v2, which supports redirection of multiple protocols.
- System requirements. Ensure that your system meets the minimum requirements listed in *System requirements*, page 17.

Upgrading from a previous version

Websense Content Gateway version 7.5 is certified on Red Hat Enterprise Linux 5, update 3 and update 4. These Red Hat versions were not supported by any prior version of Websense Content Gateway. A direct upgrade from a prior version of Websense Content Gateway to version 7.5 is not possible.

To migrate to Websense Content Gateway 7.5, update your operating system to the required version (see *System requirements*, page 17) or obtain a machine running the required operating system. Then install Websense Content Gateway 7.5 as a new installation.

Security

As noted in *Pre-installation considerations*, Websense Content Gateway can run in either an explicit or transparent deployment. In explicit deployments, client browsers are pointed to Websense Content Gateway. You accomplish this with a PAC file, with WPAD, or by having the user edit browser settings to point to Websense Content Gateway. See the Content Gateway Manager Help for information on PAC files and WPAD.

In transparent deployments, client requests are intercepted and redirected to Websense Content Gateway without client involvement. See the Content Gateway Manager Help for additional information on configuring a WCCP-enabled router or a Layer 4 switch, and about the ARM (Adaptive Redirection Module).

One issue to consider with explicit deployment is that a user can point his or her browser to another destination to bypass Websense Content Gateway. You can address this concern by setting and propagating browser configuration in your organization through Group Policy. For more information about Group Policy, search the Microsoft TechNet Web site at http://technet.microsoft.com.

This section covers:

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 Websense Content Gateway. It is strongly recommended that the Websense Content Gateway server be locked in an IT closet and that a BIOS password be enabled.

Implementing security through software

Implement the following recommendations, as appropriate, to ensure the tightest security possible:

Root permissions

Ensure that root permissions are restricted to a select few persons. This important restriction helps preclude unauthorized access to the Websense Content Gateway file system.

Ports

Websense Content Gateway uses the following ports. They must be open to support the full set of Websense Web Security Gateway features. These are all TCP ports, unless otherwise noted.

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

Restrict inbound traffic to as many other ports as possible on the Websense Content Gateway server. In addition, if your subscription does not include certain features, you can restrict inbound traffic to the unneeded ports. For example, if your subscription does not include Websense Data Security, you may choose to restrict inbound traffic to those ports related to Websense Data Security (e.g., 5819, 5820, 5821, and so forth).

Port	Function
21	FTP
22	SSH for command-line access
53	DNS
80	HTTP
443	Inbound for transparent HTTPS proxy
2121	FTP
2048	WCCP for transparent proxy (if used)
3130	(UDP) ICP for ICP Cache Hierarchy
5819	Websense Data Security fingerprint detection
5820	Websense Data Security fingerprint synchronization
5821	Websense Data Security fingerprint configuration
5822	Websense Data Security fingerprint configuration
5823	Websense Data Security fingerprint configuration
8071	SSL Manager interface
8080	Inbound for explicit HTTP and HTTPS proxy
8081	Websense Content Gateway management interface
8082	Overseer for clustering

Port	Function
8083	Autoconfiguration for clustering
8084	Process Manager for clustering
8085	Logging server for clustering
8086	Clustering
8087	Reliable service for clustering
8088	(UDP) Multicast for clustering
8089	(UDP) SNMP encapsulation
8090	HTTPS outbound (between Websense Content Gateway and the SSL outbound proxy)
8880	Websense Data Security configuration
8888	Websense Data Security configuration deployment and system health information
8889	Websense Data Security configuration deployment and system health information
8892	Websense Data Security system logging
9080	Websense Data Security statistics and system health information
9081	Websense Data Security statistics and system health information
9090	Websense Data Security diagnostics
9091	Websense Data Security diagnostics
18303	Websense Data Security local analysis
18404	Websense Data Security remote analysis

IPTables Firewall

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

The following list of rules is organized into groups that address different deployments. Be sure the **/etc/sysconfig/iptables** file contains all the rules from each section that apply to your network:

- *All deployments*, page 10
- *Local Policy Server*, page 11
- *Remote Policy Server*, page 12
- *Local Filtering Service*, page 12
- *Remote Filtering Service*, page 12
- *Websense Data Security*, page 13
- *Cluster*, page 13

- *Cache hierarchy*, page 13
- *Transparent proxy*, page 14
- *FTP*, page 14
- *Optional features*, page 14

If Websense Content Gateway is configured to use multiple NICs, for each rule that applies to an interface, specify the appropriate NIC with the "-i" option ("-i" means only match if the incoming packet is on the specified interface). Typically, multiple interfaces are divided into these roles:

- Management interface (MGMT_NIC) - The physical interface used by the system administrator to manage the computer.
- Internet-facing interface (WAN_NIC) - The physical interface used to request pages from the Internet (usually the most secure interface).
- Client-facing interface (CLIENT_NIC) - The physical interface used by the clients to request data from Websense Content Gateway.
- Cluster interface (CLUSTER_NIC) - The physical interface used by Websense Content Gateway to communicate with members of the cluster.

In the list of rules, the associated interface is shown with the "-i" option. In one rule "lo" is specified; "lo" is the local loopback interface.

