Upgrading to Forcepoint Email Security v8.5.x

The Forcepoint Email Security v8.5.x upgrade process includes appliance components (V Series appliance, X Series security blade, or virtual appliance), along with Forcepoint Security Manager and Email Log Server Windows components. A virtual appliance upgrade applies only to version 7.8.0 and later, and an X Series security blade upgrade applies only to version 7.8.4 and later.

These instructions cover the upgrade of a Websense Email Security Gateway, TRITON AP-EMAIL, or Forcepoint Email Security solution to Forcepoint Email Security version **8.5.0**, **8.5.3**, **8.5.4**, or **8.5.5**, installed on-premises or in Microsoft Azure.

- You can upgrade directly to on-premises version **8.5.5** from Forcepoint Email Security version 8.5.4 or 8.5.3.
- You can upgrade directly to on-premises version **8.5.4** from Forcepoint Email Security version 8.4.0, 8.5.0, or 8.5.3.
- You can upgrade directly to on-premises version **8.5.3** from TRITON AP-EMAIL version 8.2.0 and 8.3.0, or from Forcepoint Email Security version 8.4.0 or 8.5.0.
- You can upgrade directly to on-premises version **8.5.0** from TRITON AP-EMAIL version 8.1.0, 8.2.0, and 8.3.0, or from Forcepoint Email Security version 8.4.0.
- Upgrades for Forcepoint Email Security in Azure version **8.5.5** are not supported.
- You can migrate to Forcepoint Email Security in Azure version **8.5.4** from Forcepoint Email Security in Azure version 8.5.0 or 8.5.3, or from on-premises versions 8.4.0, 8.5.0, and 8.5.3. All upgrades to version 8.5.4 in Azure require a migration.
- You can upgrade to Forcepoint Email Security in Azure version **8.5.3** from Forcepoint Email Security in Azure version 8.5.0, or migrate from on-premises versions 8.2.0, 8.3.0, 8.4.0, and 8.5.0. If you are running AP-DATA Email Gateway version 8.3, it is not possible to upgrade to version 8.5.3; a new appliance must be installed. See Installing Forcepoint Email Security in Microsoft Azure for installation steps.
- You can upgrade to Forcepoint Email Security in Azure version **8.5.0** from AP-DATA Email Gateway version 8.3 or from Forcepoint Email Security in Azure version 8.5.0.
- If you are planning to deploy Forcepoint Email Security and Forcepoint Security Manager together in Azure, all components must be upgraded to the same version. Download the Forcepoint Email Security for Windows and the Forcepoint Email Security Virtual Appliance image files from the Forcepoint Customer Hub downloads menu. Begin by running the Windows installer first, followed by the Virtual Appliance image.

  Note that Forcepoint Email Security 8.5.5 is not supported in Azure.

Contents

Upgrade matrix

Certain versions can be upgraded directly to Forcepoint Email Security version 8.5.x; other versions must be migrated or upgraded to a different version first. The following table details the upgrade/migration paths from previous versions to version 8.5.x.

All upgrades to Forcepoint Email Security in Azure version **8.5.4** require a migration.

Version 8.5.4 and 8.5.5 Virtual Appliances are certified and supported for VMware ESXi 7 / 6.7 / 6.5 / 6.0. A stable release of ESXi is recommended to avoid unexpected issues. See v8.5.4 Release Notes or v8.5.5 Release Notes..

Note
For ESXi 7 and 6.7, users **must** use the v8.5.4 OVA file to create a new VM. Versions 8.5.3 and earlier will **not** deploy and are **not** supported on ESXi 6.7 or 7.

Platform	Version	Mode	First Step	First Version	Second Step	Final Version
Physical	7.8.4	single	upgrade	8.4.0	upgrade	8.5.0
Physical	8.0.0	single	upgrade	8.3.0	upgrade	8.5.0
Physical	8.0.1	single	upgrade	8.3.0	upgrade	8.5.0
Physical	8.1.0	single			upgrade	8.5.0
Physical	8.2.0	single			upgrade migrate	8.5.0, 8.5.3 8.5.3 Azure
Physical	8.3.0	single			upgrade migrate	8.5.0, 8.5.0 8.5.3 Azure
Physical	8.4.0	single			upgrade migrate	8.5.0, 8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure
Physical	8.5.0	single			upgrade migrate	8.5.0, 8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure

Platform	Version	Mode	First Step	First Version	Second Step	Final Version
Physical	8.5.3	single			upgrade migrate	8.5.4, 8.5.5 8.5.4 Azure
Physical	8.5.4	single			upgrade	8.5.5
Physical	7.8.4	dual	migrate	8.4.0	upgrade	8.5.0
Physical	8.0.0	dual	migrate	8.3.0	upgrade	8.5.0
Physical	8.0.1	dual	migrate	8.3.0	upgrade	8.5.0
Physical	8.1.0	dual			migrate	8.5.0
Physical	8.2.0	dual			migrate	8.5.0
Virtual	7.8.4	single	migrate	8.4.0	upgrade	8.5.0
Virtual	8.0.0	single	migrate	8.3.0	upgrade	8.5.0
Virtual	8.0.1	single	migrate	8.3.0	upgrade	8.5.0
Virtual	8.1.0	single			upgrade	8.5.0
Virtual	8.2.0	single			upgrade migrate	8.5.0, 8.5.3 8.5.3 Azure
Virtual	8.3.0*	single			upgrade migrate	8.5.0, 8.5.3 8.5.3 Azure
Azure	8.3.0	single			migrate	8.5.0 Azure
Virtual	8.4.0	single			upgrade migrate	8.5.0, 8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure
Virtual	8.5.0	single			upgrade migrate	8.5.3, 8.5.4 8.5.3 Azure, 8.5.4 Azure
Azure	8.5.0	single			migrate migrate	8.5.0 Azure 8.5.3 Azure, 8.5.4 Azure
Virtual	8.5.3	single			upgrade migrate	8.5.4, 8.5.5 8.5.4 Azure
Azure	8.5.3	single			migrate	8.5.4 Azure
Virtual	8.5.4	single			upgrade	8.5.5

*The version 8.3 virtual appliance was updated and re-released on June 2, 2017. Direct upgrade from a version 8.3 appliance to version 8.5.x is available only if you deployed from the updated OVA file released on June 2, 2017. If you deployed from the original OVA file released on December 19, 2016, you must use the migration

process described in *Migrate to version 8.5.x*, page 17.

