## Contents

### Chapter 1
- **Prerequisites and Preparation** .............................................. 5
  - Pre-installation considerations .............................................. 6
  - Security ........................................................................... 6
    - Physical security .......................................................... 6
    - Implementing security through software. ................................. 7
  - Network configurations ....................................................... 13
    - Explicit deployment, single proxy ........................................ 13
    - Explicit deployment, multiple proxies .................................... 14
    - Transparent deployment, single proxy .................................... 14
    - Transparent deployment, multiple proxies ................................. 14
  - System requirements .......................................................... 14
    - Hardware ..................................................................... 14
    - Software ...................................................................... 15
    - Websense filtering software .................................................. 16
  - Online Help ...................................................................... 16
  - Technical Support ............................................................... 17

### Chapter 2
- **Checklist** ........................................................................ 19

### Chapter 3
- **Installation** ..................................................................... 23
  - Downloading Websense Content Gateway ............................... 23
  - Installing Websense Content Gateway ..................................... 23
  - Uninstalling Websense Content Gateway .................................. 28

### Chapter 4
- **Post-installation Tasks** ..................................................... 31
  - Running with Web filtering .................................................... 31
    - Websense Manager ............................................................ 31
    - Content Manager ............................................................. 32
  - Running with Data Security Suite .......................................... 33

### Chapter 5
- **Upgrading to a New Version** ............................................. 35
  - Quick upgrade or roll back .................................................... 35
  - Getting ready ...................................................................... 35
  - Upgrading when integrated with Web filtering ........................ 36
  - Downloading Websense Content Gateway .............................. 36
Upgrading Websense Content Gateway

37
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 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 anti-virus 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 Websense Manager Help for information on the scanning options.

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

- In an explicit proxy deployment, client browsers must be configured to point to the proxy.
- In a transparent proxy deployment, client requests are intercepted and redirected to the proxy 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 Suite, which inspects HTTPS and FTP traffic, you must enable the SSL Manager feature. See the Websense Content Manager Help system for information on SSL Manager and Websense Content Gateway support for the ICAP protocol.
Pre-installation considerations

Before you install Websense Content Gateway, consider the following:

- 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 6.

- Network configuration. Websense Content Gateway can run as an explicit proxy (where browsers point to the proxy), 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 the proxy). See Network configurations, page 13 and see the Websense Content Manager Help system for information on the ARM.

  Websense Content Gateway can proxy HTTP, HTTPS, FTP, and other protocols. To transparent 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 14.

Security

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

In transparent deployments, the client request is intercepted and redirected to the proxy without client involvement. See the Websense Content Manager Help system for additional information on configuring a WCCP-enabled router or a Layer 4 switch and on 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 the proxy. You can address this concern by setting and propagating browser configuration in your organization through Group Policy. For more information, see the Microsoft FAQ on Group Policy at http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/faq.mspx.

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 the proxy. It is strongly recommended that the proxy 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 requires that the following ports be open to support the full set of Websense Web Security Gateway features. These are all TCP ports, unless otherwise noted.

<table>
<thead>
<tr>
<th>Port</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP</td>
</tr>
<tr>
<td>22</td>
<td>SSH for command-line access</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>443</td>
<td>Inbound for transparent HTTPS proxy</td>
</tr>
<tr>
<td>2121</td>
<td>FTP</td>
</tr>
<tr>
<td>2048</td>
<td>WCCP for transparent proxy (if used)</td>
</tr>
<tr>
<td>3130</td>
<td>(UDP) ICP for ICP Cache Hierarchy</td>
</tr>
<tr>
<td>8070</td>
<td>Inbound for explicit HTTPS proxy</td>
</tr>
<tr>
<td>8071</td>
<td>SSL Manager interface</td>
</tr>
<tr>
<td>8080</td>
<td>Inbound for explicit HTTP proxy</td>
</tr>
<tr>
<td>8081</td>
<td>Websense Content Gateway management interface</td>
</tr>
<tr>
<td>8082</td>
<td>Overseer for clustering</td>
</tr>
<tr>
<td>8083</td>
<td>Autoconfiguration for clustering</td>
</tr>
</tbody>
</table>

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 the full set of features, restrict inbound traffic to the unneeded ports, as well. For example, if your subscription does not include scanning, restrict inbound traffic to port 30900.
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.

