Forcepoint DLP Email Gateway Administrator Help

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

This Administrator Help describes the management component for the Forcepoint DLP Email Gateway virtual appliance. When deployed in a Microsoft Azure environment, Forcepoint DLP Email Gateway allows outbound email from Exchange Online to be analyzed for data loss or theft. Email containing sensitive data can be permitted, quarantined, or encrypted. Sensitive attachments can also be dropped. See Installing Forcepoint Email Security in Microsoft Azure for detailed information about deploying the virtual appliance.

Topics:

Initial Forcepoint DLP Email Gateway configuration

Some initial configuration settings are important for proper Forcepoint DLP Email Gateway operation.

Configure the appliance in the Forcepoint Security Manager

Forcepoint DLP Email Gateway steps

Some initial configuration settings are important for Forcepoint DLP Email Gateway operation. Perform the following activities after you install Forcepoint DLP Email Gateway management components.

1. Log on to the Forcepoint Security Manager and select the tab **Email**.

   The Email module displays.

2. At the prompt, enter your subscription key and click **OK**.

   If you skip this step, you can enter your subscription key later on the page **Settings > General > Subscription**.

3. Register the Forcepoint Email Security DLP Module.

   The DLP Module can be registered at any point, but it is recommended to do this before any other configuration is completed. See *Registering with Forcepoint DLP*, page 9.

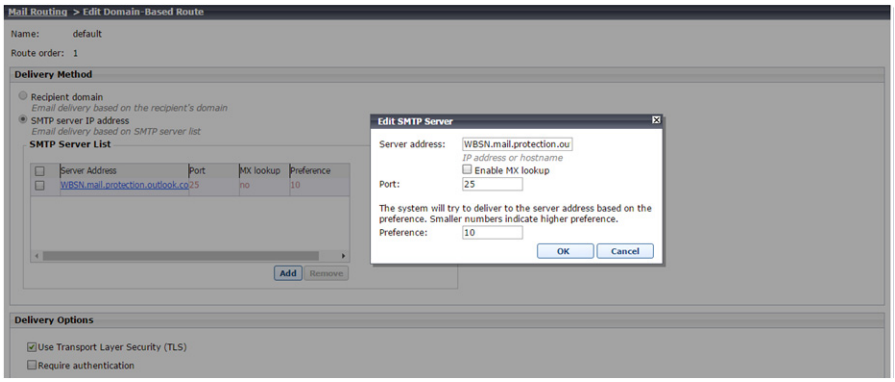
4. Configure the system to send email through Office 365 to Forcepoint DLP Email Gateway.

   a. Navigate to **Settings > Inbound/Outbound > Mail Routing**.

   b. Select the default route.

   c. From Delivery Method, select **SMTP server IP address**.

   d. Under SMTP Server List, click **Add**.



   e. For Server Address, add the FQDN of your organization's Microsoft Office 365 account. This is the same as the MX record of the Office 365-hosted domain. To find it:

      - In the Office 365 Admin Center, select **Settings > Domains**.
      - Select the domain name you configured for your organization.
      - Under Exchange Online, you will see a row for MX. The MX record is listed in that row.

   f. For Port, enter **25**.

   g. Enter a Preference.

   h. Click **OK**.

i. Under Delivery Options, select **Use Transport Layer Security (TLS)**.

j. Click **OK**.

k. Repeat this step for each Forcepoint DLP Email Gateway VM you have.

5. Specify an email address to which system notification messages should be sent. This is typically an administrator address. See *Setting system notification email addresses*, page 14.
6. In the Email module, data loss prevention policies are enabled by default. To manage DLP policies, navigate to **Main > Policy Management > DLP Policies > Manage Policies**.
7. In the Data module, you can view all of the VMs in the System Modules list. Select the Data tab and click **Deploy**.

   Click **Help** on any Forcepoint Security Manager page for help about the page. See Forcepoint DLP Administrator Help for complete information about the DLP Module.

Forcepoint Security Manager steps

These steps are necessary if you have existing DLP policies.

1. From the Forcepoint Security Manager, select the tab **Data**.
2. Add the network email destination to any existing policies that should be used for this appliance.
3. Click **Deploy**. No other configuration steps are required.

The Forcepoint DLP Email Gateway module is shown on the System Modules page, as well as System Health and System Logs.

Use the System Modules page to edit the display name or description for the appliance. If desired, you can balance the load on the gateway by selecting **System Modules > Load Balancing** and then editing the Forcepoint DLP Email Gateway module.

Refer to Forcepoint DLP Administrator Help for more information.

Viewing subscription information

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

You should receive a subscription key when you purchase Forcepoint DLP Email Gateway.

If you did not enter the subscription key the first time you opened the Email Security module, enter it on the page **Settings > General > Subscription**. This subscription key can be entered in one appliance and is applied to all the appliances controlled by the Email Security module.

Enter a new key any time you receive one to update your subscription. If your subscription includes the Forcepoint Email Security Hybrid Module, you must register

with the email hybrid service every time you enter a new subscription key to establish the connection and synchronize email protection system functions. After you enter a valid subscription key, the expiration date and number of subscribed users are displayed. Purchased subscription features appear in the Subscribed Features list.