Important

Starting in version 8.5, vCPU specifications changed for virtual appliances, which will require you to increase your vCPU and RAM allocations following an upgrade from version 8.3 or lower.

See the Knowledge Base article Resource Upgrade on OVA and Forcepoint Appliances Getting Started Guide for additional information and virtual appliance specifications.

Versions older than 7.8.4

For systems running a version 7.6.x or 7.7.x deployment, and requiring an upgrade to version 8.5.x, it is necessary to upgrade to version 7.7.0 or 7.8.0 first, then upgrade to version 7.8.4, then to version 8.4, and finally to version 8.5.x. See the following:

- Upgrading Email Security Gateway v7.6.x to v7.7.0
- Upgrading Email Security Gateway v7.7.x to v7.8.0
- Upgrading Email Security Gateway v7.8.0 to v7.8.x
- Upgrading to Forcepoint Email Security version 8.4

For systems running Email Security Gateway on an X10G security blade, it is necessary to upgrade to version 8.0.0 before upgrading to version 8.3. Next, a direct upgrade to version 8.5.0 is possible.

Certain older V10000 and V5000 appliances are not supported with version 8.0.0 and later. See V Series appliances supported with version 8.x.

Any version 7.6.x Email Security component that is currently installed on Windows Server 2003 must be migrated to Windows Server 2008 R2 before the upgrade to v7.7.0. Migration to Windows Server 2012 may be performed after an upgrade to v7.8.0.

Ensure that third-party components are upgraded as well, to work with your new email protection solution version.

Appliance upgrades

For upgrade instructions, see:

- V Series Upgrade Guide
- X Series Upgrade Guide

We recommend that you perform a complete system backup in the event your system experiences a power outage or other interruption during the upgrade process. Recovery procedures are also included in case they are needed.

The upgrade process includes Forcepoint appliance components (V Series appliance, virtual appliance, or X Series chassis security blade), along with Forcepoint Security Manager and Email Log Server Windows components. Ensure that your deployment additionally includes Forcepoint DLP for data loss prevention (DLP) capabilities. The upgrade process detects and upgrades this module during the Security Manager upgrade.

Warning

Please contact Technical Support before you begin the upgrade process if Forcepoint personnel have customized any Email Security Gateway, TRITON AP-EMAIL, or Forcepoint Email Security back-end configuration settings.

Starting with v8.3.0, a single ISO image (v8.x.x Unified Appliance Installer) is offered to restore an appliance back to the factory settings as well as to upgrade all installed modules in the target appliance to the corresponding version.

Modules include:

- **App** — Base appliance infrastructure and appliance controller

Forcepoint Web Security:

- **Web** — Forcepoint Web Security core components
- **Proxy** — Content Gateway web proxy

Forcepoint Email Security:

- **Email** — Forcepoint Email Security core components

To upgrade an appliance prior to v8.3.0, the legacy RPM upgrade package is required. Refer to the dedicated upgrade guide for V Series or X Series appliances.

If deploying on a virtual appliance, verify the ESXi version. Users of SXi 6.7 must use the v8.5.4 OVA file to create a new VM. Versions 8.5.3 and earlier will not deploy and are not supported on ESXi 6.7.

Dual-Mode appliances

The V Series appliance and the email virtual appliance were re-architected at version 8.3. Dual security mode on the V Series appliance (TRITON AP-EMAIL and TRITON AP-WEB or Web Filter & Security) is no longer supported. It is recommended to migrate the Email module off any dual-mode appliance to a new version 8.5.x appliance, leaving the web security system on the existing appliance. **Before beginning the upgrade**, see Upgrading V Series Dual-Mode Appliances to Version 8.5 for important upgrade instructions. Email data and messages on an existing virtual appliance must also be migrated to a new version 8.5.x appliance. See *Migrate to version 8.5.x*, page 17.

Upgrade preparation

Several issues should be considered, and certain steps taken, before beginning an email protection solution upgrade.

Before you begin

- **Verify current deployment.** Ensure that your current deployment is functioning properly before you begin the upgrade, and that required network interfaces have reliable connections to Forcepoint components and the Internet. The upgrade process does not repair a non-functioning system.
- Check the Certified Product Matrix to verify the supported operating systems for your initial and target versions. For example, version 8.5.3 does not support Windows 2008, which may cause errors when attempting to upgrade from a Windows 2008 operating system.
- Ensure that your existing deployment includes Forcepoint Email Security Solutions before you upgrade. If you have used the custom option to install Forcepoint Email Security, you must install Forcepoint Email Security Solutions as well, for data loss prevention capabilities. Consult the Forcepoint Security Manager Data Security module upgrade procedures, to ensure a smooth upgrade experience. See Upgrading to Forcepoint DLP v8.7.x for details.
- If you are not already familiar with the preparation required for upgrading off-appliance components, review the requirements before upgrading your appliances.
  - For web protection solutions, see Before upgrading v8.5.x web protection solutions and the Release Notes for the web protection solution to which you are upgrading: v8.5.0 Web Protection Release Notes, v8.5.3 Web Protection Release Notes, or v8.5.4 Web Protection Release Notes.
  - Review the Release Notes for the email protection solution to which you are upgrading: v8.5.0 Forcepoint Email Security Release Notes, v8.5.3 Forcepoint Email Security Release Notes, or v8.5.4 Forcepoint Email Security Release Notes.
- **Verify the system requirements** for the version to which you are upgrading to ensure your network can accommodate the new features and functions. See System requirements for this version for a detailed description.
- **Prepare Windows components.** See Preparing for installation for an explanation of general preparations for upgrading the Windows components in your email protection system.
- **Ensure that your firewall is configured correctly** so that the ports needed for proper email protection operation are open. See Forcepoint Email Security ports for information about all email security system default ports, including appliance interface designations and communication direction.
- **Prepare Microsoft Azure virtual network** if you are upgrading to Forcepoint Email Security in Azure. See Installing Forcepoint Email Security in Microsoft Azure.

