



**Forcepoint CASB**  
Administration Guide

© 2021 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 2021

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this document 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 document or the examples herein. The information in this document is subject to change without notice.

Last modified: **19-Dec-2021**



# CONTENTS

## CHAPTER 1 Preface

## CHAPTER 2 Overview

Introducing Forcepoint CASB .....	3
The Forcepoint CASB workflow .....	4
The Forcepoint CASB workspace .....	6
System architecture .....	9
Gateway enforcement .....	11
Accessing the Forcepoint CASB management portal .....	13
Logging in to Forcepoint CASB .....	13
Logging out of Forcepoint CASB .....	14

## CHAPTER 3 Discovery and Asset Management

Setting up discovery .....	16
Installing and configuring the Cloud Discovery tool .....	16
Scanning for discovery .....	19
Scheduling automatic scans .....	21
Scan automation on Linux .....	23
Uploading scan results .....	24
Upgrading or uninstalling the Cloud Discovery tool .....	25
Monitoring organizational cloud access .....	28
The Discovery dashboard .....	28
Investigating accessed applications .....	34
Application risk analysis .....	37
Acknowledging accessed applications .....	39
Restricting application access .....	41
Investigating apps through the Cloud App Directory .....	44

## CHAPTER 4 Activity Analysis and Investigation

Activity audit types .....	48
----------------------------	----

Monitoring real-time activities .....	48
Monitoring service provider log activities .....	49
About the activity impact score .....	51
Monitoring and investigating user activities .....	53
Investigating activity logs .....	53
Graphically investigating activities .....	60

## CHAPTER 5 Understanding Forcepoint CASB Policies

Access policies .....	64
Enabling user access policies .....	64
Configuring user activity policies .....	66
Anomaly detection policies .....	70
The anomaly detection policies table .....	70
Enabling or disabling a policy from the anomaly detection policy table .....	70
Excluding users from an anomaly detection policy .....	70
Setting notifications for an anomaly detection policy .....	71
Configuring anomaly detection policies .....	72
Data leak prevention policies .....	75
Configuring data leak prevention policies .....	75
Custom policies .....	79
The custom policy table .....	79
Enabling or disabling a custom policy from the custom policy table .....	80
Configuring custom policies .....	80
Excluding users from a custom policy .....	86
Setting notifications for a custom policy .....	87
Deleting a custom policy .....	88
Custom access policy predicates .....	88

## CHAPTER 6 Security Monitoring and Enforcement

Monitoring and investigating security .....	94
Policy violations .....	94
Security activity analysis .....	97
Security detail widgets .....	98

## CHAPTER 7 Monitoring and Investigating Alerts and Incidents

The Incidents log .....	102
Incidents log column descriptions .....	106
Incident records .....	109
Handling policy violations .....	112

## CHAPTER 8 User Behavior Analysis

Machine learning-based anomaly detection using Forcepoint CASB .....	115
Activity auditing and user profile .....	115
User risk .....	116
Monitoring user risk .....	118
Users at Risk .....	118
Top High Risk Users .....	119
Watchlist .....	119
Organizational Behavior .....	120
Top Business Units at Risk .....	120
Organizational Geographic Risk .....	120
Investigating accounts .....	122
The Accounts table .....	122
Accounts table column descriptions .....	125
The Account summary .....	127
The Detailed Account page .....	130

## CHAPTER 9 Governance and Compliance

Account access and security governance .....	138
Monitoring account access and security .....	138
Managing account access and security remediation .....	142
Configuring the governance policy .....	145
Data classification .....	149
The Data Classification dashboard .....	149
Data Classification reports .....	150
Investigating stored sensitive files .....	152
File Analytics table column descriptions .....	160
Configuring Data Classification policies .....	163

## CHAPTER 10 Encryption Broker

Managing the data encryption policy .....	172
Configuring the data encryption policy .....	172
Setting a key rotation plan .....	174
Exporting active keys .....	176
Disabling and enabling a data encryption policy .....	176
Resetting a data encryption policy .....	177
Monitoring encryption-based events .....	179
The data encryption audit log .....	179

## CHAPTER 11 Forcepoint CASB System Administration

Providing a user directory .....	182
Manually uploading a user directory .....	182
Configuring Active Directory retrieval .....	185
Setting up Active Directory Agent retrieval .....	189
Creating an LDAPS TrustStore for the Active Directory Agent .....	193
Configuring Forcepoint CASB administration .....	195
Configuring administrator accounts and permissions .....	195
Configuring administrator account security settings .....	202
Configuring administrator single sign-on .....	206
Configuring account privacy .....	208
Stopping account monitoring .....	208
Deleting an account .....	210
Restarting account monitoring .....	212
Managing your key management services .....	213
Adding a new key management service .....	213
Generating a new key .....	215
Deleting a key .....	216
Deleting a key management service .....	217
Managing REST API connections .....	218
Enabling API access .....	218
Disabling API access .....	218
Managing API access keys .....	219
Endpoint enrollment .....	224
Configuring endpoint enrollment .....	224
Customizing the enrollment form and URL .....	226
Administrative enrollment, approval and revocation .....	227
Configuring internal domains .....	231
Configuring IP ranges .....	233
Importing IP ranges .....	234
Exporting IP ranges .....	236
Configuring trusted proxies .....	237
Configuring trusted IP addresses for IP Reputation .....	238
About IP Reputation .....	238
Configuring trusted IP addresses .....	238
Configuring notifications .....	239
Configuring an SMS notification .....	239
Configuring an email notification .....	242
Notification message variables .....	246

Configuring data types .....	249
Data type syntax .....	249
Data type examples .....	250
Adding a custom data type to Forcepoint CASB .....	253
Configuring an ICAP connection .....	255
Adding a new ICAP connection .....	255
Creating a DLP Policy .....	257
Setting up a secure tunnel using stunnel .....	257
Setting up SIEM / syslog integration .....	259
Activities and alerts CEF mapping .....	262
Incidents CEF mapping .....	265
Downloading Tools and Agents .....	267
Licensing .....	268

## CHAPTER 12 Managing Service Assets

Creating an asset .....	270
Configuring asset governance connections .....	278
Configuring a web connection .....	279
Configuring an API connection .....	280
Customizing access enforcement .....	283
Customizing account and activity blocking .....	283
Customizing identity verification .....	284
Updating Forcepoint CASB asset data .....	287
Configuring a custom asset .....	288

## CHAPTER 13 Setting up Gateway Enforcement

Setting up reverse proxy (IdP Proxy) .....	290
IdP proxy overview .....	290
Using Forcepoint CASB as a single sign-on identity provider .....	291
Configuring IdP proxy .....	294
Configuring IdP proxy for Office 365 .....	300
Setting up endpoint routing solutions .....	305
Deploying the Forcepoint CASB Security Service .....	305
Automated PAC file distribution .....	309
Testing and troubleshooting endpoint routing solutions .....	312
Blocking unmanaged service applications .....	314



# CHAPTER 1

## Preface

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

This Administration Guide contains all the information necessary for ongoing use of Forcepoint CASB, including monitoring and analyzing user activity using the management portal, setting up cloud discovery and service asset protection, and system administration.

For information about initially setting up Forcepoint CASB for your organization, please contact your reseller or Forcepoint support.

Some Forcepoint CASB features are independently licensed. If any features described in this guide are unavailable in your Forcepoint CASB deployment, please contact your reseller or the Forcepoint sales team to extend your license.





## Overview

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

This chapter introduces Forcepoint CASB and the high-level concepts you need to get started with it.

This chapter discusses the following:

Introducing Forcepoint CASB .....	3
The Forcepoint CASB workflow .....	4
The Forcepoint CASB workspace .....	6
System architecture .....	9
Gateway enforcement .....	11
Accessing the Forcepoint CASB management portal .....	13

# Introducing Forcepoint CASB

---

Forcepoint CASB is an integrated solution for cloud application access discovery, user behavior analysis, activity analysis, access control, security monitoring and enforcement, governance, policy compliance, and data loss prevention.

Cloud applications provide significant advantages to organizations, but also incur risks to IT control, security, and compliance. Traditional perimeter and endpoint controls do not properly identify cloud access activity and provide little or no control over information access, application access, and privileged activities. To make cloud application use safe and productive, Forcepoint CASB provides these visibilities and controls, in addition to monitoring and preventing account security breaches and policy violations.

# The Forcepoint CASB workflow

---

Forcepoint CASB enables you to perform the following main high-level functions:

- ▶ **Discovery** (see ["Discovery and Asset Management" on page 15](#)): Scan network log files to see all active cloud accounts, with usage metrics and risk information for found cloud applications. Eliminate shadow IT by bringing found applications into the Forcepoint CASB system as managed assets, enabling the additional functions listed below.
- ▶ **User behavior analysis and risk analysis** (see ["User Behavior Analysis" on page 114](#)): Scan network log files to identify high risk users and related threats to your organization. UBA reduces security management costs and improves security team focus by:
  - Understanding the typical user through automatic user behavior profiling and comparing that to your approved business flows.
  - Automatically detecting deviations from typical behavior and using that to improve your policy accuracy.
  - Focusing your attention on the key users at risk, highlighted by Forcepoint CASB based on smart risk calculation.
  - Understanding your risk by following a quick investigative flow to get all of the information you need on a high-risk user, including usage patterns, activities, incidents, and more.
- ▶ **Access monitoring and enforcement** (see ["Security Monitoring and Enforcement" on page 93](#)): Configure access policies to managed assets, without needing to rely on applications' native permission systems which in some cases can be limited or insecure.
- ▶ **Threat and risk detection and prevention** (see ["Security Monitoring and Enforcement" on page 93](#)): For managed assets, detect user account behavior that is anomalous relative to automatically-learned usual behavior, according to preconfigured and configurable policies. Optionally, threat detection can trigger automatic account blocking.
- ▶ **Activity analysis** (see ["Activity Analysis and Investigation" on page 47](#)): For applications that have been configured as managed assets, obtain in-depth visibility into organizational cloud user activities. You can investigate these activities according to various parameters, including action types, business units, accessed data types, administrative activity, suspicious activity, user accounts, endpoints, geographical locations and more. Filtered activity lists can be exported for further analysis and for compliance.
- ▶ **Access and Security Governance** (see ["Account access and security governance" on page 138](#)): For managed assets, assess risk by monitoring account compliance with regulatory standards and with organizational policy regarding user accounts and user authentication settings.

- ▶ **Data Classification** (see "[Data classification](#)" on page 149): For managed assets, Forcepoint CASB scans the contents of stored files and provides detailed information about stored sensitive material – as defined by configurable [data types](#) – including how it is accessed and shared inside and outside the organization.

# The Forcepoint CASB workspace

Forcepoint CASB administrators work in two environments:

- ▶ Forcepoint CASB management portal
- ▶ Forcepoint CASB Cloud Discovery tool

The main Forcepoint CASB work environment is the **Forcepoint CASB management portal**. The management portal includes dashboards for user risk analysis, cloud access discovery, compliance, and activity analysis and security monitoring. The portal also includes tools for investigating endpoints, policy configuration, and system configuration.

The management portal includes four main dashboards, and additional pages for further investigation and configuration:



The dashboards are:

- ▶ **Risk Summary** (see "[User Behavior Analysis](#)" on page 114): The Risk Summary page is the default page that appears upon login.  
For supported cloud services that have been defined as managed assets, includes:
  - **User Risk dashboard**: Displays a high-level view of user activity, including risks to your organization, with drill-down to accounts and the watchlist.
  - **Accounts**: Displays user accounts, including current and recent activity and alert details, with drill-down to incidents and audit logs.
- ▶ **App Discovery** (see "[Discovery and Asset Management](#)" on page 15), including:
  - Scan results from the Discovery tool (described below), with details on all active cloud accounts, including usage metrics and risk information for found cloud applications.
  - Configurable parameters for the above risk information.
  - Tools for bringing found applications into the Forcepoint CASB system as managed assets, upon which they will appear in the other dashboards as well.
- ▶ **Compliance** (see "[Governance and Compliance](#)" on page 137): For supported cloud services that have been defined as managed assets, includes:
  - **Data Classification** (see "[Data classification](#)" on page 149): For managed assets, Forcepoint CASB scans the contents of stored files and provides detailed information

about stored sensitive material – as defined by configurable [data types](#) – including how it is accessed and shared inside and outside the organization.

- **Governance** (see ["Account access and security governance" on page 138](#)): Displays information about user accounts that should be removed or validated, and violations of configurable regulatory standards and organizational policy.
- **Encryption Broker** (see ["Encryption Broker" on page 170](#)): For managed assets, the Encryption Broker service leverages a bring your own key (BYOK) capability offered by the cloud services. Forcepoint CASB connects to your key management service (KMS) to access your encryption keys, then connects to the cloud service, where the data is encrypted and decrypted based on the key provided by Forcepoint CASB from the KMS.

The Encryption Broker service also helps with regulatory compliance by maintaining and rotating the encryption keys from within Forcepoint CASB.

- ▶ **Audit & Protect** (see ["Security Monitoring and Enforcement" on page 93](#)): For applications that have been defined as managed cloud assets, the Audit & Protect dashboard provides visibility into the user activities performed on the cloud asset. The dashboard displays summaries and details of alerts including threats, risks, and violated policies, with drill-down to Accounts for further investigation. It also includes some general activity summaries.

- **Activity Audit** (see ["Activity Analysis and Investigation" on page 47](#)): Activity audit logs identify activity details such as source devices, source locations, and actions (for example, password change or data modification). Using this information, Forcepoint CASB provides various activity summaries and tools for investigating organizational user activities in cloud services according to various parameters. Filtered activity lists can be exported for further analysis and compliance.

Other management portal pages (for example, **Security** and **Accounts**) provide links to the Audit Logs, automatically filtered according to the relevant context.

- **Incidents** (see ["Alert and Incident Analysis and Investigation" on page 1](#)): Forcepoint CASB analyzes alerts for similarities and combines these similar alerts into an Incident. Incidents let you quickly see and understand the overall problems affecting your network. The Incidents log displays a summary of the Incidents captured, and the Incident records display details information about the incident, including user information and a log of all alerts attached to the incident.

Other management portal pages (for example, **User Risk** and **Accounts**) provide links to the Incidents log, automatically filtered according to the relevant context.

The **Endpoints** page displays details of devices used to connect to managed assets, separately listing devices managed by the organization and unmanaged devices, with drill-down to Accounts. The Endpoints page also enables administrative approval or revocation of device enrollment (see ["Administrative enrollment, approval and revocation" on page 227](#)).

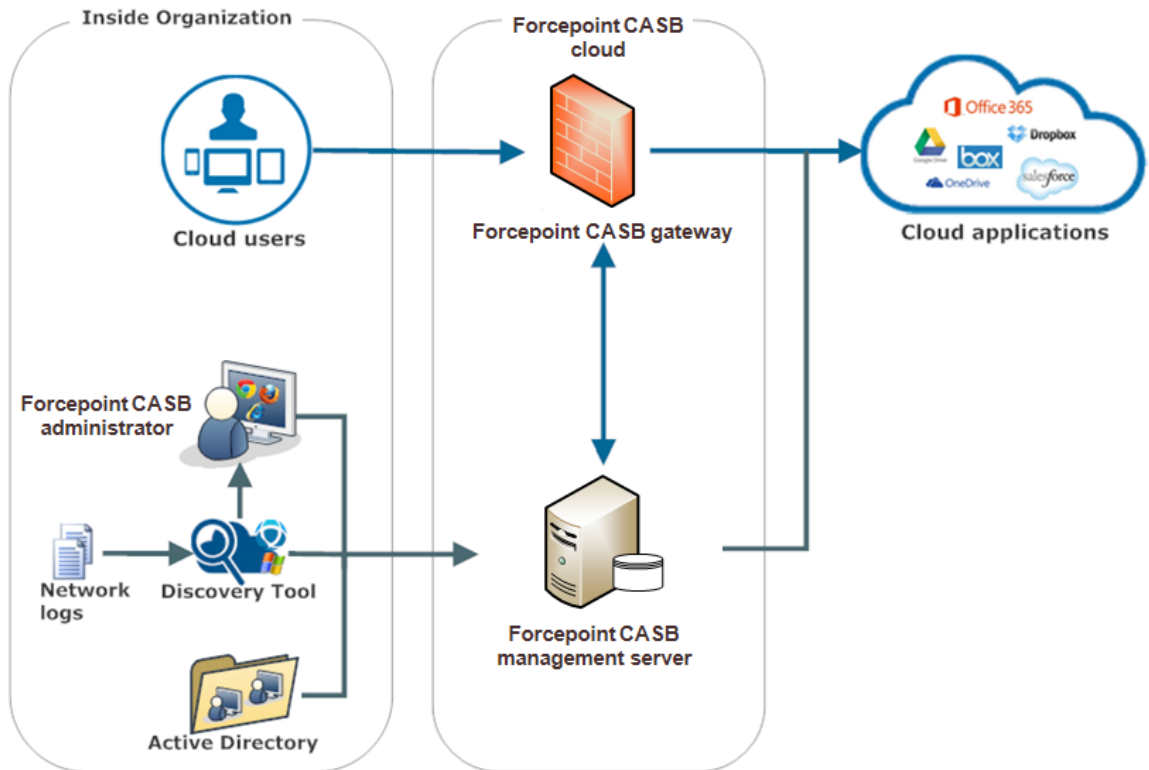
Additional pages allow managing endpoint, configuring system settings, and viewing Help contents.

In addition to the management portal, for initial cloud access discovery, Forcepoint CASB provides the Cloud Discovery tool (see "[Setting up discovery](#)" on page 16), which scans network log files from any device such as a firewall, web proxy, SIEM, or router, and produces details on all active cloud accounts, including usage metrics and risk information for found cloud applications. You can view scan results locally in a produced PDF, or, after the results are uploaded to the Forcepoint CASB management server, in the Forcepoint CASB web interface, where they are more interactive and from where you can bring accessed applications into the Forcepoint CASB system as managed assets.

For scan results to appear in the management portal, they need to be manually or automatically uploaded to the Forcepoint CASB management server. If you configure the Discovery tool to periodically perform automated scans and to automatically upload scan results to the management server, you can subsequently work solely in the Forcepoint CASB web interface.

# System architecture

Forcepoint CASB includes the following main components:



- ▶ **Forcepoint CASB gateway:** The gateway acts as a proxy between organizational users and cloud applications, monitors cloud account activities, and enforces organizational policy. It receives policy decisions from, and submits activity logs to, the Forcepoint CASB management server.

The Forcepoint CASB gateway runs as a virtual appliance, and is hosted and managed by Forcepoint.

- ▶ **Forcepoint CASB management server:** The management server serves the Forcepoint CASB management portal, determines policy application to the gateway, performs analysis, and creates alerts. It also collects account settings and user information directly from cloud applications (for Governance). The management server includes a database that stores all relevant information, including policy, system settings, and activities.



The Forcepoint CASB management server is hosted by Forcepoint. You connect to the management server through the cloud, so you do not install it on-premises.

- ▶ **Cloud Discovery Tool:** A local Windows application that scans network logs and provides Discovery results directly and/or to the management server.

In addition to the above components, Forcepoint CASB provides two agent applications for relevant scenarios:

- ▶ **Endpoint agent** (see ["Gateway enforcement" on the next page](#)): For routing relevant endpoint connections to the Forcepoint CASB gateway.
- ▶ **Active Directory (AD) agent** (see ["Providing a user directory" on page 182](#)): In deployments where the management server cannot access the organizational Active Directory (for example, the management server is in the Forcepoint CASB cloud), the AD agent can be installed locally to access Active Directory and relay the information to the management server (see ["Providing a user directory" on page 182](#)).

# Gateway enforcement

---

From existing organizational logs, Forcepoint CASB can identify accessed cloud applications, and by collecting information directly from cloud accounts, it can provide Governance features. However, these sources do not enable monitoring specific activities. For cloud applications to become fully monitored managed assets, access to cloud applications needs to go through the organizational Forcepoint CASB gateway. After configuring an application as a managed asset (see ["Managing Service Assets" on page 269](#)), you'll configure the Forcepoint CASB gateway to act as a proxy between the client applications and the cloud application servers, so that the gateway can fully monitor activity details and enforce organizational policies, enabling full user behavior analysis (see ["User Behavior Analysis" on page 114](#)), activity analysis (see ["Activity Analysis and Investigation" on page 47](#)) and security monitoring and enforcement (see ["Security Monitoring and Enforcement" on page 93](#)).

For cloud user activities to go through the Forcepoint CASB gateway, browsers and other client applications need be directed to the gateway URLs. Using the gateway URLs can be enforced in either or both of two ways:

- ▶ **Reverse proxy** (= server-side enforcement): Configure cloud applications to accept service requests for the relevant account(s) only from the Forcepoint CASB gateway. This can be done for each cloud application in either of two ways:
  - **IdP proxy**: Configure the application to authenticate users by an external single sign-on Identity Provider (SSO IdP; a third-party IdP, which might already be configured for your organization, or Forcepoint CASB can itself be the IdP), and configure the IdP to redirect via Forcepoint CASB. Upon authentication, the IdP redirects the connection (with identity assertion) via Forcepoint CASB.
  - **IP restriction**: For cloud applications that enable this, configure accounts to accept service requests only from the gateway's IP address.

Reverse proxy provides a secure solution by disabling non-gateway connections to cloud assets. However, non-browser client applications, such as most Office 365 desktop applications and most mobile client applications, can only access their native server URL. If only reverse proxy is used, these applications will not work.

- ▶ **Endpoint routing**: Set up organizational endpoints so that their outgoing connections to asset destinations are automatically routed via the gateway.

The recommended method of endpoint routing for desktop endpoints is installing the Forcepoint CASB Security Service on organizational endpoints. The Forcepoint CASB Security Service (also known as the Forcepoint CASB Endpoint agent) automatically routes connections from all browsers and applications on an endpoint to their destinations via the Forcepoint CASB gateway. The Forcepoint CASB Security Service has an

extremely low resource impact and merges its routing functionality with existing organizational proxy settings to provide a seamless user experience. The service is maintained with a watchdog service.

Endpoint routing provides a good solution for controlled organizational devices, including for applications that do not support URL changes, but does not disable non-gateway connections from other devices.

A comprehensive solution recommended in many cases is to use both types of solutions in parallel (supported by Forcepoint CASB): Implement reverse proxy as the primary enforcement method, and distribute the Forcepoint CASB endpoint routing solutions as needed for applications that cannot otherwise be directed to the Forcepoint CASB gateway.

# Accessing the Forcepoint CASB management portal

---

Upon deployment, Forcepoint CASB is configured with a single administrative account. Forcepoint creates the new administrator based on your organization's domain and provides the access credentials as part of the purchase fulfillment email. To configure additional accounts and permissions, see ["Configuring Forcepoint CASB administration" on page 195](#).

## Logging in to Forcepoint CASB

To access the Forcepoint CASB management portal, go to the Forcepoint CASB management server URL in your browser, then log in using the credentials provided to you by your administrator.

When you log in for the first time, Forcepoint CASB displays an End User License Agreement (EULA). Read the EULA, select the **I have read and agree to these terms** check box, then click the **Confirm EULA** button.

If your organization has set up a system notification, it is displayed to you after you enter your login credentials. You must acknowledge this notification to access the management portal.

## Locking a Forcepoint CASB account


When you attempt to log in to Forcepoint CASB, you may receive a message stating that you cannot log in. This can happen for the following reasons:

- ▶ **Too many unsuccessful login attempts.** If you enter an incorrect password too many times within a specific time period, you are locked out of the account. The number of attempts and timeout period are configured on the Administrator Account Security settings page. For more information, see ["Configuring login lockout restrictions" on page 203](#).
- ▶ **The password expired:** Administrator passwords can be set to expire after a specific number of days. This setting is configured on the Administrator Account Security settings page. After the setting is enabled, you can set the active time period (between 30 and 180 days) and set up email notifications. For more information, see ["Configuring password restrictions" on page 202](#).
- ▶ **The account has not been accessed within a set number of days:** If you do not log in to your account within a specific time period, the account is locked because of inactivity. This setting is configured on the Administrator Account Security settings page. For more information, see ["Configuring login lockout restrictions" on page 203](#).

## Changing your password

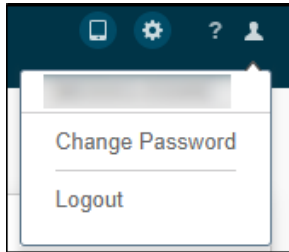
If your password has expired, or your password was reset by another administrator, you are prompted to change your password after you log in. Enter your **Old Password**, then enter a **New Password**. Enter the new password a second time in the **Confirm Password** field, then click **Change Password**.

---

 **Note:** A list of password guidelines are displayed on the Change Password window. For more information about configuring these guidelines, see "[Configuring password restrictions](#)" on page 202.

---

To change your password at any time through the management portal, open the Admin menu and click **Change Password**.



## Logging out of Forcepoint CASB

For optimal security, when you're finished working, open the Admin menu and click **Logout**.

## Automatic logouts

You will be logged out automatically if no activity is detected for 15 minutes.



# CHAPTER 3

## Discovery and Asset Management

Forcepoint CASB | 2021 R4 | Updated: December 19, 2021

With the Forcepoint CASB Discovery module, you can [scan and upload network log files](#) to see all active cloud accounts, with [usage and risk information for found cloud applications](#). You can then eliminate shadow IT by bringing found applications into the Forcepoint CASB system as [managed assets](#), which enables, for those assets, [activity analysis](#) and [security monitoring and enforcement](#).

This chapter discusses the following:

Setting up discovery .....	16
Monitoring organizational cloud access .....	28
Restricting application access .....	41
Investigating apps through the Cloud App Directory .....	44

# Setting up discovery

---

To scan and upload network log files for cloud access discovery, you'll need to [set up the Forcepoint CASB Cloud Discovery tool](#) for it to [scan relevant traffic logs](#) and for the scan results to be automatically or manually [uploaded to your Forcepoint CASB management server](#). For continuous discovery, you can [schedule automatic scans](#).


## Installing and configuring the Cloud Discovery tool

The Cloud Discovery tool is a local application for Windows (7 and above or Server 2008 and above), Mac OS (10.5 and above), or Linux (Ubuntu, Mint, Debian, or CentOS). For Windows and Mac OS, it is delivered as a standard installation executable. For automation on Linux, Forcepoint CASB provides a [Linux CLI-only version of the tool](#).

For automated scans and/or result uploads, the Cloud Discovery tool must be installed in a location where it can access relevant network traffic log files. If you would like to upload the scan results to Forcepoint CASB, the Cloud Discovery tool must be installed in a location where it can access your Forcepoint CASB management server. For the Discovery tool to be able to download updates, including software updates and updated information for service identification, risk factors and characteristics, make sure that the tool can access the internet.

The Cloud Discovery tool is available through the Forcepoint CASB portal by going to **Settings > Tools and Agents**. Under the Application Discovery Tool section, click the Download link for your operating system. The executable file is downloaded to your local machine.

---

 **Note:** You must have a valid Forcepoint CASB license to download this tool. This tool will only be visible on the Tools and Agents page if you have a valid license. Contact Forcepoint Support if you would like to use the tool, but do not see the tool on this Settings page.

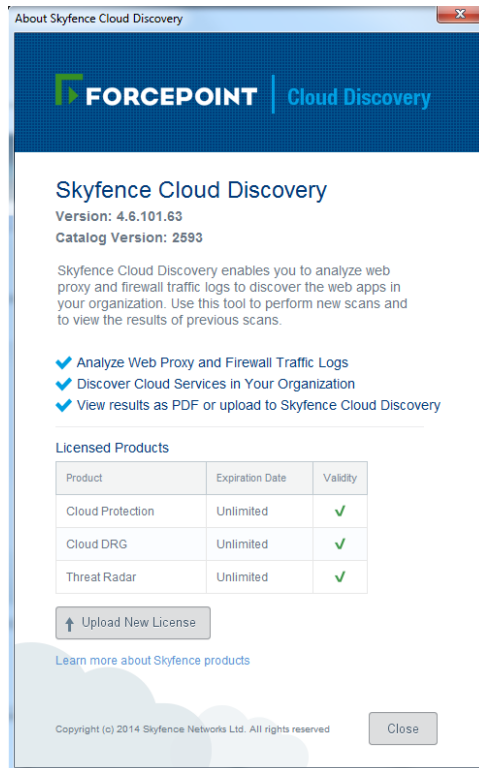
---

The Cloud Discovery tool can be installed through either of the following methods:

- ▶ **Attended installation through the user interface:** This method allows you to install the Cloud Discovery tool through an interactive Wizard. This installation requires the user to confirm the installation settings through a series of prompts before starting the installation.
- ▶ **Unattended installation through the command line:** This method allows you to install the Cloud Discovery tool without user interaction. This is a *silent* installation and does not display any indication of the installation progress.

To install and configure the Cloud Discovery tool through the user interface (Windows / Mac OS):

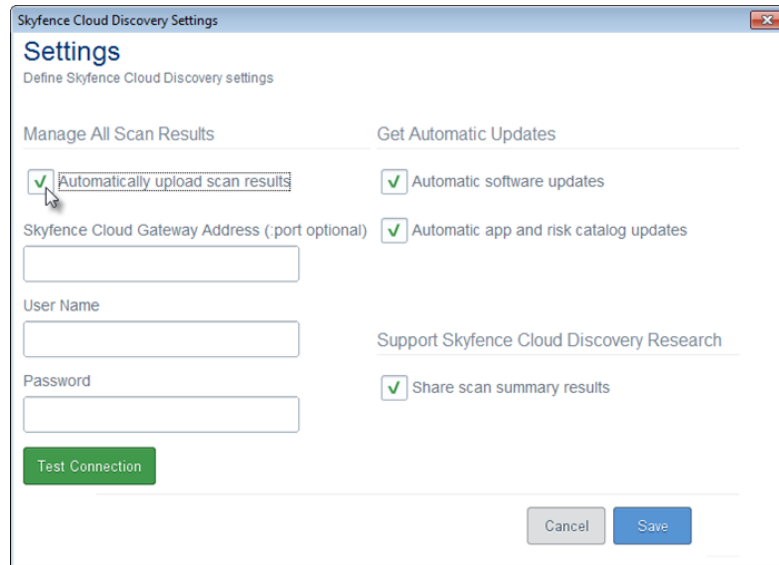
1. Obtain the installation source for the relevant OS from **Settings > Tools and Agents**.
2. Run the installation source and go through the installation wizard.
3. If you're prompted for a product or catalog update, confirm the update.
4. Either during the wizard, upon starting the tool, or subsequently in **Help > About**, upload an appropriate Forcepoint CASB license file:



The trial license you automatically received upon downloading the tool enables only limited functionality. For full functionality, use a license provided by your Forcepoint sales representative or reseller for your specific Forcepoint CASB management server. If this license is already installed in Forcepoint CASB, you can download it from the Forcepoint CASB management portal by going to **Settings > Tools and Agents > Application Discovery Tool > Download License**.

5. In the tool, go to **File > Settings**.
6. Under **Manage All Scan Results**, for all scan results to be automatically uploaded, select **Automatically upload scan results**:





7. Provide the **Address** of your organizational Forcepoint CASB management server (can be automatically populated from license) and credentials of a Forcepoint CASB administrator with Cloud Discovery permissions.

You can **Test Connection**.

8. Under **Get Automatic Updates**, select both options (recommended):
  - ▶ **Automatic software updates:** Updates to the discovery tool.
  - ▶ **Automatic app and risk catalog updates:** Updated information for service identification, risk factors and characteristics.
9. Optionally, select to **Share scan summary results** with Forcepoint CASB. Selecting this option shares anonymized statistics with Forcepoint, which helps improve the analytics we provide to all customers.
10. Click **Save**.

To install the Cloud Discovery tool through the command line as an unattended installation (Windows):

1. Obtain the Windows installation source from **Settings > Tools and Agents**.
2. Open the Windows command line interface as an administrator.
3. Run the following command:

```
<path> --mode unattended
```

where **<path>** is the directory where the Cloud Discovery tool source file is located.

For example:

```
CloudDiscovery-4.6.1.333-win-installer_  
jre.app/Contents/Windows/win-intel --mode unattended
```

To install the Cloud Discovery tool through the command line as an unattended installation (Mac OS / Linux):

1. Obtain the Linux or Mac OS installation source from **Settings > Tools and Agents**.
2. Open the command line interface.
3. Run the following command:

```
sudo <path> --mode unattended
```

where **<path>** is the directory where the Cloud Discovery tool source file is located.

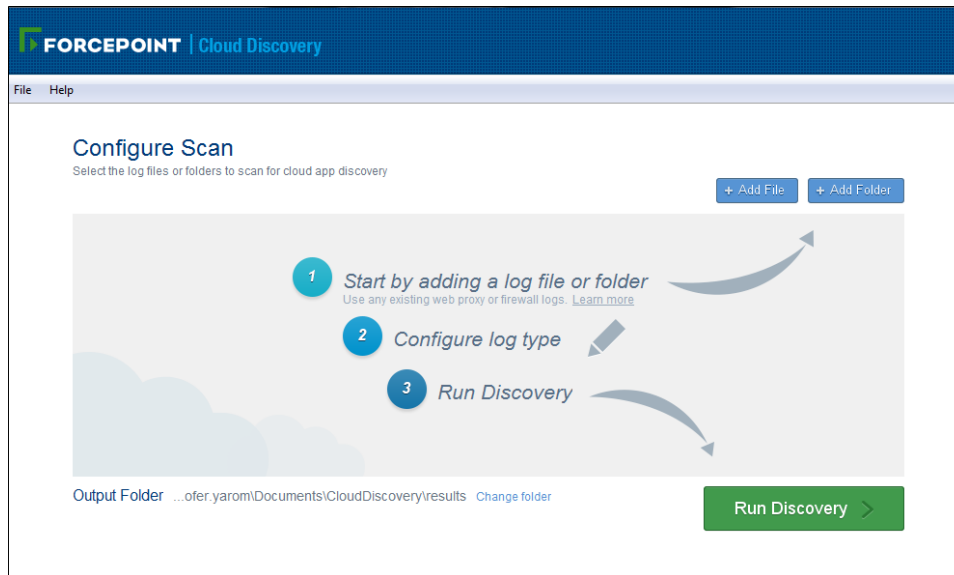
For example:

```
sudo CloudDiscovery-4.6.1.333-osx-installer_  
jre.app/Contents/MacOS/osx-intel --mode unattended
```

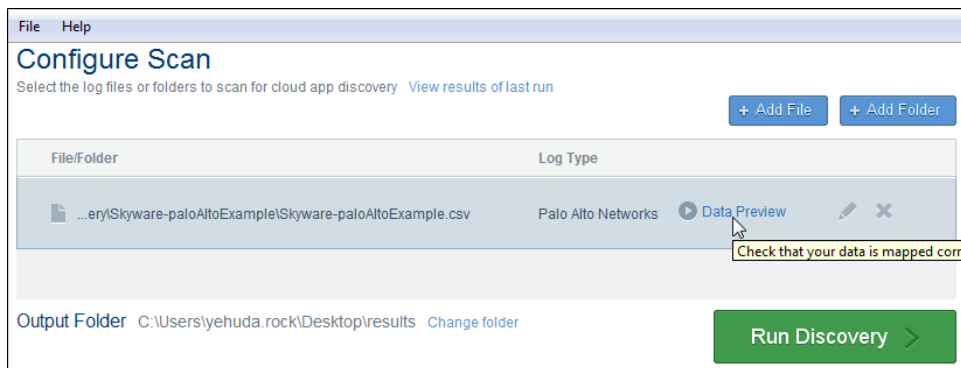
## Scanning for discovery

To scan network log files for cloud access discovery:

1. Export relevant log files from an organizational perimeter device such as a firewall, web proxy, SIEM, or router. If your organization is distributed among multiple sites, include logs from all sites. For full relevant results, the logs should represent a week or more of well-distributed user traffic (excluding periods of low user access activity). You can include multiple files of the same format in a folder to be scanned; different-format files should be placed in separate folders.
2. In the Cloud Discovery tool, click **Add File** (for a single log file) or **Add Folder**:

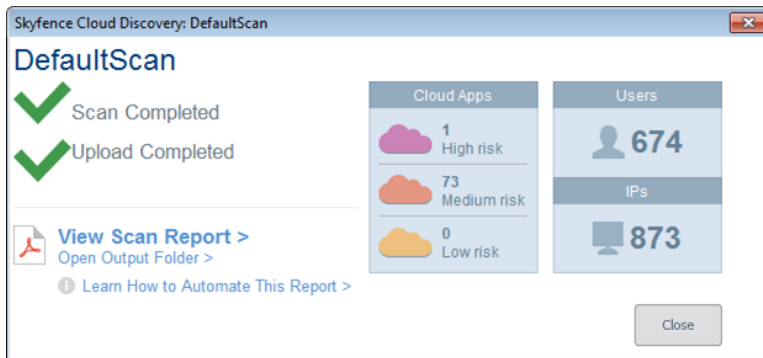


3. For each folder or file to be included in the scan:
  - a. **Browse** to and select the relevant file or folder.
  - b. Under **Log Type**, select the relevant **Category** and **Format** of the device that produced the logs.
  - c. Click **Save**.
  - d. Optionally, to validate that the tool is correctly parsing the logs, click **Data Preview**:



4. Click **Run Discovery**. You'll be prompted to save scan settings for future scans including [automatic scheduled scans](#).

The Cloud Discovery tool scans and analyzes the logs, and if [so configured](#) uploads results to the organizational Forcepoint CASB management server. Upon completion, basic result statistics are displayed:



You can **View Scan Report** (basic summary and results). For full interactive results, go to the [Discovery dashboard](#).

## Scheduling automatic scans

You can schedule automatic scanning of network log files for continuous cloud access discovery, after the Discovery tool has been properly [installed and configured](#).

You can also [schedule automatic scanning on Linux](#). To schedule automatic scanning on Windows or Mac OS:

1. Configure an organizational perimeter device such as a firewall, web proxy, SIEM, or router to regularly export relevant log files. If your organization is distributed among multiple sites, include logs from all sites.
2. If the above log files can't be exported directly to a location accessible by the Cloud Discovery tool, have them copied to such a location, such as by using a scheduled script.
3. In the Cloud Discovery tool, configure a scan (see "[Scanning for discovery](#)" on page 19) for the above log files and save the scan settings, either at being prompted upon running discovery, or by clicking **File > Save Scan As**. The scan settings are saved as a **.scan** file; make note of its location.
4. Using the operating system's standard scheduling tools (for example, the Windows Task Scheduler or the Mac OS Automator and Calendar), schedule running the following command:

```
<path>\cloudDiscoveryCLI.bat -s "<scan>" [-d "<output>"]
```

where

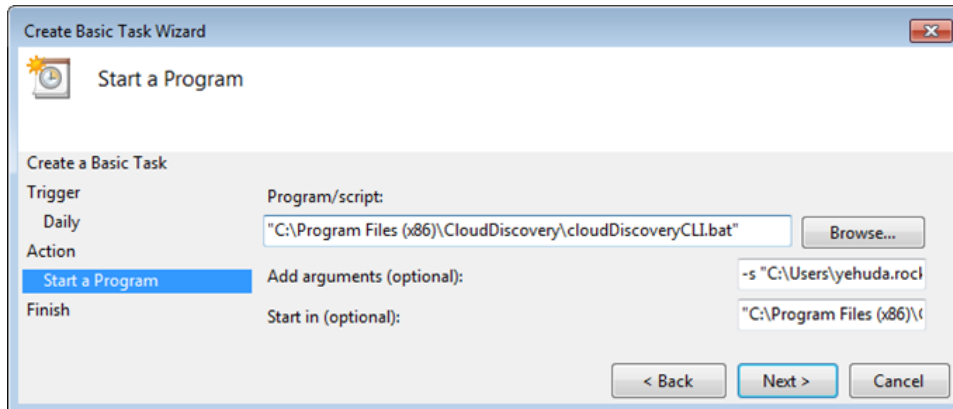
**<path>** is the Cloud Discovery tool installation directory;

**<scan>** is the path and filename of the saved .scan file; and

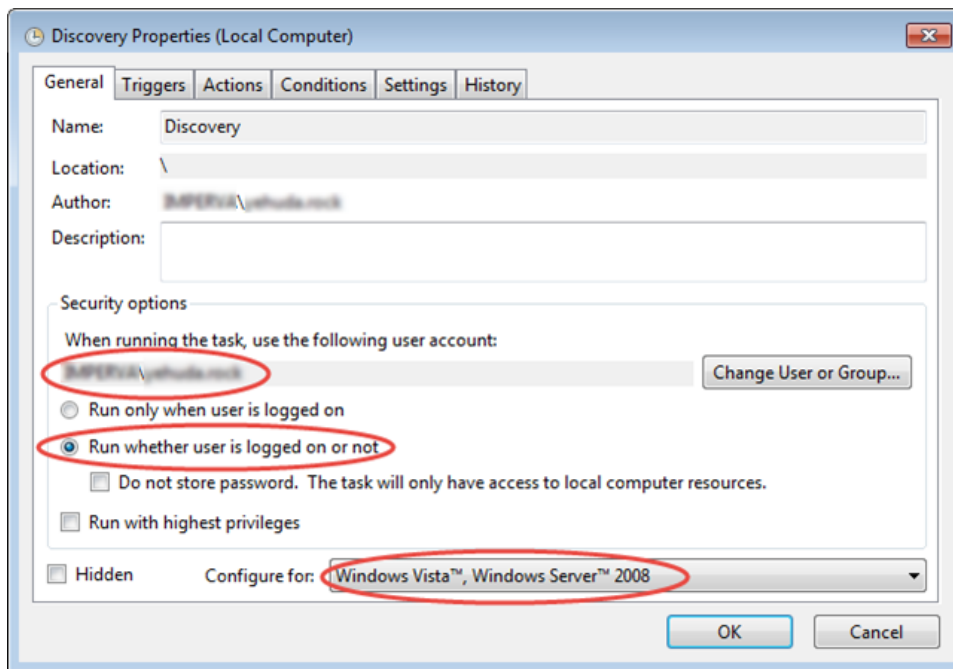
<output> (optional) is the directory in which to place scan results. If omitted, scan results will be placed in the location recorded in the .scan file as the last output location.

The command should run from the Cloud Discovery tool installation directory.

For example:



5. If you used the Windows Task Scheduler, open the task **Properties**, and make sure that the task is configured to use the current user account even if not logged in, and is configured for **Windows Vista, Windows Server 2008**:



# Scan automation on Linux

For scan automation on Linux, Forcepoint CASB provides a CLI-only Linux version of the Cloud Discovery tool.

The Discovery tool should be installed in a location where it can access relevant network traffic log files and your Forcepoint CASB management server. To be able to download updates, including software updates and updated information for service identification, risk factors and characteristics, make sure that the tool can access the internet.

To install the Discovery tool and schedule automatic scans on Linux:

1. On the Linux host, execute the Cloud Discovery **.run** file, and continue through the wizard according to prompts.

For **Share scan summary results**, enter **Y**.

For **Launch Cloud Discovery**, enter **n**.

2. From the Cloud Discovery installation folder (by default: **/opt/CloudDiscovery/**), run:

```
sh cloudDiscoveryConfig.sh --install.license <license>
```

where **<license>** is the path and name of an appropriate Forcepoint CASB license file.

The trial license you automatically received upon downloading the tool enables only limited functionality. For full functionality, use a license provided by your Forcepoint sales representative or reseller for your specific Forcepoint CASB management server. If this license is already installed in Forcepoint CASB, you can download it from the Forcepoint CASB management portal by going to **Settings > Tools and Agents > Application Discovery Tool > Download License**.

3. To enable automatic uploading of scan results, provide credentials of a Forcepoint CASB administrator with Cloud Discovery permissions, by running:

```
sh cloudDiscoveryConfig.sh --set.username <user> --set.password <password>
```

where **<user>** and **<password>** are the relevant credentials. You don't need to provide the address of your organizational Forcepoint CASB management server; it should have been automatically configured by Forcepoint CASB in your license.

4. Optionally, test the connection to the management server:

```
sh cloudDiscoveryConfig.sh --test.connection
```

5. Configure an organizational perimeter device such as a firewall, web proxy, SIEM, or router to regularly export relevant log files. If your organization is distributed among multiple sites, include logs from all sites. If the log files can't be exported directly to a location accessible

by the Linux Cloud Discovery tool, have them copied to such a location, such as by using a scheduled script.

6. On a Windows or Mac host with the Cloud Discovery tool, [configure a scan](#) for the above log files and save the scan settings, either at being prompted upon running discovery, or by clicking **File > Save Scan As**. The scan settings are saved as a **.scan** file; copy this file to the Linux host.
7. On the Linux host, configure a cron job to periodically run the following command:

```
sh <path>/cloudDiscoveryCLI.sh -s <scan> [-d <output>]
```

where

**<path>** is the Cloud Discovery tool installation directory;

**<scan>** is the path and filename of the saved **.scan** file; and

**<output>** (optional) is the directory in which to place scan results.

The Linux Discovery tool cannot perform automatic software updates. To manually update the tool itself, run:

```
sh cloudDiscoveryConfig.sh --update.app
```

To manually update information for service identification, risk factors and characteristics, run:

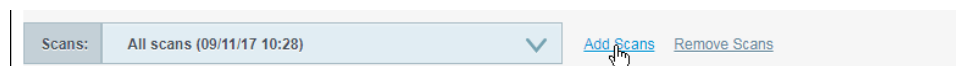
```
sh cloudDiscoveryConfig.sh --update.cat
```

## Uploading scan results

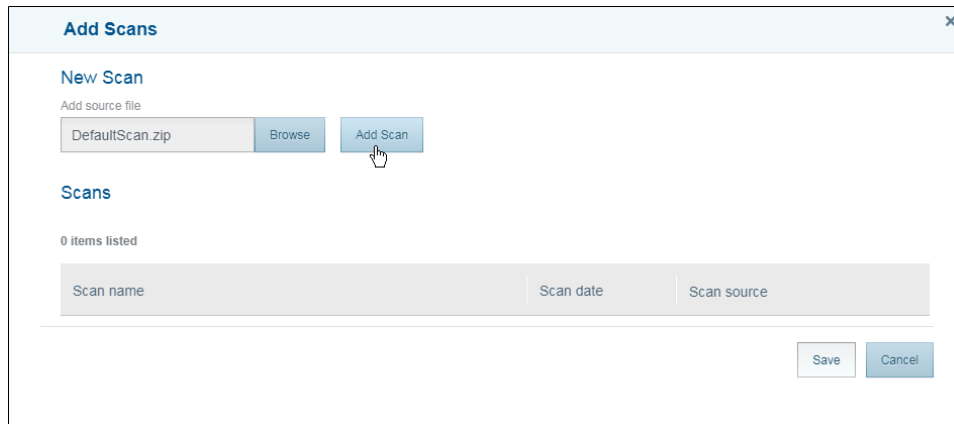
It is recommended to [configure automatic upload of scan results](#). Alternatively, you can manually upload results.

To manually upload scan results:

1. In Forcepoint CASB, go to **Discovery > Add / Remove Scans**:



2. **Browse** to and select the scan result **ZIP** file. The default location for scan results is:  
**C:\Users\<user>\Documents\CloudDiscovery\results\<date><ScanName><#>\<ScanName>.zip**
3. Click **Add Scan**:



4. Click **Save**.

When scan results are not uploaded automatically by the Discovery tool, the Forcepoint CASB management server might not receive app and risk catalog updates. In this case, to manually provide Forcepoint CASB with an updated catalog file, in Forcepoint CASB go to **Settings > Cloud Discovery**, under **New Catalog** upload the updated file and click **Add Catalog**.

## Upgrading or uninstalling the Cloud Discovery tool

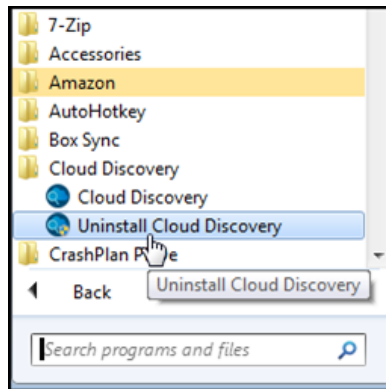
The Cloud Discovery tool can be uninstalled through either of the following methods:

- ▶ **Attended through the user interface:** This method allows you to uninstall the Cloud Discovery tool through the operating system's user interface. This requires the user to confirm the removal before starting the removal process.
- ▶ **Unattended through the command line:** This method allows you to uninstall the Cloud Discovery tool without user interaction. This is a *silent* removal and does not display any indication of the removal progress.

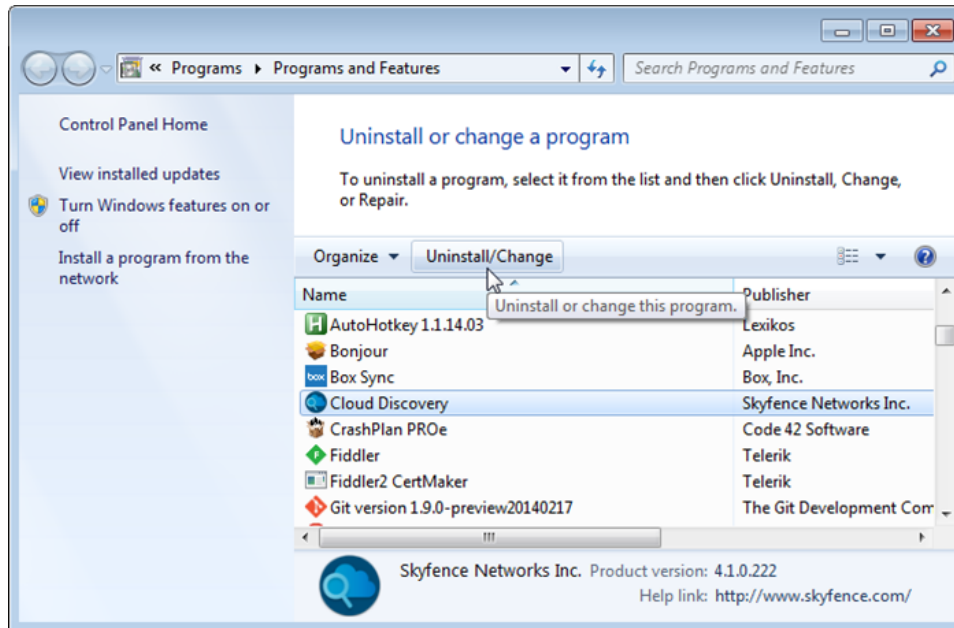
To uninstall the Cloud Discovery tool from a Windows computer, do one of the following:



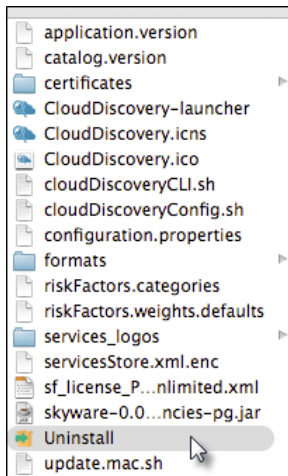
- ▶ In the programs menu go to **Cloud Discovery > Uninstall Cloud Discovery**:



- ▶ In **Windows Programs and Features**, select **Cloud Discovery** and click **Uninstall/Change**:



To uninstall the Cloud Discovery tool from a Mac computer, go to the **/Applications/Cloud Discovery** folder, and run **Uninstall**:



Upgrading the Cloud Discovery tool occurs automatically (with prompt for user confirmation) if [so configured](#). Otherwise, to upgrade the Cloud Discovery tool, first remove it as above (when prompted, to keep your settings, select **not** to remove **custom configuration**), then [install the newer version](#).

To uninstall the Cloud Discovery tool through the command line (Windows):

1. Open the Windows command line interface as an administrator.
2. Run the following command:

```
<path> --mode unattended
```

where **<path>** is the directory where the Cloud Discovery tool source file is located.

For example:

```
CloudDiscovery-4.6.1.333-win-installer_  
jre.app/Contents/Windows/win-intel --mode unattended
```

To uninstall the Cloud Discovery tool through the command line (Mac OS / Linux):

1. Open the command line interface.
2. Run the following command:

```
sudo <path> --mode unattended
```

where **<path>** is the directory where the Cloud Discovery tool source file is located.

For example:

```
sudo CloudDiscovery-4.6.1.333-osx-installer_  
jre.app/Contents/MacOS/osx-intel --mode unattended
```

# Monitoring organizational cloud access

After discovery is properly [set up](#), you can see all active cloud accounts, with usage and risk information for found cloud applications.

The [Discovery dashboard](#) provides an overview of organizational cloud access, from which you can drill-down for [comprehensive details on a specified cloud application](#). Displayed risk evaluations are based on a [configurable aggregation of various factors](#).

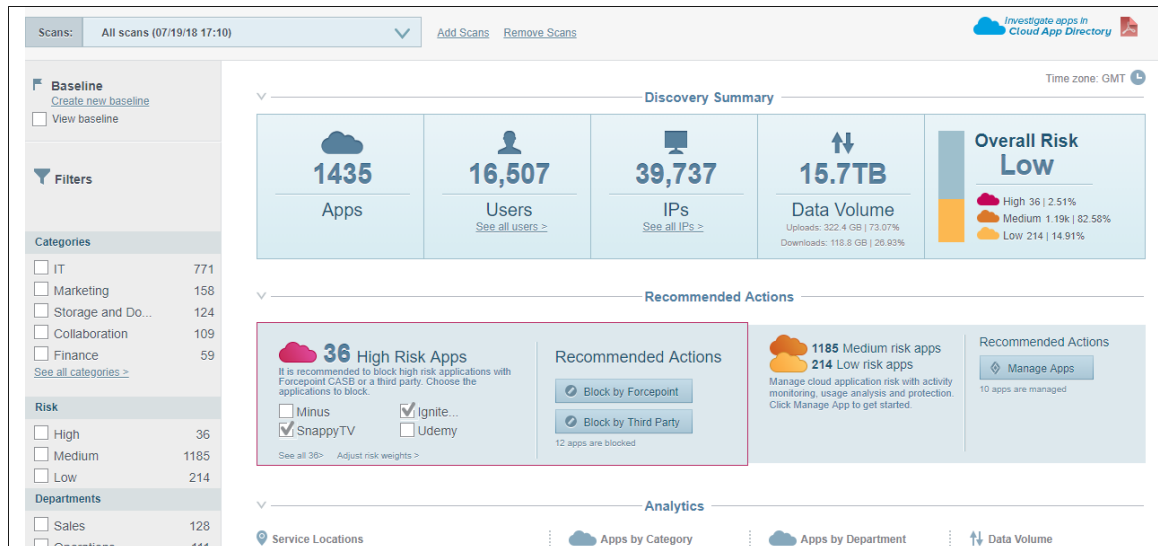
For found applications, Discovery provides options to [prevent the application from continuing to appear in Discovery](#), to [block users from accessing it](#), or to [begin managing with Forcepoint CASB](#).

## The Discovery dashboard

The [Discovery dashboard](#) provides an [overview of organizational cloud access, filtered or configured in several ways](#).