All the rules in the following sections must be preceded by `iptables` in the file. For example:

```
iptables -i eth0 -I INPUT -p tcp --dport 22 -j ACCEPT
```

For a list of rules that shows each complete command, go to the Websense Knowledge Base, log in to the Web Security Gateway area, and search for the article titled *Configuring IPTables for Websense Content Gateway.* The article also links to an example iptables script.

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

All deployments

These rules are required to enable Content Gateway communications, regardless of the deployment.

The following rules should be first.

Disable tracking of internal connections	`-I OUTPUT -o lo -t raw -j NOTRACK` **Note:** This rule must be the first output rule invoked.
Block ALL inbound	`--policy INPUT DROP`

The following rules are important for general system security, and should be entered immediately after the first rule:

Allow ALL outbound	`--policy OUTPUT ACCEPT`
Block ALL forward requests	`--policy FORWARD DROP`
Allow ALL traffic on the local (loopback) interface	`-I INPUT -i lo -j ACCEPT`
Allow ALL responses on established connections	`-I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT`
Allow ALL inbound port 22	`-i <MGMT_NIC> -I INPUT -p tcp --dport 22 -j ACCEPT`
Allow ALL inbound ICMP	`-i <MGMT_NIC> -I INPUT -p ICMP -j ACCEPT`

The next group is required for Websense Content Gateway to receive and proxy traffic.

Allow ALL inbound port 8070	`-i <CLIENT_NIC> -I INPUT -p tcp --dport 8070 -j ACCEPT`
Allow ALL inbound port 8071	`-i <MGMT_NIC> -I INPUT -p tcp --dport 8071 -j ACCEPT`
Allow ALL inbound port 8080	`-i <CLIENT_NIC> -I INPUT -p tcp --dport 8080 -j ACCEPT`
Allow ALL inbound port 8081	`-i <MGMT_NIC> -I INPUT -p tcp --dport 8081 -j ACCEPT`

ip_conntrack_max

In addition to the above rules, it is a best practice to increase the size of `ip_conntrack_max` to 100000 to improve performance. Typically, this can be done using the following command:

```
/sbin/sysctl net.ipv4.ip_conntrack_max=100000
```

Note that this should be done after iptables is invoked. Also, this change in value will not be preserved after reboot unless you configure your system to set this value upon startup. To do so, add the following line to **/etc/sysctl.conf**:

```
net.ipv4.ip_conntrack_max=100000
```

Local Policy Server

Include these rules in your IPTables firewall if the Websense Policy Server runs on the Content Gateway machine.

Allow ALL inbound port 40000	`-i <MGMT_NIC> -I INPUT -p tcp --dport 40000 -j ACCEPT`
Allow ALL inbound port 55806	`-i <MGMT_NIC> -I INPUT -p tcp --dport 55806 -j ACCEPT`

Allow ALL inbound port 55880	`-i <MGMT_NIC> -I INPUT -p tcp --dport 55880 -j ACCEPT`
Allow ALL inbound port 55905	`-i <MGMT_NIC> -I INPUT -p udp --dport 55905 -j ACCEPT`

Remote Policy Server

Include this rule in your IPTables firewall if the Websense Policy Server does **not** run on the Content Gateway machine. This is required because Websense Content Gateway has bidirectional communication over ephemeral ports.

Be sure to replace *<Policy Server IP>* in the command with the actual IP address of the Policy Server machine.

Allow ALL from <Policy Server IP> ports 1024+	`-i <MGMT_NIC> -I INPUT -p tcp -s <Policy Server IP> --dport 1024:65535 -j ACCEPT`

Local Filtering Service

Include these rules in your IPTables firewall if the Websense Filtering Service runs on the Content Gateway machine.

Allow ALL inbound port 55807	`-i <MGMT_NIC> -I INPUT -p tcp --dport 55807 -j ACCEPT`
Allow ALL inbound port 15868	`-i <MGMT_NIC> -I INPUT -p tcp --dport 15868 -j ACCEPT`

Remote Filtering Service

Include this rule in your IPTables firewall if the Websense Filtering Service does **not** run on the Content Gateway machine. This is required because Websense Content Gateway has bidirectional communication over ephemeral ports.

Be sure to replace *<Filtering Service IP>* in the command with the actual IP address of the Filtering Service machine.

Allow ALL from <Filtering Service IP> ports 1024+	`-i <MGMT_NIC> -I INPUT -p tcp -s <Filtering Service IP> --dport 1024:65535 -j ACCEPT`

Websense Data Security

Include the following rules in your IPTables firewall if Websense Content Gateway is installed as part of Websense Web Security Gateway Anywhere or deployed with Websense Data Security.

Allow ALL inbound port 5820	`-i <MGMT_NIC> -I INPUT -p tcp --dport 5820 -j ACCEPT`
Allow ALL inbound port 8880	`-i <MGMT_NIC> -I INPUT -p tcp --dport 8880 -j ACCEPT`
Allow ALL inbound port 8888	`-i <MGMT_NIC> -I INPUT -p tcp --dport 8888 -j ACCEPT`
Allow ALL inbound port 8889	`-i <MGMT_NIC> -I INPUT -p tcp --dport 8889 -j ACCEPT`
Allow ALL inbound port 9080	`-i <MGMT_NIC> -I INPUT -p tcp --dport 9080 -j ACCEPT`
Allow ALL inbound port 9090	`-i <MGMT_NIC> -I INPUT -p tcp --dport 9090 -j ACCEPT`

Cluster

Include the following rules in your IPTables firewall if you have multiple instances of Websense Content Gateway in a cluster.

