Upgrading Forcepoint Security Solutions to v8.4

Upgrade Instructions | Web, Data, and Email Solutions | Version 8.4.x

This guide describes how to upgrade a Forcepoint deployment with multiple modules —web, email, and/or data—to v8.4.x. For information on upgrading systems that include stand-alone installations of data, email, or web protection solutions, refer to the Deployment and Installation Center in the Forcepoint Technical Library.

Forcepoint security solutions must be at one of the following versions to upgrade to v8.4:

- v7.8.4
- v8.1.x
- v8.2.x
- v8.3.x

Note that it is not possible to upgrade directly from v8.0.x to v8.4. Upgrade to v8.3.0 first, then upgrade to v8.4.

- For information on upgrading from earlier versions to version 7.8.4, see Upgrading TRITON Enterprise v7.7.x to v7.8.x.
- For information about upgrading from v8.0 to v8.3, see Upgrading TRITON APX Suite to v8.3.

Because Forcepoint Email Security includes Forcepoint DLP components, the upgrade procedure for combined web and email solutions is the same as the upgrade procedure for all Forcepoint modules.

To upgrade to v8.4, see:

Perform the upgrade in the order described. This sequence is critical, because if you upgrade supplemental servers or agents before the management server, they stop

communicating. If you upgrade the management server first, it continues communicating with the components until they are upgraded.

Important

Forcepoint Security Solutions v8.4 does not support dual-mode appliances. Dual-mode appliances host both Forcepoint Email Security and Forcepoint Web Security, or Forcepoint Email Security and Forcepoint URL Filtering.

If you are upgrading a dual-mode appliance, see Upgrading Dual Mode Appliances to v8.3.

Important

V Series appliance users:

Some older V10000 and V5000 appliances are not supported with version 8.0.0 and higher.

See Appliances supported with version 8.x.

Before upgrading Forcepoint security solutions

To prepare for the upgrade:

- Read the relevant v8.4 release notes.
  - Release Notes for Forcepoint Web Security and Forcepoint URL Filtering
  - Release Notes for Forcepoint DLP
  - Release Notes for Forcepoint Email Security
  - Release Notes for Forcepoint Appliances
- Unless instructed otherwise by Forcepoint Technical Support, ensure your system is functional prior to upgrade.
- Ensure the time set on all appliances is synchronized prior to upgrade.
- Make sure the installation machine meets the System requirements for this version.
- If you are already using Virtual Machines (VMs) for Forcepoint Security Manager or for Microsoft SQL Server, take a snapshot of the VMs before you start a Forcepoint upgrade.
- If you have a remote database, ensure that the SQL account has a sysadmin role.
- Back up all of your Forcepoint components before starting the upgrade process. If you are upgrading from v7.x, see Backup and Restore FAQ for instructions. If you are upgrading from v8.x, see Backup and Restore FAQ v8.x.

The Backup and Restore FAQ includes instructions for backing up all of the pieces that make up Web Security Gateway Anywhere (now Forcepoint Web Security Hybrid Module) on all platforms:

- Forcepoint Management Infrastructure
- Web Security components
- Content Gateway
- Data Security components

The upgrade process guides you through upgrading **all** components on the selected machine.

- You cannot choose which components to upgrade.
- Partial upgrades are not supported.

When upgrading the Forcepoint management server, if upgrade fails for any component **except** Forcepoint Management Infrastructure, you can either continue to upgrade the rest of the components or exit the process and modify component settings.

- You cannot continue if the infrastructure upgrade fails.
- You cannot roll back a component that was upgraded successfully.

After upgrade, your system has the same configuration as before the upgrade. Apart from the option to edit the Forcepoint Email Security database IP address if it has changed since installation, the upgrade process does not allow you to change your configuration or settings.

Upgrade sequence for Forcepoint security solutions

When upgrading multiple Forcepoint components, upgrade them in the following order. For information on upgrading systems that include standalone installations of data, email, or web protection solutions, refer to the Deployment and Installation Center in the Forcepoint Technical Library.

Important

Forcepoint Security Solutions v8.4 does not support dual-mode V Series appliances (that is, appliances that host Forcepoint Email Security and Forcepoint Web Security, or Forcepoint Email Security and Forcepoint URL Filtering).