## Understanding the Discovery dashboard

To view the Discovery dashboard, go to **App Discovery**:



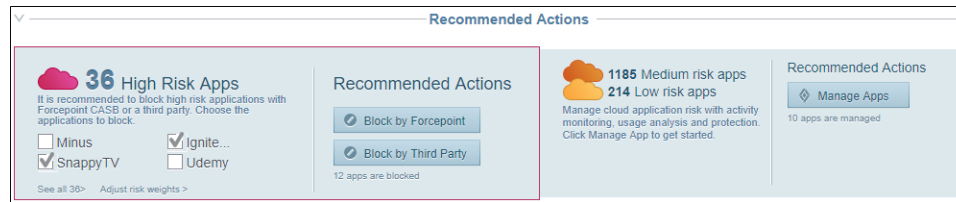
The dashboard includes the following sections:

- ▶ Left-hand [filtering pane](#)
- ▶ **Discovery Summary:** The total numbers of accessed cloud **Apps**, accessing **Users**,

Source **IP** addresses, and access traffic **Data Volume**; and, **Overall Risk** level and risk-level distribution:



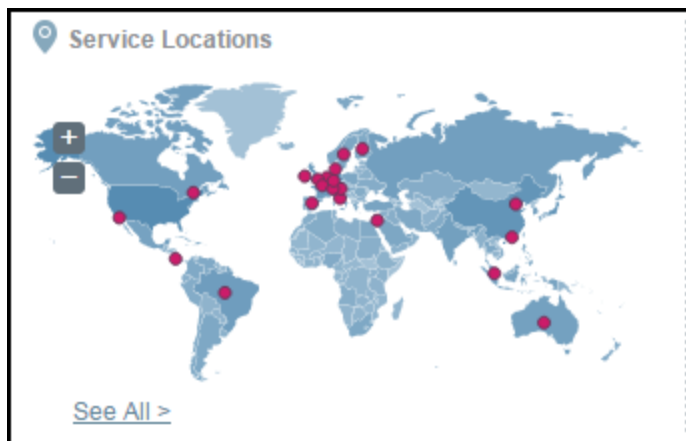
► **Recommended Actions:** According to risk level:



- **High-Risk Apps** with [blocking options](#)
- **Medium- and Low-risk apps** with the option for bringing them into Forcepoint CASB as [managed assets](#)

► **Analytics:** Includes the following widgets:

- **Service Locations:** Where the service's servers are located. This enables you to know where your organization's data is being stored:



You can zoom in and out with **+** **-**; to pan the map, drag it. Tooltips display country name and usage numbers:



To view a list of the countries, click **See All**. You can then export the **Locations** list to CSV:

**Locations** ✕

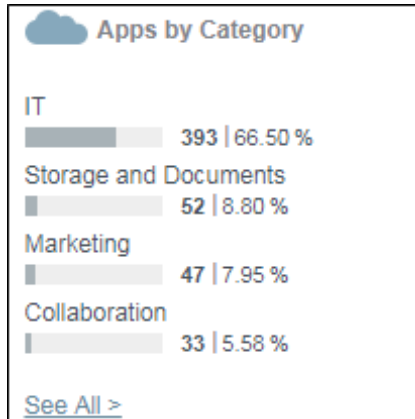
🔍 📄

282 items listed 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | >

Service Name	Countries
123 Contact Form	United States
1and1	United States
AB Tasty	Ireland
AddThis	United States
Adobe Creative Cloud	United States
Aerohive	United States
Airtel Business	India
Amazon Advantage	Ireland
Amazon Affiliate Program	United States
Amazon Web Services (AWS)	Japan

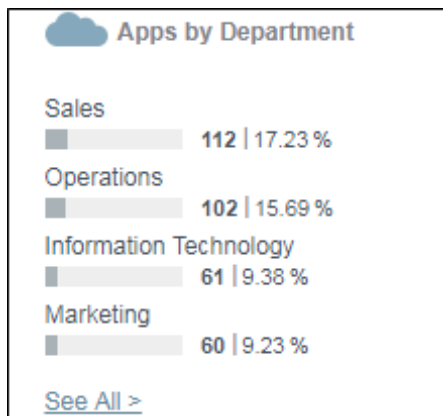
Close

- ▶ **Apps by Category:** Application distribution by application type:



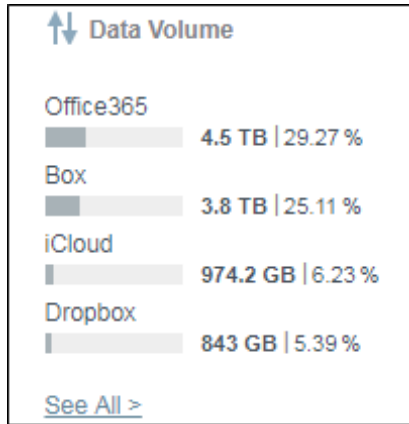
To view a full list, exportable to CSV, click **See All**.

- ▶ **Apps by Department:** Application distribution among user departments as defined in the organizational user directory, by numbers of accessing users:

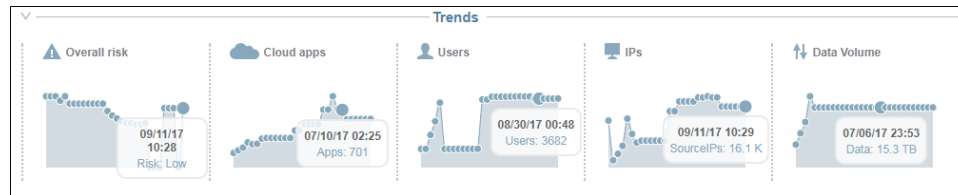


To view a full list, exportable to CSV, click **See All**.

- ▶ **Data Volume:** Application distribution by access data volume:



- **Trends** - available only when **All scans** are **displayed**: Recent values of **Overall risk**, numbers of accessed **Cloud apps**, numbers of accessing **Users**, and **Data volume**:



Hover over any point in a graph to see what it represents.

- **Cloud Apps**

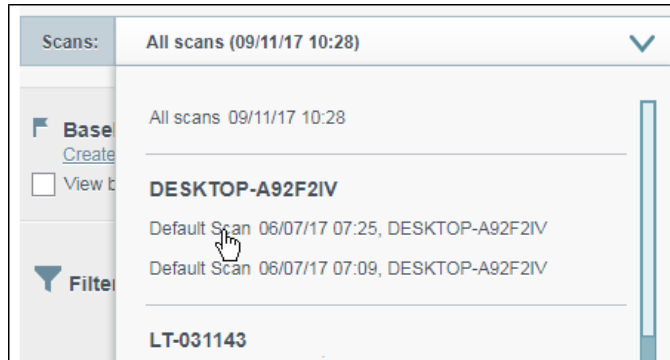
Each of the above sections is collapsible:



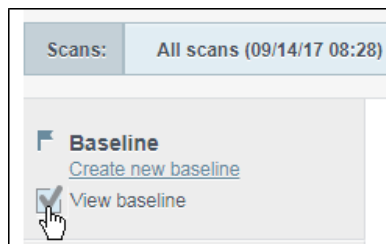
## Filtering the Discovery dashboard

You can filter or configure the information about the page in the following ways:

- By **Scans**: Select whether to display aggregated information from **All scans** or just from a specified scan (the last 100 scans are listed):



- ▶ Set a **Baseline**: To ignore existing scan results and in the future display only usage information from scans received from this time onwards, **Create new baseline**, then select **View baseline**:



To subsequently revert to including pre-baseline information, unselect **View baseline**.

- ▶ By cloud application service **Categories**: To display information only for applications of specified types, select those application types:

Categories	
<input type="checkbox"/> IT	393
<input type="checkbox"/> Storage and Do...	52
<input type="checkbox"/> Marketing	47
<input type="checkbox"/> Collaboration	33
<input type="checkbox"/> Social Network	19
<a href="#">See all categories &gt;</a>	

Only applications that belong to all selected categories (AND) are included. If not all categories are listed, you can **See all categories**. To include all applications, unselect all categories.

- ▶ By cloud application **Risk** level:



Risk	
<input type="checkbox"/> High	24
<input type="checkbox"/> Medium	508
<input type="checkbox"/> Low	59

Only applications of any of the selected risk levels (OR) are included. To display information for applications of all risk levels, unselect all three levels.

- ▶ By user **Departments**, as defined in the organizational user directory, [if configured](#):

Departments	
<input type="checkbox"/> Sales	112
<input type="checkbox"/> Operations	102
<input type="checkbox"/> Information Tech...	61
<input type="checkbox"/> Marketing	60
<input type="checkbox"/> Research & D...	56
<a href="#">See all departments &gt;</a>	

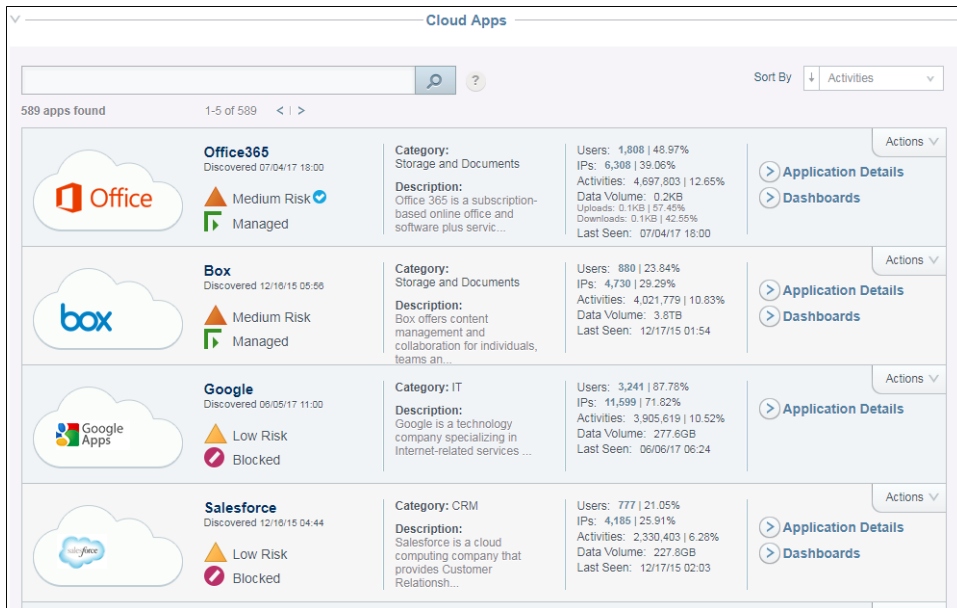
Only usage by users that belong to all selected departments (AND) are included. If not all departments are listed, you can **See all departments**. To include all usage, unselect all departments.

- ▶ To include applications that you marked to [Hide](#), select to **Show hidden cloud apps**:

General	
<input checked="" type="checkbox"/>	Show hidden cloud apps

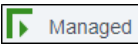
## Investigating accessed applications

A list of accessed cloud applications appears at the bottom of the [Discovery dashboard](#):



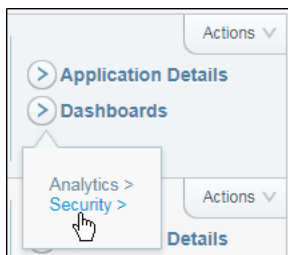
You can **Sort** the list by various parameters, and you can search the list.

For each application, the following is displayed:

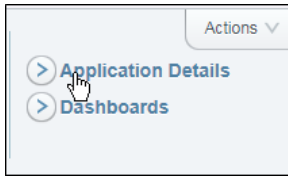
- ▶ Date **Discovered**, **Risk** level, and whether it has been brought into Forcepoint CASB as a **managed asset**: 
- ▶ Service **Category** and **Description**
- ▶ Discovered usage and traffic statistics (quantities and distributions of **Users**, **Activities**, **Data Volume**; and date **Last Seen**)

From an application's **Actions** menu, you can **Hide it**, **Block it**, or **Manage it as an asset**.

For managed assets, you can go to the **Security** or **Analytics** dashboard:



To drill-down to further investigate an application, click the application name or **Application Details**:



The application's details page appears:

 A screenshot of the Office365 application details page. The page is divided into several sections:
 

- Header:** 'Office365' title, Office logo, 'Medium Risk' status with a checkmark, 'Managed' status with a checkmark, and a 'Dashboards' link.
- Category:** 'Storage and Documents'.
- Description:** A paragraph describing Office 365 as a subscription-based online office and software suite.
- Service Provider:** 'Microsoft Corp'.
- Headquarters:** 'Microsoft Redmond Campus, Redmond, Washingt...'
- Service Website & Terms & Conditions:** Links for 'Service Website >' and 'Terms & Conditions >'.
- Controls:** A vertical list of buttons: 'Block by Third Party', 'Block by Skyfence', 'Manage App', and 'Unacknowledge'.
- Summary Cards (Upper Right):**
  - Users:** 1,808 (with 'See all users >' link)
  - IPs:** 6,308 (with 'See all IPs >' link)
  - Data Volume:** 0.2KB (Uploads: 0.1KB | 57.45%, Downloads: 0.1KB | 42.55%)
  - Activities:** 4.7m (First activity: 07/04/17 18:00, Last activity: 07/04/17 18:00)
- Service Locations:** A world map with a red dot in North America and zoom controls (+, -).
- Service IPs >:** A link to view IP addresses.
- Top Departments:** A horizontal bar chart showing:
  - Operations: 1.89k | 38.28%
  - Sales: 1.76k | 35.49%
  - Marketing: 340 | 6.87%
  - Research & Development: 269 | 5.44%
 (with 'See All >' link)
- Hourly Usage:** A line graph showing activity over time, with a callout for '19:00 Activities: 184081'.
- Admins:** A list of users and their last activity times:
  - hbeals: 12/17/15 03:02
  - abattle: 12/17/15 02:41
  - mellett: 12/17/15 02:23
  - cremington: 12/17/15 02:07
 (with 'See All >' link)
- Application Risk Categories:** A section with 'Compliance' and 'Security Settings' sub-sections, and an 'Adjust risk weights >' link.

The upper-left section includes general details about the application service, and controls for [blocking access](#), for [managing the application as an asset](#), and for [hiding it](#).


The upper-right section includes usage and traffic statistics for the application. Below that, the following sections are displayed:

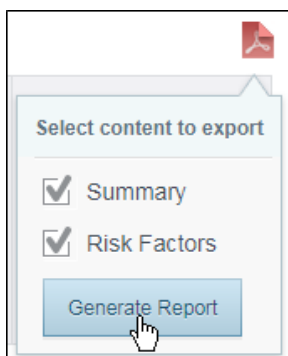
- ▶ **Service Locations:** Where the application's servers are located. You can zoom in and out with **+** **-**; to pan the map, drag it. To view a list of the application servers' IP addresses,

click **Service IPs**.

- ▶ **Hourly Usage:** Activity distribution by time of day.
- ▶ **Top Departments** - available with a known [organizational directory](#): Organizational departments that access the application the most.
- ▶ **Admins:** The number of user accounts used to access application pages that require administrative permissions.

Below, the application's risk analysis factors are [listed](#).

You can produce a PDF report with the information of the application details page. At the upper-right, click , select the parts to include, and click **Generate Report**.



## Application risk analysis

Each discovered accessed cloud application is marked with a **Risk** level: **High**, **Medium**, or **Low**, evaluated according to various characteristics. Each such characteristic defines a risk value which is used as a factor with a designated weight for calculating the application's overall risk.

High-risk applications are recommended to be [blocked](#). Medium- and low-risk applications are candidates for being [managed in Forcepoint CASB as assets](#).

Applications' overall risk levels are displayed in several places in the [Discovery dashboard](#), and can be used to [filter the dashboard](#) or to [sort the application list](#).

The characteristics that are used in evaluating application risk are categorized and listed at the bottom of application detail pages, under **Application Risk Categories**. For example:

**Application Risk Categories** [Adjust risk weights>](#)

- > Compliance
- > Security Settings
- > General information
- > Data Leakage
- > Data Ownership
- ▼ Account Termination Policy

**Data Access Revoke**  
Ability to immediately revoke access

Cloud app settings	Risk impact	Risk weight (3/5)
Yes	▲ Low	0 1 2 3 4 5
No	▲ High	0 1 2 3 4 5

**Data Status Post Account Termination**  
What happens to data if you terminate your account

Cloud app settings	Risk impact	Risk weight (3/5)
Retained	▲ High	0 1 2 3 4 5
Returned	▲ Low	0 1 2 3 4 5
Deleted	▲ Medium	0 1 2 3 4 5

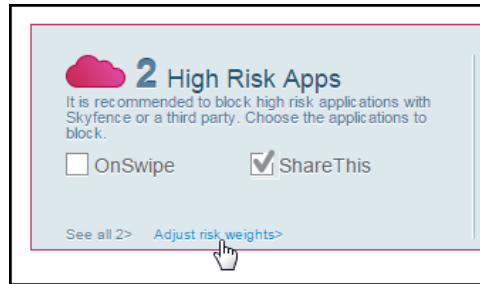
> Auditing

In this example, the **Account Termination Policy** category (in the example, the only expanded category) includes two characteristics. The second indicates that upon account termination, the service provider retains data, which causes a **High Risk impact** with a medium **Risk weight (3/5)** for calculating the application's overall risk.

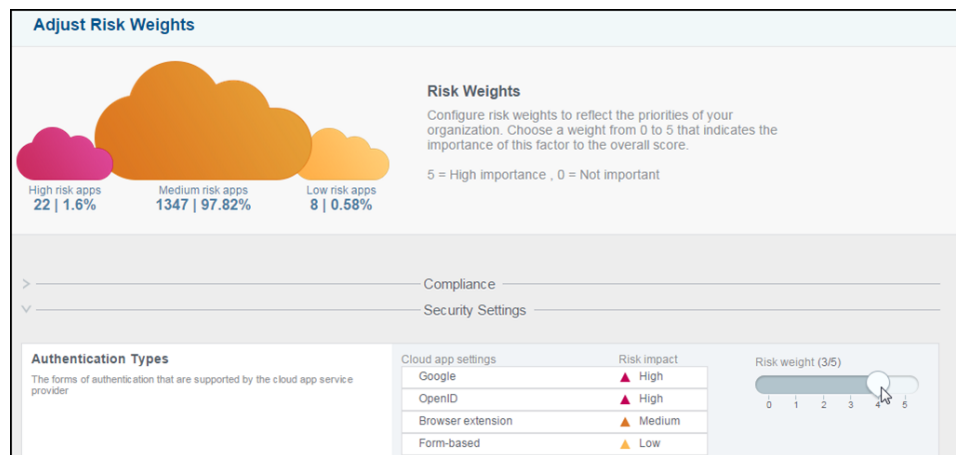
The default risk weights are based on Forcepoint CASB research and risk assessment, but you can change them according to your organization's needs. For example, a compliance standard such as HIPAA can be critical, calling for a risk weight of 5, while another standard is not important at all, calling for a risk weight of 0.

To configure risk weights:

1. Do one of the following:
  - ▶ In the [Discovery dashboard](#), under **Recommended Actions > High-Risk Apps**, click **Adjust risk weights**:



- ▶ In an application's details page, by **Application Risk Categories**, click **Adjust risk weights** (see above).
2. Expand categories to see their listed characteristics, and slide risk weight selectors as relevant:

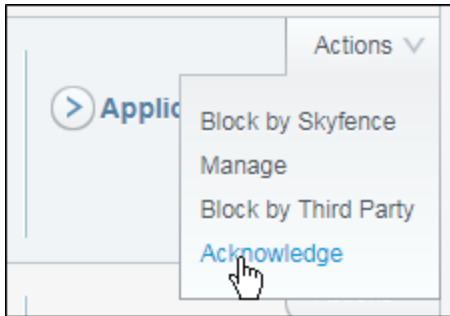


As you make changes, the information at the top of the page is automatically updated to reflect how the changes affect application risk levels.

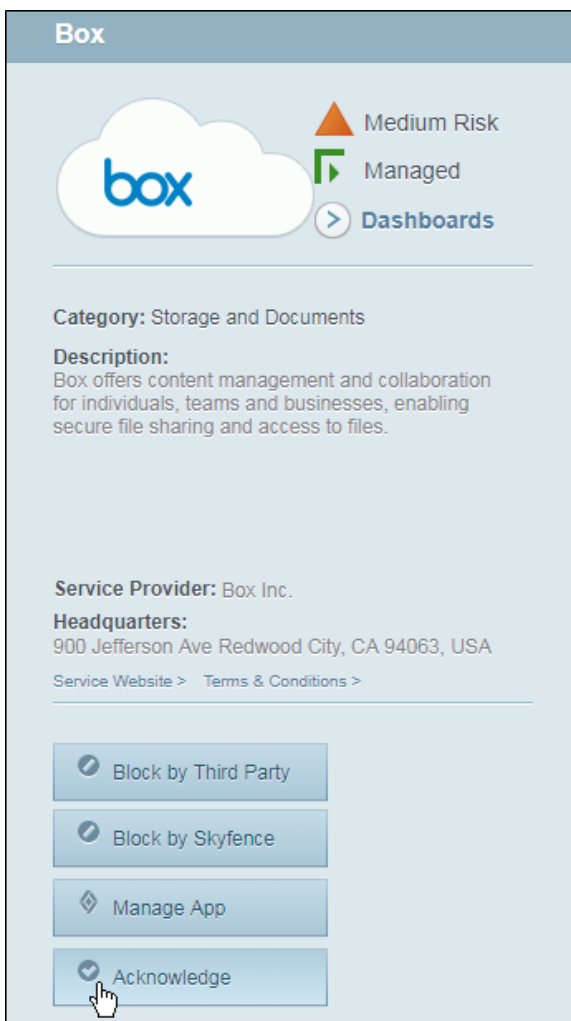
3. At the bottom of the page, click **Save**.

## Acknowledging accessed applications

If you decide that an application does not need to be managed or monitored, to prevent it from continuing to appear in Discovery, in the [Discovery dashboard](#), go down to the list of found applications, and in the relevant row click **Actions > Acknowledge**:



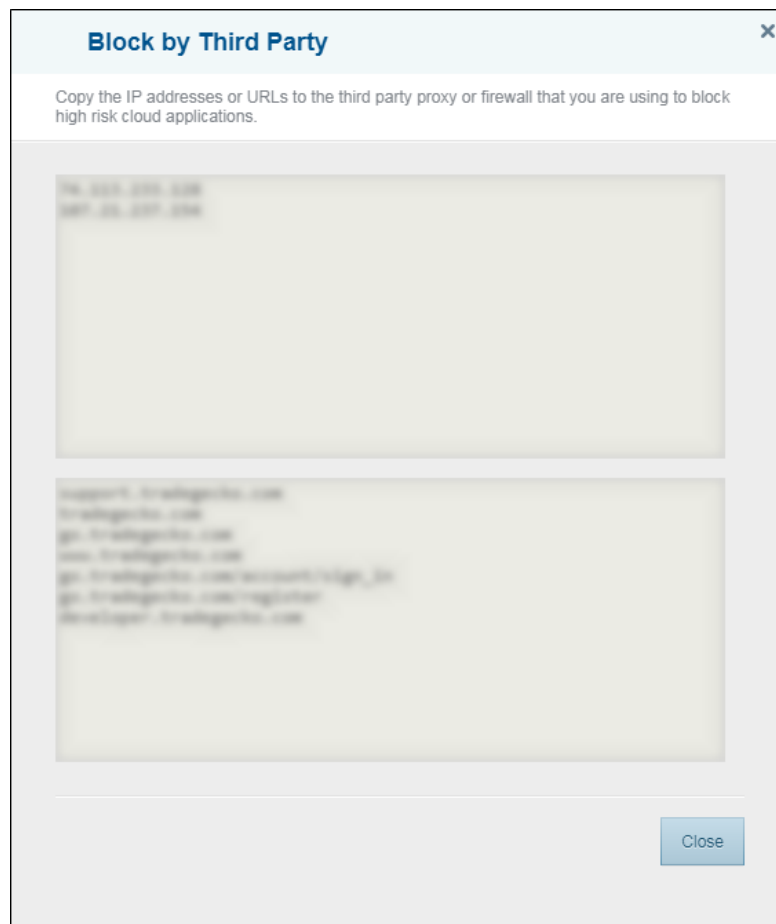
Alternatively, in the application's [details page](#), select **Acknowledge**:



# Restricting application access

If you want to block user access to a service application, you can do this in either (or both) of two ways:

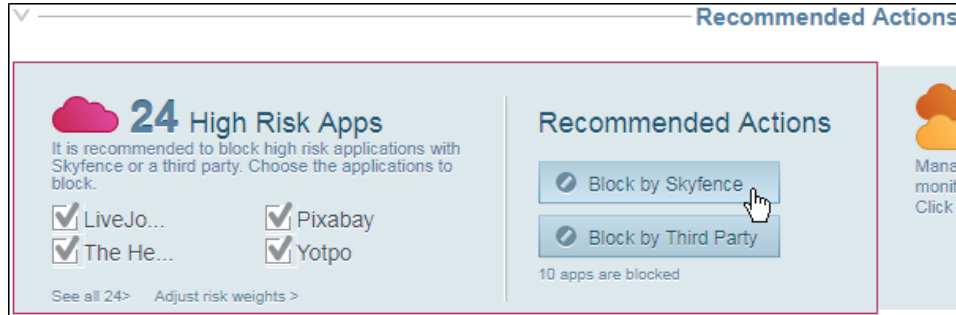
- ▶ **Block by Skyfence:** If your Forcepoint CASB deployment includes [endpoint routing](#), you can add the application's address domains to the list of [blocked domains](#).
- ▶ **Block by Third Party:** Forcepoint CASB provides destination addresses that you can copy to organizational firewalls to configure them to block access to the application:



To block an application in either of the above two ways, do one of the following:

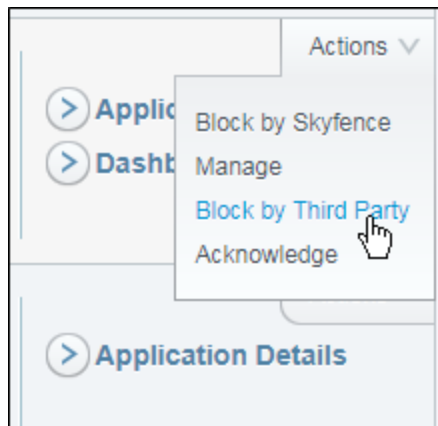


- ▶ If the application is listed in the [Discovery dashboard](#) under **Recommended Actions** as a **High-Risk App**, select the application and click the relevant **Block** option:




If there are too many applications to list here, click **See all**.

- ▶ In the Discovery dashboard list of [accessed cloud applications](#), by the application, click **Actions** and the relevant **Block** option:



- ▶ In the application's [detail page](#), at the bottom of the upper-left section, click the relevant **Block** option:

## Dropbox

▲ Medium Risk  
▶ Managed  
➤ Dashboards

---

**Category:** Storage and Documents

**Description:**  
Dropbox is a file hosting service that offers cloud storage, file synchronization, and client software. It allows users to create a folder on each of computers, which Dropbox then synchronizes.

**Service Provider:** Dropbox

**Headquarters:**  
185 Berry St 4th Floor, San Francisco, CA, USA

[Service Website >](#) [Terms & Conditions >](#)

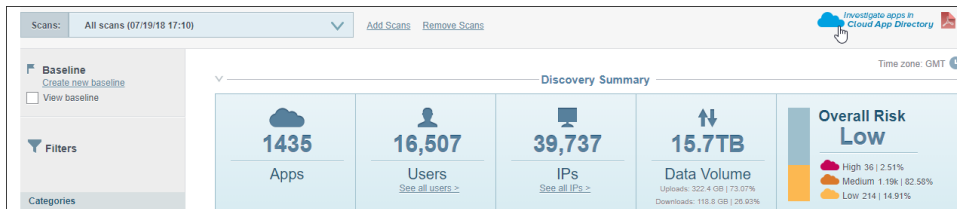
---

✔ Block by Third Party  
✔ Block by Skyfence  
◆ Manage App  
✔ Acknowledge

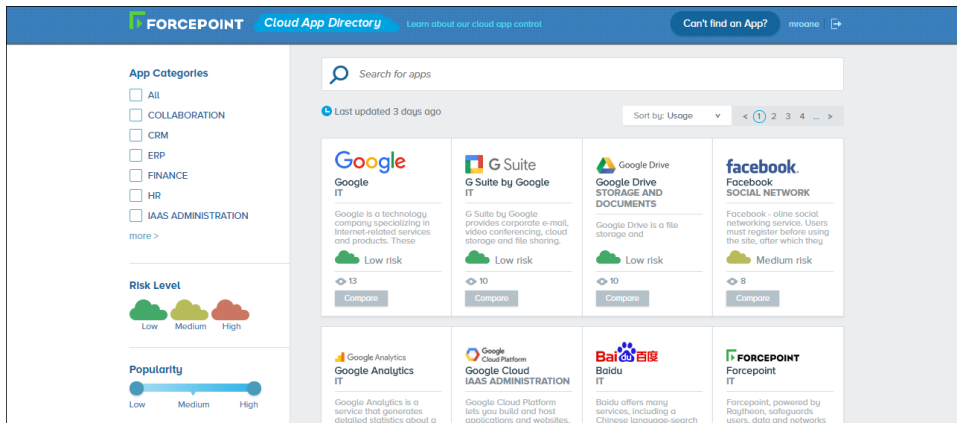
# Investigating apps through the Cloud App Directory

The Cloud App Directory provides detailed information about thousands of available cloud applications, allowing users to review the risk and compliance aspects of cloud applications, compare similar applications, and investigate services. The information provided includes general information about the provider and the application, regulatory compliance notes, and details about the security aspects supported by the application.

To open the Cloud App Directory from the management portal, go to the **App Discovery** tab, then click the **Investigate apps in Cloud App Directory** link.



The default list of cloud apps displays all apps in the directory. Each cloud app is displayed within a summary box that contains basic information, such as the app category, a short description of the app, the risk level, and the usage number for your organization.



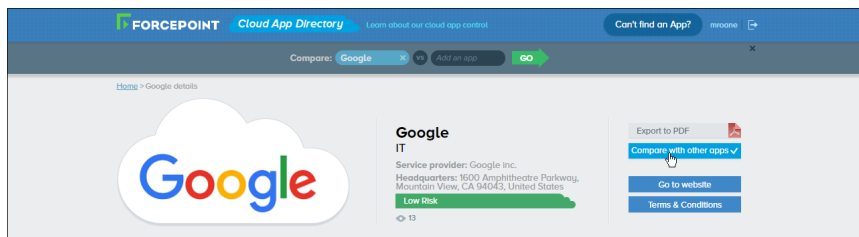
To sort the list, open the **Sort by:** drop-down menu above the directory. The default sort is by **Popularity**. You can also choose to sort by **Risk level**, cloud app **Name**, or **Usage**.

To filter the list of cloud apps and only display the apps that meet the filter criteria, select the desired **App Categories**, **Risk Level**, and/or **Popularity** from the menus to the left of the directory.

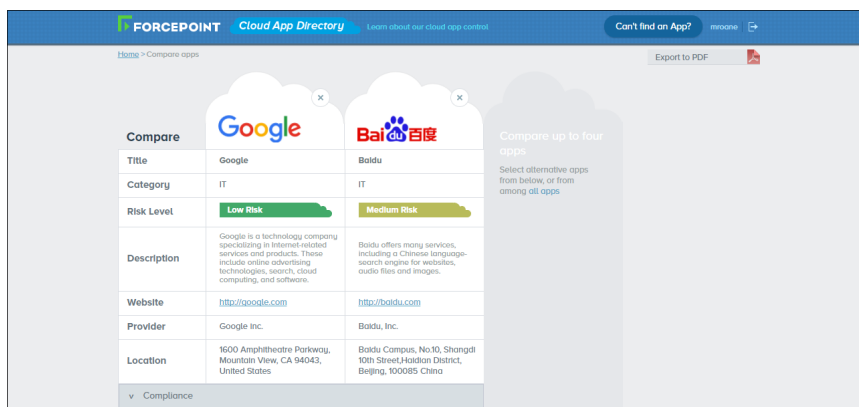
To view the full details of a cloud app, locate it in the directory and click on the cloud app's summary box. Forcepoint CASB displays the details for the selected cloud app.

The top of the detailed page contains summary information about the cloud app, as well as links to additional information:

- ▶ Click the **Export to PDF** button to create a PDF report of the cloud app's detailed information, including all information from the Info and Risk Factors tabs. The PDF report is displayed in a new tab or window, where you can view, print, or save a copy of the report.
- ▶ Click the **Compare with other apps** button to add this cloud app to the compare apps list. You can compare up to four cloud apps.
  - Forcepoint CASB displays a new section at the top of the window. The selected cloud app is listed, as well as any other selected apps.



- To select additional apps to compare, navigate back to the directory and either click the **Compare** button located in the cloud app's summary box or open the cloud app's detailed page and click the **Compare with other apps** button.
- After you select all of apps you wish to compare, click the **Go** button. The Cloud App Directory displays a table with the detailed information for each compared cloud app.



- To save a copy of the comparison results, click the **Export to PDF** button.
- ▶ Click the **Go to website** button to open a new browser tab or window that displays the

primary URL for the cloud app.

- ▶ Click the **Terms & Conditions** button to open a new browser tab or window that displays the terms and conditions for the cloud app.

Under the cloud app 's summary are two tabs: Info and Risk Factors.

- ▶ The **Info** tab displays a description of the cloud app and a map of service locations.
  - Click **see service IPs and URLs** to display lists of the IP addresses and URLs associated with the service.
  - To save the IP addresses and URLs to a CSV file, click the **Export to CSV** button.
- ▶ The **Risk Factors** tab displays the cloud app settings that contribute to the cloud app's overall risk level. These risk factors are separated into the following categories:
  - Compliance
  - Security Settings
  - General Information
  - Data Leakage
  - Data Ownership
  - Account Termination Policy
  - Auditing

The **Alternative apps** section displays the cloud apps that are most similar to the selected app. You can either click the cloud app's summary box to display the cloud app's detailed page, or click **Compare** to compare the alternative app to the selected app.

Click **See all alternative apps** to open the directory page with the results filtered to display all cloud apps that match the selected app's App Category.



# CHAPTER 4

## Activity Analysis and Investigation

Forcepoint CASB | 2021 R4 | Updated: December 19, 2021

For service applications that have been defined as [managed assets](#), Forcepoint CASB has the ability to identify activity details such as source devices, source locations, and actions (for example, password change or data modification). Using this information, Forcepoint CASB provides various [graphic activity summaries](#) and tools for [investigating user activities according to various parameters](#). Filtered activity lists can be exported for further analysis and compliance.

You can use the investigative tools for compliance, IT planning, and security purposes. For example, you can investigate issues identified in [Security](#), periodically review organizational behavior patterns, or identify sensitive actions such as password changes.

You can [investigate user accounts and their activities](#), including handling their policy violations.

This chapter discusses the following:

Activity audit types .....	48
About the activity impact score .....	51
Monitoring and investigating user activities .....	53

# Activity audit types

---

Forcepoint CASB monitors user activities from two types of sources:

- ▶ **Real-time Monitoring:** This method is proxy-based. Forcepoint CASB connects the user to the cloud service through a Forcepoint CASB proxy and collects user activity as the user interacts with the cloud service. Because Forcepoint CASB is set up between the user and the cloud service, Forcepoint CASB monitors the activities in real time, and if the activity violates a policy, performs a mitigation action to block the activity.
- ▶ **Service Provider Log:** This method is API-based. Forcepoint CASB collects user activity from audit logs provided by the cloud service. When the user performs an action on the cloud service, the cloud service records detailed information about the action in an audit log. Forcepoint CASB connects to the cloud service through an API connection to download the audit logs and provide the information for analysis.

To view the user activity collected for either Activity Audit type, go to **Audit & Protect > Activity Audit**.


Under Activity Audit, you will see the two Activity Audit types:

- ▶ [Realtime Monitoring](#)
- ▶ [Service Provider Log](#)

Each Activity Audit type has two user activity pages:

- ▶ [Dashboard](#): The information displayed in the Dashboard is the same for each type.
- ▶ [Audit Log](#): The information displayed by default in the Audit Log is the same for each type. You can display additional columns in the Audit Log table, but the columns available in the Service Provider Logs correspond to the information received from the individual cloud service (asset), and might not match the information captured through Real-time Monitoring.

---

 **Note:** A Forcepoint CASB asset can have both Real-time and Service Provider Log user activity, but the activities will be separated into a Real-time Monitoring audit log and a Service Provider Log audit log. Forcepoint CASB cannot combine the two logs.

---

## Monitoring real-time activities

This option audits all activities as they are performed by the user. With real-time monitoring, all user activity is filtered through a proxy, so Forcepoint CASB has full visibility into all activities the user performs on the cloud service.

To configure an asset's connection to collect real-time activities, see "[Configuring a web connection](#)" on page 279.

## Monitoring service provider log activities


Cloud services provide audit logs of user activity that can be uploaded to Forcepoint CASB for analysis. These audit logs provide detailed information about user activity that was performed through the cloud service. Because Forcepoint CASB receives the information from the cloud service, Forcepoint CASB receives the information after the user has performed the activity. This provides near real-time monitoring, which provides mitigation actions, recommendations, and record keeping.

Service Provider Log monitoring is API-based. Forcepoint CASB connects to the cloud service's Activity APIs through an API call. The cloud service then sends detailed information about the user's activities to Forcepoint CASB.


To enable Service Provider Log monitoring on a cloud service asset, the cloud service must have an Activity API available. Currently, Activity APIs are available for the following cloud services:

- ▶ Salesforce.com
- ▶ Microsoft Office 365
- ▶ Microsoft Azure
- ▶ Microsoft Exchange
- ▶ Box
- ▶ Google G Suite
- ▶ ServiceNow
- ▶ Dropbox
- ▶ Amazon Web Services (AWS)
- ▶ Cisco Webex

---

 **Note:** Because each cloud service creates their own Activity APIs, the data collected from each cloud service varies. Data categories from one cloud service might not match the data categories from another cloud service.

---

 **Note:** Salesforce does not support the Quarantine mitigation option. If you are configuring a Salesforce asset and the Quarantine option is available, do not select it. If you select the Quarantine option, it does not work.

---

To configure an asset's API connection, see "[Configuring an API connection](#)" on page 280.



For more information about setting up the administrator account on each supported cloud service, see the [Forcepoint CASB Service Provider API Connection Guide](#).

# About the activity impact score

An activity impact score reflects the potential confidentiality, integrity, and availability (CIA) impact of a single user activity on specific data in a cloud application. The score is a numerical value that can range from 1 to 100. A higher score means a higher impact.


The activity impact score is divided into the following levels.

Level	Range	Description
Critical	81–100	Sensitive activities. For example, sensitive administrative actions, modifying or disabling main security controls, bulk data export, mass deletion, bulk sharing.
High	55–80	High impact activities that usually require high level permissions, but do not need to be reviewed by a security department each time they occur. For example, modifying a Price Book in Salesforce, resetting a user password.  Individually, these activities do not need to generate a security alert or a push notification. It is recommended to use additional conditions with these activities to generate an alert.
Medium	31–54	Activities that require common permissions. For example, sharing a file, exporting a report, viewing a lead.  Individually, these activities do not need to generate a security alert or a push notification. It is recommended to use additional conditions with these activities to generate an alert.
Low	1–30	Activities that do not require special roles or permissions. For example, modifying personal profile settings, uploading or downloading content to personal user folder.

The activity impact score is only available for real-time activities. In Forcepoint CASB, you can use the activity impact score in the following ways:

- ▶ Monitor the impact score in the Realtime Monitoring audit log. For more information, see ["Investigating activity logs" on the facing page](#) and ["Audit log column descriptions" on page 56](#).
- ▶ Add the impact score as a predicate in custom policy rules where you can apply common mitigation for user activities with similar impact score level. For more information, see ["Configuring custom policies" on page 80](#) and ["Custom access policy predicates" on page 88](#).
- ▶ Send the impact score to a SIEM in the activity record. For more information, see ["Setting up SIEM / syslog integration" on page 259](#) and ["Activities and alerts CEF mapping" on page 262](#).

---

 **Note:** Not all real-time assets have been mapped to include an activity impact score. If a real-time asset is unmapped, an activity impact score is not shown for the asset.

---

# Monitoring and investigating user activities

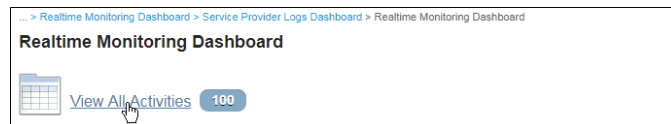
## Investigating activity logs

To investigate organizational user activities in cloud applications, in addition to using the preconfigured [graphic analysis summaries](#), you can view activity logs and filter them according to various parameters.

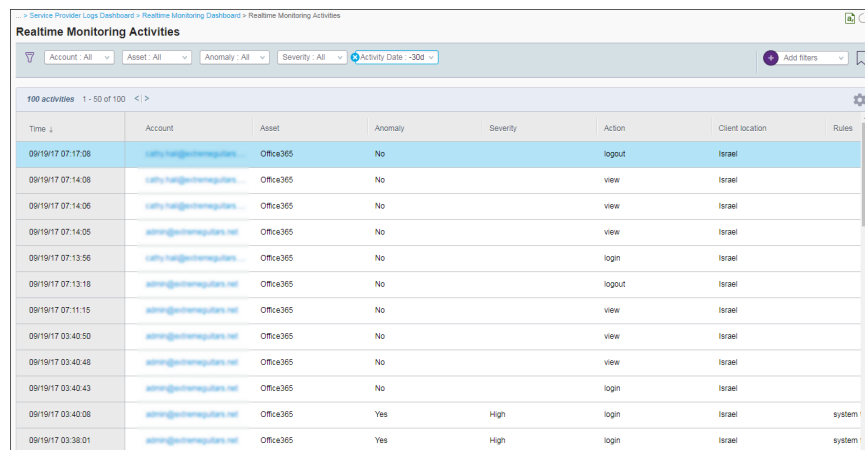
To view a log of all activities for an application asset or for all assets:

1. In Forcepoint CASB, go to **Audit & Protect > Activity Audit**.
2. Select the relevant asset from the top left list of assets.
3. Under **Activity Audit**, select the **Audit Log** for the type of activity you are searching (**Realtime Monitoring** or **Service Provider Log**).

Alternatively, you can select the **Dashboard**, then click **View All Activities**:



4. The activity log appears:



Time	Account	Asset	Anomaly	Severity	Action	Client location	Rules
09/19/17 07:17:08	lily.hal@gethempublers.net	Office365	No		logout	Israel	
09/19/17 07:14:09	lily.hal@gethempublers.net	Office365	No		view	Israel	
09/19/17 07:14:06	lily.hal@gethempublers.net	Office365	No		view	Israel	
09/19/17 07:14:05	admin@gethempublers.net	Office365	No		view	Israel	
09/19/17 07:13:56	lily.hal@gethempublers.net	Office365	No		login	Israel	
09/19/17 07:13:18	admin@gethempublers.net	Office365	No		logout	Israel	
09/19/17 07:11:15	admin@gethempublers.net	Office365	No		view	Israel	
09/19/17 03:40:50	admin@gethempublers.net	Office365	No		view	Israel	
09/19/17 03:40:48	admin@gethempublers.net	Office365	No		view	Israel	
09/19/17 03:40:43	admin@gethempublers.net	Office365	No		login	Israel	
09/19/17 03:40:08	admin@gethempublers.net	Office365	Yes	High	login	Israel	system
09/19/17 03:38:01	admin@gethempublers.net	Office365	Yes	High	login	Israel	system

For more information about the columns available in the Audit Log, see ["Audit log column descriptions"](#) on page 56.

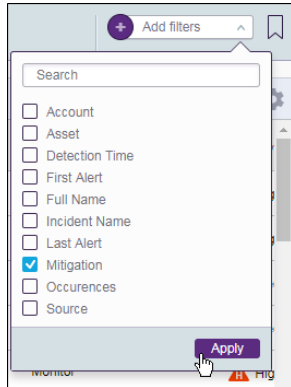
Some column values are links to relevant details elsewhere in Forcepoint CASB. Some columns that might require explanation are:

- ▶ **Category:** The data object category as in [Data Access policies](#).
- ▶ **Data Types:** As [configured](#) and tracked for DLP.
- ▶ **Client Location:** As configured in [internal IP ranges](#).
- ▶ **Managed:** Whether [enrolled](#).


To navigate through the pages, click the arrows next to the number of the activities above the table.

To filter the log results:

1. Click the **Add filters** drop-down menu.
2. Select one or more of the options and click **Apply**. The new filter is added to the list of active filters above the table.



---

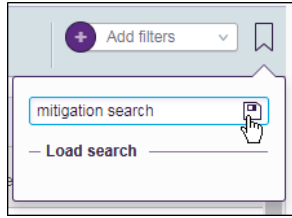
 **Note:** The filter values are dependent on the values available for that table and can differ from the values shown in the images above and below.

---


3. Expand the new filter, select the filter option, then click **Apply**.

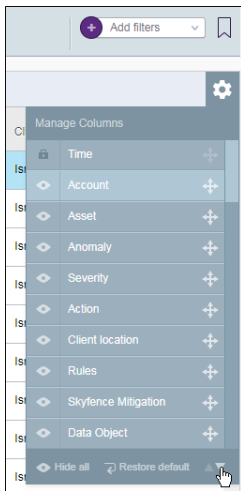


4. To save the current filters as a search, click the bookmark button to the right of the **Add filters** field, type a name for the search, and click the save button.




5. To load the saved search, click the button to the right of the **Add filters** field and select the search from the **Load search** list.

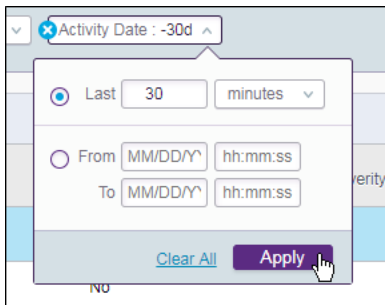
To configure the displayed columns and their order, click the  button.



To export the table to a CSV file, click . To refresh the display, click .

 **Note:** The CSV export is limited to the past 30 days or 100,000 entries, whichever is lower.

To limit the logs to represented activities from a recent specified time period, select the time period:



## Audit log column descriptions

The following table provides detailed descriptions about the type of information displayed in the Audit Log. While most of the columns are shared between Realtime Monitoring Audit Logs and Service Provider Logs Audit Logs, each log also displays some columns that are only available for that type of log. This information is included in the column description.

Column name	Column description
Time	The date and time when the activity took place (adjusted to the Forcepoint CASB administrator's time zone).  This column is labeled <b>Activity Date</b> in the Service Provider Logs Audit Log.
Account	The account used to access the cloud service (sAMAccountName if the Active Directory connection is set; otherwise, the login name).
Asset	The asset name assigned with the cloud service (e.g., My Office365).
Anomaly	A flag indicating if the activity is a breach of a Forcepoint CASB policy (Yes) or not (No).
Severity	The severity assigned with the Forcepoint CASB policy breached by the activity. If more than one policy was breached, the highest severity across these policies is displayed. This column is empty if no policy was breached.
Action	The activity performed by the user (e.g., view page, delete file).
Target	The activity's destination subject (e.g., the email destination, the person/group a file is shared with, the user account when an admin changes permissions)
Client location	The geographic location from which the user activity was detected.
Rules	The policy rules breached by the activity.
Mitigation Action	The mitigation action taken by Forcepoint CASB as a result of the policies breached by the activity.
Data Object	The cloud service object accessed.
Record	The record type depends on the action type. For example, when the user action is File Upload, the record contains the file name.
Properties	General properties relevant to the type of activity.
Message	The activity subject (e.g., the email subject, chat message, or searched

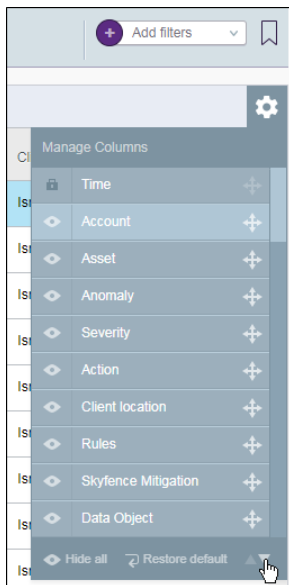
Column name	Column description
	content).
Impact Score	The impact score given to the activity by Forcepoint CASB. For more information, see <a href="#">"About the activity impact score" on page 51</a> .
Service Type	The sub-service used (e.g., Outlook Web Access or SharePoint Online for Office 365).
Full Name	The full name of the user. This data is retrieved from the Active Directory if integration is in place; otherwise, it is empty.
Category	The data object category (i.e., logical group based on the cloud service modules).
Data Types	The data types detected in the activity.
Data types occurrences	The total number of matched data types in the activity.
Managed	A flag indicating if the device used to access the service is "Managed" or "Unmanaged" by Forcepoint CASB.
Source IP	The source IP address for the activity.
Admin	A flag indicating if the user performing the activity is an administrator (Admin) or a user (User).
File Size	The size of the file accessed in the activity.
Event ID	A unique ID identifying the activity.
Activity Status	The activity status (Success / Failure / Unknown). This column is labeled <b>Status</b> in the Service Provider Logs Audit Log.
Data Types details	The data types detected in the activity.
Is sensitive data	A flag indicating whether the data detected in the activity is sensitive (Yes) or not sensitive (No).
File type	The type of the file related to the activity.
IP Chain	The IP chain of the client in the activity.



Column name	Column description
Title	The title of the user. This data is retrieved from the Active Directory if integration is in place; otherwise, it is empty.
Department	The business unit of the user. This data is retrieved from the Active Directory if integration is in place; otherwise, it is empty.
OS Username	The user name for the account logged in to the operating system of the computer used for the activity (available only when the Forcepoint CASB endpoint agent is deployed).
Endpoint type	The type of endpoint used for the activity. This column is labeled <b>Client Type</b> in the Service Provider Logs Audit Log.
Endpoint OS	The operating system of the endpoint used for the activity. This column is labeled <b>Device OS</b> in the Service Provider Logs Audit Log.
Host	The endpoint client hostname.
Service Location	The geographic location of the cloud service (based on destination IP).
Server IP	The IP address of the cloud service.
External	A flag indicating whether the endpoint client IP address is considered an external location (External) or an internal location (Internal). This is based on your organization's internal IP ranges settings. If the location cannot be determined, this flag displays "Unknown".
Authentication Type	The authentication method used for the activity (e.g., form authentication). This column is labeled <b>Authentication</b> in the Service Provider Logs Audit Log.
Direction	The data flow direction of the activity (Upload / Download).
Session ID	The session ID of the activity.
Device locale	The endpoint client locale (requires endpoint deployment).
User Agent	The endpoint client user agent.
Endpoint ID	The endpoint client assigned ID.
URL	The URL accessed in the activity.

Column name	Column description
Data policies	The data type policies detected in this activity.
Aggregation values	Data used to correlate this activity as part of a single incident.

In addition, Forcepoint CASB hides some columns from the default view. These columns can be added to the Audit Log view by selecting them from the Manage Columns menu.



The following columns are hidden by default.

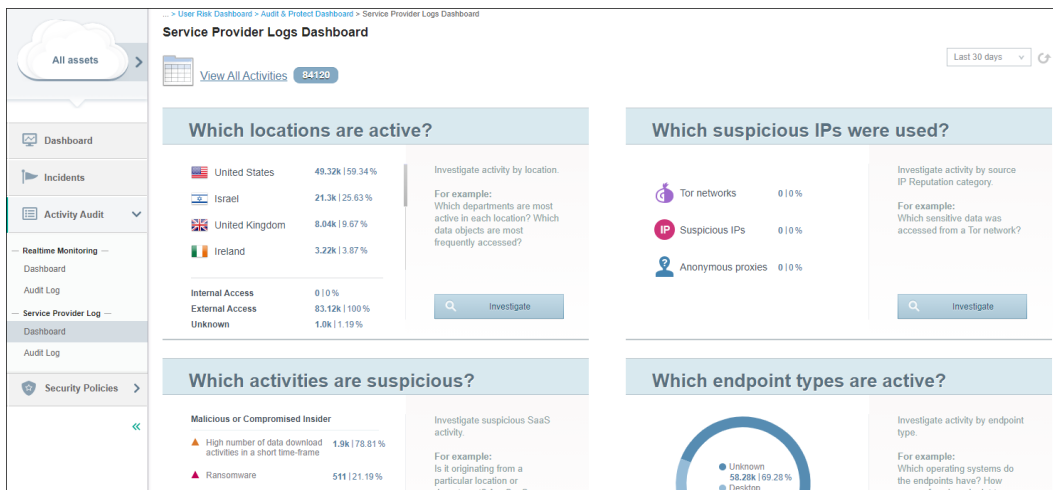
Column name	Column description
Login name	The account used to access the cloud service.
Data Object ID	The ID assigned to the data object.
Source IP reputation	The detected category based on the source IP address for the <a href="#">IP Reputation</a> service. The category can be either Anonymous proxies, Suspicious IPs, or Tor networks.
TOR Networks	The IP addresses of the Tor networks detected in the activity.
Anonymous proxies	The anonymous proxy IP addresses of the Tor networks detected in the activity.

Column name	Column description
Suspicious IPs	The suspicious IP addresses of the Tor networks detected in the activity.
Follow Up Mitigations	The mitigation actions taken after the activity is detected (e.g., Remove sharing permissions).
System messages	The error messages detected for the activity.
Amount	The monetary value of the activity.

## Graphically investigating activities

The **Activity Audit** dashboards provide statistics regarding user behavior, allowing you to investigate activity patterns, detect deviations from organizational workflows, identify missing access rules, and more.

The Activity Audit dashboards show various activity summary charts, such as the most active source locations or administrative activity. The summaries shown depend on availability of relevant activities, and whether **All Assets** or an individual asset is selected. For example:

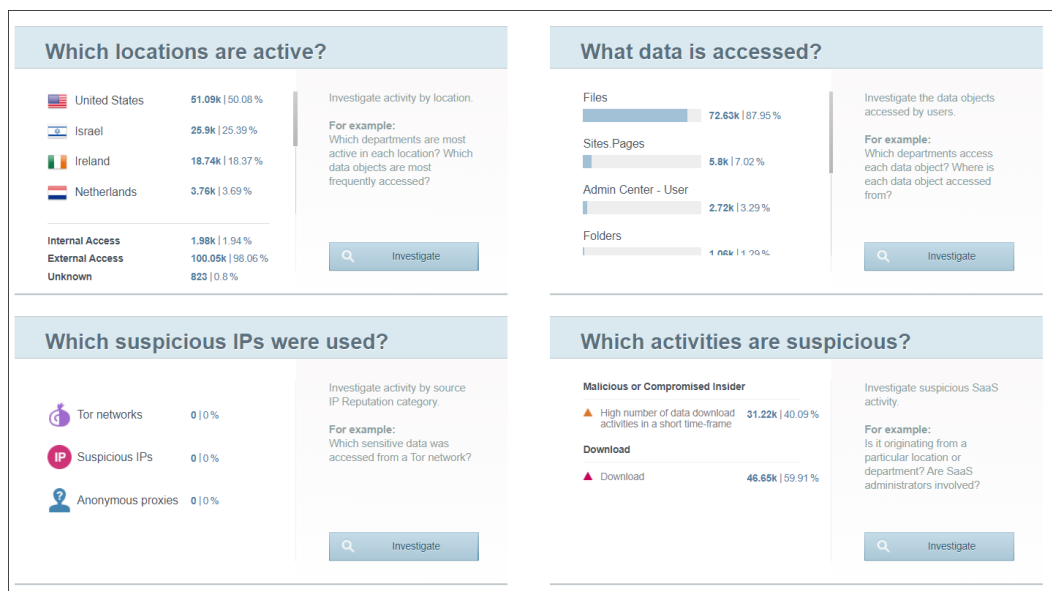


**Note:** The summary charts displayed in the Activity Audit dashboards might differ from those shown in the above example. The Activity Audit dashboards gather information from

- components within Forcepoint CASB. If a component is not set up, the chart is not displayed. For example, if DLP is not defined, then Forcepoint CASB is not capturing information about sensitive data and the Activity Audit does not display the "What sensitive data is being accessed?" chart.

For tracking user access behavioral patterns, from each chart you can click **Investigate** to view additional charts. For each value of the parent chart, Forcepoint CASB displays a group of child charts including only activities matching that value.