Allow ALL inbound tcp on port 8086	`-i <CLUSTER_NIC> -I INPUT -p tcp --dport 8086 -j ACCEPT`
Allow ALL inbound udp on port 8086	`-i <CLUSTER_NIC> -I INPUT -p udp --dport 8086 -j ACCEPT`
Allow ALL inbound tcp on port 8087	`-i <CLUSTER_NIC> -I INPUT -p tcp --dport 8087 -j ACCEPT`
Allow ALL inbound udp on port 8088	`-i <CLUSTER_NIC> -I INPUT -p udp --dport 8088 -j ACCEPT`
Allow ALL inbound udp on the multicast IP address	`-i <CLUSTER_NIC> -I INPUT -p udp -d <Multicast_IP_Address> -j ACCEPT`

Cache hierarchy

Include the following rule in your IPTables firewall if you have multiple instances of Websense Content Gateway in a cache hierarchy.

Allow ALL inbound port 3130	`-i <MGMT_NIC> -I INPUT -p udp --dport 3130 -j ACCEPT`

Transparent proxy

Include the following rules in your IPTables firewall if your network uses transparent proxy.

Allow ALL inbound port 80	`-i <CLIENT_NIC> -I INPUT -p tcp --dport 80 -j ACCEPT`
Allow ALL inbound port 443	`-i <CLIENT_NIC> -I INPUT -p tcp --dport 443 -j ACCEPT`
Allow ALL inbound port 2048 - for WCCP (used only if your network uses WCCP for transparent proxy)	`-i <CLIENT_NIC> -I INPUT -p udp --dport 2048 -j ACCEPT`
Allow ALL inbound port 53 - for DNS (optional)	`-i <CLIENT_NIC> -I INPUT -p udp --dport 53 -j ACCEPT`
Allow ALL inbound port 5353 - for DNS (optional)	`-i <CLIENT_NIC> -I INPUT -p udp --dport 5353 -j ACCEPT`

FTP

Include the appropriate rules, below, in your IPTables firewall if you plan to proxy FTP traffic (optional).

Allow ALL inbound port 21 - for FTP	`-i <CLIENT_NIC> -I INPUT -p tcp --dport 21 -j ACCEPT`
Allow ALL inbound port 2121 - for FTP	`-i <CLIENT_NIC> -I INPUT -p tcp --dport 2121 -j ACCEPT`

Optional features

Include the appropriate rules, below, in your IPTables firewall if you use the features listed.

Allow gathering of statistics over the overseer port	`-i <MGMT_NIC> -I INPUT -p tcp --dport 8082 -j ACCEPT`
Allow PAC file distribution from Websense Content Gateway (Browser Auto-Config)	`-i <CLIENT_NIC> -I INPUT -p tcp --dport 8083 -j ACCEPT`
Allow collation of logs for multiple proxies	`-i <MGMT_NIC> -I INPUT -p tcp --dport 8085 -j ACCEPT`

Configuring the router

For transparent proxy deployment, it is recommended that you configure your router to use WCCP v2, which can support both the HTTP and HTTPS protocols. See the Content Gateway Manager Help for additional information on configuring a WCCP-enabled router or a Layer 4 switch and on the ARM (Adaptive Redirection Module).

Configuring client browsers

For explicit proxy deployments, you must configure each client browser to send Internet requests to Websense Content Gateway, over the ports that Websense Content Gateway uses for the associated protocol.

The default proxy port in Websense Content Gateway for both HTTP and HTTPS traffic is 8080.

Use the instructions below to configure client browsers manually. Alternatively, use a PAC or WPAD file to configure client browsers.

> **Note**
> The instructions below are for the most common client browsers. For other client browsers refer to the browser's documentation for instructions on manual explicit proxy configuration.

Configuring Internet Explorer 7.0 and later

1. From the Internet Explorer browser, select **Tools** > **Internet Options** > **Connections** > **LAN Settings**.
2. Select **Use a proxy server for your LAN**.
3. **Click** Advanced.
4. For **HTTP**, enter the Websense Content Gateway IP address and specify port 8080.
5. For **Secure**, enter the Websense Content Gateway IP address and specify port 8080.
6. Clear **Use the same proxy server for all protocols**.
7. Click **OK** to close each screen in this dialog box.

Configuring Firefox 3.0

1. From the Firefox browser, select **Tools** > **Options** > **Advanced**, and then select the **Network** tab.
2. Select **Settings**.
3. Select **Manual proxy configuration.**
4. For **HTTP Proxy**, enter the Websense Content Gateway IP address and specify port 8080.
5. For **SSL Proxy**, enter the Websense Content Gateway IP address and specify port 8080.
6. Click **OK** to close each screen in this dialog box.