There are two different license modes: Forcepoint Email Security and Forcepoint DLP Email Gateway. Forcepoint DLP Email Gateway is an alternative to Forcepoint Email Security and provides capability to analyze inbound or outbound mail for data loss or theft. If you use Forcepoint DLP, you can add a subscription key to register Forcepoint DLP Email Gateway. It is not possible to deploy Forcepoint DLP Email Gateway concurrently with Forcepoint Email Security.

If you enter a new subscription key for a different license mode, the email protection system automatically reloads the configuration to provide access to the functionality available with the subscription. All menu options are available with a new installation of Forcepoint Email Security. If you register a new Forcepoint DLP Email Gateway license, the email protection system automatically updates to allow access to Forcepoint DLP Email Gateway menu options. See *Forcepoint Email Security versus Forcepoint DLP Email Gateway*, page 5, for a comparison table of the menu options available in each product.

Add subscription key

1. Navigate to the page **Settings > General > Subscription**.
2. In the field **Subscription key**, enter the subscription key.
3. Click **OK**.

   If this is a changed subscription rather than a new installation, Forcepoint Email Security automatically reloads configuration. The dialog box Reload System Configuration displays with a countdown to the reload. After the system reloads, the menu options change according to the license mode.

   A success message displays at the top of the Subscription page. The expiration date and number of subscribed users display below the subscription key. Purchased subscription features display in the Subscribed Features list.

   When a subscription key is added for Forcepoint DLP Email Gateway, DLP policies are applied by default to inbound and outbound traffic. See *Enabling data loss prevention policies*, page 28.
4. (*Optional*) Mark the check box **Block incoming email connections when subscription expires**.

   Functionality blocks inbound email traffic when your subscription expires. Selecting this option also blocks inbound connections when your email protection system has not had a successful database download in two weeks. This function is disabled by default.

   A valid subscription includes a grace period of two weeks in which to renew your product licenses after the subscription expires. Alerts are sent daily during the grace period as a reminder that the subscription has expired.
5. (*If your subscription key includes Forcepoint Email Security Hybrid Module*) Navigate to the page **Settings > Hybrid Service > Hybrid Configuration**.

Register with the email hybrid service to establish the connection and synchronize email protection system functions. See the topic titled Registering the Email Security Hybrid Module in Forcepoint Email Security Administrator Help.

Forcepoint Email Security versus Forcepoint DLP Email Gateway

The following table details the menu options available in Forcepoint Email Security and Forcepoint DLP Email Gateway.

Menu	Email Security	DLP Email Gateway
Status	• Dashboards • Alerts • Logs • Presentation Reports • Real-Time Monitor	N/A
Message Management	• Blocked Messages • Delayed Messages • Message Queues	N/A
Policy Management	• Policies • Filters • Actions • Always Block/Permit	• Policies • Filters (Disclaimer filter only)
General	• Subscription • Email Appliances • Cluster Mode • System Settings • Backup/Restore • Database Downloads • Proxy Server • URL Analysis • Advanced File Analysis • Data Loss Prevention • SIEM Integration	• Subscription • Email Appliances • System Settings • Data Loss Prevention
Administrators	• Delegated Administrators • Roles	N/A
Users	• User Directories • Domain Groups • User Authentication	• Domain Groups

Menu	Email Security	DLP Email Gateway
Inbound/Outbound	• Mail Routing • Connection Control • True Source IP • IP Groups • Relay Control • Message Control • DKIM Settings • DMARC Settings • Directory Attacks • Exceptions • Non-Delivery Options • Encryption • Enforced TLS Connections • TLS Certificate • Address Rewriting • URL Sandbox • Phishing Detection • Traffic Shaping	• Mail Routing • IP Groups • Relay Control • Exceptions • Encryption
Hybrid Service	• Hybrid Configuration • Hybrid Service Log Options	N/A
Personal Email	• General Settings • Notification Message • User Accounts • End-User Portal • SSL Certificate	N/A
Alerts	• Enable Alerts • Alert Events	• Enable Alerts
Reporting	• Log Database • Log Server • Preferences	• Log Database

Navigating the Forcepoint Security Manager Email Security module

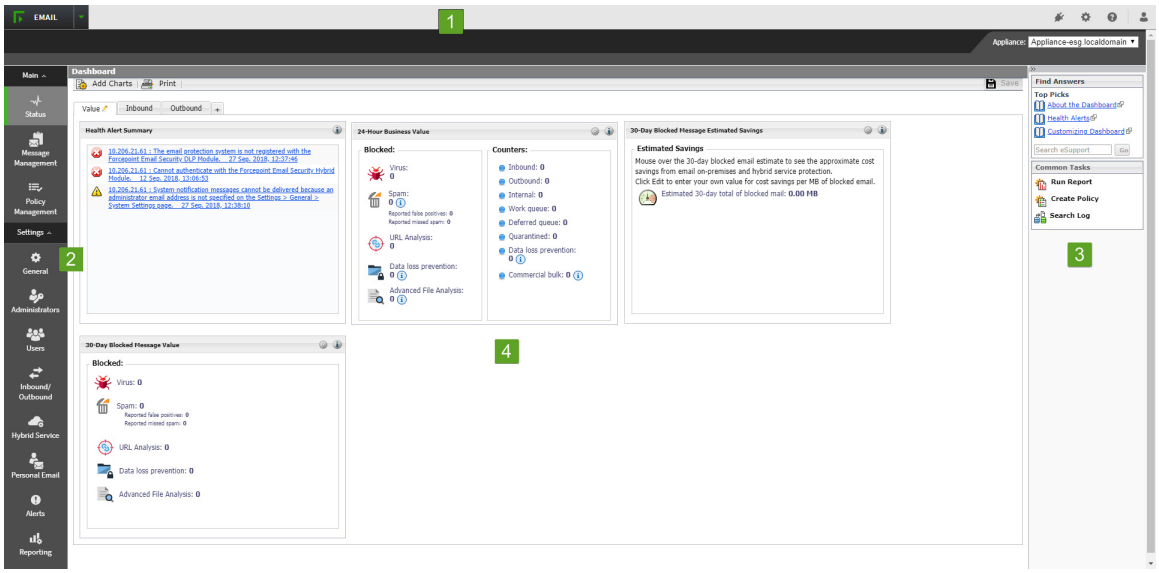
Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The Email Security module user interface can be divided into four main areas:

- The Security Manager toolbar
- The left navigation pane
- The right shortcut pane

- The context pane

The following image displays the user interface for Security Manager version 8.5.4:



1. Security Manager toolbar
2. Left navigation pane
3. Right shortcut pane
4. Content pane

Forcepoint Security Manager toolbar

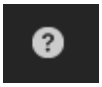
The Forcepoint Security Manager toolbar displays across the top of the Forcepoint Security Manager and provides:

- Access to the Security Manager product modules
- Icons to access the Manage Appliances and Global Settings pages
- An icon to access product Help information
- The status for your current logon account; i.e., Administrator or Super Administrator
- A Log Off button, for ending your administrative session

The module tray is used to launch the Data Security module of the Security Manager. Click **Data** to open that module.

An Appliances icon in the module tray opens a Manage Appliances window, which lets you add and remove an appliance in your system.

Help options



The Help icon provides access to Explain This Page context-sensitive Help, complete Help system contents, and the Forcepoint Support Portal.

Access Explain This Page

1. From the Security Manager banner, click the icon **Help**.

   The Help options display.
2. Click **Explain This page**.

   A new tab displays, showing the Help topic for the current page of the Forcepoint Security Manager.
3. (*Optional*) From the Help topic, click **Open topic with navigation**.

   The complete Help system displays.

Left navigation pane

The left navigation pane, just under the module tray, provides access to two groups of menu items: Main and Settings.

The Main menu is used to access policy management features and functions. The Settings menu is used to perform system administration tasks. Individual configuration pages are accessed from the menu items. The toolbar also includes a pull-down menu of system appliances.

Right shortcut pane

The right shortcut pane contains a Find Answers portal that may include links to topics related to the active screen. The search function can be used to find relevant information in the Forcepoint Support Portal.

Use Find Answers portal

1. From the Common Tasks section of the right shortcut pane, click a link.

   A new tab displays, showing the Help topic for the selected item.
2. (*Optional*) In the field **Search eSupport**, enter search terms and click **Go**.

   A new tab displays, showing the search results from the Forcepoint Support Portal.

Access common tasks

- From the Common Tasks section of the right shortcut pane, click an item.

  The page on which the selected task performs displays.

Minimize the right shortcut pane

1. From the top of the right shortcut pane, click the double arrow icon (>>).

   The right shortcut pane minimizes.
2. Reopen the right shortcut pane; click the double arrow icon (<<).

The right shortcut pane opens.

Registering with Forcepoint DLP

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

With Forcepoint DLP Email Gateway, your email can be analyzed for regulatory compliance and acceptable use and protect sensitive data loss via email by enabling DLP policies on the page **Main > Policy Management > Policies**. Data loss prevention policies are enabled by default.

See *Enabling data loss prevention policies*, page 28, for more information about activating DLP policies.

Email DLP policy options are configured in the Security Manager Data Security module (**Main > Policy Management > DLP Policies > Manage Policies**). A new policy wizard provides the steps for creating a new email DLP policy. See Forcepoint DLP Administrator Help.

If you plan to use email encryption functions, you must configure an email DLP policy with an action plan that includes message encryption. See Forcepoint DLP Administrator Help.

You must register email appliances with Forcepoint DLP in order to take advantage of its acceptable use, data loss prevention, and message encryption features. Registration is automatic with a valid Forcepoint DLP subscription key. See subscription information in the Data Security module. Subsequent appliances are registered when you add them to the Security Manager from the Email Security module.

If the Status field in the Email Security module **Settings > General > Data Loss Prevention** page displays **Unregistered**, you must manually register with Forcepoint DLP. The following steps detail how to manually register an appliance manually with Forcepoint DLP:

Manually register the DLP module

1. From the pull-down menu Communication IP address, specify the IP address used for communication with the email protection system.

   Note

   If you are running Forcepoint Email Security in Azure, you must use the C interface IP address, as Forcepoint Email Security in Azure only supports a single interface.

   The appliance IP address is the one assigned to the virtual appliance by the cloud service.

2. Select the registration method **Manual**.

   The Properties entry fields are enabled.