- **Prepare for service disruption during upgrade**. Appliance services are not available while the upgrade is applied, continuing until the appliance continues its final restart. Service is not disrupted while the off-box components are upgraded.
- If you are using link aggregation and plan to enable VLAN support after upgrade, disable link aggregation before enabling VLAN support on the blade or chassis. VLAN is only available on X Series appliances.
- **Ensure you have the most recent hotfix installed for your version**. Additionally, ensure that you have the following hotfixes installed or uninstalled, as appropriate.
  - **Uninstall the following hotfix**:
    - If you have any appliance with Hotfix 200 (Spectre/Meltdown Hotfix) installed, you must uninstall the hotfix before upgrading to v8.5.x. After upgrading, reinstall Hotfix 200 on the new version.
  - **Install the following hotfix**:
    - If you are a Forcepoint V5000 G2R2 customer upgrading from v8.4 to v8.5.x, you must install 8.4 Appliance Hotfix 101 (APP-8.4.0-101) before upgrading.
- **Back up and remove tomcat log files and remove temporary manager files** (optional; recommended to facilitate timely Forcepoint Security Manager upgrade). Use the following steps:
  1. Log onto the Windows server where the Forcepoint Security Manager resides.
  2. Navigate to the following directory:

     C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\logs
  3. Copy **C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\logs** to another location (for example, to **C:\WebsenseBackup\Email)**, and then delete it in the directory mentioned in step 2.
  4. Navigate to the following directory:

     C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\tempEsgUploadFileTemp
  5. Delete all the downloadFile* files.
- **Inventory all configuration customizations and make a plan for restoring any that are required**. Customizations are not retained through the upgrade process. Before your upgrade, contact Forcepoint Technical Support for assistance with validating files from your pre-upgrade file system. Customizations can include:
  - Custom patches
  - Hand updated files
  - Extra packages added
  - Extra files added, binary or configuration
    - Please allow some lead time for Forcepoint Technical Support to complete this validation.

- **Inventory customized HTML notification templates for the Personal Email Manager and Forcepoint Secure Messaging end-user portals**. Any customizations you make to notification message templates are lost when upgrading to a new version of Forcepoint Email Security. After upgrade, you will need to reconfigure your customized templates.
- **Back up appliance configuration and settings**. It is critical to perform a full appliance configuration backup and save it to a filestore.
  1. Log onto the CLI and elevate to **config** mode.
  2. To perform an immediate full backup, use:

     ```
     create backup now --location filestore_alias [--desc
     "<description>"]
     ```

  3. Include a unique description to make it easier to identify backup files that may have very similar names and dates.

  Important
  Before upgrading a virtual appliance, see *Virtual appliance*, page 15, for important upgrade issues specific to the virtual appliance.

- **Back up DKIM keys and SSL certificates**. DKIM keys and Personal Email Manager SSL certificates are removed (not transferred) when upgrading to v8.5.4 or v8.5.5.
  - Before beginning your upgrade, export DKIM keys and signing rules from the page **Settings > Inbound/Outbound > DKIM Settings**. Following the upgrade, re-import the DKIM keys and signing rules.
  - SSL certificates and keys cannot be exported from Personal Email Manager. Ensure that you have the original SSL certificate and key pair available, and use the page **Settings > Personal Email > SSL Certificate** to import the certificate following the upgrade.
- If you are using an Always On Availability group with SQL Server, remove the log database from the group prior to starting the upgrade. Re-add the database to the group after the upgrade to synch it.

  See this article for additional information SQL Server Always On High Availability Groups and Forcepoint Email Security.

Encrypted connection to Email Log Database

Starting in version 8.5.4, more stringent connection string and certificate requirements are needed for establishing an encrypted connection with SQL Server. Specifically, the hostname or fully qualified domain name (FQDN) used for the connection string must match the Common Name (CN) field on the certificate that SQL Server is using if you have an encrypted database connection. Not doing so will result in failure to connect.

Before beginning your upgrade, configure your Email Log Database as follows:

1. On the page **Settings > Reporting > Log Database**, enter either a hostname or a FQDN in the field Log Database.
2. In the Log Server Configuration Utility, enter either a hostname or a FQDN for the esglogdb76 system DSN under ODBC Data Sources.

   See Email Log Server Configuration Utility for additional help with configuring your Log Database.
3. On the certificate used by SQL Server for encryption, verify that the Common Name field exactly matches the hostname or FQDN that is used in the Log Database settings and esglogdb76 system DSN.

Reminders

- Immediately following your upgrade, it is necessary to install the latest hotfix for your version. See the Forcepoint Customer Hub downloads menu to download the latest hotfix.
- All components in your deployment, including those running off-appliance, must run the same version of Forcepoint software, if applicable. Refer to the Release Notes to determine the Forcepoint Security Manager, Forcepoint Web Security, and Forcepoint DLP versions supported with your version of Forcepoint Email Security.
- Version 8.5.0 was the last supported software release for the V5K G2R2 appliance and the V10K G3R1 appliance. Hardware support will continue to be available throughout End-of-Life for these appliance models. Please refer to the related Tech Alert and the official Product Support Life Cycle matrix for details.
- The Forcepoint V5000 G2R2 appliance may encounter a memory shortage after upgrading to version 8.2 or later. This issue is the result of newer versions of software requiring additional memory, and was only captured under a heavy load. A DIMM Kit (2 x 8GB) is certified to expand the physical memory of the V5000 G2R2 Appliance. It is now generally available and recommended for V5000 G2R2 deployment moving to versions 8.2 and later. Please contact your sales representatives for purchase information. For more details, see the related Knowledge Base article and the DIMM Kit installation instructions.
- The upgrade to version 8.3 added the following default elements:
  - Spoofed Email policy filter
  - Spoof policy action
  - Antispoof policy rule
  - “url-analysis” default queue

  If your system currently uses policy elements or a queue with these names, change them before the upgrade process begins, to avoid having duplicate names after the upgrade. The email security system may not function properly with the duplicate names.
- The upgrade to version 8.4 added the following default elements:
  - Email Attachment policy filter
  - Email Attachment policy action

  - Email Attachment policy rule
  - “attachment” default queue

  If your system currently uses policy elements or a queue with these names, you must change them before the upgrade process begins. The version 8.5.x upgrade process includes a pre-check function that terminates the upgrade if duplicate policy components are detected.
- New presentation reports were added in version 8.3 for spoofed email and URL analysis data. Examples include:
  - Outbound Spoofed Email Percentage Summary
  - Top Inbound Spoofed Email Sender Domains
  - Top Inbound Recipients of Spoofed Email
  - Top Outbound Embedded URL Categories Detected
  - Outbound Embedded URL Detection Volume Summary

  The upgrade process may not complete successfully if you have existing custom reports with the same names as these reports.