If the proxy 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 the proxy.
- Cluster interface (CLUSTER_NIC) - The physical interface used by the proxy to communicate with members of the cluster.

In the list of rules, the associated interface is shown with the “-i” option. In 1 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...
Prerequisites and Preparation

.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 rule should be first.

<table>
<thead>
<tr>
<th>Block ALL inbound</th>
<th>--policy INPUT DROP</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Allow ALL outbound</th>
<th>--policy OUTPUT ACCEPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block ALL forward requests</td>
<td>--policy FORWARD DROP</td>
</tr>
<tr>
<td>Allow ALL traffic on the local (loopback) interface</td>
<td>-I INPUT -i lo -j ACCEPT</td>
</tr>
<tr>
<td>Allow ALL responses on established connections</td>
<td>-I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT</td>
</tr>
<tr>
<td>Allow ALL inbound port 22</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 22 -j ACCEPT</td>
</tr>
<tr>
<td>Allow ALL inbound ICMP</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p ICMP -j ACCEPT</td>
</tr>
</tbody>
</table>

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 |
Prerequisites and Preparation

Local Policy Server

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

<table>
<thead>
<tr>
<th>Rule</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ALL inbound port 40000</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 40000 -j ACCEPT</td>
</tr>
<tr>
<td>Allow ALL inbound port 55806</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 55806 -j ACCEPT</td>
</tr>
<tr>
<td>Allow ALL inbound port 55880</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 55880 -j ACCEPT</td>
</tr>
<tr>
<td>Allow ALL inbound port 55905</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p udp --dport 55905 -j ACCEPT</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ALL from &lt;Policy Server IP&gt; ports 1024+</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp -s &lt;Policy Server IP&gt; --dport 1024:65535 -j ACCEPT</td>
</tr>
</tbody>
</table>

Local Filtering Service

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

<table>
<thead>
<tr>
<th>Rule</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ALL inbound port 55807</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 55807 -j ACCEPT</td>
</tr>
<tr>
<td>Allow ALL inbound port 15868</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 15868 -j ACCEPT</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ALL from &lt;Filtering Service IP&gt; ports 1024+</td>
<td>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp -s &lt;Filtering Service IP&gt; --dport 1024:65535 -j ACCEPT</td>
</tr>
</tbody>
</table>
**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).

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ALL inbound port 21 - for FTP</td>
<td><code>-i &lt;CLIENT_NIC&gt; -I INPUT -p tcp --dport 21 -j ACCEPT</code></td>
</tr>
<tr>
<td>Allow ALL inbound port 2121 - for FTP</td>
<td><code>-i &lt;CLIENT_NIC&gt; -I INPUT -p tcp --dport 2121 -j ACCEPT</code></td>
</tr>
</tbody>
</table>

Optional features

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

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow gathering of statistics over the overseer port</td>
<td><code>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 8082 -j ACCEPT</code></td>
</tr>
<tr>
<td>Allow PAC file distribution from the proxy (Browser Auto-Config)</td>
<td><code>-i &lt;CLIENT_NIC&gt; -I INPUT -p tcp --dport 8083 -j ACCEPT</code></td>
</tr>
<tr>
<td>Allow collation of logs for multiple proxies</td>
<td><code>-i &lt;MGMT_NIC&gt; -I INPUT -p tcp --dport 8085 -j ACCEPT</code></td>
</tr>
</tbody>
</table>

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 Websense Content Manager Help system 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 the proxy, over the ports that the proxy uses for the associated protocol.

The standard port for HTTP is 80; the standard port for HTTPS is 443.

Because the proxy handles both HTTP and HTTPS traffic, two proxy ports are recommended to support the two protocols. The default proxy port in Websense Content Gateway for HTTP traffic is 8080. For HTTPS traffic, the default proxy port is 8070.

Use the instructions below to configure client browsers manually. Alternatively, use a PAC or WPAD file to configure client browsers.
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 8070.
6. Clear Use the same proxy server for all protocols.
7. Click OK to close each screen in this dialog box.

Configuring Firefox 2.0 and later

1. From the Firefox browser, select Tools > Options > Advanced, and then select the Network tab.
2. Select Settings.
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 8070.
6. Click OK to close each screen in this dialog box.

