



# Web Security Cloud

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 21 August 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

<b>1 Getting Started</b> .....	7
Introduction.....	7
Initial steps.....	8
Logging on and portal security.....	8
Cloud Web setup.....	10
Using the Resource Center.....	16
Navigating the cloud portal.....	17
Cloud portal dashboards.....	19
Alerts.....	25
<b>2 Account Settings</b> .....	27
Introduction.....	27
My Account.....	28
Configuring SIEM storage.....	28
Contacts.....	30
Identity Management.....	41
End Users.....	41
Groups.....	42
Licenses.....	43
Administrator single sign-on.....	44
Privacy protection.....	47
Data Protection Settings.....	48
Important rules for configuring accounts.....	50
<b>3 Working with External Directories</b> .....	51
Introduction.....	51
What is SCIM?.....	52
How the service works with SCIM.....	52
What is LDAP?.....	53
How the service works with LDAP.....	53
Planning for your first synchronization.....	54
Basic steps.....	57
Cloud portal tasks.....	58
Maintenance.....	63
<b>4 Configuring Web Settings</b> .....	69
Introduction.....	69
Configure General settings.....	70
Configure Remote Browser Isolation.....	76
Configure File Sandboxing settings.....	77
Configure End User Single Sign-On settings.....	80
Configure Bypass Settings.....	81
Configure Domain settings.....	89
Configure Endpoint settings.....	91
Configure protected cloud apps.....	109
Configure Full Traffic Logging settings.....	111
Configure custom categories.....	112
Time periods.....	115

Configure custom protocols.....	117
Configure block and notification pages.....	118
Configure Content Classifiers for Data Security (DLP Lite).....	126
<b>5 Managing Network Devices.....</b>	<b>133</b>
Introduction.....	133
Global options.....	133
Managing edge devices.....	135
Generating device certificates.....	144
Managing EasyConnect services.....	146
Managing I Series appliances.....	148
<b>6 Defining Web Policies.....</b>	<b>159</b>
Introduction.....	159
Creating a new policy.....	160
Testing policy enforcement.....	162
Uploading a policy assignment file.....	163
General tab.....	163
Connections tab.....	168
Access Control tab.....	171
Endpoint tab.....	178
End Users tab.....	180
Cloud Apps tab.....	188
Custom Categories tab.....	191
Web Categories tab.....	193
Protocols tab.....	204
Application Control tab.....	205
File Blocking tab.....	207
Data Protection tab.....	212
Data Security tab (DLP Lite).....	213
Web Content & Security tab.....	217
<b>7 Report Center.....</b>	<b>223</b>
Introduction.....	223
Using the Report Catalog.....	224
Using the Report Builder.....	231
Scheduling reports.....	236
Exporting data to a third-party SIEM tool.....	239
<b>8 Web Reporting Tools.....</b>	<b>247</b>
Introduction.....	247
Using the Transaction Viewer.....	248
Using the Incident Manager.....	249
Report attributes: Web and Data Security.....	250
Report metrics: Web and Data Security.....	264
Web predefined reports.....	265
<b>9 Account Reports.....</b>	<b>275</b>
Introduction.....	275
Endpoint Auditing Report (Classic Proxy Connect and Direct Connect).....	276
Service reports.....	276
Downloading report results.....	277
Saving reports.....	278

Scheduling reports.....	278
<b>10 Audit Trails.....</b>	<b>281</b>
Introduction.....	281
Configuration audit trail.....	281
SCIM audit trail.....	282
<b>11 Standard Web Configuration.....</b>	<b>283</b>
Overview.....	283
<b>Appendices.....</b>	<b>287</b>
<b>A Use Cases for Setting up User Provisioning.....</b>	<b>289</b>
New Web and/or email customers (LDAP).....	289
New Web customers (SCIM).....	293
Existing Web and/or email customers (LDAP).....	294
Existing Web customers (SCIM).....	298
<b>B Data Security Content Classifiers (DLP Lite only).....</b>	<b>301</b>
Personally Identifiable Information (PII).....	301
Protected Health Information (PHI).....	313
Payment Card Industry (PCI).....	315
Data Theft.....	315



## Chapter 1

# Getting Started

### Contents

- [Introduction](#) on page 7
- [Initial steps](#) on page 8
- [Logging on and portal security](#) on page 8
- [Cloud Web setup](#) on page 10
- [Using the Resource Center](#) on page 16
- [Navigating the cloud portal](#) on page 17
- [Cloud portal dashboards](#) on page 19
- [Alerts](#) on page 25

## Introduction

---

Cloud web protection products protect your organization against the threats of malware, spam, and other unwanted content in web traffic.

The following web products are available in the cloud:

- Forcepoint URL Filtering offers malware protection and customizable web content categories, enabling you to create highly granular acceptable use policies.
- Forcepoint Web Security Cloud includes the above features, plus real-time security analysis, real-time content classification, detection of inappropriate content in dynamic websites, granular configuration for social web controls, and SSL decryption by category.

The cloud service offers the following add-ons for web products:

- The I Series appliance is an add-on to Forcepoint Web Security Cloud, and provides on-premises URL analysis and application/protocol detection for web traffic, along with centralized policy management and reporting capabilities in the cloud. When policy indicates that a request requires additional analysis, it is transparently routed to the cloud, where cloud analytics are applied and policy is enforced.
- The Advanced Malware Detection for Web module enables you to send suspicious files to a cloud-hosted sandbox for further analysis.

You configure and administer these services using the Forcepoint Cloud Security Gateway Portal, also referred to in this Help as the Security Portal, or the cloud portal. The portal provides a central, graphical interface to the general configuration, policy management, and reporting functions of your web protection service, making it easy to define and enforce web security.

To get started, see the below topics:

### Related concepts

- [Logging on and portal security](#) on page 8
- [Navigating the cloud portal](#) on page 17

**Related tasks**

[Initial steps](#) on page 8

# Initial steps

If you have not already done so, take the following steps to get started. If you are not able to complete all of the in-network configuration steps immediately, you can complete them after you perform the cloud portal configuration steps.

## Steps

- 1) Configure your firewall to allow connectivity to the cloud service.  
See *Configuring your firewall to connect to the cloud service*.
- 2) Log on to the Security Portal.  
See *Logging on and portal security* for instructions.
- 3) Add your Internet gateway IP addresses to your policy. See *Proxied connections* for instructions.
- 4) Configure end-user authentication (if required).

## Next steps

If you have not already completed these steps, please see the [Getting Started Guide](#) for detailed instructions.

**Related concepts**

[Logging on and portal security](#) on page 8

[Proxied connections](#) on page 168

**Related reference**

[Configuring your firewall to connect to the cloud service](#) on page 10

# Logging on and portal security

**Note**

To use the Security Portal, your browser must have JavaScript enabled.

To access the portal, visit <https://admin.forcepoint.net/portal>. (For tips on navigating the portal, see *Navigating the cloud portal*.)



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

If the 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 portal perceives 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.

### Related concepts

[Navigating the cloud portal](#) on page 17

## Privacy statement

---

The 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 your cloud service account and are inactive for a pre-defined 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 area of the portal 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**.

### Next steps

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

# Cloud Web setup

Setting up cloud web involves a combination of steps performed in your network (to allow communication with the cloud service) and steps performed in the cloud portal (policy configuration).

If you are not able to complete all of the in-network configuration steps immediately, you can complete them after you perform the cloud portal configuration steps.

## Related concepts

[Sending end user information to the cloud service](#) on page 11

[Configuring SCIM](#) on page 12

[Configuring the Directory Synchronization Client](#) on page 12

[Adding users manually](#) on page 12

[Directing user traffic to the cloud service](#) on page 14

[Finishing the setup \(next steps\)](#) on page 16

## Related tasks

[Setting up your first policy](#) on page 13

[Configuring policy connections](#) on page 13

[Adding end users](#) on page 14

## Related reference

[Configuring your firewall to connect to the cloud service](#) on page 10

## Configuring your firewall to connect to the cloud service

In order for the cloud service to manage web traffic from your network, your firewall must allow TCP connections outbound to Forcepoint data centers on specific ports. The table below details the ports that may be used, depending on your configuration.

Port	Required for
8081	Web browsing when using standard PAC file addresses.
8082 (default)	Retrieving cloud service PAC files (standard PAC file address).
8087 (default)	Retrieving cloud service PAC file over HTTPS (standard PAC file address).
8006	End user single sign-on authentication. See <i>Configure End User Single Sign-On settings</i> .
8089	Secure form authentication. See <i>Access Control tab</i> .

Port	Required for
80	<ul style="list-style-type: none"> <li>Retrieving cloud service PAC files via the alternate PAC file address.</li> <li>Web browsing when using the alternate PAC file address.</li> </ul>
443	<ul style="list-style-type: none"> <li>Retrieving cloud service PAC files securely via the alternate HTTPS PAC file address.</li> </ul>



#### Tip

To guarantee availability, Forcepoint Web Security Cloud uses global load balancing to direct traffic across multiple geographic locations. In the event of localized connectivity issues, data center load balancing automatically routes requests to the next closest location. To make the most of the resilience offered by this infrastructure, users must be allowed to connect to the entire cloud network.

For details of the IP address ranges in use by cloud service data centers, see the article [Cloud service IP addresses and port numbers](#) in the Forcepoint Knowledge Base.

In addition to the above, ports 80 and 443 can be used by:

- Block and notification page components, including stylesheets and images, served from a separate website used by the cloud infrastructure (not directly through the cloud proxy).
- Non-proxied destinations. IP addresses and domains configured using the Proxy Bypass setting are configured to route directly to the origin server. Browsers will connect directly via port 80 (or 443 for HTTPS).
- The roaming home page. Although this service is principally for remote users, you may choose to configure all browsers to use this as their home page. This page is always unproxied when using cloud service PAC files.
- The proxy query page. Users can access a query page to find out whether their browser settings are correct for accessing the proxy.



#### Note

Remote users should use the alternate PAC file addresses (using port 80 or 443) if requesting access from networks that may have port 8081, 8082, or 8087 locked down.

#### Related concepts

[Access Control tab](#) on page 171

#### Related tasks

[Configure End User Single Sign-On settings](#) on page 80

## Sending end user information to the cloud service

End user information can be sent to the cloud service in one of 3 ways:

- Use System for Cross-domain Identity Management (SCIM) (recommended when using a cloud directory service) to provision user and group identity data from a cloud-based identity provider to the cloud service. See *Configuring SCIM*.
- **Directory synchronization** (recommended when using a private Active Directory or LDAP) involves installing the Directory Synchronization Client in your network and configuring it to synchronize user and group information from your LDAP directory to the cloud service. See *Configuring the Directory Synchronization Client*.
- Manually enter end user information (name, email address, and NTLM identity) to use in testing. User details are added to policies using the End Users tab options. See *Adding users manually*.

#### Related concepts

[Configuring SCIM](#) on page 12

[Configuring the Directory Synchronization Client](#) on page 12

[Adding users manually](#) on page 12

## Configuring SCIM

Your identity provider must be configured to work with the cloud service so that user and group data can be synchronized from the provider. See *Configure identity management* for more details.



#### Note

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

#### Related tasks

[Configure identity management](#) on page 59

## Configuring the Directory Synchronization Client

To enable directory synchronization between your LDAP directory and the cloud service, start by creating a contact with Directory Synchronization permissions. The user name and password will be used by the Directory Synchronization Client to connect to the cloud service.

Refer to the [Directory Synchronization Client Administrator's Guide](#) for further information, including how to download and configure the client software.

## Adding users manually

User accounts that you plan to use for testing can be added when a new policy is added. See the step for *Adding end users* when setting up a policy.

#### Related tasks

[Adding end users](#) on page 14

# Setting up your first policy

Use the **Web > Policy Management > Policies** page to create a basic policy to determine which websites can and cannot be accessed by users whose traffic is managed by the cloud service.

This process walks you through creating a very basic policy that you can customize later if necessary. See *Creating a new policy* for complete instructions and details.

## Steps

- 1) Click **Add**.
- 2) Enter a policy name and administrator email address. This email address is used as the address from which system messages are sent.
- 3) Select a pre-defined policy template to use as the basis for your new policy:
  - **Default** blocks access to sites in commonly blocked categories, like Adult Material, Gambling, and sites that present a security risk, while permitting access to sites commonly used for business or educational purposes.
  - **Basic** blocks the most frequently blocked categories and permits the rest.
  - **Security only** blocks only sites that present a security risk (like phishing- related sites or sites that host malware) and permits access to all others.
  - **Monitor only** does not block any websites, but does log user activity for use in reporting.
- 4) Select a **Time zone** for this policy. This may be used both for time-based policy enforcement and reporting log records.
- 5) When you are finished, click **Save**.

### Related tasks

[Creating a new policy](#) on page 160

# Configuring policy connections

When the page re-displays, click **Connections** and use the options on that page to identify the traffic originating from your organization that should be managed by the policy that you are creating.

Each connection added to **Proxied Connections** is a public-facing IP address, range, or subnet for the gateway through which users' traffic reaches the Internet.

To get started, click **Add** under Proxied Connections, then:

## Steps

- 1) Enter a unique **Name** and **Description** for the connection.
- 2) Select a connection **Type**: IP address, IP address range, or subnet.
- 3) Enter the connection definition for the type that you selected.

- 4) Optionally, select a **Time zone** for this connection. If no time zone is selected, the time zone defined for the policy as a whole is used.
- 5) Click **Continue** to save your change and return to the Connections tab.

## Next steps

Repeat this process for each connection that you want to define for this policy.

# Adding end users

---

The **End Users** tab is where all end-user registration configuration is performed. Registration is a method of getting user credentials into your cloud service account.

To get started with this new policy, select **Invite an end-user** in the User Management section.

## Steps

- 1) In the Name field, enter the user's display name (for example, Jane Doe).
- 2) Enter the user's **Email address** (for example, jdoe@mydomain.com)..
- 3) Enter the user's **NTLM identity** (for example, mydomain/jdoe).
- 4) Click **OK**.

## Next steps

Repeat this process as needed.

To remove an account entry, mark the check box next to the user name and click **Delete**.

# Directing user traffic to the cloud service

---

Use the **Default Pac file addresses** on the **Web > Settings > General page** to get the information you need to use a PAC file to direct user traffic from your network to the cloud service.

Perform the following steps on a machine that is inside the network that you defined as a connection in the previous step. This may optionally be the same machine that you are using.

## Configure Chrome to use the PAC file

---

### Steps

- 1) Open Chrome on the selected machine.
- 2) Open the **Settings** menu.
- 3) Click the **Advanced Settings** link, then scroll down to the **Network** section.

- 4) Click **Change proxy settings**. This opens an Internet Explorer dialog box to the Connections tab.
- 5) Click **LAN Settings**.
- 6) Mark the **Use automatic configuration script** check box, then paste the URL from the portal page in the address field.
- 7) Click **OK** twice to close the dialog box.

## Configure Internet Explorer to use the PAC file

---

### Steps

- 1) Open Internet Explorer on the selected machine.
- 2) Open the **Internet options** menu.
- 3) Select the **Connections** tab, then click **LAN Settings**.
- 4) In the settings dialog box, mark the **Use automatic configuration script** check box and paste the URL from the portal page in the address field.
- 5) Click **OK** twice to close the dialog box.

## Configure Firefox to use the PAC file

---

### Steps

- 1) Open Firefox on the selected machine.
- 2) Open the **Options** menu.
- 3) Select the **Advanced > Network** tab.
- 4) Click **Settings**, in the Connection section at the top of the tab.
- 5) Select **Automatic proxy configuration URL** and paste in the URL from the portal page.
- 6) Click **OK**.

## Finishing the setup (next steps)

After completing the initial setup, you have the basic setup needed to test and start becoming familiar with your cloud web protection solution. Use the Help system you are reading right now or the Resource Center options (See *Using the Resource Center*) to help you:

- Become familiar with the portal (see *Navigating the cloud portal*).
- Use dashboards to monitor overall system health and activity (see *Cloud portal dashboards* and *Alerts*).
- View, create, and manage policies (see *Defining Web Policies*).
- Set up SSL decryption so that your web protection product can analyze secure traffic (see *Web Categories tab*).
- Configure data privacy options.
- Report on enforcement activity (see *Report Center*).

The *Getting Started Guide* can provide more details about the initial process of configuring the cloud service. It also includes information about methods other than PAC file redirection for sending traffic to the cloud service.

### Related concepts

[Web Categories tab](#) on page 193

[Using the Resource Center](#) on page 16

[Navigating the cloud portal](#) on page 17

[Cloud portal dashboards](#) on page 19

### Related information

[Defining Web Policies](#) on page 159

[Report Center](#) on page 223

## Using the Resource Center

The Cloud Security Gateway portal provides a Resource Center that offers users various forms of assistance with product configuration and routine tasks.

As you navigate through the portal (see: *Navigating the cloud portal*), click **Resource Center** in the lower right of each portal page to open a list of context-sensitive selections. Depending on the page in use, one or more of the following is offered:

- Resources Related to This Page.
- Forcepoint Remote Browser Integration.
- Remote Browser Isolation Powered by Ericom.
- Forcepoint Security manager and CASB integration Tasks.
- Reporting Documentation.
- Email Security Cloud Product Documentation.

These lists may include how-to guides, videos, or links to documentation related to the tasks to be performed on the current portal page.

The following appear for every portal page:



- **Web Security Cloud Product Documentation**  
This sections offers links to product documents and guides.

- **Useful Links**

Links to Forcepoint Technical Support and other training resources are provided.

New options are added to the Resource Center as they become available.

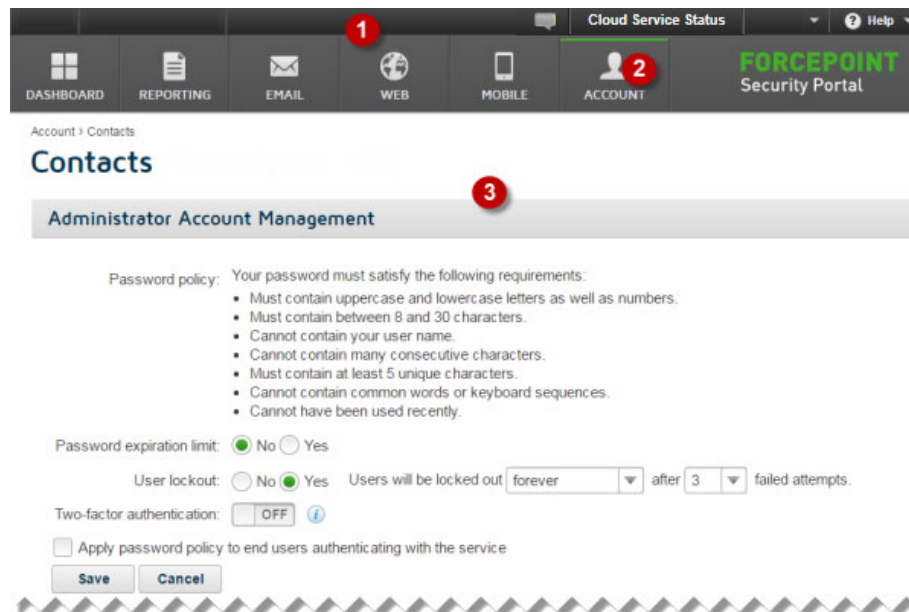
When you're finished reviewing the lists, use the X in the upper right to close the window. The Resource Center option re-displays on the page.

### Related concepts

[Navigating the cloud portal](#) on page 17

# Navigating the cloud portal

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

Each PIN is unique per portal 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 portal 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 threat, productivity, and bandwidth dashboards. See *Cloud portal dashboards*.
- **Reporting** gives access to all reporting options, including account service reports, your saved reports, and the Report Catalog and Report Builder. See *Report Center*.
- **Web** contains all configuration settings relating to your web protection product, including account-wide web settings, policy management, access to endpoint and end user single sign-on configuration, and management of devices in your network that connect to the cloud service. To manage appliances, your subscription must include the I Series appliance. See:
  - *Configuring Web Settings*
  - *Defining Web Policies*.
- **CASB**, available when the Protected Cloud Apps feature has been purchased and enabled, opens the Forcepoint CASB portal.
  - Users with account level **Modify configuration** permissions are logged in to the portal. (See *Configuring permissions*.)
  - All other users are required to provide login credentials to access the portal. See *Configure protected cloud apps* for more information.
- **Account** provides access to configuration options that apply to all cloud services. This includes administrator management, identity management, licenses, and groups. See *Account Settings*.

When you select an item in the toolbar, a **navigation pane** drop-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

[Cloud portal dashboards](#) on page 19

#### Related tasks

[Configuring permissions](#) on page 32

[Configure protected cloud apps](#) on page 109

#### Related reference

[Alerts](#) on page 25

**Related information**

[Report Center](#) on page 223

[Configuring Web Settings](#) on page 69

[Defining Web Policies](#) on page 159

[Account Settings](#) on page 27

# Cloud portal dashboards

Click **Dashboard** in the cloud portal toolbar to see a snapshot view of how the cloud service is performing. It includes the following tabs:


- The **Threat Dashboard** appears when you first access this page. It shows information about suspicious activity that may be related to malware threats in your network. See *Threat Dashboard*.
- The **Bandwidth Dashboard** shows information about traffic patterns in your network, including the categories, groups, and users consuming the most bandwidth. See *Bandwidth Dashboard*.
- The **Productivity Dashboard** shows information about blocked requests, and activity in social media categories. See *Productivity Dashboard*.
- The **Cloud Apps Dashboard** shows information about cloud app usage, by category and risk level. See *Cloud Apps Dashboard*.
- The **Data Security Dashboard** shows information about potential data leaks in your organization. See *Data Security Dashboard*.

You can also add your own *Creating custom dashboards in the cloud portal*.

Drag a tab to re-order it on the page.

If you do not wish to see all of the standard dashboards, you can click the Settings icon in the top right corner and select **Hide Current Dashboard**. Click **Continue** to confirm. You can restore hidden dashboards at a later time by using the **Settings > Unhide Dashboard** option.

Each dashboard includes the following features:

- A number of charts that provide detailed web activity information. Most dashboard charts can be customized to change their display format (for example stacked column, area chart, line chart, bar chart, or pie chart). On most charts, you can click the **Maximize** button (  ) to see a larger version in a pop-up window. You can also click columns or sections on a chart to drill down to the relevant report in the Report Builder (see *Using the Report Builder*).  
For more information on the available charts, see the sections for the individual dashboard tabs.
- A summary statistic in the top left that covers web activity relevant to the current dashboard over a defined time period (the last day by default). The selected time period relates to both the number in the summary statistic, and the range displayed in the dashboard charts. You can select a different time period from the drop-down list: the alternative options are 1 hour, 4 hours, 8 hours, 12 hours, 3 days, 5 days, and 7 days.
- One or more filters that define the range of content shown in the charts. To edit a filter:
  - 1) Click the filter name. 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 filter type. For example, you may be able to include or exclude values, or state that search terms contain or do not contain your text.
  - 2) Enter or select the search term or values that you wish 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.

For filters where you enter free text, enter the terms you want separated by commas.

**3) Click OK** when done.

If you change the filters and then wish to revert to the default **All** filter, click **Reset**. Filters apply to individual dashboard tabs, so, for example, editing the filters on the Threats tab has no effect on the Productivity tab.

The dashboard is automatically refreshed whenever you make a change, such as editing the filters. You can also click the **Refresh** button in the top right corner to force the charts to refresh.

#### Related concepts

- [Threat Dashboard on page 20](#)
- [Bandwidth Dashboard on page 21](#)
- [Productivity Dashboard on page 21](#)
- [Cloud Apps Dashboard on page 22](#)
- [Data Security Dashboard on page 22](#)
- [Using the Report Builder on page 231](#)

#### Related tasks

- [Creating custom dashboards in the cloud portal on page 23](#)

## Threat Dashboard

Use the **Threats** tab of the dashboard to monitor security risks and malware threats for your organization. The summary statistic displays the number of web threats over the time period that you specify.

The following charts are displayed:

- **Security Event Summary** shows a list of users who have triggered security events, grouped by Critical, High, Medium, and Low severity. Click a figure in the Hits column to see further details of the sites accessed in the Transaction Viewer (see *Viewing report results*).
- **Top Threat Types by Request** provides a trend chart of the top threat types that have been blocked in the selected time period. Click a threat type definition at the bottom of the chart to include or exclude it in the chart.
- **Top Security Risk Locations** displays a map pinpointing the countries that are considered a security risk. You can filter this map by either Source IP country or Destination IP country. The larger the dot on the map, the greater the number of threats; hover over a dot to see the country name and number of threats. Click a dot to see a breakdown of the security risks by user for that country in Report Builder.
- **Top Security Threats** shows a chart of the most frequently-accessed security threats over the defined time period. Click a bar or section in the chart to see a report of the users accessing a particular security threat.
- **Top Security Risk Sites** shows the domains that triggered the Security risk class over the defined time period. Click a bar or section in the chart to see a report of the users triggering security threats in each domain.

- **X-Labs News** shows an RSS feed of the latest news and blog entries from our Security Labs.

### Related concepts

[Viewing report results](#) on page 234

## Bandwidth Dashboard

---

Use the **Bandwidth** tab of the dashboard to see how bandwidth is being used in your organization. The summary statistic displays the total amount of bandwidth used in the time period that you specify.

The following charts are displayed:

- **Overall Bandwidth Usage** shows a trend chart of the bandwidth used during the selected time period.
- **Top Categories by Bandwidth** shows a trend chart of the categories that used the most bandwidth during the selected time period. Click a category definition at the bottom of the chart to include or exclude it in the chart.
- **Top Connection IPs by Bandwidth** displays a trend chart of the connection IP addresses that used the most bandwidth during the selected time period. Click an IP address at the bottom of the chart to include or exclude it in the chart.
- **Top Groups by Bandwidth** shows the groups who have used the most bandwidth in the selected time frame. Click a bar or section in the chart to see a report of the users within that group who have used the most bandwidth.
- **Top Sites by Bandwidth** displays the domains that have used the most bandwidth in the selected time frame. Click a bar or section in the chart to see a report of the top 20 users who have accessed that domain.
- **Top Users by Bandwidth** shows the users who have used the most bandwidth in the selected time frame. Click a bar or section in the chart to see a report of the domains accessed by that user that have used the most bandwidth.

## Productivity Dashboard

---

Use the **Productivity** tab of the dashboard to monitor how requests are being filtered, which requests are being blocked, and how social media is being used in your organization. The summary statistic displays the number of blocked requests over the time period that you specify.

The following charts are displayed:

- **Top Requested Categories** shows a trend chart of the most requested categories during the specified time frame. Click a category definition at the bottom of the chart to include or exclude it in the chart.
- **Top Filtering Actions by Request** shows a trend chart of the actions (for example, allowed or blocked) performed on web requests during the specified time frame. Click an action definition at the bottom of the chart to include or exclude it in the chart.
- **Top Groups for Blocked Requests** displays the groups who have most frequently requested websites that were blocked. Click a bar or section in the chart to see a report of the users within that group who have had requests blocked.
- **Top Users for Blocked Requests** displays the users who have most frequently requested websites that were blocked. Click a bar or section in the chart to see a report of the domains that were blocked for that user.
- **Top Social Web Channels** shows a trend chart of the most frequently-accessed social media parent categories (for example, Facebook or Twitter).

- **Top Social Web Activities** displays a chart of the most frequently-accessed social media parent categories, broken down into activities within each category. For example, the Facebook category might be broken down into Facebook Commenting and Facebook Events.

## Cloud Apps Dashboard

---

Use the **Cloud Apps** tab of the dashboard to monitor cloud app usage by risk level and category. Statistics are shown for the number of hits, the amount of cloud apps used, and the quantity of users accessing cloud apps. The summary statistic displays the number of cloud apps that have been accessed over the time period that you specify.

The following charts are displayed:

- **Cloud App Use by Risk Level** displays a breakdown of cloud app usage by the risk level of the app (high, medium, and low risk). Select an option button to display app usage for the number of unique cloud apps used, the number of users accessing cloud apps, and the amount of bandwidth used. Click a section of the chart to see a report showing further details for that risk level. Depending on the display option, this report will show the number of hits by cloud app, the number of hits by user, or the amount of bandwidth by cloud app.
- **Top Cloud Apps** displays the ten most-used cloud apps. Select an option button to display the top ten apps by the number of hits or the amount of bandwidth used. Click a bar in the chart to see a report showing the number of hits or bandwidth per user for the selected cloud app.
- **Top Cloud Apps by Risk Level** displays the five most-used cloud apps in each risk level. Click a cloud app definition at the bottom of the chart to include or exclude it in the chart. Click a section of the chart to see a report showing the number of hits per user for the selected cloud app.
- **Top Cloud Apps by Category** displays the five most-used cloud apps in each of the five most-used categories (such as “HR”, “IT”, or “Social Network”). Click a cloud app definition at the bottom of the chart to include or exclude it in the chart. Click a section of the chart to see a report showing the number of hits per user for the selected cloud app.
- **Cloud App Activity by Category** for the top ten cloud app categories, this table shows the number of cloud apps accessed and the number of unique users accessing them, as well as bandwidth usage for that category. Click an item in the table to see a transaction view showing details of individual web transactions for the selected category.
- **Top Cloud App Users** displays the top ten users of cloud apps by the number of hits. Click a section of the chart to see a report showing the number of hits for that user.

## Data Security Dashboard

---

Use the **Data Security** tab of the dashboard for an overview of potential data leaks in your network and information about the kinds of violations that are being made.

Charts provide details of potential data loss whether Data Protection Service or DLP Lite (Data Security) is used to enforce policies. However, data returned to the cloud proxy by Data Protection Service does not include values for each field that may be included in the charts. Use Forcepoint DLP to view and report on incidents not included in the dashboard. See [Viewing Incidents and Reports](#) for more information.

Data Security charts include:

- **Incident Count Timeline** shows a daily incident count for the designated period. With it, you can quickly identify trends and make policy changes as required.
- **Total Incidents by Content Type** shows the number of regulatory incidents, data theft incidents, and custom classifier incidents in the designated period.

- **Top Sources** shows the users, machines, or IP addresses most frequently instigating data security violations as well as the severity of their incidents.
- **Top Destination Domains** shows the Internet domains most frequently targeted with sensitive data.
- **Top Web Categories** shows the website categories most frequently targeted with sensitive data. These can be custom categories or the categories classified by the URL category database.



#### Note


Data returned to the cloud proxy by Data Protection Service does not support all of the fields use to generate the dashboard charts.

## Creating custom dashboards in the cloud portal

In addition to the standard dashboards, you can create a number of custom dashboards per portal account (up to a total of 10 visible dashboards), enabling you to easily access the data you most frequently need. Each custom dashboard can contain up to 6 charts.

To create a custom dashboard:

### Steps

- 1) From any dashboard, click the Settings icon (  ) in the top right corner of the page.
- 2) Select **Add Dashboard**.
- 3) Give your dashboard a name, and click **Add**.  
Your new dashboard appears as a blank tab. You can rename or delete the dashboard from the Settings menu.

### Next steps

To add charts to a custom dashboard, click the Settings icon and select **Add Chart**. Then choose whether you want to create a new chart, or a chart from an existing report.

- *Creating a new chart*
- *Creating a chart from a report*

Once you have added charts to your dashboard, you can reorder them by dragging them around the screen. You can also change the date range for all charts from the drop-down at the top of the dashboard (the default is 24 hours).

To edit or delete a chart, click the arrow in the top right of any chart and select the option you want.

#### Related tasks

[Creating a new chart on page 24](#)

[Creating a chart from a report on page 25](#)



# Creating a new chart

## Steps

- 1) Select **Create New Chart**.
- 2) In the Chart Editor, drag up to 2 attributes from the Attributes list to the Grouping field. For more information on the available attributes, see *Report attributes: Web and Data Security*.
  - The Chart Editor 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 cross icon on the attribute box.
- 3) To add filters to the chart, 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 term or value(s) that you wish 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.

For filters where you enter free text, enter each term that you want on a new line.
    - c) Click **OK** when done.

To edit a filter, click its attribute box. To remove an attribute from the Filters field, click the cross icon on the attribute box.

- 4) Select the chart metric from the drop-down list. For more information on the available metrics, see *Report metrics: Web and Data Security*.



- 5) Select the type of chart to display from the icons next to the Metric field. The following are available:
  - column chart
  - bar chart
  - pie chart
  - line chart
  - area chart

All of these charts are available for a single-level grouping chart. For a chart with 2 attributes, only column and bar charts are available.

- 6) When you have finished defining your chart, you can click the Update button to see how the chart results look.
- 7) Once you are happy with your chart, click Save, and give your chart a name and optionally a description. Then click **Save Chart**.

The chart now appears on your custom dashboard. If you included a description, you can see it by hovering your mouse over the information icon next to the chart name.

#### Related concepts

Report attributes: [Web and Data Security](#) on page 250

Report metrics: [Web and Data Security](#) on page 264

## Creating a chart from a report

### Steps

- 1) Select **Create New Chart from Report**.
- 2) In the Convert Report window, expand the tree and click the report you want to convert to a chart. You can also search for a report name.
- 3) If you want to add more than one converted report to the dashboard, mark **Add another**.
- 4) Click **Convert Report**.





The report is converted into a chart on your dashboard. If you marked **Add another**, the Convert Report window stays open for you to add further charts; otherwise it closes.

## 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:

	<b>Error.</b> Your service has been interrupted, and you must act on this alert immediately.
	<b>Severe.</b> 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.
	<b>Warning.</b> This alerts you to future events that might affect your service – for example portal outages, or license expiration.
	<b>Information.</b> 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 27
- My Account on page 28
- Configuring SIEM storage on page 28
- Contacts on page 30
- Identity Management on page 41
- End Users on page 41
- Groups on page 42
- Licenses on page 43
- Administrator single sign-on on page 44
- Privacy protection on page 47
- Data Protection Settings on page 48
- Important rules for configuring accounts on page 50

## 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 *Contacts* 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 logons 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.
- 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 web accounts or 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.
- Select if you want to prevent end-user identifying information and/or data security incident trigger values from appearing in logs and web reports.

- 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 web service options, click **Web** in the toolbar and select the appropriate setting type or policy.

#### Related concepts

[My Account](#) on page 28

[Contacts](#) on page 30

[Identity Management](#) on page 41

[Groups](#) on page 42

#### Related tasks

[Administrator single sign-on](#) on page 44

[Data Protection Settings](#) on page 48

#### Related reference

[End Users](#) on page 41

#### Related information

[Audit Trails](#) on page 281

## 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 37

## 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.

## Next steps

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 bot tom 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 239

# 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 logons that you create.

### Related concepts

[Password settings](#) on page 35

# 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 concepts

[Forgotten passwords](#) on page 37

### Related tasks

[Password expiration limit](#) on page 36

[Two-factor authentication](#) on page 38

## 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) Use the Group Filtering for Cloud Web Reporting options to restrict reporting access to selected groups.
  - When you select one or more groups, only the users in those groups are visible in the reports that the selected administrator can run.
  - Group filtering can be combined with the View Filtered Reports option for a Web policy: for example, a user can view only reports that apply to the IT and Engineering groups in the Default policy.



### Note

The **Group Filtering for Cloud Web Reporting** option may not be enabled in your account.

6) 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
- **View Data Security Reports:** view data security reports, which may or may not contain incident forensics and trigger data, depending on your privacy protection settings
- **Manage edge devices:** configure edge devices in the network that connect to the cloud service (see *Managing Network Devices*)
- **Log Export:** export SIEM data when using Forcepoint storage (see *Running the SIEM log file download script for Forcepoint storage*) or download full traffic logs, if Full Traffic Logging is available for your account (see *Configure Full Traffic Logging settings*)

The following web permissions can be assigned at an account or policy level:

- **Modify Configuration:** modify all options within Account Settings except users' logons which requires **Manage Users** permissions (required to access the Neo management portal)
- **View Configuration:** view all configurations within Setup, without the ability to make changes
- **View Configuration Audit Trail:** access and search the policy setup audit trail
- **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 and View Data Security Reports options may not be enabled in your account.

Users with any of these permissions can access the web service non-policy-specific configuration options.



#### Note

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 concepts

[Configure Full Traffic Logging settings on page 111](#)

#### Related tasks

[Set up authentication \(Directory Synchronization only\) on page 61](#)

#### Related reference

[Running the SIEM log file download script for Forcepoint storage on page 243](#)

#### Related information

[Managing Network Devices on page 133](#)

# 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 36](#)

# 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 31

# 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:

- 1) The user enters their portal user name and click **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 click **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.

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**.

### Next steps

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.

## Next steps

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>.



### Note

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 44

## 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**.

### Next steps

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 tasks**

[Configure block and notification pages on page 118](#)

## 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 59](#)

## End Users

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

Column	Description
<b>Criteria to use</b>	Check the boxes on the left to indicate what search criteria to use.
<b>Search Criteria</b>	Narrow down the search by entering or selecting precise data in the middle column. Under source, you can choose whether to search <i>SCIM</i> users, <i>DirSync (Directory Synchronization Client)</i> users, or <i>Portal-managed</i> users.
<b>Show in Results</b>	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) Move one or more users to another web policy, performing a manual override
- 2) Undo the manual override (applies to identity management)
- 3) Enable or disable web access
- 4) 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.

If available in your account, you can select how synchronized users are assigned to web policies if they appear in more than one group in the directory. Click the **Policy assignment method** link, and select one of the following:

- **Directory hierarchy** means that a user in multiple groups is assigned to the policy associated with the group that has the fewest intermediate group memberships. For example, if a user is a member of GroupA, and is also a member of GroupB which itself is a member of GroupC, the policy for GroupA takes precedence.
- **Group ordering** means that a user in multiple groups is assigned the policy associated with the group highest in the list on the **Groups** page. The list starts in alphabetical order and can be changed.

## 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.



### 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](http://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

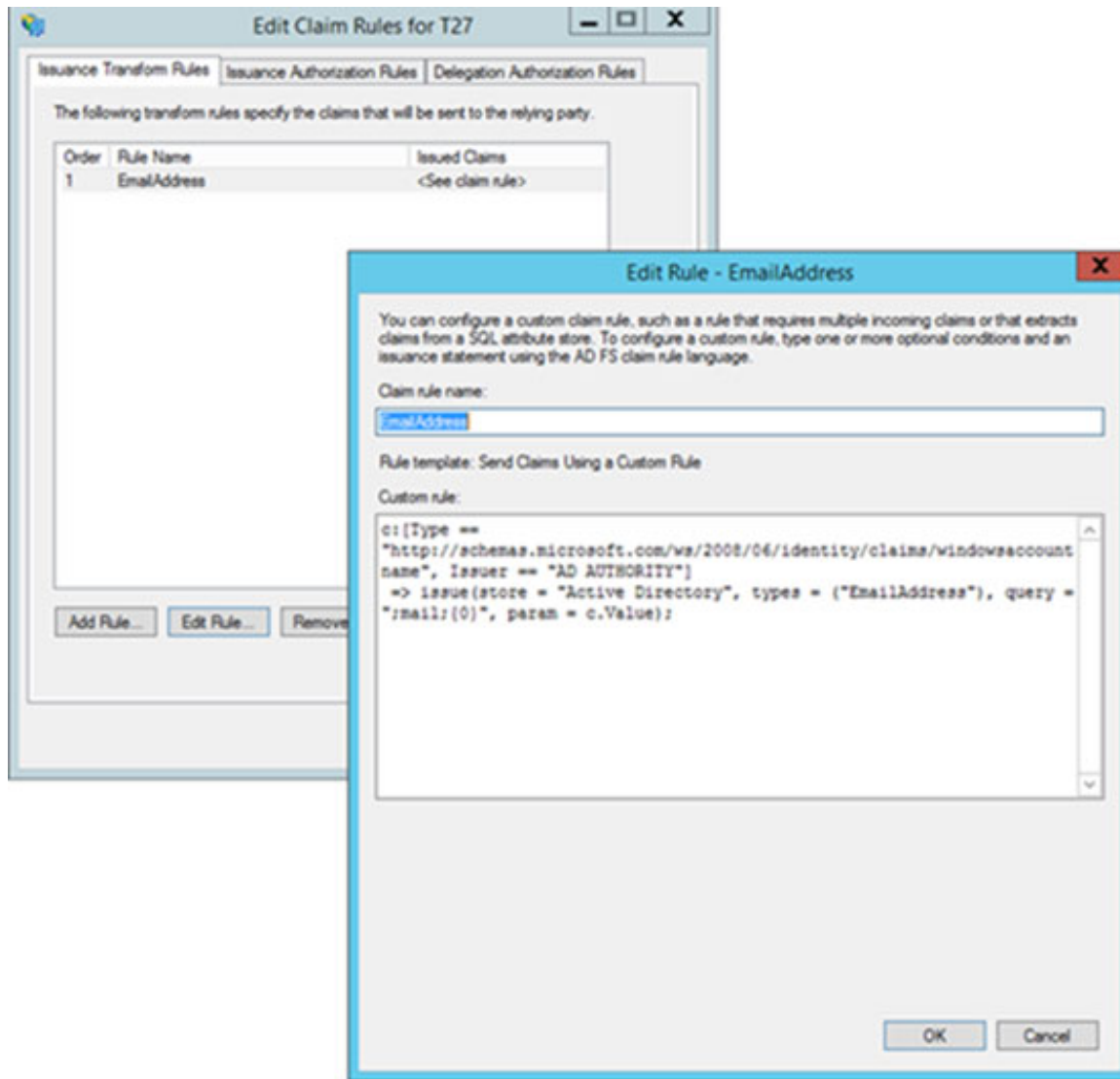
To ensure continuity of service, you should accept any pending licenses as soon as possible. This requires Modify Configuration permissions.

## 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.  
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.
- 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.
- 7) Once you have completed the setup on this page, you must do the following to complete single sign-on activation:
  - a) Add the downloaded SAML metadata file to your identity provider.
  - b) Select the required Login option to enable SSO as an administrator authentication mechanism. See *Login options* for more information



#### Important

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

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.

Configure your identity provider with a custom claim for a relying party trust. Do not Configure your identity provider with an existing claim rule template. If you are using ADFS as the identity provider, configure custom claims to send EmailAddress or domain to the Forcepoint service provider. The attribute names must exactly match those shown in the sample below for custom claim configuration.

```
For Email:
c:[Type == http://schemas.microsoft.com/ws/2008/06/
identity/claims/windowsaccountname, Issuer == "AD
AUTHORITY"]
=> issue(store = "Active Directory", types =
("EmailAddress"), query = ";mail;{0}", param = c.Value);
```

```
For Name ID:
c:[Type == http://schemas.microsoft.com/ws/2008/06/
identity/claims/windowsaccountname, Issuer == "AD
AUTHORITY"]
=> issue(Type = "NameID", Value = c.Value);
```

#### Related concepts

[Login options](#) on page 39

# Privacy protection

Use the **Account > Privacy Protection** page to prevent end-user identifying information and/or data security incident trigger values from appearing in logs and web reports. If required, you can still collect this information for security threats.

## Web Privacy Settings

End user identifying information comprises user names and IP addresses. If you want to prevent this information from appearing only for some of your end users, ensure those users are all registered to a specific policy or policies.

### Steps

- 1) Select **Anonymize end user information**.
- 2) Define whether to anonymize user information in all policies, or only selected policies.



#### Note

If you select **All policies**, this applies to all existing policies and any new policies you create in the future.

- 3) If you choose **Only selected policies**, select the policies you want from the Available policies list. Use the **Ctrl** and/or **Shift** keys to make multiple selections.
- 4) Click the **>** button to move the policies into the Selected policies list.
- 5) To override all privacy protection selections in the event of a security threat, mark **Preserve end user information for security threats**.
- 6) Define the attributes that should be anonymized in web reports.
  - By default, User name, Connection IP, Source IP, and Workstation are all selected. When the Connection IP option is selected, the connection name is also anonymized.
  - You can select and clear the options most appropriate for your organization, but at least one check box must be selected.



#### Note

If you have selected **Preserve end user information for security threats**, the attributes that you select are not anonymized for any web traffic considered to be a security risk.

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

## Data Security Incident Settings (DLP Lite only)

Select **Store and display incident data** if you want the values that triggered data security incidents to be captured, stored in the incident database, and displayed in reports. (Credit card numbers, social security numbers, and email addresses are masked when they are stored, as are passwords in certain instances.)

By default, incident data is *not* captured, stored, or displayed. Administrators with permission to view incident data are able to see the number of matches in the report, but not the match values or context.

Changing this setting has no impact on incident data that has already been collected.

## 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 filename 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 **Web Defaults** section to configure how data security is handled in new web policies.
- a) Select the option to be used, by default, when adding a policy.
- When **Use DLP Lite** is selected, a Data Security tab is available for new policies. When a policy uses DLP Lite, basic data protection is provided by the cloud proxy.
  - When **Use Data Protection Service** is selected, a Data Protection tab is available when adding a new policy. When a policy uses Data Protection Service, enterprise data protection is provided and handled by Forcepoint DLP through the data protection service. DPS is an external service that is part of the on-premises Forcepoint DLP product.
- User requests considered to represent a potential data security risk are forwarded to Data Protection Service by the proxy. DPS then determines the risk and returns a response telling the proxy to block or allow the request.
- When a user is not identified, DPS returns specific allow or block instructions only if a DLP policy for all sources exists. If all DLP policies apply to specific users or groups, no match is found and the proxy allows the request.



#### Important

The same user information must exist in both Forcepoint Web Security Cloud and Forcepoint DLP in order for user requests to be accurately inspected by Forcepoint DLP.

- b) Accept the default provided or enter a new value for **DPS timeout**. This value determines the length of time, in seconds, that the cloud service waits for a response from DPS after sending an inspection request.
- c) Select **Block** or **Allow** as the **DPS fallback behavior** if a timeout or other error occurs. If a response from DPS is not received within the time configured in **DPS timeout**, the user request will be blocked or allowed based on this setting.
- d) Use the tables to change the data security selection for existing policies. Each list contains the existing policies that currently use the data security option indicated in the table heading. Use the arrows to move selected policies from one list to the other. When the changes are saved, the policies are updated to include the new data security type.



#### Note

Return to **Web > Policy Management > Policies** and edit each of the changed policies to fully configure the new data security option. Otherwise, default values are applied to the policy.

- e) Click **Export** in the **Export Categories to DPS** section to create an xml file containing all web categories, including Forcepoint URL Database categories, account-level custom categories, and policy-level custom categories. This file can then be uploaded to DPS and the categories can be used when defining Forcepoint DLP policies. Note that the export needs to be repeated each time a new custom category is added.
- The **Export** button is not available for users with **View Configuration** web permissions.

## Log records (web) with DPS

---

Records returned to the cloud proxy from DPS do not contain all of the data elements included in log records generated by Data Security (DLP Lite).

In addition, when the timeout is exceeded, the request is blocked or allowed based on the fallback selection but no log record is generated.



### Important

---

Requests that include files that exceed 10MB in size are not forwarded to Data Protection Service. These requests are allowed and no log record is generated.

## 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.
- Cloud web products analyze inbound and outbound web traffic as well. 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.

To access a web policy, go to the **Web > 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 51
- What is SCIM? on page 52
- How the service works with SCIM on page 52
- What is LDAP? on page 53
- How the service works with LDAP on page 53
- Planning for your first synchronization on page 54
- Basic steps on page 57
- Cloud portal tasks on page 58
- Maintenance on page 63

## 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.

# 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.

## Email Address

The customer organization must ensure that the right value is being set currently for the user email before enabling SCIM. Failure to do this will lead to incorrectly provisioned users and loss of log history.



### 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.
- If NTLM based identification is used in the customer deployment, then the NTLM ID for the user should also be sent over SCIM. This is a recommendation only.