3. Specify the following data management server properties:
   - IP address
   - User name
   - Password
4. Click **Register**.
5. To complete the process, you must deploy DLP policies in the Data Security module; click the Data Security module and then click **Deploy**.

Important
Wait until DLP policies are completely deployed before you register another appliance.

Configuring email system alerts

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

Your email protection system can notify administrators via an email message that various system events have occurred. Use the page **Settings > Alerts > Enable Alerts** to enable and configure this notification method.

Enable email alerts

1. From the Security Manager, navigate to the page **Settings > Alerts > Alert Events**.
2. From the section Email Alerts, mark the check box **Enable email alerts**.

   Selection indicates to deliver alerts and notifications to administrators by email.
3. In the text fields, configure the following settings:
   - **From email address**

     Email address to use as the sender for email alerts.
   - **Administrator email address (To)**

     Email address of the primary recipient of email alerts. Each address must be separated by a semicolon.
   - **Email addresses for completed report notification**

     Email addresses for recipients of completed report notifications. Each address must be separated by a semicolon.
4. Click **OK**.

   Email alerts are enabled.

Setting system preferences

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The page **Settings > General > System Settings** is used to configure the following email system preferences:

- *Entering the fully qualified domain name*
- *Setting the SMTP greeting message*
- *Setting system notification email addresses*

Entering the fully qualified domain name

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The Fully Qualified Domain Name (FQDN) section of the System Settings page is used to define the FQDN. SMTP protocol requires the use of FQDNs for message transfer. Enter the appliance fully qualified domain name in the **Fully Qualified Domain Name** field (format is appliancehostname.parentdomain.com).

Important

This setting is important for proper email security system operation. You must replace the default fully qualified domain name entry with the correct appliance name.

An incorrect fully qualified domain name may cause disruptions in email traffic flow.

Setting the SMTP greeting message

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The SMTP Greeting section of the System Settings page is used to define an SMTP greeting. The SMTP greeting message is the response to a connection attempt by a remote server. It can also be used to indicate that the system is working properly. For example, an SMTP greeting could be:

```
The email security service is ready.
```

Enter the SMTP greeting

1. In the text field SMTP greeting, enter a new start-up message
2. Click **OK**

   The settings are saved.

Setting system notification email addresses

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The System Notification Email Addresses section of the System Settings page is used to define default notification addresses. The email system can automatically send notifications of system events to a predefined address, often an administrator address. When this address is defined, notification messages can also be sent to or from an administrator email address for other events. For example, configuring a notification to be sent to or from an administrator address when a message triggers a filter requires the administrator address to be defined on the page System Settings.

Define system notification email addresses

1. In the text field Administrator email address, enter the desired recipient address for notifications of system events
2. In the text field Default sender email address, enter the desired sender address from which user notification messages should be sent
3. Click **OK**

   The settings are saved.

Managing appliances

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

Before adding an appliance to Forcepoint DLP Email Gateway, it is necessary to created a virtual appliance in the cloud service and performed initial configuration steps for the appliance. See the Forcepoint DLP installation guide for detailed installation and configuration information.

Beginning with version 8.5, Forcepoint DLP Email Gateway may be deployed on a virtual appliance in Microsoft Azure. See Installing Forcepoint Email Security in Microsoft Azure for more information.

If you change either the appliance hostname or C interface IP address on the appliance, you must make the same change on the page **Settings > General > Email Appliances**. Forcepoint DLP Email Gateway does not detect this change automatically.

Appliances overview

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

You can manage multiple email appliances from the page **Settings > General > Email Appliances** without having to log on to each machine separately. Forcepoint DLP Email Gateway appliances operate in standalone mode.

The Email Appliances page lists all current system appliances in a table that displays information about the appliance and its status, as well as functionality to switch to a

different appliance that is in standalone mode or to remove an unconnected primary appliance from a cluster. The following table details the functionality on the Email Appliances page:

Option	Description
Hostname	Displays the hostname of the appliance. Selection displays the Edit Appliance page for editing the IP address.
Platform	Displays the appliance platform.
C/E1 interface IP address	Displays the appliance C/E1 interface IP address.
System Connection Status	Displays the appliance connection status.
Mode	Displays the appliance mode.
Action	Displays the actions available for the appliance; N/A, Launch, or Remove. Launch is used to switch to a different appliance; Remove is used to remove an unconnected primary appliance from a cluster. When a primary appliance is removed, all its secondary appliances change to standalone mode. The current and all secondary appliances display "N/A".
Delete	Selection of the appliance and **Delete** removes the appliance from the Email Appliances page. An appliance cannot be deleted that is being accessed by another user. Once an appliance is removed from the list, you cannot manage it from the Email Appliances page.

Add an appliance

1. From the page **Settings > General > Email Appliances**, click **Add**

   The Add Appliance dialog box displays.
2. In the text field C/E1 interface IP address, enter the IP address used for communication with Forcepoint DLP Email Gateway
3. Click **OK**.

   The dialog box closes and the appliance is added to the Email Appliances page.

Important

Changing the C interface IP address of an appliance terminates the appliance connection with Forcepoint DLP Email Gateway. In order to re-establish the connection, the IP address must also be changed on the **Settings > General > Email Appliances**.

