Upgrade Guide: Forcepoint Web Security

Upgrade Instructions | Forcepoint Web Security | v8.5.x | 30-Nov-2018

Version 8.4 reset the product names and solution bundles for web protection solutions.

New Name	Older Name
Forcepoint Web Security	TRITON AP-WEB
Forcepoint Web Security with: ● Hybrid Module ● DLP Module ● Forcepoint Advanced Malware Detection (if purchased)	TRITON AP-WEB with: ● Web Hybrid Module ● Web DLP Module ● Web Sandbox Module (if purchased) Websense TRITON Web Security Gateway Anywhere

For more information about how these changes may affect you, contact your sales partner or Forcepoint Sales representative.

These instructions describe how to upgrade from v8.1, v8.2, v8.3 and v8.4 web protection solutions to Forcepoint Web Security **v8.5** or from v8.2, v8.3, v8.4 and v8.5 to **v8.5.3.** Direct upgrades from v7.8.x or v8.0.x to v8.5, or from 7.8.x, 8.0.x or 8.1.x to v8.5.3 are not supported.

If your deployment includes a Forcepoint Appliance, see this upgrade guide for additional information.

Important

If you are currently running a Web Security Gateway or Gateway Anywhere version earlier than v7.8.4, upgrade to v7.8.4 first, then upgrade to v8.4.x first. See this upgrade guide for instructions.

- Content Gateway Hotfix 94 must be applied to v7.7.x prior to upgrading Content Gateway (software or appliance) to v7.8.4. This retains the default Sync Mode setting for real-time analysis, and can prevent latency.
- Appliance Hotfix 90 must be applied to v7.7.x prior to upgrading the appliance to v7.8.4. See the v7.8.x Upgrade Instructions.

If you have an earlier version, there are interim steps to perform. These are shown in the table below.

Your current version	Step 1	Step 2	Step 3	Step 4	Step 5
v7.1.x	Upgrade to 7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x
v7.5.x	Upgrade to 7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x
v7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x	
v7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x	none	
v7.8.1 v7.8.2 v7.8.3	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x	none	
v7.8.4	Upgrade to 8.4.x X Series: Upgrade to 8.0.0	Upgrade to 8.5.x X Series: Upgrade to 8.3.x	X Series: Upgrade to 8.5.x	none	
v8.0.x	Upgrade to 8.3.x*	Upgrade to 8.5.x	none	none	
v8.1.x	Upgrade to 8.5.	Upgrade to 8.5.3.	none	none	

Your current version	Step 1	Step 2	Step 3	Step 4	Step 5
v8.2.x	Upgrade to 8.5.x	none	none	none	
v8.3.x	Upgrade to 8.5.x	none	none	none	
v8.4.x	Upgrade to 8.5.x				
v8.5	Upgrade to v8.5.3				
*** TRITON AP-WEB customers upgrading from v8.0.x to v8.3 should install Content Gateway v8.3 Hotfix 3 if v8.3 will be used in production prior to upgrading to v8.5.**					

The following operating systems are not supported in this version. If you are using one of these operating systems, you must migrate your operating system before upgrading to v8.5.x, as outlined below:

v8.5: Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6.1 - 6.7 v8.5.3: Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6.1 - 6.8	1. Migrate to Red Hat Enterprise Linux 6.x (from Red Hat Enterprise Linux 5, if necessary) 2. Migrate to Red Hat Enterprise Linux 6.8. 3. Upgrade to v8.3.x on the new platform. 4. Migrate to Red Hat Enterprise Linus 6.9. 5. Upgrade to v8.5.x on the new platform.
v8.5: Red Hat Enterprise Linux 7.0 - 7.1. v8.5.3: Red Hat Enterprise Linux 7.0 - 7.2.	1. Migrate to Red Hat Enterprise Linux 7.3. 2. Upgrade to v8.4.x on the new platform. 3. Upgrade to v8.5.x on the new platform.
v8.5.x: Windows 2008 (32-bit)	1. Migrate to Windows 2012 R2. 2. Upgrade to v8.0.x on the new platform. 3. Upgrade to v8.3.x on the new platform. 4. Upgrade to v8.5.x on the new platform.
v8.5.3: Windows 2008 R2	1. Migrate to Windows 2012 R2. 2. Upgrade to v8.0.x on the new platform. 3. Upgrade to v8.3.x on the new platform. 4. Upgrade to v8.5.x on the new platform.

To perform an operating system migration and upgrade, see Order of migration and upgrade steps (links to detailed instructions are at the bottom of the page).

For the versions covered in this document, you have the option to upgrade your deployment incrementally, rather than upgrading all machines and components at the same time. This allows you to upgrade individual Policy Server instances and their dependent components as separate "logical deployments." Policy Server instances that have not been upgraded and their dependent components continue to function normally at the original version. Please see the Incremental Upgrade guide for details.

When you are ready to begin, upgrade your deployment as follows:

Step 1: Prepare for upgrade

Warning

The upgrade process is designed for a properly functioning web protection deployment. Upgrading does not repair a non-functional system.

Before upgrading:

1. Make sure the installation machine meets the hardware and operating system recommendations in System requirements for this version.

   In addition, with v8.5.3, Master Database enhancements were made that greatly increased the size of the database files. When upgrading to v8.5.3, the new database files will replace the existing files. Prior to upgrading, confirm there is at least 6 GB of additional free space available on each Filtering Service machine.

2. Verify that third-party components, including your database engine and directory service, are supported with Forcepoint Web Security. See Requirements for web protection solutions.

3. Back up **all of your Web protection components** before starting the upgrade process. See the **Backup and Restore FAQ** for your version for instructions for backing up both software-based and appliance-based components.

   On appliances, be sure to perform a **full appliance configuration** backup.

4. Before upgrading Filtering Service, make sure that the Filtering Service machine and the management server have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.

5. Before upgrading any Policy Server, make sure that all instances of Multiplexer are enabled and started. This step is required even if you are not integrated with a third-party SIEM solution.

6. If your product includes the Web Security DLP Module, before upgrading the management server, make sure those components are ready for upgrade:

   a. Stop all discovery and fingerprinting tasks.

   b. Route all traffic away from the system.

   c. Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.

   d. Make sure all settings are deployed successfully. Log onto the Data Security manager. If the **Deploy** button is highlighted, click it.

   e. If your organization was supplied with custom file types, change the name of the following files in the **policies_store\custom_policies\config_files** folder on the management server; otherwise they will be overwritten during upgrade.