## 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.

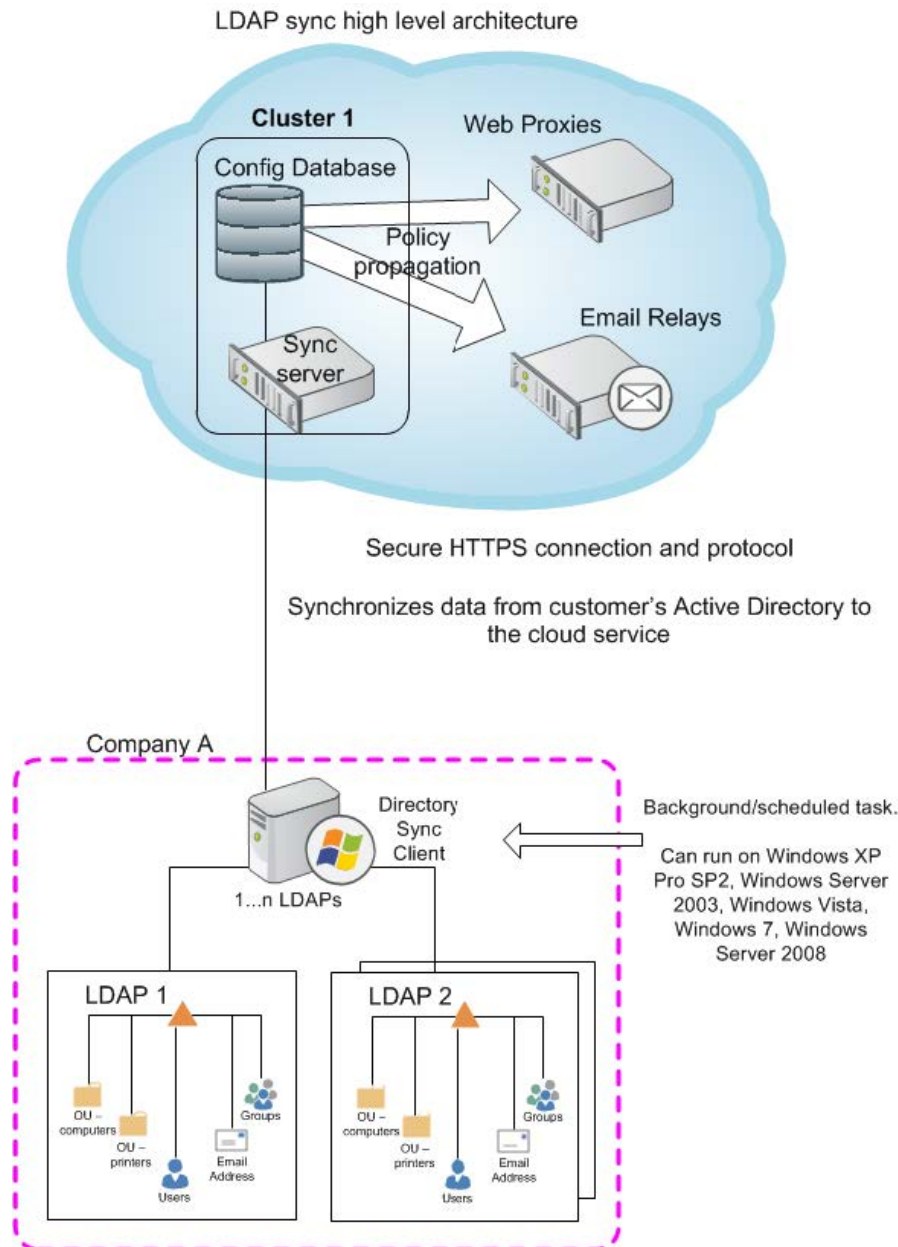
## How the service works with LDAP

---

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)*
- 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 55

#### Related tasks

[Synchronizing users/groups with a single Web policy and exceptions](#) on page 290

[Synchronizing users/groups with more than one policy, and planning to manage policy assignment through an LDAP directory](#) on page 291

[New Web customers \(SCIM\)](#) on page 293

[Wanting to manage users/groups from an LDAP directory](#) on page 294

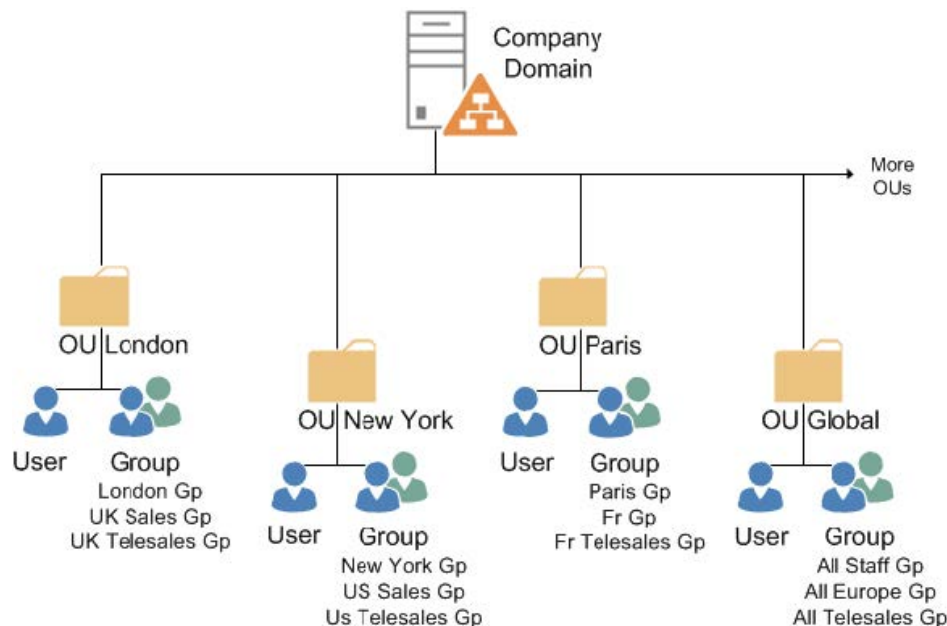
[Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal](#) on page 296

[Existing Web customers \(SCIM\)](#) on page 298

## 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 59



# 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 59

[Set up authentication \(Directory Synchronization only\)](#) on page 61

## 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.

### Next steps

Refer to the [Directory Synchronization Client Administrator's Guide](#) for instructions on items 2-5.

**Related tasks**

[Client tasks \(Directory Synchronization only\)](#) on page 62

[Restore directories](#) on page 66

## Cloud portal tasks

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

### Steps

- 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 59](#)

[Set up authentication \(Directory Synchronization only\) on page 61](#)

## 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.

- 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

[Configure block and notification pages](#) on page 118

[Turn off identity management](#) on page 68

## 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) *Assign a group to a different policy*
- 3) *View and print reports*
- 4) *View recent directory synchronizations*
- 5) *Restore directories* to previous version
- 6) *Troubleshoot synchronization failures*
- 7) *Turn off identity management*

## Related tasks

[View and manage user data](#) on page 63

[Assign a group to a different policy](#) on page 64

[Restore directories](#) on page 66

[Turn off identity management](#) on page 68

## Related reference

[View and print reports](#) on page 65

[View recent directory synchronizations](#) on page 65

[Troubleshoot synchronization failures](#) on page 67

## 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) Move users to another web policy, performing a manual override.
  - b) Undo the manual override.
  - c) Enable or disable web access for users.
  - d) 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.

## Next steps

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

# Assign a group to a different policy

You can modify the web policy to which members (i.e., users) of synchronized groups are to be assigned. This assignment takes place either when the user is initially created on the cloud service or when group membership or group policy assignment changes, depending on how you configured the **User policy assignment** setting on the Identity Management page (see *Configure identity management*).



### Note

Data from LDAP is read-only; you cannot change users and groups relationships that were synchronized from the client directory. If a change is required, you must make it in the client directory itself.

## Steps

- 1) Open the policy to which you want to assign groups. For example, select **Web > Policy Management > Policies > DEFAULT**.
- 2) Click the **End Users** tab.
- 3) Under Identity Management, click **Modify list of groups**.
- 4) Select the groups you want assigned to this policy.
- 5) Click **Submit**.

## Next steps

If you set **User policy assignment** to **Follow group membership** when you configured directory synchronization, the effect of this action is to assign all members of the group already in the service to this policy. Users that are not members of groups, or users in groups that are not explicitly assigned to a policy,



are automatically assigned to the default policy. All future additional users who are members of the group are synchronized into the policy as well.

If you set **User policy assignment** to **Fixed**, the change affects only future additional users.

### Related tasks

[Configure identity management](#) on page 59

## 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 276

## View recent directory synchronizations

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

The Recent Directory 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.

Column Heading	Description
Status	<p>An indication of whether the synchronization completed or failed. Possible HTTP response codes include:</p> <ul style="list-style-type: none"> <li>■ 200 OK - Completed successfully.</li> <li>■ &gt;400 - Synchronization failed <ul style="list-style-type: none"> <li>■ 403 Error text - The client synchronization failed for reasons given in the error text. For example: <ul style="list-style-type: none"> <li>■ 403 Groups contain circular references</li> <li>■ 403 Transaction failed</li> <li>■ 403 Attempt to overwrite cloud-managed group.</li> <li>■ 403 Email address exists in another account</li> </ul> </li> <li>■ 503 Service Unavailable.</li> </ul> </li> </ul>
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 directory 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.
503 Service unavailable.	<ul style="list-style-type: none"> <li>■ The cloud service is heavily loaded, so a synchronization is not currently possible.</li> <li>■ Synchronization is not enabled on the account</li> <li>■ Your account has exceeded its daily synchronization limit</li> </ul>	<ul style="list-style-type: none"> <li>■ No action. The client automatically re-tries later.</li> <li>■ Enable synchronization by selecting <b>Account &gt; Identity Management &gt; Edit &gt; Enabled</b>.</li> <li>■ Retry tomorrow (or when next scheduled).</li> </ul>

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 reference

[View recent directory synchronizations](#) on page 65

## 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**.

### Next steps



#### 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 Web Settings

### Contents

- Introduction on page 69
- Configure General settings on page 70
- Configure Remote Browser Isolation on page 76
- Configure File Sandboxing settings on page 77
- Configure End User Single Sign-On settings on page 80
- Configure Bypass Settings on page 81
- Configure Domain settings on page 89
- Configure Endpoint settings on page 91
- Configure protected cloud apps on page 109
- Configure Full Traffic Logging settings on page 111
- Configure custom categories on page 112
- Time periods on page 115
- Configure custom protocols on page 117
- Configure block and notification pages on page 118
- Configure Content Classifiers for Data Security (DLP Lite) on page 126

## Introduction

---

Use the options in the **Web > Settings** and **Web > Policy Management** menus to configure web protection settings for your account. You are presented with a number of tools and configuration options.

Some options appear only if the corresponding feature has been enabled for your account. Some features require the purchase of additional modules before they can be enabled.

### Settings

- *Configure General settings*
- *Configure Remote Browser Isolation*
- *Configure File Sandboxing settings*
- *Configure End User Single Sign-On settings*
- *Configure Bypass Settings*
- *Configure Domain settings*
- *Configure Endpoint settings*
- *Configure protected cloud apps*
- *Configure Full Traffic Logging settings*

### Network Devices

- *Managing Network Devices*
- *Generating device certificates*

### Policy Management

- *Time periods*
- *Configure custom categories*
- *Configure custom protocols*
- *Configure block and notification pages*
- *Configure Content Classifiers for Data Security (DLP Lite)*

#### Related concepts

[Configure General settings](#) on page 70  
[Configure Bypass Settings](#) on page 81  
[Configure Domain settings](#) on page 89  
[Configure Endpoint settings](#) on page 91  
[Configure Full Traffic Logging settings](#) on page 111  
[Configure custom categories](#) on page 112  
[Time periods](#) on page 115  
[Configure custom protocols](#) on page 117  
[Configure Content Classifiers for Data Security \(DLP Lite\)](#) on page 126

#### Related tasks

[Configure Remote Browser Isolation](#) on page 76  
[Configure File Sandboxing settings](#) on page 77  
[Configure End User Single Sign-On settings](#) on page 80  
[Configure protected cloud apps](#) on page 109  
[Configure block and notification pages](#) on page 118  
[Generating device certificates](#) on page 144

#### Related information

[Managing Network Devices](#) on page 133

## Configure General settings

Use the **Web > Settings > General** page to access information about how traffic is routed for your account.

By default, end user web traffic is routed to the nearest cloud point of presence (data center or local PoP) based on the egress IP address of your Domain Name Server (DNS). If your DNS is in a different geographic location from some or all of your end users, this may mean that traffic is not routed to the nearest point of presence to those users. To route your web traffic to points of presence based on the location of the end user, rather than your DNS, mark **Route traffic based on end users' egress IP**.

The General page also includes the following reference information:

- The proxy auto-configuration (PAC) file defines how web browsers choose an appropriate proxy for fetching a given URL or whether it should be fetched directly from the server of origin. For more information, see *Proxy auto-configuration (PAC)*.
- The proxy query page enables you to determine if a browser is correctly configured. For more information, see *Proxy query page*.
- The web monitoring tool allows you to check web connectivity and speed. For more information, see *Web performance monitor*.
- The roaming home page is designed for remote users, enabling them to connect to the Internet via the cloud service from any location. For more information, see *Roaming home page*.

#### Related concepts

[Proxy auto-configuration \(PAC\)](#) on page 71

[Proxy query page](#) on page 74

[Web performance monitor](#) on page 74

[Roaming home page](#) on page 75

## Proxy auto-configuration (PAC)

We recommend that for all web browsers that will connect directly to the cloud proxy, you use the PAC file configured within the cloud service. This file contains a number of global settings and allows you to enter exclusions of your own (for example, intranet sites) that should not use the cloud service proxy (see *Proxy bypass*).

The exact mechanism for configuring a user's browser to use the PAC file depends on the browser and your network environment. For example, if you are using Microsoft Active Directory and Internet Explorer or Mozilla Firefox, you might want to automate the process by using group policies.

There are a number of different URLs you can use to retrieve a service-generated PAC file. The URL you choose determines which version of the PAC file is retrieved.

Different variants of the PAC file are suited to different network environments.

#### Related tasks

[Proxy bypass](#) on page 170

## Default and alternate PAC file addresses

PAC file addresses can be located on the **Web > General** page and on the **General** tab of a policy. In both locations, a default and alternate address is listed.

- Default PAC file address: the PAC file is retrieved over port 8082 by default, or 8087 for HTTPS. Browsing with this PAC file is performed via port 8081.
- Alternate PAC file addresses: the PAC file is retrieved over port 80 by default, or 443 for HTTPS. Web browsing is also performed via ports 80/443. Useful for locations where non-standard ports are locked down.

Both default and alternate PAC files can be retrieved via HTTP, or over a secure HTTPS connection. Select the HTTP or HTTPS URL as required. See *Accessing PAC files over HTTPS*.

**Related concepts**

[Accessing PAC files over HTTPS on page 74](#)

## Default PAC file addresses

Default PAC file URLs are in the following format:

<http://pac.webdefence.global.blackspider.com:8082/proxy.pac>

<https://pac.webdefence.global.blackspider.com:8087/proxy.pac>

The default PAC file address retrieves the PAC file over port 8082 (or 8087 for HTTPS). Web browsing is performed via port 8081.

This URL should be used where ports 8081 and 8082/8087 are permitted, such as your corporate network.

For more information on which ports are required to use the cloud service, see *Configuring your firewall to connect to the cloud service*.

**Related reference**

[Configuring your firewall to connect to the cloud service on page 10](#)

## Alternate PAC file addresses

Alternate PAC file URLs are in the following format:

<http://pac.webdefence.global.blackspider.com/proxy.pac>

<https://pac.webdefence.global.blackspider.com:443/proxy.pac>

Alternate PAC file URLs use the standard ports for web browsing: port 80 for HTTP traffic, and port 443 for HTTPS. This is useful for users who connect from locations (such as guest or public networks) where non-standard ports may be locked down.

For locations where ports 8081 and 8082/8087 are locked down, use the alternate PAC file address to ensure that users can retrieve the PAC file and browse via the cloud service.

## Standard and policy-specific PAC files

Your account has two locations that list PAC file URLs:

- Standard (account-wide) PAC file URL (found on the **Web > General** page). This URL is an account-wide PAC file URL. This fetches a policy-specific PAC file on connections from recognized IP addresses, and the standard, global PAC file from unrecognized addresses.
- Policy-specific PAC file URL (found on the **General** tab of a policy). This URL includes a policy identifier, which ensures that the PAC file specific to the policy is always retrieved. This can be useful to ensure that remote users always get the PAC file for a particular policy.

See the sections below for further information, and guidance on when to use each option.

### Standard PAC file

The URLs for the standard account-wide PAC file is found on the **Web > Settings > General** page.



When the cloud service receives a request for the standard PAC file, if it knows which policy the requester is using, it delivers the PAC file for that policy; otherwise it delivers a global PAC file.

Remote users whose browsers are configured to use the standard PAC file URL will receive a global PAC file for the cloud service.



#### Note

If you have already deployed a standard cloud PAC file that uses a different URL than the one displayed on the page, there is no need to change it unless you wish to. PAC file URLs provided with earlier versions of your web product will continue to work.

## Policy-specific PAC file

Policy-specific PAC file URLs are in the following form:

<http://pac.webdefence.global.blackspider.com:8082/proxy.pac?p=xxxxxx>

<https://pac.webdefence.global.blackspider.com:8087/proxy.pac?p=xxxxxx>

Here, xxxxxx is a unique identifier for your policy.

Your **Policy Specific PAC File Address** is shown on your policy's **General** tab. To access this screen, go to the **Web > Policy Management > Policies** page, then click the name of the policy.

You should use the policy-specific PAC file in the following circumstances:

- You cannot use a proxied connection on your policies. (You do not need to use a policy-specific URL when connecting from an IP address configured as a proxied connection in a policy, since the policy-specific PAC file is automatically served.)
- A remote user needs to access bypass destinations specified in the policy-specific PAC file, but is able to access these destinations directly, for example, via a VPN client.
- A remote user requests access from a network that has port 8082 locked down (or port 8087 for HTTPS). In this case, use the alternate PAC file address listed on the policy's General tab. This accesses the PAC file via port 80 (port 443 for HTTPS).

Remote users should also use the alternate policy-specific PAC file address if requesting access from a network that has port 8081 locked down. Even if they can access the PAC file on port 8082 or 8087, port 8081 is the standard required port to be able to use the cloud service.

The policy-specific PAC file allows remote users to always use the correct PAC file for their policy, although this is not always appropriate, because bypass destinations may not be relevant for the remote users' locations.



#### Important

There is a security implication related to the use of PAC files. If someone could guess your unique policy identifier and download it, that person would know what sites were not protected by the cloud service and could, in theory, use them as an attack vector. To prevent this, PAC file identifiers are generated as non-sequential alphanumeric strings. Users cannot assume that the number on either side of their PAC file identifier is valid.

For additional security, use the HTTPS PAC file URL. Forcepoint also recommends disabling the **Automatically detect settings** option in your LAN automatic configuration settings.

# Accessing PAC files over HTTPS

Both standard and policy-specific PAC files can be accessed via HTTP or HTTPS URLs. Accessing PAC files over HTTPS provides an additional level of security. The standard PAC file HTTPS URL retrieves the PAC file over port 8087. Browsing is performed via port 8081.

For users accessing the service via networks where these ports are locked down, the alternate HTTPS PAC file URL should be used. This uses port 443 to access the PAC file, and port 80 for browsing.

## Proxy query page

For clients that use a PAC file to connect to the cloud service, a proxy query page is available that allows you to confirm whether the browser is correctly configured. (Because clients using the Direct Connect endpoint do not send traffic through the proxy, the query page cannot be used to validate connections from these machines.)

Click the **Proxy query page** link on the General page to see whether you can access the query page through the cloud service, or whether you are accessing it directly. You receive a message stating either “Yes, you are using the Forcepoint Web Security Cloud filtering proxy server” or “No, you are not...”

To check which point of presence (data center or local PoP) and policy you are currently using, as well as connection and HTTP header information, access the query page using the following URL (note the “with=all” query):

<http://query.webdefence.global.blackspider.com/?with=all>

The point of presence hostname is displayed under the Server Information section, in the form: *aaa##a.srv.mailcontrol.com* (for example *prx24lonb.srv.mailcontrol.com*). That data center name is also provided.

Optionally, check the point of presence identifier (e.g. “lonb”) against the knowledge article: [Cloud service data center IP addresses and port numbers](#).

## Web performance monitor

The web performance monitoring tool is a page that allows you to determine whether the cloud service is introducing latency and adversely affecting performance and end-user experience when accessing certain websites.



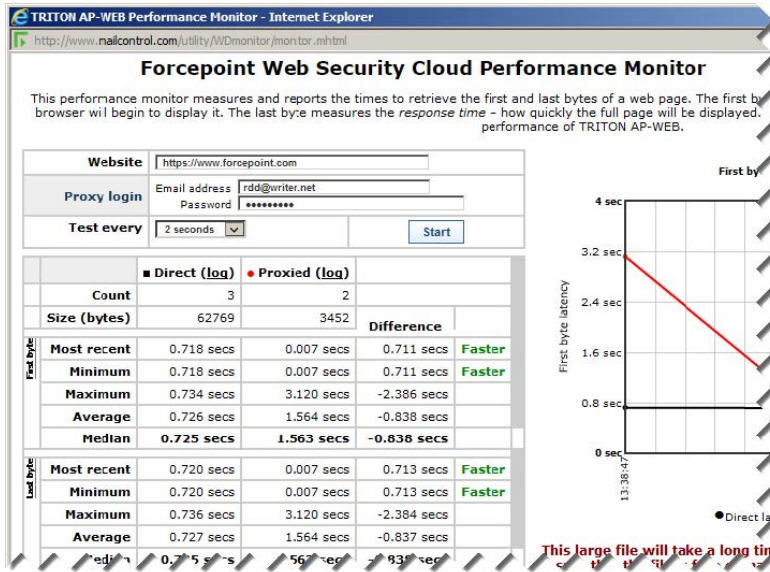
### Note

The web monitoring tool requires Microsoft Internet Explorer.

To run a test, click the **Monitoring tool** link on the **Web > General** page, then enter the web address that you want to test.

Depending on your policy and current location, you may also be required to enter a registered user's email address and password (see *Access Control tab* for when and why this is required).

The test sends a request to the specified website both directly and via the proxy to which you are connected. The results show the time to receive the first and last bytes of the web page returned for each direct and proxied request. The median first byte latency provides the best indication of how the cloud service feels to an end user, (i.e., generally how quickly the page starts to display). The median last byte latency provides an indication of how quickly the page is completely displayed, even though the end user begins to read or even click another link before the page is displayed completely.



The results are affected by any local network and Internet connectivity issues and cannot be assumed to prove where a fault lies if a website is responding slowly. However they do provide a good indication of whether a slow website response is a cloud-related issue or a problem with the website being accessed.

### Related concepts

[Access Control tab on page 171](#)

## Roaming home page

A roaming user (also known as a remote or offsite user) is someone who is connecting to the web from an IP address that has not been configured as a proxied connection on any policy.

When roaming users try to proxy through the cloud service from an unknown IP address, the service does not know which policy to apply to them and must therefore serve a non-policy specific notification page asking them to identify themselves. This is a global page and cannot be customized.

**Internet Access Login**

Your organization is using an internet security provider to protect your web browsing. We detected that you are connecting from outside your organization and need to determine who you are before proceeding.

Log in if you already have credentials to access the internet through your company workstation, otherwise please register first.

[Forgot password](#)  
[Not Registered?](#)

If you have reached this page in error or have the endpoint client installed on your workstation, please see further instructions on the [support site](#).

**FORCEPOINT**  
Web Security Cloud

Once a user is logged on with a unique user ID, the cloud service knows which policy to apply to the user.

# Challenges supporting roaming users

There are a number of scenarios that must be supported to allow deployment of the cloud web service for roaming users. This presents a number of challenges: connection difficulties related to browser type, the connectivity method, and many other variables. For the latest advice, known issues, and workarounds please check the articles in the [Knowledge Base](#) and the [Getting Started Guide](#).

## Configure Remote Browser Isolation



### Note

Remote browser isolation is a limited-availability feature and may not be enabled for your account.

Available at the account level, the remote browser isolation feature allows a user to redirect a blocked request to a remote browser isolation service. A block page, available for selection when a category is configured with Block Access, provides the user the option to **View in Remote Browser**. When that option is available and selected, the request is forwarded to the provider. See *Managing categories, actions, and SSL decryption* for information on configuring categories in a policy

Use the **Web > Settings > Remote Browser Isolation** page to enable and configure the feature.

### Steps

- 1) By default, **Disabled** is selected. Click the radio button next to the appropriate provider and continue with the configuration to enable remote browser isolation.

Only one provider can be selected.

The block page that allows a user to **View in Remote Browser** is available for selection when configuring categories in a policy when remote browser isolation is enabled and configured. Remote browser isolation cannot be disabled If this block page has been assigned for use by a category



### Note

This feature requires a subscription with a supported remote browser isolation provider.

- 2) Enter the **Tenant ID** or **Hostname or IP address** used for the provider.  
Customers using Ericom as the provider should get the Tenant ID from the fulfillment letter received when the feature was purchased.  
An read only entry on the **Proxy Bypass** tab of the Bypass Settings page is automatically added. The entry is added so that all traffic sent to the provider's IP address bypasses the cloud service for all policies. The entry is automatically updated or removed based on changes made to remote browser isolation configuration.
- 3) Use the **Test** button to confirm a connection to the provider.  
Click the button to open [www.google.com](http://www.google.com) in a new browser window, where you can enter the credentials required by the provider. The Google home page should then display.  
Note that only clientless provider services are supported. Connections that require the installation of an agent or browser plugin are not supported.

#### 4) Click **Save**.



##### Note

If a user has opted to **View in Remote Browser**, the request is no longer handled by the cloud service. Subsequent requests from the same browser will continue to be handled by the remote browser isolation provider until browser window is closed.

#### Related tasks

Managing categories, actions, and SSL decryption on page 195

## Configure File Sandboxing settings



##### Note

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

Use the **Web > Settings > File Sandboxing** page to upload suspicious files to a cloud-hosted sandbox for analysis. The sandbox activates the file, observes the behavior, and compiles a report. If the file is malicious, 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:

- Has been downloaded by an end user.
- Is **not** classified as “malicious” in the Forcepoint URL Database
- Passes all **File Type Analysis** checks
- Fits the Security Labs profile for suspicious files
- Is a supported file type. Executable files are always supported. See *Supported file types*.



##### Note

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

For file sandboxing to be most effective, you should enable all of the advanced analysis options in your policies. For more information, see *Web Content & Security tab*.

### Steps

- 1) File analysis is disabled by default. Select **On** to send qualified executable files to the cloud-hosted sandbox for analysis.
- 2) Select **Submit additional document types** to send additional supported file types to the sandbox for analysis.



##### Note

For clients using Direct Connect Endpoint, the specified file types are uploaded to the File Sandboxing service for traffic only from sites with elevated risk profiles.

- 3) Select **Block access to files that have previously been detected as potentially malicious** to block requests made to files that were previously found to be malicious.
- 4) Specify the email address of at least one person in your organization who will receive notifications. This does not have to be a cloud service administrator. If you specify multiple email addresses, ensure you enter one address per line.
- 5) Filename encoding can be used so that filenames display properly in Report Center reports. Enable **Filename encoding** and select the appropriate character set from the drop-down provided.
- 6) Click **Save**.

Web > File Sandboxing

## File Sandboxing

Specify whether to send risk-prone file types downloaded by end users for further analysis.

File Analysis:  OFF

Submit **additional document types**:

Block access to files that have previously been detected as potentially malicious:

Define who receives notification messages when a malicious file is identified:

*At least one email address is required. Enter one address per line.*

Filename encoding:  Use alternative filename character set

### Related concepts

[Supported file types](#) on page 78

[Web Content & Security tab](#) on page 217

## Supported file types

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

- Windows executable files

The following file types are supported for file sandboxing if you select **Submit additional document types** on the **Web > Settings > File Sandboxing** page:

- 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)
- Archive files:
  - RAR
  - 7z
  - GZIP
  - TAR
  - ZIP
  - ARJ
  - BZ
- PDF files

## What does a file sandboxing transaction look like?

---

- 1) An end user browses to a website and explicitly or implicitly downloads a file.
- 2) The URL is **not** categorized as “malicious” and file analysis does **not** find the file to be malicious.
- 3) The file is delivered to the requester.
- 4) However, the file fits the Security Labs profile for suspicious files and is sent to the cloud for analysis.
- 5) The file is analyzed, which may take as long as 5 to 10 minutes, but is typically much quicker.
- 6) If the file is found to be malicious, the cloud proxy sends a malicious file detection message to the configured alert recipients. The alert email includes a link to the compiled report.
- 7) 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
- 8) Separately, the cloud sandbox updates ThreatSeeker Intelligence with information about the file, the source URL, and the command and control targets.
- 9) ThreatSeeker Intelligence updates the Forcepoint URL Database, Advanced Classification Engine (ACE) analytic databases, and other security components.
- 10) The next time someone tries to browse the site, they and the organization are protected by their cloud deployment.



# Configure End User Single Sign-On settings

The end user single sign-on feature uses a third-party identity provider that authenticates user identity, attributes, and roles using your enterprise directory. End user single sign-on uses the Security Assertion Markup Language 2.0 (SAML2.0) data format to send messages to and receive responses from your identity provider. All communications between components are secured.

If you already have an identity provider supported by the cloud service, you can configure your provider to authenticate users browsing via the cloud proxy, enabling seamless end-user login.

When end users single sign-on is enabled, end users connecting to the cloud proxy are redirected to your identity provider, if specified in their policy. Once a user has been authenticated against your directory service, they are directed back to the proxy and the appropriate policy is applied. Clients who have authenticated once do not then have to re-authenticate for subsequent web browsing sessions, for a specified period of time (see *Session timeout*).

To configure end user single sign-on:

## Steps

- 1) Go to **Web > Settings > End User Single Sign-on**.
- 2) Mark **Use identity provider for single sign-on**.
- 3) For customers new to end user single sign-on, the Identity provider entry displays SAML 2.0 Compliant Identity Provider and cannot be changed.  
For customers who had configured end user single sign-on prior to the introduction of the SAML 2.0 Compliant Identity Provider option, the previously selected identity provider is displayed and a drop-down list offers the original provider and SAML 2.0 Compliant Identity Provider. The vendor-specific options remain available strictly to support customers already using them. It is recommended that all customers select the generic option.
- 4) To enable your identity provider to work with end user 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) In order for the cloud proxy 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.
- 6) Click the Root Certificate link and save the certificate file to a location on your network.
- 7) 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 either reverting to the previous metadata source if one was configured, or disabling the **Use identity provider for single sign-on** checkbox if you are configuring end user 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 end user single sign-on activation:

- Add the downloaded SAML metadata file to your identity provider.
- Deploy the root certificate to end users' machines, using your preferred distribution method such as Group Policy Object (GPO).
- Enable single sign-on for your policies on the *Access Control* tab.



### Note

For more information on the end user single sign-on service, including detailed configuration guidance for supported providers, see the [End User Single Sign-On Guide](#) on the Support website.

### Related concepts

[Session timeout](#) on page 174

[Access Control tab](#) on page 171

# Configure Bypass Settings

The cloud service includes the following options for bypassing security and authentication checks, if required for your end users:

- The **Authentication Bypass** tab enables you to add custom settings that bypass authentication and content filtering for applications, user agents, and sites for which authentication with the cloud service is problematic. If you have an I Series appliance or a supported edge device, you can add authentication bypass rules for internal networks behind the device. See *Bypassing authentication settings*.
- The **Proxy Bypass** tab enables you to add, and import in bulk, destinations that bypass the cloud service for all policies. See *Adding and importing sites that bypass the proxy*.
- The **SSL** tab enables you to specify trusted HTTPS domains that your end users can always access even if the certificate is detected to be invalid (see *Bypassing certificate verification*), and to define web categories that should never be decrypted for end users authenticating with single sign-on or secure form-based authentication. For I Series appliances, this applies to all authentication methods. See *Bypassing authentication decryption*.

### Related concepts

[Bypassing authentication settings](#) on page 81

[Adding and importing sites that bypass the proxy](#) on page 86

[Bypassing certificate verification](#) on page 88

[Bypassing authentication decryption](#) on page 89

## Bypassing authentication settings

The following options are available in this section:

- *Bypassing authentication for cloud-based applications*
- *Bypassing authentication and filtering for user agents or sites*
- *Bypassing authentication and filtering for internal networks.* This option is available only if you have an I Series appliance, or a supported edge device that connects to the cloud service.

#### Related concepts

[Bypassing authentication for cloud-based applications](#) on page 82

#### Related tasks

[Bypassing authentication and filtering for user agents or sites](#) on page 82

[Bypassing authentication and filtering for internal networks](#) on page 84

## Bypassing authentication for cloud-based applications

If your organization uses Microsoft Office 365, select the Office 365 box under Cloud Applications to bypass authentication for these services and ensure seamless operation.

## Bypassing authentication and filtering for user agents or sites

Some applications cannot authenticate with the cloud service. This might occur with applications such as instant messaging programs, antivirus updates, or software update services.

The **Authentication Bypass** tab on the **Web > Settings > Bypass Settings** page enables you to add and edit custom settings to change the default behavior for failing applications or websites that cause problems with authentication.

To bypass authentication for particular applications or sites that do not properly handle authentication challenges, you can specify user agents, domains, URLs, or a combination of these.



#### Tip

A user agent is identified by a string sent from your browser or Internet application. This identifies which browser or application you are using, its version number, and details about your system, such as the operating system and version. The destination server can use this information to provide content suitable for your specific browser or application. For example, this is the user agent information for Firefox:

*Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6)*

In this example, Windows NT 5.1 indicates that the operating system is Windows XP, and the language setting is US English.

To add a setting for an application or site:

### Steps

- 1) On the **Authentication Bypass** tab, click **Add** under User Agents & Destinations.

- 2) Enter a **Name** for the rule. This name appears in the Authentication Bypass list on the Bypass Settings page, and you can click on it at a later date to edit your settings.
- 3) Select the **Authentication method** for the rule. Note that you can only select a fallback option for the authentication type configured in the policy - for example, if the policy specifies only NTLM identification, you can select Basic or No authentication, but not Form login.

- **Use defaults:** Uses your default authentication method.
- **NTLM:** Uses NTLM identification for the specified user agent(s) and destination(s). If an application is not NTLM-capable, basic authentication will be used instead. For more information about NTLM identification, see *NTLM transparent identification*.



#### Note

You must have NTLM identification enabled for your account to use this option.

- **Form login:** Displays the secure login form to users before they use their cloud credentials to proceed over a secure connection. For more information, see *Access Control tab*.
  - **Basic:** Uses the basic authentication mechanism supported by many web browsers. No welcome page is displayed. For more information on basic authentication, see *Access Control tab*.
  - **Welcome page:** Displays a welcome page to users before they use basic authentication to proceed. The welcome page is configurable in each policy on the *Access Control tab*. Note that the welcome page is not available for traffic from I Series appliances. For more information, see *Pre-logon welcome page*.
  - **No authentication:** Bypasses all authentication and identification methods in the cloud. Select this option for Internet applications that are incapable of authentication.
- 4) **Content filtering** is enabled by default. Optionally, you can bypass all content filtering for the specified user agent(s) and destination(s) by selecting **Disabled**.



#### Warning

We strongly recommend you do not disable content filtering unless it is for applications and sites that do not work with the cloud service and that you trust implicitly. Disabling content filtering overrides all other filtering rules, including web category filtering actions. This means that **all content is allowed**. This could allow viruses and other malware into your network.

- 5) Define the user agents, if any, for the rule:

- If the application does not send a user agent string to the Internet, select **No user agent**.



#### Note

This option will match against all applications that do not send a user agent. In this case, we recommend you refine the rule by entering one or more URLs or domains in the **Destination sites** field.

- To apply the rule to all user agents, select **All user agents**. You might want to do this if you are setting up a custom rule that applies to all browsers on all operating systems in your organization.
- If you want to apply the bypass rule to one or more user agents, select **Specific user agents**, and enter each user agent on a separate line. Use the asterisk wildcard to match one line to multiple user agent strings, for example Mozilla/5.0\*.

- 6) Define the destination sites (if any) for the rule:
  - To match against all domains and URLs, select **All destinations**. You might want to do this if you are setting up a custom rule that applies to a specific user agent that accesses multiple sites.
  - To apply the rule to one or more sites, select **Specific destinations**, and enter each URL or domain on a separate line. URLs must include the protocol portion (http://) at the beginning and a forward slash (/) at the end - for example, <http://www.google.com/>. If these elements are not present, the string is treated as a domain. Domains cannot include a forward slash at the end - for example, mydomain.com. Use the asterisk wildcard to match one line to multiple destinations: for example, entering \*.mydomain.com would match against all domains ending in 'mydomain.com.'
- 7) Click **Save**.

## Next steps

To view the user agents that have made authentication requests via the cloud service, run the User Agents report (under **Reporting > Report Catalog > Advanced**). If a user agent in this report has a high number of authentication requests, it may be experiencing authentication problems.

### Related concepts

[NTLM transparent identification](#) on page 185

[Access Control tab](#) on page 171

[Pre-logon welcome page](#) on page 174

# Bypassing authentication and filtering for internal networks

If you have an I Series appliance or an approved edge device that connects to the cloud service, you can override policy authentication and content filtering settings based on the IP addresses in your internal networks, so that specific nodes in a network (for example, guest networks) are forced to authenticate using an alternative method, or will not be authenticated at all.

If there is a conflict between the settings in this section and the settings in *Bypassing authentication and filtering for user agents or sites*, the IP address settings for the internal network take precedence.

To add a setting for an internal network:

## Steps

- 1) On the **Authentication Bypass** tab, click **Add** under Internal Network Traffic.
- 2) Enter a **Name** for the rule. This name appears in the internal networks list on the Bypass Settings page, and you can click on it at a later date to edit your settings.

- 3) Select the **Authentication method** for the rule. Note that you can only select a fallback option for the authentication type configured in the policy - for example, if the policy specifies NTLM identification, you can select Basic or No authentication, but not Form login.

- **Use defaults:** Uses your default authentication method.
- **NTLM:** Uses NTLM identification for the specified internal network(s). If an application is not NTLM-capable, basic authentication will be used instead. For more information about NTLM identification, see *NTLM transparent identification*.

**Note**

You must have NTLM identification enabled for your account to use this option.

- **Form login:** Displays the secure login form to users before they use their cloud credentials to proceed over a secure connection. For more information, see *Access Control tab*.
  - **Basic:** Uses the basic authentication mechanism supported by many web browsers. No welcome page is displayed. For more information on basic authentication, see *Access Control tab*.
  - **No authentication:** Bypasses all authentication and identification methods in the cloud service. Select this option for internal networks that should never use authentication credentials.
- 4) **Content analysis** is enabled by default. Optionally, you can bypass all filtering for the specified internal network(s) by selecting **Disabled**.

**Warning**

We strongly recommend you do not disable content filtering unless it is for applications and sites that do not work with the cloud service and that you trust implicitly. Disabling content filtering overrides all other filtering rules, including web category filtering actions. This means that **all content is allowed**. This could allow viruses and other malware into your network.

- 5) To specify the internal network details, click **Add**.
- a) Enter a name for the network (for example, "Guest Network").
  - b) Select the network type. This can be an individual IP address, an IP address range, or a subnet.
  - c) Enter the IP address, range, or subnet details.
  - d) Click **OK** when you are done.
- 6) Click **Save**.

**Related concepts**

[NTLM transparent identification](#) on page 185

[Access Control tab](#) on page 171

**Related tasks**

[Bypassing authentication and filtering for user agents or sites](#) on page 82

# Adding and importing sites that bypass the proxy

The **Proxy Bypass** tab of the Bypass Settings page enables you to define sites that bypass the cloud service for all policies. This may include, for example, internal sites that are not accessible from the Internet, so the cloud service cannot serve or analyze them.

A proxy bypass destination can be a domain name, an IP address, or a subnet.

- Both the Proxy Connect and Direct Connect endpoint clients use the bypass definitions. In the case of the Neo or Direct Connect endpoint, destinations in the bypass list are not analyzed by the cloud service.
- When a PAC file is used to direct traffic through the cloud proxy, configured destinations are added to the PAC file for your organization.

Recommended bypass destinations include organizational webmail sites, internal IP addresses, and system traffic such as Microsoft and antivirus updates. If remote browser isolation is configured, the provider IP address or domain name is automatically added as a bypass destination.

If your organization uses Microsoft Office 365, select the **Office 365** box under Cloud Applications and click **Save** to bypass the cloud service for sites and URLs associated with Office 365.



## Note

The URLs included in the bypass list for Office 365 are those domains that are owned by Microsoft and used directly by the Office 365 application, listed here:

<https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges>

This list also includes third-party URLs that host Certificate Revocation Lists (CRLs), which are not included in the bypass when you select the **Office 365** checkbox. Bypassing these domains may not be appropriate for all customers.

If you have difficulty installing or using Office 365 with this option selected, you may need to add one or more of these additional URLs as non-proxied domains. If you need further assistance, please contact Technical Support.

You can also configure policy-specific bypass destinations on the Connections tab of each policy. For more information, see *Proxy bypass*.

## Related tasks

[Proxy bypass](#) on page 170

# Adding a new bypass destination

## Steps

- 1) Click **Add**.
- 2) Enter a **Name** and helpful **Description** for the destination.
- 3) Specify the destination **Type**, then enter the **Address** (single IP address), **Subnet** (using CIDR notation or subnet mask), or **Domain**.

- 4) If the traffic should bypass the cloud proxy, but go through a third-party proxy in your network, mark **Send traffic to another proxy**.
- 5) Use the optional **Comment** box to add helpful information, such as why the entry was created.
- 6) Click **Submit**.

## Importing bypass destinations in bulk

### Steps

- 1) Click **Import Destinations**.
- 2) Click the CSV template link, and save the template in a location of your choice.
- 3) Add the bypass destination information to the template file.  
The template file contains the following columns: Name, Type, Destination, and Description. Only Description is optional; all other columns must be filled in.

Ensure the Type column contains either Address, Domain, or Subnet, and any destinations with the Subnet type use CIDR notation. For example:

Name	Type	Destination	Description
Dest1	Domain	destination1.com	Here is a description
Dest2	Address	154.10.2.36	Another description
Dest3	Subnet	154.10.2.38/19	Yet another description

- 4) Save the file.
- 5) On the Import Destinations page, browse to your CSV file, then click **Import**.  
Once the destinations are successfully imported, the Import Destinations page closes and the imported destinations are listed on the Proxy Bypass tab. If the import fails, any errors are listed on the Import Destinations page. Each error states which line of the CSV file is affected, and explains the problem; fix any issues before trying the import process again.



#### Note

You can add a total of 1000 proxy bypass destinations per policy. Account-level bypass destinations (added via **Web > Proxy Bypass**) count towards this limit for each policy. For example, if your policy has 10 bypass destinations, and you have 10 account-level bypass destinations, this is counted as a total of 20 destinations for the policy.

# Bypassing certificate verification

The cloud service verifies certificates for HTTPS sites that it has decrypted and analyzed. Certificate verification is enabled by default on the **SSL** tab of the Bypass Settings page, and happens automatically in one of the following cases:

- SSL decryption has been enabled for web categories (see *Web Categories tab*).
- You have enabled notification pages to be served for HTTPS sites (see *HTTPS notifications*).
- You are using secure form-based authentication (see *Access Control tab*).
- You have configured end user single sign-on functionality.
- You have deployed an I Series appliance and enabled any of the authentication methods available in the policy.

Certificate verification checks are numerous and apply to all certificates in the trust chain. For example:

- The certificate must be issued by a trusted Certificate Authority (CA). For a list of supported CAs, see the Knowledge Base article [What are the trusted Certificate Authorities?](#)
- The certificate must be current (within its “Valid from...to...” date range).
- The certificate must not be on a revocation list (either CRL or OCSP).

To choose whether or not to use certificate verification, in the Certificate Verification Bypass section on the **SSL** tab, set **Perform certificate verification** to On or Off.



## Important

We strongly recommend that you verify certificates for HTTPS sites. If you switch this option off, there is a chance of increased security risks from malicious sites with certificates that misrepresent their identity (for example, a site called gogle.com pretending to be Google).

If certificate verification fails, the end user sees an error page and cannot access the website unless you allow them to access sites with certificate errors by marking **Allow end users to bypass all certificate errors**. In this case, end users see a notification page informing them that a certificate error has been detected, and have the option to either proceed to the site or go back. This notification page is not available for I Series appliances.

If you choose to perform certificate verification, you can maintain a list of domains and IP addresses for which the cloud service bypasses certificate verification errors. This enables end users to visit a site even if the certificate is invalid. You may want to do this for sites that you trust even if, for example, the certificate has expired, is not yet valid, or is self-signed.

You can manage domains and IP addresses for bypass as follows:

- To add items for certificate verification bypass, enter one or more domain names or IP addresses separated by commas, then click **Add**. IP addresses can also include the port number (for example 127.0.0.1:80). You cannot add IP address ranges.
- To delete a domain name or IP address from the bypass list, select the item and click **Delete**. You can use the **Ctrl** and/or **Shift** keys to select multiple items for deletion.

Click **Save** when done.

## Related concepts

[Web Categories tab](#) on page 193

[Access Control tab](#) on page 171



**Related tasks**[HTTPS notifications](#) on page 120

## Bypassing authentication decryption

If end users authenticate with either single sign-on or secure form-based authentication, web traffic is decrypted as part of the authentication process, regardless of whether SSL decryption is enabled in the policy. There may be some categories with privacy implications where you do not want this decryption to occur, for example financial data sites.

Authentication decryption bypass also applies to traffic going through I Series appliances that is subject to any type of authentication.

**Note**

The appliance does not currently support authentication decryption bypass for custom categories.

To define a web category that is never decrypted during authentication on the **SSL** tab, under Authentication Decryption Bypass, select the category in the **Available categories** list, and click the > button to move it to the **Selected categories** list.

Note the following for the selected categories:

- The selections apply only to end users browsing from proxied connections. They do not apply to roaming users.
- Users browsing these categories will be considered anonymous for both policy enforcement and reporting.

## Configure Domain settings

Email domains can be used to enable end-users to self-register with the cloud service. Users with email addresses belonging to the domains that you add can create a password to self-register with the service. Domains can be configured at either the account level or policy level. Domains can be used to determine which policy users are assigned when they register.

Before reading this section, we recommend that you read *Proxied connections*.

**Related concepts**[Proxied connections](#) on page 168

## Permissions implications

Administrators who have permissions only for individual policies can access domain configuration only from within the policy, and they cannot amend account-level domains. They also receive a restricted set of controls when editing policy-level domains. From this view, they can see all domains but have editing rights only to the policy-level domains associated with their policy.

# Legal requirements

---

Your terms and conditions for use of the service include a clause that restricts the use of domains to those that are legally registered to your organization. *Bulk registering end users* explains the process of bulk registration, where the cloud service sends email to a list of email addresses uploaded to the service. The legal restriction is to prevent someone from maliciously or unintentionally spamming a third party with email originating from the cloud service.

## Related concepts

[Bulk registering end users](#) on page 182

# Policy-level domains

---

Policy-level domains are created in the policies themselves. Users with an email address in this domain are registered to the policy to which the domain is assigned. This is useful if you have users in your account with different email domains, who you wish to manage using different policies.

To create a policy-level domain:

## Steps

- 1) Select **Web > Policy Management > Policies**.
- 2) Click the name of the policy to open.
- 3) Click the **End Users** tab.
- 4) Under Self Registration, click **Add**.

## Next steps

No policy-level domain can exist in multiple policies or accounts.

When you are adding a policy-level domain, some options are grayed out, because they are only applicable to account-level domains.

# Account-level domains

---

Account-level domains can be added in order to allow users to self-register to any policy in your account. The actual policy they are assigned to is determined by the IP address from which they register (see *Proxied connections*).

Account-level domains must have a default policy for remote users. Users registering with email addresses belonging to the domain, and connecting from unknown IP addresses, will be added to this default policy. If there is no default policy, then remote users cannot register and receive an error message when they try to do so.

