Upgrading Websense Content Gateway from v7.5.0 to v7.5.x

Topic 60026 / Updated: 20-June-2011

Applies To:	Websense Content Gateway
	Websense Web Security Gateway

The installer for Websense Content Gateway handles software only version upgrades and replacements. You can:

◆ Upgrade or replace an installed v7.5.x proxy with a different v7.5.x version. The replacement version can be either newer or older.

◆ Re-install a v7.5.x proxy

To handle V-Series appliance upgrades refer to:

◆ *V-Series Release Notes v7.5.2*
◆ *V-Series Release Notes v7.5.3*
◆ *V-Series Release Notes v7.5.5*

Upgrading from versions prior to v7.5.0

The following steps are required to upgrade from versions prior to v7.5.0.

◆ Back up files and perform a new installation of v7.5.0 Content Gateway as described in the *v7.5.0 Installation Guide*.

◆ Upgrade from v7.5.0 to the desired maintenance version described in this document.

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 the Content Gateway 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.
- Keep in mind that the installed version numbers for Websense Content Gateway and proxy components must be the same. The Websense Web and proxy components must be at the same base version (v7.5). If multiple proxies are installed, they must all be upgraded to the same revision. Upgrade all components to v7.5.2, v7.5.3 or v7.5.5 or restore all to their previous version. There is no cross-version compatibility.

Upgrading when integrated with Web filtering

When upgrading Websense Content Gateway, you must also upgrade Websense Web Security or Websense Web Filter to v7.5.0 or higher for the products to work together properly.

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

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*.

4. Start the services for both products to resume proxy and filtering activity.

Downloading Websense Content Gateway

1. Download the installer tar archive for v7.5.x from mywebsense.
2. Create a temporary directory to unpack the archive.
   For example:

   ```
   mkdir wcg_v753
   ```

3. Move the tar archive to the temporary directory.
   For example:

   ```
   mv /root/Desktop/WebsenseCG753Setup_Lnx.tar.gz /wcg_v753
   ```

4. Change to the temporary directory.
   For example:

   ```
   cd wcg_v753
   ```

5. Unpack the tar archive.
   For example:

   ```
   tar -xvzf WebsenseCG753Setup_Lnx.tar.gz
   ```

Upgrading Websense Content Gateway

⚠️ **Warning**

Before you begin, ensure that **/tmp** has enough free space to the 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:

    ```
    su root
    ```

2. In the directory where you opened the tar archive, begin the upgrade or replacement, and respond to the questions.

    ```
    ./wcg_install.sh
    ```

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

    ```
    Warning: Websense Content Gateway cd 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 to 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 7.5.0-1013 was found.
Do you want to replace it with version 7.5.3-1035 [y/n]?
```

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

```
Stopping Websense Content Gateway processes...done


Copying settings from /opt/WCG to /home/Websense/
OldVersions/7.5.0-1013-20110127-145300/...done


Copying SSL Manager settings to /home/Websense/OldVersions/
7.5.0-1013-20110127-145300/...done


Moving log files from /opt/WCG/logs to /opt/wcg_tmp/logs/
...done
```

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

```
Previous installation selections </home/Websense/Current/
WCGinstall.cfg> found.


Use previous installation selections [y/n]?
```

Enter **y** to use previous installation selections. Proceed to step 8.

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 7, 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
```

```
Installing the DSS Policy Engine...done


Restoring settings from /home/Websense/OldVersions/7.5.0-
1013-20110127-145300/ to /opt/WCG...done


Restoring SSL Manager settings from /home/Websense/
OldVersions/7.5.0-1013-20110127-145300/...done


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


Zipping old settings...done


Starting services...

Starting Websense Download Service...

Starting Websense Content Gateway...


*COMPLETED* Websense Content Gateway 7.5.3-1035
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 (Content Gateway Manager):
------------------------------------------------------------------------------------------
```

1. Start a browser.
2. Enter the IP address of the Websense Content Gateway
   server, followed by a colon and the management interface
   port (8081 for this installation).

   For example: https://11.222.33.44:8081.
3. Log on using username admin and the password you chose
   earlier.

   A copy of the CA public key used by the Manager is located
   in /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 7 above, then the previously installed version of
    Websense Content Gateway is removed, and you are prompted with the first
    installation question.

11. Specify the full path to the Websense Content Gateway installation directory. The default is **/opt/WCG**.

Press **Enter** to accept the default.

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

12. 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. 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.

```
Websense Content Gateway Administration Information
------------------------------------------------------
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)*

13. 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

14. 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.

```
Websense Content Gateway Integrations Configuration
------------------------------------------------------
Enter the Policy Server IP address (leave blank if
integrating with Data Security only): [] > 11.222.33.444
```

15. 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.

```
Enter the Filtering Service IP address: [11.222.33.444] >
```

16. 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.

```
Websense Content Gateway Port Configuration

--------------------------------------------------

Websense Content Gateway uses 14 ports on your server.


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
```

17. 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:
'1-9,E,M,N,D' - specific port changes
'X' - no change
'H' - help
```

```
[X] >
```

18. 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.

    ```
    Websense Content Gateway Clustering Information

    ---------------------------------------------------

    Websense Content Gateway requires at least 2 interfaces to
    support clustering.


    Press ENTER to continue without clustering...


    '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] >
    ```

19. 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] >
```

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

```
Websense Content Gateway Cache Disk Configuration
---------------------------------------------------
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 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.
'Q' - Quit Websense Content Gateway installation.
Option: >A
[ ] (1) /dev/sdb 146778685440 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.
'Q' - Quit Websense Content Gateway installation.
```

Option: >**X**

A listing of the selected disks is displayed.

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

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

```
Websense Content Gateway Optional Feedback Configuration
--------------------------------------------------
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]?
```

22. 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                   : 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**.

23. 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 system for details on importing certificates.

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

25. Perform the *post-installation* steps.

Post-installation Tasks

Topic 60027 / Updated: 09-June-2011

Applies To:	Websense Content Gateway v7.5.2, v7.5.3 or v7.5.5
	Websense Web Security Gateway v7.5.2, v7.5.3 or v7.5.5

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, or both.

Running with Web filtering

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

TRITON - Web Security console

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

1. Log on to the TRITON - Web Security console 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.

   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**. 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 the TRITON - Web Security console 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 the TRITON - Web Security console only after you enter your subscription key in the proxy management interface. So, enter your subscription key in the Content Gateway Manager. See *Content Gateway Manager*.

   b. Return to the TRITON - Web Security console 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 browser and enter the IP address of the machine running the Content Gateway Manager:

   ```
   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 of the left navigation pane.

5. Enter the Websense subscription key:

   a. Click **My Proxy > Subscription > Subscription Management**.

   b. Enter your Websense subscription key and click Apply.

> 💡 **Important**
> 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.

    c. Click **Basic > General** and then the **Restart** button to restart the Websense 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 system for details. You can access help by clicking **Get Help** in the top right corner of each page in the management interface.

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

Enable SSL Manager and WCCP

In the Content Gateway Manager:

1. Click **Configure > My Proxy > Basic > General**

2. If 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 the 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 the Content Gateway Manager, and configure the WCCP settings. See the Content Gateway Manager Help for details.

Running with Data Security Suite

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.