      - Change **extractor.config.xml** to **custom_extractor.config.xml**.
      - Change **extractorlinux.config.xml** to **custom_extractorlinux.config.xml**.

      The filenames are case-sensitive.

   f. If custom policies were provided, submit a request for updated versions before proceeding.

7. When upgrading to v8.5, a new logging partition is added to your Log Database. Please make sure you do not have 70 active partitions (the limit) prior to upgrading. Use the **Web > Settings > Reporting > Log Database** page of the Forcepoint Security Manager to disable at least one active partition prior to upgrading.

8. Back up your current Log Database and stop Log Server.

Warning

If database operations are active during upgrade, the Log Database may be rendered unusable.

When this occurs, it can be difficult to fix.

Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

a. Back up your reporting databases.

Refer to Microsoft documentation for instructions. The databases are named wslogdb70 (the catalog database), wslogdb70_*n* (standard logging partition databases), and wslogdb70_amt_1 (threats partition database).

b. On the Log Server machine, use the Windows Services tool to stop **Websense Log Server**.

9. It is best to **stop all Log Database jobs** prior to starting the upgrade, but, before it upgrades the Log Database, the upgrade process will attempt to stop any Log Database jobs not already stopped. If the jobs cannot be stopped, you will need to stop them manually. However, you do not need to exit the installer to do that.

Stop the Log Database jobs using these steps:

a. If you have a **full version of Microsoft SQL Server** (not Express), stop **all database jobs** as follows. (See below for steps to stop SQL Express jobs.)

- Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).
- To disable all currently active SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:

  Websense_ETL_Job_wslogdb70

  Websense_AMT_ETL_wslogdb70

  Websense_IBT_DRIVER_wslogdb70

  Websense_Trend_DRIVER_wslogdb70

  Websense_Maintenance_Job_wslogdb70

  Disabling the jobs prevents them from executing at the next scheduled time, but does not stop them if a job is in process.

  Make sure all jobs have completed any current operation before proceeding with upgrade.

- After upgrade, verify that the jobs have been to enabled.

  Enable any that were not automatically enabled by the upgrade process. Normal database operations will then resume.

- Continue with step 9.

b. If you have **SQL Server Express, stop all database jobs** as follows:

- Log in to the Microsoft SQL Server Management Studio.
- Expand the **Databases** tree to locate the catalog database (wslogdb70, by default), then expand the catalog database node.
- Expand **Service Broker > Queues**.
- Right click **dbo.wse_scheduled_job_queue** and select **Disable Queue**.
- The upgrade process will re-enable the job queue. After upgrade, verify that the Queue has been enabled.

  Enable it, if necessary, by repeating the process, this time ultimately selecting **Enable Queue** to resume normal database operations.

When Log Server is upgraded, the upgrade process first checks the Log Database version and updates the database, if necessary. If you have multiple Log Servers, the database update occurs with the first Log Server upgrade. The database

update, including the need to stop the database jobs, is not repeated when additional Log Server instances are upgraded.

10. If Log Server uses a Windows trusted connection to access the Log Database, be sure to log on to the Log Server machine using the trusted account to perform the upgrade. To find out which account is used by Log Server:
    a. Launch the Windows Services tool.
    b. Scroll down to find **Websense Log Server**, then check the **Log On As** column to find the account to use.
11. If your deployment includes appliances, see the this Upgrade Guide for additional information.

    If you have a software-only deployment, skip to *Step 3: Prepare to upgrade Content Gateway*, page 7.

Important

As a result of a change made to avoid a potential vulnerability when a presentation report is included as a link in an email, report links in emails that exist prior to upgrading from v8.1, or v8.2 to v8.5 will no longer work.

Step 2: Prepare appliances for upgrade (appliance-only)

Before applying the 8.5.x patch, perform the pre-upgrade instructions described in the V Series Upgrade Guide. or X Series Upgrade Guide.

Important

V Series appliance users:

Some older appliances are not supported with this version.

See V Series appliances supported with version 8.x.

Important

For recent information on the Forcepoint Security Appliance Manager, see Forcepoint Security Appliance Manager Release Notes.

Step 3: Prepare to upgrade Content Gateway

Before upgrading Content Gateway, be aware of the following:

- Most SSL configuration settings are saved and applied to the upgraded Content Gateway, except for dynamic certificates. Note that:
  - The Incident list is retained. Before upgrading, consider performing maintenance on the Incident list; remove unwanted entries.
  - SSLv2 is not enabled by default. If it is enabled prior to upgrade, the setting is retained.
- For user authentication, there is one credential cache for both explicit and transparent proxy mode, and one Global Authentication Options page for setting the caching method and Time-To-Live.

  During upgrade, the Cache TTL value is retained from the Transparent Proxy Authentication tab **unless** the value on the Global Authentication Options tab is not the default. In this case, the customized value is used.
- If you use Integrated Windows Authentication (IWA), be aware that IWA domain joins should be preserved through the upgrade process. However, in case the joins are dropped, make a record of the settings before starting the upgrade. Log on to the Content Gateway manager and record the IWA settings, including the names of domains to which IWA is joined. Keep this record where it is easily retrieved after the upgrade.
- If you have software instances of Content Gateway, make sure the host system meets the following hardware requirements before upgrading:

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum 8 GB recommended
Disk Space	2 disks: ● 100 GB for the operating system, Content Gateway, and temporary data. ● Max 147 GB for caching If caching will not be used, this disk is not required. The caching disk: ■ Should be at least 2 GB and no more than 147 GB ■ Must be a raw disk, not a mounted file system ■ Must be dedicated ■ Must *not* be part of a software RAID ■ Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64 MB of write-through cache
Network Interfaces	2

- In addition, to support **transparent proxy** deployments:

Router	Must support WCCP v2. A Cisco router must run IOS 12.2 or later. The latest version is recommended. To support IPv6, WCCP v2.01 and Cisco router version 15.4(1)T or later are required. Client machines, the destination Web server, and Content Gateway must reside on different subnets.
—or—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). 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).