**Note**

If all users within your account are on a single email domain and you have multiple policies, you must configure an account-level domain assigned to all policies.

Click **Web > Settings > Domains** to see the end-user registration domains, and the policy each domain is associated with. If they are account-level domains, the words “By connection” are shown instead of a policy name.

**Related concepts**

[Proxied connections](#) on page 168

## Editing a domain

In the list of domains, click the name of a domain you want to edit, and then click **Edit**.

A domain can be associated with a specific policy or all policies. If you select **Associate this domain with all policies**, you are prompted to assign a default policy for remote users. If no account-level domains are assigned, remote users are registered into the policy associated with the account to which their domain is assigned.

If remote users try to register using an email address that is associated with an account-level domain and there is no default policy, they receive an error message.

## Configure Endpoint settings

Use the **Web > Settings > Endpoint** page to configure the settings that apply to all web endpoint clients deployed in your network.

- For information about the available web endpoint clients, see *Endpoint overview*.
- Endpoint client deployment is managed within your policies. See the *Endpoint tab* topic under *Defining Web Policies* for more information.

**Related concepts**

[Endpoint overview](#) on page 92

[Endpoint tab](#) on page 178

**Related information**

[Defining Web Policies](#) on page 159

## Web endpoint configuration options

On the **Web > Settings > Endpoint** page:

- Use the **General** tab to access the Forcepoint Neo management portal, define a default policy for roaming users, set the anti-tampering password when needed, find information used to deploy endpoint client software via GPO, and download endpoint client software.

Anti-tampering passwords must:

- Be between 14 and 32 characters.
- Contain upper case characters.
- Contain lower case characters.
- Contain numbers.

See:

- *Configure General endpoint settings* for more information about the options on the General tab.
- *Windows operating system users* for instructions on configuring and deploying the endpoint client to Windows machines.
- *Mac operating system users* for instructions on configuring and deploying the endpoint client to Mac machines.
- Use the **End User Control** tab to define which users can enable or disable the endpoint software on their machines.



#### Note

Endpoint end user control is not supported for the Mac version of the Classic Proxy Connect Endpoint client.

Instructions for using the End User Control tab are included in the configuration procedures for Windows clients, linked in the previous step.

See also *Configure endpoint End User Control settings* for more information about the options on the End User Control tab.

- Use the **Endpoint Bypass** tab to specify applications on end user machines that can access the Internet directly, bypassing endpoint policy enforcement.

See *Endpoint bypass* for instructions.

#### Related concepts

[Configure General endpoint settings](#) on page 96

[Mac operating system users](#) on page 103

[Endpoint bypass](#) on page 107

#### Related tasks

[Windows operating system users](#) on page 99

[Configure endpoint End User Control settings](#) on page 98

## Endpoint overview

Forcepoint Endpoint agents are lightweight software clients that run in the background on user devices, providing a seamless browsing experience for your end users. Endpoint agents automatically authenticate users with the service, and provide policy enforcement and data security features. The endpoint clients have been designed to consume minimal CPU, memory, and disk resources, and have tamper controls to prevent users disabling the software.

Available endpoint agents are:

- **Neo:** this endpoint agent can be used in either proxy connect mode or direct connect mode, and can automatically switch from one to the other when necessary. For customers who have also purchased Forcepoint Dynamic User Protection, Neo sends user activities there for analysis to compute the risk score.
- **Proxy Connect:** this classic endpoint agent redirects all traffic to the cloud proxy for analysis. Proxy Connect is recommended for most scenarios, and supports the widest set of security features.
- **Direct Connect:** this classic endpoint agent contacts the cloud service for each request to determine whether to block or permit a website, but routes the web traffic itself directly to the Internet. Direct Connect also routes traffic to the cloud service to perform content analysis, if configured in your policy. Direct Connect is recommended for scenarios in which proxy connections may be problematic.

The differences between endpoint agents are further outlined below.

## Neo

The **Neo** endpoint agent is a single agent that installs on the endpoint machine and includes both proxy connect and direct connect modes. Neo can automatically switch between the two modes depending on network conditions and performance.

Once Neo is activated, full functionality of proxy connect or direct connect is available. Neo uses the appropriate endpoint mode, based on network conditions. When proxy connect mode is in use but cannot connect to the proxy or if performance becomes an issue, Neo will switch to the direct connect mode.

Neo collects activity data from the endpoint and, for customers who have purchased Forcepoint Dynamic User Protection, sends the data there where it is analyzed for the purpose of risk score calculation.

## Proxy Connect (Classic)

The **Proxy Connect** endpoint redirects all traffic to the cloud proxy for analysis. Proxy Connect is ideal where proxy connections can be used without issue. This endpoint type supports the widest set of security features, such as data security scanning. Proxy Connect is regarded as the default option, and is recommended for most situations.

For more information on the current version, please see the Release Notes for Forcepoint Web Security Proxy Connect Endpoint, available in the portal on the **Web > Endpoint > General** page.

## Direct Connect (Classic)

The **Direct Connect** endpoint contacts the cloud service for each request, to determine whether to block or permit a website, but routes the web traffic itself directly to the Internet. Direct Connect also routes traffic to the cloud service to perform content analysis, if configured in your policy, and connects to the cloud service to retrieve its configuration settings.



### Note

The Direct Connect endpoint is not suitable where data security features are required, since this requires all traffic to be directed to the cloud service.

Direct Connect endpoint is designed for use in situations where the use of proxy connections may be problematic. Direct Connect endpoint can improve the security and usability of the service in the following scenarios:

- Off-site (roaming) users for whom proxy connections may cause issues

- In complex or changing network environments
- In areas where geographic firewalls prohibit the use of proxies
- When users need to access websites that do not work well with a proxy
- When users need to use non-browser or custom applications that do not work well with a proxy
- When geographically localized content is critical.



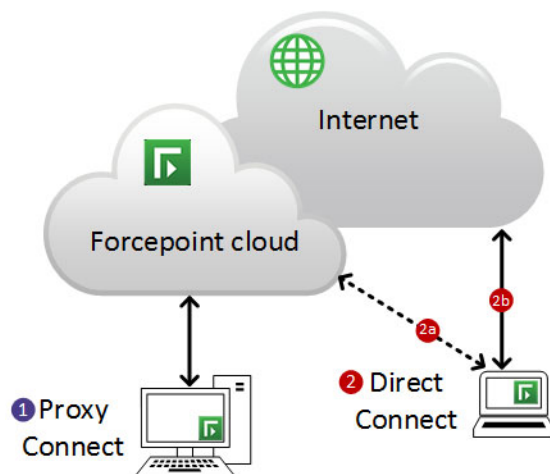
### Important

While the Direct Connect endpoint can provide improved security coverage in these scenarios, administrators should check that the networking requirements and level of feature support are acceptable for your intended deployment.

For more information on feature support, see the Release Notes for Forcepoint Web Security Direct Connect Endpoint, available in the portal on the **Web > Endpoint > General** page.

## Endpoint connectivity

The following diagram illustrates the connectivity for Proxy Connect (through Neo or the Classic Proxy Connect endpoint) and Direct Connect (through Neo or the Classic Direct Connect endpoint).



The diagram shows the two different endpoint versions servicing a web request:

- 1) In the first scenario, Neo or the Classic Proxy Connect endpoint directs all web traffic via the cloud proxy. If the request is permitted, the proxy connects to the requested website and sends content back to the end-user client. (If the request is blocked, the user is shown a block page.)
- 2) In the second scenario, a web request via Neo or the Classic Direct Connect endpoint consists of two stages:
  - a) The endpoint connects to the cloud service to look up the user's policy settings for the requested site.
  - b) If the request is permitted, the client then redirects the request directly to the Internet. (If the request is blocked, the user is redirected to a block page.)

If required, you can deploy a combination of Proxy Connect and Direct Connect endpoints in your organization. However, only one classic endpoint instance (Classic Proxy Connect or Classic Directory Connect) can be installed on a client machine at any one time. The Neo endpoint agent includes both proxy connect and direct connect modes.

**Note**

Neo is regarded as the default option and is recommended for most situations.

If in doubt about which version is appropriate for your deployment, please consult the endpoint release notes, and/or contact Technical Support for advice.

## Endpoint deployment options

Neo, Classic Proxy Connect, and Classic Direct Connect endpoint versions can be deployed on Windows and Mac operating systems (excluding iOS devices, such as iPhones, iPods, or iPads).

After configuring the endpoint client (as described in the next section), you have the following deployment options:

### Windows operating system users

- Download the endpoint installation file for Windows and:
  - Push it manually to selected client machines using your preferred distribution method - for example, Microsoft Group Policy Object (GPO).
  - (*Classic Proxy Connect only*) Allow users to download and install the endpoint software themselves from a link that you provide.
- (*Classic Proxy Connect only*) Deploy the endpoint client to the end users in a web policy directly from the cloud. Each affected user is asked to install the endpoint software on their machine when they start a browsing session. See *Endpoint tab*.

### Mac operating system users

- Neo
  - Download the endpoint installation package for Mac. (Neo for Mac is only supported on macOS 11 (Big Sur).)
  - Deploy to individual client machines using mobile device management (MDM), such as Jamf, which distributes the installation package to a group of machines and performs the installation on that group.
- Classic Proxy Connect and Direct Connect
  - Download the endpoint installation package for Mac on individual client machines and launch the installer by double-clicking the package.
  - Remotely install the endpoint client using MDM, such as Jamf, which distributes the installation package to a group of machines and performs the installation on that group.

Users who do not install the endpoint client are authenticated according to the options specified on the Access Control tab for their policy. Single sign-on is used if configured; otherwise the cloud-based service falls back to NTLM identification or basic authentication. Users are prompted to install the endpoint software each time they start a browsing session, until they complete the installation process.

**Related concepts**

[Endpoint tab](#) on page 178

# Configure General endpoint settings

---

Use the **General** tab of the **Web > Settings > Endpoint** page to configure settings that apply to all endpoint clients deployed in your network, and to find information needed for manual endpoint client deployment.

## Manage Neo

---

Click the **Forcepoint Neo management portal** link to open that portal in a new tab. Access to this option requires Modify Configuration permissions.

On the Neo management portal you can access the endpoint dashboard, endpoint management, and advanced settings. Use the advanced settings to control the auto- update mode and generate a release code to allow end users to uninstall the Neo endpoint.

Select *Dashboards*, *Endpoint management*, or *Settings* in the [Forcepoint Dynamic User Protection Help](#) for additional information.

## Select the default endpoint policy

---

Assign a default policy to users outside the network (roaming users) who are not synchronized to the cloud service as follows:

### Steps

- 1) Select a **Policy** from the drop-down list.
- 2) Click **Save**.

### Next steps

If you do not select a default policy, any non-synchronized user is auto-generated in the cloud service with their NTLM ID as reported by the endpoint client. The newly- created user becomes visible in the system within approximately 10 minutes. In the meantime, they are browsing anonymously and are reported as such.

Once the user is visible, you can assign them a different policy on the **Account > Settings > End Users** page, or assign them to groups on the **Account > Settings > Groups** page. Reports will also include the correct user information.

## Find and update deployment settings (Classic Proxy Connect and Direct Connect)

---

Use the WSCONTEXT code when deploying the endpoint client to Windows machines via GPO. More information about using the code can be found in the deployment instructions (*Windows operating system users*).

Before you can download the installation file or enable deployment from the cloud, you must define an anti-tampering password to be used to stop the endpoint service or uninstall the endpoint software. The password is automatically linked to any deployments of the endpoint client.





### Important

For security reasons, the cloud service does not retain a copy of your anti-tampering password. If you forget your password, you can reset it in the portal by entering and confirming a new password. All installed endpoints will be updated to use the new password next time they connect to the Internet.

To set the password:

## Steps

- 1) Click **Set Anti-Tampering Password**.
- 2) Enter and verify the password.
- 3) Click **Submit**.

## Next steps

The endpoint client has a number of key protections against tampering, which should prevent the majority of end users from uninstalling or deleting it, even if they have local administrator rights:

### Related tasks

[Windows operating system users](#) on page 99

## Windows and Mac operating systems

- Endpoint files and folders are protected from deletion and cannot be modified, moved, or renamed.
- The endpoint process will automatically restart if it is stopped or killed.
- A password is required to uninstall the endpoint client or stop the endpoint service.

## Windows operating systems only

- Endpoint registry settings cannot be modified or deleted.
- The Service Control command to delete the endpoint service is blocked.

## Download the endpoint client software

If you plan to deploy the endpoint client software manually, use the Endpoint Client Download table to download endpoint installers.

### Steps

- 1) Select your **Endpoint type**: **Neo**, **Proxy Connect (Classic)**, or **Direct Connect (Classic)**. See *Endpoint overview* to help select the appropriate type.
- 2) Select the operating system **Platform** on which the client software will be deployed.

- 3) Select the version to download the installation package.
- 4) Repeat for each type of endpoint client and operating system platform that you tend to deploy.

## Next steps

For deployment instructions, see:

- [Windows operating system users](#)
- [Mac operating system users](#)

Whether you are deploying the endpoint client manually or automatically, use the links provided to find information about the current endpoint software version.

### Related concepts

[Endpoint overview](#) on page 92

[Mac operating system users](#) on page 103

### Related tasks

[Windows operating system users](#) on page 99

# Configure endpoint End User Control settings

Use the **End User Control** tab of the **Web > Settings > Endpoint** page to define which users can enable or disable the endpoint client software on their machines.

It may be necessary to allow users to disable the endpoint client if they are working in a location that blocks web traffic to the cloud service. This can introduce vulnerabilities, since it permits end users to circumvent the protections offered by the endpoint software.



### Important

Priority precedence to add to the end user control list is:

- 1) Connections
- 2) Policy
- 3) Groups
- 4) Users

If an end user holds multiple group memberships, the application of the rule would require only one of them.

To allow users to disable the endpoint client:

## Steps

- 1) Toggle **End user control** to **ON**.
- 2) For **Apply to**:
  - Select **Specified users or selections** to allow those you specify to enable or disable the endpoint on their machines.
  - Select **Everyone except specified users or selections** to prevent those you specify from enabling or disabling the endpoint on their machines.
- 3) To add users to the end user control list, on the Users tab enter each user email address on a separate line in the **Users** field.
- 4) To select groups, policies, or connections to add to the end user control list, on the appropriate tab, click the item you want in the **Available** field, then click > to move it to the **Selected** field. **Ctrl + click** to select multiple items.
- 5) Click **Save** when done.

## Windows operating system users

---

To deploy the endpoint client manually to end users:

### Steps

- 1) Go to the **Web > Settings > Endpoint** page.
- 2) On the **General** tab, if you have roaming users who are not synchronized to the cloud service and wish to assign them to a particular policy once they browse via the endpoint, select a **Default endpoint policy** from the drop-down list. Click **Save**.
- 3) Under Deployment Settings, click **Set Anti-Tampering Password**.  
This anti-tampering password is not used when Neo is deployed. Neo uses a release code configured in the Neo management portal. See the instructions provided in the [Settings](#) section of the [Forcepoint Dynamic User Protection Help](#).
- 4) Enter and confirm your anti-tampering password, then click **Submit**.
- 5) Under Endpoint Client Download, if available in your account, select the type of endpoint you wish to download: Neo, Proxy Connect, or Direct Connect.
- 6) Select the version of the endpoint that you want to download. Click **Download**.
- 7) (*Neo*) Deploy Neo using the instructions provided in the *Neo installation* section of [Forcepoint Dynamic User Protection Help](#).

- 8) *(Classic Proxy Connect and Direct Connect)* Note the GPO configuration code displayed under Deployment Settings and use it to configure the msixexec command in your GPO deployment script or manual installation. This is in the format:

```
WSCONTEXT=xxxxx
```

Here, xxxx is a unique code for your account.

The code is required during installation to associate the endpoint with your customer account and enable your end users to log on transparently.

- 9) *(Classic Proxy Connect and Direct Connect)* On the **End User Control** tab, select whether end users have the option to enable or disable endpoint software on their machines. You may wish to enable this feature if your users are working in a location that blocks web traffic to the cloud service. Note that this option can introduce vulnerabilities: if enabled, it permits end users to circumvent the protections offered by the endpoint software.
- For **Apply to**, select **Specified users or selections** to allow those you specify to enable or disable the endpoint on their machines. Select **Everyone except specified users or selections** to prevent those you specify from enabling or disabling the endpoint on their machines.
  - To add users to the end user control list, on the Users tab enter each user email address on a separate line in the **Users** field.
  - To select groups, policies, or connections to add to the end user control list, on the appropriate tab, click the item you want in the **Available** field, then click > to move it to the **Selected** field. **Ctrl + click** to select multiple items.
  - Click **Save** when done.

## Installing and uninstalling Neo

For more information about installing and uninstalling Neo, select *Neo installation* in the [Forcepoint Dynamic User Protection Help](#).

## Distributing the endpoint via GPO (Classic Proxy Connect and Direct Connect)



### Note

See the *Neo installation* section of the [Forcepoint Dynamic User Protection Help](#) for information about distributing the Neo endpoint using Microsoft Endpoint Configuration Manager.

Details below apply to classic Proxy Connect and Direct Connect only.

Follow the steps below to deploy endpoint clients through an Active Directory group policy object (GPO). You need to write different installation scripts for a 32-bit versus a 64-bit operating system. Check in your script to see if the endpoint is installed, because your script should only install the endpoint if it is not already installed.

### Steps

- 1) Create a shared folder (create a folder and turn on sharing in the Properties menu).

- 2) Create a batch file (.bat) in the shared folder, for example "installmsi.bat". This can be done in any text editor.  
Type the following `msiexec` command into the batch file and save it.  

```
msiexec /package "\\path\WebSenseEndpoint.msi" /quiet /norestart  
WSCONTEXT=xxxx
```

  
Here:
  - *path* is the path to the installer that you downloaded from the portal
  - *xxxx* is the unique code noted from the Endpoint Download page in the portal
- 3) Test your batch file manually to make sure it runs on other workstations. You can do this by opening the server path to the file on a workstation and attempting to run the file. If the file does not run, check your permissions.
- 4) Open the Group Policy Management Console (GPMC).
- 5) Create a new (or open an existing) GPO on the organization unit (OU) in which your computer accounts reside. To create a new GPO:
  - a) In the console tree, right-click **Group Policy Objects** in the forest and domain in which you want to create a Group Policy object (GPO).
  - b) Click **New**.
  - c) In the **New GPO** dialog box, specify a name for the new GPO, and then click **OK**.
- 6) Open **Computer Configuration > Windows Settings > Scripts**, and double-click **Startup** in the right pane of the screen.
- 7) Click **Add**.
- 8) In the **Script Name** field type the full network path and filename of the script batch file you created in step 2.
- 9) Click **OK**.
- 10) Close the GPMC.
- 11) Run the `gpupdate /force` command at the command prompt to refresh the group policy.

## Next steps

The application should be installed on startup. The client may not be fully functional until a reboot occurs.

# Installing the endpoint on a single machine (Classic Proxy Connect and Direct Connect)

Follow the steps below to deploy an endpoint client on a single machine.

## Steps

- 1) Unzip the downloaded endpoint file to a location on the machine.
- 2) Open a command-line window, and navigate to the location of the unzipped endpoint files.
- 3) Enter the following command:  

```
msiexec /package "WebsenseEndpoint.msi" /norestart WSCONTEXT=xxxx
```

Where `WSCONTEXT=xxxx` is the unique GPO configuration code noted from the Endpoint Download page in the portal.
- 4) To confirm the endpoint client is installed and running, go to **Start > Control Panel > Administrative Tools > Services**. Check that "Websense SaaS Service" is present in the Services list, and is started.

## Uninstalling the endpoint from Windows (Classic Proxy Connect and Direct Connect)

You can uninstall the endpoint client by doing the following:

### Steps

- 1) Go to **Control Panel > Programs and Features**, and select **Websense Endpoint**.
- 2) Click **Uninstall**.
- 3) Click **Yes** to continue. Then enter the endpoint anti-tampering password that you set in the cloud portal.
- 4) Click **OK** to begin uninstalling the endpoint.
- 5) You will receive a confirmation message if the endpoint was successfully uninstalled.

### Next steps

You can also uninstall the endpoint through the command line by running this command:

```
msiexec /uninstall "<path>\WebsenseEndpoint.msi" /qb / promptrestart XPSWDPXY=xxxx
```

Here, `<path>` is the path to your endpoint package, and `xxxx` is the anti-tampering password you set in the cloud portal.



#### Important

If you uninstall the endpoint client, be sure to restart your operating system or your web browsing experience may be affected.

To stop the endpoint client, navigate to the endpoint installation folder and run this command:

```
wepsvc -stop -password <password> wspxy
```

Replace `<password>` with the anti-tampering password.

# Mac operating system users

---

## Installing and uninstalling Neo

---

For more information about installing and uninstalling Neo, see this [Knowledge Base Article](#).

## Installing the endpoint (Classic Proxy Connect and Direct Connect)

---

To deploy the endpoint client manually to end users on a single machine:

### Steps

- 1) Navigate to the **Web > Settings > Endpoint** page.
- 2) On the **General** tab, if you have roaming users who are not synchronized to the cloud service and wish to assign them to a particular policy once they browse via the endpoint, select a default policy from the **Policy** drop-down list. Click **Save**.
- 3) Under Deployment Settings, click **Set Anti-Tampering Password**.  
This anti-tampering password is not used when Neo is deployed. Neo uses a release code configured in the Neo management portal. See the instructions provided in the *Settings* section of the [Forcepoint Dynamic User Protection Help](#).
- 4) Enter and confirm your anti-tampering password, then click **Submit**.
- 5) Under Endpoint Client Download, select Mac from the Platform drop-down list and click **Download** to download the endpoint zip file.
- 6) On the **End User Control** tab, enter users or select groups, policies, or connections who are allowed to disable the endpoint on their machines. You may wish to do this if your users are working in a location that blocks web traffic to the cloud service. Note that this option can introduce vulnerabilities: if enabled, it permits end users to circumvent the protections offered by the endpoint software.
  - To specify end users who can disable the endpoint client, enter each user email address on a separate line in the **Users** field.
  - To select groups, policies, or connections who can disable the endpoint client, click the item you want in the **Available** field, then click **>** to move it to the **Selected** field. Use the **Ctrl** key to select multiple items.
  - Click **Save** when done.

- 7) (Classic Proxy Connect only) If you want the Classic Proxy Connect endpoint client to use port 80 for proxying and PAC file retrieval, do the following before installation:
  - Ask your endpoint support representative to add the “Send HWS endpoint to port 80” template to your account. You can add this template globally, or to specific policies.
  - Look at the endpoint client files, and locate the endpoint.pkg and HWSConfig.xml files. The latter is specific to your account. The files must reside in the same directory for the endpoint to successfully install.
  - In the HWSConfig file, make the following change:  
Change this:  

```
<PACFile URL="http:// webdefence.global.blackspider.com:8082/proxy.pac" />
```

  
To this:  

```
<PACFile URL="http:// pac.webdefence.global.blackspider.com/proxy.pac" />
```

  
By applying this template, you will also move to port 80 any Proxy Connect endpoints that are already installed.
- 8) Double-click the endpoint package to open an introductory screen for the installer. Click **Continue** for step-by-step instructions on the installation process.
- 9) When you reach the “Standard install on Macintosh HD” screen, click **Install** to begin the installation process.  
You must install the endpoint on the local hard disk. You can change the installation location on this screen by clicking **Change Install Location...**
- 10) Enter a user name and password for a user with administrator rights to install the software.  
If the installation process fails, check that the HWSConfig.xml file is present and is in the correct format if you have edited it.
- 11) A confirmation screen informs you if the installation is successful. Click **Close**.
- 12) After installation, go to **System Preferences > Other**.
- 13) Click the icon for the endpoint program.  
This brings you to a page where you can see components for the version you have installed. You can also do the following:
  - **Save Debug Logs to Desktop**  
This allows your endpoint support team to quickly access all troubleshooting logs in one place. Clicking it creates an archive file on the Mac desktop beginning with ClientInfo\*.zip. If you need to open a support ticket about the endpoint, include this zip file with your request.
  - **Uninstall Endpoint**  
See *Uninstalling the endpoint from the Mac (Classic Proxy Connect and Direct Connect)*.

### Related tasks

[Uninstalling the endpoint from the Mac \(Classic Proxy Connect and Direct Connect\)](#) on page 105



# Identifying Mac endpoint end users

When a Mac user is logged into an active directory-based domain, the endpoints identify users in the same way as for Windows operating system users. For Mac users not logged into a domain, however, the endpoint formats the user details in the cloud service as `mac.local.[local_username]@[local_address]`.

For example, if you are logged in as “Joe Bloggs,” it might appear as `mac.local.joebloggs@123-nosuchdomain.autoregistration.proxy`.

To search for all locally logged-on Mac users, do the following:

## Steps

- 1) Go to **Account > Settings > End Users**.
- 2) In the **Name** field, enter “mac.local\*”
- 3) Click **Search**.

## Next steps

This brings up a list of all Mac users that are logged on locally.

# Changing the policy of a Mac end user

To change the policy of a Mac user, do the following:

## Steps

- 1) After searching for all locally logged-on users (see *Identifying Mac endpoint end users*), the list that displays allows you to select **Change Web Policy** from the **Please select an action...** drop-down menu.
- 2) Choose the policy that you want to move the selected Mac user to.
- 3) Select each of the displayed Mac users you want to move and click the **Go** button.  
The new policy is applied to these users.

Note that two Mac usernames will be common across all of your Mac users: `mac.local.root` and `mac.local._softwareupdate`. These users receive software updates from the Internet. It is recommended that access to these users be limited to just a few categories, such as Information Technology.

### Related tasks

[Identifying Mac endpoint end users](#) on page 105

# Uninstalling the endpoint from the Mac (Classic Proxy Connect and Direct Connect)

You can uninstall the endpoint client by doing the following:

## Steps

- 1) Go to **System Preferences > Other**, and click the icon for the endpoint software.
- 2) Click **Uninstall Endpoint**.
- 3) Enter the local administrator name and password.
- 4) Enter the local administrator name and password.
- 5) Click **OK** to begin uninstalling the endpoint client.
- 6) You will receive a confirmation message if the endpoint client was successfully uninstalled
- 7) Click **OK** to finish the process.

## Next steps

You can also uninstall the endpoint client through the command line:

- 1) After entering the Mac administrator password, run this command:  

```
sudo wpepsvc --uninstall
```
- 2) You will be asked for the anti-tampering password that you set in the portal.

To stop the endpoint client, do the following through the command line:

- 1) After entering the Mac administrator password, run this command:  

```
sudo wpepsvc --stop
```
- 2) You will be asked for the anti-tampering password that you set in the portal.

# Updating the endpoint



### Note

For Neo, automatic updates are enabled by default but can be configured on the Neo management portal, accessed from the **Web > Settings > Endpoint** page. For more information, see the *Settings* section of the [Forcepoint Dynamic User Protection Help](#).

Details below apply to classic Proxy Connect and Direct Connect only.

# Windows operating system users

For users with Windows operating systems, the Endpoint tab in your web policies includes an auto-update feature which can automatically deploy newer versions to browsers without desktop administrators getting involved. If you select this option, it applies to all users in the policy who have installed the endpoint client, regardless of whether it has been deployed via GPO or directly from the policy, assuming their browser supports deployment from the cloud. For more information, see *Endpoint tab*.

To deploy endpoint updates via GPO, first download the latest version from the **Web > Settings > Endpoint** page. The latest version appears at the top of the list of available downloads.

You can check which version of the endpoint client your end users have by running the Installed Endpoint Client Statistics report.

#### Related concepts

[Endpoint tab](#) on page 178

## Mac operating system users

For Mac operating system users, the endpoint client for the Mac can automatically deploy newer versions to browsers without involvement from desktop administrators.

## Endpoint bypass

If you have deployed the endpoint client to your end users, occasionally some applications do not work properly in conjunction with endpoint enforcement. This is more likely with the Proxy Connect endpoint and might affect, for example, custom- designed applications for your organization.

If you are experiencing problems with applications on end users' machines, use the **Endpoint Bypass** tab of the **Web > Settings > Endpoint** page to add the names of any applications that you want to bypass endpoint policy enforcement. For the Proxy Connect endpoint, this feature does not work for applications that use system browser settings to determine a proxy.



#### Note

You must update your endpoint deployments, if required, to a version that supports this feature. See *Updating the endpoint*.

#### Related concepts

[Updating the endpoint](#) on page 106

## Application entries in the endpoint bypass list

This section explains about the addition and deletion of the application entries in the following endpoint bypass lists:

- Standard Application Bypass List
- List Extension for Newer Neo Endpoints

## To add/delete an application entry in the Standard Application Bypass List:



### Note

- You can add up to 1920 characters only in the Standard Application Bypass List.
- Entries in this Standard Application Bypass List are applicable to both Neo and F1E endpoint types and versions.
- Make sure to enter both the domain and the extension for Microsoft application. For example, thissite.com and thissite.net are distinct entries. Apple applications do not need extension.

### Steps

- 1) Click the **Windows** tab to add the Microsoft applications or **Mac** tab to add the Apple applications.
- 2) Click **Add** below to the Standard Application Bypass List.
- 3) Enter one or more application names in the Applications field.
  - Ensure you include the file extension where appropriate, for example myapp.exe
  - You can use the asterisk wildcard in the application names, for example app.\*
  - Separate multiple application names with commas
- 4) Click **Add**.
- 5) To delete an application, select its check box and then click **Delete**.

## To add/delete an application entry in the List Extension for Newer Neo Endpoints:



### Note

- If you have the Newer Neo Endpoint, then you can add up to 1920 further characters, in addition to the 1920 characters already entered in the standard list.
- Newer Neo Endpoint versions use both the Standard List and Extension List bypass entries. The specific version number that defines the newer Neo Endpoint will be show in the UI.

### Steps

- 1) Click the **Windows** tab to add the Microsoft applications or **Mac** tab to add the Apple applications.
- 2) Click **Add** below to the List Extension for Newer Neo Endpoints.

- 3) Enter one or more application names in the Applications field.
  - Ensure you include the file extension where appropriate for Microsoft applications, for example myapp.exe

**Note**

For Mac applications, do not include the file extension.

- You can use the asterisk wildcard in the application names, for example app.\*
  - Separate multiple application names with commas
- 4) Click **Add**.
  - 5) To delete an application, select its check box and then click **Delete**.

## Next steps

If you want to move any application entry from one list to another, you can do that by clicking the left and right navigation arrows.

The used character count is displayed at the top of the table specific to the list type selected. The exact number of characters depends on how the regex is calculated rather than matching exactly with the number of characters typed.

Click **Save** to keep the changes.

# Configure protected cloud apps

The **Web > Settings > Protected Cloud Apps** feature allows you to nominate a set of cloud applications to use within your organization that are protected by Forcepoint CASB. Forcepoint CASB is an integrated solution for cloud application access discovery, activity analysis, access control, security monitoring and enforcement, governance, policy compliance, and data loss prevention.

**Note**

The Protected Cloud Apps feature requires an additional license. If you would like further information on accessing this feature, please contact your account manager.

The Protected Cloud Apps feature cannot be used with the Direct Connect endpoint or Neo when it is in direct connect mode.

Use the Protected Cloud Apps page to connect the service to your Forcepoint CASB account, to manage the applications that are protected, and to open the Forcepoint CASB management portal. When an end user accesses one of your protected cloud apps, the service forwards traffic to Forcepoint CASB for analysis, and CASB determines whether to allow the request or apply an enforcement action, based on your CASB configuration.

To protect cloud app usage via Forcepoint CASB:

## Steps

- 1) Navigate to **Web > Settings > Protected Cloud Apps**.

- 2) Set the **Enable connection with Forcepoint CASB** toggle switch to **ON**.
- 3) In the dialog, enter the connection details provided in the fulfillment letter you received when you purchased your Forcepoint CASB license.  
If your fulfillment letter did not include these details, configure a new API access key on the **Settings > Access Management > API page** of the Forcepoint CASB portal. See **Create a new API access key** in the [Forcepoint CASB Administration Guide](#) for instructions.
  - Access key ID
  - API key secret
  - Service URL
- 4) Click **Connect**.  
The list of cloud apps (referred to as assets in CASB) is automatically populated with the list that is in CASB, including customer apps that were created. The list changes based on changes made in the CASB portal.
- 5) From the list of cloud apps, select which apps to protect in Forcepoint CASB. You can select up to the maximum number of apps that your CASB license covers.  
Use the scrollbar, or begin typing the name of an app in the Search field. To view only the apps that are currently selected, set the search menu drop-down menu to **Selected apps**.
- 6) The list of selected apps can be used by all policies or applied to a specified subset of policies. In the Traffic Forwarding section, **Forward traffic to Forcepoint CASB**:
  - **For all policies** (the default) to forward all user requests to any of the selected apps to Forcepoint CASB for enforcement.
  - **Per policy** to select the policies that should use the list of selected apps when the policy is enforced.
- 7) When **Per policy** is selected, the **Forward to Forcepoint CASB** column provides the complete list of existing policies. Use the arrows to move selected policies for which protected cloud apps should not be applied to the **Do Not Forward to Forcepoint CASB** column.  
Use the arrows to move policies from one list to the other.
- 8) When you are done, click **Save**.

## Next steps

While the **Enable connection with Forcepoint CASB** switch is set to **ON**, traffic for these cloud apps is forwarded to CASB for analysis and protection.

To stop CASB from protecting your traffic, set the switch to **OFF** and click **Save**.



### Note

Setting the connection with Forcepoint CASB to **OFF** has no effect on the cloud app usage and risk reporting features available in the *Cloud Apps Dashboard* and *Cloud App reports*. Reporting information is always recorded for cloud app activity, allowing you to discover and monitor cloud app usage in your organization.

See the [Cloud Security Gateway Integration Guide](#) for additional information.

**Related concepts**[Cloud Apps Dashboard](#) on page 22**Related reference**[Cloud App reports](#) on page 267

## Logging on to Forcepoint CASB

When a valid connection to Forcepoint CASB is enabled, you can log on to the Forcepoint CASB management portal to configure policy settings for your cloud app traffic.

To log on to Forcepoint CASB:

- Use the **CASB** option available in the toolbar to open the Forcepoint CASB management portal.
  - Users with account level **Modify configuration** permissions are logged in to the portal. (See *Configuring permissions*.)
  - All other users are required to provide login credentials to access the portal.
- Click one of the buttons beneath the app selection box. Forcepoint CASB opens to the relevant page in a new browser tab.
  - **View Incidents**: open the Forcepoint CASB incident log to view incidents such as alerts and policy violations.
  - **View Access Policies**: manage user access policies for cloud apps within your Forcepoint CASB account.
  - **View Assets**: manage settings for the cloud apps protected by Forcepoint CASB.

For more information on using Forcepoint CASB, see the [Forcepoint CASB Administration Guide](#).

**Related tasks**[Configuring permissions](#) on page 32

## Configure Full Traffic Logging settings

**Important**

The full traffic logging feature is not available by default. To make it available in your account, contact Support.

As an alternative, consider migrating to SIEM Integration. Take advantage of **Bring your own storage** or switch between Forcepoint storage and your own. See *Configuring SIEM storage*.

Use the **Web > Settings > Full Traffic Logging** page to enable the ability to download raw proxy request data from the cloud service for retention and analysis.

Mark the **Enable full Web traffic logging** checkbox to enable log retention for your account. Note that if you enable this feature, the cloud service starts saving large amounts of data that you must download to your own systems.

Log data is retained for 14 days. If you do not download the traffic data for a period of 14 days, log retention is disabled for your account.

For full details of how to set up and use full traffic logging, we strongly recommend you read the “Configuring Full Traffic Logging” technical paper.

You can also retain full traffic logs for specific policies. For more information, see *General tab*.

#### Related concepts

[General tab](#) on page 163

#### Related tasks

[Configuring SIEM storage](#) on page 28

## Configure custom categories

The cloud web service categorizes websites into dozens of built-in categories to help you manage your end users' web surfing. See *Category list* for further information about the built-in categories.

You can also create custom categories, each of which comprises a set of sites (for example, “[www.google.com](http://www.google.com)”) or URLs (for example, “<http://www.yahoo.com/index.html>”). Custom categories defined on the **Web > Policy Management > Custom Categories** page are created at the account level and are available to all policies.

For information on creating custom categories at the policy level, see *Custom Categories tab*.

Use the **Web > Policy Management > Custom Categories** page to view and manage the custom categories for your account.

If you have already created custom categories in a Forcepoint web on-premises solution, you can import them to the cloud service in CSV file format.



#### Note

There is a limit to the maximum number of custom categories and sites you can add. Based on analysis of custom category usage, this limit is designed to provide ample capacity. If you have any questions about the custom category limit, please contact Technical Support.

#### Related concepts

[Category list](#) on page 203

#### Related tasks

[Custom Categories tab](#) on page 191

## To create custom categories for your account



## Steps

- 1) Click **Add**.
- 2) Assign a name to your new custom category and give it a description.
- 3) Click **Submit**.
- 4) Add hostnames, IP addresses, IP address ranges, or URL paths. For detailed guidance on how to enter sites, and how entries are interpreted, see *Adding sites to custom categories*. Note the following general guidance:
  - Ensure that hostnames are added only once.
  - Protocols (for example “http://”, “ftp://”) are ignored. Entries are matched to all protocols.
  - Standard ports for the protocol being used are ignored (for example, ports 80 for HTTP, and 443 for HTTPS).
- 5) Click **Add** again.  
Use the buttons at the bottom of the page to **Download sites** to or **Upload sites** from a CSV file. A downloaded file can be edited and then uploaded for easy maintenance of the list of sites for the category.



### Important

When a file is uploaded, the contents of the file will replace the list of sites previously associated with the category. It will not add to that list.

### Related concepts

[Adding sites to custom categories](#) on page 114

# To import a custom categories file from a Forcepoint on-premises solution

## Steps

- 1) Click **Print Policies to File** on the Policies page in the on-premises management console.
- 2) Locate the Custom Categories and Recategorized URLs sections in the output file.
- 3) Copy your custom categories and recategorized URLs to a CSV file using this format:  
CategoryName, RecategorizedURL  
CategoryName, RecategorizedURL  
CategoryName, RecategorizedURL
- 4) Save the CSV file.

- 5) In the cloud portal, click **Import File** on the **Web > Policy Management > Custom Categories** page.
- 6) In the Import Custom Categories dialog box, browse to your CSV file and click **Import File**.

## Next steps

These custom categories can be used in the same way as the built-in categories; see *Category list* for further information.

Use the toggle at the bottom of the page to **Enable custom categories per policy**. If this option is disabled, the Custom Categories tab is not available on the **Web > Policy Management > Policies** page and policy level custom categories cannot be added.

When this option is enabled, all policy level custom categories display by policy.

### Related concepts

[Category list](#) on page 203

## Adding sites to custom categories

When adding sites to a custom category, you can add hostnames, IP addresses or address ranges, or URL paths.



### Note

Certain characters have significance to the pattern matching mechanism, and should be preceded with a backslash (\). These characters are: [ ] { } \ + \*

## Hostnames

Enter hostnames without a protocol, for example: abc.com. This will match:

- Any resource at the domain, using any protocol (for example <http://abc.com>, <https://abc.com>, <ftp://abc.com>).
- Any subdomains of abc.com using any protocol, for example [www.abc.com](http://www.abc.com), [123.abc.com](http://123.abc.com), [www.123.abc.com](http://www.123.abc.com).

You can use a wildcard (\*) within a hostname or at the beginning of a hostname. Wildcards at the beginning of a hostname match any hostname that ends with the string you enter, for example \*abc.com matches 123abc.com, and any subdomains (for example [www.123.abc.com](http://www.123.abc.com), [www.xxx.123abc.com](http://www.xxx.123abc.com)).

A wildcard at the beginning of a hostname, followed by a dot (\*.abc.com) matches any subdomains of abc.com (for example 123.abc.com), but **not** the abc.com domain itself.



### Note

Wildcards placed at the **end** of the string are removed.

## URL paths

Any address with a slash (/) following the hostname or IP address is treated as a URL path (for example [www.abc.com/](http://www.abc.com/), [www.abc.com/mysite](http://www.abc.com/mysite)).

If you specify a URL path, it is treated as the start of a path, and matches anything beginning with the string you enter (for example, [www.abc.com/mysite](http://www.abc.com/mysite) matches [www.abc.com/mysite/folder/page.htm](http://www.abc.com/mysite/folder/page.htm)).



#### Note

URL paths will not match for HTTPS requests unless SSL decryption is being performed. For HTTPS requests, the full path is not provided to the proxy.

## IP addresses

Enter IPv4 IP addresses or ranges in one of the following formats:

- **Explicit address:** a single address. Example: 12.13.14.15
- **Explicit range:** 2 addresses separated by a dash (-). Example: 12.13.14.15- 12.13.14.99 (a space before and after the dash is allowed, but not required)
- **Subnet:** An address followed by a slash (/) and the number of bits, which is a number between 1 and 32. Example: 12.13.14.15/24
- **Subnet with subnet mask:** an address followed by a slash (/) and a netmask. Example: 12.13.14.15/255.255.255.0



#### Important

If you have entered an IP address range, subnet, or subnet mask, be sure your entry does not have unintended impact. When a policy is applied, all addresses are handled the same way. For example, if the category is blocked, all qualifying addresses are blocked.

IP addresses and ranges are used to match the resolved address of a requested hostname, using any protocol and port.

## Ports

If you include a port number that is the standard port number for the protocol being used (for example port 80 for HTTP, port 443 for HTTPS), the port number is ignored and the entry is treated as described above. If the port number is a non-standard port for the protocol being used, the proxy will match only URLs that include the port number.

For example, if you enter [www.abc.com:8080/](http://www.abc.com:8080/), then <http://www.abc.com:8080/mysite> will match, but <http://www.abc.com/mysite> will not.

## Time periods

The cloud service allows you to configure policies that restrict web surfing by time of day for either the whole policy or for website categories, users, and groups. When an exception rule is configured, it is applied to a time period.

Use the **Web > Policy Management > Time periods** page to configure time periods for your account. These are configured at the account level so that they can be available for use in multiple policies, if required.

Each account is provided with 4 default time periods.

## To edit or view a time period

---

Click the name of a time period (for example, “Working hours”).

You can assign the time zone for the period, which is typically the default for the policy or connection where the users are located (see *Proxied connections*).

The dark area defines the actual time period. Each division is a 15 minute period and can be set with either a single click or by clicking and dragging to produce a wider area. As you roll your mouse over the area, the absolute time is displayed below the time chart.

### Related concepts

[Proxied connections](#) on page 168

## To define a new period

---

### Steps

1) Click **Add time period**.

2) Enter a name and description for the new period.

3) Choose a time zone.

If you do not want to use the default for the policy or connection, you can select a particular geographical location and city (for example Australia/Sydney), or a time zone such as GMT or UTC.



#### Note

Daylight saving time is supported where valid on all time zones except GMT and UTC, which are static. For example, if you select GMT, British Summer Time is not taken into account for this time period.

4) Click the **Paint** radio button.

5) Click and drag the mouse over the desired time period. Release the mouse when you're done.

6) Click **Submit** to save your changes.

## To delete a period

---

If you want to delete a time period, make sure that it is not being used by any rules first. If it is in use, the **Delete** button is grayed out.

# Configure custom protocols



## Important

This feature requires an I Series appliance.

The **Policy Management > Protocols** page provides a list of the protocol groups in the cloud service database. Each protocol group includes similar types of Internet protocols (like FTP or IRC) and applications (like MSN Messenger or BitTorrent). The database of protocol groups is updated regularly. These protocols cannot be edited or deleted.

You can also add, edit, or delete custom protocols on the Protocols page. Custom protocols are available to all policies.

- Use the **Search** field to search for a particular protocol or group in the protocols list.
- To define a new custom protocol, click **Add**. See *Adding or editing a custom protocol* for instructions.
- To modify a custom protocol, select it in the list and click **Edit**. See *Adding or editing a custom protocol* for instructions.
- To remove a custom protocol, select it in the list and click **Delete**.

## Related tasks

[Adding or editing a custom protocol](#) on page 117

## Adding or editing a custom protocol

On the **Web > Protocols > Protocol Details** page, use the following steps to define or modify a custom protocol:

### Steps

- 1) Enter or modify the unique protocol name. Use only alphanumeric characters.
- 2) Select a group from the drop-down list (default value is **User Defined**).
- 3) Click **Add** to display the Add Protocol Identifier dialog box, or click an existing Port/Range link to display the Edit Protocol Identifier in dialog box.

- 4) Specify the following details:
  - a) Ports: You can select **All ports** or **Specific port/range** (default selection) to indicate a single port or port range. Separate the components of a port range with a hyphen.
  - b) IP addresses: You can select **All IP addresses** or **Specific IP address/range** (default selection) to indicate a single IP address or address range. Separate the components of an address range with a hyphen.
  - c) Transport method: Select either **TCP** or **UDP**.  
Transmission control protocol (TCP) is slower than UDP but provides reliable, ordered data delivery. User datagram protocol (UDP) is stateless and therefore faster than TCP, but it can be unreliable.
  - d) Click **OK**. Your identifiers appears in the Protocol Identifier list.
- 5) Repeat steps 3 and 4 for each additional identifier that you want to define or modify.
- 6) Click **Save**.
- 7) To delete a protocol identifier, select it in the list and click **Delete**.

## Configure block and notification pages

Use the **Web > Policy Management > Block & Notification Pages** page to view or edit block page text and notification messages for your account.

When a cloud 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 web 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.

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

General notification pages that you create are listed under Custom. Custom AUP pages are listed under Acceptable Use Policy (a limited-availability feature that may not be enabled for your account).

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:

### Steps

- 1) Click **New Page** for a new notification page or **New AUP Page** for a new Acceptable Use Policy 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.

## Next steps

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

For additional information about AUP pages, see *Acceptable use policy*.

### Related tasks

[Editing notification pages](#) on page 121

[Acceptable use policy](#) on page 166

# Default 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.

The end user registration pages for secure form-based authentication are already available in the following languages: French, German, Italian, Dutch, Spanish, Simplified Chinese, and Japanese.

See *Language support*.

### Related tasks

[Language support](#) on page 125

## Default logo

By default, the logo displayed on the notification pages is the Forcepoint Web 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**.



### Note

If you choose to display a custom logo, we recommend that you host it on an HTTPS site. This ensures that your end users do not see warnings about unsecure elements on notification pages that use HTTPS, such as end-user registration and secure form authentication.

## 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**.

## HTTPS notifications

To enable the cloud proxy to serve the correct notification page to the user for HTTPS sites - for example, a block page if the site is in a category that the end user is prevented from accessing, or the *Pre-logon welcome page* for authentication - you need a root certificate on each client machine that acts as a Certificate Authority for secure requests to the cloud proxy.

To install the root certificate for your end users and enable notification pages for HTTPS sites:

### Steps

- 1) In the Settings area, click the **root certificate** link and download the certificate to a location on your network. You can then deploy the certificate manually, using your preferred distribution method



- 2) Once the certificate has been deployed, return to this page and mark **Use certificate to serve notifications for HTTPS pages**.
- 3) Click **Save**.

### Related concepts

Pre-logon welcome page on page 174

## Editing notification pages

Each notification 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 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.
  - To add a variable to the section, click **Variables/tokens**, and select from the drop-down list. See *Notification page variables*, page 120.Click **OK** when done.
- 5) To edit the page footer:
  - a) Click the footer section to open a text editor window.
  - b) If you have already specified *Default footer text*, clear the **Use default footer text** box.
  - c) 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.
  - d) Click **OK** when done.

- 6) To edit an image on the page:
  - a) Click on the image. The Image Properties pop-up window is displayed.
  - b) To use one of the standard images provided by the cloud service, 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.

**Note**

Your browser may warn you that you are switching to an unsecured connection.

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

If you wish to discard customizations 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 the cloud service.