If you are upgrading a dual-mode appliance, see Upgrading V-Series Dual Mode Appliances to v8.3.

1. The machine hosting Web **Policy Broker**
   - For a software installation, run the Forcepoint Security Installer or Web Linux installer.

- If Policy Broker is on the management server, you can upgrade the Infrastructure and Web, Email, and Data management components at the same time as upgrading Policy Broker.

2. Additional instances of Web **Policy Server**

   May be software-based or on **user directory and filtering** appliances. For a software installation, run the Forcepoint Security Installer. For an appliance, install the v8.4 upgrade patch.

3. Additional instances of Web **Filtering Service** or **User Service**

   - Additional instances of Filtering Service may be software-based or on **filtering only** appliances.
   - If you have filtering only appliances in your deployment, upgrade these appliances **after** the corresponding full policy source or user directory and filtering appliance has been upgraded. This is because appliances that have instances of Policy Server must be upgraded before you upgrade any components that point to it.

4. Web and Email **Log Server**

   If these components are on separate machines, it does not matter which is upgraded first.

   

   Important

   Make sure that no Email Log Database or Web Log Database jobs are running while the Log Server instances are being upgraded.

5. **Management server** (if not already upgraded as part of an earlier step)

   - Whenever possible, upgrade the management server before any other Data components. This ensures that policy engines continue to function until they are upgraded themselves.

     Note new policies cannot be deployed to the policy engines until they are upgraded to the same version as the management server.

   - If you need to upgrade a policy engine before upgrading the management server—because the policy engine resides on a full policy source appliance—detection of fingerprinted content might not work on the appliance until the management server is upgraded.

     The policy engine embedded in Content Gateway and Email products continues to monitor the old Web and Email DLP policies and block/permit accordingly.

6. Upgrade all other appliances in your network. This can be done in any order, and can be completed in parallel.

   - If Email Security Gateway or TRITON AP-EMAIL is deployed in cluster mode, upgrade the primary appliance before any secondary appliances. You do not need to release the appliances from the cluster in order to perform the upgrade.

- The Email MTA continues to function after the management server upgrade, but the logs are cached on the appliance until TRITON AP-EMAIL is upgraded as well. For best practice, redirect email traffic to another MTA as cached messages may be lost otherwise.

7. Upgrade all other **Web** and **Data** components. This can be done in parallel. For example:
   - Network Agents
   - Transparent user identification agents
   - Remote Filtering Server
   - Data Security secondary servers
   - Data Security components on ISA and TMG servers
   - Software-based installations of Content Gateway

Upgrade procedure for Forcepoint security solutions

This procedure covers the steps required to upgrade either the all on-premises security solutions or Web and Email solutions (given that Email includes Data components).

Important

Forcepoint Security Solutions v8.4 does not support dual-mode V Series appliances (that is, appliances that host Forcepoint Email Security and Forcepoint Web Security, or Forcepoint Email Security and Forcepoint URL Filtering).

If you are upgrading a dual-mode appliance, see Upgrading V-Series Dual Mode Appliances to v8.3.

Step 1: 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 2008 R2 SP1, 2012, or 2012 R2 machine.
- A RHEL 6.5 or later, 7.0, 7.1, or 7.2 machine.

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.

If Policy Broker resides on the management server, running the Forcepoint Security Installer also upgrades the infrastructure and web, data, and email management components as described in *Step 5: Upgrade the management server*, page 11. Ensure you also follow the steps in *Post-upgrade steps*, page 15, to configure the management server.

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see the Upgrade Guide: Forcepoint Web Security.

1. Make sure that no administrators are logged on to the management console.
2. Log on to the installation machine with an account having **domain** and **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. Go to the **Downloads** tab of My Account to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint84xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.
5. Right-click **Forcepoint84xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security 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 services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been 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 components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized, and then the upgrade begins.

    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.

Step 2: 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. Policy Server may reside on:

- **user directory and filtering** appliances
- Windows Server 2008 R2 SP1, 2012, or 2012 R2 machines
- RHEL 6.5 and later, 7.0, 7.1, or 7.2 machines

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see Upgrade Guide: Forcepoint Web Security.