Step 4: Restart services before starting the upgrade

1. To ensure the success of the upgrade, manually stop and start all the web protection services **except Log Server** before beginning the upgrade. (Log Server should remain stopped, as described in *Step 1: Prepare for upgrade*, page 4.)
   - *Windows*: Navigate to the **Web Security** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\, by default) and enter the following command:

     ```
     WebsenseAdmin restart
     ```

   - *Linux*: Navigate to the **Websense** directory (/opt/Websense/, by default) and enter the following command:

     ```
     ./WebsenseAdmin restart
     ```

   - *Appliance*: In the Appliance Manager or CLI, restart the appliance.
2. Make sure that all web protection services (except Log Server) are running successfully before you begin the upgrade. If any service is stopped, start the affected service or services.

During the upgrade, when web protection services are stopped, policy enforcement stops. Users have unrestricted access to the Internet until the services are restarted.

The Master Database is removed during the upgrade process. Filtering Service downloads a new Master Database after the upgrade is completed.

Step 5: Upgrade the Policy Broker machine

You must upgrade the machine that hosts **Policy Broker** first, regardless of which other components on are on the machine. Policy Broker may reside on:

- A **full policy source** appliance.
- A Windows Server machine.
- A RHEL machine.

See the Certified Product Matrix for a list of supported operating systems.

Any other components on the Policy Broker machine are upgraded along with Policy Broker.

If your configuration includes a primary Policy Broker and one or more replica Policy Brokers, you **must** upgrade the primary Policy Broker first.

Upgrade replica Policy Brokers after the primary has been upgraded and before attempting to upgrade any Policy Servers associated with the replicas. If Policy Server is installed on the Policy Broker machine, it is upgraded at the same time.

Jump to the section with the upgrade instructions for the platform that hosts Policy Broker:

- *Policy Broker: Appliance upgrade instructions*, page 10
- *Policy Broker: Windows upgrade instructions*, page 11
- *Policy Broker: Linux upgrade instructions*, page 12

Policy Broker: Appliance upgrade instructions

Follow the instructions in the **Upgrade procedure** section of the V Series Upgrade Guide or X Series Upgrade Guide.

When the appliance upgrade is complete, continue with *Step 6: Upgrade additional Policy Server machines*.

Do not upgrade any other appliances or off-appliance components until the full policy source appliance has successfully completed the upgrade process.

Note

Run “restart web” from the Forcepoint Appliance Manager or using the Appliance CLI after upgrading the full policy source appliance.

To finish the upgrade process for the Content Gateway module on the appliance, be sure to perform the steps in *Step 12: Post-upgrade activities*, page 29.

Policy Broker: Windows upgrade instructions

1. Make sure that no administrators are logged on to the management console.
2. Log on to the installation machine with an account having **local** administrator privileges.

   Important
   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   Warning
   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint85xSetup.exe**.
   - Installer files occupy approximately 5 GB of disk space.
5. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. A progress dialog box appears, as files are extracted.

   The file extraction process takes several minutes. Please be patient.
6. The installer detects software components from an earlier version and asks whether you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for web protection services to be stopped.

   In some cases, the installer may be unable to stop the services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. Next, the **Installing...** screen appears.

If Policy Broker resides on the management server, or on the same machine as Log Server, the upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.

11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Policy Broker: Linux upgrade instructions

1. Make sure no administrators are logged on to the management console.
2. Log on the installation machine with administrator privileges (typically, as **root**).
3. Close all applications and stop any antivirus software.
4. Check the **etc/hosts** file. If there is no host name for the machine, add one.
5. Create a setup directory for the installer files, such as **/root/Websense_setup**.
6. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Linux installer. The installer file is called **Web85xSetup_Lnx.tar.gz**.
7. Uncompress the installer file using:

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

8. Use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

   To launch the command-line installer, omit the -g switch:

   ```
   ./install.sh
   ```

9. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

10. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
11. On the Upgrade screen, select **Start the upgrade** and then click **Next**.
12. When you click **Next**, a “Stopping All Services” progress message appears. Wait for services to be stopped.

In some cases, the installer may be unable to stop the services. If this occurs, stop them manually using the **/opt/Websense/WebsenseDaemonControl** command. Once you have manually stopped the services, return to the installer.

13. On the Pre-Upgrade Summary screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized, then the **Installing...** screen appears.

14. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
15. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

16. If you stopped your antivirus software, restart it.

Step 6: Upgrade additional Policy Server machines

The central Policy Server resides on the same machine as the primary Policy Broker, and was automatically upgraded in the previous section.

If you have additional Policy Server instances, upgrade them next, regardless of what other services reside on the machines. Before upgrading any Policy Server, reboot the machine. If you are using a Forcepoint Appliance, do a full restart of the appliance.

Policy Server may reside on:

- **User directory and filtering** appliances.
- A Windows Server machine.
- A RHEL machine.

See the Certified Product Matrix for a list of supported operating systems.

Each Policy Server is required to have an on-box Multiplexer. To accomplish that, during upgrades from v8.1 or v8.2:

- If Policy Server and Multiplexer reside on the same machine, both are upgraded as usual.
- Instances of Multiplexer that do not have Policy Server on the same machine are automatically uninstalled.

  Note that any other components on the same machine are upgraded.
- Multiplexer is added to any Policy Server machine that did not previously include a Multiplexer instance.

  If Policy Server was associated with an off-box Multiplexer (on Windows), the off-box Multiplexer instance is removed and a local instance is installed.

If the off-box Multiplexer is on Linux and it not installed with other web protection components, you will need to run the upgrade on that Linux machine to make sure that Multiplexer instance is removed.

Jump to the section with the upgrade instructions for the platform that hosts Policy Server:

- *Policy Server: Appliance upgrade instructions*, page 14
- *Policy Server: Windows upgrade instructions*, page 14
- *Policy Server: Linux upgrade instructions*, page 15

Policy Server: Appliance upgrade instructions

Follow the instructions in the **Upgrade procedure** section of the V Series Upgrade Guide or X Series Upgrade Guide.

When the appliance upgrade is complete, continue with *Step 7: Upgrade additional Filtering Service, Network Agent, and User Service machines*.

To finish the upgrade process for the Content Gateway module on the appliance, be sure to perform the steps in *Step 12: Post-upgrade activities*, page 29.