**Related tasks**

[Default footer text](#) on page 120

**Related reference**

[Notification page variables](#) on page 122

## Notification page variables

Some mark-up strings or variables are available. At the time a page is rendered to the end user, these are replaced either with request-specific or user-specific data or with values configured elsewhere in the system. The parameters are generally textual components of the page and their use should be clear from the page preview.

Variables have the following attributes:

- Variables are always surrounded by underscores, for example, `_URL_`
- If the cloud service recognizes a variable, it replaces it with the value it represents. If it does not recognize a variable, it leaves it untouched.

The following variables are available.



#### Note

When you edit a notification page, the **Variables/tokens** drop-down list contains the only variables that are relevant to that page. From the list of valid variables, hover over the name to see the associated HTML value.

Manually entering a variable name on the **Edit Page Content** panel that is not included in the drop-down might result in the variable name displaying as part of the notification page.

Variable	Description
Category	The web category that applies to the requested site and has triggered the block or notification page.
Client IP address	The IP address of the user attempting to authenticate, register, or access a web page. This is optional on most pages, and can be submitted for reporting purposes when a user authenticates or confirms that they want to access the URL via quota time or continue/confirm. It is mandatory on the secure form logon page.
Agree Acceptable Use Policy	Link to accept your Acceptable Use Policy and continue to the requested website. Mandatory on any Acceptable Use Policy page.
Close Acceptable Use Policy page	Link to close an Acceptable Use Policy page without agreeing to the policy. Mandatory on those pages.
Cloud app name	The cloud application that the user is trying to access.
Content category	Use to show the type of sensitive content that was detected. For example, regulations, data theft, or custom.
Content classifier	Use to show the content classifier that was matched. For example, key phrase, regular expression, or dictionary.
Custom text	Use to include your own text on an Acceptable Use Policy page.
File extension	Displays the file extension that the user has attempted to access when file extension blocking is in use.
Maximum file size	Displays the maximum file size allowed when file size blocking is in use.
Requested file size	Displays the size of the file that the user has attempted to access when file size blocking is in use.
Host name	The host name of the site that the user is trying to access.
Login host name	The host name used for transactions involved in logging on to the cloud service. For example, clicking the 'Log in' button on the Welcome page submits a form to this host.

Variable	Description
Login URL	Link to log on to the cloud service using basic authentication or NTLM identification.
HTTP request method	The 'method' in the HTTP request that is being handled (for example, 'GET', 'POST')
NTLM domain name	The domain part of a user's NTLM ID.
NTLM ID	User's NTLM ID, in the format domain\username.
NTLM username	The user name part of a user's NTLM ID.
Policy name	The policy that has been applied to the web request.
Protocol	Either HTTP or HTTPS. Used in embedded URLs, such as image links, so the service can use a common page for mixed HTTP and HTTPS without getting browser warnings that the page uses one protocol but image links use the other one.
Quota time disabled	Used on the quota page to disable the OK button when the user's daily quota has been used up.
Quota remaining	The number of minutes remaining in the user's daily quota time.
Quota session length	The session length available to the user if they choose to use quota time to browse the site they have requested, as well as other sites in that category (if per-category quotas are enabled) or that are in categories set to use quota time.
Reason	The reason the request was blocked. Only valid on pages triggered by a blocked request.
Registered email address	End user's email address as registered in the cloud service. This address is used to send emails as part of the end-user registration process and the password reset process.
Registration URL	Link included in forgotten password and end-user registration email notification templates. When clicked, the link takes the user to a page where they can reset their password or complete their registration. This is mandatory in both email notifications.
Requested URL	The URL that the user is attempting to access, and that has caused the block or notification page to be displayed. If the notification page is a request for authentication, or to use quota time or continue/confirm, the user is automatically redirected to the URL when they authenticate or confirm.
Username	End user's user name. Can be used on an Acceptable Use Policy compliance page, or in end-user notification emails for password resets and self-registration.

# Language support

You can create multiple language versions of block and notification pages to display to end users, allowing a single corporate policy to be applied to a multi-national user base. If you create multiple language versions of standard or custom pages, the most appropriate version of the page is served to end users based on their browser settings. The language version displayed to end users will be the version that matches the primary language set in the user's browser, if a version exists for that language. If a version does not exist, the default language version will be used.

The default language for block and notification pages is English. You can change this default in the Settings area of the **Block & Notification Pages** page (see *Default notification page settings*).

To add a different language version for a notification page:

## Steps

- 1) Click the page name to open it for editing.
- 2) Click **Add Language**.
- 3) Select the languages you wish to add from the Available Languages panel. You can use the Shift and Ctrl keys to select multiple languages.
- 4) Click the right arrow (>) to move the languages to the Selected languages list.
- 5) Click **OK**.

## Next steps

The languages you selected are now available in the **Languages** drop-down list. Select a language from the list to edit the page content for that language, as described in *Editing notification pages*.

To delete a language version of a notification page, click **Delete Language**.



### Note

You are responsible for translating and editing the content for different language versions of a notification page.

### Related concepts

[Default notification page settings](#) on page 119

### Related tasks

[Editing notification pages](#) on page 121

# Configure Content Classifiers for Data Security (DLP Lite)

Use the **Web > Policy Management > Content Classifiers** page to classify your data using custom phrases, dictionaries, or regular expressions containing business-specific terms or data. This can help to prevent the loss of intellectual property or sensitive data over the web.

Once content classifiers are defined, select the classifiers that you want to enable for the policy using the Data Security tab in the policy. (See *Custom* for instructions.)

You can use more than one classifier in your policies to reduce false positives.



## Note

The total number of content classifiers you can create in your account is 100.

## Related concepts

[Custom](#) on page 216

## To edit or view a content classifier

### Steps

- 1) Click a classifier name to view details on the classifier.
- 2) Use the Edit screen to modify the name, description, or value of the classifier. You cannot edit its type.
- 3) Click **OK** when you're done.

## To delete a content classifier

### Steps

- 1) Select one or more classifiers.
- 2) Click **Delete**.
- 3) When asked if you are sure you want to delete the classifiers, click **Yes**.



## Note

You cannot delete classifiers that are being used in a policy. You must remove the classifier from all the web policies that use it before you can delete it.

# To define a new content classifier

## Steps

- 1) Click **Add** and select one of the following:
  - **Regular expression:** used to describe a set of search criteria based on syntax rules. For example: `(abc{21,40}){1,30}`  
See *Regular expression content classifiers*.
  - **Key phrase:** a keyword or phrase that indicates sensitive or proprietary data (such as product code names or patents).  
See *Key phrase content classifiers*.
  - **Dictionary:** a container for words and expressions relating to your business. See *Dictionary content classifiers*.
- 2) Complete the fields, and then click **OK**.  
Instructions for completing the fields for each classifier type is provided in the topics referenced in step 1.
- 3) Repeat steps 1-2 until you've added all the classifiers you require.

### Related reference

[Regular expression content classifiers](#) on page 127

[Key phrase content classifiers](#) on page 129

[Dictionary content classifiers](#) on page 129

## Regular expression content classifiers

Regular expression (regex) patterns can be detected within content, such as the patterns found in U.S. Social Security numbers and credit card numbers.

You can define the patterns to search for using this screen.

When extracted text from a transaction is scanned, the system searches for strings that match the regular expression pattern and may be indicative of confidential information.

To create a regular expression classifier, complete the fields as follows:

Field	Description
Name	Enter a name for this pattern, such as Visa card.
Description	Enter a description for this pattern, such as Visa credit card patterns.

Field	Description
Regular expression pattern.	<p>Enter the regular expression for which you want the system to search, such as all 3-character strings followed by the sequence “123”. The expression should be compatible with Perl syntax.</p> <p>You can use alphanumeric characters and any of the following values:</p> <pre> .           Any single character [ ]        Any one character in the            set ^          Beginning of line [^]       Any one character not in the       set \s        White-space character           Or \r?\n     Line break \&lt;         Escape special character ?         Previous expression exists  or not  { }        Range or frequency ( )        The expression in the            parenthesis is treated as            one term \b        Word boundary \<x{hex-number} (0-9)="" <="" \d="" \w="" alphanumeric="" character="" digit="" non-alphanumeric="" non-digit="" pre="" unicode=""> <p>To include Unicode characters in your pattern, use the format <code>\X{hex- number}</code>.</p> <p>Do not use <code>+</code>, <code>*</code>, or <code>{X,}</code> without an upper limit. Instead use a limited quantifier such as <code>{0,500}/{1,500}/</code> <code>{X,500}/{X}</code>. When using a line break, use the exact syntax shown above.</p> <p>For example: <code>\b[a-zA-Z][347]d{3}\b</code> will match strings (separated with word boundaries) starting with a letter followed by 3, 4 or 7 and then 3 digits, like “c3122”.</p> </x{hex-number}></pre>
Test	<p>Because a regular expression pattern can be quite complex, it is important that you test the pattern before saving it. If improperly written, a pattern can create many false-positive incidents and slow down the system.</p> <p>Create a .txt file (less than 1 MB) that contains values that match this regex pattern. The file must be in plain text UTF8 format.</p> <p>Browse to the file and click <b>Test</b> to test the validity of your pattern syntax. If the pattern you entered is invalid, you’re given an opportunity to fix it. You cannot proceed until the test succeeds.</p>



## Key phrase content classifiers

The presence of a keyword or phrase (such as “Top Secret” or “Project X”) in a web post may indicate that classified information is being leaked. You can learn about activity like this by defining a key phrase classifier.

To create a key phrase classifier, complete the fields as follows:

Field	Description
Name	Enter a name for this key phrase classifier.
Description	Enter a description for this key phrase.
Key phrase	Enter the key word or phrase that might indicate classified information, up to 255 characters. Key phrases are not case sensitive.  Leading and trailing white spaces are ignored. If you need to use slashes, tabs, hyphens, underscores, or carriage returns, define a regular expression classifier rather than a key word classifier.

Unlike dictionaries, key phrases also identify partial matches. For example, the key phrase “uri” reports a match for “security”.

## Dictionary content classifiers

A dictionary is a container for words and expressions pertaining to your business. To create a dictionary classifier, complete the fields as follows:

Field	Description
Name	Enter a name for this pattern, such as Diseases.
Description	Enter a description for this dictionary, such as Disease names.

Field	Description
Dictionary Content	<p>Dictionaries can have up to 100 phrases. To add content to the dictionary, click <b>Add</b>. Complete the fields on the resulting dialog box as follows:</p> <ul style="list-style-type: none"><li>■ <b>Phrase:</b> Enter a word or phrase to include. This phrase, when found in the content, affects whether the content is considered suspicious.</li><li>■ <b>Weight</b> - Select a weight, from -999 to 999 (excluding 0). When matched with a threshold, weight defines how many instances of a phrase can be present, in relation to other phrases, before triggering a policy. Thresholds are defined on the policy's Data Security tab.</li></ul> <p>By default, if no weight is assigned, each phrase is given a weight of 1.</p> <p>For example, if the threshold is 100 and a phrase's weight is 10, a web post can have 9 instances of that phrase before a policy is triggered, provided no other phrases are matched. If phrase A has a weight of 10 and phrase B has a weight of 5, 5 instances of phrase A and 10 instances of phrase B will trigger the policy.</p> <p>Click <b>OK</b> and the phrase appears in the content list. You can add phrases one by one, or import them from a CSV file using the import button described below.</p> <p>Remove phrases by selecting them and clicking <b>Remove</b>.</p>

Field	Description
Import	<p>If you have many phrases to include, create a text file listing the phrases, then click <b>Import</b> and navigate to the text file.</p> <p>The text file must be of UTF8 format. In the text file:</p> <ul style="list-style-type: none"> <li>■ List each phrase on a separate line. The phrase can be up to 256 characters.</li> <li>■ Optionally, provide one weight per phrase on the same line. <ul style="list-style-type: none"> <li>■ Separate the phrase and weight by a comma. Enclose the phrase in quotes (not required if there is no weight). For example, "private information", 3</li> <li>■ Valid weights are from -999 to 999, but you cannot assign a weight of 0.</li> <li>■ If a phrase has no weight, it is assigned the default weight of 1.</li> </ul> </li> <li>■ Each phrase must be distinct. (Repeated values are ignored.)</li> <li>■ You can include up to 100 unique phrases. If you include more, only the first 100 are added to the list. If there are already phrases in the dictionary, fewer than 100 are imported.</li> <li>■ White spaces are ignored.</li> <li>■ Slashes, tabs, hyphens, underscores, and carriage returns are included in the search.</li> <li>■ Common words are also included.</li> </ul> <p><b>Sample file, custom_dictionary.txt:</b></p> <pre style="background-color: #f0f0f0; padding: 5px;">"confidential",5 "ProjectX",8 "ProjectY",3</pre>
The phrases in this dictionary are case- sensitive	<p>Select this check box if you want the phrases that you entered to be added to the dictionary with the same case you applied.</p>

Each dictionary classifier is limited to 100 phrases.



## Chapter 5

# Managing Network Devices

### Contents

- Introduction on page 133
- Global options on page 133
- Managing edge devices on page 135
- Generating device certificates on page 144
- Managing EasyConnect services on page 146
- Managing I Series appliances on page 148

## Introduction

---

The **Web > Network Devices > Device Management** page lists the devices and tunnel connections currently registered with the cloud portal. Depending on your account, these may be edge devices, Forcepoint appliances, EasyConnect services, or all.

Use this page to:



- Add, edit, or remove devices.
- Organize devices into folders, for ease of management.
- Investigate details for each device.

A table displays your current devices and connections. Use the left selection menu or the drop-down list at the top of the table to filter what is shown. Above the table are the tools that can be used to manage and review your appliances or devices.

## Global options

---

A variety of controls above the table can be used to:

- Search for devices.  
Enter all or part of a device name to start searching. The table is updated to show only results that match your search. Matched elements of the device name string are highlighted.
- Add an edge device or EasyConnect service.  
Click  , then select **Add Edge Device** (see *Adding or editing edge device information*) or **Add EasyConnect Service** (see *Adding or editing an EasyConnect service*).
- Add an appliance  
Click  , then select **Add Appliance** (see *Adding or editing appliance information*).

- Add a folder or sub-folder to group similar edge devices, EasyConnect services, or appliances for ease of management in large deployments.

Click , then enter a folder name and click **Add**. You can nest folders as needed for ease of management.

Once you have created folders, you can use drag and drop to move devices into folders, and to move folders.

- Delete network devices or folders from the table.  
Mark the check box next to each device or folder that you want to delete, then click the Delete button.
- For **I Series appliances**, use the **Optimize performance** link at the top, right of the page to determine what traffic to send to the cloud service for analysis (see *Optimizing appliance performance* for details).

#### Related concepts

[Adding or editing edge device information](#) on page 138

[Adding or editing appliance information](#) on page 151

#### Related tasks

[Adding or editing an EasyConnect service](#) on page 146

[Optimizing appliance performance](#) on page 151

## The detail pane

A detail pane to the right of the table that displays important device information and access to configuration tools.

For information about the details available for each device, see the below topics:


#### Related reference

[Managing edge devices](#) on page 135

[Managing EasyConnect services](#) on page 146

[Managing I Series appliances](#) on page 148

## Configuration tools for edge devices and EasyConnect services

- To edit device information, click **Edit** , then see *Adding or editing edge device information* or *Adding or editing an EasyConnect service*.

- To remove an entry from the Device Management table, click **Delete** .


#### Related concepts


[Adding or editing edge device information](#) on page 138

**Related tasks**

[Adding or editing an EasyConnect service](#) on page 146

## Configuration tools for appliances

To edit appliance information, click , then see *Adding or editing appliance information*.

Click  for a menu of other available options. The options are different for unregistered and registered appliances.

- For appliances that are not yet registered, select **Register Appliance**. Registration instructions and the registration key appear in a pop-up window.
- For registered appliances:
  - Select **Download Update** to select from a list of available software updates. The selection pop-up includes a link to the release notes for each available version.
  - Select **Upgrade History** to review a list of updates downloaded to or installed on the appliance.
  - Select **Delete Appliance** to remove the appliance entry from the Device Management table.

**Related concepts**

[Adding or editing appliance information](#) on page 151


## Managing edge devices

Select **Edge Devices and Services** in the left selection pane of the Device Management table to view or add your edge devices for tunneling connectivity.

- GRE tunneling is used to forward traffic to the cloud service over a GRE tunnel via a virtual point-to-point connection.
- IPsec Advanced tunneling is our next generation IPsec service, supporting wide device interoperability, and devices with dynamic IP addresses using pre-shared key authentication.

The number of configured devices is displayed below the table. By default, you can create 200 tunnel connections for your account. To add more connections, contact your account manager to discuss your requirements.

The table displays the following elements for each device. Not all columns are relevant for each tunneling type, and some columns are hidden when the right detail pane is expanded.






Item	Description
Status	<p>An icon indicating the current connection status of the device's tunnels, based on connectivity and tunnel status. (See the table below.)</p> <p>When an IPsec Advanced device is added or edited, a Configuring icon displays. This process can take several minutes per device to complete. Refresh the screen to confirm that the Provisioned icon has replaced the Configuring icon.</p> <p>If any tunnels for the device have a warning or error, the status indicator for the worst condition will be shown in the status column. Hover over the status icon to display the status for each tunnel.</p>
Name	Device name, specified when a device is added or edited.
Description	Optional device description, specified when an edge device is added or edited.
Folder	<p>The folder containing the device.</p> <p>When you drill down into a folder, this column is not displayed.</p>
Authentication	Options are PSK (pre-shared key), Certificate, or N/A. GRE tunnels do not use authentication.
Device Type	<p>Device model, specified when a device is added or edited.</p> <p>An entry of "Not configured" indicates that the device was added without a device type specified. You can update this property for your devices using the <b>Edit Edge Device</b> page. (Device type is a required property for newly added devices.)</p>
Tunneling	The type of tunnel connection this device is using. Options are IPsec Advanced or GRE.
Point of Presence	<p>The data center or local point of presence configured for the device. If the information displays with  there is a redundancy issue that should be corrected.</p>

You can filter the list to find specific devices based on the authentication type, tunneling type, device type, or devices that use a specific policy. Click a filter name under Edge Devices and Services in the left-hand pane, or select a filter from the drop-down menu above the list.

The device status icons are shown in the following table. If a device has multiple tunnels, hovering over the status indicator in the list reveals the status for each tunnel.

Icon	Description	Explanation
	Up	The tunnel has successfully connected.



Icon	Description	Explanation
	Unavailable	The tunnel has previously connected to the cloud service, but may be experiencing connectivity issues.
	Down	The tunnel could not be established, or the device is disconnected. This may be due to a configuration or connectivity issue.
	Configuring	Used for GRE and IPsec Advanced devices, the device is being configured.
	Provisioned	Used for GRE and IPsec Advanced devices, the device has been configured and can now be connected.  Note that a refresh of the screen is required before this icon will display for newly configured devices.
	Status Unknown	No connection attempts have been detected for this tunnel. This may be due to a configuration or connectivity issue.

When a device is selected, the right detail pane shows additional information for each device and tunnel. The Status section displays the following connectivity information:

Item	Description
Point of Presence	The location of the PoP to which the device is connected.
Server name	The name of the server currently hosting the connection. (For GRE devices, the server name is shown in brackets after the PoP name.)
Average speed	An indicative sample of the data transfer rate over the last few minutes, in Mbps (IPsec Advanced tunnels only).
Tunnel uptime	The length of time the tunnel has been established, in days, hours, and minutes (IPsec Advanced tunnels only).
Last activity	The date and time traffic was last received from the device via this tunnel.

The Configuration section shows setup information for the device. The information shown here depends upon the tunneling type your device is using. The following items are shown for all devices:

- Device type
- Tunneling type
- Primary PoP (and Secondary PoP): the name and identifier of the point of presence to which each tunnel connects.

- Default policy - an entry of “N/A” indicates that the device was assigned to a policy, but the cloud service does not recognize the policy name.
- Other policies (if any) assigned to internal networks managed by the device

For devices connecting via IPsec Advanced tunneling, the following additional information is shown:

- Service Address: address to which the edge device should connect.
- Pre-shared key details include the egress IP address and IKE ID. Administrators also have the option to view the key.

For devices connecting via GRE tunneling, the following additional information is shown for each tunnel:

- Public IP
- Destination IP: address for the remote (PoP) end of the GRE tunnel, assigned by the cloud service.
- Source IP: address for the local (edge device) end of the GRE tunnel, assigned by the cloud service.
- Service address: address to which the edge device should connect..



#### Note

You must configure two points of presence for redundancy when you configure GRE or IPsec tunnels. The above information is repeated for each connection.

To import a CSV file containing edge device information, click the **Add** button and select **Import Edge Devices**. See *Import multiple edge devices via a CSV file*.

To edit an existing device, select the device in the table, then click the **Update** button in the detail pane. See *Adding or editing edge device information*.



#### Note

For detailed guidance on configuring your edge device, see the following guides:

- [Forcepoint IPsec Advanced Guide](#)
- [Forcepoint GRE Guide](#)

#### Related concepts

[Adding or editing edge device information](#) on page 138

#### Related tasks

[Import multiple edge devices via a CSV file](#) on page 142

## Adding or editing edge device information

Use the **Device Management** > **Add Edge Device**  or **Edit Edge Device**  options to add a device, or change the configuration settings for an existing device.

When you add a device, you are asked to specify the tunneling type. You can create devices that connect via IPsec Advanced or GRE tunneling. See the below topics:

**Related tasks**

To add a new edge device for IPsec Advanced tunneling on page 139

To add a new edge device for GRE tunneling on page 140

# To add a new edge device for IPsec Advanced tunneling

## Steps

- 1) Click **Add**, and select **Add Edge Device**.
- 2) Select the tunneling type: **IPsec Advanced**.
- 3) Under **General**, enter or update your device **Name**.
- 4) Select the **Device Type** from the drop-down list.
- 5) Provide a device **Description** (up to 512 alphanumeric characters).
- 6) Under **Device Authentication**:
  - a) Select the **IKE Version**. The IKEv2 protocol is selected by default.
  - b) Select an **IKE identity**. The valid options are based on the IKE Version selected. If IKEv1 was selected as the **IKE Version**, the only option is Public IP address.
  - c) Enter the Public IP address or DNS hostname.
  - d) Select a **Pre-shared key** option. Define whether to use your own key (keys must be a minimum of 8 characters long) or generate a new key from the cloud service.
  - e) If you select **Use your own key**, enter the key string. If you select **Auto generated new key**, the new key is displayed.

Click the **encryption settings** link to view supported IKE and IPsec settings for the device.

- 7) Under **Points of Presence (PoPs)**, use the drop-down lists provided to select the two most appropriate points of presence (data center or local PoP) for your location.
- Optionally, click on the entry field and begin entering text to filter the list of PoPs to those that contain that search sub-string. The list is reduced as each character is entered. Make your selection from the filtered list. You can also use the up and down arrow keys on your keyboard to highlight your selection. Press Enter to select it. Press Esc to remove the filter and restore the previous selection.
- Once the **Primary** selection is made, the list for the **Secondary** selection is limited to those PoPs not included in the Data Center of the primary selection.
- Note that, if the two selections reside in the same physical location, redundancy is not supported. To avoid this, a message appears with instructions to select a different secondary location.
- If you change selections, make sure your device configuration is correct.

**Important**

If your device supports it, configure one PoP as the primary and one as the backup. We strongly recommend you configure your device to fail over to the backup PoP automatically.

- 8) Under **Policy Assignment**, select the **Default policy** to apply to traffic managed by this device. The Default policy is pre-selected but can be changed.
- 9) If you want to apply different policies to different internal networks whose traffic is managed by the device, click **Add** under the Policy Assignment table, then:
- Provide a unique Name for the network.
  - Use the Type list to specify how you want to define the network (as an IP address, subnet, or IP range).
  - Enter the network information in the format that you specified.
  - Select the policy to apply to traffic from the network.
  - Click **Add**.


Repeat these steps for each internal network managed by the device to which you want to assign a specific policy.

Note that networks (IP address ranges and subnets) may not overlap, and you can assign only one policy to each network.

- 10) When you are finished configuring the device, click **Save**.

## To add a new edge device for GRE tunneling

### Steps

- 1) Click **Add** , and select **Add Edge Device**.
- 2) Select the tunneling type: **GRE**.

- 3) Under **General**, enter or update your device **Name**.
- 4) Select the **Device Type** from the drop-down list.
- 5) Provide a device **Description** (up to 512 alphanumeric characters).
- 6) Add the **Public IP address** for the device. This is the external egress IP for the device.
- 7) Under **Points of Presence (PoPs)**, use the drop-down lists provided to select the two most appropriate points of presence (data center or local PoP) for your location. Once the **Primary** selection is made, the list for the **Secondary** selection is limited to those PoPs not included in the Data Center of the primary selection.

Note that, if the two selections reside in the same physical location, redundancy is not supported. To avoid this, a message appears with instructions to select a different secondary location.

If you change selections, make sure your device configuration is correct.



#### Important

If your device supports it, configure one PoP as the primary and one as the backup. We strongly recommend you configure your device to fail over to the backup PoP automatically.

For each connection, the destination (PoP) inner tunnel address and source (edge device) inner tunnel IP address are provided when the data is saved. You will need these addresses to configure the tunnel on your device.

- 8) Under Policy Assignment, select the **Default policy** to apply to traffic managed by this device. The Default policy is pre-selected but can be changed.
- 9) If you want to apply specific policies to different internal networks whose traffic is managed by the device, click **Add** under the Policy Assignment table, then:
  - a) Provide a unique Name for the network.
  - b) Use the Type list to specify how you want to define the network (as an IP address, subnet, or IP range).
  - c) Enter the network information in the format that you specified.
  - d) Select the policy to apply to traffic from the network.
  - e) Click **Add**.

Repeat these steps for each internal network managed by the device to which you want to assign a specific policy.

Note that networks (IP address ranges and subnets) may not overlap, and you can assign only one policy to each network.

- 10) When you are finished configuring the device, click **Save**.

# Import multiple edge devices via a CSV file

Use the **Device Management > Import Edge Devices** page to create and import a CSV file containing details of devices to be added to the cloud service. This option is available for devices connecting via GRE and IPsec Advanced with PSK authentication.

The import CSV can be used to bulk import IPsec Advanced devices, GRE devices, or a combination of both. For ease of use, it is recommended that you import devices that use one tunneling type at a time, using the appropriate CSV template as a guide.

Web > Device Management > Import Edge Devices

## Import Edge Devices



Instructions for importing devices:

- Download the CSV [IPSec template](#) or [GRE template](#).
- Populate the file with details of the devices to be imported.
- Enter a name, supported device type, tunneling type, default policy, and egress IP for each entry.
- Populate other required fields for IPsec and GRE tunnels as appropriate. Refer to the help for further information.
- When you have finished, select a target folder for the imported devices, and upload the file.

Target folder:  *Devices will be imported into this folder.*

CSV file:

## Steps

- 1) To get started, click the **template** link for the appropriate devices, and save the template file to your local machine. This template provides the column headings for information that must be provided for each type of device.

- 2) Open the CSV template, and populate the file with the following details for each device you want to add. Note that if an incorrect format is used in any cell of the file, the import process fails.

For IPsec Advanced tunneling:

- Name
- Description
- Device Type
- Points of Presence (PoPs): enter up to two PoPs, identified by their ID, space separated.
- Pre-shared key: include this if you are using your own key. Leave the column blank to auto-generate a key for each device
- IKE Version
- Egress IP address
- Default Policy for traffic from the device

For GRE tunneling:

- Name
- Description
- Device Type
- Public IP
- Points of Presence (PoPs): enter up to two PoPs, identified by their ID, space separated.
- Default Policy for traffic from the device



#### Note

The Default Policy and Device Type fields must be populated with policy and device names as listed in the portal. These fields are not case sensitive.

Supported devices are listed on the Add Device page, in the Device Type drop-down menu (enter "Other" if using a device type that is not yet certified). For details of supported devices, see the [Forcepoint IPsec Guide](#) and the [Forcepoint GRE Guide](#).

- 3) When you have added your devices, save and close the file.
- 4) If you have defined multiple folders on the Device Management page, select the **Target folder** for the devices in the CSV file. All devices must be imported into the same folder.
- 5) Click **Browse** to select your CSV file.
- 6) Click **Import**.  
Once the devices are added successfully, they are added to the list on the Device Management page. Use the Device ID and pre-shared key information on this page to configure your IPsec Advanced devices.



#### Note

There is a different set of required columns for the IPsec Advanced and GRE device import. For convenience, we recommend using the available CSV templates and importing each device type separately.

# Generating device certificates

The portal includes a feature that allows you to generate a certificate for your device, using the private key and passphrase for the certificate authority. Once generated, you can download the certificate and add it to your device.




## Note

If you do not have access to this feature, contact Technical Support.

To generate certificates from the **Device Management** page:

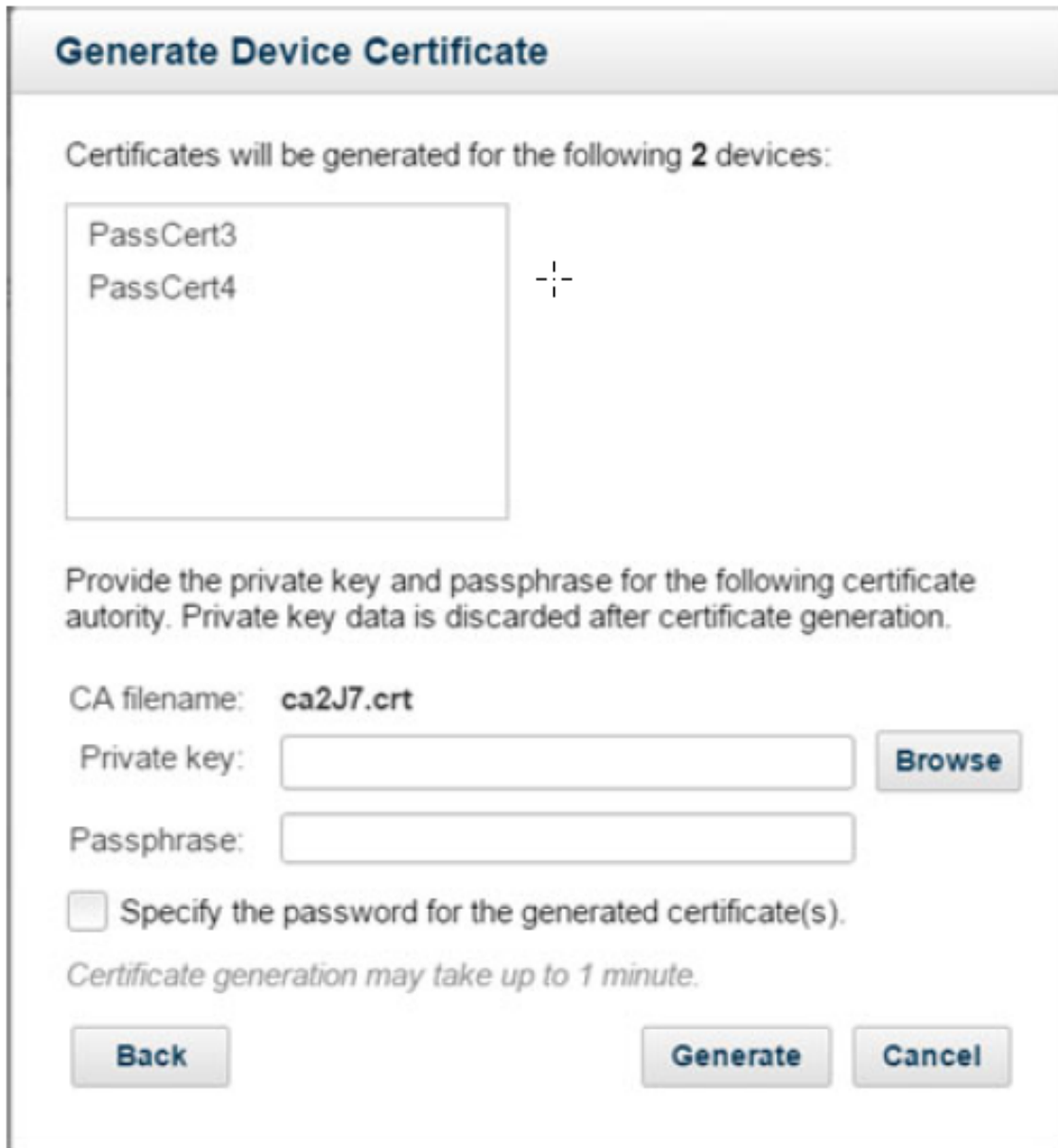
## Steps

- 1) Use the check boxes in the Device Management table to select one or more edge devices.
- 2) Click the **Generate Certificate** button () in the toolbar above the table. This button is disabled when no CA has been defined for the selected device.



- 3) In the Generate Device Certificate dialog box, click **Browse** to navigate to the **Private key** for the certificate authority.

The private key file has a name like “cakey.pem” or “privkey.key.” It is either provided with a purchased CA or generated with your organization’s self-signed



**Generate Device Certificate**

Certificates will be generated for the following **2** devices:

- PassCert3
- PassCert4

Provide the private key and passphrase for the following certificate authority. Private key data is discarded after certificate generation.

CA filename: **ca2J7.crt**

Private key:  **Browse**

Passphrase:

Specify the password for the generated certificate(s).

*Certificate generation may take up to 1 minute.*

**Back** **Generate** **Cancel**

CA.

- 4) Enter the private key **Passphrase**.



#### Important

For security reasons, private key data is not saved after the certificate is generated. As a result, you must enter the key and passphrase each time you generate a device certificate for this CA.

- 5) Indicate whether or not to **Specify the password** for the device certificate or certificates. If you select this option, enter and confirm the certificate password.
- 6) Click **Generate**.

- 7) Follow the on-screen instructions for downloading the certificates.

## Managing EasyConnect services

EasyConnect is a service that allows you to connect on-premises Forcepoint NGFW edge devices to the cloud service. EasyConnect services can be applied to multiple Forcepoint NGFW devices connecting to the service with the same default policy. One of four provided authentication keys is used to authenticate an NGFW device with an EasyConnect service.

The following elements are displayed in the table when All Services is selected in the left select pane of the Device Management table.

Item	Description
Name	Service name, specified when a service is added or edited.
Description	Optional description of the service, specified when a service is added or edited.
Folder	The folder containing the service.  When you drill down into a folder, this column is not displayed. In other views, like <b>All</b> or <b>Specific version(s)</b> , if you have created folders, the Folders column is displayed.
Authentication	N/A
Device Type	Forcepoint NGFW
Tunneling	EasyConnect

You can filter the list to find specific services based on various properties. Click a filter name under “EasyConnect Services” in the left-hand pane, or select a filter from the drop-down menu above the list.

The right details pane provides additional information for each service. The Configuration section shows the Device type, Tunneling type, and Default policy associated with the selected EasyConnect service.

## Adding or editing an EasyConnect service

Use the **Add** or **Edit** buttons on the **Device Management** page to add an EasyConnect service or change the configuration settings for an existing service.

Web &gt; Device Management &gt; Add Forcepoint EasyConnect Service

## Add Forcepoint EasyConnect Service

EasyConnect services can be applied to multiple Forcepoint NGFW devices connecting to the Web Security Cloud.

**General**

Name:

Device type: **Forcepoint NGFW**

Description:

Customer ID:

**Device Authentication**

Each Forcepoint NGFW device must authenticate with the EasyConnect service using one of the following keys

Key ID	Password	
Key 1	*****	<input type="button" value="Re-Generate"/>
Key 2	*****	<input type="button" value="Re-Generate"/>
Key 3	*****	<input type="button" value="Re-Generate"/>
Key 4	*****	<input type="button" value="Re-Generate"/>

When configuring your NGFW device, you will need the following [Connectivity Details](#).

**Policy Assignment**

Configure internal networks for this service and assign each network a policy.

Default policy:

<input type="checkbox"/>	Name ▲	Network Definition	Policy

To add a new EasyConnect service:

### Steps

- 1) Click the **Add** icon and select **Add EasyConnect Service**.
- 2) Under **General**, add or update your service **Name**.  
Forcepoint NGFW is automatically added as the **Device Type** and the field is disabled.
- 3) Provide a **Description** (up to 512 alphanumeric characters).
- 4) **Customer ID** is generated by the portal and is a display only field. This value can be copied for use when configuring the service in the NGFW Security Management Center.

- 5) The **Device Authentication** table lists the **Key ID** and **Password** of the 4 keys generated by the portal and used to authenticate devices with the cloud service.

The table cannot be edited but key values can be copied, and passwords can be regenerated by clicking **Re-Generate**. Passwords are protected but can be viewed by clicking **Show Passwords**.

Click the **Connectivity Details** link to view Customer ID, port information, Domain Name Server (DNS) and the keys that have been configured. Note that you can copy the Customer ID, DNS name, and key values from this panel so they can be used when configuring the service in the NGFW Security Management Center.

Ports 8090 (HTTP) and 8011 (HTTPS) are used for communication between the EasyConnect Service and NGFW.

- 6) Under **Policy Assignment**, select the **Default policy** to apply to traffic managed by this service.
- 7) If you want to apply different policies to different internal networks whose traffic is managed by the service, click **Add** under the Policy Assignment table, then:
- Provide a unique **Name** for the network.
  - Use the **Type** list to specify how you want to define the network (as an IP address, subnet, or IP range).
  - Enter the network information in the format that you specified.
  - Select the policy to apply to traffic from the network.
  - Click **Add**.

Repeat these steps for each internal network managed by the service to which you want to assign a specific policy.

Note that networks (IP address ranges and subnets) may not overlap, and you can assign only one policy to each network.

- 8) When you are finished configuring the service, click **Save**.

## Managing I Series appliances







When you select **I Series Appliances** in the left selection pane of the Device Management table, the table displays the following elements for each appliance. Some of these columns are hidden when the right detail pane is expanded.

Item	Description
Status	<p>An icon indicating the current status of the appliance, based on connectivity, reported issues, version, and registration status. (A legend explaining these icons is shown below this table.)</p> <p>If an error or warning icon appears, select the appliance in the table and check the detail pane for more information.</p>

Item	Description
Name	Appliance name, specified when an appliance is added or edited.
Description	Optional appliance description, specified when an appliance is added or edited.
Folder	The folder containing the appliance. When you drill down into a folder, this column is not displayed. In other views, like <b>All</b> or <b>Specific version(s)</b> , if you have created folders, the Folders column is displayed.
Hostname	Appliance host name or FQDN, specified on the appliance. If the appliance is not registered, or this information has not been received from the appliance, "N/A" is displayed.
Version	The appliance version. If the appliance is not registered, or this information has not been received from the appliance, "N/A" is displayed.

You can filter the list to find specific appliances based on various properties such as the appliance type, version, status or a specified policy. Click a filter name under "I Series Appliances" in the left-hand pane, or select a filter from the drop-down menu above the list.

The available status icons are:

Icon	Meaning	Icon	Meaning
	Status OK		Warning
	Information		Error
	Filtering disabled or registration incomplete		Critical error

The **General** tab of the right detail pane includes additional information, including:

Item	Description
Filtering	Indicates whether or not a registered appliance is enabled for managing web traffic.
Connectivity	Indicates the state of the Internet connection between the appliance and the cloud portal.

Item	Description
------	-------------

Version	<p>In addition to the version number, a message is displayed for versions that have expired or are nearing expiration.</p> <p>Click the message to see a list of available software updates with release notes for each available update. Select an update and click <b>Download</b> to download the update to the appliance.</p>
Issues	<p>Displays the number of issues for the appliance for the past 24 hours, along with an icon indicating the highest severity level represented among the issues.</p> <p>If the appliance has not generated issues for the past 24 hours, “No issues reported” is displayed.</p> <p>If any issues exist, click the number of issues to see a list with details of each issue. You can review issues from the last 24 hours (default) or last 7 days.</p>
Registration	<p>Indicates whether the appliance is registered or not</p> <p>If the appliance is not registered, click the <b>Not registered</b> link to get the registration key. Copy the registration key and enter it in the Appliance manager under <b>Configuration &gt; Registration</b> to complete the registration process.</p> <p>Note that it takes some time for registration status to be updated in the cloud portal after you enter the registration key in the appliance. This delay does <b>not</b> indicate a problem with the registration.</p>
Default policy	The name of the default policy for the appliance
Other policies	Lists policies other than the default policy (if any) assigned to internal networks defined for this appliance
Last response	<p>Shows the date and time of the latest response from the appliance.</p> <p>If the appliance is not registered, or has not sent any information to the cloud service, the display is “N/A”.</p>
Uptime	Shows the time since the last appliance restart.

The **Performance** tab of the right detail pane displays 4 charts showing appliance performance over the **Last 24 hours** (by default). Use the drop-down list at the top of the tab to optionally expand the performance charts to show information for the **Last 7 days**.

- Resource Usage
- Web Traffic (Transactions per second or Bandwidth)
- Protocol Traffic (Transactions per second or Bandwidth)
- Session Peaks

# Optimizing appliance performance

When appliance performance optimization is turned on (default), only content from sites with elevated risk profiles is sent to the cloud for analysis. This applies:

- To both Advanced Classification Engine (ACE) advanced analysis and file type analysis
- Even when ACE advanced analysis is configured to include sites with a lower risk profile

When appliance performance optimization is turned off:

- All traffic is sent to the cloud for true file type analysis.
- Sites with a lower risk profile may receive ACE advanced analysis, depending on the options selected on the **Web Content & Security** tab.

See *Web Content & Security tab* for more information about configuring ACE and file type analysis.

To turn off performance optimization:

## Steps

- 1) Click the next to **Optimize performance** (in the top, right corner of the Device Management page).
- 2) On the pop-up that is displayed, select **Off**.
- 3) Click **Save** to confirm.

### Related concepts

[Web Content & Security tab](#) on page 217

# Adding or editing appliance information

On the **Web > Network Devices > Device Management** page, use the following steps to add an appliance to the cloud service, or to edit an existing appliance.

To get started, do one of the following:

- To add a new appliance to the portal, click the **Add** button above the table.
  - If your deployment includes only appliances (no edge devices), the Add Appliance page opens.
  - If your deployment includes both appliances and edge devices, a drop-down menu is displayed. Select **Add Appliance** to open the Add Appliance page.
- To edit an existing appliance, select the appliance entry in the table, then click the **Update** button in the detail pane.

Perform the following tasks on the **Add Appliance** or **Edit Appliance** page:

- *Configure general settings*
- *Configure a certificate authority*
- *Define internal network settings*
- *Configure advanced settings (if needed)*

When you are finished making changes, click **Save**.

**Related tasks**

- [Configure general settings on page 152](#)
- [Configure a certificate authority on page 153](#)
- [Define internal network settings on page 155](#)
- [Configure advanced settings \(if needed\) on page 157](#)

## Configure general settings

**General**

Filtering:  ON [i](#)

Name:

Description:

Default policy:  ▼

Timezone:  ▼

Authentication domain:  *Used for transparent NTLM authentication.*

Session timeout:  ▼

Forward traffic to the cloud for advanced analysis [i](#)

### Steps

- 1) Use the toggle at the top of the page to indicate whether this appliance is used for filtering (**ON**, the default). When filtering is set to OFF, the appliance can communicate with the cloud service, but allows all web traffic to pass through unfiltered.
- 2) Under General, enter a unique appliance **Name** (1 - 512 alphanumeric characters) and **Description** (up to 1024 characters).
- 3) Select a **Default policy** for this appliance, and the **Time zone** used to apply policy settings. You will have a chance to apply different policies to different internal networks managed by this appliance later.



- 4) If you are using transparent NTLM identification and your appliance is not connected to a local Active Directory instance, enter the domain that forms part of your users' NTLM identity. The NTLM domain is the first part of the domain\username with which users log on to their Windows PC; for example, MYDOMAIN\jsmith.



#### Important

You must configure your end users' browsers to support transparent NTLM identification, either manually or via GPO or similar. For more information, see [Deploying an I Series Appliance](#) on the Forcepoint Support site.

If you have connected your appliance to a local Active Directory for NTLM identification, this field is not required because the appliance automatically retrieves this information from the local directory.

- 5) Select a time period after which a user's login and password must be revalidated from the **Session timeout** drop-down list. The default is 1 day.
- 6) **Forward traffic to the cloud for advanced analysis** is selected by default. This means that appropriate web traffic is redirected to the nearest cloud service cluster for additional analysis. Deselect this option if you do not want any traffic to be forwarded to the cloud. All traffic will be analyzed through the appliance, but without any cloud analytics.

## Configure a certificate authority

### Certificate Authority



Configure the certificate authority used by this appliance

Use existing certificate files ▼

Public certificate: ca2.crt

Private key: ca2.key

Chained certificate: chain.crt

Under Certificate Authority:

- If you are adding a new appliance, use the drop-down list to indicate whether to **Upload certificate files now**, or **Provide certificate later**.



### Important

It is recommended that you define certificates when you add an appliance, in order to avoid browser warnings regarding SSL termination block, authentication, or quota/confirm operations. Some browsers, for example later versions of Chrome, may block the transaction and display an error message.

Be sure to:

- 1) Generate a CA certificate. Each appliance should have a valid X.509 identity certificate with an unencrypted key. This certificate can be generated using a variety of tools, for example OpenSSL. For details and an example, see *Generating an appliance certificate*.
- 2) Import this certificate to all relevant browsers.
- 3) Upload this certificate to each appliance as described below.

To use the cloud service SSL decryption feature, you should also install the Forcepoint root certificate on each client machine. See *Enabling SSL decryption* for details.

- If you are editing an existing appliance, indicate whether to **Use existing certificate files** or **Upload certificate files**.

To upload the certificate files:

## Steps

- 1) Click **Browse** to navigate to the public certificate file, then click **Open** to populate the **Public certificate** field.
- 2) Click **Browse** to navigate to the private key file, then click **Open** to populate the **Private key** field. The private key must be in either PEM or .key format.
- 3) If you have chained certificates, click **Browse** and navigate to the intermediate certificate, then click **Open** to populate the **Chained certificate** field.  
The certificate chain should include the root CA, and optionally additional intermediate CAs.

### Related concepts

[Generating an appliance certificate](#) on page 154

### Related tasks

[Enabling SSL decryption](#) on page 194

# Generating an appliance certificate

Each appliance should have a valid X.509 version 3 identity certificate in PEM format with an unencrypted key. This certificate can be generated using a variety of tools. Below is a simple procedure using OpenSSL to generate a private key and CA that can be used for your appliance.

This section assumes that you are familiar with OpenSSL and have a working OpenSSL installation.

The following OpenSSL statement creates a 2048-bit RSA private key with a password of 1234:

```
openssl genrsa -passout pass:1234 -des3 -out CA_key_password.pem 2048
```

You must supply a password, as OpenSSL does not allow the creation of a private key without one. You can then strip the password from the key as follows:

```
openssl rsa -in CA_key_password.pem -passin pass:1234 -out CA_key.pem
```

This also renames the private key file from CA\_key\_password.pem to CA\_key.pem. Finally, use the following statement to create the CA:

```
openssl req -x509 -days 11000 -new -sha1 -key CA_key.pem - out CA_cert.pem
```

Note that this command prompts you to input information about different parameters, such as country, state, locality, or your organization's name.

Once you have created the private key (CA\_key.pem) and public certificate (CA\_cert.pem), import the certificate to all relevant browsers, and upload the certificate to each appliance using the Certificates tab.

## Define internal network settings

### Internal Networks

Policy Assignment
Trusted Networks
Session-Based Authentication

Configure internal networks to use specific policies. The default policy is applied to traffic not originating from these networks.

	Name ▲	Network Definition	Policy
<input type="checkbox"/>	1	Subnet: 1.1.1.1 / 32	DEFAULT
<input type="checkbox"/>	2	Subnet: 2.2.2.2 / 32	P1YE
<input type="checkbox"/>	3	Subnet: 3.3.3.3 / 32	P2YE

Add
Delete

Use the Internal Networks section of the page to optionally:

- Assign different policies to different internal networks.
- Identify trusted networks for which incoming or outgoing traffic, or both, should not be analyzed.
- Configure session-based authentication for specific networks.

