



Email Security Cloud

Online Help

© 2024 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 20 December 2024

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

1 Getting Started	7
Introduction.....	7
About this guide.....	8
Initial steps.....	8
Logging on and portal security.....	8
Cloud portal navigation.....	10
2 Account Settings	13
Introduction.....	13
My Account.....	14
Configuring SIEM storage.....	14
Contacts.....	16
Custom file types.....	26
Identity Management.....	26
End Users.....	26
Groups.....	27
Licenses.....	28
Administrator single sign-on.....	29
Data Protection Settings.....	31
Important rules for configuring accounts.....	32
3 Working with External Directories	33
Introduction.....	33
What is SCIM?.....	34
How the service works with SCIM.....	34
What is LDAP?.....	34
How the service works with LDAP.....	35
Planning for your first synchronization.....	36
Basic steps.....	39
Cloud portal tasks.....	40
Maintenance.....	45
4 Configuring Email Settings	51
Introduction.....	51
File sandboxing.....	51
DNS records and service IP addresses.....	54
Aliases.....	55
Blocklist and allowlists.....	56
Personal Email Subscriptions.....	56
Email notifications.....	62
Configure block and notification pages.....	65
Image allowlist.....	69
Email connectivity testing.....	70
URL Sandboxing utility.....	72
5 Defining Email Policies	75
Introduction.....	75
General tab.....	76

Domains tab.....	80
Connections tab.....	83
Antivirus tab.....	88
URL Sandboxing tab.....	92
Antispam tab.....	95
Antispoofing tab.....	104
Content Filter tab.....	110
Encryption tab.....	128
Data Protection tab.....	140
6 Message Center.....	143
Introduction.....	143
Understanding your results.....	148
Performing actions on the results.....	149
Viewing message details.....	151
7 End-User Self Service.....	155
Introduction.....	155
Requesting a message report.....	155
Understanding the report.....	157
Accessing quarantined email.....	159
Changing subscription details.....	160
Consolidating email report data.....	162
8 Email Reporting Tools.....	163
Introduction.....	163
Email Report Center.....	163
Legacy Email Reporting.....	174
9 Report Center.....	191
Introduction.....	191
Using the Report Catalog.....	192
Using the Report Builder.....	199
Scheduling reports.....	203
Exporting data to a third-party SIEM tool.....	207
10 Account Reports.....	215
Introduction.....	215
Account Summary report.....	216
Service reports.....	217
Downloading report results.....	219
Saving reports.....	220
Scheduling reports.....	220
11 Audit Trails.....	223
Introduction.....	223
Configuration audit trail.....	223
SCIM audit trail.....	224
Administrator audit trail.....	224
12 Standard Email Configuration.....	227
Introduction.....	227
13 Appendices.....	233

Use Cases for Setting up User Provisioning.....	233
Standard Regular Expression Strings.....	246
Supported File Types.....	248

Chapter 1

Getting Started

Contents

- Introduction on page 7
- About this guide on page 8
- Initial steps on page 8
- Logging on and portal security on page 8
- Cloud portal navigation on page 10

Introduction

Forcepoint Email Security Cloud protects your organization against the threats of malware, spam, and other unwanted content in email traffic.

Forcepoint Email Security Cloud provides maximum protection for email systems to prevent malicious threats from entering an organization's network. Each message is analyzed by a robust set of antivirus and antispam filters to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email.

The following add-on email modules are available in the cloud:

- The Forcepoint Advanced Malware Detection for Email module enables you to:
 - Send suspicious files received in email messages to a cloud-hosted sandbox for analysis
 - Define whether suspected phishing messages should be quarantined, or allowed with suspicious URLs replaced by a link to a block page that you specify
- The Forcepoint Email Security - Encryption Module provides an additional encryption option beyond TLS and manual exchange of passwords, offering identity-based encryption and customization of the email notification that the recipient sees before decrypting the message.
- The Forcepoint Email Security - Image Analysis Module enables you to quarantine messages that have images attached to prevent potentially questionable images from entering your organization. You can also add permitted images to an allowlist.

You configure and manage your services using the Cloud Security Gateway Portal, also referred to in this Help as the cloud portal, or the cloud portal. The portal provides a central, graphical interface to the general configuration, policy management, and reporting functions of your service, making defining and enforcing email security an easy, straightforward process. You maintain control over the system through on-demand statistics and reporting, while powerful self-service tools allow end users to manage quarantined mail, helping relieve the burden on IT staff.

About this guide

This guide is intended for IT administrators who are responsible for setting up and operating Forcepoint Email Security Cloud accounts.

It relates to all Forcepoint Email Security Cloud services, although the functionality available to you depends on licensing.

The layout of the cloud portal screens is similar for all services. Wherever possible this guide indicates where a feature or functionality is specific to a particular service.

Initial steps

Take the following steps to get started with Forcepoint Email Security Cloud.

It is likely that you have already completed these steps. If not, please see the [Forcepoint Email Security Cloud Getting Started Guide](#).

Steps

- 1) Request an evaluation.
- 2) Register for the service.
- 3) Log on to the cloud portal.
- 4) Add inbound and outbound connections.
- 5) Add domains.
- 6) Set up outbound email routing.
- 7) Set up inbound email routing.
- 8) Restrict connections to your mail servers.
- 9) Set up users and groups.

Logging on and portal security



Note

To use the cloud portal, your browser must be Javascript-enabled.

To access the cloud portal, visit <https://admin.forcepoint.net/portal>.

The logon process uses cookies where possible. For the best user experience, we recommend that you accept cookies from the cloud portal. If your web browser is unable to, or is configured not to accept cookies from the cloud portal, an additional screen appears during logon reminding you of the benefits of securing your session.

If the cloud portal cannot use cookies to secure the session, it falls back to ensuring that all requests for the session come from the same IP address. This may cause problems for you if your company has several load-balanced web proxies, because the cloud portal interprets requests coming from several sources as a security breach. Companies with a single web proxy or a cooperating web proxy farm should not be affected.

To avoid problems, we recommend enabling cookies on your web browsers.

Locking down your firewalls

If you have not already done so, we strongly recommend that you follow the advice provided in the Forcepoint Email Security Cloud [Getting Started Guide](#) and restrict connections to your email servers so that they only accept email from the IP address ranges used by Forcepoint. These can be found on the *DNS records and service IP addresses* page.

Related concepts

[DNS records and service IP addresses](#) on page 54

Privacy statement

The cloud portal uses 2 cookies during logon. The first is used to identify whether the user's Web browser is willing to accept and store cookies for the portal; it contains no information. If the first cookie is successfully stored, a second cookie is stored containing temporary information about the session. No personal information is stored in either cookie, and both cookies are used only for the duration of the session.

Idle timeout

For security reasons, if you are logged on to the cloud portal and are inactive for a predefined period, you are automatically logged off. When you next attempt to perform an action, you are asked to log on again. Once you have done so, you are taken to the page that you requested. The inactivity timer is between 30 and 60 minutes.

Customizable landing page

By default, administrators logging onto the portal are taken to the **Account > Licenses** page. To change your landing page:

Steps

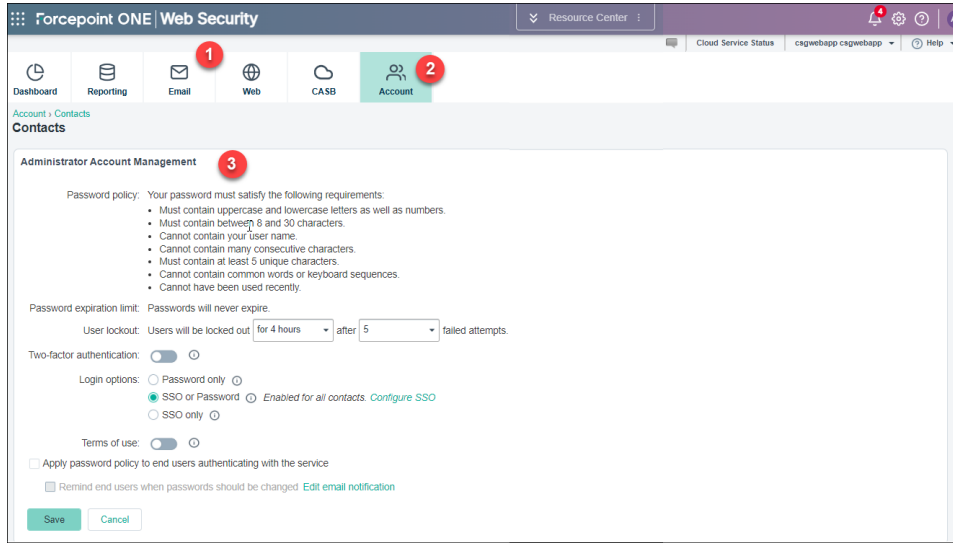
- 1) Navigate to the page you would like to use as your portal landing page.
- 2) Click the arrow next to your logon account name in the banner at the top of the page.

3) Select **Set Landing Page**.

Note that some pages have been deliberately excluded from supporting this option.

Cloud portal navigation

The cloud portal interface can be divided into the following main areas:



1) Banner

2) Toolbar

3) Content pane

The **banner** shows:

- Any **Alerts** that are available for your account.
- A **Cloud Service Status** option that provides a link to the Cloud Operations customer dashboard. Use this link if you are experiencing any kind of pervasive service problem to determine what might be happening and see what steps are being taken to correct the issues.
- Your current **logon account**. When you're ready to end your administrative session, click the arrow next to the administrator name and select **Log Off**.
- The **Help** menu, from which you can access assistance for the page you are currently viewing, further product information, and Forcepoint Technical Support resources.

The Help menu also includes the **Support PIN**. You must authenticate yourself with this PIN when calling Forcepoint Technical Support.

Each PIN is unique per user, and is generated when a user logs on. The PIN is then valid for 24 hours after logon. After a 24-hour period has expired, a new PIN is generated at the next logon.



Important

In order to preserve and maintain the security of your data, support representatives will not be able to provide customer support without an accurate, up-to-date PIN.

The **toolbar** indicates which part of the cloud portal is currently active:

- **Dashboard** provides access to the Forcepoint Email Security Cloud dashboards.
- **Reporting** gives access to all reporting options, including email reports, account service reports, and your saved reports.
- **Email** contains all configuration settings relating to Forcepoint Email Security Cloud, including account-wide email settings, policy management, and the *Message Center*.
- **Account** provides access to configuration options that apply to all cloud services. This includes administrator management, directory synchronization, licenses, and groups.

When you select an item in the toolbar, a **navigation pane** drops down, containing the available navigation choices for that item. Click the toolbar item again to close the navigation pane.

The **content pane** varies according to the selection you make in the navigation pane.

Related concepts

Alerts on page 12

Related information

Message Center on page 143

Dashboard

To view your main email dashboard, go to **Dashboard**. If you are a cloud web and email customer, select the **Email** tab. The dashboard provides a snapshot view of how your cloud email services are performing.

The panels you see depend on your subscription settings. You may see the following:

- **Email Activity Overview** - the number of inbound and outbound email requests processed for your account in the last 7 days.
- **Inbound Composition Categories** and **Outbound Composition Categories** - reports how Forcepoint Email Security Cloud categorized your inbound and outbound email. Composition categories include:

Spam	Messages marked as spam by the Antispam rules.
Valid	Messages that pass analysis or that are in allowlist.
Content	Messages that triggered a Content Filter rule.
Viruses	Messages detected by Antivirus or ThreatSeeker as containing a virus.
Phishing	Messages maliciously designed to acquire information, such as user names, passwords, or credit card information by masquerading as a trusted or well-known entity.
Commercial Bulk	Solicited bulk email, such as newsletters
Backscatter	Maliciously generated bounce messages (e.g., non-delivery report/ receipt (NDR); delivery status notification (DSN); and non-delivery notification (NDN) messages) sent by spammers to spoofed return addresses

Access	Messages to which Notifications and Annotations rules were applied.
Other	Messages flagged for other reasons, such as having a message loop, encryption, or generating a system or operational error.

- **Top 5 Viruses** - indicates the top 5 viruses seen in your account along with the number of email carrying each of these viruses.
- **URL Categories in Email** - indicates how Forcepoint Email Security Cloud classified all of the URLs found in your organization's email.
- **Cloud Email Spam Detection Rate** - from an email flow of know spam messages (separate from all subscriber email flow), indicates the percentage of messages classified as spam by Forcepoint Email Security Cloud analysis. This is a good indicator of the Forcepoint Email Security Cloud spam detection rate.





You have the option of viewing this data in either a bar graph or pie chart.

Alerts

Click the speech bubble icon in the toolbar to see alerts for your account.

Alerts are the primary means of communicating with customers to keep you fully informed of service issues. If you suspect that there may be a problem with the service, log on and check for new alerts. The number of alerts for your account is displayed with the alert icon.

You may see the following alert types:

	Error. Your service has been interrupted, and you must act on this alert immediately.
	Severe. You must act on this alert as soon as possible. If you do not act by the date given in the alert, it will be upgraded to Error and you risk interruption of your service.
	Warning. This alerts you to future events that might affect your service – for example portal outages, or license expiration.
	Information. This might be announcing a new release or upcoming maintenance work.

Select an alert summary in the left pane to see more detail, if available, in the right pane.

Chapter 2

Account Settings

Contents

- Introduction on page 13
- My Account on page 14
- Configuring SIEM storage on page 14
- Contacts on page 16
- Custom file types on page 26
- Identity Management on page 26
- End Users on page 26
- Groups on page 27
- Licenses on page 28
- Administrator single sign-on on page 29
- Data Protection Settings on page 31
- Important rules for configuring accounts on page 32

Introduction

Administrators with account-level privileges can click **Account** in the cloud portal toolbar to see the configuration options that apply to the complete account. The exact options available on the menu depend on the services you are licensed for.

- To change the password for your cloud service administrator account, select *My Account*.
- To view the configuration audit database for your account, select *Audit Trails*.
- Select *Contact* to view and modify the contact details of people in your organization who administer, support, and pay for services. The administrator contacts can be given logon to the portal and their permissions restricted as necessary. You can also use this page to modify your password settings, set two-factor authentication, and display a terms of use page for administrators.
- To set up your own combinations of file types, MIME types, and file extensions for email attachment blocking, choose *Custom file types*.
- Before configuring user provisioning for your account, see *Identity Management*.
- Select *End User* to search for end users so you can enable or disable their Web access, delete them, or change their policy assignments. (This option is available only to accounts enabled for identity management.)
- When you define *Groups*, they are available in all your policies in all services. This allows you to define a consistent set of rules across the services for groups of end users.
- Enable and configure *Administrator single sign-on* to allow administrator access to the cloud portal using a third-party identity provider.
- Configure *Data Protection Settings* to integrate with the Data Protection Service and let that service handle your enterprise data security, including blocking or monitoring data loss.

This chapter covers the configuration of account-level options. To configure the majority of email service options, click **Email** in the toolbar and then select the appropriate setting type or policy.

Related concepts

[My Account](#) on page 14

[Contacts](#) on page 16

[Custom file types](#) on page 26

[Identity Management](#) on page 26

[End Users](#) on page 26

[Groups](#) on page 27

Related tasks

[Administrator single sign-on](#) on page 29

[Data Protection Settings](#) on page 31

Related information

[Audit Trails](#) on page 223

My Account

Use the My Account page if you need to change your password or generate a new one. Enter and confirm a password, then click **Submit** when done. The password must conform to your password policy, as described on the screen.

Optionally, you can also change your password question. Select a question from the drop-down list, then enter an answer to the question and click **Submit**.

See *Changing passwords* for more information about passwords.

Related concepts

[Changing passwords](#) on page 22

Configuring SIEM storage

Use the **Account > SIEM Storage** page to configure the storage options for SIEM output generated on the **Reporting > Account Reports > SIEM Integration** page. (See *Exporting data to a third-party SIEM tool* for additional information.)

Click the radio button next to the **Storage type** you wish to use for SIEM output. SIEM data can be stored by **Forcepoint** or you can **Bring your own storage**. If **Forcepoint** is selected (the default selection), no further configuration is required. If **Bring your own storage** is selected, follow the instructions provided to add and test up to 5 storage devices to the **Storage List: Bring Your Own** table and activate a specific device.

Note that the same storage selections are used for each data type (Web Security or Email Security).

AWS is selected, by default, as the storage solution. To add storage options to the Storage List:

Steps

- 1) Create one or more AWS S3 buckets on the AWS portal.
Note that bucket names must be globally unique.
Encryption for the AWS S3 buckets is not supported.
- 2) Click **Add** to add your bucket to the table.
 - a) Enter the **Bucket name** from the AWS portal. See [this site](#) for details on valid bucket names.
 - b) A **Prefix** is optional.
 - Add text that will be used as a prefix to each data file created when SIEM data is exported.
 - Enter a '/' to create a folder where the data files will be stored. If no '/' is included, the prefix is prepended to the file name.Valid prefix values are SIEMData, log_files/, or traffic-logs. More information can be found [here](#).
 - c) Click **Save** when you have finished. The bucket information is added to the table.

Click the bucket name in the table to open the **Edit Bucket** page and make changes.
Delete an inactive bucket by clicking **Delete** on the **Edit Bucket** page.
- 3) In the table, click the **JSON** link in the row for the bucket you just added.
 - a) On the **Bucket Policy** page, click **Copy Text** to copy the contents of the JSON pane to a clipboard.
 - b) In the AWS Management Console, open the **Bucket policy editor** on the **Permissions > Bucket policy** tab of the AWS S3 Bucket Policy and paste the contents of the JSON pane.
 - c) On the **Bucket Policy** page, click **BACK** when you have finished with the page.
- 4) In the table, click **Check connection** to test the connection to the S3 bucket in your account. If the connection is successful, a token file is written in order to confirm that files can be written to the bucket. The token number then appears in the connection_token object in the AWS S3 bucket (on the AWS Management Console). If a folder was created based on the contents of the prefix for the bucket, the connection_token appears in that folder.
The generated token is valid for 3 hours. After that time, a new token must be generated.
 - a) On the **Check Connection** page, paste the token number from the connection_token object.
 - b) Click **Check Connection** to confirm that files written to the AWS S3 bucket can be read.
If more than 20 connection attempts are made within 60 minutes, the account will be locked for an hour.
 - c) Click **Back** when you are finished.
- 5) The **Status** column displays with a green check if the token is confirmed. When the check mark appears, the bucket can be enabled for SIEM storage.

- 6) A single bucket must be selected as **Active**. SIEM data is exported to the active bucket. If **Bring you own** has been enabled but there is no active bucket, **Save** is not enabled, and the **Enable data export** switch on the **Reporting > Account Reports > SIEM Integration** page cannot be set to On.
- 7) Click **Save** to save all of your changes. If **Storage type** is changed from **Forcepoint** to **Bring your own** after Forcepoint storage has been in use, any data files that have not been downloaded will be transferred to the configured active bucket.
Metrics at the bottom of the page provide details on the status of SIEM data files. The specific metrics provided are determined by the **Storage type** selection. Use the **Refresh Metrics** button to update the displayed values.

Related tasks

[Exporting data to a third-party SIEM tool](#) on page 207

Contacts

Use the **Contacts** page to define the password policy for administrators in your account, and to manage the contact list and administrator logons.

The Account Management area displays the current requirements for passwords in your account, as well as any expiration limit. For more information, see *Password settings*.

The contact information in the **Contacts** area is created with the details supplied during enrollment. The initial contact assumes the role of master user, a super administrator with the highest rights and privileges for your account.

Forcepoint Support uses the contact details defined on this page should they need to contact you. You can specify multiple contact addresses and numbers for each contact, plus a call order that specifies the order in which each contact method should be attempted.



Note

If the contact also has logon privileges, you must enter an email address to enable them to use the password reset function, if required.

It is your responsibility to administer the logon privileges for the contacts in your account, and to ensure access to the cloud portal is maintained or protected as appropriate. You are also responsible for any actions taken by the users of the administrator logon that you create.

Related concepts

[Password settings](#) on page 20

Adding a contact

To add a new contact:

Steps

- 1) Click **Add**.
- 2) Select the new contact's **Title**, and enter the first name and surname. The **Full name** field is automatically populated.
- 3) Select the **Contact type** from the drop-down list.
- 4) Optionally, enter further details for the contact, including the job title, department, and address.
- 5) Enter a telephone number, email address, or both. It is recommended that you provide at least one form of contact that Support can use if required.
- 6) Select a preference for each contact method, to inform Support of the preferred order in which to attempt each contact method.
- 7) Click **Submit**.

Adding logon details

To assign logon privileges to the contact you just created:

Steps

- 1) In the **User name** field, click the hyperlink in **No user name. Click here to add one**. This opens the Add User Name screen.



Note

You can also access this screen by clicking the contact's logon ID in the User Name column on the main Contacts screen.

- 2) By default, the email address is used as the contact's logon ID. To change this, edit the User Name field.
- 3) Enter and confirm a password for the user.
You can type a password for the user and confirm it. Alternatively, if you want to automatically generate a password that complies with the password policy, click **Create a password for me**. The password, which meets the stated password policy, populates into the Password field.
- 4) Define when the user's password should expire. By default this uses the expiration settings defined as part of your account's password policy (see *Password expiration limit*).
- 5) To force the user to change the password when they log on, mark **Change password next log on**. This is recommended.

Next steps

When the user first logs on, a screen is displayed giving them 8 days to select a password question from the list provided and enter an answer. This password question and answer is used if the user later forgets their password

(see *Forgotten passwords*). If the user does not set a password question within the 8-day limit, they are forced to do so at their next logon



Note

If you have enabled two-factor authentication for a user, this page can be used to reset authentication for users who have been locked out, or who are unable to use their authenticator app. Click **Reset** beside the Two-factor authentication label to require the user to configure authentication again. See *Two-factor authentication*.

This page also displays the date and time of the user's last successful and unsuccessful logon, if available.

Related tasks

[Password expiration limit](#) on page 21

[Forgotten passwords](#) on page 22

[Two-factor authentication](#) on page 23

Configuring permissions

By default, all rights are assigned to the master user (the initial contact established in your account, with super administrator privileges). When the master user creates a new user, by default only the **View All Reports** permission is assigned to that account. This is the minimum permission a user needs to be able to log on; it grants permissions over only the Reporting tab on the main menu bar.

We provide flexible users' rights so you can create a hierarchy of administrators. For example, much of the functionality accessed from the portal is useful for help desk agents to aid with problem isolation; but they do not necessarily require control over policy configuration.

Likewise, you should assign Directory Synchronization privileges to the contact you set up for the Directory Synchronization Client (see *Set up authentication (Directory Synchronization only)*), but no-one else should need this privilege.

Permissions are granted at an account and policy level. This lets you create multiple policies, and administrators can control their own policy but no one else's.



Note

Visibility for some account and policy permissions depends upon the permission being assigned to your administrator account. If your administrator account does not have full account level permissions, you are only able to view or modify settings for policies you have been explicitly given permissions to. For example, full account level permission is required to access the **Global Custom Category** list.

To modify an administrator user's permissions:

Steps

- 1) On the **Account > Contacts** page, click the name of the user whose permissions you want to edit in the **User Name** column of the Contacts table (not the Full Name column).
- 2) Click **Edit**.

- 3) Under **Account Permissions**, mark or clear check boxes to add or remove permissions. Refer to the list below for more information about each permission set.
- 4) Use the Policy Permissions table to add or remove policy, audit trail, and related permissions.
 - Refer to the list below for information about each permission set.
 - To refine policy-level permissions, click **Advanced**.

**Note**

The **Advanced** button does not show for contacts with Manage Users permissions, because their selected permissions will apply to all policies.

- 5) When you are finished, click **Save**.
The following are account-level permissions:

- **Manage Users**: view, create, edit, and remove user logons and permissions
- **Directory Synchronization**: synchronize an LDAP directory with the cloud service
- **View All Reports**: run all reports associated with the licensed services
- **Manage edge devices**: configure edge devices in the network that connect to the cloud service (see *Managing Network Devices*)

or download full traffic logs, if Full Traffic Logging The following email permissions can be assigned at the account or policy level:

- **Modify Configuration**: modify all options within Account Settings except users' logons—for this, the user must have **Manage Users** permissions.
- **View Configuration**: view all configurations within Account Settings without the ability to make changes
- **View Configuration Audit Trail**: access and search the policy setup audit trail, and access the blocklist and allowlist search facility
- **Quarantine Administration**: use Message Center to search quarantined messages, plus the ability to perform actions on the messages
- **View Quarantine**: use Message Center to search quarantined messages, without the ability to perform any actions on the messages
- **View Administrator Audit Trail**: access and search the Message Center audit trail, and access the blocklist and allowlist search facility
- **View Quarantined Images**: access and search the Message Center for quarantined images (“View Quarantine” must also be enabled to use this option.)
- **View Delivered Messages**: same as “View Quarantine,” but the user can view message logs as well as quarantined email
- **Block and Allow Lists**: access, search, and manage all blocklists and allowlists
- **View Filtered Reports**: view only reports that can be filtered by the specified policy or policies (not available if View All Reports is selected)

**Note**

The View Filtered Reports option may not be enabled in your account.

If users are logged on to the portal when their permissions are changed, the changes do not take effect until they log off and then log on again.

Related tasks

[Set up authentication \(Directory Synchronization only\)](#) on page 43

Password settings

Click **Account > Contacts > Edit** to define password settings for your account. On this screen, you can define an expiration limit for your users, set the user lockout option, and set two-factor authentication for all users. If you have more than one password policy (a policy that defines how “strong” your users’ passwords must be), you can also choose which policy to use.

If available in your account, you can also use the selected password policy for your end users. Select **Apply password policy to end users authenticating with the service** (not available to Forcepoint Web Security Hybrid Module customers) to impose the same password requirements for any end users who are registered for the service and using manual authentication, including the minimum and maximum length and restrictions on using previous passwords. If you have also defined a *Password expiration limit*, you can select **Remind end users when passwords should be changed** to send an email reminder to end users when they need to change their passwords.

**Note**

Password policies for end users is a limited-availability feature and may not be enabled in your account.

Click **Update** when you’re finished making your selections.

Note that you can override these settings for individual users on their permissions settings screen.

Related tasks

[Password expiration limit](#) on page 21

Password policy

A password policy defines how “strong” your users’ passwords are required to be. (A strong password is a secure password.) The password policy in the cloud portal sets the minimum length, maximum length, password history, sequence rules, and unique character rules of a user’s password.

Following are the minimum requirements:

Parameter	Default policy value
Minimum length	8
Maximum length	30
Password history size (number of former passwords to check)	3
Maximum number of characters in sequence	4
Minimum number of unique characters	5

In addition, passwords:

- Cannot contain the user's logon ID
- Cannot contain common words or keyboard sequences
- Must include uppercase letters
- Must include lowercase letters
- Must include numbers

Password expiration limit

We recommend that you require users to change their passwords on a regular basis. Passwords can be set to automatically expire after a set number of days. You can override this setting for individual users on their Login details screen (see *Adding logon details*).

Steps

- 1) Navigate to **Account > Contacts**.
- 2) Select a **Password expiration limit** setting. If you select No, passwords will never expire (not recommended). If you select Yes, a drop-down menu allows you to set the number of days after which passwords will expire.
From the menu, select one of the following as the expiration period: 30, 60, 90, 120, 180 days, or Custom days. If you select **Custom days**, a new field appears so you can enter any number of days you want. Periods longer than 365 days are not supported.
- 3) Click **Save**.

Related tasks

[Adding logon details](#) on page 17

User lockout

If a user enters an incorrect password when attempting to log on, they have a limited number of further attempts before they are locked out for a period of time. You set up the number of further attempts and the lockout time period on the main setup screen for the user.

Steps

- 1) On the **Contacts** screen, click **Edit**.
- 2) From the **User lockout** drop-down list, select a lockout time period. The options are 15 minutes, 1 hour, 4 hours, 24 hours, or Forever.
If you select **Forever**, an administrator with Manage Users permissions must unlock the user account before the user can log on again.
- 3) Select the number of permitted failed attempts from the drop-down list. This can be between 3 and 10.
- 4) Click **Update**.

Unlocking user accounts

If a user is locked out because they failed to enter the correct password after the allotted number of attempts, an administrator with Manage Users permissions can unlock the user account before the lockout time period has ended. If the lockout time period is set to **Forever**, the user must be unlocked by an administrator.

Steps

- 1) Select **Account > Contacts**
- 2) In the User Name column of the contact list, click the required user name.
- 3) Click **Edit** on the User screen.
- 4) Click **Unlock**.
- 5) Click **Submit**.

Changing passwords

Users are required to change passwords when they expire or when a change is forced by an administrator. Only administrators with Manage Users permissions can force a user to change his or her password. To force a change, select the **Change Password next logon** box on the user's contact screen. When users are required to change their passwords, they see a Change Password screen the next time they log on.

Users can also opt to change their password from **Account > My Account**, which displays the same Change Password screen.

If a user creates a password that does not meet the password policy standards, they receive an error message and are asked to try again. For example:

This password has been used recently. Please try another.

To implement the changed password, users should click **Save**. They should also make note of the password for future reference.

Forgotten passwords

If a user forgets their password, they can click the **Forgot your password?** link on the logon screen and follow the instructions to reset the password:

Steps

- 1) The user enters their portal user name and clicks **Submit**.
- 2) The cloud service sends an email to the email address listed in the contact details associated with that user name.



Note

If the email address set up for the user name on the Contacts page is out of date or invalid, the user must contact their administrator to get their password reset.

- 3) The user clicks the link in the email to go to a secure page.
- 4) The user enters the answer to their password question, and clicks **Submit**.
- 5) When the question is answered correctly, the user can enter and confirm a new password. They also have the option to change their password question.



Note

If a user forgets the answer to their password question, they must contact their administrator to get their password reset.

Next steps

Should you need to generate a new password for a user, follow these steps:

- 1) Go to **Account > Contacts**.
- 2) In the User Name column of the contact list, click the required user name.
- 3) Click **Edit** on the User screen.
- 4) Click **Create a password for me**.
- 5) Make note of the password.
- 6) Click **Submit**.

Two-factor authentication

Two-factor authentication (also known as 2FA) provides an additional level of security for administrator access to the cloud portal. When this setting is applied, all portal users using a password to sign in are required to enter both their password and a code generated by an authenticator app.

To enable two-factor authentication for all portal users:

Steps

- 1) Go to the **Account > Contacts** page.
- 2) Toggle the **Two-factor authentication** switch to **ON**.

3) Click **Save**.

The next time portal users log on, they will be prompted to set up two-factor authentication.



Note

Compatible authenticator apps are available for Android, iOS, Blackberry, and Windows Phone. Desktop and browser-based apps are also available for Microsoft Windows, Mac OS, and Linux. This feature is validated with the Microsoft Authenticator app, but alternative apps that use the Time-based One-time Password Algorithm (TOTP) protocol, such as Google Authenticator, are also supported.

Logging on with two-factor authentication

When two-factor authentication is enabled for your account, all administrators require an authenticator app to access the portal. This app must be configured before the user can log on.

When users log on with two-factor authentication for the first time (or after their account has been reset), a setup wizard guides them through the configuration process. In the wizard, portal users who do not already have an authenticator app are given instructions for downloading Microsoft Authenticator.

During the setup process, portal users are prompted to:

Steps

- 1) Select a supported authenticator app.
- 2) Set up the app by scanning a QR code shown on the screen or by manually entering a secret key.
- 3) Enter the 6-digit code shown on the authenticator app.

Next steps

Once setup has been completed successfully, users are logged on to the portal.

Each time users subsequently log on with their password, they are also prompted to enter the code displayed on their authenticator app. Users have 3 attempts to enter a valid code before being asked to re-enter their password.

Resetting two-factor authentication for a portal user

For portal users who have been locked out, or who cannot use their authenticator app (for example, users who have lost their phone), an administrator with the appropriate permissions can reset the user's two-factor authentication status. This requires the user to complete the setup process again.

To reset a user's two-factor authentication status:

Steps

- 1) Go to the **Account** page.
- 2) Click the username of the user whose account needs to be reset to open the User page. Under **Log On Details**, the current two-factor authentication status for the user is shown, including the date and time that setup was completed.

- 3) Click **Reset** to reset the user's authentication status.

The user will be prompted to repeat the two-factor authentication setup process when next logging on.

Login options

The administrators **Login options** determine how administrators are allowed to sign in to the portal and are enabled only when Administrator Single Sign-on is enabled. See *Administrator single sign-on* for more information.

Select the sign in method to be used by administrators to access the cloud portal.

- **Password only:** Selected by default, this option is always used when administrator single sign-on has not been enabled and configured. Administrators are required to enter a user name and password if this option is selected. When two-factor authentication is enabled, administrators are prompted to enter the code displayed on their authenticator app.
- **SSO + Password:** When this option is selected, administrators may sign in to the cloud portal using a user name and password, or the single sign-on option. When two-factor authentication is enabled, administrators using the password option are prompted to enter the code displayed on their authenticator app.
- **SSO:** Administrators must sign in to the portal using single sign-on. If necessary, administrators who have Managed User permissions are allowed to sign in using a user name and password as a fallback option. If this fallback option is used, and two-factor authentication is enabled, administrators are prompted to enter the code displayed on their authenticator app.



Important

When using the SSO related login options, you must access the portal with the following link <https://admin.forcepoint.net/portal>.

If enabling SSO Only - remember to review your existing Administrator permissions and remove the **Manage User** permission from any Administrator that should not be able to login using their username and password as a fallback option.

Related tasks

[Administrator single sign-on](#) on page 29

Terms of use

The **Terms of use** option allows you to display a page that requires administrators to agree to your company's terms of use before logging on to the portal. If enabled, this setting applies to all portal administrators. Administrators must agree to the terms of use each time they log on.

Note that this option is not available to Forcepoint Web Security Hybrid Module customers.

Your "Agree to Terms of Use" block page should be customized to include details of (or provide a link to) your terms.

See *Configure block and notification pages* for details of how to customize block pages.

To enable the terms of use acceptance page for all portal users:

Steps

- 1) Go to the **Account > Contacts** page.

2) Toggle the **Terms of use** switch to **ON**.

3) Click **Save**.

The next time portal administrators log on, they will be prompted to either accept your terms of use, or log off.



Note

By default, a generic “Agree to Terms of Use” block page is provided. Before enabling this feature, ensure you customize this page to include details of (or a link to) your company’s terms of use. See *Configure block and notification pages* for details of how to customize block pages.

Related concepts

[Configure block and notification pages on page 65](#)

Custom file types

The cloud service provides a number of file formats and file types to enable you to manage messages containing attachments. File types allow you to quarantine attachments by specific formats, for example GIF files or HTML documents. File formats are more generic: for example, the Sound format includes anything related to sound files, including RealAudio, Windows Media Audio, MPEG Audio, and MIDI files.

If the available file formats and types do not meet your requirements, you can set up custom file types containing one or more file types and MIME types. You can then use the custom file types to quarantine or park messages with the attachments you specify.

For more information, see *Creating custom file types*.

Related tasks

[Creating custom file types on page 116](#)

Identity Management

Click **Account > Identity Management** when you want to configure your account for user provisioning. See *Configure identity management* for details on this screen and directory integration considerations.

Related tasks

[Configure identity management on page 40](#)

End Users

To view and manage user data, click **Account > End Users**. (This option is only available if you have identity management enabled.) The resulting screen has 3 columns.

Column	Description
Criteria to use	Check the boxes on the left to indicate what search criteria to use.
Search Criteria	Narrow down the search by entering or selecting precise data in the middle column. Under source, you can choose whether to search <i>synchronized</i> users or <i>portal-managed</i> users.
Show in Results	Check the boxes on the right to indicate what information to include in the results.

Click **Search** when done. Please note that the search may be slow if there are a large number of users.

From the resulting data, you can make individual edits or bulk edits. For example, you can:

- 1) Undo the manual override (applies to identity management)
- 2) Delete one or more users

Use the **Download results** option at the bottom of the screen to export the search results to a CSV file.

Using the drop-down list between the search box and the search results, select the action you want to make, then select the users on which to perform the action and click **Go**. All changes made on this screen override any group/policy assignments (existing or future ones).

You can view and manage user data at the policy level as well using the **End Users** screen for the policy. The account-level page shown here is available only to users with account-level privileges.

Groups

The groups functionality enables you to create policies using your organization's hierarchy.

Groups can contain:

- email addresses of users in your organization
- other groups

Groups are configured at the account level. To set up groups in the cloud service, click **Account > Groups**.

The resulting screen shows a list of groups currently defined for your account, an indication of whether they were added manually on the portal or automatically through user provisioning, and the web policy to which the group is assigned.

On this screen, you have the ability to create new groups and edit group membership. Click a group name to edit it, or click **Add** to add a new group.



Important

Add or load groups only if you intend to use them for policy assignment or exceptions. You don't need them just because users are members of them.

Downloading and uploading groups

If you are managing groups strictly in the cloud (in other words, you are *not* using identity management), you have the option to upload or download a list of groups in a comma-separated values (CSV) file. You can then edit this using a simple text editor or a spreadsheet application such as Microsoft Excel.

If a policy includes a group that contains email addresses not on domains routed by the cloud email service, those email addresses are ignored.



Warning

If you already have groups in place for web users and there are dependencies between the groups and rules, selecting **Replace all groups with CSV file** could void exceptions to your rules. (For example, if a rule states that no one but the Accounting group can access www.financialnews.com, and then you upload a new Group list, it is possible that Accounting could lose access to that website.)

To maintain existing group/rule associations, make sure that group names in the CSV file match group names in the portal exactly. The best way to achieve this is to download existing group configurations to a PC, manipulate them as needed, then upload the changes to the cloud.

Licenses

Our subscription model operates in a similar manner to many software vendors: to use the service, you must accept the terms of your agreement. Once you have done this, your services are automatically enabled, renewed, or upgraded depending upon the subscription type.

The purchase and billing systems are fully integrated with the cloud portal. Each cloud service has a subscription associated with it, and that subscription is applied to each customer account.

To view the subscriptions associated with your account, go to **Account > Licenses**. You can use this area of the portal to view and manage your rights to use cloud services.



Note

If an alert indicates that your account is currently unlicensed, or that a license has been added or changed and must be accepted to place the provisions into service, please check the **Account > Licenses** page for further information.

Licenses page

The **Licenses** page provides basic information about your account, including:

- The account status
- Your enrollment key
- A summary of licenses for available products and add-on modules. A tick appears next to the components that your account is licensed for.
- The length of time your reporting data is retained
- The location where your reporting data is stored.

Depending on the subscriptions associated with your account, you may also see up to 3 sections:

- 1) Pending licenses: Licenses that require accepting.
- 2) Current licenses: Licenses that have been accepted and are currently valid.
- 3) Previous licenses: Licenses that have either expired or been replaced by another license.

License information

Subscriptions are generated automatically when you order a service. Each subscription contains the following information:

- Users: The number of users or mailboxes for which your account is licensed.
- Started/Expires: Start and end dates of the license.
- Contract: The contract governing the license. This contains a link to a copy of the contract.

Accepting licenses

The first time you log on to a new cloud service account, you are shown the licenses screen and must accept the terms of the agreement to activate your account and continue. If multiple subscriptions exist, you can accept them all at once.

Whenever a new subscription is ordered for you (for example, at renewal time or following an upgrade), it is added to your account in a pending state. You must accept this subscription to use the service. Each time you log on, you are taken to the licenses screen to remind you that a subscription requires accepting.



Note

To ensure continuity of service, you should accept any pending licenses as soon as possible. This requires Modify Configuration permissions.

If your license expires before you have a chance to renew it, you receive a grace period. During that period, please order a new subscription as soon as possible.

Administrator single sign-on

The Administrator single sign-on feature allows portal users to sign in to the Security Portal using a supported third-party identity provider. When enabled, this feature applies to all contacts.

Before enabling this feature, you must configure the details for your identity provider on the **Account > Administrator Single Sign-On** page. You must also configure your third-party identity provider to provide the cloud portal with sign-on authentication for your administrators.

To configure administrator single sign-on:

Steps

- 1) Go to **Account > Administrator Single Sign-On**.

- 2) Mark **Use identity provider for administrator single sign-on**.
- 3) From the Identity provider drop-down, select **SAML 2.0 Compliant Identity provider**.
- 4) To enable your identity provider to work with administrator single sign-on, you must provide metadata from your product.
 - If you select **URL**, locate the URL of your identity provider's metadata and enter it in the field provided.
 - If you select **File upload**, click **Browse** to locate the exported metadata file from your identity provider. If you have previously uploaded a metadata file, the file name and date and time of upload are displayed on the page.
- 5) Use the links provided in Download Links to get the details needed to fully configure administrator single sign-on.
 - a) In order for the cloud portal to talk to your identity provider, you must upload cloud service SAML metadata to your product. Click the Metadata link to download this data file.
 - b) Click the Root Certificate link and save the certificate file to a location on your network.
- 6) Click **Save**.

When you click **Save**, the specified metadata source is validated. If it is found to be invalid, the cloud portal displays an error and restores the previous configuration. This means:

 - Reverting to the previous metadata source if one was configured
 - Disabling the **Use identity provider for single sign-on** check box if you are configuring single sign-on for the first time.

Next steps

Once you have completed the setup on this page, you must do the following to complete single sign-on activation:

- Add the downloaded SAML metadata file to your identity provider.
- Deploy the root certificate to administrator's machines, using your preferred distribution method such as Group Policy Object (GPO).
- Select the required Login option to enable SSO as an administrator authentication mechanism. See *Login options* for more information.

When configuring your identity provider for administrator single sign-on, use the following URL to obtain the Forcepoint metadata:

<https://admin.forcepoint.net/login/saml.xml>

Note that this metadata source is different from the metadata source for end-user single sign-on provided on the **Web > End User Single Sign-On** page.

You can configure your identity provider to fetch this metadata dynamically using this URL, or save the page as an XML file, and upload it to your identity provider.



Important

When using the SSO related login options, you must access the portal with the following link <https://admin.forcepoint.net/portal>.

Related concepts

Login options on page 25

Data Protection Settings

Use the **Account > Data Protection Settings** page to enable and configure the integration with Data Protection Service, part of Forcepoint DLP. With this integration, enterprise data security, including blocking or monitoring data loss, is handled by the Data Protection Service (DPS), rather than the cloud proxies or relays.

The cloud proxies and relays continue to handle all other aspects of processing web and email traffic.

**Note**

Data Protection Service integration requires an additional license. If you would like further information on integrating with Data Protection Service, contact your account manager.

To monitor and prevent data loss using the Data Protection Service:

Steps

- 1) In the **Tenant Information** section, upload the configuration file provided by Forcepoint in the fulfillment email you received. This file provides the information needed to connect the cloud service to DPS and is the same file used when configuring Data Protection Service in the Data module of the on-premises Forcepoint Security Manager.
 - a) Click **Browse**, then locate and select the file.
The file name appears in the Configuration file entry.
 - b) Click **Upload**.
When the upload is successful, the remaining fields are automatically populated.

The **Browse** and **Upload** buttons are not available for users with **View Configuration** permissions.

- 2) Use the **Email Defaults** section to view how data security is handled in new email policies. DPS fallback behavior is set to **Allow** by default and cannot be changed.

DPS fallback behavior is configured as a backup in the event of a DPS timeout or other error. With this behavior set to Allow, all email messages received while DPS is unreachable are delivered. This ensures that emails are not unnecessarily quarantined.

Navigate to **Email > Policy > Policy Name > Data Protection** to configure your email policies with the new data security option. See the *Data Protection tab* for more information.

Related concepts

Data Protection tab on page 140

Important rules for configuring accounts

- Your account can enforce multiple policies on your email and web traffic.
- It is good practice to keep the number of policies to a minimum, because if a global change is required, you must make it across all policies.
- To prevent accidental changes, many configuration options are grayed out until you click the appropriate edit box.
- Each service has its own configuration screen accessed by clicking the appropriate tab on the main policy setup screen. Regardless of the services that you are licensed to use, you see all tabs. If you click the tab for a service that you are not licensed to use, you are informed of such.
- Where multiple email addresses, domains, or user names are entered into a screen, they should be separated by commas.
- You can click **Help** at any time to access online help information.
- All changes are made in real time and usually only take a few minutes to propagate across the cloud infrastructure.
- Forcepoint Email Security Cloud analyzes inbound and outbound email including both inbound and outbound spam. Analyzing outbound spam helps detect email that might be being sent by a botnet or otherwise compromised system at your site.
- Most settings in the policy screens are specified separately for inbound and outbound policy application. It is often not appropriate to set these identically for each direction. For example if a virus is detected in outbound email, then you probably do not want to send a notification to the intended recipient, whereas you might for an inbound email.
- Each Forcepoint Email Security Cloud policy applies to a domain or set of domains and specifies settings that the cloud email service uses to determine how to process your email.
- If you need to route email for different domains to different servers, you need to create a separate policy for each set of domains. Each policy includes its own routing table.

To access an email policy, go to the **Email > Policy Management > Policies** page. On the Policies page, you are presented with a choice of service-specific policies.

Working with External Directories

Contents

- Introduction on page 33
- What is SCIM? on page 34
- How the service works with SCIM on page 34
- What is LDAP? on page 34
- How the service works with LDAP on page 35
- Planning for your first synchronization on page 36
- Basic steps on page 39
- Cloud portal tasks on page 40
- Maintenance on page 45

Introduction

The cloud service allows you to make use of System for Cross-domain Identity Management (SCIM) or LDAP directories, such as Active Directory, so you don't have to re-create user accounts and groups for your email and web services or manage users and groups in two places.

User identity information maintained in a cloud-based service such as Okta or Microsoft Azure Active Directory can be forwarded to the cloud service using SCIM. Changes made to the user information are forwarded to the cloud automatically.



Note

SCIM is not supported with Forcepoint Email Security Cloud.

The cloud service optionally synchronizes with LDAP directories via a client-resident application known as the Directory Synchronization Client. Changes made to a directory, such as deleting a former employee or adding a new one, are picked up by the service on the next scheduled update. If you have more than one LDAP directory, the client can merge them together before synchronizing the data with the service.