For example, if you notice activity from an unexpected location in the Active Locations chart, you can click **Investigate** to view a group of charts for each location, where you could check if users from the suspicious location are accessing any sensitive data objects:



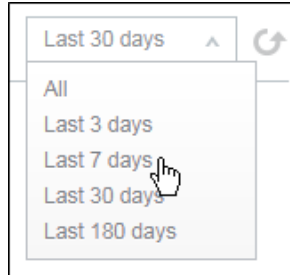
You can expand any of the groups to view its charts.


- Note:** Similar to the parent charts on the Activity Audit dashboards, the summary charts displayed in the child charts might differ from those shown in the above example. The child charts gather information from components within Forcepoint CASB. If a component is not set up, the chart is not displayed.

For another example, if you notice a significant number of unmanaged endpoints listed in the Dashboard, you could click **Investigate** to check if there is a correlation with any particular OS. This might indicate a problem with the distribution of endpoint routing solutions.

In the main Dashboard page or in any page of child charts:

- ▶ To drill down to [represented activity logs](#), click a representing number in the chart.
- ▶ To show only the activities from a recent, specific time period, select the time period:



- ▶ To refresh the dashboard data, click .



# CHAPTER 5

## Understanding Forcepoint CASB Policies


Forcepoint CASB | 2021 R4 | Updated: December 19, 2021

Forcepoint CASB analyzes all incoming user activity and compares it to the policies defined for that asset. If the user activity matches a policy, Forcepoint CASB applies the mitigation actions defined for that policy.

A policy is a set of rules that you can apply to the users of your sanctioned cloud services and the data that flows between your network and the cloud service. For example, if you do not want your users to store credit card information on a cloud service, you can set up a policy in Forcepoint CASB to block files with credit card numbers from being uploaded to the cloud service.

Forcepoint CASB provides standard policies that can be customized to fit your organization's security posture. These quick policies can be set up for user access management, user activity control, data leak prevention (DLP), and anomaly detection. If you would like to set up a policy that does not fit under a specific quick policy, you can create a custom policy where you define the policy's predicates (who, what, how, where, and when).

---

 **Note:** Quick and custom policies must be configured to match the user data activity type. User activity control, DLP, anomaly detection, and quick policies can be set up to mitigate both Proxy-based activities (i.e., realtime activities) and API-based activities (i.e., service provider log activities). User access management policies are only available for Proxy-based activities.

---

This chapter discusses the following:

Access policies .....	64
Anomaly detection policies .....	70
Data leak prevention policies .....	75
Custom policies .....	79

# Access policies

---

You can configure access policies to managed assets without needing to rely on applications' native permission systems, which in some cases can be limited or insecure. Forcepoint CASB includes several preconfigured simple access policies that can be enabled and in some cases further configured. Additionally, you can create granular custom policies.

If you have implemented Forcepoint CASB endpoint routing, you can block domains of services that should not be accessed from the organization.

## Enabling user access policies

Forcepoint CASB includes several preconfigured simple user access policies that can be enabled and in some cases further configured.

To enable simple access policies:

1. In Forcepoint CASB, go to **Audit & Protect > Security Policies > User Access Management**, select the relevant asset, then enable the relevant policies.



2. Some policies, when enabled, present configuration options. See the table below.
3. Optionally, select **Apply Changes to All Assets** to save these policy changes for all assets.
4. Click **Save Access Policies**.

The following user access management policies are available:

Policy	Description	Configurable options
Client Locations	Allow access only from specified countries	Select allowed source countries
Service Locations	Allow access only to services hosted in specified countries	Select allowed service countries
Endpoint Management	Allow access only from managed source devices	<ul style="list-style-type: none"> <li>▶ Select what to block from unmanaged devices: all access, or just downloads and/or data modifications</li> <li>▶ Configure <a href="#">enrollment criteria</a></li> </ul>
Internal Networks	Allow access only from inside organizational networks	Configure <a href="#">internal IP ranges</a>
Strong Authentication	Require identity verification by code sent via configured notification	<ul style="list-style-type: none"> <li>▶ Select whether to require verification for all activities, or just from unmanaged devices and/or from external networks</li> <li>▶ Configure relevant <a href="#">self-service notifications</a></li> <li>▶ Configure device <a href="#">enrollment criteria</a> and/or <a href="#">internal IP ranges</a></li> </ul>
IP Reputation	Block access from risky IP addresses	Select to block access from Tor networks, suspicious IP addresses, or anonymous proxies. To add exceptions to the restricted list, configure the <a href="#">trusted IP addresses</a> .



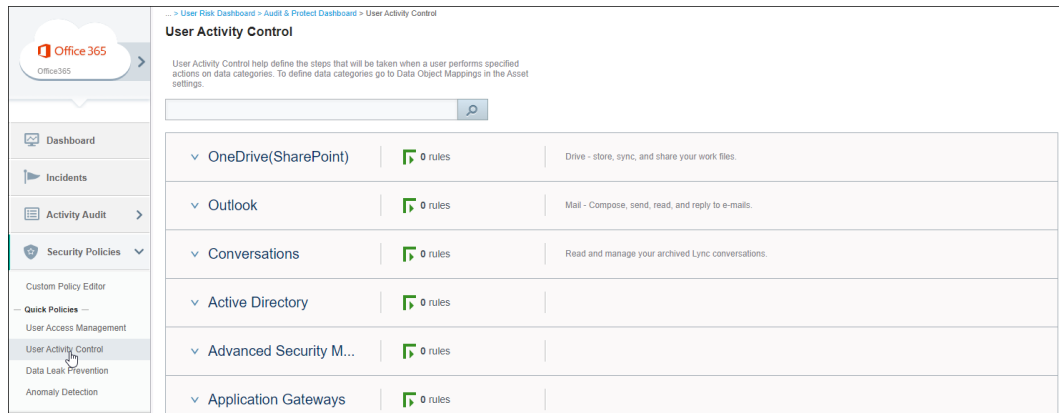
# Configuring user activity policies

You can easily configure policies to apply specified enforcement actions and notifications upon specified user actions on asset-specific predefined categories of relevant data objects.

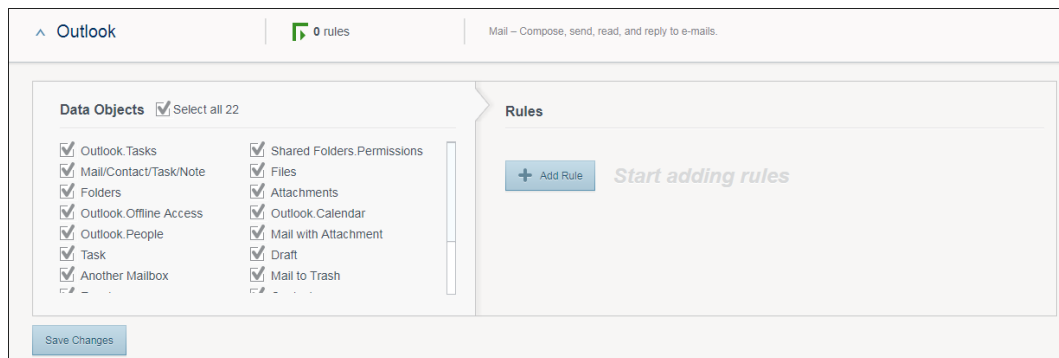
For greater flexibility, data object categories can also be used in [custom policies](#).

To configure a Data Access policy rule:

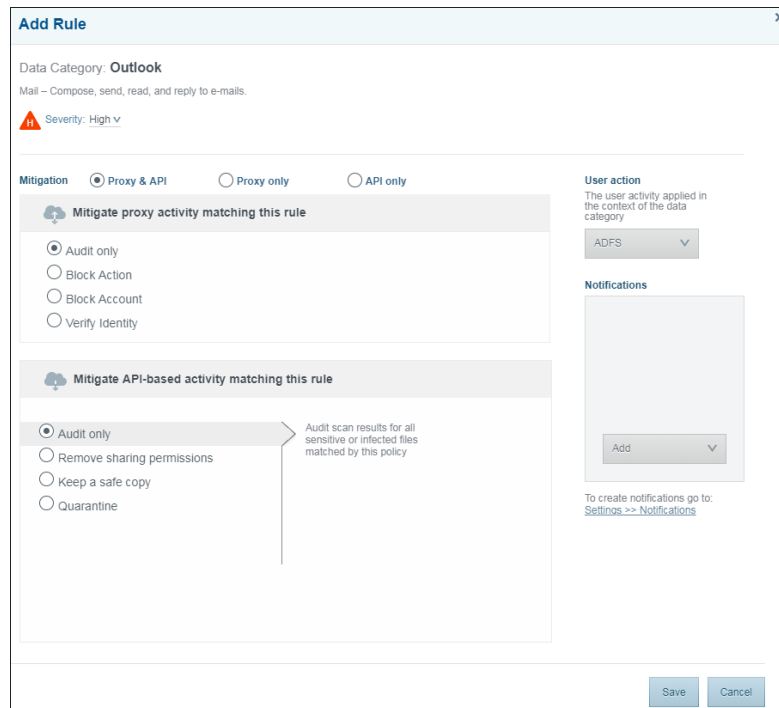
1. In Forcepoint CASB, go to **Audit & Protect > Security Policies > User Activity Control**:



2. To find which of the displayed category or categories includes a specific data object, use the Search field.
3. Expand the relevant data category:



4. Select one or more **Data Objects** to include in the rules, or select **Select all** to add all available data objects.
5. Click **Add Rule**:



6. Select a **Mitigation** option:
  - ▶ **Proxy & API:** Applies the rule to both proxy-based and API-based activities.
  - ▶ **Proxy only:** Applies the rule to activities captured through the proxy and recorded in the [Realtime Monitoring](#) Dashboard and Audit Log. The API-based Activity options are disabled.
  - ▶ **API only:** Applies the rule to activities captured through an API call and recorded in the [Service Provider Log](#) Dashboard and Audit Log. The Proxy-based Activity options are disabled.
7. If you selected **Proxy & API** or **Proxy only**, select one of the proxy-based mitigation rules:
  - ▶ **Audit:** An alert will appear in the Audit & Protect dashboard, and Forcepoint CASB will send notifications if configured (as below). Forcepoint CASB will allow the access.
  - ▶ **Block Action:** In addition to an alert and notifications as above, Forcepoint CASB will block this action. The user can continue to perform other actions.
  - ▶ **Block Account:** In addition to an alert and notifications as above, Forcepoint CASB

will lock this account until the alert is [released by a Forcepoint CASB Administrator](#).

- ▶ **Verify Identity:** In addition to an alert and notifications as above, Forcepoint CASB will send the user a verification code according to [asset identity verification settings](#) and block access until the user enters that code.
8. If you selected **Proxy & API** or **API only**, select one of the API-based mitigation rules:
- ▶ **Audit:** An alert will appear in the Audit & Protect dashboard, and Forcepoint CASB will send notifications if configured (as below). Forcepoint CASB will allow the access.
  - ▶ **Remove sharing permissions** (Office 365, Google G Suite, Salesforce, and Box only): In addition to an alert and notification as above, Forcepoint CASB will remove the sharing permissions for all or a partial set of users.
    - For Google G Suite and Salesforce assets: Select either **All** users (only the file's owner will be able to access the file) or a **Partial** set of users (only remove file sharing for users **External** to our organization, or remove file sharing from **Everyone**).

Optionally for G Suite assets, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.
    - For Office 365 and Box assets: Select **All** users to remove sharing permissions for all users (the file will only be accessible to the file owner), or select **Publicly Shared** to remove sharing permissions for users outside of your organization.

Optionally, select **Unshare parent folder** to remove sharing permissions for sensitive files that inherit the sharing permissions from one of their parent folders in the hierarchy. This removes the sharing permissions for the affected folders and all files located in them.

Optionally, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.
  - ▶ **Keep a safe copy:** In addition to an alert and notification as above, Forcepoint CASB will save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder. The Archive folder must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.
  - ▶ **Quarantine:** In addition to an alert and notification as above, Forcepoint CASB will move every infected or sensitive file that matches this policy to an authorized Archive folder. If you select **Leave a note**, Forcepoint CASB will leave a note in the

quarantined file's original location. This note will indicate to the user that the file is quarantined. The Archive folder and note must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.

9. Under **User actions**, select a user action trigger.
10. Under **Notifications**, click **Add** and select relevant notifications. To configure alert notifications for the policy rule here, you need to have configured relevant Alert [notifications](#) in Settings.
11. Click **Save** to save the rule and close the **Add Rule** window.
12. Click **Save Changes** to save the changes to the data category.

# Anomaly detection policies

---

For [managed assets](#), Forcepoint CASB can detect user account behavior that is anomalous relative to automatically learned usual behavior, according to preconfigured and configurable policies. Optionally, threat detection can trigger various security actions, including automatic account blocking.

For more information about analyzing user behavior, see ["User Behavior Analysis" on page 114](#).

Each predefined policy represents a different type of anomaly and defines several events that trigger an alert for this policy. You can configure policy rules to enable or disable them; to set their severity levels, alert notifications, and enforcement actions; and to exclude users.

## The anomaly detection policies table

The anomaly detection policy table lists all of the predefined anomaly detection policies. The policies are organized under policy categories, such as Brute Force and Account Takeover. From this table, you can enable, disable, and edit a policy. You can also sort the policies by clicking the column header. When you sort the policies, the policies are only sorted within their policy category.

To view the anomaly detection policy table, open Forcepoint CASB, go to **Audit & Protect > Security Policies > Anomaly Detection**, then select the relevant asset.

## Enabling or disabling a policy from the anomaly detection policy table

An anomaly detection policy must be enabled before it can start monitoring activity on the asset. To see if a policy is enabled, view the indicator under the **Status** column.

- ▶ If the indicator is **on**, the anomaly detection policy is enabled.
- ▶ If the indicator is **off**, the anomaly detection policy is disabled.

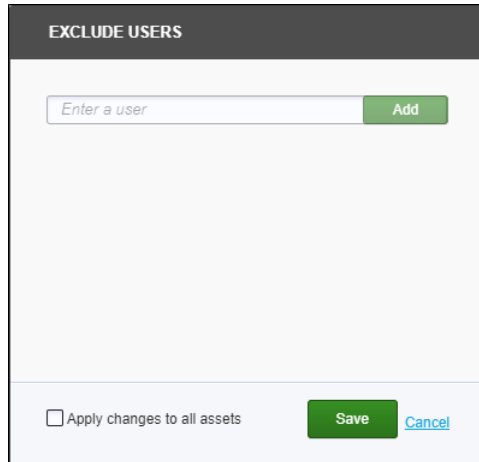
To change the status of the policy, click the toggle until it shows the desired status.

You can also change the status when you edit the policy. For information about editing an anomaly detection policy, see ["Configuring anomaly detection policies" on page 72](#).

## Excluding users from an anomaly detection policy

To exclude users from the policy trigger:

1. Expand the policy, then click **Exclude users**.
2. For each user to be excluded, type the account user name and click **Add**:



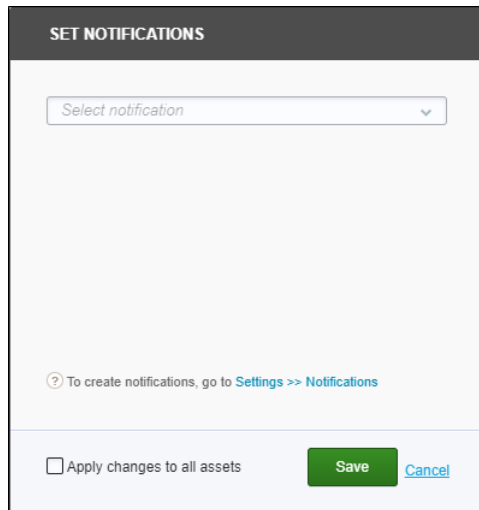
The screenshot shows a dialog box titled "EXCLUDE USERS". It features a text input field with the placeholder "Enter a user" and a green "Add" button. At the bottom, there is a checkbox for "Apply changes to all assets" and "Save" and "Cancel" buttons.

3. Optionally, select **Apply Changes to All Assets**. This option is effective if authentication is via an IdP, or if the user name is an email address. If you do not select this option, the changes here apply to the current asset only.
4. Click **Save**.

## Setting notifications for an anomaly detection policy

To configure alert notifications for the policy, you need to have configured relevant [Alert notifications](#). After alert notifications are configured, you can add them to anomaly detection policies:

1. In the policy, click **Set Notifications**.
2. Select the notification from the drop-down menu:



The list of notifications shown here come from the Notifications settings page. To create and configure new messages, go to **Settings > Notifications**.

3. Optionally, select **Apply Changes to All Assets**. If you do not select this option, the changes here apply to the current asset only.
4. Click **Save**.

## Configuring anomaly detection policies

To enable and configure a policy rule:

1. In Forcepoint CASB, go to **Audit & Protect > Security Policies > Anomaly Detection**.
2. Go to a policy you want to edit, then click the  edit icon:

Severity	Rule name	Real-time	API-based	Last updated	Status
<b>BRUTE FORCE</b>					
> 	Brute force attack from a single IP	Audit	Audit	27.06.19 02:26:39	 
> 	Brute force attack on a single account	Audit	Audit	27.06.19 02:26:39	 
> 	Successful Brute force attack on a single account	Audit	Audit	27.06.19 02:26:39	 
<b>ACCOUNT TAKEOVER</b>					
> 	Access from 3 countries within 30 minutes	Audit	Audit	27.06.19 02:26:39	 

The **Anomaly Detection Editor** window opens:

ANOMALY DETECTION EDITOR

**Brute force attack from a single IP**  
Multiple failed login attempts from a single IP.

Severity: ▲ High Status:  off Disabled

---

**Mitigation:**

Real-time: Audit ▼

API-based: Audit

---

**Thresholds:**

Max failed login attempts: 200

Time frame: 600 (seconds)

---

Apply changes to all assets Save [Cancel](#)

3. Select the **Severity** level.
4. Select the **Status**. This option can be either **Enabled** or **Disabled**.
5. Select the **Mitigation** for each relevant type of activity to which the rule should be applied:
  - ▶ **Real-time:** Applies the rule to activities captured through the proxy and recorded in the [Realtime Monitoring](#) Dashboard and Audit Log. The API-based Activity options are disabled.
  - ▶ **API-based:** Applies the rule to activities captured through an API call and recorded in the [Service Provider Log](#) Dashboard and Audit Log. The Proxy-based Activity options are disabled.

Select the relevant mitigation option:

- ▶ **Audit:** An alert will appear in the Audit & Protect dashboard, and Forcepoint CASB will send notifications if configured (as below). Forcepoint CASB will allow the access.
- ▶ **Block Action:** In addition to an alert and notifications as above, Forcepoint CASB



will block this action. The user can continue to perform other actions.

- ▶ **Block Account:** In addition to an alert and notifications as above, Forcepoint CASB will lock this account until the alert is [released by a Forcepoint CASB Administrator](#).
  - ▶ **Verify Identity:** In addition to an alert and notifications as above, Forcepoint CASB will send the user a verification code according to [asset identity verification settings](#) and block access until the user enters that code.
6. Depending on the policy you are editing, you may need to configure additional options. For example, in the image above, you need to provide **Thresholds**. The policy is triggered when the thresholds set here are met.
  7. Optionally, select to **Apply Changes to All Assets**. If you do not select this option, the changes here apply to the current asset only.
  8. Click **Save**.

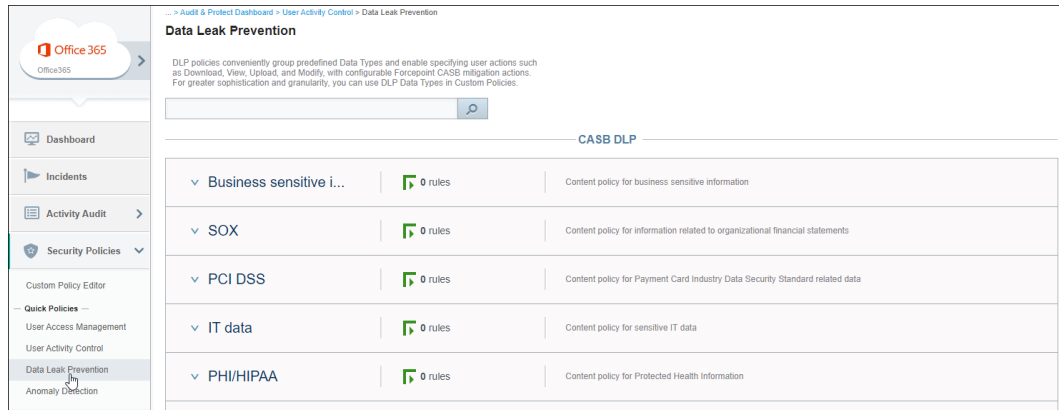
# Data leak prevention policies

You can use [data types](#) in [custom policies](#). However, if you don't need the level of sophistication and granularity available in [custom policies](#), you can quickly and easily configure regular data leak prevention (DLP) policies that conveniently group predefined data types into meaningful categories and allow you to specify user actions, such as Download, View, Upload, and Modify, with configurable Forcepoint CASB actions.

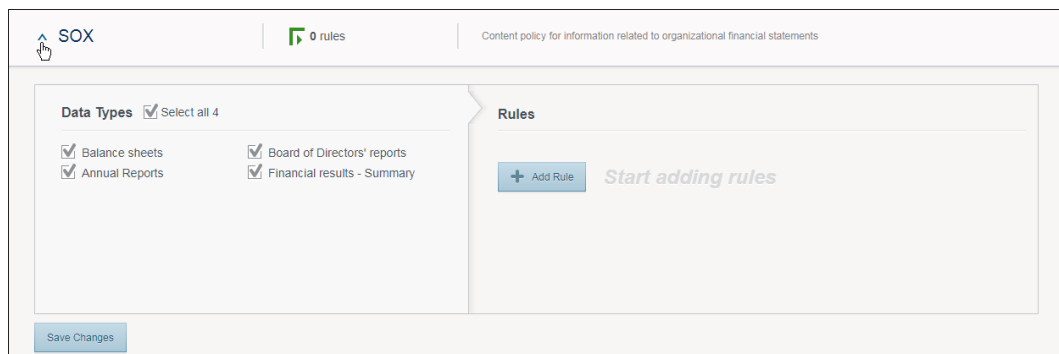
## Configuring data leak prevention policies

To configure a DLP policy rule:

1. In Forcepoint CASB, go to **Audit & Protect > Security Policies > Data Leak Prevention** for the relevant asset:



2. To find categories including a specific data type, use the search field.
3. Expand the relevant policy:



4. Select one or more **Data Types** to include in the policy, or select **Select all** to enable the policy for all available data types.
5. Click **Add Rule**.
6. Click **Enter Rule Name**, type a unique rule for the rule, then click the save icon next to the rule name field.

7. Select the **Severity** level.
8. Select a **Mitigation option**:
  - ▶ **Proxy & API**: Applies the rule to both proxy-based and API-based activities.
  - ▶ **Proxy only**: Applies the rule to activities captured through the proxy and recorded in the [Realtime Monitoring](#) Dashboard and Audit Log. The API-based Activity options are disabled.
  - ▶ **API only**: Applies the rule to activities captured through an API call and recorded in

the [Service Provider Log](#) Dashboard and Audit Log. The Proxy-based Activity options are disabled.

9. If you selected **Proxy & API** or **Proxy only**, select one of the proxy-based mitigation rules:

- ▶ **Audit:** An alert will appear in the Audit & Protect dashboard, and Forcepoint CASB will send notifications if configured (as below). Forcepoint CASB will allow the access.
- ▶ **Block Action:** In addition to an alert and notifications as above, Forcepoint CASB will block this action. The user can continue to perform other actions.
- ▶ **Block Account:** In addition to an alert and notifications as above, Forcepoint CASB will lock this account until the alert is [released by a Forcepoint CASB Administrator](#).
- ▶ **Verify Identity:** In addition to an alert and notifications as above, Forcepoint CASB will send the user a verification code according to [asset identity verification settings](#) and block access until the user enters that code.

10. If you selected **Proxy & API** or **API only**, select one of the API-based mitigation rules:

- ▶ **Audit:** An alert will appear in the Audit & Protect dashboard, and Forcepoint CASB will send notifications if configured (as below). Forcepoint CASB will allow the access.
- ▶ **Remove sharing permissions** (Office 365, Google G Suite, Salesforce, and Box only): In addition to an alert and notification as above, Forcepoint CASB will remove the sharing permissions for all or a partial set of users.
  - For Google G Suite and Salesforce assets: Select either **All** users (only the file's owner will be able to access the file) or a **Partial** set of users (only remove file sharing for users **External** to our organization, or remove file sharing from **Everyone**).  
Optionally for G Suite assets, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.
  - For Office 365 and Box assets: Select **All** users to remove sharing permissions for all users (the file will only be accessible to the file owner), or select **Publicly Shared** to remove sharing permissions for users outside of your organization.  
Optionally, select **Unshare parent folder** to remove sharing permissions for sensitive files that inherit the sharing permissions from one of their parent folders in the hierarchy. This removes the sharing permissions for the affected folders and all files located in them.

Optionally, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.

- ▶ **Keep a safe copy:** In addition to an alert and notification as above, Forcepoint CASB will save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder. The Archive folder must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.
- ▶ **Quarantine:** In addition to an alert and notification as above, Forcepoint CASB will move every infected or sensitive file that matches this policy to an authorized Archive folder. If you select **Leave a note**, Forcepoint CASB will leave a note in the quarantined file's original location. This note will indicate to the user that the file is quarantined. The Archive folder and note must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.

11. Under **User actions**, click **Add** to select user action triggers.
12. Under **Notifications**, click **Add** and select relevant notifications. To configure alert notifications for the policy rule here, you need to have configured relevant [Alert notifications](#) in Settings.
13. Click **Save** to save the rule and close the **Add Rule** window.
14. Click **Save Changes** to save the policy.

# Custom policies

You can create custom policies to be triggered by granularly defined custom conditions. Conditions are configured as Boolean logical phrases (AND / OR / NOT) of generic and asset-specific parameters (**predicates**). For a list of available predicates, see "[Custom access policy predicates](#)" on page 88.

For example, the following Office 365 policy condition defines that the policy should be triggered if any user tries to delete a Word template (.dot, .dotx, or .dotm) or SharePoint site:

**Condition**  
Create your policy by choosing predicates and operators

... [Action: delete] ... AND ... ( ... [Record: \*.dotx, \*.dot, \*.dotm] ... OR ... [Data Object: Sites] ... ) ...

**Summary:** Any occurrence of: Action is [ delete ] AND ( Record is [ \*.dotx , \*.dot , \*.dotm ] OR...  
[Clear Condition](#)  
[Set Occurrences](#) [Incident Settings](#)

A policy can be configured to be triggered only if the condition is met a specified number of times in a session. You can set the policy's severity level, alert notifications, and enforcement actions, and you can exclude users from the policy.

The **What > Data Object Category** predicate categorizes data objects as in [Data Access policies](#).

## The custom policy table

The custom policy table lists all custom policies created for a specific asset. You can add a new custom policy (rule), edit an existing custom policy, and enable or disable the policy. You can also sort all custom policies by column header.

To view the custom policy table, open Forcepoint CASB, go to **Audit & Protect > Security Policies > Custom Policy Editor**, then select the relevant asset.

For information about adding a new custom policy, or editing an existing policy, see "[Configuring custom policies](#)" below.

## Enabling or disabling a custom policy from the custom policy table

A custom policy must be enabled before it can start monitoring activity on the asset. To see if a custom policy is enabled, view the indicator under the **Status** column.

- ▶ If the indicator is **on**, the custom policy is enabled.
- ▶ If the indicator is **off**, the custom policy is disabled.

To change the status of the custom policy, click the toggle until it shows the desired status.

You can also change the status when you edit the custom policy. At the top of the custom policy's Editor page, select the status from the drop-down.

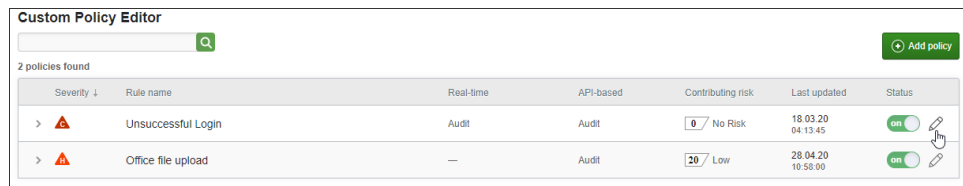
## Configuring custom policies

To configure a custom policy:

1. In Forcepoint CASB, go to **Audit & Protect > Security Policies > Custom Policy Editor**, select the relevant asset, and do one of the following:
  - ▶ To add a new policy, click **Add policy**:



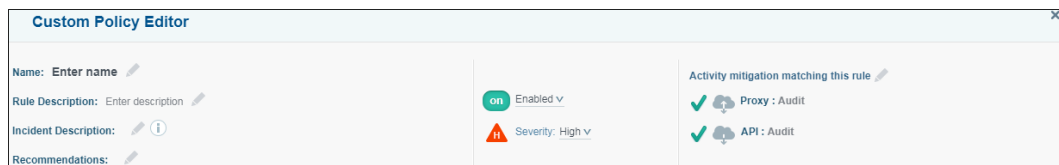
To edit an existing policy, find the policy in the table, then click the pencil icon:



The screenshot shows the 'Custom Policy Editor' interface with a table of policies. The table has columns for Severity, Rule name, Real-time, API-based, Contributing risk, Last updated, and Status. Two policies are listed: 'Unsuccessful Login' and 'Office file upload'. The 'Unsuccessful Login' policy has a severity of 'No Risk' and is 'on'. The 'Office file upload' policy has a severity of 'Low' and is 'on'. A pencil icon is visible next to the status of the 'Office file upload' policy.

Severity ↓	Rule name	Real-time	API-based	Contributing risk	Last updated	Status
> ▲	Unsuccessful Login	Audit	Audit	0 / No Risk	18.03.20 04:13:45	on
> ▲	Office file upload	—	Audit	20 / Low	28.04.20 10:58:00	on

2. Enter a **Policy Name**, **Rule Description**, **Incident Description**, and **Recommendations**:



The screenshot shows the 'Custom Policy Editor' form. It has fields for Name, Rule Description, Incident Description, and Recommendations. The Status is set to 'Enabled' and the Severity is 'High'. The Activity mitigation section shows 'Proxy : Audit' and 'API : Audit' with checkmarks.

The Recommendations text is displayed in the Incident record.

3. Select **Enabled** and a **Severity** level.
4. Click the **Activity mitigation matching this rule** edit icon, then select a **Mitigation** option:
  - ▶ **Proxy & API:** Applies the rule to both proxy-based and API-based activities.
  - ▶ **Proxy only:** Applies the rule to activities captured through the proxy and recorded in the [Realtime Monitoring](#) Dashboard and Audit Log. The API-based Activity options are disabled.
  - ▶ **API only:** Applies the rule to activities captured through an API call and recorded in the [Service Provider Log](#) Dashboard and Audit Log. The Proxy-based Activity options are disabled.
5. If you selected **Proxy & API** or **Proxy only**, select one of the proxy-based mitigation rules:
  - ▶ **Audit:** An alert will appear in the Audit & Protect dashboard, and Forcepoint CASB will send notifications if configured (as below). Forcepoint CASB will allow the access.
  - ▶ **Block Action:** In addition to an alert and notifications as above, Forcepoint CASB will block this action. The user can continue to perform other actions.
  - ▶ **Block Account:** In addition to an alert and notifications as above, Forcepoint CASB will lock this account until the alert is [released by a Forcepoint CASB Administrator](#).
  - ▶ **Verify Identity:** In addition to an alert and notifications as above, Forcepoint CASB will send the user a verification code according to [asset identity verification settings](#) and block access until the user enters that code.
6. If you selected **Proxy & API** or **API only**, select one of the API-based mitigation rules:
  - ▶ **Audit:** An alert will appear in the Audit & Protect dashboard, and Forcepoint CASB will send notifications if configured (as below). Forcepoint CASB will allow the access.
  - ▶ **Remove sharing permissions** (Office 365, Google G Suite, Salesforce, and Box only): In addition to an alert and notification as above, Forcepoint CASB will remove the sharing permissions for all or a partial set of users.
    - For Google G Suite and Salesforce assets: Select either **All** users (only the file's owner will be able to access the file) or a **Partial** set of users (only remove file sharing for users **External** to our organization, or remove file sharing from **Everyone**).



Optionally for G Suite assets, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.

- For Office 365 and Box assets: Select **All** users to remove sharing permissions for all users (the file will only be accessible to the file owner), or select **Publicly Shared** to remove sharing permissions for users outside of your organization.

Optionally, select **Unshare parent folder** to remove sharing permissions for sensitive files that inherit the sharing permissions from one of their parent folders in the hierarchy. This removes the sharing permissions for the affected folders and all files located in them.

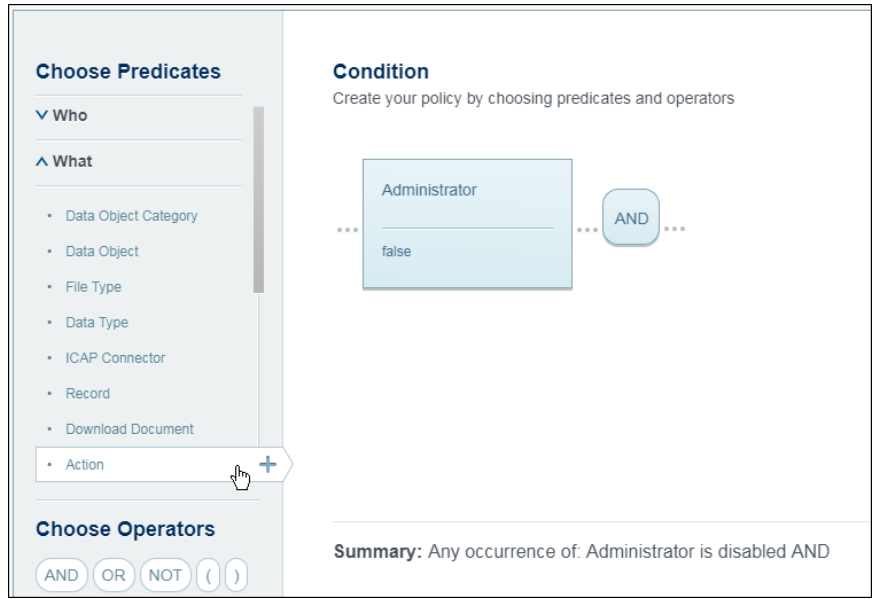
Optionally, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.


- ▶ **Keep a safe copy:** In addition to an alert and notification as above, Forcepoint CASB will save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder. The Archive folder must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.
- ▶ **Quarantine:** In addition to an alert and notification as above, Forcepoint CASB will move every infected or sensitive file that matches this policy to an authorized Archive folder. If you select **Leave a note**, Forcepoint CASB will leave a note in the quarantined file's original location. This note will indicate to the user that the file is quarantined. The Archive folder and note must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.

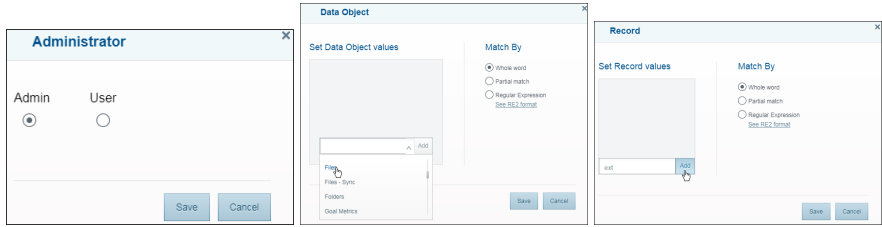
7. Click **Save** to return to the **Custom Policy Editor**.

8. Configure the **Condition** that will trigger the above policy action:

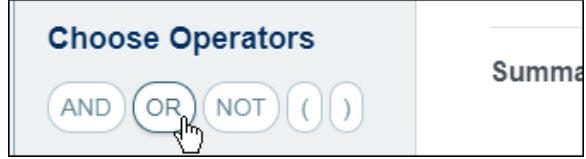
- ▶ To add a parameter (**Predicate**) to the condition, expand a category (**Who, What, How, Where, or When**) and click a parameter.



- ▶ To set a parameters value(s):
  - ▶ In the parameter, click .
  - ▶ Depending on the parameter type, select, select and **Add**, or type and **Add**; then click **Save**:

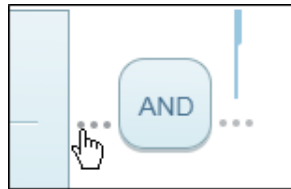


- ▶ To add a Boolean operator, click **AND**, **OR**, **NOT**, **(**, or **)** under the **Choose Operations** section.

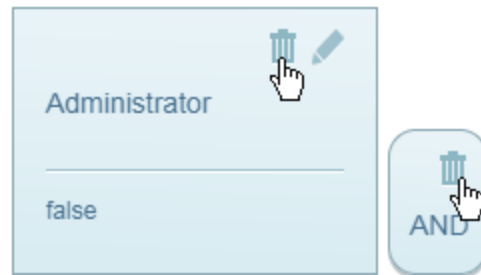


- ▶ Parameters and operators are added at the insertion point ( | ). To set the insertion

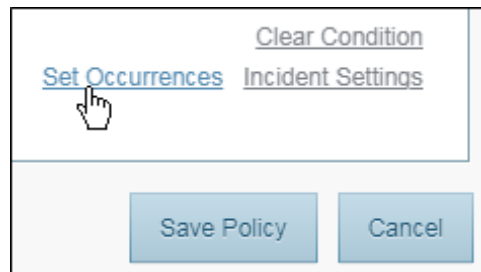
point's location, click ... :



- ▶ To remove an element (parameter or operator), click :



9. To set the policy to be triggered only if the condition is met a specified number of times in a session, click **Set Occurrences**:



- a. Select one of the available options:

**Frequency Settings**

Apply this policy:

Only if the policy condition is met  times within 24 hours

On any event that matches the policy condition

Save Cancel

- ▶ Select **Only if the policy condition is met \_\_ times within a session**, then type the number of occurrences, to identify the user activities that matches this custom policy only if they recur a specific number of times in one day.
- ▶ Select **On any event that matches the policy condition** to apply this policy to every user activity that matches this custom policy.

- b. Click **Save**.

10. To configure the custom policy settings for Incidents, click **Incident Settings**.

**Incident Settings**

**Incident risk contribution**

When a custom rule is matched it may impact the calculation of the account risk. You may use the following risk levels to change the risk contribution of incidents matching this rule

No Risk

**Incident aggregation parameters**

Forcepoint CASB aggregates multiple occurrences of similar alerts happening in a short time frame to a single incident. Incidents are aggregated by user account, matched rule, and time aggregation parameters. Use this page to modify the time aggregation parameters for this rule.

**Incident span time**

Alerts will be aggregated into the same incident as long as they continue to occur in this timeframe (sliding). For example, if the same alert happens every 10 minutes and the aggregation span time is 30 minutes we will continue to aggregate coming alerts into the same incident.

1 Hours

**Incident max aggregation time**

Max aggregation time defines the maximum time frame for an incident after which a new incident will be created even if new alerts are still within the incident span time. For example: regardless of the aggregation span time, create new alert every 24 hours if the attack continues. If not defined it will be regarded as infinity.

24 Hours

Save Cancel

- a. Select the **Incident risk contribution** from the drop-down menu: **No Risk, Low, Medium, or High**.

This is the risk level for this custom policy. When an alert from this custom policy is added to an Incident, the risk level selected here impacts the Incident's overall risk level.

- b. Select the **Incident span time**. You must select both a duration (number) in the first field and a unit (**Hours or Minutes**) in the second field.

The Incident span time is the time frame when Forcepoint CASB adds a new alert to the same Incident after the last alert is added to the Incident. The duration timer starts when the last alert is added to the Incident. When this time expires, a new alert creates a new Incident.

For example, set an Incident span time of 30 minutes. If Forcepoint CASB creates a new Incident based on an alert, then a new alert matching the policy from the first alert is recorded 28 minutes later, the new alert is added to the Incident. If the new alert is recorded 31 minutes after the previous alert, it is outside of the span time, so Forcepoint CASB creates a new Incident and resets the span time.

- c. Select the **Incident max aggregation time**. You must select both a duration (number) in the first field and a unit (**Hours or Minutes**) in the second field.

The max aggregation time is the total time where alerts can be added to an Incident, regardless of Incident span time. The duration timer starts when the first alert is added to the Incident. When this time runs out, a new Incident is created and the max aggregation time resets.

For example, set the Incident span time to 30 minutes and the max aggregation time to 2 hours. If new alerts are recorded at 30 minutes, 1 hour, 1 hour 30 minutes, 2 hours, and 2 hours 30 minutes, the first 4 alerts are added to the same Incident. The last alert (at 2 hours 30 minutes) is outside of the max aggregation time (2 hours), so it is added to a new Incident, even though it is within the span time since the previous alert (30 minutes).

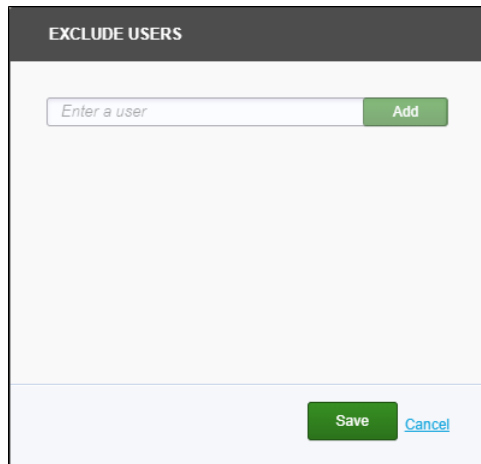
- d. Click **Save**.

11. Click **Save Policy**.

## Excluding users from a custom policy

To exclude users from the policy:

1. Expand the policy, then click **Exclude users**.
2. For each user to be excluded, type the account user name and click **Add**:

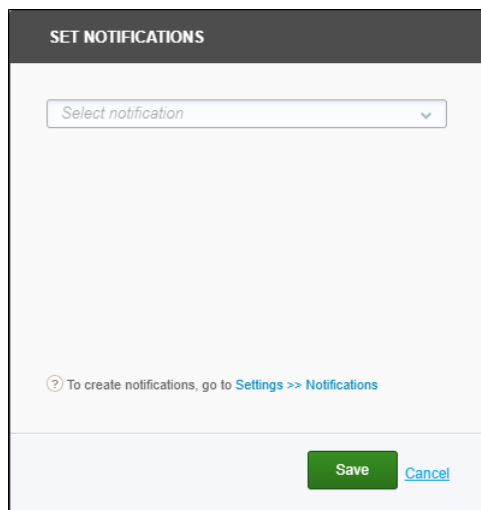


3. Click **Save**.

## Setting notifications for a custom policy

To configure alert notifications for the policy, you need to have configured relevant [Alert notifications](#). After alert notifications are configured, you can add them to your custom policies:

1. Expand the policy, then click **Set Notifications**.
2. Select the notification from the drop-down menu:



The list of notifications shown here come from the Notifications settings page. To create

and configure new messages, go to **Settings > Notifications**.

3. Click **Save**.

## Deleting a custom policy

To delete a custom policy:

1. Expand the policy, then click **Delete rule**.
2. In the confirmation box, click **Yes, delete this rule**.

The custom policy is removed from your list of custom policies.

## Custom access policy predicates

The following configurable predicates are available in custom policies.

Section	Predicate	Value for Matching	Description
Who	Login name	String: exact / partial / RegEx	Username used to log into the service asset
	Account	String: exact / partial / RegEx	Account name from the known user directory. See <a href="#">"Providing a user directory" on page 182</a> .
	Full name	String: exact	The account user's full name from the known user directory. See <a href="#">"Providing a user directory" on page 182</a> .
	Source IP	IP network: CIDR	Endpoint IP address as identified by Forcepoint CASB gateway
	External IP	<b>External / Internal</b>	Endpoint IP address compared to known organizational networks. See <a href="#">"Configuring IP ranges" on page 233</a> .
	Host name	String: exact / partial / RegEx	Endpoint hostname
	Business Unit	Drop-down list	Account department from the

Section	Predicate	Value for Matching	Description
			known user directory. See <a href="#">"Providing a user directory" on page 182.</a>
	Administrator	<b>Admin / User</b>	User's role in service asset
	Custom1 Custom2 Custom3	String: exact / partial / RegEx	User's custom data from the known user directory. See <a href="#">"Providing a user directory" on page 182.</a>
	OS Username	String: exact / partial / RegEx	User name for the account logged in to the operating system of the computer used for the activity
What	Data Object Category	Drop-down list	Category of accessed service asset component, as listed in data access policies. See <a href="#">"Configuring user activity policies" on page 66.</a>
	Data Object	Drop-down list + String: exact / partial / RegEx	Name of accessed service asset component, as listed in data access policies. See <a href="#">"Configuring user activity policies" on page 66.</a>
	File Type	Drop-down list	Type of accessed or uploaded file
	Data Type	Drop-down list	Detected data types of accessed or uploaded file. See <a href="#">"Configuring data types" on page 249.</a>
	ICAP Connector	Drop-down list	The ICAP connector configured in Forcepoint CASB
	Record	String: exact / partial / RegEx	Relevant content text such as file or folder name, posted comment, or IP address



Section	Predicate	Value for Matching	Description
	Download Document	String: exact / partial / RegEx	Name of downloaded file
	Action	Drop-down list	Service asset-specific available activities
	Action status	<b>Success / Failure</b>	Whether the action succeeded or not
	File size	<b>Upload</b> and/or <b>Download</b> + number + <b>KB / MB / GB</b>	Size of uploaded or downloaded file. Files at least this size match
	Unusual activity volume	<b>All user activities / Download activities</b>	The type of activity to evaluate
	Forcepoint DLP	N/A	Monitors activity through the Forcepoint DLP connection
	Server IP	IP network: CIDR	IP address of accessed service asset's server
	URL	String: exact / partial / RegEx	Accessed URL
	Target	String: exact / partial / RegEx	The activity's destination subject (e.g., the email destination, the person/group a file is shared with, the user account when an admin changes permissions)
	Data object ID	String: exact / partial / RegEx	The ID assigned to the data object
	Message	String: exact / partial / RegEx	The activity subject (e.g., the email subject, chat message, or searched content)
	Properties	String: exact / partial / RegEx	General properties relevant to the type of activity
	Amount	Drop-down list	The monetary value of the activity

Section	Predicate	Value for Matching	Description
	Impact Score	<b>Critical / High / Medium / Low / Custom</b>	The impact score given to the activity by Forcepoint CASB. See <a href="#">"About the activity impact score"</a> on page 51.
How	Endpoint Type	<b>Desktop / Mobile</b>	Whether the endpoint is a desktop or a mobile device
	Endpoint ID	String: exact	Forcepoint CASB's identifier for the endpoint, as appearing in <b>Endpoints</b>
	Endpoint Enrollment	<b>Managed / Unmanaged</b>	Whether the endpoint is enrolled as managed. See <a href="#">"Endpoint enrollment"</a> on page 224.
	Typical user endpoint	Boolean	Whether the endpoint is typically used to access this service asset
	Endpoint OS	String: exact / partial / RegEx	Endpoint operating system
	Service Type	Drop-down list	Service asset-specific applications. For example, for Office 365: OneDrive, Outlook, Lync, etc.
	Authentication	Check boxes	Authentication protocol used
	User Agent	String: exact / partial / RegEx	Client application originating the activity
	Locale	Drop-down list	Country code as defined in endpoint OS locale
Where	Client Location	Drop-down list	Country name by endpoint IP address
	Typical Client Location	Boolean	Whether this user typically accesses the service asset from this country

Section	Predicate	Value for Matching	Description
	Service Location	Drop-down list	Country name of accessed service asset server
	IP Reputation Category	Check boxes	The IP address source category for the <a href="#">IP Reputation</a> service: Tor networks, suspicious IPs, and anonymous proxies
When	Time Frame	Day(s) of week + From HH:mm to HH:mm	When the activity occurred



# CHAPTER 6

## Security Monitoring and Enforcement

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

Forcepoint CASB provides visibility into the user activity performed on your organization's sanctioned cloud applications. By providing this visibility, you can apply controls, such as policy-based access controls, and build a user behavior profile to detect anomalous behavior that suggests an account takeover or malicious intent.

The Audit & Protect dashboard provides the visibility into a user's activities. From there, you can drill-down to the activities and incidents that affect the security posture of your organization.

This chapter discusses the following:

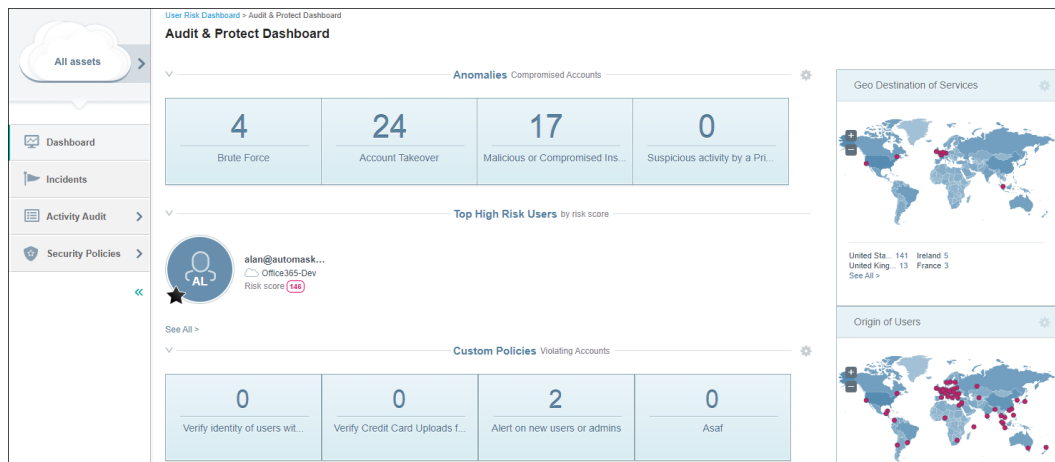
Monitoring and investigating security .....	94
---	----

# Monitoring and investigating security

For cloud services that have been defined as [managed assets](#), the [Audit & Protect Dashboard](#) provides an overview of the accounts at risk based on policy violations for **All Assets** or for a selected asset. The Audit & Protect Dashboard also includes activity summaries for both Real-Time and Service Provider Log activity.

The Audit & Protect Dashboard provides visibility into two types of information:

- ▶ **Processed, policy-based information:** This information violates a policy set by the organization and requires mitigation. For more information, see "[Policy violations](#)" below.
- ▶ **Statistical information:** This summary information allows you to gain insights based on your organization's Real-time and Service Provider Log activity. These summaries help adjust work processes and detect issues based on existing issue data. For more information, see "[Security activity analysis](#)" on page 97.

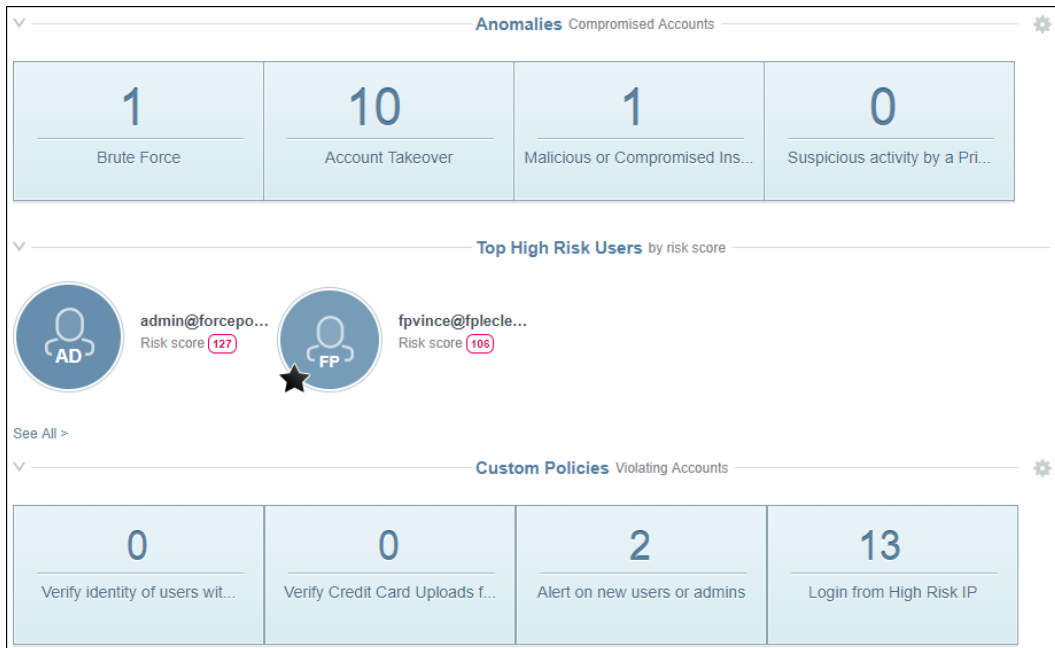


The Audit & Protect dashboard includes three areas, as explained in the following sections.

## Policy violations

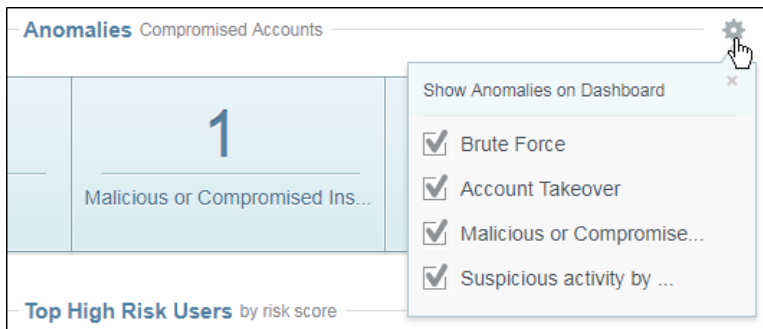
The [Audit & Protect Dashboard](#) displays the number of policy violations, grouped by:

- ▶ **Anomalies:** Includes accounts where violations of the Anomaly detection policies were detected.
- ▶ **Top High Risk Users:** Includes the top 5 user accounts in the organization that are considered high risk (based on risk level).
- ▶ **Custom Policies:** Includes accounts where violations of [custom policies](#) were detected.



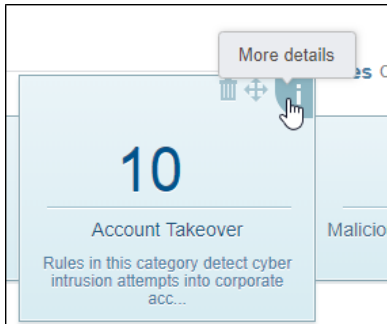
Each group area is collapsible (above it, click ▾).

Each policy in the group area displays the number of violating user accounts. To configure which policies are displayed, click ⚙️:

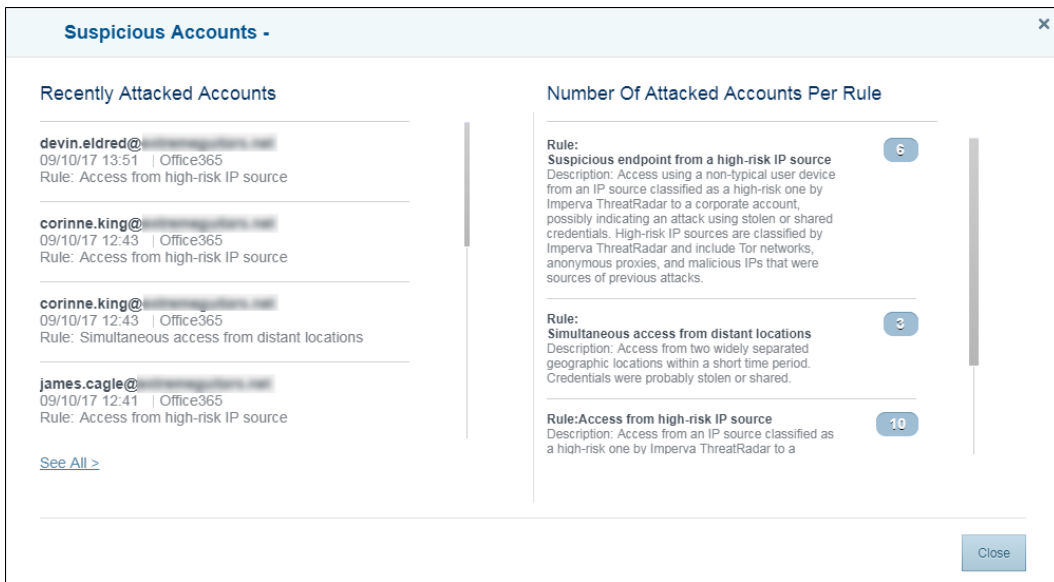


Any policy can be used for a [detail widget](#).