To begin:

## Steps

- 1) Select the **Policy Assignment** tab and click **Add** to identify a network to which you want to assign a policy other than the appliance default. In the **Add Policy Assignment** dialog box:
  - a) Enter a unique **Name** for the network.
  - b) Use the **Type** list to indicate how you want to identify the network (IP address, Subnet, or IP range).
  - c) Enter the subnet, address, or range.
  - d) Select a **Policy** from the drop-down list.
  - e) Click **Add**.

Repeat these steps for each internal network to which you want to assign a policy.

Note that networks (IP address ranges and subnets) may not overlap, and you can assign only one policy to each network.

- 2) Select the **Trusted Networks** tab and click **Add** to identify IP addresses or address ranges whose traffic should not be analyzed. In the **Add Trusted Network** dialog box:
  - a) Enter a unique **Name** for the network.
  - b) Use the **Type** list to indicate how you want to identify the network (IP address, Subnet, or IP range).
  - c) Enter the subnet, address, or range.
  - d) Indicate whether to **Bypass analysis for traffic from this network**, **Bypass analysis for traffic to this network**, or both.
  - e) Click **Add**.

Repeat these steps for each internal network whose incoming or outgoing traffic, or both, should not be analyzed.

- 3) Select the **Session-Based Authentication** Tab and click **Add** to define network addresses and IP address ranges that should use session-based authentication. The defined addresses will be authenticated based on a cookie sent to the browser on the local machine.

This authentication is valid for the length of time defined in the **Session timeout** drop-down list (under **General**).

- a) Enter a unique **Name** for the network.
- b) Use the **Type** list to indicate how you want to identify the network (IP address, Subnet, or IP range).
- c) Enter the subnet, address, or range.
- d) Click **Add**.

Repeat these steps for each internal network that will use session-based authentication.



#### Note

When session-based authentication is enabled, policy SSL decryption rules that apply to sites or categories with the **Confirm** action are not currently supported.

## Configure advanced settings (if needed)

### Steps

- 1) If you need to update the appliance password, mark **Change appliance password**, then enter and confirm the new password.
- 2) If your network uses virtual LANs (VLANs), next to **VLAN traffic tagging**, indicate whether to **Analyze untagged traffic only** (default), **Analyze tagged traffic only**, or **Analyze all traffic (tagged and untagged)**.
- 3) If you have elected to analyze tagged traffic, indicate whether to **Bypass analysis for specific VLAN tags**. If you select the **bypass** option, enter trusted tag numbers in the entry field (one entry per row).  
For information about tagging traffic explicitly generated by this device using the appliance user interface, see the topic “Routing” in the appliance Help.
- 4) To specify **HTTP ports** other than the default (80), enter comma-separated port numbers.
- 5) To specify **HTTPS ports** other than the default (443), enter comma-separated port numbers.
- 6) Specify how the cloud service handles requests for IPv6 destinations (allow or block). Traffic to IPv6 destinations that is allowed (default setting) is not filtered or logged.



## Chapter 6

# Defining Web Policies

### Contents

- Introduction on page 159
- Creating a new policy on page 160
- Testing policy enforcement on page 162
- Uploading a policy assignment file on page 163
- General tab on page 163
- Connections tab on page 168
- Access Control tab on page 171
- Endpoint tab on page 178
- End Users tab on page 180
- Cloud Apps tab on page 188
- Custom Categories tab on page 191
- Web Categories tab on page 193
- Protocols tab on page 204
- Application Control tab on page 205
- File Blocking tab on page 207
- Data Protection tab on page 212
- Data Security tab (DLP Lite) on page 213
- Web Content & Security tab on page 217

## Introduction

---

On the **Web > Policy Management > Policies** page, there is a list of policies currently configured for your account. Click a policy name to view or edit a policy.

Standard account-level settings are shown in *Standard Web Configuration*.

There are several tabs associated with each policy. Depending on your subscription settings, you may not see all the tabs:

### Related concepts

[General tab](#) on page 163  
[Connections tab](#) on page 168  
[Access Control tab](#) on page 171  
[Endpoint tab](#) on page 178  
[End Users tab](#) on page 180  
[Web Categories tab](#) on page 193  
[Protocols tab](#) on page 204  
[Application Control tab](#) on page 205  
[File Blocking tab](#) on page 207  
[Data Protection tab](#) on page 212  
[Data Security tab \(DLP Lite\)](#) on page 213  
[Web Content & Security tab](#) on page 217

### Related tasks

[Cloud Apps tab](#) on page 188  
[Custom Categories tab](#) on page 191

### Related information

[Standard Web Configuration](#) on page 283

## Creating a new policy

To create a new policy:

### Steps

- 1) Click **Add**.
- 2) Enter a policy name and administrator email address. This email address is used as the address from which system messages are sent. Your users may occasionally reply to these messages, so this should be an email address that is monitored by your IT staff or administrative contact.



- 3) Select the template you want to use for your policy. This can be one of the following:
- A predefined template that determines which URL categories are blocked and which are permitted for a policy:
    - **Default** blocks a standard set of categories, including categories relating to adult material, drugs, violence, productivity, and security.
    - **Basic** blocks the most frequently blocked categories and permits the rest.
    - **Basic Security** blocks only categories considered to be a security risk.
    - **Monitor Only** permits all categories.

You can further refine how web traffic is managed changing the actions for individual categories on the *Web Categories tab*.

All other policy settings are as defined in *Standard Web Configuration*.

- A copy of an existing policy. If you select **Existing policy** and choose one of your policies from the drop-down list, all of the current settings in that policy are copied into your new policy, except for the following:
  - Proxied connections
  - End user details
  - Category and application control exceptions



#### Note

Selecting **Default** from the policy template drop-down is different than selecting the Default policy from the **Existing policy** drop-down. The first option applies only to web category blocking, while the second option uses the settings across all tabs in the Default policy for your new policy.

You can select a policy template only when creating a new policy. Once you have saved your settings for a new policy on the General tab, you cannot select a different template.

- 4) To use time-based policy enforcement, select the *Time zone* where your users are located.
- 5) In Internet availability, define any time-based web access controls that you want to use. The default setting is to allow Internet access at all times. For more information, see *Internet availability*.
- 6) If required, define confirm timeouts, quota settings, and search filtering. For more information, see *General tab*.
- 7) If available, define whether your users should see and agree to an *Acceptable use policy*.  
When enabled, use the drop-downs to select the AUP page to use when this policy is enforced and how frequently the notice should display.
- 8) Click **Save** when you are finished.

#### Related concepts

[Web Categories tab](#) on page 193

[Time zone](#) on page 164

[Internet availability](#) on page 164

[General tab](#) on page 163

**Related tasks**

[Acceptable use policy on page 166](#)

**Related information**

[Standard Web Configuration on page 283](#)

# Testing policy enforcement

Use the Filtering Test section on the **Policies** page to check how your policies handle a request for a URL. You can also test particular situations that may be causing issues for your end users, such as including a user name or user agent header.

To run the test:

## Steps

- 1) Under Filtering Test, enter the full URL that you want to test, including the `http://` or `https://` prefix.
- 2) Optionally, enter the email address of an end user registered or synchronized with your account.
- 3) Specify the **Egress point** for the test. By default this is the current IP address that you have used to access the cloud portal. You can also use:
  - **Other IP** to specify a different IP address that is registered as a proxied connection in one of your policies

**Note**

If you select **Other IP** and then enter an IP address that is not associated with your account, an error message results.

- **Unknown IP** to test a roaming user scenario
  - **Edge device** or **Appliance** to test connections forwarded to the cloud by an on-premises network device. If you have defined internal networks for your network device, you can optionally also specify the internal IP address that you want to test.
- 4) To identify a particular user agent that may be causing policy enforcement issues, mark **Specify user agent header** and enter the user agent string in the field provided.
  - 5) Click **Test**.  
The results pop-up window displays the following information:
    - The details that you entered, including the user email address and user agent if defined
    - The policy applied, as derived from the source IP address that you selected
    - The category or categories that contain the URL
    - The action applied to the URL by this policy
  - 6) Click **Close** when you are done.

# Uploading a policy assignment file

You can automatically assign end users to policies by uploading a file of policy and user information to the cloud service.

Format the CSV file as two columns, with a header row consisting of the words “EmailAddress” and “Policy”. The two columns must contain:

- An email address belonging to an existing user in your account
- A policy name in your account.

For example:

- *EmailAddress,Policy*
- *address1@domain1.com,Default*
- *address2@domain1.com,Sales Policy*

Note that you do not have to include all of your existing users in the file, only those whose policy assignment you wish to change. If a field contains a comma, it must be quoted.

To upload the file:

## Steps

- 1) Under Policy Assignment, browse to the file that you wish to use.
- 2) Click **Upload**.

## Next steps

The email addresses in the file are checked against the existing users in the account, and a confirmation message is displayed once the file has uploaded successfully. If there are errors in the file—for example, incorrect formatting, a non-existent policy name, or an invalid, unknown, or duplicate email address—the upload is canceled and an error message is displayed to explain the problem.

You can also download a CSV file containing the current list of end users assigned to policies by clicking **Download existing policy assignments**.

# General tab

Use the **General** tab to configure settings that cover basic aspects of your users’ web browsing, for example availability at certain times of the day, quota time limits, and agreement to your acceptable use policy.

This is also the tab that you see, with some additional options, when you create a new policy. For more information, see *Creating a new policy*.

If you make any changes to this tab, click **Save** when done.

### Related tasks

[Creating a new policy](#) on page 160

## Policy name

---

The name of the policy, which you may want to rename from Default to something more meaningful to your organization, especially if you have a requirement for multiple policies.

## Administrator email

---

This is the email address for the web administrator of this policy. This email address is used as the address from which system messages are sent. Your users may occasionally reply to these messages, so this should be an email address that is monitored by your IT staff or administrative contact.

## Default and alternate PAC file address

---

The default PAC file address is the policy-specific PAC file for this policy. The alternative PAC file address can be used for remote user requests from a network that has port 8081, 8082 or 8087 locked down.

See *Policy-specific PAC file* for further details.



### Note

If you have already deployed a policy-specific PAC file that uses a different URL than the one displayed on this page, there is no need to change it unless you wish to. PAC file URLs provided with earlier versions of your cloud web product will continue to work.

### Related concepts

[Policy-specific PAC file](#) on page 73

## Time zone

---

To use time-based web filtering, the cloud service must first determine the time zone where users are located. The time zone you set can be used as a single zone for the whole policy, or you can set up time zones for one or more of your proxied connections that override the time zone on the General tab (see *Proxied connections*).

Daylight saving time is supported where valid on all time zones except GMT and UTC, which are static.

### Related concepts

[Proxied connections](#) on page 168

## Internet availability

---

Use this option to configure time-based policy enforcement. The default setting is to allow Internet access at all times, although you can apply user and group-based exceptions (see *User and group exceptions for time-based access control*).

Alternatively, you can restrict all access by time and display an appropriate block page when access is unavailable. There are 2 formats for this:

- 1) Block access for the duration of a defined period (for example, during working hours).
- 2) Block access outside a defined period (for example, allowing users to access the Internet only during their lunch period).

The drop-down list contains the standard time periods and any custom periods you have set up (see *Time periods*).

#### Related concepts

[Time periods](#) on page 115

#### Related tasks

[User and group exceptions for time-based access control](#) on page 167

## Full traffic logging



#### Important

The full traffic logging feature is not available by default. To make it available in your account, contact Support.

As an alternative, consider migrating to SIEM Integration. Take advantage of **Bring your own storage** or switch between Forcepoint storage and your own. See *Configuring SIEM storage*.

When you enable full traffic logging for your account, all web policies inherit the default setting that you configure. If you want to override the default log retention for a particular policy, change the selection in the Full traffic logging drop-down list from **Use account default** to either **Enabled** or **Disabled**.

For full details of setting up and using full traffic logging, see the “Configuring Full Traffic Logging” technical paper.

#### Related tasks

[Configuring SIEM storage](#) on page 28

## Confirm timeout

Enter the maximum time in minutes (default 10) that a user who clicks Continue can access sites in categories governed by the Confirm action. See *Policy enforcement actions*.

#### Related concepts

[Policy enforcement actions](#) on page 196

## Quota time

Use this option to configure quota times for web categories accessed by users in this policy. See *Using quota time to limit Internet access* for more information. Select one of the following:

- A **Daily quota** applies to all users accessing categories with Quota as the filtering action or exception. Enter the **daily limit** in minutes (default 60) for all users of this policy. Then define the **session length** in minutes (default 10) during which users can visit sites in quota-limited categories.
- A **Per-category quota** allows you to specify a **daily limit per category** and a **session length per category** that applies to all quota-limited categories by default. You can then change the daily quota time settings for particular categories or filtering exceptions on the Web Categories tab. See *Managing categories actions, and SSL decryption*.

A session begins when the user clicks the Use Quota Time button.

The daily quota allocation for users within a policy is refreshed at midnight in the time zone defined for the user's proxied connection. If no specific time zones are defined in either the proxied connection or the policy, the quota allocation is refreshed at midnight UTC.

If you change the total quota time or session time after a user has started to use their daily quota or has received the quota block page from the cloud-based service, the changes will not take effect until the next day. Similarly, if you move a user to a different policy after they have started to use their daily quota or has received the quota block page from the cloud-based service, the change does not take effect until the next day.

### Related concepts

[Using quota time to limit Internet access](#) on page 198

### Related tasks

[Managing categories, actions, and SSL decryption](#) on page 195

## Search filtering

Search filtering is a feature offered by some search engines that helps to limit the number of inappropriate search results displayed to users.

To activate this option, select **Enable search filtering**.

Ordinarily, Internet search engine results may include thumbnail images associated with sites matching the search criteria. If those thumbnails are associated with blocked sites, the cloud service prevents users from accessing the full site, but does not prevent the search engine from displaying the image.

When you enable search filtering, the cloud service activates a search engine feature that stops thumbnail images associated with blocked sites from being displayed in search results. Enabling search filtering affects both local and roaming users.

## Acceptable use policy



### Note

Acceptable use policy is a limited-availability feature and may not be enabled for your account.

This feature does not apply to I Series appliances.

You can display a notice to users informing them of your organization's acceptable use policy for Internet use and asking them to agree to accept its terms before they can continue browsing.

To display the notice, mark **Require users to agree with acceptable use policy every** In the drop-down menus, select the AUP page and how frequently you would

like to display the notice. The choices are 1, 7, and 30 days.

You can tailor the default acceptable use policy notification to meet your needs, or add different AUP pages for different policies. See *Configure block and notification pages*.

To apply exceptions to the acceptable use policy for certain domains:

## Steps

- 1) Click **Domain Exceptions**. This button appears only when you have selected the Require users to agree with acceptable use policy box.
- 2) Enter one or more domain names, separated by commas. When users in this policy browse to these domain names, they will never be asked to agree to the acceptable use policy notification page configured for the policy.
- 3) Click **Add**. The domains you have specified are listed below the Add field. To delete a domain, select it from the list and click **Delete**.
- 4) Click **Save** when you are done.

### Related tasks

[Configure block and notification pages](#) on page 118

# User and group exceptions for time-based access control

You can apply both user and group exceptions to any time-based access control that you set up on the **Web > Policies > Time Access Exceptions** page for a given policy. To view the list of exceptions, or to add or edit an exception, click the link next to **Internet availability** on the General tab for the policy.

To edit an exception, click the exception, then click **Edit**. To add an exception:

## Steps

- 1) Click **Add exception**.
- 2) The rule **State** is set to ON by default, meaning the rule will be enabled for the users and groups you select. If you want to set up a rule but not enable it immediately, click the State switch to set it to OFF.
- 3) Enter a **Name** and **Description** for the rule.
- 4) Choose the notification page that appears to users in this exception.

- 5) Select the **Time period** during which the rule is active. If you select *During* or *Outside*, the drop-down list contains the standard time periods and any custom periods you have set up (see *Time periods*).
- 6) For an exception that should be applicable to roaming users only, mark **Apply only when user is roaming**.
- 7) Do one of the following:
  - a) To set up an exception for specific users or groups, select **For these users and groups**. You can then enter a comma-separated list of email addresses, or select one or more groups, or both.
  - b) To set up an exception for everyone except those in a specific group, select **For everyone not in the group**, and choose a group from the drop-down list.
- 8) Click **Save**.

#### Related concepts

[Time periods](#) on page 115

## Connections tab

Use the **Connections** tab of the **Web > Policy Management > Policies** page for any policy to define:

- The source IP addresses (proxied connections) assigned to the selected policy (see *Proxied connections*)
- Destination domains and IP addresses that users assigned this policy can access without going through the cloud service (see *Proxy bypass*)

#### Related concepts

[Proxied connections](#) on page 168

#### Related tasks

[Proxy bypass](#) on page 170

## Proxied connections

Most organizations have at least one proxied connection configured per policy. The proxied connection address is used to identify traffic from your organization's egress IP address and, by default, apply the policy to that traffic.

Proxied connections:

- Are public-facing IP addresses, IP address ranges, or IP subnets for offices in your organization using the cloud service.
- Are often the external address of your Network Address Translation (NAT) firewall.
- May be appliances or edge devices configured on the **Web > Settings > Network Devices** page.
- Could include branch offices, remote sites, or satellite campuses.



Proxied connections are NOT:

- 1) IP addresses of individual client machines.
- 2) IP addresses outside your organization.

If you have several points of presence on the Internet, you can combine all of these under one policy, or have separate policies for each public-facing IP address.



#### Note

If you do not add any proxied connections to the policy, all users are treated as remote and must authenticate to use the service. In this case, the policy they use is determined by their email domain. They see a service-wide Remote User Welcome page that is not configurable. Once logged on, they are served configurable notification pages from the customer account.

## To add a proxied connection

### Steps

- 1) Click **Add** under the Proxied Connections table.
- 2) In the Add Proxied Connection dialog box, enter a unique **Name** and helpful **Description** for the connection.
- 3) Specify the connection **Type**, then enter the **Address** (single IP address), **Subnet**, or **Range**.
- 4) Select the **Time zone** for this connection.

If you have a single policy for multiple Internet gateways in different countries, you may want to set each to a different time zone. If all connections are in the same time zone, it is easier to set the time zone for the complete policy (see *Time zone*) and select the “use policy time zone” option.

Daylight saving time is supported where valid on all time zones except GMT and UTC, which are static.

- 5) Optionally, mark the **Override Google redirect behavior** checkbox, then determine which override option to use.

By default, Google redirects browsers to the appropriate site for the country it detects (for example, google.fr for France). Sometimes this is not accurate (for example, if end users browse through a cloud proxy in a different country).

The Google redirect setting for the connection takes precedence over the setting for the policy (see *User and group exceptions for time-based access control*). If you do not configure Google settings for the connection, the policy-level, if any, are used.

This feature requires that you enable SSL decryption for the Search Engines and Portals category on the **Web Categories** tab (see *Managing categories, actions, and SSL decryption*), and install the Forcepoint root certificate on end user machines. If you mark the checkbox without enabling SSL decryption, a warning appears.

The available options are:

- **Ensure requests for google.com are not redirected**, which prevents Google from redirecting to a local country site when the end user enters “google.com”
- **Redirect requests for google.com to**, which ensures all google.com requests are redirected to a local country site of your choice. Enter the country code in the text field (for example, **fr** for google.fr, or **co.uk** for google.co.uk).

- 6) Click **Continue** to save your change and return to the Connections tab.

#### Related concepts

[Time zone](#) on page 164

#### Related tasks

[User and group exceptions for time-based access control](#) on page 167

[Managing categories, actions, and SSL decryption](#) on page 195

## Proxy bypass

Proxy bypass sites are destinations that users can access either directly, or through an alternate (third-party) proxy, without going through the cloud service. For example, organizational webmail sites and system traffic, like Microsoft and antivirus updates, should be added to the bypass list.

- For users with the Neo or Direct Connect endpoint, bypass destinations are not analyzed by the cloud service.
- For users whose traffic is sent to the cloud service via PAC file, including users of the Proxy Connect endpoint, bypass destinations are added to the policy PAC file.
  - By default, the PAC file excludes all non-routable and multicast IP address ranges; so if you are using private IP address ranges defined in RFC 1918 or RFC 3330, you need not enter these.
  - Browsers configured to use the policy’s PAC file automatically use the cloud service, but bypass it for the specified destinations.

Any destinations that you add to the Proxy Bypass table apply only to the selected policy. To add bypass destinations that apply to all policies, use **Proxy Bypass** tab of the **Web > Settings > Bypass Settings** page.

To define bypass destinations:

## Steps

- 1) Click **Add** under the Proxy Bypass table.
- 2) In the Add Proxy Bypass dialog box, enter a unique **Name** and helpful **Description** for the destination.
- 3) Specify the destination **Type**, then enter the **Address** (single IP address), **Subnet**, or **Domain**.
- 4) If traffic to the specified destination is managed by a third-party proxy, mark the **Send traffic to another proxy** check box, then enter the proxy IP address or hostname in the field provided.



### Important

The alternate proxy specified here **must not** be another Forcepoint proxy.

- 5) Use the optional **Comment** box to add helpful information, such as why the entry was created.
- 6) Click **Continue** to save your changes and return to the Connections page.



### Note

You can add a total of 1000 proxy bypass destinations per policy. Account-level bypass destinations (added via **Web > Proxy Bypass**) count towards this limit for each policy. For example, if your policy has 10 bypass destinations, and you have 10 account-level bypass destinations, this is counted as a total of 20 destinations for the policy.

## Access Control tab

Use the **Access Control** tab to configure how your end users are identified by the cloud service. You can configure multiple authentication or identification options for your users if required.

The cloud service works “out of the box” for many organizations. A single policy applied to an organization’s web traffic provides protection from malware and inappropriate content. However, most customers want to tailor the service to align it with their Internet acceptable use policy, which may require granular configuration on a per-user and per-group basis, with different users or groups assigned to specific policies. Often, organizations want to report on the surfing habits of their employees. These use cases require the service to identify specific users in order to apply the correct policy, and to log user actions for reporting purposes.

There are a number of events that can lead to an end user being asked to authenticate:

- The user is connecting from an IP address configured as a proxied connection in one of your policies, and the policy has the **Always authenticate users** option enabled on the Access Control tab.
- The user is accessing a website within a category that has an action of **Require user authentication**. You configure this within the category itself.
- The user is attempting to access a website for which there is a group or user exception. At this point, the cloud service needs to find out who the user is in order to determine whether the exception applies.
- The end user connects from an unknown IP address, so is considered a remote user.

When a request is made from an unknown IP address, users are served a notification page asking them to authenticate. Because the cloud service does not know who the users are at this time, the notification page is a generic service-wide page. See *Roaming home page* for further information.

**Note**

If user authentication is required by a connection-based policy, the service checks whether the user is assigned to a specific policy, and applies the user's policy. The user's "home" policy overrides the IP-based policy for enforcement actions.

**Related concepts**

[Roaming home page](#) on page 75

## To configure user authentication

---

### Steps

- 1) Under **Authentication Settings**, define when to authenticate.
  - Select **Always authenticate users on first access** to force all users of this policy (whose source IP address or appliance is configured on the Connections tab) to identify or authenticate themselves to proceed. If they do not, they are unable to use the cloud service.
  - Select **Only authenticate when** if you want to use authentication only if either of the following is true:
    - Users are accessing the web from an unknown IP address.  
In this case, if web endpoint software or single sign-on is not available, the user receives the service-wide Welcome page. Users must log on to allow the correct policy to be applied.
    - The requested site is in a category or has a user or group exception that requires authentication.

2) Select the authentication methods you wish to use.

If you do not select any authentication methods, when users try to access a website, they are presented with a basic authentication dialog into which they must enter their cloud logon credentials to proceed.

The cloud service provides the following options for identifying end users transparently:

- Select **Endpoint** to use web endpoint software, which is installed on client machines to provide transparent authentication, enforce use of web policies, and pass authentication details to the cloud-based service. See *Configure Endpoint settings*.
- Select **Single sign-on** to use clientless transparent authentication via a supported identity provider. See *Configure End User Single Sign-On settings*.

If you do not deploy web endpoint software or use single sign-on, the cloud service can use one of the following methods to identify users transparently or manually when they connect to the Internet.

- Select **NTLM transparent identification** to identify users in this policy with their NTLM credentials. Then, select the NTLM registration page or use the default setting. See *NTLM identification* and *NTLM registration*.

NTLM transparent identification is also used as a fallback if either the web endpoint or single sign-on fails.



#### Note

NTLM transparent identification is not valid for remote users (connecting from unknown IP addresses). Such users must always authenticate with the web endpoint, single sign-on, or a valid email address and password.

- Select **Secure form-based authentication** to display a logon form to the end user. When the user enters their cloud credentials, they are sent over a secure connection for authentication. If the users have not previously registered to use the service, they can do so by clicking **Register**. This takes them into the registration process. See *End Users tab* for further details.

Note that manual authentication is always used if none of the above methods is available.

- 3) Select **Welcome page** to show a configurable welcome page to end users prior to the basic authentication dialog box, if their browser supports it. See *Pre-logon welcome page*.
- 4) If you have selected single sign-on or secure form authentication, set a **Session timeout** period to specify the time interval after which a user's login and password are revalidated. See *Session timeout*.
- 5) Click **Save**.

#### Related concepts

[Configure Endpoint settings](#) on page 91  
[NTLM identification](#) on page 175  
[NTLM registration page](#) on page 175  
[End Users tab](#) on page 180  
[Pre-logon welcome page](#) on page 174  
[Session timeout](#) on page 174

#### Related tasks

[Configure End User Single Sign-On settings](#) on page 80

# Pre-logon welcome page

When you select **Welcome page (where client software supports it)**, a configurable welcome page is presented to end users prior to the basic authentication dialog box, if their browser supports it. You can specify a single page that is presented for connection requests or different pages for requests using HTTP. The default pages provide three buttons: **Log in**, **Register**, and **Forgotten your password?**

- **Log in:** To continue, users click **Log in** and are presented with the basic authentication dialogue.
- **Register:** If the users have not previously registered to use the service, they can do so by clicking **Register**. This takes them into the registration process. See *End Users tab* for further details.
- **Forgotten your password?:** If users cannot remember their password, they can click **Forgotten your password?** They are redirected to a web page where they enter their email address. An email is sent containing a link to the cloud service, where they must create a new password before being allowed to continue to authenticate.

As with all notification pages, you can tailor the default to meet your needs and use it to remind your users that they are using company resources that are governed by an acceptable use policy. In addition, you can select the option to display a notice to your users that asks them to agree to accept the terms of your acceptable use policy if they wish to continue browsing. See *Acceptable use policy*.

## Related concepts

[End Users tab](#) on page 180

## Related tasks

[Acceptable use policy](#) on page 166

# Session timeout



## Note

The session timeout option of this page does not apply to traffic from an I Series appliance. For information on configuring session timeout for appliances, see *Adding or editing appliance information*.

Users' credentials for single sign-on and secure form-based authentication are not sent every browser session. However, the credentials must be revalidated periodically for security reasons, and you define the time period for that revalidation under **Session timeout**. The options are 1 day, 7 days, 14 days, 30 days, 3 months, 6 months, or 12 months.

Once the selected period has elapsed after a user's credentials were last validated, the user is either re-authenticated transparently through your identity provider, or asked to supply their logon credentials again for form-based authentication.

## Related concepts

[Adding or editing appliance information](#) on page 151

# NTLM identification

---

Select **NTLM transparent identification where possible** to use the Windows NT and LAN Manager authentication protocol (NTLM) identification for all users of this policy except those whose user agent types are known not to support it—for example, Firefox on Linux. Non-supported user agents are presented with the pre-login welcome page, and users can log on using the basic authentication mechanism.



## Note

---

NTLM transparent identification is not valid for remote users (connecting from unknown IP addresses). Such users must always authenticate with the web endpoint, single sign-on, or a valid email address and password.

# NTLM registration page

---

Users of policies where NTLM is selected must undergo an additional, once only, registration task to associate their NTLM credentials with their registered cloud credentials. See *NTLM transparent identification* for further information. As with all notification pages, you can use the default page, customize it, or create your own.

## Related concepts

[NTLM transparent identification](#) on page 185

# Further information about NTLM

---

NTLM has evolved through numerous Windows and Windows NT versions. It provides a way for users to authenticate themselves with the company network.

# NTLM identity

---

The NTLM identity is the domain\username with which users log on to their Windows PC; for example, MYDOMAIN\jsmith.

# NTLM credentials

---

NTLM credentials include the NTLM identity (as defined above), the PC's identity, and a non-reversible encryption of the user's password. These are sent by the browser when a server (in this case a cloud service proxy) sends an NTLM challenge.

# NTLM security implications

---

There are a number of security implications associated with the use of NTLM in the cloud service. These are discussed below.

## The NTLM credentials are being passed across an unsecure Internet connection

---

NTLM is a secure protocol that does not carry the user's password, but a cryptographic hash of the password. To authenticate a user by validating a password hash, a network service must know the user's password. The cloud service is outside of the company network, and so does not know the user's network password. For this reason, the cloud service can use NTLM only to identify users, not to authenticate them. This limitation helps to preserve the security of the user's network passwords.

## Transparent identification compared to basic authentication

---

Because NTLM does not require the user to actually authenticate with the cloud service by entering a password, one might argue that it is less secure than basic authentication. This is not the case. Most cloud service users save their usernames and passwords in their browsers and therefore, if someone wanted to surf the Internet as another user, they can do so if they can access that user's PC. This is exactly the same situation as NTLM. To protect against this, in both cases, and with any product that provides web filtering, you should consider physical security and keyboard locking when users leave their desks to keep the network secure.

## Limitations

---

- 1) Transparent identification does not authenticate; for example, it does not do password checking. It relies on the customer site having secure NT or Active Directory domains set up, along with physical security to stop unauthorized access to the company network or the users' computers.



### Note

Although NTLM Identification works with Windows workgroups, it is not a recommended solution if you are concerned about security and correctly identifying end users.

- 2) You cannot use transparent identification for remote users. Remote users must be registered and must log on using their email addresses.
- 3) Users of non-Windows systems in a transparent identification policy still have to log on manually.
- 4) Many proxies do not pass NTLM challenges, so if you have a chained proxy deployment, you should check this. Microsoft ISA/TMG Server and Blue Coat ProxySG do support NTLM pass-through.
- 5) A browser that supports NTLM but is operating in a non-Windows environment (e.g., Firefox on a Linux platform), may exhibit strange behavior and may not work with a cloud policy that is configured to use NTLM. Where possible, we attempt to identify such browsers by user agent type and send an authentication request rather than an NTLM challenge.
- 6) The existing Welcome page is not shown to users of NTLM-capable browsers in a transparent identification policy.



# How NTLM works once users are fully configured

*Fully configured* means that users are registered with the cloud service and their NTLM identities are known. See *End Users tab* for details on registering users, and *NTLM transparent identification* for details on NTLM identity.

- 1) Users start their browsers and try to visit a website.
- 2) The cloud service checks the users' source IP address and applies the correct policy.
- 3) The cloud service finds that transparent identification is enabled in the policy and initiates the NTLM conversation, during which the browser sends the NTLM credentials with no involvement of the users. Note that it is the local policy (i.e., the one identified by IP address) that determines whether NTLM is to be used.
- 4) The cloud service finds the users' information in the policy by looking up the NTLM identity, and marks this connection as identified.
- 5) The cloud service processes the original request as normal. This all happens transparently, behind the scenes.

## Related concepts

[End Users tab](#) on page 180

[NTLM transparent identification](#) on page 185

# Setting authentication options for specific users

If you wish to enforce specific authentication options for certain end users, overriding the authentication settings defined in the policy, you can do this via a setting in the user's PAC file URL. For those users who need to use a specific authentication mechanism, deploy a PAC file URL using the "a=" switch, in the following format:

`http://webdefence.global.blackspider.com:8082/proxy.pac?a=X`

The **a=** parameter controls the authentication option used, where **X** can be one of the following:

Parameter	Description
a=n	NTLM identification is used. If NTLM is not supported by the browser or application, basic authentication is used.
a=t	Authentication is performed using single sign-on. If the application or user agent cannot use single sign-on, NTLM identification or basic authentication is used. If a remote user cannot log on using single sign-on, they are given the option to try again or log on using other credentials.

Parameter	Description
a=f	Authentication is performed using secure form-based authentication.

For further details about PAC files, see *Proxy auto-configuration (PAC)*.

#### Related concepts

[Proxy auto-configuration \(PAC\)](#) on page 71

## Endpoint tab

Use the **Endpoint** tab to enable secure transparent authentication with the web endpoint for end users whose requests are managed by this policy.

The cloud service uses the User Principal Name (UPN) or the NTLM ID provided by the endpoint agent to match endpoint users to the appropriate policy. The service first attempts to match the UPN. If no match is found, or if no UPN is available, the service attempts to find a user match using the NTLM ID.

From this tab you can deploy the Proxy Connect endpoint to either the roaming users or all users in the policy directly from the cloud. (The Direct Connect endpoint and Neo must be installed manually; automatic installation from this tab is not supported.)

- Proxy Connect users in your network will be asked to install the endpoint software on their machine when they start a browsing session.
- Roaming users must first authenticate themselves via the *Roaming home page* before being asked to install the endpoint software.

See [this Knowledge Base article](#) for a list of browsers that support Proxy Connect endpoint deployment directly from the cloud.

For Neo, Proxy Connect, and Direct Connect endpoint software, you can push the endpoint manually to selected client machines using your preferred distribution method. For more information, see *Configure Endpoint settings*.



#### Note

You must set an anti-tampering password for Proxy Connect or Direct Connect endpoint installations before you can deploy the endpoint software. Set this password on the **Web > Settings > Endpoint** page.

For both classic Direct Connect and Proxy Connect endpoint clients, you can choose to automatically update endpoint whenever a new version is released. Note that if you select an automatic update option, it applies to all users in the policy who have installed the endpoint on the selected operating system, regardless of how the endpoint software was originally deployed.

For Neo, automatic updates are enabled by default but can be configured on the Neo management portal, accessed from the **Web > Settings > Endpoint** page. For more information, see *Settings* section of the [Forcepoint Dynamic User Protection Help](#).

#### Related concepts

[Roaming home page](#) on page 75

[Configure Endpoint settings](#) on page 91

# Neo

Use this section to select the Neo mode to use. Select:

- **Intelligent auto-switching...** to automatically switch between proxy connect and direct connect modes based on performance and network conditions. This is the recommended option.  
Neo uses the appropriate endpoint mode, based on network conditions. When proxy connect mode is in use but can't connect to the proxy or if performance becomes an issue, Neo will switch to the direct connect mode.
- **Proxy Connect** to use only the Proxy Connect endpoint mode. This Neo mode corresponds to the functionality available in the standalone classic Proxy Connect agent.
- **Direct Connect** to use only the Direct Connect endpoint mode. This Neo mode corresponds to the functionality available in the standalone classic Direct Connect agent.

From the **Fallback mode** drop-down, select the fallback behavior that should be applied to a user request if the network connection to Neo is interrupted.

- **Open** to allow the user request.
- **Closed** to block the user request.
- **Safe** (not available with Proxy Connect) uses local cache to apply policy.

## Endpoint PAC Control

By default, Neo and Proxy Connect endpoint clients retrieve the cloud service PAC file and use it to determine which websites should be accessed through the cloud proxy, and which port to use for web browsing.

Use the settings in the Endpoint PAC Control section to determine which PAC file URL Endpoint should access for users in this policy.

The options are:

- **Use default PAC file URL...**: retrieves the PAC file over port 8082 (or 8087 for HTTPS). Web browsing is performed via port 8081.
- **Use alternate PAC file URL...**: retrieves the PAC file over port 80 (or port 443 for HTTPS). Web browsing is also performed via ports 80 or 443. Use this option for locations where ports 8081 and 8082/8087 are locked down.

For more information on the default and alternate PAC file URLs, see *Proxy auto-configuration (PAC)*.

Select **Retrieve PAC file over HTTPS** to download PAC files over a secure (HTTPS) connection. For more information on this setting, see *Accessing PAC files over HTTPS*.



### Note

These settings only apply to the Proxy Connect endpoint. The **Retrieve PAC file over HTTPS** option requires build 2826 or later. Earlier versions of the Proxy Connect endpoint will always download the PAC file over HTTP, and are not affected by this setting. Ensure that your Endpoint clients have connectivity to a Forcepoint point of presence (data center or local PoP) on TCP ports 8087 or 443, as appropriate, before enabling this option.

### Related concepts

[Proxy auto-configuration \(PAC\) on page 71](#)

[Accessing PAC files over HTTPS on page 74](#)

# Classic Endpoint installation

---

To configure web endpoint software installation:

## Steps

- 1) If you want to deploy the Proxy Connect endpoint client automatically, mark the **Deploy endpoint software on user machines...** checkbox.  
This setting defines whether the endpoint is deployed to the end users in this policy. If you clear this option at a later date, there will be no further new deployments of the endpoint. However, the installed endpoint software will continue to work unless it is uninstalled from the client machines.
- 2) Choose whether the Proxy Connect endpoint is deployed to all cloud end users, or only to roaming users.
- 3) To ensure that your endpoint client software always uses the latest version, mark one or more automatic update check boxes.  
If you clear these options at a later date, there will be no further automatic updates of existing installations, although the installed endpoints will continue to work.
- 4) Define which PAC file URL the Proxy Connect endpoint should use, and whether to retrieve the PAC file via a secure (HTTPS) connection.  
Use the alternate PAC file address for locations where non-standard ports are locked down (see *Endpoint PAC Control*).
- 5) Under Classic Endpoint Installation Screen, you can provide a customized message that appears to end users on Windows machines at the beginning of the Proxy Connect endpoint download and installation process.  
The message can be used to reassure the user that the download is company- approved, and to provide any further information they may need. To customize the message, enter the message you want to display in the **Branding text** field.
- 6) Click **Submit** when done.

### Related concepts

[Endpoint PAC Control](#) on page 179

## End Users tab

---

The **End Users** tab is where all end-user registration configuration is performed. Registration is the method of getting user credentials into your cloud service account.

There are currently 3 methods of registering end users:

- 1) *Registering by invitation*
- 2) *Bulk registering end users*

### 3) *End user self-registration*

For (2) and (3) above, you must enter the email domains where the users' email addresses reside into the account or policy. See *Configure Domain settings* for further information. For (1), users do not need an email address within your configured domains.

If you have chosen to use the identity management feature to synchronize your user and group data with the cloud as described in *Working with External Directories*, you do not need to register end users at all. You can synchronize your organization's users with the cloud service instead. When you synchronize, users are automatically registered with the cloud-based service. (They only need to self-register when they travel.)

Directory synchronization can include NTLM IDs. You can then enable NTLM identification on the **Access Control** tab. This allows your users to use the service immediately after synchronization, without their having to perform any self-registration actions or manual logon. If you enable NTLM identification but for some reason do not synchronize NTLM IDs from your directory, your users are required to complete the self-registration process, and then perform a second registration operation to associate their NTLM ID with their user account on the service. (See *NTLM transparent identification* for more information.)

If you don't want to use NTLM identification, you can configure the service to send invitations to all newly synchronized users. They can then complete self-registration process and log on using email address (or name) and password.

Through the Directory Synchronization feature (not supported by SCIM), you have the option to notify new users that they are protected by the cloud-based service when they surf the web.

If System for Cross-domain Identity Management (SCIM) has been configured for identity management users can use the service immediately after synchronizing user information with your identity provider, without first having to perform self-registration. Note, however, that it can take a number of minutes before all new information is propagated to policies

#### Related concepts

[Bulk registering end users](#) on page 182

[End user self-registration](#) on page 184

[Configure Domain settings](#) on page 89

[NTLM transparent identification](#) on page 185

#### Related reference

[Registering by invitation](#) on page 181

#### Related information

[Working with External Directories](#) on page 51

## Registering by invitation

There may be users that you want to use your policy who do not have an email address within your email domains; for example consultants or contractors working at your location that you want to be bound by your Internet usage policy. You can invite these users to use the policy by selecting **Invite an End User** from the End Users tab.

Once you have added the end users' names, email addresses, and if available NTLM identification, the cloud service sends them the registration email in the same way as if they had self-registered. They click on the link and are asked to enter their password.

Field	Description
Name	Name of the user you want to invite to use the policy.
Email address	Email address of the user to invite.
NTLM Identity	The NTLM identity of the user, if available.
State	Enabled or disabled. If enabled, you can choose which block page to display for this user.

## Bulk registering end users

Bulk end-user registration simplifies the self-registration process by reducing it from 2 steps to 1. Rather than the end users visiting the portal and entering their names and email addresses into a form, you upload their names and email addresses in bulk, and the cloud service automatically dispatches them email. The users can then register at stage 2, where they click a link in the email they receive and enter their password into the portal.

## Uploading users' details

Click **Bulk register end-users** from the End Users tab when you want to upload end users' email addresses all at once. On the resulting screen, specify the file to upload and various other parameters:

Field	Description
Upload File	Browse to the text file to upload. See <i>Bulk upload file format</i> below.
Character Set	The character set of the file; this is normally either iso-8859-1 or Unicode.
Add New Users to Groups	You can add new users to a single or multiple groups by selecting them on this page. Alternatively you can specify group membership in the upload file.
File Contains NTLM Identities	Click if the file contains NTLM identities.
Replace details of existing users	Click if you want to replace a current record with this one.
Notification Email Address	Notification email address is the sender address of the registration email.
Invitation Email Language	The language variant of the registration email. To include language variants of this email, edit the End User Registration Email notification page. See <i>Editing notification pages</i> .
Batch the Invitation Emails	Registration emails are batched to prevent your email servers being flooded by thousands of messages at once. You can specify the frequency.

### Related concepts

[Bulk upload file format](#) on page 183

**Related tasks**

[Editing notification pages](#) on page 121

## Bulk upload file format

You can specify group membership in the uploaded file. The format of the file is shown below:

*Name,EmailAddress,Groups*

For example:

*Fred Bloggs,fred.bloggs@acme.com,"Corporate Finance,All in Reading,"*

*Hans Bloggs,hans.bloggs@acme.de,All in Germany*

**Note**

You can specify multiple groups, but because the field itself contains commas, you must enclose them in quotes.

If you are including NTLM identities, they may appear at the beginning or end of the line.

*Name,EmailAddress,Groups,NTLMIdentity*

*NTLMIdentity,Name,EmailAddress,Groups*

For example:

*Anita Rao,arao@acme.com,QAGroup,testdomain\anita*

The end of each line can be either a line feed, carriage return or both but you cannot mix them. For example, you cannot end one line with a carriage return and another with a line feed.

**Note**

If you are saving a file from Excel, do not Save As CSV (comma delimited) (\*.csv), because this does not end lines consistently. Save As CSV (MS-DOS) (\*.csv) instead.

The default notification template (end-user registration message) is available in HTML and TEXT. The version displayed to users depends on whether they use an HTML- or text-based email client.

## Bulk upload results

After the file is uploaded, a status page is shown indicating whether any records were rejected and, if so, a link is displayed enabling you to download the rejected records, if desired.

## Monitoring email dispatch

The status page also provides a link that lets you monitor the dispatch of registration messages.

The user management area also has a link to the upload status page. If there are multiple dispatches in progress, a list is shown.

# End user self-registration

---

For individual end user self-registration, a user must have an email address on a domain that has been assigned to the policy or account. This allows you to control who can register to use each of your policies. Click **Add** on the End User tab to add domains to the policy.

Individual end-user self registration is a 2-stage process:

## Stage 1

---

End users visit <https://www.mailcontrol.com/enduser/reg/index.mhtml> and enter their name and unique email address.

They can also access this page by clicking **Register** on the default logon page. Once they have submitted their name and email addresses, the cloud service sends them an email with a link, asking them to click it to confirm their registration.

## Stage 2

---

Users click the link and are prompted for a password. From then on, if challenged by the proxy service, they can enter their email address and password to gain access to authenticated resources.

# Identity management

---

When you enabled identity management for your account, you can specify how users are assigned to policies. If you have multiple web policies, you can use group membership to assign users to policies. The assignment can be static (assigning a user to a policy only when that user is initially registered) or dynamic (changing policy assignment as group membership changes). This is all configured on the **Identity Management** page: see *Configure identity management*.

The End Users tab enables you to assign the current policy to a group or groups of synchronized users, overriding the default assignment:

## Steps

- 1) Choose the **End Users** tab.
- 2) Under **Identity Management**, click **Modify list of groups**.
- 3) Select the group(s) you want assigned to this policy.
- 4) Click **Submit**.  
The effect of this action is to assign all members of the group to this policy.

### Related tasks

[Configure identity management on page 59](#)



# NTLM transparent identification

---

In order to access the cloud service using NTLM transparent identification, some users are prompted to associate their NTLM credentials with their registration details the first time they access the service (or the first time transparent identification is enabled on their policy). This includes users who register themselves, are invited to register, or are bulk registered.



## Note

If you are using directory synchronization and have synchronized NTLM IDs, users are not prompted for this information.

For non-directory users, the following process occurs one time:

- 1) The users start their browsers and try to visit a website.
- 2) The cloud service checks the users' source IP address and applies the correct policy.
- 3) The cloud service finds that transparent identification is enabled in the policy and initiates the NTLM conversation, during which the browsers send the NTLM credentials with no involvement of the users.
- 4) The cloud service fails to find the users' NTLM information in the policy.
- 5) The cloud service displays the NTLM registration page.
- 6) The users, if already registered, enter their email addresses and passwords and submit the form. If they are not already registered, they can click **Register**, also on this page, and are taken through the standard end-user self-registration process.
- 7) The cloud service validates the usernames and passwords that are entered. If the validation fails, it re-displays the form.
- 8) If the validation succeeds, the cloud service records the previously received NTLM identity against this user, and marks this connection as being identified.

Request processing continues as for a fully configured user.

## Editing end-user registration pages

---

You can edit all end-user registration pages and the registration message to suit your requirements. The default pages include instructions to help users understand the process but these are limited for ease of editing.

## Managing registered users

---

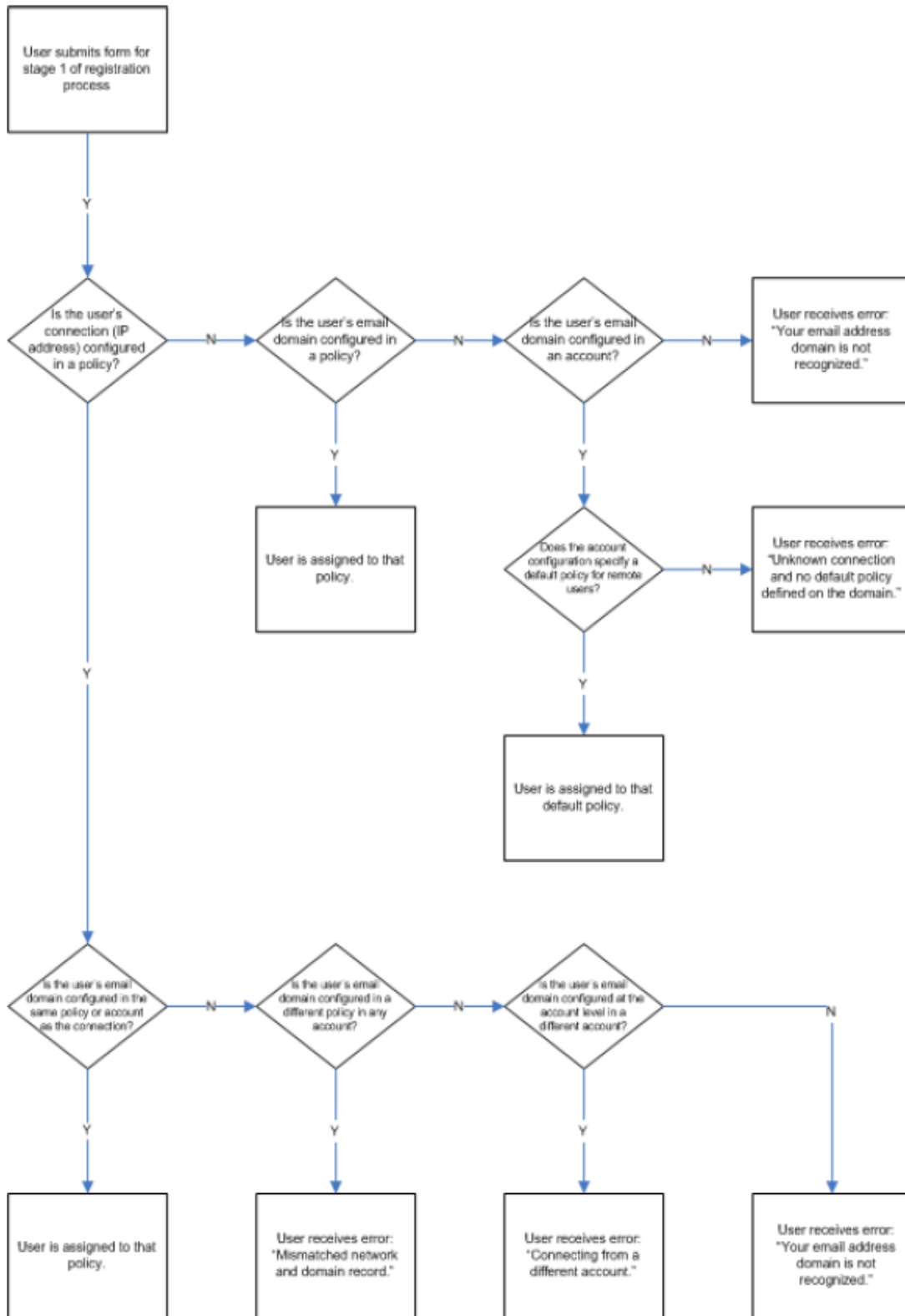
You can search the list of end users who are registering or have registered by clicking the link where the number of registered users is reported on the End Users tab. This page is the same as the account-level end users page, except that it applies changes at the policy-level.