Network configurations

Consider how Websense Content Gateway will be used on your network. The following configurations are described below. For other deployment options, see the Websense Deployment Guide Supplement, Deploying with Websense Content Gateway.

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

Explicit deployment, single proxy

Explicit proxy deployment requires pointing the client browser to the proxy. HTTP, or HTTPS, or FTP over HTTP traffic gets to the proxy 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 the proxy, there is some risk that users will edit their browser settings to avoid the proxy. 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](http://example.com/rfc3768) for information on VRRP.

**Transparent deployment, single proxy**

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

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

**Transparent deployment, multiple proxies**

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

**System requirements**

**Hardware**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Quad-core running at 2.8 GHz or faster</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>2 disks:</td>
</tr>
<tr>
<td></td>
<td>• 100 GB for the operating system, Websense Content Gateway, and temporary data.</td>
</tr>
<tr>
<td></td>
<td>• 147 GB for caching</td>
</tr>
<tr>
<td></td>
<td>If caching will not be used, the disk is not required.</td>
</tr>
<tr>
<td></td>
<td>• The caching disk:</td>
</tr>
<tr>
<td></td>
<td>‒ Must be a raw disk (not a mounted file system)</td>
</tr>
<tr>
<td></td>
<td>‒ Must be dedicated</td>
</tr>
<tr>
<td></td>
<td>‒ Must not be part of a software RAID</td>
</tr>
<tr>
<td></td>
<td>‒ For best performance, use a 10k RPM SAS disk on a controller that has at least 64MB of write-through cache.</td>
</tr>
</tbody>
</table>

Network Interfaces 2
Prerequisites and Preparation

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:**
This is the only version and kernel supported.

- Red Hat Enterprise Linux Advanced Server Release 4, Update 5, kernel 2.6.9-55
  - To display the kernel version installed on your system, enter the command:
    
    ```
    /bin/uname -r
    ```
- RPM compat-libstdc++-33-3.2.3-47.3.i386.rpm
  - 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
    ```

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

- Version 7.1

**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.

**Integration with Websense Data Security Suite:**

- Version 7.1
The order of installation does not matter.

**Supported browsers:**

- Websense Content Gateway is configured and maintained with a Web-based user interface called the Content Manager. Supported browsers include:
  - Internet Explorer 7 or 8
  - Mozilla Firefox 2 or 3

**Websense filtering software**

You must install your Websense filtering software (Websense Web Filter or Websense Web Security) before you install Websense Content Gateway. Be sure to install your filtering software as an integration, selecting Websense Content Gateway as the integration product. See the Websense Web Security installation guide for your configuration.

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 DNS is configured before installing your Websense products. In addition, be sure that the time is set on the server. Use of a Network Time Protocol (NTP) server is recommended.

**Online Help**

Select the Help option within the program 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.)

To view Websense Content Gateway Knowledge Base articles:

1. Log in to [MyWebsense](#).
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.

<table>
<thead>
<tr>
<th>Location</th>
<th>Contact information</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>+1-858-458-2940</td>
</tr>
<tr>
<td>France</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227</td>
</tr>
<tr>
<td>Germany</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347</td>
</tr>
<tr>
<td>UK</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401</td>
</tr>
<tr>
<td>Rest of Europe</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401</td>
</tr>
<tr>
<td>Middle East</td>
<td>Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401</td>
</tr>
</tbody>
</table>
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
Before proxy installation, install your Websense filtering product. (This is not required when you are running with only Websense Data Security Suite).

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

Use this checklist in preparation for installing Websense Content Gateway.

**Operating system information**

Please complete these steps on the Websense Content Gateway server:

1. Configure the hostname:
   ```
   hostname mycompany.com
   ```
2. Update the HOSTNAME entry in the `/etc/sysconfig/network` file:
   ```
   HOSTNAME=mycompany.com
   ```
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 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).
   ```
   xx.xxx.xxx.xx  mycompany.com  mycompany
   127.0.0.1       localhost.localdomain  localhost
   ```
   ```
   search mycompany.com site2.com site3.com
   nameserver 1.2.3.4
   nameserver 1.2.3.5
   ```
   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.
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 (8070-8090). See *Ports*, page 7.