When you add an appliance, it is automatically registered with Forcepoint DLP Email Gateway for data loss prevention (DLP). To complete the registration process and deploy DLP policies, click the Data Security module on the Security Manager toolbar and then click **Deploy**.

Editing appliance settings from the appliances list

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The page Edit Appliance is used to edit the appliance C interface IP address. The system connection status and mode cannot be changed on this page.

Edit appliance settings

1. From the page **Settings > General > Email Appliances**, click the hostname of an appliance

   The Edit Appliance page displays.
2. In the text field C/E1 interface IP address, enter the new IP address
3. Click **OK**

   The settings are saved.

Managing domain and IP address groups

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

A collection of domain names or IP addresses can be defined in a single group for use in email functions. For example, you can define a domain name group to establish domain-based delivery options, or you can define an IP address group for which some email analysis is not performed. IP address groups can also be used for the email encryption functions. Domain groups are added and configured on the page **Settings > Users > Domain Groups**; IP groups are added and configured on the page **Settings > Inbound/Outbound > IP Groups**.

You can perform the following operations on domain or IP address groups:

- *Adding a domain group*
- *Editing a domain group*
- *Adding an IP address group*
- *Editing an IP address group*

There are two special default groups of domain or IP addresses:

- Protected Domain group
- Trusted IP Address group

See *Third-party encryption application*, page 22, for information about using the Encryption Gateway default IP address group. Default groups cannot be deleted.

Protected Domain group

The Protected Domain group should contain all the domains that an organization owns and needs the email system to protect. An open relay results when both the sender and recipient addresses are not in a protected domain.

The default Protected Domain group is empty after product installation. Domains may be added to or deleted from the Protected Domain group, but you cannot delete the Protected Domain group itself.

Important

Ensure that the Protected Domain group contains all the domains you want your email system to protect.

An open relay is created when mail from an unprotected domain is sent to an unprotected domain within your organization. As a result, all mail from any domain that is not protected may be rejected.

The Protected Domain group should not be used to configure email delivery routes (on the page **Settings > Inbound/Outbound > Mail Routing**) if you need to define domain-based delivery routes via multiple SMTP servers. See *Domain-based routes*, page 19.

Trusted IP Address group

By default, the Trusted IP Addresses group is populated with all the IP addresses referenced in Microsoft Office 365. IP addresses may be added to or deleted from the Trusted IP Addresses group, but you cannot delete the Trusted IP Addresses group itself. The Trusted IP Addresses group may include up to 1024 addresses.

Trusted IP addresses may include your internal mail servers or a trusted partner mail server.

Mail from trusted IP addresses can bypass some relay controls (**Settings > Inbound/Outbound > Relay Control**).

Note

Mail from trusted IP addresses does not bypass policy and rule application.

Adding a domain group

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The page Add Domain Group is used to add a new domain group.

Add new domain group

1. On the page **Settings > Users > Domain Groups**, click **Add**
   The Add Domain Group page displays.
2. In the field Domain Group Name, enter a name for the new domain group
   This field is required.

3. In the field Description, enter a brief description of the domain group
4. In the section Domain Group Details, add a predefined domain group; from the field Domain address file, click **Browse** and navigate to the desired text file

   The file format should be one domain address per line, and its maximum size is 10 MB. If a file contains any invalid entries, only valid entries are accepted. Invalid entries are rejected.
5. Manually add domain entries; in the field Domain address, enter an individual domain address and click **>**

   The information is added to the Added Domains box on the right. Use wildcards to include subdomain entries (e.g., *.domain.com).
6. Click **OK**

   The settings are saved.

Export a domain group

- From the section Added Domains, click **Export**

  The list of domain address entries in the group is exported to your local drive as a text file.

Remove an entry from the domain group

- From the section Added Domains, select an individual entry and click **Delete**

  The entry is removed.

Editing a domain group

Administrator Help | Forcepoint DLP Email Gateway| Version 8.5.x

The page **Settings > Users > Domain Groups** is used to edit existing domain groups, including adding or removing individual domains or editing the domain group description.

If a domain is in use, you will be asked to confirm any changes that involve the domain.

Edit a domain group

1. From the page **Settings > Users > Domain Groups**, click the domain group name

   The page Edit Domain Group displays.
2. Configure the settings
3. Click **OK**

   The settings are saved.

Adding an IP address group

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The page **Settings > Inbound/Outbound > IP Groups** is used to view and add an IP address group.

Add a new IP address group

1. On the page **Settings > Inbound/Outbound > IP Groups**, click **Add**

   The Add IP Group page displays.
2. In the field IP Address Group Name, enter a name for the new IP address group

   This field is required.
3. In the field Description, enter a brief description of the IP address group
4. In the section IP Address Group, add a predefined IP address group; from the field IP address file, click **Browse** and navigate to the desired text file

   The file format should be one IP address per line, and its maximum size is 10 MB

   Note

   The default Encryption Gateway IP address group supports only the entry of individual IP addresses. Subnet address entries are considered invalid and are not accepted for this IP address group.

   Subnet addresses may be entered for other default and custom IP address groups.
5. Manually add IP address entries; in the field IP address, enter an individual IP address and click **>**

   The information is added to the Added IP Addresses box on the right.
6. Click **OK**

   The settings are saved.