Backup procedures

The backup procedures outlined in the following steps are safeguards against an unexpected interruption of your upgrade process. A power outage or appliance restart may not allow the upgrade process to finish successfully. You may need to restore your settings databases to their pre-upgrade state in order to re-initiate and complete the upgrade.

Use the following backup procedure to prepare for your email protection solution upgrade:

1. Back up the Forcepoint Security Manager settings. See the topic titled Backup and Restore of Global Settings Data in Forcepoint Security Manager Help for backup procedures.
2. Back up the Forcepoint DLP management server configuration. See the Technical Library topic titled How do I back up and restore Forcepoint DLP? for backup instructions.
3. Back up your Microsoft SQL Server databases. Ensure that all the files in the following directories are included in your backup:

   \\Database\\esglogdb76

   \\Database\\esglogdb76_*n*

   \\SQL Server Agent\\Jobs\\ ESG_ETL_Message_Insert_Job

   \\SQL Server Agent\\Jobs\\ESG_ETL_Message_Process_Job

   \\SQL Server Agent\\Jobs\\ESG_ETL_Message_Summary_Address_Job

   \\SQL Server Agent\\Jobs\\ESG_ETL_Message_Summary_Job

   \\SQL Server Agent\\Jobs\\ESG_ETL_Message_Update_Job

\\SQL Server Agent\\Jobs\\ESG_Maintenance_Job

See your Microsoft SQL Server documentation for backup procedure details.

4. Back up email appliance configuration settings using appliance-appropriate back-up procedures.
   - See the topic titled How do I back up and restore Forcepoint appliances? for backup procedures.
   - See the Forcepoint Appliances Command Line Interface guide for backup and restore command options.
5. Back up Email Security module configuration settings in the Forcepoint Security Manager using options on the **Settings > General > Backup/Restore** screen. Click **Backup** to store your settings locally. You can also specify the Log Database for your configuration settings backup location and then click **Backup**.

   See the topic titled Backing up and restoring management server settings in Administrator Help for Forcepoint Email Security backup details.
6. Upgrade any third-party integration products if necessary for use with your email protection system. See third-party product documentation for appropriate backup and upgrade requirements and procedures.
7. Redirect email traffic out of the system that is being upgraded. If you do not redirect mail traffic, you may lose messages cached during the upgrade process.

Note

The Personal Email Manager end-user utility is not available until after the appliance upgrade is complete.

Recovery procedures

In the event that your upgrade was unexpectedly interrupted (for example, by a power outage or appliance restart) and the automatic rollback facility also fails, you can use the backup files you created earlier in the process to restore your system to its pre-upgrade state. (See *Backup procedures*.)

Note

Any quarantined or archived messages stored in the appliance local queues may be lost as a result of the recovery process.

Use the following procedure to restore your email protection system:

1. Use the appropriate recovery image to re-image your appliance to the version from which you were upgrading.
2. Run firstboot.
3. Restore the backup files to your system in the following order, using the restore information for each component referenced in *Backup procedures*:

a. Appliance
b. Microsoft SQL Server databases
c. Forcepoint Security Manager
d. Data Security module
e. Email Security module

Important

Your backup files should match the version of the email protection system to which you are restoring.

For example, if your backup files are from v8.1.0, you should not upgrade to v8.5 before restoring the v8.1.0 email files.

4. Verify that your system works as it did before the interrupted upgrade.

You can now initiate the upgrade process.

Upgrade instructions

Once you have completed the activities outlined in *Upgrade preparation*, you can proceed with the product upgrade. This section provides instructions for performing an upgrade of an email security system deployment.

Important

If your network includes a Forcepoint web security solution, you must upgrade the Policy Broker/Policy Server machine first, whether or not these components reside on an appliance. Other Forcepoint services located on the Policy Broker/Policy Server machine should be upgraded at the same time. See Upgrade Instructions for Forcepoint Web Security.

This section provides a description of an email system upgrade to the following components:

1. Email Log Server (*Upgrade the Email Log Server*, page 13)
2. Forcepoint Security Manager Email Security Module (*Upgrade the Forcepoint Security Manager Email Security Module*, page 14)

3. Forcepoint Appliances (*Upgrade or migrate Forcepoint Appliances*, page 14)

> **Important**
> When the upgrade is applied, the original file system is preserved. Should the upgrade procedure encounter a fatal error, the original file system is restored. Off-appliance components may need to be restarted.

Upgrade the Email Log Server

If the Email Log Server is installed on a separate machine from the Forcepoint Security Manager, upgrade the Email Log Server using the Forcepoint Security Installer from the Forcepoint Customer Hub downloads menu.

If the Email Log Server is installed on the same machine as the Forcepoint Security Manager, it is included in the upgrade process described in *Upgrade the Forcepoint Security Manager Email Security Module*, page 14.

> **Important**
> If you are upgrading multiple Log Servers, perform the upgrades one at a time to avoid possible upgrade process errors.

1. Download the **Forcepoint Security Installer** from the Forcepoint Customer Hub downloads menu.
2. Run the installer and follow the installation wizard instructions for Log Server.
   - The installer does not allow you to change existing configuration settings. Changes must be made after the upgrade.
   - The upgrade installer stops the Email Log Server service, updates the Email Log Server and the Email Log Database, and then restarts the Email Log Server service.

> **Important**
> If you are running appliances in a cluster, you must release all appliances from the cluster before performing an upgrade or a migration. Upgrade or migrate each appliance as needed, and then rebuild your cluster after the process is complete.

Upgrade the Forcepoint Security Manager Email Security Module

Use the Forcepoint Security Installer from the Forcepoint Customer Hub downloads menu. The upgrade process includes Forcepoint DLP and the Email Log Server if it is installed on the Security Manager machine.

