Upgrading to Forcepoint Email Security v8.4

These instructions cover the upgrade of a Websense Email Security Gateway or TRITON AP-EMAIL solution to Forcepoint Email Security version 8.4. You can upgrade directly to version 8.4 from Email Security Gateway version 7.8.4 and TRITON AP-EMAIL version 8.1.x, 8.2.x, and 8.3.x.

Important

If you are currently running TRITON AP-EMAIL version 8.0.x, you must first upgrade to version 8.3, then to version 8.4. You cannot upgrade directly from version 8.0.x to version 8.4.

If you are currently running a version 7.6.x deployment, and you want to upgrade to version 8.4, you must upgrade to version 7.7.0 first, then upgrade to version 7.8.0, and then to version 7.8.4. See Upgrading Email Security Gateway v7.6.x to v7.7.0, Upgrading Email Security Gateway v7.7.x to v7.8.0, and Upgrading Email Security Gateway v7.8.0 to v7.8.x for procedures.

If you are currently running a version 7.7.x deployment, and you want to upgrade to version 8.4, you must upgrade to version 7.8.0 first, and then upgrade to version 7.8.4 before you upgrade to version 8.4. See Upgrading Email Security Gateway v7.7.x to v7.8.0 and Upgrading Email Security Gateway v7.8.0 to v7.8.x for procedures.

If you are running Email Security Gateway on an X10G security blade, you must upgrade to version 8.0.0 before performing an upgrade to version 8.3. Then you can perform a direct upgrade to version 8.4.

See Upgrading Email Protection Solutions for:

- Specific product upgrade paths
- Links to all intermediate upgrade instructions
- Important information about backing up your system before you upgrade. Having backup files is an important safeguard in the event of a power outage or other interruption during the upgrade process.

Important

Some older V10000 and V5000 appliances are not supported with version 8.0.0 and later. See V Series appliances supported with version 8.0.

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 also 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 or TRITON AP-EMAIL back-end configuration setting

Some customizations may be lost during the upgrade process.

Important

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. We recommend that you migrate the Email module off any dual-mode appliance to a new version 8.3 or 8.4 appliance, leaving the web security system on the existing appliance. See Upgrading V Series Dual-Mode Appliances to Version 8.4 for important upgrade instructions **before you begin your upgrade.**

Email data and messages on an existing virtual appliance must also be migrated to a new version 8.3 or 8.4 appliance. See *Virtual appliance*, page 8, for more information.

Contents:

- *Upgrade preparation*
- *Upgrade instructions*
- *Post-upgrade activities*

Upgrade preparation

Several issues should be considered before you begin an email protection solution upgrade.

- **Verify current deployment.** Ensure that your current deployment is functioning properly before you begin the upgrade. The upgrade process does not repair a non-functioning system.
- **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 All Forcepoint solutions 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.
- The upgrade to version 8.0.x and 8.2.x renames the following default policy filters, policies, and rules:
  - ThreatScope is renamed File Sandbox; at version 8.2.x, File Sandbox is renamed Advanced File Analysis.
  - URL Scanning is renamed URL Analysis.

  If you currently have custom rules with these new names, you should change them before the upgrade process begins, to avoid having duplicate rule names after the upgrade. The email security system may not function properly with the duplicate names.
- 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 you currently have policy elements or a queue with these names, you should 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 adds the following default elements:
  - Email Attachment policy filter
  - Email Attachment policy action
  - Email Attachment policy rule

- "attachment" default queue

Important

If you currently have policy elements or a queue with these names, you must change them before the upgrade process begins.

The version 8.4 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 be successfully completed if you have existing custom reports with the same names as these reports.

- **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 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.

Important

If you are upgrading a virtual appliance, see *Virtual appliance*, page 8, for important upgrade issues specific to the virtual appliance.

Upgrade instructions

Once you have completed the activities outlined in *Upgrade preparation*, you can perform 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 procedure for solutions that include web, email, and data protection for more information.

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

1. Email Log Server
2. Security Manager Email Security Module
3. Forcepoint Appliances

Upgrade the Email Log Server

Use the Forcepoint Security Installer from the Forcepoint My Account downloads page to upgrade Email Log Server if it is installed on a machine other than the one on which the Security Manager is installed. Follow the installation wizard instructions for Log Server.

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

- 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.

Upgrade the Forcepoint Security Manager Email Security Module

Use the Forcepoint Security Installer from the Forcepoint My Account downloads page. 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.

Warning

On the Select Components screen in the upgrade installer, ensure that the **Forcepoint Email Security** option is selected. This option is required if you are running your email security system on a V or X Series appliance or an on-premises (ESXi server) virtual appliance.

The **Forcepoint DLP Cloud Email** option applies to a cloud-hosted virtual appliance running with Forcepoint DLP. **This Forcepoint DLP component is not supported in version 8.4. Do not select this option.**

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 TRITON Appliances

Email traffic should not be directed through appliances during the upgrade process.

X Series

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

Important

If you are running an X10G security blade version 8.0.x, you must upgrade to version 8.3 before you upgrade to version 8.4. You cannot upgrade directly to version 8.4 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.