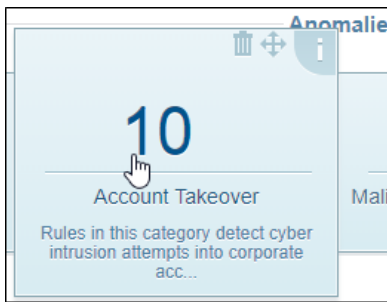
To view recent violations and per-rule violations, hover the mouse pointer over the policy and click **i**:



Forcepoint CASB opens a screen that displays the recent violations and per-rule violations:



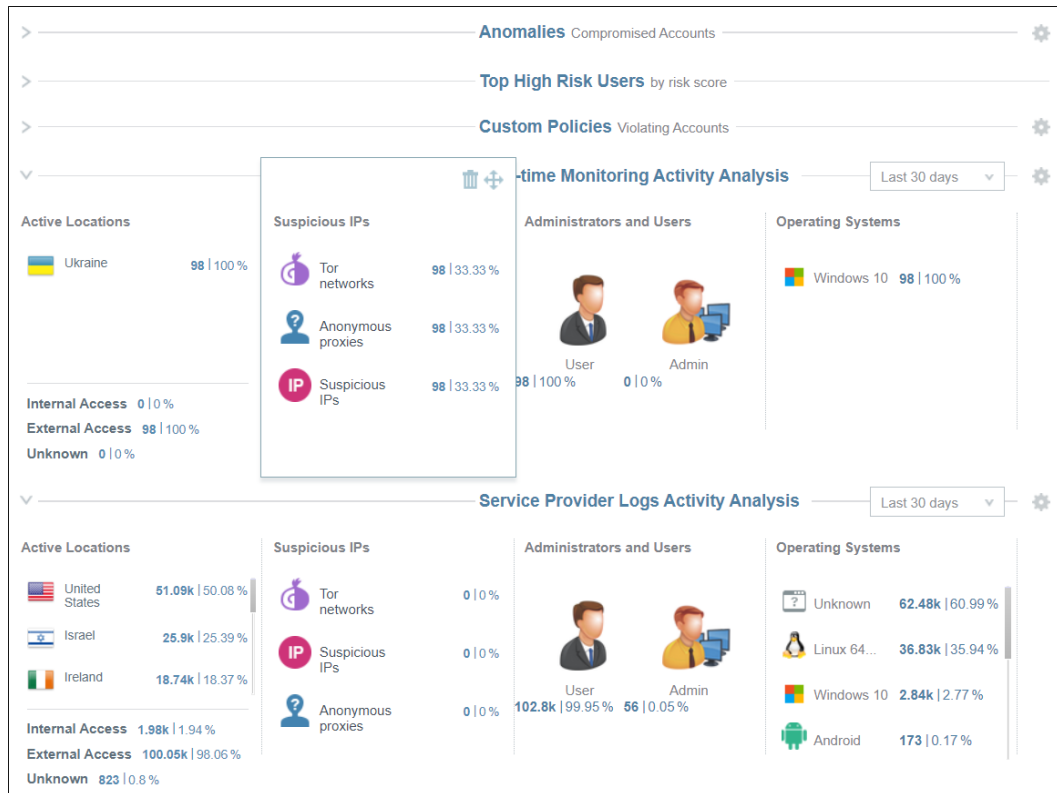
To view violation details by accounts and to handle violations, click the number:




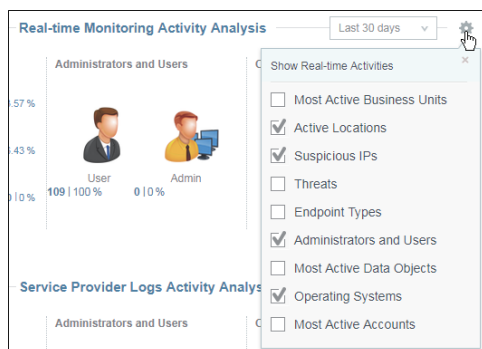
Forcepoint CASB opens the [Accounts page](#), filtered to display accounts that violated the policy. There, you can [handle the violations](#).

# Security activity analysis

The bottom of the [Audit & Protect Dashboard](#) displays several activity summaries that can be useful in the context of security analysis:



The Audit & Protect dashboard separates these summaries by monitoring type: **Real-time Monitoring Activity Analysis** and **Service Provider Logs Activity Analysis**. To configure which summaries are displayed, click  :



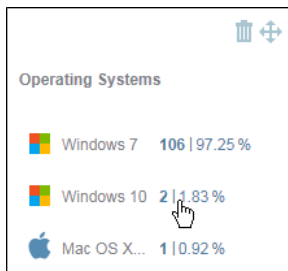


Any of the summaries can also take the place of a [detail widget](#).

To configure the time period, open the drop-down menu in the top-right corner and select one of the available options:



To view represented activities in the [Analytics page](#), click a number or account in the summary:




## Security detail widgets

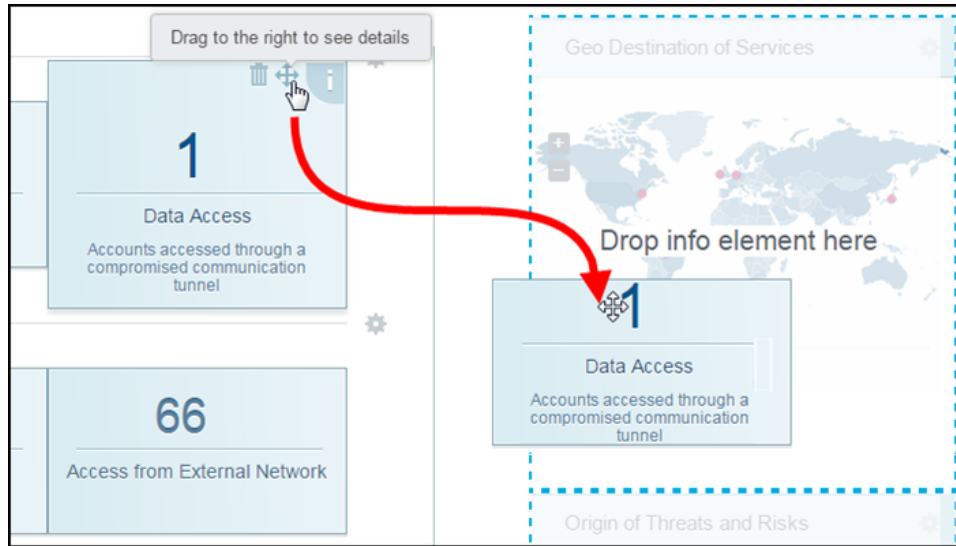
The right side of the [Audit & Protect Dashboard](#) includes two frames containing detail widgets. By default, the two widgets are **Geo Destination of Services** (asset server locations) and **Origin of Threats** (policy violation source locations):



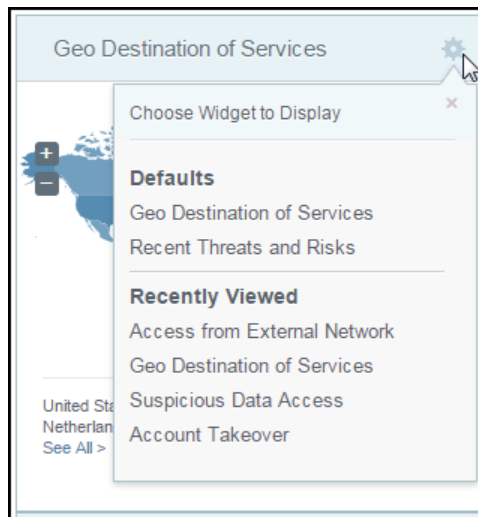
To view represented [activities](#), click a number in the widget.

You can replace the contained detail widgets with widgets containing details of [policy violations](#) or with [security activity summaries](#), in either of two ways:

- ▶ Hover the mouse pointer over a policy violation or activity summary, and drag the  onto a detail widget:



- To display a recent or default widget, click  on a detail widget, then select a widget:





# CHAPTER 7

## Monitoring and Investigating Alerts and Incidents

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

Forcepoint CASB analyzes user activity to determine if the activity breaks a policy rule. If the activity breaks a policy rule, it becomes an alert. Forcepoint CASB then analyzes all incoming alerts for similarities, such as a common alert type or user account. These similar activity alerts are grouped together into an Incident record.

Incidents let you see and understand the overall problems affecting your network, instead of searching through and investigating the multiple individual symptoms of the problem. For example, you can review a list of incidents and quickly see a Brute Force attempt on your network instead of searching through potentially thousands of alerts to find each Brute Force alert and investigate every alert to see if they are connected.

By combining these alerts into a single incident, the alerts in the incident can be monitored, acknowledged, or ignored either individually or as a group.

This chapter discusses the following:

The Incidents log .....	102
Incidents log column descriptions .....	106
Incident records .....	109
Handling policy violations .....	112

# The Incidents log

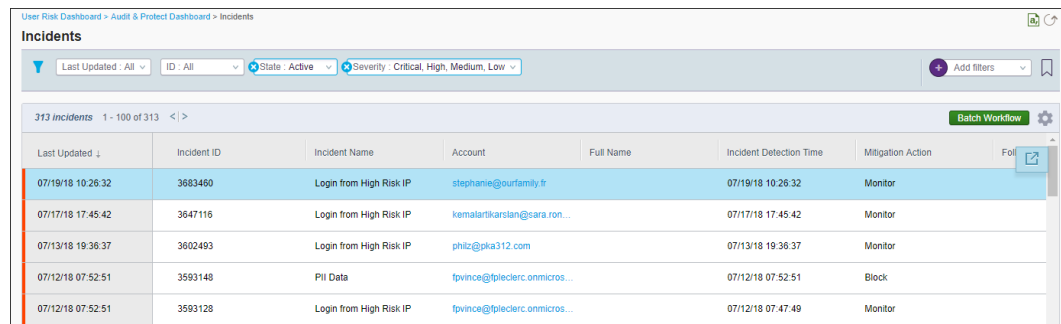
You can view the Incidents log and filter the results according to various parameters.

Forcepoint CASB provides different ways to view incidents, including:

- ▶ By user (see [Handling Policy Violations](#))
- ▶ By asset (see the details in this section below)

To view a list of incidents by asset:

1. In Forcepoint CASB, go to **Audit & Protect > Incidents**.
2. Select the relevant asset from the top left list of assets. To view the incidents for all assets, select **All Assets**.
3. The Incidents log opens:



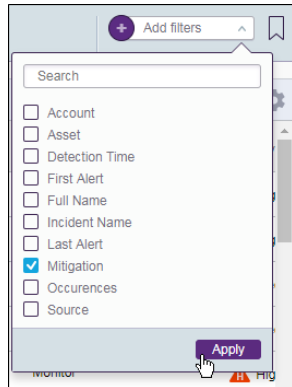
Last Updated ↓	Incident ID	Incident Name	Account	Full Name	Incident Detection Time	Mitigation Action	Follow
07/19/18 10:28:32	3683460	Login from High Risk IP	stephanie@ourfamily.fr		07/19/18 10:28:32	Monitor	
07/17/18 17:45:42	3647116	Login from High Risk IP	kemalartikarslan@sara.ron...		07/17/18 17:45:42	Monitor	
07/13/18 19:36:37	3602493	Login from High Risk IP	phitz@pka312.com		07/13/18 19:36:37	Monitor	
07/12/18 07:52:51	3593148	PII Data	fpvince@fpieclerc.onmicros...		07/12/18 07:52:51	Block	
07/12/18 07:52:51	3593128	Login from High Risk IP	fpvince@fpieclerc.onmicros...		07/12/18 07:47:49	Monitor	

For more information about the columns available in the Incidents log, see "[Incidents log column descriptions](#)" on page 106.

To sort by any column (ascending / descending), click the column header.

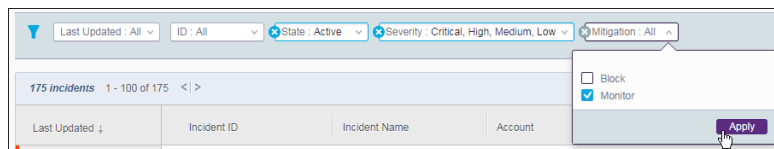
To filter the table by the values of any column:

1. Click the **Add filters** drop-down menu.
2. Select one or more of the options and click **Apply**. The new filter is added to the list of active filters above the table.

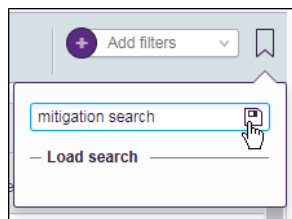


**Note:** The filter values are dependent on the values available for that table and can differ from the values shown in the images above and below.


- Expand the new filter, select the filter option, then click **Apply**.

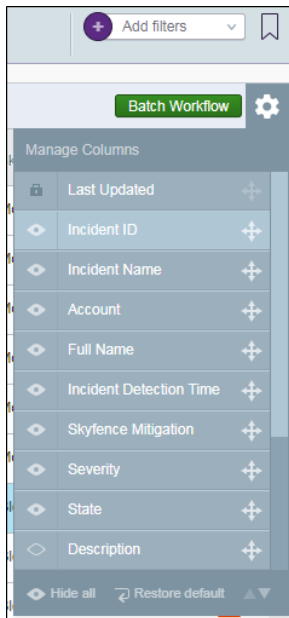


- To save the current filters as a search, click the bookmark button to the right of the **Add filters** field, type a name for the search, and click the save button.



- To load the saved search, click the button to the right of the **Add filters** field and select the search from the **Load search** list.

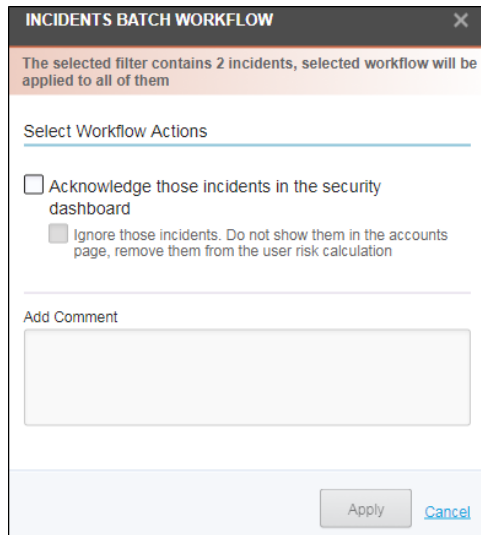
To configure the displayed columns and their order, click the  button.



To export the table to a CSV file, click . To refresh the display, click .

To perform a workflow action for more than one incident:

1. From the Incidents log, filter the list to display only the incidents to which you want to apply the workflow action.
2. Click **Batch Workflow**.
3. The incident's batch workflow actions are displayed:



The dialog box is titled "INCIDENTS BATCH WORKFLOW" and has a close button (X) in the top right corner. Below the title bar, there is a message: "The selected filter contains 2 incidents, selected workflow will be applied to all of them". Underneath, there is a section titled "Select Workflow Actions" with a horizontal line below it. This section contains two options: "Acknowledge those incidents in the security dashboard" with an unchecked checkbox, and "Ignore those incidents. Do not show them in the accounts page, remove them from the user risk calculation" with a checked checkbox. Below the actions is a section titled "Add Comment" with a large text input field. At the bottom right of the dialog, there are two buttons: "Apply" and "Cancel".

4. Select an action:

- ▶ **Acknowledge those incidents in the security dashboard:** New alerts will no longer be added to the incidents. These incidents will continue to impact the user's risk score, but will be removed from the security dashboard. Acknowledged incidents are still displayed in the Incidents Log with a status of **Acknowledged**.
- ▶ **Ignore those incidents:** (Optional) The incidents are no longer displayed in the account's incident timeline or impact the user's risk score. Ignored incidents are still displayed in the Incidents Log with a status of **Ignored**.

5. Optionally, add a **Comment** to provide more details concerning the action.

6. Click **Apply**.



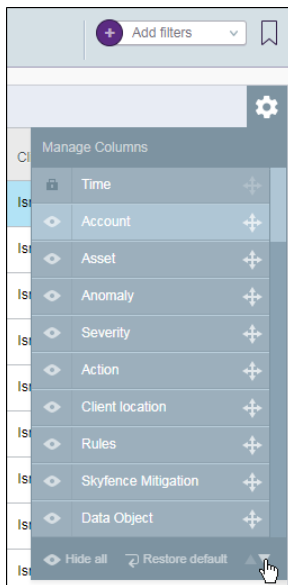
# Incidents log column descriptions

The following table provides detailed descriptions about the type of information displayed in the Incidents log.

Column name	Column description
Last Updated	The date and time when the last activity attached to the incident took place (adjusted to the Forcepoint CASB administrator's time zone).
Incident ID	A unique ID assigned by Forcepoint CASB to the incident.
Incident Name	The rule name to which the incident relates. If you move the mouse over the Incident Name, Forcepoint CASB displays a tooltip of the rule's description.
Account	The account used to access the cloud service (sAMAccountName if the Active Directory connection is set; otherwise, the login name).
Full Name	The full name of the user. This data is retrieved from the Active Directory if integration is in place; otherwise, it is empty.
Incident Detection Time	The date and time Forcepoint CASB detected the incident. This is the time Forcepoint CASB processed the data and can be days after the first activities.
Mitigation Action	The mitigation action taken by Forcepoint CASB as a result of the policies breached by the incident.
Follow-Up Mitigation	The mitigation actions taken after the incident is created (e.g., Remove sharing permissions).
Severity	The severity assigned with the Forcepoint CASB policy breached by the incident. If more than one policy was breached, the highest severity across these policies is displayed. This is empty if no policy was breached.
State	The status of the incident based on the workflow actions. The incident could be: <ul style="list-style-type: none"><li>▶ <b>Active:</b> The incident is active from the Forcepoint CASB administrator's perspective and still needs attention (default).</li><li>▶ <b>Acknowledged:</b> The Forcepoint CASB administrator has acknowledged the incident through the workflow action. Existing violations of the policy will no longer be listed. The incident still impacts the user's risk score calculation.</li></ul>

Column name	Column description
	<ul style="list-style-type: none"> <li>► <b>Ignored:</b> The Forcepoint CASB administrator set the incident to be ignored. The incident has been removed from the user's Account page and no longer impacts the user's risk score calculation.</li> </ul>
Occurrences	The number of alerts attached to the incident.
First Alert Time	The date and time of the first alert attached to the incident (i.e., the alert that created the incident).
Last Alert Time	The date and time of the current last alert attached to the incident.
Source	The activity audit type (i.e., Real Time or Service-logs).
Asset	The asset name assigned with the cloud service (e.g., My Office365).

In addition, Forcepoint CASB hides some columns from the default view. These columns can be added to the Incidents log view by selecting them from the Manage Columns menu.




The following columns are hidden by default:

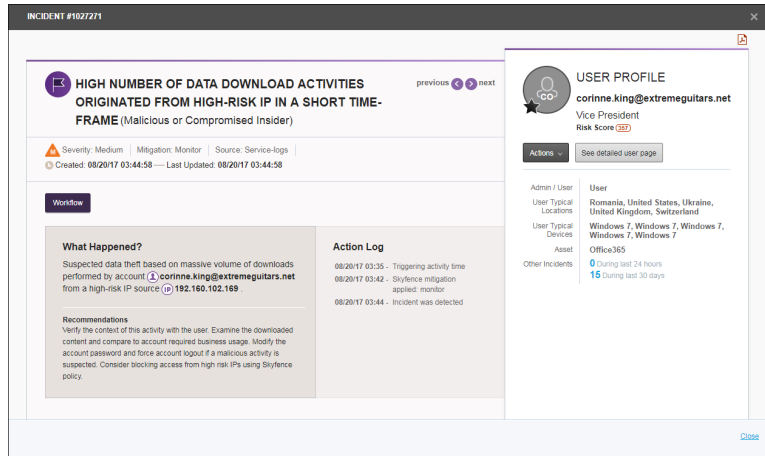
Column name	Column description
Login name	The account used to access the cloud service.

Column name	Column description
Description	The relevant rule's description.

# Incident records

The incident record contains all detailed information for the incident on one page.

To open an incident record, either double-click the incident row, or select the row and click the  button on the right side.



The incident record contains the following areas:

- ▶ Incident details
- ▶ User Profile
- ▶ Alerts table

The incident details area displays general information about the incident, such as:

- ▶ **Severity:** The incident severity is calculated based on the severity of the individual alerts within the incident record.
- ▶ **Mitigation:** The mitigation action is based on the mitigation actions of the individual alerts within the incident record.
- ▶ **Source:** The source corresponds to the activity audit type: **Real-time** (proxy-based activity) or **Service-logs** (API-based activity).
- ▶ **Created** date: The date and time when Forcepoint CASB detected the incident. This date is also referenced in the **Action Log**.
- ▶ **Last Updated** date: The date and time when the incident record was last updated, either automatically by Forcepoint CASB or manually by an administrator. This date is also referenced in the **Action Log**.

- ▶ **Workflow** button: Click the **Workflow** button to acknowledge or ignore the incident. Details are provided below.
- ▶ Details and recommendations: The **What Happened?** area provides details of the incident, including the user account, IP address, and policy information. Depending on the type of policy violation, Forcepoint CASB might provide detailed **Recommendations** on how to mitigate the incident.

The Recommendations text can be added to a custom policy. For more information, see ["Configuring custom policies" on page 80](#).

- ▶ **Action Log**: The action log displays the sequence of actions taken on this incident, either automatically by Forcepoint CASB or manually by an administrator.

You can view the Incidents log's previous incident record by clicking the **previous** arrow at the top of the incident record. To view the next incident, click the **next** arrow.

To perform a workflow action for a single incident:

1. From an incident record, click **Workflow**.
2. The incident's workflow actions screen opens:

3. Select an action:

- ▶ **Acknowledge this incident in the security dashboard**: Existing violations of this policy will no longer be listed. This incident will continue to impact the user's risk score calculation, but will be removed from the security dashboard. Acknowledged incidents are still displayed in the Incidents Log with a status of **Acknowledged**.
- ▶ **Ignore this incident**: (Optional) The incident is removed from the user's Account page and

no longer impacts the user's risk score calculation. Ignored incidents are still displayed in the Incidents Log with a status of **Ignored**.

- ▶ **Add <user> to the exception list of this rule:** This user account will no longer trigger a violation of this policy.
4. Optionally, add a **Comment** to provide more details concerning the action.
  5. Click **Apply**.

The User Profile provides details, such as email address, job title, risk score, typical locations, typical devices, and the asset, about the user account connected to this incident.

You can also view the user's detailed account page (see "[The Detailed Account page](#)" on [page 130](#).)

The Alerts table provides a list of the alerts from the last 30 days that contribute to this incident:

TIME	ACTIVITY	MITIGATION	SOURCE IP	LOCATION	DEVICE TYPE	SEVERITY
08/20/17 03:36	download	Monitor	192.160.102.169	Canada	Desktop	⚠ Medium
08/20/17 03:36	download	Monitor	192.160.102.169	Canada	Desktop	⚠ Medium
08/20/17 03:36	download	Monitor	192.160.102.169	Canada	Desktop	⚠ Medium
08/20/17 03:35	download	Monitor	192.160.102.169	Canada	Desktop	⚠ Medium

[View in Activity Table](#)

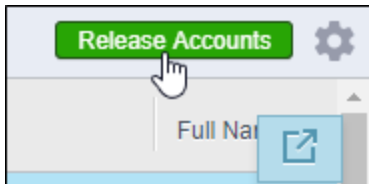
This table displays a summary of important alert information from the last 30 days. To view the alerts in the more detailed activity audit log, or to see alerts older than 30 days, click the button under the table. This opens the list of alerts in either the Realtime Monitoring or Service Provider Log audit log, depending on the source identified at the top of the incident record. See "[Investigating activity logs](#)" on [page 53](#) for more information.

# Handling policy violations

In the [Account page](#), user accounts that have triggered any policy rules are listed in the table. Select a user account to view its details on the right.

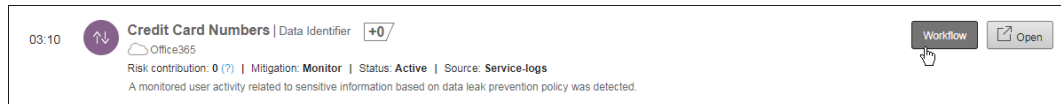
You can release all filtered accounts (as filtered by search), or handle violating accounts one at a time.

To release all filtered accounts, click **Release Accounts**:

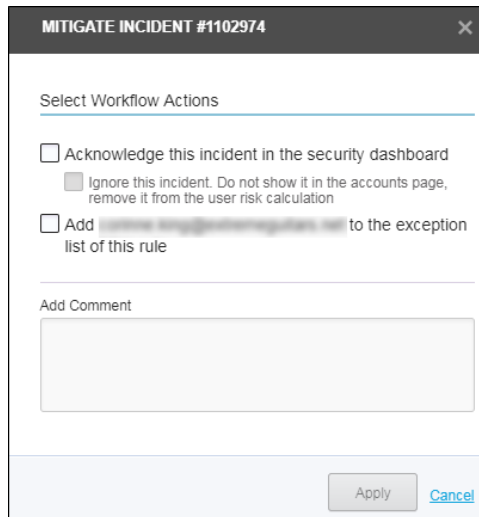


To handle a single violating account:

1. From the user's Details Account Page, hover over an incident and click **Workflow**:



2. The incident's workflow actions screen opens:



3. Select an action:

- ▶ **Acknowledge this incident in the security dashboard:** Existing violations of this policy will no longer be listed. This incident will continue to impact the user's risk score calculation, but will be removed from the security dashboard. Acknowledged incidents are still displayed in the Incidents Log with a status of **Acknowledged**.
  - ▶ **Ignore this incident:** (Optional) The incident is removed from the user's Account page and no longer impacts the user's risk score calculation. Ignored incidents are still displayed in the Incidents Log with a status of **Ignored**.
  - ▶ **Add <user> to the exception list of this rule:** This user account will no longer trigger a violation of this policy.
4. Optionally, add a **Comment** to provide more details concerning the action.
  5. Click **Apply**.





# CHAPTER 8

## User Behavior Analysis

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

Forcepoint CASB analyzes user behavior to detect patterns of suspicious activity, identifies anomalies from those patterns, and runs mitigation actions based on those anomalies.

In Forcepoint CASB, you monitor user risk through the User Risk Dashboard, the user Accounts list, and the detailed user pages.

This chapter discusses the following:

Machine learning-based anomaly detection using Forcepoint CASB .....	115
Monitoring user risk .....	118
Investigating accounts .....	122

# Machine learning-based anomaly detection using Forcepoint CASB

---

Traditional security is about providing controls to known tactics. If we have seen an attack pattern in the past, then we can apply controls to stop it.

We can easily mark the bad activities that we are familiar with and form them into security access rules. We can also easily detect the legitimate scenarios that are part of the key business flows and mark these as exceptions. But what about the gray areas in between?

To use a simplified example, think about a simple access policy that grants complete access from the main office location and blocks all access from countries we are not authorized to communicate with. This policy covers the easy *good* and *bad* activities, but what if we see a location that belongs in neither list? Allow the connection and you may miss an attack. Block it and you may be tampering with productivity. Alert on it and you add one more alert to the many thousands of alerts cluttering your IT systems.

The one thing missing when making this "good or bad" decision is the **context** of the situation.

For example, if we know that the user accessing the system in the above example has been connecting from the same location for many days, and that the data they are accessing is of the same type they have been accessing for a long time, deciding that this is a *good* activity would be easy.

On the flip side, if we know that this connection is coming from a location this user has never been at before, that they are accessing non-typical data items, and that they are running an unusually high volume of data download, it would quickly be marked as a *bad* activity.

Understanding the context helps us make better decisions and reduces the clutter considerably. This context is different for each user. Forcepoint CASB maintains a user profile that includes all the relevant context information to allow the system to make these smart decisions.

## Activity auditing and user profile

The most basic requirement for a CASB service is to have visibility into user activities in the cloud. This is a basic prerequisite to providing auditing and controls over cloud application access and usage.

Forcepoint CASB gains visibility into user activity via multiple detection methods, ranging from Inline proxy traffic analysis to leveraging service providers' APIs. Regardless of the detection method, Forcepoint CASB provides visibility into user activity properties, with dozens of such properties being audited per each user activity. Examples include user IP address, geographic location, device type & operating system, trusted / untrusted device, user action, service module accessed, and specifics such as file / folder name and impacted users.

Once Forcepoint CASB gains visibility into this data, a profiling process begins. This process identifies typical user behavior, such as typical locations for that user, activity volume, or devices used.

To build the user profile, Forcepoint CASB leverages supervised machine learning (ML) algorithms, such as Support Vector Machine (SVM) classifier, and unsupervised ML algorithms, such as Unsupervised Outlier Detection.

Using these ML mechanisms, Forcepoint CASB maintains a real-time user profile, allowing the CASB service to take immediate actions based on rules and policies for real-time traffic and API-based activities.

Smart anomaly detection policies allow smarter access controls as explained above, but also the ability to defend against zero-day attacks.

Zero-day attacks are typically designed to avoid security systems searching for patterns used in past attacks. Forcepoint CASB anomaly detection looks into the user behavior and detects deviations from usage patterns, thus detecting the attack through changes of account behavior rather than searching for attack fingerprints. These deviations are usually someone else (malware/malicious user) leveraging the account details.

## User risk

Understanding user risk is a key action toward optimizing the security analysis and investigation time. Attending to multiple alerts across many enterprise accounts is not an ideal use of a security analyst's time. Understanding which user in the organization currently poses the most risk and attending to the key issues about their account is a much more focused approach and one that prioritizes attending to the key risks to the organization first.

Forcepoint CASB assigns a risk score to every user and highlights the risk as part of the key dashboards in the management portal, allowing the administrators to attend to the riskiest issues first.

A risk, by definition, is the combination of the probability of something bad happening, and the impact on the organization if something bad happened. Forcepoint CASB leverages this approach to determine the potential risk of users.

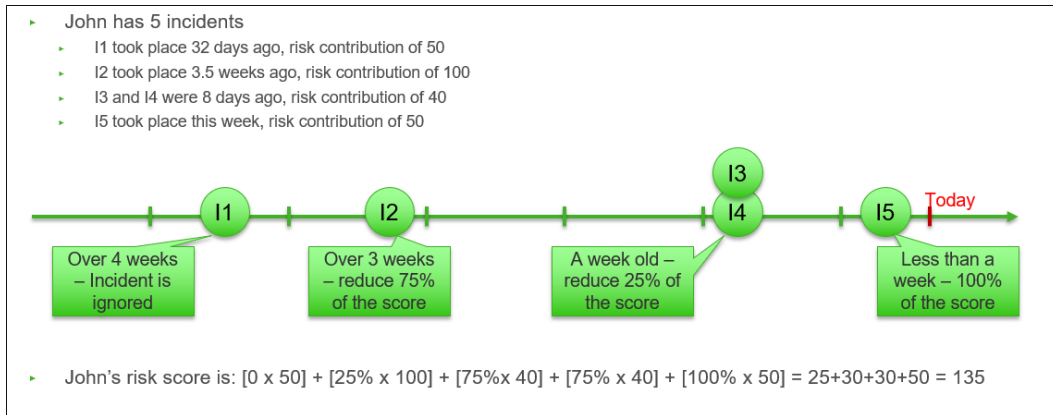
The probability is determined based on past behavior and the severity of the current action. The impact is determined by many factors, such as the access level of that user for sensitive data or their privileges at the service.

The risk score is calculated based on the above and every incident that takes place may modify the user risk. Further to that, the risk decays over time and if no new incidents are introduced for this user, after a while the risk score will reset.

Incident risk scores (which contribute to the user risk score) can be adjusted by the customer administrator by assigning different risk levels with different policies. The customer administrator

may further optimize the risk calculation by marking investigated incidents as relevant/irrelevant to the calculation.

Here is an example of the risk calculation, which shows the risk score decay over time:



# Monitoring user risk

The User Risk Dashboard focuses on user activity within specific Cloud service assets, providing a high-level view of the user risks within your organization and allowing you to drill-down to the specific details for each user.

To open the User Risk Dashboard, log in to Forcepoint CASB. The User Risk Dashboard opens by default as the starting page. If you are already logged in to Forcepoint CASB, click the **Risk Summary** tab at the top of the page to open the User Risk Dashboard.

The screenshot shows the 'User Risk Dashboard' interface. At the top, it displays '5 / 114 USERS AT RISK'. Below this, there are two categories: '0 / 3 ADMINS & Power Users' and '5 / 111 NON ADMIN USERS'. The main content area is divided into two sections: 'TOP HIGH RISK USERS' and 'WATCHLIST'. The 'TOP HIGH RISK USERS' section shows two users: 'admin@forcepointsea.onmicrosoft.com' with a risk score of 127 and 'fpvince@pleclerc.onmicrosoft.com' with a risk score of 106. The 'WATCHLIST' section shows four users: 'fpvince@pleclerc.onmicroso...' with a risk score of 106, 'alan@veridinet.com' with a risk score of 0, 'James Cagle' with a risk score of 0, and 'Corinne King' with a risk score of 0. At the bottom, there are tabs for 'ORG BEHAVIOR' and 'TOP BUSINESS UNITS AT RISK'.

The User Risk Dashboard displays six summary areas: Users at Risk, Top High Risk Users, Watchlist, Organizational Behavior, Top Business Units at Risk, and Organizational Geographic Risk. Each area is explained in the following sections.

**Note:** User accounts are connected to specific Cloud service assets. Because a person within your organization can have accounts for several assets, they can have more than one user account listed on the User Risk Dashboard.

## Users at Risk

This section provides an overview of the users at risk, separated by **Admins & Power Users** and **Non Admin Users**.

This block shows the summary metrics for 'Users at Risk'. It displays '5 / 114 USERS AT RISK'. Below this, there are two categories: '0 / 3 ADMINS & Power Users' and '5 / 111 NON ADMIN USERS'.

To be listed as a user at risk, the user must have a risk score higher than 0. The risk score is calculated based on the number of incidents assigned to the user, with each incident weighted. Incidents are activity records that combine one or more similar alerts that originate from the same attack. For more information about Incidents, see "[Monitoring and Investigating Alerts and Incidents](#)" on page 101

Each group (total Users at Risk, Admins & Power Users, and Non Admin Users) displays two numbers separated by a slash (/). The first number denotes the number of users at risk for that group. The second number denotes the total number of users in that group.

If you are viewing **All Assets**, an additional **Users at Risk by Asset** section is displayed to the right side of the Non Admin User list. This section displays an icon for each affected asset and a number of affected users. Click the number to open the Accounts page filtered to only display the list of affected user accounts.

## Top High Risk Users

This section lists the highest risk users in your organization, based on risk score. To be listed as a high risk user, the user must have a risk score higher than 100.

The User Risk Dashboard lists the top high risk users, up to 5 users. Each user record lists the month and day when the user was added to the Top High Risk Users list.

To view the user's [Detailed Account Page](#), click the user's picture or risk score.

To view the list of all high risk users, click the **All High Risk Users** button. Forcepoint CASB opens the Accounts page, filtered to only display the list of high risk users. From the Accounts page, you can view the Detailed Account Page for an individual user.

## Watchlist

The Watchlist allows you to mark specific users to closely monitor them over time. After a user is added to the Watchlist, they can be monitored from the User Risk Dashboard.

The User Risk Dashboard displays the top 15 user accounts, based on risk score. To view the list of all watched users, click All Watched Users. Forcepoint CASB opens the Accounts page, filtered to only display the list of watched users. From the Accounts page, you can view the Detailed Account Page for an individual user.

All users on the Watchlist are denoted by a black star. This star is always visible either next to the user's image, or next to their name. The icon **ON WATCHLIST** also is displayed on the user's Detailed Account Page.

Account	Risk Score ↓
★ corinne.king@extrem...	177

While the other areas of the User Risk Dashboard are populated by Forcepoint CASB based on available data, the user accounts added to the Watchlist are populated by you. You can add any account to the Watchlist.

To add a user to the Watchlist, expand the **Actions** menu, then click **Add to Watchlist** from either the user's Detailed Account Page or the user's summary information on the right side of the Accounts page.

## Organizational Behavior

This section displays a chart of activity and incidents for your organization over the past 30 days. Incidents are displayed above the date, while activities are displayed under the date.

Hover over the date, incident bar, or activity bar to display the numbers of incidents and activity for that date. Click it to open the Incidents page with the table of incidents filtered for that date.

To display the Incidents page with all incidents, click **All Incidents**. For more information about incidents, see "[Monitoring and Investigating Alerts and Incidents](#)" on page 101

## Top Business Units at Risk

This section displays the number of users at risk attached to each business unit of your organization. As mentioned above, a user is considered at risk if their risk score is above 0.

Click a business unit to open the Accounts page, with the table of accounts filtered for that business unit.

---

**Note:** Business unit data is retrieved from Active Directory. If Active Directory is not set up, or if business units are not available for your organization, then this section will not display any information.

---

## Organizational Geographic Risk

This section displays a map to graphically display the global distribution of the users at risk. As mentioned above, a user is considered at risk if their risk score is above 0.

Each affected country displays a pin. Each pin displays the number of users at risk within that country. If a user is active within more than one country, the user is counted in each country in which they are at risk.

Click the pin to open the Accounts page filtered to only display the list of affected user accounts for that country.



# Investigating accounts

The **Accounts** page displays user accounts that were used to access managed assets, for **All Assets** or for a selected asset.

To access the Accounts page, go to **Risk Summary > Accounts**. The page is divided into two areas:

- ▶ The Accounts table
- ▶ The Account summary

User Risk Dashboard > Accounts

**Accounts**

Account: All High Risk: All Asset: All Add filters

109 accounts 1 - 100 of 109 < > Release Accounts

Account	Risk Score ↓	Last Activity	Admin / User	Full Name
admin@forcepointsea.on...	255	07/09/18 00:02:24	User	
fpvince@fpclerc.on...	148	07/12/18 07:57:11	User	
demo@nv17.onmicrosoft...	42	06/20/18 12:04:05	User	
alex@nv17.onmicrosoft.c...	21	06/20/18 10:48:12	User	
nat@u@skyfence.com	0	05/29/18 09:16:36	User	
jcagle	0	06/20/18 10:24:35	User	James Cagle
cking	0	05/02/18 04:19:07	User	Corinne King
cathy.hall@extremeg...	0	05/02/18 04:00:48	User	Cathy Hall
delidred	0	05/02/18 04:00:57	User	Devin Eldred
avargas	0	06/19/18 10:10:59	User	Annette Vargas
app@sharepoint	0	07/11/18 17:31:11	User	
justin.dimattia@extremeg...	0	04/15/18 18:43:51	User	Justin Dimattia

**admin@forcepointsea.on...** Risk: 255 Office365

Comments (0)

Actions See detailed user page

**LOCATIONS**

Singapore Last seen: 07/09/18

**DEVICES**

Windows 10 Last seen: 07/09/18 Windows 10 Last seen: 07/09/18

**INVESTIGATE**

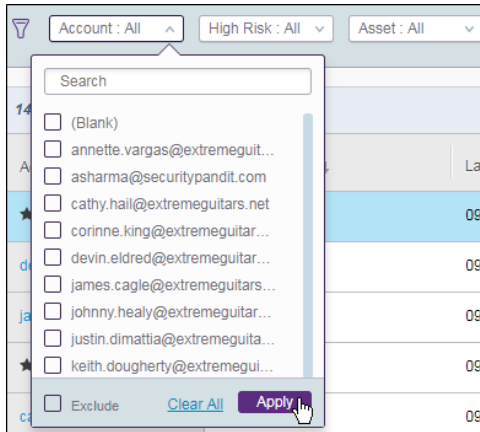
All user activities 5 incidents 0 quarantined files

## The Accounts table

The Accounts table displays a tabular list of the accounts within your organization, and lets you focus on the accounts with the highest risk score. Forcepoint CASB sorts the table by Risk Score, from highest to lowest, by default.

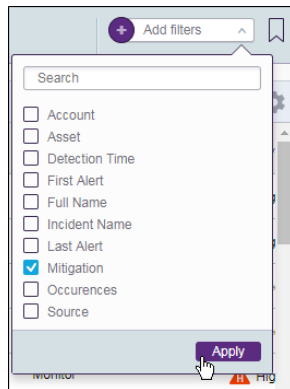
For more information about the columns available in the Accounts table, see "[Accounts table column descriptions](#)" on page 125.

By default, all accounts affiliated with the selected asset display in the table. To filter the accounts displayed in the table by specific criteria, select one or more of the default filters (Account, High Risk, or Asset) above the table, then click **Apply**.



To filter the table by a column value that is not one of the defaults, select a value from the **Add filters** drop-down menu:

1. Click the **Add filters** drop-down menu.
2. Select one or more of the options and click **Apply**. The new filter is added to the list of active filters above the table.

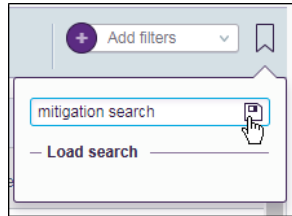


**Note:** The filter values are dependent on the values available for that table and can differ from the values shown in the images above and below.


3. Expand the new filter, select the filter option, then click **Apply**.

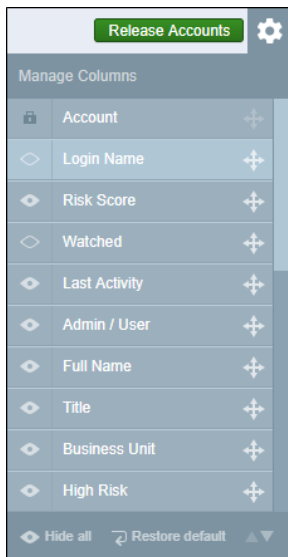


4. To save the current filters as a search, click the bookmark button to the right of the **Add filters** field, type a name for the search, and click the save button.



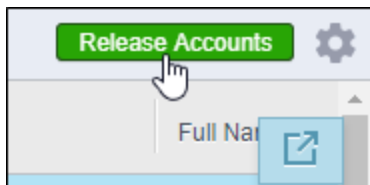
5. To load the saved search, click the button to the right of the **Add filters** field and select the search from the **Load search** list.

To configure the displayed columns and their order, click the  button.



To export the table to a CSV file, click . To refresh the display, click .

Select the **Release Accounts** action to release an account that is blocked due to a policy breach. Accounts are blocked if the policy action is set to **Block Account**.



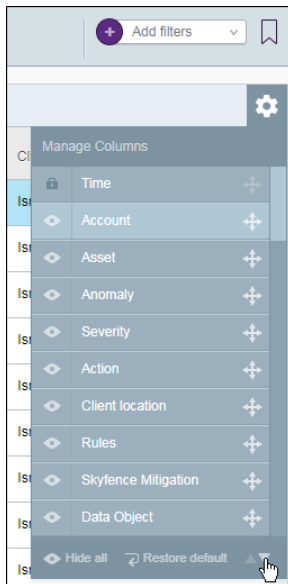
## Accounts table column descriptions

The following table provides detailed descriptions about the type of information displayed in the Accounts table.

Column name	Column description
Account	The account used to access the cloud service (sAMAccountName if the Active Directory connection is set; otherwise, the login name).
Risk Score	The account's current risk score.
Last Activity	The date and time when the last activity was detected on the account.
Admin / User	A flag indicating whether the account is an administrator (Admin) or a user (User), as detected in the Users and Configuration Governance scan on the asset.
Full Name	The full name of the user. This data is retrieved from the User Directory if integration is in place; otherwise, it is empty.
Title	The title of the account. This data is retrieved from the Active Directory if integration is in place; otherwise, it is empty.
Business Unit	The business unit of the account. This data is retrieved from the Active Directory if integration is in place; otherwise, it is empty.
High Risk	A flag indicating whether the account is considered high risk (Yes) or not (No). This flag is based on the account's current risk score.
Asset	The asset name assigned with the cloud service (e.g., My Office365).
Locations	The geographic locations from which the account's activities were detected.
Orphan	When Forcepoint CASB performs a Users and Configuration Governance scan and finds the account in the User Directory, this flag indicates whether the account was marked as Disabled in the User Directory (Yes) or not (No).
Dormant	When Forcepoint CASB performs a Users and Configuration Governance scan, this flag indicates whether the account's last login date was earlier than the threshold set in the Users and Configuration Governance scan (Yes) or not (No).
Incidents	A list of incidents related to the account.

Column name	Column description
Account Status	A flag indicating whether the account is blocked due to rule enforcement (Blocked) or not blocked (Active).
Last Incident updates	The date and time when an incident attached to the account was last updated.

In addition, Forcepoint CASB hides some columns from the default view. These columns can be added to the Accounts table by selecting them from the Manage Columns menu.



The following columns are hidden by default.

Column name	Column description
Login name	The account used to access the cloud service.
Watched	A flag indicating whether the account is on the Watchlist (Yes) or not (No).
External	When Forcepoint CASB performs a Users and Configuration Governance scan, this flag indicates whether the account was found in the User Directory (No) or not found in the User Directory (Yes). If the account was not found in the User Directory, the account is considered an External account.
Scan ID	The ID of the last internal Users and Configuration Governance scan where the account took part.

Column name	Column description
Governance Last Activity	The date and time of the last activity on the account that was detected by the Users and Configuration Governance scan.
Policies	A list of policies related to the account.
External Location	A flag indicating whether the account's location is considered an external location (Yes) or an internal location (No). This is based on your organization's internal IP ranges settings.
Internal Location	A flag indicating whether the account's location is considered an internal location (Yes) or an external location (No). This is based on your organization's internal IP ranges settings.

## The Account summary

When you select an account from the Accounts table, Forcepoint CASB provides summary information for the account on the right side of the screen. Some details appear only if the user is recognized from the [organizational user directory](#).

This area displays the following account information for the user:

- ▶ **User image:** An image of the user retrieved from Active Directory. If no image is available, a placeholder image is used. If the user is on the Watchlist, a black star is displayed in the lower left corner of the image.
- ▶ **Asset:** The asset associated with this account.
- ▶ **Email address:** The user's email address. This information is retrieved from Active Directory.
- ▶ **User name:** The full name of the user. This information is retrieved from Active Directory.
- ▶ **Job title:** The job title of the user within your organization. This information is retrieved from Active Directory.
- ▶ **Comments:** A list of all comments added by the Forcepoint CASB administrators for this account. Each comment displays the date, time, and Forcepoint CASB account email address of the administrator who added the comment. To add a new comment, click **Comments**, add the new comment in the text field, then click **Add**.
- ▶ **Actions** button:
  - **Delete Account:** This option removes the account from Forcepoint CASB. Forcepoint CASB removes all data associated with this account: Incidents, Alerts,

Offline Alerts, Activities, Offline Activities, and Profile data.

---

**⚠ Warning:** Deleting an account removes this user account and all user activities from the Forcepoint CASB records. Although the user record can be added back if the user performs new activities, the deleted activities are permanently deleted from Forcepoint CASB and cannot be recovered.

---

- **Add to Watchlist/Remove from Watchlist:** This option adds the user to your Watchlist. The Watchlist is available from the User Risk Dashboard, and provides a quick way to view all accounts you wish to track.

- ▶ **See detailed user page** button: Click this button to open the user's Detailed Account Page. For more information, see ["The Detailed Account page" on page 130](#).
- ▶ **Locations:** The Locations from which this account has connected to the asset. When the area is collapsed, Locations displays an image of the country flag for the top locations used with this account (up to 5). When expanded, Locations displays the image of the country flag, the name of the country, and the date when the user last connected from that location.

If there are more than 5 locations associated with this account, a link to view all of the locations is displayed next to the Locations heading. Click the link to display a list of all locations. This list displays the image of the country flag, the name of the country, and the date when the user last connected from that location.

- ▶ **Devices:** The devices from which this account has connected to the asset. When the area is collapsed, Devices displays an image of the operating system for the top devices used with this account (up to 5). When expanded, Devices displays the image of the operating system, the name of the operating system, and the date when the user last connected from that device.

If there are more than 5 devices associated with this account, a link to view all of the devices is displayed next to the Devices heading. Click the link to display a list of all devices. This list displays the image of the operating system, the name of the operating system, and the date when the user last connected from that device.

- ▶ **Investigate**
  - **All user activities:** Click this link to display the two options: **Realtime activities** and **API-based activities**. Clicking **Realtime activities** opens the Realtime Monitoring Audit Log. Clicking **API-based activities** opens the Service Provider Log Audit Log. Each Audit Log is filtered to display the incidents associated with this account and asset.

For more information about Realtime and API-based activities, see ["Activity audit types" on page 48](#).

- **xx incidents**, where xx is the number of incidents associated with this account. Click this link to open the Incidents page, filtered to display the incidents associated with this account and asset.

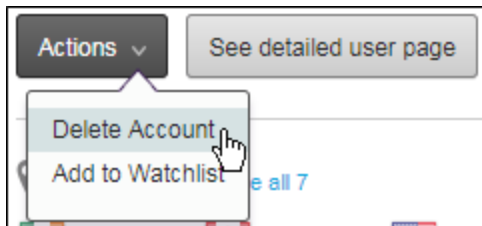
For more information about incidents, see ["Monitoring and Investigating Alerts and Incidents" on page 101](#).

- **xx quarantined files**, where xx is the number of quarantined files associated with this account. Click this link to open the File Analytics page, filtered to display the files with either a **Quarantine** or **Keep a safe copy** mitigation status associated with this user account.

Quarantine and Keep a safe copy are mitigation actions available for API-based activities:

- Data Classification policies
- User Activity Control policies
- Data Leak Prevention policies
- Custom policies

To remove a displayed account (as filtered by search) from the list until they perform any more activities, click **Actions>Delete Account**:



**⚠ Warning:** Deleting an account removes this user account and all user activities from the Forcepoint CASB records. Although the user record can be added back if the user performs new activities, the deleted activities are permanently deleted from Forcepoint CASB and cannot be recovered.

To view the user's detailed information, including a timeline of incidents and activities, click **See detailed user page**. For more information about the detailed user page, see ["The Detailed Account page" on the facing page](#).



# The Detailed Account page

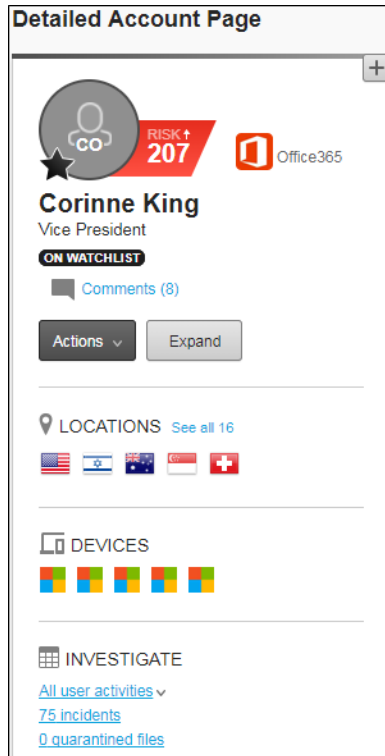
The Detailed Account Page displays information for a specific user account. It is divided into three areas:

- ▶ User profile
- ▶ User Behavior
- ▶ Incident Timeline



# User profile

The user profile is on the left side of the Detailed Account Page.



This area displays the following account information for the user:

- ▶ **User image:** An image of the user retrieved from Active Directory. If no image is available, a placeholder image is used. If the user is on the Watchlist, a black star is displayed in the lower left corner of the image.
- ▶ **Risk score:** The overall risk score associated with this user account. The risk score is the sum of the scores from all incidents associated with this account.
- ▶ **Asset:** The asset associated with this account.
- ▶ **User name:** The full name of the user.
- ▶ **Job title:** The job title of the user within your organization.
- ▶ **Comments:** A list of all comments added by the Forcepoint CASB administrators for this account. Each comment displays the date, time, and Forcepoint CASB account email address of the administrator who added the comment. To add a new comment, click

**Comments**, add the new comment in the text field, then click **Add**.

▶ **Actions** button:

- **Delete Account:** This option removes the account from Forcepoint CASB. Forcepoint CASB removes all data associated with this account: Incidents, Alerts, Offline Alerts, Activities, Offline Activities, and Profile data.
- **Add to Watchlist/Remove from Watchlist:** This option adds the user to your Watchlist. The Watchlist is available from the User Risk Dashboard, and provides a quick way to view all accounts you wish to track.
- **Apply Workflow to all Incidents:** This option allows you to Acknowledge and/or Ignore all of the active Incidents in this account. This is a batch option, so it will affect all incidents in the Incident Timeline.
  - ▶ If you acknowledge all incidents, new alerts will no longer be added to the incidents. These incidents will continue to impact the user's risk score, but will be removed from the security dashboard. Acknowledged incidents are still displayed in the Incidents Log with a status of **Acknowledged**.
  - ▶ If you ignore all incidents, they are no longer displayed in the account's incident timeline or impact the user's risk score. Ignored incidents are still displayed in the Incidents Log with a status of **Ignored**.

For more information about the Incidents log and Incident records, see "[Monitoring and Investigating Alerts and Incidents](#)" on page 101.

- ▶ **Expand** and **Collapse** buttons: Click the **Expand** button to enlarge the user profile area. Expanding the area displays the users' email address and provides additional details for each Location (country and last active date) and Device (operating system and last active date). Click **Collapse** to return the area to its original view.

You can also expand the user profile area by clicking the  button in the top right corner of the area. To collapse the area, click the  button.

- ▶ **Locations:** The Locations from which this account has connected to the asset. When the area is collapsed, Locations displays an image of the country flag for the top locations used with this account (up to 5). When expanded, Locations displays the image of the country flag, the name of the country, and the date when the user last connected from that location.

If there are more than 5 locations associated with this account, a link to view all of the locations is displayed next to the Locations heading. Click the link to display a list of all locations. This list displays the image of the country flag, the name of the country, and the date when the user last connected from that location.

- ▶ **Devices:** The devices from which this account has connected to the asset. When the area

is collapsed, Devices displays an image of the operating system for the top devices used with this account (up to 5). When expanded, Devices displays the image of the operating system, the name of the operating system, and the date when the user last connected from that device.

If there are more than 5 devices associated with this account, a link to view all of the devices is displayed next to the Devices heading. Click the link to display a list of all devices. This list displays the image of the operating system, the name of the operating system, and the date when the user last connected from that device.

► Investigate

- **All user activities:** Click this link to display the two options: **Realtime activities** and **API-based activities**. Clicking **Realtime activities** opens the Realtime Monitoring Audit Log. Clicking **API-based activities** opens the Service Provider Log Audit Log. Each Audit Log is filtered to display the incidents associated with this account and asset.

For more information about Realtime and API-based activities, see "[Activity audit types](#)" on page 48.

- **xx incidents**, where xx is the number of incidents associated with this account. Click this link to open the Incidents page, filtered to display the incidents associated with this account and asset.