Network configuration

Consider how Websense Content Gateway will be used in your network:

- *Explicit deployment, single proxy*
- *Explicit deployment, multiple proxies*
- *Transparent deployment, single proxy*
- *Transparent deployment, multiple proxies*

These configurations are described below. For other deployment options, see the Websense Deployment Guide Supplement, *Deploying with Websense Content Gateway*.

Explicit deployment, single proxy

Explicit proxy deployment requires pointing the client browser to Websense Content Gateway. HTTP, or HTTPS, or FTP over HTTP traffic gets to Websense Content Gateway because you configure the browser manually, or through a PAC or WPAD file. Explicit proxy deployment does not require a WCCP-enabled router. The configuration can also be through a Group Policy.

Because the client browser must be configured to point to Websense Content Gateway, there is some risk that users will edit their browser settings to avoid Websense Content Gateway. This risk can be mitigated by corporate outbound firewall rules.

Explicit deployment, multiple proxies

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.

Transparent deployment, single proxy

In transparent deployment, traffic is redirected to Websense Content Gateway via a WCCP-enabled router or Layer 4 switch in your network.

See the Content Gateway Manager Help for additional information on configuring a WCCP-enabled router or a Layer 4 switch, and about the ARM (Adaptive Redirection Module).

Transparent deployment, multiple proxies

A WCCP-enabled router can help facilitate load balancing among proxies.

System requirements

Hardware

CPU	Quad-core running at 2.8 GHz or faster
Memory	4 GB
Disk space	2 disks: • 100 GB for the operating system, Websense Content Gateway, and temporary data. • 147 GB for caching If caching will not be used, this disk is not required. The caching disk: – Should have minimum size of 2 GB, maximum 147 GB for optimal performance – Must be a raw disk, not a mounted file system (for instructions on creating a raw disk from a mounted file system, see *Cache Disk*, page 19.) – 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 64MB of write-through cache
Network Interfaces	2

To support transparent proxy deployments:

Router	WCCP v1 routers support redirection of HTTP only. If your deployment requires additional protocols, such as HTTPS, your router must support WCCP v2. A Cisco router must run IOS 12.2 or later. The clients, the destination Web server, and Websense Content Gateway must reside on different subnets.
—or—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. 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

Linux operating system:

- Websense Content Gateway version 7.5 is certified on Red Hat Enterprise Linux 5, update 3 and update 4, base or Advanced Platform (32-bit only)
  - 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
    ```

  Important
  If SELinux is enabled, disable it before installing Websense Content Gateway.

- PAE (Physical Address Extension)-enabled kernel required
  - By default, Red Hat Enterprise Linux 5, update 3 and later has PAE enabled. If you are running the non-PAE kernel, reboot with the PAE-enabled kernel before installing Websense Content Gateway.
- RPM compat-libstdc++-33-3.2.3-47.3.i386.rpm (or higher version of this package)

- To display a list of RPMs installed on your system with the string “compat-libstdc” in their name, enter the command:
  `rpm -qa |grep compat-libstdc`

- GNU C library (glibc) version 2.5-42 or later
  - Note that Red Hat Enterprise Linux 5, update 3 ships with glibc version 2.5-34. Be sure to update it to version 2.5-42 or later.
  - Example command to update this library (running as `root`): `yum update glibc`.

Websense Web filtering products—Websense Web Security Gateway, Websense Web Security, Websense Web Filter:

- Version 7.5

> **Important**
> Websense filtering software must be installed prior to Websense Content Gateway. When the filtering software is installed, Websense Content Gateway must be specified as the integration product. For more information, see *Websense filtering software*, page 21.

Integration with Websense Data Security:

- Version 7.5

  The order of installation does not matter. Websense Data Security may be installed before or after Websense Content Gateway.

- Version 7.x prior to 7.5

  Must use ICAP. See the Content Gateway Manager Help for configuration instructions.

Web browsers:

- Websense Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway Manager. Content Gateway Manager supports the following Web browsers:
  - Internet Explorer 7 or 8
  - Mozilla Firefox 3.0.x - 3.5.x

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

Cache Disk

For Websense Content Gateway to operate as a caching proxy, it must have access to at least one raw disk. Otherwise, Content Gateway can function as a proxy only.

To create a raw disk for the proxy cache when all disks have a mounted file system:

> **Note**
>
> This procedure is necessary only if you want to use a disk already mounted to a file system as a cache disk for Content Gateway. Perform this procedure **before** installing Content Gateway.

> **Warning**
> Do not use an LVM (Logical Volume Manager) volume as a cache disk.

> **Warning**
> The Content Gateway installer will irretrievably clear the contents of cache disks.

1. Enter the following command at the prompt to examine which file systems are mounted on the disk you want to use for the proxy cache:

   ```
   df -k
   ```

2. Open the file /etc/fstab and comment out or delete the file system entries for the disk.
3. Save and close the file.
4. Enter the following command for each file system you want to unmount:

   ```
   umount <file_system>
   ```

   where `<file_system>` is the file system you want to unmount.

When the Content Gateway installer prompts you for a cache disk, select the raw disk you created.

> **Note**
>
> It is possible to add cache disks after Content Gateway is installed. For instructions, see the Websense Security Gateway Knowledge Base:
>
> 1. Log into www.mywebsense.com.
> 2. Click **Support**.
> 3. Under **Knowledge Base**, select **Websense Security Gateway**.
> 4. Search for *Adding cache disks after installation*.