In addition:

1. Ensure that your Linux operating system is Red Hat Enterprise Linux (RHEL) AS Release 4, Update 5, kernel 2.6.9-55.
2. Verify that the following RPM is on your system:
   `compat-libstdc++-33-3.2.3-47.3.i386.rpm`
3. Set the system time. Use of a Network Time Protocol (NTP) server is recommended.
4. 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 Data Security Suite only, or with filtering)
- 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 Suite.)
- IP address of Filtering Service. (This is not needed when Websense Content Gateway runs with Websense Data Security Suite.)
- 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 your browser is either Internet Explorer v7 (or higher) or Firefox v2 (or higher). This is required to run the Websense Content Gateway management interface (Websense Content Manager).

### Information needed for proxy deployment

- Will this be an explicit or transparent proxy deployment? See *Network configurations*, page 13.
Checklist

- 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 a 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.

**Note**

☑ If Websense Content Gateway will be run in proxy-only mode, only one disk is required.
Installation

Before installing Websense Content Gateway:
- Put proper security measures in place. (See Security, page 6.)
- Install Websense filtering software, and note the IP addresses for Policy Server and Filtering Service. Install the filtering software as an integration, with Websense Content Gateway as the integration product. (Filtering software is not needed when you are running with only Websense Data Security Suite.)
- Configure DNS.
- 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 14.
- 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.

Downloading Websense Content Gateway

1. Download the installer files.
2. Create a directory for the tar archive, and then move the archive to the new directory. For example:
   ```
   mkdir wcg_v7xx
   mv xxx.gz wcg_v7xx
   ```
3. Change to the directory you created in Step 2.
   ```
   cd wcg_v7xx
   ```
4. Open the tar archive:
   ```
   tar -xvzf filename
   ```

Installing Websense Content Gateway

Use the following procedure to install the software.
1. Make sure you have root permissions:
   
   su root

2. In the directory where you opened the tar archive, begin the installation, and respond to the questions 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 Websense Content Manager. Do not use spaces in the password. Do not enter more than 16 characters. 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 logon to the Websense Content Manager

   Username: admin
   Password:
   > (your password does not appear)
   Confirm password:
   > (your password does not appear)

7. Enter an email address where Websense Content Gateway can send alarms. 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 Suite only.
Enter the Policy Server IP address (or leave blank for Data Security Suite-only integration): [] > 11.222.33.444

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: [11.222.33.444] >

10. Websense Content Gateway uses 14 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 10 ports for Websense Content Gateway. Ports preceded by letters are needed if you have subscribed to Websense Web Security Gateway.

Current port assignments:
----------------------------------------------
'0'  Websense Content Gateway Proxy Port  8080
'1'  Web Interface port                   8081
'2'  Overseer port                        8082
'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'  SNMP encapsulation port              8089
'E'  HTTPS inbound port                   8070
'N'  HTTPS outbound port                  8090
'M'  HTTPS management port                8071
'D'  Download Service port                30900

11. If you are not using these ports, 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.

Enter the port assignment you would like to change:
'0-9,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 disks are detected, Websense Content Gateway runs in proxy-only mode, and no Web pages are cached.

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 is the list of selections
(1) /dev/sdb 146778685440 0x0

b. Indicate if you want to add or remove disks individually or in 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.
Installation

Option: > A
[ ] (1) /dev/sdb 146778685440 0x0

 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 Websense Content Manager: admin
  Alarm Email Address : user@corp.com
  Policy Server IP Address : 11.222.33.444
  Filtering Service IP Address : 11.222.33.444
  Websense Content Gateway Cluster Type : NO_CLUSTER
Websense Content Gateway Cache Type : LRAW_DISK
Cache Disk               : /dev/sdb
Total Cache Partition Used : 1

************************
* WARNING *
************************
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 need to make changes, enter n to restart the installation process. If the configuration is satisfactory, enter y.

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

18. When installation is complete, reboot the Websense Content Gateway server.

19. Perform the post-installation steps described under Post-installation Tasks, page 31.

Uninstalling Websense Content Gateway

Uninstalling Websense Content Gateway requires that you use the original installer files. If they have been deleted from the machine, download them again before following this procedure to uninstall the software.