If you are planning to deploy both Forcepoint Email Security and Forcepoint Security Manager in Azure, this procedure is necessary to first upgrade Forcepoint Security Manager using the Forcepoint Email Security for Windows package.

1. Download the **Forcepoint Security Installer** from the Forcepoint Customer Hub downloads menu.
2. Run the installer and ensure that Forcepoint Email Security and Forcepoint DLP are selected for upgrade.

   The upgrade process includes Forcepoint DLP and the Email Log Server if it is installed on the Security Manager machine.
3. Follow the installation wizard instructions.

   The Data Security module upgrade occurs after the Forcepoint Management Infrastructure upgrade. The Email Security module upgrade follows the Data Security module.

   - The upgrade installer Configuration page shows the IP address of the database engine that manages the Email Log Database and logon type. If you have changed the database since your previous installation or upgrade, use this page to change these settings.
   - The upgrade script stops the Email Security module service, updates the Email SQL Server databases (and Log Server if found), and then restarts the Email Security module service.

Note

The Security Manager Email Security module is not available until after the Security Manager upgrade completes.

Upgrade or migrate Forcepoint Appliances

Appliance services are not available while the upgrade is being applied; email traffic should not be directed through appliances during the upgrade process. Disruption

continues until the appliance completes its final restart. It is a best practice to perform the upgrade at a time when service demand is low.

Important

If you are running appliances in a cluster, you must release all appliances from the cluster before performing an upgrade or a migration. Upgrade or migrate each appliance as needed, and then rebuild your cluster after the process is complete.

X Series

For the X Series hardware appliance, see the Forcepoint X Series upgrade guide for upgrade instructions and command options on this platform.

If you are running an X10G security blade version 8.0.x, you must upgrade to version 8.3 before you upgrade to version 8.5.x. You cannot upgrade directly to version 8.5.x from version 8.0.x.

V Series

For the V Series hardware appliance, see the Forcepoint V Series Appliance upgrade guide for complete upgrade instructions and command options.

The version 8.3 and later V Series appliance introduced a command-line interface (CLI) to replace the Appliance Manager. For an introduction to the CLI, see the Forcepoint Appliances CLI Guide.

The V Series appliance upgrade process includes a check for:

- Adequate disk space for Forcepoint Email Security (at least 8 GB required)
- Cached message log file size (cannot exceed 10 MB)

A backup and restore function to save existing appliance configuration settings is also included. You are prompted to contact Technical Support if any configuration file is missing.

Note

You may need to restart the appliance if you cannot establish an **ssh** connection after the upgrade is complete.

Virtual appliance

The Forcepoint Email Security virtual appliance platform was re-architected at version 8.3. As a result, email security system data and email messages that reside on a pre-version 8.3 virtual appliance must be migrated off that appliance when you upgrade to a new version. The migration is accomplished via a command-line interface (CLI) **migrate** command performed on the version 8.5.x appliance.

Migration is necessary when upgrading any version of Forcepoint Email Security to Forcepoint Email Security in Azure. See *Migrate to version 8.5.x*, page 17.

Upgrade to version 8.5.x

Use the following steps to upgrade directly to version 8.5.x.

1. Download the v8.5.x **Forcepoint Security Installer** from the Forcepoint Customer Hub downloads menu and save it to a location from which it is easy to copy it to Windows servers hosting Forcepoint web, email, and data components, such as Forcepoint Security Manager (formerly TRITON Manager) and Log Server.
2. Perform *Upgrade preparation*, page 6.

   Skip to Step 4 if your deployment does not include Forcepoint Web Security.
3. If your deployment includes Forcepoint Web Security, upgrade the policy source machine (Policy Broker/Policy Database) before upgrading web protection components on your security blades. If the *Full policy source* machine is an X10G, upgrade that blade first. After upgrading the policy source machine, confirm that Policy Broker and Policy Database services are running.

   All Forcepoint components on the *Full policy source* machine are upgraded when Policy Broker/Policy Database are upgraded.

   In all instances, you must upgrade Forcepoint Web Security components in the following order:

   a. *Full policy source*

      Upon completion, confirm that Policy Broker and Policy Database services are running. See Upgrading Web Protection Solutions.

   b. *User directory and filtering* (sometimes called *policy lite*) blades and non-appliance servers that host Policy Server

   c. *Filtering only* blades, and non-appliance servers that host Filtering Service

   d. Off-appliance servers hosting other web protection components (like Log Server or Logon Agent)

      Successful upgrade of *User directory and filtering* and *Filtering only* appliances requires connectivity with the Policy Broker and Policy Database services.
4. If the appliance is registered in Forcepoint Security Manager, navigate to **Appliances > Manage Appliance** and unregister the appliance.

   Re-registration is a post-upgrade activity.

   If the appliance is a *User directory and filtering* appliance, unregister the appliance. In the Web module of Forcepoint Security Manager, navigate to **Settings > General > Policy Servers** and unregister the appliance.
5. Using the CLI, download and apply the v8.5.x upgrade:

   a. Download the upgrade file.

      ```
      load upgrade
      ```

   b. Install the upgrade.

```
install upgrade
```

Select the v8.5.x upgrade file from the list.

When prompted, confirm to continue, then accept the subscription agreement.

The upgrade performs several system checks. The checks may take several minutes.

When installation is complete, the appliance automatically restarts.

If the upgrade fails, the blade server automatically rolls back to the prior version. If the source of the failure is not obvious or cannot be easily address, contact Forcepoint Technical Support.

If an error message displays indicating that ISO verification has failed, repeat the command with the following parameter added:

```
--force <iso_file_name>
```

If installation seems to stop, allow the process to run for at least 90 minutes. If installation has not completed in that time, contact Forcepoint Technical Support.

6. Perform *Post-upgrade activities*, page 21.
7. Return to Step 5 and upgrade remaining appliances.
8. Upgrade the management server (if not upgraded when Policy Broker/Policy Database were upgraded), and other servers that host Forcepoint components. See Upgrading Forcepoint Security Solutions to v8.5.x.