Websense filtering software

You must install your Websense filtering software (Websense Web Filter or Websense Web Security) before installing Websense Content Gateway. Be sure to install your filtering software in integrated mode, selecting Websense Content Gateway as the integration product. See the *Websense Web Security and Websense Web Filter Installation Guide*.

Be sure to note the IP addresses of Policy Server and Filtering Service. You will need them when installing Websense Content Gateway.

Note

Be sure that hostname and DNS are configured before installing your Websense products (see *Operating system information*, page 25). In addition, synchronize the time on the filtering-software and Content Gateway machines. It is a best practice to use a Network Time Protocol (NTP) server.

Online Help

Select the **Help** option in Websense Content Gateway Manager to display detailed information about using the product.

IMPORTANT

Default Microsoft Internet Explorer settings may block operation of the Help. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

To view Websense Content Gateway Knowledge Base articles:

1. Log in to MyWebsense (www.mywebsense.com).
2. Click the **Support** tab and select **Websense Security Gateway** from the **Knowledge Base** drop down list.
3. Enter the article title or number in the **Search** box.

Technical Support

Technical information about Websense software and services is available 24 hours a day at:

www.websense.com/support/

- the latest release information
- the searchable Websense Knowledge Base
- Support Forums
- Support Webinars
- show-me tutorials
- product documents
- answers to frequently asked questions
- Top Customer Issues
- in-depth technical papers

For additional questions, click the **Contact Support** tab at the top of the page.

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

For less urgent cases, use our online **Support Request Portal** at ask.websense.com.

For faster phone response, please use your **Support Account ID**, which you can find in the Profile section at MyWebsense.

Location	Contact information
North America	+1-858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033

Location	Contact information
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200
Latin America and Caribbean	+1-858-458-2940

For telephone requests, please have ready:

- Websense subscription key
- Access to the Websense management console.
- Access to the machine running reporting tools and the database server (Microsoft SQL Server or MSDE)
- Familiarity with your network's architecture, or access to a specialist

2 Checklist

Install your Websense filtering product before installing Websense Content Gateway (proxy). Note: This is not required when you are running with only Websense Data Security.

Review the *Deployment Guide* for Websense Web Security Solutions and the *Deploying with Websense Content Gateway* deployment guide supplement. Then, configure your network to support Websense Web Security Gateway Anywhere, Websense Web Security Gateway, or your Websense filtering software plus Websense Content Gateway (depending on the solution your subscription includes). This includes configuring DNS.

Use this checklist in preparation for installing Websense Content Gateway:

Operating system information

Complete these steps on the Websense Content Gateway server:

1. Configure the hostname:

   `hostname <host>`

   where <*host*> is the name you are assigning this machine.
2. Update the HOSTNAME entry in the **/etc/sysconfig/network** file:

   `HOSTNAME=<host>`

   where <*host*> is the same as in Step 1.
3. Specify the IP address to associate with the hostname in the **/etc/hosts** file. This should be static, and not served by DHCP. The proxy uses this IP address in features such as transparent authentication and hierarchical caching. This must be the first line in the file. Do not delete the second line in the file (the one that begins with 127.0.0.1).

   ```
   xxx.xxx.xxx.xxx   <FQDN>    <host>
   127.0.0.1       localhost.localdomain   localhost
   ```

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

4. Configure DNS in the **/etc/resolv.conf** file.

   ```
   search <subdomain1>.<top-level domain> <subdomain2>.<top-level domain> <subdomain3>.<top-level domain>
   nameserver xxx.xxx.xxx.xxx
   nameserver xxx.xxx.xxx.xxx
   ```

   This example demonstrates that more than one domain can be listed on the search line. Listing several domains may have an impact on performance, because each domain is searched until a match is found. Also, this example shows a primary and secondary nameserver being specified.

5. Gather this information:
   - Default gateway (or other routing information)
   - List of your company's DNS servers and their IP addresses
   - DNS domains to search, such as internal domain names. Include any legacy domain names that your company might have acquired.
   - List of additional firewall ports to open beyond SSH (22) and the proxy ports (8080-8090). See *Ports*, page 8.

In addition:

1. Make sure your operating system meets the requirements listed under *Software*, page 18.
2. Set the system time to match that of the filtering software machine. It is a best practice to use a Network Time Protocol (NTP) server.
3. If you are using a Cisco router, ensure that the operating system is IOS v12.x.

Information needed when you install Websense Content Gateway

- Deployment type (Websense Web Security Gateway Anywhere, Websense Web Security Gateway, or Websense Data Security only)
- IP address of Policy Server. Be sure to install your Websense filtering product before installing Websense Content Gateway. (This is not needed when you are running with only Websense Data Security.)
- IP address of Filtering Service. (This is not needed when Websense Content Gateway runs with only Websense Data Security.)
- Which disk will be used to hold the cache
- For clustering:
  - Name of the interface used for cluster communication. This must be a dedicated network interface.
  - Multicast group IP address.