1. Make sure you have root permissions.
   su root
2. Change to the directory when you opened the tar archive. For example:
   cd wcg_v7xx
3. Uninstall Websense Content Gateway:
   ./wcg_install.sh -u
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.
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 Data Security Suite.

Running with Web filtering

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

**Websense Manager**

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

1. Log on to Websense Manager as WebsenseAdministrator or another unconditional Super Administrator.
   
   If you’re not sure how to log on to Websense Manager, see the Websense Manager Help system 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*. 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 Websense Manager 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. You can configure scanning options in Websense manager only after you enter your subscription key in the proxy management interface. So, enter your subscription key in Websense Content Manger. See *Content Manager*. 
b. Then, return to Websense Manager 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 Manager

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

1. Open a browser and enter the IP address of the machine running Websense Content Gateway followed by a colon (:) and the Web interface (Websense Content Manager) port. The default port is 8081.

   https://xx.xxx.xxx.xx:8081

2. Click the Configure tab of the left navigation pane.
3. Click My Proxy > Subscription > Subscription Management.
4. Enter your Websense subscription key.

   ![Note]

   The subscription key is the same for both Websense Content Gateway and your Websense filtering product. It is necessary to enter the key in both products.

5. Turn On features and protocols on Configure > My Proxy > Basic > General. See the Websense Content Manager Help system for details. You can access help by clicking Get Help in the top right corner of each page in the management interface.
6. Restart Websense Content Gateway.

Enable SSL Manager and WCCP

In Websense Content Manager:

1. Go to the Configure > My Proxy > Basic > General page.
2. Set HTTPS to On.
3. Click Apply, and then click Restart.
4. Confirm the ports listed on Configure > Protocols > HTTPS > General.
5. Configure SSL Manager by providing information on the Configure > SSL pages in Websense Content 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 Websense Content Manager Help system.

6. If you are supporting transparent proxy through WCCP-enabled routers, enable WCCP in Websense Content Manager, and configure the WCCP settings. See the Websense Content Manager Help system for details.

**Running with Data Security Suite**

In Websense Content Manager:

1. Click ICAP **On** on **Configure > My Proxy > Basic > General**.
2. Provide the requested information on **Configure > My Proxy > Networking > ICAP**.
3. Click **Apply**, and then click **Restart** on **Configure > My Proxy > Basic > General**.

See your Websense Data Security Suite documentation for additional details.
The installer for Websense Content Gateway handles version upgrades and replacements, as well as new installations. You can:

- Install a v7.x proxy for the first time (see Chapter 3: Installation, Installing Websense Content Gateway)
- Uninstall (see Chapter 3: Installation, Uninstalling Websense Content Gateway)
- Re-install a v7.x proxy
- Upgrade or replace an installed v7.x proxy with a different v7.x version. The replacement version can be either newer or older.

### Quick upgrade or roll back

To upgrade or roll back to a previous version quickly:

- Run the installer for the desired version (new or previous).
- Choose to re-use the installation selections made during the previous installation.
- Choose to retain all proxy settings that were previously made (via the user interface and via configuration files).

This quick upgrade or roll back stops proxy services; backs up settings and logs; removes the proxy software that is currently installed; installs the version whose installer was used; restores all settings, and restarts the proxy.

### Getting ready

Before upgrading or replacing a version:

- Determine if you want to use the same installer selections you used when you last installed (as an alternative, you can answer all installer questions again).
- Determine if you want to use the same proxy settings already in place on your system. These are settings you made in Websense Content Manager or in proxy configuration files. Alternatively, you can revert to Websense default settings.
- 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 14.

- Keep in mind that both Websense Content Gateway and Web filtering components
  must run at the same version. You must upgrade all to v7.1 or restore all to their
  previous version. There is no cross-version compatibility.

### Upgrading when integrated with Web filtering

When you are ready to upgrade Websense Content Gateway, you must also upgrade
Websense Web Security (or Websense Web Filter) to the same version in order for the
products to interact properly.

Be sure to plan the timing of the upgrade. Both products are unavailable during the
upgrade, which affects users’ Internet access.

---

**Important**

Be sure to choose a quiet time on the network for the upgrade. During the upgrade, users will have either
unfiltered access or no access, depending on how your Internet access is configured.