Migrate to version 8.5.x

Consider the following issues before you initiate your virtual or Azure appliance migration process:

- Ensure that your source and destination appliances in the migration are configured in the same subnet. If they are not, the migration process may complete, but the new appliance interfaces are not correctly updated.
- You may need to reconfigure some network settings for the migration process. The version 8.3 and later virtual appliance supports three network interfaces: C, P1, and P2. In the migration, the C interface retains the setting you assigned it during firstboot. The P1 and P2 interfaces (eth0 and eth1) inherit the settings of P1 and P2 when migrating from a V5000, or the E1 and E2 settings when migrating from a V10000.
  - Forcepoint Email Security in Azure supports only the C interface.
- Dynamic Host Configuration Protocol (DHCP) is not supported in version 8.3 and later. If your existing appliance has DHCP enabled, those network settings are not migrated. You must configure static network interface IP addresses for your appliance.
- Calculate the disk space used on your existing appliance and ensure that the new appliance has adequate disk space for all data you wish to migrate.

Use the following steps to migrate data and email messages to a version 8.5.x appliance.

1. Install a new version 8.5.x appliance.

   The VMware virtual machine requires ESXi version 6.0 or later. See the topic titled *Virtual Appliance Setup* in the Forcepoint Appliances Getting Started Guide for detailed instructions for downloading and creating a virtual machine.

   If you are migrating to an Azure deployment, skip to Step 4. See Installing Forcepoint Email Security in Microsoft Azure.

2. On the source appliance, ensure that the following ports are open (not blocked by firewalls), so that the new appliance can communicate with the source appliance:

   - On-premises: port 22
   - Azure: port 22222

3. On the new appliance (version 8.5.x), run the firstboot wizard to select appliance security mode (email), enter appliance management settings (e.g., C interface IP address, hostname, DNS server IP addresses), and define some basic configuration settings (e.g., hostname, administrator password, system time zone). This step is not applicable in Azure.

   See the topic titled *Firstboot Wizard* in the Forcepoint Appliances Getting Started Guide for detailed firstboot instructions.

   Note
   The source appliance hostname is not migrated to the destination appliance. The destination appliance uses the hostname set during firstboot, and then the upgrade process adds "-esg" to the end of the name.

4. Log on to the new version 8.5.x appliance CLI and elevate to **config** mode.

   If you are migrating to an Azure deployment, skip to Step 6.

5. Set the appliance P1 interface using the **set interface ipv4** command with the following syntax:

   ```
   set interface ipv4 --interface p1 --ip <ipv4_address>
   [--mask <ipv4_netmask>] --gateway <ipv4_address>
   ```

   Setting this interface now can facilitate the migration process in the event that your current P1 interface is a virtual IP address, which will not be migrated.

   The P1 interface you configure in the CLI is displayed as "E1" in the Forcepoint Security Manager. This step is not applicable in Azure.

   Note
   If you use a client interface like PuTTY to connect to the appliance, configure a longer connection session to accommodate a slightly lengthy migration process.

   For example, in the PuTTY configuration interface, select the **Connection** category. Enter **30** in the **Seconds between keepalives (0 to turn off)** entry field.

6. Download the appropriate hotfix for your source appliance version from the Forcepoint Customer Hub downloads menu
   - Version 8.1.0, 8.2.0, 8.3.0, 8.4.0, 8.5.0, 8.5.3, or 8.5.4 on-premises: Hotfix 300
   - Version 8.3, 8.5.0, 8.5.3, or 8.5.4 in Azure: Hotfix 301
7. Contact Forcepoint Technical Support for assistance to apply the hotfix to your previous version appliance.

   See the ReadMe file packaged with the hotfix for more information about hotfix contents.
8. In the version 8.5.x appliance CLI, ensure you are still in **config** mode and then log in to the email module:

   ```
   login email
   ```
9. You may perform the migration using the **migrate** CLI command on the version 8.5.x appliance with one of two options: interactive or silent.

   Interactive mode is a step-by-step process that requires user input during the process.

   The following displays an example of the interactive mode command:

```
email85(config)(Email)# migrate
interactive  silent
email85(config)(Email)# migrate interactive

Welcome to the Forcepoint Email Security Migration Tool.

Destination Forcepoint Email Security System Information:

    Platform: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

    Hostname: email85-esg

    Eth0:10.206.12.47  Mask:255.255.255.0

    9188MB of 32125MB disk space used for running the system

    60MB of 95863MB disk space used for the email messages

Checking Forcepoint Email Security services...

Forcepoint Email Security services check has been successfully completed.

Would you like to migrate the source system to this appliance? [yes/no]
yes
Preparing certificates...

Certificates have been successfully prepared.

Please enter the Forcepoint Email Security interface IP address for the source appliance:
10.206.21.239
```

   Interactive mode requires the following information to be entered:
   - Source appliance (pre-version 8.5.x) IP address.
   - Confirmation for the start of the migration.
   - Selection of a mode option; **Azure** or **On-Premises**.

     Select **Azure** if you are migrating to a version 8.5.x Azure appliance.

     Select **On-Premises** if you are migrating to a version 8.5.x on-premises appliance.

The following displays the selection of **On-Premises** to migrate to an 8.5.x on-premises appliance:

```
Please select a mode option: [1/2]

    1. Azure mode. Select this mode if either your source or destination appliance is an Azure appliance.
    2. On-Premises mode. Select this mode if both your source and destination appliances are on-premises.

2
When making your selection, please ensure that both your source and destination appliances are on-premises. Do you wish to proceed in On-Premises mode? [yes/no]
yes
Reading appliance information...

sending incremental file list

sent 1131 bytes  received 15 bytes  2292.00 bytes/sec
total size is 761902  speedup is 664.84

Source Forcepoint Email Security System Information:

    Platform: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

    Hostname: evasquez_appliance-esg

    Eth0:10.206.21.239  Mask:255.255.255.0

    9372MB of 32125MB disk space used for running the system

    60MB of 95863MB disk space used for the email messages


Disk space is available on this appliance.

Checking Forcepoint Email Security services...

Forcepoint Email Security upgrade pre-check has been successfully completed.
```

- Selection of a transfer option.

  If you migrate email message queues in addition to configuration settings, be aware that the transfer of large-volume queues may take a few hours to complete.

