Upgrade Instructions: Forcepoint URL Filtering

Upgrade Instructions | Forcepoint URL Filtering | v8.5.x | 8-June-2020

Version 8.4 introduced new product names and solution bundles for web protection solutions. Web Filter & Security (v8.0 and later), Web Filter, and Web Security are now Forcepoint URL Filtering.

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**
- v8.2, v8.3, v8.4 and v8.5 to **v8.5.3**
- v8.4, v8.5 and v8.5.3 to **8.5.4.**

Direct upgrades from v7.8.x or v8.0.x to v8.5, from 7.8.x, 8.0.x or 8.1.x to v8.5.3, or from 7.8.x, 8.0.x, 8.1.x, 8.2.x or 8.3.x to v8.5.4 are not supported.

If you have an earlier version, there are interim steps you must take.

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	

Your current version	Step 1	Step 2	Step 3	Step 4	Step 5
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 8.4.x	Upgrade to 8.5.x	none	
v8.1.x	Upgrade to 8.4	Upgrade to 8.5.x	none	none	
v8.2.x	Upgrade to 8.4	Upgrade to 8.5.4	none	none	
v8.3.x	Upgrade to 8.4	Upgrade to 8.5.4	none	none	
v8.4.x	Upgrade to 8.5.x				
v8.5.x	Upgrade to v8.5.x				

These instructions also describe how to upgrade appliance-based components.

If you are currently running an appliance with v7.7.x, Appliance Hotfix 90 must be applied to v7.7.x prior to upgrading to v7.8.x. See the v7.8.x Upgrade Instructions.

Important

V Series appliance users:

Some older V10000 and V5000 appliances are not supported with this version.

See V Series appliances supported with version 8.x.

Important

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

The following operating systems are not supported/ 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 v8.5.4: Red Hat Enterprise Linux 6.1 - 6.9	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 or v8.5.3 on the new platform. 6. Migrate to Red Hat Enterpise Linux 7.5. 7. Upgrade to v8.5.4 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. v8.5.4: Red Hat Enterprise Linux 7.0 - 7.4.	1. Migrate to Red Hat Enterprise Linux 7.3. 2. Upgrade to v8.4.x on the new platform. 3. Upgrade to v8.5 or v8.5.3 on the new platform. 4. Migrate to Red Hat Enterprise Linux 7.5. 5. Upgrade to v8.5.4.
v8.5: 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 on the new platform.
v8.5.3: Windows 2008 (32-bit) 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 v8.5.3 on the new platform.
v8.5.4: Windows 2008 (32-bit) Windows 2008 R2 Windows 2012 R2 Datacenter Edition	1. Migrate to Windows 2012 R2 Standard Edition. 2. Upgrade to v8.0.x on the new platform. 3. Upgrade to v8.3.x on the new platform. 4. Upgrade to v8.4.x on the new platform. 5. Upgrade to 8.5.4 on the new platform.

To perform a migration and incremental upgrade, see:

- Migration instructions for upgrading to v7.7.x (Find links to detailed instructions at the bottom of the page, under the table.)
- Instructions for upgrading to v7.7.x
- Migration instructions for upgrading to v8.0.x (Find links to detailed instructions at the bottom of the page, under the table.)

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.

Important

SIEM Integration feature enhancements made in v8.5.4 may result in the loss of SIEM data during an incremental upgrade to that version. There is no loss of reporting data.

See the Incremental Upgrade Guide for more information.

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 or v8.5.4 from v8.5 or earlier, 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. If your web protection software is integrated with a third-party firewall, proxy server, or caching application, make sure that your integration product is supported in this version.

   In v8.5.x, the supported third-party integration products are:

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

   In addition, Blue Coat appliances can be integrated via the ICAP Service.

3. Verify that third-party components that work with your web protection software, including your database engine and directory service, are supported. See Requirements for web protection solutions.

4. 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.

5. 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.

6. 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.

7. When upgrading from v8.4 or earlier, 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 left in an inconsistent state, rendering it unusable.

   When this occurs, it can be difficult to fix.

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

   a. Back up your reporting databases.

      Refer to Microsoft documentation for instructions on backing up databases. 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, continue with the next section (*Step 2: Prepare appliances for upgrade (appliance-only)*, page 8.

    If you have a software-only deployment, skip to *Step 3: Restart services before starting the upgrade*, page 8.

> **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.

Potential issue when upgrading to v8.5.4

A security update done for the v8.5.4 product release has resulted in a new requirement for a specific dynamic-link library (dll) when upgrading to v8.5.4 Forcepoint URL Filtering software on a Windows platform.

If you have not recently downloaded the Visual C++ Redistributable Package from Microsoft, it is likely that the upgrade will prompt with the error “Installation failed with error code 3004”. The log file generated by the upgrade process, available in the Temp folder of the user running the installer, will contain a line similar to:

```
java.lang.UnsatisfiedLinkError:
C:\Users\Administrator\AppData\Local\Temp\2\I1588276985\Windows\resource
\jre\bin\freetype.dll: Can't find dependent libraries
```

The dependency referenced in this log entry is for **vcruntime140.dll**, a file that is part of the Redistributable Package.