For cloud web products, if you have set up the account for NTLM identification and synchronized NTLM IDs, end users do not need to register for the service on the portal (unless they are traveling outside of the network).



Important

The cloud service supports only one instance of the Directory Synchronization Client for each account. Using multiple synchronization configurations, or even using multiple installations of the Directory Synchronization Client, can cause data on the cloud service to be overwritten.

For cloud email products, you can synchronize primary and secondary email addresses and groups into the portal, improve spam detection, and improve the quality of reporting (less spam in the report). Directory synchronization makes it easier to manage groups as well.

What is SCIM?

System for Cross-domain Identity Management (SCIM) is a protocol used to provision user and group identity data from a cloud-based identity provider to the cloud service. Updates to user information in the identity provider are automatically forwarded to the cloud service as they happen.



Important

An NTLM ID is required when Forcepoint One Endpoint (Classic Proxy Connect or Direct Connect Endpoint) is used with SCIM and users are synchronized from the cloud directory. Refer to the Knowledge Base Article that explains how to configure SCIM with your preferred cloud directory.

Note that, while the NTLM ID is not required when Neo is used with SCIM, it is highly recommended that one be provided for consistency.



Note

SCIM is not supported with Forcepoint Email Security Cloud.

How the service works with SCIM

The cloud-based identity provider is configured with the URL of the System for Cross-domain Identity Management (SCIM) interface made available by the cloud service.

- 1) User and group information in the identity provider are assigned to the cloud service integration.
- 2) Each change to a user or group on the identity provider is sent to the cloud service via Secure Hypertext Transfer Protocol (HTTPS).
- 3) The uploaded data is stored in the cloud service, alongside any user and group data managed directly via the Security Portal.
- 4) The identity provider authenticates with the cloud service using a token generated in the portal and copied into the identity provider configuration.



Note

Okta and Microsoft Azure Active Directory are the only identity providers currently supported.

What is LDAP?

Lightweight Directory Access Protocol (LDAP) is a networking protocol for querying and modifying directory services. An LDAP directory contains data with similar attributes and organizes data in a directory tree structure. It is considered "lightweight" because it is a reduced version of the X.500 directory standard.

Active Directory (AD) is Microsoft's LDAP-compliant directory service, and is an integral part of the Windows Server architecture. Active Directory is a hierarchical framework of resources (such as printers), services (such

as email), and users (user accounts and groups). It allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization.

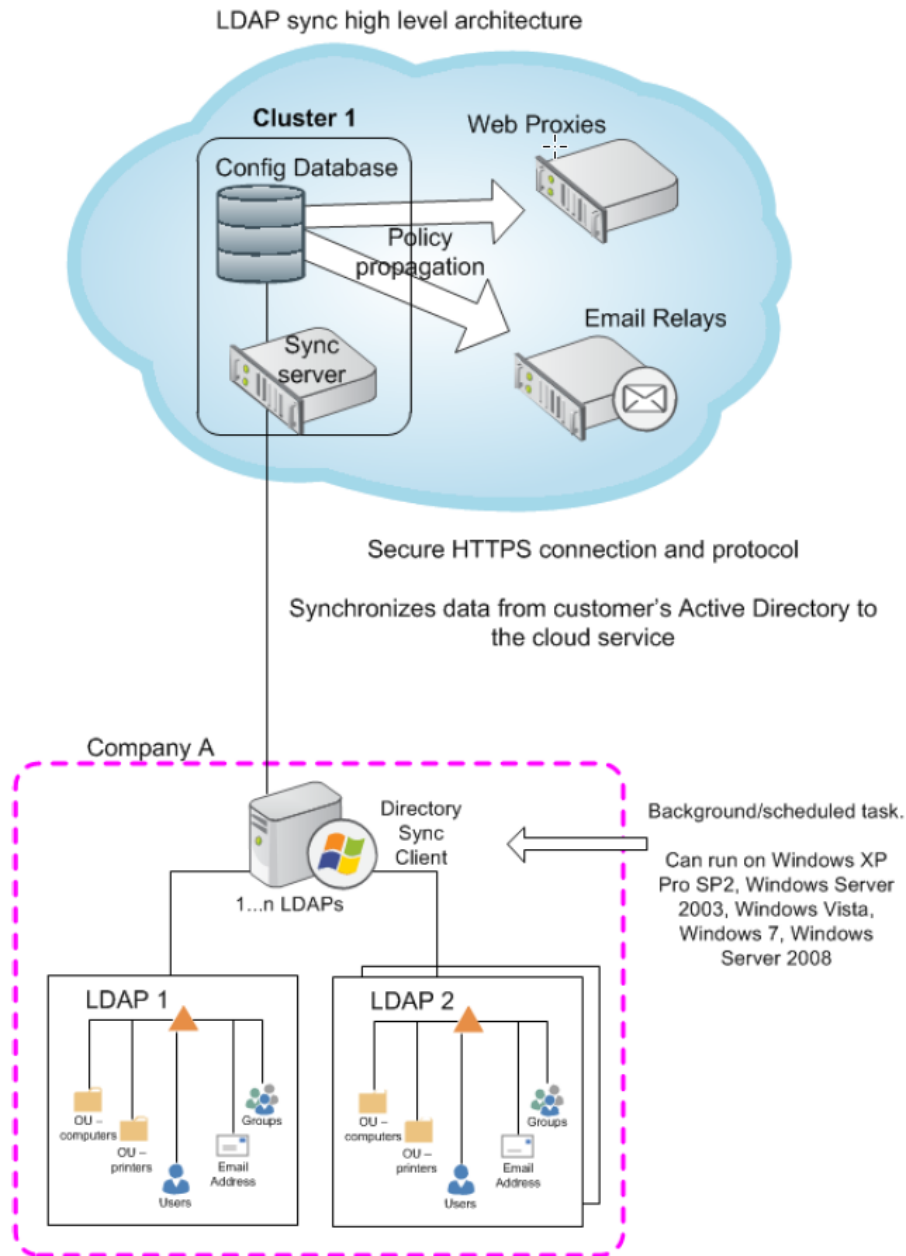
The cloud service integrates with LDAP directories and has been certified to work with Microsoft Active Directory. If you have enterprise information stored in AD, you do not have to enter it into the cloud portal manually.

How the service works with LDAP

For each data synchronization:

- 1) The Directory Synchronization Client communicates with the LDAP server and returns the selected data (users, groups, and email addresses).
- 2) The Directory Synchronization Client performs a synchronization and returns incremental changes to the portal via Secure Hypertext Transfer Protocol (HTTPS). You can force a full synchronization when necessary.
- 3) The uploaded data is stored in the cloud service, alongside any user and group data managed directly via the Security Portal.
- 4) If both user and group data is required, the update occurs in 2 transactions. If one fails, the other can still succeed. Email addresses are a third transaction.
- 5) The client authenticates with the portal using a username and password that you establish manually on the **Contacts** page. (Consider an appropriate password expiration policy for that user so you don't have to regularly update the client application with the password changes.)
- 6) LDAP synchronized data is viewable but not editable through the portal.

The synchronization client resides on a computer at the customer's site and accesses one or more LDAP directories via the customer's network. If more than one LDAP directory is accessed, then this data can be merged together by the synchronization client before it is synchronized with the cloud service.



Planning for your first synchronization

When you are setting up user provisioning, it is important that you review the data you are about to provision. The way that you structure user data in your identity provide or LDAP-compliant directory affects how you should structure groups and users in the portal for policies and exceptions. You should devise a strategy before you start.

To start, what data do you want to get out of your user data and what do you plan to do with it?

Second, how is that data organized?

Third, how do you need to structure users and groups in the portal to accommodate your security requirements?

In a typical directory, users are members of many groups. For example, users may be members of global groups like “All Sales;” they may be members of geographical groups like “London” or “New York;” and they may be members of a department such as “NY Telesales” and many others. When deciding on which groups to provision, select only groups that are going to be useful to the cloud service, typically for setting policy or group-based exceptions. See *Deciding what to synchronize* for more guidelines on this decision.

If you already have users and groups in the portal, then you’ll need to determine how and whether to adjust that structure to match the data that is to be provisioned (or vice versa).

For customers using LDAP, following are the most common use cases. Follow the links to review considerations and checklists designed just for you.

- New customers:
 - *Synchronizing users/groups with a single Web policy and exceptions*
 - *Synchronizing users/groups with more than one policy, and planning to manage policy assignment through an LDAP directory*
 - *New Web customers (SCIM)*
- New and existing email customers:
 - *Synchronizing email addresses to provide a “allowlist” of valid email addresses*
 - *Synchronizing users/groups to provide per-user/per-group exceptions to email policies*
- Existing customers:
 - *Wanting to manage users/groups from an LDAP directory*
 - *Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal*
 - *Existing Web customers (SCIM)*

Related concepts

[Deciding what to synchronize](#) on page 37

Related tasks

[Synchronizing users/groups with a single Web policy and exceptions](#) on page 234

[Synchronizing users/groups with more than one policy, and planning to manage policy assignment through an LDAP directory](#) on page 235

[New Web customers \(SCIM\)](#) on page 240

[Wanting to manage users/groups from an LDAP directory](#) on page 241

[Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal](#) on page 243

[Existing Web customers \(SCIM\)](#) on page 245

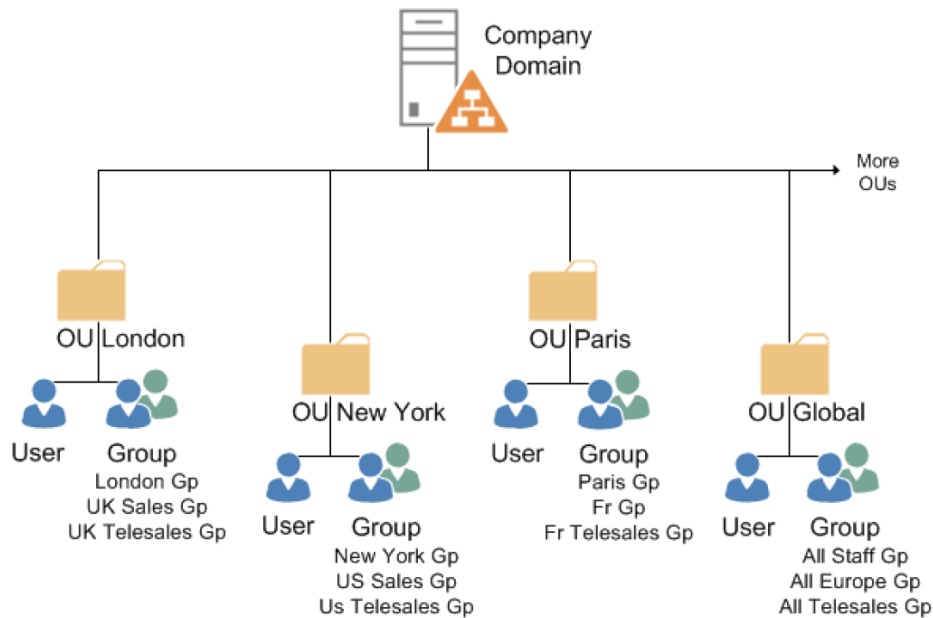
[Synchronizing email addresses to provide a “allowlist” of valid email addresses](#) on page 237

[Synchronizing users/groups to provide per-user/per-group exceptions to email policies](#) on page 238

Deciding what to synchronize

You do not need to provision all of the groups and users in your directory. Instead, provision only groups that are useful to the cloud service.

Consider this example:



If you are going to set up a policy for members of a US Telesales department that gives them special permission to access certain websites, you should provision the “US Telesales” group. There is no need to provision the “London” group if you are not going to set up geographical policies in the cloud service, even if the London users are going to be using the service.

Sometimes when users are provisioned to the cloud service, they are members of multiple groups, but only a subset of those groups is provisioned. This is not a problem: the cloud service is designed to accept users with group references that are not on the service.

Synchronizing with SCIM

Synchronization of user and group data occurs automatically after the identity provider is configured with:

- The base URL provided in the SCIM Settings section of the **Account > Identity Management** portal page.
- The token generated on the **Account > Identity Management** page.
- provisioning details required by the specific identity provider. See *Configure identity management*.

When the identity provider notifies the cloud service of the updates, new user information is added to a policy. It can take a number of minutes before all new information is propagated and policies are assigned to users as expected.

Related tasks

[Configure identity management](#) on page 40

Synchronizing with the Directory Synchronization Client



Note

Support for Directory Synchronization Client is limited to the most recent version and the version that immediately preceded it.

You specify which groups to synchronize using an LDAP search facility on the Directory Synchronization Client. There is great flexibility in selecting the appropriate data to synchronize. For example, you can use the *membership of an LDAP group* attribute to select the users you want, even though you may not select that group in the group synchronization setup itself.



Note

If you add or change a group name in Active Directory or move a group from one organizational unit (OU) to another, be sure to add the new name to the group inclusion list on the Directory Synchronization Client before the next synchronization. Otherwise, the group is deleted from the portal.

Regardless of how many groups you synchronize, user detail must be sent as part of a separate user synchronization. When you synchronize a group, you transfer information about the group but not about its contents. User synchronizations include details of the group(s) to which users belong. When you apply a web policy or an email policy to a synchronized group, that policy is applied to all synchronized users who are members of that group.

Please refer to the [Directory Synchronization Client Administrator's Guide](#) in the Technical Library for more information on using the LDAP search feature to target only those users and groups that are required.

Basic steps

Although the steps for your use case may vary, the basic steps for setting up user provisioning follow:

In the portal

Steps

- 1) *Configure identity management* for your account.
- 2) When using SCIM, configure your identity provider, providing details from the SCIM Settings section of **Account > Identity Management**.
- 3) When using the Directory Synchronization, *Set up authentication (Directory Synchronization only)* for the client machine. The client should have its own username and password to gain access to the cloud service.

Related tasks

[Configure identity management](#) on page 40

[Set up authentication \(Directory Synchronization only\)](#) on page 43

On the client (Directory Synchronization only)

Steps

- 1) Download the Directory Synchronization Client (see *Client tasks (Directory Synchronization only)*) and install it on a network client machine. Download the client administrator's guide as well. This contains valuable information on helping you integrate your directory service with the cloud service.
- 2) Configure the client. Use the username and password established in the **Contacts** section of the portal to authenticate.
- 3) Test the Directory Synchronization Client to make sure it is returning the correct data from the LDAP server to the client. If you are an existing customer switching to directory synchronization for the first time, you should compare the data with that which already exists in the cloud.
- 4) Initiate a synchronization. The service updates its groups and users, including policy assignment where appropriate.
If a synchronization is unsuccessful, you can use the **Restore** feature to restore the directory information to a previous version. (See *Restore directories* for more information.)
- 5) Schedule automatic synchronization. You can update the cloud service several times a day if required. Refer to the [Directory Synchronization Client Administrator's Guide](#) for instructions on items 2-5.

Related tasks

[Client tasks \(Directory Synchronization only\)](#) on page 44
[Restore directories](#) on page 47

Cloud portal tasks

To set up your account for user provisioning, perform the following steps in the portal:

- 1) *Configure identity management* for your account.
- 2) *Set up authentication (Directory Synchronization only)* for the client machine (if using Directory Synchronization).

Related tasks

[Configure identity management](#) on page 40
[Set up authentication \(Directory Synchronization only\)](#) on page 43

Configure identity management

Steps

- 1) On the main menu bar, click **Account**.
- 2) Click **Identity Management**.
- 3) Check the **Enable identity management** box.
 - Click **Directory Synchronization Client** to use an LDAP directory.
You cannot connect the Synchronization Client to the cloud without doing so, even if you have a valid username and password.
 - Click **SCIM Integration** (cloud web only) to use a cloud-based identity provider.
 - Because you are provisioning user and group data, you can manage policy membership through group membership. Select from the **Default user policy** drop-down the web policy to which you want to assign users if they have no group-based policy assignment already. By default, the first policy in the list is chosen.

- 4) If you selected Directory Synchronization Client, Directory Synchronization Settings display.
- Select **Overwrite groups** to overwrite current groups with the provisioned groups when there is a group name conflict.
If you are a new customer with no group data in the cloud, leave this box unchecked.
If you have existing data, check this box if you want to overwrite current groups with the provisioned groups when there is a group name conflict.
Users, groups, and email addresses are overwritten by LDAP data of the same name. Once this occurs, they are manageable only by LDAP synchronization.
If you are switching to LDAP for the first time, take care to match your LDAP group names and membership to the existing setup. Doing so allows existing policy selections and settings to be maintained, as well as existing usernames/ passwords where applicable.
If you have duplicate names, you have 2 options: make sure the duplicate can be overwritten or don't allow overwriting and rename the duplicates to avoid a conflict.
If you don't select this option and duplicate names are found, the transaction is rejected. In the cloud, you receive the error "403: Attempt to overwrite portal-managed group 'nnnn'." On the client, you receive "Error communicating with the Hosted Service portal. Update abandoned."

Under Web:

- Specify whether you want the **User policy assignment** to be fixed after the initial user provisioning, or if you want the service to check the group policy membership every time users are provisioned or group policy assignments are changed in the cloud.
 - Select **Fixed** if you want to manage policy assignments in the cloud. When this option is selected, the service makes a policy assessment for an individual user only when that user first appears in the system (in other words, is synchronized for the first time). It either assigns the user a group- based policy or the default policy specified above. If you want to move someone to a new policy, you need to do so in the cloud.
 - Select **Follow group membership** if you want users' policy assignments to change automatically when there are changes to their group membership. If you move someone to another group, he or she moves to a different policy. This is the default.
- Select one of the **Email settings** radio buttons to indicate whether you want email sent to new end users to notify them that they are now protected by the cloud service.
You can select to **Email all new users**, only those who do not have an NTLM identity, or no one.
Be aware that sending to end users could flood your email servers with messages and slow down performance. You're asked to confirm this decision. We recommend you do this at a quiet time.
- Choose which **Email template** you want to use to notify end users of their enrollment in the cloud service. Initially, only the default message is offered, but you can create custom notifications if desired. See *Configure block and notification pages* for more information.
- For **Sender's address**, enter the address from which you want notification messages sent to new users.

Under Email:

- **(Quarantine/discard/bounce)** mail for unknown users. This determines what happens to email arriving at the cloud service that is sent to an unknown email address. By default it is quarantined.
Check this box if you want the message handled in this way. Leave it unchecked if you do not.
Only Forcepoint Technical Support can modify the disposition of this option.
Occasionally customers cannot enable or disable this option. This happens when addresses have not been synchronized, a similar access control has been manually added to your policy, or Customer Services has explicitly turned it off.

- 5) If you selected SCIM, configuration details required to connect your identity provider to the cloud service are provided.
 - The **Base URL** is used to allow your identity provider to access the cloud service. Use the copy option provided to easily paste the URL into the appropriate configuration page for your provider.
 - The **Bearer token** provides a unique authentication key used to authorize requests to the cloud service. Click **Generate New Token** to generate the key and then use it when configuring your identity provider.

Note that **Overwrite groups** and **Follow group memberships**, configurable when Directory Synchronization is selected, are automatically applied when SCIM is selected.



Important

When you generate a new token, it will be displayed only once. Ensure you make a note of the token. When you generate a new token, any existing token will become invalid. If you have an existing token in use, it will need to be replaced with the new token.

- 6) Click **Save** when done.



Note

You can turn off identity management any time and revert to managing all users, groups, and email addresses in the cloud. If you plan to do this, please see *Turn off identity management* for possible considerations.

Related tasks

[Turn off identity management](#) on page 49

Set up authentication (Directory Synchronization only)

On the **Contacts** page, set up authentication for the client machine. We strongly recommend that the client have its own username and password to gain access to the cloud service. This keeps the synchronization process separate from your other administration tasks and enables you to establish longer password expiration policies.

Once you establish a contact for the client machine, you configure the client to pass these logon credentials when connecting to the service.

Steps

- 1) On the main menu bar, click **Account**.
- 2) Click **Contacts**.
- 3) In the Contacts section, click **Add**.
- 4) Enter identifying information for the client machine in the **First name** and **Surname** fields. For example, "Directory Sync" and "Client."
- 5) Click **Submit**.

- 6) In the User Name field, click [here](#) to add a user name.
- 7) Enter a password for the client machine. It must conform to the password policy on the main Contacts page.
- 8) Enter a password expiration date for the client. To avoid having to regularly update it, this should be different than the regular account settings; it should span a longer period.
- 9) Under **Account Permissions**, check the **Directory Synchronization** box, and any other permissions you want to give this “user”. You can act as an administrator from this logon.
- 10) Click **Submit**.

Client tasks (Directory Synchronization only)

The Directory Synchronization Client is designed to run on a machine with at least 2GB of RAM, and requires approximately 10MB of disk storage. The following operating systems are supported:

- Windows XP Professional Service Pack 2
- Windows Server 2003
- Windows Vista
- Windows 7
- Windows Server 2008

To download the client:

Steps

- 1) From the client machine, log on to the portal.
- 2) Select **Account > Identity Management**.
- 3) Under Download Directory Sync Client, download the directory synchronization client.
Select a client tool to download it. If you already have a Java Runtime Environment (JRE), download the tool without a JRE. Otherwise, download the one that includes a JRE. A JRE is required to run the client software.
- 4) When the download is complete, run the executable file.
- 5) Navigate through the installation wizard as prompted, accepting the license agreement and indicating where to install the application. Review the installation instructions in the client administrator’s guide for assistance.
- 6) Configure the client as described in the client administrator’s guide. Provide the logon credentials that you established as part of the configuration.

Maintenance

After identity management is set up and running properly, you can perform the following tasks in the portal:

- 1) *View and manage user data*. Note you cannot edit data that has been provisioned from your directory.
- 2) *View and print reports*
- 3) *View recent synchronizations*
- 4) *Restore directories to previous version*
- 5) *Troubleshoot synchronization failures*
- 6) *Turn off identity management*

Related concepts

[View and print reports on page 46](#)

Related tasks

[View and manage user data on page 45](#)

[View recent synchronizations on page 46](#)

[Restore directories on page 47](#)

[Turn off identity management on page 49](#)

Related reference

[Troubleshoot synchronization failures on page 48](#)

View and manage user data

You can view account- or policy-level data about end users at any time. The portal provides a clear indication of which records are maintained in the service and which have been synchronized from your directory.

Steps

- 1) To view account-level data on users, select **Account > End Users**.
- 2) Check the boxes on the left to indicate which search criteria to use.
- 3) Narrow down the search by entering or selecting precise data in the middle column.
- 4) Check the boxes on the right to indicate what information to include in the results.

- 5) Choose how many results to show per page and click **Search**.
- 6) From the resulting data, you can make individual edits or bulk edits. For example, you can:
 - a) Undo the manual override.
 - b) Delete users.
All changes made on this screen override any group/policy assignments (existing or future ones). To return to the automatic settings, manually undo your changes here.

You can view and manage user data at the policy level as well as using the End Users screen for the policy.

View and print reports

You can view and print reports that show the history of synchronizations, including high-level statistics on success/failure and numbers of items synchronized, on the **Reporting > Account Reports > Services** page.

The following reports are available:

Report	Description
Synchronization History Log	The history log provides a connection history for the specified period, up to 1000 rows.
Synchronization Time Summary	The time summary provides a list of the 20 longest synchronization times.

See *Service reports* for more information.

Related concepts

[Service reports on page 217](#)

View recent synchronizations

Steps

1) Select **Account > Identity Management**.

The Recent Synchronizations section shows your recent synchronization history.

Column Heading	Description
Date	The date and time that the synchronization was performed in coordinated universal time (UTC). Format YYYY-MM-DD HH:MM:SS.
Status	An indication of whether the synchronization completed or failed. Possible HTTP response codes include: <ul style="list-style-type: none"> ■ 200 OK - Completed successfully. ■ >400 - Synchronization failed <ul style="list-style-type: none"> ■ 403 Error text - The client synchronization failed for reasons given in the error text. For example: <ul style="list-style-type: none"> ■ 403 Groups contain circular references ■ 403 Transaction failed ■ 403 Attempt to overwrite cloud-managed group. ■ 403 Email address exists in another account ■ 503 Service Unavailable.
Type	The type of record that was synchronized: Users, Groups, Addresses, or Test. Test indicates that the client connected to the cloud service to verify its settings, but did not synchronize.
Additions	The number of new records added during the synchronization. If the synchronization is not yet complete, "In progress" is displayed.
Deletions	The number of records deleted during the synchronization.

2) Click the timestamp in the date column to view details about a specific synchronization.

In the resulting screen, you can see the time that the connection started and ended in the local time zone of the client machine. (This lets you see how long the synchronization took). You can view the IP address of the source connection, the username of the client initiating the synchronization, and the number of records amended, added, or deleted. You can also see reporting and logging information.

Restore directories

If necessary, you can undo the last directory synchronization and restore the system to its state before the synchronization.

**Important**

It is not possible to undo the restore, so changes you made in the cloud between the last synchronization and the restore operation may be lost. You are warned of the potential impact and asked to confirm the action.

Steps

- 1) Select **Account > Identity Management**.
- 2) Click **Restore**.
- 3) Click **Restore** to restore your directory to the current backup version or click **Cancel** to cancel.
- 4) Confirm your action when prompted, "Are you sure?"

Troubleshoot synchronization failures

Should a synchronization fail to complete, a record is saved by the cloud service along with your details, date/time stamps, and an error message. You can access this information by selecting **Account > Identity Management**. See *View recent synchronizations* for more information. You can also view it in the Synchronization History log, available under **Account > Reports > Services**.

In the status column, any response code greater than 400 indicates a failed synchronization.

HTTP Response Code	Explanation	Recommended Action
403 Groups contain circular references	An attempt has been made to synchronize a hierarchy of groups that contain one or more circular references. For example, GroupA is a member of GroupB, but GroupB is a member of GroupA.	The list of groups forming the cycle are listed in the response code. Check these groups and fix the memberships to break the cycle.
403 Transaction failed	Further explanation is added to the response code to explain the problem. This is usually due to some uniqueness constraint failing--for example, if 2 users have the same email address or LDAP domain name.	Resolve the issue detailed in the full response code.
403 Attempt to overwrite portal managed group.	An attempt has been made to synchronize a group with the same name as a cloud-managed group, and the Overwrite Portal Groups option is off.	On the Identity Management screen, check the Overwrite Groups box to allow overwriting, or rename the duplicate groups to remove the conflict.
403 Email address exists in another account	An email address in the LDAP directory already exists in another account.	Remove this email user from your directory if it is your error. If it is a valid address that you own, contact Customer Services to have the address removed from the other account.

HTTP Response Code	Explanation	Recommended Action
503 Service unavailable.	<ul style="list-style-type: none"> ■ The cloud service is heavily loaded, so a synchronization is not currently possible. ■ Synchronization is not enabled on the account ■ Your account has exceeded its daily synchronization limit 	<ul style="list-style-type: none"> ■ No action. The client automatically re-tries later. ■ Enable synchronization by selecting Account > Identity Management > Edit > Enabled ■ Retry tomorrow (or when next scheduled).

Partially transmitted and temporarily stored data remains in the cloud service for a few days as a possible debugging aid. This data is not used when you try to synchronize again.

Related tasks

[View recent synchronizations](#) on page 46

Turn off identity management

You can turn off identity management any time and revert to managing all users, groups, and email addresses in the portal. To do so:

Steps

- 1) (Directory Synchronization only) Cancel any scheduled synchronizations on the client machine. For more information, see the section “Removing the synchronization schedule” in the [Directory Synchronization Client Administrator’s Guide](#).
(SCIM) Disable the cloud service integration in your identity provider to avoid seeing errors when a synchronization is attempted by the IdP.
- 2) Log on to the portal.
- 3) Navigate to the **Account > Identity Management** page and click **Edit**.
- 4) Clear the **Enable identity management** check box.
- 5) Click **Save**.



Important

Ensure that a synchronization is not under way when you disable the feature. If a synchronization is running, you may end up with an incomplete set of data: for example, your groups might have synchronized successfully, but your users might not.

When you turn off directory synchronization, Group and user IDs on previously synchronized items are retained, so you can easily re-enable synchronization at a later date. SCIM users will, however, need to generate a new authentication token and set it in the identity provider configuration details.

Please note that changes made manually in the cloud to data items that were previously synchronized are lost if you later re-synchronize. When you re-enable synchronization, you are indicating that it is now the identity provider or LDAP directory that holds the master data, and a full re-synchronization is performed.

Chapter 4

Configuring Email Settings

Contents

- Introduction on page 51
- File sandboxing on page 51
- DNS records and service IP addresses on page 54
- Aliases on page 55
- Blocklist and allowlists on page 56
- Personal Email Subscriptions on page 56
- Email notifications on page 62
- Configure block and notification pages on page 65
- Image allowlist on page 69
- Email connectivity testing on page 70
- URL Sandboxing utility on page 72

Introduction

Use the **Email > Settings** options to configure account-level settings for Forcepoint Email Security Cloud, including aliases, blocklist and allowlists, and end user email reports (Personal Email Subscriptions) for your account.

File sandboxing



Note

You must have the Forcepoint Advanced Malware Detection for Email module to use this feature.

Use the **Email > Settings > File Sandboxing** page to send suspicious files received in email messages to a cloud-hosted sandbox for analysis. The sandbox activates the file, observes the behavior, and compiles a report. If the file is malicious, the message is either quarantined, or an email alert is sent to the administrators that you specify, containing summary information and a link to the report.

A file that qualifies for sandboxing:

- Is **not** classified as “malicious” by virus scanning or Forcepoint ThreatSeeker Intelligence
- Fits the Security Labs profile for suspicious files
- Is a supported file type for sandboxing.

**Note**

Because the file was **not** detected as malicious, it was **not blocked** and has been delivered to the email recipient.

Steps

- 1) File analysis is disabled by default. Select **On** to send qualified files to the cloud- hosted sandbox for analysis.
- 2) Select the analysis mode you wish to use:
 - **Monitor only** performs the file analysis; however, because the file was not originally detected as malicious, it is not blocked and is delivered to the email recipient regardless of the analysis results.
 - **Enforce** holds any messages with attachments sent for analysis, and then quarantines those messages found to contain malicious attachments.
- 3) Specify the email address of at least one person in your organization who will receive notifications. Notifications are sent only for monitor mode. If you have selected the Enforce mode, you may still want to enter an email address in case a message pending analysis is released from quarantine with no further processing before analysis is complete. In this case, a notification will be sent if the attachment is found to be malicious.

The specified person does not have to be a Forcepoint Email Security Cloud administrator. If you specify multiple email addresses, ensure you enter one address per line.
- 4) Select the file types you want to submit for analysis from the **File types to scan** list.
- 5) Click **Save**.

Supported file types

When file sandboxing is enabled, the following file types can be sent to the cloud sandbox if potentially suspicious:

- Windows executable files
- Microsoft Office files:
 - Word (.doc, .docx, .dot, .dotx, .dotm, .docm)
 - Excel (.xls, .xlsx, .xlt, .xlam, .xltm, .xlsm, .xlsb, .xltx, .xla)
 - PowerPoint (.ppt, .pptx, .pps, .pot, .ppsx, .potx, .ppsm, .pptm)
- PDF files

What does a file sandboxing transaction look like?

- 1) The cloud service receives an email message for an end user that explicitly or implicitly includes a file.

- 2) The message is not classified as malicious, and virus scanning or Forcepoint ThreatSeeker Intelligence does **not** find the attachment(s) to be malicious. However, the attached file matches the configured file types to be sent to the sandbox in the cloud for analysis.
- 3) If monitor mode is selected, the message with the attached file is delivered to the email recipient. If enforcement is selected, the message is held, pending analysis.
- 4) The sandbox analyzes the file, which may take as long as 5 to 10 minutes, but is typically much quicker.
- 5) If the file is found to be malicious, the cloud service sends a malicious file detection message to the configured alert recipient(s). The alert email includes a link to the report. If enforcement mode is in use, the message is quarantined.
- 6) Upon receipt of the message, administrators should:
 - a) Access and evaluate the report for the file
 - b) Assess the impact of the intrusion in their network
 - c) Plan and begin remediation
- 7) Separately, the file sandbox updates Forcepoint ThreatSeeker Intelligence with information about the file and the source email message.
- 8) ThreatSeeker Intelligence updates its rules and other security components.
- 9) The next time someone receives an email message containing this file, they and the organization are protected by their Forcepoint Email Security Cloud deployment.

File sandbox reports

Reports are available in the **Report Center** package (Report Catalog/Report Builder). If the Report Center package is not enabled for your account, contact Technical Support to have it enabled.

Custom file sandbox reports can be constructed in the Report Builder. See *Using the Report Builder*.

Two predefined file sandbox reports are available in the Report Catalog.

- Summary of File Sandboxing Results by Status
- Detailed File Sandboxing Report

See *Email predefined reports*.

Related concepts

[Using the Report Builder](#) on page 199

[Email predefined reports](#) on page 170

DNS records and service IP addresses

MX record DNS entries

Forcepoint Email Security Cloud uses customer-specific DNS records to route email from the service to your email gateway, and from your email gateway back to the service. You can view your customer-specific DNS records by selecting **Email > Settings > DNS Records & Service IPs**. The records are listed under MX Record DNS entries.

CNAME records

The CNAME Records section lists the DNS CNAME records you must publish in order to enable DKIM signing for outbound messages (see *DKIM Signing*). The domains listed on this page include a code that is unique to your account.

Prior to enabling a DKIM signing rule, you must create CNAME records in each domain you wish to use as the DKIM signing domain (note that the same DKIM signing domain can be used for all sender domains that are sub-domains of the signing domain).

The public/private key pairs used for DKIM signing are managed by Forcepoint, and are rotated periodically, with a period of validity overlap to allow the successful signing of delayed messages. Two CNAME records must be published for each of your signing domains, enabling a DNS lookup to validate signed messages.

In the DNS records for your signing domain, map the *host* subdomains listed in the table to the corresponding out.mailcontrol.com domain. For example:

Type	Host	Points to
CNAME	fpkeyNNN-1._domainkey	fpkeyNNN-1._domainkey.out.mailcontrol.com
CNAME	fpkeyNNN-2._domainkey	fpkeyNNN-2._domainkey.out.mailcontrol.com



Note

Keys are automatically rotated after six months. Forcepoint will publish the TXT record for the secondary key (fpkeyNNN-2) six months after the creation of the fpkeyNNN-1 record. Customers are required to add both CNAME entries at the outset, so that key rotation can occur without further action needed.

Note that NNN in the examples above represents a number unique to your account.

Use the CNAME Record check function on the **Antispoofing** tab to ensure that your CNAME records have been published correctly. See *Enabling a DKIM signing rule*.

Service IP addresses

Because Forcepoint Email Security Cloud is a hosted service, we are responsible for managing system capacity. For this reason, we may occasionally choose to alter the route of your email within our service. To enable us to do this seamlessly without requiring you to make further changes, you must allow SMTP connections from all the IP ranges listed under Service IP Addresses on this page. To access the cloud portal, ensure that ports 80 and 443 are also permitted for these IP ranges.

Related concepts[DKIM Signing on page 107](#)[Enabling a DKIM signing rule on page 109](#)

Aliases

Forcepoint Email Security Cloud can rewrite email addresses as email enters and leaves your system. Aliases must be to and from domains associated with your Forcepoint Email Security Cloud policies. Aliases let you rewrite email addresses both inbound from the Internet and outbound to the Internet. When an alias has been applied, email passes through the policy for the new address. Addresses in the SMTP envelope and in those header fields defined in the standard Internet message format (as defined in RFC 2822) are rewritten.

- An alias can apply both inbound and outbound. In this case, there is a one-to-one mapping of an internal address to an external address and vice-versa. This is often called masquerading an address.
- An outbound-only alias is also a one-to-one mapping.
- An inbound-only alias can be a one-to-one or a one-to-many mapping (a distribution list). To specify a distribution list, separate email addresses with commas.
- If an alias is neither inbound nor outbound, it is a disabled record.

To view the aliases that have been configured for your system, select **Email > Settings > Aliases**.

To search for all aliases in the system, enter an asterisk in the **Email address** field, check both the **Inbound** and **Outbound** check boxes, then click **Search**.

To narrow the list to specific entries, enter search criteria in the **Email address** field, such as “*john*”. Wildcards are supported.

Adding or modifying an alias

Steps

- 1) Select **Email > Settings > Aliases > Add Alias**.
- 2) Enter the internal and external addresses for which you want to create an alias.
- 3) Specify whether the alias applies inbound or outbound mail, or both.
- 4) Click **Submit** to save your changes.

Downloading and uploading aliases

You can download the complete alias list as a comma-separated values (CSV) file. You can then edit this using a simple text editor or a spreadsheet application such as Microsoft Excel. If you are intending to upload aliases,

be very careful not to change the format of the file. The first line of the file is a header line - it must always be exactly:

Inbound,Outbound,External,Internal

Subsequent lines follow this format:

yes,no,addr1@external.domain.com,addr2@internal.domain.com

All values must be separated by commas and enclosed in double-quotes if they contain commas.

During the alias upload, Forcepoint Email Security Cloud performs a complete syntax check before it imports the aliases to the system configuration. If it finds any errors, it reports them and abandons the file import.

Blocklist and allowlists

- 1) Select **Email > Settings > Block & Allow Lists** to see which email addresses are in blocklist or allowlist for your account.
- 2) Enter search criteria into the fields provided, then click **Search**.

Field	Description
Address Pattern	Enter a specific address for which to search, or use wildcards to expand your search. Enter an asterisk (*) to search for all addresses that are in blocklist or allowlist.
Action	Select the type of search you want to perform. You can search for Accept actions (allowlist), Reject actions (blocklist), or both.
Minimum policies contained in	Indicate a policy threshold for your search. You can specify an interest in addresses that are in blocklist or allowlist in at least <i>nn</i> policies.

The resulting screen shows addresses in blocklist or allowlist that appear in the specified number of policies for your account.

To manage blocklist and allowlists for your policies or end users, go to the Antispam tab for the policy. See *Adding an entry to the allowlist or blocklist* for more information.

Related tasks

[Adding an entry to the allowlist or blocklist on page 101](#)

Personal Email Subscriptions

To configure the content of email message reports sent to end users, select **Email > Messages > Personal Email Subscriptions**. The personal email subscription gives end users a summary of the messages that they have received and sent.

You can choose to subscribe your end users to personal email message reports via the portal. Users receive a single report in the format that you configure, and the report contains a link that a user must click to receive the report on a weekly basis. Otherwise, to receive a report, users must request it via a website. They can also subscribe to the report for automatic delivery. For information on the contents of the report and the request process, see *End-User Self Service*.

On the **Personal Email Subscriptions**, there are 4 tabs:

- Subscriptions
- Settings
- Text and Language
- Bulk Upload

Related information

[End-User Self Service](#) on page 155

Subscriptions tab

In the Subscriptions tab, you can see a list of the recipients of a personal email subscription, the email addresses or accounts covered in the subscription, and a description of the subscription, if provided. Optionally, you can filter elements in the list.

To create a new personal email subscription for an end user:

Steps

- 1) Click **Add**.
- 2) Under **Subscription**, enter an email address for the **Recipient**, and optionally, enter a **Description**.
- 3) Under **Manage Accounts**, enter any other email aliases or accounts that you wish to consolidate into this subscription.

Enter one email address at a time, clicking **Add Address** after each. If you choose to consolidate multiple email addresses into one report, the recipient gets a report containing details of all sent and received mail for all associated email addresses.

Note that any allowlist or blocklist entries associated with the email addresses are not merged – i.e. if a sender has previously been in allowlist for one address, it is not automatically in allowlist for other addresses in the same report subscription. However, if the report recipient later chooses to allowlist or blocklist an address by clicking the **Allowlist** or **Blocklist** buttons in the report, it will apply to all email accounts or aliases associated with the report.

- 4) Under Report Options, define the following options:
 - Select the **Email types to include** in the report.
 - Choose how information about quarantined and non-quarantined messages should be sorted: by status, date/time, subject, from, or to. You can then define ascending or descending order. Note that clean messages will always be shown by date and time.



Note

Subscriptions to the Forcepoint Email Security Cloud message report lapse after 93 days. 62 days after subscribing, each time users receive a report, they are reminded that they should renew their subscription. To see the expiration date for a subscription, go to **Reporting > Account Reports > Services**. In the **Show** drop-down list, choose **Personal Email Subscriptions - Subscriptions**. Click **Generate Report**. The report includes the expiration date as well as recipient and subscriber addresses.

- Select the language and time zone you want reflected in the report.
- 5) Click **OK**. This becomes the default configuration for all future message reports. You can change this configuration at any time.

To edit existing subscriptions, click on the pencil icon next to the recipient's name. The Edit Subscription box appears in which you can perform the same steps outlined above.

Settings tab

The Settings tab shows the default settings for your personal email subscription reports, which are used when an end user first subscribes and if new subscriptions are created via LDAP synchronization. In Settings, you can perform actions, such as allowing end users to modify report content, and several other features described below. Report options that you define when adding a new subscription override these general settings.



Note

These settings are used as the default options for new subscriptions. Changing these settings does not modify existing subscriptions.

Below is a summary of what you can do. Click **Apply** after you've made your selections.

Fallback language

For Fallback language, specify the language to use when the end user's browser uses a language for which there are no translations available.

There are 14 languages available:

- Czech
- Dutch
- English (U.K.)
- English (U.S.)
- French
- German
- Greek

- Italian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Slovak
- Spanish
- Swedish

Fallback timezone

Use the Fallback timezone drop-down to specify the default timezone used in the report.

Report frequency

Select how often the message report should be delivered.

If you select **daily** or **weekdays**, you can also configure multiple reports to be sent each day by choosing the hours when the report should be generated. Note that the maximum frequency is every 3 hours, so if you click 6, for example, 7 and 8 are disabled and the next hour you can select is 9.

Reporting period

Select the period over which the report will be run. This defines how many days' worth of data is included in the report. Select a period between 1 day and 30 days.

Report content

Use the check boxes to indicate which of the 6 possible sections to include in the message report:

- suspicious messages that have been quarantined (received and sent)
- suspicious messages that have not been quarantined (received and sent)—for example discarded or bounced messages, or a message that has had its subject line tagged because it matched a lexical rule
- clean messages (received and sent)

In the **Sort by** area, indicate the order in which you want suspicious and clean messages to be sorted:

- Date/Time
- Subject
- Originator
- Recipient
- Status

Also indicate whether you want the quarantined or non-quarantined messages to be sorted in ascending or descending order.

Allow end users to modify report content

Check this box if you want to allow end users to customize the content to include in their message reports and the order of that content. When this is checked, end users are given access to a customization page on their report. Any changes they make override your settings here.

Allow delivery of empty reports

Check this box if you want to send reports to end users even when there is no content to include in the report. If you do not check the box, the report is not sent if there is nothing to go into it.

List previously released messages

This box is checked by default. Check the box if you want to include in the report all messages that have already been released from quarantine, either by an administrator or the end user. Clear the box to remove all previously-released messages from the report.

Subscribe users from future user directory synchronizations



Note

This option may not be available in your account. To enable the option, contact Support.

If you are synchronizing your end users with the cloud service using the Directory Synchronization Client, you can check the **Subscribe users from future user directory synchronizations** box to subscribe new end users to the personal email reports rather than asking them to subscribe themselves. After you have checked this box, whenever there is an update of users in the directory and the update is synchronized to Forcepoint Email Security Cloud, the new users are automatically subscribed to the report.

Optionally, you can click **Subscribe current users** to subscribe all of your synchronized end users currently in the cloud.

The subscribed end users get a report in the format defined on this page. The report includes a link that, when clicked, subscribes the end user to the report on a weekly basis.

Text and Language tab

When a report is requested or scheduled for delivery, Forcepoint Email Security Cloud sends an email message that includes the personal email subscription report. To edit the text that appears in the email message, select **Email > Messages > Personal Email Subscriptions**, then go to the **Text and Language** tab.

Click **Add** to select a language for which you want to customize the text. Then follow the steps described below.

On the resulting screen:

Steps

- 1) From the **Language** drop-down menu, select the language you wish to use.
- 2) To specify customized email subject lines:
 - Clear the **Use the default value** boxes.
 - Supply a subject line for normal circumstances, one that you would like to appear when a user's report subscription is about to expire, and one to appear after it has expired.
- 3) Click **Submit**.

If you do not have any report content selected, an error results. Return to the Personal Email Subscriptions page, click **Edit**, check some boxes under **Report content** and try again. If the submission is accepted, **Edit Source** buttons appear.
- 4) Click **Edit Source** to customize the message text that appears at the top or bottom of the message. This allows you to edit the HTML source code for the message.
- 5) Type in the text editor's entry field.

You can also include predefined keywords in the text (for example, `_TOTAL_RECEIVED_`). When the report is generated, keywords are substituted with data, such as the total number of messages received.

To view the keywords that are available for substitution, click **View available keyword substitutions**. Click a keyword to paste it into the cursor position in the active field.
- 6) Click **Submit**.
- 7) To view how the message looks to users, click **View Report**.

Next steps

To put your customizations into effect, click **Enable this customization**, then click **Submit**. If you do not click **Enable this customization**, the text set for the default account is used. Click **Edit** to go back and edit the check boxes for email subject and **Enable this customization**.

Choose another language to edit if desired and customize the message for that language in the same way. Be sure to enable it before you submit it if you want it to take effect.

New languages that you add appear on the Text and Language tab page with a check if enabled. You can click on the link to the language, such as "en-us - English (US)" to edit the email message text for that language.

Bulk Upload tab

To upload multiple email aliases in CSV format, do the following:

Steps

- 1) Go to **Email > Messages > Personal Email Subscriptions**.
- 2) Open the **Bulk Upload** tab.

3) Browse to the CSV file that you wish to upload.

4) Click **Upload**.