Export an IP address group

- From the section Added IP Addresses, click **Export**

  The list of IP address entries in the group is exported to your local drive as a text file.

Remove an entry from the IP address group

- From the section Added IP Addresses, select an individual entry and click **Remove**

  The entry is removed.

Editing an IP address group

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The page Edit IP Group is used to edit existing IP address groups, including adding or removing individual IP addresses and editing the IP address group description.

If an IP address is in use, you will be asked to confirm any changes that involve that address.

Edit an IP address group

1. From the page **Settings > Inbound/Outbound > IP Groups**, click the IP address group name

   The Edit IP Group page displays.
2. Configure the settings
3. Click **OK**

   The settings are saved.

Configuring relay control options

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

You can prevent the unauthorized use of your mail system as an open relay by limiting the IP address groups for which your server is allowed to relay outbound mail. Configure relay control settings on the page **Settings > Inbound/Outbound > Relay Control**.

In the Outbound Relay Options section, select the relay setting for senders in protected domains when SMTP authentication is not required. Default setting is **Allow relays only for senders from trusted IP addresses**. When you use this option, the sender domain must be included in the Forcepoint DLP Email Gateway Protected Domains group (**Settings > Users > Domain Groups**).

Allowing all outbound relays may create a security vulnerability in your system.

Configuring delivery routes

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

Configure domain-based delivery routes on the page **Settings > Inbound/Outbound > Mail Routing** page. See *Domain-based routes*, page 19, for details.

Change the order of a domain-based route by marking its associated check box and using the **Move Up** or **Move Down** buttons.

Copying a route

Use the following steps to copy a route on the page **Settings > Inbound/Outbound > Mail Routing**:

1. Select a route in the route list by marking the check box next to its name
2. Click **Copy**

   A new route appears in the route list, using the original route name followed by a number in parentheses. The number added indicates the order that copies of the original route are created (1, 2, 3, etc.).
3. Click the new route name to edit route properties as desired

Removing a route

To remove a route, select the route by marking the check box next to its name and click **Delete**.

The default domain-based route cannot be deleted.

Domain-based routes

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The Protected Domain group defined on the page **Settings > Users > Domain Groups** should not be used to configure delivery routes if you need to define domain-based delivery routes via multiple SMTP servers. Create domain groups that contain subsets of the Protected Domain group for mail routing purposes.

Use the following steps to add a domain-based delivery route on the page **Settings > Inbound/Outbound > Mail Routing**:

1. Click **Add**

   The Add Domain-based Route page displays.
2. In the field Name, enter a name for your new route
3. From the pull-down menu Route order, select an order number to determine the route's scanning order
4. From the pre-defined domains in the pull-down menu Domain group, select a destination domain

   Default is Protected Domain. Information about the domain group appears in the Domain details box.

   To edit your selected domain group, click **Edit** to open the Edit Domain Group page. See *Editing a domain group*, page 16.
5. Select the delivery method:
   - Based on the recipient's domain (using the Domain Name System [DNS])
   - Based on SMTP server IP address designation (using smart host)

     If you select this option, an SMTP Server List opens.

a. Click **Add**

The Add SMTP Server dialog box displays.

b. Enter the SMTP server IP address or hostname and port

c. Mark the check box **Enable MX lookup** to enable the MX lookup function

Important

If you entered an IP address in the previous step, the MX lookup option is not available.

If you entered a hostname in the previous step, this option is available.

- Mark the check box **Enable MX lookup** for message delivery based on the hostname MX record.
- If you do not mark this check box, message delivery is based on the hostname A record.

d. Enter a preference number for this server (from 1–65535; default value is 5).

If a single route has multiple defined server addresses, mail is delivered in order of server preference. When multiple routes have the same preference, round robin delivery is used.

You may enter no more than 16 addresses in the SMTP Server List.

6. Select any desired security delivery options:
   a. Enable email traffic to use opportunistic TLS protocol; select **Use opportunistic Transport Layer Security (TLS)**
   b. Ensure that users supply credentials; select **Require authentication**

   Enter the appropriate user name and password in the Authentication Information box. You must use the SMTP server IP address delivery method for users to authenticate.

Configuring message exception settings

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The page **Settings > Inbound/Outbound > Exceptions** specifies how messages that cannot be processed for some reason are handled. Configure message exception settings as follows:

1. Specify whether a message should be delivered when an exception is caused by a data loss prevention policy.
2. To send a notification regarding the unprocessed message, mark the check box **Send notification** to enable the Notification Properties section
3. Specify the notification message sender from the following choices:

- Original email sender

  This is the default.
- Administrator

  If you use this option, you must configure a valid administrator email address on the page **Settings > General > System Settings** (see *Setting system notification email addresses*, page 12).
- Custom

  Specify a single email address in this field.

4. Specify one or more notification message recipients from among the following choices:
   - Original email sender
   - Original email recipient
   - Administrator

     This is the default. If you use this option, you must configure a valid administrator email address on the page **Settings > General > Settings** (see *Setting system notification email addresses*, page 12).
   - User specified; enter one or more email addresses, separated by semicolons, in this field
5. In the text field Subject, specify the subject line of your notification message
6. In the text field Content, enter the body of your notification message
7. Attach the original message to the notification message; mark the check box **Attach original message**

If you do not specify either the delivery option or the notification option, the message that triggered the data loss prevention exception is dropped.