  If you are migrating Forcepoint Security Manager to Azure and leaving database partitions behind, we recommend using option 1, because there is no need to transfer mail queues. If you select option 2, you will not be able to perform actions on transferred messages, such as delivering a quarantined message.

  The following image displays an example of the CLI for this section:

```
Source Forcepoint Email Security System Information:

    Platform: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

    Hostname: evasquez_appliance-esg

    Eth0:10.206.21.239  Mask:255.255.255.0

    9372MB of 32125MB disk space used for running the system

    60MB of 95863MB disk space used for the email messages


Disk space is available on this appliance.

Checking Forcepoint Email Security services...

Forcepoint Email Security upgrade pre-check has been successfully completed.


Would you like to start the migration process from the source appliance: 10.206.21.239 to this appliance (services on both appliances will stop)? [yes/no]
yes
Please select a transfer option: [1/2/3]

    1. Transfer only configuration files, defer logs, and policy incidents.
    2. Transfer configuration files, defer logs, policy incidents, and email messages.
    3. Quit

2
```

Silent mode requires the following information to be entered:

- Source appliance (pre-version 8.5.x) IP address.
- Migration mode; **Azure** or **On-Premises**.
- Subscription key.

The subscription key is only required when the migration mode is Azure.

The second transfer option is automatically selected for silent mode, and the migration runs without the need for subsequent user input.

The following image displays an example of the CLI for silent mode:

```
email85(config)(Email)# migrate silent --host 10.206.21.239 --mode On-Premises

Welcome to the Forcepoint Email Security Migration Tool.

Destination Forcepoint Email Security System Information:

    Platform: Forcepoint Email Security VMwareOVA running software version 8.5.0 build 11

    Hostname: email85-esg

    Eth0:10.206.12.47  Mask:255.255.255.0

    9185MB of 32125MB disk space used for running the system

    60MB of 95863MB disk space used for the email messages

Checking Forcepoint Email Security services...
```

Important

You must use your existing Forcepoint Security Manager Windows machine. Use of a newly installed Forcepoint Security Manager for an upgrade is not currently supported.

Consider the following after you perform your virtual appliance migration process:

- If you have an email DLP policy configured to use a Forcepoint DLP quarantine action, and the Release Gateway on the page **Settings > General > Remediation** is set to **Use the gateway that detected the incident**, you should change the Release Gateway to the IP address of your new appliance. Otherwise, when a Data Security module administrator releases a pre-migration quarantined message, an "Unable to release incident" error is generated.
- Virtual IP address settings in filter actions are not retained after an appliance migration. You need to reconfigure virtual IP address settings manually.

Important

Please contact Technical Support if Forcepoint personnel have customized your appliance iptables settings. These customizations are not preserved by the migration process.

Post-upgrade activities

Your system should have the same configuration after the upgrade process as it did before the upgrade. Any configuration changes can be made after the upgrade process is finished.

After your upgrade is completed, redirect email traffic through your system to ensure that it performs as expected.

Email hybrid service registration information is retained during the upgrade process, so you do not need to complete the registration again, unless you have performed an appliance migration (e.g, from a virtual appliance to a new virtual appliance). See *Update appliance management interface configuration settings (for migration only)*, page 24, for information.

Perform the following tasks in the Forcepoint Security Manager or the CLI:

- *Install Email Security hotfixes*
- *Repair Email Security registration with Data Security*, page 22
- *Update data loss prevention policies and classifiers*
- *Update Forcepoint databases*
- *Update Email Security module backup file*
- *Configure email DNS lookup*
- *Increase vCPU and RAM allocation*
- *Update appliance management interface configuration settings (for migration only)*
- *Verify the system and configuration in the CLI*, page 26

Install Email Security hotfixes

Navigate to the Forcepoint Customer Hub downloads menu and select your version, then install the latest Windows and appliance hotfixes.

Alternatively, appliance hotfixes can be installed using the appliance command-line interface (CLI) or Forcepoint Security Appliance Manager (FSAM). See Forcepoint Appliances CLI Guide and Forcepoint Security Appliance Manager Help for more information.

Repair Email Security registration with Data Security

Re-register the new appliance with the Data Security module as follows:

1. In the Email Security module, navigate to the page **Settings > General > Data Loss Prevention** and click **Unregister**.
2. Register the appliance with the Data Security module; click **Register**.
3. Navigate to the page **Settings > General > Data Loss Prevention** and ensure that the appliance management (C) interface IP address appears in the field **Communication IP address**.
4. In the Data Security module, navigate to the page **Settings > Deployment > System Modules** and select the Email Security module.
5. In the upper left corner, click **Delete**.
6. Deploy the changes; click **Deploy**.

Update data loss prevention policies and classifiers

1. Select the Data Security module.
2. Follow the prompts that appear for updating data loss prevention 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.
3. Deploy the changes; in the upper right of the Data Security module, click **Deploy**.

Update Forcepoint databases

- From the page **Settings > General > Database Downloads**, click **Update Now**.

  This action performs an immediate database download update.

Update Email Security module backup file

Due to a change in implementation at version 8.1, the Security Manager Email Security module backup file format is not compatible with versions earlier than 8.1. You must remove any pre-version 8.1 backup log file before you create a new backup file for version 8.5.x. If you do not remove the old log file before you create the new file, the backup/restore function may not be accessible.

Use the following steps:

1. Navigate to the following directory on the Security Manager machine:

   C:\Program Files (x86)\Websense\Email Security\ESG Manager
2. Locate and remove the following file:

   `ESGBackupRestore`

   Copy this file to another location if you want to save it.
3. Create a new backup file on the page **Settings > General > Backup/Restore**.

Configure email DNS lookup

The virtual appliance firstboot process includes the entry of DNS server settings. You can enhance DNS lookup query performance by configuring a second set of DNS server entries specifically for the Email Security module. Use the following CLI commands, as needed:

```
set interface dns --module email --dns1  <DNS_IP>
set interface dns --module email --dns2  <DNS_IP>
set interface dns --module email --dns3  <DNS_IP>
```

Not applicable for Forcepoint Email Security in Azure.