Note that the uploaded CSV file updates existing subscriptions, adds any new subscriptions, and deletes existing subscriptions that are not in the CSV file. You can also download and edit current subscriptions from this page.

If you want to include the time zone for the report subscriptions in the bulk upload, you can download a list of all the supported time zones.

Email notifications

Notification messages can be sent when email is quarantined for any reason. Use the **Email > Policy Management > Notification Email** screen to view, edit, and delete notification messages.

Click **Add Notification** on the **Notification Email** screen to create a new notification message, or click the name of an existing notification message to edit the message contents and properties (See *Adding notifications* or *Editing notifications* for more information.) On this page, you can also set the time zone to use for dates that are included in notifications and park attachment annotations by clicking on the link next to **Time Zone**.

You can set up separate notification messages for different types of policy breaches and notifications to be sent to the intended recipient of an inbound email, the postmaster, and to other addresses of your choice within policies. You can also notify senders of outbound email but only if the outbound email is being sent from an address within your organization, not from an external address. Note that you cannot notify recipients of outbound messages.

Use the **General** and **Content Filter** policy tabs (navigate to **Policy Management > Policies** and click a policy name) to configure when notification messages are sent and which notification messages are used in each policy. (See *General tab* and *Content Filter tab* for more information.)



Note

By default, Forcepoint Email Security Cloud does not send a notification when email is quarantined as spam. A quarantine-notify disposition is available, but its use is not recommended.

Related concepts

[Editing notifications](#) on page 65

[General tab](#) on page 76

[Content Filter tab](#) on page 110

Related tasks

[Adding notifications](#) on page 62

Adding notifications

Click **Add Notification** on the **Notification Email** screen to write and configure a custom notification message from scratch, rather than using the default message.

Steps

- 1) Define a name and description for the notification message.
- 2) Select **Copy configuration from existing notification** to use an existing notification as a template for creating this one. Selecting this option copies the following data from the specified message:
 - Subject line prefix
 - Message body
 - Domain variations
- 3) Enter a subject line prefix (optional).

Note that if you type `_SENDER_` as part of the subject line prefix, this variable is replaced with the envelope sender address when the notification is generated.
- 4) If you want to change the character set used in the message (UTF-8 by default), select **Change character set** and select from the drop-down menu.

- 5) Enter the text for the notification in the message body field.

To view and use supported variables and tokens in notification messages, click **Variables/tokens** in the top toolbar.

Variables/tokens	Description
<code>_msgurl_</code>	Generates a partial URL that gives access to the message held in quarantine. Embed it using the syntax
<code>_NOTIFIED_RECIPIENTS_</code>	Generates a string if the intended recipients have been notified.
<code>_RECIPIENTS_</code>	The intended recipients of the message.
<code>_DATE_</code>	Displays the date Forcepoint Email Security Cloud received the email that generated the notification. The date is based on the time zone set on the Notification Email screen.
<code>_DISPOSITION_</code>	What happened to the message causing the notification. This usually takes the value "quarantined."
<code>_NOTIFIED_ADMIN_</code>	Generates a string if the specified postmaster has been notified.
<code>_MESSAGEID_</code>	The ID as specified in the message headers.
<code>_ENDIF_</code>	End of a <code>_IF_QUARANTINE_</code> or <code>_IF_ENCRYPT_</code> block
<code>_IF_ENCRYPT_</code>	Place this at the beginning of a section that is relevant only if the message has been encrypted. The section must end with <code>_ENDIF_</code> .
<code>_NOTIFIED_SENDER_</code>	Generates a string if the originator has been notified.
<code>_ADMIN_MAIL_</code>	The postmaster address for the policy.
<code>_DOMAIN_</code>	The domain associated with the currently active policy.
<code>_IF_QUARANTINE_</code>	Place this at the beginning of a section that is relevant only if the message has been quarantined. The section must end with <code>_ENDIF_</code> .
<code>_SENDER_</code>	The message originator.
<code>_SUBJECT_</code>	The subject of the message.

- 6) If you want to edit a separate plain text version of the notification message, select **Edit a separate plain text version**.

- 7) If you want to send a separate version of this message to specific domains when this notification is enabled, select **Send variations of this message for specific domains**. The **Add Domain Variation** screen appears.
 - a) Select or enter the intended domain in the **Domain** field.
 - b) Specify a **Subject line prefix** (optional).
 - c) Enter the text for the notification in the message body field.
 - d) Click **Save**.
 - e) If you want to add additional variations for other domains, you can repeat this process by selecting **Add variation** (the button will be disabled when all domains have a variation assigned to them).

- 8) Click **Save Changes** when done.

Editing notifications

Click the name of a notification message on the **Notification Email** page to edit the contents of the notification, the character set used, and variations of the message for specific domains.

For information about configuration options, see *Adding notifications*.

Related tasks

[Adding notifications](#) on page 62

Configure block and notification pages

Use the **Email > Policy Management > Block & Notification Pages** page to view and edit block and notification pages.

When an email policy denies access to a resource or needs to inform the user of an event, it can serve any configured notification page. There is a standard set of pages included with your email product, and you can either modify these to suit your needs, or add your own pages. You can then refer to the notification pages from any of your policies.

Standard block and notification pages include:

Phishing

(See *Phishing*)

Phishing Attack Blocked – This page provides information about phishing emails, including a definition of phishing, a description of common tactics, and an example of a phishing email message. You can either modify this to suit your needs, or add your own page. The page is then used if a user clicks a link in an email that is classified as part of a phishing attack.

URL Sandboxing

(See *URL Sandboxing tab*)

Analysis Declined – This page displays when the user elects to not analyze a suspicious link. (See **Prompt for Analysis**, below.) The default page title is **Analysis Declined**.

Malicious Threat Detected – This page displays when a suspicious link is determined to be malicious and is blocked. The default page title is **Access Denied**.

Prompt for Analysis – This page displays when a user clicks on a suspicious link in an email. This page notifies the user and gives the user the option to analyze the link. (The other standard notification pages handle the possible outcomes.) The default page title is **Suspicious Link**.

URL Verified – This page displays when an analyzed link is determined to be safe. The default page title is **URL Verified**.

Uncategorized URL – This page displays when the link submitted for analysis cannot be categorized. The default page title is **Access Denied**.

Unreachable URL – This page displays when a link cannot be reached. The default page title is **Unable to Analyze**.

Unsupported Protocol – This page displays when the protocol is not supported for analysis. The default page title is **Unable to Analyze**.

The pages are grouped for ease of navigation. Click a down arrow next to a group name to see a list of all the pages within that group. To see all available pages, click **All**.



Note

Pages that you create are listed under Custom.

To delete a custom page, click the delete icon next to the page name. The delete icon is displayed only if the custom page is not used in any policies.

Click the name of a page to edit its contents.

To create a new notification page:

- 1) Click **New Page**.
- 2) Enter a **Name** for the new page.
- 3) Enter a short **Description** of the page. This appears under the page name in the Block & Notification Pages list, and should clearly identify the purpose of the page to any administrator.
- 4) Click **Save**.
The Page Details page is displayed, with the name and description at the top. You can now edit the page as required.

For information about editing the content of a new or existing block page, see *Editing block and notification pages*.

If you are also a web protection customer, you can configure default options for your web policy block and notification pages. See *Default notification page settings*.

Related concepts

[Phishing on page 88](#)

[URL Sandboxing tab on page 92](#)

Related tasks

[Editing block and notification pages on page 68](#)

Default block and notification page settings

Use the **Settings** area to configure default options for your block and notification pages. You can override any of these settings for individual pages.

Default language

The default language for block and notification pages is English. You can change this by selecting a different language from the **Default language** drop-down list.

If you select a different default language and then click **Save**, your changes are immediately visible to end users. Ensure that you have saved pages in the new default language; if a page is not available in the new default language, the English page is displayed.

Default logo

By default, the logo displayed on the notification pages is the Forcepoint Email Security Cloud company logo. To change the logo:

Steps

- 1) Click **Edit**. The Default Logo popup window is displayed.
- 2) Select **Custom images**, and enter the URL of the image you want.
The image must be a JPEG, GIF, or PNG file. Click **Verify Image** to confirm the format and location of the image file.
- 3) Click **OK**. The new logo is displayed in the Settings area.
- 4) Click **Save**.

Default footer text

Any footer text that you specify appears at the bottom of each notification page. You may wish to use this area to provide contact information for end users.

To change the footer text:

Steps

- 1) Click **Edit**. The Footer Properties popup window is displayed.

- 2) Enter or edit text as required.
You can select all or part of your text and use the text formatting buttons to add bold, italic, color and other formatting. Hover over each text formatting button to see its function.
- 3) Click **OK** when done. The new footer text is displayed in the Settings area.
- 4) Click **Save**.

Editing block and notification pages


Each block and notification page is a complete HTML page. The **Page Details** page presents a simple view of the page with editable sections, enabling you to customize the text and images.

To change the content of a block or notification page:

Steps

- 1) For custom pages, click **Edit** to update the page **Name** or **Description**. Click **Save** when done.
- 2) To change the page name that appears in the browser's title bar, edit the **Page title** field.
- 3) Hover your mouse over the page content to highlight the sections that are editable. To edit a line of text or block of content, click its section to open a text editor window.
- 4) Edit the text as required.
You can select all or part of the text and use the text formatting buttons to add bold, italic, color and other formatting. Hover over each text formatting button to see its function.
Click **OK** when done.
- 5) To edit the page footer:
 - a) Click the footer section to open a text editor window.
 - b) Enter the footer text to use for this notification page. You can select all or part of the text and use the text formatting buttons to add bold, italic, color and other formatting.
 - c) Click **OK** when done.

- 6) To edit an image on the page:
 - a) Click on the image. The Image Properties popup window is displayed.
 - b) To use one of the standard images, select **Standard images** and click on the image you want.
 - c) To use an image of your choosing, select **Custom images** and enter the URL of the image you want. The image must be a JPEG, GIF, or PNG file. Click **Verify Image** to confirm the format and location of the image file.
 - d) Click **OK**.
- 7) To view and edit the HTML source, click **HTML Editing**. Any valid HTML may be used within a notification page.



Note

If you edit a page in the HTML view and then click **Basic Editing** to return to the basic editor, you will lose any changes made in the HTML view.
- 8) To see how the page appears to end users, click **Preview**. The page appears in a separate window.
- 9) Click **Save** when done.

If you want to discard customizations made to a standard page, click **Revert to Default**. This removes all changes that have been made to the page in your account, and reverts the page to the original one supplied in Forcepoint Email Security Cloud.

Image allowlist

Select **Email > Settings > Image Allow List** to view and edit the list of images that are not analyzed by Forcepoint Email Security Cloud.

**Note**

You must have the Forcepoint Email Security Image Analysis Module to use this feature.

Add images to the allowlist if they are known to be clean – for example, you might want to add acceptable images that have been quarantined to ensure they do not get blocked in future.



**Note**


You can allowlist images directly from the Message Center. See *Managing quarantined images*.

The image allowlist can contain a maximum of 200 images. Images are displayed in the order they were added, with the most recent at the top.

To add an image on the Image Allow List page:

Steps

- 1) Click **Browse**, and navigate to the location of the image file on your network.
- 2) Select the image, then click **Open**.
- 3) Click **Upload**.
The image is added to the top of an allowlist.
- 4) To edit the image name, click the pencil icon under the image thumbnail and enter the new name. Click  to confirm the name, or  to cancel the edit.

To remove an image from the allowlist, click the  icon in the top right corner of the image thumbnail.

Related concepts

[Managing quarantined images](#) on page 152

Email connectivity testing

If you think that inbound or outbound messages are not being delivered, use the mail testing options to check connectivity. The inbound mail test checks your MTAs and performs testing for the domain you specify, optionally based on sender and recipient addresses. The outbound mail test requires sender and recipient information to perform checks on whether mail is being routed correctly.

Related tasks

[Inbound mail testing](#) on page 70
[Outbound mail testing](#) on page 71

Related reference

[Viewing results](#) on page 71

Inbound mail testing

To perform an inbound mail test:

Steps

- 1) Go to **Email > Messages > Toolbox**.
- 2) Select the **Inbound Mail Test** tab.

- 3) Select the domain you wish to check against.
- 4) Optionally, enter a sender address.
- 5) Optionally, enter a recipient address.
- 6) Click **Run Test**.
Running the test does the following for all the connections and mail routing rules that apply to the specified domain:
 - Checks connectivity to your MTA
 - Performs a full SMTP test
 - Checks TLS functionality
 - Generates a message from the cloud email service to your selected domainIf one of these tests fails, subsequent tests are not performed.

Outbound mail testing

To perform an outbound mail test:

Steps

- 1) Go to **Email > Messages > Toolbox**.
- 2) Select the **Outbound Mail Test** tab.
- 3) Enter a sender address. This must be for a domain registered and checked with your cloud service account.
- 4) Enter a recipient address.
- 5) Click **Run Test**.
Running the test does the following:
 - Checks the outbound route connectivity to the recipient domain
 - Generates a message from the cloud email service to your selected recipient domain using TLS

Viewing results

Feedback is displayed in a popup on screen while the tests are running, and results are displayed on the page once available. Click **Download Full Results** to download detailed results to a text file in a location of your choice.

You may see one or more of the following in your results:

Problem	Resolution
SMTP Test Failure	The cloud service could not connect to port 25 on your connection. Confirm port 25 is open, and also check the text file for traceroute results for that connection, to see where the connectivity error occurs.
Server Security Error	<p>The cloud service could not connect to your domain using the security settings specified in the connection. This may be due to one of the following:</p> <ul style="list-style-type: none"> ■ the host name could be verified against the certificate. Ensure the common name on the certificate matches the MTA with which the cloud service is communicating. ■ The security settings are set to Encrypt or Encrypt +CN and the certificate is not from a trusted certificate authority (CA). ■ The connection does not support the encryption strength set in the policy (encryption algorithms must support a 128 or 256 bit key).
TLS error	The cloud service could not send a message to either the connection or the mail recipient using TLS. If you have enabled mandatory TLS, ensure all security settings between the cloud service, your MTAs, and all required third-party MTAs are configured correctly.
Outbound route connectivity failure	The cloud service could not connect to the recipient domain's MTA. This may be because port 25 is not open, or because the connection attempt timed out.

URL Sandboxing utility

With URL sandboxing, if users click on a link within an email and that link or elements associated with that link are suspicious, they receive a warning that "The link may not be safe." To view details of a URL that has the URL sandboxing feature applied to it:

Steps

- 1) Go to **Email > Messages > Toolbox** and select the **URL Sandboxing Utility** tab.

- 2) Enter a sandboxed URL, and then click **Submit** to show the original URL and its recipient, security and policy settings. An administrator in the account that sandboxed the URL sees:

Sandboxed URL	Shows the sandboxed URL entered.
Original URL	Shows the original URL before sandboxing.
Block Policy Flags	Shows if the recipient is allowed to see unclassified URLs. Also shows if suspicious URLs are masked for the recipient.
Policy Name	Shows the name of the policy that owns the recipient domain.
Recipient	Shows the email address of the recipient of the message containing this URL.

An administrator in the account that did not sandbox the URL only sees:

- Sandboxed URL
- Original URL
- Block Policy Flags
- Recipient email address

Chapter 5

Defining Email Policies

Contents

- [Introduction](#) on page 75
- [General tab](#) on page 76
- [Domains tab](#) on page 80
- [Connections tab](#) on page 83
- [Antivirus tab](#) on page 88
- [URL Sandboxing tab](#) on page 92
- [Antispam tab](#) on page 95
- [Antispoofing tab](#) on page 104
- [Content Filter tab](#) on page 110
- [Encryption tab](#) on page 128
- [Data Protection tab](#) on page 140

Introduction

To configure an email policy, select **Email > Policy Management > Policies**, then click the name of the policy to configure. If you have not previously configured a policy, click the policy named **DEFAULT**. You can rename the default policy to something more meaningful to your organization, especially if you plan to create multiple policies.

Notice that each policy has multiple tabs to configure:

- *General tab*
- *Domains tab*
- *Connections tab*
- *Antivirus tab*
- *URL Sandboxing tab*
- *Antispam tab*
- *Antispoofing tab*
- *Content Filter tab*
- *Encryption tab*
- *Data Protection tab*

Click the link to learn how to configure each one of these settings. Standard account-level settings are shown in *Standard Email Configuration*.

Use the **Policy Management > Notification Email** screen to configure notification messages sent when email is quarantined (see *Email notifications* for more information).

Related concepts

[General tab](#) on page 76
[Domains tab](#) on page 80
[Connections tab](#) on page 83
[Antivirus tab](#) on page 88
[URL Sandboxing tab](#) on page 92
[Antispam tab](#) on page 95
[Antispoofing tab](#) on page 104
[Content Filter tab](#) on page 110
[Encryption tab](#) on page 128
[Data Protection tab](#) on page 140
[Email notifications](#) on page 62

Related information

[Standard Email Configuration](#) on page 227

General tab

The **General** tab lets you perform general functions on your email account. There are 2 functional areas on this screen:

- *General policy information*
- *Notifications and Annotations*

To change a policy name or postmaster address for a policy, click **Edit** under the general policy information.

To enable notifications or annotations for inbound mail, click **Edit** in the Inbound box. To enable notifications or annotations for outbound mail, click **Edit** in the Outbound box.

On the resulting screen, use the check boxes to indicate whether you want to notify senders, recipients, or others, and whether you want to annotate messages. You can only notify senders of outbound email if the outbound email is being sent from an address within your organization, not from an external address. Note that you cannot notify recipients of outbound messages.

Related concepts

[General policy information](#) on page 76
[Annotations](#) on page 77

Related tasks

[Notifications](#) on page 77

General policy information

To change a policy name or postmaster address for a policy, click **Edit** in the top section of the **General** tab.

Complete the fields as follows:

Field	Description
Policy Name	Enter a name for the policy.
Postmaster	Enter an email address for the postmaster. The postmaster address is used as the address from which system notifications are sent. Your users may occasionally reply to these notifications, so this should be an email address that is monitored by your IT staff or administrative contact.

Click **Submit** when you're done.

Notifications

Notification messages can be sent when email is quarantined for any reason. Use the **Policy Management > Notification email** screen to view, edit, and delete notification messages. For more information, see *Email notifications*.

In a policy, you can set up different notifications to be sent for inbound and outbound messages.

To define the notifications used in a policy:

Steps

- 1) On the General tab, click **Edit** under either Inbound or Outbound.
- 2) Specify who receives a notification message when an email is quarantined. You can select the recipient (for inbound messages only), the sender (for outbound messages only), the administrator, or others. If you select Others, enter the email address(es), separated by commas.
- 3) For each option that you specify in step 2, select a notification message from the drop-down list.
- 4) Click **Submit**.

Related concepts

[Email notifications](#) on page 62

Annotations

Annotations are added to messages as they pass through Forcepoint Email Security Cloud. By default, they are set up for entire policies; however, you can also set up more specific annotations.

Examples of annotations that you might add to inbound messages are, Click [here](#) to report this message as spam, and "This message has been analyzed for malware by Forcepoint Email Security Cloud."

For inbound email, you can create annotations specific to each domain in your policy. For outbound email, you can create annotations specific to an arbitrary list of sender domains, sender email addresses, or groups.

If you have the Forcepoint Email Security Encryption Module, you can also add specific annotations for decrypted messages. These annotations are created from the **Encryption** tab; see *Editing advanced encryption settings*.


Related tasks

[Editing advanced encryption settings](#) on page 139

Editing an annotation

Because email can be sent as HTML or plain text, Forcepoint Email Security Cloud maintains two versions of each annotation. To edit an annotation:

Steps

- 1) On the **General** tab of a policy, click one of the **annotation** links (taking care to choose an Inbound or Outbound annotation).
- 
- Note**
- If you are adding an annotation for a decrypted message on the **Encryption** tab, click **Edit**, then click the **annotation** link.
- 2) On the resulting screen, click the annotation name of interest, or click ***. * [default]** to view the default annotation.
 - 3) Indicate where you want annotations to be placed in each message by selecting **Top** or **Bottom** from the **Position** drop-down list.
 - 4) Choose a default character set from the drop-down list.
 - 5) Click **Edit HTML**. For best results, use the most recent version of Internet Explorer available.
 - 6) Make whatever changes you wish to the annotation. The limit is 4 KB.
If you want to embed a message in the annotation, use the substitution tag `_MESSAGE_`. When the `_MESSAGE_` tag is present, Forcepoint Email Security Cloud ignores the “Top” or “Bottom” setting and wraps the annotation around the message text. You can use this tag to add annotations to the top and bottom of messages at the same time.
 - 7) Click **Submit** to save your changes.
 - 8) Click **Edit Plain Text**.
 - 9) Repeat your text changes. Plain text messages also have a 4 KB limit.
 - 10) Click **Submit**.

- Repeat for each annotation that you want to edit.



Note

If your HTML annotation contains a block of text, it is recommended that you split up the lines with line breaks. Lines longer than 190 characters can cause unwanted exclamation marks to appear in the annotation.

Make sure that annotations are enabled for this policy by checking the annotation box on the policy page.

Report this email as spam



Important

If you choose to edit the default inbound annotation, you lose the **Report this email as spam** feature. See *Report this email as spam* for more information.

We strongly recommend that you apply the default inbound annotation “Click [here](#) to report this email as spam.” For new policies, this annotation is enabled by default. This gives users immediate feedback and helps us tune our spam filter for future releases. Here is the feedback that users receive when they click this link:

Report as Spam

Thank you for reporting this spam message.

We are committed to delivering the best possible spam protection and your action helps us achieve this. Please continue to report any messages which you believe to be spam in this way.

Although you will not receive any further update from us about this spam message, the anti-spam system is being automatically updated to treat similar messages with more suspicion in future. This will reduce the likelihood of your receiving them again.

Reporting this message will not automatically block all messages from this sender - if you want to do this you should add the sender to your blacklist. See the user guide or contact your email administrator for further instructions.

To aid in the process of spam tuning, when you use the “Report as spam” annotation, we recommend that you configure Forcepoint Email Security Cloud to keep a private copy of clean email messages for a short period, separate from the quarantine area (see *Keep a copy of clean messages*). If Forcepoint Email Security Cloud has the original message available, our operations staff and automated systems can analyze the message.

Related concepts

[Keep a copy of clean messages](#) on page 96

Adding annotations

If desired, you can write an annotation message from scratch rather than editing the default. Just click **Add** on the Inbound or Outbound Annotations screen.

On the resulting screen:

Steps

- Choose the domain or address list to annotate.

- 2) Choose the position of the screen on which to put the annotation: bottom or top.
- 3) Choose the default character set to use.
- 4) Enter text into the text editor as desired.
- 5) Click **Submit** when done.

Make sure that annotations are enabled for this policy by checking the annotation box on the policy page. A check indicates enabled. An X indicates disabled.

Domains tab

Select the **Domains** tab on the policy to view or change domains for the policy.

Each Forcepoint Email Security Cloud policy applies to a set of domains. Before a domain is accepted by Forcepoint Email Security Cloud and processed according to your policy, it must first be checked to ensure that we can deliver mail for the domain to your mail server and that the domain does in fact belong to your company.

The **Route Status** column displays the result of the inbound route check. The **Ownership Status** column shows the result of each domain's ownership check. Status can be **Unchecked** (awaiting validation or check failed; unavailable for use within policy), or **Checked** (check passed; active within policy). To view more details of the domain and its status, click the domain name link. If your domain has failed one or both of its checks and the domain does belong to you, please contact Support.

When viewing a domain for a policy, click **Show MX records** to check the MX record configuration for the domain.

Adding domains

To add domains to any policy (including the default policy), you must first set up a valid inbound connection on the *Connections* tab that will accept messages for the domain you plan to add. A valid inbound connection is one that accepts messages on port 25 for the domain. If it is behind the firewall, the firewall must allow email traffic from the IP address ranges listed on the *DNS records and service IP addresses* page. The connection is checked as part of the validation.

To add a domain or sub-domains to the policy:

Steps

- 1) Click **Add** on the **Domains** tab.
- 2) Enter the domain name in the **Domain** field.
- 3) To apply the policy to all sub-domains in the current domain, select **Include sub- domains**.
- 4) Select **Outbound only** configuration to process only outbound messages for the registered Outbound only domains, inbound email processing is not applied to these domains.

5) Click Submit.

At this stage Forcepoint Email Security Cloud checks for a valid inbound connection for this domain and displays the result on the Add Domain screen. If it cannot find or validate a connection, an error message appears.

**Important**

The inbound connection checking does not guarantee the correct delivery of email messages. It is strongly recommended that you run your own testing on the inbound connection that you have specified.

Outbound only domains do not require route connectivity tests.

The Add Domain screen also displays the following options for you to verify ownership of the domain you have entered. The ownership check initially displays as **Failed**, because it cannot succeed until you have done one of the following:

- Create a CNAME record in your DNS that aliases the character string shown on the screen to autodomain.mailcontrol.com. For more information, see *CNAME records and A records*.
- Create an A record for the character string shown on the screen, pointing to the IP address of autodomain.mailcontrol.com. For more information, see *CNAME records and A records*.
- Add your customer-specific DNS records into your MX records in your DNS. For more information about adding and editing MX records, see *MX records*.

Once you have made one of the above changes, click **Check Now**.

**Important**

If you choose to use MX record verification, the service will accept email messages for this domain as soon as the MX records are set up.

MX record checking is not available for outbound only domains.

If you return to the list of domains on the Domains tab before the required record has been added or successfully propagated, the details you entered appear in the domain list with the status **Unchecked**. Once you have created the required records, click the domain name to view the details, and then click **Check Now** again to retry the validation.

**Important**

Do not configure domains until you are ready to verify ownership, because all domains are marked **Rejected** after 7 days if ownership verification has not been completed. You must then call Support to edit or re-enable the domain.

Related concepts

[Connections tab](#) on page 83

[DNS records and service IP addresses](#) on page 54

[CNAME records and A records](#) on page 81

[MX records](#) on page 82

CNAME records and A records

Contact your DNS manager (usually your Internet service provider) and ask them to set up either a CNAME record or an A record as directed on the Add Domain page.

CNAME records

CNAME records are used to assign an alias to an existing hostname in DNS. A CNAME record might look like this:

abcdefgh.mydomain.com CNAME automain.mailcontrol.com.

Where CNAME indicates that you are specifying a CNAME record.

Make sure you include the trailing period in the domain name. Both the domain name and the character string are provided on the Domains screen when you add a new domain.

The above example indicates that *abcdefgh.mydomain.com* is forwarded to *automain.mailcontrol.com*. This enables Forcepoint Email Security Cloud to confirm that you own *mydomain.com*.

A records

An A record is the Address record which maps a domain or subdomain to a valid IP address. In this case, it is matching a character string provided on the Add Domain screen. The record indicates that the specified string can be reached at the given IP address.

An A record might look like this:

abcdefgh.mydomain.com IN A 86.111.217.190

Where

- IN indicates Internet
- A indicates the Address record.

The above example indicates that the IP address for *abcdefgh.mydomain.com* is 86.111.217.190.

MX records

An MX record is an entry in a DNS database that defines the host willing to accept mail for a given machine. Your MX records must route email through Forcepoint Email Security Cloud to your Internet mail gateway.

Your DNS records, which end in **in.mailcontrol.com**, are available on the *DNS records and service IP addresses* page.

Contact your DNS manager (usually your Internet service provider) and ask them to set up or replace your current MX records for the domain you have added with the customer-specific DNS records listed on the *DNS records and service IP addresses* page (the ones that end in **in.mailcontrol.com**). For example, they might change:

Change	From	To
MX Preference 1	mydomain.com. IN MX 50 mail.mydomain.com.	mydomain.com. IN MX 5 cust000-1.in.mailcontrol.com.
MX Preference 2	mydomain.com. IN MX 51 mail.mydomain.com.	mydomain.com. IN MX 5 cust000-2.in.mailcontrol.com.

Make sure they include the trailing period, and ask them to set both of these records to an equal preference value.

It can take up to 24 hours to propagate changes to your MX records across the Internet. During this time, you should keep your previous mail routing active to ensure all your mail is delivered: while your MX records are

changing over, some mail will be delivered using your old MX information, and some mail will be delivered using your new MX information.

Related concepts

[DNS records and service IP addresses](#) on page 54

Connections tab

Select the **Connections** tab on the policy to view or change connections for the policy. Your policy must have at least one default inbound connection and one outbound connection in order to be active on the system.

The **Inbound Mail Routing Rules** section of the tab specifies rules that route inbound mail from Forcepoint Email Security Cloud to particular email servers depending on the recipients. The rules are applied in the order listed; you can change the order by dragging the priority numbers up and down the list, then clicking **Save Order**.

To add a new inbound mail routing rule, click **Add New Rule**, then see *Configuring inbound mail routing rules*.

You can check which of your mail routing rules, if any, applies to a particular email address by clicking **mail routing test utility**. See *Testing mail routing*.

The **Default Inbound Routes** section defines where the service sends email that is not matched by an inbound routing rule after processing messages received from the Internet - these are the connections to your email servers.

The **Outbound** box specifies from which connections the service is prepared to accept email for your domains (for onward delivery to the Internet).

Note that the service always attempts to deliver or receive email messages over a TLS connection if the sending or receiving MTA supports it. If opportunistic TLS is not available, the data transfer is made via plain text, rather than encrypted text. In either case, the data transfer is successfully accomplished. If you wish to use mandatory TLS, see *Transport Layer Security*.

Related concepts

[Transport Layer Security](#) on page 128

[Testing mail routing](#) on page 85

Related tasks

[Configuring inbound mail routing rules](#) on page 83

Configuring inbound mail routing rules

Click **Add New Rule** on the **Connections** tab to add an inbound routing rule that applies to specified users, groups, domains, or content types. This enables you to route mail to different mail hosts for certain groups of users in your network, useful if, for example, your organization has multiple mail servers for different locations or subsidiaries.

If a message is sent to a user who is in more than one group covered by your inbound routing rules, the first rule in the list that matches the user will be applied. A message sent to multiple users who have different routing rules will be split into multiple copies and routed as configured for each individual user.

If you set up a content type rule, the rule is applied to messages that are encrypted with PGP. You can apply that rule to all PGP-encrypted messages, or choose to apply it to messages for specific users, groups, or domains.

Before it can be enabled for mail routing, a rule must be checked to ensure the following:

- Forcepoint Email Security Cloud can connect to the specified inbound mail hosts.
- The mail hosts accept messages for all domains explicitly specified in the rule. This is required for the rule to be valid.
- The mail hosts accept messages for the domains contained in all email addresses explicitly specified in the rule. This is required for the rule to be valid.
- The mail hosts accept messages for at least one domain within the policy.




Note

If a group includes a domain that the mail hosts do not accept messages for, some mail may not be delivered. We recommend that you check your groups for domains not accepted by your mail hosts, and that you recheck your inbound mail routing rules if you change or resynchronize your groups in the portal.

The mail host checking takes place as you configure the inbound rule.

Steps

- 1) Enter a **Rule Name**. This is required.
- 2) In the **Apply To** field, enter one or more recipients for the rule to apply to. These can be individual email addresses, groups configured in Forcepoint Email Security Cloud, or domain names. You can enter multiple recipients, separated by commas.
This field is required unless you are creating a rule that routes by content type and select **PGP Encrypted only** as described below.
To edit an existing recipient, click the item. Press **Enter** to save your changes as a new entry in the Apply To list. To discard your changes, press **Esc**.
To remove an item from the Apply To list, click the Delete icon next to the item.
- 3) To apply the rule only to confidential messages encrypted with PGP, mark **PGP Encrypted only**.
If you select this option, the **Apply To** field is no longer mandatory.
- 4) Optionally, select a **Security** value: Unenforced, Encrypt, Encrypt+CN, Verify, or Verify+CN. See *Encryption tab* for further information.
- 5) If you are enforcing security, select an **Encryption Strength**: 128 or 256.
- 6) Click **Add Mail Host** to add a receiving mail server to the rule.
You can add up to 10 mail hosts to a rule. If Forcepoint Email Security Cloud cannot deliver inbound email to the first mail host in the list, it tries the other servers in order until the message is delivered. To change the order of the mail hosts, click an order number and drag it up or down the list.

- 7) Enter a **Host Name** (for example mail.mycompany.com) for the server. If the host name cannot be resolved on the Internet, enter an **IP Address** for the server as well. Click the  button to confirm.

Forcepoint Email Security Cloud checks the mail host and sets the **Status** to Passed or Failed.

If the route check failed, click Failed to open a popup window that displays details of the failure. Filter the results of the check to view domains that are required or optional for the rule, and those that passed or failed.

In this window, you can recheck all the domains in the rule, or just the domains that failed. You can also choose to **Ignore Failed** domains, which changes the mail host's **Status** to Passed. Be aware that if you ignore failed domains, some messages may be undelivered.

You can edit the server settings by clicking the pencil button.


- 8) To enable the rule for use, mark **Enabled**.



Note

At least one mail host in the list must pass the check for the rule to be saved as enabled. If the check fails, you can still save the rule, but you must first clear the **Enabled** check box.

If you make changes to the rule, for example changing the recipients it applies to or editing the

Security settings, each mail host must be rechecked. Click the **Check all mail hosts**  button to run the check again.

- 9) Once you have finished configuring your rule, click **Save**.

Related concepts

[Encryption tab](#) on page 128

Testing mail routing

The mail routing test utility enables you to check which inbound mail routing rules apply to specific email addresses.

Enter one or more email addresses, separated by commas. If you have defined mail routing rules that apply to PGP-encrypted messages, you can select **Show rules for PGP emails to these addresses** to include those rules in your test. Then click **Test Addresses**.

The Test Results section contains a line for each entered email address, displaying which groups the address is a member of, and which inbound routing rule or rules, if any, applies to the address. Click on a rule name to see and edit the rule details.

Adding inbound routes

To add an inbound route:

Steps

- 1) On the Connections tab, click **Add** under **Default Inbound Routes**.

- 2) In the **Server** field, enter a fully qualified host name or an IP address.
If you enter an IP address you are asked to give this connection a name. The name you give your IP address connection is not important and can just be “inbound” or whatever you feel is appropriate.
If you enter an invalid IP address such as one from the reserved, private range, an error results.
- 3) Enter a **Preference** value to specify the order in which connections should be used. (Connections with preference value 1 are used before all other connections.)
- 4) Optionally, choose a **Security** value: Unenforced, Encrypt, Encrypt+CN, Verify, or Verify+CN. See *Encryption tab* for further information.
- 5) If you have selected a Security value, select an **Encryption Strength**: 128 or 256.
- 6) Click **Submit**.

Related concepts

[Encryption tab](#) on page 128

Adding outbound routes

To add an outbound route:

Steps

- 1) On the Connections tab, click **Add** under **Outbound Routes**.
- 2) In the **Server** section, either:
 - Select Server name or IP address, and enter a fully qualified host name or an IP address.
If you enter an IP address you are asked to give this connection a name. The name you give your IP address connection is not important and can just be “outbound” or whatever you feel is appropriate.
If you enter an invalid IP address such as one from the reserved, private range, an error results.
Or:
 - If your organization is using Microsoft Office 365 for email, select **Office 365**.
Or:
 - If your organization is using Google Apps for email, select **Google Apps**.



Note

If you select Office 365 or Google Apps, you must configure the outbound mail gateway in your Office 365 or Google Apps account to point to your customer- specific DNS records. These are the records ending in “out.mailcontrol.com” on the *DNS records and service IP addresses* page.

- 3) Optionally, choose a **Security** value: Unenforced, Encrypt, Encrypt+CN, Verify, or Verify+CN. See *Encryption tab* for further information.

**Note**

If you have selected Office 365 or Google Apps in the **Server** section, you cannot set encryption options as part of the connection. To enforce encryption on your outbound route, configure your Office 365 or Google Apps account.

If you have the Email Security Encryption Module, all outbound connection routes must have a security value of Verify+CN. See *Advanced encryption* for further information.

- 4) If you have selected a Security value, select an **Encryption Strength**: 128 or 256.
- 5) Click **Submit**.

Related concepts

[Encryption tab](#) on page 128

[DNS records and service IP addresses](#) on page 54

[Advanced encryption](#) on page 136

Disaster recovery

Forcepoint Email Security Cloud provides a number of features that can help in the event of a major disaster or a failure of your Internet connectivity or email server.

Specifying secondary routes

If Forcepoint Email Security Cloud cannot deliver inbound email to the primary connection specified it looks to see if a secondary connection is configured. This can be to a backup email server or a disaster recovery site.

Email queuing

If Forcepoint Email Security Cloud cannot deliver email to any of the specified inbound connections, it queues all email for up to seven days and attempts to deliver queued email to each route approximately every thirty minutes. The queue operates on a first-in first-out basis, so the oldest email is delivered first when a connection becomes available.

Connectivity test

For an inbound connection, click **Test** to carry out a connectivity test to its destination from your Forcepoint Email Security Cloud clusters. The connectivity test shows you the response Forcepoint Email Security Cloud received from the email server, plus information about the time taken to reach that destination. You can run this test from various clusters in order to troubleshoot local connectivity issues.

Antivirus tab

Select the **Antivirus** tab on the policy to set up rules for antivirus protection.

Listed are the inbound and outbound antivirus rules that have been set for this policy. To edit the inbound or outbound rules, click **Edit** in either the **Inbound Rules** or **Outbound Rules** box.

Editing inbound or outbound rules

The majority of the antivirus functionality is the same for inbound and outbound email. Field descriptions are provided below.

Virus

Check this box if you want viruses to be quarantined when detected. Viruses are software programs capable of reproducing themselves and usually capable of causing great harm to files or other programs on the computer.

Phishing

This option is applicable to inbound email only. Define whether suspected phishing messages should be quarantined, or allowed with suspicious URLs replaced by a link to a block page that you specify.

To set up block pages for phishing messages, see *Configure block and notification pages*.

To bypass phishing checks for certain users, domains, or groups, click **Phishing Exceptions**. See *Antivirus exceptions*.

Related concepts

[Configure block and notification pages](#) on page 65

[Antivirus exceptions](#) on page 91

Content

Filter active HTML content

This ThreatSeeker Intelligence feature automatically analyzes HTML inside messages and disables any potential dangerous content (by disabling specific HTML tags). You can define how strictly the system applies this security feature. Available settings are:

Setting	Description
Low	Disable embedded scripts (<SCRIPT> and <OBJECT> tags) and disable unknown HTML tags that are deemed to be potentially dangerous.

Setting	Description
Medium	As Low but also disable “Web bugs” (URLs that are referred to inside a message, excluding links to images) and HTML styles that contain code.
High	As Low but disable all “Web bugs” and all HTML styles.
Very high	Extremely strict: as High, but this also disables all hypertext links to protect against a number of known vulnerabilities in common email clients.

The recommended setting is **Medium**; setting the level higher than this may cause messages to display too poorly for general users.

Block potentially malicious macros

This feature looks for potentially malicious macros in common Microsoft Office document formats. By changing the sensitivity, you can control how suspicious Forcepoint ThreatSeeker Intelligence is when it carries out its analysis. We recommend setting this to High initially. You may need to amend this setting if you find that a lot of documents just over the threshold are being quarantined. Documents containing known viruses are quarantined by the antivirus engines, regardless of this setting.

Strict checks on message structure

This feature runs a set of structural checks on email messages to determine whether they conform to an accepted structure. For example, one of the attachment checks would quarantine a MIME attachment with a filename that ends in a period but has no file extension (such as “attachment1.”). Messages with a malformed message structure can be a potential attack vector.

This option is disabled by default. We recommend leaving it disabled unless you are running an old mail client that may be vulnerable to malformed email messages, or if you are performing penetration testing on your messages. Enabling this feature may result in false positives.

Encrypted Messages

An encrypted email message must be decrypted before it can be analyzed for viruses. Since the cloud service does not have access to the necessary decryption key, it cannot analyze an encrypted message. Similarly, the contents of a password-protected archive file attachment such as ZIP or RAR cannot be analyzed, because the password is unknown. To protect against the possibility of virus infection, Forcepoint Email Security Cloud allows such messages to be quarantined. Administrators can open quarantined messages later in a secure environment.

Select the **Quarantine all messages containing encrypted archive files** checkbox to quarantine emails with password-protected archive files attached (such as ZIP or RAR files).

Select the **Quarantine all encrypted messages** checkbox to quarantine encrypted email messages (such as those using PGP or S/MIME encryption). This setting also quarantines emails with password-protected PDF files or Microsoft Office files (such as DOC or DOCX) attached.

Encrypted Message Bypass

Encrypted Message Bypass is used to override the encrypted message settings for specific sender/recipient, domain, and group.

To enable the bypass setting:

Steps

- 1) Navigate to the **Antivirus** tab and click **Encrypted Message Bypass**.
- 2) Click **Add** to add a new rule.
- 3) Enter a name in the **Name** field.
- 4) Enter the sender email address, domain, or group in the **Sender** field.
- 5) Enter the recipient email address, domain, or group in the **Recipient** field.



Note

Accepted values for Sender and Recipient fields are *, a single email address, a single domain, or a single group. The * character can be used to apply the rule to any address. Include all addresses for a domain by using `*@domain.com`.

For the Inbound policy, the group option is available for the Recipient field, and for the Outbound policy, the group option is available for the Sender field.

Email addresses are case sensitive. Ensure email addresses are added using lowercase.

- 6) Enter the description in the **Description** field.
- 7) Toggle the **State** switch to **ON** to enable the rule.
- 8) Click **Save**.

Executables

To protect against the possibility of virus infection, Forcepoint Email Security Cloud allows you to quarantine messages whose contents appear to contain scripts or executables, or with attachments with potentially dangerous file extensions.

Administrators can view quarantined messages later in a secure environment.

Select **Quarantine messages containing scripts and executables** to quarantine emails containing scripts and executable file attachments (such as EXE or BAT files).

Select **Deliver all containing scripts and executables** to allow email messages containing scripts and executable files.

To allow executables for certain users, domains, or groups, click **Executable Exceptions**. See *Antivirus exceptions*.



Warning

Forcepoint Email Security Cloud uses commercial antivirus (AV) engines to identify known viruses, and its own ThreatSeeker Intelligence technology to identify viruses for which AV vendors have not yet released a patch. However, even with multiple layers of protection, it is impossible to predict the types of exploit that may become available to malicious actors. We recommend that, where possible, email containing executable attachments be quarantined. If this is not appropriate for all users, best practice is to enforce this policy globally and use the Executable Exceptions option for specific users.

Quarantining messages containing scripts and executables

If you choose to block scripts and executables, messages containing any file whose contents appear to be executable are blocked, along with those with the following potentially dangerous file extensions: A6P, AC, ACR, ACTION, AIR, APK, APP, APPLESCRIPT, AWK, BAS, BAT, BIN, CGI, CHM, CMD, COM, CPL, CSH, DEK, DLD, DLL, DRV, DS, EBM, ELF, ESH, EXE, EZS, FKY, FRS, FXP, GADGET, GPE, GPU, HLP, HMS, HTA, ICD, IIM, INF, INS, INX, IPA, IPF, ISU, JAR, JS, JSE, JSX, KIX, KSH, LIB, LNK, MCR, MEL, MEM, MPX, MRC, MS, MSC, MSI, MSP, MST, MXE, OBS, OCX, PAF, PCD, PEX, PIF, PL, PLSC, PM, PRC, PRG, PVD, PWC, PYC, PYO, PY, QPX, RBX, RGS, ROX, RPJ, SCAR, SCPT, SCR, SCRIPT, SCT, SEED, SH, SHB, SHS, SPR, SYS, THM, TLB, TMS, U3P, UDF, VB, VBE, VBS, VBSCRIPT, VCARD, VDO, VXD, WCM, WIDGET, WORKFLOW, WPK, WS, WSC, WSF, WSH, XAP, XQT.

Related concepts

[Antivirus exceptions](#) on page 91

Antivirus exceptions

Exceptions are available for the following options on the Antivirus tab:

Related tasks

[Phishing Exceptions](#) on page 91

[Executable Exceptions](#) on page 91

Phishing Exceptions

Click **Phishing Exceptions** to override the phishing settings for named users, groups, or domains. Click the appropriate policy in the **Apply to** column of the Phishing Exceptions screen. You can then change the way phishing messages are handled for specific users, groups, or domains. For example, you can allow URLs to be replaced in messages for certain groups (such as marketing), and quarantine messages for other groups.

To create an exception:

Steps

- 1) Click **Add phishing exception**.
- 2) Choose an email address, domain name, or group from the list. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user's email address, not LDAP user name.
- 3) Define whether suspected phishing messages should be quarantined, or allowed with suspicious URLs replaced by a link to a block page that you specify.
- 4) Click **Submit**.

Executable Exceptions

Click **Executable Exceptions** to override the executable settings for named users, groups, or domains.

Click the appropriate policy in the **Apply to** column of the Executable Exceptions screen. You can then change the way executables are handled for specific users, groups, or domains. For example, you can deselect “Quarantine messages containing scripts and executables” for developers receiving internal mail.

To create an exception:

Steps

- 1) Click Add executable attachment exception.
- 2) Choose an email address, domain name, or group from the list. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user’s email address, not LDAP user name.
- 3) Clear the **Quarantine messages containing scripts and executables** box.
- 4) Click **Submit**.

URL Sandboxing tab

Use the **URL Sandboxing** tab in a policy to inspect uncategorized URLs in email by tagging them for additional real-time advanced security analysis. Doing so helps protect end users from accessing malicious websites.



Note

If a website is uncategorized, URL sandboxing changes (“wraps”) the URL in the email delivered to users. To add an exception for specific URLs to prevent them from being sandboxed, add a sandboxing exception. See *URL sandboxing exceptions*.

With URL sandboxing, if users click on a link within an email and that link or elements associated with that link are suspicious, they receive a warning that “The link may not be safe.” The notification includes:

- The domain they are trying to access.
- The reasons the link is considered suspicious: for example, the sender email address may be unknown to our service or the sending mail server may have a suspicious reputation.
- The option to analyze the page further.