Handling encrypted messages

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

An email content policy configured in the Data Security module may specify that a message should be encrypted for delivery. To encrypt specific outbound messages, you must create an email DLP policy that includes an encryption action plan in the Data Security module (**Main > Policy Management > DLP Policies**).

The following types of message encryption are supported:

- *Mandatory Transport Layer Security (TLS) encryption*
- *Third-party encryption application*

Use the page **Settings > Inbound/Outbound > Encryption** to specify the type of encryption to use.

Mandatory Transport Layer Security (TLS) encryption

TLS is an Internet protocol that provides security for all email transmissions. The client and server negotiate a secure “handshake” connection for the transmission to occur, provided both the client and the server support the same version of TLS.

In the Email Security module, if you select only TLS for message encryption and the client and server cannot negotiate a secure TLS connection, the message is sent to a delayed message queue for a later delivery attempt. Select **Transport Layer Security (TLS)** in the pull-down menu **Encryption method** and the option **Use TLS only (no backup encryption method; message is queued for later delivery attempt)** to use only TLS for message encryption.

If you select TLS for message encryption, you can designate a third-party application as a backup method, in case the TLS connection fails. Specifying a backup option allows you a second opportunity for message encryption in the event of an unsuccessful TLS connection. If both the TLS and backup connections fail, the message is sent to a delayed message queue for a later connection attempt.

Select the option **Transport Layer Security (TLS)** option in the pull-down menu **Encryption method** to enable TLS encryption. Then mark **Use third-party application as backup encryption method** to use that backup method.

Third-party encryption application

The email protection system supports the use of third-party software for email encryption. The third-party application used must support the use of x-headers for communication with the email system.

You can also specify third-party application encryption as a backup encryption method if mandatory TLS encryption is selected. See *Mandatory Transport Layer Security (TLS) encryption*, page 22.

The email protection system can be configured to add an x-header to a message that triggers a DLP encryption policy. Other x-headers indicate encryption success or failure. These x-headers facilitate communication between the email system and the encryption software. You must ensure that the x-header settings made in the Encryption page match the corresponding settings in the third-party software configuration.

X-header settings are entered on the page **Settings > Inbound/Outbound > Encryption**. Select **Third-party application** in the pull-down menu **Encryption method** to configure the use of external encryption software. Use the following steps to configure third-party application encryption:

1. Add encryption servers (up to 32) to the Encryption Server List:
    a. Enter each server’s IP address or hostname and port number
    b. Use the MX lookup feature; mark the check box **Enable MX lookup**
    c. Click the arrow to the right of the Add Encryption Server box to add the server to the Encryption Server List

Delete a server from the list; select it and click **Remove**

2. In the pull-down menu **Encrypted IP address group**, specify an IP address group if encrypted email is configured to route back to the email software

   Default is Encryption Gateway.

3. Configure users to present credentials to view encrypted mail; mark the check box **Require authentication** and supply the desired user name and password in the appropriate fields

   Authentication must be supported and configured on your encryption server to use this function.

4. In the field **Encryption X-Header**, specify an x-header to be added to a message that should be encrypted

   This x-header value must also be set and enabled on your encryption server.

5. In the field **Encryption Success X-Header**, specify an x-header to be added to a message that has been successfully encrypted

   This x-header value must also be set and enabled on your encryption server.

6. In the field **Encryption Failure X-Header**, specify an x-header to be added to a message for which encryption has failed

   This x-header value must also be set and enabled on your encryption server.

7. Select any desired encryption failure options:

   - Mark the check box **Send notification to original sender**
   - In the section Notification Details, enter the notification message subject and content in the appropriate fields
   - Include the original message as an attachment to the notification message; mark the check box **Attach original message**
   - Deliver the message that failed the encryption operation; select **Deliver message**

     This is the default.
   - Do not deliver the message that failed the encryption operation; select **Drop message**

Managing a filter

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

A predefined disclaimer filter is available for Forcepoint DLP Email Gateway. The disclaimer filter automatically adds defined text to the beginning or end of a message. Specify the desired text in the Filter Properties section of the Edit Filter page for the Disclaimer filter. See *Disclaimer filter*, page 24, for information.

Disclaimer filter

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

A primary disclaimer may be written in any language, as long as the email message supports the same character set. The secondary disclaimer must be written in English, to be used when the email does not support the primary disclaimer character set. Disclaimer text can display at the beginning or the end of a message and may be between four and 8192 characters in length. A line break uses two characters.

The default disclaimer filter is combined with the default disclaimer action to form the Disclaimer policy rule.

Configure a disclaimer filter

1. From the section Filter Properties, in the text field Primary disclaimer, enter the text for the primary disclaimer

   A primary disclaimer may be written in any language, as long as the email message supports the same character set. Disclaimer text may be between four and 8192 characters in length. A line break uses two characters.
2. In the text field Secondary disclaimer, enter the text for the secondary disclaimer

   The secondary disclaimer must be written in English, to be used when the email does not support the primary disclaimer character set.
3. From Disclaimer position, click the radio button to specify where the disclaimer should appear in the email, **Beginning of message** or **End of message**
4. Allow message recipients to report a message as spam; mark the check box **Enable Report Spam feature**

   Text boxes are enabled to configure either a rich text or plain text version of the Report Spam disclaimer. The link in the rich text disclaimer sends the recipient to the Personal Email Manager, where the message is automatically reported to Forcepoint as spam. The plain text disclaimer provides a default message with instructions for reporting spam to Forcepoint.
5. Configure additional disclaimer filter settings and click **OK**.