Policy Server: Windows upgrade instructions

1. Make sure that no administrators are logged on to the management console.
2. Log on to the installation machine with an account having **local** administrator privileges.

   Important
   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   Warning
   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint85xSetup.exe**.
   - Installer files occupy approximately 5 GB of disk space.
   - Verify that the MD5 value of the downloaded file matches the value shown on the download page.

5. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. A progress dialog box appears, as files are extracted.

   The file extraction process takes several minutes. Please be patient.

6. The installer detects software components from an earlier version and asks how you want to proceed.

   Click **OK**.

7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

8. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for services to be stopped.

   In some cases, the installer may be unable to stop the services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.

10. On the **Pre-Upgrade Summary** screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing...** screen appears.

11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

Important

The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Policy Server: Linux upgrade instructions

1. Make sure no administrators are logged on to the management console.
2. Log on the installation machine with administrator privileges (typically, as **root**).
3. Close all applications and stop any antivirus software.
4. Check the **etc/hosts** file. If there is no host name for the machine, add one.
5. Create a setup directory for the installer files, such as **/root/Websense_setup**.
6. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Linux installer. The installer file is called **Web85xSetup_Lnx.tar.gz**.
7. Uncompress the installer file using:

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

8. Use one of the following commands to launch it:

To launch the graphical installer (available only on English versions of Linux):

```
./install.sh -g
```

To launch the command-line installer, omit the -g switch:

```
./install.sh
```

9. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

10. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
11. On the Upgrade screen, select **Start the upgrade** and then click **Next**.
12. When you click **Next**, a "Stopping All Services" progress message appears. Wait for services to be stopped.

    In some cases, the installer may be unable to stop the services. If this occurs, stop them manually using the **/opt/Websense/WebsenseDaemonControl** command. Once you have manually stopped the services, return to the installer.
13. On the Pre-Upgrade Summary screen, review the list of components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing...** screen appears.
14. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
15. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

16. If you stopped your antivirus software, restart it.

Step 7: Upgrade additional Filtering Service, Network Agent, and User Service machines

If you have additional Filtering Service, Network Agent, or User Service instances, upgrade them next, regardless of what other services reside on the machines. Filtering Service, Network Agent, and User Service may reside on:

- A Windows Server machine.

- A RHEL machine.

See the Certified Product Matrix for a list of supported operating systems.

Filtering Service and Network Agent may also reside on **filtering only** appliances.

When Filtering Service or the management server is upgraded from v8.1, v8.2, or v8.3, the Cloud App Agent component is added to the machine.

Filtering Service and Network Agent: Appliance upgrade instructions

Follow the instructions in the **Upgrade procedure** section of the V Series Upgrade Guide or X Series Upgrade Guide.

When the appliance upgrade is complete, continue with *Step 8: Upgrade Log Server*.

To finish the upgrade process for the Content Gateway module on the appliance, be sure to perform the steps in *Step 12: Post-upgrade activities*, page 29.

Filtering Service, Network Agent, or User Service: Windows upgrade instructions

1. Make sure that no administrators are logged on to the management console.
2. Log on to the installation machine with an account having **local** administrator privileges.

   Important
   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   Warning
   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint85xSetup.exe**.
   - Installer files occupy approximately 5 GB of disk space.
5. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. A progress dialog box appears, as files are extracted.

   The file extraction process takes several minutes. Please be patient.

6. The installer detects software components from an earlier version and asks how you want to proceed.

   Click **OK**.

7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

8. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for services to be stopped.

   In some cases, the installer may be unable to stop the services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.

10. On the **Pre-Upgrade Summary** screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing** screen appears.

11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Filtering Service, Network Agent, or User Service: Linux upgrade instructions

1. Make sure no administrators are logged on to the management console.
2. Log on the installation machine with administrator privileges (typically, as **root**).
3. Close all applications and stop any antivirus software.
4. Check the **etc/hosts** file. If there is no host name for the machine, add one.
5. Create a setup directory for the installer files, such as **/root/Websense_setup**.
6. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Linux installer. The installer file is called **Web85xSetup_Lnx.tar.gz**.
7. Uncompress the installer file using:

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

8. Use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

To launch the command-line installer, omit the -g switch:

```
./install.sh
```

9. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

10. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
11. On the Upgrade screen, select **Start the upgrade** and then click **Next**.
12. When you click **Next**, a "Stopping All Services" progress message appears. Wait for services to be stopped.

    In some cases, the installer may be unable to stop the services. If this occurs, stop them manually using the **/opt/Websense/WebsenseDaemonControl** command. Once you have manually stopped the services, return to the installer.
13. On the Pre-Upgrade Summary screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing** screen appears.
14. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
15. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

16. If you stopped your antivirus software, restart it.

Step 8: Upgrade Log Server

Next, upgrade the Log Server machine. Any other services on the machine are also upgraded.

Log Server runs on Windows Server machines. See the Certified Product Matrix for a list of supported operating systems.

To upgrade Log Server:

1. Make sure that no administrators are logged on to the management console.

2. Log on to the installation machine with an account having **local** administrator privileges.

   Important
   If Log Server uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

   Warning
   Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint85xSetup.exe**.
   - Installer files occupy approximately 5 GB of disk space.
5. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. A progress dialog box appears, as files are extracted.

   The file extraction process takes several minutes. Please be patient.
6. The installer detects software components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for services to be stopped.

   In some cases, the installer may be unable to stop the services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized, then the **Installing** screen appears.

    The upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.

12. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

13. If management server was upgraded in the course of upgrading another component, restart the **Websense TRITON - Web Security** service on the management server.
14. If you stopped your antivirus software, restart it.
15. Enable the database jobs that you disabled prior to upgrade.

Step 9: Upgrade the management server

If you have not already upgraded the management server in the course of upgrading another component, use the following steps to upgrade the management server machine.

When Filtering Service or the management server is upgraded from v8.1, v8.2, or v8.3, the Cloud App Agent component is added to the machine.

1. Make sure that no administrators are logged on to the management console.
2. Log on to the installation machine with an account having **ocal** administrator privileges.
3. Close all applications and stop any antivirus software.

> **Warning**
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint85xSetup.exe**.
   - Installer files occupy approximately 5 GB of disk space.
5. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. A progress dialog box appears, as files are extracted.