If they answer **No** to **Analyze the page?**, the suspicious link is not analyzed. They can then close the notification window. For their protection, they cannot access the page.

If they answer **Yes**, the page is analyzed using Forcepoint Email Security Cloud real-time advanced security analysis. They then receive one of the following messages.

The notification messages can be customized. See *Configure block and notification*.

Notification	Description
The link appears to be safe	No malicious threats found. The notification lists the URL and category or categories of the page. Users can proceed to view the page if they choose to do so.

Notification	Description
Access denied	Malicious threats detected in the page. The notification lists any matched categories along with the sites suspected of being infected with a malicious link. Users cannot access the page.
Access denied	Users may also receive an Access denied notification if their organization does not permit them to browse uncategorized web pages.
Unable to access page	The web server may be down or the link may be incorrect. They may want to try again later, or contact their administrator for more information.
Unable to analyze URL	The page could not be analyzed because its protocol is not supported. Supported protocols are HTTP, HTTPS and FTP. If you have selected the Allow the recipient to follow links with an unsupported protocol option, the user can proceed to view the page if they wish; otherwise, the user cannot access the page.



Important

Websites that rely on cookies are not supported. When analyzed, URLs that resolve to sites that rely on cookies may return an error or an incorrectly rendered page. See the article [Embedded URL sent for analysis fails with an error or incorrectly rendered page](#) in the Knowledge Base.

Administrators can retrieve the original URL in the cloud portal using the URL Sandboxing Utility located in **Email > Toolbox**.

Any administrator or end user can check any URL for malicious content by going to the online Advanced Classification Engine (ACE) CSI Insight page (<https://csi.forcepoint.com>) and entering the URL.

If a user must access a link that gets an error (or is otherwise blocked by the URL sandbox), the user should work with Technical Support to resolve the issue.

Forcepoint Email Security on-premises administrators need to contact Technical Support with the sandboxed URL and request the original URL.

Related concepts

[Configure block and notification pages](#) on page 65

Related tasks

[URL sandboxing exceptions](#) on page 94

Modifying rules for URL sandboxing

To modify rules for URL sandboxing:

Steps

- 1) Click **Edit**.
- 2) Under Default settings, select **Analyze suspicious URLs**.
- 3) To allow the user to click through to the site after looking at the category of the Web page, select **Allow the recipient to follow links to unclassified URLs**.
- 4) Links cannot be analyzed if Forcepoint Email Security Cloud does not recognize the network protocol used. Supported protocols are HTTP, HTTPS and FTP. To allow the user to click through to the site if it cannot be analyzed, select **Allow the recipient to follow links with an unsupported protocol**.
- 5) If required, enter customized text to display in email messages instead of suspicious URLs, such as “Danger, do not click!”.
- 6) Under Policy-wide settings, enter any trusted domains that you do not want to be inspected in email messages. Use this list with caution: if a site on the list is compromised, Forcepoint Email Security Cloud does not analyze the site and cannot detect the security problem.
- 7) Define whether to analyze suspicious URLs contained in signed messages.



Note

The options to allowlist domains and analyze suspicious URLs in signed messages apply to all users and groups in a policy, and cannot be over-ridden by exceptions.

- 8) Click **Submit**.

URL sandboxing exceptions

It is possible to tailor some URL sandboxing settings in Forcepoint Email Security Cloud for individual users or groups of users. These settings override the settings made on the URL Sandboxing tab for the policy.

Steps

- 1) On the URL Sandboxing tab, click **URL sandboxing exceptions**. This brings you to a list of URL sandboxing exceptions if you have created any.
- 2) Click **Add Exception**.
- 3) Enter the domain(s) or end-user email address(es), or select a group to which this policy applies. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user's email address, not LDAP user name.
- 4) Define the URL sandboxing settings for these users or groups. For details of the settings, see *URL Sandboxing tab*.

- 5) Click **Submit**.

Related concepts

[URL Sandboxing tab](#) on page 92

Antispam tab

Select the **Antispam** tab on the policy to view or modify rules for spam protection, and to configure settings to detect commercial bulk mail in inbound messages.

By design, email is checked for spam under the following conditions:

- Email is inbound from the Internet.
- The email message is not stopped by some other rule, for example it contains a virus or a barred attachment type.
- The Antispam service is enabled for the policy (i.e., you are licensed for the service).

All such email is assigned a spam score (unless it is blocked by system-wide rules that identify bulk spam). This is visible in the message header and message tracking results. The higher the spam score, the more likely it is to be spam. Many rules are used to generate the spam score, including analysis of the words within the message, where it came from, its headers, and comparisons with other spam and non-spam email.

Spam Options

Check **Filter for Spam** if you want inbound email filtered for spam.

There must be at least one spam rule defined. By default two rules are set up:

- 1) Quarantine all email with a spam score greater than 6.
- 2) Discard any email with a spam score greater than 15.

You can define multiple rules for different spam thresholds and associate actions with each of these. For example, you can create a rule that forces all email with a spam score greater than 6.0 to be forwarded to an administrator, all email with a score greater than 7.0 to be quarantined, and all email with a score over 10.0 to be discarded.

Lower values detect more spam at the risk of false positives - email wrongly detected as spam. Higher values reduce the risk of false positives but could miss some spam. Forcepoint Email Security Cloud aims to ensure that no false positives occur with spam scores over 6.0. This is the recommended default setting for quarantining email.

To define spam rules:

- 1) From the first **Spam scoring more than** drop-down list, select a spam threshold.
- 2) From the second **Spam scoring more than** drop-down list, select an action for that threshold.
The following actions are available:

Action	Description
Quarantine-Notify	Messages are quarantined as above and a notification is sent to an email address. This is not recommended, because you are simply replacing one email with another. It is included for those that wish to use notifications during an evaluation phase rather than the more widely used “tag” option.
Quarantine	Messages are kept in quarantine for up to 30 days. This is the normal setting used for messages identified as spam. Note that no notifications are sent for this action.
Forward	Messages are forwarded to one or more email addresses in a comma-separated list. You can use this setting to forward all spam to a single account for management purposes.
Tag subject	Message subjects are tagged with a prefix that you’ve assigned (in the Tag subject prefix box under Existing Rules).
Bounce	Messages are bounced back to the sender.
Discard	Messages are discarded. This is often used to discard messages with a very high spam score.

- 3) Click **Add Rule>>** to create a rule based on these parameters. Depending on the action you select, you may be prompted for additional information first, such as the email address to which to forward the message.

A list of existing rules is displayed. You can also delete rules here.

Keep a copy of clean messages

By default, Forcepoint Email Security Cloud does not keep a copy of any messages unless they are quarantined, in which case they are held for 30 days before being automatically deleted. Checking **Keep a copy of clean messages** allows Forcepoint Email Security Cloud to keep a private copy of clean email messages, for a short period, separate from the quarantine area, to aid in the process of spam tuning when the “Report this email as Spam” link is used (see *Report this email as spam* for more details). If Forcepoint Email Security Cloud has the original message available, our operations staff and future automated systems can analyze it.

Related concepts

[Report this email as spam](#) on page 79

Commercial bulk email detection

The service offers a way to configure your settings to detect inbound commercial bulk email messages and to perform certain actions on them, such as quarantining, or tagging the message subject so that users can easily identify commercial email.

To enable commercial bulk email detection, do the following:

Steps

- 1) Under **Commercial Bulk Email Detection**, select **Analyze for commercial bulk email**.
- 2) Select the action you'd like performed when commercial bulk email is detected:
 - **Take no action.** No action is taken on the commercial bulk email detected.
 - **Tag the message subject.** The subject of detected commercial bulk email messages are tagged with "COMMERCIAL:" or a custom tag that you enter.
 - **Quarantine the message.** Commercial bulk email messages are kept in quarantine for up to 30 days. Note that no notifications are sent for this disposition.
- 3) Select the sensitivity level of the feature:
 - **Normal** detects email that comes from known commercial bulk email sources.
 - **High** detects email that comes from known commercial bulk email sources or email that contains commercial content.
- 4) Click **Submit** when you are finished.
Note that the subject tag that you select will also be used in all antis spam exceptions.



Note

If you wish to run a report that shows the number of commercial bulk email messages you have received, these messages will only be counted if you have selected **Analyze for commercial bulk email**.

Allowlists and blocklists

Here you can configure allowlists and blocklists that override your spam filtering settings, affecting inbound messages for the whole policy.

- Allowlist entries can include the sender's email address, domain, or IP address. Allowlists define addresses that are permitted to send mail to you without spam filtering being applied.
- Blocklist entries can also include the sender's email address, domain, or IP address. Blocklists define addresses from which you do not want to receive email.

**Note**

Allowlists always take priority over blocklists. If you add an address to both the allowlist and the blocklist, messages from that sender address are allowed.

Allowlists and blocklists are processed in the following order. The first match found is applied:

- Policy IP address allowlists
- Policy IP address blocklists
- Per-user email address/domain allowlists (see *Antispam exceptions*)
- Policy email address/domain allowlists
- Per-user email address/domain blocklists (see *Antispam exceptions*)
- Policy email address/domain blocklists

If Forcepoint Technical Support has enabled a custom antispam rule for your account, this may override any addresses in allowlist you have configured.

If you enable/select allowlist, you can also configure the following options:

- **Apply allowlist matching even if the message has a spoofed email addresses.** If the service detects a message is spoofed, allowlist is not applied by default. However, you may wish to allow some messages that are legitimately spoofed, for example a message from an email distribution list that appears to come from a specific person. Select this option if you want to allow spoofed addresses through even if the address appears in your allowlist.
- **Do not apply allowlist matching on From: headers.** An email message has two addresses associated with it: the envelope sender, and the From: header. The envelope sender is used by mail servers to check where the message originates and where to respond (for example, if there is an error or the message bounces); the From: header is what the message recipient sees. The envelope sender and the From: header often match, but not always. There are a number of legitimate reasons why an envelope sender might not match the From: header, for example if the message comes from a mailing list, or from an organization that has implemented a specific address for bounced messages.

Email spammers can take advantage of this, by changing the From: header on a spam email to be a domain that you recognize, while the envelope sender is related to a domain under their control.

By default, the service performs email address/domain allowlist on both the From: header and the envelope sender. If you select this option, allowlist matching applies only to the envelope sender.

To populate your allowlists and blocklists, click the links in **Allowlist these addresses** or **Blocklist these addresses**. See *Adding an entry to the allowlist or blocklist* for more information.

Use **Forward messages with more than [N] recipients from specified domains** to forward messages with more than the specified number of recipients from the specified domains.

When this rule is triggered, the intended recipients do not receive the message.

Example: To forward messages from example.com sent to more than 5 recipients, enable the option, specify 5 for the number of recipients, specify a forwarding address, and specify example.com for the domain. You can specify additional domains, if desired.

**Note**

The **Forward messages** option is a limited-availability feature, and may not be available in your account.

Related concepts

[Antispam exceptions](#) on page 99

Related tasks

[Adding an entry to the allowlist or blocklist on page 101](#)

End user permissions

Forcepoint Email Security Cloud antispam provides a range of end-user self-service options. These are all initiated using the Forcepoint Email Security Cloud personal email report (see *End-User Self Service*).

You can enable or disable the ability for users to populate and manage their own individual blocklist and allowlist, and the option to release a copy of quarantined spam to themselves. These settings can be set for the policy, and can also be set for individual users, groups, or domains, using Antispam Exceptions. See *Antispam exceptions*.

**Note**

A user can never prevent an email containing a virus from being quarantined and, regardless of these settings, can never release one.

Allowlists always take priority over blocklists. If you have an email address in blocklist for the policy, a user can allowlist it and, assuming it has no other issues, such as containing a virus or contravening a Content rule, it is delivered. To prevent a user receiving certain types of email, we recommend that you configure a content filtering policy. See *Content Filter tab*).

Related concepts

[Antispam exceptions on page 99](#)

[Content Filter tab on page 110](#)

Related information

[End-User Self Service on page 155](#)

Spam detection methods

For information about the methods that Forcepoint Email Security Cloud uses to identify spam, see the article [Detecting spam](#) in the Forcepoint Knowledge Base.

Antispam exceptions

It is possible to tailor some antispam settings in the Forcepoint Email Security Cloud service for individual users, groups, or domains. Antispam exceptions can control the following settings:

- Spam Options and Commercial Bulk Email Detection: define per user, group, or domain rules for spam and commercial message filtering
- Allow & Block Lists: enable or disable per-user, group, or domain allowlists and blocklists

- End-Users settings: control user permissions for populating allowlist and blocklists, and releasing quarantined messages.

To add an antispam exception:

- 1) Click **Antispam Exceptions**.
- 2) Click **Add**.
- 3) Enter end-user email addresses, domains, or select the user groups to which the exception applies.



Tip

If you are making a user exception, be sure to enter the user's email address, not LDAP user name.

Allow users to send themselves copies of their spam email

- 4) Click **Save**. Your exception settings will override those in the main policy, and changes to these settings in the main policy will not be inherited.
When the **Synchronize...** setting is applied, your settings will be overwritten by those in the main policy, and updates to the settings in the main policy are automatically applied to the exception.

Once you have saved the exception, you can re-open it to modify the spam and commercial bulk email, and allow and blocklist settings, if required.

To modify these settings:

- 1) On the **Antispam Exceptions** page, click the entry for the exception you want to edit.
- 2) To set Spam Options and Commercial Bulk Email Detection settings that differ from those in the main policy, clear the **Synchronize...** checkbox. Configure your own spam and commercial email settings, as appropriate, and click **Save**. Changes to these settings will not be inherited from the main policy.
When the **Synchronize...** setting is applied, your rules will be overwritten by those in the main policy, and updates to the settings in the main policy are automatically applied to the exception.
- 3) Use the Allow & Blocklist settings to define whether per-user, domain, or group- specific allowlists and blocklists are used in addition to policy-wide allowlists and blocklists:
 - Select **Allowlist these addresses** to enable per-user, domain, or group allowlists. Clear this checkbox to ignore these allowlists, and **only** apply allowlists defined for the main policy.
 - Select **Blocklist these addresses** to enable per-user, domain, or group blocklists. Clear this checkbox to ignore these blocklists, and **only** apply blocklists defined for the main policy.

You can modify exception allowlist and blocklist addresses by clicking the links in **Allowlist these addresses** and **Blocklist these addresses**. Exception allowlists and blocklists can be uploaded in bulk via CSV files.



Note

Policy-wide allowlists and blocklists, if enabled, are always applied. Updates to the allowlists and blocklists in the main policy are automatically applied.

4) Click **Save.**

Synchronization settings for spam options and end-user settings can be modified in bulk for all exceptions using the **Modify All** button on the **Antispam Exceptions** page.

Allowlist and blocklists can be imported for your account via CSV files, using the Bulk Operations options on the **Antispam Exceptions** page. See *Uploading allowlist and blocklist exceptions in bulk* for more information.

Related tasks

Uploading allowlist and blocklist exceptions in bulk on page 103

Adding an entry to the allowlist or blocklist

Steps

1) On the Antispam tab, click the link in **Allowlist these addresses** or **Blocklist these addresses**. A list of currently in allowlist or blocklist addresses appears. You can sort the list in ascending or descending order by address or description. You may need to click **Next** to see all of the addresses in the list. You can narrow the list by adding search criteria and clicking **Search**.

2) Click **Add** to add a new entry to the list.

3) In the **Address** field, enter an email address, domain name, or IP address.

Asterisk (*) is supported as a wildcard at the beginning or end of an email address or domain name. (Note: wildcards are not supported for IP addresses).

Some examples of wildcard usage are given in the following table.

*acme.co.uk	Covers all email addresses at acme.co.uk and any sub-domain of acme.co.uk
*@acme.co.uk	Covers all email addresses at acme.co.uk but none at any sub- domain
*.acme.co.uk	Covers any address at any sub-domain but excludes the main domain
@acme	Covers all email addresses at any domain or sub-domain beginning with 'acme'
acme	Covers all email addresses containing 'acme'

4) Enter a description if desired.

5) Click **Submit**.

Uploading a allowlist or blocklist

If you have permission to modify configurations, you can populate a allowlist or blocklist in a policy or exception by uploading an address list in a comma-separated value (CSV) file.

The header of the file must be this string exactly, "Address, Description" and every line must contain the following 2 fields separated by a comma:

- An email address or domain name (wildcards permitted), or an IP address (wildcard not permitted).
- A description (free text, up to 255 characters).

The fields can be quoted or not. If a field contains a comma, it must be quoted. If 1 field is quoted, the rest of the line must be quoted. If a field contains a quotation mark, this character must be surrounded by additional quotation marks. If a line contains only 1 field, it is interpreted as the email address and the description is omitted. If a line contains more than 2 fields, the file is rejected and an error message is displayed.

For example:

Address, Description

"address1@domain1.com", "Description of address1, containing comma"

address1@domain1.com, Description of address1 without comma

"address1@domain1.com", "Description of address1, containing ""quotes"""

"domain2.com", "Description of domain2"

To upload the file:

Steps

- 1) Click the link, **Upload addresses from a CSV file**.
- 2) Browse to the name of the file to upload.
- 3) Select an action:

Action	Description
Append to current list	<p>Elements imported from the file are added to the existing elements. The resulting list is a union of all elements.</p> <p>If any of the entries in the file is already included in the list, it is not added again and a warning message is displayed. This does not stop the processing of the file.</p>
Replace current list	<p>Elements already existing in the list are deleted and replaced by the elements in the file. You are asked to confirm this action.</p>

- 4) Click **Upload**. Note that large files take a while to transfer to the server. If the file is empty, too large, or cannot be opened, an error results. An error also results if any of the elements are invalid.

You can also download the current addresses into a CSV file for viewing in a spreadsheet, or you can delete entries from the allowlist or blocklist by checking the box next to the address and clicking **Delete**.

Uploading allowlist and blocklist exceptions in bulk

You can upload allowlist and blocklist exception information in bulk if you have the blocklist or allowlist exceptions for all of your users and groups in a single file.

The file must be in comma-separated value (CSV) format, and the header of the file must be this string exactly: "Apply To, Address, Description". Every line must contain 3 fields separated by commas:

- An email address, domain name, or group that the allowlist or blocklist address applies to (no wildcards permitted).
- An email address or domain name (wildcards permitted).
- An optional description (free text, up to 255 characters).

The fields can be quoted or not. If a field contains a comma, it must be quoted. If 1 field is quoted, the rest of the line must be quoted. If a field contains a quotation mark, this character must be surrounded by additional quotation marks. If a line contains more than 3 fields, the file is rejected and an error message is displayed.

For example:

Apply To, Address, Description

"UK Sales", "address1@domain1.com", "Description of address1, containing comma"

john@example.com, address1@domain1.com, Description of address1 without comma

"example.com", "domain2.com", "Description of domain2"

"Marketing", "address2@domain1.com", "description of address2", "this field is not processed"

To upload the file:

Steps

- 1) On the Antispam Exceptions page, do one of the following:
 - To upload a bulk allowlist, click the link **Upload addresses from a CSV file** under Allowlist Bulk Operations.
 - To upload a bulk blocklist, click the link **Upload addresses from a CSV file** under Blocklist Bulk Operations.
- 2) Browse to the name of the file to upload.
- 3) Select an action:

Action	Description
Append to current list	Elements imported from the file are added to the existing elements. The resulting list is a union of all elements.
Replace current list	Elements already existing in the list are deleted and replaced by the elements in the file. You are asked to confirm this action.

- 4) Click **Upload**. Note that large files take a while to transfer to the server. If the file is empty, too large, or cannot be opened, an error results. An error also results if any of the elements are invalid.

You can also download the current blocklist and allowlist into a CSV file for viewing and editing in a spreadsheet.

Note that if no exceptions are created, the default spam policy will apply.

Antispoofing tab

Use the **Antispoofing** tab to configure inbound and outbound spoofing protection for the policy.

Inbound spoofing controls are used to detect when incoming messages are from forged sender addresses, or when fake messages appear to come from named executives in your organization (known as spear phishing). For inbound antispoofing controls, see:

- *Spoofed Message Detection*
- *Internal Executive Spoofing*

Outbound spoofing controls help you to provide better protection for message recipients against messages that forge your domains, by adding a DKIM signature to validate your outbound messages, and applying strict outbound message authenticity checks. For outbound antispoofing controls, see:

- *DKIM Signing*
- *Antispoofing Checks*

Related concepts

[Spoofed Message Detection](#) on page 104

[Internal Executive Spoofing](#) on page 106

[DKIM Signing](#) on page 107

[Antispoofing Checks](#) on page 109

Spoofed Message Detection

Spoofed message detection is used to filter incoming messages where the sender's address has been forged. The service can detect messages that spoof internal domains or external domains.

- Messages that spoof **internal** domains are from forged addresses that appear to come from users within your organization. Internal domain validation uses Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) authentication, as well as checking the sender's IP address against those configured as outbound routes in the policy.
- Messages that spoof **external** domains are from forged addresses that appear to come from legitimate external organizations. External domain validation uses Domain-based Message Authentication, Reporting and Conformance (DMARC) authentication.

Filter messages that spoof internal domains

Select **Filter inbound messages that spoof your internal domains** to detect spoofed incoming messages that appear to be sent from domains within the policy to recipient domains within the policy. A sender address is considered to be authentic if any of the following conditions are true:

- The IP address of the sending message transfer agent (MTA) matches any of the outbound connections configured in the policy.
- The Mail From sending address passes Sender Policy Framework (SPF) authenticity checks.
- The Mail From sending address passes DomainKeys Identified Mail (DKIM) authenticity checks.

Select **“From” address header validation** to check that the sender address the message recipient sees (in the “From:” field) matches domains defined in your policies. (By default, the From: address is ignored and authenticity checks are performed only on the envelope sender address if it matches one of your policies.) If you select this option, one of the following happens:

- If the envelope sender and recipient address both match domains in your policy, the cloud service performs message authenticity checks on the envelope sender only.
- If the envelope sender address does not match a domain in your policy, but the From: address and recipient domain do match, the cloud service performs message authenticity checks on the From: address instead of the envelope sender address.



Tip

The envelope sender address is used by mail servers to check where the message originates and where to respond (for example, if there is an error or the message bounces) and often matches the From: address, but not always. For example, the message might come from a mailing list, or from an organization authenticated to send messages on your company's behalf.

From the drop-down menu, select the action to perform when spoofed internal messages are detected:

- **Quarantine:** This is the default option. Spoofed messages are kept in quarantine for up to 30 days.
- **Discard:** Spoofed messages are discarded.
- **Tag subject with:** The subject line of detected spoofed messages are tagged with “SPOOFED:” or a custom tag that you enter.

Messages detected as spoofing internal domains will be logged as “Spoofed”.

By default, if authentication checks fail to complete, the message is considered spoofed and the selected action is applied. To specify an alternative action when authentication checks fail to complete, select **Apply alternative action when spoofed message checks fail to complete**. Available options depend upon the action selected for spoofed messages:

- When the Action is **Quarantine** or **Tag Subject**, the alternative option is **Tag Subject**.
- When the Action is **Discard**, the alternative options are **Quarantine** and **Tag Subject**.

Select **Allow spoofing from these sources** to apply an allowlist of allowed domains or IP addresses. Messages originating from these domains or IP addresses are allowed to spoof addresses from domains in this policy. This may be useful if, for example, you use a third-party provider who is allowed to send email messages to your users that appear to come from an internal address.

Adding the allowlist spoofing sources

To add the allowlist spoofing sources for a policy:

Steps

- 1) Select **Allow spoofing from these sources**, and click the **these sources** link.
- 2) In the panel that appears:
 - Select the **Domains** tab to add allowed sender domain names, for example “forcepoint.com”.
 - Select the **IP Addresses** tab to add allowed sender IP addresses, either as a list of individual addresses, or address blocks in CIDR notation (for example, 10.10.10.8/30). List entries are separated by a line break.
- 3) Click **Add** to enter a new domain or list of IP addresses. You can add multiple domains or addresses, and you can add a combination of domain names and/or IP addresses if required.
- 4) For IP addresses or ranges, enter a short description/name to identify the IP addresses.
- 5) When you are finished, click **Save**.

Filter messages that spoof external domains

Select **Filter inbound messages that spoof external domains using DMARC** to detect spoofed incoming messages that appear to be sent from legitimate external domains, but which fail DMARC validation checks. This option validates both the Mail From sending address and the From address. DMARC is built on SPF and DKIM validation, and allows the owner of a domain to publish a policy (via DNS TXT records) that defines how the receiver should deal with spoofed messages.

From the drop-down menu, select the action to perform when spoofed messages are detected:

- **Use DMARC policy:** This is the default option. Spoofed messages will be quarantined or rejected, depending upon the domain owner's policy.
- **Quarantine:** Spoofed messages are kept in quarantine for up to 30 days.
- **Discard:** Spoofed messages are discarded.
- **Tag subject with:** The subject line of detected spoofed messages are tagged with “SPOOFED:” or a custom tag that you enter.

Messages detected as spoofing external domains will be logged as “Spoofed- External”.

By default, if authentication checks fail to complete, the message is considered spoofed and the selected action is applied. To specify an alternative action when authentication checks fail to complete, select **Apply alternative action when spoofed message checks fail to complete**. Available options depend upon the action selected for spoofed messages:

- When the Action is **Use DMARC policy**, **Quarantine**, or **Tag Subject**, the alternative option is **Tag Subject**.
- When the Action is **Discard**, the alternative options are **Quarantine** and **Tag Subject**.

Internal Executive Spoofing

The Internal Executive Spoofing feature provides protection against spear phishing attacks targeting individuals within your organization. Such emails may come from legitimate (non-spoofed) email addresses, thereby passing other spoofing checks, but use the display name of a known user (often an executive), with the intention of tricking employees into sending money or information.

If an incoming email appears to be from one of your named executives, the feature will check that the message comes from one of a set of approved email addresses for that individual. Messages that appear to come from a named executive, but originate from an address you have not added, are treated as spoofed, and the action you define will be taken (quarantine, discard, or tag). If the email comes from an address you have added for the executive, the usual spoofing checks are performed against the email address to check it is genuine.

Enabling the internal executive spoofing check

To enable the internal executive spoofing check:

Steps

- 1) Select Apply internal executive spoofing check to these names.
- 2) Click the **these names** link to configure the list of executive and their approved email addresses:
 - Click **Add**, and enter a first name and last name (both fields are required). Various combinations of the name are protected (for example, “John Smith” as well as “Smith, John”).
 - Enter a list of approved email addresses for the executive, separated with a comma or a line break. This list should include any addresses the executive uses, including work or personal addresses.
 - Click **Add** to repeat the process for each executive whose name and addresses you wish to check. Click **Save** when finished.



Tip

Where executives may use various spellings of a first name (for example Elizabeth/ Liz, David/ Dave), add multiple name entries for the user. Each entry should include a duplicate set of allowed email addresses for the user.

- 3) Select an action to perform on messages detected as potentially spoofed. The options are:
 - **Quarantine**: This is the default option. Messages are kept in quarantine for up to 30 days.
 - **Discard**: Spoofed messages are discarded.
 - **Tag subject with**: The subject line of spoofed messages are tagged with a custom tag that you enter.

Messages detected as spoofing named executives will be logged as “Spoofed- Targeted”. Messages quarantined for this reason will be excluded from end users’ Personal Email Subscription reports, in order to prevent users from inadvertently acting upon a targeted phishing message.

DKIM Signing

DomainKeys Identified Mail (DKIM) is an authentication method designed to protect recipients from spoofed messages. DKIM authenticates the message sender address and message body to provide validation that the sender has not been forged and that the message has not been altered.

When DKIM signing is enabled, the cloud service signs outgoing messages from specified sender domains/ subdomains with a private key, adding a *DKIM-Signature* header. Recipient servers can use the information in this header to perform a DNS lookup. The DNS response provides the Forcepoint public key, which can be used to decrypt the signed header and authenticate the message.

A DKIM signing rule defines which of your sender domains/subdomains to protect with a specified signing domain. Granular sender/recipient options can be applied, to include or exclude specific sender addresses, or sender/recipient combinations.

**Important**

a single signing domain can be used by multiple rules to validate different sender subdomains. A sender domain/subdomain can only be signed by one signing domain, and consequently can only be added to one rule.

Before enabling a signing rule, you must publish DNS CNAME records for your signing domain. CNAME records enable the DNS lookup to Forcepoint in order to provide the public key to recipient mail servers. Details of the CNAME records you must publish can be found on the **DNS Records and Service IPs** page. See *DNS records and service IP addresses* for more information.

Related concepts

[DNS records and service IP addresses](#) on page 54

Adding a DKIM signing rule

To add a DKIM signing rule:

Steps

- 1) Navigate to **Email > Policies > [policy name] > Antispoofing** tab.
- 2) Under DKIM Signing, click **Add**.
- 3) On the **Add DKIM Signing Rule** page, enter a rule name.
- 4) In the Sender domains/subdomains field, add one or more sender domain/ subdomains that will be signed by this rule, separated by a line break.

**Note**

Sender domains/subdomains can appear in only one signing rule.

- 5) In the Signing domain field, enter the domain that will be used as the signing domain for this rule.
- 6) Optionally, select **Enable granular DKIM sender/recipient options** to include or exclude specific senders, or sender/recipient combinations. Otherwise, click **Submit**.
- 7) Using the options that appear, select either:
 - **Sign messages from these addresses** to sign messages from specific addresses, or
 - **Do not sign messages from these addresses** to sign messages from all senders within your sender domains except specific addresses.
- 8) In the Senders field, enter one or more email addresses for the senders who will be included or excluded by this rule. Email addresses must be separated by a line break. Use **@domain.com* to include all addresses for a domain.

**Note**

This field is required when granular sender/recipient options are enabled.

- 9) In the Recipients field, optionally enter recipients that will be included or excluded by this rule. Email addresses must be separated by a line break. Use `*@domain.com` to include all addresses for a domain.
- When **Sign messages from these addresses** is selected, only messages from a specified sender address to any of the entered recipient addresses will be signed.
 - When **Do not sign messages from these addresses** is selected, messages from all addresses within your sender domains will be signed, except for messages that are from a specified sender address to any of the specified recipient addresses.
- 10) Click **Submit**.
- Once you have added a signing rule, the service checks the CNAME records for your signing domain. If the CNAME record check fails, an error message is shown. A rule cannot be enabled until the CNAME record check has passed.

Enabling a DKIM signing rule

DKIM signing rules are initially set to **OFF**. In order to enable a DKIM signing rule, the signing domain must have passed a CNAME record check.

Enable a DKIM signing rule on the **Email > Policies > [policy name] > Antispoofing** tab, under DKIM Signing. To enable a rule:

- If the CNAME record check has passed, toggle the State switch on **ON**, then click **Save**.
- If the CNAME record check has failed, ensure that the CNAME record has been published for the signing domain. For further information on publishing the CNAME record, see *DNS records and service IP addresses*. Once you have published the CNAME record, click **Recheck** to perform the check again.

To disable a rule, toggle the State switch to **OFF**, then click **Save**.

Related concepts

[DNS records and service IP addresses](#) on page 54

Editing a DKIM signing rule

Click the name of the rule in the DKIM Signing table to edit the sender domains/ subdomains or signing domain for the rule, or to make changes to the granular sender/ recipient options.

For more information on the configuration options for DKIM signing, see *Adding a DKIM signing rule*.

To delete a rule, click the rule name in the DKIM Signing table to open the **Edit DKIM Signing Rule** page. Click **Delete** to remove the rule.

Related tasks

[Adding a DKIM signing rule](#) on page 108

Antispoofing Checks

The strict outbound message authenticity check performs additional tests on outbound messages processed by the policy. With the option enabled, the service checks that outbound messages originate from an IP address

in the policy, or have a valid DKIM signature. Messages that fail the test are quarantined, providing additional protection to prevent your domains being spoofed by a third party.

Select **Enable strict outbound message authenticity checks** to apply strict checks to all outbound messages for the policy.

With this option enabled, outbound messages must either:

- Originate from an IP address defined as an Outbound Route on the **Connections** tab of the policy, OR:
- Have a valid DKIM signature applied by your email provider. (Required for customers that use a hosted service provider such as Microsoft Office 365 or Google Apps.)

Messages that do not meet these criteria will be quarantined as “Spoofed”.



Note

Do not enable this option if your policy is used to process messages that legitimately spoof your domains. For example:

- If your users are likely to send mail from the networks of other companies (for example, consultancy firms whose employees visit other customer sites).
- If your organization uses mailshot companies who are authorized to send email on your behalf.

Allowed signing domains

Where DKIM needs to be used to validate the authenticity of a message (for example, for messages originating from Office 365 or Google Apps), the service checks that the signing domain matches the domain of the message content “From:” header. By default, if the domains do not match, the message will be considered spoofed.

Click **Allowed Signing Domains** to specify one or more additional DKIM signing domains that will be accepted to validate outbound messages from your hosted provider for sender domains in the policy.

In the panel that appears, add one or more signing domains, and click **Save**. Messages with a valid DKIM signature from a domain you have added will be treated as authentic.

Content Filter tab

Content filtering rules are typically different for inbound and outbound email, because the email usage policy that you want to enforce more than likely specifies different sets of rules for email entering the organization than it does for email leaving the organization.

Select the **Content Filter** tab on the policy to view or modify rules for filtering content.

Editing content rules

Click **Edit** in the **Inbound Attachment Rule** or **Outbound Attachment Rule** box to edit the content rules for your policy.

The majority of the content filtering functionality is the same for inbound and outbound email.

Section	Field
Attachments	<ul style="list-style-type: none"> ■ <i>Masking attachments</i> ■ <i>Quarantining messages with specific file types</i> ■ <i>Parking attachments</i> ■ <i>Attachment exceptions</i> ■ <i>Image analysis and quarantining</i> ■ <i>Securing suspicious attachments</i>
Message Size	<ul style="list-style-type: none"> ■ <i>Message Size</i>
Content Filtering	<ul style="list-style-type: none"> ■ <i>Filtering using lexical rules</i> ■ <i>Quarantining messages where analysis does not complete</i>

Related concepts

[Masking attachments](#) on page 112

[Quarantining messages with specific file types](#) on page 112

[Parking attachments](#) on page 114

[Image analysis and quarantining](#) on page 113

[Securing suspicious attachments](#) on page 117

[Message Size](#) on page 118

[Filtering using lexical rules](#) on page 119

Related tasks

[Attachment exceptions](#) on page 114

[Quarantining messages where analysis does not complete](#) on page 123

Attachments

The following actions are available for email attachments:

Related concepts

[Masking attachments](#) on page 112

[Quarantining messages with specific file types](#) on page 112

[Parking attachments](#) on page 114

[Image analysis and quarantining](#) on page 113

[Securing suspicious attachments](#) on page 117

Related tasks

[Attachment exceptions](#) on page 114

Masking attachments

Masking an attachment renames attachments with the specified extensions. The renaming replaces the last character of the extension with an underscore ‘_’. For example, if you mask “EML” attachments, a file named “test_email.eml” is renamed “test_email.em_”.

This stops the attachment being automatically associated with its appropriate executable in Windows and therefore avoids dangerous actions being triggered automatically.

We recommend that you mask “EML” attachments, because these can cause email clients such as Outlook and Outlook Express to execute code automatically.

Click the link on **Mask attachments with these extensions** to specify which attachments to mask.

Inverting the mask action

You can invert masking by extension. This enables you to specify that all extensions except those specified are subject to the Mask action. If you want to do this, select the radio button Mask all extensions except these.

Quarantining messages with specific file types

You can quarantine messages containing attachments matching file types that you specify.

File types are grouped together into file formats. For example, if you select the Sound format, this quarantines anything related to sound files, including RealAudio, Windows Media Audio, MPEG Audio, and MIDI files.

You can expand a file format to select or remove specific file types from the quarantine list. For example, you can select the Standard Graphics format to block all standard image attachments, but then choose to clear the JPEG file type within that format to allow JPEGs to be delivered.

If the available file types do not meet your requirements, you can set up custom file types containing one or more file extensions and MIME types. For more information, see *Creating custom file types*. The custom file types you create are available for all policies, and appear as part of a default custom file format on the same page as the supplied file formats.



Note

Options on the Antivirus tab are the most effective way to block unsafe executables. For more information, see *Executables*.

Related concepts

[Executables](#) on page 90

Related tasks

[Creating custom file types](#) on page 116

To quarantine attachments

Steps

- 1) On the Content Filter tab, click the link **Quarantine messages containing files with these types**. The page displays the file formats and types currently being quarantined.
- 2) Click **Edit**.
- 3) Check the boxes for file formats you wish to quarantine.
- 4) To select particular file types within a file format, click the + icon to expand the format. If you have selected the file format, all of the subsidiary file types are also selected. You can select or clear as many file type options as you wish. The information next to each file format tells you how many are currently selected from that format.
- 5) Click **Submit**.

Next steps

Inverting the quarantine action

Inverting the quarantine action enables you to specify that all file types except those selected are quarantined. If you want to do this, select that do not match the selected file types from the drop-down list.

Image analysis and quarantining

If you have the Forcepoint Email Security Image Analysis Module, you can choose to quarantine messages that have images attached to prevent potentially pornographic images from entering your organization. Messages are quarantined if they contain an image attachment considered to be inappropriate. This can be set up for inbound messages, outbound messages, or both.

To quarantine images, select **Quarantine messages containing inappropriate images**, and define how strictly the system applies this security feature by selecting a sensitivity level. By changing the sensitivity, you can control how suspicious the image scanner is when it carries out its analysis.

It is difficult to impose absolute thresholds on what constitutes an “inappropriate” image, as perceptions can vary. Therefore depending on the sensitivity level you select, you may see a proportion of messages containing acceptable images being quarantined. If there are images that you don’t want to be analyzed and quarantined, perhaps because they are repeatedly blocked, you can add them to the image allowlist. See *Image allowlist* and *Managing quarantined images*.

If a message includes an image attachment that Forcepoint Email Security Cloud cannot analyze, perhaps because it is too large, you can select **Quarantine messages with images that could not be analyzed** to quarantine that message for further analysis.

Related concepts

[Managing quarantined images](#) on page 152

Related tasks

[Image allowlist](#) on page 69

Attachment exceptions

You can override some of the attachment settings for users, groups, or domains. To do this:

Steps

- 1) Click **Attachment Exceptions** for either inbound outbound attachments.
- 2) Click **Add Exception**.
- 3) In the **Domain or address list** field, enter the address(es), domain(s), or select the appropriate group(s) to which this configuration applies. In most cases, particularly if you are synchronizing LDAP directories, you will make exceptions based on group names, such as Dev. If you are making a user exception, be sure to enter the user's email address, not LDAP user name.
- 4) Make whatever changes you want to the policy for this user, group, or domain.
- 5) Click **Submit**.
To edit an existing attachment exception, click the appropriate policy in the **Apply to** column of the Attachment Exceptions page.

Parking attachments

Use the **Policy > Content Filter > Park Attachment Rules** page to park large message attachments on the Forcepoint Email Security Cloud system. The file is removed from the message and stored. An annotation is added to the message including the filename, its size, and a Web link from where the file can be retrieved over a secure HTTP (HTTPS) connection. The wording of the annotations is completely configurable.

To create a park attachment rule

Steps

- 1) Click **Add Rule**.
- 2) Define whether the rule should be initially enabled or disabled.
- 3) Enter a **Rule name**.
- 4) Select an **Attachment size** and a **Message size** from the drop-down lists. For example, you might choose to park any attachment with a size of 2MB or larger in messages that are 3MB or larger in size.
You can also select Ignore for either of these options, for example if you want all attachments larger than a certain size to be parked regardless of the message size.
- 5) Choose how long the parked message should be stored for. The default is 7 days.
- 6) Define whether the system should keep a copy of the original message.

- 7) Under **Apply To**, define who the rule affects. By default, the rule applies to all the senders (for an outbound rule) or recipients (for an inbound rule) in the policy. Alternatively you can apply the rule to only the senders or recipients that you specify. Enter the domains, addresses, or groups to include, separated by commas.
- 8) To exclude certain sender and recipients from your rule, select **Exclude these senders and recipients**, then list the domains, addresses, or groups to exclude, separated by commas. For example, you can specify that a rule does not apply if an email is from `xyz@externaldomain.com` or is sent to `xyz@internaldomain.com`. You can enter up to 65,535 characters.
- 9) Under **Annotations**, you can edit the annotation that appears in the original message sent to the recipient. A default annotation like the one below is included.
The attachment attach1-2100.txt (2.1 MB) was parked. It can be retrieved from here.
 In addition, you can include the following variables:

Variables/tokens	Description
<code>_RECIPIENTS_</code>	The intended recipients of the message.
<code>_DATE_</code>	The date Forcepoint Email Security Cloud received the email that generated the annotation. This date is based on the time zone set on the Notification Email screen.
<code>_SENDER_</code>	The message originator.
<code>_SUBJECT_</code>	The subject line of the message that is being annotated.
<code>_ATTACH_TYPE_</code>	The file type of the attachment parked.
<code>_NAME_</code>	The name of the attachment parked.
<code>_RETRIEVE_END_</code>	Used in HTML annotations surrounding some text that displays as a link. For example, "It can be retrieved from <code>_RETRIEVE_START_</code> here <code>_RETRIEVE_END_</code> ."
<code>_RETRIEVE_START_</code>	Used in HTML annotations surrounding some text that displays as a link. For example, "It can be retrieved from <code>_RETRIEVE_START_</code> here <code>_RETRIEVE_END_</code> ."
<code>_RETRIEVE_LINK_</code>	Used to include a link to download the attachment. For example, "It can be retrieved from <code>_RETRIEVE_LINK_</code> ."
<code>_SIZE_</code>	The size of the attachment parked.

Click on **Variables/tokens** to select these variables from the drop-down list.

- 10) Under **Notification Options**, select who should be notified about the parked attachment. In all cases, you have the option to include the original message with the notification.

- 11) Click **Submit** when done.

After a rule has been created and enabled, you have the option to add parking by file format or type. See *Park attachments by file type*.

Related tasks

[Park attachments by file type](#) on page 116

Park attachments by file type

You can add parking by file format or type to an existing, enabled park attachments rule.

You can combine attachment and message size checks with file types. For example, you can specify a rule that parks all video files larger than 5 MB.

To park attachments by file type:

Steps

- 1) From the Park Attachment Rules window, click the name of the rule you want to edit.
- 2) Select the **Park attachments by file type** check box to enable parking by file type.
- 3) Click the link **Choose file types to specify file types for parking**.
- 4) Check the boxes for file formats you wish to park. To select particular file types within a file format, click the + icon to expand the file format.
- 5) Click **Save**.

Creating custom file types

You can set up custom file types to meet your organization's needs. For example, you might want to block a file extension not covered by the supplied file types, or create a type that groups a number of specific extensions.

You can also use custom file types to set up attachment blocking for MIME types.

To create a custom file type:

Steps

- 1) Go to **Account > Custom File Types**.
- 2) Click **Add**.
- 3) In the **Extensions** field, enter the file extensions to include in the custom type, separated by commas. For example, to block particular types of image file, you might enter JPG, GIF, PNG.
- 4) Enter any MIME types in the format content type/content subtype. For example, video/mpeg or text/csv.

- 5) Enter a description for your custom file type. This description appears in the **Custom File Type** list when you are selecting file types and formats for attachment quarantine.
- 6) Click **Submit**.

Unknown attachment types

If a message includes an attachment type that Forcepoint Email Security Cloud cannot identify, you can choose to quarantine that message for further analysis. This can be set up for inbound messages, outbound messages, or both.

To quarantine unknown attachment types:

Steps

- 1) On the **Content Filter** tab, click **Edit** for either inbound or outbound rules.
- 2) Select Quarantine messages containing files of unknown type.
- 3) Click **Submit**.

Securing suspicious attachments



Note

Securing suspicious attachments is a limited-availability feature, and may not be available in your account.

Even when analysis does not find malicious content in an attachment, some attributes of an attachment can make it suspicious. Such attributes include sender and domain reputation, attachment file type, attachment size, the spam score of the message, and other attributes.

When a suspicious attachment is identified, you can choose to place the attachment in a password protected zip file that is delivered to the recipient along with a report that includes the message details, a preview of the attachment content, and a link to retrieve the password to the secured zip file. When the **Retrieve Password** link is clicked, a separate email is sent to the recipient that includes the password. Note that only an original recipient can receive the password. If a message with secured file attachments is forwarded, recipients of the forwarded message must ask the original recipient for the password.

If you choose to secure suspicious file attachments, it's very important that you prepare users to receive them and to take appropriate action. Users should know that:

- 1) The email security service analyzes email attachments for malicious content. When found, the attachment is not delivered.
- 2) The email security service also looks for suspicious file attachments. An attachment can be suspicious for several reasons including the reputation of the sender or sending domain, attachment file type, attachment size, the spam score of the message, and other attributes.
- 3) When a suspicious attachment is found:
 - The attachment is placed in a password protected zip file and delivered, along with the original message, to the intended recipients.

- A **Secured Attachment Report** is also attached to the original message. The report includes the message details, a preview of the attachment content, and support for retrieving the password for the secured zip file.
- 4) Recipients should carefully examine the Secured Attachment Report to help determine if the attachment is safe.
- 5) Opening a suspicious attachment could lead to the computer being compromised or infected. Recipients should open the attachment only if they're sure that it's safe. If in doubt, contact the IT team for assistance.
- 6) If a user receives a forwarded copy of a message with the secured zip file, they need to ask to original recipient for the password. Only the original recipients can retrieve the password.

To secure suspicious attachments

Steps

- 1) In the **Inbound Content Filter** section of the Content Filter tab, select **Secure suspicious attachments**.
- 2) Click **Customize settings** to:
 - a) Review and customize the message that is inserted into the original message (annotates the message).
 - b) Add or remove sender addresses or domains to exclude from the secure attachment rule.
 - c) Click **Save** or **Cancel** to return to the Content Filter page.
- 3) Click **Save** to save your settings.