   The disclaimer filter settings are saved.

Managing policies

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

One predefined default policy is available for outbound email, in which the sender address is from a protected domain in your organization and the recipient address is not in a protected domain. This policy cannot be modified.

A data loss prevention (DLP) policy is also available. Data loss prevention policies are configured in the Data Security module of the Forcepoint Security Manager and can only be enabled or disabled in the Email Security module. You need to register

Forcepoint DLP Email Gateway with the Data Security module and click **Deploy** in the Data Security module for the policies to be active.

Enabling data loss prevention policies

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

In addition to creating and enabling a policy that protects your email system from email threats, you can enable DLP policies that can detect the presence of sensitive data in your organization's email and execute appropriate actions to prevent data loss.

Email DLP policies must be configured in the Forcepoint Security Manager Data Security module (**Main > Policy Management > DLP Policies > Manage Policies**). A new policy wizard provides the steps for creating a new email DLP policy. See *Data Security Manager Help* for detailed information.

You should create a DLP policy in the Data Security module to use message encryption. Ensure the policy has an action plan of "encrypt." See *Handling encrypted messages*, page 21, for information about email encryption options.

Data loss prevention policies are enabled by default in the Email Security module. However, the Email Security module must be registered with the Data Security module before the policies are applied to email. See *Registering with Forcepoint DLP*, page 9, for instructions on how to register with the Data Security module.

If you need to enable DLP policies, click the DLP policy name on the page **Main > Policy Management > Policies**, and set the following options in the Edit Policy page:

- **Status:** Enabled or Disabled. Enable or disable the DLP policy. Data loss prevention policies are enabled by default.
- **Mode:** Monitor or Enforce. Select **Monitor** to enable the data loss prevention function to simply monitor your email, and select **Enforce** to apply DLP policies to your email.
- **Notification.** Add a notification to a message when an email attachment to that message has been dropped as a result of a DLP policy.
  1. Mark the check box **Send notification when a message attachment is dropped** to enable the sending of notifications
  2. Enter the notification message text
  3. Determine whether the notification text appears above or below the message body of the mail whose attachment was dropped

Editing a policy

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

Click the outbound policy name on the page **Main > Policy Management > Policies** to edit the default policy. You can change the description of the policy in the Description field, and toggle its status between **Enabled** and **Disabled**.

Edit the disclaimer rule by clicking the link in the Rule Name column of the Rules table. See *Editing a rule*, page 26.

Editing a rule

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

Click **Edit** on the Edit Rule page to open the Edit Filter page. You can perform the following activities on this page:

- Enter or modify the filter description.
- Enter or modify the primary disclaimer text.
- Enter or modify the secondary disclaimer text.
- Specify whether the disclaimer appears at the beginning or end of a message.

See *Disclaimer filter*, page 24.

Configuring Log Database options

Administrator Help | Forcepoint DLP Email Gateway | Version 8.5.x

The Log Database stores appliance configuration and management data. It is not used to store message logs when used with Forcepoint DLP Email Gateway.

Making changes to Log Database settings on one appliance applies those changes to all the appliances in your network.

The Log Database page is divided into six sections, as detailed in the following table. After making changes in any of these sections of the Log Database page, click the **OK** button within the section to save and implement the changes in that section.

Parameter	Description
Log Database Location	Provides options to configure the IP address/instance or hostname/instance of your Log Database server. By default, the Log Database created at installation is entered. See *Configuring the Log Database location*, page 27.
Database Rollover Options	Provides options to specify when you want the Log Database to create a new database partition, a process called a rollover.
Maintenance Configuration	Provides options to configure aspects of database processing, such as the time for running the database maintenance job, some of the maintenance tasks performed, and deletion of database partitions and error logs.

Parameter	Description
Database Partition Creation	Provides options to define characteristics for new database partitions, such as location and size options. This area also lets you create a new partition right away, rather than waiting for a planned rollover.
Available Partitions	Lists all database partitions available for reporting. The list shows the dates covered by the partition, as well as the size and name of each partition. Use this list to control what database partitions are included in reports, and to select individual partitions to be deleted
Log Activity	Displays log activity to review database maintenance status and event and error messages recorded during the jobs run on the Log Database.

Configuring the Log Database location

Use the section Log Database Location on the page **Settings > Reporting > Log Database** to enter the IP address\instance or hostname\instance of your Log Database server. By default, the Log Database created at installation is entered. It must be the IP address assigned to the Log Database when it was added to the VPN. If you chose to encrypt the database connection at product installation, the **Encrypt connection** check box is marked. If you did not select the encryption option during installation, you can encrypt the database connection by marking the check box here.

Other settings created at installation and displayed here include the designated authentication method (Windows or SQL Server), user name, and password.

Determine the availability of the server

- From the section Log Database Location, click **Check Status**.