---

1. Stop all services for both the proxy and the filtering software.
2. Upgrade the filtering software, starting with Policy Broker and Policy Server. See
   the Websense *Installation Supplement for Upgrading* for instructions.
3. Upgrade the proxy software, as described in this chapter. See *Upgrading
   Websense Content Gateway*, page 37.
4. Start the services for both products to resume proxy and filtering activity.

### Downloading Websense Content Gateway

5. Download the files.
6. Create a directory for the tar archive, and then move the archive to the new
directory. For example:
   ```bash
   mkdir wcg_v7xx
   mv xxx.gz wcg_v7xx
   ```
7. Change to the directory you created in Step 6.
   ```bash
   cd wcg_v7xx
   ```
8. Open the tar archive and install the files:
   ```bash
   tar -xvzf filename
   ```
Upgrading Websense Content Gateway

**Warning**

*Before you begin*, ensure that /tmp has enough free space to hold existing Websense Content Gateway log files. During the upgrade procedure, the installer temporarily copies log files located in /opt/WCG/logs to /tmp. If the /tmp partition doesn’t have enough available space and becomes full, the upgrade will fail.

If you determine that /tmp doesn’t have enough space, manually move the contents of /opt/WCG/logs to a partition that has enough space and then delete the log files in /opt/WCG/logs. Run the installer to perform the upgrade. When the upgrade is complete, move the logs files from the temporary location back to /opt/WCG/logs and delete the files in the temporary location.

For step-by-step instructions, see the Knowledge Base article titled *Upgrading can fail if the /tmp partition becomes full.*

**Also:** Snapshots saved in /opt/WCG/config/snapshots are not saved during the upgrade procedure. To preserve your snapshots, manually copy them to a temporary location and copy them back after the upgrade is complete.

**Note:** /opt/WCG is the default installation location. Substitute the location of your installation.

Use the following procedure to install the software.

1. Make sure you have root permissions:
   ```bash
   su root
   ```

2. In the directory where you opened the tar archive, begin the upgrade or replacement, and respond to the questions.
   ```bash
   ./weg_install.sh
   ```