Message Size

There are 3 predefined actions available for application to 3 configurable message size thresholds:

- 1) You can set a global limit above which email should be discarded. By default this cannot exceed 50 MB. (This is applicable only to inbound email.)



Note

When an email is discarded because it exceeds the maximum allowable size, Forcepoint Email Security Cloud does not issue a notification (see *Email notifications* for more details). A failed delivery code is returned to the sending email server.

- 2) You can quarantine email above a specified size.
- 3) You can defer email above a specified size for delivery within a configurable time window. Deferral of large email is useful when you have Internet bandwidth capacity limitations and the user impact of delivering large email is noticeable during the main working day.

Related concepts[Email notifications](#) on page 62

Filtering using lexical rules

The lexical rules feature provides a powerful content filtering capability to mitigate the risks associated with email. A lexical rule compares words in a dictionary to those in an email and performs an action when there is a match.

You can use this feature to analyze messages for profanity and other undesirable content entering or leaving your organization. This might be profanity or inappropriate words but could also include company confidential information, or communications that could cause loss of business, or loss of reputation.

**Note**

We do not recommend using this feature to attempt to block spam, because generating ad-hoc rules is both time-consuming and prone to the introduction of false positives.

To set up lexical filtering rules, select the **Content Filter** tab of your policy, then click the link under Inbound or Outbound content: **Filter using these lexical rules**.

From this screen you can do the following:

- To add new lexical rules, click one of the buttons under **Add Lexical Rule**.
- To edit an existing rule, click the rule you want to edit.

Phrase score and lexical rule thresholds

Each word or phrase in a dictionary is assigned a score that is used to determine the disposition in a lexical rule. Typically a higher score indicates a worse contravention of the rule. For example, a higher score would be assigned to the most obscene words in a list of profane words.

A lexical rule specifies a set of thresholds and actions on each. When a message is compared to the phrases, it accumulates scores for each of the phrases on which it matches. The scores for the phrases within each dictionary are totaled. The greatest threshold that is breached causes an action to be taken on the message.

Creating a lexical rule in simple mode

The simple mode for entering lexical rules enables you to set up a single action to take when a message matches a phrase from the list you specify. If you want to set up lexical rules to match against system or custom dictionaries, or want to include multiple actions depending on the number of phrases matched, see *Creating a lexical rule in advanced mode*.

Steps

- 1) On the main Lexical Rules screen, click **Add Simple Rule**.
- 2) Enter a name for the rule and a description if desired.

- 3) In the **Apply To** field, enter the domain(s) or individual email address(es) or select the group to which this rule applies. Note that these must be domains or email addresses associated with your account: for an outbound rule, this would apply to senders, and for an inbound rule it would apply to recipients. If you do not enter any information in this field, the rule applies to everyone.
- 4) Select the **Exclude certain senders/recipients** checkbox to specify domains, email addresses, or groups to exclude from the rule. The **Excluded recipients** and **Excluded senders** fields appear.
In the exclude fields, enter any domains or individual email addresses, or select the group to be excluded from this rule. If you do not enter any exclusion information, nobody is excluded from the rule.



Important

For inbound and outbound lexical rules, you can create a list that excludes certain senders and a list that excludes certain recipients. For example, you can specify that a lexical rule does not apply if an email is from xyz@externaldomain.com or is sent to xyz@internaldomain.com. In all exclusion lists, you can enter up to 65,535 characters, consisting of domains, addresses, or groups, separated by commas.

If the service detects an email's sender address is spoofed, lexical rule exclusions are not applied.

- 5) In the **Phrases** field, enter one or more phrases for the rule to match against.
- 6) Select an **Action** from the drop-down list. The following actions are available:
 - **Quarantine** the message. Optionally:
 - Elect to notify recipients, the postmaster, and/or others, with the selected notification messages.
 - Elect to give end users, in their Personal Email Subscription report, the option to view or release messages that trigger the rule.
 - **Encrypt** the message (optionally notify the sender and/or others). This option is only available for outbound lexical rules, and if you have the Email Security Encryption Module (see *Advanced encryption*).
 - **Forward** message to a specific address.
 - **Tag the subject**, deliver it, **and send a blind carbon copy** to another address.
 - **Blind carbon copy** the message to another address.
 - **Tag the subject** with a specified phrase and deliver the message.
 - Deliver the message without any tags and **keep a copy** for checking.



Note

There is a quota for the number of messages that can be retained with the Keep Copy action. When you select Keep Copy or manage a lexical rule that uses Keep Copy, the used and available quota is displayed. If you exceed this quota, messages matching the Keep Copy criteria are logged in the Message Center, but you cannot read the message contents. To free space, delete some messages in the Message Center and then contact Support to have the lexical rule(s) using Keep Copy checked and re-enabled.

- 7) Define whether the rule should match against the message headers, or the whole message body and subject.
- 8) Click **Submit**.

Related concepts[Advanced encryption](#) on page 136**Related tasks**[Creating a lexical rule in advanced mode](#) on page 121

Creating a lexical rule in advanced mode

The advanced mode for entering lexical rules enables you to match against system or custom dictionaries, and include multiple actions depending on the number of phrases matched. (If you want to specify a single action to take when a message matches a phrase from a list, see *Creating a lexical rule in simple mode*.)

From this page, you can access the Dictionaries page to create or edit your custom dictionaries.

**Note**

You can also access the dictionaries page by navigating to **Email > Settings > Dictionaries**. Dictionaries can include simple phrases, complex multi-word searches, or regular expressions. For more information, see *Managing dictionaries*.

To add a lexical rule in advanced mode:

Steps

- 1) On the main Lexical Rules screen, click **Add Advanced Rule**. (To edit an existing rule, click the rule that you want to edit).
- 2) Enter a name for the rule and a description if desired.
Note that the new rule is enabled by default. You can change this later if required.
- 3) From the **Dictionary** drop down box, select the dictionary you want to use for this rule.
- 4) In the **Include recipients or senders** field, enter the domain(s) or individual email address(es) or select the group to which this rule applies. Note that these must be domains or email addresses associated with your account: for an outbound rule, this would apply to senders, and for an inbound rule it would apply to recipients. If you do not enter any information in this field, the rule applies to everyone.
- 5) In the **Excluded recipients** and **Excluded senders** fields, enter any domains or individual email addresses, or select the group to be excluded from this rule. If you do not enter any exclusion information, nobody is excluded from the rule.

**Note**

For inbound and outbound lexical rules, you can create a list that excludes certain senders and one that excludes certain recipients. For example, you can specify that a lexical rule does not apply if an email is from [xyz@externaldomain.com](#) or is sent to [xyz@internaldomain.com](#). In all exclusion lists, you can enter up to 65,535 characters consisting of domains, addresses, or groups, separated by commas.

- 6) Click **Submit**.
The rule details are displayed. You can click **Edit** to change any of the details entered in the steps above, or to disable the rule.
- 7) Click **Add...** to tell Forcepoint Email Security Cloud what to do when a message matches entries in the dictionary. The Lexical Rule Action screen appears.
- 8) Specify a threshold, an action, and any notification options related to the selected action, then click **Add** to save your changes. The rule is triggered when the combined value of all matched words in the message is greater than or equal to this threshold.

Next steps

There are 7 different actions that can be performed on the email. You can therefore configure up to 7 different thresholds, each with a separate action:

- Quarantine message (optionally notify sender, recipients, and/or others with the selected notification messages).



Note

Once an email message is quarantined, no further actions can be performed on that message. Therefore, if you set a quarantine action at a certain threshold, any other action set at a higher threshold will fail.

- Encrypt the message (optionally notify the sender and/or others). This option is only available for outbound lexical rules, and if you have the Email Security Encryption Module (see *Advanced encryption*).
- Forward message to a specific address.
- Tag the subject with a specified phrase and deliver the message.
- Blind carbon copy the message to another address.
- Tag the subject, deliver it, and send a blind carbon copy to another address.
- Deliver the message without any tags and keep a copy for checking.



Note

There is a quota for the number of messages that can be retained with the Keep Copy action. When you select Keep Copy or manage a lexical rule that uses Keep Copy, the used and available quota is displayed. If you exceed this quota, messages matching the Keep Copy criteria are logged in the Message Center, but you cannot read the message contents. To free space, delete some messages in the Message Center and then contact Support to have the lexical rule(s) using Keep Copy checked and re-enabled.

For quarantined messages, you can also define whether end users can view or release any messages caught by this lexical rule from their personal email report.

In the example above, inbound email is checked against a dictionary of offensive phrases to protect the intended recipient. Those that score 1.5 or above are quarantined. Email that scores 5 or above is likely to have matched multiple words or matched against words that have been allocated a higher score.

To help you choose an appropriate threshold for the actions you require, click **Show dictionary statistics** to display a statistical analysis of the selected dictionary. On the left side is a graphical representation of the distribution of scores in the dictionary. On the right side are a few statistics that may help you to choose a threshold.

**Note**

There is a limit on the number of regular expressions you can include in lexical rules for each policy. If your dictionaries include a large number of regular expressions, it might restrict the ability of the service to process your email. A warning appears when you are nearing this limit, and once you exceed the limit, you cannot save the lexical rule.

Related concepts

[Managing dictionaries](#) on page 124

[Advanced encryption](#) on page 136

Related tasks

[Creating a lexical rule in simple mode](#) on page 119

Creating a compliance rule

Forcepoint Email Security Cloud includes dictionaries for 2 compliance standards:

- PCI Compliance isolates email messages that contain payment card information
- State Data Privacy Laws (SDPL) compliance isolates email messages that contain Social Security numbers

When you add a compliance rule, the dictionary, threshold score, and action are predefined. If you need to edit any of the default settings, you can do so after the rule has been created.

Steps

- 1) On the main Lexical Rules screen, click **Add Predefined Compliance**.
- 2) Select the compliance rule type you want to use.
- 3) To edit the rule's default settings, click the rule name.
From the resulting screen, you can edit the rule name, description, and the groups or users included in or excluded from the rule. You can also define different thresholds.

Quarantining messages where analysis does not complete

If lexical rule processing does not complete for a message, you can specify that it is quarantined immediately. This might occur if you have set up a large amount of lexical rules and regular expressions.

If you choose to quarantine a message of this type, you can examine it in the Message Center by searching for messages labeled Lexical Rule, with the sub-reason Analysis Failure. For more information, see *Message Center*.

You can select different settings for inbound and outbound messages.

Steps

- 1) On the Content Filter tab, click **Edit** under either Inbound or Outbound.

- 2) Check the **Quarantine message if content analysis does not complete** box. If the box is not checked, any messages with incomplete lexical rule analysis are allowed through for further processing.
- 3) Click **Submit**.

Related information

[Message Center](#) on page 143

Managing dictionaries

Dictionaries are used to define phrases that are used in lexical rules, used for inbound and outbound email content filtering. (See *Content Filter tab*).

Forcepoint Email Security Cloud defines two types of dictionary: those that are predefined and your custom dictionaries. The former are maintained by Forcepoint and include common profanities; dictionaries relating to categories such as finance, gambling, and shopping; and compliance rules for payment card information and Social Security numbers. You can exclude phrases from these lists (see *Excluding phrases from a dictionary*) but you cannot include additional words or phrases; if you need to add phrases, system dictionaries can be embedded inside your own dictionaries.

Once defined, a phrase is available for use with both inbound and outbound lexical rules across all policies.

You can add 3 types of phrase to a custom dictionary:

- A simple string, for example “project rhine”.
- A complex multi-word search. This option searches on different variations of the phrase you define; for example if you enter “confidential email”, a lexical rule might match the exact phrase or any instances of the words “confidential” and “email” appearing close to each other in a message. See *Advanced dictionary configuration* for more examples.
- A regular expression. See *Including regular expressions*.

Assign each phrase that you add a score. This is used to determine the disposition in a lexical rule: typically a higher score indicates a worse contravention of the rule. When the rule is used analyze a message, the scores of all matching phrases are summed and the total is measured against the lexical rule threshold value.

Phrases can have positive values (meaning they increase the likelihood of the rule being triggered), negative values (meaning they decrease this likelihood), or a zero value (meaning they have no effect on the total value).

You can also select the following options instead of a numerical score:

- **Always trap this phrase** – assigns a score of +20 to the phrase, making it likely that a message will exceed your configured threshold.
- **Always let through** – assigns a score of -20 to the phrase, making it unlikely that a message will exceed your configured threshold.
- **Ignore this phrase** – assigns a score of 0 to the phrase, meaning that the phrase will not influence whether a message exceeds your configured threshold.

For instructions on how to configure lexical rules and threshold values for your policies, see *Creating a lexical rule in advanced mode*.

Related concepts

[Content Filter tab](#) on page 110

[Advanced dictionary configuration](#) on page 127

Related tasks

[Excluding phrases from a dictionary](#) on page 126

[Including regular expressions](#) on page 126

[Creating a lexical rule in advanced mode](#) on page 121

To add a new dictionary

Steps

- 1) On the Dictionaries screen, click **Add Custom Dictionary**. (To view the contents of an existing dictionary or to edit a custom dictionary, click the dictionary name.)
- 2) Enter a name for the dictionary and a description if desired; then click **Add**. (If you are editing an existing name or description, click **Submit**.)
- 3) To include an existing dictionary:
 - a) Click **Attach dictionary**.
 - b) Select an existing dictionary from the drop-down list, then click **Submit**.

Including simple phrases in a custom dictionary

Steps

- 1) Click **Attach phrase**.
- 2) In **Search type**, select **Simple substring search**.
- 3) Enter the phrase to add in the **Phrase** field, assign it a score, and indicate which parts of the message you want to apply it to.
- 4) Click **Submit**.

Including complex searches

Steps

- 1) Click **Attach phrase**.
- 2) In **Search type**, select **Complex multi-word search**.
- 3) Enter the phrase to add in the **Phrase** field.

- 4) Assign a score to the phrase, and indicate which parts of the message you want to apply it to.
- 5) Click **Submit**.

Including regular expressions

Regular expressions (RegEx) are a powerful way of matching a sequence of simple characters. Using regular expressions in your dictionaries enables you to specify precise phrase matching for your email.



Note

Regular expressions are not case-sensitive.

There is a limit on the number of regular expressions that can be included in lexical rules for each policy. If your dictionaries include a large number of regular expressions, it might restrict the ability of the service to process your email. Lexical rules that include a large number of regular expressions cannot be saved.

For syntax and some examples, see *Standard Regular Expression Strings*.

Steps

- 1) Click **Attach phrase**.
- 2) Click **Regex view**.
- 3) Enter the regular expression in the **Regex** field.
- 4) Enter a description for the regular expression. This description appears in the dictionary items list with “regex” next to it to signify that a regular expression was defined.
- 5) Assign a score to the phrase, and indicate which parts of the message you want to apply it to.
- 6) In the **Test against** field, enter some text that can test whether your regular expression is well-formed and meets your requirements, then click **Test regex**.
- 7) When you are happy with the regular expression, click **Submit**.



Note

To return to the simple substring search or complex multi-word search options, click **Simple phrase view**.

Related information

[Standard Regular Expression Strings](#) on page 246

Excluding phrases from a dictionary

You can exclude words or phrases from both system and custom dictionaries.

Steps

- 1) On the Dictionaries screen, click the dictionary name.
- 2) Under Dictionary Items, select the phrase you want to exclude.
- 3) Select a phrase exclusion option. If you choose to exclude the phrase within specific policies, select the policy or policies to apply the exclusion to.
You can select multiple items from each list by holding down the **Ctrl** key and clicking the items. To make selection easier, you can expand the list to appear in a larger window by repeatedly clicking on the **Grow list** link.
- 4) Click **Submit**.
The excluded phrase appears in the dictionary with a line through it.

Advanced dictionary configuration

There are a number of techniques you can use for more advanced content filtering:

- If a pair of words must appear close to each other in the message, separate them with the NEAR keyword, for example, dear NEAR sir. By default, NEAR allows up to 8 words between the two phrases. To control the number of words allowed (the *nearness*), specify it inside square brackets after the NEAR keyword, for example, dear NEAR[2] sir.
- If the phrase consists of a set of words, on which any one can be matched, you can use the OR keyword. However, a better way of dealing with this situation is to create a separate phrase for each word. For example, you can use bow OR bough but, more simply, you can create two phrases, one for bow and one for bough.

Importing language packs

By default, you have access to the English language dictionaries. You can add other language dictionaries if you wish. Dictionaries are provided for the following languages:

- Dutch
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish
- Traditional Chinese
- Simplified Chinese

To import an additional language pack or remove existing packs:

Steps

- 1) On the Dictionaries screen, click **Manage Language Packs**.
- 2) Select the language packs you want to use.
- 3) Click **Save**.



Note

You cannot remove a language pack that is being used by a lexical rule. You must first remove all dictionaries in that language from your lexical rules.

Encryption tab

Select the **Encryption** tab to view or modify encryption policies.

Email encryption secures delivery of email by ensuring that it is not forwarded as plain text “in the clear.” Forcepoint Email Security Cloud encrypts the transport layer protocols being used to deliver the email at the edge of the network – the point where it leaves the secure environment of the local area network.

The following encryption functionality is available:

- Transport Layer Security (TLS) for secure enterprise-to-enterprise email communications (see *Transport Layer Security*)
- Standard encryption rules for securing email to individuals (see *Standard encryption*)
- Advanced encryption rules for secure identity-based encryption (see *Advanced encryption*). This option requires the Email Security Encryption Module.

To add a secure transport policy setting, or an encryption rule, click the relevant **Add** button.

Related concepts

[Transport Layer Security](#) on page 128

[Advanced encryption](#) on page 136

Related tasks

[Standard encryption](#) on page 133

Transport Layer Security

TLS provides a transport layer encrypted “tunnel” between email servers or mail transfer agents (MTAs).

By default, Forcepoint Email Security Cloud always attempts to deliver or receive email using opportunistic TLS if the sending or receiving MTA supports it. With opportunistic TLS, if a connection attempt is made using the TLS protocol, the connection recipient must provide appropriate TLS credentials for an encrypted data transfer. If the TLS “handshake” fails, the data transfer is made via plain text, rather than encrypted text. In either case, the data transfer is successfully accomplished.

Alternatively, you can enforce TLS connections. There are 2 stages to configuring mandatory TLS:

- 1) Add security settings to the connections between your mail transfer agent (MTA) and the Forcepoint Email Security Cloud relays. See *Configuring TLS on your connections*.
- 2) Add routes to the third-party MTAs with whom you want to communicate using TLS and add security settings to these.

When the conditions within the TLS policy are not met, Forcepoint Email Security Cloud does not deliver the email.

See this article for a full list of [trusted certificate authorities](#) supported by Forcepoint Email Security Cloud.



Note

Forcepoint Email Security Cloud can enforce TLS only on the immediate next SMTP hop. Situations may exist where Forcepoint Email Security Cloud does not deliver directly to recipients (e.g., they may be using a service similar to Forcepoint Email Security Cloud). In such situations, it is your responsibility to ensure that all intermediate SMTP hops support TLS. If this is outside of your control, we recommend you use the Forcepoint Email Security Cloud standard or advanced encryption functionality to provide secure delivery.

Related tasks

[Configuring TLS on your connections](#) on page 129

Configuring TLS for a connection or route

Similar configuration is required for both the connections between Forcepoint Email Security Cloud and your MTAs, and between Forcepoint Email Security Cloud and the third party MTAs that you wish to communicate with using TLS. These settings and the options are described below.

Each rule relates to a specific inbound or outbound connection and specifies whether TLS is enforced, a certificate is required and should be verified, and the encryption strength. If an attempt is made to deliver an email and the specified criteria are not met, the email delivery fails and the sending MTA is notified.

Configuring TLS on your connections

The first stage of setting up a TLS policy is to configure the security settings on the connections between the Forcepoint Email Security Cloud relays and your email gateways. To do this:

Steps

- 1) Select the **Connections** tab.
- 2) Click the server name of the inbound or outbound email gateway that you want to configure.
- 3) Click **Edit**.

- 4) Add security and encryption strength settings to the connections on which you wish to enforce TLS. Typically these are the same inbound and outbound.



Note

Inbound TLS settings apply to all inbound connections. If you have multiple MTAs receiving email from Forcepoint Email Security Cloud, all must be configured to use TLS.

Configuring third-party TLS connections

You must add the connections to and from the businesses with whom you wish to communicate using TLS. To do so:

Steps

- 1) Select the **Encryption** tab.
- 2) Click **Add** in the Secure Transport section.
- 3) In the **Domain/Server** field, enter the IP address or fully qualified domain name of the business with whom you are establishing connection. For outbound connections, enter the recipient's domain. For inbound connections, enter a server name or IP address. Do not specify a server that is part of your MX records. Click **Check SMTP Connectivity** to confirm that you can connect to the domain name or IP address.
- 4) Select a direction for the connection: **Inbound** or **Outbound**.
- 5) Select a security level:

Security Level	Description
Unenforced	Forcepoint Email Security Cloud does not attempt to use TLS for this connection.
Encrypt	Delivery of a message fails (inbound or outbound) if the MTA with which it is communicating cannot use TLS to force an encrypted connection at the encryption strength configured for this connection or route. No certificate is required.
Encrypt + CN	As Encrypt but a certificate must also be presented on which the common name matches the MTA with which Forcepoint Email Security Cloud is communicating.
Verify	As Encrypt but the certificate must be from a trusted certificate authority (CA).
Verify + CN	As Encrypt + CN but the certificate presented must be from a trusted CA.

We recommend that you use Verify + CN, but you may opt to use Encrypt + CN if you want to use a self-signed certificate rather than paying for use of one from a CA. This may be acceptable for the connections between your MTA and Forcepoint Email Security Cloud.

- 6) Select an encryption strength:

Encryption Strength	Description
128	An encryption algorithm that supports a 128 bit key must be negotiated between Forcepoint Email Security Cloud and the MTA with which it is communicating.
256	An encryption algorithm that supports a 256 bit key must be negotiated between Forcepoint Email Security Cloud and the MTA with which it is communicating.



Note

You must ensure that the MTA supports the policy configured for its connections (certificate and encryption strength) and it must support an algorithm also supported by Forcepoint Email Security Cloud.

- 7) To enable the connection for TLS immediately, check **Enabled**.
- 8) Click **Save**.

Next steps

For outbound connections, we recommend that you check the TLS status of the server before enabling it. If you route mail to domains that do not support TLS, it will result in the non-delivery of your messages. For more information, see *Testing an outbound connection*.

The companies with whom you want to communicate using TLS must ensure that their MTAs support one of the encryption algorithms supported by Forcepoint Email Security Cloud and the encryption strength that you configure in the policy. They must also be able to present a certificate appropriate to the policy that you configure.



Note

The third-party MTA must support the required configuration on the inbound and outbound connections or email delivery fails.

Related tasks

[Testing an outbound connection](#) on page 131

Testing an outbound connection

You can test an outbound TLS connection, because Forcepoint Email Security Cloud is responsible for initiating the connection.

Steps

- 1) Click a connection you have added to the Secure Transport section of the Encryption tab, then click **Check TLS status of server**. This brings up a test message using TLS. (Alternatively, click **Check** in the TLS Status column on the Encryption tab.)

- 2) Modify the test parameters if desired: the email address, the encryption strength, the security level.
- 3) From the drop-down list, select a service cluster from which to perform the test.
- 4) Click **Send**. The test results appear.

The response indicates whether or not Forcepoint Email Security Cloud was able to deliver the email in accordance with the configured policy. Note that if the service finds 2 MX records, it sends 3 messages. Check that all have arrived.

If the TLS check fails, check that the mail transfer agent (MTA) supports the settings in the policy.

When TLS fails

Forcepoint Email Security Cloud does not deliver a message in the clear if the policy dictates that it should use TLS. If TLS cannot be used when dictated by the policy, Forcepoint Email Security Cloud rejects the message. The report that is returned to the sender is dependent upon their email server.

Condition	Action when TLS cannot be started	Message Center reporting for the log entry
You try to send email to the service from a connection specified as secure.	The service rejects the email with a permanent error. Your email server should send a non-delivery notification to the sender.	TLS (not verified) - message rejected
The service tries to send email to a third-party domain specified in the secure transport policy.	The service rejects the email with a reason "cannot start TLS". Your email server should send a non-delivery notification to the sender.	Email is shown as "clean" because it was accepted from the customer, but the log indicates that onward delivery failed.
A third party tries to send email to the service from a connection specified in the secure transport policy.	The service rejects the email with a permanent error. The third party's email server should send a non-delivery notification to the sender.	TLS (not verified) - message rejected
The service tries to send an email to you through a connection specified as secure.	The service rejects the email with a reason "cannot start TLS". The third party's email server should send a non-delivery notification to the sender.	Email is shown as "clean" because it was accepted from the third party, but the log indicates that delivery failed.

Adding an encryption rule

There are 2 types of encryption rule available in Forcepoint Email Security Cloud:

Standard encryption is typically used to enforce encryption policy when the recipient's MTA does not support TLS. This functionality relies on a TLS connection with you to secure communications between your MTA and Forcepoint Email Security Cloud. Recipients require a manually-generated password to access the encrypted email.

Advanced encryption uses identity-based encryption (IBE) to protect data without the need for certificates. Protection is provided by a key server that controls the mapping

of identities to decryption keys. The recipient of an encrypted email authenticates against the key server to receive the decrypted version of the message.

To enable advanced encryption, you must have the Email Security Encryption Module, and you must set the security on your outbound connection routes to Verify+CN. See *Connections tab*.

Related concepts

[Advanced encryption](#) on page 136

[Connections tab](#) on page 83

Related tasks

[Standard encryption](#) on page 133

Standard encryption

Standard encryption comprises rules that, when matched, trigger the standard functionality process. This process is as follows:

- 1) Sender sends email that triggers the rule.
- 2) The email is saved to the Encryption service quarantine store.
- 3) The recipient is sent an email notification containing an encrypted link that when clicked allows access to the Encryption service quarantine store by HTTPS.
- 4) The sender is sent one or more notifications, depending on the number of recipients. Each notification contains a password that is required by a recipient to access the email. The sender needs to notify the recipient(s) of their password.

The criteria for the “parking” rules can include:

- Sender addresses
- Recipient addresses
- Messages marked as “sensitive” in the email headers
- Messages including a pre-defined prefix (trigger word) in the subject line.

To set up standard encryption, click **Add** in the Encryption section of the **Encryption** tab.

Steps

- 1) Enter a name for the encryption rule, and select **Standard Encryption** as the encryption type.
- 2) Define the password generation criteria (see *Password specification*).

- 3) Optionally, enter one or more senders or recipients for the rule to apply to. These can be individual email addresses, groups configured in Forcepoint Email Security Cloud, or domain names. You can enter multiple senders or recipients, separated by commas.
To edit an existing sender or recipient, click the item. Press **Enter** to save your changes as a new entry in the sender or recipient list. To discard your changes, press **Esc**.
To remove an item from a sender or recipient list, click the Delete icon next to the item.
- 4) If you are including subject criteria in the encryption rule, select whether the message should match any of the criteria, or all of the criteria you select to trigger the rule.
- 5) To include messages with a sensitivity setting in the email headers for encryption, mark **The message contains a sensitivity header**, and select an option from the drop-down list. If you want the rule to match against all sensitivity headers, select **Any**.
- 6) To define a trigger word that appears at the beginning of the subject line for messages to be encrypted, mark **The subject starts with** box, and enter the trigger word.



Note

A trigger word is not case sensitive and **MUST** be followed by a space.

- 7) If required, edit the notifications sent to sender and recipient (see *Notifications*).
- 8) Click **Submit**.
When an outbound email meets all of the specified criteria, the email is subjected to the standard encryption process.

Related concepts

[Notifications](#) on page 135

[Password specification](#) on page 134

MIME details

You can choose to include (default) or exclude the MIME details when a parked, standard encryption message is retrieved and delivered to the recipient (end user). The setting you select applies to all policies.

To change the setting, in the Encryption section click the **Standard encryption preferences** link, move the slider to the desired setting, and click **Save**.

Password specification

The password can be automatically generated by the system or specified in the subject of the email.

Automatic password generation: This occurs if **Allow sender to specify a password** is not checked.

If **Allow sender to specify a password** is checked, the user must include the password in the subject line of the email. There are two options for inclusion:

- 1) If the rule specifies a trigger word, the password follows this in the subject line.

- 2) If the rule does not specify a trigger word, you must add a prefix that is used to identify the password in the **subject prefix** field. Note this is different from the trigger in that it is not a criterion for rule execution.

The password must consist of alphanumeric characters only. Both the prefix and password must be followed by a space and the password must be enclosed in parentheses (). Both are stripped from the email by Forcepoint Email Security Cloud.

For example, to trigger standard encryption with a specified password from a message with the following subject:

Forcepoint Email Security Cloud test of standard encryption

You would augment the message subject as follows:

ENCRYPT (xyz987) Forcepoint Email Security Cloud test of standard encryption



Note

The **subject prefix** field is available only when the **Where the subject begins with** box is not checked.

Notifications

When an email is “parked,” the sender and recipient(s) are notified by email. The notification sent to the recipient(s) includes a link to the cloud service portal from where the message can be retrieved. The notification(s) sent to the sender includes a password that the sender must communicate to the recipient(s). The recipient(s) needs this password in order to retrieve the message. To set up notifications, open the standard encryption rule (click the name of the rule in the Encryption section of the **Encryption** tab), then edit the **Sender** or **Recipient** text under **Notifications**.

Both sender and recipient notifications can be fully customized on a per-rule basis, in both plain text and HTML format.

Accessing email

To access a parked message, the recipient clicks the link, accesses the cloud service portal using HTTPS, and is prompted to enter a password.

Once recipients enter a password, a message is shown. They can access each part of the message and download any attachments. The message itself can be downloaded and viewed by an email client that supports a MIME type message/rfc822.

Combining standard encryption with content filtering rules

To guard against end users inadvertently sending unsecured sensitive data outside your organization, you can set up a lexical rule that triggers standard encryption for any message that matches against that rule.

For example, from the **Content Filter** tab set up a predefined PCI compliance rule (see *Creating a compliance rule*), and then edit it to include the Tag subject action at a threshold you choose. Tag the subject line with a phrase such as “Encrypt”.

Next, click **Add** in the Encryption section of the **Encryption** tab. In the **The subject starts with** field, enter the phrase you chose to tag the subject line.

When the standard encryption rule is set up, this ensures that a message matching against the compliance rule is parked for secure HTTPS retrieval by the recipient, with notifications going to the sender and recipient as configured in the encryption rule.

Related tasks

[Creating a compliance rule](#) on page 123

Advanced encryption

If you have the Email Security Encryption Module, you can send messages that use identity-based encryption, with no need for users to manually exchange passwords. You can also customize the email notification that the recipient sees before decrypting the message.

Related concepts

[Prerequisites for advanced encryption](#) on page 136

[How advanced encryption works](#) on page 137

Related tasks

[Adding an advanced encryption rule](#) on page 138

Prerequisites for advanced encryption

To use advanced encryption, you must have a TLS certificate on the server designated as an outbound connection. This certificate must meet the following requirements:

- The certificate is issued by a supported certificate authority. For a list of supported CAs, see the knowledge base article [trusted certificate authorities](#)
- Wildcard certificates are supported. Note that multi-level subdomains (for example, sub2.sub1.mydomain.com) are not supported with a standard subdomain wildcard certificate (for example, *.mydomain.com).
- Subject Alternative Name (SAN) certificates are not fully supported. Only the name listed as the Common Name (CN) will be recognized. Any names defined as SANs will be ignored.
- The Subject CN of the certificate must match the outbound connection's fully-qualified domain name (FQDN).

In addition, note the following requirements for your TLS connection:

- The sending IP address must resolve to the outbound connection's FQDN.
- The outbound connection's FQDN must resolve to the sending IP address.
- Your MTA's sending HELO string must match the outbound connection's FQDN.

For more information about TLS, see *Transport Layer Security*.

Related concepts[Transport Layer Security](#) on page 128

How advanced encryption works

When an advanced encryption rule is matched, the following process takes place:

- 1) Sender sends email that triggers the rule.
- 2) The email is encrypted by Forcepoint Email Security Cloud using identity-based encryption, and sent on to the recipient's MTA for delivery.
- 3) The recipient is sent an email notification containing an HTML attachment. When opened in a browser, the attachment displays a button that the recipient clicks to access to the secure encryption network via HTTPS. The recipient must register their email address and a password with the secure encryption network if this is the first time they have received an encrypted message via Forcepoint Email Security Cloud. The recipient then uses this password to access all subsequent encrypted messages sent to their email address.
- 4) If the recipient replies to the encrypted message, the message is decrypted by Forcepoint Email Security Cloud and then analyzed in the same way as other inbound mail before delivery.

There are 3 ways to use advanced encryption:

- **Content-based:** Set up lexical rules so that a message will automatically be encrypted if it contains certain phrases. See *Creating a lexical rule in advanced mode*.
Note that if a message triggers a lexical rule with a Quarantine action and a rule with an Encrypt action, the Quarantine action will take precedence and the message will be quarantined without encryption.
If a message triggers a rule with the Encrypt action and a rule with either Forward, Tag Subject, BCC, or BCC and Tag Subject, the Encrypt action will take precedence and the other action(s) will not be applied.
If a message triggers lexical rules with the Encrypt and Keep Copy actions, both actions will be applied.
- **Sender/recipient-based:** Set up an advanced encryption rule that encrypts a message sent from or to specific users.
- **Subject and content-based:** Set up an advanced encryption rule that encrypts a message with a certain trigger word in the subject header, a particular sensitivity header, or specific phrases in the message headers or body.

You can combine these methods to configure the encryption policy that you require. Advanced encryption integrates with other aspects of your email policy as follows:

- If you have set up attachment parking, an attachment that meets the parking criteria will be parked before the message is encrypted. The decrypted message will contain a link to retrieve the attachment. See *Parking attachments*.
- If you have outbound aliases, the aliases will be applied before the message is encrypted. The resulting encrypted message will always show the external address.

Related concepts[Parking attachments](#) on page 114

Related tasks[Creating a lexical rule in advanced mode on page 121](#)

Adding an advanced encryption rule

To set up sender/recipient-based or subject and content-based advanced encryption, click **Add** in the Encryption section of the **Encryption** tab.

Steps

- 1) Enter a name for the encryption rule, and ensure **Advanced Encryption** is selected as the encryption type.
- 2) To notify the message sender when a message has been encrypted, mark **Notify sender**. You can also notify others by entering a comma-separated list of email addresses.

- 3) Optionally, enter one or more senders or recipients for the rule to apply to. Recipients can be either specifically included in or excluded from the rule.

You can enter individual email addresses, groups configured in Forcepoint Email Security Cloud, or domain names. You can enter multiple senders or recipients, separated by commas.

To edit an existing sender or recipient, click the item. Press **Enter** to save your changes as a new entry in the sender or recipient list. To discard your changes, press **Esc**.

To remove an item from a sender or recipient list, click the Delete icon next to the item.

- 4) If you are including subject criteria, content criteria, or both in the encryption rule, select whether the message should match any of the criteria, or all of the criteria you select to trigger the rule.
- 5) To include messages with a sensitivity setting in the email headers for encryption, mark **The message contains a sensitivity header**, and select an option from the drop-down list. If you want the rule to match against all sensitivity headers, select **Any**.
- 6) To define a trigger word that appears in the subject line for messages to be encrypted, mark **The subject** box, and select whether the trigger word is at the start of the subject or is contained anywhere in the subject line. Then enter the trigger word.

**Note**

A trigger word is not case sensitive and **MUST** be followed by a space.

- 7) To specify phrases that trigger encryption if contained in a message, mark **The message contains any of the following phrases**, and select whether the phrases appear in the message body or headers. Enter each phrase on a new line, by pressing **Enter** after each phrase. The phrases are not case sensitive.
- 8) Click **Submit**.

Editing advanced encryption settings

Use the Advanced Encryption Settings area of the **Encryption** tab to fine-tune the content of the email notification template delivered to recipients. For example, you might want to include your organization name, and a contact method in case the recipient has trouble accessing the message.

A Forcepoint logo appears in the email notification by default. You can replace this logo with a custom version, for example the logo of your organization. The logo must be hosted at a URL that will be accessible by all encrypted message recipients, such as your company website.

You can also add annotations to the decrypted message, and define the action to take on messages that have already been encrypted before being sent through Forcepoint Email Security Cloud.

Steps

- 1) Under Advanced Encryption Settings, click **Edit**.
- 2) To include an annotation at the end of the decrypted message, select **Add annotations to the inbound decrypted message**.
Click the **annotations** link to edit the annotation (see *Editing an annotation*).
- 3) Select **Quarantine messages that are already encrypted** if you want to quarantine outbound messages that have been encrypted using a different method, for example S/MIME.
If you do not select this option, outbound messages that have been encrypted using a different method are processed without adding advanced encryption.
- 4) To replace the Forcepoint logo in the notification template, select **Use custom logo**, and enter the URL where the custom logo is located.
- 5) Select **Add custom text to encrypted message template** to include your own text in the email notification sent to recipients.
Enter the text in the field below the check box. Note that HTML tags are not supported. The text appears in the email notification in addition to the standard text that explains how to access the encrypted message.

- 6) If required, specify the language in which to display the standard text of the email notification. The following languages are available:
 - Czech
 - Dutch
 - English
 - French
 - German
 - Greek
 - Italian
 - Polish
 - Portuguese (Brazilian)
 - Portuguese
 - Romanian
 - Slovak
 - Spanish
 - Swedish

- 7) Click **Submit**.

Related tasks

[Editing an annotation](#) on page 78

Data Protection tab

When the Data Protection Service (DPS) is enabled for your account, a Data Protection tab is available when adding or editing a policy.

Click the **Data Protection** tab in the policy to configure options for handling potential data issues using DPS.



Note

Data Protection Service integration requires an additional license. If you would like further information on integrating with Data Protection Service, contact your account manager.

When Data Protection Service is enabled, enterprise data protection is handled by DPS: the cloud service sends outbound email messages containing sensitive data to DPS for inspection. Sensitive data may include intellectual property, data that is protected by national legislation or industry regulation, and data suspected to be stolen by malware or malicious activities. Email messages containing such data are then blocked or allowed based on information provided to the cloud service by DPS, using the policies defined in Forcepoint DLP.

On the Data Protection tab:

Before you begin, ensure that you have uploaded the configuration file on the **Account > Data Protection Settings** page.

- 1) When you are ready for DPS to be used for data security, toggle the Enable Data Protection Service button to **ON**.

Until this switch has been turned on and the change saved, data security is not monitored for the policy.

- 2) From Analysis mode, select the type of analysis provided by DPS: **Enforce** or **Monitor**.
When Enforce is selected, data security is monitored on the policy and enforced through DPS. When Monitor is selected, data security is monitored on the policy, but not enforced, and results are logged.
- 3) The default selection for DPS fallback behavior is **Allow**. This cannot be changed. In the event of a DPS timeout or other error, all email messages are allowed.
- 4) Click **Save**.

Message Center

Contents

- Introduction on page 143
- Understanding your results on page 148
- Performing actions on the results on page 149
- Viewing message details on page 151

Introduction

The Forcepoint Email Security Cloud Message Center is a powerful message tracking and management tool that provides access to all quarantined messages and message logs for your account.

To access the Message Center, select **Email > Messages > Message Center**. You are presented with a search form.

The search form lets you search for messages based on several layers of search criteria, such as the From, To, or Subject fields, the date sent, whether the message contained spam or a virus, and much more. The check box controls allow a granular search for clean email and/or those with an issue that caused Forcepoint Email Security Cloud to perform an action.



Note

Enter as much detail as possible to minimize the data returned and so reduce the time that the search takes. This is especially important for large accounts.

Search

Select the type of message for which you are looking. If you search for accepted messages, only clean messages are returned; if you search for quarantined messages, only quarantined messages are returned. You can also search for messages that have had certain actions performed on them, for example messages that have been released, forwarded, or deleted from quarantine. Information on deleted messages still appears in the search results, even though they have been deleted from the quarantine itself and cannot be viewed.



Note

To display deleted messages you must search for them specifically from the search drop-down list, or check the **Show deleted messages** box.

Show

Once a message is viewed by an end user or administrator, it is marked as reviewed. If an end user has viewed a multi-recipient message, it is shown as partially reviewed. If an administrator views a multi-recipient message, it is shown as reviewed for all recipients.

Date sent

You must specify a date range to search. The more exact the date range, the faster a search completes. The default drop-down list allows you to choose common ranges; for more exact time ranges, click **more** and use the calendar picker.

Clicking **more** reveals the date range. From here you can specify exact dates and times (by the hour) to search. Click the calendar icon to open the calendar picker. Choose the date of interest by clicking the relevant date link. This closes the pop up and populates the appropriate field with the date. You can select the To and From hour from the drop-down lists. The default is to search all hours in the selected day.

From

The sender of the email; you can include a wildcard in the search by entering an asterisk (*) character to denote multiple characters.

To

The recipient of the email; you can include a wildcard in the search by entering an asterisk (*) character.

Subject

The email subject; you can include a wildcard in the search by entering an asterisk (*) character.

Email direction

Select the direction to search: Inbound, Outbound, or Both.

When you select Outbound, the *Delivery status* drop-down appears if TLS reporting is enabled for your account.

Related concepts

[Delivery status](#) on page 145

Results per page

The number of results to display per page.

Show deleted messages

Indicate whether you want deleted messages to be included in the search results.

Delivery status

Select the delivery status for outbound messages. The default is to search for all messages; you can filter on messages delivered with TLS, delivered without TLS, pending delivery, or delivery failed.

This option only appears if TLS reporting is enabled for your account and you select Outbound for the email direction.

Clean

Indicate whether you want uninfected, non-spam messages to be included in the search results.

General

Access control	Messages blocked by an access control policy. This applies only to customers that have been asked to implement access controls by Forcepoint Email Security Cloud operations.
Operational	Messages blocked by controls set up by Forcepoint Email Security Cloud operations in response to a virus outbreak.
Message loop	Messages stopped automatically because they are part of a message loop caused by auto-forwarding or auto-replying.
System	Messages that could not be processed, for example, messages that contravene email protocols.

Antivirus

Virus	Messages that contain known viruses as identified by one of the commercial antivirus engines used in the Forcepoint Email Security Cloud service.
Macro	Messages that contain highly suspicious Microsoft Office document macros that operate outside the document, that you have chosen to quarantine under your policy.
Blocked executable	Messages that contain an executable file attachment that you have chosen to quarantine under your policy.
Phishing	Messages that are suspected to be phishing emails.

ThreatSeeker Intelligence

Format	Messages that deliberately attempt to expose vulnerabilities in email software with unusually formatted headers or body.
Dangerous content	Messages that contain potentially dangerous content.
Greylisted	Messages that contain executable content that is temporarily quarantined awaiting confirmation that it is safe for automatic release.
Potential viruses	Messages that contain potential viruses, identified by Forcepoint ThreatSeeker Intelligence but not yet identified by one of the commercial antivirus analyzers used within the Forcepoint Email Security Cloud service.
Confirmed viruses	Messages that contain a virus, identified by Forcepoint ThreatSeeker Intelligence and subsequently confirmed by one of the commercial antivirus analyzers.
File Sandboxing	Messages that have been analyzed by the File Sandbox. You can refine this further by selecting a File Sandboxing status from the drop-down list: choose from All, Clean, Malicious attachment(s), Malicious and pending further analysis, and Pending analysis.

Antispam

Spam	Unsolicited bulk messages. You can select a maximum and minimum spam score range to narrow this search further.
-------------	---

In blacklist	Messages that are in blacklist by the default or per-user policy.
In allowlist	Messages that are in allowlist by the default or per-user policy.
Bulk	Outbound messages that have been classified as bulk messages.
Commercial bulk email	Inbound messages that have been classified as commercial bulk email by the default or per-user policy.

Content Filter

Too large	Messages that exceed any size limits defined by the policy.
Extension masked	Delivered messages that contain an attachment whose file extension was masked as specified in the content filtering policy. You can restrict searches to one or more specific extensions by listing them in the associated field, separated by commas.
Blocked attachment	Messages that have been quarantined due to their file type being specified in the content filtering policy. You can restrict searches to one or more specific extensions by listing them in the associated field, separated by commas.
Lexical rule	Messages that have contravened a lexical rule in the content filtering policy. You can restrict searches to specific sub- reasons—either messages caught by the lexical filter or messages that have experienced analysis failure—by selecting the relevant option from the drop-down list.
Blocked images	Messages that contain an image attachment that has been analyzed and is considered inappropriate. Messages with this status may also have been quarantined because the image could not be analyzed, for example because it was too large. This option only appears if you are licensed for the Forcepoint Email Security Image Analysis Module.
Copy kept	Messages marked as available for delivery, but with a copy kept for review by administrators. If you have exceeded your quota for this type of message, the message delivery is logged, but you cannot view the content. To free quota space, delete some messages. Note that messages with this status may also have been caught by the lexical filter and quarantined for other reasons.

Encryption

TLS	Messages that policy dictates should be delivered using TLS whose delivery failed because the sender attempted to send them in the clear.
Ad hoc	Messages that triggered a standard encryption policy rule.
Advanced	Messages that triggered an advanced encryption policy rule. This option only appears if you have enabled advanced encryption.

Understanding your results

The query is hidden once a search has returned results. To show the query again, click

Show Query near the top left of the page. The search results are explained below:

Field	Description
From	The sender of the email.
To	The recipient of the email. If there is more than one recipient, the number of recipients is shown and, if you hover your mouse over the area, a popup appears listing up to 10 recipients. Open the message to see all the recipients.
Subject	The subject of the email. If the subject is long, it is truncated by ellipses (...). If you hover your cursor over the area, a pop-up appears. Click the subject to view a detailed log for the message.
Date / Time	The date and time of the email in your local time zone. If you hover your cursor over the area, a pop-up shows you the time in UTC.
Spam Score	The score assigned by Forcepoint Email Security Cloud.
Issue	The issues applicable to the email. If you hover your cursor over the area, a pop-up gives more information on the issues.
Action	The action(s) applied to the message. If you click the Action link for a message, you can view other actions that may have been applied to the message. Possible actions are listed below this table.