   The file extraction process takes several minutes. Please be patient.
6. The installer detects software components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

8. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for services to be stopped.

   In some cases, the installer may be unable to stop the services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing** screen appears.

    The upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Step 10: Upgrade software instances of Content Gateway

Content Gateway runs on web protection full policy source, user directory and filtering, and filtering only appliances (all of which should already have been upgraded at this point).

Content Gateway is supported on:RHELmachines. See the Certified Product Matrix for a list of supported operating systems.

> **Note**
> If you have multiple Content Gateway instances deployed in a cluster, you **do not** have to disable clustering or VIP (if used). As each member of the cluster is upgraded, it will rejoin the cluster.

Important

At the beginning of the upgrade procedure, the installer checks to see if the partition that hosts **/opt** has enough space to hold a copy of the existing Content Gateway log files (copied to **/opt/WCG_tmp/logs**). If there's not enough space, the installer prints an error message and quits.

In this situation, if you want to retain the log files you must copy the contents of **/opt/WCG/logs** to a location that has enough space, and then delete the log files in **/opt/WCG/logs**.

When the upgrade is complete, move the files from the temporary location back to **/opt/WCG/logs** and delete the files in the temporary location.

1. If your existing web protection solution is deployed with Web DLP or a data protection product:
   a. Log on to the Content Gateway manager.
   b. Navigate to the **Configure > My Proxy > Basic** page.
   c. Disable **Web DLP**.

   When the upgrade is complete:
   d. Return to the **Configure > My Proxy > Basic** page.
   e. Enable the new **Web DLP** option.
   f. Restart Content Gateway.
   g. Navigate to the **Configure > Security > Web DLP** page and confirm that automatic registration was successful. If it was not, confirm that the Data module of management console is running as expected.
2. Log on to the Content Gateway Linux host and acquire root permissions:

   ```
   su root
   ```
3. Disable any currently running firewall on this machine for the duration of the upgrade. Bring the firewall back up after the upgrade is complete, opening ports used by Content Gateway.

   For example, if you are running IPTables:
   a. At a command prompt, enter **service iptables status** to determine if the firewall is running.
   b. If the firewall is running, enter **service iptables stop**.

c. After upgrade, restart the firewall. In the firewall, be sure to open the ports used by Content Gateway on this machine. See default ports for more information.

Important

Forcepoint Web Security customers using Red Hat Enterprise Linux or CentOS 7.x must disable firewalld prior to installing Content Gateway.

On the machine where Content Gateway will be installed, execute the following:

```
systemctl stop firewalld
systemctl disable firewalld
```

4. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Content Gateway version 8.5.x installer, and save it to a temporary directory. For example, place it in:

   ```
   /tmp/cg_v85
   ```

5. Unpack the Content Gateway installer tar archive:

   ```
   cd /tmp/cg_v85
   tar -xvzf <installer tar archive>
   ```

Important

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

6. If you intend to upgrade Red Hat Enterprise Linux 6.x to a more recent version, perform the upgrade now. See your Red Hat Enterprise Linux documentation.
7. In the directory where you unpacked the tar archive (for example, /tmp/cg_85), start the installation/upgrade script.

   ```
   ./wcg_install.sh
   ```

   Respond to the prompts.

   Content Gateway is installed and runs as **root**.

Note

Up to the point that you are prompted to confirm your intent to upgrade, you can quit the installer by pressing CTRL+C. If you change your mind after you choose to continue, do **not** use CTRL+C to stop the process. Instead, allow the installation to complete and then uninstall.

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

   ```
   Error: Content Gateway v8.5.x on x86_64 requires several
   packages that are not present on your system.

   Please install the following packages: <list of packages>

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

   yum install <list of packages>

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

   To make it easier to install the needed packages, the Content Gateway distribution includes a Linux "rpm" containing the needed packages. To install its contents, ensure that the operating system has access to the Red Hat Linux distribution library (for example the DVD), and enter:

   ```
   yum install wcg_deps-1-0.noarch.rpm
   ```

   Upon successful completion, a list of updated packages displays and then the word "Complete!".

   Here is an example of a system resource warning:

   ```
   Warning: Content Gateway requires at least 6 gigabytes of
   RAM.

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

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

   Enter **y** to continue the upgrade. You should not install or upgrade on a system that does not meet the minimum requirements. If you choose to run Content Gateway after receiving a system resource warning, performance and stability may be affected.

9. Read the subscription agreement. At the prompt, enter **y** to accept the agreement and continue the upgrade, or **n** to cancel.

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

10. The installer checks for the presence of an existing Content Gateway installation. When asked, choose to replace the existing version with version 8.5.x.

    ```
    WCG version 8.1.n-nnnn was found.

    Do you want to replace it with version 8.5.x-nnnn [y/n]? y
    ```

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

    ```
    Stopping Content Gateway processes...done

    Copying settings from /opt/WCG to /root/WCG/OldVersions/
    8.1.0-1418-PreUpgrade/...done

    Zipping configuration archive...done

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

12. You can either re-use the installation selections you entered during the last install, or provide new answers to all installation prompts, such as admin password, admin email address, Policy Server IP address, etc.:

    ```
    Previous installation selections </root/WCG/Current/
    WCGinstall.cfg> found.

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

    Enter **y** to use previous installation selections.

    Enter **n** to revert to default values, and receive all installation questions and answer them again.

13. If you answered **y** at Step 12, then you can also leave proxy settings at their current values or revert to default values (which perform a fresh install!).

    ```
    Restore settings after install [y/n]?
    ```

    Enter **y** to keep the proxy settings as they are.

    Enter **n** to restore default settings for the proxy.

    Caution: If you answer **n** (no), the current installation of Content Gateway is removed, and a fresh install of 8.5.x begins. See Installation Instructions: Forcepoint Web Security for a detailed description of the installation procedure. This is not an upgrade, but rather a fresh install.

14. The previously installed version of Content Gateway is removed, and the settings and selections you chose to retain are re-used. Details of the upgrade process are output to the screen. Please wait.

    ```
    *COMPLETED* Content Gateway 8.5.x-nnnn installation.

    A log file of this installation process has been written to
    /root/WCG/Current/WCGinstall.log

    For full operating information, see the Content Gateway Help
    system.