3. If your system does not meet the minimum recommended requirements, you receive a warning. For example:
   ```bash
   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. The installer displays the version of Websense Content Gateway currently on the server, and asks if you want to replace it. If you do not confirm that you want to replace it, the installation stops.

   WCG version 7.0.0-0 was found.
   Do you want to replace it with version 7.1.0-0 [y/n]?

6. Existing settings and logs are copied to backup files and stored. For example:

   Copying SSL Manager settings to /home/Websense/OldVersions/7.0.0-0-20081030-143642/...done

   Stopping Websense Content Gateway processes...done

   Copying settings from /opt/WCG to /home/Websense/OldVersions/7.0.0-0-20081030-143642/...done

   Moving log files from /opt/WCG/logs to /tmp/WCGInstall/logs/...done

7. You can either re-use the installation selections you entered last time, or provide new answers to all installation prompts:

   Previous install configuration </home/Websense/Current/WCGinstall.cfg> found.

   Use current installation selections [y/n]?

   Enter y to use previous installation selections. Proceed to step 7.

   Enter n to revert to Websense default values, and receive all installation questions and answer them again. Proceed to step 9.

8. If you answered y at step 6, then you can also leave proxy settings at their current values or revert to Websense default values.

   Restore settings after install [y/n]?

   Enter y to keep the proxy settings as they are.

   Enter n to restore Websense default settings for the proxy.

9. The previously installed version of Websense Content Gateway is removed, and the settings and selections you chose to retain are re-used.

   The upgrade (or replacement) 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.

To start the Websense Content Gateway management interface:

   a. Start a browser.

   b. 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.
c. Log on using username admin and the password you chose earlier.

Sample text is shown here as an upgrade moves to completion, for a scenario in which both the previous installation selections and the previous proxy settings are retained:

Removing old WCG installation...done

Using configuration file: /tmp/WCGinstall.cfg

Extracting files...done

Installing Adaptive Redirection Module (ARM)...done

Websense Content Gateway will operate in proxy-only mode...done

Setting Websense Content Gateway environment...done

Installing SSL Manager...done

Restoring settings from /home/Websense/OldVersions/7.0.0-0-20081030-143642/ to /opt/WCG...done

Restoring log files from /tmp/WCGInstall/logs to /opt/WCG/logs/...done

Starting services...
Starting Websense Download Service...
Starting Websense Content Gateway...
Restoring SSL Manager settings from /home/Websense/OldVersions/7.0.0-0-20081030-143642/...done

Zipping old settings...done

*COMPLETED* Websense Content Gateway 7.1.0-0 installation.
A log file of this installation process has been written to /home/Websense/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 (Websense Content 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 /home/Websense.

[root@RHEL45_TEST WSInstall]#

The upgrade (or replacement) is now complete, and the proxy software is running.

10. If you answered `n` at step 6 above, then the previously installed version of Websense Content Gateway is removed, and you are prompted with the first installation question. 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]

11. 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 Websense Content Manager. Do not use spaces in the password. Do not enter more than 16 characters. 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 logon to the Websense Content Manager
Username: admin
Password:
> (your password does not appear)
Confirm password:
> (your password does not appear)

12. Enter an email address where Websense Content Gateway can send alarms. 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@company.com

13. 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 Suite only.

Please enter the IP address for Policy Server: [] >11.222.33.444

14. 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 13.

Please enter the IP address for Filtering Service: [11.222.33.444] >
15. Websense Content Gateway uses 14 ports on your server. Review a listing of these ports, below, to determine if you will encounter any port conflicts.

Ports preceded by numbers in the list are considered the 10 ports for Websense Content Gateway. Ports preceded by letters are needed if you have subscribed to Websense Web Security Gateway.

Current port assignments:
----------------------------------------------
'0'  Websense Content Gateway Proxy Port  8080
'1'  Web Interface port                   8081
'2'  Overseer port                        8082
'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'  SNMP encapsulation port              8089
'E'  HTTPS inbound port                   8070
'N'  HTTPS outbound port                  8090
'M'  HTTPS management port                8071
'D'  Download Service port                30900

16. If you are not using these ports, 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.

Enter the port assignment you would like to change:
'0-9,E,M,N,D' - specific port changes
'X'  - no change
'H'  - help

[X] >

17. 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 as full clustering, in which the nodes in the cluster act as a single aggregate cache, and it includes the function of a management cluster.
'2'  - Select '2' to configure Websense Content Gateway as management clustering, in which the nodes would share configuration information within the cluster automatically.
'3'  - Select '3' to operate this Websense Content Gateway as a single node.

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

18. 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] >

19. Provide information about cache disks. If no disks are detected, Websense Content Gateway runs in proxy-only mode, and no Web pages are cached.
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 is the list of selections
(1) /dev/sdb 146776685440 0x0

b. Indicate if you want to add or remove disks individually or in a group.
Choose one of the following options:
'A' - Add number(s) to selection
'R' - Remove number(s) from selection
'S' - Add all numbers to selection
'U' - Remove all numbers from selection
'D' - Display current selection
'X' - Done with selection, continue Websense Content Gateway installation.
'O' - Quit Websense Content Gateway installation.

Option: >A
[ ] (1) /dev/sdb 146776685440 0x0

c. Specify which disk(s) to use for the cache.
Enter number to select 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 number(s) to selection
'R' - Remove number(s) from selection
'S' - Add all numbers to selection
'U' - Remove all numbers from selection
'D' - Display current selection
'X' - Done with selection, continue Websense Content Gateway installation.
'O' - Quit Websense Content Gateway installation.

Option: >X

A listing of the selected disks is displayed.

Here is the final selection
/dev/sdb 146778685440 0x0

20. 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]?

21. 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 Websense Content Manager: admin
Alarm Email Address                      : username@company.com
Policy Server IP Address                 : 11.222.33.444
Filtering Service IP Address            : 11.222.33.444
Websense Content Gateway Cluster Type   : NO_CLUSTER
Websense Content Gateway Cache Type     : PROXY_ONLY

Do you want to continue installation with this configuration [y/n]? y

If you need to make changes, enter n to restart the installation process. If the configuration is satisfactory, enter y.
22. Note the location of the certificate required for Websense Content Manager: 
/home/Websense/content_gateway_ca.cer. See the Getting Started section of the 
Websense Content Manager Help system for details on importing certificates.

23. When installation is complete, reboot the Websense Content Gateway server.

24. Perform the post-installation steps described under Post-installation Tasks, page 31.