Possible Actions

- **Accepted** - The email was accepted and delivered.

- **Quarantined** - The email was quarantined for the reason described by the issue.
- **Released** - The email was quarantined, but a copy of the email has since been released to the recipients.
- **Release-pending** - The email was quarantined and a copy of the email has been requested to be released to the recipients.
- **Release-failed** - The email was quarantined and a release action was requested but it has failed.
- **Forwarded** - The email was quarantined, but a copy has since been forward to a specified email address.
- **Forward-pending** - The email was quarantined and a copy has been requested to be forwarded to a specified email address.
- **Forward-failed** - The email was quarantined and a forward action was requested but it has failed.
- **Multiple** - The email was quarantined and has had multiple actions performed on it; to see a description of these actions, hover your mouse over the multiple text and a pop-up appears. Multiple actions might include “released” and “forwarded”.
- **Deleted** - The email was quarantined and has now been deleted. It still appears in the search results, but the message itself has been deleted from the system. Clicking the message reveals the message log, rather than the message itself.
- **Discarded** - Forcepoint Email Security Cloud discarded the message but did not report this to the sending email server which believes the message was delivered.
- **Rejected** - Forcepoint Email Security Cloud rejected the message and reported this to the sending email server.

Reviewed and Not Reviewed Messages

Messages that have been reviewed are displayed differently from those that have not been reviewed. Reviewed messages appear in a slightly lighter shading and have an open envelope icon by them. Messages that are not reviewed have a darker shading and a closed envelope icon next to them. Messages can also be partially reviewed by end users from their personal email subscription report. These messages are shown as a partially opened envelope icon.

Downloading CSV results

You can download a comma-separated values (CSV) file of results from your query for use by other programs such as Excel to generate graphs or analyze the results in greater detail. The CSV download includes all instances of the messages per recipient.



Note

CSV downloads are limited to 50,000 lines.

Performing actions on the results

If you have permission, you may perform actions on the messages. The message center allows you to review, release, forward, and delete one or more messages.

To select a message, select the checkbox next to the envelope icon for that message. To select all messages on the page, click **Select All** in the header bar of the search results. Messages on other pages of the result set are not affected.

Having selected a set of messages, you can select the required action from the action bar drop-down list and click **Go**. When the operation is complete, the “Action” column for the message is updated; and if the message was previously marked as “Not Reviewed,” its status changes to “Reviewed.” If any errors occur during the action, they are displayed at the top of the page.

You can also perform actions on a message from the message’s details page. For more information, see *Viewing message details*.

The available actions are explained below.

Action	Description
Release	Releases a copy of the message to continue processing.
Release (no further processing)	Releases a copy of the message directly to the intended recipient, bypassing any further rules that you have set up for your inbound or outbound mail. We recommend that you review the message carefully before selecting this action.
Forward To	Forwards a copy of the message to the email address you specify. Note that this sends the message for further processing before delivery.
Forward (no further processing)	Forwards a copy of the message to the email address you specify, bypassing any further rules that you have set up for your inbound or outbound mail.
Mark as Reviewed	Indicates this message has been reviewed.
Mark as Not Reviewed	Use this to indicate that you have not yet read this message.
Delete Message	Deletes the message from the message center.

Related concepts

[Viewing message details on page 151](#)

Release and forward actions

Release and forward actions performed on a message via the Message Center are executed asynchronously by a separate process. All other actions execute immediately. For example, if a release action is requested, the message is marked as **release-pending** until the request is completed. It is then be marked as **released**. If the release fails it is marked as **release-failed**. Similar action states apply to forward actions. This functionality can be applied to multiple messages.

In order to view pending or failed requests, it is possible to search for these states via the **Search** drop-down list. Possible action states are as follows:

- Released
- Release-pending
- Release-failed

- Forwarded
- Forward-pending
- Forward-failed



Note

Actions can be performed only on messages that are in quarantine and have not been marked as deleted.

Action limitations

You cannot request a new forward action on a specific message until the previous forward action has completed. Similarly, you cannot request a release action for a specific message until the previous release action has completed.

In order to check for successful completion of an action, you must perform a fresh search.

Message actions page

A **Message Actions** page displays the actions applied to an individual message. This is accessed by clicking the **Action** for a message on the **Message Center Results** screen.

The Message Actions screen shows general information about the message and details of actions that have been applied to the message and the order in which they were applied.

Viewing message details

Click a message subject to view details for that message.

This page explains why a quarantined message was blocked or if a message was classified as commercial bulk email and includes the message headers, message text, and details of any attachments. If the message has been analyzed by the File Sandbox and found to be suspicious, the page includes a link to the File Sandbox report. From this page you can perform the actions described in *Performing actions on the results*.

To download the quarantined message, click **Download Message**. (Administrators must have the View Quarantine policy permission to download quarantined messages.)



Important

Quarantined messages may contain malicious content. Exercise caution when downloading and viewing message contents.

If you want to release or forward a message from this page, clicking **Release** or **Forward to** sends the message for any further processing before delivery. If you want to bypass any other processing rules that you have set up and deliver the message directly to its recipient, check the **No further processing** box before releasing or forwarding. We recommend that you review the message carefully before doing this.

For quarantined messages, you can also choose to allowlist or blocklist the sender's email address or domain. When you do this, the item in blocklist or allowlist becomes a per-user antispam policy within the email policy that applies to the intended message recipient. For more information, see *Antispam exceptions*.

Related concepts[Performing actions on the results](#) on page 149[Antispam exceptions](#) on page 99

Viewing logs

Click **View log** to see full details of the message processing and results. The log appears at the bottom of the message details page.

For a quarantined message, the log details provide the exact reasons for the quarantine. For example:

- For messages quarantined due to a virus, the log lists the virus name.
- For blocked attachments, the log includes the file type or class that matched against the attachment.
- For blocked images, the log includes a thumbnail of the image. See *Managing quarantined images*.
- For lexical rule failures, the log lists the phrase that triggered the quarantine.
- For spoofed messages, the log details the outcome of the spoofing detection checks used to validate the message. The log entry may include the following items:
 - DMARC: pass or fail, based on DKIM and SPF checks
 - DKIM: checks the digital signature of the sender's domain
 - SPF: checks the SPF record for the envelope sender address
 - SPF_HELO: checks the SPF record for the SMTP HELO name
 - SPF_P2: checks the SPF record for the content sender ("from") address.

If email is classified as commercial bulk email, the message details page may also contain log lines indicating the action taken:

- Commercial bulk message subject tag added for <recipient>.
- Commercial bulk message quarantined for <recipient>.
- Commercial bulk message detected and allowed due to policy settings for <recipient>.

**Note**

You cannot view logs for discarded messages.

Related concepts[Managing quarantined images](#) on page 152

Managing quarantined images

**Note**

You must have the Email Security Image Analysis Module to use this feature.

If a message has been quarantined due to an inappropriate image attachment, a thumbnail of the image appears under Blocked Images at the end of the message log details. Note that you must have the “View Quarantine Images” permission to access these images.

If you consider a quarantined image to be acceptable, you can add it to the image allowlist by clicking **Add to allow list** under the thumbnail. If the image is already in the allowlist and you wish to remove it, click **Remove from allow list**.



Note

We recommend that you only add images to the allowlist that are likely to cause the repeated quarantining of messages.

The image allowlist can contain a maximum of 200 images; if you have already reached this limit, the **Add to allow list** option is greyed out.

For more information on the image allowlist, see *Image allowlist*.

Related tasks

[Image allowlist](#) on page 69

End-User Self Service

Contents

- Introduction on page 155
- Requesting a message report on page 155
- Understanding the report on page 157
- Accessing quarantined email on page 159
- Changing subscription details on page 160
- Consolidating email report data on page 162

Introduction

Forcepoint Email Security Cloud allows end users to review personal lists of suspicious and clean email based on criteria that the user chooses, see details about each message, and decide whether to release a message, allowlist it, or blocklist it. The service does this by providing a personal email report. As an administrator, you can configure what the report contains, how it is sorted, and whether or not you want end users to be able to customize certain aspects of the report. You also specify the default language, time zone, and schedule for the report. This is all done by clicking **Email > Messages > Personal Email Subscriptions**. (See *Personal Email Subscriptions* for specifics.)

You can choose to subscribe your end users to the personal email report via the cloud portal. In this case, users receive a single report in the format that you configure as described above, and the report contains a link that a user must click to receive the report on a weekly basis.

Otherwise, end users are not set up to receive the message report by default. To receive a personal email report, users must request it from a cloud service website. The *Forcepoint Email Security Cloud End User's Guide* and the *Forcepoint Email Security Cloud End User's Quick Start Guide* provide instructions for your users.

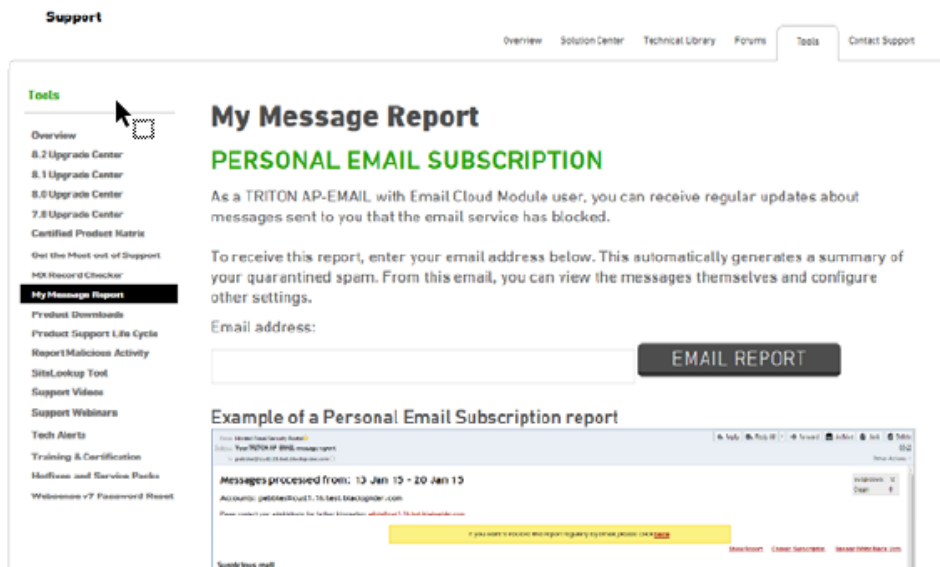
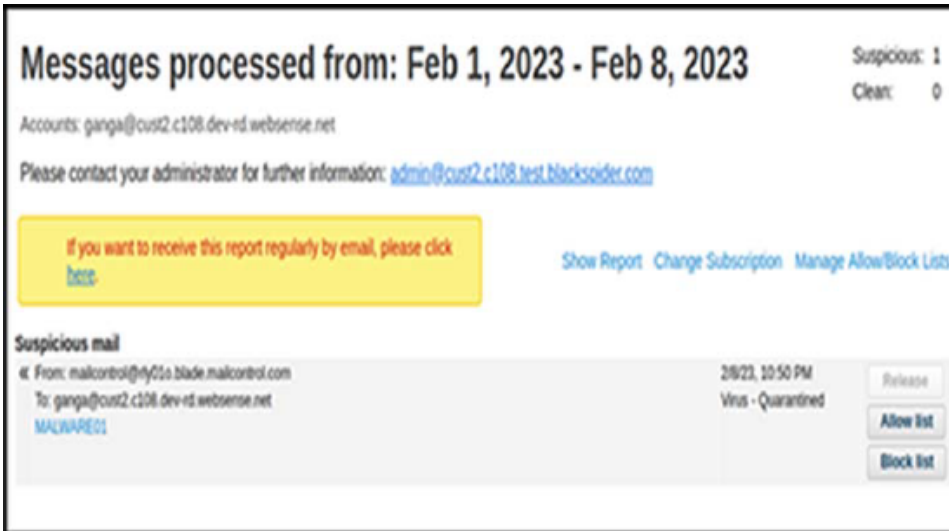
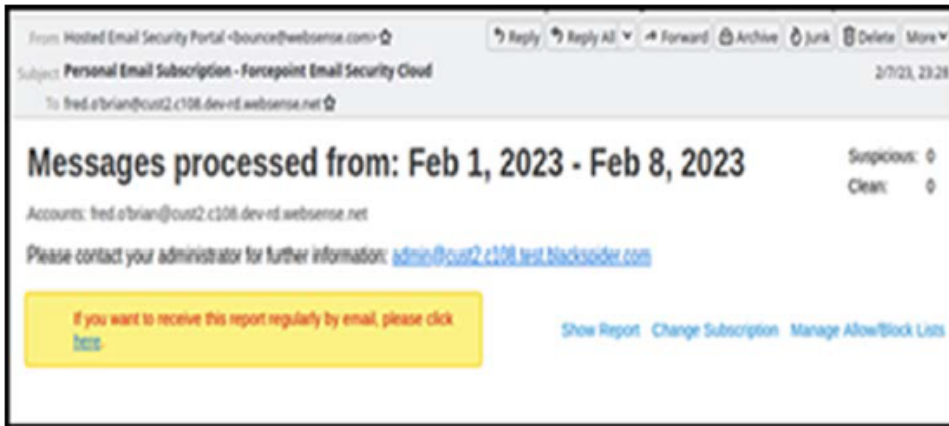
Related concepts

[Personal Email Subscriptions](#) on page 56

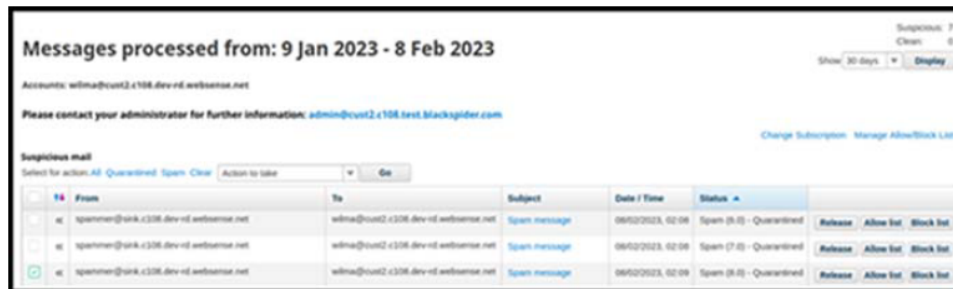
Requesting a message report

Users can request a personal email report by going to the following website and entering their email address.

www.websense.com/content/messagereport.aspxThe report is emailed to the email address entered. This normally takes no longer than a few seconds depending on the amount of data included.



Understanding the report



Information included on the personal email report

Section	Contents
A	The date range for which the report was processed
B	Your email address. Note that if you have consolidated message report data from multiple email accounts into one report, you will see all the email addresses included in that subscription.
C	The number of suspicious and clean messages that were processed for you during the period
D	An option to change the number of days shown in the report
E	A link to receive this report by email on a regular basis
F	The ability to select all quarantined and/or spam message and take actions on them, such as delete or release
G	A link to change your report subscription
H	A link to manage your personal allowlist and blocklist
I	<p>A list of your email arranged in the following order (list depends on user and account configuration):</p> <ul style="list-style-type: none"> ■ Suspicious messages you received or sent ■ Clean messages you received or sent <p>If you are viewing the online version of your report, you can change the order of the messages by clicking a column heading link. For example, you can sort by the From or To column, the Date/Time column, or the Status column.</p>

Section	Contents
J	An indication of whether a message has been received or sent.
K	<p>The actions you can take action on a message. (Select a message by clicking in the check box on the left.) Options include:</p> <ul style="list-style-type: none"> ■ Details - Access details about the message ■ Release - Release the message from quarantine. (Inbound messages only. This is not possible for all messages, such as those containing known viruses.) If the message to be released was originally sent to a distribution list address that is included in a consolidated report, you are given the option to release the message to the whole list or a specific email address. ■ Allowlist - Send this message or domain to your personal allowlist. This tells the cloud-based service to always allow messages from this sender or domain. ■ Blocklist - Send this message or domain to your personal blocklist. This tells the cloud-based service to never allow messages from this sender or domain.

Information included on the message summary line

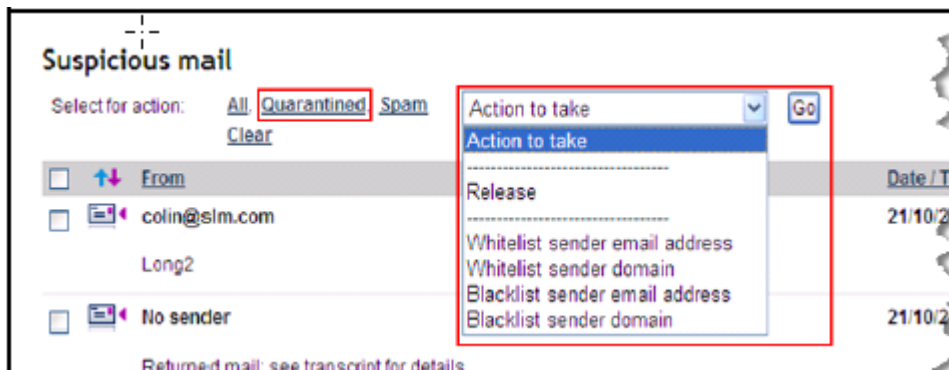
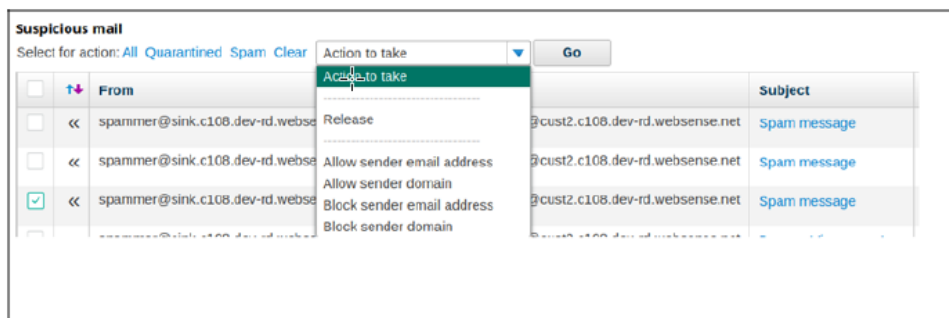
Information included on the message summary section:

- An indication of whether the message was inbound or outbound
- The message sender
- The message recipient
- The time and date that Forcepoint Email Security Cloud logged the email
- The status of the email - what action Forcepoint Email Security Cloud took on the email
- The subject line of the message

Default information included

The first time a user requests a personal email report, it contains a maximum of 50 lines and covers the period of the last 7 days.

When looking at the online version of their report, users can take action on all of the messages in their quarantine at once. To do so, they click **Quarantined**, then select an action to take from the drop-down list.



If, in the report, the user clicks a link to a message that was accepted, only the message log entries are shown, because the message is no longer available to Forcepoint Email Security Cloud.

Changing subscription details

If you have selected the **Allow end users to modify report content** option when setting up your Personal Email Subscriptions, end users can configure the system to send themselves message reports at any time interval. To define subscription details, they click the link **Change Subscription**.

Change Subscription

Manage Accounts

Add or remove addresses to your message report

jcuevas2@cust2.com

After you save changes, the owner is emailed and asked to approve the subscription request.

Report Options:

Reporting period:

Frequency sent:

Maximum length:

Email types to include:

- Quarantined email received
- Quarantined email sent
- Non-quarantined email received
- Non-quarantined email sent
- Clean email received
- Clean email sent

Sort by: in order
Applies to quarantined and non-quarantined messages only.

Timezone:

Language:

On the **Change Subscription** screen, users can specify the following subscription:

- **Manage Accounts**
Do they want to consolidate the report data for multiple aliases or email accounts into one report? (See *Consolidating email report data*).
- **Report Options**
 - What time period do they want reported: the last 1, 2, 7, 14, or 30 days?
 - How often should the report be delivered: daily, weekdays, weekly, biweekly, or monthly?
 - How many rows do they want on each page in the report: 20, 50, 100, 200, or 500?
 - What sections do they want included in the report: quarantined suspicious messages received or sent, non-quarantined suspicious messages received or sent, clean messages received or sent?
 - In what order do they want the information about quarantined and non-quarantined messages to appear: status, date/time, subject, from, or to? Ascending or descending?



Note

Subscriptions to the message report lapse after 93 days. 62 days after subscribing, each time users receive a report, they are reminded that they should renew their subscription.

- What time zone should the report assume?
- In what language do they want the report delivered? 14 languages are supported:
 - Czech
 - Dutch
 - English (U.K. and U.S.)
 - French
 - German

- Greek
- Italian
- Polish
- Portuguese (Brazilian)
- Romanian
- Slovak
- Spanish
- Swedish

Regardless of the settings for the scheduled report, users can request a report by following the process outlined in *Requesting a message report*.

Related concepts

[Consolidating email report data](#) on page 162

[Requesting a message report](#) on page 155

Consolidating email report data

End users who are allowed to modify settings in their personal email report can consolidate data from their other email accounts or aliases into one report. They can also consolidate another person's email addresses, such as an assistant consolidating a manager's addresses into one report. Reviewing and managing one report versus several reports may help save time.

Note that if LDAP synchronization is enabled for the account, all aliases associated with an end user will be automatically listed on the Change Subscription screen under Manage subscription addresses. The end user can then add one or more of them into one consolidated report.

End users who want to consolidate addresses can do the following:

- From the personal email report, click **Change Subscription**.
- Under **Manage Accounts**, check the box for the email address or addresses to be added if a list is given, or enter the email address. The address must be from one of the domains owned by your company. For example, company xyz might have these domains: xyz.com, xyz.co.uk, or xyz.com.au.
- Click **Add Address**.
- To add a new email address, the end user must receive approval from the owner of that address. Clicking **Add Address** sends an email request for approval to the address owner. Until the owner approves the request, the email is marked "pending approval by owner." If the owner approves the request, the requestor is notified by email and the "pending" status is removed. The owner may choose to decline the request in which case the user may not add the email address to their personal email report.
- To remove an address from the report, clear the check box next to the email address that they want to remove. Clearing the box reveals a "Remove" link. End users who click on this link are asked to confirm they want to remove the address.

Note that after they have created a consolidated personal email report, end users who then order a message report, or are set up to automatically receive a report, receive the consolidated report. If the end user wishes to receive reports from more than one subscription (for example, an individual and a consolidated subscription), you, the administrator, must create these subscriptions in the cloud portal portal.

Email Reporting Tools

Contents

- [Introduction](#) on page 163
- [Email Report Center](#) on page 163
- [Legacy Email Reporting](#) on page 174

Introduction

Email protection reporting provides many tools for profiling and investigating email security and usage. On the toolbar, select **Reporting** to see all available reporting options.

Reporting allows you to:

- Monitor service performance
- Monitor traffic volumes and patterns for capacity planning purposes
- Enforce your email acceptable use policy
- Isolate and resolve problems

Reporting tools include:

- The **Email Dashboard charts** provide threat, risk, usage, and system information. For most charts, the time period, chart style, and set of results shown can be customized. You can also select columns or sections on a chart to drill down to the relevant report in the Report Builder.
- The **Report Center** menu—Report Catalog, Report Builder, Message Details, and Scheduler—offers a set of predefined reports, the ability to create custom reports, a method for digging into message details, and a facility for report scheduling.
- The **Legacy Email Reports** menu includes reports that were available before Report Center was released, and remain available to support existing customers. This section allows you to generate a set of standard reports, organized by Address, Content, Inbound, Outbound, Virus, Volumes, and Spam. See *Legacy Email Reporting*.

Related concepts

[Legacy Email Reporting](#) on page 174

Email Report Center

The **Report Catalog** contains a number of predefined reports that cover common scenarios, available in bar chart, trend chart, and tabular formats. You can copy any predefined report to apply your own filters to create a custom report, and share your reports with other administrators. See *Using the Report Catalog*.

Use **Report Builder** to create multi-level, flexible reports that allow you to analyze information from different perspectives and gain insight into your organization's email message trends. If a high-level summary shows areas of potential concern, you can drill down to find more details. See *Using the Report Builder*.

Related concepts

[Using the Report Catalog](#) on page 192

[Using the Report Builder](#) on page 199

Viewing detailed reports

You can use Report Builder reports as a starting point for accessing more detailed information about email activity, either by drilling down into a particular aspect of a report, or by using the Message Details option to see further information about a report item.

Drilling into report items

To drill down into a report item:

Steps

- 1) Mark the check box next to each item for which you want more information.
You can select multiple items and change your selections, even after the pop-up window appears.
- 2) In the pop-up window, select an available attribute from the Drill Into By the drop- down list.
- 3) The new report loads. Note that as you have moved down a level in the report, the items you selected in step 1 are now in the Filters field, while the Grouping field contains the other report attributes, including the one you selected in step 2.
You can edit the content of the Grouping and Filters fields, and view the report in different formats, in exactly the same way as for the previous report.
- 4) To drill down a further level, repeat steps 1-3 above.

Using Message Details

The Message Details view is available for report items at all levels. To see the details for one or more report items:

Steps

- 1) Mark the check box next to each item you wish to view.
You can select multiple items and change your selections, even after the pop-up window appears.
- 2) In the pop-up window, select **View Transactions**.
The Report Center Message Details page loads, listing details for each message within the report items you selected.

Next steps

In the Message Details page, you can:

- Edit the filters and date range for the messages you wish to see.
- Select the columns to display from the **Columns** drop-down. Click **Done** when you have made your selections.
- Click a column heading to make it the active column for sorting transactions. Click again to switch between ascending and descending order.
- Delete columns by clicking the X icon in a column heading. Note that you cannot delete the current active column.
- Drag metrics from the left-hand pane into the Filters field.
- Enable Detail View to see more detail for the selected message. The Message Details pane opens at the bottom of the page, and displays the timestamp, sender address, recipient address, direction, action, and filtering reason of the message.
- Export message details to PDF or CSV format. Either select one or more messages and then click **Export to PDF** or **Export to CSV** in the pop-up window that is displayed, or click the PDF or CSV icon in the top right to export all messages on the page.

Email report attributes


Below is a list of available report attributes.

Name	Description	Filter values
Direction	The direction of the message: inbound or outbound.	Check boxes
Envelope Sender	Used by mail servers to check where the message originates and where to respond (for example, if there is an error or the message bounces). Often matches the From: address, but not always. For example, the message might come from a mailing list, or from an organization authenticated to send messages on your company's behalf.	Manual text
From: Address	The address the message recipient sees in the From: field of the message.	Manual text
Policy	The email policy used for filtering.	Autocompleted text
Recipient Address	The email address of a message recipient.	Manual text
Recipient Domain	The domain associated with a message recipient.	Manual text
Sender Domain	The domain associated with a message sender.	Manual text

Name	Description	Filter values
Sender Name	The name of a message sender.	Manual text
Subject	The text in the subject line of a message. There are also options to filter by results with no subject, and to perform a case- sensitive search.	Manual text
Action	The action applied to the message. Options are Accepted, Bounced, Bypassed processing, Discarded, Quarantined, Temporarily bounced.	Check boxes
Blocklist/Allowlist	Groups and filters messages by whether they are in blocklist, allowlist, or neither.	Check boxes
Blocked Attachment Ext	Groups and filters messages by the extension of their blocked attachments (for example, EXE). There is also an option to include results with no blocked attachment extension.	Manual text

Name	Description	Filter values
Filtering Reason	<p>The result of filtering the message.</p> <ul style="list-style-type: none"> ■ Blocked attachment – Message quarantined due to attachment filename extension. ■ Blocked attachment type – Message quarantined due to the actual attachment file type. ■ Clean – No threats detected. No rule or policy violations. No analysis failures or errors. ■ Custom rule – Message triggered a rule that applies to select accounts. ■ Encrypted content/message – Message encrypted or message body included encrypted content. ■ Exceeds size limit – Message exceeded the size limit. ■ Format problem – Message body failed structural analysis. ■ Global rule – Message triggered an operational rule. ■ Inappropriate image – Message contained an inappropriate image. ■ Lexical rule violation – Message content triggered a lexical rule. ■ Malicious macro – Message contained a malicious macro. ■ Masked attachment extension – Message attachment filename extension was masked. ■ Message parked – Message parked for secure download. ■ Other – Unspecified or unknown filtering reason. ■ Phishing – Message included phishing content. ■ Spam – Message determined to be spam. ■ Spoofed – Message failed internal domain spoofing checks. ■ Spoofed-External – Message failed DMARC validation. 	Check boxes

Name	Description	Filter values
	<ul style="list-style-type: none"> ■ Spoofed-Targeted – Message failed the Internal Executive Spoofing check. ■ System error – Message processing error. ■ Threatseeker issue – ThreatSeeker Intelligence detected suspicious content. ■ TLS requirements not met – TLS connection required; the MTA did not offer it. ■ Virus – Message contained a virus. 	
Lexical Rule	The lexical rule applied to a message. There is also an option to include results with no lexical rules applied.	Manual text
Sender IP	The IP address of a message sender. There is also an option to include results with no sender IP address.	Manual text
Sender IP Country	The country from which the sender IP address originates.	Autocompleted text
Attachment File Type	A description of the type of file attached to a message - for example Microsoft Excel or Portable Network Graphic (PNG).	Autocompleted text
Attachment Filename	The name of a specific file attached to a message.	Manual text
Attachment MIME Type	MIME type of a message attachment in the format content type/content subtype. For example, video/mpeg or text/csv.	Manual text
Content Type	The type of content detected within the message. Options are Archive, Audio, Encrypted, Executable, HTML, Image, None, Office Document, Signed, Video.	Check boxes
Emb. Domain	The domain of an embedded URL within a message.	Manual text
Emb. Full URL	The full URL embedded within a message.	Manual text
Emb. Host	The host name embedded within a message.	Manual text

Name	Description	Filter values
Emb. URL Category	The category of a URL embedded within a message.	Autocompleted text
Emb. URL Risk Class	The risk class associated with a URL embedded within a message.	Check boxes
Emb. URL Severity	The severity level associated with a URL embedded within a message.	Check boxes
Advanced Encryption	The type of advanced encryption applied to the message. Options are Decrypted Inbound, Encrypted Outbound, or None. This attribute requires the Forcepoint Email Security Encryption Module.	Check boxes
File Sandbox Status	<p>The result of analysis of files attached to messages that were sent to the File Sandbox. Status can be:</p> <ul style="list-style-type: none"> ■ No threat detected – Sandbox analysis did not detect any malicious behavior. ■ Malicious – Sandbox analysis detected potentially damaging, malicious behavior. ■ Pending analysis – The file has been submitted to the sandbox and is queued for analysis. <p>The report includes date/time, sender, recipient address, Subject, and status.</p> <p>This attribute requires the Forcepoint Advanced Malware Detection for Email module.</p> <div data-bbox="630 1402 1042 1604" style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Note</p> <p>A secondary grouping is not allowed when File Sandbox Status is the primary grouping.</p> </div>	Check boxes
Message Sandboxing	The type of sandboxing applied to the message. Options are Attachment Wrapped, None, Phishing URL Sandboxed, URL Sandboxed. This attribute requires the Advanced Malware Detection for Email module.	Check boxes

Name	Description	Filter values
Virus Name	The name of a virus detected in a message. There is also an option to include results with no virus name associated with them.	Manual text
Date	Enables you to group report entries by date. Note that this attribute is not available for filtering as the Date Range field performs this function.	N/A
Day of Week	Enables you to group and filter report entries by days of the week.	Check boxes
Hour	Enables you to group and filter report entries by hour.	24 hour selection
Month	Enables you to group and filter report entries by month.	Check boxes

Email report metrics

The table below lists the report metrics that can be added to Report Builder and Message Center reports.

Metric Name	Description
Message Size	
Filtering Time	The time in milliseconds to process the message.
Spam Score	
Attachment Size	The size of each file attachment, in bytes.

Email predefined reports

Below is a list of predefined reports.

Related reference

- [Advanced reports](#) on page 171
- [Email Activity reports](#) on page 171
- [Lexical Rules reports](#) on page 172
- [Message Size reports](#) on page 172
- [Security reports](#) on page 172
- [Spam reports](#) on page 173
- [TLS reports](#) on page 173

Advanced reports

Report Name	Description
Message Analysis Delay	The time taken in rounded-up seconds to process and analyze messages.
Unprocessed Message Statistics	Details of messages discarded due to access control rules in the last 7 days.

Email Activity reports

Report Name	Description
Full Message Statistics	Total number of inbound and outbound email messages processed in the last 7 days.
Inbound Email Statistics	Total number of inbound messages in the last 7 days.
Outbound Email Statistics	Total number of outbound messages in the last 7 days.
Outbound Senders	Email addresses of users sending messages from your mail servers in the last 7 days.
Top Inbound Policies	Policies containing users receiving the most messages in the last 7 days.
Top Inbound Receiving Domains	Domains in your account receiving the most messages in the last 7 days.
Top Inbound Recipients	Most frequent recipients of inbound messages in the last 7 days.
Top Inbound Senders	Most frequent senders of inbound messages in the last 7 days.
Top Inbound Sending Domains	Domains sending the most inbound messages to your account in the last 7 days.
Top Inbound Sources	Most frequent source IP addresses of inbound messages in the last 7 days.
Top Outbound Policies	Policies containing users sending the most messages in the last 7 days.
Top Outbound Receiving Domains	Domains receiving the most messages from your account in the last 7 days.
Top Outbound Recipients	Most frequent recipients of outbound messages in the last 7 days.
Top Outbound Senders	Most frequent senders of outbound messages in the last 7 days.
Top Outbound Sending Domains	Domains in your account sending the most outbound messages in the last 7 days.
Top Recipients	Most frequent recipients of messages, both inbound and outbound, in the last 7 days.

Report Name	Description
Top Senders	Most frequent senders of messages, both inbound and outbound, in the last 7 days.

Lexical Rules reports

Report Name	Description
Most Matched Lexical Rules	The top 10 lexical rules matched in the last 7 days.
Top Recipients for Lexical Rule Blocks	Recipients of messages most frequently blocked by lexical rules in the last 7 days.
Top Senders for Lexical Rule Blocks	Senders of messages most frequently blocked by lexical rules in the last 7 days.

Message Size reports

Report Name	Description
Large Messages	Details of the largest messages processed through the service in the last 7 days.
Total Message Size	Total size of all messages processed for your account in the last 7 days.

Security reports

Report Name	Description
Detailed File Sandboxing Report	<p>Details of analysis performed on files attached to messages that were sent to the File Sandbox in the last 7 days. Report includes date/time, sender, recipient address, Subject, and result of analysis (Status). Status can be:</p> <ul style="list-style-type: none"> ■ No threat detected – Sandbox analysis did not detect any malicious behavior. ■ Malicious – Sandbox analysis detected potentially damaging, malicious behavior. ■ Pending analysis – The file has been submitted to the sandbox and is queued for analysis. <p>This report is available to subscribers of the Advanced Malware Detection for Email module.</p>
Emails Containing Viruses	Messages containing viruses detected in the last 7 days, using all techniques including ThreatSeeker Intelligence.
Inbound Virus Percentage	Percentage of inbound messages containing viruses in the last 7 days.

Report Name	Description
Outbound Virus Percentage	Percentage of outbound messages containing viruses in the last 7 days.
Sandboxed URLs	Messages containing URLs that were sandboxed in the last 7 days.
Summary of File Sandboxing Results by Status	<p>Summary of File Sandboxing by number of messages processed for each Status in the last 7 days. Status can be:</p> <ul style="list-style-type: none"> ■ No threat detected – Sandbox analysis did not detect any malicious behavior. ■ Malicious – Sandbox analysis detected potentially damaging, malicious behavior. ■ Pending analysis – The file has been submitted to the sandbox and is queued for analysis. <p>This report is available to subscribers of the Advanced Malware Detection for Email module.</p>
Top Inbound Virus Sources	Most frequently-seen domains for inbound viruses in the last 7 days.
Top Virus Sources	Common source domains of viruses in the last 7 days.
Top Viruses	Top 20 most commonly-detected viruses in the last 7 days.

Spam reports

Report Name	Description
Inbound Commercial Bulk Email Statistics	Details of inbound messages detected as commercial bulk email in the last 7 days.
Inbound Spam Percentage	Percentage of inbound messages detected as spam in the last 7 days.
Inbound Spam Statistics	Details of inbound messages detected as spam in the last 7 days.
Outbound Spam Percentage	Percentage of outbound messages detected as spam in the last 7 days.
Outbound Spam Statistics	Details of outbound messages detected as spam in the last 7 days.

TLS reports

Report Name	Description
Mandatory TLS Delivery Failures	Details of messages in the last 7 days that could not be delivered because a TLS connection was not available.

Legacy Email Reporting

The Legacy Email Reporting menu provides reports that were available before the Report Center was released, and remain available to support existing customers. Use this menu to generate a set of standard reports organized by Address, Content, Inbound, Outbound, Virus, Volumes, and Spam. These reports can be generated using a range of filters, and can be downloaded as PDF or XLS files.

To access legacy email reporting features, go to **Reporting > Legacy Email Reports**.

For more information on these reports, refer to *Categorized reports*. To see what a specific email report contains, see *Email report list*.

All reports are generated in real time. Most include charts and tables that are presented in an easy to read, printable format.



Note

For larger accounts, where a lot of data is to be retrieved, the reports may take some time to generate. As soon as the relevant data has been retrieved it is displayed while the remainder of the report is being compiled.

Commonly-used report criteria can be saved for easy access. For more information, see *Saving reports*. Saved reports can be scheduled for regular delivery to one or more recipients as described in *Scheduling categorized reports*.

Related concepts

[Email report list](#) on page 178

Related tasks

[Categorized reports](#) on page 175

[Saving reports](#) on page 176

[Scheduling categorized reports](#) on page 177

Reporting periods

Reports can be generated for periods of hours to years. When accessing a report, you can drill down from within the report to a shorter time period. For example, an email volumes report for 7 days returns a table of volumes by day and a corresponding bar chart. By clicking a link on the relevant day on the table or chart, the report drills down and provides an hourly table and chart for that day. This allows not only the creation of management reports, but also reactive tracking of day-to-day issues.

You can select the reporting period from the drop-down list or you can click **more** to select absolute From and To dates and times. The available dates and times are dependent on the type of report and the availability of the data.

Downloading report results

On each report, you have the option to download the data as a PDF or CSV file.

**Note**

You can also download charts as image files or in PDF format. To download a chart, right-click the chart and select the format to download (PDF, PNG, or JPEG).

Downloading a CSV file

You can download the statistics for the majority of reports as a comma-separated values (CSV) file. This allows you to import it into a third-party application, such as Microsoft Excel, for viewing and manipulation. On each table of results, click **Download CSV** to begin the download.

**Note**

For some email reports, the totals in the CSV file might be higher than the totals in the report on screen. This is because the generated reports contain 1 line per email message, whereas the CSV version contains 1 line per recipient which means that a single email message might appear several times.

Downloading a PDF file

Report results can be output to Portable Document Format (PDF) for easy distribution or printing. The PDF report is generated by clicking the **Download PDF** button on a table of results.

Categorized reports

To access an email report:

Steps

- 1) Go to **Reporting > Email Reporting**.
- 2) Select a report category from the navigation pane.
- 3) Select a report from the **Show** drop-down list. The reports you see depend on your subscriptions.

Next steps

Initially you can access only the **Selection** tab to enter selection criteria. Once you have generated a report, you can click the **Chart** and **Table** tabs to view the results in chart or table form.

For most reports, you can select filtering criteria that restricts the report results. Next to each of the filtering criteria is a note describing in more detail how to use that option.

**Note**

If your account is enabled for filtered reporting, you may only be able to view reports that filter on certain policies. See *Configuring permissions*.

When you select a report, you are shown a list of the time periods for which the report is available. Alternatively you can select a specific time period (from and to) for the report by clicking **more** next to the period list.

To make selection from some criteria lists easier, you can expand the list to appear in a larger window by repeatedly clicking on the **Grow list** link.

Once you have decided on the report and the appropriate criteria, click **Generate report**. You may receive feedback at this point advising that the report might take some time to generate. Typically this is due to the amount of data that must be searched. You can often avoid this by adding more criteria to narrow the search. Click **Back** if you want to cancel the report.

Related tasks

[Configuring permissions](#) on page 18

Report results

Most report results are displayed in chart and table format in the relevant screen. Note that not all reports are available in both formats.

Drilling down

Many of the reports contain links to more detailed reports. For example, for time-based reports, clicking the chart column or data table entry for a day generally displays the hourly report for that day, using any filtering criteria that applied to the original report.

Some reports allow you to drill down into the data in a more flexible way. If this is the case, there is a drop-down list above the chart and data table listing the available views. Select the view required from the list and then click the chart or table to display the new report.

Saving reports

You can choose to save any categorized report. Use this option to identify the reports you generate most frequently and want to be able to locate quickly.

To see the list of reports that you have saved, select **Reporting > Account Reports > Saved Reports**.

To save a report:

Steps

- 1) Select the email report you want.
- 2) Use the **Selection** screen to enter your report criteria as described in *Categorized reports*.
- 3) Click **Save report**.
- 4) Enter a name for the report, and click **Save**.
The Saved Reports list is displayed, and the report you entered is now listed.

Next steps

As well as accessing the report from this screen, you now have the option to delete the saved report or schedule it for regular delivery.

Related tasks[Categorized reports](#) on page 175

Scheduling categorized reports

You can run reports as they are needed, or you can define a schedule for running one or more saved reports.

Reports generated by scheduled jobs are distributed to one or more recipients via email. The reports can be in HTML, PDF, or CSV format. There is a limit on the number of reports you can schedule for delivery: the Saved Reports list displays the remaining number you can schedule in addition to any existing deliveries.

**Note**

You cannot schedule reports that have defined start and end dates, or that span periods of less than 24 hours.

To schedule a report:

Steps

- 1) Select **Reporting > Account Reports > Saved Reports**.
- 2) You can schedule an existing saved report by clicking the report you want to schedule on the Saved Reports list. If you do this, skip to step 5 below.
Otherwise, to create a new report for scheduling, click the **Generate a new report** link. The page that appears includes only reports that are eligible for scheduling.
- 3) Create and save your report as described in *Saving reports*.
- 4) On the Saved Reports list, click the name of your new report.
- 5) Click **Schedule email report**.
- 6) Enter the email address of the report recipient. Multiple email addresses should be separated by commas or spaces.
If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.
- 7) Enter a subject for the report email, and the text you want to appear in the body of the email.
- 8) Select the report format.

9) Set one of the following delivery periods for your reports:

- daily
- weekdays
- weekly
- every other week (biweekly)
- monthly (the default option)

If you want to stop the a scheduled report temporarily, select **suspend delivery**.

10) Click **Save**.

You are returned to the Saved Reports list. Reports that have been scheduled display the recipient list in the **Email to** column. Click an item in this column to open the schedule, where you have the option to edit or delete the report delivery.

Related tasks

[Saving reports on page 176](#)

Email report list

The tables below show the email reports that are available. Note that some reports appear in more than one report category.



Note

You may not see all of the reports listed here, depending on the features enabled in your account.

Related reference

[Address reports on page 179](#)

[Content reports on page 181](#)

[Inbound reports on page 182](#)

[Outbound reports on page 182](#)

[Spam reports on page 184](#)

[Virus reports on page 185](#)

[Volume reports on page 187](#)

Address reports

Report	Available Periods	Formats	Description
Outbound Senders	Daily	Table CSV Link PDF Link	Senders of email originating from your mail servers. Note that this can include senders of email that was auto-forwarded by your mail system and was originally from outside your organization.
Top Sources of Viruses	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses by volume of inbound viruses.
Top Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of messages regardless of direction
Top Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of messages regardless of direction
Top Inbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of inbound messages
Top Inbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of inbound messages
Top Inbound Sources	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequent source IP addresses by volume of inbound messages

Report	Available Periods	Formats	Description
Top Outbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of outbound messages
Top Outbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of outbound messages
Top Transit Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of messages that were sent to and from the service
Top Transit Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent senders by volume of messages that were sent to and from the service
Top Spamtraps	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequently used spamtraps
Top Senders to Spamtraps	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequent senders by volume of messages sent to spamtraps
Top Sources to Spamtraps	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses by volume of messages sent to spamtraps
Top Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for recipients
Top Senders blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for senders

Report	Available Periods	Formats	Description
Top Sender/ Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for pairs of senders and recipients

Content reports

Report	Available Periods	Formats	Description
Most Frequent Lexical Rules	Hourly Daily	Chart Table CSV Link PDF Link	The lexical rules that most frequently matched
Top Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for recipients
Top Senders blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for senders
Top Sender/ Recipients blocked by Lexical Rule	Hourly Daily	Table CSV Link PDF Link	The most frequent lexical rule violations for pairs of senders and recipients
Parked Attachments	Minutes Hourly Daily	Table CSV Link PDF Link	Lists email messages that had attachments parked
Parked Attachments Summary	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Summarizes parked attachments over specified period
Lexical Analysis Failure Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of email messages failing lexical analysis
Inbound Lexical Analysis Failure Volumes	Minutes Hourly Daily	Chart Table CSV Link	The total number of inbound email messages failing lexical analysis

Report	Available Periods	Formats	Description
	Monthly	PDF Link	
Outbound Lexical Analysis Failure Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound email messages failing lexical analysis

Inbound reports

Report	Available Periods	Formats	Description
Inbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of inbound messages
Top Inbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of inbound messages
Top Inbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of inbound messages
Top Inbound Sources	Minutes Hourly	Chart Table CSV Link PDF Link	The most frequent source IP addresses by volume of inbound messages

Outbound reports

Report	Available Periods	Formats	Description
Outbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of outbound messages

Report	Available Periods	Formats	Description
Outbound Senders	Daily	Table CSV Link PDF Link	Senders of email originating from your mail servers. Note that this can include senders of email that was auto-forwarded by your mail system and was originally from outside your organization.
Top Outbound Recipients	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent recipients by volume of outbound messages
Top Outbound Senders	Minutes Hourly Daily	Chart Table CSV Link PDF Link	The most frequent originators by volume of outbound messages
Encrypted Messages	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of encrypted messages sent in the selected time period
Encrypted Messages by Domain	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most popular domains for sending encrypted messages in the selected time period
Encrypted Messages by Policy	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most used policies for sending encrypted messages in the selected time period
Encrypted Messages by Encryption Rule	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most frequently-used encryption rules for sending encrypted messages in the selected time period
Opportunistic TLS	Hourly Daily	Chart Table CSV Link PDF Link	Shows the number of delivered messages that used, or did not use, opportunistic TLS

Spam reports

Report	Available Periods	Formats	Description
Inbound Spam Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound email messages detected as spam
Outbound Spam Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of outbound email messages detected as spam
Inbound Spam Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of inbound email detected as spam
Outbound Spam Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of outbound email detected as spam
Inbound Spam Bandwidth Saved	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Estimates the bandwidth saved for your company due to the filtering of inbound spam. The estimate is based on the number of inbound messages for your account in the selected time period, the approximate number of blocked messages for your account, and the average size of spam messages as calculated from the overall spam data for all Forcepoint Email Security Cloud accounts.
Spam False Positives and Negatives	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The number of false positives and false negatives generated during spam message processing.