From the search results page, you can select an individual user and modify his or her details. You can change a user's name (but not email address, because that uniquely identifies the user), delete the user, or block the user from accessing the service. Note that the service's self-registration feature means that deleting a user does not prevent that user from re-registering. However a blocked user is not able to re-register using the same email address.

## Rules for policy association during end-user registration

---

The following diagram shows the rules that the cloud service uses when determining with which policy a user is associated when they complete stage 1 of the registration process.



# Cloud Apps tab

---

The cloud service includes a database of cloud applications that can be used to allow or block user access to selected applications.

Click the **Cloud Apps** tab to configure a list of cloud apps to be blocked and a separate list of cloud apps to be allowed by this policy.

Note that customers who have licensed and use the Protected Cloud Apps feature will see slight differences when using the Cloud Apps tab for policies for which protected cloud apps should be applied. See *Using the Cloud Apps tab with Protected Cloud Apps* below.

## Steps

- 1) Enable **Always allow access to cloud apps on the Allow Access list** to always permit user access to cloud apps that have been added to the Allow Access list. User requests to these applications are allowed regardless how the corresponding category is configured on the Web Categories tab.  
See *Filtering action order* for details on how the cloud service applies filtering actions.
- 2) Select **Block all high risk level applications** to block access to any cloud app that is considered high risk. The number of high risk applications is provided in a link that can be used to open a scrollable list of the qualifying apps. When the list is open, use your browser search feature to locate specific apps.
- 3) Click the link to the **Cloud Apps** block page to navigate to **Web > Block & Notification Pages > Page Details** and customize the block page created specifically for blocking user access to cloud apps.

- 4) In the **Block Access** list, select specific cloud apps that should always be blocked, regardless of their risk level.
  - a) Enter all or part of a cloud app name in the search box.
  - b) A drop-down list appears, containing cloud app names that qualify for the search. As text is entered, the list of qualifying apps changes to match the search criteria. Search results are listed alphabetically within each risk level.

Note that, if **Block all high risk level applications** has been selected, the selection list is limited to medium and low risk apps. Search results provide only the total number of high risk apps.
  - c) Select the app or apps you wish to add to the blocked list by marking the check box next to the app name.

Apps that have already been included in the **Allow Access** list cannot be selected. They must first be removed from that list.

Click **Done** when you have finished making your selections. Each selected cloud app is added to the blocked list.
  - d) Remove an app from the list by removing the check mark.

The number of selected apps included in each risk level is provided next to the risk level name. Cloud apps in the list are sorted alphabetically within each risk level.

If **Block all high risk level applications** was enabled, the risk level and total is automatically included in the list. The actual apps are not listed. If one of the high risk apps is specifically selected in the **Allow Access** list, the count is reduced by the number of high risk apps allowed.



#### Important

The **Block Access** list takes precedence over actions assigned on the Web Categories tab. If a blocked cloud app is requested using a URL categorized in a category that is set to allow, access to it is blocked.

- 5) In the **Allow Access** list, select cloud apps that should always be permitted.
  - a) Enter all or part of a cloud app name in the search box.
  - b) A drop-down list appears, containing cloud app names that qualify for the search. As text is entered, the list of qualifying apps changes to match the search criteria. Search results are listed alphabetically within each risk level.
  - c) Select the app or apps you wish to add to the allowed list by marking the check box next to the app name.

Apps that have been included on the **Block Access** list cannot be selected. They must first be removed from that list.

Click **Done** when you have finished making your selections. Each selected cloud app is added to the permitted list.

**Important**

The **Allow Access** list takes precedence over the **Block all high risk level applications** option. Access to a high risk app that is on the permitted list is allowed even if **Block all high risk level applications** is enabled.

- d) Remove an app from the list by removing the check mark.

The number of selected apps included in each risk level is provided next to the risk level name. Cloud apps in the list are sorted alphabetically within each risk level.
- 6) Click **Save**.

**Important**

Block actions assigned on the Web Categories tab take precedence over the **Allow Access** list. If a permitted cloud app is requested using a URL categorized in a category that is set to block, access to it is blocked.

A count of the number of selected apps is provided above each selection pane. Each list is limited to 100 selections. When the limit is reached, search results no longer allow selection of additional apps. An app that was previously selected must first be removed from the list.

**Related concepts**

[Using the Cloud Apps tab with Protected Cloud Apps](#) on page 190

[Filtering action order](#) on page 201

## Using the Cloud Apps tab with Protected Cloud Apps

When the Protected Cloud App feature has been enabled (see *Configure protected cloud apps* for details), the selections made on the **Web > Settings > Protected Cloud Apps** page impact the **Block Access** and **Allow Access** selections.

- Protected cloud apps display on both lists and are indicated with a hash mark (#). To easily find them, use a hash mark at the beginning of the search string.
- Cloud apps selected on **Web > Settings > Protected Cloud Apps** as a protected app are automatically selected on the **Allow Access** list. They appear in search results on both lists, but cannot be selected or removed on either.  
Attempts by an end user to access these apps are forwarded to Forcepoint CASB for analysis and policy enforcement unless the app is in a blocked category (configured on the Web Categories tab).
- Cloud apps listed but not selected on **Web > Settings > Protected Cloud Apps** can be either allowed or blocked on the Cloud Apps tab. If an app is blocked and later selected on **Web > Settings > Protected Cloud Apps**, it is automatically moved to the Allow Access list and marked as selected.

### Related tasks

[Configure protected cloud apps on page 109](#)

## Custom Categories tab

Use the Custom Categories tab to view and add custom categories used for this policy only. Unlike the custom categories defined on the **Web > Policy Management > Custom Categories** page, which are available for use in all policies, the categories defined here can be applied only to the policy being edited.

Note that this tab is not available unless **Enable custom categories per policy** has been enabled on the **Web > Policy Management > Custom Categories** page.



### Note

There is a limit to the maximum number custom categories and sites you can add. The number of used and available category entries is displayed on the page.

Based on analysis of custom category usage, this limit is designed to provide ample capacity. If you have any questions about the custom category limit, please contact Technical Support.

To create custom categories for the policy:

### Steps

- 1) Click **Add**.
- 2) Assign a name to your new custom category and give it a description.
- 3) Click **Submit**.
- 4) Add hostnames, IP addresses, IP address ranges, or URL paths. For detailed guidance on how to enter sites, and how entries are interpreted, see *Adding sites to custom categories*. Note the following general guidance:
  - Ensure that hostnames are added only once.
  - Protocols (for example “http://”, “ftp://”) are ignored. Entries are matched to all protocols.
  - Standard ports for the protocol being used are ignored (for example, ports 80 for HTTP, and 443 for HTTPS).

5) Click **Add** again.

Use the buttons at the bottom of the page to **Download sites** to or **Upload sites** from a CSV file. A downloaded file can be edited and then uploaded for easy maintenance of the list of sites for the category.



#### Important

When a file is uploaded, the contents of the file will replace the list of sites previously associated with the category. It will not add to that list.

#### Related concepts

[Adding sites to custom categories](#) on page 192

## Adding sites to custom categories

When adding sites to a custom category, you can add hostnames, IP addresses or address ranges, or URL paths.



#### Note

Certain characters have significance to the pattern matching mechanism, and should be preceded with a backslash (\). These characters are: [ ] { } \ + \*

## Hostnames

Enter hostnames without a protocol, for example: `abc.com`. This will match:

- Any resource at the domain, using any protocol (for example <http://abc.com>, <https://abc.com>, <ftp://abc.com>).
- Any subdomains of `abc.com` using any protocol, for example [www.abc.com](http://www.abc.com), `123.abc.com`, [www.123.abc.com](http://www.123.abc.com).

You can use a wildcard (\*) within a hostname or at the beginning of a hostname. Wildcards at the beginning of a hostname match any hostname that ends with the string you enter, for example `*abc.com` matches `123abc.com`, and any subdomains (for example [www.123.abc.com](http://www.123.abc.com), [www.xxx.123abc.com](http://www.xxx.123abc.com)).

A wildcard at the beginning of a hostname, followed by a dot (`*.abc.com`) matches any subdomains of `abc.com` (for example `123.abc.com`), but **not** the `abc.com` domain itself.



#### Note

Wildcards placed at the **end** of the string are removed.

## URL paths

Any address with a slash (/) following the hostname or IP address is treated as a URL path (for example [www.abc.com/](http://www.abc.com/), [www.abc.com/mysite](http://www.abc.com/mysite)).

If you specify a URL path, it is treated as the start of a path, and matches anything beginning with the string you enter (for example, [www.abc.com/mysite](http://www.abc.com/mysite) matches [www.abc.com/mysite/folder/page.htm](http://www.abc.com/mysite/folder/page.htm)).

**Note:** URL paths will not match for HTTPS requests unless SSL decryption is being performed. For HTTPS requests, the full path is not provided to the proxy.



## IP addresses

---

Enter IPv4 IP addresses or ranges in one of the following formats:

- **Explicit address:** a single address. Example: 12.13.14.15
- **Explicit range:** 2 addresses separated by a dash (-). Example: 12.13.14.15- 12.13.14.99 (a space before and after the dash is allowed, but not required)
- **Subnet:** An address followed by a slash (/) and the number of bits, which is a number between 1 and 32. Example: 12.13.14.15/24
- **Subnet with subnet mask:** an address followed by a slash (/) and a netmask. Example: 12.13.14.15/255.255.255.0

IP addresses and ranges are used to match the resolved address of a requested hostname, using any protocol and port.

## Ports

---

If you include a port number that is the standard port number for the protocol being used (for example port 80 for HTTP, port 443 for HTTPS), the port number is ignored and the entry is treated as described above. If the port number is a non-standard port for the protocol being used, the proxy will match only URLs that include the port number.

For example, if you enter `www.abc.com:8080/`, then `http://www.abc.com:8080/mysite` will match, but `http://www.abc.com/mysite` will not.

# Web Categories tab

---

The cloud service includes dozens of website categories (see *Category list* for more details). These categories are designed to help you apply policy to your organization's Web surfing. If a website has not previously been categorized, we assign it the "Unknown" category.



### Note

---

Websites can exist in one standard category, but multiple custom categories.

Click the **Web Categories** tab to configure:

- Whether to use SSL decryption. See *Enabling SSL decryption*. Depending on your account, this may allow:
  - HTTPS traffic to be inspected to ensure the correct notification or authentication page is delivered to the end user
  - HTTPS traffic in categories that you specify to be analyzed for malware and other threats
- The action you want the cloud service to take when users try to access websites in each of the categories. See *Managing categories, actions, and SSL decryption*. If available for your account, when applying actions, you can also specify whether or not to use SSL decryption to analyze specific web categories.
- If SSL decryption is enabled, a list of host names for which SSL decryption is not performed. See *Bypassing SSL decryption for specific sites*.

**Related concepts**[Category list on page 203](#)**Related tasks**[Enabling SSL decryption on page 194](#)[Managing categories, actions, and SSL decryption on page 195](#)[Bypassing SSL decryption for specific sites on page 199](#)

## Enabling SSL decryption

SSL (Secure Sockets Layer) is the industry standard for transmitting secure data over the Internet. It is based on a system of trusted certificates issued by certificate authorities and recognized by servers.

When you enable SSL decryption for your end users, SSL-encrypted traffic is decrypted, inspected, and then re-encrypted before it is sent to its destination. This enables the cloud proxy to serve the correct notification page to the user. For example, a block page if the SSL site is in a category that the end user is prevented from accessing, or the *Pre-logon welcome page* for authentication.

**Note**

Encrypted client hello is not supported when decrypting traffic.

To implement SSL decryption for your end users, you need a root certificate on each client machine that acts as a Certificate Authority for SSL requests to the cloud proxy.

To install the root certificate for your end users and enable notification pages for SSL sites:

### Steps

- 1) On the Web Categories tab, click the **root certificate** link and download the certificate to a location on your network. You can then deploy the certificate manually, using your preferred distribution method.
- 2) Once the certificate has been deployed, return to this page and toggle the **SSL decryption** switch to **ON**.
- 3) Click **Save**.

**Note**

You should also define a certificate when you add an appliance and install that certificate on users' machines, in order to avoid browser warnings regarding SSL termination block, authentication, or quota/confirm operations. See *Generating device certificates*.

**Related concepts**[Pre-logon welcome page on page 174](#)**Related tasks**[Generating device certificates on page 144](#)

# Managing categories, actions, and SSL decryption

The category list on the Web Categories tab includes the **standard categories** provided with your subscription, and any **custom categories** that you have defined on the **Custom Categories** tab for this policy (shown as Policy Custom Categories) or on the **Policy Management > Custom Categories** page (shown as Account Custom Categories).

- **Actions** (described in *Policy enforcement actions*) are applied to either standard or custom categories to determine whether and how end users are allowed to access websites in the category.
- When SSL decryption is available and enabled, **decryption** may be applied to standard categories only.
  - This option is available for Forcepoint Web Security Cloud only.
  - Decryption is disabled for all categories by default.
  - If you enable one or more categories for decryption, you must also enable at least one of the analysis options on the *Web Content & Security* tab since these options define the types of security analysis that takes place. If you do not enable any of these options on the Web Content & Security tab, the categories you select are decrypted to enable correct notification pages, but not analyzed.



## Note

If you enable *Analysis exceptions* on the Web Content & Security tab and a site defined as an exception is also in a category selected for SSL decryption, the exception defines whether or not the HTTPS version of the site is analyzed. For example, if “google.com” is set to **Never Analyze** and the Search Engines and Portals category is selected for SSL analysis, <https://www.google.com> would be decrypted but not analyzed.

In the Standard Categories section, child categories are indented under their parent categories. Expand the parent category to see its child categories.

Parent categories allow specific categories to be grouped by a more generic description—for example, **Internet Communication** is the parent category for **General Email**, **Organizational Email**, **Text and Media Messaging**, and **Web Chat**. However, there is no hierarchical relationship between parent categories and the child categories within them: you can set a filtering action for a parent category without it affecting the child category, and vice versa.

**Privacy categories** are marked with a padlock icon. This predefined group includes the following categories that may be subject to regulatory requirements:

- Financial Data and Services
- Prescribed Medications
- Education
- Government
- Health

Websites in these categories may include personal identification information that should not be decrypted, and you may want to avoid specifying these sites for decryption.

To edit the action applied to a category, or the SSL decryption behavior for a category:

## Steps

- 1) Select a web category from the category list.  
You can select a category directly from the list, or enter text in the search box to locate the category you want.  
To select multiple categories, use the **Shift** and/or **Ctrl** keys. You can also use the drop-down menu above the category list to select Web 2.0 categories or privacy categories, or to select or deselect all categories.
- 2) Select an **Action** for the category. See *Policy enforcement actions*.
- 3) If SSL decryption is enabled, select whether or not to decrypt sites in the category.
- 4) If you have made changes to one or more parent categories, optionally click **Apply to Subcategories** to use the same settings for both parent and child categories.
- 5) Click **Save**.  
If you have selected the Decrypt option for a privacy category, a warning message appears.



### Important

The **Block Access** list configured on the Cloud Apps tab (see *Cloud Apps tab*) takes precedence over actions assigned on the Web Categories tab. If a blocked cloud app is requested using a URL categorized in a category that is set to allow, access to it is blocked.

### Related concepts

[Policy enforcement actions](#) on page 196  
[Web Content & Security tab](#) on page 217  
[Analysis exceptions](#) on page 220

### Related tasks

[Cloud Apps tab](#) on page 188

# Policy enforcement actions

Each category has an **action** assigned to it. This is the action that the cloud service takes in response to a user's Internet request. The action applies to all users of this policy unless exceptions are configured.

The available actions are:

## Allow access

Allow access means that any website within the category is always accessible, regardless of whether it exists in another category that has the **Block access** action.

## Do not block

---

If you do not want websites to be blocked, select **Do not block**. This ensures that the site is not blocked under this rule, but if it also exists in another category that has an action of **Block access**, it is blocked under that category.

## Require user authentication

---

This action allows you to monitor who is accessing sites in this category. If you are forcing users to be identified or authenticate themselves, it has the same impact as **Do not block**. If the users are not already identified or authenticated, they are forced to do so to access the site. If the site also exists in a category that has the action **Allow access** the users are not forced to identify or authenticate themselves.

## Confirm

---

Users receive a block page, asking them to confirm that the site is being accessed for business purposes. Clicking **Continue** enables the user to view the site.

Clicking **Continue** starts a timer. During the time period that you configure (10 minutes by default), the user can visit other sites in the confirmed category without receiving another block page. Once the time period ends, browsing to any other **Confirm** site results in another block page.

The default time can be changed on the **General** tab for the policy.

## Use Quota

---

Users receive a block page, asking them whether to use quota time to view the site. If a user clicks **Use Quota Time**, he can view the site.

Clicking **Use Quota Time** starts two timers: a quota session timer and a total quota allocation timer.

- If the user requests additional quota sites during a default **session** period (10 minutes by default), he can visit those sites without receiving another block page. If you are using per-category quotas, the user can visit only other sites in the same category without receiving another block page.
- **Total** quota time is allocated on a daily basis. Once it is used up, each user must wait until the next day to access sites in quota categories. The default daily quota allocation is set on the **General** tab for the policy. If you are using per-category quotas, the total quota time applies to each category and once it is used up for a particular category, a user can still use quota time in another category, if available.

The session length and total quota time available for each category depend on the options selected on the **General** tab. If you have defined per-category quotas, you can select **Use Quota** for a category on the **Web Categories** tab to change the total quota time and session length available to users in the policy for that category.

See *Using quota time to limit Internet access* for more information.

## Block access

---

This blocks access to websites in this category unless they exist in another category with that is assigned the **Allow access** action. If the website exists in another category with the action **Do not block**, it is blocked under this category. When a site is blocked, you can choose a notification page to be displayed.

Note that the block page that allows a user to **View in Remote Browser** is available for selection only if the remote browser isolation feature is enabled. See *Configure Remote Browser Isolation* for details.

**Related concepts**

[Using quota time to limit Internet access](#) on page 198

**Related tasks**

[Configure Remote Browser Isolation](#) on page 76

## Using quota time to limit Internet access

When a user clicks Use Quota Time, she can view sites in any quota category until the quota session ends. The default quota session time (configured via the **General** tab of the policy) is 10 minutes.

Once the quota session ends, a request for a quota site results in another quota block message. Users who have not depleted their daily quota allocation can start a new quota session.

Internet applets, such as Java or Flash applets, may not respond as expected to quota time restrictions. Even if it is accessed from a quota-restricted site, an applet that runs within the browser can continue running beyond the configured quota session time.

This is because such applets are downloaded completely to a client machine and run just like applications, without communicating back to the original host server. If the user clicks the browser's Refresh button, however, the cloud service detects the communication to the host server, and then blocks the request according to applicable quota restrictions.

## YouTube Restricted mode

The YouTube category, which appears under Bandwidth on the Web Categories tab, includes the option to enable YouTube Restricted mode.

This service allows you to limit access to the content available on YouTube, and is designed for use by schools, libraries and other institutions. The content that appears in Restricted mode is controlled by YouTube, and excludes material that contains potentially mature content. Videos may be flagged as restricted if mature content is detected by an automated system, or if a YouTube employee has set an age restriction to a video.

To enable the feature, select **Filter using YouTube Restricted mode**. Then select the filtering level, either **Strict** or **Moderate**.

This feature is active for end users only if the YouTube web category is not blocked. If you choose to block the category by default but configure exceptions for specific users or groups (see *Exceptions*), those users and groups can access the YouTube content that is available in Restricted mode.

**Note**

YouTube Restricted mode replaces the YouTube for Schools feature, which has been withdrawn by YouTube.

**Related concepts**

[Exceptions](#) on page 199

# Bypassing SSL decryption for specific sites

The SSL Decryption Bypass option enables you to define specific websites that are not subject to decryption as they flow through the proxy. Some websites may include personal identification information that should not be decrypted. In order to avoid liability for inspecting this type of information, you may want to specify some or all of these sites for decryption bypass. The selected sites will not be decrypted even if the category or categories that the sites belong to are selected for SSL analysis.

End users can determine that the website they are viewing is not decrypted by checking who has issued the certificate for that site. If the certificate was issued by Websense, Inc., or Forcepoint LLC, traffic to the site has been decrypted.



## Note

End user single sign-on uses SSL decryption to handle encrypted traffic and redirect SSL sites for authentication. If you have enabled single sign-on in a policy, you can maintain a list of hostnames for which SSL decryption is not performed on the Web Categories tab.

An end user accessing one of the specified hostnames using HTTPS will not be able to use single sign-on. End users can still access these sites using HTTP and authenticate successfully.

To set up the bypass of SSL decryption for certain sites:

## Steps

- 1) Under **SSL Decryption Bypass** on the Web Categories tab, enter a site's hostname in the entry field.
  - You can enter multiple hostnames, each on a separate line.
  - You can use the asterisk wildcard in a hostname, for example \*.google.com.
  - To edit or delete an existing site, select the name in the entry field and make your change.
- 2) Click **Save**.

# Exceptions

Exceptions allow the default action for a category to be overridden for specified users, groups, and roaming users, and for defined time periods.

Note that **Require user authentication** is not available for category exceptions, because for an exception to be applied, the cloud service must be aware of the users - they must already be authenticated. If a user has not been authenticated, but wants to access a category that has an exception for a user or a group, the cloud service automatically asks the user to authenticate.



## Note

If you set up an Allow exception, note that this overrides only the Block action on URL categories. It does not bypass any other actions, including user authentication and antivirus analysis.

When you select a category, the Category Exceptions section at the bottom of the page shows the number of exceptions applied to that category. If no category is selected, the list shows all category exceptions that have been defined.

On occasion you may want to add users to exceptions for policies they are not yet using or leave users in an exception list for a policy they no longer use. This allows you to set rules for users before they are moved

between policies—for example, when policy assignment has been changed in an LDAP directory. If you add an unknown user or if the user belongs to another policy, you receive a message to this effect. You can save rules that include users in other policies as well. These users are shown in the exception list with a red asterisk.

The exceptions table provides the following summary information about each rule:

- The name assigned to the rule.
- The category or categories to which the rule applies. If there are multiple categories in the exception, click the link to see the category list.
- The users and groups to which the rule applies. If none are shown, it applies to all users of the policy.
- The time period to which the rule applies.
- The action for the rule, and whether it applies only to roaming users.
- The state of the exception rule - on or off. You can change the rule's state in this table by clicking the State switch.

## To create an exception rule

---

### Steps

- 1) On the Web Categories tab, click a category name.
- 2) Click **Add exception**.
- 3) The rule **State** is set to ON by default, meaning the rule will be enabled for the users and groups you select. If you want to set up a rule but not enable it immediately, click the State switch to set it to OFF.
- 4) Enter a **Name** and **Description** for the rule.
- 5) Select the **Action** to apply from the drop-down list.
  - For the **Confirm** action, enter the time period for which a user who clicks Continue can access sites in the selected category or categories.
  - For **Use Quota**, any further options depend on the quota time configured on the policy's **General** tab. If the policy has an overall daily quota set, that quota applies to the exception and cannot be changed. If the policy is using the per-category daily quota, enter the total quota time and session length available to users and groups in the rule.
- 6) Select the **Time period** during which the rule is active.
- 7) For an exception that should be applicable to roaming users only, mark **Apply only when user is roaming**.
- 8) Select the category or categories to which the rule applies. To select multiple categories, use the **Shift** and/or **Ctrl** keys.
- 9) Enter or select the users and groups that will use the rule. You can also specify that the rule applies to all users and groups in the policy except the group you select.
- 10) Click **Submit**.



# Auto tunneling of WebSocket Traffic

For web applications using WebSockets for communication, the **Tunnel WebSocket Traffic** option makes it possible to automatically tunnel WebSocket traffic, significantly reducing the need to add SSL decryption bypasses when SSL Inspection is enabled.



## Note

Auto-tunneling applies only to the Web Socket traffic for that web application. Regular HTTP/S traffic for that web application will still be subject to inspection.

Using this option, cloud web administrators can enable or disable WebSocket auto-tunneling at the individual policy level allowing for phased roll-out.

To enable or disable the auto tunneling of web socket traffic:

## Steps

- 1) Navigate to **Web > Policies > policy name > Web Categories > Tunnel WebSocket Traffic**.
- 2) Set the **Automatically tunnel all WebSocket traffic for this policy** option to ON or OFF.



## Note

The default value is OFF.

SSL Inspection bypasses may still be needed:

- a) If the application is using pinned certificates
- b) If the application's best practice recommendation is to bypass SSL inspection generally
- c) If inspection of the application's regular HTTPS traffic causes the application to be blocked due to policy settings that you do not wish to apply

# Filtering action order

When a user requests access to a site, the cloud service determines whether to block or permit access based on the details in the policy associated with the user. See *Creating a new policy* for information.

By default, the cloud service applies the appropriate policy enforcement action to a user request using these steps. If, at any step, the appropriate action is to block the request, the user receives the appropriate block page.

- 1) Security category
- 2) Application control, File extension, File type, File Size
- 3) Cloud Apps
- 4) Standard or custom web categories:
  - a) Allow access

- b) Require user authentication
- c) Confirm
- d) Quota
- e) Block
- f) Do not block

If the **Always allow access to cloud apps on the Allow Access list** option is selected on the Cloud Apps tab of the policy, then requests to any cloud app listed on the Allow Access list are allowed, regardless of the action assigned to the associated web category or its security status. Requests to the apps listed on the Protected Cloud Apps list are always forwarded to CASB for further enforcement.



#### Note

If you do not see the **Always allow access to cloud apps on the Allow Access list** option on the Cloud Apps tab, contact Technical Support.

When this option is enabled, the cloud service applies the appropriate policy enforcement action to requests using these steps.

- 1) File extension, File type, File Size
- 2) Cloud apps (This includes protected cloud apps. Requests to those apps are forwarded to Forcepoint CASB for enforcement.)
- 3) Security category
- 4) Application control
- 5) Standard or custom web categories
  - a) Allow
  - b) Require user authentication
  - c) Confirm
  - d) Quota
  - e) Block
  - f) Do not block

When a category exception specifies a time period, several factors affect whether the exception is applied:

- If the time period includes a timezone, the timezone is used.
- If a time period does not include a timezone, but the user request originates from a proxied connection that has an associated timezone, the connection's timezone is used.

- If the time period does not include a timezone, and the user is either roaming or at a proxied connection that has no timezone, the policy timezone is used.
- If no timezone is available for a time period, any exceptions based on that time period are ineffective.

Given the considerations above, when a per-time, per-user, or per-group exception also exists, it applies actions in this order:

- users with a time period defined
- users with no time period defined
- groups with a time period defined
- groups with no time period defined
- default with a time period defined
- default without a time period defined

In other words, rules with a usable time period defined take precedence over equivalent rules with no time period. Within each of these, the cloud service uses the same order as the default.

### Related tasks

[Creating a new policy](#) on page 160

## Category list

The cloud service uses the Forcepoint URL Database, which organizes similar websites (identified by URLs and IP addresses) into **categories**. Each category has a descriptive name, like Adult Material, Gambling, or Peer-to-Peer File Sharing.

The categories include the following:

- **Advanced Malware Command and Control** focuses on outbound network transmissions from a compromised machine to a malicious command and control center
- **Advanced Malware Payloads** focuses on inbound network transmissions of payloads intended to exploit a machine
- **Mobile Malware** focuses on malicious websites and applications that are designed to run on mobile devices
- **Unauthorized Mobile Marketplaces** focuses on websites that potentially distribute applications that are unauthorized by the mobile operating system manufacturer, the handheld device manufacturer, or the network provider. (Traffic to websites in this category may be a sign of a jailbroken or rooted device.)

You can also create your own, custom categories or import a custom category file (in CSV format) to group sites of particular interest to your organization (see *Configure custom categories*). Together, the Forcepoint URL Database categories and user-defined categories form the basis for Internet filtering.



### Note

Categories are designed to create useful groupings of the sites of concern to subscribing customers. They are not intended to characterize any site or group of sites or the persons or interests who publish them, and they should not be construed as such. Likewise, the labels attached to categories are convenient shorthand and are not intended to convey, nor should they be construed as conveying, any opinion or attitude, approving or otherwise, toward the subject matter or the sites so classified.

Go to the **Web > Settings > Forcepoint URL URL Database Categories** link in the cloud portal to see an up-to-date list of Forcepoint URL Database categories.

To suggest that a site be added to the Forcepoint URL Database, use the Forcepoint Site Lookup Tool. To access the tool:

- 1) Log in to your support account at <https://support.forcepoint.com/Login>.
- 2) From the Tools & Links menu, click **Site Lookup Tool**.

#### Related concepts

Configure custom categories on page 112

## Protocols tab

Click the **Protocols** tab to manage how protocols, or non-HTTP Internet traffic, are handled by a policy.



#### Important

This feature requires an I Series appliance.

The list of protocols appears in a 2-level tree display similar to that in the Categories tab. Protocol groups can be expanded to show the individual protocols within each group.

The list on the Protocols tab includes both standard protocols and any custom protocols that you have defined on the **Policy Management > Protocols** page. The standard protocol groups are updated regularly.

Configure how a protocol is filtered by selecting it in the protocols tree and specifying an action (**Allow** or **Block**) from the box on the right. You can select a protocol directly from the list, or enter text in the search box to locate the protocol you want.

Use the **Shift** and/or **Ctrl** keys to select multiple protocols.

## Protocol exceptions

Protocol exceptions allow the default action for a protocol to be overridden for specified users and groups of users. The number of exceptions to the default filtering action is shown at the bottom of the Protocols tab. Click a protocol to view exception rules that may apply to it.

The exceptions table provides the following information about each rule:

- The name assigned to the rule
- The protocol or protocols to which the rule applies.
- The users and groups to which the rule applies. If none are shown, the rule applies to all users of the policy.
- The action for the rule (**Allow** or **Block**)
- The status of the exception rule (**Active** or **Inactive**)

To create an exception rule:

### Steps

- 1) Click **Add Exception**.

- 2) On the Add Exception page, enter a **Name** (1 - 512 alphanumeric characters) and **Description** (1 - 1024 characters) for the rule.
- 3) Select the **Action** to apply from the drop-down list near the top of the page.
- 4) Mark the **Status > Active** button to enable the rule for the users and groups you have selected. To stop using the exception without deleting it, select **Inactive** status.
- 5) Select the protocol or protocols to which the rule applies. To select multiple protocols, use the **Shift** and/or **Ctrl** keys. Use the arrow key to move a selection to the **Selected protocols** list.
- 6) Enter or select the users and groups for the rule:
  - Enter individual email addresses and use the arrow key to move the addresses to the **Selected users** list. Separate multiple addresses with a comma.
  - Select the user groups to which the rule applies and use the arrow key to move the groups to the **Selected groups** list.You can also specify that the rule applies to all users and groups in the policy except the group you select.
- 7) Click **Save**.

To edit an existing exception, click the name link in the Protocol Exceptions list. The Edit Exception page appears showing the current settings for that rule.

To delete an exception, mark the check box to the left of the name and click **Delete**.

## Application Control tab

---

Click the **Application Control** tab in the policy to configure social web controls for your end users. This tab is available for Forcepoint Web Security Cloud only.

To use the options on the Application Control tab, you must enable Real-time Security Classification on the Web Content & Security tab. See the *Web Content & Security tab*.

Social web controls enable you to safely fine-tune access to popular sites within social media such as Facebook, Twitter, and YouTube. For each available site, you can specify whether users can access particular functions within the site, such as posting a comment or joining a group. For example, you may want to allow users to access their Facebook page, but not to upload photos or videos to the site.

The following filtering actions are available for social web controls:

- **Do not block**. This ensures that the function is not blocked, unless the category to which the parent site belongs has the action **Block access**. If you select Do not block for a function and the parent site is blocked on the Web Categories tab, a popup warning appears when you save your changes.
- **Block access**. This blocks the function and depending on the nature of the function, either displays the block page that you select, stops the function from working, or displays an error message.

The functions specific to each site are grouped together. If you set a particular filtering action for the parent application (for example, Twitter), it is also applied to all child functions for that application. You can subsequently change the action for individual functions.

Top-level sites related to the social web controls remain classified and filtered under their existing categories on the *Web Categories tab*. For example, Facebook Chat is classified as Web Chat. You can only apply social web controls to a site if its corresponding web or custom category allows access or does not block the site.

If the top-level site is part of a category that has quota time applied to it, application controls are applied according to your configuration when the user is in a quota period. Similarly, if the site is in a category has the Confirm action applied to it, application controls are applied according to your configuration once the user has clicked Continue.

### Related concepts

[Web Content & Security tab](#) on page 217

[Web Categories tab](#) on page 193

## To configure application controls

### Steps

- 1) Select an application from the Applications list.  
You can select an application directly from the list, or enter text in the search box to locate the application you want.  
To select multiple applications, use the **Shift** and/or **Ctrl** keys. You can also use the drop-down menu above the Applications list to select or deselect all applications.
- 2) Select an **Action** for the category. Note that if you have selected a parent application (for example Facebook or Twitter), the action you select also applies to all the controls within that application by default.
- 3) If you have selected Block access, select a block page to display.
- 4) Click **Save**.

## Application control exceptions

Exceptions allow the configured action for an application control to be overridden for specified users, groups of users, and roaming users.

On the Application Control tab, the exceptions to the default configuration are listed at the bottom of the page. Click an application to view exception rules that may apply.

On occasion you may want to add users to exceptions for policies they are not yet using or leave users in an exception list for a policy they no longer use. This allows you to set rules for users before they are moved between policies—for example, when policy assignment has been changed in an LDAP directory. If you add an unknown user or if the user belongs to another policy, you receive a message to this effect. You can save rules that include users in other policies as well. These users are shown in the exception list with a red asterisk.

The exceptions table provides the following summary information about each rule:

- The name assigned to the rule.
- The application to which the rule applies. It always applies to the application you are viewing, but this indicates whether it applies to other applications. If there are multiple applications in the exception, click the link to see the application list. Note that if this is the case, the exception is also listed when you select the other application(s).
- The users and groups to which the rule applies. If none are shown, it applies to all users of the policy.

- The action for the rule, and whether it applies only to roaming users.
- The state of the exception rule - on or off. You can change the rule's state in this table by clicking the State switch.

## To create an exception rule

---

### Steps

- 1) On the Application Control tab, click a web application.
- 2) Click **Add exception**.
- 3) The rule **State** is set to ON by default, meaning the rule will be enabled for the users and groups you select. If you want to set up a rule but not enable it immediately, click the State switch to set it to OFF.
- 4) Enter a **Name** and **Description** for the rule.
- 5) Select the **Action** to apply from the drop-down list.
- 6) For an exception that should be applicable to roaming users only, mark **Apply only when user is roaming**.
- 7) Select the application to which the rule applies. To select multiple applications, use the **Shift** and/or **Ctrl** keys.
- 8) Enter or select the users and groups that will use the rule. You can also specify that the rule applies to all users and groups in the policy except the group you select.
- 9) Click **Submit**.

## File Blocking tab

---

Click the **File Blocking** tab in the policy to configure file download blocking for categories that users are allowed to access according to your settings in the Web Categories tab. This capability allows your organization to restrict access to particular files from websites in some or all permitted categories, based on true file type, file extension, or size. For example, you could permit the category Sports, but block multimedia (audio and video) files from sites in the Sports category.

Under **Advanced Options**, you can block the upload of executable files, or define file download size limits, or size limits per category.

The following file blocking options are available:

- **True file type blocking:** True file types are detected during security analysis. Several predefined groups of file types (for example, common image files) are included on the File Blocking tab for ease of selection. For example:
  - 1) The General Email category has the Allow access action, but file type blocking is enabled for multimedia files in the category.

- 2) An end user attempts to download a file with a known extension (for example, “movie.mpeg”) or unknown extension (for example, “myfile.111”).
- 3) If analysis determines that the file is classified as multimedia, the user receives a block page indicating that the download was blocked.
- 4) If analysis determines that the file is not a multimedia file, the download request is permitted as long as the file is not categorized as another blocked file type.

For more details, see *Blocking by file type*.

- **File extension blocking:** This blocks files based solely on file extensions that you specify. For example:

- 1) The General Email category has the Allow access action, but the file extensions “.zip” and “.rar” are blocked for the category.
- 2) An end user attempts to download a file with a file with a .zip extension (for example, “myfile.zip”).
- 3) The user receives a block page indicating that the download was blocked by file extension, because the “.zip” file extension is specifically blocked for this category.

For more details, see *Blocking by file extension*.



#### Important

Archived/compressed files are not extracted to determine if the contents contain a file that should be blocked based on the type or extension. However, they are inspected for malware. Archived and compressed files can be blocked, if needed, in which case, all files contained in those archived files are blocked.

- **Executable file upload blocking:** This blocks the upload of any file identified as an executable. For more details, see *Blocking executable file uploads*.
- **File size blocking:** This blocks files based on the maximum size that you specify. You can block all files based on the following:
  - The file type and size.
  - The file type and size in a specific category or categories.
  - The file extension and size.
  - The file extension and size in a specific category or categories.
  - File size alone.
  - File size and category. See *Block file downloads based on size, or size and category*.

#### Related concepts

[Blocking executable file uploads](#) on page 211

#### Related tasks

[Blocking by file type](#) on page 209

[Blocking by file extension](#) on page 210

[Block file downloads based on size, or size and category](#) on page 211



# Blocking by file type

---

Note that this option is available for Forcepoint Web Security Cloud only.

## Steps

- 1) On the File Blocking tab, click the file type that you want to configure for blocking.
- 2) On the File Block Details page, set the file blocking Rule State to **Enabled**.
- 3) To configure blocking by file size:
  - a) Under **Blocking Options**, select **Block all files over... KB**.
  - b) Define whether you want to block all files of this type over a particular size that you enter, or block files over a particular size for this type but only in specific categories. You also have the option to block files in specific categories without regard to size.
- 4) To block files in specific categories:
  - a) Select **Category specific blocking**.
  - b) Optionally, to block files by size, select **Block files in certain categories over... KB**, then fill in the size in kilobytes.  
Only files of the selected type that are over this size will be blocked in the categories you choose.
  - c) By default, the selected file type is blocked for all categories. To change this, use the category and action lists.  
You can select a category directly from the list, or enter text in the search box to locate the category you want. Click on the plus sign to the left of each category to view subcategories to which you can also apply blocking actions. If the parent and subcategory actions differ, an asterisk appears next to the parent category.  
  
To select multiple categories, use the **Shift** and/or **Ctrl** keys. You can also use the drop-down menu above the category list to select all Web 2.0 categories or privacy categories, or to select or deselect all categories.
- 5) Optionally, enter or select the users and groups to whom the file blocking applies. You can also specify that the file blocking applies to all users and groups in the policy except the group you select.
- 6) Select the block page that will be displayed when this file type is detected and blocked. Block pages are not displayed for image files; instead images are replaced by a 1x1 pixel transparent image.
- 7) Click **Save**.



### Important

Archived/compressed files are inspected for malware but are not extracted to determine if the contents contain a file that should be blocked based on file type. Archived and compressed files can be blocked, if needed, and access to all files contained in those archived files is blocked.

# Blocking by file extension

## Steps

- 1) On the File Blocking tab, click **Add Extensions**.
- 2) Enter the extension you wish to block. You can enter groups of extensions, separated by commas.



### Note

If you include the period in the extension (for example, .jpg) it will be removed. Wildcards are not supported.

- 3) Set the file blocking **Rule State** to **Enabled**.
- 4) To configure blocking by file size:
  - a) Under **Blocking Options**, select **Block all files over... KB**.
  - b) Define whether you want to block all files with this extension over a particular size that you enter or block files with this extension over a particular size but only in specific categories. You also have the option to block files in specific categories without regard to size.
- 5) To block files in specific categories:
  - a) Select **Category specific blocking**.
  - b) Optionally, to block files by size, select **Block files in certain categories over... KB**, then fill in the size in kilobytes.

Only files of the selected type that are over this size will be blocked in the categories you choose.



### Note

Blocking by file size is not available for web traffic that has been handled by an appliance.

- c) By default, files with the selected extensions are blocked for all categories. To change this, use the category and action lists.

You can select a category directly from the list, or enter text in the search box to locate the category you want. Click on the plus sign to the left of each category to view subcategories to which you can also apply blocking actions. If the parent and subcategory actions differ, an asterisk appears next to the parent category.

To select multiple categories, use the **Shift** and/or **Ctrl** keys. You can also use the drop-down menu above the category list to select all Web 2.0 categories or privacy categories, or to select or deselect all categories.
- 6) Optionally, enter or select the users and groups to whom the file blocking applies. You can also specify that the file blocking applies to all users and groups in the policy except the group you select.
  - 7) Select the block page that will be displayed when this file extension is detected and blocked.

- 8) Click **Save**.



#### Important

Archived/compressed files are inspected for malware but are not extracted to determine if the contents contain a file that should be blocked based on file extension. Archived and compressed files can be blocked, if needed, and access to all files contained in those archived files is blocked.

## Advanced options

---

Click **Advanced Options** to:

- Block the upload of all executable files
- Block the download of all files based on size, or size and category.

## Blocking executable file uploads

---

To block the upload of executable files, click **Advanced Options**. Under Executable File Uploads, select **Block executable file uploads**. This setting blocks the upload of all executable files across your organization.

You can enable analysis of inbound executables on the Web Content & Security tab. See *Configuring file analysis*. To block the download of executable files, see *Blocking by file type*.



#### Important

Executable files included in archived/compressed files are not blocked. Archived/ compressed files are inspected for malware but are not extracted to determine if the contents contain an executable file that should be blocked. Archived and compressed files can be blocked, if needed, to avoid uploading an unwanted executable file.

#### Related concepts

[Configuring file analysis](#) on page 219

#### Related tasks

[Blocking by file type](#) on page 209

## Block file downloads based on size, or size and category

---

To limit the download of all files based on file size, or size and category, click **Advanced Options**. Then:

### Steps

- 1) Under File Size Limits, set the file blocking Rule State to **Enabled**.

- 2) To configure blocking by file size for all categories:
  - a) Under **Blocking Options**, select **Block all files over... KB**.
  - b) Specify the size limit (1000 KB, by default).
- 3) To block files in specific categories:
  - a) Select **Category specific blocking**.
  - b) Fill in the size in kilobytes. Files over this size in the categories you choose will be blocked.

You can select a category directly from the list, or enter text in the search box to locate the category you want. Click on the plus sign to the left of each category to view subcategories to which you can also apply blocking actions.

To select multiple categories, use the **Shift** and/or **Ctrl** keys. You can also use the drop-down menu above the category list to select Web 2.0 categories or privacy categories, or to select or deselect all categories.

- 4) Optionally, enter or select the users and groups to whom the file blocking applies. You can also specify that the file blocking applies to all users and groups in the policy except the group you select.
- 5) Select the block page that will be displayed when this file size is detected and blocked.  
When you are finished making changes, click **Save**.

## Data Protection tab

Click the **Data Protection** tab in the policy to configure options for handling potential data issues using Data Protection Service (DPS).

This tab is available when adding a policy if **Use Data Protection Service** is selected on the **Web > Settings > Data Protection Settings** page.



### Note

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

To enable this tab for an existing policy, navigate to **Web > Settings > Data Protection Settings** and use the table at the bottom to reset the data security selection for the policy. See *Data Protection Settings* for details.

When Data Protection Service is enabled, the cloud proxy sends user requests that may include sensitive data or files being posted to HTTP, HTTPS, and FTP sites to Data Protection Service 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. Such requests are then blocked or allowed based on information provided to the cloud service by DPS, using the policies defined in the on-premises Forcepoint DLP product.



### Important

Data Protection is not compatible with the I Series appliance.

On the Data Protection tab:

- 1) When you are ready for DPS to be used for data security, toggle the **Enable Data Protection Service** to **ON**. Until that switch has been turned on and the change saved, data security is not monitored for the policy.
- 2) The default selections for **DPS timeout** value and **DPS fallback behavior** are based on the same options on the **Web > Settings > Data Protection Settings** page. Edit them as necessary for this policy. See *Data Protection Settings* for more information.
- 3) Click **Save**.



#### Important

The same user information must exist in both Forcepoint Web Security Cloud and Forcepoint DLP in order for user requests to be accurately inspected by Forcepoint DLP.

Users blocked for data security incidents receive a special block page. The block page can be configured by doing one of the following:

- Click the **Data Protection block page** link at the top of the Data Protection tab in a policy.
- Go to the **Web > Policy Management > Block & Notification Pages** page, expand the **General** section, and then select **Data Protection**.



#### Note

Requests that include files that exceed 10Mb in size are not forwarded to Data Protection Service. These requests are allowed and no log record is generated.

#### Related tasks

[Data Protection Settings](#) on page 48

## Data Security tab (DLP Lite)

Click the **Data Security** tab in the policy to configure options for blocking or monitoring data loss over web channels.

This tab is available when adding a policy if **Use DLP Lite** is selected on the **Web > Settings > Data Protection Settings** page or if the Data Protection Service is not licensed.

To enable this tab for an existing policy, navigate to **Web > Settings > Data Protection Settings** and use the table at the bottom to reset the data security selection for the policy. See *Data Protection Settings* for details.



#### Important

Data security features are not compatible with the I Series appliance.

When data security features are enabled, the cloud service searches for sensitive data or files being posted to HTTP, HTTPS, and FTP sites, and reports on any incidents that it discovers. 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. You can configure whether such incidents are blocked or just monitored.

To search for data over HTTPS, be sure SSL decryption is enabled by following the instructions provided in *Enabling SSL decryption*.

When blocking is enabled for data security incidents, users receive a special block page. To configure this block page, do one of the following:

- Click the **Data Security block page** link at the top of the Data Security tab in a policy.
- Go to the **Web > Policy Management > Block & Notification Pages** page, expand the **General** section, and then select **Data Security**.

### Related tasks

[Data Protection Settings](#) on page 48

[Enabling SSL decryption](#) on page 194

## Regulations

Most countries and certain industries have laws and regulations that protect customers, patients, or staff from the loss of personal information such as credit card numbers, social security numbers, and health information.