    Follow these steps to start the Content Gateway management
    interface (Content Gateway Manager):

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

    1. Start a browser.

    2. Enter the IP address of the 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.
    ```

15. The automated portion of the upgrade is now complete, and the proxy software is running.

    If you chose to revert to default proxy settings, be sure to configure any custom options.

16. Check Content Gateway status with:

    ```
    /opt/WCG/WCGAdmin status
    ```

    All services should be running. These include:

    - Content Cop

- Content Gateway
- Content Gateway Manager
- Analytics Server

Important

If Content Gateway fails to complete startup after upgrade, check for the presence of the **no_cop** file. Look for:

```
/opt/WCG/config/internal/no_cop
```

If the file exists, remove it and start Content Gateway:

```
/opt/WCG/WCGAdmin start
```

To finish the upgrade, be sure to perform the post-upgrade instructions at the end of this document.

Step 11: Upgrade any additional components

Upgrade any additional server components, including Sync Service, Directory Agent, transparent identification agents and Remote Filtering Server, that may be running on other machines.

See:

- *Additional components: Windows upgrade instructions*, page 27
- *Additional components: Linux upgrade instructions*, page 28

Additional components: Windows upgrade instructions

1. Log on to the installation machine with an account having **local** administrator privileges.
2. Close all applications and stop any antivirus software.

Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

3. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint85xSetup.exe**.
   - Installer files occupy approximately 5 GB of disk space.
4. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. A progress dialog box appears, as files are extracted.

   The file extraction process takes several minutes. Please be patient.

5. The installer detects software components from an earlier version and asks how you want to proceed.

   Click **OK**.

6. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.

7. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
8. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for services to be stopped.

   In some cases, the installer may be unable to stop the services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.

9. On the **Pre-Upgrade Summary** screen, review the list of web protection components that will be upgraded, and then click **Next**.

   Critical files are backed up and install properties initialized. And then the **Installing** screen appears.

10. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
11. Reboot the machine.

Important

The machine must be rebooted to complete the upgrade process.

12. If you stopped your antivirus software, restart it.

Additional components: Linux upgrade instructions

1. Log on the installation machine with administrator privileges (typically, as **root**).
2. Close all applications and stop any antivirus software.
3. Check the **etc/hosts** file. If there is no host name for the machine, add one.
4. Create a setup directory for the installer files, such as **/root/Websense_setup**.
5. Use the Downloads tab of the My Account page at support.forcepoint.com to download the Linux installer. The installer file is called **Web85xSetup_Lnx.tar.gz**.
6. Uncompress the installer file using:

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

7. Use one of the following commands to launch it:

   To launch the graphical installer (available only on English versions of Linux):

   ```
   ./install.sh -g
   ```

   To launch the command-line installer, omit the -g switch:

   ```
   ./install.sh
   ```

8. On the Introduction screen, click **Next**.

> **Note**
> These instructions refer to the graphical installer screens. If you are using the command-line installer, the same prompts appear. Enter the menu-item number or character, corresponding to the button described in each step.

9. On the Subscription Agreement screen, click **I accept the terms of the Subscription Agreement** and click **Next**.
10. On the Upgrade screen, select **Start the upgrade** and then click **Next**.
11. When you click **Next**, a "Stopping All Services" progress message appears. Wait for services to be stopped.

    In some cases, the installer may be unable to stop the services. If this occurs, stop them manually using the **/opt/Websense/WebsenseDaemonControl** command. Once you have manually stopped the services, return to the installer.
12. On the Pre-Upgrade Summary screen, review the list of web protection components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing** screen appears.
13. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
14. Reboot the machine.

> **Important**
> The machine must be rebooted to complete the upgrade process.

15. If you stopped your antivirus software, restart it.

Step 12: Post-upgrade activities

After you have finished upgrading components, refer to the following to ensure that your Web Security upgrade is complete.

Web protection components

1. If the upgrade process involved upgrading multiple Policy Servers that are assigned to the same Policy Broker, and any of them reside on a Microsoft Windows 2016 server, some of the services on all of the Policy Server machines in the deployment that use Windows 2016 may fail to restart at the end of the upgrade process.

Log on to each Policy Server machine and restart the following services as needed:

- Websense Event Message Broker
- Websense Cloud App Service
- Websense Bridge Service
- Websense SIEM Connector

Optionally, reboot each Policy Server machine.

2. In v8.5, DC Agent was modified to remove the use of SMBv1 for domain discovery.

   During the upgrade, the new DC Agent settings replaced the current configuration. Customers preferring to use SMBv1 can reset the appropriate settings in transid.ini. See Using DC Agent for Transparent User Identification for information.

   In conjunction with this change, the default selection for **Domain Discovery**, when the feature is enabled on the **Settings > General > User Identification > DC Agent** page of Forcepoint Manager, is **DC Agent**. (APWEB-12178)

   In v8.5.3, the **Domain Discovery** section of the **Settings > General > User Identification > DC Agent** page was changed to remove the component selections for domain discovery. After upgrade, domain discovery will always be done by DC Agent.

3. In v8.5, Microsoft SQL Server 2016 Express SP1 replaces Microsoft SQL Server 2008 R2 Express SP2 in v8.5 for new installations. However, SQL Server 2008 R2 Express SP2 will continue to function on upgraded deployments.

   In v8.5.3, Microsoft SQL Server 2017 Express replaces 2016 Express SP1.

4. Version 8.5 introduces Report Center, a new reporting tool. In organizations that use the delegated administration reporting features, access to Report Center and its tools is defined for each administrator role. The upgrade process assigns the following permissions, based on existing permissions assigned to a given role:

Existing reporting permission	New Report Center permission
Access presentation reports	Access Report Center and Schedule Reports
Access investigative reports with View user names in investigative reports	Access Report Center
Report on all clients with Access investigative reports, View user names in investigative reports, and Schedule investigative reports	Access Report Center and Schedule Reports

Report Center permissions are not automatically assigned for any other combination of existing reporting permissions. See Administrator Help for more information on Report Center and Delegated Administration.

Version 8.5.3 adds to this list with the addition of **View user names and hostnames in reports**, which has been added under **Access the Report Center**. This option allows administrators to view user information when creating or viewing reports. For upgrades to 8.5.3:

- The option will be on for upgrades from v8.5.

  The Schedule Reports option will continue to be enabled if it was enabled in the v8.5 settings.