Report	Available Periods	Formats	Description
Inbound Commercial Bulk Email Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound email messages detected as commercial bulk email
Top Spamtraps	Hourly	Chart Table CSV Link PDF Link	The most frequently used spamtraps
Top Senders to Spamtraps	Hourly	Chart Table CSV Link PDF Link	The most frequent senders, by volume, of email messages sent to spamtraps
Top Sources to Spamtraps	Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses associated with messages sent to spamtraps

Virus reports

Report	Available Periods	Formats	Description
Most Common Viruses	Hourly Daily Monthly	Chart Table List CSV Link PDF Link	The most commonly-detected viruses
Zero-day viruses caught by ThreatSeeker	Hourly Daily Monthly	Chart Table Text CSV Link PDF Link	Recent viruses caught by Forcepoint ThreatSeeker Intelligence before any virus signature updates within your account
Largest windows of exposure closed by ThreatSeeker	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Recent viruses caught by Forcepoint ThreatSeeker Intelligence by largest window of exposure in your account

Report	Available Periods	Formats	Description
Virus Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of email detected as containing viruses by all techniques including Forcepoint ThreatSeeker Intelligence
Inbound Virus Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of inbound email detected as containing viruses by all techniques including Forcepoint ThreatSeeker Intelligence.
Outbound Virus Percentage	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The percentage of outbound email detected as containing viruses by all techniques including Forcepoint ThreatSeeker Intelligence.
Top Sources of Viruses	Hourly	Chart Table CSV Link PDF Link	The most frequently seen IP addresses, by volume, associated with inbound viruses
Sandboxed URLs	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The number of messages containing sandboxed URLs.
Clicked Sandboxed URLs	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The number of times sandboxed links were clicked in messages, and the action the user took after clicking.
Targeted Phishing Attacks	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Phishing topics that are part of a targeted attack, directed multiple recipients, listed by number of recipients.
Top Phishing Attacks	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The most frequently seen phishing topics by number of recipients.

Report	Available Periods	Formats	Description
Top Repeat Phishing Victims	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The end users who have most frequently clicked a link in a phishing email.
Top Phishing Recipients	Hourly Daily Monthly	Table CSV Link PDF Link	The end users who have most frequently received phishing email messages.
Phishing Topic Details	Hourly Daily Monthly	Table CSV Link PDF Link	A list of phishing topics for specified recipients.
Phishing Recipient Details	Hourly Daily Monthly	Table CSV Link PDF Link	A list of recipients for specified phishing topics.

Volume reports

Report	Available Periods	Formats	Description
Total Messages	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of email processed (both inbound and outbound)
Total Message Size	Up to 12 hours	CSV Link PDF Link	How much mail in megabytes, has been processed or stopped by the service.
Inbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of inbound messages
Outbound Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of outbound messages

Report	Available Periods	Formats	Description
Transit Volumes	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total volume of messages in transit (both to and from your account, i.e., internal messages)
Unprocessed Message Volumes	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Messages discarded because of access control rules
Largest Messages	Minutes Hourly	Table CSV Link PDF Link	The largest messages
Message Size Distribution	Minutes Hourly	Chart Table CSV Link PDF Link	The distribution of message sizes
Top Inbound Policies	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The policies receiving the most mail
Top Outbound Policies	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The policies sending the most mail
Top Inbound Receiving Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains receiving the most mail from the Internet
Top Inbound Sending Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains sending the most mail from the Internet

Report	Available Periods	Formats	Description
Top Outbound Receiving Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains receiving the most mail from this account
Top Outbound Sending Domains	Minutes Hourly Daily Monthly	Chart Table CSV Link PDF Link	The domains sending the most mail to the Internet
Message Analysis Delay	Hourly	Chart Table CSV Link PDF Link	The time taken in seconds (rounded up) to analyze email, i.e., excluding any delivery attempts
Top Mandatory TLS Failures	Hourly Daily	Chart Table CSV Link PDF Link	The volume of email messages that failed to be delivered due to TLS being unavailable.
Top Mandatory TLS Domains	Hourly Daily	Chart Table CSV Link PDF Link	The volume of email messages sent using mandatory TLS.

Report Center

Contents

- [Introduction](#) on page 191
- [Using the Report Catalog](#) on page 192
- [Using the Report Builder](#) on page 199
- [Scheduling reports](#) on page 203
- [Exporting data to a third-party SIEM tool](#) on page 207

Introduction

Web and email cloud protection solutions include many tools for reporting on service activity and security events. For information specific to email reporting, see *Email Reporting Tools*. The following sections describe the Report Center.

Report Center features include:

- **Report Catalog** offers predefined reports. You can copy a predefined report to apply your own filters to create a custom report. See *Using the Report Catalog*.
- **Report Builder** supports the definition and creation of custom reports. See *Using the Report Builder*.
- **Scheduler** allows reports to be generated on a schedule that you define. Optionally, reports are sent to recipients that you specify. See *Scheduling reports*.
- The **Transaction Viewer** supports flexible, detailed display of web transactions and requests. See *Using the Transaction Viewer*.
- The email **Message Center** supports flexible, detailed display of email transactions. See *Viewing detailed reports*.

Related concepts

[Using the Report Catalog](#) on page 192

[Using the Report Builder](#) on page 199

[Scheduling reports](#) on page 203

[Viewing detailed reports](#) on page 202

Related information

[Email Reporting Tools](#) on page 163

Using the Report Catalog

Use the **Reporting > Report Center > Report Catalog** page to access predefined reports for common scenarios.

The Report Catalog includes the following elements:

- The **Toolbar**, at the top, contains buttons for returning to the previous page, creating new reports and folders, copying, sharing, and deleting items. Hover the mouse over a button to see a description of its function.
- The **folder list**, in the left-hand pane, contains the following top-level folders:
 - The **Favorites** folder enables you to easily locate your most frequently-used reports. You can mark a report or report folder as a favorite in the following ways:
 - Click the star to the left of the report or folder name in the Report Catalog. The star turns yellow when selected.
 - Click the star to the right of the report name in the Report Builder or Transaction View. You do not need to save your changes.

To remove a report from Favorites, click the star again to turn it gray.

When viewing the Favorites folder, note that you are essentially viewing a list of shortcuts to the reports. Choose **View in folder** from a favorite report's drop-down menu to see the report in its original folder.

- **My Reports** contains all of the reports and folders that you create.
- **Standard Reports** contains the predefined reports provided in the cloud service. If you have more than one service, separate subfolders contain the predefined reports for each service. For information about email protection predefined reports, see *Email predefined reports*.
- **Shared by Others** contains items that have been shared for use by all administrators in your account. Each folder has the user name of another administrator, and contains the reports shared by that administrator.

If a folder contains one or more subfolders, click the arrow to see those subfolders in the left-hand page. Click a folder name to see its contents in the right-hand pane.

- The table in the right-hand pane displays the contents of the folder you select in the folder list. This can be one or more subfolders, or a list of reports. To see a description of a particular report, hover the mouse over the report name. From this pane, you can perform actions on one or more reports and folders, such as copying, renaming, and deleting folders, or editing, running, or sharing a report. The actions available to you depend on the permissions configured. For example, you cannot delete reports in the Standard Reports folder. See *Managing reports* and *Managing folders*.
- The **Search** field, in the top right corner, enables you to search for specific words or phrases in report titles. Search results list the report name, its location, and if applicable, the report owner and the last time it was edited. You can manage a report directly from the search results list. For example you can run it, or if you have suitable permissions, share or delete it.

Related concepts

[Email predefined reports](#) on page 170

[Managing reports](#) on page 193

[Managing folders](#) on page 196

Managing reports

The Report Catalog offers the options to run, edit, share, copy, schedule, and delete reports. You can also access the Report Builder to create and save new reports.

The actions available to you depend on the permissions configured – for example, you cannot delete reports in the Standard Reports folder.

Select a link below for further instructions:

Related concepts

[Schedule a report on page 196](#)

Related tasks

[Run a report on page 193](#)

[Add a new report on page 193](#)

[Copy a report on page 194](#)

[Edit an existing report on page 194](#)

[Share a report on page 195](#)

[Delete a report on page 196](#)

Run a report

Steps

- 1) In the left-hand pane, navigate through the folder structure and select the subfolder containing the report you want. The reports appear in the table on the right of the screen.
- 2) Click the report you want to run. Alternatively, click the down arrow next to the report, and select **Run** from the menu.
- 3) The results are displayed in the Report Builder. See *Viewing report results* and *Viewing detailed reports*.

Related concepts

[Viewing report results on page 201](#)

[Viewing detailed reports on page 202](#)

Add a new report

Steps

- 1) In the toolbar, click the **New Report** button, and select whether you want to use the Report Builder or Transaction View.

- 2) Define attributes (for a grouped report), filters, and date ranges for your report as described in *Creating a report*.
- 3) To save your new report to the Report Catalog, click the **Save** button in the toolbar.
- 4) Enter a name and optionally a description for the report. The name can be a maximum of 200 characters, and the description a maximum of 400 characters.
- 5) Select the folder to store the report in. By default this is the My Reports folder; if you have created subfolders, you can use the **Folder** drop-down to choose one of those.
- 6) Click **Save Report**.

Related tasks

[Creating a report on page 200](#)

Copy a report

Steps

- 1) Navigate through the Report Catalog to find the report you want to copy. This can be a standard report, one created by you, or a report shared by someone else.
- 2) Click the down arrow next to the report you want, and select **Copy** from the menu.



Note

To copy multiple reports, mark the check box to the left of each report, then click the **Copy** button in the toolbar.

- 3) If you are copying a standard or shared report, select the folder where you want to store the copied report. By default this is the My Reports folder; if you have created subfolders, you can use the **Folder** drop-down to choose one of those.
If you are copying one of your own reports, it is automatically saved to the same folder as the original. You can move it to a different location later if required; see *Move items between folders*.
- 4) Click **Copy**.
The report is saved to the selected location. If you are copying a report that you own, “Copy” is appended to the report name. You can now rename the report by clicking its down arrow and selecting **Rename** from the menu. You can also edit it as required.

Related tasks

[Move items between folders on page 197](#)

Edit an existing report

Steps

- 1) Navigate through the Report Catalog to find the report you want to edit. This can be a standard report, one created by you, or a report shared by someone else.
- 2) Click the down arrow next to the report you want, and select **Edit before running** from the menu. This opens the Report Builder or Transaction View, depending on whether you are editing a grouped or a transaction report.
- 3) Edit the attributes, filters, and date range of the report as required, then click the **Update Report** button in the toolbar.
- 4) If you are editing a report that you created, or a shared report for which you have editing permissions, you can save your changes by clicking the **Save** button in the toolbar. The report is saved with the same name and in the same location, overwriting the previous version.
If you are editing a standard report, or a shared report for which you do not have editing permissions, click the **Save As** button in the toolbar to save the edited report to one of your folders.

Share a report

Steps

- 1) In My Reports, click the down arrow next to the report you want, and select **Sharing** from the menu. Alternatively, mark the check box next to one or more reports, and click the **Share** button in the toolbar.



Note

You can also share a report after running it in the Report Builder.

- 2) In the popup window, select one of these options:
 - **Not shared** means you are the only person who can access the report. Select it if you want to remove sharing from a report.
 - **View only** allows others to run the report, but not save any changes to it.
 - **Allow editing** enables others to both run and save changes to the report.
- 3) Click **OK**.
The report now has the sharing icon next to it in the report list. Hover the mouse over the icon to see the sharing permissions allocated to the report.



Note

If a shared report is set to automatically detect the time zone, a user accessing the report will always get the report in their local time zone.

Schedule a report

In My Reports, click the down arrow next to the report you want, and select **Schedule** from the menu. Alternatively, mark the check box next to one or more reports, and click the **Schedule** button in the toolbar. You can select a maximum of 5 reports for each scheduling job.



Note

You can also share a report after running it in the Report Builder.

The Add Job scheduler window opens. For more information, see *Scheduling reports*.

Related concepts

[Scheduling reports](#) on page 203

Delete a report

Steps

- 1) In My Reports, click the down arrow next to the report you want to delete, and select **Delete** from the menu. Alternatively, mark the check box next to one or more reports, and click the **Delete** button in the toolbar.
- 2) In the popup window, click **Delete** to confirm.

Managing folders

The Report Catalog offers the options to create, copy, share, delete, and move items between folders. The actions available to you depend on the permissions configured. For example, you can only move and share your own folders.

Select a link below for further instructions:

Related tasks

[Create a new folder](#) on page 196

[Copy a folder](#) on page 197

[Move items between folders](#) on page 197

[Share a folder](#) on page 198

[Delete a folder](#) on page 198

Create a new folder

You can create new folders only within the My Reports folder, up to a maximum of 4 levels of subfolders. Folder names can have a maximum of 200 characters.

To create a new folder:

Steps

- 1) Navigate to the location in My Reports where you want to place the new folder.
- 2) Click the Add Folder button in the toolbar.
- 3) Enter the new folder name, then click **Add**.
You can rename the folder later, if required, by clicking its down arrow and selecting **Rename** from the menu.

Copy a folder

When you copy a folder, you also copy all of the contents in that folder, including subfolders and their contents.

To copy a folder:

Steps

- 1) Navigate through the Report Catalog to find the folder you want to copy. This can be a folder containing standard reports, one created by you, or a folder shared by someone else.
- 2) Click the down arrow next to the folder you want, and select **Copy** from the menu.



Note

To copy multiple folders, mark the check box to the left of each folder, then click the **Copy** button in the toolbar.

- 3) If you are copying a standard or shared folder, select the location where you want to store the copied folder. By default this is the My Reports folder; if you have created further subfolders, you can use the **Folder** drop-down to choose one of those.
If you are copying one of your own folders, it is automatically saved to the same location as the original.
- 4) Click **Copy**.
The folder is saved to the selected location. If you are copying a folder that you own, “Copy” is appended to the folder name. You can now rename the folder by clicking its down arrow and selecting **Rename** from the menu. You can also edit the reports in the folder as required.

Move items between folders

If you have several folders under My Reports, you can easily move reports and folders around using drag-and-drop:

Steps

- 1) Select the items that you want to move.
- 2) Drag the items to the destination folder, in either the left-hand or right-hand pane. Note that a “Move items” popup appears as you start the drag: this turns green when hovering over a valid location, or red when over a folder where you cannot drop the report – for example, in Standard Reports.

- 3) A success message appears once you have moved the items to a valid location.



Note

If a report is shared, moving it to a folder that is not shared does not change the sharing permission assigned to the report. If you move a report to a shared folder, the report inherits the folder's sharing permissions.

Share a folder

When you share a folder, you also share the reports in that folder with the same permissions. You can then edit the sharing permissions for individual reports within the folder, although note that changes will remove the sharing permission from the folder. See *Share a report* for more information.

To share a folder:

Steps

- 1) Navigate through My Reports until the folder you want to share is shown in the right-hand pane.
- 2) Click the down arrow next to the folder, and select **Sharing** from the menu. Alternatively, mark the check box next to one or more folders, and click the **Share** button in the toolbar.
- 3) In the popup window, select one of these options:
 - **Not shared** means you are the only person who can access the folder. Select it if you want to remove sharing from a folder.
 - **View only** allows others to run the reports in this folder, but not save any changes to them.
 - **Allow editing** enables others to both run and save changes to the reports in this folder.
- 4) Click **OK**.
The folder now has the sharing icon next to it in the list. Hover the mouse over the icon to see the sharing permissions allocated to the folder.

Related tasks

[Share a report](#) on page 195

Delete a folder

Deleting a folder also deletes all reports and subfolders contained within it.

To delete a folder:

Steps

- 1) Navigate through My Reports until the folder you want to delete is shown in the right-hand pane.
- 2) Click the down arrow next to the folder you want to delete, and select **Delete** from the menu. Alternatively, mark the check box next to one or more folders, and click the **Delete** button in the toolbar.

- 3) In the popup window, click **Delete** to confirm.

Using the Report Builder

The **Reporting > Report Center > Report Builder** page offers an enhanced model for creating multi-level, flexible reports that allow you to analyze information from different perspectives. If a high-level summary shows areas of potential concern, you can drill down to find more details.

When you select the Report Builder, you may be asked which type of report you want to create: web, data, or email.

The Report Builder has the following elements:

- The **Toolbar** contains buttons for starting a new report, saving, scheduling, sharing, and updating the current report. There are also buttons for exporting reports in PDF or CSV format.
- The **Attributes** list, in the left pane, contains the data types that you can use to create reports. For information about email report attributes, see *Email report attributes*.
Use the Search box at the top of the list to filter the Attribute list further.
- The **Metrics** list, in the left pane, contains options that you can add as columns to the report. Drag metrics into and out of the report results area to add them to or remove them from the report. The available metrics change depending on the attributes that are selected. For information about email protection metrics, see *Email report metrics*.
- In the right pane, the **Grouping** field can contain up to 2 attributes to define the data grouping that appears in the report. For example, in a web report, if you drag the Category attribute followed by the Action attribute into this field, this creates a summary report on hits by category, and also displays the data broken down by action within those categories. In an email report, if you drag the Policy attribute followed by the Recipient Address attribute into this field, this creates a summary report on messages by policy, and also displays the data broken down by recipient addresses within those policies. For more information about defining grouping data, see *Creating a report*.
- The **Filters** field can contain attributes to filter the report results further. For more information about defining filters, see *Creating a report*.
- The **Date range** defines the time period covered by the report. This can be a standard period (between 1 hour and 8 months) or a specific date and time range. You can also choose whether to automatically detect the time zone for the report, or choose a specific time zone from the drop-down list.
- Next to the date range, the **display options** enable you to select how many rows appear in your report. Once a report has been generated, this section also includes options to page through longer reports, and to display the report results in different table and graph formats. For more information, see *Viewing report results*.
- The **report results** appear in the right pane when you click **Update Report**, and by default are in a table format. You can choose to display the results in different formats as described above, and to select report elements to drill down further. For more information, see *Viewing detailed reports*.

Related concepts

[Viewing report results](#) on page 201

[Viewing detailed reports](#) on page 202

Related tasks

[Creating a report](#) on page 200

Related reference[Email report attributes](#) on page 165[Email report metrics](#) on page 170

Creating a report

To create a report:

Steps

- 1) Drag up to 2 attributes from the Attributes list to the Grouping field.
 - The Report Builder does not allow you to add more than 2 attributes, nor can you add the same attribute more than once.
 - By default, the report shows the top 10 matches by number of hits. Click an attribute box in the Grouping field to change the grouping data to show a specified number of top results, a specified number of bottom results, or all results.

**Note**

Choosing to view all results may mean the report takes a long time to generate.

- To remove an attribute from the Grouping field, click the “x” icon on the attribute box.

- 2) To add filters to the report, drag an attribute to the Filters field.
 - a) On the popup that appears, use the drop-down list to define how the filter handles the values that you specify. The options available depend on the attribute that you have selected. For example, you may be able to include or exclude values, or state that search terms equal or do not equal your text.
 - b) Enter or select the search terms or values that you want to filter on. Depending on the filter, you can:
 - Select one or more check boxes
 - Start typing text that will autocomplete based on data in the system
 - Enter the exact text that you want to use

For filters where you are including or excluding values already stored in the system, start typing to see a list of potential matches. Then select the option you want from the list. You can add multiple values to the filter.



Note

A **Use free text entry** check box is available for filters that use autocompleted text. Selecting this allows you to copy and paste multiple values into the text box rather than entering each one individually. Any autocompleted values already added are converted to free text when the check box is selected, and if the check box is cleared, any free text values are converted to autocompleted values.

For filters where you enter free text, enter the terms you want separated by commas.

- c) Click **OK** when done.

To edit a filter, click its attribute box. To remove an attribute from the Filters field, click the “x” icon on the attribute box.
- 3) Click in the Date range field to define the report period.
 - To specify a set period in hours, days, or months, select an option from the **Last** drop-down list.
 - To specify a particular date range, select the **From** radio button and use the calendars to choose the required dates. Date ranges include the whole 24-hour period, unless you mark **Specify start and end time** to enable and edit the times for the report as well as the dates.

Note that reports are run using your local time zone unless you specify otherwise. Click **Done** when you are finished.

- 4) Click the Update Report button to generate the report.



Note

The Update Report button turns yellow when you enter or change valid report content, signifying that you can generate a report with the selected criteria.

Viewing report results

Your report results are initially shown as a table, with a column for the grouping and filters you selected, and a column for each of the selected metrics. Report results use your local time zone.

Use the arrows next to each first-level attribute to expand or collapse the second-level attribute content below it.

Use the options in the toolbar to define how you display and navigate through report results:



Select the number of rows to see on each page. The default is 100 rows; you can also select 50, 150, or 200 rows.

Use the arrow keys to page through longer reports, and quickly jump to specific pages.

View the report results as one of the following:

- column chart
- bar chart
- pie chart
- line chart
- area chart

Hover the mouse over an item in a chart to see more information, for example a percentage or a number of hits.

All of these charts are available for a single- level grouping report. For grouping reports with 2 attributes, only column and bar charts are available.

Each item in the report has a check box. Select one or more check boxes to open a pop-up window that enables you to:

- Drill down into more detailed information. See *Drilling into report items*.
- Show only the report items you have selected
- Filter out the report items you have selected
- View individual transactions for the items you have selected.
- Cancel any selections you have made.

Related tasks

[Drilling into report items](#) on page 203

Viewing detailed reports

You can use grouping reports as a starting point for accessing more detailed information, either by drilling down into a particular aspect of a report, or using Transaction View (web), Incident Manager (web), or Message Center (email) to see further information about a report item.

Drilling into report items

To drill down into a report item:

Steps

- 1) Mark the check box next to each item you want to drill down into.
You can select multiple items and change your selections, even after the pop-up window appears.
- 2) In the pop-up window, select an available attribute from the Drill Into By the drop- down list.
- 3) The new report loads. Note that as you have moved down a level in the report, the items you selected in step 1 are now in the Filters field, while the Grouping field contains the other report attributes, including the one you selected in step 2.
You can edit the content of the Grouping and Filters fields, and view the report in different formats, in exactly the same way as for the previous report.
- 4) To drill down a further level, repeat steps 1-3 above.

Exporting a report

You can export your report results as either a PDF or CSV file.

To export a CSV file, click the **Export to CSV** button in the top right corner.

To export a PDF:

Steps

- 1) Click the **Export to PDF** button in the top right corner.
- 2) On the pop-up window that appears, enter a name, and optionally a description, for the report.
- 3) Choose a page size and orientation for the PDF.
- 4) Click **Export**.

Scheduling reports

The **Reporting > Report Center > Scheduler** page lists the scheduled jobs created for reports. The list gives basic information about the job, such as how frequently it runs and which administrator owns it. From this page, you can add and delete scheduled jobs, and edit the content and frequency of jobs.

The list provides the following information for each job.

Column	Description
Job Name	The name assigned when the job was created.

Column	Description
Recurrence	The recurrence pattern (Once, Daily, Weekly, Monthly) set for this job. For daily, weekly, and monthly reports, the recurrence includes further options for the days the report is run.
Starting	The defined start date for the job.
Ending	The end date for the job. If no end date is set, the column displays Never.
Owner	The user name of the administrator who scheduled the job.

Use the options on the page to manage the jobs:

- Click the job name link to edit the job definition. See *Adding and editing scheduled jobs*.
- Click **Add Job** to define a new job. See *Adding and editing scheduled jobs*.
- Select a job and then click **Delete** to delete a scheduled job. After a job has been deleted, it cannot be restored.

The Allowance in the top right corner shows you how many jobs are currently scheduled, and the maximum number of jobs available to you.

Related concepts

[Adding and editing scheduled jobs](#) on page 204

Adding and editing scheduled jobs

You can run reports as they are needed, or you can use the **Scheduler > Add Job** page to create jobs that define a schedule for running one or more reports. Once a job has been created, you can use the **Scheduler > Edit Job** page to change the job details, for example editing the reports in the job or altering the frequency.

Reports generated by scheduled jobs are distributed to one or more recipients via email. As you create scheduled jobs, consider whether your email server will be able to handle the size and quantity of the attached report files.

To access the Add Job page, do one of the following:

- Select a report in the Report Catalog and click the **Schedule** button in the toolbar.
- Once you have run a report in the Report Builder, click the **Schedule** button in the toolbar.
- Click **Add Job** on the Scheduler page to create a new job.

To access the Edit Job page:

- Click the job name link on the Scheduler page.

The Add Job or Edit Job page contains several tabs for selecting the reports to run and the schedule for running them.

For detailed instructions, see:

- *Selecting reports to schedule*
- *Setting the schedule*
- *Selecting report recipients*

■ *Selecting delivery options*

You can cancel the job creation or editing at any time by clicking **Cancel**. If you are editing a job, you can click **Save** once you have made the required changes, without needing to work through all the tabs.

After creating jobs, use the job list on the Schedule page to review job summaries and find other helpful information (see *Scheduling reports*).

Related concepts

Selecting report recipients on page 206

Scheduling reports on page 203

Related tasks

Selecting reports to schedule on page 205

Setting the schedule on page 205

Selecting delivery options on page 207

Selecting reports to schedule

Use the **Report Selections** tab of the Add Job or Edit Job page to choose reports for the job.

Steps

- 1) Enter a **Job name** that uniquely identifies this scheduled job.
- 2) Highlight a report for this job in the Report Catalog tree.
- 3) Click the right arrow (>) button to move that report to the **Selected reports** list.



Note

Reports saved with a static date range (for example, from 1 May to 1 June) cannot be scheduled. If you move a report with a static date range to the **Selected reports** list, a warning appears, and you can change the date range for the scheduled version of the report using the drop-down in the **Date Range** column.

- 4) Repeat steps 1 and 2 until all reports for this job appear in the **Selected reports** list, to a maximum of 5 reports.
- 5) Click **Next** to open the Scheduling Options tab.

Setting the schedule

Define a reporting job to occur once or on a repeating cycle on the **Scheduling Options** tab of the Add Job or Edit Job page.

Steps

- 1) Select a **Frequency** for the job. The specific options available depend on the frequency selected.

Frequency	Options
Once	No additional recurrence options are available.
Daily	Select whether the job is run every weekday, or on a certain number of days in the month – for example every 3 days.
Weekly	Click each day of the week the job is to run.
Monthly	<p>Either:</p> <p>Select how frequently the job should run, in a range of every month to every 12 months, then click each date the job is to run.</p> <p>Or:</p> <p>Select how frequently the job should run, in a range of every month to every 12 months, then select a frequency and a day of the week. For example, you could run the report every 2 months on the 2nd Tuesday of the month.</p>

- 2) Under **Starting**, set the start date for running the job.
- 3) Under **Ending**, select an option for ending the job.

Option	Description
Never	<p>The job continues to run according to the established schedule, indefinitely.</p> <p>To discontinue the job at some time in the future, either edit or delete the job.</p>
On	Set the date when the job stops running. It does not run on or after this date.
After	Select the number of times to run the job. After that number of occurrences, the job does not run again, but it stays in the Job Queue until you delete it.

- 4) Select a **Timezone** for the report. The reports in the scheduled job will be delivered by 6am in the selected time zone on the days you define.
- 5) Click **Next** to open the Recipients tab.

Selecting report recipients

Use the **Recipients** tab of the Add Job or Edit Job page to select the recipients of reports in this scheduled job.

Select one of the following:

- **Specific administrators** – Choose the administrators in your cloud service account that should receive the reports in this job.
- **All administrators** – All administrators in your cloud service account receive the reports.

You can also enter additional email addresses if you want the job results to go to people who are not cloud service administrators. Enter each address on a separate line.

Click **Next** to open the Delivery Options tab.

Selecting delivery options

Use the **Delivery Options** tab of the Add Job or Edit Job page to define the report output format and email options.

Steps

- 1) Select the **File format** for the finished report.

Format	Description
PDF	Portable Document Format. Recipients must have Adobe Reader v7.0 or later to view the PDF reports.
CSV	Comma Separated Variable file. This can be opened in Microsoft Excel or another spreadsheet program.

- 2) Define whether the report should display in Letter or A4 size.
- 3) Define whether the report should be password-protected for secure delivery. If you select **Password protected**, enter and confirm a password that the report recipient must use to view the report contents.
- 4) Edit the custom **Subject** and **Body** text for this job's distribution email, if required.
A list of reports in the scheduled job is included in the email message by default. If you remove this and then want to reinstate it at a later time, click **Insert Report List**.
You can revert to the default text at any time by clicking **Reset Email**.
- 5) Click **Finish** to save and implement the job definition, and display the Scheduler page.

Exporting data to a third-party SIEM tool

Use the **Reporting > Account Reports > SIEM Integration** page to format reporting data for use by a third-party SIEM tool. Select data columns and apply filters to the data, just as you do in other areas of the Report Center (for Web, see *Using the Transaction Viewer*, for Email, see *Using Message Details*).

Before data can be exported, you need to configure **SIEM Storage** details. Navigate to **Account > SIEM Storage** to select a storage type and configure your own storage if you do not wish to use Forcepoint storage (the default). See *Configuring SIEM storage* for details.

After selecting the type of data that you want to export to your SIEM tool, define the data format, and enable SIEM data export.

To configure and enable SIEM integration:

Steps

- 1) Select a data type (Web Security or Email Security) from the drop-down list. Note that:
 - You can select one or both options.
 - Only options appropriate to your account are displayed.
- 2) Use the **Columns** drop-down list, or drag items into the report panel from the **Attributes** or **Metrics** lists to customize the information that will appear in the exported data. You can drag columns in the report panel to re-order them.

The default columns vary, depending on which data type you have selected.

The number of columns allowed also varies, depending on the data type. For Web Security, the limit is 35. For Email Security, the limit is 25.

See *Report attributes: Web and Data Security* or *Email report attributes* for additional information.

- 3) Drag items from the **Attributes** or **Metrics** lists to the **Filters** field to define any filters you want to apply to your reporting data before it is exported. On the popup that appears, use the drop-down list to define how the filter handles the value that you specify.

The attributes available for use as Filters is a subset of those available to add as a column. Customers exporting Web data can select filters for the following:

- Action
- Category
- Parent Category
- Risk Class
- Severity
- Policy
- Cloud App Risk level

Customers exporting Email data can select filters for:

- Action
- Direction
- Emb. URL Category

Only data that matches the selected filters will be included in the downloadable files.



Note

You can click a column heading to sort the data by the entries in that column. This may be useful to check that the export will include the data that you want. However, note that this sort will not be applied to the data that is exported.

- 4) When you are satisfied with the columns and filters that you have selected, toggle the **Enable data export** switch to **ON**.

**Note**

Enable data export cannot be set to **ON** unless a valid storage option has been configured on **Account > SIEM Storage**.

The option is automatically set to **OFF** if:

- **Forcepoint** storage is enabled but no logs have been downloaded for 30 days.
- **Bring your own** storage is enabled but no SIEM data could be forwarded to the active bucket for 14 days.

Multiple emails are sent prior to disabling the export option.

Click **Refresh** to display the last 2 hours of data.

- 5) When you are finished, click **Save**.

Related tasks

[Configuring SIEM storage](#) on page 14

[Using Message Details](#) on page 164

Related reference

[Email report attributes](#) on page 165

Using Bring your own storage

The output generated by the export process is forwarded to the active AWS S3 bucket listed on the SIEM Storage page. Files are assigned names using the format `web|email_<accountid>_<timestamp>_<server>_<timestamp>.csv.gz`, and will use any prefix values defined for the bucket.

Using Forcepoint storage

To get the formatted SIEM data to your network, you can either use the sample Perl script included in the zip file linked at the top of the SIEM integration page, or create a script of your own. The account used to run this script must have “Log Export” permissions (see *Running the SIEM log file download script for Forcepoint storage* for more information about using the script) but permission to log onto the portal is not required.

**Note**

If you give this contact only the **Log Export** permission and nothing else, the user name and password cannot be used to log on to the cloud portal. Although log on permissions are not needed to run the script, the **View Reports** permission is the minimum permission a user needs to be able to log on.

Minimum permissions should be given to this user. The user password is needed to run the script and is viewable in plain text. For that reason, it is recommended that this user not be one with permissions to modify reports or account policies.

To download the sample script:

Steps

- 1) Click the link in the introductory text on the SIEM Integration page.

- 2) Save the file to a location of your choice and unzip it. It contains 4 files and provides all you need to run the script.
 - A set of binary library files.
 - A configuration file that can be used to pass parameters to the script. Then, use the `cfg` file parameter when you execute the script. See *Running the SIEM log file download script for Forcepoint storage*. Note that adding parameters to the command line when executing the script will override the parameters in the config file.
 - The default script file.
 - a ReadMe file with details on how to handle the other files.

The set of library files and the script should always be kept together in the same folder. The configuration file can be located in a different folder, if necessary. The path to it can be included in the `cfg` file parameter.



Warning

Forcepoint provides the sample log download script as a convenience to its customers, but does not provide support for customization and will not be responsible for any problems that may arise from editing the script.

The script can be run on Windows or Linux, and does the following:

- Connects to the cloud service using the URL specified in the script
- Optionally reports the log files available for download
- Downloads the available log files to a location of your choice, or by default to the directory where the script is located
- Optionally checks the MD5 hash of each downloaded file to verify the file's integrity before deletion from the server
- Uses the HTTP DELETE method to exclude downloaded files from the list of files to be processed.

Whether they have been downloaded or not, files that are 14 days old are deleted.



Note

Running the script on Windows requires a Perl distribution, which you can download from <http://www.perl.org/get.html>.

The script (`par` file) contains all of the necessary modules, but, should you need to install them manually, a list of the required modules is included in the ReadMe that is part of the zip file.

If you customize the sample script or choose to write your own script, you must always include the DELETE method to avoid listing the same files again and to remove the downloaded files from the server. This is because files are only retained for 14 days.

Optionally, you can use the Windows Scheduler or Linux **cron** and **crontab** commands to schedule the script to run at regular intervals. Use the `infinite_loop` option (see *Running the SIEM log file download script for Forcepoint storage*) to run the script as a background process.

For information about using the sample script, see *Running the SIEM log file download script for Forcepoint storage*.

Related reference

[Running the SIEM log file download script for Forcepoint storage](#) on page 212

Running the SIEM log file download script for Forcepoint storage

You can use the parameters described below to customize the sample download script used to download reporting logs from the cloud service for use by your SIEM tool.

Some parameters have a short form (for example, **-v**) and a long form (for example, **--verbose**). For these parameters, both options are listed.

Parameter	Description
-u <username> --username	Mandatory. Defines the logon user name for connecting to the cloud service. This must be an administrator contact with Log Export permissions. For example: -u siem_user@example.com
-p <password> --password	Mandatory. This is the password for the specified user name. For example: -p Ft2016Logs
--stream	Mandatory. This is used to determine the type of files to be downloaded. Valid values are web, email, or all. If "all" is specified, /web and /email folders are created under the destination directory and files are downloaded to the corresponding folder.
-v --verbose	Optional. Runs the script in verbose mode, which displays progress messages. Verbose mode provides feedback on the script's progress, for example: <ul style="list-style-type: none"> ■ Downloading filelist from <host name> as <user name> ■ No files available to download ■ Downloading <file> to <file name location>
-h <hostname> --host	Optional. Defines the host name to connect to. This is specified in the script by default, so you would only need this option if you have edited the script to remove it, or if you have been given a different URL to connect to. For example: -h https://sync-web.mailcontrol.com

Parameter	Description
-d <file path> --destination	Optional. Defines the destination directory for the downloaded log files. If not specified, the files are downloaded into your current working directory. For example: -d /cloudweb/logs
-m --md5sum	Optional. Checks the md5sum of each downloaded file. The MD5 hash is commonly used to verify the integrity of files and can be used to check the files before they are deleted from the server.
-l --list-only	Optional. Displays a list of available log files without downloading them.
--proxy <proxy details>	Optional. Specifies an HTTP proxy to use if you are having difficulty connecting to the cloud service. The proxy must be in the form <code>http://username:password@host:port</code> For example: --proxy http://jsmith:Abc123@proxy_server:80
--max_download_children	Optional. Specifies the number of downloading processes to run in parallel. If not set, a single process is used. The maximum number of processes that can run in parallel is 10. If the list-only parameter returns a large number of files not yet downloaded, set this value to 10 to allow the downloads to process those files.
--infinite_loop	Optional. When configured, the download and reformat processes are run in an infinite loop. If not set, files that become available when the script is running are not downloaded.
--man	Optional. Displays the list of parameters with their descriptions.
--help	Optional. Displays a brief description of the program's purpose.
--cfgfile	Optional. Specifies the location of a configuration file which can include values for the other parameters.

A configuration file might look like this:

```
username=admin@company.com password=password1
host=sync- web.mailcontrol.com infinite_loop=false
verbose=true max_download_children=3 md5sum=false
list_only=true stream=all destination=/tmp proxy=http://
user2@company.com:password2@myproxy.com:8081/ pidfile=/var/tmp/ftl.pid
```

See [Getting started with SIEM integration](#) for additional details on setting up SIEM integration and scheduling the download.

Account Reports

Contents

- [Introduction](#) on page 215
- [Account Summary report](#) on page 216
- [Service reports](#) on page 217
- [Downloading report results](#) on page 219
- [Saving reports](#) on page 220
- [Scheduling reports](#) on page 220

Introduction

Go to **Reporting > Account Reports** to see the account-level reports available to you.

- For cloud email, the account summary report provides a summary of the email traffic that has been processed for your account during a defined time period.
- If you have identity management enabled for your account, you can generate synchronization statistics for the service.
- With cloud email, you can report on the end users who are subscribed to Personal Email Subscriptions.

All reports are generated in real time using the cloud manager. Most include charts and tables that are presented in an easy to read, printable format.



Note

For larger accounts, where a lot of data is to be retrieved, the reports may take some time to generate. As soon as the relevant data has been retrieved it is displayed while the remainder of the report is being compiled.

Commonly-used report criteria can be saved for easy access. For more information, see *Saving reports*. Saved reports can be scheduled for regular delivery to one or more recipients as described in *Scheduling reports*.

The Fallback mode for Neo is configurable and can be set to allow the user request, block the user request, or use local cache to apply policy.

Related tasks

[Saving reports](#) on page 220

[Scheduling reports](#) on page 220

Account Summary report

The Account Summary report is a combination of reports that can be obtained elsewhere in the service. Select the time period, click **Go**, and you are presented with a summary of the email traffic that has been processed for your account during the selected time period. (If you have a lot of mail flowing through the system, this may take a while.) The report is organized by section and preceded by a table of contents with hyperlinks into specific data. Click the links to view the report, or scroll down the page using the scroll bar.

Scheduling Account Summary reports

If you would like non-graphical versions of the Account Summary reports to be sent to one or more email addresses on a regular basis:

Steps

- 1) Select **Reporting > Account Reports > Account Summary**.
- 2) Click the **click here** link on the Account Summary Report page to set up report delivery.
- 3) Enter one or more email addresses to which you want the report sent.
If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.
- 4) Set up a subscription schedule by specifying one of the following delivery periods for your reports:
 - daily
 - weekdays
 - weekly
 - every other week (biweekly)
 - monthly (the default option)If you want to stop the a scheduled report temporarily, select **suspend delivery**.
- 5) Click **Save**.
Your schedule details are then shown on the Account Summary page. You can edit or delete your details from the **click here** link.



Note

You must renew your subscription to the Account Summary report every 3 months or your subscription expires.

Printing Account Summary reports

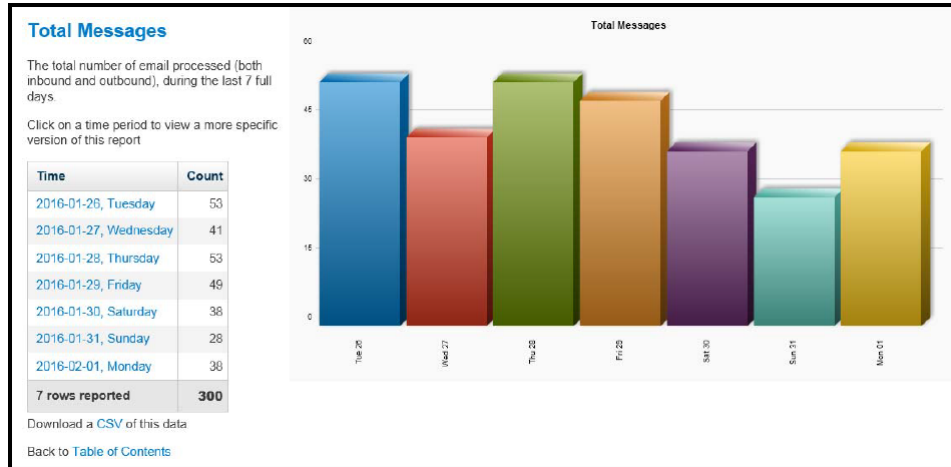
Once you have generated the Account Summary report, click **Click here to print this page** to get a printer-friendly version of the report. After a few seconds a printer selection dialog box appears.

Please leave plenty of time for the graphics to appear before printing. We recommend that you select “Landscape” format.

Viewing detailed information

To view detailed daily information, click the relevant bar in the chart or the date in the table. The result is shown below.

You can expand each section in the Account Summary report in this manner.



Service reports

The Service reports provide data that relates to directory synchronization and to end user message report subscriptions.

If System for Cross-domain Identity Management (SCIM) has been selected for identity management, an audit trail can be configured to collect the synchronization data for that feature. See *SCIM audit trail* for details.

Related concepts

[SCIM audit trail on page 224](#)

Directory synchronization reports

If you have Directory Synchronization selected for identity management on your account, you can view and print reports on the portal that show the history of directory synchronizations, including high-level statistics on success/failure and numbers of items synchronized.

Steps

- 1) Select **Reporting > Account Reports > Services**.

- 2) From the **Show** drop-down list, select a report to show:

Report	Description
Synchronization History Log	The history log provides a connection history for the specified period, up to 1000 rows.
Synchronization Time Summary	The time summary provides a list of the 20 longest synchronization times.

- 3) From the **during** drop-down list, select the time period for the report. Click **more** to select a specific date or time.



Note

The 'last 6 full hours' period does not include a synchronization just performed. You must wait for the hour to pass for it to appear in this report. You can view the very latest synchronization history in the Identity Management page.

- 4) Click **Generate report**. Following is a sample Synchronization History Log:

Date (UTC)	SourceIP	Type	Status	Additions	Deletions
2008-10-21 10:56:53	10.5.21.32	test	200 OK		
2008-10-21 10:57:21	10.5.21.32	Addresses	200 OK		
2008-10-21 10:59:15	10.5.21.32	test	200 OK		
2008-10-21 10:59:54	10.5.21.32	Addresses	200 OK	27	0
2008-10-21 11:01:13	10.5.21.32	Groups	200 OK	8	0
2008-10-21 11:01:43	10.5.21.32	Users	403 SQL command failed after 1 attempts: DBD::mysql::st execute	0	0
2008-10-21 13:07:06	10.5.21.32	Groups	200 OK	8	0
2008-10-21 13:07:18	10.5.21.32	Users	403 SQL command failed after 1 attempts: DBD::mysql::st execute	0	0
2008-10-21 13:10:19	10.5.21.32	test	200 OK		
2008-10-21 13:10:40	10.5.21.32	Groups	200 OK	0	0
2008-10-21 13:10:50	10.5.21.32	Users	200 OK	0	0
2008-10-22 09:16:14	10.5.21.32	test	200 OK		
2008-10-22 09:16:39	10.5.21.32	Addresses	200 OK	27	0
2008-10-22 09:16:52	10.5.21.32	Groups	200 OK	0	0
2008-10-22 09:17:05	10.5.21.32	Users	200 OK	0	0

You can download the report to a CSV or PDF file. You can also print the report.

Subscriptions report

The Personal Email Subscriptions report lists the end users who are subscribed to personal email subscriptions for the criteria you specify.

Steps

- 1) Select **Reporting > Account Reports > Services**.
- 2) From the **Show** drop-down list, select **Personal Email Subscriptions - Subscriptions**.
- 3) From the **during** drop-down list, select the time period for the report. Click **more** to select a specific date or time.

- 4) Select the policy or policies for the report.
- 5) Select the domain(s) for the report.

**Note**

You can use the **Shift** and/or **Ctrl** keys to select multiple domains and policies.

- 6) Click **Generate report**.

**Note**

You can see the expiration date of each subscription, as well as subscriber and recipient addresses, in the report that is generated. The latter may be useful for consolidated end user message reports (one report for multiple email accounts).

Downloading report results

On each report, you have the option to download the data as a PDF or CSV file.

**Note**

You can also download charts as image files or in PDF format. To download a chart, right-click the chart and select the format to download (PDF, PNG, or JPEG).