For more information about incidents, see "[Monitoring and Investigating Alerts and Incidents](#)" on page 101.

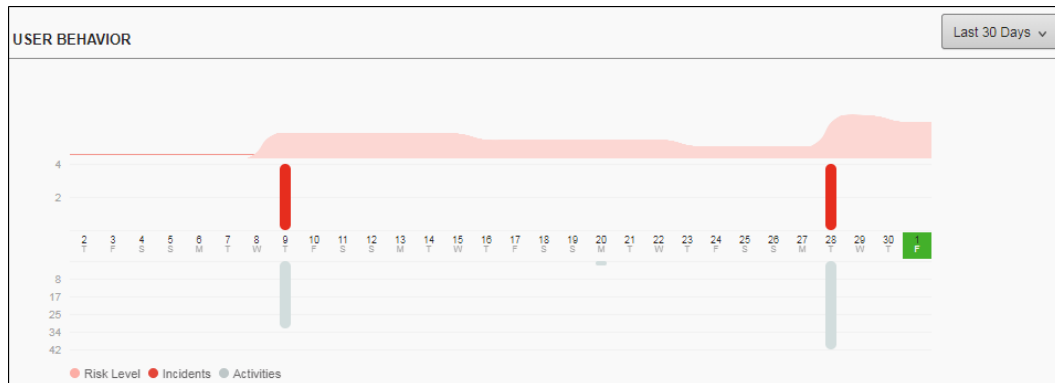
- **xx quarantined files**, where xx is the number of quarantined files associated with this account. Click this link to open the File Analytics page, filtered to display the files with either a **Quarantine** or **Keep a safe copy** mitigation status associated with this user account.

Quarantine and Keep a safe copy are mitigation actions available for API-based activities:

- Data Classification policies
- User Activity Control policies
- Data Leak Prevention policies
- Custom policies

## User behavior

This area displays a chart of activity and incidents for this account over the past 30 days. To display the timeline for the past 180 days, click the Last 30 Days drop-down menu at the top right corner of the area and select Last 180 Days.

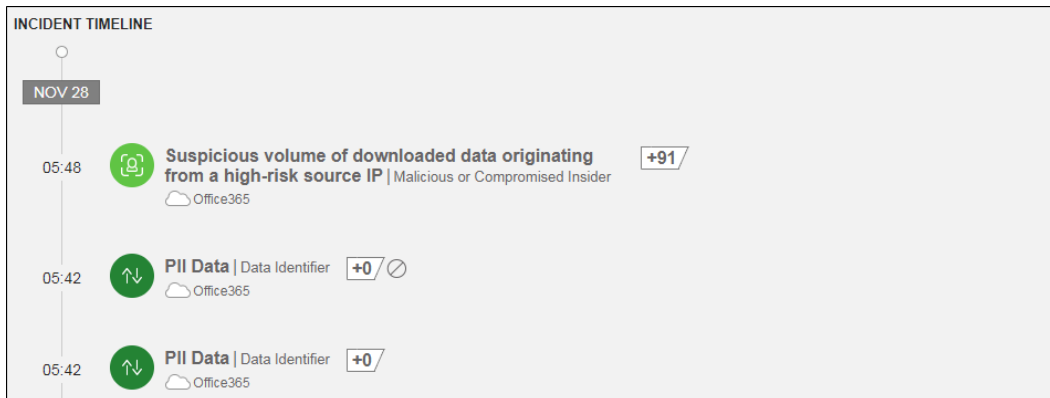


Incidents are displayed above the date, while activities are displayed under the date. Above the chart, there is a graph that displays the risk score timeline. The area in red denotes the risk score number. As the risk score increases, the graph line goes higher and the amount of red space increases. This provides a quick visual cue of the account's risk score.

Hover over the date, incident bar, activity bar, or risk score graph to display the numbers of incidents and activity, along with the risk score, for that date. Click to open the Incidents page, with the table of incidents filtered for that date.

## Incident timeline



The Incident Timeline displays the latest Incidents associated with the user account in chronological order, with the latest Incident at the top of the timeline.



Each record in the Incident timeline displays the following information:

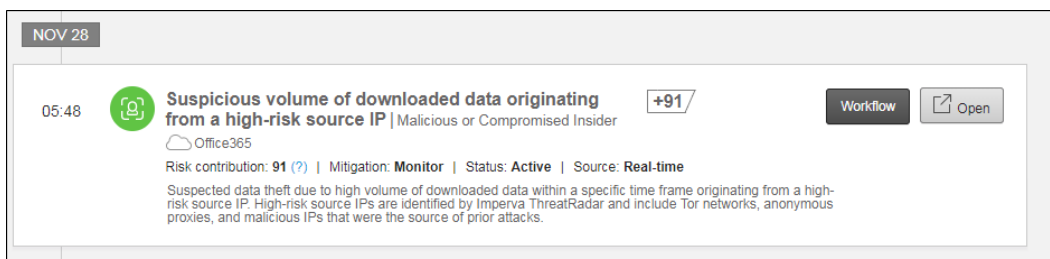
- ▶ **Incident time:** The date on which the incident occurred is displayed above the timeline of incidents for that date. The time at which the incident occurred is displayed on the left side of the Incident record.
- ▶ **Type of Policy Violation:** The Incident record displays an icon to visually identify the type of policy violation. The record also displays the affected rule (e.g., Suspicious volume of downloaded data originating from a high-risk source IP) and policy (e.g., Compromised Insider).
- ▶ **Risk Score change:** The number of points from this incident that are added to the user's overall risk score. This number decreases over time.
- ▶ **Asset:** The asset associated with this account.

---

 **Note:** If the mitigation action for the incident is Block, a  icon is displayed next to the risk score.

---

When you hover over the Incident record, it expands to display additional information:



- ▶ **Risk contribution:** The number of points from this incident that are added to the user's overall risk score. This number decreases over time.
- ▶ **Mitigation:** The mitigation action for the policy. This action is set up in the policy, and differs between Real-time activities and Service-logs (API-based) activities.
- ▶ **Status:** Can be either Active, Acknowledged, or Ignored. The default status is Active, but can be changed to Acknowledged or Ignored in the Incident's Workflow.
- ▶ **Source:** Indicates from which activity log the incident originated. This can be either Real-time (from the Real-time Monitoring audit log) or Service-logs (from the API-based Service Provider Log).
- ▶ **Rule description:** This description is taken from the rule and provided here as a reference.
- ▶ **Workflow** button: Click Workflow to add a comment to the Incident record, acknowledge or ignore the incident, or add the user to the exception list.
  - If you acknowledge the incident, new alerts will no longer be added to the incident. The incident will continue to impact the user's risk score calculation, but it will be removed from the security dashboard. Acknowledged incidents are still displayed in the Incidents Log with a status of **Acknowledged**.
  - If you ignore the incident, it is no longer displayed in the account's incident timeline or impact the user's risk score calculation. Ignored incidents are still displayed in the Incidents Log with a status of **Ignored**.
  - If you add the user to the exception list, the account will no longer trigger a violation of this policy.
- ▶ **Open** button: Click this button to open the Incident record. For more information about the Incident record, see "[Incident records](#)" on page 109.

To view more Incidents, select one of the following options at the bottom of the timeline:

- ▶ **Expand Timeline** button: Click this button to display all earlier incidents in the timeline. The earlier incidents are added to the bottom of the timeline.
- ▶ **See all in Incidents Log** link: Click this link to open the Incidents page, with the table of incidents filtered by this account and asset. For more information about the Incidents log, see "[The Incidents log](#)" on page 102.



# CHAPTER 9

## Governance and Compliance

Forcepoint CASB | 2021 R4 | Updated: December 19, 2021

For managed assets, Forcepoint CASB can provide information about cloud account configuration and deployment, and stored and shared sensitive organizational information.

The following types of governance features are available:

- ▶ **Account access and security governance:** Provides a detailed risk assessment of your specific deployment by providing information about service ownership (administrative accounts and recent usage), user accounts that are potential security risks, and account configuration, enabling you to monitor how the actual configuration of your accounts complies with regulatory standards and organizational policy.

For found policy violations, you can perform [remedial tasks](#).

- ▶ **Data governance:** For managed assets, Forcepoint CASB scans the contents of stored files and provides detailed information about stored sensitive material – as defined by configurable [data types](#) – including how it is accessed and shared inside and outside the organization.

This chapter discusses the following:

Account access and security governance .....	138
Data classification .....	149



# Account access and security governance

---

As opposed to [Discovery](#), which provides only generic service risk information, access and security governance provides a more accurate risk assessment of your specific deployment by providing information about service ownership (administrative accounts and recent usage), user accounts that are potential security risks, and account configuration, enabling you to monitor how the actual configuration of your accounts complies with regulatory standards and organizational policy.

The features in this section require the Governance feature to have been [configured for supported cloud service assets](#), and are then available even when Forcepoint CASB is not deployed as a gateway between users and the assets.

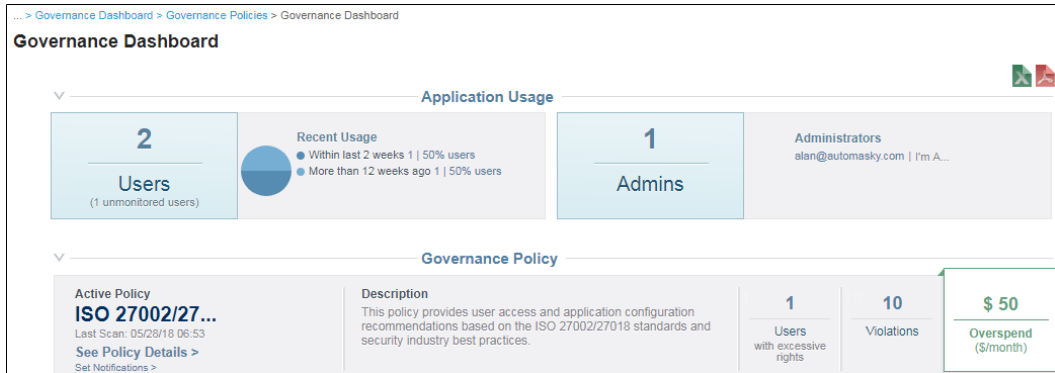
Account Access & Security Governance is currently supported for the following cloud services:

- ▶ Amazon AWS
- ▶ Box
- ▶ Dropbox
- ▶ Google G Suite
- ▶ Office 365
- ▶ Salesforce

## Monitoring account access and security

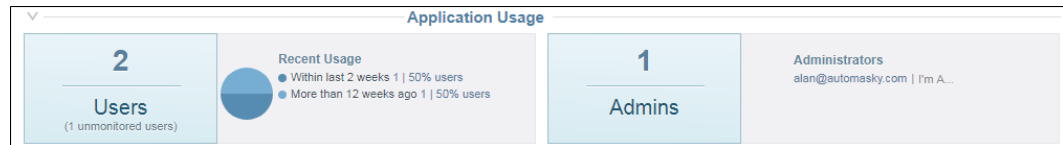
For applications that have been defined as [managed assets](#), for which [Governance has been configured](#), the **Governance Dashboard page** displays account governance and compliance information including account ownership (administrative accounts), configuration policy violations, and user accounts that should be removed, according to [configured policy](#).

To view the information, go to **Compliance > Governance > Dashboard**:



The displayed information includes:

- ▶ Statistics on recent usage, and configured administrative user accounts, providing insight on account ownership:



If you have unmonitored accounts, the number of unmonitored accounts is displayed under the total number of **Users** and **Admins**. Forcepoint CASB does not display unmonitored accounts in the Users and Configuration governance report.

- ▶ Violations of [configurable](#) regulatory standards and organizational policy:

**Governance Policy**

<p>Active Policy <b>PCI DSS V3.0...</b> Last Scan: 03/28/16 03:41 <a href="#">See Policy Details &gt;</a> <a href="#">Set Notifications &gt;</a></p>	<p>Description PCI DSS V3.01 with a much lower dormancy time</p>	<p><b>4</b> Users with excessive rights</p>	<p><b>9 *</b> Violations</p>	<p><b>\$ 1000</b> Overspend (\$/month)</p>
--	--	---	----------------------------------	--

**Excessive Rights** (4 users)

<b>!4</b>	<p><b>Dormant Users</b></p> <p>User accounts that have not been used for over 1 days are considered dormant. It is recommended to remove them.</p> <p>(0) Tasks open <span style="float: right;"><a href="#">Create Task &gt;</a></span></p>
<b>!1</b>	<p><b>Orphaned Users</b></p> <p>These are users that are disabled in the Organizational Directory but still have valid accounts in the cloud application. It is recommended to remove those accounts.</p> <p>(0) Tasks open <span style="float: right;"><a href="#">Create Task &gt;</a></span></p>
<b>0</b>	<p><b>External Users</b></p> <p>These users do not appear in the Organizational Directory although they have valid accounts in the cloud application. It is recommended to verify these accounts.</p> <p>(0) Tasks open <span style="float: right;"><a href="#">Create Task &gt;</a></span></p>

**Configuration Settings Review** (9 Violations)

**Password Requirements**

- ! Account lockout

Cloud app setting	Recommended value	<a href="#">Create Task &gt;</a>
15 minutes <small><a href="#">See previous scan results &gt;</a></small>	30 minutes <span style="color: blue;">?</span>	(0) Tasks open
- > ! Max number of failed logins
- > ! Password expiration
- > ✓ Min length
- > ✓ Password complexity
- > ! Prevent password re-use

**Authentication Requirements**

- > ✓ \* Multi-factor authentication
- > ! SSO

**API Access**

At the top of **Governance Policy**, the selected standard is described, and the total number of **Violations** appears. Details of the requirements and their violations appear below **Configuration Settings Review**; click any requirement to expand its details. \* means a new violation as defined by [policy](#). You can click to **See previous scan results** for the requirement.

Hover over ? to view the relevant sections of the standard. For example:

**Configuration Settings Review (9 Violations)**

- > -! Password expiration
- > ✓ Min length
- > ✓ Password complexity
- > -! Prevent password re-use

**Authentication Requirements**

- > ✓ \* Multi-factor authentication
- > -! SSO

**API Access**

- > ✓ Root access

**Session Settings**

- ∨ -! \* Remember me

Cloud app setting: Enabled (See previous scan results >) / Disabled (0) Tasks open

**Relevant sections in PCI DSS:**  
 3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

► User accounts that should be removed or validated, including:

**Governance Policy**

Active Policy: **PCI DSS V3.0...**  
 Last Scan: 03/28/16 03:41  
[See Policy Details >](#)  
[Set Notifications >](#)

Description: PCI DSS V3.01 with a much lower dormancy time

4 Users with excessive rights | 9 \* Violations | \$ 1000 Overspend (\$/month)

**Excessive Rights (4 users)**

**!4 Dormant Users**  
 User accounts that have not been used for over 1 days are considered dormant. It is recommended to remove them.  
 (0) Tasks open [Create Task >](#)

**!1 Orphaned Users**  
 These are users that are disabled in the Organizational Directory but still have valid accounts in the cloud application. It is recommended to remove those accounts.  
 (0) Tasks open [Create Task >](#)

**0 External Users**  
 These users do not appear in the Organizational Directory although they have valid accounts in the cloud application. It is recommended to verify these accounts.  
 (0) Tasks open [Create Task >](#)

**Configuration Settings Review (9 Violations)**

**Password Requirements**

∨ -! Account lockout

Cloud app setting	Recommended value
15 minutes <a href="#">See previous scan results &gt;</a>	30 minutes ?

(0) Tasks open [Create Task >](#)

- > -! Max number of failed logins
- > -! Password expiration
- > ✓ Min length
- > ✓ Password complexity
- > -! Prevent password re-use

**Authentication Requirements**

- > ✓ \* Multi-factor authentication
- > -! SSO

**API Access**

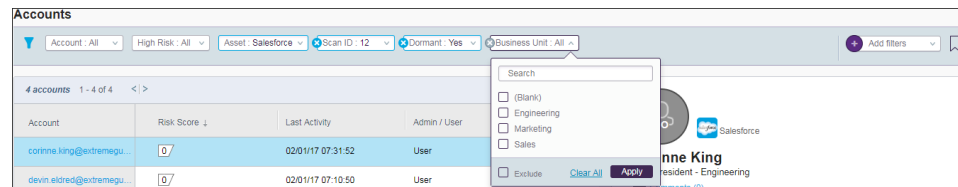
- ▶ **Dormant Users:** Asset user accounts that have not been used recently, within a time span defined by **policy**. The number of dormant users is multiplied by the **configured average price** to produce the displayed **Overspend**.
- ▶ **Orphaned Users:** Asset user accounts that have been disabled in the organizational directory and therefore might belong to users who have left the organization.
- ▶ **External Users:** Asset user accounts that do not appear in the organizational directory at all.

Categories with new users as defined by **policy** are marked ✨.

All three categories are aggregated at the top as **Users with excessive rights**.

Click any of the numbers to go to the **Accounts page**, filtered as relevant.

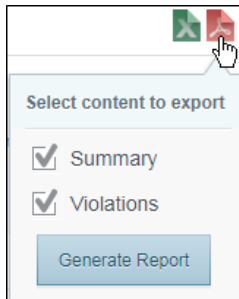
You can filter the user account information by business units as defined in the **organizational directory**, by adding a **Business Unit** filter on the right side, then selecting the relevant business unit:



By each policy violation and user account category, you can **Create Task**.

You can produce an Excel spreadsheet that contains user information.

You can produce a PDF report with configurable sections similar to the Governance dashboard:



## Managing account access and security remediation

Forcepoint CASB provides a task management system for creating, assigning, and tracking the status of Governance remediation tasks.

Forcepoint CASB automatically populates tickets with information that will be needed by task handlers. Assigned task handlers receive a link to a Forcepoint CASB that does not require logging in and enables only configuring the ticket.

Tickets can be configured to integrate with external ticketing systems via email.

To create a remediation task:

1. Go to **Compliance > Governance > Dashboard** for the selected asset:

The screenshot shows the 'Governance Dashboard' for a selected asset. It is divided into two main sections: 'Application Usage' and 'Governance Policy'.

**Application Usage:** This section contains three cards. The first card, 'Users', shows '2' users, with a sub-note '(1 unmonitored users)'. The second card, 'Recent Usage', features a pie chart and two data points: 'Within last 2 weeks 1 | 50% users' and 'More than 12 weeks ago 1 | 50% users'. The third card, 'Admins', shows '1' admin and lists 'Administrators: alan@automasky.com | I'm A...'.

**Governance Policy:** This section displays an 'Active Policy' named 'ISO 27002/27...' with a 'Last Scan' of '05/28/18 06:53'. A description states: 'This policy provides user access and application configuration recommendations based on the ISO 27002/27018 standards and security industry best practices.' To the right, there are three summary boxes: '1 Users with excessive rights', '10 Violations', and '\$ 50 Overspend (\$/month)'. A 'See Policy Details >' link and a 'Set Notifications >' link are also visible.

2. By the relevant policy violation or user account category, click **Create Task**:

The screenshot shows the 'Session Security' settings page. At the top, there is a status indicator with a red exclamation mark and a yellow star, followed by the text 'Remember password'. Below this is a table with two columns: 'Cloud app setting' and 'Recommended value'. The 'Cloud app setting' is 'Enabled' (with a link 'See previous scan results >') and the 'Recommended value' is 'Disabled' (with a question mark icon). To the right of the table is a blue 'Create Task >' button. Below the button, it says '(0) Tasks open' with a hand cursor icon pointing to the button.

3. Configure the ticket fields, including:

**Task: • Fix Session Remember Password** Created On: 22.09.2017

---

Name:

Type: Session Remember Password

Priority:  ▾

Assignee:

Status:  ▾

Resolution:  ▾

Affected Accounts (0)

Notifications

Notify Skyfence admins

Send ticket to external system

► By **Assignee**, select from among known asset administrators:

<b>Assignee</b>	<input type="text" value=""/>
<b>Status</b>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>sales@extremeguitars.net (SaaS Admin)</p> <p>admin@wininet.com (SaaS Admin)</p> <p>hr@forcepoint.com</p> <p>rac@forcepoint.com</p> </div>
<b>Resolution</b>	

The **Tasks assignee notification** must be properly [configured](#).

- ▶ Assignees are automatically notified; you can select to additionally **Notify Forcepoint CASB admins**. The **Tasks notify admins email** must be properly [configured](#).
- ▶ You can select to **Send** an email to open a **ticket** in an external ticketing **system**. The **Tasks mail to case notification** must be properly [configured](#).

4. Click **Save**.

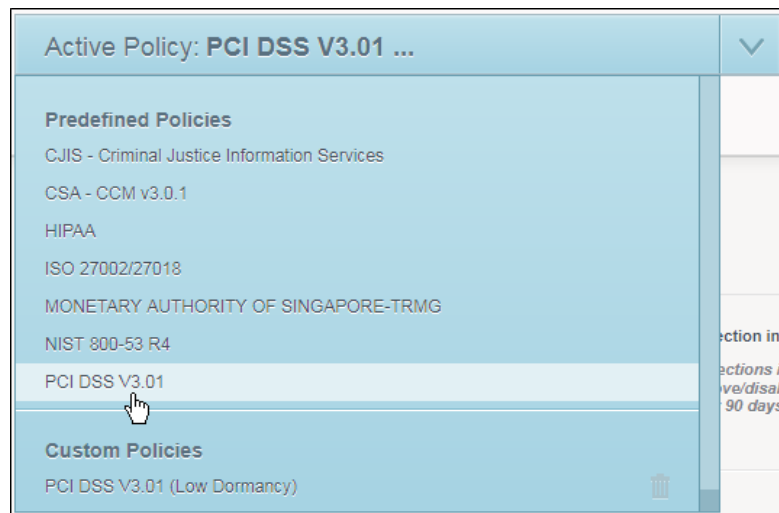
## Configuring the governance policy

You can configure the policy standards for the [Governance dashboard](#).

For each supported cloud application asset, Forcepoint CASB provides several predefined policies that conform to recognized legal and regulatory standards. New Forcepoint CASB versions include up-to-date versions of these policies. You can use any of them as is, or clone and customize any of them to adjust to organizational policy. You can copy customized policies between systems (for example, from a testing environment to production) or between assets.

To configure the Governance policy and settings for an application asset:

1. Go to **Compliance > Governance > Policies**.
2. Select a predefined policy (to use as is, or to copy and customize):



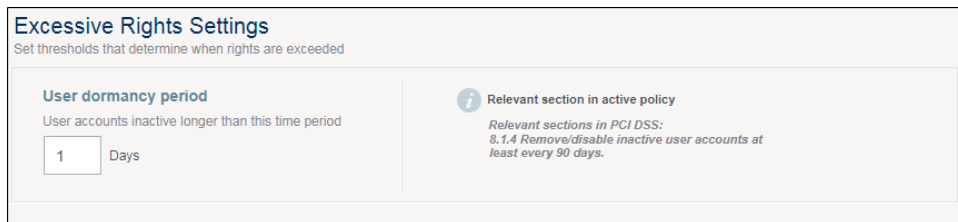
3. To copy the policy and customize its requirements:



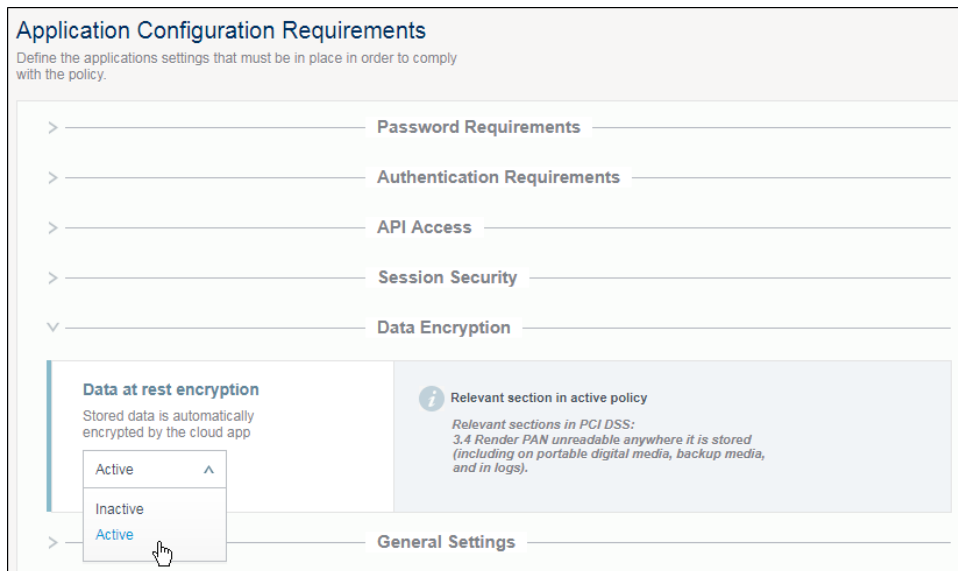
- a. Click **Clone Policy**:



- b. Under **Excessive Rights Settings**, set the number of days after which an unused user account is considered dormant:



- c. Under **Application Configuration Requirements**, go through the requirement values and customize as relevant. For example:

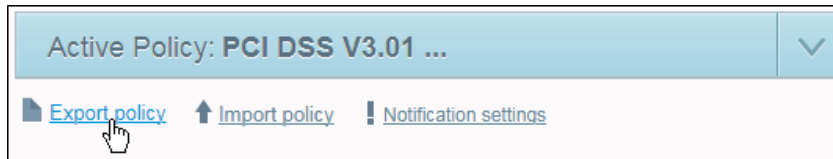


- d. Under **Advanced Settings**, configure the number of days after which newly-found items (policy violations or excessive-right users) should no longer be marked as new.

4. Click **Save Changes**.

Changes will take effect upon the [next scan](#).

To copy a customized policy between systems or between assets, you can **Export** and **Import** policies:



Optionally, define a **Scan Schedule**:

1. Go to **Compliance > Governance > Policies**.
2. Open the **Schedule** tab and choose your scheduling options.

### Scan Schedule

Choose manual scan or define a schedule for automatic scanning

Not Scheduled

Daily  :

Weekly  :

Monthly  :

Timezone:

3. Click **Save Changes**.
4. If you do not define a schedule, you will need to periodically come back here and click **Run Scan Now**. You can view here the status of latest scans:

### Governance scanning status

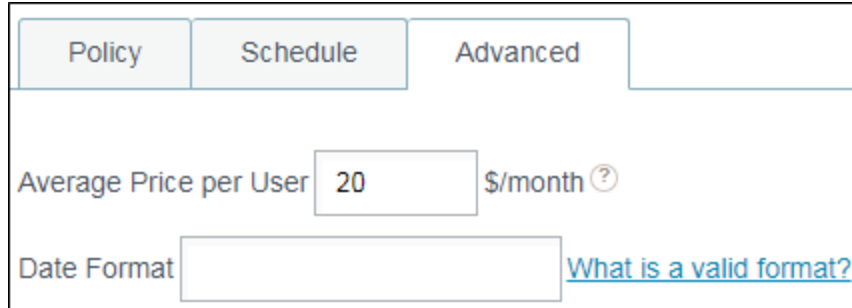
This section will describe the import access & security governance status and the next run due date

<p>Last Execution</p> <p>Start Time: 9/27/17 1:53:02 AM</p> <p>Status: <span style="color: green;">Ready</span></p> <p>Elapsed Time: 1 min 28 sec</p>	<p>Last Successful Execution</p> <p>Start Time: 9/27/17 1:53:02 AM</p> <p>Elapsed Time: 1 min 28 sec</p>
---	--

5. Upon scan completion, notifications are sent as [configured](#). These notifications include information about changes relative to the previous scan.

Optionally, set an **Average Price Per User**, to be used for calculating [Overspend](#):

1. Go to **Compliance > Governance > Policies**.
2. Open the **Advanced** tab and choose your options.



The screenshot shows a web interface with three tabs: 'Policy', 'Schedule', and 'Advanced'. The 'Advanced' tab is selected. Below the tabs, there are two input fields. The first is labeled 'Average Price per User' and contains the value '20', followed by the unit '\$/month' and a help icon. The second is labeled 'Date Format' and is currently empty, with a blue link 'What is a valid format?' to its right.

3. For Forcepoint CASB to properly parse activity logs received from the service, enter the **Date Format** in which the service displays the date and time for activities. To view format syntax, click **What is a valid format?**.
4. Click **Save Changes**.  
Changes take effect only upon the next scan.

# Data classification

---

For managed assets, Forcepoint CASB scans the contents of stored files and provides detailed information about stored sensitive material – as defined by configurable [data types](#) – including how it is accessed and shared inside and outside the organization.

Supported assets are:

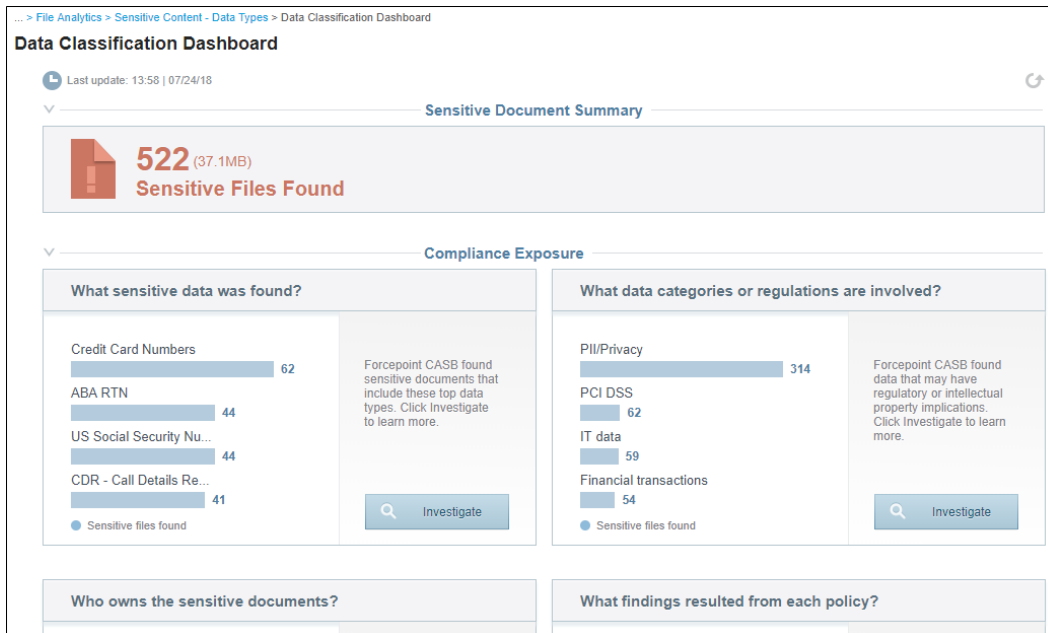
- ▶ Office 365
- ▶ Box
- ▶ Google G Suite
- ▶ Dropbox
- ▶ ServiceNow
- ▶ Salesforce.com
- ▶ Amazon Web Services (AWS)
- ▶ Cisco Webex

Scan locations, schedules, and the data types to be matched are configurable by [policy](#). Forcepoint CASB displays the latest scan results in a high-level [dashboard](#) that can drill down to specialized [reports](#), and also in the detailed and comprehensive [File Analytics](#).

Scan results from multiple policy scans are aggregated per-asset; found files' originating policies are listed in File Analytics.

## The Data Classification dashboard

The [Data Classification dashboard](#) provides high-level information from latest scan results in a high-level [dashboard](#) with drill-down to specialized [reports](#). The dashboard is at **Compliance** > asset > **Data Classification** > **Dashboard**:



The **Summary** at the top displays the number of **Sensitive Files Found**. Click the number to drill-down to [File Analytics](#).

Under **Compliance Exposure**, the found files are presented in several ways:

- ▶ **What Sensitive Data Was Found:** The most common [data types](#) found
- ▶ **What data categories or regulations are involved:** The most-found data type categories (predefined, as appearing in [DLP policies](#))
- ▶ **Who owns the sensitive documents:** The owners (as defined by the storage asset) of most-found files
- ▶ **What findings resulted from each policy:** The scan policies that produced most results

Click any number to drill-down to represented files in [File Analytics](#). To view a detailed [report](#) based on any of the above criteria, click **Investigate**.

## Data Classification reports

Forcepoint CASB provides [Data Classification Reports](#) that list and arrange found sensitive or shared files according to a specific criterion:

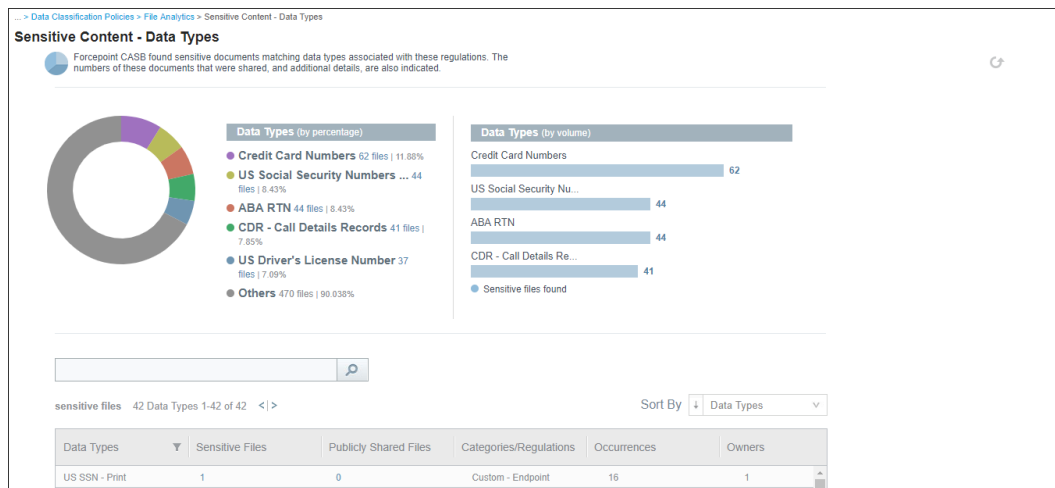
The following reports are available for investigating sensitive content:

- ▶ **Data Type:** This report displays the sensitive content that matches [data types](#) associated with specific regulations.
- ▶ **Data Category:** This report displays the sensitive content sorted by the data categories defined in [DLP policies](#).
- ▶ **Content Owner:** This report displays the sensitive content sorted by the file owners defined by the storage asset.
- ▶ **Policy:** This report displays the sensitive content sorted by the [policies](#) that define the scans that found the files.
- ▶ **External DLP System:** This report displays the sensitive content found by the external DLP products that are connected to Forcepoint CASB through an ICAP connector.

The following reports are available for investigating content that has been publicly shared:

- ▶ **Data Type:** This report displays the shared content that matches [data types](#) associated with specific regulations.
- ▶ **Data Category:** This report displays the shared content sorted by the data categories defined in [DLP policies](#).
- ▶ **Content Owner:** This report displays the shared content sorted by the file owners defined by the storage asset.

You can reach reports from the [Data Classification dashboard](#) by clicking **Investigate Data**, or from **Compliance** > asset > **Data Classification** > **Reports** > report type:



Found files are arranged in either a pie chart or a bar chart. Click the icon in the upper right corner of the chart pane to switch between the pie chart and the bar chart. Below the chart, each value is listed in a table, along with information about the files relevant to that value. You can further sort and filter the table.

Wherever a number of files appears, click the number it to analyze the files on the [File Analytics](#) page.

## Investigating stored sensitive files

The **File Analytics** page enables detailed investigation of stored files found by [Data Classification](#) and [Malware Inspection](#) scans.

You can access the File Analytics page by drilling down from the [dashboard](#) or [reports](#) pages, in which case the File Analytics page is automatically filtered as relevant, or directly at **Compliance > asset > Data Classification > File Analytics**:

The screenshot shows the File Analytics interface. At the top, there are filters for Data type, Sharing Status, and Owner. Below the filters, a table lists 633 files. The table has columns for Last Inspected, File Name, Sensitive Data, Occurrences, and 3rd Party Analysis. The first row is highlighted, showing a file named 'pdt-10 DRIVER LICENSE.d...' with 2 occurrences of 'PII/Privacy US Driver's Lice...'. To the right of the table, a detailed view for the selected file is shown. It includes a 'Scan history' section with a link to 'Documents/Work/pdt-10 DRIVER LICENSE.docx' and a 'Data classification results' section showing 1 occurrence of 'PII/Privacy: US Driver's License Number (?)'. The 'Sharing permissions' section indicates the file is not shared, and the 'Owner' section lists Corinne King as the owner.


Last Inspected	File Name	Sensitive Data	Occurrences	3rd Party Analy
07/22/18 17:42	pdt-10 DRIVER LICENSE.d...	PII/Privacy US Driver's Lice...	2	
07/22/18 17:42	pdt-9.docx	PII/Privacy Hong Kong ID(2)	4	
07/22/18 17:42	pdt-8.docx		0	
07/22/18 17:42	pdt-14 NHS NUMBER.docx	PII/Privacy UK NHS(1)	2	
07/22/18 17:42	Pdt-7 Credit Report.pdf	PCI DSS: Credit Card Num...	8	
07/22/18 17:41	pdt-7 Clients- Billings may ...	PCI DSS: Credit Card Num...	7	
07/22/18 17:41	pdt-6 project53.txt		0	
07/22/18 17:41	pdt-6 ip list.xlsx		0	
07/22/18 17:41	pdt-6 project53.cpp		0	
07/22/18 17:41	pdt-46 BOD report .pdf	PII/Privacy Canadian SIN(1...	15	

Each row of the table represents a file. Click within a row to open the file's detailed view on the right side of the screen. The detailed view displays information about the file, including type of sensitive data found and the number of occurrences, the sharing permissions, and the file's owner.

For more information about the columns available in the File Analytics table, see ["File Analytics table column descriptions"](#) on page 160.

You can view a log of changes to the file as found in previous scans. Click **Scan history** to open a table of changes from previous scans:

Last Inspected	File Name	Sensitive Data	Occurrences	3rd Party Analysis	Sharing Status	Shared With	
09/24/17 18:26	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
07/16/17 16:31	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
07/09/17 16:31	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
05/30/17 16:31	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
05/30/17 07:34	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
05/12/17 16:41	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
05/03/17 12:48	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
12/15/16 15:31	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
12/11/16 15:31	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl
10/05/16 15:31	pd1-10 DRIVER LICENSE.d...	PII/Privacy/US Driver's Lice...	1		Not Shared		Cl

 **Note:** Files that are no longer considered sensitive continue to appear, with their **File Sensitivity Status** marked accordingly.

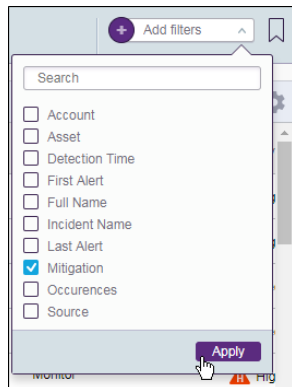
If a Malware Inspection policy finds a file infected with malware, the **Detected Malwares**, **File Infection Status**, and **Malware Risk** columns are populated. Also, the file's detailed view displays the malware name and severity level (as a triangular icon filled with the severity level's color code) in the **Malware Inspection Results** section. To view a detailed analysis report in PDF format, click **see report**.

To sort by any column (ascending / descending), click the column header.

To filter the table by any column value:

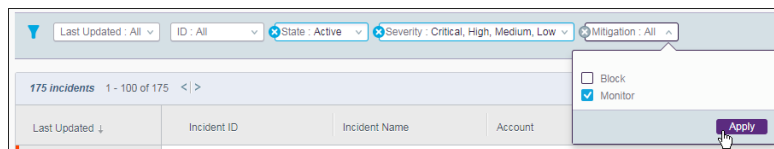
1. Click the **Add filters** drop-down menu.
2. Select one or more of the options and click **Apply**. The new filter is added to the list of active filters above the table.



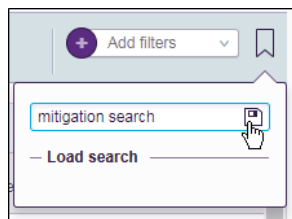


**Note:** The filter values are dependent on the values available for that table and can differ from the values shown in the images above and below.

- Expand the new filter, select the filter option, then click **Apply**.



- To save the current filters as a search, click the bookmark button to the right of the **Add filters** field, type a name for the search, and click the save button.





- To load the saved search, click the button to the right of the **Add filters** field and select the search from the **Load search** list.

To export the table to a CSV file, click . To refresh the display, click .

## Scanning for malware infection

If you have purchased a license for the Advanced Malware Detection add-on, the File Analytics page can also display files infected with malware.

---

 **Note:** To use this capability, you must purchase a license for the Advanced Malware Detection add-on. To see if you already have a license, click  > **About**. If **Advanced Malware Detection** is listed under the **Licensed Add-ons** section, you have purchased a license for this add-on.

---

To scan stored files for malware infection, you must first create a Data Classification policy and select **Malware Inspection** as the **Content**. For more information, see "[Configuring Data Classification policies](#)" on page 163.

Forcepoint CASB then scans the stored files, identifies files infected with malware, and applies the mitigation actions recorded in the policy. For a list of file types analyzed by the Advanced Malware Detection add-on, see "[Advanced Malware Detection supported file types](#)" below.

## Advanced Malware Detection supported file types

The Advanced Malware Detection add-on analyzes the following file types:

File extension	Description
.7z	7-zip archive data
.ace	ACE archive data
.apk	Android APK archive
.bat, .cmd	Batch script text
.bat, .exe, .cpl, .cmd, .pif, .com, .scr	PE executable
.bundle	Mach-O executable bundle
.bundle, .o, .dylib	Mach-O executable
.bundle, .o, .dylib	Mach-O fat file
.cab	Microsoft Cabinet archive data
.chm	Microsoft Windows HtmlHelp data
.class	compiled Java class data

File extension	Description
.com	COM executable for DOS
.com	EICAR test virus
.csv	CSV Data
.dat	Transport Neutral Encapsulation Format
.diagcab	Microsoft Diagnostic Cabinet archive data
.doc	Microsoft Word document in MHTML format
.doc	Microsoft Office Word document
.doc, .docx	Microsoft Office Word document (with password)
.docm	Microsoft Office Word document, Office Open XML format, with macros
.docx	Microsoft Office Word document, Office Open XML format
.dot	Microsoft Office Word document template
.dotm	Microsoft Office Word document template, Office Open XML format, with macros
.dotx	Microsoft Office Word template document, Office Open XML format
.eml	RFC2822-formatted Email file
.exe	MS-DOS executable
.exe	RAR SFX PE executable
.exe	Zip SFX PE executable
.exe	7zip SFX PE executable
.hta	HTA Script File text
.htm, .html	HTML document
.hwp	Hangul Word Processor document
.hwp	Hangul HWP3/HWP2000 document

File extension	Description
.iqy	Internet Inquiry data file
.iso	ISO 9660 CD-ROM filesystem data
.jar	Java JAR archive
.js	JavaScript text
.jse	JScript encoded script
.lappbundle, .lapp, .tar	Lastline Application Bundle Document Type
.lappbundle, .lapp, .tar	Lastline Application Bundle macOS Executable Type
.lappbundle, .lapp, .tar	Lastline Application Bundle Windows Executable Type
.lappbundle, .lapp, .tar	Lastline Application Bundle Web Replay Type
.lzh, .lha	LHa archive data
.lzma	LZMA compressed data
.msi	Microsoft Installer file
.nupkg	NuGet package archive
.o	Mach-O executable program
.o, .dylib	Mach-O executable program
.odp, .ods, .odt, .otg, .otp, .ott, .odg	Open/LibreOffice document
.oxps	OpenXPS document
.pcapng, .pcap	tcpdump capture file
.pdf	PDF document

File extension	Description
.pl, .pm	Perl script text
.pot	Microsoft Office PowerPoint template document
.potm	Microsoft Office PowerPoint presentation template, Office Open XML format, with macros
.potx	Microsoft Office PowerPoint template document, Office Open XML format
.pps, .ppt	Microsoft Office PowerPoint document
.ppsm	Microsoft Office PowerPoint Slideshow, Office Open XML format, with macros
.ppsx	Microsoft Office PowerPoint Slideshow, Office Open XML format
.ppt	Microsoft PowerPoint document in MHTML format
.pptm	Microsoft Office PowerPoint document, Office Open XML format, with macros
.pptx, .ppsx	Microsoft Office PowerPoint document, Office Open XML format
.pptx, .ppt	Microsoft Office PowerPoint document (with password)
.psm1, .psd1, .ps1	PowerShell text
.pub	Microsoft Publisher document
.py	Python script text
.rar	RAR archive data
.rar	RAR archive data, version 5
.rtf	RTF document
.settingcontent-ms	Microsoft Content-Settings data file
.sh, .command	Shell script text
.smi, .dmg	Apple disk image

File extension	Description
.svg	SVG image data
.swf	Macromedia Flash data
.sylnk, .slk	Symbolic Link data file
.sys, .exe, .dll	Lastline PE test file
.tar	POSIX tar archive data
.tbz2, .tbz, .bz2, .bz	bzip2 compressed data
.tgz, .gz	gzip compressed data
.tiff, .tif	TIFF image data
.udf, .iso	UDF filesystem data
.url, .lnk	Microsoft Windows shortcut
.url, .website	Internet Shortcut file
.vba	Visual Basic for Applications text
.vbe	VBScript encoded script
.vbs	VBScript text
.war	Java Webapp archive
.wpd	WordPerfect document
.wsf	Windows Script File text
.xar, .pkg	XAR archive data
.xdp	Adobe XDP document
.xlam	Microsoft Office Excel add-in, Office Open XML format, with macros
.xls	Microsoft Excel document in MHTML format
.xls	Microsoft Office Excel document
.xlsb	Microsoft Office Excel document, Office Open XML format, with macros and

File extension	Description
	binary storage
.xlsm	Microsoft Office Excel document, Office Open XML format, with macros
.xlsx	Microsoft Office Excel document, Office Open XML format
.xlsx, .xls	Microsoft Office Excel document (with password)
.xlt	Microsoft Office Excel template document
.xltn	Microsoft Office Excel spreadsheet template, Office Open XML format, with macros
.xltx	Microsoft Office Excel template document, Office Open XML format
.xml	XML-based Microsoft Office Excel document, pre-Office 2007
.xml	XML-based Microsoft Office Powerpoint presentation, pre-Office 2007
.xml	XML-based Microsoft Office Word document, pre-Office 2007
.xps	Microsoft XPS document
.xsl	eXtensible Stylesheet Language for XML file
.xz, .txz	XZ compressed data
.zip	Zip archive data

Source: [Lastline Supported Artifacts](#)

## File Analytics table column descriptions

The following table provides detailed descriptions about the type of information displayed in the File Analytics table.

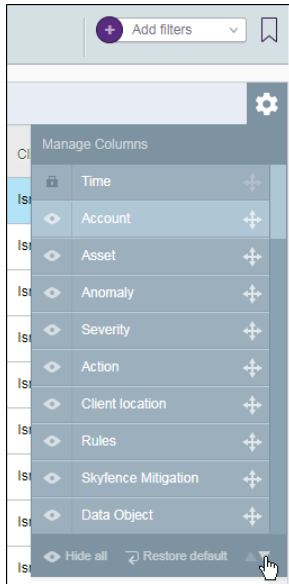
Column name	Column description
Last Inspected	The date and time when the file was last inspected by Forcepoint CASB.
File Name	The name of the file, including the file extension.
Sensitive Data	A list of the sensitive data found in the file. This information is provided in the following format: <Data Type Category>:<Data Type Name>(<Data Type Occurrences>).

Column name	Column description
Occurrences	The total number of times the sensitive data was found in the file.
3rd Party Analysis	The name of the 3rd party who analyzed the file. This is currently the ICAP connector's name.
Sharing Status	The status of the file's sharing permissions: <ul style="list-style-type: none"> <li>▶ <b>Not Shared:</b> The file is not shared with other accounts.</li> <li>▶ <b>Shared Externally:</b> The file is shared with one or more accounts outside of your organization's domain(s).</li> <li>▶ <b>Shared Internally:</b> The file is shared with one or more accounts inside of your organization's domain(s).</li> <li>▶ <b>Shared Publicly:</b> The file is shared with one or more accounts outside of your organization's domain(s) or with everyone within the domain(s).</li> </ul>
Shared With	A list of accounts (both internal and external) that the owner is sharing the file with.
Owner	The full name of the file's owner. This data is retrieved from the User Directory if integration is in place; otherwise, it is empty.
Owner Email	The email address of the file's owner.
File Sensitivity Status	The status of the file's sensitivity: <ul style="list-style-type: none"> <li>▶ <b>Not sensitive:</b> The file contained sensitive data, but was then found to be free of sensitive data during the last inspection.</li> <li>▶ <b>Removed:</b> The file is no longer found at the location identified by Forcepoint CASB.</li> <li>▶ <b>Sensitive:</b> The file contains sensitive data.</li> </ul>
File Path	The directory path of the file on the cloud service.
Mitigation Status	The mitigation action taken by Forcepoint CASB as a result of the policies breached by the file.
Archive Path	The archive folder location, if the file was quarantined or copied by Forcepoint CASB.
Modification	The date and time when the file was last modified.



Column name	Column description
Time	
Creation Time	The date and time when the file was created.
Access Time	The date and time when the file was last accessed by any account.
File Type	The file type as detected by Forcepoint CASB.
File Size	The file size as detected by Forcepoint CASB.
Policies	A list of data classification policies attached to this file.
Detected Malwares	A list of malware found in the file by the Advanced Malware Detection service.  An Advanced Malware Detection add-on license is required to gather this information.
File Infection Status	The status of the infected file: <ul style="list-style-type: none"> <li>▶ <b>Clean:</b> The file was infected with malware, but was then found to be free of malware during the last inspection.</li> <li>▶ <b>Removed:</b> The file is no longer found at the location identified by Forcepoint CASB.</li> <li>▶ <b>Infected:</b> The file is infected with malware.</li> </ul> An Advanced Malware Detection add-on license is required to gather this information.
Malware Risk	The risk level associated with the malware found in the file (e.g., Critical, High, Medium, or Low).  An Advanced Malware Detection add-on license is required to gather this information.
File hash	The internal file hash record made by Forcepoint CASB.

In addition, Forcepoint CASB hides some columns from the default view. These columns can be added to the File Analytics table by selecting them from the Manage Columns menu.



The following columns are hidden by default.

Column name	Column description
Data Type	A list of all the data types found in the file.
Data Type Category	A list of all the data type categories found in the file.

## Configuring Data Classification policies

[Data Classification](#) policies define the scheduling, target storage folders, and inspection parameters for Data Classification and Malware Inspection scans. You can configure multiple policies.

Configured policies are listed in the **Data Classification > Policies** page, with summaries of configuration and latest results:

**Data Classification Policies** + Add Policy

---

### Business Confidential Information

All business sensitive data in all files for all users.

**Not Scheduled**

Summary: Canadian SIN, Business Confidential Information, Board of Directors' reports,...(4)  
Remediation Actions: Audit only

**Last result:**  
39 sensitive files out of 638 scanned

[Run Scan](#) [Clear scan cache](#)

[Edit](#) [Delete](#)

---

### PCI DSS data

Any payment card information for any user in any documents.

**Not Scheduled**

Summary: Credit Card magnetic stripe data, Credit Card Numbers,(2)  
Remediation Actions: Audit only

**Last result:**  
57 sensitive files out of 656 scanned  
**Scan completed with errors**

[Run Scan](#) [Clear scan cache](#)

[Edit](#) [Delete](#)


---

### Personal Health Information

Any health information in any file for any user.

**Not Scheduled**

**Last result:**  
39 sensitive files out of 656 scanned  
**Scan completed with errors**

 **Note:** You must have a configured API connection to create and run Data Classification policies. If you see a message stating "Asset governance API is not configured" on the policies page, or a message stating "Asset token is not configured" on the New Policy page, then an API connection is not configured for this asset. For more information about configuring this connection, see ["Configuring an API connection" on page 280](#).

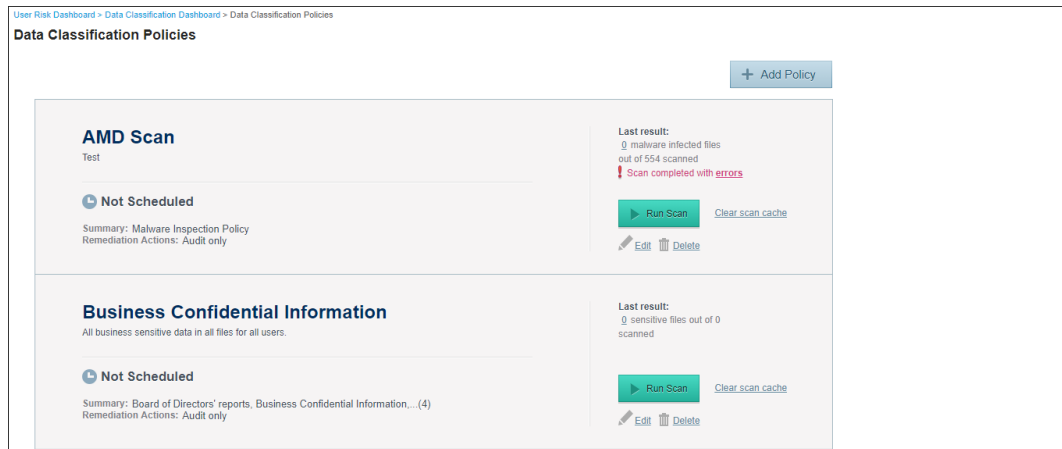
To manually activate a Data Classification policy, click **Run Scan**.

To edit an existing Data Classification policy, click **Edit**.

To delete a Data Classification policy, click **Delete**.

To create a Data Classification policy:

1. In Forcepoint CASB go to **Compliance > asset > Data Classification > Policies**:



2. Click **Add Policy**. The policy configuration window appears:

### New Policy

General Content Filters Schedule Mitigation

#### General

Title

Description

#### Scan Path

Folder Path

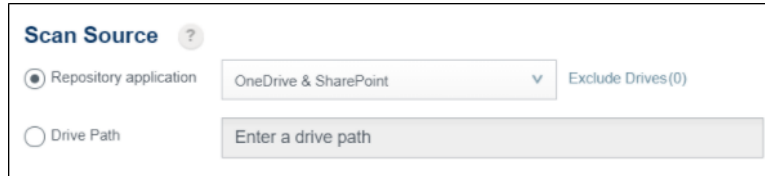
Exclude Subfolders(0)

[Save](#) [Cancel](#)

3. Enter a **Title** and **Description**.

- Under **Scan Path > Folder Path**, enter the full URL of the storage folder to be scanned. Optionally, click **Exclude Subfolders**, then enter the full paths of all subfolders that should not be included in the scan.


For Office 365 assets, the **Scan Path** settings are replaced by **Scan Source** settings:



Select either **Repository application** or **Drive Path**.

- ▶ If you select **Repository application**, select the repository to be scanned (**OneDrive**, **SharePoint**, or **OneDrive & SharePoint**). Optionally, click **Exclude Drives**, then enter the full paths of all drives that should be excluded from the scan.
  - ▶ If you select **Drive Path**, enter the full path of the drive to be scanned. By default, all folders and files in the drive path are scanned.
- (optional) To scan files with a specific sharing status, select **Scan by sharing status**, then select one of the options:
    - ▶ **Externally shared files**: Scans all files that are shared with accounts outside of your organization's domain(s).
    - ▶ **All shared files**: Scans all files that are shared with another account, including all files shared within your organization and outside of your organization's domain(s).