Should the error occur during the upgrade process:

1. Close the error window but do NOT stop the upgrade process. Leave the installer window open.
2. Locate the latest 64-bit Redistributable Package for your Windows version from this site.
3. Download and install the package.
4. Return to the installation window and continue the process.

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

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

Important

Some older V10000 and V5000 appliances are not supported with this version.

See V Series appliances supported with version 8.x

Important

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

Step 3: 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*: On the **Status > General** page in the Appliance manager, click **Restart Appliance** to restart all services.

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 4: 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 them. If Policy Server is installed on the same machine, it will be 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 9
- *Policy Broker: Windows upgrade instructions*, page 10
- *Policy Broker: Linux upgrade instructions*, page 11

Policy Broker: Appliance upgrade instructions

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

When the appliance upgrade is complete, continue with *Step 5: 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.

Policy Broker: Windows upgrade instructions

Important
If, during the upgrade process, you encounter the error "Installation failed with error code 3004", refer to *Potential issue when upgrading to v8.5.4* for 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 web protection 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.

    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 web protection services to be stopped.

    In some cases, the installer may be unable to stop the web protection 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 5: Upgrade additional Policy Server machines

The central Policy Server resides on the same machine as 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 to v8.5 or v8.5.3:

- 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 13
- *Policy Server: Windows upgrade instructions*, page 13
- *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.

When the appliance upgrade is complete, continue with *Step 6: Upgrade additional Filtering Service, Network Agent, and User Service machines*.

Policy Server: Windows upgrade instructions

Important

If, during the upgrade process, you encounter the error "Installation failed with error code 3004", refer to *Potential issue when upgrading to v8.5.4* for 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 web protection services to be stopped.

   In some cases, the installer may be unable to stop the web protection 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 web protection services to be stopped.

    In some cases, the installer may be unable to stop the web protection 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 6: 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 to v8.5, 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.

When the appliance upgrade is complete, continue with *Step 7: Upgrade Log Server*.

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

> **Important**
> If, during the upgrade process, you encounter the error "Installation failed with error code 3004", refer to *Potential issue when upgrading to v8.5.4* for 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 web protection services to be stopped.

   In some cases, the installer may be unable to stop the web protection 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 web protection services to be stopped.

    In some cases, the installer may be unable to stop the web protection 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 7: 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.

> **Important**
> If, during the upgrade process, you encounter the error "Installation failed with error code 3004", refer to *Potential issue when upgrading to v8.5.4* for instructions.

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 web protection services to be stopped.

   In some cases, the installer may be unable to stop the web protection 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 the 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 8: 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.

> **Important**
> If, during the upgrade process, you encounter the error "Installation failed with error code 3004", refer to *Potential issue when upgrading to v8.5.4* for instructions.

When Filtering Service or the management server is upgraded from v8.1, v8.2, or v8.3 to v8.5 or v8.5.3, 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 **local** 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 web protection services to be stopped.

   In some cases, the installer may be unable to stop the web protection 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 9: Upgrade any additional components

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

See:

- *Additional components: Windows upgrade instructions*, page 23
- *Additional components: Linux upgrade instructions*, page 24

Additional components: Windows upgrade instructions

Important

If, during the upgrade process, you encounter the error "Installation failed with error code 3004", refer to *Potential issue when upgrading to v8.5.4* for 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 web protection services to be stopped.

   In some cases, the installer may be unable to stop the web protection 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 web protection services to be stopped.

    In some cases, the installer may be unable to stop the web protection 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 10: Post-upgrade activities

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

1. If the upgrade process involves 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 v.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**.

   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 upgrading to v8.5.3 or v8.5.4, 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 v8.5.3 or v8.5.4:

- 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. As of v8.5, Active Directory (Mixed Mode) is not supported. When upgrading to v8.5.x, 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 or v8.5.4 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
      ```

7. Due to a security enhancement in v8.5.4, if the **Use SSL to connect to the Log Database** option has been selected on the **Web > Settings > Reporting > Log Server** page, and the SSL certificate currently in use has not been properly deployed to the SQL Server management server and Log Server machines, is not valid, or has expired, connection between Log Server and the Log Database will fail and data will no longer be forwarded by Log Server. A new certificate will need to be installed on both machines.

   If you use this feature, after upgrading, use the **Test Connection** option on that same page to confirm continued connectivity.

8. When upgrading to 8.5.4, the internal flag that resets the SIEM Integration feature from the new functionality provided in the v8.4 release of Forcepoint Web Security back to the old functionality in v8.3 and earlier, is reset. This allows all customers to automatically use the improved 8.5.4 SIEM Integration functionality.