Downloading a CSV file

You can download the statistics for the majority of reports as a comma-separated values (CSV) file. This allows you to import it into a third-party application, such as Microsoft Excel, for viewing and manipulation. On each table of results, click **Download CSV** to begin the download.

**Note**

For some email reports, the totals in the CSV file might be higher than the totals in the report on screen. This is because the generated reports contain 1 line per email message, whereas the CSV version contains 1 line per recipient which means that a single email message might appear several times.

Downloading a PDF file

Report results can be output to Portable Document Format (PDF) for easy distribution or printing. The PDF report is generated by clicking the **Download PDF** button on a table of results.

Saving reports

You can choose to save any Services report. Use this option to identify the reports you generate most frequently and want to be able to locate quickly.

To see the list of reports that you have saved, select **Reporting > Account Reports > Saved Reports**.

To save a report:

Steps

- 1) Under **Reporting > Account Reports > Services**, select the report you want.
- 2) Use the **Selection** screen to enter your report criteria.
- 3) Click **Save Report**.
- 4) Enter a name for the report, and click **Save**.

The Saved Reports list is displayed, and the report you entered is now listed.

As well as accessing the report from this screen, you now have the option to delete the saved report or schedule it for regular delivery.

Scheduling reports

You can run reports as they are needed, or you can define a schedule for running one or more saved reports.

Reports generated by scheduled jobs are distributed to one or more recipients via email. The reports can be in HTML, PDF, or CSV format. There is a limit on the number of reports you can schedule for delivery: the Saved Reports list displays the remaining number you can schedule in addition to any existing deliveries.



Note

You cannot schedule reports that have defined start and end dates, or that span periods of less than 24 hours.

To schedule a report:

Steps

- 1) Select **Reporting > Account Reports > Saved Reports**.
- 2) You can schedule an existing saved report by clicking the report you want to schedule on the Saved Reports list. If you do this, skip to step 5 below.
Otherwise, to create a new report for scheduling, click the **Generate a new report** link. The page that appears includes only reports that are eligible for scheduling.
- 3) Create and save your report as described in *Saving reports*.
- 4) On the Saved Reports list, click the name of your new report.

- 5) Click **Schedule email report**.
- 6) Enter the email address of the report recipient. Multiple email addresses should be separated by commas or spaces.
If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.
- 7) Enter a subject for the report email, and the text you want to appear in the body of the email.
- 8) Select the report format.
- 9) Set one of the following delivery periods for your reports:
 - daily
 - weekdays
 - weekly
 - every other week (biweekly)
 - monthly (the default option)If you want to stop the a scheduled report temporarily, select **suspend delivery**.
- 10) Click **Save**.
You are returned to the Saved Reports list. Reports that have been scheduled display the recipient list in the **Email to** column. Click an item in this column to open the schedule, where you have the option to edit or delete the report delivery.

Related tasks

[Saving reports](#) on page 220

Contents

- [Introduction](#) on page 223
- [Configuration audit trail](#) on page 223
- [SCIM audit trail](#) on page 224
- [Administrator audit trail](#) on page 224

Introduction

The following audit trails are available:

- *Configuration audit trail* lets you examine the configuration audit database for your account. This gives you visibility into all of the configuration changes that have been made on the account. Access it from the **Account > Settings > Audit Trail** page.
- *SCIM audit trail* lets you examine the records forwarded to the cloud service by your identity provider.
- *Administrator audit trail* lets you examine the quarantine audit database for your account. This gives you visibility into the actions taken by administrators in the Message Center. Access it from the **Email > Messages > Administrator Audit Trail** page.

Related concepts

- [Configuration audit trail](#) on page 223
- [SCIM audit trail](#) on page 224
- [Administrator audit trail](#) on page 224

Configuration audit trail

Use the **Account > Settings > Audit Trail** page to find information about administrator actions and configuration changes.

To run the default search, which shows results for all users, actions, descriptions, and SQL queries that have occurred so far today, click **View Results** without making any changes on the page.

To perform a more targeted search, use the fields and selectors on the screen to specify the type or range of data that you want to see. You can enter:

- All or part of an administrative **User name**, or * (default) to specify any user
- An **Action type**, like “Login” or “Delete,” or **All** (default) to specify all actions
- All or part of a **Description** of the action that occurred, like an IP address or policy number, or * (default) to specify any description text

- All or part of the specific **SQL** query used to perform the action, or * (default) to specify any SQL query
- A **Date range** (today's date, by default) for the query

By default, when you enter a string in any field, the search looks for an exact match. To configure the search to look for any string that contains the value you specify, precede your entry with an asterisk (*) character (for example, *DELETE or *admin).

When you click **View Results**, any audit trail information that matches your search parameters is displayed in a table. All results include the date and time that the action occurred, a description of the action, the action type, and the user who performed the action. If the action resulted in a change to the configuration database, the SQL query used to make the change is also displayed.

Paging controls are displayed just above the results table. Use the controls to configure how many results to display on the page, and to move through the results.

Click the back arrow above the table to return to the Audit Trail page where you can enter new search parameters.

Click **Export to CSV** on either the Audit Trail page or the Search Results page to export the results of your audit trail search to a file named **audit_trail.csv**. You can open the file, save the file with the default name, or save the file with a new name.

SCIM audit trail

When System for Cross-domain Identity Management (SCIM) is configured for identity management, identity providers send user and group changes to the cloud service as they happen. The changes are recorded by the cloud server against the user SCIM and an audit trail can be configured to provide details of these changes.

To configure an audit trail to collect this information, go to **Account > Settings > Audit Trail** and enter the following parameters:

- SCIM as the **User**.
- An **Action type** such as Add, Delete, or Modify, or use the default (All).
- A specific user or group in the **Description** to view events for the specified user or group or use the default (*) to all events.
- * for **SQL**.
- A Date range to limit the results to events that occurred during a specific time frame.

Select **View Results** to view the events in a table or **Export to CSV** to a file (audit_trail.csv.)

See *Configuration audit trail* for more details on configuring an audit trail.

Related concepts

[Configuration audit trail](#) on page 223

Administrator audit trail

The administrator audit trail provides visibility into actions performed by an administrator in the Message Center. To access it, choose **Email > Messages > Administrator Audit Trail**.

You can base searches on message sender, recipient, subject, who performed the action, and the action itself, within a defined date range.

Standard Email Configuration

Contents

- Introduction on page 227

Introduction

The Forcepoint Email Security Cloud service provides a standard configuration for all email accounts. The settings for the standard configuration are described below, as well as the reasoning behind the settings. As an administrator, you can customize policy settings to suit your needs. Do this by clicking **Email**, then following the instructions in *Defining Email Policies*.

Each table in this section represents a section in email configuration settings. Column 4 suggests various use cases for changing the standard setting.

1. Policy Management	Standard setting	Reason for standard setting	Consider changing setting if...
Policies	One policy has been set up with the standard account configuration shown in this document.	(see individual settings below)	Additional policies should be added to support aliases, or to support a domain (or domains) that require differing configurations.

2. General tab	Standard setting	Reason for standard setting	Consider changing setting if...
Notifications	Inbound: Recipient Outbound: Sender	Intended recipient needs visibility of blocking. Sender needs visibility of blocking.	Volume of notifications is too high, visibility is not required, or notifying sender is preferable.
Annotations	Inbound: on Outbound: on	Allows recipient to report spam easily and automatically. To give confidence to recipient that message is virus-free.	Transparency of Forcepoint Email Security Cloud service is important. Company-specific annotation is required.

3. Domains tab	Standard setting	Reason for standard setting	Consider changing setting if...
Domains	Registered domain is shown.	At least one valid domain name must be provided.	Additional domains are to be analyzed.

4. Connections tab	Standard setting	Reason for standard setting	Consider changing setting if...
Inbound Mail Routing Rules	No rules set up.	No inbound routing rules are provided at the time of registration.	Inbound mail is to be routed to different email servers depending on the recipients.
Default Inbound and Outbound Routes	Registered route information is shown.	At least one inbound and one outbound route must be provided.	More servers are to send email to or receive from the cloud service. An "A record" is needed if load balancing across servers is required.

5. Antivirus tab	Standard setting	Reason for standard setting	Consider changing setting if...
Active Content	Inbound: HTML: medium	Protect user from non-obvious active elements.	HTML mail is not rendered correctly.
	Outbound: HTML: off	Active HTML content is from trusted source.	HTML mail should be filtered.
	Inbound: Macro analyzer: high	Protect user from suspicious macros.	Too many relevant files are blocked.
	Outbound: Macro analyzer: off	Macros are from trusted source.	Additional security is required.
Encrypted messages	Inbound: password-protected zips: on	Not possible to analyze content of password-protected zips.	Requirement to transmit password-protected zips
	Outbound: password-protected zips: off	Files are from trusted source.	Additional security required
	Inbound: Encrypted mail: on	Not possible to analyze encrypted mail.	Requirement to exchange encrypted mail
	Outbound: Encrypted mail: off	Messages are from trusted source.	Additional security required
Executables	Inbound: Quarantine exe: on	Most administrators do not allow users to receive executables.	Most users need to transmit executables.
	Outbound: Quarantine exe: on	Most administrators do not allow users to send executables.	Most users need to transmit executables.

6. Antispam tab	Standard setting	Reason for standard setting	Consider changing setting if...
Existing Rules	Spam Score > 15.0 - discard Spam Score > 6.0 - quarantine	No false positives score as high as 15.0. System default spam threshold	Discarding of spam not required or score needs to be higher or lower Quarantining of spam not required or score needs to be higher or lower
Exceptions	Allowlist these addresses: off Blocklist this address: off	No allowlist entries are provided at the time of registration. No blocklist entries are provided at the time of registration.	Administrator may populate a allowlist for the account. Administrator may populate a blocklist for the account.
End Users	Allow users to populate their own allowlists and blocklists: on	Allow users some control over incoming senders for their own address	No control or visibility is desired for end users.
	Allow users to obtain a copy of an email that has been quarantined as spam: on	Allow users safe control over spam email sent to their own address	No control or visibility is desired for end users.
Keep Messages	Keep a copy of clean messages so they can be learnt from if later reported as spam: on	Cloud service keeps a private copy of the message for a short time to aid in spam-tuning when the 'Report this email as Spam' link is clicked.	No retention of clean messages for spam tuning is desired.

7. Content Filter tab	Standard setting	Reason for standard setting	Consider changing setting if...
Attachments	Inbound: Mask attachments with .eml extension	Unable to analyze .eml files	.eml files are not a concern or if more file extensions are to be added
	Outbound: Do not mask any attachments	Files are from trusted source.	Different file types are to be considered suspicious.
	Inbound: Quarantine messages containing nominated file types: off	Allow admin to populate list before applying it	Blocking of certain file types is required.
	Outbound: Quarantine messages containing nominated file types: off	Allow admin to populate list before applying it	Blocking of certain file types is required.
	Inbound: Quarantine messages containing files of unknown type: off	Cloud service can identify majority of file types	There is a need for quarantining unknown attachments.

7. Content Filter tab	Standard setting	Reason for standard setting	Consider changing setting if...
	Outbound: Quarantine messages containing files of unknown type: off	Files are from trusted source	Outgoing attachments are to be considered suspicious.
	Inbound: Quarantine messages containing inappropriate images: off	Requires license for Forcepoint Email Security Image Analysis Module	There is a need to analyze images.
	Outbound: Quarantine messages containing inappropriate images: off	Requires license for Email Security Image Analysis Module	Outgoing images are to be considered suspicious.
	Inbound: Quarantine messages with images that could not be scanned: off	This setting can only be enabled when image quarantine is on.	There is a need to check large images.
	Outbound: Quarantine messages with images that could not be analyzed: off	Files are from trusted source	There is a need to quarantine and check large images.
	Inbound: Park attachments meeting nominated criteria: off	Most large attachments can be delivered successfully	There is a need to conserve users' mailbox size.
	Outbound: Park attachments meeting nominated criteria: off	Files are from trusted source	There is a need to conserve recipients' mailbox size.

7. Content Filter tab	Standard setting	Reason for standard setting	Consider changing setting if...
Message Size	Inbound: Non-deliver > 50MB: on	Contractual maximum message size	Lower limit is required.
	Outbound: Non-deliver > 50MB: on	Contractual maximum message size	Lower limit is required.
	Inbound: Quarantine > 10MB: off	Max message size usually acceptable	Lower the limit below the maximum size to conserve your bandwidth.
	Outbound: Quarantine > 10MB: off	Max message size usually acceptable	Lower the limit below the maximum size to conserve recipient organization's bandwidth.
	Inbound: Defer delivery: off	Requires your policy to be applied	There is a need to conserve your bandwidth during certain time periods.

7. Content Filter tab	Standard setting	Reason for standard setting	Consider changing setting if...
	Outbound: Defer delivery: off	Requires your policy to be applied	There is a need to assist with conserving recipient organization's bandwidth during certain time periods.
7. Content Filter tab	Standard setting	Reason for standard setting	Consider changing setting if...
Content Filtering	Inbound: Filter using these lexical rules: on	Allow new rule to be implemented immediately.	Suspension of lexical filtering
	Outbound: Filter using these lexical rules: on	Allow new rule to be implemented immediately.	Suspension of lexical filtering
	Inbound: Quarantine messages if content analysis does not complete: off	Cloud service rarely fails to complete lexical analysis.	There is a large number of lexical rules and regular expressions, which could mean analysis does not complete.
	Outbound: Quarantine messages if content analysis does not complete: off	Cloud service rarely fails to complete lexical analysis.	There is a large number of lexical rules and regular expressions, which could mean analysis does not complete.

Related information

Defining Email Policies on page 75

Contents

- [Use Cases for Setting up User Provisioning](#) on page 233
- [Standard Regular Expression Strings](#) on page 246
- [Supported File Types](#) on page 248

Use Cases for Setting up User Provisioning

Whether you are a new or existing customer, you should plan your approach before performing your first synchronization. This section provides checklists for setting up user provisioning in various use cases. Find yours to determine the best course of action.

- [New Web and/or email customers \(LDAP\)](#)
- [New and existing email customers](#)
- [New Web customers \(SCIM\)](#)
- [Existing Web and/or email customers \(LDAP\)](#)
- [Considerations for existing customers \(LDAP\)](#)
- [Considerations for existing customers \(SCIM\)](#)

Related concepts

[New web and/or email customers \(LDAP\)](#) on page 233
[Existing Web and/or email customers \(LDAP\)](#)
[Considerations for existing customers \(LDAP\)](#)
[Considerations for existing customers \(SCIM\)](#)
[New web and existing email customers](#) on page 237

Related tasks

[New Web customers \(SCIM\)](#) on page 240

New web and/or email customers (LDAP)

For new web and/or email customers, see the following:

- [Synchronizing users/groups with a single Web policy and exceptions](#)

- *Synchronizing users/groups with more than one policy, and planning to manage policy assignment through an LDAP directory*

Related tasks

[Synchronizing users/groups with a single Web policy and exceptions](#) on page 234

[Synchronizing users/groups with more than one policy, and planning to manage policy assignment through an LDAP directory](#) on page 235

Synchronizing users/groups with a single Web policy and exceptions

Steps

- 1) Plan the cloud data structure: users and groups (See *Groups*), policies (See *Defining Web Policies*) and exceptions. (See *Exceptions*).
- 2) Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed cloud data structure more closely.
- 3) Download the client and install it on the target client machine.
- 4) Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file (ensure NTLM ID is included). (See the [Directory Synchronization Client Administrator's Guide](#) for instructions). Review the results and modify the search as necessary to ensure it returns expected results.
- 5) In the cloud manager, set up a contact with Directory Synchronization permissions. (See *Set up authentication (Directory Synchronization only)*). This will be the username/logon used for the Directory Synchronization Client to log onto the portal.
- 6) Decide whether email will be sent after new users are synchronized from LDAP.
- 7) Now you are ready! In the cloud manager, enable Directory Synchronization. (See *Configure identity management*).
- 8) In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#)).
- 9) During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- 10) Log onto the cloud manager. Using **Account > End Users** and **Account > Groups**, check that users' and groups' policies are as expected. (See *View and manage user data*).

- 11) On the Identity Management page, view Recent Directory Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See *View recent directory synchronizations*).
- 12) If you are planning to set up exceptions based on group membership, do this now in the cloud manager. (See *Exceptions*).
- 13) The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See *Restore directories*).
- 14) If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Related concepts

Groups on page 27

Exceptions

Related tasks

Set up authentication (Directory Synchronization only)

Configure identity management

View and manage user data

Restore directories

Related reference

View recent directory synchronizations

Related information

Defining Web Policies

Synchronizing users/groups with more than one policy, and planning to manage policy assignment through an LDAP directory

Steps

- 1) Plan the cloud data structure: users and groups (See *Groups*), policies (See *Defining Web Policies*) and exceptions. (See *Exceptions*). Create an extra policy or policies as required.
- 2) Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed cloud data structure more closely.
- 3) Download the client and install it on the target client machine.

- 4) Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file (ensure NTLM ID is included). (See the [Directory Synchronization Client Administrator's Guide](#) for instructions). Review the results and modify the search as necessary to ensure it returns expected results.
- 5) In the cloud manager, set up a contact with Directory Synchronization permissions. (See Set up authentication (Directory Synchronization only)). This will be the username/logon used for the Directory Synchronization Client logs into the cloud manager.
- 6) Decide whether email will be sent after new users are synchronized from LDAP.
- 7) Now you are ready! In the cloud manager, enable Directory Synchronization. (See *Configure identity management*).
- 8) In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#)).
- 9) During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- 10) Log onto the cloud manager. Using **Account > End Users** and **Account > Groups**, check that users' and groups' policies are as expected. (See *View and manage user data*).
- 11) On the Identity Management page, view Recent Directory Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See *View recent directory synchronizations*).
- 12) Go to each policy in turn, and set up the group/policy assignments. This moves users to the appropriate policies. (See *Assign a group to a different policy*).
- 13) Go to the Identity Management configuration page and check that the default policy setting is correct.
- 14) Return to the **Account > End Users** page and check that users are in the correct policies.
- 15) If you are planning to set up exceptions based on group membership, do this now in the cloud manager. (See *Exceptions*).
- 16) The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See *Restore directories*).
- 17) If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Related concepts[Groups on page 27](#)[Exceptions](#)

Related tasks

Set up authentication (Directory Synchronization only)
Configure identity management
View and manage user data
Restore directories

Related reference

View recent directory synchronizations

Related information

Defining Web Policies

New web and existing email customers

For Forcepoint Email Security Cloud customers, see the following:

- *Synchronizing email addresses to provide a “allowlist” of valid email addresses*
- *Synchronizing users/groups to provide per-user/per-group exceptions to email policies*

Related tasks

Synchronizing email addresses to provide a “allowlist” of valid email addresses on page 237
Synchronizing users/groups to provide per-user/per-group exceptions to email policies on page 238

Synchronizing email addresses to provide a “allowlist” of valid email addresses

Steps

- 1) Review the existing LDAP/Active Directory data structure and decide how to search for all relevant email addresses.
- 2) Download the client and install it on the target client machine.
- 3) Configure the Directory Synchronization Client to search the LDAP directory and extract groups and extract email addresses to a local file. (See the [Directory Synchronization Client Administrator’s Guide](#) for instructions). Review the results and modify the search as necessary to ensure it returns expected results.
- 4) In the cloud manager, set up a contact with Directory Synchronization permissions. (See *Set up authentication (Directory Synchronization only)*). This will be the username/logon used for the Directory Synchronization Client to log onto the cloud manager.

- 5) In the cloud manager, enable Directory Synchronization. (See *Configure identity management*). Make sure “Reject mail for unknown users” is not enabled. (Turn this on only when you are sure the mail list is synchronized and correct).
- 6) In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator’s Guide](#)).
- 7) During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- 8) Go to the cloud manager, Configure Directory Synchronization page and download a CSV file of email addresses. (See *Configure identity management*) Check if these are correct, perhaps by comparing them against a known list from Active Directory.
- 9) On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See *View recent synchronizations*).
- 10) If everything appears to be working, go to the Configure Directory Synchronization page again and select **Reject mail for unknown users**. Email address filtering is now live.
- 11) Set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool. If there is a problem with the first scheduled synchronization, you can restore the directory to its previous version. See *Restore directories*.

Related tasks

[Set up authentication \(Directory Synchronization only\)](#)
[Configure identity management](#)
[Restore directories](#)

Related reference

[View recent directory synchronizations](#)

Synchronizing users/groups to provide per-user/per-group exceptions to email policies

Steps

- 1) Plan the cloud data structure: users and groups (*Groups*), policies (*Defining Email Policies*) and exceptions.
- 2) Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed cloud data structure more closely.
- 3) Download the client and install it on the target client machine.

- 4) Configure the Directory Synchronization Client to search the LDAP directory and extract groups and extract email addresses to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions). Review the results and modify the search as necessary to ensure it returns expected results.
- 5) In the cloud manager, set up a contact with Directory Synchronization permissions. (See *Set up authentication (Directory Synchronization only)*). This will be the username/logon used for the Directory Synchronization Client to log onto the cloud manager.
- 6) Decide whether email will be sent after new users are synchronized from LDAP.
- 7) Now you are ready! In the cloud manager, enable Directory Synchronization. (See *Configure identity management*).
- 8) In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#)).
- 9) During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- 10) Log onto the cloud manager. Using **Account > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See *View and manage user data*).
- 11) On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See *View recent synchronizations*).
- 12) If you are planning to set up per-user/per-group configurations for Antispam, Antivirus or Content Filter in email policies then do it now. Use the **per-user** link on each of these tabs to configure custom rules for each user or group. (You can enter user or group names into the per-user dialogs.) Refer to *Configuring Email Settings*, for more information on per-user configuration options.
- 13) The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See *Restore directories*).
- 14) If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Related concepts

[Groups on page 27](#)

Related tasks

[Set up authentication \(Directory Synchronization only\)](#)

[Configure identity management](#)

[View and manage user data](#)

[Restore directories](#)

Related reference

[View recent directory synchronizations](#)

Related information

[Configuring Email Settings](#) on page 51

[Defining Email Policies](#) on page 75

New Web customers (SCIM)

For new web and/or email customers using System for Cross-domain Identity Management (SCIM), see the following when synchronizing users/groups with Web policies and exceptions.

Steps

- 1) Plan the cloud data structure: users and groups (See *Groups*), policies (See *Defining Web Policies*) and exceptions. (See *Exceptions*).
- 2) In the cloud manager, configure SCIM. (See *Synchronizing with SCIM*).
- 3) In the identity provider, provision a new application. It is assumed that the SCIM identity provider is already populated with users and groups.
- 4) Synchronize user and group information from the identity provides. (See *Configure identity management*).
- 5) If you have more than one Web policy, go to each policy and assign groups to it (See *Assign a group to a different policy*).
- 6) Log onto the cloud manager. Using **Account > End Users** and **Account > Groups**, check that users' and groups' policies are as expected. (See *View and manage user data*).
- 7) If you are planning to set up exceptions based on group membership, do this now in the cloud manager. (See *Exceptions*).
- 8) On the **Account > Audit Trail** page, confirm that the correct actions have been taken. (See *SCIM audit trail*).

Related concepts

[Groups](#) on page 27

[Exceptions](#)

[Synchronizing with SCIM](#) on page 38

[SCIM audit trail](#) on page 224

Related tasks

Configure identity management
View and manage user data
Assign a group to a different policy

Related information

Defining Web Policies

Existing Web and/or email customers (LDAP)

For existing cloud web and/or email customers, see the following:

- *Wanting to manage users/groups from an LDAP directory*
- *Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal.*

Related tasks

Wanting to manage users/groups from an LDAP directory on page 241
Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal on page 243

Wanting to manage users/groups from an LDAP directory

Steps

- 1) Review the existing cloud data structure, specifically the structure of users, groups, and policies. Go to **Account > End Users** and **Account > Groups** to view groups and users. (See *Groups*). Make sure the structure is still as you require. This is a good opportunity to review and amend the structure. Review the exceptions in the policy. (See *Defining Web Policies*) and exceptions. (See *Exceptions*).
- 2) Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the cloud data more closely.
- 3) Modify cloud and/or LDAP data to match each other as closely as possible. You might do this by creating new LDAP groups with the same name and members as the cloud groups.
- 4) Download the client and install it on the target client machine.
- 5) Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Compare the results against the cloud data, old CSV files, and/or expectations. Modify the search as necessary to ensure it returns expected results.

- 6) Decide whether to allow overwriting of groups of the same names. In the cloud manager, set **Overwrite groups** as necessary. (See *Configure identity management* for information.) If you allow overwriting, LDAP groups then take over existing groups but retaining their structure in policies and exceptions. If you do not overwrite groups, make sure that all groups being synchronized from LDAP have different names than those in the cloud, then change any group-based notification in the cloud manager to the new LDAP names as required.
- 7) If you have more than one Web policy, go to each policy and assign groups to it (See *Assign a group to a different policy*).
- 8) Then on the Identity Management screen, assign users to a default policy and for **User policy assignment**, select **Follow group membership**. With this setting, as users are moved to a different LDAP group, their policy assignment changes in step.
- 9) Decide whether email will be sent after new users are synchronized from LDAP.
- 10) In the cloud manager, set up a contact with Directory Synchronization permissions. (See *Set up authentication (Directory Synchronization only)*). This will be the username/logon used for the Directory Synchronization Client logs into the cloud manager.
- 11) Now you are ready! In the cloud manager, enable Directory Synchronization. (See *Configure identity management*).
- 12) In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#)).
- 13) During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- 14) Log onto the cloud manager. Using **Account > End Users** and **Account > Groups**, check that users' and groups' policies are as expected. (See *View and manage user data*).
- 15) On the Identity Management page, view Recent Directory Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See *View recent directory synchronizations*).
- 16) The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use **Restore** to undo the synchronization data, and try again. (See *Restore directories*).
- 17) If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Related concepts[Groups on page 27](#)[Exceptions](#)

Related tasks

Configure identity management
Assign a group to a different policy
Set up authentication (Directory Synchronization only)
View and manage user data
Restore directories

Related reference

View recent directory synchronizations

Related information

Defining Web Policies

Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal

Steps

- 1) Review the existing cloud data structure, specifically the structure of users, groups, and policies. Go to **Account > End Users** and **Account > Groups** to view groups and users. (See *Groups*). Make sure the structure is still as you require. This is a good opportunity to review and amend the structure.
- 2) Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the cloud data more closely.
- 3) Modify cloud and/or LDAP data to match each other as closely as possible.
- 4) Download the client and install it on the target client machine.
- 5) Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Compare the results against the cloud data, old CSV files, and/or expectations. Modify the search as necessary to ensure it returns expected results.
- 6) Decide whether to allow overwriting of groups of the same names. In the cloud manager, set **Overwrite groups** as necessary. (See *Configure identity management* for information.) If you allow overwriting, LDAP groups then take over existing groups but retaining their structure in policies and exceptions. If you do not overwrite groups, make sure that all groups being synchronized from LDAP have different names than those in the cloud, then change any group-based notification in the cloud manager to the new LDAP names as required.
- 7) If you have more than one Web policy, go to each policy and assign groups to it (See *Assign a group to a different policy*).

- 8) Then on the Identity Management screen, assign users to a default policy and for **User policy assignment**, select **Fixed**. With this setting, new web users are assigned to the web policy when first synchronized into the service. After that you must manage all movement of users between policies in the cloud manager using the Manage Users page. (Group membership is ignored.)
- 9) Decide whether email will be sent after new users are synchronized from LDAP.
- 10) In the cloud manager, set up a contact with Directory Synchronization permissions. (See *Set up authentication (Directory Synchronization only)*). This will be the username/logon used for the Directory Synchronization Client logs into the cloud manager.
- 11) Now you are ready! In the cloud manager, enable Directory Synchronization. (See *Configure identity management*).
- 12) In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#)).
- 13) During a slow period, select **Replace** on the client. Data is synchronized to the cloud manager. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- 14) Log onto the cloud manager. Using **Account > End Users** and **Account > Groups**, check that users' and groups' policies are as expected. (See *View and manage user data*).
- 15) On the Identity Management page, view Recent Directory Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See *View recent directory synchronizations*).
- 16) The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use **Restore** to undo the synchronization data, and try again. (See *Restore directories*).
- 17) If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Related concepts

[Groups on page 27](#)

Related tasks

[Configure identity management](#)

[Assign a group to a different policy](#)

[Set up authentication \(Directory Synchronization only\)](#)

[View and manage user data](#)

[Restore directories](#)

Related reference

[View recent directory synchronizations](#)

Considerations for existing customers (LDAP)

If you have already set up users, groups, passwords, policies, and exceptions in the cloud manager and you want to switch to LDAP synchronization, consider the following:

- You can minimize the impact by carefully matching your LDAP group names and membership to the existing setup. Matching LDAP group names and membership to those already in the cloud service allows existing policy selections and settings to be maintained, as well as existing usernames/passwords where applicable.
- You are responsible for avoiding ambiguous configurations, for example, users belonging to multiple groups which are assigned to different policies. It is up to you to set up groups in the LDAP directories in such a way that ambiguities don't occur. (When there are ambiguities, the service selects the closest group-to-policy assignment for each individual user, taking the first group in alphabetical order where there are multiple assignments at the same hierarchical level.)
- Existing users can retain their passwords and whether you manage users through the portal, LDAP synchronization, or both is completely transparent to them.

Existing Web customers (SCIM)

Steps

- 1) Review the existing cloud data structure, specifically the structure of users, groups, and policies. Go to **Account > End Users** and **Account > Groups** to view groups and users. (See *Groups*). Make sure the structure is still as you require. This is a good opportunity to review and amend the structure.
- 2) In the cloud manager, configure SCIM. (See *Synchronizing with SCIM*).
- 3) In the identity provider, provision a new application. It is assumed that the SCIM identity provider is already populated with users and groups. To populate the identity provider with users and groups already managed by the cloud service, consider provisioning using a CSV file.
 - a) Users
 - i) In the cloud portal, go to **Account > End Users**.
 - ii) Search for all portal-managed users by select **Portal managed** from the **Source** drop-down.
 - iii) Use the **Download results** option at the bottom of the screen to export the results to a CSV file.
 - iv) Import the results into your identity provider.
 - b) Groups (Not supported by Okta.)
 - i) In the cloud portal, go to **Account > Groups**.
 - ii) Click the **Download all portal-managed groups in CSV format** option.
 - iii) Import the results into your identity provider.

- 4) Synchronize user and group information from the identity providers. (See *Configure identity management*).
- 5) Log onto the cloud manager. Using **Account > End Users** and **Account > Groups**, check that users' and groups' policies are as expected. (See *View and manage user data*).
- 6) On the **Account > Audit Trail** page, confirm that the correct actions have been taken. (See *SCIM audit trail*).

Related concepts

[Groups](#) on page 27

[Synchronizing with SCIM](#) on page 38

[SCIM audit trail](#) on page 224

Related tasks

[Configure identity management](#)

[View and manage user data](#)

Considerations for existing customers (SCIM)

If you have already set up users, groups, passwords, policies, and exceptions in the cloud manager and you want to switch to SCIM, consider the following:

- You can minimize the impact by carefully matching your SCIM group names and membership to the existing setup. Matching SCIM group names and membership to those already in the cloud service allows existing policy selections and settings to be maintained, as well as existing usernames/passwords where applicable.
- You are responsible for avoiding ambiguous configurations, for example, users belonging to multiple groups which are assigned to different policies. It is up to you to set up groups in SCIM in such a way that ambiguities don't occur. (When there are ambiguities, the service selects the closest group-to-policy assignment for each individual user, taking the first group in alphabetical order where there are multiple assignments at the same hierarchical level).
- Existing users can retain their cloud web local passwords and whether you manage users through the portal, SCIM, or both is completely transparent to them.

If you are already using Directory Synchronization and would like to switch to SCIM:

- In order to maintain your existing users, ensure that the information for each user contains a synced email address that is equivalent to their UPN. This allows the service to match the user using the email address when it receives SCIM provisioning requests and allows for a seamless move from Directory Synchronization to SCIM.
- If synced email addresses are not possible, a provisioning reset is recommended to avoid user duplication and additional management complexity and overhead. In this case, SCIM users will appear as new users. Note, however, that history reporting information for the directory synchronized users will no longer be available after the reset.

Standard Regular Expression Strings

Regular expressions (RegEx) are a powerful way of matching a sequence of simple characters. You can use regular expressions in Forcepoint Email Security Cloud to create dictionary entries for lexical rules (see *Filtering using lexical rules*).

You can enclose a range of characters in square brackets to match against all of those characters. For example:

Expression	Description
[]	may also be used on a range of characters separated by a – character.
[0-9]	matches any digit.
[a-z]	matches any alpha character
[a-z0-9]	matches any alphanumeric character
^	is the “not” character, so [^0-9] matches against any character that is not a digit.

Although you can use ranges to specify a group of characters, you can also use the following shortcuts:

Expression	Description
.	matches against any character
\d	matches against a digit [0-9]
\D	matches against a non-digit [^0-9]
\s	matches against a whitespace character (such as a tab, space, or line feed character)
\S	matches against a non-whitespace character
\w	matches against an alphanumeric character [a-zA-Z_0-9]
\W	matches against a non-alphanumeric character
\xhh	matches against a control character (for the hexadecimal character hh)
\uhhhh	matches against a Unicode character (for the hexadecimal character hhhh)



Note

As the backslash character is used to denote a specific search expression, if you want to match against this character, you must enter a double backslash (\\).

To match against occurrences of a character or expression, you can use the following:

Expression	Description
*	matches against zero or more occurrences of the previous character or expression
+	matches against one or more occurrences of the previous character or expression
?	matches zero or one occurrences of the previous character or expression
{n}	matches n occurrences of the previous character or expression

Expression	Description
{n,m}	matches from n to m occurrences of the previous character or expression
{n,}	matches at least n occurrences of the previous character or expression

You can provide text to replace all or part of your search string. To do this, you need to group together matches by enclosing them in parentheses so they can be referenced in the replacement. To reference a matched parameter, use \$*n* where *n* is the parameter starting from 1.

Regular expression examples

Example 1: IP address

The following regular expression matches against any IP address:

```
\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b
```

You can test this regex with any phrase including a standard IP address, for example 192.23.44.1.

Example 2: Dates

The following regular expression matches against dates in the format DD-MMMYYYY:

```
\b\d\d?-[w]w[w]-\d\d\d\d\b
```

To test this regex, enter a sentence similar to "The project completes on 14-Feb-2009".

Example 3: Social Security Numbers

The following regular expression matches against Social Security numbers in UK format:

```
\b[w]{2}\d{6}\w\b
```

You can test this regex with any Social Security number in the format XY123456Z.

Related concepts

[Filtering using lexical rules](#) on page 119

Supported File Types

This appendix provides a list of all the file formats and types supported for email attachment blocking and parking.

File format	File type
Compressed and Encoded Formats	Serialized Object Format (SOF) Disk Doubler ZIP Archive PAK/ARC Archive cpio archive (CRC Header) cpio archive (CHR Header) SUN PEX Binary Archive UU encoded Stuffit (MAC) WANG Office GDL Header OLE Compound Document SHAR Unix Compress GZ Compress TAR BinHex SMTP MIME Compactor / Compact Pro PGP Secret Keyring PGP Public Keyring PGP Encrypted Data PGP Signed Data PGP Signed and Encrypted Data PGP Signature Certificate PGP Compressed Data ASCII-armored PGP Public Keyring ASCII-armored PGP encoded MacBinary Apple Single Apple Double Microsoft Outlook Microsoft Outlook PST RAR RAR5 IBM Lotus Notes Database NSF/NTF OpenPGP Message Format (with new packet

File format	File type
	format) LHA Archive IBM Lotus representation of Domino design elements in XML format Legato Extender Native Message ONM Transport Neutral Encapsulation Format (TNEF) Legato EMailXtender Archives Format (EMX) 7 Zip Format (7z) Microsoft Cabinet File (CAB) Group Wise File Surf email (GWFS) Archive by Robert Jung (ARJ) Microsoft Outlook Restricted Permission Message (RPMSG) Microsoft Outlook for Macintosh (OLM) Web ARChive (WARC) ICHITARO compressed B1 archive EDB Internet Calendaring and Scheduling (iCalendar) XZ archive
Database Formats	MORE Database MAC Filemaker MAC SmartWare II (DB) Microsoft Works for MAC Microsoft Works for DOS Microsoft Works for Windows Reflex Borland Reflex 2 Paradox dBase Ability DB Microsoft Access Microsoft Access 95 Microsoft Access 97 Microsoft Access 2000

File format	File type
Desktop Publishing Formats	PageMaker for Macintosh PageMaker for Windows FrameMaker Maker Markup Language Quark Xpress MAC Microsoft Publisher
Executable Formats	MS-DOS Batch File SDOS/Windows Program DOS/Windows Object Library Unix Executable (PDP-11/pre-System V VAX) Unix Executable (Basic-16) Unix Executable (x86) Unix Executable (iAPX 286) Unix Executable (MC680x0) Unix Executable (3B20) Unix Executable (WE32000) Unix Executable (VAX) Unix Executable (Bell 5.0) Unix Object Module (VAX Demand) Unix Object Module (old MS 8086) Unix Object Module (Z8000) DOS/Windows Object Module PC (.COM) MSDOS Device Driver ELF Relocatable ELF Executable ELF Dynamic Library Java Class format (CLASS)

File format	File type
High-End Graphics	Corel Draw Computer Graphics Metafile (CGM) Lotus PIC PostScript Windows Metafile (no header) Freehand MAC HP Graphics Language AutoCAD DXF OS/2 PM Metafile Lasergraphics Language AutoShade Rendering GEM VDI HP Printer Control Language VRML QuickDraw 3D Metafile Corel CMX AutoDesk Drawing (DWG) AutoDesk WHIP Micrografx Designer Simple Vector Format (SVF) Enhanced Metafile Microsoft Office Drawing DeVice Independent file (DVI) Harvard Graphics Chart Harvard Graphics Symbol File Harvard Graphics Configuration File Harvard Graphics Palette Intergraph Standard File Format (ISFF) V7 DGN (non-OLE) MicroStation V8 DGN (OLE) CADAM Drawing CADAM Drawing Overlay NURSTOR Drawing HP Graphics Language (Plotter) CATIA Formats (CAT*) ODF Drawing

File format	File type
Other Formats	SmartWare II (Other) Microsoft Works for MAC Framework Framework II WordPerfect auxiliary file Windows Help File Ability Other NeWS bitmap font SUN vfont Definition Windows Group TrueType Font Program Information File (PIF) Windows C++ Object Storage FTP Session Data Netscape Bookmark File Office 2007 document Unknown binary Advanced Systems Format (ASF) Yahoo! Messenger chat log (YCHAT) MATLAB file format (MAT, FIG) SEG-Y Seismic Data format (SGY, SEGY) Microsoft Windows NT Event Log (EVT) Microsoft Windows Vista Event Log (EVTX)

File format	File type
Presentations	PowerPoint PC PowerPoint MAC PowerPoint 95 PowerPoint 97 Persuasion Applix Graphics Lotus Freelance for DOS Lotus Freelance for Windows Lotus Freelance for OS/2 Lotus Freelance 96 Lotus Freelance 97 Corel Presentations Harvard Graphics Microsoft PowerPoint 2000 Microsoft Visio Microsoft Visio 2013 Microsoft Visio 2013 macro Microsoft Visio 2013 stencil Microsoft Visio 2013 stencil macro Microsoft Visio 2013 template Microsoft Visio 2013 template macro Microsoft PPT 2007 XML Microsoft PPT Macro 2007 XML ODF Presentation Apple iWork Keynote format
Scheduling/Planning	Microsoft Project PlanPerfect Microsoft Project 4 Microsoft Project 4.1 Microsoft Project 98 Microsoft Project 2000

File format	File type
Sound	Microsoft Wave MIDI NeXT/Sun Audio Data RIFF MIDI Audio Interchange File Format (AIFF) Amiga MOD Amiga IFF (8SVX) Sound Creative Voice (VOC) MPEG Audio Real Audio Window Media Audio Format (WMA) Conifer Wavpack Sony Wave64 Xiph Ogg Vorbis

File format	File type
Spreadsheets	Multiplan (PC) Multiplan (Mac) SYLK Symphony Uniplex Ucalc Data Interchange Format (DIF) Enable Spreadsheet Supercalc UltraCalc SmartWare II (Spreadsheet) Microsoft Works for MAC Microsoft Works for Windows Quattro Pro for DOS Quattro Pro for Windows Ability Spreadsheet CSV (Comma Separated Values) PeachCalc Lotus 1-2-3 Lotus 1-2-3 Formatting Lotus 1-2-3 97 Microsoft Excel Microsoft Excel 95 Microsoft Excel 97 Lotus 1-2-3 Release 9 Applix Spreadsheets Microsoft Excel 2000 Microsoft Excel 2007 XML Microsoft Excel Macro 2007 XML ODF Spreadsheet Microsoft Excel Binary 2007 Quattro Pro 9+ for Windows Apple iWork Numbers format Apple iWork 2013 Numbers

File format	File type
Standard Graphics	Windows Bitmap Encapsulated PostScript CCITT G3 1D Graphics Interchange Format (GIF87a) Graphics Interchange Format (GIF89a) GEM Bit Image Sun Raster MacPaint PC Paintbrush Graphics (PCX) QuickDraw Picture Lotus Ami Pro Draw Targa TIFF Windows Metafile WordPerfect Graphics JPEG Interchange Format Windows Icon Format Windows Cursor Ability Image Curses Screen Image DCX FAX Format (PCX images) Lotus Notes Bitmap Portable Network Graphics (PNG) Windows Animated Cursor Windows Palette RIFF Device Independent Bitmap OLE DIB object SGI Image MS Windows Device Independent Bitmap Portable Bitmap Utilities ASCII Format Portable Bitmap Utilities Binary Format Portable Greymap Utilities ASCII Format Portable Greymap Utilities Binary Format Portable Pixmap Utilities ASCII Format Portable Pixmap Utilities Binary Format X Bitmap Format X Pixmap Format

File format	File type
	FPX Format PCD Format Microsoft Document Imaging Format PaperPort image file (MAX)
Text	EBCDIC Text HTML Text
Vector Graphics	Windows Draw (Micrografx)
Videos	Video for Windows (AVI) RIFF Multimedia Movie MPEG Movie QuickTime Movie AutoDesk Animator FLIC AutoDesk Animator Pro FLIC Lotus ScreenCam Macromedia Director Window Media Video Format (WMV) MPEG-PS container with CDXA stream (MPG) ISO/IEC MPEG-4

File format	File type
Word Processing	Multiplus (AES) APPLIX ASTERIX Convergent Technologies DEF Comm. Format Word Connection COMET TOP CEOwrite DSA101 (Honeywell Bull) DCA-RFT (IBM Revisable Form) CDA / DDIF DG Common Data Stream (CDS) Vistaword DECdx Enable Word Processing HP Word PC IBM 1403 Line Printer DCF Script DCA-FFT (IBM Final Form) Interleaf Display Write Lotus Ami Pro Lotus Ami Pro Style Sheet Lyrix Word Processing MASS-11 Microsoft Word for Macintosh Microsoft Word for Windows MultiMate MultiMate Footnote File MultiMate Advantage MultiMate Advantage Footnote File MultiMate Advantage II MultiMate Advantage II Footnote File Rich Text Format (RTF) Microsoft Word for PC Microsoft Word for PC Style Sheet Microsoft Word for PC Glossary Microsoft Word for PC Driver Microsoft Word for PC Miscellaneous File

File format	File type
	NBI Async Archive Format
	Navy DIF
	NBI Net Archive Format
	NIOS TOP
	OLIDIF (Olivetti)
	Office Writer
	CPT
	Philips Script
	PRIMEWORD
	Q-One V1.93J
	Q-One V2.0
	SAMNA Word
	SmartWare II (WP)
	Targon Word
	Uniplex
	Microsoft Word UNIX
	WANG PC
	WordERA
	WANG WPS
	WordPerfect MAC
	WordPerfect
	WordPerfect VAX
	WordPerfect Macro
	WordPerfect Spelling Dictionary
	WordPerfect Thesaurus
	WordPerfect Resource File
	WordPerfect Driver
	WordPerfect Configuration File
	WordPerfect Hyphenation Dictionary
	WordPerfect Miscellaneous File
	WordMARC
	WordStar
	WANG WITA
	Xerox 860
	Xerox Writer
	Microsoft Works for MAC
	Microsoft Works for DOS

File format	File type
	Microsoft Works for Windows
	MacWrite
	MacWrite II
	Maker Interchange Format (MIF)
	Windows Write
	Volkswriter
	Ability WP
	XYWrite / Nota Bene
	IBM Writing Assistant
	WordStar 2000
	WriteNow MAC
	Q & A for DOS
	Q & A for Windows
	WPS-PLUS
	DCS
	Lotus Notes CDF
	ODA / ODIF
	ALIS
	Envoy
	Portable Document Format
	USENET
	SGML
	ACT
	Applix Words
	XML
	Unicode
	Lotus Word Pro 96
	Lotus Word Pro 97
	Microsoft Word 95
	Microsoft Word 97
	Microsoft Pocket Word
	Microsoft Word 2000
	Folio Flat File
	HWP(Arae-Ah Hangul)
	ICHITARO V4-10
	Verity XML
	Oasys format

File format	File type
	Microsoft Word 2003 XML Microsoft Excel 2003 XML Microsoft Visio 2003 XML StarOffice Text XML StarOffice Spreadsheet XML StarOffice Presentation XML XHTML SWF Microsoft Word 2007 XML Microsoft Word Macro 2007 XML Microsoft XML Paper Specification(XPS) ODF Text Yahoo! Instant Messenger History Founder Chinese E-paper Basic (ceb) MHT format Microsoft Office Groove Format Apple iWork Pages format Apple iWork 2013 Pages Windows Journal format (JNT) PKCS #12 VCF file