Important

Dual security mode V Series appliances are not supported in version 8.3 and later. If you are upgrading a V Series appliance from a version earlier than 8.3, we recommend that you migrate the Email Security module off the dual-mode appliance to a new version 8.3 or version 8.4 appliance. See Upgrading V Series Dual-Mode Appliances to Version 8.4 for details on upgrading a dual-mode (Web and Email) appliance.

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 V Series 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.

If your V Series appliances are configured in a cluster, the primary box should be upgraded first, followed by all its secondary machines, 1 at a time. You do not need to release the appliances from the cluster in order to perform the upgrade.

Note

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

Virtual appliance

The following table shows the upgrade paths for the Forcepoint Email Security virtual appliance:

Current Version	Upgrade Path		Migration Required?
7.8.0, 7.8.2, 7.8.3	7.8.4	8.4.0	Yes
7.8.4	8.4.0		Yes
8.0.x	8.3.0	8.4.0	Yes
8.1.x, 8.2.x	8.4.0		Yes
8.3.x	8.4.0		Depends on version 8.3 installation package used

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 8.4 appliance.

Important

Direct upgrade from a version 8.3 appliance to version 8.4 is available only if you deployed from the OBVA file released on June 2, 2017. If you deployed from the OVA file released on December 19, 2016, you must use the migration process described in the following section to upgrade to version 8.4.

You should consider the following issues before you initiate your virtual 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 must release your virtual appliances from a cluster before performing the migration. Migrate each appliance, and then rebuild your cluster after the migration process is complete.
- You may need to reconfigure some network settings for the migration process. The version 8.3 and later virtual appliance supports 3 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.
- Dynamic Host Configuration Protocol (DHCP) is not supported in version 8.3 and later. If your existing appliance has enabled DHCP, you should note that 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.

Direct upgrade from version 8.3.x to version 8.4

You can upgrade directly from version 8.3.x to version 8.4 using the appliance CLI upgrade commands. See the appliance upgrade guide for details about downloading and applying the upgrade file.

Migration/Upgrade:

- **From version 8.0.x to version 8.3.x or**
- **From version 7.8.4, 8.1.x, or 8.2.x to version 8.4**

If you are currently running TRITON AP-EMAIL version 8.0.x, you must first upgrade to version 8.3, then to version 8.4. This process involves migrating your data and email messages off your current virtual appliance to the new one.

If you are currently running TRITON AP-EMAIL version 7.8.4, 8.1.x, or 8.2.x, upgrading to Forcepoint Email Security version 8.4 also involves the migration process outlined below.

Use the following steps to migrate TRITON AP-EMAIL data and email messages to a version 8.3 or 8.4 virtual appliance:

1. Install a new version 8.3 or 8.4 virtual 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.
2. On the new appliance (version 8.3 or 8.4), 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). See the topic titled *Firstboot Wizard* in the Forcepoint Appliances Getting Started Guide for detailed firstboot instructions.

> ✓ **Note**
>
> Note that 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.

3. Log on to the new version 8.3 or 8.4 appliance CLI and enter “config” mode. 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.

✓ **Note**

If you use a client interface like PuTTY to connect to the appliance, you will want to configure a longer connection session to accommodate a somewhat 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.

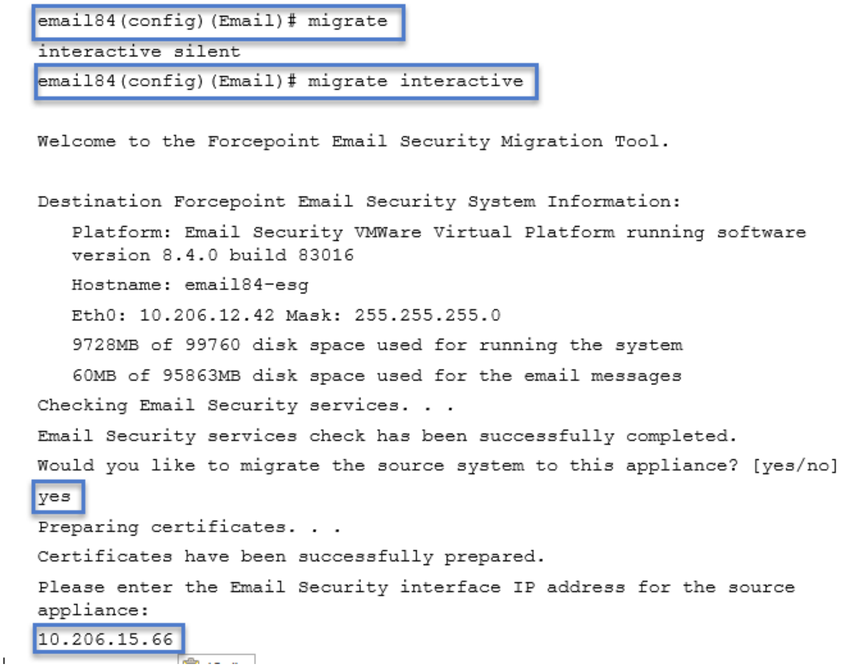
4. Download TRITON AP-EMAIL Hotfix 300 for your source virtual appliance version (7.8.4, 8.0.0, 8.0.1, 8.1.0, 8.2.0, or 8.3.0) from the Forcepoint My Account Downloads page.
5. Contact Forcepoint Technical Support for assistance to apply the hotfix to your previous version appliance.