- Enter the following at the 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
  ```

In addition:

- Ensure that the Web browser on the Content Gateway machine is one of those listed under *Software*, page 18. This is required to run the Websense Content Gateway management interface (Content Gateway Manager).

Information needed for proxy deployment

- Will this be an explicit or transparent proxy deployment? See *Network configuration*, page 16.
- List of hosts or Web sites that have special requirements, such as access control lists (ACLs) and security key fobs.
- List of all internal networks that should not go through the proxy.
- List of all trusted partner Web sites that do not need to be decrypted and inspected.

Hardware checklist

- Your CPU is quad-core running at 2.8 GHz or faster.
- Your system has 4 GB of RAM.
- Your system has 2 disks:
  - 100 GB disk for the operating system and Websense Content Gateway.
  - 147 GB disk for caching (2 GB minimum, 147 GB maximum for optimal performance).

Notes

- If Websense Content Gateway will be run in proxy-only mode, a cache disk is not required.
- See *Hardware*, page 17 for detailed requirements.

3 Installation

This chapter covers:

Before installing Websense Content Gateway:

- Put proper security measures in place. (See *Security*, page 7.)
- Install Websense filtering software, and note the IP addresses for Policy Server and Filtering Service. Install the filtering software in integrated mode, with Websense Content Gateway as the integration product. (Filtering software is not needed when you are running with only Websense Data Security.)
- Configure DNS. (See *Operating system information*, page 25.)
- For transparent proxy deployment, configure your WCCP-enabled router or Layer 4 switch. In addition, you must complete router configuration in Websense Content Gateway after the installation is done. Note the IP addresses and ensure that the router or switch is running the correct IOS version. See *System requirements*, page 17.
- Ensure that the Websense Content Gateway host computer has Internet connectivity. If the system does not have access to the Internet, Websense Content Gateway will fail to install.
- For Websense Content Gateway to operate as a caching proxy, at least one raw disk must be available for use as a cache disk. The installer will detect raw disks and allow you to select which you want to use as cache disks. For more information, see *Cache Disk*, page 19.

Downloading Websense Content Gateway

1. Download the installer tar archive to a temporary directory.

   Go to the Websense Knowledge Base, log in to the Web Security Gateway area, and search for the article titled *v7: Accessing Websense Content Gateway downloads*.

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

   ```
   mkdir wcg_v75
   mv <installer tar archive> wcg_v75
   ```

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

   ```
   cd wcg_v75
   ```

4. Unpack the tar archive:

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

Installing Websense Content Gateway

Use the following procedure to install the software.

Note

Up to the configuration summary (Step 16 below), you can quit the installer by pressing CTRL-C. The installation will be cancelled. 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.

Important

If SELinux is enabled, disable it before installing Websense Content Gateway. Do not install or run Websense Content Gateway with SELinux enabled.

1. Make sure you have root permissions:

   ```
   su root
   ```

2. In the directory where you unpacked the tar archive, begin the installation, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

3. If your system does not meet the minimum recommended requirements, you receive a warning. For example:

   ```
   Warning: Websense Content Gateway requires at least 2
   gigabytes of RAM.

   Do you wish to continue [y/n]?
   ```

   Enter **n** to end the installation, and return to the system prompt.

Enter **y** to continue the installation. If you choose to run Websense Content Gateway after receiving a warning, performance may be affected

4. If you choose to continue, accept the subscription agreement. If you do not accept the subscription agreement, the installation stops.

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

5. Specify the full path to the Websense Content Gateway installation directory. The default is **/opt/WCG**. Press **Enter** to accept the default.

   ```
   Enter the full path of the directory to install Websense
   Content Gateway: [/opt/WCG]
   ```

6. Enter and confirm the password for the administrator account. This account enables you to log on to the management interface for Websense 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.

   ```
   Enter the administrator password for the Websense Content
   Gateway management interface.
   Username: admin
   Password:> (your password does not appear)
   Confirm password:> (your password does not appear)
   ```

   

   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, the cursor does not move and masked characters are not shown. After typing a password, press **Enter**. Then repeat to confirm it.

7. Enter an email address where Websense Content Gateway can send alarm messages. Be sure to use @ notation. Do not enter more than 64 characters for this address.

   ```
   Websense Content Gateway requires an email address for alarm
   notification.
   Enter an email address using @ notation: [] > user@corp.com
   ```

8. Enter the IP address for Policy Server. Use dot notation. Press **Enter** to leave this field blank if this Websense Content Gateway deployment is with Websense Data Security only.

   ```
   Enter the Policy Server IP address (leave blank if
   integrating with Data Security only): [] >xxx.xxx.xxx.xxx
   ```

9. Enter the IP address for Filtering Service.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 8.

   ```
   Enter the Filtering Service IP address: [xxx.xxx.xxx.xxx] >
   ```

10. Websense Content Gateway uses 13 ports on your server. Review a listing of these ports to determine if you will encounter any port conflicts.

    Ports preceded by numbers in the list are considered the 9 ports for Websense Content Gateway. Ports preceded by letters are needed if you have subscribed to Websense Web Security Gateway or Web Security Gateway Anywhere.

    ```
    Current port assignments:
    ------------------------------------------
    '1'  Websense Content Gateway Proxy Port  8080
    '2'  Web Interface port                   8081
    '3'  Overseer port                        8082
    '4'  Auto config port                     8083
    '5'  Process manager port                 8084
    '6'  Logging server port                  8085
    '7'  Clustering port                      8086
    '8'  Reliable service port                8087
    '9'  Multicast port                       8088
    'E'  HTTPS inbound port                   8070
    'N'  HTTPS outbound port                  8090
    'M'  HTTPS management port                8071
    'D'  Download Service port                30900
    ```

11. If you do not want to use these ports for Content Gateway, or if the installation program indicates that a port conflict exists, indicate any necessary changes. Any new port numbers you assign must be between 1025 and 65535, inclusive. The default is that no changes are required. It is a best practice to accept the default port assignments unless a port conflict exists.

    ```
    Enter the port assignment you would like to change:
    '1-9,E,M,N,D' - specific port changes
    'X'   - no change
    'H'   - help
    [X] >
    ```

12. If only one network interface is detected, the installation script indicates that two are required for clustering and prompts you to continue the installation.

    Otherwise, enter the number that represents your clustering environment.

    ```
    '1' - Select '1' to configure Websense Content Gateway
            for full clustering. The nodes in the cluster will
    ```