1. Make sure that no administrators are logged on to Forcepoint Security Manager.

2. Log on to the installation machine with an account having **domain** and **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. Go to the **Downloads** tab of My Account to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint84xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.
   - Verify that the MD5 value of the downloaded file matches the value shown on the download page.
5. Right-click **Forcepoint84xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web 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.

   The **Pre-Upgrade Summary** screen appears when the services have been 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 components that will be upgraded, and then click **Next**.

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

Step 3: Upgrade additional Filtering Service and User Service machines

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

- Windows Server 2008 R2 SP1, 2012, or 2012 R2 machines
- RHEL 6.5 or later, 7.0, 7.1, or 7.2 machines

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

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see Upgrade Guide: Forcepoint Web Security.

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

1. Log on to the installation machine with an account having **domain** and **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.

2. Close all applications and stop any antivirus software.

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

3. Go to the **Downloads** tab of My Account to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint84xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.

4. Right-click **Forcepoint84xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
5. The installer detects Web Security 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.

   The **Pre-Upgrade Summary** screen appears when the services have been 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 components that will be upgraded, and then click **Next**.

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

Step 4: Upgrade Log Servers

Upgrade the Web and Email Log Server machines, if they have not already been upgraded with other components. Any other services on the machine are also upgraded in the correct order.

For information on Web Security Log Server, see Upgrade Guide: Forcepoint Web Security.

For information on Email Security Log Server, see Upgrading to Forcepoint Email Security v8.4.

Step 5: 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.

1. Make sure that no administrators are logged on to the management console.
2. Log on to the installation machine with an account having **domain** and **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. Go to the **Downloads** tab of My Account to download the Forcepoint Security Installer.
   - The installer file is **Forcepoint84xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.
5. Right-click **Forcepoint84xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears as files are extracted.
6. The installer detects 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 that appear in subsequent stages of the upgrade.
8. Follow the screens in the upgrade wizard as described in the sections below:
   - *Management Infrastructure*
   - *Management Infrastructure*
   - *Forcepoint Web Security*
   - *Forcepoint DLP*
   - *Forcepoint Email Security*
9. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
10. Reboot the machine.

> **Important**
> You may be prompted to restart the machine after each component is upgraded. This is optional. You may prefer to restart the machine once after all components are upgraded.

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

12. Follow the instructions in *Post-upgrade steps*, page 15.

Management Infrastructure

The Forcepoint Management Infrastructure provides basic framework for all of the management components that make up the Forcepoint Security Manager. This framework includes a central settings database that stores shared configuration (like administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Welcomes you to the installation and upgrade wizard. 1. Click **Next** to begin the upgrade process. The system checks disk space requirements. 2. When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows: ● The destination folder for the installation files. ● The name of the SQL Server machine and the user name of an authorized database administrator. ● The IP address of the Forcepoint management server and administrator credentials. Click **Next** to accept the properties.
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A popup message appears at this stage, warning that you must also upgrade all modules. This popup may be hidden behind the main installer window. If your installation appears to freeze, locate the hidden popup by moving the main installer window, and click **OK** to proceed with the installation.
Summary	When module upgrade is complete, summarizes your system settings, including: ● The destination folder for the installation files. ● The name of the SQL Server machine and the user name of an authorized database administrator. ● The IP address of the Forcepoint management server and administrator credentials. Click **Finish** to complete the upgrade for this module.

Forcepoint Web Security

The Web Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	Welcomes you to the upgrade wizard. Click **Next** to continue.
Upgrade	Select **Start the upgrade**, then click **Next**. 1. Accept the subscription agreement and click **Next**. 2. The installer proceeds to stop all Forcepoint services.
Pre-Upgrade Summary	Provides a list of components that will be upgraded. Click **Next** to start the upgrade. The installer backs up critical files.
Installing	Shows installation progress. When complete, the installer configures your software. This can take up to 10 minutes.
Upgrade Complete	You're notified when installation of this module is complete. Click **Done** to exit the installer.

Forcepoint DLP

Before running the data upgrade wizard, the installer validates system requirements to ensure your upgrade will be successful.

The pre-upgrade check validates hardware requirements, credentials for your SQL management database, endpoint security certificates, manager configuration, administrator upgrade permissions, and your database structure. As it proceeds, it reports whether a step succeeded or failed, or it gives you a warning.