- When upgrading from any other version, the value of the option is determined by the current setting for **View user names in investigative reports**. or **Access presentation reports.** The new option will be enabled for all delegated administrators who previously had permission to view user names in investigative reports or to access presentation reports.

In addition, some of the existing options were renamed:

- The **Access the Threats dashboard** option has been moved and renamed to **Access Threat data (Threats dashboard + Report Center)**.
- Similarly, **Access forensics data in the Threats dashboard** has been renamed to **Access forensics data**.

Use the new options to allow administrators to view the data in two new tabs for the Detail view of the Transaction Viewer as well as to view the same data in the Threats dashboard.

5. With v8.5, Active Directory (Mixed Mode) is not supported. When upgrading to v8.5, deployments configured to use Active Directory Mixed Mode will be modified to use Active Directory (Native Mode).

   Re-add client information and re-assign clients to existing policies after the upgrade completes.

6. If an upgrade to v8.5.3 involves upgrading services on a Linux server, some of the services on the Linux server may fail to restart. If that happens:

   a. Navigate to /opt/Websense/bin on the Linux server.

   b. Delete all .p12 tiles.

   c. Start all services.

      ```
      WebsenseAdmin start
      ```

Content Gateway

1. If, at the start of the upgrade process, you manually moved your existing log files to a temporary location, move them back to **/opt/WCG/logs** and delete the files in the temporary location.
2. Register Content Gateway nodes in Forcepoint Security Manager on the **Web > Settings > Content Gateway Access** page.

   Registered nodes add a link to the Content Gateway manager logon portal and provide a visual system health indicator: a green check mark or a red X.

3. Configure Content Gateway system alerts on the **Settings > Alerts > System** page in the Security Manager.

   This subset of Content Gateway system alerts can be configured to be sent to administrators, in addition to being displayed in the Content Gateway manager.

4. If you use SSL support:

   a. If your clients don't yet use a SHA-256 internal Root CA, create and import a SHA-256 Root CA into all affected clients. See Internal Root CA in Content Gateway Help.

   b. Using the notes you compiled prior to upgrade, rebuild your Static Incident list.

5. If you use proxy user authentication, review the settings on the **Global Authentication Options** page (**Configure > Security > Access Control > Global Configuration Options**).

6. If you use IWA user authentication, confirm that the AD domain is still joined. Go to **Monitor > Security > Integrated Windows Authentication**. If it is not joined, rejoin the domain. Go to **Configure > Security > Access Control > Integrated Windows Authentication**.

7. If you use Rule-Based Authentication, review your configuration. Go to **Configure > Security > Access Control**.

   a. Check the **Domains** page.

      - IWA domains that were joined before upgrade should still be joined.
      - LDAP and Legacy NTLM domains should be listed.

   b. Check each rule.

      - Go to the **Authentication Rules** page and enter the editor.
      - Select each rule and check the configuration.
      - For Multiple Realm Authentication rules that used Cookie Mode Caching, check the cookie list on the Global Authentication Option page.
      - Check that the expected domain is in the **Auth Sequence** list.

   Important: The Rule-Based Authentication feature is very rich and can satisfy many user authentication requirements. To make best use of it, please refer to Rule-Based Authentication.

8. If a web protection and data protection solution were deployed together, confirm that Content Gateway has automatically re-registered with the Data module of the Forcepoint Security Manager. If it has not, manually re-register.

   a. Ensure that the Content Gateway and the Security Manager server system clocks are synchronized to within a few minutes.

   b. In the Content Gateway manager:

      - Go to **Configure > My Proxy > Basic**, ensure that **Web DLP: Integrated on-box** is enabled, and click **Apply**.
      - Next to **Integrated on-box**, click the **Not registered** link. This opens the **Configure > Security > Web DLP registration** screen.
      - Enter the IP address of the Security Manager server.

- Enter a user name and password for logging onto Security Manager. The user must be a Forcepoint DLP administrator with Deploy Settings privileges.
- Click **Register**. If registration is successful, a message confirms the result and prompts you to restart Content Gateway. If registration fails, an error message indicates the cause of failure. Correct the problem and perform the registration process again.

9. If web and data protection products were deployed together and upgraded, you may need to remove stale entries of Content Gateway instances registered in Forcepoint DLP system modules:
   a. Log onto Security Manager.
   b. Select the **Data** tab and navigate to the **Settings > Deployment > Modules** page.
   c. Listed are 2 instances of each Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.
   d. Click **Deploy**.
10. If web and data protection products were deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance may need to be deleted from the list of Forcepoint DLP system modules or the deployment will fail. Go to the **Data > Settings > Deployment > System Modules** page, click on the affected Content Gateway instance to open its **Details** page, click **Delete** and then **Deploy**.
11. If your explicit proxy deployment was customized to support an external load balancer with IWA user authentication, the configuration is preserved during upgrade. You do not need to re-apply the custom configuration. You should, however, test your deployment to verify that the load balancer is performing as expected.
12. With v8.2.x, the basic functionality for 2 features was changed slightly:
    - **Send authentication to parent proxy**, configured on the **Configure > My > Proxy > Basic > General** page
    - **X-Forwarded-For**, enabled on the **Configure > Perotocols > HTTP > Privacy**

    In both cases, header values are forwarded only to a configured parent proxy.

    If you are upgrading from v8.1 to v8.5, enabled either of these settings in your previous version, and are expecting header values to be forwarded for all outbound requests, add the appropriate variable to your records.config file (in the **/opt/WCG/config** directory, by default).

    - To add the user name to outbound requests, add:

      ```
      CONFIG proxy.config.http.insert_xua_to_external INT
      ```

    - To send X-Forwarded-For header values directly to the Internet, add:

      ```
      CONFIG proxy.config.http.insert_xff_to_external INT 1
      ```
13. If you were using v8.1 with custom cipherlist settings using these variables in records.config:

```
proxy.config.ssl.server.cipherlist
proxy.config.ssl.client.cipherlist
```

you need to reconfigure the custom settings because these variables were replaced in v8.2.

- proxy.config.ssl.server.cipherlist_suffix replaces proxy.config.ssl.server.cipherlist
- proxy.config.ssl.client.cipherlist_suffix replaces proxy.config.ssl.client.cipherlist

The non-default cipherlist being used prior to the upgrade are saved as a comment in records.config, where it can be used for reference. Default values for the new variables are put into place during the upgrade and can be reconfigured after the upgrade is complete.