```
        act as a single aggregate cache, including the
        functionality of a management cluster.
'2' - Select '2' to configure Websense Content Gateway
        for management clustering. The nodes in the cluster
        will share configuration/management information
        automatically.
'3' - Select '3' to operate this Websense Content Gateway
        as a single node.

Enter the cluster type for this Websense Content Gateway
installation:
[3] > 3
```

13. If you select 1 or 2, provide information about the cluster. Note that the listed interfaces are examples.

    ```
    Enter the cluster type of this Websense Content Gateway
    installation:
    [3] >1
    Enter the name of this Websense Content Gateway cluster.
    >cluster_name

    Enter a network interface for cluster communication.
    Available interfaces:
    eth0
    eth1
    Enter the desired cluster network interface:
    >eth0

    Enter a multicast group address for cluster cluster0.
    Address must be in the range 224.0.1.27 - 224.0.1.254:
    [224.0.1.37] >
    ```

14. Provide information about cache disks. If no raw disks are detected, Websense Content Gateway runs in proxy-only mode, and no Web pages are cached.

    > **Note**
    > If you choose to not enable raw disk cache now, cache disks may be added after Content Gateway has been installed. For instructions, search the Websense Security Gateway Knowledge Base for *Adding cache disks after installation*.

    ```
    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
```

15. You can elect to send Websense, Inc., information about scanned content. Individual users are never identified.

```
Websense Content Gateway can send information about scanned
content to Websense, Inc. This information helps Websense,
Inc. improve filtering and scanning technology and accuracy.

Websense software never includes information that would
identify specific users.

Do you want to enable the Websense Content Gateway Feedback
Agent [y/n]?
```

16. You are then shown the configuration options you entered, and prompted to complete the installation.

```
Configuration Summary
-------------------------------------------------------------
Websense Content Gateway Install Directory : /opt/WCG
Admin Username for Content Gateway Manager: admin
Alarm Email Address                       : user@corp.com

Policy Server IP Address                  : 11.222.33.44
Filtering Service IP Address              : 11.222.33.44

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]? y
```

If you want to make changes, enter **n** to restart the installation process at the first prompt. If the configuration is satisfactory, 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.

17. Wait for the installation to complete.

Note the location of the certificate required for Content Gateway Manager: **/home/Websense/content_gateway_ca.cer**. See the Getting Started section of the Content Gateway Manager Help for information on importing this certificate.

You may receive an email from Websense Content Gateway (to the address you specified during installation for receiving alerts) with "WCG license download failed" in the subject line. This does not mean a problem occurred with the installation; this alert is generated because a subscription key has not been entered yet. You will enter a key as part of post-installation tasks.

18. When installation is complete, reboot the Websense Content Gateway server.
19. Perform the post-installation steps described under *Post-Installation Tasks*, page 37.

Uninstalling Websense Content Gateway

To uninstall Websense Content Gateway, use the uninstall script (/home/Websense/Current/wcg_uninstall.sh).