---

 **Note:** Scan by sharing status is only available for Office 365, Box, Dropbox, G Suite, and AWS assets.

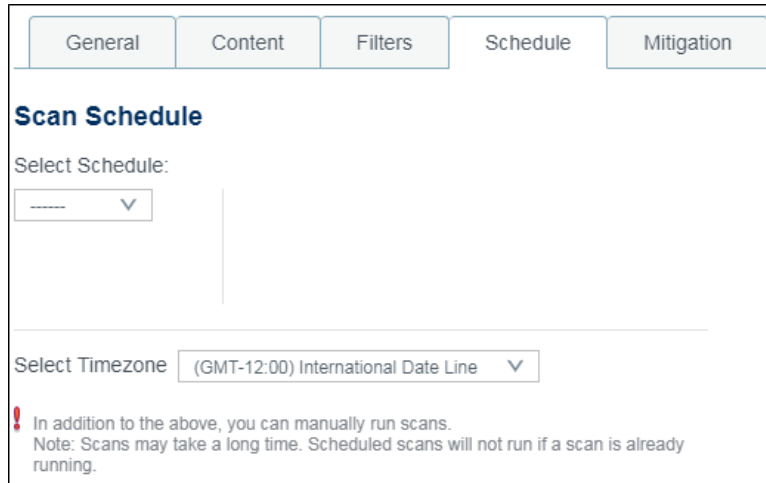
---

- On the **Content** tab, select one of the following options:
  - ▶ **Data Classification**: Select this option, then select [data types](#) to scan stored files and identify the files that contain the selected data types.
  - ▶ **Malware Inspection**: Select this option to scan stored files and identify the files infected with malware.

The Advanced Malware Detection add-on is required to select Malware Inspection. If Malware Inspection is disabled on this screen, check if you have an active Advanced Malware Detection license.

7. On the **Filters** tab, optionally limit the scan to files that were last modified in a specified date range:

8. For the policy to run automatically, on the **Schedule** tab, select the frequency and scheduling for scans:



General Content Filters Schedule Mitigation

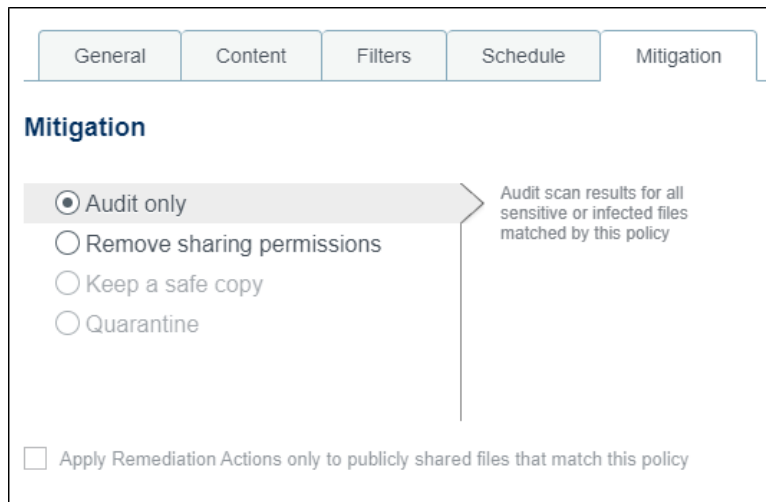
### Scan Schedule

Select Schedule:

Select Timezone: (GMT-12:00) International Date Line

**!** In addition to the above, you can manually run scans.  
Note: Scans may take a long time. Scheduled scans will not run if a scan is already running.

9. On the **Mitigation** tab, select a mitigation action:



General Content Filters Schedule Mitigation

### Mitigation

Audit only  
 Remove sharing permissions  
 Keep a safe copy  
 Quarantine

Audit scan results for all sensitive or infected files matched by this policy

Apply Remediation Actions only to publicly shared files that match this policy

Some assets have **Audit only** as the only available option, but some assets (like Office 365) list all mitigation actions available for API-based assets:

- ▶ **Audit only:** Forcepoint CASB audits the scan results for all sensitive or infected files matched by this policy. The scan results will appear in the Data Classification dashboard, file analytics, and reports.
- ▶ **Remove sharing permissions** (Office 365, Google G Suite, Salesforce, and Box only): Forcepoint CASB will remove the sharing permissions for all or a partial set of

users.

- For Google G Suite and Salesforce assets: Select either **All** users (only the file's owner will be able to access the file) or a **Partial** set of users (only remove file sharing for users **External** to our organization, or remove file sharing from **Everyone**).

Optionally for G Suite assets, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.

- For Office 365 and Box assets: Select **All** users to remove sharing permissions for all users (the file will only be accessible to the file owner), or select **Publicly Shared** to remove sharing permissions for users outside of your organization.

Optionally, select **Unshare parent folder** to remove sharing permissions for sensitive files that inherit the sharing permissions from one of their parent folders in the hierarchy. This removes the sharing permissions for the affected folders and all files located in them.

Optionally, select **Safe copy** to save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder.

- ▶ **Keep a safe copy:** Forcepoint CASB will save a copy of every infected or sensitive file that matches this policy to an authorized Archive folder. The Archive folder must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.
- ▶ **Quarantine:** Forcepoint CASB will move every infected or sensitive file that matches this policy to an authorized Archive folder. If you select **Leave a note**, Forcepoint CASB will leave a note in the quarantined file's original location. This note will indicate to the user that the file is quarantined. The Archive folder and note must be set up through the asset's Data Classification settings at **Settings > Resources > Assets > asset > Data Classification**.

10. Click **Save**.





# Encryption Broker

Forcepoint CASB | 2021 R4 | Updated: December 19, 2021


For managed assets, the Encryption Broker service leverages a bring your own key (BYOK) capability offered by the cloud services. Forcepoint CASB connects to your key management service (KMS) through an API connection to access your encryption keys. Then, Forcepoint CASB connects to the cloud service through another API connection, where the data is encrypted and decrypted based on the key provided by Forcepoint CASB from the KMS.

Enabling Forcepoint CASB as your encryption broker requires the following steps:

1. Connect Forcepoint CASB to your existing KMS instances through an API connection. See ["Adding a new key management service" on page 213](#) for more information.
2. Generate a new key on each KMS instance. See ["Generating a new key" on page 215](#) for more information.
3. Connect Forcepoint CASB to your asset through an API connection. See ["Configuring an API connection" on page 280](#) for more information.
4. Configure the asset's data encryption policy with the selected KMS, keys, and key rotation plan. See ["Configuring the data encryption policy" on page 172](#) for more information.
5. Review the data encryption audit log for policy and key rotation events. See ["Monitoring encryption-based events" on page 179](#) for more information.

Forcepoint CASB provides an easy interface within the management portal to define the key rotation policies and enforce those policies across services.

---

 **Note:** Currently, Forcepoint CASB only supports Office 365 OneDrive and SharePoint Online with the Azure Key Vault KMS.

---

This chapter discusses the following:

Managing the data encryption policy .....	172
---	-----

Monitoring encryption-based events ..... 179


For information about managing your KMS, see ["Managing your key management services" on page 213](#).

# Managing the data encryption policy

---

After you set up a new KMS in Forcepoint CASB, you can then configure and save a new data encryption policy for each asset. The data encryption policy determines which KMS and keys are used for the asset, configures the key rotation plan, and enables auditing to the data encryption audit log.

---

 **Note:** You can only create one data encryption policy per asset.

---

To manage the data encryption policy, you can:

- ▶ **Configure the data encryption policy:** Saves the data encryption policy. You must specify the KMS, keys, and key rotation plan before saving the data encryption policy. For more information, see ["Configuring the data encryption policy" below](#).
- ▶ **Disable the data encryption policy:** Stops running the data encryption policy, but keeps the configuration details in case you want to restart the policy in the future. For more information, see ["Disabling and enabling a data encryption policy" on page 176](#).
- ▶ **Reset the data encryption policy:** Stops running the data encryption policy and removes all configuration details in case you want to change the policy's configuration. For more information, see ["Resetting a data encryption policy" on page 177](#).

## Configuring the data encryption policy

To configure the data encryption policy, you need to:

- ▶ Identify the key sources and keys to be used with the data encryption policy.
- ▶ Save the data encryption policy.
- ▶ Configure the key rotation plan.

The configuration steps vary depending on the cloud service asset. Currently, Forcepoint CASB only supports Office 365 OneDrive and SharePoint Online with the Azure Key Vault KMS.

For more information about configuring the KMS and keys for the Office 365 data encryption policy, see ["Configuring the Office 365 data encryption policy" on the next page](#).

For more information about setting up a key rotation plan, see ["Setting a key rotation plan" on page 174](#).

# Configuring the Office 365 data encryption policy

Your data encryption policy is enabled by default, but not active until it has been configured and saved.

First, you must identify the key sources (in this case, Azure Key Vaults) and keys to be used with this data encryption policy. Office 365 encryption requires keys from 2 different Azure Key Vaults.

1. In Forcepoint CASB, go to **Compliance > Encryption Broker > Data Encryption Policy**, then select the relevant asset from the top left list of assets.

The screenshot displays the 'Data Encryption Policy' configuration interface. At the top, there is a breadcrumb trail: 'User Risk Dashboard > Data Encryption Policy'. The main heading is 'Data Encryption Policy'. Below this, there is a section for 'Enable Policy' with a toggle switch that is currently turned on. The 'Key Source and Key(s)' section is divided into two columns: 'Primary' and 'Secondary'. Each column has an 'Azure Key Vault' dropdown menu and a 'Key' dropdown menu. The Primary column shows 'BenVault1' for the vault and 'BV1Key1' for the key. The Secondary column shows 'BenVault2' for the vault and 'BV2Key1' for the key. To the right of these columns is a blue information icon and a text box explaining that Office 365 encryption requires keys from two different Azure Key Vaults (AKVs) and that only keys configured on the same tenant as the Office 365 asset and marked as Soft Delete AKV are available. Below this is the 'Key Rotation Plan' section, which includes radio buttons for 'None', 'Regulation-Based Rotation' (set to 'PCI - Once a Year'), and 'Custom: Rotate every' (set to '1' weeks). A 'Rotate Now' button is visible next to the 'None' option. To the right of the rotation plan, there is a 'Last Rotation' timestamp of '05/03/18 09:41:49' and a 'Key(s) Rotation State' of 'Rotated Successfully'. At the bottom of the page, there are buttons for 'Save', 'Export Active Keys', and 'Reset Policy'.

2. Under **Key Source and Key(s)**, set the **Primary** key vault and key:
  - a. Select a key vault from the **Azure Key Vault** drop-down menu.

If you do not have an available key vault, click **Create New AKV** to create one. For more information about creating a new Azure Key Vault KMS, see ["Adding a new Office 365 key management service" on page 213](#).

After you select a key vault, the **Key** drop-down menu populates with the keys available in that key vault. Only keys that are enabled, do not have an expiration date, and are not used by other policies are available.

- b. Select an available key from the **Key** drop-down menu.

If you do not have an available key, click **Create New Key** to create one. For more information about generating a new key, see "[Generating a new Office 365 key](#)" on [page 215](#).

3. Under **Key Source and Key(s)**, set the **Secondary** key vault and key:

a. Select a key vault from the **Azure Key Vault** drop-down menu.

If you do not have an available key vault, click **Create New AKV** to create one.

After you select a key vault, the **Key** drop-down menu populates with the keys available in that key vault. Only keys that are enabled, do not have an expiration date, and are not used by other policies are available.

b. Select an available key from the **Key** drop-down menu.

If you do not have an available key, click **Create New Key** to create one.

4. Click **Save**.

---

**!** **Important:** If your key rotation plan is not set to **None**, changing the keys on an active, enabled policy will trigger an immediate key rotation when you save the changes.

---

After the policy is saved, Forcepoint CASB logs all operations within the scope of the data encryption policy to the data encryption audit log. Also, the key rotation plan starts if you set one up. For more information, see "[Setting a key rotation plan](#)" below.

## Setting a key rotation plan

Forcepoint CASB can manually or automatically rotate the relevant keys in the Azure Key Vaults and update the Office 365 bring your own key (BYOK) configuration based on the key rotation plan you have configured. When you rotate your active keys, Forcepoint CASB replaces the active key in the data encryption policy with a different key in your KMS.

1. In Forcepoint CASB, go to **Compliance > Encryption Broker > Data Encryption Policy**.
2. Under **Key Rotation Plan**, select and configure your key rotation:

- a. **None:** This option allows you to manually rotate your keys at any time. Click **Rotate Now** to rotate the keys.

---

 **Note:** Keys can only be rotated once within a 24 hour period.

---

- b. **Regulation-Based Rotation:** This option allows you to set your rotation schedule to comply with specific regulations:
  - ▶ **NIST:** rotates the keys every two years.
  - ▶ **PCI:** rotates the keys every one year.
- c. **Custom:** This option allows you to set a rotation schedule that is set to a specific time interval. In the field, type a number, then select either **weeks**, **months**, or **years** from the drop-down menu.

For example, to rotate your keys every two weeks, type **2** in the field and select **weeks** from the drop-down menu.

3. Click **Save**.

After the key rotation schedule is saved, the rotation status information updates:

- ▶ **Last Rotation** displays the date and time when the keys were last rotated.
- ▶ **Key(s) Rotation State** displays the status of the last key rotation:
  - **Rotated Successfully:** The last rotation was successful. The key rotation plan is now waiting for the next rotation.
  - **In Progress:** The keys are currently under rotation. Key rotation can take a while to complete.
  - **Failed:** The last rotation was unsuccessful.
- ▶ **Next Rotation** displays the upcoming date when the keys will be rotated. If the key rotation plan is set to **None**, this entry is blank.

## Exporting active keys

Forcepoint CASB allows you to export your active keys to provide a backup. Forcepoint recommends keeping a backup of your active keys in case of a critical problem with your KMS instance.

- !** **Important:** The exported keys are not the actual keys that are being used to encrypt the data at the cloud service; they are only a backup. The exported keys are encrypted by KMS, so the exported keys can only be imported back to the same KMS instance. In addition to being encrypted by the KMS, the keys are stored encrypted within Forcepoint CASB for extra safety.

1. In Forcepoint CASB, go to **Compliance > Encryption Broker > Data Encryption Policy**.
2. Click **Export Active Keys** at the bottom of the page.



- ✎ Note:** Active keys can only be exported after a successful key rotation and cannot be exported when a key rotation is in progress.

3. Forcepoint CASB downloads the active keys from your last successful key rotation to your local endpoint machine. For Office 365, the keys are downloaded in a ZIP file.

## Disabling and enabling a data encryption policy

If you no longer want Forcepoint CASB to serve as the broker between the cloud service and your KMS, you can disable the data encryption policy for the asset.

When the policy is disabled, Forcepoint CASB:

- ▶ Stops the key rotation plan.
- ▶ Stops all actions on the asset. (Configuration on the asset side is left as-is.)
- ▶ Marks the policy page as disabled.
- ▶ Blocks the policy from making any additional changes.
- ▶ Updates the data encryption audit log to reflect that the policy has been disabled.

To disable the policy:

1. In Forcepoint CASB, go to **Compliance > Encryption Broker > Data Encryption Policy**.
2. Select the relevant asset from the top left list of assets.
3. Next to **Enable Policy**, click the toggle switch.
4. Confirm that you want to disable the policy. When the switch turns gray, the policy is disabled.

To enable a disabled policy:

1. In Forcepoint CASB, go to **Compliance > Encryption Broker > Data Encryption Policy**.
2. Select the relevant asset from the top left list of assets.
3. Next to **Enable Policy**, click the toggle switch. When the switch turns green, the policy is enabled.

When the policy is enabled, the key rotation plan reactivates. If the **Next Rotation** date passed while the policy was disabled, the key rotation starts automatically.

## Resetting a data encryption policy

Reset the policy if you want to disable the current policy and remove the current configuration, returning the policy to its initial state (as if it were a new policy). When you reset the policy, Forcepoint CASB:

- ▶ Returns all policy settings (i.e., KMS, keys, rotation plan) to the default values.
- ▶ Stops the key rotation plan.
- ▶ Stops all actions on the asset. (Configuration on the asset side is left as-is.)
- ▶ Updates the data encryption audit log to reflect that the policy has been reset.
- ▶ Clears the **Used By Asset** column in the Keys table.
- ▶ Removes the active keys backup.

To reset the policy to its initial state:

1. In Forcepoint CASB, go to **Compliance > Encryption Broker > Data Encryption Policy**.
2. Click **Reset Policy** at the bottom of the page.





3. Confirm that you want to reset the policy.
4. Click **Save**.
5. To configure the policy again, see "[Configuring the data encryption policy](#)" on page 172.

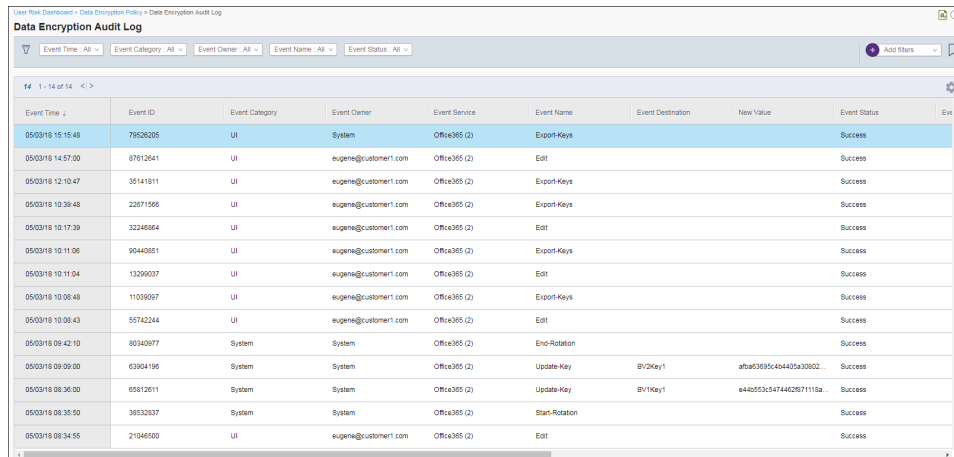
# Monitoring encryption-based events

After a data encryption policy is enabled and saved, Forcepoint CASB collects the encryption-based events in the data encryption audit log. For more information, see ["The data encryption audit log" below](#).

## The data encryption audit log

The data encryption audit log provides details about the actions and changes made to the data encryption policy, such as disabling the policy or executing a manual key rotation. You can view the state of automatic processes, such as data encryption policy health changes (e.g., if a key is no longer valid), or track the key rotation progress and state, with relevant error messages in case of a rotation failure.

1. In Forcepoint CASB, go to **Compliance > Encryption Broker > Data Encryption Audit Log**.
2. Select the relevant asset from the top left list of assets.
3. The audit log appears:



The screenshot shows the 'Data Encryption Audit Log' interface. At the top, there are filter options for Event Time, Event Category, Event Owner, Event Name, and Event Status. Below the filters, a table displays a list of events. The table has columns for Event Time, Event ID, Event Category, Event Owner, Event Service, Event Name, Event Destination, New Value, and Event Status. The events listed include actions like 'Export-Keys', 'Edit', and 'Start-Rotation' for 'Office365 (2)'.

Event Time	Event ID	Event Category	Event Owner	Event Service	Event Name	Event Destination	New Value	Event Status
05/03/18 15:15:48	79526205	UI	System	Office365 (2)	Export-Keys			Success
05/03/18 14:57:00	87812641	UI	eugene@customer1.com	Office365 (2)	Edit			Success
05/03/18 12:10:47	35141811	UI	eugene@customer1.com	Office365 (2)	Export-Keys			Success
05/03/18 10:39:48	22871566	UI	eugene@customer1.com	Office365 (2)	Export-Keys			Success
05/03/18 10:17:39	32246984	UI	eugene@customer1.com	Office365 (2)	Edit			Success
05/03/18 10:11:06	90448851	UI	eugene@customer1.com	Office365 (2)	Export-Keys			Success
05/03/18 10:11:04	13299037	UI	eugene@customer1.com	Office365 (2)	Edit			Success
05/03/18 10:08:48	11028997	UI	eugene@customer1.com	Office365 (2)	Export-Keys			Success
05/03/18 10:08:43	55742244	UI	eugene@customer1.com	Office365 (2)	Edit			Success
05/03/18 09:42:10	80340977	System	System	Office365 (2)	Enc-Rotation			Success
05/03/18 09:09:00	63904196	System	System	Office365 (2)	Update-Key	B\2Key1	afba3695c494405a30802	Success
05/03/18 08:36:00	65812611	System	System	Office365 (2)	Update-Key	B\1Key1	e44053c547446287111ba...	Success
05/03/18 08:35:50	38532837	System	System	Office365 (2)	Start-Rotation			Success
05/03/18 08:34:55	21046500	UI	eugene@customer1.com	Office365 (2)	Edit			Success

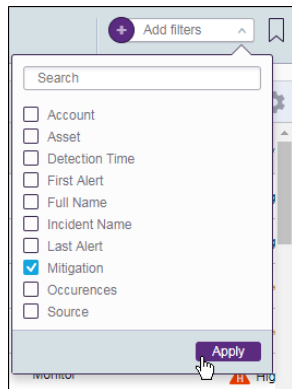
To navigate between pages, click the arrows next to the number of the activities above the table.


To sort by any column (ascending / descending), click the column header.

To filter the table by the values of any column:

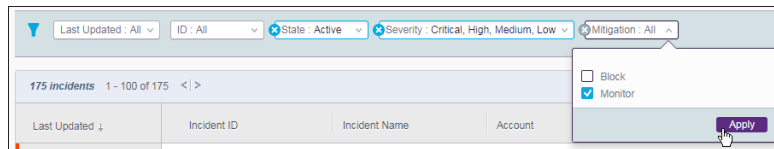
1. Click the **Add filters** drop-down menu.
2. Select one or more of the options and click **Apply**. The new filter is added to the list of

active filters above the table.

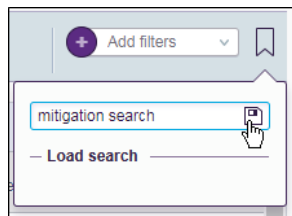


 **Note:** The filter values are dependent on the values available for that table and can differ from the values shown in the images above and below.


3. Expand the new filter, select the filter option, then click **Apply**.



4. To save the current filters as a search, click the bookmark button to the right of the **Add filters** field, type a name for the search, and click the save button.



5. To load the saved search, click the button to the right of the **Add filters** field and select the search from the **Load search** list.

To configure the displayed columns and their order, click the  button.

To export the table to a CSV file, click . To refresh the display, click .



# CHAPTER 11

## Forcepoint CASB System Administration

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

This chapter explains how to configure various aspects of the Forcepoint CASB system that are relevant to all managed assets. Configuration tasks that apply to service assets individually are explained in [Managing Service Assets](#).

This chapter discusses the following:

Providing a user directory .....	182
Configuring Forcepoint CASB administration .....	195
Configuring account privacy .....	208
Managing your key management services .....	213
Managing REST API connections .....	218
Endpoint enrollment .....	224
Configuring internal domains .....	231
Configuring IP ranges .....	233
Configuring trusted proxies .....	237
Configuring trusted IP addresses for IP Reputation .....	238
Configuring notifications .....	239
Configuring data types .....	249
Configuring an ICAP connection .....	255
Setting up SIEM / syslog integration .....	259
Downloading Tools and Agents .....	267
Licensing .....	268

# Providing a user directory

---

Forcepoint CASB needs access to an organizational user directory, for the following purposes:

- ▶ To display full user details wherever they appear
- ▶ To send email and SMS [notifications](#)
- ▶ To perform [identity verification](#) and [endpoint enrollment](#)
- ▶ To identify asset user accounts that are [orphaned or external](#)

You can provide Forcepoint CASB with an organizational user directory in one of two ways:

- ▶ [Manual file upload](#): Prepare a user directory file and upload it to Forcepoint CASB. To update Forcepoint CASB with organizational changes, you'll need to periodically upload an updated complete file.
- ▶ (Recommended) [Active Directory retrieval](#): Provide a connection to the organizational Active Directory to retrieve user information. If the Forcepoint CASB server cannot access the organizational Active Directory, the [Forcepoint CASB AD Agent](#) can access the Active Directory from inside the organizational network and upload the user account information to the Forcepoint CASB server.

To view Forcepoint CASB's currently known user information, go to **Settings > Account Management > User Data**.

Discovery information for existing scan results is not automatically updated with new user information. To update existing Discovery information, remove the scan results, then upload them again.

## Manually uploading a user directory

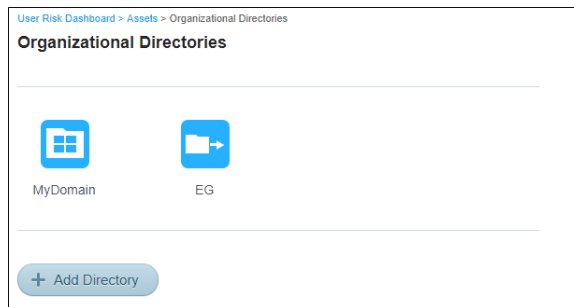
One way of providing Forcepoint CASB with a [user directory](#) is by manual upload. You can provide multiple directories for different parts of the organization.

To upload a user directory:

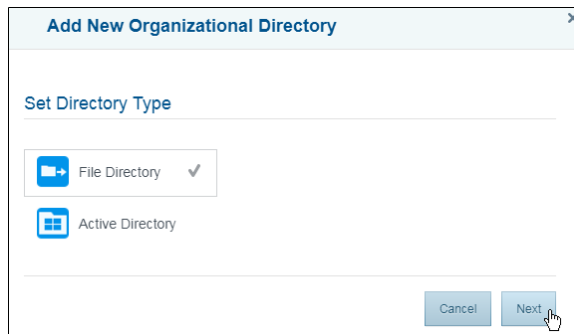
1. From the organizational Active Directory, export a CSV file and edit as necessary. The CSV file must include a single header row and a row for each user account; it must include 13 fields (columns) with the following exact headers. Fields marked below as optional can be with empty content, but the column and header must be defined. All field values will appear wherever user details are displayed.
  - ▶ **accountName**
  - ▶ **firstName**

- ▶ **lastName**
- ▶ **email**
- ▶ **phone**
- ▶ **title**
- ▶ **businessUnit**
- ▶ **custom1, custom2, custom3** (optional): For display, and can also be used as criteria in [custom policy Who sections](#)
- ▶ **picture** (optional)
- ▶ **disabled**: true / false
- ▶ **distinguishedName**: The user's LDAP DN

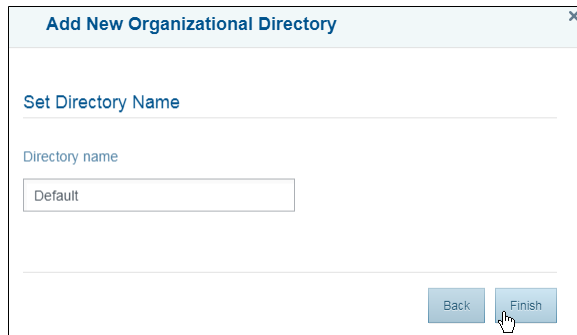
2. In Forcepoint CASB, go to **Settings > Account Management > Organizational Directories**, then click **Add Directory**:



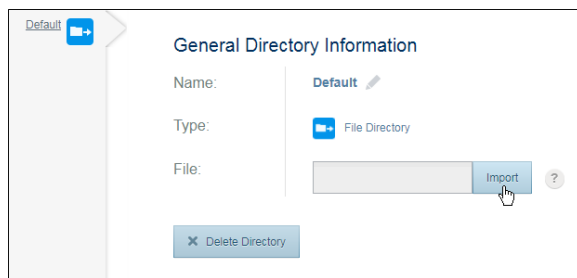
3. Select **File Directory**, then click **Next**:




4. Enter a **Directory Name**, then click **Finish**:

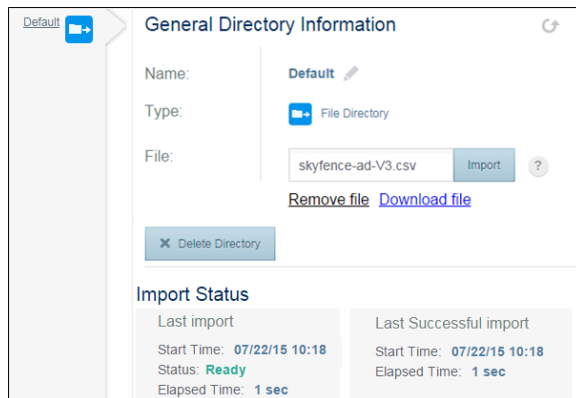


5. With this directory selected, click **Import** and upload the CSV file:



The directory is now available to Forcepoint CASB. To update Forcepoint CASB with organizational changes, you'll need to periodically upload an updated complete file.

Under **Import Status**, Forcepoint CASB displays information about the last file upload for this directory item. To refresh this information, click  :



You can subsequently **Download** the file from here, then use it as a basis for changes.

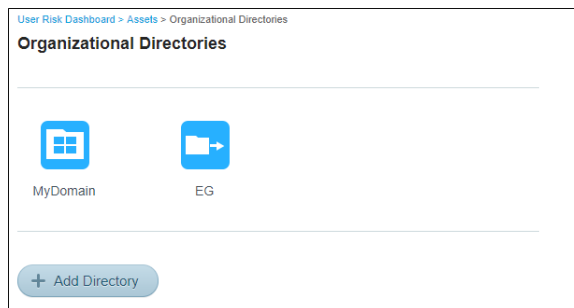
You can **Delete** the directory from Forcepoint CASB. Or, if you plan to replace the file but want Forcepoint CASB to immediately stop using the directory, you can **Remove** the file and leave the configured directory item available for the future file.

## Configuring Active Directory retrieval

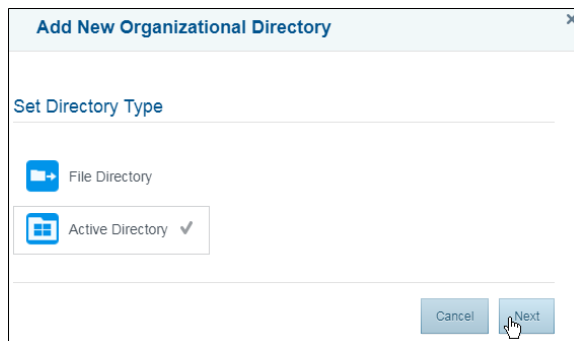
The recommended method of providing Forcepoint CASB with user information is via Active Directory retrieval. If the Forcepoint CASB server cannot access the organizational Active Directory, the [Forcepoint CASB AD Agent](#) can access the Active Directory from inside the organizational network and upload the user account information to the Forcepoint CASB server.

To configure Active Directory retrieval:

1. Obtain Active Directory connection details from your organizational Active Directory administrator.
2. In Forcepoint CASB, go to **Settings > Account Management > Organizational Directories**, then click **Add Directory**:




3. Select **Active Directory**, then click **Next**:



4. Enter a **Directory Name**, then click **Finish**:



5. With this directory selected, click  to edit the Active Directory LDAP connection fields:

- ▶ **Address:** Resolvable name or IP address of Active Directory server.
- ▶ **Port:** Active Directory listening port; usually 389 (clear connection) or 636 (encrypted connection).
- ▶ **Use LDAPS (optional):** Configures Forcepoint CASB to connect to the Active Directory using the LDAPS protocol. This also changes the Port configuration to 636

automatically.

- ▶ **User and Password:** Credentials of a user account with Read permissions for the user accounts.
  - ▶ **LDAP Root:** Base DN of users to be imported.
  - ▶ **Default Domain** (optional): Optional for connecting to Active Directory.
6. Under **Import Method**, select whether the Active Directory retrieval will be from the Forcepoint CASB AD Agent (**Agent connection**) or directly from the Forcepoint CASB server (**Direct connection**):

**Import Settings**

**Import Method**  
Forcepoint CASB can connect to the directory directly or using an agent installed on premise with the directory.

Direct connection  
 Agent connection

---

**Schedule Information**  
You can import the directory manually or schedule regular imports

Not Scheduled

Daily    0 : 0

Weekly    0 : 0    Sunday ▾

Monthly    0 : 0    1st ▾

Timezone    (GMT-12:00) International Date Line ▾

7. Configure the retrieval **Schedule Information**.
8. Click **Save Settings**.
9. If you selected **Direct connection** as the **Import Method**, click the **Check Connection** button to test the connection to the Active Directory server.
- If you selected the **Agent connection** import method, you cannot check the connection until after you complete the configuration through the AD Agent.
10. If field names in the organizational Active Directory are non-standard, type those field

names in the **Map to** column under **Field Mappings**. Forcepoint CASB will use those fields' values for the Forcepoint CASB fields listed in the **Field Name** column.

Optionally, if you want to stop Forcepoint CASB from importing data associated with a specific field, deselect the checkbox to the left of the **Field Name**. If the box does not have a check mark, Forcepoint CASB does not import that data from your Active Directory.

**Field Mappings**

Change imported field names.  
 Uncheck an Active Directory field name to stop importing this field's data from your Active Directory.  
 Note: Changes will only take place at the next import operation.

<input type="checkbox"/>	Field Name	Map to	Search Expression	Replace Expression
<input checked="" type="checkbox"/>	Account	samaccountname		
<input checked="" type="checkbox"/>	First Name	givenname		
<input checked="" type="checkbox"/>	Last Name	sn		
<input checked="" type="checkbox"/>	Account Email	mail		
<input checked="" type="checkbox"/>	Account Phone	mobile		
<input checked="" type="checkbox"/>	Title	title		
<input checked="" type="checkbox"/>	Business Unit	department		
<input type="checkbox"/>	Picture	thumbnailphoto		
<input checked="" type="checkbox"/>	Disabled	userAccountControl		
<input checked="" type="checkbox"/>	DN	distinguishedName		

Optionally, you can provide **Search Expressions** and **Replace Expressions** to manipulate field values as needed; the part of the field value identified by the **Search Expression** regular expression (RegEx) will be replaced by the **Replace Expression**, which can be a fixed string or another part of the field value identified by regular expression.

- Optionally, you can configure custom fields to be displayed; these fields can also be used as criteria in [custom policy Who sections](#). To configure custom fields, under **Custom Mappings**, in the left-hand column add any or all of (exactly) **custom1**, **custom2**, and **custom3**, and to its right type the Active Directory fields to use for their values:

You can also manipulate field values as for the required fields above.

12. You can click **Test Mapping** to see the results of the mapping configuration, if you selected **Direct connection** as the **Import Method** above.

If you selected the **Agent connection** import method, you cannot test the mapping until after you complete the configuration through the AD Agent.

If you made any changes to **Field Mappings** or to **Custom Mappings**, click **Save Field Mappings**.

If you are not using the AD Agent, you can initiate an immediate retrieval by scrolling back up and clicking **Import Now**.

If you are using the AD Agent, see "[Setting up Active Directory Agent retrieval](#)" below for more information about configuring the AD Agent.

If you need to remove the directory from Forcepoint CASB, click Delete Directory back at the top.

To view Forcepoint CASB's currently known user information, go to **Settings > Account Management > User Data**. Mappings are reflected in this list.

## Setting up Active Directory Agent retrieval

The recommended method of providing Forcepoint CASB with user information is via Active Directory retrieval. If the Forcepoint CASB server cannot access the organizational Active Directory, install the AD Agent provided by Forcepoint CASB inside the organizational network. The AD Agent will retrieve connection and scheduling details from the Forcepoint CASB server and will automatically upload retrieval results to the Forcepoint CASB server.

To set up agent retrieval:


1. Set up [Active Directory retrieval](#), selecting **Import Method: Agent connection**.
2. Download the trust store: In Forcepoint CASB, go to **Settings > Tools and Agents**. Under

the **Active Directory Tool** section, click **Download Trust Store**.

Place the downloaded file in a location that will be accessible by the AD Agent after it is installed.

3. Download the agent: Go to **Settings > Tools and Agents**. Under the **Active Directory Tool** section, click **Download**.

---

 **Note:** You must have a valid Forcepoint CASB license to download this tool. This tool will only be visible on the Tools and Agents page if you have a valid license. Contact Forcepoint Support if you would like to use the tool, but do not see the tool on this Settings page.

---

4. Install the Forcepoint CASB AD Agent in a location that can access the Active Directory and the Forcepoint CASB server. For redundancy, it is recommended to install and configure the AD Agent on more than one computer.
5. Upon completing installation, the AD Agent configuration page appears. Alternatively, in the AD Agent installation folder (usually: **C:\Program Files (x86)\SkyfenceADAgent**), run **agentConfigurator.exe**.
6. Configure the AD Agent. All settings are required, unless specifically marked as optional (some have default values):

**FORCEPOINT** | Agent Configuration

Connection Settings | **Agent Settings** | Log Settings

Skyfence Administrator User Name

Skyfence Administrator Password

Skyfence URL ⓘ

Forcepoint CASB Certificate TrustStore (optional) ⓘ  
 Browse

LDAPS Certificate TrustStore (optional) ⓘ  
 Browse

Enable Proxy ⓘ

Proxy address (optional)

Proxy port (optional)

**Test Connection**

Please restart the AD Agent service after saving

Cancel Save

© 2017 Forcepoint

- ▶ On the **Connection Settings** tab:
  - **Skyfence Administrator User Name** and **Password**: Credentials with permissions to configure User Directories.
  - **Skyfence URL**: Management portal URL.
  - **Forcepoint CASB Certificate TrustStore**: Location of the file downloaded above.
  - **LDAPS Certificate TrustStore**: List of trusted certificate authorities of the

LDAP service in a TrustStore format. For more information, see "[Creating an LDAPS TrustStore for the Active Directory Agent](#)" on the facing page.

- **Enable Proxy:** If you are connecting through a proxy server, select this option, then enter the **Proxy address** and **Proxy port** for the proxy server.
  - ▶ On the **Agent Settings** tab:
    - **Agent Name:** If you're installing multiple agents, make sure each has a unique name. The agents will be listed in Forcepoint CASB user directory settings.
    - **Agent file storage folder:** A local folder where the agent can store user directories, enabling subsequent incremental retrievals.
    - **Active Directory Names:** Name(s) of Forcepoint CASB user directory configuration item(s). The Agent will retrieve these items' configurations for Active Directory connection details and for retrieval scheduling. You can click **Import AD names** to retrieve from the Forcepoint CASB server available user directory configuration items.
  - ▶ On the **Log Settings** tab:
    - **Log Output File** and **Log Level:** For local agent logs.
7. Click **Test Connection** to test the connection between the AD Agent and the Forcepoint CASB management portal, based on the administrator user name, administrator password, and the URL provided in the agent.
  8. Click **Save**.
  9. In the Windows service manager, start or restart the **SkyfenceADAgent** service.
  10. In the Forcepoint CASB management portal, navigate to the new Active Directory settings page (**Settings > Account Management > Organizational Directories > directory**), or refresh the page if you are already there, and see if the new AD Agent appears.

### Import Settings

**Import Method**

Forcepoint CASB can connect to the directory directly or using an agent installed on premise with the directory.

Direct connection

Agent connection

Agent Name	Agent IP	Agent Host	Last Update
AD-Agent	10.12.143.3	LT-032154	04/10/18 07:51

After the Active Directory configuration is complete, you can do the following tasks on the Active Directory settings page (**Settings > Account Management > Organizational Directories > directory**):

- ▶ Click **Check Connection** to test the connection between the Forcepoint CASB management portal, AD Agent, and the Active Directory server.
- ▶ Click **Test Mapping** to see the results of the mapping configuration. For more information, see "[Configuring Active Directory retrieval](#)" on page 185.

## Creating an LDAPS TrustStore for the Active Directory Agent

When working with the Forcepoint CASB AD Agent using the LDAPS protocol, you need to provide the AD Agent with the server's CA certificate in truststore format to enable trust from the client to the Active Directory Federation Services (AD FS).

Generate the truststore:

1. Export the CA certificate (in CER format) from the AD FS.
2. Copy the CA certificate to a system with Java Keytool installed.
3. Run the following command to add the CA certificate to a new keystore using the Keytool:

```
keytool -import -alias <alias name> -file <ca certificate> -  
keystore <keystore> -storepass <password> -noprompt
```

The certificate is now added to the keystore.

4. Run the following command to check if the CA certificate was added to the new truststore:

```
keytool -list -v -keystore <keystore>  
Enter keystore password: <your password>
```

The truststore information appears. If the CA certificate was correctly added, then the CA certificate information appears with the truststore information.

5. Add the truststore location to the AD Agent:
  - a. Open the AD Agent Configuration window.
  - b. On the Connection Settings tab, in the **LDAPS Certificate TrustStore** field, enter the directory where the truststore is located.
  - c. Click **Save**.
6. Restart the AD Agent service.

If you cannot trace the certificate presented by the proxy, and the AD Agent refuses to connect:



1. Add the following line to **runagent.bat**:  

```
"jre/bin/java" -Djavax.net.debug=ssl:handshake -cp "lib/"  
com.skyfence.management.idp.client.ADAgentService %
```
2. Run **runagent.bat** as an administrator.
3. Check the log, and verify that the certificate is present.

# Configuring Forcepoint CASB administration

---

Organizational Forcepoint CASB administrators can:

- ▶ Create additional administration accounts with configurable permissions. For more information, see ["Configuring administrator accounts and permissions" below](#).
- ▶ Configure administration account password requirements and login restrictions. For more information, see ["Configuring administrator account security settings" on page 202](#).
- ▶ Configure single-sign on so that Forcepoint CASB Administrators are authenticated by the organizational IdP and automatically logged into Forcepoint CASB. For more information, see ["Configuring administrator single sign-on" on page 206](#).

## Configuring administrator accounts and permissions

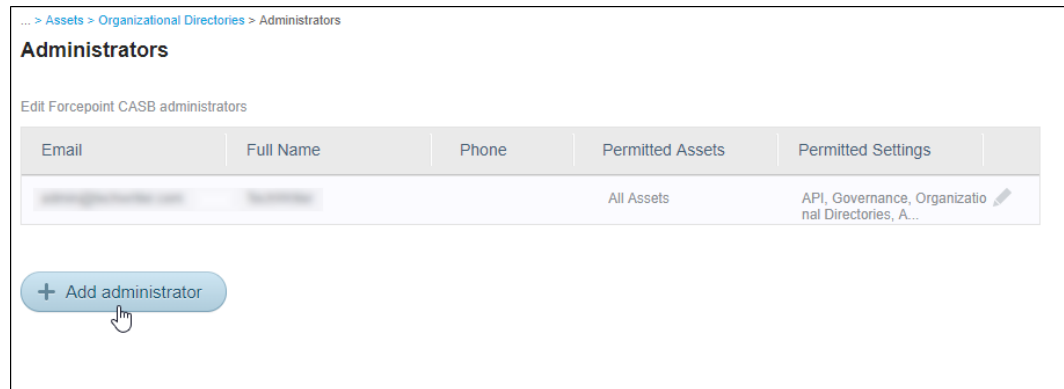
Organizational Forcepoint CASB administrators can create and configure additional administrative accounts:

- ▶ Creating a new administrator account (See ["Creating a new administrator account" below](#).)
- ▶ Editing an administrator account (See ["Editing an administrator account" on page 198](#).)
- ▶ Changing an administrator password (See ["Changing an administrator password" on page 200](#))
- ▶ Locking an administrator account (See ["Locking an administrator account" on page 198](#).)
- ▶ Unlocking an administrator account (See ["Unlocking an administrator account" on page 199](#).)

## Creating a new administrator account

To create a Forcepoint CASB administrator account:

1. In Forcepoint CASB, go to **Settings > Access Management > Administrators**:



2. On the **Administrators** page, click **Add administrator**:

**Administrator Details** ✕

### Details

Email	<input type="text"/>	Password	<input type="text"/>
Full Name	<input type="text"/>	Verify Password	<input type="text"/>
Timezone	<input type="text" value="(GMT-10:00) Hawaii"/>	<input checked="" type="checkbox"/> Requires a password change at first login	
Phone	<input type="text"/>	<input type="checkbox"/> Password never expires	

Your password must include at least:

- 8 characters
- One number (0-9)
- One uppercase letter
- One lowercase letter
- One special character (~ ! @ # \$ % ^ \* ( ) \_ +)

---

### Permissions

Define permissions to edit assets, policies and settings

<p><b>Assets</b></p> <p><input checked="" type="radio"/> All Assets</p> <p><input type="radio"/> Specific Assets</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Amazon AWS</li> <li><input type="checkbox"/> Box</li> <li><input type="checkbox"/> Office365</li> <li><input type="checkbox"/> G Suite</li> </ul>	<p><b>Settings</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Assets</li> <li><input checked="" type="checkbox"/> Organizational Directories</li> <li><input checked="" type="checkbox"/> User Data</li> <li><input checked="" type="checkbox"/> Administrators</li> <li><input checked="" type="checkbox"/> Notifications</li> <li><input checked="" type="checkbox"/> Endpoint Management</li> <li><input checked="" type="checkbox"/> Identity Providers</li> <li><input checked="" type="checkbox"/> IP Ranges</li> <li><input checked="" type="checkbox"/> Cloud Discovery</li> <li><input checked="" type="checkbox"/> Domains</li> <li><input checked="" type="checkbox"/> Governance</li> <li><input checked="" type="checkbox"/> Agent / Endpoint Monitoring</li> <li><input checked="" type="checkbox"/> Data Types</li> <li><input checked="" type="checkbox"/> API</li> <li><input checked="" type="checkbox"/> Single Sign On</li> <li><input checked="" type="checkbox"/> ICAP</li> <li><input checked="" type="checkbox"/> Tools and Agents</li> <li><input checked="" type="checkbox"/> Key Management Services</li> <li><input checked="" type="checkbox"/> Account Privacy</li> <li><input checked="" type="checkbox"/> Administrators Security</li> </ul>	<p><b>Screens</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Security Policies</li> <li><input checked="" type="checkbox"/> App Discovery</li> <li><input checked="" type="checkbox"/> Endpoints</li> <li><input checked="" type="checkbox"/> Accounts</li> <li><input checked="" type="checkbox"/> Dashboard</li> <li><input checked="" type="checkbox"/> Analytics</li> <li><input checked="" type="checkbox"/> Reports</li> <li><input checked="" type="checkbox"/> Upload License</li> <li><input checked="" type="checkbox"/> Governance</li> <li><input checked="" type="checkbox"/> Incidents</li> <li><input checked="" type="checkbox"/> User Risk Dashboard</li> <li><input checked="" type="checkbox"/> Data Classification</li> <li><input checked="" type="checkbox"/> Service Provider Audit</li> <li><input checked="" type="checkbox"/> Encryption Broker</li> </ul>	<p><b>Advanced</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Allow File Download</li> <li><input checked="" type="checkbox"/> Bypass SSO</li> <li style="color: red; font-size: 0.8em; margin: 5px 0;">! Cannot remove permission ⓘ</li> <li><input checked="" type="checkbox"/> Watchlist control allowed</li> </ul>
--	--	--	---

3. Configure user **Details**:

- a. Admin contact details: Enter the administrator's **Email** address, **Full Name**, **Timezone**, and **Phone** number.
- b. Admin password details: Enter the administrator's **Password**, then enter the same password in the **Verify Password** field. The password requirements are displayed in the right column. These requirements are configured on the Administrator Account

Security settings page. For more information about setting password restrictions, see ["Configuring administrator account security settings" on page 202](#).

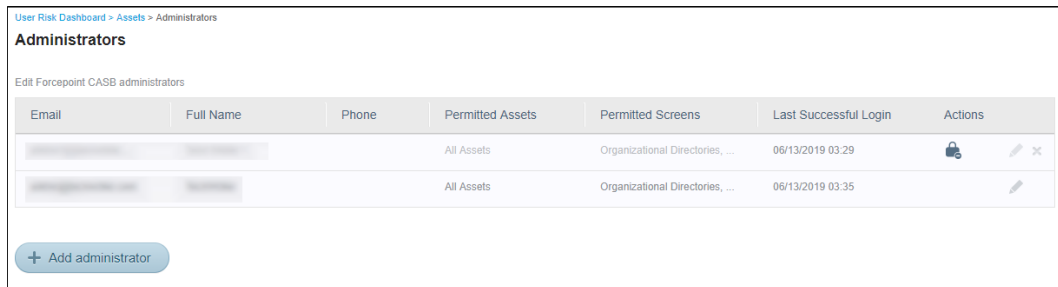
You can set two options when you create the password:

- ▶ **Requires a password change at first login:** When the administrator logs on with the password created here, Forcepoint CASB forces them to set a new password.
  - ▶ **Password never expires:** The password created here does not expire. This setting overrides the password expiration settings configured on the Administrator Account Security settings page.
4. Configure **Permissions**. Select the **Assets**, **Settings**, and **Screens** that the administrator can view and modify.
  5. Click **Save**.

## Editing an administrator account

To change an existing administrator account after you create it:

1. In Forcepoint CASB, go to **Settings > Access Management > Administrators**:



Email	Full Name	Phone	Permitted Assets	Permitted Screens	Last Successful Login	Actions
[REDACTED]	[REDACTED]	[REDACTED]	All Assets	Organizational Directories, ...	06/13/2019 03:29	[Lock] [Edit] [Delete]
[REDACTED]	[REDACTED]	[REDACTED]	All Assets	Organizational Directories, ...	06/13/2019 03:35	[Edit]

+ Add administrator

2. On the **Administrators** page, click the edit icon in the **Actions** column to display the **Administrators Details** screen.
3. Edit the administrator **Details** as necessary.
4. Click **Save**.

## Locking an administrator account

An administrator can be locked out of their account either manually by another administrator or automatically for the following reasons:

- ▶ **Too many unsuccessful login attempts.** If the administrator enters an incorrect password too many times within a 15 minute period, they are locked out of the account.
  - Commercial Forcepoint CASB administrators: The number of attempts and timeout period can be configured on the Administrator Account Security settings page. For more information, see ["Configuring login lockout restrictions" on page 203.](#)
- ▶ **The password expired:** Administrator passwords can be set to expire after a specific number of days.
  - Commercial Forcepoint CASB administrators: This setting is configured on the Administrator Account Security settings page. After the setting is enabled, you can set the active time period (between 30 and 180 days) and set up email notifications. For more information, see ["Configuring password restrictions" on page 202.](#)
- ▶ **The account has not been accessed within a set number of days:** If an administrator does not log in to their account within a set period of time, the account is locked because of inactivity.
  - Commercial Forcepoint CASB administrators: The timeout period is configured on the Administrator Account Security settings page. For more information, see ["Configuring login lockout restrictions" on page 203.](#)

An administrator can also be manually locked out of their account by another administrator:

1. In Forcepoint CASB, go to **Settings > Access Management > Administrators:**

Email	Full Name	Phone	Permitted Assets	Permitted Screens	Last Successful Login	Actions
[Redacted]	[Redacted]	[Redacted]	All Assets	Organizational Directories, ...	06/13/2019 03:29	🔒 ✎ ✕
[Redacted]	[Redacted]	[Redacted]	All Assets	Organizational Directories, ...	06/13/2019 03:35	✎

+ Add administrator

2. In the table, find the administrator account you wish to lock and click the lock icon.

## Unlocking an administrator account

To manually unlock a locked administrator account:

1. In Forcepoint CASB, go to **Settings > Access Management > Administrators**:

User Risk Dashboard > Assets > Administrators

### Administrators

Edit Forcepoint CASB administrators

Email	Full Name	Phone	Permitted Assets	Permitted Screens	Last Successful Login	Actions
[REDACTED]	[REDACTED]	[REDACTED]	All Assets	Organizational Directories, ...	06/13/2019 03:29	
[REDACTED]	[REDACTED]	[REDACTED]	All Assets	Organizational Directories, ...	06/13/2019 03:35	

+ Add administrator

Locked accounts display a black lock icon in the **Actions** column.

2. In the table, find the locked administrator account and click the gray lock icon.
3. A pop-up window opens and displays the reason why the account is locked. Click **Unlock**.

---

**!** **Important:** An administrator can not unlock their own account.

---

## Changing an administrator password

An administrator password can be changed at any time through the Administrator Details page.

1. In Forcepoint CASB, go to **Settings > Access Management > Administrators**:

User Risk Dashboard > Assets > Administrators

### Administrators

Edit Forcepoint CASB administrators

Email	Full Name	Phone	Permitted Assets	Permitted Screens	Last Successful Login	Actions
[REDACTED]	[REDACTED]	[REDACTED]	All Assets	Organizational Directories, ...	06/13/2019 03:29	
[REDACTED]	[REDACTED]	[REDACTED]	All Assets	Organizational Directories, ...	06/13/2019 03:35	

+ Add administrator

2. On the **Administrators** page, click the edit icon in the **Actions** column to display the **Administrators Details** screen.

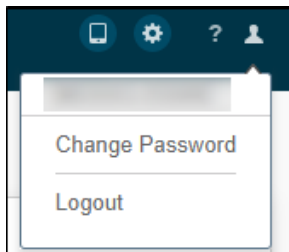
- In the **Details** section, update the administrator's **Password**, then enter the same password in the **Verify Password** field. The password requirements are displayed in the right column. These requirements are configured on the Administrator Account Security settings page. For more information about setting password restrictions, see "[Configuring administrator account security settings](#)" on the next page.

You can set two options when you update the password:

- ▶ **Requires a password change at first login:** When the administrator logs on with the new password created here, Forcepoint CASB forces them to set a new password when they log in with this password.
- ▶ **Password never expires:** The password created here does not expire. This setting overrides the password expiration settings configured on the Administrator Account Security settings page.

- Click **Save**.

Administrators can subsequently change their own passwords in Forcepoint CASB by selecting the **Change Password** option from the **Admin** menu:





# Configuring administrator account security settings

Organizational Forcepoint CASB administrators can modify the security settings for all Forcepoint CASB administrators within the organization. These security settings allow administrators to:

- ▶ Define the way administrator passwords are created. For more information, see ["Configuring password restrictions" below](#).
- ▶ Lock administrators out of their account. For more information, see ["Configuring login lockout restrictions" on the facing page](#).
- ▶ Restrict access by IP range. For more information, see ["Configuring IP address restrictions" on page 205](#).

## Configuring password restrictions

Password restrictions allow administrators to set specific requirements for all administrator passwords and prevent administrators from creating easy-to-guess passwords or reusing the same password. To set password restrictions for Forcepoint CASB administrator accounts:

1. In Forcepoint CASB, go to **Settings > Access Management > Administrator Account Security**.

User Risk Dashboard > Assets > Administrator Account Security

### Administrator Account Security

#### Password Restrictions

Configure the organizational guidelines for creating local passwords for Forcepoint CASB. These guidelines are enforced when a Forcepoint CASB administrator account is created or edited, and when an administrator requests to change their password at login.

##### Minimal Password Length

Set the minimum number of characters required in the password. Minimum length can be set between 8 and 64 characters. The maximum password length is 64 characters.

Minimum password length:  characters

##### Password Complexity

Set the requirements for using specific types of characters in the password to increase the password complexity. All character types are enabled by default, but none are required. You can disable one or all options to match your preferred guidelines.

- Uppercase letters
- Lowercase letters
- Special characters (~!@#\$%^&\*()\_+)
- Numbers (0-9)

2. In the **Password Restrictions** section, configure the requirements needed to create a password for administrator accounts:
  - a. To set the password length, enter the smallest number of characters required for your administrator passwords into the **Minimum password length** field in the **Minimal Password Length** subsection.

Administrator passwords must be between 8 and 64 characters.
  - b. To require specific types of characters in the passwords, select the relevant option(s)

in the **Password Complexity** subsection:

- ▶ **Uppercase letters:** Select this option to require at least one uppercase letter (A-Z).
- ▶ **Lowercase letters:** Select this option to require at least one lowercase letter (a-z).
- ▶ **Special characters:** Select this option to require at least one special character (~ ! @ # \$ % ^ & \* ( ) \_ +).
- ▶ **Numbers:** Select this option to require at least one number (0-9).

Selecting password complexity options is optional. You can select one, all, or none of these options, depending on your preferred organizational guidelines.