   See the ReadMe file packaged with the hotfix for more information about hotfix contents.
6. In the version 8.3 or 8.4 appliance CLI, ensure you are still in **config** mode and then log in to the email module:

   ```
   login email
   ```
7. You may perform the migration using the **migrate** CLI command on the version 8.3 or 8.4 appliance with 1 of 2 options: interactive or silent.

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

   An example of the interactive mode command follows (user entries are in bold):



```
email84(config)(Email)# migrate
interactive silent
email84(config)(Email)# migrate interactive

Welcome to the Forcepoint Email Security Migration Tool.

Destination Forcepoint Email Security System Information:
   Platform: Email Security VMWare Virtual Platform running software
   version 8.4.0 build 83016
   Hostname: email84-esg
   Eth0: 10.206.12.42 Mask: 255.255.255.0
   9728MB of 99760 disk space used for running the system
   60MB of 95863MB disk space used for the email messages
Checking Email Security services. . .
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 Email Security interface IP address for the source
appliance:
10.206.15.66
```

You enter the following information:

- Source appliance (pre-version 8.4) IP address
- Confirmation for the start of the migration
- Selection of a transfer option:

  Example CLI for this section of the migration looks like:

  ```
  Would you like to start the migration process from the
  source appliance: 10.206.15.66 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

  Are you sure you want to transfer all configuration
  files, defer logs, policy incidents, and email messages?
  [yes/no]

  yes
  ```

  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.

Silent mode requires the user to enter only the source appliance (pre-version 8.4) IP address. In our example:

```
migrate silent --host <10.206.15.66>
```

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

Important

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

You should consider the following issues after you perform your virtual appliance migration process:

- If you have an email DLP policy configured to use a TRITON AP-DATA or Forcepoint DLP quarantine action, and the **Settings** > **General** > **Remediation** page Release Gateway 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.

After a successful migration to version 8.3, perform the direct upgrade process shown in the previous section titled *Direct upgrade from version 8.3.x to version 8.4*, page 9.

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 14, for information.

You should perform the following tasks in the TRITON Manager or Forcepoint Security Manager:

- *Repair Email Security registration with Data Security*
- *Update data loss prevention policies and classifiers*
- *Update Forcepoint databases*
- *Update Email Security module backup file*
- *Configure email DNS lookup*
- *Update appliance management interface configuration settings (for migration only)*
- *Update Log Database (for migration only)*

Repair Email Security registration with Data Security

1. In the Email Security Gateway module, navigate to **Settings** > **General** > **Data Loss Prevention** and click **Unregister**.
2. Click **Register** to re-register the Email Security appliance with Data Security.
3. In the Data Security module, click **Deploy** in the upper right area of the screen.

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. Click **Deploy**.

Update Forcepoint databases

Click **Update Now** in the **Settings** > **General** > **Database Downloads** page. 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.x. If you don’t 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 **Settings > General > Backup/Restore** page.

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>
```

Update appliance management interface configuration settings (for migration only)

If your upgrade to version 8.3 or 8.4 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 is new for virtual appliance users at version 8.3.

These configuration settings include:

- *Data loss prevention*
- *Email hybrid service*
- *Personal Email Manager notification message*

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

7. 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 **Settings** > **Hybrid Service** > **Hybrid Configuration** page.
2. Click **Edit** at the bottom of the page.
3. Replace the SMTP server IP address with the new C interface IP address.
4. Click **OK**.

Personal Email Manager notification message

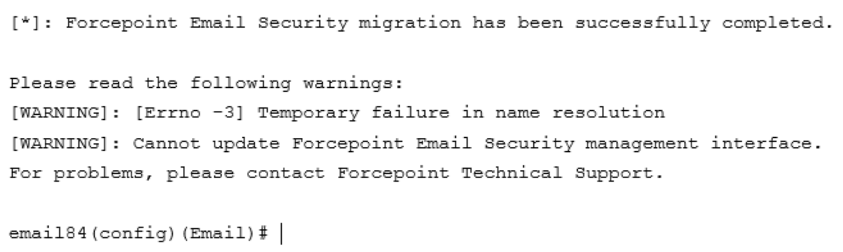
This action is required only if you used the C interface on a hardware appliance that you have migrated.

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 **Settings** > **Personal Email** > **Notification Message** page.
2. Enter the new appliance management (or C) interface in the **IP address or hostname** entry field.
3. Click **OK**.

Update Log Database (for migration only)

If you encounter the following warnings after your upgrade, 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.

email84(config)(Email)# |
```

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 the **esg_device_id**, **admin_manage_ip**, and **device_c_port_ip** from the 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. Execute the following command using the values you obtained in the previous steps:

   ```
   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>'
   ```
7. Enter **GO**.
8. Run the query.