See Content Gateway Manager Help for more information on how these new variables now work with proxy.config.ssl.server.cipherlist_option and proxy.config.ssl.client.cipherlist_option to create cipher lists.

14. The **Tunnel Skype** option on the **Configure > Protocols > HTTPS** page of Content Gateway Manager was removed in v8.3. Variables stored in the records.config file that apply to Skype are removed during upgrades from v8.1 or v8.2.
15. The settings on the **Configure > Networking > Connection Management > Low Memory Mode** page of Content Gateway manager was removed in v8.3. Corresponding variables stored in the records.config file are removed by upgrades from v8.1or v8.2.
16. If **LOW** encryption cipher suites was previously selected on the **Configure > SSL > Decryption/Encryption > Inbound** or **Outbound** pages of Content Gateway manager, upgrades from v8.1 or v8.2 will change the setting to **MEDIUM**. LOW is no longer a valid option on those pages.

    The corresponding records.config variables are also updated by the upgrade.
17. During upgrades from v8.1 or v8.2, the **Enable the certificate verification engine** on the **Configure > SSL > Validation > General** page of Content Gateway manager will be changed to ON for any customer who does not already have the feature enabled.
18. In v8.3 and continued in v8.4 and v8.5, improvements were made to the Adaptive Redirection Module (ARM). The ARM component now utilizes iptables, policy routing, and transparent sockets which are configured during product installation or upgrade.

    The Content Gateway Manager was changed to reflect these improvements.

    - The **Network Address Translation (NAT)** section of the **Configure > Networking > ARM > General** page has been renamed to **Redirection Rules** to better reflect the contents of the table.
    - Text on that page has also been updated.

    To facilitate interception and redirection of traffic:

    - IPTables rules are configured during upgrade.
        - Forcepoint IPTables chains are inserted.

- Forcepoint IPTables rules are also inserted into existing chains.
- Forcepoint chains and rules use “NC_” as a prefix for identification purposes.

- IPTables rules configured outside of Content Gateway Manager must
  - Be inserted *after* Forecepoint rules.
  - Never be added to Forcepoint chains.
- Forcepoint chains and rules should never be edited.
- If customized chains or rules impact the Forcepoint configuration, navigate to /opt/wcg/bin and execute the following to re-establish the Forcepoint IPTables chains and rules:

  ```
  netcontrol.sh -r
  ```

For some customers, the GRE **Packet Return Method** (GRE return) may not be as expected. In all cases, GRE return, as documented by Cisco (see this site), is fully functional. However, tunneling back through a router (enhanced GRE tunnel return) now requires a specific kernel module. Contact Forcepoint Technical Support to enable this functionality.

To provide more appropriate statistical data for the new ARM, the **Bypass Statistics** now provide information for:

- Total Packets Bypassed
- Packets Dynamically Bypassed
- DNS Packets Bypassed
- Packets Shed

19. A change was made in v8.4 to resolve customer issues with SSL retry logic. The default values for the following records.config variables are reset to 1 during an upgrade from v8.1, v8.2, or v8.3.

    ```
    proxy.config.http.connect_attempts_max_retries
    ```

    ```
    proxy.config.http.connect_attempts_max_retries_dead_server
    ```

20. Automatic updates to the Certificate Authority tree were added to v8.4.

    After upgrading from v8.1, v8.2, or v8.3, when the initial CA tree update occurs, CAs in the customer deployment but not in the 8.5 CA db, any CA that is no longer a root CA, and CAs that are no longer trusted are converted to a private CA. This process also removes expired CAs.

    After the initial update, review the CA tree on the **Configure > SSL > Certificates** page of Content Gateway manager and remove any certificates that are no longer trusted or may be revoked.

21. With v8.5, default IPTables include a rule that will drop traffic that is neither HTTP, HTTPS, nor FTP and not forward it through the proxy.

    On upgrade, this feature is disabled by default. To add the rule and not forward traffic that is neither HTTP, HTPTS, nor FTP, add the following to records.config ((located in /opt/WCG/config, by default):

    ```
    CONFIG proxy.config.arm.forward_unwanted_traffic INT 0
    ```

    After this entry is added and Content Gateway is restarted, an IPTables rule is added and traffic that is neither HTTP, HTTPS, nor FTP will not be forwarded.

22. For customers who have purchased the v8.5.x Protected Cloud Apps feature, the setting for **Parent Proxy** on the **Configure > Content Routing > Hierarchies** page of Content Gateway Manager will be enabled. If you previously enabled and configured **Parent Proxy** and later disabled the option, the configured settings will be used and should be updated as necessary.
23. With v8.5.x, the option of **TLSv1** on the **Configure > SSL > Decryption/ Encryption** page (Inbound and Outbound tabs) and on the **Configure > Security > FIPS** page of Content Gateway Manager is no longer a default selection. Options for **TLSv1.1** and **TLSv1.2** are added and enabled by default.

    During upgrade, if **HTTPS** (SSL) was enabled on the **Configure > My Proxy > Basic > General** page of Content Gateway Manager prior to upgrade, the SSL settings are not changed.

    IF **HTTPS** (SSL) is enabled after the upgrade, the settings will be handled like a fresh installation of the product and TLSv1.1 and TSLv1.2 will be enabled by default. TLSv1 will not be enabled.
24. Beginning with v8.5.3, Content Gateway will no longer accept nor download SHA-1 intermediate certificates. SHA-1 certificates that were added by Content Gateway will be removed during an upgrade to v8.5.3. Note that SHA-1 certificates that were manually added will not be deleted.

    A new variable has been added in v8.5.3 that will disable the automatic adding of new certificates to the certificate database. Upgrades to v8.5.3 will add this new parameter to records.config, set to use the default functionality.

    To disable the default functionality edit the following in records.config (located in /opt/WCG/config, by default)

    ```
    CONFIG proxy.config.ssl.cert.verify.add_cert_to_database
    INT 0
    ```

    Reset the value to 1 to restore the default functionality.
25. Version 8.5.3 adds the ability to manually add a dynamic certificate key. Each key requires a passphrase. Both the key and passphrase are stored in the certificates database and a