1. Make sure you have root permissions.

   ```
   su root
   ```

2. Change to the /../Websense/Current directory:

   ```
   cd /home/Websense/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.

4 Post-Installation Tasks

This chapter lists tasks you must perform after installing Websense Content Gateway. The tasks depend on whether Websense Content Gateway is with a Websense Web filtering product or with Websense Data Security.

Running with Web Filtering

To complete the configuration, follow these steps in your Websense filtering product, and in Websense Content Gateway:

TRITON - Web Security

Perform the following steps to configure Websense filtering software to communicate with Websense Content Gateway.

1. Log on to TRITON - Web Security as WebsenseAdministrator or another unconditional Super Administrator.

   Open a Web browser on any machine in your network and enter the following URL:

   `https://<IP address>:9443/mng`

   where `<IP address>` is the IP address of the TRITON - Web Security machine.

> **Note**
> Only Internet Explorer 7 and 8, or Firefox 3.0.x - 3.5.x, are supported by TRITON - Web Security. On Linux, use Firefox 3.5.x to access all reporting features of TRITON - Web Security.

For more information about logging on to TRITON - Web Security, see the TRITON - Web Security Help available in PDF format on the Websense Support Portal.

2. Click the **Settings** tab of the left navigation pane.
3. Click **Account**.
4. Enter your Websense subscription key.
5. Click **OK**, and then **Save All** (upper right of screen). This initiates a download of the Master Database. A status window shows the progress of the download.
6. When the download is complete, it is recommended that you log off from TRITON - Web Security and log on again before performing any policy configuration.
7. Configure policies and reporting.
8. If you have subscribed to Websense Web Security Gateway:
   a. Enter your subscription key in Websense Content Gateway Manager. See *Content Gateway Manager* below.
   b. Return to TRITON - Web Security and configure scanning options in your Websense filtering software. Go to **Settings** > **Scanning**. This option appears in the Settings pane only after Websense Content Gateway has identified itself to the filtering software. It may take a few minutes for this identification to complete.

Content Gateway Manager

Follow these steps to complete the initial configuration of Websense Content Gateway.

1. Open a Web browser supported by Content Gateway Manager (see *Software*, page 18) and enter the following URL:

   `https://<IP address>:8081`

   where `<IP address>` is the IP address of the Content Gateway machine. Note: 8081 is the default port.

   If the browser warns you about the site's security certificate, choose to proceed to the site anyway:

   - Internet Explorer: Click **Continue to this website (not recommended)**.

- Firefox: Scroll to the bottom of the invalid certificate message and click **Or you can add an exception**. Next, click **Add Exception** > **Get Certificate**. Select **Permanently store this exception**. Then click **Confirm Security Exception**.

> **Note**
> A pending alarm may be indicated on the screen. Clicking it will display more information. If it is a "WCG license download failed" alarm, you may clear it. This condition is resolved by entering a subscription key, which you will do in the next few steps.

2. Enter the user name (**admin**) and password for the Content Gateway Manager default administrator user.

   The password was set up during installation.

3. If you are using Internet Explorer, install the Content Gateway Manager's security certificate:
   a. Next to the address bar, click **Certificate Error**.
   b. Click **View certificates**.
   c. Click **Install Certificate**.
   d. In the Certificate Import Wizard, click **Next** on the welcome dialog box. Select **Automatically select the certificate store based on the type of certificate** and click **Next**. On the last dialog box, click **Finish**.
   e. You are asked if you want to install the certificate. Click **Yes**.
   f. An *Import was successful* message appears. Click **Yes**.
   g. You are returned to the Certificate dialog box. Click **OK**.
4. Click the **Configure** tab on the upper left of the screen.
5. Enter your Websense subscription key:
   a. Click **My Proxy > Subscription > Subscription Management**.
   b. Enter your Websense subscription key and click **Apply**.

   > **Note**
   > The subscription key is the same for both Websense Content Gateway and your Websense filtering product. You must enter the key in both products.

   c. Click **Basic** > **General** and then the **Restart** button to restart Content Gateway.
6. Choose the basic proxy features you want to enable:
   a. Click **My Proxy > Basic > General**.
   b. Under **Features**, click **On** to enable a feature.

See the Content Gateway Manager Help for details. You can access help by clicking **Get Help** in the top right corner of each page of Content Gateway Manager.

7. At the top of the **General** tab, click the **Restart** button to restart Content Gateway.

Enable SSL Manager and WCCP

In Content Gateway Manager:

1. Click **Configure** > **My Proxy** > **Basic** > **General**.
2. If it is not already enabled, set **HTTPS** to **On**. Then click **Apply** and the **Restart** button.
3. Confirm the ports listed on **Configure** > **Protocols** > **HTTPS** > **General**.
4. Add the Content Gateway Manager root security certificate:
   a. In the left navigation pane, click **SSL** > **Certificates** > **Add Root CA**.
   b. Click **Browse**.
   c. Select /**home/Websense/content_gateway_ca.cer** and click **Open**.
   d. Click **Add Certificate Authority**.

   "Issuer successfully imported!" appears.
5. Configure SSL Manager by providing information on the **Configure** > **SSL** pages in Content Gateway Manager.

   Make sure the **Enable the certificate verification engine** option is cleared (default) on the **Configure** > **SSL** > **Validation** > **General** page. When this selection is cleared, HTTPS traffic is decrypted and re-encrypted, but certificates are not checked against the certificate tree on **Configure** > **SSL** > **Certificates** > **Certificate Authorities**.

   Then, monitor HTTPS activity and create incidents to instruct Websense SSL Manager how to process HTTPS traffic. See *Working with Encrypted Data* in the Content Gateway Manager Help.
6. If you are supporting transparent proxy through WCCP-enabled routers, enable WCCP in Content Gateway Manager, and configure the WCCP settings. See the Content Gateway Manager Help for details.

Running with Websense Data Security

Websense Content Gateway can be configured to work with Websense Data Security in the following deployments:

- Websense Content Gateway as part of a Websense Web Security Gateway Anywhere deployment (software or appliance)
- Websense Content Gateway integrated with Websense Data Security

In both cases, you must install the Data Security Management Server on a Windows server, and you must register Content Gateway with it.

To complete the registration, you must choose Deploy in TRITON - Data Security and can perform additional configuration there if desired.

See Chapter 5 of the *Websense Data Security Deployment and Installation Guide* for more information.

Index

R

S

T

U

V

W