If there is a failure, the upgrade stops. For details, see **\AP-DATA-PreUpgradeTests.log** in the directory where you installed Forcepoint DLP.

If there are only warnings, you have the option to proceed with the upgrade or stop it. If you continue, your system may behave unexpectedly, but this will not have a critical impact.

If the pre-upgrade check succeeds or if you proceed with warnings, the Forcepoint DLP wizard is launched, followed by wizards for each installed component.

The Data Security upgrade wizard contains the following screens:

Wizard Screen	Fields
Welcome	This screen welcomes you to the installation and upgrade wizard. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Installation Confirmation	Verify your system settings and click **Install** to continue the upgrade.

Wizard Screen	Fields
Installation	This screen shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more. In certain circumstances, you may receive an internal SQL error. If you do, do not click OK until you have resolved the issue with Forcepoint Technical Support. If you continue prematurely, you can cause problems with your reporting database.
Summary	When installation of this module is complete, this screen summarizes your system settings. 1. Click **Done** and you're prompted to update your predefined policies and content classifiers. 2. Click **OK** to install the updates. You're shown the status of the updates, the items being updated, and details such as how many policies are updated, deleted, or added. 3. Click **Close** when the updates are complete.

Forcepoint Email Security

The Email Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	This screen welcomes you to the upgrade wizard. Click **Next** to continue.
Select Components	This screen shows the components that will be upgraded (those that are currently installed). Click **Next** to continue.
Configuration	This page shows the IP address of the database engine configured to manage the Email Security Log Database and the logon type. If you have changed the database since your previous installation, modify the settings here.
Pre-Installation Summary	This screen shows: ● The components to be installed ● The pre-existing and new version numbers ● The destination folder for the installation files ● The required and available disk space Click **Install** to begin the upgrade.
Installation	This screen shows that the installation is progressing. The management component is upgraded on the Forcepoint management server. The Email Security Log Server is upgraded on machines where it is found. When complete, the installer configures your Forcepoint Email Security software. This can take up to 10 minutes.
Summary	You're notified when installation of this module is complete. Click **Done** to exit the installer.

Post-upgrade steps

Once the Forcepoint management server upgrade is complete:

1. Restart the management server.
2. Log onto Forcepoint Security Manager:

   ```
   https://<IP_address_or_hostname>:9443
   ```

3. Click **Data** in the Security Manager toolbar to select the Data Security module.
4. Follow the prompts that appear for updating data loss protection policies and classifiers.

   Depending on the number of policies you have, this can take up to an hour. During this time, do not restart the server or any of the services.
5. If you removed applications from Forcepoint DLP's predefined endpoint application groups prior to upgrade, go to the **Main > Resources > Endpoint Application Groups** page after logging on and remove them again. The upgrade process restored these to their original state.
6. Click **Deploy**.
7. Click **Email** in the Security Manager toolbar to select the Email Security module.
8. Go to the **Settings > General > Database Downloads** page and click **Update Now** to perform an immediate database download update.

Step 6: Upgrade appliances

Upgrade all appliances that have not been upgraded in the above steps. This can be done in any order, and can be completed in parallel.

If you have deployed Forcepoint Email Security in cluster mode, ensure that you upgrade the primary appliance before any secondary appliances. You do not need to release the appliances from the cluster in order to perform the upgrade.

For more information, see the V Series Appliance Upgrade Guide and X Series Appliance Upgrade Guide.

Step 7: Upgrade additional components

Once you have completed the above steps, you can upgrade any additional software components and client components:

1. Upgrade any additional software instances of Network Agent and Content Gateway. If these components run on Forcepoint V Series, X Series, and Virtual Appliances, this step has already been done.
2. Upgrade any additional Web Security server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines.
3. Upgrade supplemental servers, protectors, mobile agents, and other Forcepoint DLP agents.

4. Upgrade client components, including the logon application (LogonApp.exe), Remote Filtering Client, Forcepoint Web Security Endpoint and Forcepoint DLP Endpoint.

These actions can be done in parallel. For more information, see the following upgrade guides:

- Upgrade Guide: Forcepoint Web Security
- Upgrade Instructions for Forcepoint DLP