- c. To set the length of time in which the password is active, select the **Administrator must change password every XX days** option in the **Password Rotation** subsection, then enter the number of days into the field.

The number of days must be between 30 and 180.

When the set number of days have passed, the password expires. The administrator cannot log in to Forcepoint CASB until the password is changed. When the password is changed, the time until expiration reverts back to the time set in this subsection.

To let the administrator know that their password is about to expire, select the **Notify administrator when a password is about to expire** option. Selecting this option sends an email notification to the administrator. For more information about configuring email notifications, see ["Configuring an email notification" on page 242](#).

- d. To prevent administrators from reusing passwords, select one or more options in the **Password History** subsection.
  - ▶ **Administrator cannot reuse one of the last XX passwords:** The number of passwords must be between 4 and 12.
  - ▶ **Administrator cannot reuse a password used within the past XX days:** The number of days must be between 30 and 180.

3. Click **Save** at the bottom of the page.

## Configuring login lockout restrictions

Login lockout restrictions prevent administrators from accessing the management portal after they attempt to log in multiple times with the incorrect password.

To set login lockout restrictions for Forcepoint CASB administrator accounts:

1. In Forcepoint CASB, go to **Settings > Access Management > Administrator Account Security**.
2. On the **Administrator Account Security** screen, scroll down to the **Lockout settings** section.

**Lockout settings**

Setup lockout settings for administrators. Configure how long an account remains locked after failed logins, and what happens when an account becomes inactive.

**Failed Logins**

When an administrator fails to login 3 times in row in 15 minutes, they get locked until the lock expires. They can be released through the Administrators page.

Enable administrator lockout

Allow max:  failed login attempts before account lockout (3-10)

Release account after:  minutes (10-1440)

**Account Deactivation**

Setup how long after an administrator doesn't login to Forcepoint CASB, their account is deactivated. Inactive accounts can be reactivated through the Administrators page.

Enable account deactivation

Deactivate accounts after:  days since last successful login (1-90)

3. To lock administrators out of their accounts after entering an incorrect password, go to the **Failed Logins** subsection, select **Enable administrator lockout**, and configure the lockout options:

- ▶ **Allow max XX failed login attempts before account lockout:** Enter the number of times an administrator can enter a failed login before they are locked out of their account. This number must be between 3 and 10 login attempts.
- ▶ **Release account after XX minutes:** Enter the amount of time in which the administrator is locked out of the account. During this time, no login attempts are allowed. The administrator can try to log in to the account after the timer expires. This number must be between 10 and 1440 minutes.

An account can be manually released or manually disabled by another administrator from the Administrators settings page. For more information, see ["Configuring administrator accounts and permissions" on page 195](#).

4. To deactivate inactive accounts, go to the **Account Deactivation** subsection, select **Enable account deactivation**, and configure the option:

- ▶ **Deactivate accounts after XX days since last successful login:** Enter the number of days in which the account does not have a login attempt. If an administrator does not successfully login during this time period, the account is deactivated. This number must be between 1 and 90 days.

When this setting is enabled, Forcepoint CASB immediately applies the new setting and deactivates accounts that meet the new limit. For example, if you select 30

days and save the setting, Forcepoint CASB automatically deactivates the accounts that have already been inactive for 30 days.

Forcepoint CASB sends email notifications to the administrator 7 days before their account is to be deactivated, then when the account is deactivated.

An account can be manually reactivated or manually deactivated by another administrator from the Administrators settings page. For more information, see "[Configuring administrator accounts and permissions](#)" on page 195.

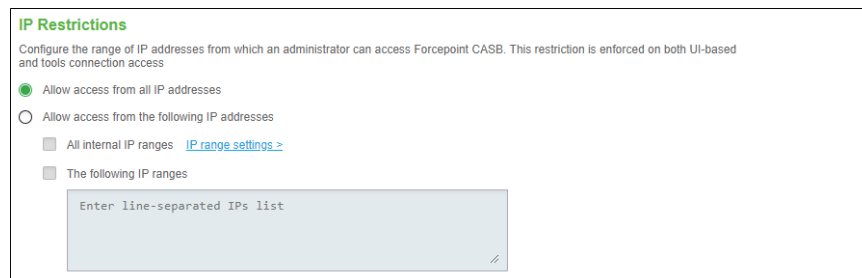
5. Click **Save** at the bottom of the page.

## Configuring IP address restrictions

IP address restrictions prevent administrators from logging in from specific IP address ranges.

To set IP address restrictions for Forcepoint CASB administrator accounts:

1. In Forcepoint CASB, go to **Settings > Access Management > Administrator Account Security**.
2. On the **Administrator Account Security** screen, scroll down to the **IP Restrictions** section.



3. In the **IP Restrictions** section, select one of the two options:
  - ▶ **Allow access from all IP addresses:** Administrators can log in to Forcepoint CASB from any IP address. logins are not restricted by IP address when you select this option.
  - ▶ **Allow access from the following IP addresses:** Select this option to restrict administrator logins to specific IP ranges:
    - **All internal IP ranges:** Administrators can only log in to Forcepoint CASB from an IP address that is within the organizational IP ranges defined on the IP Ranges settings page. For more information, see "[Configuring IP ranges](#)" on page 233.

- **The following IP ranges:** Administrators can only log in to Forcepoint CASB from an IP address that is within the IP ranges defined in this list. Each IP range must be on a separate line in the list and be in standard CIDR format (i.e., x.x.x.x/y).

4. Click **Save** at the bottom of the page.

## Configuring administrator single sign-on

You can configure single sign-on, so that Forcepoint CASB Administrators are authenticated by the organizational Identity Provider (IdP) and automatically logged into Forcepoint CASB.

The administrators still need to be defined as such in Forcepoint CASB. Administrators' ability to bypass the IdP, logging in directly to Forcepoint CASB, is defined in their [permissions](#).

At least one administrator must be able to bypass the IdP.

To configure single sign-on:

1. In Forcepoint CASB, go to **Settings > Access Management > Single Sign On**:

2. Select **Enable Single-Sign On**.
3. In your organizational IdP, add an application for Forcepoint CASB.  
If Forcepoint CASB does not appear in the IdP's catalog, create a custom SAML 2.0 application with the details provided in Forcepoint CASB by **1**.
4. Get the IdP's SAML 2.0 parameters and enter them in Forcepoint CASB by **2**.

If the IdP does not provide them explicitly, you can extract them from XML.

5. Click **Save SSO Settings**.

If you experience problems with the integration, click **provide the SAML response XML** to check for misconfigurations.

# Configuring account privacy

---

Forcepoint allows administrators to configure the personal data collected through Forcepoint CASB to be compliant with government privacy regulations. For any user account available in Forcepoint CASB, administrators can:

- ▶ **Stop account monitoring:** When an account becomes unmonitored, Forcepoint CASB stops collecting and storing personal data, such as Active Directory data, activities and accounts attached to the account. The data already collected is still stored.

For more information, see ["Stopping account monitoring" below](#).

- ▶ **Delete the account:** When an unmonitored account is deleted, Forcepoint CASB removes the account from storage. The data already collected is permanently deleted.

For more information, see ["Deleting an account" on page 210](#).

- ▶ **Restart account monitoring:** If an unmonitored or deleted account needs to be monitored again, Forcepoint CASB can restart monitoring on the account. Forcepoint CASB starts collecting and storing personal data again.


For more information, see ["Restarting account monitoring" on page 212](#).

## Stopping account monitoring

You can stop monitoring a user account in Forcepoint CASB. When you stop monitoring the account, Forcepoint CASB:

- ▶ Stops importing account data from Active Directory.
- ▶ Stops attaching activities and incidents to the account.

---

 **Note:** Stop monitoring affects all assets attached to the account. You cannot stop monitoring on specific assets.

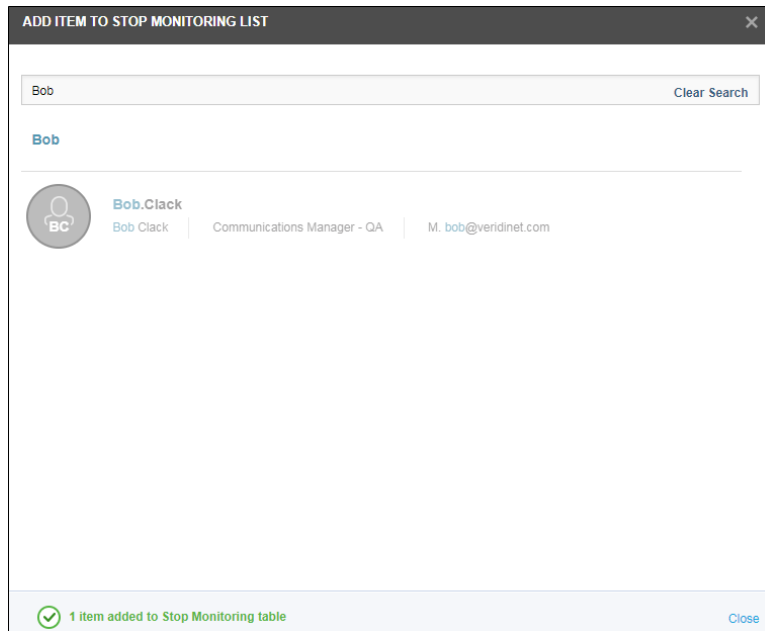
---

- ▶ Stops displaying account data in new Users and Configuration Governance and App Discovery reports.

Data classification file analytics is not stopped for unmonitored accounts. Forcepoint CASB continues to scan and display the data classification files of unmonitored accounts.

1. In Forcepoint CASB, go to **Settings > Account Management > Accounts Privacy**.
2. Under **Configure Account Monitoring**, click **Add to list**.
3. In the pop-up window, type keywords to search for the account. As you type, the search

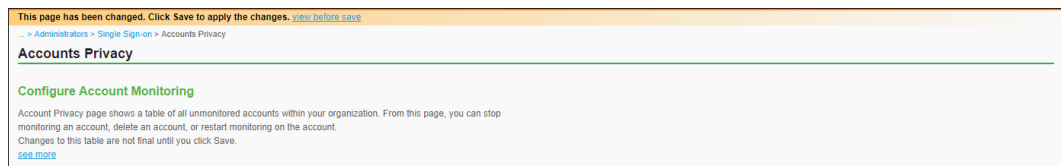
results automatically populate the table under the search field.



4. Select the account (or accounts) and click **Done**.


You return to the **Accounts Privacy** page. The accounts are listed in the Configure Account Monitoring table.

5. The **Accounts Privacy** page displays a message at the top of the window stating that changes have been made. To view a list of all changes that have not been saved, click **view before save**. This list includes all changes waiting to be saved: accounts to be unmonitored, accounts to be deleted, and accounts to be returned to monitoring.



6. Click **Save** to save all pending changes.

---

 **Note:** If you have other pending changes, such as deleting or restarting accounts, those processes also start.

---

7. If you are sure that you want to stop monitoring the account, continue through the pop-up



confirmation messages.

The accounts are added to the Configure Account Monitoring table.

To restart account monitoring, see ["Restarting account monitoring" on page 212](#).

## Deleting an account

---

**⚠ Warning:** Deleting an account **permanently removes** all data for this account. Only delete an account if you are sure that the account data will not be needed in the future. After an account's data is deleted, it can not be returned.

Forcepoint recommends that you export and save any important account data before deleting the account.

---

If you have stopped monitoring an account, you can also choose to delete the account from Forcepoint CASB. When you choose to delete an account, Forcepoint CASB deletes the following data from all assets attached to the account:

- ▶ Active Directory data
- ▶ Activities and incidents
- ▶ Endpoints

In addition, the account's data will be anonymized in App Discovery reports.

Data classification file analytics is not stopped for unmonitored or deleted accounts. Forcepoint CASB continues to scan and display the data classification files of unmonitored accounts.

---

**✎ Note:** You can delete an account only after you stop monitoring the account. For more information about how to stop monitoring an account, see ["Stopping account monitoring" on page 208](#).

---

To delete an account, first make sure that you have stopped monitoring the account. The account must be in the Configure Account Monitoring list to be deleted.

1. In Forcepoint CASB, go to **Settings > Account Management > Accounts Privacy**.
2. Under **Configure Account Monitoring**, select the account you want to delete by checking the box to the left of the User Name.

You can select more than one account. To select all accounts, click **Select All**.


3. Either click the **Delete Account** button located above the accounts table, or click the account's delete button at the far right of the row.

The account is now marked for deletion. The delete button is replaced with a message: **Pending deletion.**




If you want to cancel the deletion request, click **Undo**.

- The **Accounts Privacy** page displays a message at the top of the window stating that changes have been made. To view a list of all changes that have not been saved, click **view before save**. This list includes all changes waiting to be saved: accounts to be unmonitored, accounts to be deleted, and accounts to be returned to monitoring.
- Click **Save** to save all pending changes and start the deletion process.

 **Note:** If you have other pending changes, such as stopping or restarting accounts, those processes also start.

- If you are sure that you want to delete the account, continue through the pop-up confirmation messages.

 **Warning:** Deleting an account **permanently removes** all data for this account. Only delete an account if you are sure that the account data will not be needed in the future. After an account's data is deleted, it can not be returned.

Forcepoint recommends that you export and save any important account data before deleting the account.

- Deleting an account may take up to several days to completely remove all account data. Some data storage is on a 30 day rotation schedule to remove data; therefore, an account is only considered deleted after 30 days have passed from the initial deletion request.



After the account is deleted, the account remains in the table of unmonitored accounts. The account row no longer displays the delete button, but displays the message **Account was deleted** instead.




The account can be returned to monitoring, but only new data is collected. To restart account monitoring, see ["Restarting account monitoring" on the next page](#).

# Restarting account monitoring

Forcepoint CASB allows administrators to restart account monitoring for any unmonitored or deleted account. When you restart monitoring the account, Forcepoint CASB:

- ▶ Imports account data from Active Directory.
- ▶ Attaches activities and incidents to the account.

---

 **Note:** Restarting monitoring affects all assets attached to the account. You cannot restart monitoring on specific assets.

---

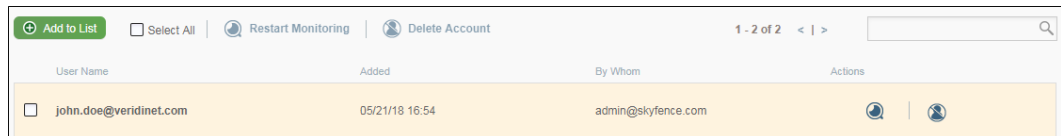
- ▶ Displays account data in new Users and Configuration Governance and App Discovery reports.



To restart account monitoring:

1. In Forcepoint CASB, go to **Settings > Account Management > Accounts Privacy**.
2. Under **Configure Account Monitoring**, select the account you want to restart by checking the box to the left of the User Name.

You can select more than one account. To select all accounts, click **Select All**.


3. Either click the **Restart Monitoring** button located above the accounts table, or click the account's Restart Monitoring button at the far right of the row.



User Name	Added	By Whom	Actions
<input type="checkbox"/> john.doe@veridinet.com	05/21/18 16:54	admin@skyfence.com	 

4. The **Accounts Privacy** page displays a message at the top of the window stating that changes have been made. To view a list of all changes that have not been saved, click **view before save**. This list includes all changes waiting to be saved: accounts to be unmonitored, accounts to be deleted, and accounts to be returned to monitoring.
5. Click **Save** to save all pending changes and restart the monitoring process.

---

 **Note:** If you have other pending changes, such as stopping or deleting accounts, those processes also start.

---

6. Continue through the pop-up confirmation messages.

After the account monitoring restarts, the account is removed from the Configure Account Monitoring list.

# Managing your key management services


---

For managed assets, the Encryption Broker service leverages a bring your own key (BYOK) capability offered by the cloud services. Forcepoint CASB connects to your organization's existing key management service (KMS) to access your encryption keys. Then, Forcepoint CASB connects to the cloud service, where the data at rest is encrypted and decrypted based on the key provided by Forcepoint CASB from the KMS.

Connecting Forcepoint CASB to your KMS requires the following steps:

- ▶ Connect Forcepoint CASB to your existing KMS instances through an API connection. See ["Adding a new key management service" below](#) for more information.
- ▶ Generate a new key on each KMS instance. See ["Generating a new key" on page 215](#) for more information.

---

 **Note:** Currently, Forcepoint CASB only supports Office 365 OneDrive and SharePoint Online with the Azure Key Vault KMS.

---

## Adding a new key management service

To set up the Encryption Broker service, you must connect Forcepoint CASB to your existing KMS through an API connection. After the connection is established, Forcepoint CASB can manage and generate keys from your KMS and provide them to the cloud services through an API connection.

Currently, Forcepoint CASB only supports Office 365 OneDrive and SharePoint Online with the Azure Key Vault KMS. To set up an Azure Key Vault KMS, see ["Adding a new Office 365 key management service" below](#).

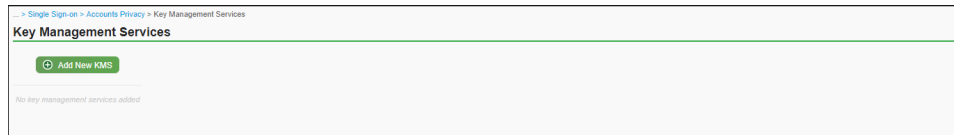
## Adding a new Office 365 key management service

Microsoft Office 365 allows bring your own key (BYOK), but requires that the key be stored in an Azure Key Vault. Office 365 then pulls the key directly from that Azure Key Vault. Also, Office 365 BYOK requires that customers provide two different keys from two different Azure Key Vaults for redundancy.

Through the Encryption Broker service, Forcepoint CASB generates and manages the two different keys in your Azure Key Vaults and sets BYOK in Office 365 OneDrive and SharePoint with the directions to the keys.


To add a new Azure Key Vault KMS:

1. In Forcepoint CASB, go to **Settings > Resources > Key Management Services** and click **Add New KMS**.



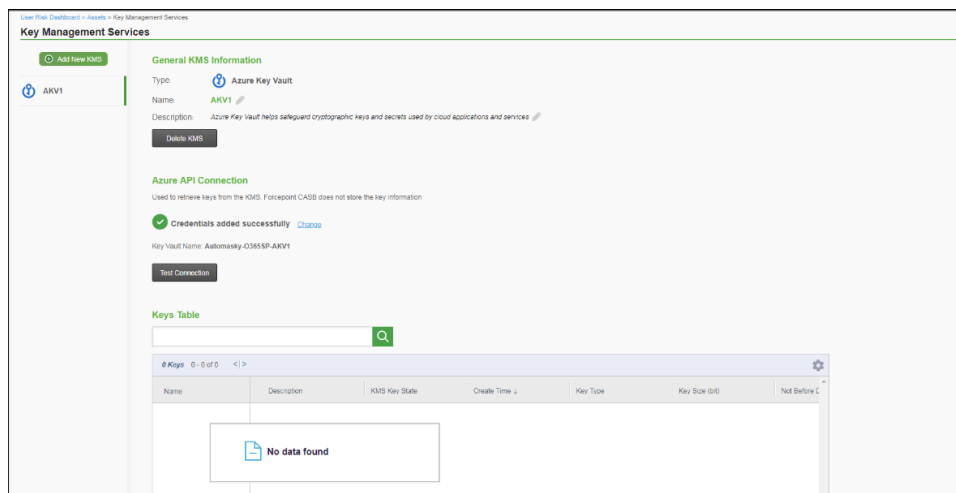
2. On the **Create KMS** pop-up window, make sure **Azure Key Vault** is selected, then click **Next**.
3. Type a **KMS Name** and **KMS Description**, then click **Next**.
4. Click **Set Connection** to establish the API connection with your Microsoft Azure instance.
5. From the **Key Vault** drop-down menu, select the Azure Key Vault where you want to store and retrieve this key. Forcepoint CASB automatically tests the connection to the Azure Key Vault and displays a message letting you know if the connection failed or succeeded.

To select a different Azure instance, click **Change**.

 **Note:** You can only manage an Azure Key Vault once. Managed Azure Key Vaults are removed from the **Key Vault** drop-down menu after setting the API connection to that vault.

6. Click **Add**.

After the new KMS is added, you can view and edit the KMS information from the **Key Management Services** settings page.



## Generating a new key

After you have set up a new KMS in Forcepoint CASB, you can generate new keys through the management portal. These keys are attached to the data encryption policy and are used by the cloud service to encrypt your data at rest.

Only the keys generated through Forcepoint CASB are displayed on the Key Management Services settings page (**Settings > Resources > Key Management Services**). When you access the Key Management Services settings page for the first time, the Keys Table is empty because you have not generated any keys through Forcepoint CASB.

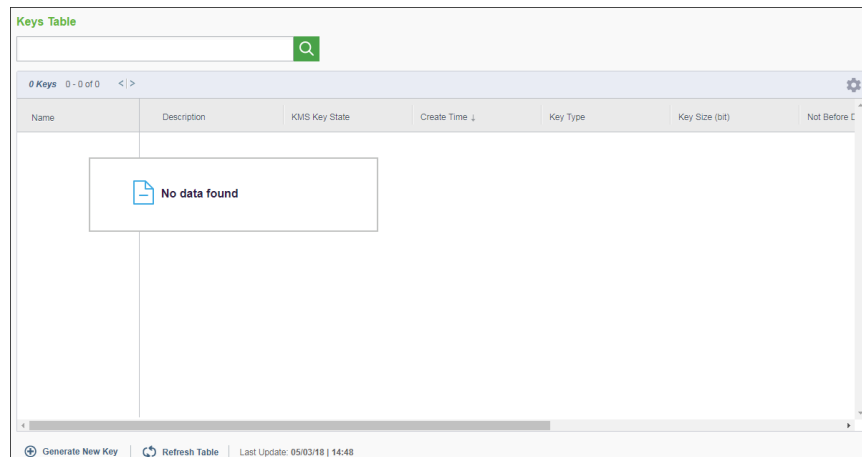
**Note:** Forcepoint CASB does not store the keys within the management portal. The KMS generates and stores all keys. When you generate a key through the management portal, Forcepoint CASB directs the KMS to generate the key through the API connection.

Currently, Forcepoint CASB only supports Office 365 OneDrive and SharePoint Online with the Azure Key Vault KMS. For more information about generating keys for Office 365 assets, see ["Generating a new Office 365 key" below](#).

## Generating a new Office 365 key

To generate a new Office 365 key from the Forcepoint CASB management portal:

1. In Forcepoint CASB, go to **Settings > Resources > Key Management Services** and select your KMS from the list.
2. Under the **Keys Table**, click **Generate New Key**.



3. On the **Generate New Key** pop-up window:

- a. Type a **Key name** and **Key Description**.

The new key's name must be unique. You cannot generate a new key that shares a name with an existing key (either within the Key Table here, or within the KMS itself, even if it is disabled or pending deletion).

- b. From the **Key Type** drop-down menu, select the default value: **RSA**.
- c. From the **Key Size (bit)** drop-down menu, select the default value: **2048**.

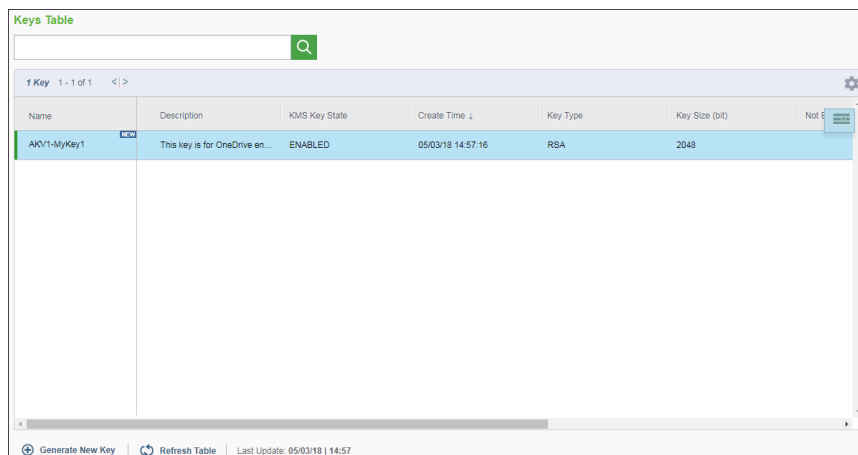
---

**Important:** Office 365 does not support keys with date limitations. If you are creating a key for an Office 365 asset, do not enter values into the **Key Not Before Date** or **Key Expiration Date** fields.

---

4. Click **Generate**.

The new key is now displayed in the Keys Table with a **KMS Key State** of **ENABLED**. Enabled (active) keys can be used in a data encryption policy.



The screenshot shows a table titled "Keys Table" with a search bar and a "1 Key 1 - 1 of 1" indicator. The table has columns for Name, Description, KMS Key State, Create Time, Key Type, Key Size (bit), and Not e. A single row is visible with the following data:

Name	Description	KMS Key State	Create Time	Key Type	Key Size (bit)	Not e
AKV1-MyKey1	This key is for OneDrive en...	ENABLED	05/03/18 14:57:16	RSA	2048	

At the bottom of the table, there are buttons for "Generate New Key", "Refresh Table", and "Last Update: 05/03/18 | 14:57".

When you create a data encryption policy for an Office 365 asset, you need to create two new keys for the data encryption policy. Office 365 encryption requires two keys: one key from a primary Azure Key Vault and one key from a secondary Azure Key Vault.

After you create your Office 365 keys, see ["Configuring the data encryption policy" on page 172](#) for more information about creating the data encryption policy.

## Deleting a key

If you have generated a key from Forcepoint CASB and this key is no longer used, you can delete the key from the Keys Table. When a key is deleted, Forcepoint CASB stops managing the key, and the key is no longer available through the Encryption Broker service.

---

**!** **Important:** When you delete a key in Forcepoint CASB, the key is only deleted from the Keys Table in Forcepoint CASB. The key is not deleted from your Azure Key Vault.

---

1. In Forcepoint CASB, go to **Settings > Resources > Key Management Services** and select your KMS from the list.
2. In the **Keys Table**, select the key you want to delete.
3. Click the delete button that appears on the right side of the key's row.
4. Confirm that you want to delete the key.
5. Click **Save**.

## Deleting a key management service

If a KMS is no longer in use, you have the option to delete the KMS from Forcepoint CASB.

---

**✎ Note:** You can only delete a KMS if it is not active. If the KMS has a key being used by an active data encryption policy, the **Delete KMS** button is disabled.

---

1. In Forcepoint CASB, go to **Settings > Resources > Key Management Services** and select your KMS from the list.
2. Click **Delete KMS**.
3. Confirm that you want to delete the KMS.

The KMS is removed from the KMS list.



# Managing REST API connections

---

Forcepoint CASB allows access to your organization's information using a simple and secure REST API. By using a REST API connection between Forcepoint CASB and an authorized third-party service within your organization, you can share your CASB data directly with the other service.

For example, if you currently use the Forcepoint DLP product within your organization, you can create a REST API connection to communicate between Forcepoint DLP and Forcepoint CASB. After the connection is established, you can view and analyze your DLP data in Forcepoint DLP using the capabilities available in Forcepoint CASB.

---

**!** **Important:** REST API access is different from API connections to cloud services. REST APIs connect Forcepoint CASB to other enterprise software within your organization so you can share data across the services. Cloud service API connections connect Forcepoint CASB to the cloud services used within your organization so you can monitor and restrict cloud service usage.

---

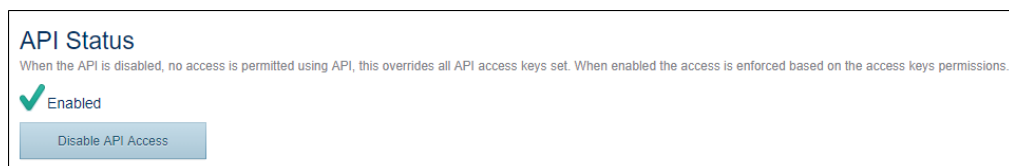
## Enabling API access

To allow your API connections to communicate with other services, you must enable API access. When API access is enabled, Forcepoint CASB allows API access through all enabled connections listed in the API Access Keys section.

To enable API access:

1. In Forcepoint CASB, go to **Settings > Access Management > API**.
2. In the **API Status** section, click **Enable API Access**.

When API access is enabled, the **API Status** section displays the status as **Enabled**.



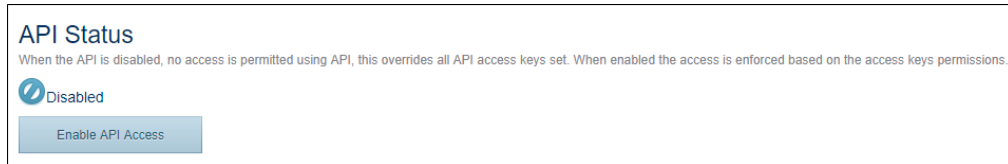
## Disabling API access

If you want to stop all Forcepoint CASB API connections to other services, you must disable API access for all access keys.

To disable API access:

1. In Forcepoint CASB, go to **Settings > Access Management > API**.
2. In the **API Status** section, click **Disable API Access**.

When API access is disabled, the **API Status** section displays the status as **Disabled**.



## Managing API access keys

An API access key is used by a third-party service to access Forcepoint CASB data through the API connection. This key authenticates Forcepoint CASB with the service to provide a secure connection.

Within Forcepoint CASB, you can:

- ▶ **Create a new API access key.** For more information, see "[Create a new API access key](#)" below.
- ▶ **Edit an existing API access key.** For more information, see "[Editing an API access key](#)" on page 221.
- ▶ **Delete an API access key.** For more information, see "[Deleting an API access key](#)" on page 222.

## Create a new API access key

To establish a REST API connection, you must create a new API access key in Forcepoint CASB:

1. In Forcepoint CASB, go to **Settings > Access Management > API**.
2. In the **API Access Keys** section, click **Add API Access Key**.
3. On the **Access key step 1/2** screen, Forcepoint CASB displays two fields:
  - ▶ **Access Key ID:** The ID that is used by other services to connect to the CASB service. Forcepoint CASB automatically generates this ID.
  - ▶ **Access key secret:** The private key used for authentication. Forcepoint CASB automatically generates this secret.

---

**!** **Important:** The key secret is only displayed on this screen. It is no longer available after you save the access key. Save a copy of this secret for reference.

---

4. Click **Next**.
5. On the **Access key properties steps 2/2** screen, add the key details:
  - a. In the **General info** section:
    - i. Add a **Key name**. This name is the primary descriptive name of the key. Forcepoint recommends naming the key after the connection target. For example, if you are using this key to connect to Forcepoint DLP, you might name the key "CASB DLP Connection".
    - ii. The **Access key ID** field cannot be edited. The key displayed here is the same key displayed on the first page.
    - iii. The **Enable key** option is turned on by default when you create the key. If you want to create the key, but enable it later, deselect the **Enable key** option.
  - b. In the **Permissions** section, choose the API capabilities to be used with this key:
    - i. The list of capabilities depends on the purchased licenses. For example, if you purchased a Cloud DLP license, then you will see **Cloud DLP** in the list.
    - ii. Each capability has two options:
      - ▶ **Read:** This permission allows a service to retrieve Forcepoint CASB data through the API connection.
      - ▶ **Write:** This permission allows a service to modify Forcepoint CASB data through the API connection. Due to restrictions with some APIs, this option is not available for every capability.

If you select all available capabilities, the key's entry in the API Access Keys table displays the **Permissions** as **Full**. If you select only some of the available capabilities, the entry displays the key's **Permissions** as **Partial**.

  - c. In the **Client Access** section, choose if the API should be restricted by IP address:
    - ▶ **Allow access from everywhere:** The REST API connection can be accessed from any IP address. Connections are not restricted by IP address when you select this option.
    - ▶ **Allow access from the following IP ranges:** The REST API connection can be accessed only from an IP address that is within the IP ranges defined in this

list. Each IP range must be on a separate line in the list and be in standard CIDR format (i.e., x.x.x.x/y).

If you allow access from all IP addresses, the key's entry in the API Access Keys table displays the **Client Access** as **From Everywhere**. If you allow access from specific IP addresses, the key's entry in the API Access Keys table displays the **Client Access** as **From Specific IPs**.

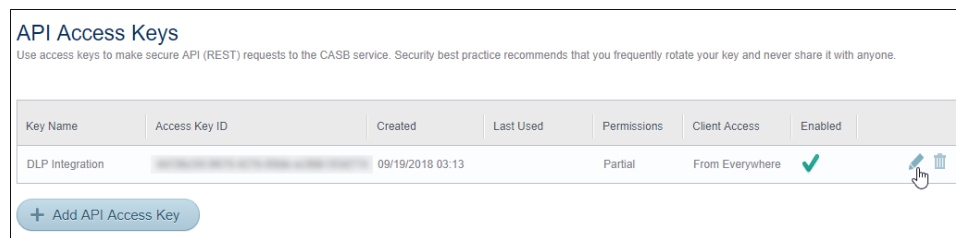
6. Click **Done**.



This new API access key must be shared with the other service before the two services can communicate. Procedures for adding the API access key vary by service. Review the third-party service's documentation for procedures on adding the API access key.

## Editing an API access key

The API access keys table contains all enabled and disabled API access keys created in Forcepoint CASB. If you need to update any key's information, you can do so from the API access key table.

1. In Forcepoint CASB, go to **Settings > Access Management > API**.
2. In the **API Access Keys** section, find the table row of the API access key you want to edit, then click the edit icon at the end of the table row.



Key Name	Access Key ID	Created	Last Used	Permissions	Client Access	Enabled	
DLP Integration	[REDACTED]	09/19/2018 03:13		Partial	From Everywhere	✓	 

[+ Add API Access Key](#)

3. On the **Edit API access key** screen, edit the key details as needed:
  - a. In the **General info** section:
    - i. Edit the **Key name**. This name is the primary descriptive name of the key. Forcepoint recommends naming the key after the connection target. For example, if you are using this key to connect to Forcepoint DLP, you might name the key "CASB DLP Connection".
    - ii. The **Access key ID** field cannot be edited. To change the key:
      - i. Click **Regenerate key**.
      - ii. On the message screen, click **Continue**.

- iii. On the **Regenerate API access key** screen, Forcepoint CASB displays the new **Access Key ID** and **Access key secret**.

---

**!** **Important:** The key secret is only displayed on this screen. It is no longer available after you save the access key. Save a copy of this secret for reference.

---

- iv. Click **Done**. The old access key is revoked and the new access key is enabled.
  - iii. The **Enable key** option is turned on by default when you create the key. If you want to disable the key, deselect the **Enable key** option.
  - b. In the **Permissions** section, edit the API capabilities used with this key:
    - i. The list of capabilities depends on the purchased licenses. For example, if you purchased a Cloud DLP license, then you will see **Cloud DLP** in the list.
    - ii. Each capability has two options:
      - ▶ **Read:** This permission allows a service to retrieve Forcepoint CASB data through the API connection.
      - ▶ **Write:** This permission allows a service to modify Forcepoint CASB data through the API connection. Due to restrictions with some APIs, this option is not available for every capability.
  - c. In the **Client Access** section, choose if the API should be restricted by IP address:
    - ▶ **Allow access from everywhere:** The REST API connection can be accessed from any IP address. Connections are not restricted by IP address when you select this option.
    - ▶ **Allow access from the following IP ranges:** The REST API connection can be accessed only from an IP address that is within the IP ranges defined in this list. Each IP range must be on a separate line in the list and be in standard CIDR format (i.e., x.x.x.x/y).
4. Click **Done**.



## Deleting an API access key

If you no longer need an API access key, you can delete it from the API settings page.

1. In Forcepoint CASB, go to **Settings > Access Management > API**.
2. In the **API Access Keys** section, find the table row of the access key you want to delete, then click the delete icon at the end of the table row.

### API Access Keys

Use access keys to make secure API (REST) requests to the CASB service. Security best practice recommends that you frequently rotate your key and never share it with anyone.

Key Name	Access Key ID	Created	Last Used	Permissions	Client Access	Enabled	
DLP Integration	[REDACTED]	09/19/2018 03:13		Partial	From Everywhere	✓	 

[+ Add API Access Key](#)

3. On the confirmation message screen, click **Yes** to confirm that you want to delete the key. Forcepoint CASB deletes the key and removes it from the API access keys table.

# Endpoint enrollment

The following Forcepoint CASB features require Forcepoint CASB to know which devices are managed by the organization:

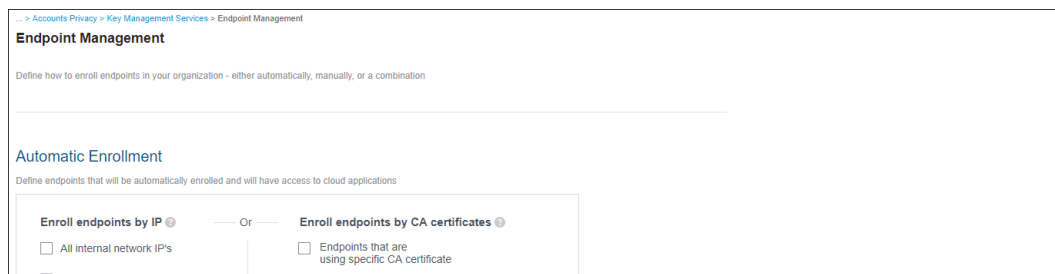
- ▶ The Endpoint Management Access Policy
- ▶ Custom policies based on managed devices
- ▶ An Analytics dashboard filter displays access from managed devices
- ▶ Analytics activity logs display whether source devices are managed or not

Enrolling source devices with Forcepoint CASB enables Forcepoint CASB to know that they are managed by the organization. Managed devices are listed on the **Endpoints** page. You can configure the enrollment criteria that define how Forcepoint CASB determines whether an endpoint is organizationally managed.

After an endpoint is enrolled, it is assigned a unique device ID and is remembered as managed. Certificate-based enrollment can be configured to last only as long as a certificate is present.

## Configuring endpoint enrollment

To configure endpoint enrollment, go to **Settings > Endpoints > Endpoint Management**:



Endpoints are considered organizational if they meet any of the following conditions, as selected:

- ▶ **Automatic Enrollment:** When an endpoint attempts to connect, Forcepoint CASB enrolls the endpoint if it meets any of the selected IP criteria (**Enroll endpoints by IP**) or if it presents an organizational certificate (**Enroll endpoints by CA certificate**). To require IP criteria and a certificate, select **Enforce combined conditions**:

**Automatic Enrollment**  
Define endpoints that will be automatically enrolled and will have access to cloud applications

**Enroll endpoints by IP** Or  **Enroll endpoints by CA certificates**

All internal network IP's  
 Specific IP's

Endpoints that are using specific CA certificate

Enrollment by client certificate is permanent

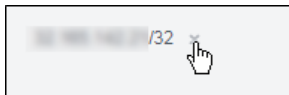
**Enforce combined conditions**  
 Endpoints will be enrolled only if they have both conditions (at least one of the IP types and the certificate)

Summary: Enroll only endpoints that

Save Automatic Enrollment

- **All internal network IPs:** Endpoints are considered organizational if they have IP addresses in IP ranges allocated to internal networks.
- **Specific IPs:** Endpoints are considered organizational if they have IP addresses in any of the IP networks listed here.

To add an IP network, type a network address in CIDR format and click **Add**. To remove a network, hover over it and click the **x**:



- **Enroll endpoints by CA certificates:** An endpoint is considered organizational if it presents a certificate digitally signed by the organizational CA.

Click **Browse** and upload all certificates in the client certificate's certification chain, as PFX files in Base 64 (not binary) format. Select whether **Enrollment by client certificate is permanent** or only as long as the endpoint still has the certificate.

For endpoints to enroll according to this option, distribute the certificate to relevant endpoints.

For certificate-based enrollment, it is highly recommended that endpoints have the Forcepoint CASB [routing solutions](#) and that the enrollment here be set to be



permanent. Otherwise, non-browser applications will not enroll the device at all, and browser enrollment will not be persistent.

After making changes, click **Save Automatic Enrollment**.

- ▶ **Manual Enrollment:** Upon attempting to connect from a non-enrolled endpoint, users will be directed to the [configured form](#), where they can request to enroll the device, upon which Forcepoint CASB will send them an enrollment code via SMS or email, as you select here and according to [notification configuration](#). The user should then submit the code in the second part of the form to finalize enrollment.

The screenshot shows the 'Manual Enrollment' configuration page. At the top, it says 'Manual Enrollment' and 'Enable users to manually register their endpoints for use with cloud applications'. There is a checked checkbox for 'Enable manual enrollment'. Below that is a text input field for 'Enrollment Page' containing 'enrollment\_verify.html' and a 'Browse' button. There are links for 'Download file' and 'Restore default'. The 'Enrollment URLs' field contains 'https://enroll.extremeguitars.net'. There are three checkboxes: 'Require administrator approval' (unchecked), 'Send enrollment code by email' (checked), and 'Send enrollment code by SMS' (checked). Below these is a text input field for 'Allow up to' with the value '10' and the text 'notifications in 24 hours'. At the bottom is a 'Save Manual Enrollment' button.

You can select to **Require administrator approval**, in which case upon verifying the submitted code Forcepoint CASB will list the device for [approval](#), and only upon approval consider the device to be managed.

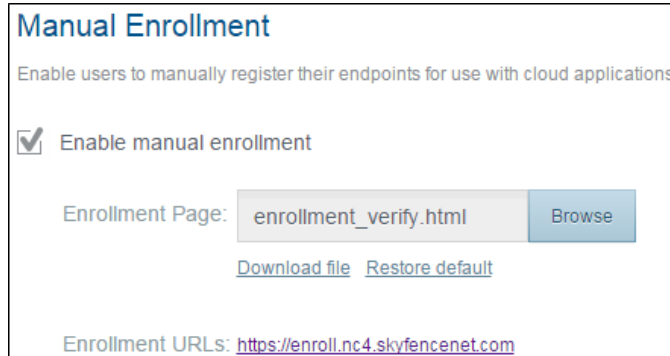
You can limit the number of **notifications in 24 hours**.

After making changes, click **Save Manual Enrollment**.

## Customizing the enrollment form and URL

To customize the enrollment form, go to **Settings > Endpoints > Endpoint Management**, and under **Manual Enrollment**, **Download** the form file and customize it. You can add a company

logo and change the CSS style elements. When you're done, click **Browse** and upload the customized file.



**Manual Enrollment**  
Enable users to manually register their endpoints for use with cloud applications

Enable manual enrollment

Enrollment Page:

[Download file](#) [Restore default](#)

Enrollment URLs: <https://enroll.nc4.skyfencenet.com>

If necessary, you can **Restore** the **default** file.

If Forcepoint CASB is hosted inside the organization, you can also customize the form's URL.

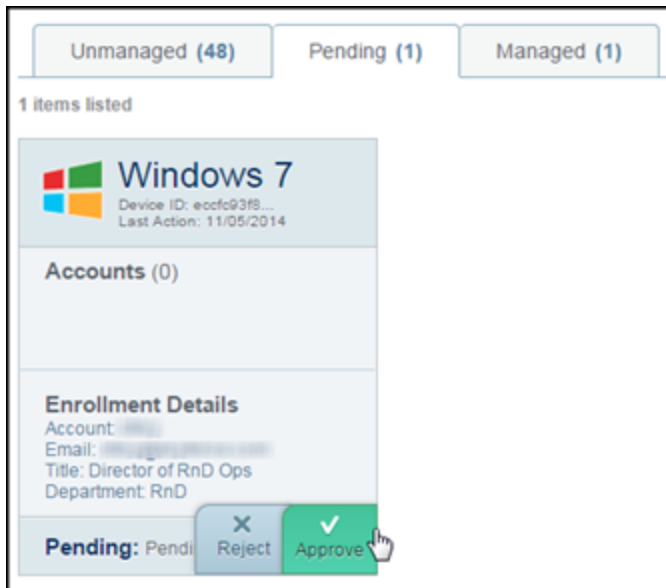
## Administrative enrollment, approval and revocation

If manual enrollment is [configured](#), an administrator needs to approve enrollment requests.

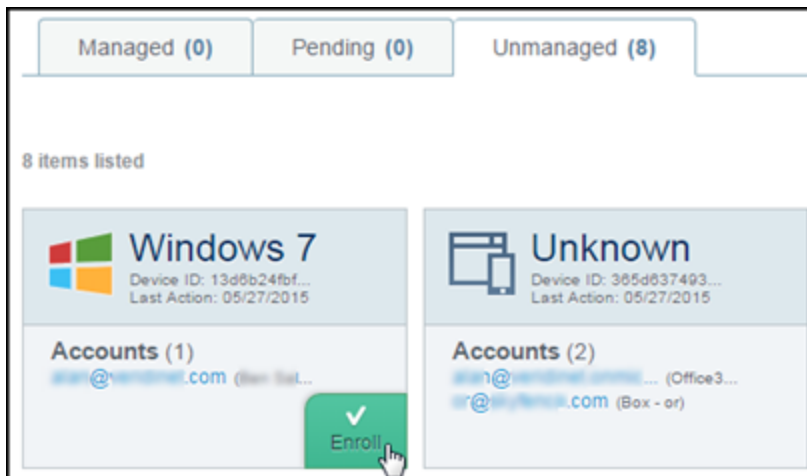
You can approve and revoke individual endpoints, or perform bulk enrollment.

### Individual enrollment approval and revocation

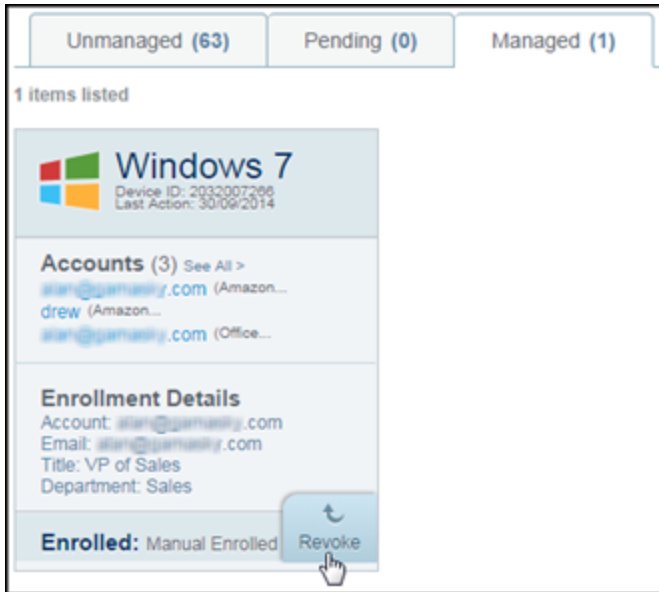
To approve an enrollment request, go to **Endpoints > Pending**, hover over the endpoint and click **Approve**:



To enroll an endpoint unrequested, in **Endpoints > Unmanaged**, hover over the endpoint and click **Enroll**:



To subsequently revoke enrollment, in the **Managed** tab, hover over the endpoint and click **Revoke**:



## Bulk enrollment

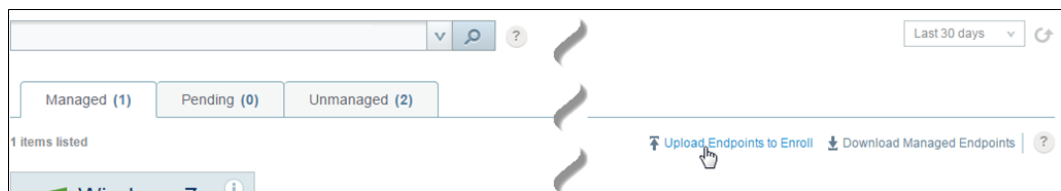
Instead of individually approving endpoints, you can provide a list of endpoints to be added to the list of managed endpoints.

To perform bulk enrollment:

1. From the **Endpoints > Pending** tab or the **Endpoints > Unmanaged** tab, **Download** a list of endpoint candidates for such approval:



2. Make changes to the downloaded list as needed.
3. In the **Managed** tab, **Upload** the changed list to effectively enroll its endpoint:



Downloaded endpoint lists are CSV text files, where each row (except for the header row) represents an endpoint and includes the following comma-separated values:

- ▶ **Device ID:** Unique identifier generated by Forcepoint CASB for the endpoint; upon upload, Forcepoint CASB identifies the endpoint by this ID.
- ▶ **Last Action:** Date and time of the endpoint's last activity observed by Forcepoint CASB.
- ▶ **Operating system:** Endpoint's operating system and version.
- ▶ **Accounts:** Comma-separated list of the user accounts using this device.

For example:

<b>Device ID</b>	<b>Last Action</b>	<b>Operating system</b>	<b>Accounts</b>
6d43d06a4cb3755	4/16/2014	mac os x 10	john@example.com(office365),
6080a656c8bbab	3/22/2014	mac os x 10	alan@example.com(office365),alan- b@myexample.com(salesforce)

Upon upload, Forcepoint CASB uses only the Device ID, so for upload only the first column is required. Further columns are disregarded.

# Configuring internal domains

During data classification, Forcepoint CASB checks the file sharing permissions to determine if the file is shared with users within the organization (internal users) or outside of the organization (external users). This information can help organizations mitigate file sharing issues by removing sharing permissions with external users.

Forcepoint CASB considers a user as internal if:

- ▶ The user connects from the customer domain in the cloud service. The customer domain is the domain registered with your customer account.
- ▶ The user connects from a domain listed in the internal domains list. Organizations with more than one customer domain can manage their domains through the internal domains list. To add or remove an internal domain, follow the procedures below.

If a user connects from a domain that does not match the criteria above, they are considered external users.

To add an internal domain:

1. In Forcepoint CASB, go to **Settings > Organizational Network > Domains**:

User Risk Dashboard > Assets > Domains

### Domains

#### Internal domains

Please specify the domains owned by your organization (example format: mycompany.com). All users detected by Forcepoint CASB from the Internal domains are classified as Internal Users. All users outside of these domains are classified as External Users. This classification is used during Data Classification to determine if files are shared internally or externally and can be used to restrict file access to external users.

Enter line-separated domains list

Save

---

#### Blocked domains

Please specify the domains that users should not access (example format: restrictedcloudservice.com). This list is used by the Endpoint Agent to restrict access to unauthorized domains.

- support.photobucket.com
- press.spotify.com
- e1.boxcdn.net
- community.igniterealtime.org
- download.spotify.com

Save

2. In the **Internal domains** section, type your organization's internal domain address(es). Each domain address must be on a separate line.
3. Click **Save**.

To remove an internal domain:

1. In Forcepoint CASB, go to **Settings > Organizational Network > Domains**.
2. In the **Internal domains** section, select the domain address(es) and press **Delete**.
3. Click **Save**.

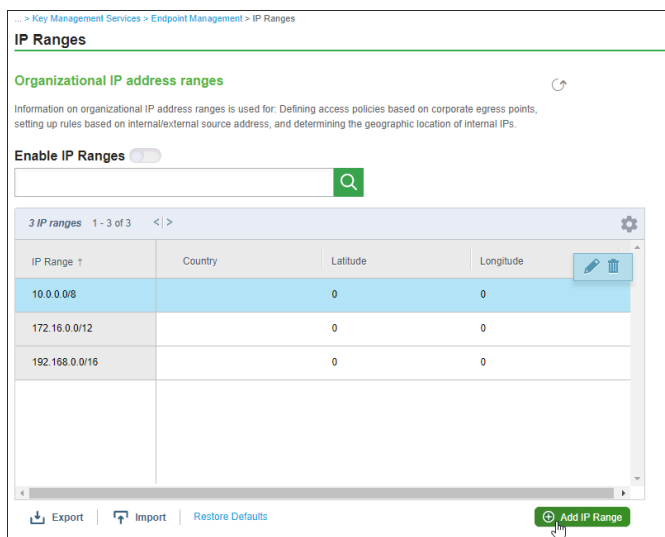
# Configuring IP ranges

Providing Forcepoint CASB with information about organizational IP address ranges enables the following Forcepoint CASB features:

- ▶ The **Internal Networks** [Access Policy](#).
- ▶ **Custom** [policies](#) based on internal/external source IP addresses.
- ▶ Security dashboard [Origin maps](#) mark internal sources.
- ▶ **Client Location** column in [Activity logs](#).

To configure internal IP addresses:

1. In Forcepoint CASB, go to **Settings > Organizational Network > IP Ranges**.
2. For each IP address range:
  - a. Click **Add IP Range**:




- b. Type the range network address in CIDR format:



- c. For representation on maps, provide the geographical location of the represented network: **Country** and coordinates.


---

 **Note:** Latitude and Longitude are not required. If you select a **Country**, but leave the **Latitude** and **Longitude** fields empty, Forcepoint CASB automatically populates the fields based on the selected country.

---

- d. Click **Save**.


To edit an IP range entry, select the IP range row in the table and click the  button.

To remove the IP range entry, select the IP range row in the table and click the  button.

## Importing IP ranges

If you need to add a list of IP ranges at one time, Forcepoint CASB allows you to import a CSV file that contains all of your IP ranges.

---

 **Warning:** Importing a new list completely overwrites the existing list of IP ranges. Ensure that all IP ranges are included in the new list, even IP ranges that are already in the existing list. Any IP ranges from the existing list that are not included in the new list will be deleted.

---

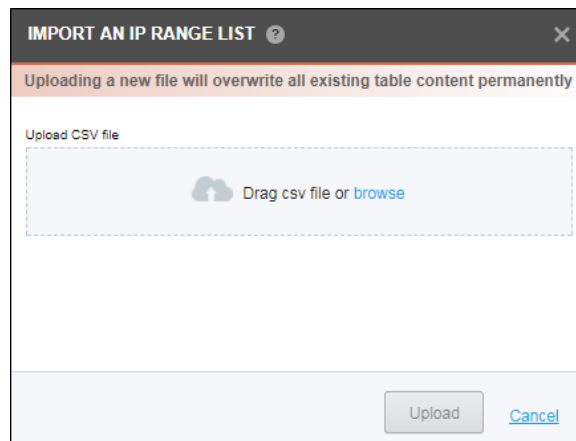
The CSV file must follow the below guidelines:

- ▶ The CSV file must be formatted with UTF-8 file encoding.
- ▶ The file must contain a header line.

- ▶ Each line must contain a single IP range.
- ▶ The columns should be in the following order:
  - IP Range (In CIDR format, e.g., 192.168.0.0/24)
  - Country (Name should match the provided list of countries)
  - Latitude (Decimal number between -90 and 90)
  - Longitude (Decimal number between -180 and 180)
- ▶ IP Range is required.
- ▶ Country, Latitude, and Longitude are optional. If the Country is included, but the Latitude and Longitude coordinates are not, the system sets the coordinates based on the Country.
- ▶ All columns must be included in the file, even if they are not used (e.g., "192.168.0.0/24,,,").

To import the list of IP ranges:

1. In Forcepoint CASB, go to **Settings > Organizational Network > IP Ranges**.
2. Click **Import**.



3. You can either:
  - a. Drag the CSV file from your local machine to the Upload CSV file box.
  - b. Click **browse** to open a Windows Explorer window and navigate to the file.
4. Click **Upload**.

Forcepoint CASB processes the CSV file and adds the IP ranges to the list. All IP ranges from the old list that are not included in the new list are removed.

# Exporting IP ranges

Exporting the IP ranges allows you to view and edit the IP ranges in a CSV file.

The exported CSV file contains four columns:

- ▶ **IP Range** (In CIDR format, e.g., 192.168.0.0/24)
- ▶ **Country** (Name should match the provided list of countries)
- ▶ **Latitude** (Decimal number between -90 and 90)
- ▶ **Longitude** (Decimal number between -180 and 180)

To export the list of IP ranges to a CSV file:

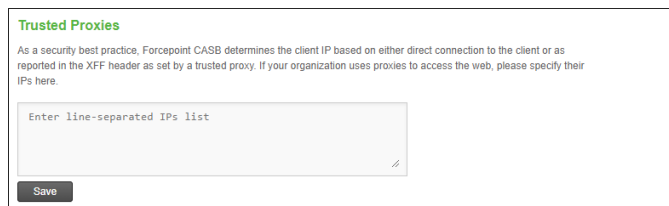
1. In Forcepoint CASB, go to **Settings > Organizational Network > IP Ranges**.
2. Click **Export**.
3. You can either:
  - a. **Export all IPs**: Select this option to export a list of all IP ranges.
  - b. **Export IPs in filter**: Select this option to export the visible, filtered list of IP ranges. You can filter this list by typing your search criteria in the search field above the list of IP ranges.
4. Forcepoint CASB downloads the list of IP ranges to your local machine as a CSV file.