To set up rules for the regulations that pertain to you:

### Steps

- 1) Click **No region selected**. (To edit regions, click the link, “*n* regions selected.”)
- 2) Select the regions in which you operate. Forcepoint Security Labs provides a set of predefined policies to cover regions all over the world and maintains those policies as regulations change.
- 3) Select the regulations of interest.

Regulation	Description
Personally Identifiable Information (PII)	Detects Personally Identifiable Information—for example, names, birth dates, driver license numbers, and identification numbers. This option is tailored to specific countries.
Protected Health Information (PHI)	Detects Protected Health Information—for example, terms related to medical conditions and drugs—together with identifiable information.
Payment Card Industry (PCI DSS)	Conforms to the Payment Card Industry (PCI) Data Security Standard, a common industry standard that is accepted internationally by all major credit card issuers. The standard is enforced on companies that accept credit card payments, as well as other companies and organization that process, store, or transmit cardholder data.

- 4) Select an action to take when matching data is detected. Select **Block** to prevent the data from being sent through the web channel. Select **Monitor** to allow it. (Incidents are created either way.)

The Action column now appears in the Incident Manager by default, showing whether each incident was monitored or blocked.

- 5) Select a sensitivity to indicate how narrowly or widely to conduct the search.

Select **Wide** for the strictest security. Wide has a looser set of detection criteria than Default or Narrow, so false positives may result. Select **Narrow** for tighter detection criteria. This can result in false negatives or undetected matches. **Default** is a balance between the two.

Severity is automatically calculated for these regulations.

For more information on the detection rules for these regulations, see *Data Security Content Classifiers (DLP Lite only)*.

#### Related information

[Data Security Content Classifiers \(DLP Lite only\)](#) on page 301

## Data Theft

Use this section to detect when data is being leaked due to malware or malicious transactions. When you select these options, the cloud service searches for and reports on outbound passwords, encrypted files, network data, and other types of information that could be indicative of a malicious act.

To see if your organization is at risk for data theft:

### Steps

- 1) Select the types of data to look for.

Information Type	Description
Common password information	Searches for outbound passwords in plain text
Encrypted files - known format	Searches for outbound transactions comprising common encrypted file formats
Encrypted files - unknown format	Searches for outbound files that were encrypted using unknown encryption formats
IT asset information	Searches for suspicious outbound transactions, such as those containing information about the network, software license keys, and database files.
Suspected malware communication	Identifies traffic that is thought to be malware “phoning home” or attempting to steal information. Detection is based on the analysis of traffic patterns from known infected machines.
Password files	Searches for outbound password files, such as a SAM database and UNIX / Linux passwords files

- 2) Select an action to take when matching data is detected. Select **Block** to prevent the data from being sent through the web channel. Select **Monitor** to allow it. (Incidents are created either way.) You can filter by action in the Data Security Incident Manager.

- 3) Select a sensitivity to indicate how narrowly or widely to conduct the search.  
Select **Wide** for the strictest security. Wide has a looser set of detection criteria than Default or Narrow, so false positives may result and performance may be affected. Select **Narrow** for tighter detection criteria. This can result in false negatives or undetected matches. **Default** is a balance between the two.  
  
Some data theft classifiers cannot be changed from their default setting. Severity is automatically calculated for these types.

## Custom

---

Use this section if you want to detect intellectual property or sensitive data using custom phrases, dictionaries, or regular expressions containing business-specific terms or data.

- 1) Define new classifiers on the **Web > Policy Management > Content Classifiers** page. See *Configure Content Classifiers for Data Security (DLP Lite)* for instructions.
- 2) On the Data Security tab, select the classifiers that you want to enable for the policy. If none are listed, none have been created yet.
- 3) Select a severity for each classifier to indicate how severe a breach would be. Select **High** for the most severe breaches. Severity is used for reporting purposes. It allows you to easily locate High, Medium, or Low severity breaches when viewing reports.
- 4) Where applicable, configure a threshold for each classifier. To do so, click a link in the Threshold column, and then indicate how many times this classifier should be matched to trigger an incident. You can indicate a range if desired, such as between 3 and 10. By default, the threshold is 1.  
Also indicate if you want the system to count only unique matches when calculating the threshold or all matches, even duplicates. Example: your classifier has the key phrase “top secret” and a threshold of 5. If the key phrase is found 6 times in a single web post, the system would count that as one match if you select **Count only unique matches** or 6 matches if you select **Count all matches even duplicates**. In the first case, the threshold is not triggered. In the second case, it is.

### Related concepts

[Configure Content Classifiers for Data Security \(DLP Lite\)](#) on page 126

## Trusted Content

---

- 1) In **Trusted domains**, enter the domains you do not want to be monitored, one entry per line. For example:  
*forcepoint.com*  
*cnn.com*

The system does not analyze trusted domains. This means users can send them any type of sensitive information via HTTP, HTTPS, or other web channels from your network.

Duplicate domains are not permitted. Wildcards are supported.

You can add up to 100 trusted domains per policy. Each one can have up to 256 characters.



- 2) Click **Select Categories** to select website categories that do not require DLP analysis—for example, office collaboration sites.

## Web Content & Security tab

Use the **Web Content & Security** tab of the **Web > Policies** page for a selected policy to configure advanced analysis options, including exceptions. This tab is available for Forcepoint Web Security Cloud only.

## Advanced Classification Engine (ACE) analysis overview

ACE advanced analysis includes:

- **Real-Time Content Classification** returns a category for URLs that have not already been blocked by the active policy, and:
  - Are not in the Forcepoint URL Database, or
  - Are classified as a dynamic site

Content classification adapts to rapidly-changing web content, including user-generated content, such as that found on social-networking sites.

Optionally, you can select **Analyze links embedded in Web content** as part of content classification to provide more accurate categorization of certain types of content. For example, a page that otherwise has little or no undesirable content, but that links to sites known to have undesirable content, can be more accurately categorized. Link analysis is particularly good at finding malicious links embedded in hidden parts of a page, and in detecting pages returned by image servers that link thumbnails to undesirable sites.

- **Real-Time Security Classification** analyzes web pages in real time to discover security threats and malicious code in HTTP. You can enable advanced analysis for one of the following:
  - Sites with elevated risk profiles, as identified by Security Labs
  - Sites with elevated risk profiles and sites with lower risk profiles. Note that analyzing all inbound content is resource intensive and may result in slower web performance.



### Note

For an I Series appliance deployment, when performance optimization is selected the cloud service analyzes only sites with elevated risk profiles.

You must enable Real-Time Security Classification to use the options on the Application Controls tab. See *Application Control tab*.

- **Antivirus File Analysis - Inbound** analyzes files using traditional antivirus (AV) definitions to find virus-infected files that users are attempting to download.
- **Advanced Detection File Analysis - Inbound** analyzes files using advanced detection techniques to discover malicious content, such as viruses, Trojan horses, and worms, returning a threat category for policy enforcement.

You can configure the specific types of files to analyze under **File Type Analysis Options**. Note that executable file analysis is configured separately (see *Configuring file analysis*).

**Note**

If file analysis is configured to include multimedia files, when the streaming media is buffered and analyzed, the connection to the server may time out. In such cases, the best remedy is to create an analysis exception for that site. See *Analysis exceptions*.

- **Rich Internet Application Analysis** is applied to active content like Flash and Silverlight to detect and block malicious content.  
There are also two ACE outbound traffic analysis options that are enabled by default and cannot be turned off. This ensures that viruses and other malicious content cannot be sent from your network.
- **Antivirus and Advanced Detection File Analysis - Outbound** parallels the inbound file analysis applied by the Antivirus File Analysis and Advanced Detection File Analysis.
- **Bot and Spyware “phone home” Traffic Analysis** detects phone-home communication attempts from malware in your network and ensures that they are categorized and blocked.

The cloud service must analyze and block outbound malicious traffic in order to protect itself from being perceived as a malicious actor. Some origin servers blocklist client IP addresses if they detect malicious communications or hack attempts. If malicious communications were permitted to go through cloud proxies, the proxies would be in blocklist. This could mean that a single infected client could cause all clients browsing via the same cluster to be in blocklist.

This traffic is also logged, so you can run a report to obtain a list of the infected computers in your network.

**Related concepts**

[Application Control tab](#) on page 205

[Configuring file analysis](#) on page 219

[Analysis exceptions](#) on page 220

## Configuring ACE analysis settings

On the **Web Content & Security** tab for the selected policy:

### Steps

- 1) To enable content security, select **Real-Time Content Classification**.
- 2) Select **Analyze links embedded in Web content** to include embedded link analysis in content categorization. Requests that are blocked as a result of link analysis are logged and can be viewed in Analysis Activity reports.
- 3) To enable security analysis, select **Real-Time Security Classification**.
  - Select **Analyze content from sites with elevated risk profiles** to enable file analysis on files from uncategorized sites and files from sites with elevated risk profiles, as identified by Security Labs.
  - Select **Analyze content from sites with elevated risk profiles and from sites with lower risk profiles** to analyze inbound files. This option is resource intensive.

- 4) Select **Antivirus File Analysis - Inbound** to enable file analysis with antivirus definitions.
  - Select **Analyze content from sites with elevated risk profiles** to enable file analysis on files from uncategorized sites and files from sites with elevated risk profiles, as identified by Security Labs.
  - Select **Analyze content from sites with elevated risk profiles and from sites with lower risk profiles** to analyze inbound files. This option is resource intensive.
- 5) Select **Advanced Detection File Analysis - Inbound** to enable advanced detection file analysis.
  - Select **Analyze content from sites with elevated risk profiles** to enable file analysis on files from uncategorized sites and files from sites with elevated risk profiles, as identified by Security Labs.
  - Select **Analyze content from sites with elevated risk profiles and from sites with lower risk profiles** to analyze inbound files. This option is resource intensive.



#### Note

For an I Series appliance deployment, when performance optimization is selected, the cloud service analyzes only sites with elevated risk profiles.

- 6) Select **Rich Internet Application analysis** to analyze Flash, Silverlight, and similar files for malicious content.
- 7) Click **Save**.

## Next steps

To manage which file types are analyzed, continue with *Configuring file analysis*.

To configure exceptions to advanced analysis, see *Analysis exceptions*.

### Related concepts

[Configuring file analysis](#) on page 219

[Analysis exceptions](#) on page 220

# Configuring file analysis

## Executable Files

Mark **Analyze executable downloads** on the Web Content & Security tab for a policy to protect your organization from inbound executables.

If you choose to analyze executable file downloads, you can block executable files by category on the *File Blocking tab*. Also use the File Blocking tab to:

- Configure the notification page presented to the user when an executable download is blocked.
- Optionally block users from uploading executable files. See *Blocking executable file uploads*.

**Related concepts**[File Blocking tab](#) on page 207[Blocking executable file uploads](#) on page 211

## File Type Analysis Options

The file type analysis options determine which types of files are analyzed for malicious content, including unrecognized files. Individual file extensions may also be specified. You can specify the maximum file size to analyze (default 10 MB).

Larger files pass through the proxy without analysis.

To specify the types of files to analyze:

### Steps

- 1) Mark the check box next to each file type that you want to analyze.  
As a best practice, analyze all suspicious files, as identified by Security Labs, and all unrecognized files.

**Note**

For an I Series appliance deployment, when performance optimization is selected, the cloud service performs file type analysis only for sites with elevated risk profiles.

- 2) To always analyze files having a specific extension, under **Analyze these file extensions**, enter the extension in the entry field and click **Add** or press **Enter**. You can enter multiple extensions, separated by commas. For example, enter gz, cad, or js.
  - To edit an existing file extension, you must delete it, and add it again with the changes that you want.
  - To remove an extension from the list, select the extension or extensions from the list, and click **Delete**. To select multiple extensions, select each extension while pressing the **Ctrl** or **Shift** key.
- 3) Next to **Maximum file size to analyze**, enter a size in megabytes. Files larger than the specified size are not analyzed.
- 4) When you're finished, click **Save**.  
To configure exceptions to advanced analysis, see *Analysis exceptions*.

**Related concepts**[Analysis exceptions](#) on page 220

## Analysis exceptions

Analysis exceptions are lists of trusted or untrusted sites that are **never analyzed** or **always analyzed**. The type of analysis to never or always perform is specified per site or group of sites.


Use the **Always Analyze** and **Never Analyze** lists to refine the advanced analysis offered by the cloud service. When real-time content classification, real-time security classification, or antivirus file analysis options are

enabled, sites on the **Always Analyze** list are always analyzed, and sites on the **Never Analyze** list are never analyzed.

Use the Never Analyze list with caution. If a site on the list is compromised, the cloud service does not analyze the site and cannot detect the security problem.

## To add/delete sites to the Always Analyze or Never Analyze lists:


### Steps

- 1) Click the Add icon .
- 2) Enter the site. You can enter the optional paths also along with the site. For example, `prelmonk.com/test/test1`.



#### Note

- While adding the Analysis exception, do not enter the protocol.
- Analysis exception on the path is only applicable, when decryption is enabled for the category of the site.
- Only a site and the optional paths are allowed, attributes are not allowed.

- 3) Click the Tick icon  to add the site to the list.  
A site can appear in only one of the two lists.
- 4) When you are finished making changes to both lists, click **Save**.
- 5) To delete a site from a list, click the red "X" (delete) icon to the right of the site.
- 6) To edit a site in either list, click the Pencil (edit) icon.
- 7) To undo the entry of a site, click the red-dash "-" (undo) icon.



### Contents

- [Introduction](#) on page 223
- [Using the Report Catalog](#) on page 224
- [Using the Report Builder](#) on page 231
- [Scheduling reports](#) on page 236
- [Exporting data to a third-party SIEM tool](#) on page 239

## Introduction

---

Web and email cloud protection solutions include many tools for reporting on service activity and security events. For information specific to web and data reporting, see *Web 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*, page 386.

### Related concepts

[Using the Report Catalog](#) on page 224

[Using the Report Builder](#) on page 231

[Scheduling reports](#) on page 236

[Using the Transaction Viewer](#) on page 248

### Related tasks

[Viewing detailed reports](#) on page 235

### Related information

[Web Reporting Tools](#) on page 247

# 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 web and data security predefined reports, see *Web 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

[Web predefined reports](#) on page 265

[Managing reports](#) on page 225

[Managing folders](#) on page 228



# 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 228](#)

## Related tasks

[Run a report on page 225](#)

[Add a new report on page 225](#)

[Copy a report on page 226](#)

[Edit an existing report on page 227](#)

[Share a report on page 227](#)

[Delete a report on page 228](#)

# Run a report

---

## Steps

- 1) In the left-hand pane, navigate through the folder structure and select the sub-folder 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 234](#)

## Related tasks

[Viewing detailed reports on page 235](#)

# 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 232](#)

## 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 230

## 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 pop-up 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 236

## 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 pop-up 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 229

[Copy a folder](#) on page 229

[Move items between folders](#) on page 230

[Share a folder](#) on page 230

[Delete a folder](#) on page 231

## 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” pop-up 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 pop-up 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 227

## 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 pop-up 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 web and data report attributes, see *Report attributes: Web and Data Security*.

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 web and data security metrics, see *Report metrics: Web and Data Security*.

All web reports contain Hits as the primary metric, as signified by a star in the column name. To change the primary metric, drag a second metric to the report and then sort by that new metric to make it the primary. For more information, see *Report Builder metrics*.

**Note**

If you add the Browse Time metric to your report, note that the browse time totals may not be accurate for second-level grouping data.

For example, if you create a report with the first attribute as User and the second as Domain, and a user goes to 2 different sites within the same minute the browse time totals are correct at the first level for the user, but at the second level the 2 sites are each allocated 1 minute of browse time. Therefore you cannot accurately add up the browse time totals at the second level.

- 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**

Report attributes: [Web and Data Security](#) on page 250

Report metrics: [Web and Data Security](#) on page 264

Viewing report results on page 234

**Related tasks**

Creating a report on page 232

Viewing detailed reports on page 235

**Related reference**

Report Builder metrics on page 264

## 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 pop-up 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

[Viewing detailed reports](#) on page 235

## 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.

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 popup 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.
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 236

## 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

[Scheduling reports](#) on page 236

[Selecting report recipients](#) on page 239

#### Related tasks

[Selecting reports to schedule](#) on page 237

[Setting the schedule](#) on page 238

[Selecting delivery options](#) on page 239

## 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 (see *Using the Transaction Viewer for Web*, see *Using Message Details for Email*).

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 concepts**

[Using the Transaction Viewer](#) on page 248

[Report attributes: Web and Data Security](#) on page 250

**Related tasks**

[Configuring SIEM storage](#) on page 28

## 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:

- 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 243

## 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: <code>-u siem_user@example.com</code>
-p <password> --password	Mandatory. This is the password for the specified user name.  For example: <code>-p Ft2016Logs</code>
--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.

Parameter	Description
-v --verbose	<p>Optional. Runs the script in verbose mode, which displays progress messages.</p> <p>Verbose mode provides feedback on the script's progress, for example:</p> <ul style="list-style-type: none"> <li>■ Downloading filelist from &lt;host name&gt; as &lt;user name&gt;</li> <li>■ No files available to download</li> <li>■ Downloading &lt;file&gt; to &lt;file name location&gt;</li> </ul>
-h <hostname> --host	<p>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.</p> <p>For example:</p> <p><i>-h https://sync-web.mailcontrol.com</i></p>
-d <file path> --destination	<p>Optional. Defines the destination directory for the downloaded log files. If not specified, the files are downloaded into your current working directory.</p> <p>For example:</p> <p><i>-d /cloudweb/logs</i></p>
-m --md5sum	<p>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.</p>
-l --list-only	<p>Optional. Displays a list of available log files without downloading them.</p>
--proxy <proxy details>	<p>Optional. Specifies an HTTP proxy to use if you are having difficulty connecting to the cloud service. The proxy must be in the form <i>http://username:password@host:port</i></p> <p>For example:</p> <p><i>--proxy http://jsmith:Abc123@proxy_server:80</i></p>
--max_download_children	<p>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.</p> <p>If the <b>list-only</b> parameter returns a large number of files not yet downloaded, set this value to 10 to allow the downloads to process those files.</p>
--infinite_loop	<p>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.</p>

Parameter	Description
<code>--man</code>	Optional. Displays the list of parameters with their descriptions.
<code>--help</code>	Optional. Displays a brief description of the program's purpose.
<code>--cfgfile</code>	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.



## Chapter 8

# Web Reporting Tools

### Contents

- Introduction on page 247
- Using the Transaction Viewer on page 248
- Using the Incident Manager on page 249
- Report attributes: Web and Data Security on page 250
- Report metrics: Web and Data Security on page 264
- Web predefined reports on page 265

## Introduction

---

Your web protection product provides several reporting tools that can help you evaluate the effectiveness of your Internet access policies.

- **Web Dashboard charts** provide threat, risk, usage, and system information to help you review Internet activity in your network at a glance. For most charts, the time period, chart style, and set of results shown can be customized, and you can also click columns or sections on a chart to drill down to the relevant report in the Report Builder. See *Web dashboards*.
- Use the **Report Builder** to create Web Security and Data Security reports from scratch.
  - See *Using the Report Builder* for details about building reports.
  - See *Report attributes: Web and Data Security* for explanations of the attribute options in reports.
  - See *Report metrics: Web and Data Security* for information about the metrics available in reports.
- The **Report Catalog** offers a list of predefined Web Security and Data Security reports. Copy any predefined report to apply your own filters to create a custom report.
  - See *Using the Report Catalog* for more information.
  - See *Web predefined reports* for information about the available reports.
- The **Transaction Viewer** provides detailed information about web transactions and requests. You can drill into the Transaction Viewer from Web Security reports, or access it directly from the Reporting menu. See *Using the Transaction Viewer*.
- The **Incident Manager** provides detailed information about data security incidents. You can drill into the Incident Manager from Data Security reports, or access it directly from the Reporting menu. See *Using the Incident Manager*.

**Related concepts**

Using the Report Builder on page 231

Report attributes: Web and Data Security on page 250

Report metrics: Web and Data Security on page 264

Using the Report Catalog on page 224

Web predefined reports on page 265

Using the Transaction Viewer on page 248

Using the Incident Manager on page 249

# Using the Transaction Viewer

Use the **Reporting > Report Center > Transaction Viewer** page to find full details of individual web transactions and requests. Where Report Builder shows you high-level analysis from the perspective you select, Transaction Viewer gives you an additional layer of granular information for each transaction. You can manipulate the data further by adding extra filters and columns.

Access Transaction Viewer directly from the Reporting tab to build your own transaction-level reports, or drill down from the Report Builder:

- 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 popup window appears.
- 2) In the pop-up window, select **View Transactions**.

You can also click an entry in any metrics column to view that entry as individual transactions.

The Transaction Viewer loads, listing the date, time, and URL of each transaction within the report item or items you selected.

In the Transaction Viewer, you can:

- Edit the filters and date range for the transactions you wish to see.
- Select the columns to display from the **Columns** drop-down. Click **Close** 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.

**Note**

To sort transactions by timestamp, click the Date column, not the Time column. Sorting by the Date column automatically orders transactions by both date and time.

- Delete columns by clicking the X icon in a column heading. Note that you cannot delete the current active column.
- Drag attributes and metrics from the left-hand pane into the Filters field.
- Drag attributes and metrics from the left-hand pane into the main report pane to add them as new columns.
- Enable Detail View to see more detail for the selected transaction. You can also double-click a row to open Detail View.

The Transaction Details pane opens at the bottom of the page, showing additional information. Depending on the content of the transaction, you may see the following tabs:



- **General** lists information such as the user who performed the transaction, the policy, the action, the Web category and risk class. When the risk class is Security, Detail View also displays threat details.
  - **Request Details** shows the full URL, source and destination IP addresses, the referrer URL, the full MIME type, and the request method.
  - **Threat Details** is displayed for transactions that involve a security risk. The tab shows the category, severity level, threat name, and threat type, as well as the direction of the transaction.
  - **File Sandbox** is displayed when the transaction is associated with a file that was sent for advanced sandboxing analysis. The tab lists all files associated with the transaction and the result returned by the File Sandbox, as well as a link to the File Sandbox report.
  - **Cloud App Details** shows further information about the cloud app associated with the transaction. The tab lists details for the cloud app, such as its name, description, risk level, provider details, and URL, along with a detailed risk profile.
  - **Advanced** lists HTTP status code, total bandwidth used, filtering time, server response time, authentication method, and user agent.
- Export selected transactions in PDF or CSV format.  
A maximum of 5,000 table rows can be exported to a PDF file, a maximum of 100,000 table rows to CSV. Data exported using Detail view (PDF format only) can include a maximum of 20 transactions.

## Using the Incident Manager

Use the **Reporting > Report Center > Incident Manager** page to find full details about data security incidents. Where Report Builder shows you high-level analysis of data security results, Incident Manager gives you an additional layer of granular information for each incident. You can manipulate the data further by adding extra filters and columns.

In the Incident Manager, you can:

- Edit the filters and date range for the incidents you want to review.
- Select the columns to display from the **Columns** drop-down. Click **Close** when you have made your selections.
- Use the **Rows** drop-down to configure the maximum number of rows displayed in the table. The default is 100, and up to 200 rows may be shown.
- Click a column heading to make it the active column for sorting transactions. Click again to switch between ascending and descending order.



### Note

To sort incidents by timestamp, click the Date column, not the Time column. Sorting by the Date column automatically orders transactions by both date and time.

- Delete columns by clicking the X icon in a column heading. Note that you cannot delete the current active column.
- Drag attributes left-hand pane into the Filters field.
- Drag attributes from the left-hand pane into the main report pane to add them as new columns.
- Enable Detail View to see more detail for the selected incident. You can also double-click a row to open Detail View. The Incident Details pane opens at the bottom of the page, and contains 3 tabs:
  - **Matches** shows the policies and classifiers that were matched, as well as the number of matches, for the incident. Administrators with appropriate permissions can also see the content that matched the classifiers.

- **Source & Destination** shows name, IP address, and group information for the end user who made the request (source), and IP address, URL, and geographical location for the target of the request (destination).
- **Properties** shows the severity, incident time, top matches, file name (if applicable), and policy for the selected incident, as well as any other available attributes from the incident table.

When you have configured the Incident Manager, you can save or export the report as follows:

- To save the report to run again, click the **Save** icon in the button bar above the table. When prompted, provide a name and description for the report, then select a folder. When you are finished, click **Save Report**.
  - To schedule a saved report, click the **Schedule** icon in the button bar above the table.
  - To share a saved report, click the **Share** icon in the button bar above the table.
- To export selected transactions in PDF or CSV format, click the PDF or Excel icon at the top, right of the page. In PDF format you have the option to export the Detail View for the incidents you select. This export is limited to 20 incidents.

If you are working in a saved report and want to create a new report, click the **New** icon in the button bar above the table.

## Report attributes: Web and Data Security

The tables below list the report attributes that are available in the Report Builder, Transaction Viewer (for Web Security transactions), and Incident Manager (for data security incidents). Attributes are listed in the order they appear on the page.

- *Web Security reports*
- *Data Security reports*

For many attributes, you have the option to choose “is”, “is not”, “contains”, “does not contain”, “starts with”, and “does not start with”. Use these qualifiers to narrow your results. For example, you may select **Destination Country is not United States** to filter out U.S. events.

For information about report metrics, see *Report metrics: Web and Data Security*.

### Related concepts

[Web Security reports](#) on page 250

[Report metrics: Web and Data Security](#) on page 264

### Related reference

[Data Security reports](#) on page 259

## Web Security reports

# Web attributes

Name	Description	Filter values
<b>General</b>		
Action	The action taken by the cloud service based on the category of the requested page. Options are Allowed, Authentication Required, Blocked, Confirmed, Quota.	Check boxes
Category	Web categories in your cloud service account.	Autocompleted text
Direction	Whether the traffic was inbound or outbound.	Check boxes
Group	Groups created in or synchronized to your account.	Autocompleted text
Localized Country	Where a virtual point of presence (vPoP) IP address is used, this field records the country to which the IP is registered for localization purposes.	Check boxes
Parent Category	Parent categories as defined in the Forcepoint URL Database.	Autocompleted text
Policy	The web policy used for filtering.	Autocompleted text
Risk Class	The type of risk posed to your organization. Options are Business Usage, Legal Liability, Network Bandwidth Loss, Productivity Loss, Security, or None.	Check boxes
Search Term	Search terms entered by your end users.	Manual text
User	Users created in or synchronized to your account.  Note: this can show the value <i>Not available</i> for transactions where authentication has been bypassed.	Autocompleted text
Workstation	Client workstations that have authenticated for web browsing. You can also choose to include authentication results that are not associated with a workstation.	Manual text
<b>URL</b>		
Domain	Requested domains, for example google.com or bbc.co.uk.	Manual text

Name	Description	Filter values
Domain - Second Level	The second-level part of requested domains, for example google or bbc.	Manual text
Domain - Top Level	The top-level part of requested domains, for example com, or co.uk.	Manual text
Host	Requested host names, for example news.bbc.co.uk, or mail.google.com.	Manual text
Path	Paths used in requested URLs.	Manual text
Protocol	Protocol used to request sites. Options are HTTP or HTTPS.	Check boxes
Query	Query entered by end user.	Manual text
URL	Requested URLs.	Manual text
URL - Full	Full requested URLs (including the http part).	Manual text
<b>Cloud Apps</b>		
Cloud App	The name of the cloud app requested by end users.	Autocompleted text
Cloud App Category	The type of cloud app.	Check boxes
Cloud App Forwarded	Whether the request was forwarded to Forcepoint CASB by the Protected Cloud Apps feature.	Check boxes
Cloud App Risk Level	The risk level of the cloud app. (High risk, medium risk, or low risk.)	Check boxes
<b>IP Address</b>		
Connection IP	IP address of connection to the cloud service.	Manual text
Connection Name	Name configured for the connection to the cloud service. Connections with no associated name are shown as "Unknown".	Autocompleted text
Connection IP Country	Country in which connection IP address is located.	Autocompleted text
Destination IP	IP address of destination site.	Manual text
Destination IP Country	Country in which destination IP address is located.	Autocompleted text
Source IP	IP address of source requesting a site. Use the "contains" or "does not contain" option to search for the required IP address.	Manual text
<b>Security</b>		

Name	Description	Filter values
Analytic Name	Web analytics applied to sites. Options are Advanced Detection, Antivirus Scanning, Application Recognition, Content Categorization, Malicious iFrame Detection, PDF Scanner, Security Scanning, Zip Bomb Detection, or None.	Check boxes
File Sandbox Status	Results returned for files analyzed by the file sandboxing service. Options are: Malicious, Safe, Failed to analyze, Pending analysis, and File not supported.  Requires the Forcepoint Advanced Malware Detection for Web module.	Check boxes
Severity	The severity classification of a security threat. Options are Critical, High, Medium, or Low.	Check boxes
Threat Name	Names associated with a security threat.	Manual text
Threat Type	Types of security threat – for example spyware, exploits, trojans, or password stealers.	Manual text
<b>Time</b>		
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
<b>Mobile Device</b> Applies only to Forcepoint Mobile Security integrated with AirWatch Mobile Device Management		
Mobile / Non- Mobile	Traffic on mobile devices that are secured by Forcepoint Mobile Security and traffic on other devices, such as laptops and desktop machines, secured by the cloud service.	Check boxes
Device Profile	Profiles defined as Corporate (individual), Corporate (shared), Personal, or Unknown.	Check boxes

Name	Description	Filter values
Device Platform	Mobile operating systems defined as Android, iOS, or Unknown.	Check boxes
Device Type	Names of devices, such as iPhone, iPad, or Android.	Manual text
IMEI Number	Unique 17- or 15-digit codes used to identify individual mobile stations to mobile phone networks.	Manual text
Mobile App Name	Names of mobile apps being accessed, such as Facebook or Barcode Scanner.	Manual text
Mobile App Category	Categories of mobile apps, such as Entertainment or Business and Economy. The same categories used for URLs, except specific to the app.	Manual text
<b>Media</b>		
File Name	Name of a downloaded file.	Manual text
File Type	Type associated with a downloaded file. Options are Archive, Document, Executable, Image, Multimedia, None, Rich Internet Application, Suspicious, Text, or Unknown	Check boxes
Full MIME Type	Full MIME type (for example text/html or image/gif) of accessed or downloaded files.	Manual text
MIME Subtype	MIME subtype (for example html or gif) of accessed or downloaded files.	Manual text
MIME Type	MIME type (for example text or image) of accessed or downloaded files.	Manual text
<b>Referrer URL</b>		
Referrer Domain	The domain of the previous item that led to the current transaction.	Manual text
Referrer Host	The host name of the previous item that led to the current transaction.	Manual text
Referrer Path	The full path of the previous item that led to the current transaction.	Manual text
Referrer Port	The port of the previous item that led to the current transaction.	Manual text
Referrer Query	The query on the previous page that led to the current transaction.	Manual text

Name	Description	Filter values
Referrer URL	The URL of the previous item that led to the current transaction. Can also include results with no referrer URL.	Manual text
Referrer URL - Full	Full URL (including the http part) of the previous item that led to the current transaction. Can also include results with no full referrer URL.	Manual text
<b>User Agent</b>		
Browser	The specific browser used, including type and version (for example, Internet Explorer 11). When filtering, if the browser you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/ manual text
Browser Type	The type of browser used across all versions (for example Internet Explorer). When filtering, if the browser type you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/ manual text
Operating System	The specific operating system used, including type and version (for example, Windows 7). When filtering, if the operating system you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/ manual text
Operating System Type	The general type of operating system used across all versions (for example, Windows or Linux).  When filtering, if the operating system type you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/ manual text

Name	Description	Filter values
User Agent	<p>The specific user agent used to access sites. This is a string sent from your browser or Internet application to the server hosting the site that you are visiting. The string indicates which browser or application you are using, its version number, and details about your system, such as the operating system and version. The destination server then uses this information to provide content suitable for your specific browser or application.</p> <p>For example, this is a user agent for Firefox:</p> <p>Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6)</p> <p>In this example, Windows NT 5.1 indicates that the operating system is Windows XP, and the language it uses is US English.</p>	Autocompleted text
User Agent Type	<p>The type of user agent used to access sites. Options are Browser, Email Client, Feed Reader, Library, Mobile Browser, Multimedia Player, Offline Browser, Robot, Validator, or Unknown.</p>	Check boxes
<b>Advanced</b>		
Authentication Method	<p>Method of authentication used by end user to access sites. Options are Basic, Downstream Authentication, Endpoint, Form-based login, NTLM, Single sign-on, or None.</p>	Check boxes
Classification Type	<p>Category types as defined by Forcepoint URL Database for standard categories, and real-time analytics for dynamic categories. Enables you to filter on Static, Static Web 2.0, Real-time, and Dynamic real-time content.</p>	Check boxes



Name	Description	Filter values
Data Center	<p>The cloud service data center that processed the request.</p> <p>Options are UK - Heathrow (A), Germany - Frankfurt (B), India - Mumbai (C), France - Paris (D), Germany - Düsseldorf (E), Switzerland - Geneva (F), USA - San Jose (G), USA - Ashburn (H), Turkey - Istanbul (I), UK - Slough (J), Hong Kong (K), Australia - Sydney (M), USA - Chicago (N), USA - Dallas (O), Brazil - São Paulo (P), USA</p> <p>- Miami (Q), Singapore (R), South Africa - Johannesburg (S), Japan - Tokyo (T), and Netherlands - Amsterdam (X).</p>	Check boxes
Filtering Source	<p>Method used to direct client traffic for filtering.</p> <p>Options are Cloud connection, Endpoint Web (Proxy), Endpoint Web (Direct), IPsec Advanced, IPsec, GRE, EasyConnect, Appliance (Cloud traffic), Appliance (Local traffic), Secured mobile traffic, Aerohive integration, Firewall redirect, or Dedicated port.</p>	Check boxes
HTTP Status Code	HTTP response code, for example 404 when a page does not exist.	Manual text
Port	Port used to access web pages, for example 80 or 443.	Manual text
Request Method	HTTP request method. Options are Connect, Delete, Get, Head, Options, Patch, Post, Purge, Put, Trace, or None.	Check boxes
TLS Version (Downstream)	For encrypted web connections, the version of TLS that was used for downstream connections (between the user device and the cloud proxy).	Manual text
User Agent	User agent used for requests.	Manual text

## Authentication attributes

Name	Description	Filter values
<b>General</b>		

Name	Description	Filter values
Authentication Method	Method of authentication used by end user to access sites. Options are Endpoint, Form, Manual, NTLM, Single sign-on, or X-Authentication.	Check boxes
Endpoint Version	Specific version of the web endpoint client used for authentication.	Manual text
Operating System	Operating systems used for authentication.	Manual text
User	Users created in or synchronized to your account.	Autocompleted text
Workstation	Client workstations that have authenticated for web browsing. You can also choose to include authentication results that are not associated with a workstation.	Manual text
32/64-bit	End user authentication from 32- or 64-bit operating systems.	Check boxes
<b>Time</b>		
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

## Protocol attributes

Name	Description	Filter values
<b>General</b>		
Action	The action taken by the cloud service based on the category of the requested page. Options are Allowed or Blocked.	Check boxes
Destination IP	IP address of destination site. Use the “contains” or “does not contain” option to search for the required IP address.	Manual text
Destination Port	Port used for destination site.	Manual text

Name	Description	Filter values
Policy	The web policy used for filtering.	Autocompleted text
Protocol	Protocol used to request sites. Options are HTTP or HTTPS.	Check boxes
Protocol Group	Protocol group for requested sites. Options are Database, File Transfer, Instant Message / Chat, Instant Messaging File Attachments, Mail and Collaborative Tools, Malicious Traffic, Malicious Traffic (Cannot block), P2P File Sharing, Proxy Avoidance, Remote Access, Streaming Media, System, Other, or User Defined.	Check boxes
Source IP	IP address of source requesting a site. Use the “contains” or “does not contain” option to search for the required IP address.	Manual text
Source Port	Port used for source requesting a site.	Manual text
User	Users created in or synchronized to your account.  Note: this can show the value <i>Not available</i> for transactions where authentication has been bypassed.	Autocompleted text
<b>Time</b>		
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

## Data Security reports

Data Security reports can contain the attributes shown in the table below.

Note that data is only displayed in your report if the relevant classifier, category, regulation, etc. is included in your web policy. This is configured on the Data Security tab of the policy and the data is specific to policies configured with DLP Lite.

Data for some attributes is not available for policies configured with Data Protection Service. Use Forcepoint DLP to view and report on incidents not included in the these reports. See [Viewing Incidents and Reports](#) for more information.

Name	Description	Filter values
<b>Data Security</b>		
Action	Select <b>Blocked</b> to view incidents where potential data loss or theft was prevented. Select <b>Monitored</b> to view those that were permitted.	Check boxes
Content Category	<p>Select the types of content classifiers to include in the report:</p> <ul style="list-style-type: none"> <li>■ <b>Regulatory Compliance</b> - detects data loss applicable to your industry and region.</li> <li>■ <b>Data Theft</b> - detects when data is being leaked due to malware or malicious transactions.</li> <li>■ <b>Custom Classifier</b> - detects when patterns, phrases, or dictionary terms that are specific to your business are being leaked.</li> </ul> <p>Only incidents that breach these types are shown in the report.</p>	Check boxes
Content Classifier	<p>Enter the names of the content classifiers that you want to include in the incident report, one entry per line. For example:</p> <p>PCI: Credit Card Magnetic Strips US PII UK PII Pattern-1 KeyPhrase-X MyDictionary</p> <p>Only incidents that breach these classifiers are shown in the report.</p>	Manual text
Event ID	<p>Enter unique incident identifiers, one entry per line. Event IDs are 15-digit numerals. For example:</p> <p>123-456-789-000-123 124-457-789-000-124</p> <p>You can enter full or partial IDs. If you enter more than 3 digits, you must include hyphens. For example, "456-7".</p> <p>"Event ID contains 547" will show all events containing that number.</p>	Manual text

Name	Description	Filter values
Content Subcategory	<p>Select the particular content subcategories to include in the report.</p> <p>For example, PII and PHI are subcategories of the content category, Regulatory Compliance. Choose them if you want to show only PII and PHI incidents in the report.</p> <p>You can choose from the following.</p> <p><b>Regulatory Compliance</b></p> <ul style="list-style-type: none"> <li>■ PII</li> <li>■ PHI</li> <li>■ PCI DSS</li> </ul> <p>See <i>Regulations</i> for a description of the regulations.</p> <p><b>Data Theft</b></p> <ul style="list-style-type: none"> <li>■ Common password information</li> <li>■ Encrypted files – known format</li> <li>■ Encrypted files – unknown format</li> <li>■ Password files</li> <li>■ IT asset information</li> <li>■ Malware communication</li> </ul> <p>See <i>Data Theft</i> for a description of the data theft policies.</p> <p><b>Custom Classifiers</b></p> <ul style="list-style-type: none"> <li>■ RegEx</li> <li>■ Dictionary</li> <li>■ Key phrase</li> </ul> <p>Create these under <b>Policy Management &gt; Content Classifiers</b>, and then enable them on the Data Security tab of your policy.</p>	Check boxes

Name	Description	Filter values
Severity	<p>Incidents can be classified as high, medium, or low severity. Select the severities to include in the report.</p> <p>The severities of regulatory and data theft incidents are automatically decided by the system. This calculation takes both the prescribed severity of the incident and the number of matched violations into account.</p> <p>Custom classifier severities are user-defined.</p>	Check boxes
Top Matches	<p>Top matches indicates the number of matches on the incident's most violated rule.</p> <p>For example, if rule A in MyPolicy has 2 matches, rule B has 5 matches, and rule C has 10 matches, top match equals 10.</p> <p>Enter the threshold for top matches to include in the report (a numeric value), and then select the operator to use: equal to, greater than, etc.</p> <p>If you enter Top Match &gt; 10, then all incidents with a top match of 10 or more are included in the report.</p>	Numeric
Transaction Size	<p>Enter a numeric value to indicate the size of transactions to include in the report—namely, transactions that resulted in incidents.</p> <p>Next, select the operator to use: equal to, greater than, etc. For example, you can show transactions greater than 200 KB.</p>	Numeric (in KB)
Web Category	Category of the website that was used for the data transaction.	Auto-completed text
Web Policy	Name of the web policy that was violated.	Auto-completed text
<b>Source &amp; Destination</b>		
Connection IP	IP address of connection to the cloud service.	Manual text
Destination Country	Country in which the destination IP address is located.	Auto-completed text
Destination IP	Enter the IP address of the destination site you want included in the report.	Manual text

Name	Description	Filter values
Domain	Enter the domain name of the destination site you want included in the report. For example: cnn.co.uk	Manual text
Full URL	Enter the full URL of the destination site you want included in the report. For example: <a href="http://entertainment.cnn.co.uk">http://entertainment.cnn.co.uk</a>	Manual text
Source Country	Country in which the source IP address is located.	Auto-completed text
User	Enter the name or IP address of the users you want included in the report. For example: jdoe 10.2.33.7  To show records where User is empty, select "Include results with no User".	Manual text
<b>Media</b>		
File Name(s)	If you want to see incidents that involved specific files, enter the name of the files, one entry per line. For example: confidential.doc myData.xls	Manual text
<b>Time</b>		
Date	In the left box, click the dates to include in the report, and then click the right arrow to select them.	Selector
Hour	Select the time of interest. For example: 9:35 23:00	Selector

**Related tasks**

[Regulations](#) on page 214

[Data Theft](#) on page 215

# Report metrics: Web and Data Security

The tables below list the report metrics that can be added to Report Builder and Transaction Viewer reports. Incident Manager reports do not include metrics options.

## Report Builder metrics

Metric Name	Description
<b>Web Security Reports</b>	
Hits	The number of individual website hits for the attribute(s) and filter(s) you have selected. This is the default metric for report results.
Bandwidth	The total bandwidth (sent and received megabytes) used for each report item.
Browse Time	The time, in minutes, logged for browsing in each report item.
MB Received	The total number of megabytes received from each line item in the report.
MB Sent	The total number of megabytes sent for each line item in the report.
Avg. Filtering Time	The average time spent on inbound and outbound analysis by the cloud proxies for a request that is part of the report item. For example, if the report item is a category, this is the average filtering time for all requests in that category in the specified time period.
Avg. Server Resp. Time	The average time taken for a request in the report item to go from the cloud service (after outbound analysis) to the target server and then back to the cloud before inbound analysis. For example, if the report item is a policy, this is the average time taken by target servers to respond to the cloud service for all requests in that policy for the specified time period.
Cloud App Count	The number of cloud apps for the attribute(s) and filter(s) you have selected.
User Count	The number of unique users for the attribute(s) and filter(s) you have selected.
<b>Data Security Reports</b>	
Hits	The number of individual matches for the attribute(s) and filter(s) you have selected. This is the default metric for report results.
Top Matches	The number of matches on an incident's most violated rule.



Metric Name	Description
Transaction Size	The size in kilobytes of the transaction for each report item.

## Transaction Viewer metrics

Metric Name	Description
Bandwidth	The total bandwidth (bytes sent and received) used for each transaction.
Bytes Received	The total number of bytes received for each transaction.
Bytes Sent	The total number of bytes sent for each transaction.
Filtering Time	The total time spent by cloud proxies on outbound and inbound analysis for each transaction. Available only for Web attribute reports.
Server Response Time	The total time taken for the transaction to go from the cloud service (after outbound analysis) to the target server and then back to the cloud service (before inbound analysis). Available only for Web attribute reports.
User	Provides user information for each authentication transaction. Available only for Authentication reports.

## Web predefined reports

The tables below list the predefined reports available in the report catalog.

### Related reference

- [Advanced reports](#) on page 266
- [Bandwidth reports](#) on page 266
- [Cloud App reports](#) on page 267
- [Misconduct reports](#) on page 267
- [Productivity reports](#) on page 268
- [Risk Activity reports](#) on page 268
- [Security reports](#) on page 269
- [Social Media reports](#) on page 270
- [Web Activity reports](#) on page 271
- [Data Security reports](#) on page 272

## Advanced reports

Report Name	Description
Authentication Method Details	Details of authentication methods employed for web access by users.
Authentication Methods	A summary of the authentication methods used for web access.
Detailed Web Access Statistics	Full web browsing statistics for users, including server response times, filtering times, and bandwidth used.
Endpoint User Traffic	Details of all users who have browsed using a web endpoint client.
Endpoint Authentication Details	A detailed transaction report that includes client workstation, user, and Endpoint version details.
Installed Endpoint Client Statistics	The status of all endpoint clients in deployment, including version numbers.
User Agents	The top 10 user agents that have made web requests.

## Bandwidth reports

Report Name	Description
The top 10 categories that have used the most bandwidth in the last month. Evaluate whether policy changes are needed to manage bandwidth.	The top 10 categories that have used the most bandwidth in the last month. Evaluate whether policy changes are needed to manage bandwidth.
Top Groups for Streaming Media Bandwidth	The top 10 groups that have used the most bandwidth accessing streaming media sites.
Top Groups in Bandwidth Category	The top 10 groups containing users who accessed sites in the Bandwidth category.
Top MIME Types by Bandwidth	The top 10 file types that have used the most bandwidth.
Top Protocols by Bandwidth	The protocols that have used the most bandwidth.
Top Streaming Media Domains by Bandwidth	The top 10 streaming media sites that have used the most bandwidth.
Top Users for Streaming Media Bandwidth	The top 10 users that have used the most bandwidth accessing streaming media sites.
Top Web 2.0 Domains by Bandwidth	The top 10 domains in Web 2.0 categories that have used the most bandwidth.

## Cloud App reports

Report Name	Description
Top Cloud App Activity by Category	Cloud application activity broken down by the top 10 most-used application categories over the last 7 days.
Top Cloud App Activity by Category (Detail)	The top 10 most-used cloud applications in each of the top 10 most-used categories, over the last 7 days.
Top Cloud Apps by Bandwidth	The top 10 cloud applications consuming the most bandwidth over the last 7 days.
Top Cloud Apps by Hits	The top 10 cloud applications with the largest number of hits over the last 7 days.
Top Cloud Apps by Risk Level	The top 10 most-used cloud apps in each risk level over the last 7 days.
Top Users of Cloud Apps	The top 10 users of cloud applications over the last 7 days.
Top Users of Cloud Apps (Detail)	The top 10 most-used cloud apps for each of the top 10 users of cloud apps over the last 7 days.
Top Users of High Risk Cloud Apps	The top 10 users of high risk cloud apps over the last 7 days.



### Note

A summary is displayed for each cloud application that appears in a report when you hover your mouse over the “i” symbol next to its name. This summary text displays the current risk level for that application. Risk levels may change over time as applications are re-evaluated, so the risk level recorded for a particular transaction may not be the same as the current risk level for that application.

Click the “i” symbol beside the cloud app name for more information about the app, including a detailed risk profile.

## Misconduct reports

Report Name	Description
Top Legal Liability Categories	The top 10 categories containing accessed sites that may be a legal liability risk. Discover potential security risks and evaluate whether policy changes are needed.
Top Users of Adult Material Sites	The top 10 users who accessed sites in the Adult Material category.
Top Users of Hacking Sites	The top 10 users who accessed sites in the Hacking category. Discover potential security risks and evaluate whether policy changes are needed.

## Productivity reports

Report Name	Description
Blocked Request Details	Full details of all blocked requests in the last 7 days.
Browsing Times of Groups and Users	The top ten users with the highest browse time for the top ten groups.
Top Blocked Domains	Which blocked sites are requested most and report on filtering effectiveness. (If there are legitimate business use sites, consider recategorizing those URLs so you can permit them while blocking the category.)
Top Blocked Users	Which users request the most blocked sites. Consider refining the organization's Internet use policy to address productivity concerns.
Top Categories for Blocked Sites	Which blocked categories are requested most. Report on filtering effectiveness. If there are legitimate business use sites in these categories, consider recategorizing those URLs so you can permit them while blocking the category.
Top Groups for Blocked Sites	Which groups of users have their Internet requests blocked most. Discover potential productivity issues, and report on filtering effectiveness. (If legitimate business use sites are being blocked, consider recategorizing those URLs so you can permit them while blocking the category.)
Top Policies for Blocked Sites	The top 10 policies that have requested blocked sites.
Top Productivity Loss Users	Which users spent the most time on possible productivity reduction sites.
Top Productivity Site Users	The top 10 users who have accessed sites in the Productivity category.
Top Quota Time Categories	The top 10 categories that contain sites accessed using quota time.