Increase vCPU and RAM allocation

If you upgraded from version 8.3 or lower to version 8.5.x, it is necessary to increase the vCPU and RAM allocations on your virtual appliance, in order to ensure adequate system resources.

See the Knowledge Base article Resource Upgrade on OVA and Forcepoint Appliances Getting Started Guide for more information.

Update appliance management interface configuration settings (for migration only)

If your upgrade to version 8.5.x included a data migration, you need to re-configure some functions that use the appliance management (C) interface after the migration and upgrade are complete. The management (C) interface was added for virtual appliance users at version 8.3.

Forcepoint Email Security in Azure supports only the C interface.

These configuration settings include:

- *Data loss prevention*
- *Email hybrid service*
- *Personal Email Manager notification message*
- *Update Log Database*
- *Reset Forcepoint Email Security license (only if Forcepoint Security Manager was migrated to Azure)*
- *Move Forcepoint DLP database (only if Forcepoint Security Manager was migrated to Azure)*

Data loss prevention

Re-register the new appliance with the Data Security module as follows:

1. Select the Email Security module and navigate to the page **Settings > General > Data Loss Prevention**.
2. Remove DLP registration; click **Unregister**.
3. In the Data Security module, navigate to the page **Settings > Deployment > System Modules**.
4. Select the Email Security module.
5. In the upper left corner, click **Delete**.
6. On the Email Security module page **Settings > General > Data Loss Prevention**, ensure the appliance management (C) interface IP address appears in the field **Communication IP address**.
7. Register the appliance with the Data Security module; click **Register**.
8. Select the Data Security module and click **Deploy**.

Email hybrid service

This action is required only if you used the C interface on a hardware appliance that you have migrated.

Re-register the new appliance with the email hybrid service as follows:

1. Select the Email Security module and navigate to the page **Settings > Hybrid Service > Hybrid Configuration**.
2. At the bottom of the Hybrid Configuration page, click **Edit**.
3. Replace the SMTP server IP address with the new C interface IP address.
4. Click **OK**.

Personal Email Manager notification message

This action is required only if you used the C interface on a hardware appliance that you have migrated.

You may need to enter your destination appliance management interface IP address for the proper distribution of Personal Email Manager notification messages.

1. Select the Email Security module and navigate to the page **Settings > Personal Email > Notification Message**.
2. In the text field **IP address or hostname**, enter the new appliance management (or C) interface.
3. Click **OK**.

If you had previously customized HTML notification templates for the Personal Email Manager, your customizations were lost when upgrading to the new version; reconfigure your templates on the page **Settings > Personal Email > Notification Message**.

Update Log Database

If you encounter the following warnings after your migration, you may need to update the Email Log Database with new values for appliance hostname, management interface IP address, C interface IP address, and device ID:

```
[*]: Forcepoint Email Security migration has been successfully completed.

Please read the following warnings:
[WARNING]: [Errno -3] Temporary failure in name resolution
[WARNING]: Cannot update Forcepoint Email Security management interface.
For problems, please contact Forcepoint Technical Support.
```

You may encounter this situation if you use Windows authentication. In that case, the migration script cannot update the C interface, resulting in this message.

1. Open SQL Server Management Studio.
2. Click **New Query**.

3. In the query window, enter the following command:

   ```
   USE [esglogdb76]
   ```

   Select **esg_device_id**, **admin_manage_ip**, **device_c_port_ip** from **dbo.esg_device_list**.
4. Enter **GO**.
5. Locate the **esg_device_id** associated with either the admin_manage_ip or the device_c_port_ip of the source appliance.
6. Note the device ID and remove the device row.
7. Execute the following command using the device ID from the previous step, and updating the C interface IP address, management IP address, and host name to the new, post-migration values:

   ```
   UPDATE dbo.esg_device_list SET esg_name = '<host name>',
   admin_manage_ip = '<appliance management IP address>',
   device_c_port_ip = '<C IP address>' WHERE esg_device_id =
   '<device id>'
   ```
8. Enter **GO**.
9. Run the query.

Reset Forcepoint Email Security license (only if Forcepoint Security Manager was migrated to Azure)

If you migrated Forcepoint Security Manager to Azure, it is necessary to reset the Forcepoint Email Security licenses for each of your appliances. Contact Forcepoint Technical Support for assistance with this step.

After Technical Support has reset your licenses, navigate to **Settings > General > Email Appliances** and add each of your appliances. See Forcepoint Email Security Administrator Help.

Move Forcepoint DLP database (only if Forcepoint Security Manager was migrated to Azure)

If you migrated Forcepoint Security Manager to Azure, it is necessary to move your Forcepoint DLP database to the new Forcepoint Security Manager in Azure. See How do I move the TRITON AP-DATA database to another MS SQL Server? for instructions.

Verify the system and configuration in the CLI

The following table details system and configuration checks made in the CLI. See the Forcepoint Appliances CLI Guide for more information.

- Log on to the CLI and elevate to **config** mode.

Action	Command

Display system information	`show appliance info`
	
	Results may be similar to:
	`Uptime: 0 days, 2 hours, 13 minutes`
	`Hostname: webapp.example.com`
	`Hardware_platform: X10G G2`
	`Appliance_version: 8.5.0`
	`Mode: Forcepoint Web Security`
	`Policy_mode: Filtering only`
	`Policy_source_ip: 10.222.21.10`

Display the upgrade history	`show upgrade history`

Display the appliance and module status	`show appliance status`
	`show <module>`
	
	If expected system services are not running, restart the module that hosts the services.
	`restart <module>`

Display network interface settings	`show interface info` If you have bonded interfaces, note that the names used to indicate the type of bonding have changed. For example, load-balancing is now balance-rr.

Check and synchronize the system time, if necessary	`show system ntp`
	`show system clock`
	`show system timezone`
	
	If the clock is off and NTP is configured, sync with:
	`sync system ntp`
	
	Otherwise, to sync when the time is set manually, see “System time and time synchronization with Forcepoint servers” in Forcepoint Appliances Getting Started.

Configure size and frequency values for archiving commands	`set log archive`

Check SNMP polling and alerting settings (if you integrate with a SIEM or SNMP server)	`show snmp config`
	`show trap config`
	`show trap events`
	
	These commands are not supported in Forcepoint Email Security in Azure.