## Risk Activity reports

Report Name	Description
Risk Class Trend by Bandwidth	The bandwidth used by requests to sites in all risk classes in the last month.
Risk Class Trend by Hits	Statistics for requests to sites in all risk classes in the last month.
Top Users of Risk Class Sites	The top 10 users who have requested sites in risk classes.

# Security reports

Report Name	Description
Antivirus Threats	Threats that have triggered the antivirus scanning analytic in the last month, and that were blocked because the response would have returned dangerous content.
Antivirus Transaction Details	Full details of malware detected through the antivirus security analytic, including the user, the connection IP address, and the requested URL.
Blocked Security Threats by Category	A listing of threat categories and types. See how many times users were blocked from downloading malicious files to determine productivity and security risks to your organization. Evaluate if changes in policy are needed.
Detailed File Sandboxing Report	Details about files downloaded by users in your organization that were analyzed by file sandboxing in the last 7 days.
Phishing Sites by Date	Blocked requests to phishing and other fraud sites in the last month.
Security Category Trend by Hits	Daily trends in blocked and permitted requests for security risk categories. Discover potential security risks and evaluate whether policy changes are needed.
Security Threat Details	Full details of all real-time blocked security threats in the last 7 days.
Security Threat Domains	Domains containing security threats that have been requested and blocked in the last month.
Security Threat Transaction Details	Full details of transactions that were considered a security risk, including the threat type, category, user, and full requested URL.
Security Threats by Date	Requests to sites in the security risk class in the last month.
Top File Sandboxing Results	The top results returned by file sandboxing analysis in the last 7 days.
Top Groups Accessing Spyware	The top ten groups with the highest number of spyware blocks.
Top Phishing Hosts	Requests to the top 10 hostnames in the Phishing category.
Top Protocols for Security Threats	The top 10 protocols containing security threats in the last month.
Top Security Categories and Threat Types	The number of times users were blocked from accessing websites containing threats to determine security risks in your organization.

Report Name	Description
Top Security Risk Users and Domains	Which users attempted to access security risk sites and had their requests blocked.
Top Security Threat Categories	Which categories in the Security Risk class are being accessed most. Assess the security risk to your organization via Internet access.
Top Security Threats	The top 10 threats from secure (HTTPS) sites in the Security risk class during the last month.
Top Spyware Hosts	The top 10 hostnames that have been blocked in the Spyware category.
Top Threat Types	The threat types users most often attempt to download. Assess the security risk to your organization through file downloads.
Top Users for Blocked File Types	A listing of users and which file types they were blocked from downloading to determine security risks in your organization.
Top Users for Outbound Spyware	The top 10 users who sent content to sites in the Spyware category.
Top Users for Security Scanning	Which users most often attempted to access Web sites containing security risks to determine if policy changes are needed.
Top Users for Security Threats by Domain	A listing of users and the websites they were blocked from accessing to see which threat categories and types they encountered. Use this information to determine security risks to your organization.
Top Users of Security Risk Sites	Which users are trying to download the greatest number of files with security risks. Assess the risk to your organization through file downloads, and consider whether policy changes are needed.
Top Users of Spyware Sites	Which users have accessed sites that may pose a spyware risk. Discover which users might be infected by spyware. (The Security categories must be enabled to view data in this report.)

## Social Media reports

Report Name	Description
Detailed Social Media Site Report	A detailed report of all social media transactions in the last 7 days.
Facebook Categories by Browse Time	Browse times for sites in the Facebook parent category in the last 7 days.
Social Networking Domains by Bandwidth	Bandwidth used for the top 10 domains in the Social Networking category in the last 7 days.

Report Name	Description
Top Facebook users by Bandwidth	Bandwidth used by the top 10 Facebook users in the last 7 days.
Top Social Media Trends	A line chart for sites in the top 10 social media categories accessed in the last 7 days.
Top Social Media Users	The top 10 users requesting sites in social media categories in the last 7 days.
Top Social Media Users and Categories	The top 10 users requesting sites in social media categories in the last 7 days, grouped by category.
Top Social Media Users and Parent Categories	The top 20 users requesting sites in social media categories in the last 7 days, grouped by parent category.
Top Social Networking Users by Bandwidth	Bandwidth used by the top 10 social networking users in the last 7 days.

## Web Activity reports

Report Name	Description
Category Trend by Browse Time	Browse times for the top 10 categories over the last month.
Category Trend by Hits	The top 10 categories accessed in the last month.
Detailed User Request Report	Detailed information about where users went, and when. Investigate their Internet requests, and the actions taken by your web protection software.
Detailed Web 2.0 Activity Report	Full details of Web 2.0 transactions in the last 7 days.
Filtering Actions Report	Actions taken on all site requests in the last 7 days.
Requested Domains by Date	Details of all domains accessed in the last 7 days, grouped by date.
Top Categories	Bandwidth, browse times, and hits for the top 20 categories in the last 7 days. Connections with no associated name are shown as "Unknown".
Top Categories and Domains	Frequently-requested domains in the top 10 categories for the last 7 days.
Top Connection Names	The top 20 connections that have had the most web activity in the last 7 days.
Top Domains	Volumes and sizes of the top 20 domains accessed in the last 7 days.
Top Groups	Which groups access the Internet most, and compare Internet usage between those groups. Use this information to refine the organization's Internet use policy or to address productivity concerns.

Report Name	Description
Top Policies	Web activity for the top 20 policies, and compare Internet usage for the users in those policies.
Top Users	Which users access the Internet most, and compare Internet usage between those users. Use this information to refine the organization's Internet use policy or to address productivity concerns.
Top Users and Categories	Which users are consuming the most bandwidth by the categories they are accessing. Discover suspicious quantities of traffic that might indicate spyware or other malicious code infection.  Evaluate whether policy changes are needed to manage bandwidth.
Top Users and Domains	Which users are consuming the most bandwidth by the domains they are accessing. Discover suspicious quantities of traffic that might indicate spyware or other malicious code infection.  Evaluate whether policy changes are needed to manage bandwidth.
Top Web 2.0 Categories	The top 20 Web 2.0 categories in the last 7 days, listed by hits and browse time.
Top Web 2.0 Users	The web activity for top 10 users in Web 2.0 categories in the last 7 days.
Web Requests by Date	The number of web requests from your organization over time.

## Data Security reports

Note that data returned from Data Protection Service to the cloud proxy does not support all of the fields included in Data Security reports. Use Forcepoint DLP to view and report on incidents not included in the these reports. See [Viewing Incidents and Reports](#) for more information.

Report	Description
<b>Content Type</b>	
Compliance Summary	Which compliance rules are most often violated in your organization and view a breakdown of the incident count for each policy or rule.
Custom Classifier Summary	Which custom classifiers triggered the most incidents during the designated period.
Data Theft Summary	A list of all data theft incidents that were detected during the designated period, along with incident details.
<b>Incidents</b>	



Report	Description
Incident List	List or chart of all data loss incidents that were detected during the designated period, along with incident details such as the destination, severity, and transaction size.
<b>Sources and Destinations</b>	
Destination Summary	Destination URLs or IP addresses involved with the most violations, broken down by severity.
Users Summary	Users, machines, or IP addresses most frequently violating data security policies and the severity of their breaches.



# Account Reports

### Contents

- [Introduction](#) on page 275
- [Endpoint Auditing Report \(Classic Proxy Connect and Direct Connect\)](#) on page 276
- [Service reports](#) on page 276
- [Downloading report results](#) on page 277
- [Saving reports](#) on page 278
- [Scheduling reports](#) on page 278

## Introduction

Go to **Reporting > Account Reports** to see the account-level reports available to you.

- For cloud web products, the Endpoint Auditing report, used for the classic endpoint agents, lists the current status of all endpoints deployed to users and workstations in your organization.
- If you have identity management enabled for your account, you can generate synchronization statistics for the service.

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*.

### Related tasks

[Saving reports](#) on page 278

[Scheduling reports](#) on page 278

# Endpoint Auditing Report (Classic Proxy Connect and Direct Connect)

Use the **Reporting > Account Reports > Endpoint Auditing** page to see the current status of all users and client machines with the endpoint installed.

By default the report displays the status of all endpoint users updated in the last 7 days, listing user names, workstation names, and the current endpoint status.

- To filter the report for one or more user names, enter the names in the search field and click **Search**.
- To change the report to list a particular endpoint status, select one of the following from the **Endpoint status** drop-down:
  - **Enabled** – all endpoints that are currently enabled
  - **Enabled (manually)** – endpoints that have been manually enabled by the end user
  - **Enabled (auto-recovery)** – endpoints that have automatically returned to an enabled state following a period of fallback due to a lack of connection with the cloud service
  - **Enabled (system restart)** – endpoints that have been automatically re-enabled on machine restart
  - **Disabled (manually)** – endpoints that have been manually disabled by the end user
  - **Fallback mode** – endpoints that cannot connect with the cloud service fall back to one of two modes. For Proxy Connect endpoints, the system allows requests to go directly to the local network/Internet. For Direct Connect endpoints, the system applies filters that have been cached for previously blocked sites before sending requests to the Internet.  
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.
- To edit the time period, select an option from the **Status updated** drop-down.
- To see further details for a particular user or workstation, click the user or workstation name. The User Details and Workstation Details pages show the following additional information:
  - When the endpoint status was last updated
  - The endpoint version
  - The operating system on which the endpoint is installed
  - The endpoint status change history for that user or workstation
- To export the report results to a CSV file, click the CSV icon in the top right of the page.

## 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 282](#)

# 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**.  
You can download the report to a CSV or PDF file. You can also print the report.

## 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.

## 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 278





### Contents

- [Introduction](#) on page 281
- [Configuration audit trail](#) on page 281
- [SCIM audit trail](#) on page 282

## 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.

### Related concepts

[Configuration audit trail](#) on page 281

[SCIM audit trail](#) on page 282

## 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 281](#)

# Standard Web Configuration

## Contents

- Overview on page 283

## Overview

The cloud service provides a standard configuration for all web accounts. These are described below. To customize your settings, follow the instructions in *Configuring Web Settings*.

**Web > Settings > General page, Proxy auto-configuration (PAC) file settings:**

Standard setting	Reason
Policy-specific PAC file should be used by default.	Allows cloud service to change cluster IP addresses without impact to your service.

**Web > Policy Management > Custom Categories page:**

Standard setting	Consider changing if...
There are no custom categories by default.	You want to create your own custom categories, each of which comprises a set of websites, for your users.

**Web > Policy Management > Protocols page:**

Standard setting	Consider changing if...
Standard protocols are provided by default.	You want to create your own custom protocols.

**Web > Policy Management > Block & Notification Pages page:**

Standard setting	Reason	Consider changing if...
Access Denied page displays by default when a policy denies access to a resource. Other standard include error, Cannot connect, HTTP authentication required, and more.	User needs to know why the requested page is not displaying.	You want a custom notification message. You can edit the default messages or create your own from scratch.

**Web > Policy Management > Time periods page:**

Standard setting	Reason	Consider changing if...
Afternoon Lunch Morning Working hours	These are the most common time periods our customers use.	You want to set up alternate time periods for your users. You can edit a time period or add a new time period.

By default, all time periods use the **Time Zone** indicate when registering for the service. Change the time zone if your end users are located in a different time zone or multiple time zones.

**Web > Settings > Domains** page:

Domains added on the Connections tab of a policy are account-level by default. Add one or more policy-level domains if you have multiple domains and want to apply a separate policy to each.

Standard setting	Consider changing if...
There are no default policy-level domains. When you add one, Include sub-domains is ON. Associate this domain with all policies is OFF.	You have multiple domains and want to apply a separate policy to each domain.

With a policy selected on the **Web > Policy Management > Policies** page:

■ **General** tab:

Standard setting	Consider changing if...
Policy name: default Administrator: email address used to register account PAC file: policy-specific PAC file address Time zone: time zone indicated during registration Time-based access: off	You want to rename your policy to something more meaningful.  You are establishing a policy for remote users.  Your users are in a different time zone.  You want to configure time-based access.  You want to apply different authentication methods to different geographical locations.

■ **Connections** tab:

Standard setting	Reason	Consider changing if...
By default, all users are treated as remote and must authenticate to use the service.	This gives you the tightest security until you configure your own connections.	If most users are connecting through a single IP address or IP range. In this case, add one or more proxied connections for your policy.  Add a non-proxied destination when you want to avoid connecting via our proxy service.

■ **Access Control** tab:

Standard setting	Reason	Consider changing if...
By default, all users are treated as remote and must authenticate to use the service.	This gives you the tightest security until you configure your own connections.	<p>You want to monitor user activity without requiring an additional login.</p> <p>You want to use Windows authentication to govern access. (Choose NTLM identification.)</p> <p>You want to authenticate users and you do not have Active Directory.</p> <p>You want to use a web endpoint client or single sign-on.</p>

■ **Endpoint tab:**

Standard setting	Reason	Consider changing if...
By default, endpoint deployment is disabled.	<p>You must choose:</p> <ul style="list-style-type: none"> <li>■ Whether you want to use an endpoint client</li> <li>■ Which endpoint client to use</li> <li>■ How to deploy the endpoint client</li> </ul>	<p>You want to deploy the Proxy Connect endpoint from the cloud.</p> <p>You want to automatically update one or more endpoint clients to new versions when available.</p>

■ **End Users tab:**

Standard setting	Consider changing if...
By default, end users are expected to self register, but they must be in your domain.	<p>You have a list of users and email addresses that you can upload. In this case bulk register end users to save them time.</p> <p>If you have end users outside of your domain, invite them to register.</p>

■ **File Blocking tab:**

Standard setting	Reason	Consider changing if...
No files are blocked by default.	You must select which file types and extensions are blocked for categories.	You want to block certain file types for particular categories, users, and groups.

■ **Web Content & Security tab:**

Standard setting	Consider changing if...
<ul style="list-style-type: none"> <li>■ Malware is blocked both inbound and outbound by default.</li> <li>■ Executables are blocked outbound by default.</li> <li>■ Real-time classification provided by the Advanced Classification Engine is on if available.</li> <li>■ Inbound antivirus analysis is enabled for sites with elevated risk profiles.</li> <li>■ File type analysis is enabled for suspicious and unrecognized files.</li> </ul>	<p>Some users require inbound executables. You do not want to block outbound traffic.</p> <p>You want to refine or disable real-time classification.</p> <p>You want to refine or disable antivirus analysis.</p> <p>You want to refine or disable file type analysis.</p>

■ **Web Categories** tab:

Standard setting	Consider changing if...
<p>Default policy blocks access to offensive and adult sites, allows news and entertainment sites, offers no blocklists or allowlists.</p>	<ul style="list-style-type: none"> <li>■ You want to customize the default policy to align with your company's acceptable use policy.</li> <li>■ You want to decrypt SSL requests for all or specific web categories.</li> </ul>

■ **Protocols** tab (I Series appliance only):

Standard setting	Consider changing if...
<p>Default policy allows or blocks a protocol based on protocol database default values.</p>	<p>You want to add custom protocols to align with your company's acceptable use policy.</p>

**Related information**

[Configuring Web Settings](#) on page 69

# Appendices

## Contents

- [Use Cases for Setting up User Provisioning](#) on page 289
- [Data Security Content Classifiers \(DLP Lite only\)](#) on page 301





## Appendix A

# Use Cases for Setting up User Provisioning

### Contents

- [New Web and/or email customers \(LDAP\)](#) on page 289
- [New Web customers \(SCIM\)](#) on page 293
- [Existing Web and/or email customers \(LDAP\)](#) on page 294
- [Existing Web customers \(SCIM\)](#) on page 298

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 Web customers \(SCIM\)](#)
- [Existing Web and/or email customers \(LDAP\)](#)
- [Considerations for existing customers \(LDAP\)](#)
- [Existing Web customers \(SCIM\)](#)
- [Considerations for existing customers \(SCIM\)](#)

### Related concepts

- [New Web and/or email customers \(LDAP\)](#) on page 289
- [Considerations for existing customers \(SCIM\)](#) on page 299
- [Existing Web and/or email customers \(LDAP\)](#) on page 294
- [Considerations for existing customers \(LDAP\)](#) on page 298

### Related tasks

- [New Web customers \(SCIM\)](#) on page 293
- [Existing Web customers \(SCIM\)](#) on page 298

## 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 290

[Synchronizing users/groups with more than one policy, and planning to manage policy assignment through an LDAP directory](#) on page 291

# 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 42

[Exceptions](#) on page 199

**Related tasks**

[Set up authentication \(Directory Synchronization only\)](#) on page 61

[Configure identity management](#) on page 59

[View and manage user data](#) on page 63

[Restore directories](#) on page 66

**Related reference**

[View recent directory synchronizations](#) on page 65

**Related information**

[Defining Web Policies](#) on page 159

## 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 42

[Exceptions](#) on page 199

**Related tasks**

- Set up authentication (Directory Synchronization only) on page 61
- Configure identity management on page 59
- View and manage user data on page 63
- Assign a group to a different policy on page 64
- Restore directories on page 66

**Related reference**

- View recent directory synchronizations on page 65

**Related information**

- Defining Web Policies on page 159

## 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**

[SCIM audit trail](#) on page 282

[Groups](#) on page 42

[Exceptions](#) on page 199

[Synchronizing with SCIM](#) on page 56

**Related tasks**

[Configure identity management](#) on page 59

[Assign a group to a different policy](#) on page 64

[View and manage user data](#) on page 63

**Related information**

[Defining Web Policies](#) on page 159

## 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 294

[Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal](#) on page 296

## 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 42

[Exceptions](#) on page 199

**Related tasks**

[Configure identity management](#) on page 59

[Assign a group to a different policy](#) on page 64

[Set up authentication \(Directory Synchronization only\)](#) on page 61

[View and manage user data](#) on page 63

[Restore directories](#) on page 66

**Related reference**

[View recent directory synchronizations](#) on page 65

**Related information**

[Defining Web Policies](#) on page 159

## 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 42](#)

**Related tasks**

- Configure identity management on page 59
- Assign a group to a different policy on page 64
- Set up authentication (Directory Synchronization only) on page 61
- View and manage user data on page 63
- Restore directories on page 66

**Related reference**

- View recent directory synchronizations on page 65

## 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 provides. (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 42

[Synchronizing with SCIM](#) on page 56

[SCIM audit trail](#) on page 282

**Related tasks**

[Configure identity management](#) on page 59

[View and manage user data](#) on page 63

## 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.

## Appendix B

# Data Security Content Classifiers (DLP Lite only)

### Contents

- [Personally Identifiable Information \(PII\)](#) on page 301
- [Protected Health Information \(PHI\)](#) on page 313
- [Payment Card Industry \(PCI\)](#) on page 315
- [Data Theft](#) on page 315

For your convenience, Forcepoint Web Security Cloud includes predefined data security content classifiers to detect and report on data loss in your organization and help you conform to industry regulations in your geo-location.

Predefined classifiers enable you to quickly and easily define what type of content is considered a security breach on your network.

Many policies are disabled by default, but you can enable them in the cloud portal by navigating to the Data Security tab of your web policy.

You can also create custom data security classifiers on the **Policy Management > Content Classifiers** page.

The predefined classifiers included in the cloud service are constantly being updated and improved. There are several types of policies:

Type	Description
Personally Identifiable Information (PII)	Policies for detecting personally identifiable information such as social security, passport, and drivers' license numbers. The rules that are enforced depend on the region you selected.
Protected Health Information (PHI)	Policies for detecting personal health information such as disease names and medications. The rules that are enforced depend on the region you selected.
Payment Card Industry (PCI)	Policies for detecting credit card numbers and cardholder data. The rules that are enforced depend on the region you selected.
Data Theft	Policies for detecting various attempts to steal sensitive data.

## Personally Identifiable Information (PII)

The following predefined policies are available for the detection of private information:

- Australia PII

Policy for detection of Australian private information. The rules for this policy are:

- Australia PII: Australia TFN
- Australia PII: Driver License and Name
- Belgium PII  
Policy for detection of Belgian private information. The rules for this policy are:
  - Belgium PII: Name and ID Card Number (Wide)
  - Belgium PII: Name and ID Card Number (Default)
  - Belgium PII: Name and Passport (Wide)
  - Belgium PII: Name and Passport (Default)
  - Belgium PII: ID Card Numbers
  - Belgium PII: Passport Numbers
- Brazil PII  
Policy for detection of Brazilian private information. The rules for this policy are:
  - Brazil PII: Name and CPF
  - Brazil PII: Name and Health
  - Brazil PII: CPF and Health
  - Brazil PII: RG
  - Brazil PII: RG (Narrow)
- Canada PII  
Policy for detection of Canadian private information. The rules for this policy are:
  - Canada PII: SIN
  - Canada PII: SIN + Name
  - Canada PII: SIN + Name (Narrow)
  - Canada PII: Name + Alberta DL
  - Canada PII: Name + British Columbia
  - Canada PII: Name + Manitoba DL
  - Canada PII: Name + New Brunswick DL
  - Canada PII: Name + Newfoundland and Labrador DL
  - Canada PII: Name + Nova Scotia DL
  - Canada PII: Name + Ontario DL
  - Canada PII: Name + Prince Edward Island DL
  - Canada PII: Name + Quebec DL
  - Canada PII: Name + Saskatchewan DL
- Czech Republic  
Policy for detection of Czech Republic private information. The rules for this policy are:
  - Czech Republic PII: Rodne Cislo (Wide)
  - Czech Republic PII: Rodne Cislo (Default)
- Denmark Finance  
Policy for detection of Danish financial information. The rules for this policy are:
  - Danish IBAN Rule (Default)

- Denmark Finance: Danish IBAN (Wide)
- Denmark PII  
Policy for detection of Danish private information. The rules for this policy are:
  - Denmark PII: CPR and Name (Wide)
  - Denmark PII: CPR and Name (Default)
  - Denmark PII: CPR and Name (Narrow)
  - Denmark PII: CPR numbers (Wide)
  - Denmark PII: CPR numbers (Default)
  - Denmark PII: CPR numbers (Narrow)
- Finland Finance  
Policy for detection of Finnish financial information. The rules for this policy are:
  - Finland Finance: Finnish IBAN (Default)
  - Finland Finance: Finnish IBAN (Wide)
- Finland PII  
Policy for detection of Finnish private information. The rules for this policy are:
  - Finland PII: SSN (Wide)
  - Finland PII: SSN (Default)
- France Finance  
Policy for detection of French financial information. The rules for this policy are:
  - France Finance: French IBAN (Default)
  - France Finance: French IBAN (Wide)
- France PII  
Policy for detection of French private information. The rules for this policy are:
  - France PII: CCN and Name
  - France PII: INSEE numbers
  - France PII: Name and Health
  - France PII: INSEE and Health
  - France PII: Name and INSEE
- Germany Finance  
Policy for detection of German financial information. The rules for this policy are:
  - Germany Finance: German IBAN (Default)
  - Germany Finance: German IBAN (Wide)
- Germany PII  
Policy for detection of German private information. The rules for this policy are:
  - Germany PII: CCN and Name
  - Germany PII: Ethnicity and Name
  - Germany PII: Health and Name
  - Germany PII: Crime and Name
- Greece Finance  
Policy for detection of Greek financial information. The rules for this policy are:
  - Greece Finance: Greece IBAN (Default)

- Greece Finance: Greece IBAN (Wide)
- Greece PII  
Policy for detection of Greek private information. The rules for this policy are:
  - Greece PII: AFM number (Default)
  - Greece PII: AFM number (Wide)
  - Greece PII: AFM number and Name (Default)
  - Greece PII: AFM number and Name (Wide)
  - Greece PII: ID (Default)
  - Greece PII: ID and Name (Default)
  - Greece PII: ID and Name (Wide)
  - Greece PII: Sensitive Medical Information and Name (Default)
  - Greece PII: Sensitive Medical Information and Name (Wide)
- Hong Kong PII  
Policy for detection of Hong Kong private information. The rules for this policy are:
  - Hong Kong PII: Common Surname and Address (Default)
  - Hong Kong PII: Common Surname and Address (Narrow)
  - Hong Kong PII: Common Surname and Address (Wide)
  - Hong Kong PII: Hong Kong ID - (Default)
  - Hong Kong PII: Hong Kong ID - (Wide)
  - Hong Kong PII: Hong Kong ID (default pattern) and Common Address
  - Hong Kong PII: Hong Kong ID (default pattern) and Common Surname
  - Hong Kong PII: Hong Kong ID (default pattern) with Common Surname and Address
  - Hong Kong PII: Hong Kong ID (formal form) and Common Address
  - Hong Kong PII: Hong Kong ID (formal form) and Common Surname
  - Hong Kong PII: Hong Kong ID (formal form) with Common Surname and Address
  - Hong Kong PII: Hong Kong ID (Wide) and Common Address
  - Hong Kong PII: Hong Kong ID (Wide) and Common Surname
  - Hong Kong PII: Hong Kong ID (Wide) and Common Surname and Address
  - Hong Kong PII: Hong Kong ID (formal form)
- Hungary PII  
Policy for detection of Hungarian private information. The rules for this policy are:
  - Hungary PII: Hungarian Szemelyi Azonosito Szam (Wide)
  - Hungary PII: Hungarian Szemelyi Azonosito Szam (Default)
  - Hungary PII: Hungarian TAJ szam (Wide)
  - Hungary PII: Hungarian TAJ szam (Default)
  - Hungary PII: Hungarian Adoazonosito jel (Wide)
  - Hungary PII: Hungarian Adoazonosito jel (Default)
- Iceland Finance  
Policy for detection of Icelandic financial information. The rules for this policy are:
  - Iceland Finance: Icelandic IBAN (Default)
  - Iceland Finance: Icelandic IBAN (Wide)



- **Iceland PII**  
Policy for detection of Icelandic private information. The rules for this policy are:
  - Iceland PII: Kennitala (Default)
  - Iceland PII: Kennitala (Wide)
- **India PII**  
Policy for detection of Indian private information. The rules for this policy are:
  - India: Form 16
  - India: PAN
  - India: PAN (Wide)
- **Ireland Finance**  
Policy for detection of Irish financial information. The rules for this policy are:
  - Ireland Finance: Irish IBAN (Default)
  - Ireland Finance: Irish IBAN (Wide)
  - Ireland Finance: Irish Bank Account
- **Ireland PII**  
Policy for detection of Irish private information. The rules for this policy are:
  - Ireland PII: Irish Personal Public Service Number (PRSI/PPS) and Name
  - Ireland PII: Irish Driver Number and Name
  - Ireland PII: Irish Passport Number and Name
- **Israeli Bank Accounts**  
Policy for identifying Israeli bank account numbers in traffic. The rules for this policy are:
  - IL BANK: General Bank Account Numbers
  - IL BANK: Leumi Bank Account Numbers
  - IL BANK: Leumi Bank Account Numbers no support
  - IL BANK: Poalim Bank Account Numbers
  - IL BANK: Discount Bank Account Numbers
  - IL BANK: Mizrahi Bank Account Numbers
  - IL BANK: BenLeumi Bank Account Numbers
  - IL BANK: HaDoar Bank Account Numbers
- **Israel PII**  
Policy for detection of Israeli private information. The rules for this policy are:
  - Israel PII: Israeli ID - 7 or 8 digits with support
  - Israel PII: Israeli ID (Default)
  - Israel PII: Israeli ID (Default) + 7 or 8 digits
  - Israel PII: Israeli ID (Narrow)
  - Israel PII: Israeli ID (Wide)
  - Israel PII: Name and ID
- **Italy Finance**  
Policy for detection of Italian financial information. The rules for this policy are:
  - Italy Finance: Italian IBAN (Default)
  - Italy Finance: Italian IBAN (Wide)
- **Italy PII**

Policy for detection of Italian private information. The rules for this policy are:

- Italy PII: Codice Fiscale
- Italy PII: Name and Codice Fiscale
- Italy PII: Name and health information
- Italy PII: Codice Fiscale and health information

■ Japan PII

Policy for detection of Japanese private information. The rules for this policy are:

- Japan PII: Telephone Numbers
- Japan PII: Surname and Account
- Japan PII: Surname and Driver License.
- Japan PII: Surname and Pension Number
- Japan PII: Surname and Ledger Number
- Japan PII: E-mail Addresses

■ Macau PII

Policy for detection of Macau private information. The rules for this policy are:

- Macau PII: ID (formal form)
- Macau PII: ID (Default)
- Macau PII: ID (Narrow)

■ Malaysia PII

Policy for detection of Malaysian private information. The rules for this policy are:

- Malaysia PII: ID (formal form)
- Malaysia PII: ID formal form (Wide)
- Malaysia PII: ID w proximity (Default)
- Malaysia PII: ID w proximity
- Malaysia PII: ID (formal form) with BP
- Malaysia PII: ID (formal form) with BP w proximity
- Malaysia PII: Malaysian Name and sensitive health information

■ Mexico PII

Policy for detection of Mexican private information. The rules for this policy are:

- Mexico PII: RFC (Default)
- Mexico PII: RFC (Wide)
- Mexico PII: CURP (Default)
- Mexico PII: CURP (Narrow)
- Mexico PII: CPISP (Default)
- Mexico PII: CPISP (Narrow)
- Mexico PII: CPISP (Wide)
- Mexico PII: SSP Contratos Internos Detection (Default)
- Mexico PII: SSP Contratos Internos Detection (Wide)

■ Netherlands and Finance

Policy for identifying Dutch financial information. The rules for this policy are:

- Netherlands Finance: Netherlands IBAN (Default)

- Netherlands Finance: Netherlands IBAN (Wide)
- Netherlands PII  
Policy for detection of Dutch private information. The rules for this policy are:
  - Netherlands PII: Sofi and Ethnicities
  - Netherlands PII: Sofi and Account with Password
  - Netherlands PII: Sofi and CCN delimiters.
  - Netherlands PII: Sofi and Crime
  - Netherlands PII: Sofi and Diseases
  - Netherlands PII: Driver License Numbers
  - Netherlands PII: Passport Numbers
- New Zealand PII  
Policy for detection of New Zealand private information. The rules for this policy are:
  - New Zealand: NHI number (Wide)
  - New Zealand: NHI number (Default)
- Norway Finance  
Policy for identifying Norwegian financial information. The rules for this policy are:
  - Norway Finance: Norwegian IBAN (Default)
  - Norway Finance: Norwegian IBAN (Wide)
- Norway PII  
Policy for detection of Norwegian private information. The rules for this policy are:
  - Norway PII: Personal Number (Wide)
  - Norway PII: Personal Number
  - Norway PII: Personal Number (Narrow)
  - Norway PII: Name and Personal Number
  - Norway PII: Name and health information
- Password Dissemination  
Detects content suspected to be a password in clear text. The rules for this policy are:
  - Password dissemination
  - Password dissemination for web traffic
  - Password Dissemination: Common Passwords without term
- Peoples Republic of China  
Policy for detection of Peoples Republic of China private information. The rules for this policy are:
  - Peoples Republic of China PII: ID
  - Peoples Republic of China PII: Chinese CV
- Peoples Republic of China Finance  
Policy for detection of PRC financial information. The rules for this policy are:
  - Peoples Republic of China Finance: Union Pay Credit Card (Wide)
  - Peoples Republic of China Finance: Union Pay Credit Card (Default)
  - Peoples Republic of China Finance: Union Pay Credit Card (Narrow)
  - Peoples Republic of China Finance: Financial cards Track1

- Peoples Republic of China Finance: Financial cards Track2 rule for detecting bank card magnetic stripe Track2
- Peoples Republic of China Finance: Financial cards Track3
- Peoples Republic of China Finance: Business Registration Number - 15 digits (Wide)
- Peoples Republic of China Finance: Business Registration Number - 15 digits (Default)
- Peoples Republic of China Finance: Business Registration Number - 15 digits (Narrow)
- Peoples Republic of China Finance: Credit Card (Wide)
- Peoples Republic of China Finance: Credit Card (Default)
- Peoples Republic of China Finance: Credit Card (Narrow)
- Philippines PII  
Policy for detection of Philippines private information. The rules for this policy are:
  - Philippines PII: Name and Address (Wide)
  - Philippines PII: Name and Address (Default)
  - Philippines PII: Name and Address (Narrow)
- Poland Finance  
Policy for detection of Polish financial information. The rules for this policy are:
  - Poland Finance: Polish IBAN (Wide)
  - Poland Finance: Polish IBAN (Default)
  - Poland Finance: IBAN and Name
- Poland PII  
Policy for detection of Polish private information. The rules for this policy are:
  - Poland: NIP numbers
  - Poland: NIP with proximity
  - Poland: NIP and Name
  - Poland: PESEL numbers
  - Poland: PESEL with proximity
  - Poland: PESEL and Name
  - Poland: Polish ID numbers
  - Poland: Polish ID with proximity
  - Poland: REGON numbers
  - Poland: REGON with proximity
  - Poland: REGON and Name
- Romania PII  
Policy for detection of Romanian private information. The rule for this policy is:
  - Romania PII: Personal numeric code
- Russia PII  
Policy for detection of Russian private information. The rules for this policy are:
  - Russia PII: Moscow Social Card Number near Serial Numbers
  - Russia PII: Moscow Social Card Numbers (Default)
  - Russia PII: Moscow Social Card Numbers (Wide)
  - Russia PII: Russian Classification on Objects of Administrative (Wide)
  - Russia PII: Russian Classification on Objects of Administrative Division (Default)

- Russia PII: Russian Individual Personal Account Insurance (Wide)
- Russia PII: Russian Individual Personal Account Insurance Numbers (Default)
- Russia PII: Russian passport and name (Default)
- Russia PII: Russian passport and name (Narrow)
- Russia PII: Russian passport and name (Wide)
- Russia PII: Russian passport number
- Russia PII: Russian Phone Numbers (Default)
- Russia PII: Russian Phone Numbers (Narrow)
- Russia PII: Russian Phone Numbers (Wide)
- Russia PII: Russian Primary State Registration Numbers - 13-digits (Default)
- Russia PII: Russian Primary State Registration Numbers - 13-digits (Wide)
- Russia PII: Russian Primary State Registration Numbers - 15-digits (Default)
- Russia PII: Russian Primary State Registration Numbers - 15-digits (Wide)
- Russia PII: Russian Taxpayer Identification Numbers - 10-digits (Default)
- Russia PII: Russian Taxpayer Identification Numbers - 10-digits (Wide)
- Russia PII: Russian Taxpayer Identification Numbers - 12-digits (Default)
- Russia PII: Russian Taxpayer Identification Numbers - 12-digits (Wide)
- Russia PII: Russian Unified Classifier of Enterprises and Organizations
  
- Saudi Arabia Finance  
Policy for detection of Saudi Arabia financial information. The rules for this policy are:
  - Saudi Arabia Finance: Saudi Arabia IBAN (Default)
  - Saudi Arabia Finance: Saudi Arabia IBAN (Wide)
  
- Singapore PII  
Policy for detection of Singaporean private information. The rules for this policy are:
  - Singapore PII: Singapore Identification numbers
  - Singapore PII: Singapore Identification numbers - No support terms
  - Singapore PII: Singapore Identification numbers with Credit Card
  - Singapore PII: Name and Address (Default) (starting with v7.8.2)
  - Singapore PII: Name and Address (Narrow) (starting with v7.8.2)
  
- Slovakia PII  
Policy for detection of Slovak private information. The rule for this policy is:
  - Slovakia PII: Rodne Cislo (Wide)
  - Slovakia PII: Rodne Cislo (Default)
  
- Social Insurance Numbers  
Detects valid Canadian Social Insurance Numbers (SIN). The rules for this policy are:
  - SIN (Wide)
  - SIN (Default)
  - SIN (Narrow)
  
- Social Security Numbers  
Policy for detection of validated social security numbers. The rules for this policy are:
  - US SSN (Wide)
  - US SSN (Default)

- US SSN (Narrow)
- US SSN Wide Minus Default
- US SSN - not masked
- SSN: ITIN
  
- South Africa PII  
Policy for detection of South African private information. The rules for this policy are:
  - South Africa PII:SA ID (Wide)
  - South Africa PII:SA ID (Default)
  - South Africa PII:SA ID (Narrow)
  - South Africa PII: SA Name and Sensitive Health information
  
- South Korea PII  
Policy for detection of South Korean private information. The rules for this policy are:
  - South Korea PII: DNA profile
  - South Korea PII: Korea Phones (Default)
  - South Korea PII: Korea Phones (Wide)
  - South Korea PII: Korea Phones (with proximity)
  - South Korea PII: South Korea ID (Default)
  - South Korea PII: South Korea ID (Wide)
  - South Korea PII: South Korea ID (with proximity)
  
- Spain Finance  
Policy for detection of Spanish financial information. The rules for this policy are:
  - Spanish IBAN rule for detecting Spanish IBANs (Default)
  - Spanish IBAN rule for detecting Spanish IBANs (Wide)
  
- Spain PII  
Policy for detection of Spanish private information. The rules for this policy are:
  - Spain PII: DNI and Account with Password
  - Spain PII: DNI and CCN
  - Spain PII: DNI and Crime
  - Spain PII: DNI and Diseases
  - Spain PII: DNI and Ethnicities
  - Spain PII: Spanish Name + Address (Default)
  - Spain PII: Spanish Name + Address (Narrow)
  - Spain PII: Spanish Name + CCN
  - Spain PII: Spanish Name + DNI
  - Spain PII: Spanish Name + IBAN
  - Spain PII: Spanish Name + Passport
  - Spain PII: Spanish Names + Email Addresses
  - Spain PII: Spanish Names + Phone Numbers
  
- Sweden Finance  
Policy for detection of Swedish financial information. The rules for this policy are:
  - Sweden Finance: Swedish IBAN (Default)
  - Sweden Finance: Swedish IBAN (Wide)

- Sweden PII  
Policy for detection of Swedish private information. The rules for this policy are:
  - Sweden PII: ID (Wide)
  - Sweden PII: ID (Default)
- Switzerland Finance  
Policy for detection of Swiss financial information. The rules for this policy are:
  - Switzerland Finance: Swiss IBAN (Default)
  - Switzerland Finance: Swiss IBAN (Wide)
- Switzerland PII  
Policy for detection of Swiss private information. The rules for this policy are:
  - Switzerland PII: Old format AHV
  - Switzerland PII: new format AHV
- Taiwan PII  
Policy for detection of Taiwanese private information. The rules for this policy are:
  - Taiwan PII: ID
  - Taiwan PII: ID formal form
  - Taiwan PII: ID formal form with Surname
  - Taiwan PII: ID formal form with Surname and Private info
  - Taiwan PII: ID with Surname
  - Taiwan PII: ID with Surname and Private info
  - Taiwan PII: Surname and address
  - Taiwan PII: Taiwan Address (Default)
  - Taiwan PII: Taiwan Address (Narrow)
  - Taiwan PII: Taiwan Address (Wide)
- Thailand PII  
Policy for detection of Thai private information. The rules for this policy are:
  - Thailand: National ID (Wide)
  - Thailand: National ID (Default)
- Turkey Finance  
Policy for detection of Turkish financial information. The rules for this policy are:
  - Turkey Finance: Turkish IBAN (Default)
  - Turkey Finance: Turkish IBAN (Wide)
  - Turkey Finance: Turkish Tax IDs (Wide)
  - Turkey Finance: Turkish Tax IDs (Default)
- Turkey PII  
Policy for detection of Turkish private information. The rules for this policy are:
  - Turkey PII: TC Kimlik
  - Turkey PII: TC Kimlik one support
- UK Finance  
Policy for detection of UK financial information. The rules for this policy are:
  - UK Finance: UK IBAN (Default)
  - UK Finance: UK IBAN (Wide)

- UK PII

Policy for detection of UK private information. The rules for this policy are:

- UK PII: Bank Account number and Name
- UK PII: NHS Numbers (Default)
- UK PII: NHS Numbers (Narrow)
- UK PII: NHS Numbers (Wide)
- UK PII: Postal Code and Name (Default)
- UK PII: Postal Code and Name (Narrow)
- UK PII: Sort Code and Name
- UK PII: UK Driver Number and Name
- UK PII: UK Driver Number and Name (Wide)
- UK PII: UK National Insurance Number and Name
- UK PII: UK Passport Number and Name
- UK PII: UK Tax ID Number and Name

- US PII

Policy for detection of US private information. The rules for this policy are:

- US PII: DNA profile (Default)
- US PII: DNA profile (Narrow)
- US PII: Name + Arizona DL
- US PII: Name + Arkansas DL
- US PII: Name + California DL
- US PII: Name + Colorado DL
- US PII: Name + Connecticut DL
- US PII: Name + Crime
- US PII: Name + District of Columbia DL
- US PII: Name + Ethnicity
- US PII: Name + Florida DL
- US PII: Name + Georgia DL
- US PII: Name + Illinois DL
- US PII: Name + Illinois State ID
- US PII: Name + Indiana DL
- US PII: Name + Iowa DL
- US PII: Name + Massachusetts DL
- US PII: Name + Michigan DL
- US PII: Name + Minnesota DL
- US PII: Name + Nevada DL
- US PII: Name + New Jersey DL
- US PII: Name + New York DL
- US PII: Name + North Carolina DL
- US PII: Name + Ohio DL
- US PII: Name + Pennsylvania DL
- US PII: Name + Texas DL



- US PII: Name + US Address
- US PII: Name + Utah DL
- US PII: Name + Virginia DL
- US PII: Name + Washington DL
- US PII: Name + Wisconsin DL
- US PII: SSN
- US PII: SSN + Name

## Protected Health Information (PHI)

---

- Australian PHI  
Policy for detection of protected health information for Australian citizens. The rules for this policy are:
  - Australia PHI: Australia Medicare and Sensitive Disease or drug
  - Australia PHI: Australia Medicare and Common Disease
  - Australia PHI: SPSS Text files
- Health Data  
Policy for detection of data types pertaining to medical conditions, drugs etc. The rules for this policy are:
  - Health Data: Credit cards and Common Diseases
  - Health Data: Credit cards and Sensitive Disease or drug
  - Health Data: DNA profile (Default)
  - Health Data: DNA profile (Narrow)
  - Health Data: DOB and Name
  - Health Data: ICD10 Code and Description
  - Health Data: ICD10 Codes
  - Health Data: ICD10 Codes and US full names
  - Health Data: ICD10 Descriptions and US full names
  - Health Data: ICD9 Code and Description
  - Health Data: ICD9 Codes
  - Health Data: ICD9 Codes and US full names
  - Health Data: ICD9 Descriptions and US full names
  - Health Data: Medical Form (Default)
  - Health Data: Medical Form (Narrow)
  - Health Data: Medical Form (Wide)
  - Health Data: Name and Common Diseases
  - Health Data: Name and Sensitive Disease or drug
  - Health Data: Names (Narrow) and Common Diseases
  - Health Data: Names (Narrow) and Sensitive Disease or drug
  - Health Data: NDC number (Default)
  - Health Data: NDC number (Narrow)
  - Health Data: NDC number (Wide)

- **Israel PHI**  
Policy for detection of protected health information for Israeli citizens, to promote compliance with Israeli privacy rules and Israeli patients rights law of 1996. The rules for this policy are:
  - Israel PHI: ID and Sensitive Medical info
  - Israel PHI: Name and Sensitive Medical info
  - Israel PHI: ID and General Medical info
  - Israel PHI: Name and General Medical info
  - Israel PHI: SPSS Text files
- **Italy PHI**  
Policy for detection of protected health information for Italy citizens. The rules for this policy are:
  - Italy PHI: Name and health information
  - Italy PHI: Codice Fiscale and health information
  - Italy PHI: SPSS Text files
- **Norway PHI**  
Policy for detection of protected health information for Norwegian citizens. The rules for this policy are:
  - Norway PHI: Name and health information
  - Norway PHI: Personal Number and health information
  - Norway PHI: ICD10 Codes
  - Norway PHI: ICD10 Code and Description
  - Norway PHI: ICD10 Descriptions
  - Norway PHI: ICD10 Code and first Name
  - Norway PHI: ICD10 Code and Last Name
  - Norway PHI: ICD10 Code and Full Name
  - Norway PHI: ICD10 Code and PIN number
  - Norway PHI: ICD10 Code and Personal number
  - Norway PHI: SPSS Text files
- **Sweden PHI**  
A policy for detection of protected health information (PHI) of Swedish citizens and residents. The policy comprises rules for detection of Health information and Medical Conditions (in Swedish or English), in proximity to personally identifiable information such as personal number (personnummer), or name. The rules for this policy are:
  - Sweden PHI: DNA profile
  - Sweden PHI: ICD10 Code and Description
  - Sweden PHI: ICD10 Code and Name
  - Sweden PHI: ICD10 Code and Name (Narrow)
  - Sweden PHI: ICD10 Code and Name (Wide)
  - Sweden PHI: ICD10 Code and Personal Number
  - Sweden PHI: ICD10 Codes
  - Sweden PHI: ICD10 Descriptions
  - Sweden PHI: Name and health information
  - Sweden PHI: Name and Sensitive Disease or drug
  - Sweden PHI: Personal Number and health information
  - Sweden PHI: Personal Number and Sensitive Disease or drug

- UK PHI  
Policy for detection of UK NHS numbers. The rules for this policy are:
  - UK PHI: NHS Numbers (Wide)
  - UK PHI: NHS Numbers (Default)
  - UK PHI: NHS Numbers (Narrow)
  - UK PHI: SPSS Text files
- US PHI  
A policy for detection of protected health information of US citizens. The rules for this policy are:
  - US PHI: Name and Common Diseases
  - US PHI: Name and HICN
  - US PHI: Name and Sensitive Disease or drug
  - US PHI: Names (Narrow) and Common Diseases
  - US PHI: Names (Narrow) and Sensitive Disease or drug
  - US PHI: SPSS Text files
  - US PHI: SSN and Common Diseases
  - US PHI: SSN and Sensitive Disease or drug

## Payment Card Industry (PCI)

---

Policy for promoting compliance with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an industry standard, accepted internationally by all major credit card issuers and is enforced on companies and organizations that accept credit card payments or process, store, or transmit cardholder data. The standard includes the mandate that credit card numbers and cardholder data should be highly secured and that transactions comprising PCI data should be encrypted.

The rules for this policy are:

- Credit card magnetic strips
- Valid credit card numbers (Wide)
- Valid credit card numbers, with proximity (Default)
- Valid credit card numbers, with proximity (Narrow)

## Data Theft

---

The cloud service includes the following data theft policies. The rules for these policies are:

- Common password information  
Searches for outbound passwords in plain text.
  - Common passwords information
  - Common passwords information (Wide)
  - Common passwords information (Narrow)
- Encrypted files - known format  
Searches for outbound transactions comprising common encrypted file formats. The rule for this policy is:

- Encrypted files (known format)
- Encrypted file: encrypted data of unknown format  
Policy for detection of encrypted files of unknown format. The rule in this policy is:
  - Encrypted file: encrypted data of unknown format
- IT asset information  
Searches for suspicious outbound transactions, such as those containing information about the network, credit card magnetic tracks, and database files. Rules in this policy include:
  - Suspicious content
  - Suspicious content (Narrow)
  - Suspicious content (Wide)
- Malware communication  
Identifies traffic that is thought to be malware “phoning home” or attempting to steal information. Detection is based on the analysis of traffic patterns from known infected machines. Rules in this policy include:
  - Malware communication (Default)
  - Malware communication (Narrow)
- Password files  
Searches for outbound password files, such as a SAM database and UNIX / Linux passwords files. Rules in this policy include:
  - Password Files: Shadow Files
  - Password Files: Shadow Files (Wide)
  - Password Files: Password Files
  - Password Files: Password Files (Wide)
  - Password Files: SAM files
  - Password Files: General files