# Configuring trusted proxies

---

As a security best practice, Forcepoint CASB determines the client IP address based on either a direct connection to the client or as reported in the XFF header as set by a trusted proxy. If your organization uses proxies to access the network, add the IP address for each trusted proxy on the **IP Ranges** settings page.

1. In Forcepoint CASB, go to **Settings > Organizational Network > IP Ranges**.
2. In the **Trusted Proxies** section, add the IP addresses for each proxy trusted by your organization. If you have more than one, add each proxy on a separate line.



**Trusted Proxies**

As a security best practice, Forcepoint CASB determines the client IP based on either direct connection to the client or as reported in the XFF header as set by a trusted proxy. If your organization uses proxies to access the web, please specify their IPs here.

Enter line-separated IPs list

Save

3. Click **Save**.

# Configuring trusted IP addresses for IP Reputation

---

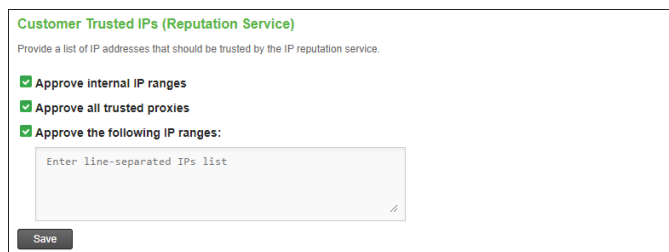
## About IP Reputation

The IP Reputation service in Forcepoint CASB allows administrators to monitor and optionally restrict the access of potentially malicious users from accessing specific IP addresses. Forcepoint maintains lists of suspicious IP addresses and updates the list daily. Every day, the updated lists are processed and distributed to the Forcepoint CASB Gateways. This daily update ensures that each customer Gateway has the most up-to-date list of suspicious IP addresses.

## Configuring trusted IP addresses

If you want to allow access to specific IP addresses, you can configure the trusted IP addresses on the IP ranges settings page. The IP Reputation service will trust these IP addresses.

1. In Forcepoint CASB, go to **Settings > Organizational Network > IP Ranges**.
2. In the **Customer Trusted IPs (Reputation Service)** section, configure the options:
  - ▶ **Approve internal IP ranges:** The IP Reputation service trusts all IP addresses saved in the **Organizational IP address ranges** section on the IP Ranges settings page.
  - ▶ **Approve all trusted proxies:** The IP Reputation service trusts all proxies saved in the **Trusted Proxies** section on the IP Ranges settings page.
  - ▶ **Approve the following IP ranges:** The IP Reputation services trusts all IP addresses entered into this field. Add each IP address on a separate line in the field.



3. Click **Save**.

# Configuring notifications

You can enable Forcepoint CASB to send notifications in the context of various Forcepoint CASB features, each of which requires configuring the relevant notifications.

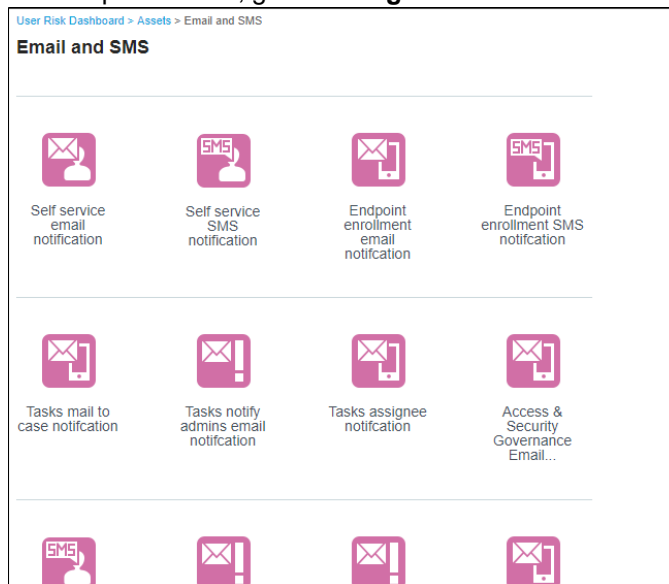
Configurable notification objects are either **Email** or **SMS**, and include relevant configuration and content settings.

Most notification types can each trigger a single designated email notification object and/or a single designated SMS notification object (for example, there is a self-service email notification and a self-service SMS notification). The exception to this is alert notifications, which need to be created and designated per-policy; multiple policies can share notifications, and a policy can trigger multiple notifications. Alert notifications can also include multiple messages to different recipient groups.

## Configuring an SMS notification

To configure an SMS notification:

1. In Forcepoint CASB, go to **Settings > Notifications > Email and SMS**:



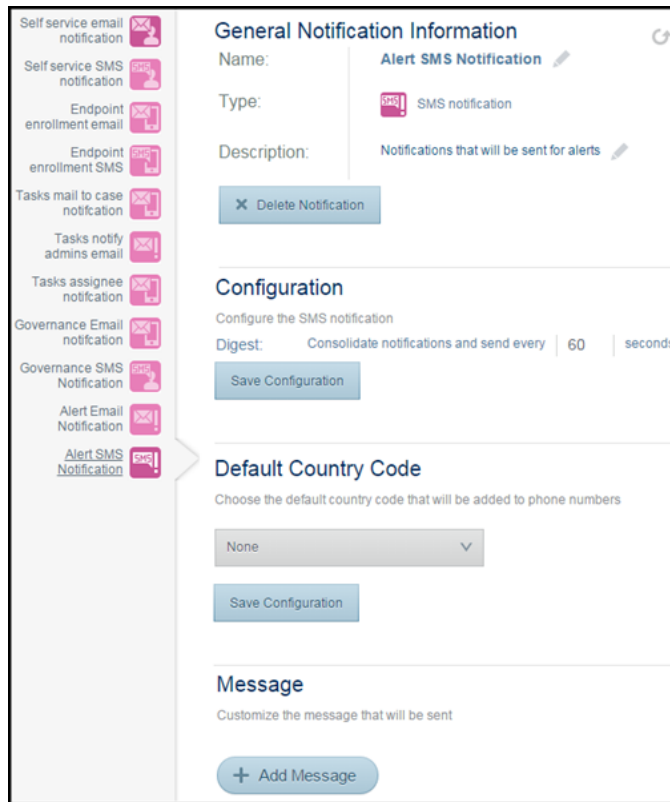
2. Alert notifications need to first be created. To create an alert notification:
  - a. Click **Add Notification**.
  - b. Select **SMS notification**, then click **Next**:



The screenshot shows a dialog box titled "Add Notification" with a close button (X) in the top right corner. Below the title bar, the text "Select Notification Type" is displayed. There are two radio button options: "Email notification" with an envelope icon, and "SMS notification" with an SMS icon and a checkmark. At the bottom right, there are two buttons: "Cancel" and "Next".

- c. Enter a **Notification Name** and **Description**, then click **Finish**:

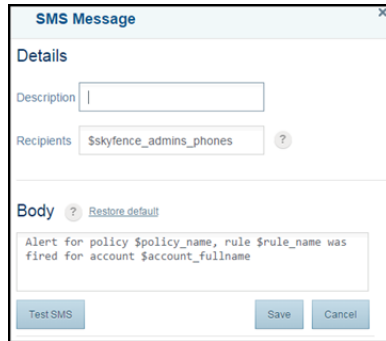
The screenshot shows the same "Add Notification" dialog box, now at the "Set Notification ID" step. Below the title bar, the text "Set Notification ID" is displayed. There are two text input fields: "Notification Name" with the value "Alert Notification" entered, and "Description" with the value "Notifications that will be sent for alerts" entered. At the bottom right, there are two buttons: "Back" and "Finish".


3. Click the relevant notification object to open the notification details:

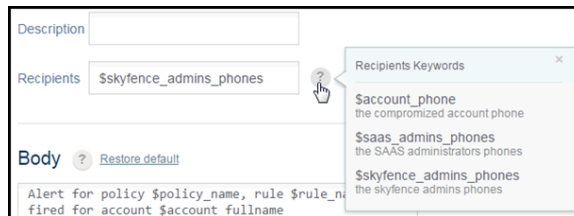


4. By **Name** and **Description**, click  to edit.
5. Under **Configuration** (not available for all notifications), configure the time period in seconds for digest consolidation.
6. Click **Save Configuration**.
7. Under **Default Country Code**, select the default code to be prefixed to phone numbers.
8. Click **Save Configuration**.
9. Under **Message**, click  to edit the default message, or click **Add Message** to add a new message.
10. Edit the message fields:





Click  to view relevant available variables that Forcepoint CASB will resolve and replace. For example:

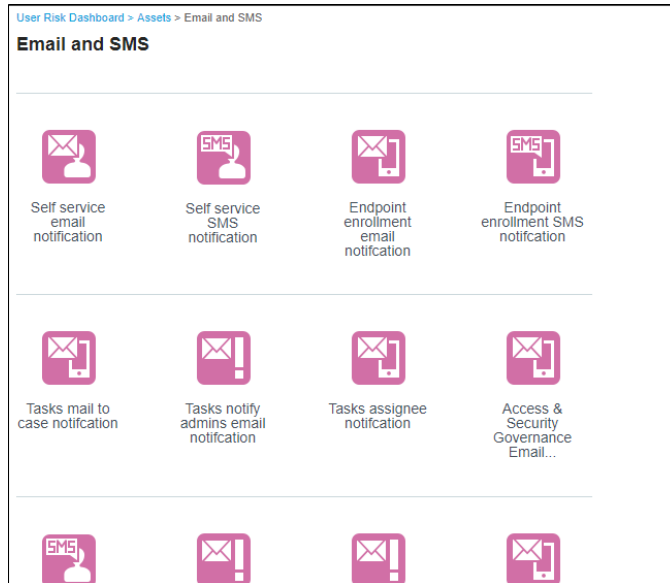


11. Click **Test SMS** to send the message to the assigned recipients.
12. Click **Save**.

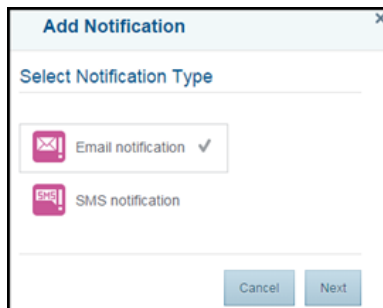
## Configuring an email notification

To configure an email notification:

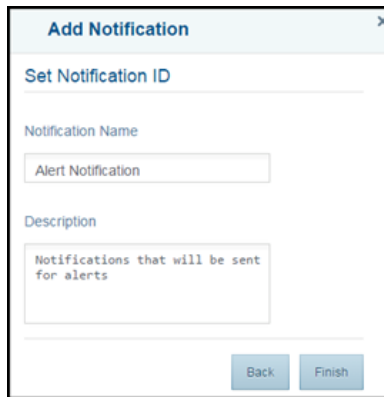
1. In Forcepoint CASB, go to **Settings > Notifications > Email and SMS:**



2. Alert notifications need to first be created. To create an alert notification:
  - a. Click **Add Notification**.
  - b. Select **Email notification**, then click **Next**:



- c. Enter a **Notification Name** and **Description**, then click **Finish**:



The screenshot shows a dialog box titled "Add Notification" with a close button (X) in the top right corner. The dialog contains the following fields and buttons:

- Set Notification ID**: A text input field.
- Notification Name**: A text input field containing the text "Alert Notification".
- Description**: A text area containing the text "Notifications that will be sent for alerts".
- Back** and **Finish**: Two buttons located at the bottom right of the dialog.

3. Click the relevant notification object to open the notification details:

**General Notification Information**

Name: **Alert Email Notification**

Type: **Email notification**

Description: **Notifications that will be sent for alerts**

[Delete Notification](#)

---

**Configuration**

Configure the SMTP server

Server:  User:

Port:  Password:

SSL:  Digest: Consolidate notifications and send every  seconds

[Save Configuration](#)

---

**Message**

Customize the message that will be sent

Alert \$skyfence\_admins\_emails

[Add Message](#)

---

**Logo File**

Choose a logo for the email message (max file size: h:100px w:220px)

Current Logo: default\_logo.png

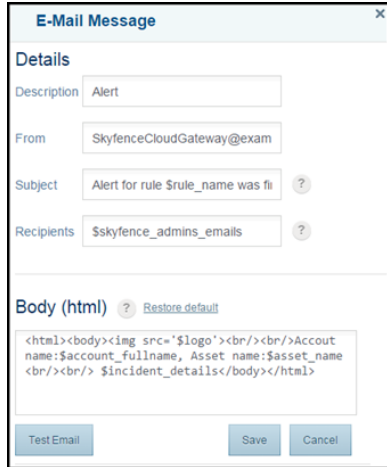
New Logo:  [Browse](#)

[Restore default](#)

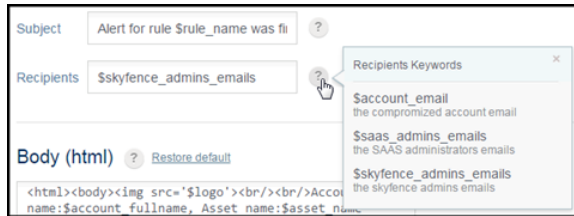
4. By **Name** and **Description**, click to edit.
5. Under **Configuration**, configure:
  - ▶ Connection details and user credentials to the organizational SMTP server
  - ▶ By **Digest**: Time period in seconds for consolidation
6. Click **Save Configuration**.
7. Under **Message**, click to edit the default message, or click **Add Message** to add a new

message.

8. Edit the message fields:



Click  to view relevant [available variables](#) that Forcepoint CASB will resolve and replace. For example:



9. Click **Test SMS** to send the message to the assigned recipients.
10. Click **Save**.
11. Under **Logo File** (not available for all notification types), click **Browse** to upload a graphic file that will replace `<img src='$logo'>` in message content.

## Notification message variables

Available variables differ according to notification type. The following variables are available for the message body, and message subject where indicated, of alert email notifications:

Variable	Description	Also available for message Subject
<code>\$incident_details</code>	Incident details	

Variable	Description	Also available for message Subject
\$incident_date	Incident date	✓
\$severity	Incident severity	✓
\$policy_name	Compromised policy name	✓
\$policy_desc	Compromised policy description	✓
\$rule_name	Compromised policy rule name	✓
\$rule_desc	Compromised policy rule description	✓
\$occurrences	Number of incident occurrences in the period	✓
\$account_fullname	Compromised account full name	✓
\$account_login_name	Compromised account login name	
\$account_title	Compromised account title	
\$account_email	Compromised account email address	
\$account_business_unit	Compromised account business unit	
\$asset_name	Service asset name	
\$service	Specific accessed service. For example: Lync, Outlook Anywhere	
\$client_ip	Endpoint IP address	
\$location	Incident location	
\$endpoint_os	Compromised endpoint OS	
\$endpoint_id	Compromised endpoint ID	

Variable	Description	Also available for message Subject
\$server_ip	Service asset server IP address	
\$authentication_method	Authentication method	
\$client_type	Endpoint type: <b>Mobile</b> or <b>Desktop</b>	
\$logo	Organizational logo	
\$endpoint_type	Mobile endpoint device model. For example: iPhone 5, Nexus 4	
\$user_agent	Endpoint's user agent	
\$external	Whether the endpoint IP address is external to the organization (boolean)	
\$host_name	Endpoint computer name or active sync ID	
\$endpoint_status	<b>Managed / Unmanaged / Pending</b>	

# Configuring data types

---

For [Data Governance](#), Forcepoint CASB inspects about 300 different data formats, and identifies data that matches its configured data types. Forcepoint CASB provides predefined configurations for many common data types, and you can also configure additional data types.

Forcepoint CASB provides predefined configurations for many common data types. You can also configure additional data types and combine data types according to granular logic, including using regular expression patterns, sophisticated Boolean logic including specified occurrences and proximity, and advanced validation algorithms.

You can create hierarchical references to other data types (predefined and custom). For example, to use a single data type for financial routing information in a custom policy, you could combine (with OR) references to the several predefined IBAN data types in a single custom data type.

Currently, custom data types are not used in regular [DLP policies](#). They can be used in [custom policies](#) and for [Data Governance](#).

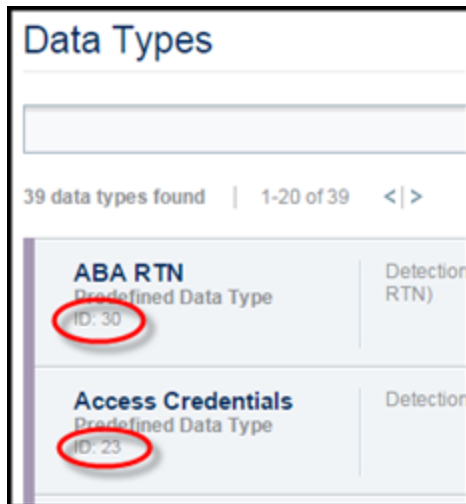
## Data type syntax

Custom data types are XML files in which you can use the following elements:

- ▶ **<data-type>** (required), with string attribute **name**: Single top-level element for the data type. The provided name will appear in Forcepoint CASB, but will be overwritten by the name provided in the management portal, if different, upon [uploading the data type](#).
- ▶ Building-block elements:
  - ▶ **<pattern>**: Each **pattern** element includes a regular expression, defining a string pattern to be located in inspected data. To escape special characters, wrap the regular expression inside a `<![CDATA[ ]>` child element.  
  
The regular expression should be in Google RE2 format. See <https://re2.googlecode.com/hg/doc/syntax.html>  
  
A couple of useful regular expression features are:
    - ▶ For case-insensitive matching, at the beginning of the Pattern content add: **(?i)**
    - ▶ To mark a word boundary (beginning or end): **\b**
  - ▶ **<data-type-ref>**, with string attribute **id**: Refers to an existing data type (predefined or custom) by its ID. To find a Data Type's ID, in Forcepoint CASB, go to **Settings > DLP > Data Types**. You can search, filter (by **Predefined / Custom / Unused**), and



sort the list; the ID appears below the Data Type name:



- ▶ **<and>**, **<or>** - wrapped around multiple child elements; **<not>** - wrapped around a single child element: Boolean logical operators defining the relationship of their child elements.

For example, to match data including both of two patterns, place the two pattern elements inside an **and** element.

- ▶ Additional determining elements:
  - ▶ **<validator>**, with string attribute **type**, wrapped around a single **pattern** element: Matches data matching its child element, if the matching data is validated according to the algorithm of the specified type. Valid types are: **luhn** and **nhs** (Modulus 11).
  - ▶ **<occurrences>**, with string attributes **min** and **isUnique**, wrapped around a single child element: Matches data that includes data matching the child element at least **min** times. If **isUnique="true"**, the occurrences must be different.
  - ▶ **<proximity>**, with string attribute **max**, wrapped around exactly two child elements: Matches data that includes data matching both of its child elements, in the order of the child elements' appearance, with no more than **max** characters from the end of the first to the beginning of the second.

## Data type examples

### Example 1

The following data type matches data that

- ▶ matches an existing data type with ID="42", and
- ▶ includes the word **Visa** or the word **Mastercard** (case sensitive), followed within 10 characters by three numbers structured like VISA credit card numbers and validated according to the Luhn algorithm, and
- ▶ does not include the word **Approved** (case insensitive):

```
<data-type name="ComplexDataType">
  <and>
    <data-type-ref id="42">
      <proximity max="10">
        <or>
          <pattern>Visa</pattern>
          <pattern>Mastercard</pattern>
        </or>
        <occurrences min="3" isUnique="false">
          <validator type="luhn">
            <pattern>
              <![CDATA[4\d{3} \d{4} \d{4} \d{4}]]>
            </pattern>
          </validator>
        </occurrences>
      </proximity>
    <not>
      <pattern>Approved</pattern>
    </not>
  </and>
</data-type>
```

## Example 2

The following data type matches data that includes either "top secret" or "confidential", with word breaks before and after, case-insensitive:

```
<data-type name="Business Confidential Information">
  <or>
```

```
        <pattern>(?!)\bconfidential\b</pattern>
        <pattern>(?!)\bTop Secret\b</pattern>
    </or>
</data-type>
```

### Example 3

The following data type matches data that contains 5 to 10 occurrences of the word "confidential", with word breaks before and after, case-insensitive:

```
<data-type name="5 Confidential">
    <occurrences min="5" max="10" isUnique="true">
        <pattern>(?!)\bconfidential\b</pattern>
    </occurrences>
</data-type>
```

### Example 4

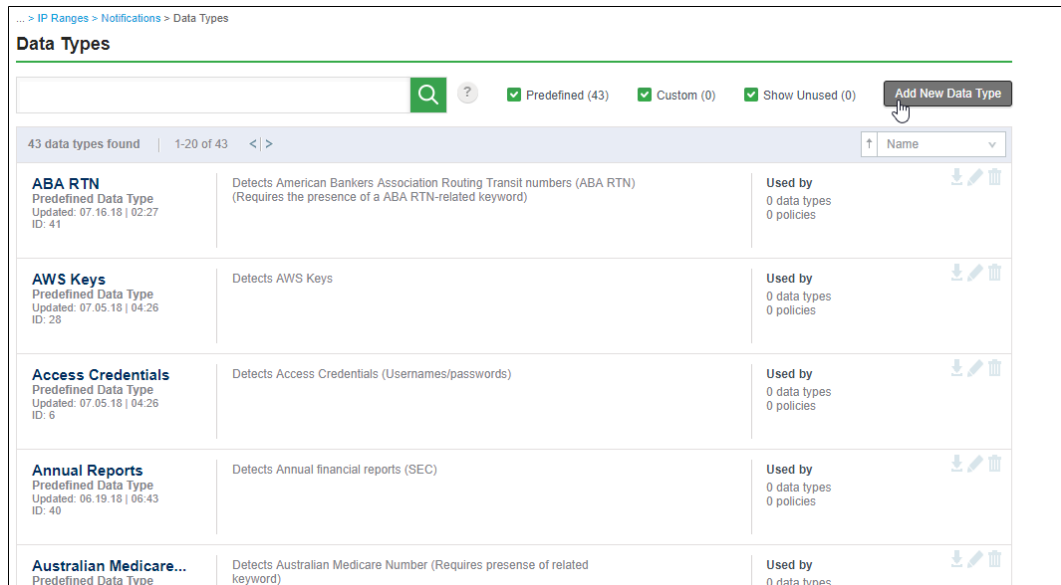
The following data type attempts to identify use of the phonetic alphabet:

```
<data-type name="Dictionary">
    <or>
        <pattern>(?!)\bAlpha</pattern>
        <pattern>(?!)\bBravo</pattern>
        <pattern>(?!)\bCharlie</pattern>
        <pattern>(?!)\bDelta</pattern>
        <pattern>(?!)\bEcho</pattern>
        <pattern>(?!)\bFoxtrot</pattern>
        <pattern>(?!)\bGolf</pattern>
        <pattern>(?!)\bHotel</pattern>
    </or>
</data-type>
```

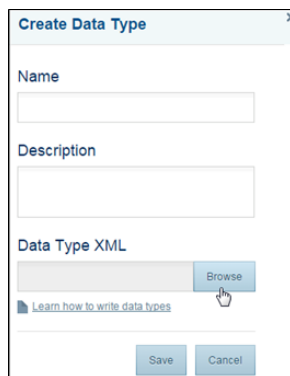
# Adding a custom data type to Forcepoint CASB

After you have [created a custom data type](#), add it to Forcepoint CASB:

1. In Forcepoint CASB, go to **Settings > DLP > Data Types > Add New Data Type**:

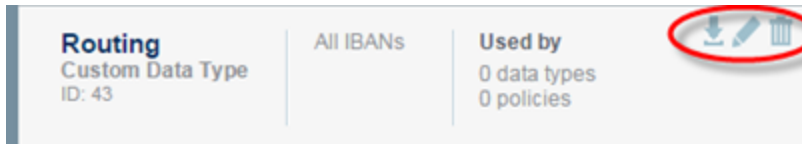


2. Enter a **Name** and **Description**.
3. Click **Browse** to upload the data type XML file:




4. Click **Save**.

After the data type is available in Forcepoint CASB, you can download (↓), edit (✎), or delete (🗑) the data type:



---

 **Note:** Predefined data types cannot be downloaded, edited, or deleted.

---

# Configuring an ICAP connection

---

Forcepoint CASB integrates with Data Leak Prevention (DLP) products to apply content scanning, content classification for inline traffic (e.g., uploaded and downloaded traffic from cloud services) and classification of data at rest in cloud storage services (data governance).

Forcepoint CASB connects to the DLP system through the Internet Content Adaptation Protocol (ICAP), the most common protocol used to integrate DLP products with other services.

Forcepoint CASB offers three ICAP deployment options:

- ▶ **Simple ICAP-based deployment**

The Forcepoint CASB ICAP connector is configured to access the DLP processing unit IP or DNS name. The ICAP protocol is sent in unsecure plain text.

Only one change is required on the processing unit: allow incoming connections over the ICAP port (1344 by default) from the Forcepoint CASB service IPs (provided by Forcepoint).

- ▶ **Secure ICAP-based deployment**

The Forcepoint CASB ICAP connector is configured to access the DLP processing unit IP or DNS name via a secure tunnel. stunnel should be deployed on the processing unit or in the same domain/VPC. The address of stunnel is configured in the Forcepoint CASB ICAP connector.

Only one change is required on the processing unit: allow incoming connections over the secure ICAP port (11344 by default) from the Forcepoint CASB service IPs (provided by Forcepoint).

- ▶ **Secure ICAP-based deployment with load balanced processing units**

The Forcepoint CASB ICAP connector is configured to access the DLP processing unit TCP level load balancer IP or DNS name via secure tunnel. The TCP level load balancer should forward connections coming over port 11344 to the processing units. stunnel should be deployed on all processing units.

All incoming connections should be allowed over port 11344 from the Forcepoint CASB service IPs (provided by Forcepoint).

## Adding a new ICAP connection

Before creating a new secure ICAP connection in Forcepoint CASB, you must deploy stunnel. For more information about deploying stunnel, see the [Setting Up a Secure Tunnel using stunnel](#) section below.

1. In Forcepoint CASB, go to **Settings > DLP > ICAP**.
2. Click the **Add External ICAP Connector** button.
3. On the **Select connector type** screen, select one of the two options, then click **Next**.
  - ▶ **Forcepoint (Formerly Websense)**: This type connects to the Forcepoint DLP product. You must have an existing, configured Forcepoint DLP server to use this connector type.
  - ▶ **Custom DLP**: This type connects to any third-party DLP product.
4. On the **Connector details** screen, type a **Connector Name** and **Connector Description**, then click **Next**.
 

If you selected **Forcepoint** on the previous screen, the name and description are pre-populated on this screen, but editable.
5. On the **Connection type** screen, select one of the two options, then click **Next**.
  - ▶ **ICAP**: This type creates a standard, plain text connection between the DLP system and Forcepoint CASB.
  - ▶ **ICAP via Secure Proxy**: This type creates a secure connection (tunneled via SSL proxy) between the DLP system and Forcepoint CASB. You must have stunnel set up before creating a connection of this type. For more information about deploying stunnel, see the [Setting Up a Secure Tunnel using stunnel](#) section below.
6. On the **Connection details** screen, enter the following information:
  - a. **ICAP Authority and Abs\_Path**: The remote procedure call to the DLP provider. The format is:
 

```
icap://<DLP Hostname>:1344/<mode>
```

 where:
    - ▶ **<DLP Hostname>** is the hostname of the DLP server.
    - ▶ **<mode>** is either `reqmod` or `respmo`.
  - b. **Mode**:
    - ▶ **Req** (Request modification mode)
    - ▶ **Res** (Response modification mode)
  - c. **Secure proxy hostname** (ICAP via Secure Proxy option only): The hostname of the stunnel proxy.
  - d. **Secure proxy port** (ICAP via Secure Proxy option only): The port used for the stunnel proxy. Default port is 11344.
7. Click **Check connection** to verify that Forcepoint CASB can connect to the provided

server. If the connection fails, check the entered information for errors and check the connection again.

8. When the connection is successful, click **Save**.

## Creating a DLP Policy

After the ICAP connector is set, you can add it to a new security policy.

Custom Security Policy:

1. Create a new [custom policy](#).
2. Under **Choose Predicates > What**, select the **ICAP Connector** option.
3. Select the new connector from the **Add ICAP Connector** drop-down menu, then **Save** the predicate.

## Setting up a secure tunnel using stunnel

To allow ICAP use over a secure tunnel, most DLP vendors recommend the usage of stunnel. stunnel should be deployed on the processing unit server or on a server in the same VPC/LAN as the processing units. Forcepoint CASB will open a secure connection with the stunnel service and use it to communicate with the processing units in clear text ICAP.

1. Install stunnel on the processing unit or a nearby computer using the proper installer or by running the following command in a Linux server:

```
yum install stunnel
```

2. Create a configuration file under **/etc/stunnel/stunnel.conf**.

- a. The content of the file should be:

```
fips=no
client=no
cert=<cert path>
key=<key path>
output=/var/log/stunnel.log
[icaps]
accept=10.100.70.7:11344
connect=10.100.70.7:1344
```



- b. Change the `accept` and `connect` IP and port:
      - i. The `accept` line determines the IP and port the stunnel listens on. It should be set to the stunnel server IP and the secure connection port used (typically 11344).
      - ii. The `connect` line determines the IP and port the stunnel opens to the processing unit ICAP server. It should be set to the processing unit's IP and the ICAP port used (typically 1344).
      - iii. Verify that the `accept` port is open.
    - c. Certificate upload:
      - i. Create a valid certificate and upload the `cert` and `key` to the stunnel server.
      - ii. Point the `cert` and `key` paths in the `stunnel.conf` above to the path of these files.
  3. Create the logs file **`/var/log/stunnel.log`**.
  4. Start the stunnel service by running the command:  
`stunnel`
  5. Check for potential errors in **`/var/log/stunnel.log`**.

# Setting up SIEM / syslog integration

---

Forcepoint CASB provides a SIEM tool (in Windows and Linux versions) that allows a scheduled, automatic export of CASB data (e.g., activity, alerts, incidents) to your preferred SIEM solution, such as ArcSight and Splunk. Exporting this data allows you to audit the Forcepoint CASB data or run your own reports and analytics from your SIEM solution.

The SIEM tool can be configured to periodically retrieve logs from Forcepoint CASB, produce activity files, and either push the activities to a syslog server (native to the SIEM system or forwarded to it) or place them where they can be available to the SIEM or syslog system.

This SIEM tool bridges the gap between the cloud-based CASB data and the on-premises SIEM solutions. The SIEM tool is deployed on-premises and opens a secure SSL connection to Forcepoint CASB to retrieve the data. This prevents the need to open an unsecure connection through your firewall to retrieve the data straight from the cloud.


The SIEM tool works with your SIEM solution in the following ways:

- ▶ The SIEM tool exports data to CEF-formatted files that are picked up by the SIEM server file connector. CEF is a standard format used by all SIEM solutions, so using CEF files ensures that every SIEM solution can import the data.
- ▶ The SIEM tool can send data to syslog, acting as a syslog client that can connect to your SIEM solution as its syslog server.

To set up SIEM / syslog integration using the SIEM tool:

1. Download the SIEM tool:
  - a. From the Forcepoint CASB management portal, go to **Settings > Tools and Agents > SIEM Tool**.


---

 **Note:** You must have a valid Forcepoint CASB license to download this tool. This tool will only be visible on the Tools and Agents page if you have a valid license. Contact Forcepoint Support if you would like to use the tool, but do not see the tool on this Settings page.

---

- b. Click **Download** to download a zip file named "SIEM-Tool-[operating system]-[release date].zip" (e.g., SIEM-Tool-Windows-2021-10-19.zip). The zip file contains one of the following files, depending on the version you download:
  - ▶ SIEMClient.bat (if you downloaded the Windows tool)
  - ▶ SIEMClient.sh (if you downloaded the Linux tool)

---

 **Note:** The SIEM tool requires that Java v1.8 or higher be installed before installing the tool.

---

2. For secure connection of the SIEM tool to the Forcepoint CASB service, the tool requires the trust store file that can be downloaded from the Forcepoint CASB management portal. From the management portal, go to **Settings > Tools and Agents > SIEM Tool**, then click **Download Trust Store**.

Place the downloaded trust store file in a location that the SIEM tool can access after it is installed.

3. Extract the provided SIEM tool archive on a host that has Java v1.8 or higher installed and can access the organizational Forcepoint CASB management server.
4. Configure the credentials. This only needs to be done one time.

Open a command prompt, navigate to the location of the **SIEMClient** files, and run the following command:

▶ **Windows:**

```
SIEMClient.bat --set.credentials --username <user> --password <password> --credentials.file <file>
```

▶ **Linux:**

```
SIEMClient.sh --set.credentials --username <user> --password <password> --credentials.file <file>
```

where the above parameters are:

- ▶ **<user>** and **<password>**: Forcepoint CASB administrator credentials. Optionally, if you omit the `--username` and `--password` arguments, you will be prompted to provide them interactively.
- ▶ **<file>**: Path and filename for the credentials store.

5. Run the SIEM tool from the command prompt:

```
<tool> --credentials.file <file> --host <host> --port <port#> --output.dir <dir> [ truststorePath=<trust> ] [ exportSyslog=true syslogHost=<syslogServer> syslogFacility=<facility> ] [ cefVersion=<cef.version> ] [ cefCompliance=<cef.flag> ] [ --proxy.host <proxy.host> ] [ --proxy.port <proxy.port> ]
```

where the above parameters are:

- ▶ **<tool>**:
  - On Windows: **SIEMClient.bat**
  - On Linux: **SIEMClient.sh**
- ▶ **<file>**: Path and filename of the credentials store.
- ▶ **<host>** and **<port#>**: Connection details to the Forcepoint CASB management server. Port is usually **443**.
- ▶ **<dir>**: Directory where the SIEM tool saves the produced activity files. Required even if pushing to syslog.
- ▶ **<trust>**: Path and filename of the trust store file downloaded above.
- ▶ To push produced activity files directly to syslog, include
 

```
[ exportSyslog=true syslogHost=<syslogServer>
  syslogFacility=<facility> ]
```

 where the above parameters are:
  - **<syslogServer>**: Address of the syslog server.
  - **<facility>**: An identifier not otherwise used by the syslog server, usually **local#** where **#** is a number from 1 to 9 (e.g., **local3**).
- ▶ **<cef.version>**: Sets the specific version of CEF.
  - If **cefVersion=1**, the tool uses the legacy CEF format.
  - If **cefVersion=2**, the tool uses the true CEF format.
  - If **cefVersion=3**, the tool uses a newer version of CEF that supports the new activities columns (Target, Message, and Properties).

If the **cefVersion** parameter is included in the command, the tool ignores the **cefCompliance** parameter.

If the **cefVersion** parameter is omitted from the command, the tool uses the **cefCompliance** parameter.
- ▶ **<cef.flag>**: Enables the true CEF format.
  - If **cefCompliance=true**, the tool uses the true CEF format.
  - If **cefCompliance=false**, the tool uses the legacy CEF format.
  - If the parameter is omitted from the command, the value defaults to **false** and the tool uses the legacy CEF format.

- ▶ **<proxy.host>** and **<proxy.port>**: Connection details to the proxy server if connecting to the Forcepoint CASB management server through a proxy server.

6. Complete one of the following activities:

- ▶ If pushing produced activity files directly to syslog: Configure the syslog server to receive the logs with the configured Facility identifier, and if necessary to forward them to the relevant SIEM system.
- ▶ If not pushing to syslog: Configure the SIEM system to retrieve new activity files from:

```
<dir>/activities_alerts_files/<NewFileName>.CEF
```

where **<dir>** is the above configured output directory.

Every time the SIEM tool is activated, it retrieves logs for the time period since the previous retrieval and generates a new activity file for the SIEM /syslog system. The tool determines the last import time by keeping a file with the last imported activity ID. To import all data (not just the data from the last import), delete this old file.

Old activity files are not automatically deleted. You should configure periodic cleaning or removal of each activity file upon retrieving it.

## Activities and alerts CEF mapping

The following table compares the true CEF format fields to the fields used in the Activities and Alerts table exported from the SIEM tool. This true CEF format replaced the legacy CEF format previously used in Forcepoint CASB.

Forcepoint CASB Field	Description	CEF Field
N/A		Vendor
N/A		Product
N/A		Version
Event ID	Activity ID	SignatureID
Action	Action	Name
Severity	6 = Info 7 = Low 8 = Medium 9 = High	Severity

Forcepoint CASB Field	Description	CEF Field
	10 = Critical	
Mitigation Action	Action taken by the Gateway	act
Service Type	Application level protocol (https, http, imap, etc)	app
N/A	"Normal Activity" or "ruleName/PolicyName"	cat
Rules	Empty or "ruleName"	cs1
Asset	Asset name	destinationServiceName
Endpoint ID	Endpoint ID	deviceExternalId
External	If IP is external = "True"	deviceFacility
Data Object	Data object	deviceProcessName
N/A		dhost
Admin	If account is Admin = "Admin" If not = "User"	dpriv
Server IP	Service Provider Server IP	dst
Login name	Username	suid
N/A		dvc
N/A		dvchost
Time	Activity date in Epoch	end
Session ID	Session ID	externalId
File Size	File Size	fsize
Title / Department / Client location / Service location	title / department / sourceCountry / destCountry	msg
Activity Status	Activity Status (failed/success)	outcome
Service Type	Service Type	proto

Forcepoint CASB Field	Description	CEF Field
Action	Action	reason
URL	URL	request
Endpoint type / Endpoint OS / User Agent	Endpoint type / Endpoint OS / User Agent	requestClientApplication
Time	Activity date in Epoch	rt
Managed	If device is Managed = "Managed" If not = "Unmanaged"	sourceServiceName
Source IP	Source IP	src
Time	Activity date in Epoch	start
Full Name	User name and last name	
Data Types	DLP data types	cs2
File type	File type	cs3
Is sensitive data	If data matched any DLP rule = "Yes"	cs5
Data Types details	DLP data type description	cs6
Source IP reputation	IP reputation category name	AD.IPReputationCategory
TOR Networks		AD.TORNetworks
Suspicious IPs		AD.SuspiciousIPs
Anonymous proxies		AD.AnonymousProxies
IP Chain		AD.IPChain
External		AD.IPOrigin
Account		AD.samAccountName
Authentication Type	Authentication type	dproc
Record	General field	flexString1

Forcepoint CASB Field	Description	CEF Field
Account	SAM account name	suser
Follow up Mitigations	API action (quarantine)	flexString2
Amount	General numeric field	cn1
Impact Score	Numeric value between 1 and 100	cn2
Target	General field	duid
Properties	General field	oldFileId
Message	General field	oldFileName
Data object ID	General field	fname
N/A	Target user SAM account name	duser

## Incidents CEF mapping

The following table compares the true CEF format fields to the fields used in the Incidents table exported from the SIEM tool. This true CEF format replaced the legacy CEF format previously used in Forcepoint CASB.

Forcepoint CASB Field	Description	CEF Field
N/A		Vendor
N/A		Product
N/A		Version
Incident ID		SignatureID
Account	The SAM account name.	suser
Incident Description	The incident description.	cs6
Mitigation Action	The mitigation action taken by Forcepoint CASB as a result of the policies breached by the incident.	act
State	Active / Acknowledged / Ignored	cat



Forcepoint CASB Field	Description	CEF Field
Incident Name	The rule name to which the incident relates. If you move the mouse over the Incident Name, Forcepoint CASB displays a tooltip of the rule's description.	cs1
Asset	The asset name assigned with the cloud service.	destinationServiceName
N/A	If account is Admin="Admin" If not="User"	dpriv
Login Name	The account used to access the cloud service.	duser
Last Alert Time	The date and time of the current last alert attached to the incident.	end
Description	The relevant rule's description.	msg
Incident Detection Time	The date and time Forcepoint CASB detected the incident. This is the time Forcepoint CASB processed the data and can be days after the first activities.	rt
Source	The activity audit type (i.e., Real Time or Service-logs).	sourceServiceName
First Alert Time	The date and time of the first alert attached to the incident (i.e., the alert that created the incident).	start
Full Name	The full name of the user. This data is retrieved from the Active Directory if integration is in place; otherwise it is empty.	cs4
Occurrences	The number of alerts attached to the incident.	flexString2

# Downloading Tools and Agents

---

Forcepoint CASB offers multiple companion applications that customers can deploy with Forcepoint CASB. To download these applications:

1. On the Forcepoint CASB management portal, go to **Settings > Tools and Agents**.
2. Locate the application you want to download and click the **Download** link. Each application has different download links for different operating systems.

The following tools and agents are available:

- ▶ **Endpoint Agents:** The Forcepoint CASB Endpoint Agents enable user access to monitored cloud services when applications and thick clients are in use. The Endpoint Agent can be deployed to endpoints using GPO or scripts.

For more information, see ["Deploying the Forcepoint CASB Security Service" on page 305](#).

- ▶ **Active Directory Tool:** The Active Directory Agent is a lightweight service allowing communication between the Forcepoint CASB service and the customer Active Directory. The Active Directory Agent allows data enrichment based on Active Directory data synced to the Forcepoint CASB service. It is mandatory for Identity verification, CASB IDP, and data enrichment.

For more information, see ["Setting up Active Directory Agent retrieval" on page 189](#).

- ▶ **SIEM Tool:** The SIEM tool is a lightweight service allowing easy export of information from the Forcepoint CASB service into SIEM services. The SIEM Tool allows the export of data to files (in CEF format) or to syslog.


For more information, see ["Setting up SIEM / syslog integration" on page 259](#).

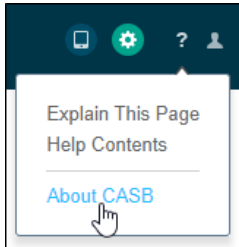
- ▶ **Application Discovery Tool:** The Application Discovery Tool scans network log files from any device (e.g., firewall, web proxy, SIEM, or router) and produces details about all cloud application activity, including usage metrics and risk information for found cloud applications. You can view scan results locally in a produced PDF, or in the Forcepoint CASB management portal after the results are uploaded.

For more information, see ["Installing and configuring the Cloud Discovery tool" on page 16](#).

# Licensing

---

All licensed products and add-ons are listed under the  icon:



On the About CASB page, you can also add new licenses provided by Forcepoint.



# CHAPTER 12

## Managing Service Assets

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

To enable Forcepoint CASB's cloud service monitoring features (except for Discovery), you need to configure Forcepoint CASB to manage the cloud services as an organizational asset. This chapter explains how to create these assets in Forcepoint CASB and to configure their features. Configuration tasks that apply to the Forcepoint CASB system in general rather than per-asset are explained in [Forcepoint CASB System Administration](#).

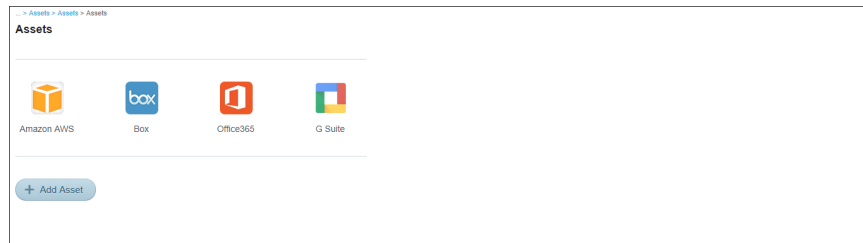
This chapter discusses the following:

Creating an asset .....	270
Configuring asset governance connections .....	278
Customizing access enforcement .....	283
Updating Forcepoint CASB asset data .....	287
Configuring a custom asset .....	288

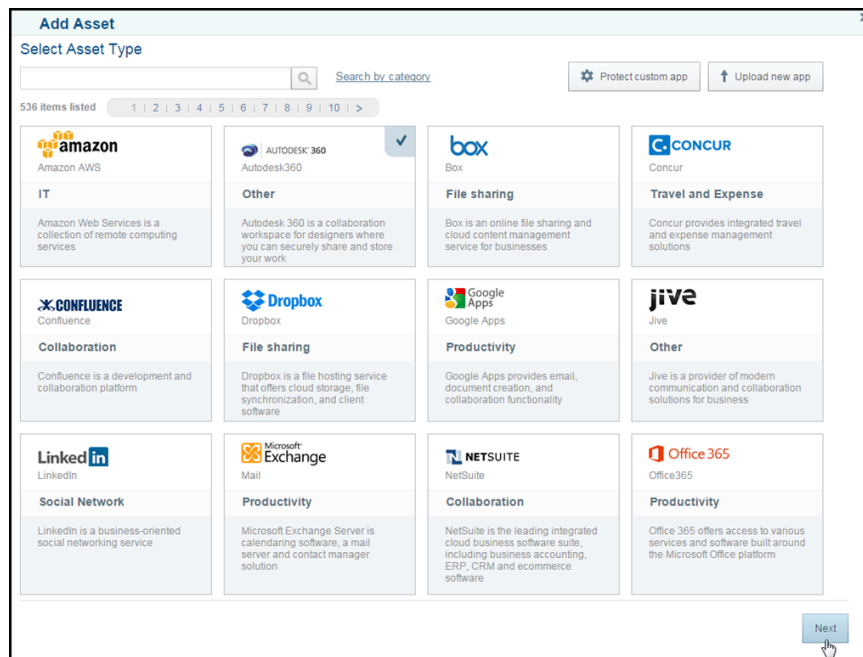
# Creating an asset

To create and initially configure an asset:

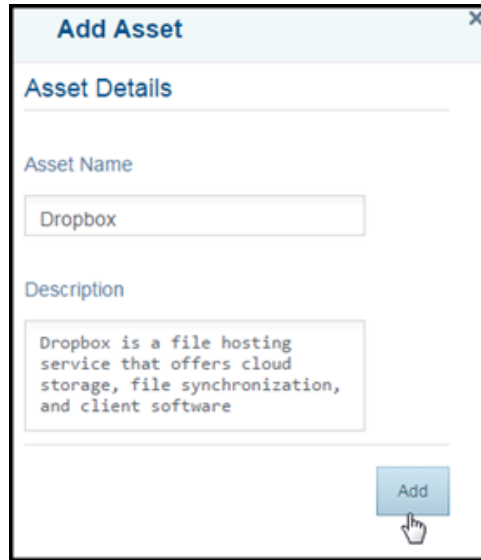
1. Create the asset in one of the following ways:
  - a. To create an asset through Settings:
    - i. Go to **Settings > Resources > Assets** and click **Add Asset**:



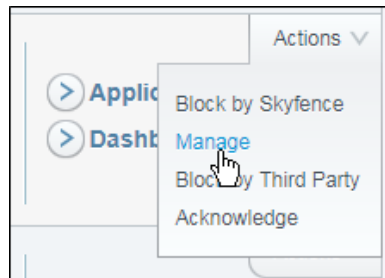
- ii. Select the relevant asset type (you can navigate pages, search, or **Search by category**) and click **Next**:



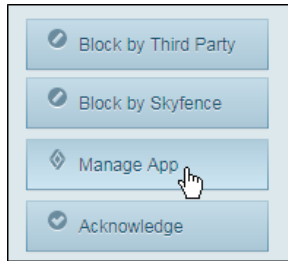
- iii. Enter a **Name** and **Description** or use the default ones, then click **Add**:



- b. If you identified access to this service [in Discovery](#):
  - i. In the Discovery dashboard [application list](#), by the relevant application, click **Actions > Manage**:



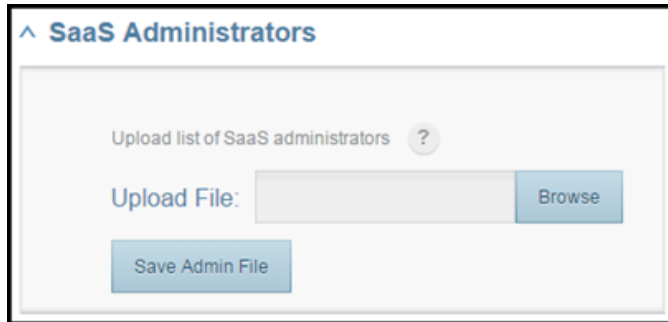
Or, in the Discovery [application details page](#), click **Manage App**:



- ii. Enter a **Name** and **Description** or use the default ones, then click **Add**:

A modal dialog box titled 'Add Asset' with a close button in the top right corner. The main content area is titled 'Asset Details'. It contains two input fields: 'Asset Name' with the text 'Dropbox' and 'Description' with the text 'Dropbox is a file hosting service that offers cloud storage, file synchronization, and client software'. At the bottom right of the dialog is a blue 'Add' button with a mouse cursor pointing at it.

- 2. To enable [activity logs](#) to identify asset administrators, and to enable various [notifications](#) to asset administrators:
  - a. Create a CSV file with a header row and a row for each asset administrator; columns are **name**, **email**, and **phone** (for SMS notifications). The **name** is the user name the administrator uses to log in to the asset. It can be viewed in the Forcepoint CASB audit logs by adding the **Login name** field to the viewed columns.
  - b. In the asset settings page, under **SaaS Administrators**, **Browse** to and upload the CSV file:



- c. Click **Save Admin File**.
3. Forcepoint CASB needs to know the organizational users' login usernames for this asset. In the asset settings page, under **Organizational Directory Settings**, configure the relationship between user information as known from the user directory and asset login names. Select one of:



### ^ Organizational Directory Settings

Define mapping between organizational directory settings and SaaS user accounts

Email Mapping  
Use the email from the organizational directory

One To One Mapping  
The account name is the same in the organizational directory and in the SaaS application

Custom Field Mapping  
Use one of the organizational directory's custom fields Custom Field ▾

Organizational directory to SaaS account mapping  
Define a regular expression to convert the account in the organizational directory to the account in the SaaS application

▶

SaaS account to Organizational directory mapping  
Define a regular expression to convert the account in the SaaS application to the account in the organizational directory

▶

File Mapping  
Choose file in the correct format. Click help to see an example. ?

Browse

Save Directory Settings

- ▶ **Email mapping:** Asset login names are users' email addresses as in the user directory.
- ▶ **One-to-one mapping:** Asset login names are users' account names as in the user directory.
- ▶ **Custom field mapping:** Asset login names match the selected directory field.
- ▶ **Organizational directory to SaaS account mapping or SaaS account to Organizational directory mapping:** Manipulate field values as needed. Type a search expression in the first field, and a replace expression in the second. The part

of the source value (organizational directory or asset login name depending on selection) identified by the regular expression (RegEx) in the first field will be replaced by the second field, which can be a fixed string or another part of the field value identified by regular expression

- ▶ **File Mapping: Browse** and upload a two-column CSV file listing, for each user, their directory account name and their asset login name.

Click **Save Directory Settings**.

To check mapping results, go to **Settings > Account Management > User Data** and look at the asset column.

4. To avoid monitoring non-organizational accounts on the asset (for example, employees' personal Gmail accounts), under **Monitoring** select to monitor **only the following users** and select to monitor users with specified **domain suffixes** and/or users who appear in the [known organizational directory](#):

^ **Monitoring**

---

**Monitor the activities of the following users:**

These users' activities will be logged, and allowed access according to policy.

**All authorized users**  
Forcepoint CASB will monitor the activities of all users who are authorized for the service asset.

**Only the following users**  
Forcepoint CASB will monitor the activities of the following selected users. Other authorized users will connect to the service asset directly, bypassing the CASB service.

**Users whose email addresses have one of the following domain suffixes**

**Users who appear in the organizational directory (AD integration required)**

All directory users

Only directory users belonging to any of the following Organizational Units (OUs)

---

**Do not monitor the activities of the following users:**

These user's activities will not be monitored, they will connect to the service directly bypassing CASB service.

Forcepoint CASB will not monitor the activities of the following selected users. These users will connect to the service asset directly, bypassing the CASB service.

---

**Monitored activities**

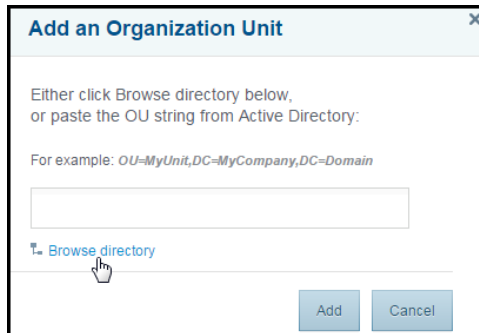
If not selected, Forcepoint CASB will monitor all activities of the above users.  
If selected, Forcepoint CASB will monitor only the login activity, subsequent activities will be directly to the service asset, bypassing the CASB service.

Monitor only login activity

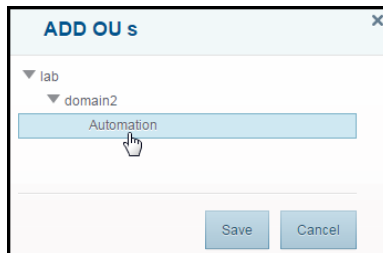
[Save User Monitoring Settings](#)

If you selected to monitor **Users who appear in the organizational directory**, select whether to monitor **All directory users**, or only users belonging to any of some specified **Organizational Units**, in which case, for each relevant OU:

- a. Click **Add an Organizational Unit**.
- b. Either type the OU string (as appearing in the organizational Active Directory), or click **Browse Directory**:



- c. If you're browsing the directory, select the relevant OU:



Click **Save**.

- d. Click **Add**.

Optionally, select **Monitor only login activity**. This feature is for reverse proxy only.

Click **Save Monitoring Settings**.

5. It is recommended to configure [Account Access and Security Governance for the asset](#).
6. It is highly recommended to deploy [gateway enforcement](#).
7. You can customize asset [access enforcement](#).

# Configuring asset governance connections

---

For [activity details](#), [data classification](#), and [account access & security governance features](#), and for some [activity details](#), Forcepoint CASB needs to be able to collect account settings, user information, and (when available) audit logs directly from cloud application servers. These features are then available even when Forcepoint CASB is not deployed as a [gateway to the cloud applications](#).

Account Access & Security Governance is currently supported for the following cloud services:

- ▶ Amazon AWS
- ▶ Box
- ▶ Dropbox
- ▶ Google G Suite
- ▶ Office 365
- ▶ Salesforce

For Forcepoint CASB to be able to collect information directly from a cloud application asset, configure the connections to each relevant cloud service asset as follows:

1. Prepare the following types of accounts to the cloud service:
  - ▶ **Web Connection:** To collect information via web requests ('scraping'). A web connection is required for Governance configuration review, specifically comparing security settings configuration to benchmarks and policies.
  - ▶ **API Connection:** To collect information via an API call to the cloud service. An API connection is required for the following capabilities:
    - Activity import
    - Data classification
    - Mitigation actions
    - Excessive rights (Dormant, orphaned, or external users)

The accounts should have full administrative permissions; alternatively, for a description of a sufficient but more restrictive permission set, see the *Forcepoint CASB Service Provider API Connection Guide*.

# Configuring a web connection

In Forcepoint CASB, a web connection is used to collect user activity through web requests ('scraping').

1. In Forcepoint CASB, go to **Settings > Resources > Assets > asset > Asset Governance**, and configure the **Web connection**:

The screenshot shows the 'Asset Governance' configuration interface. It is divided into two main sections: 'API connection' and 'Web connection'. The 'API connection' section has a description: 'Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials'. It shows a success message: 'Credentials added successfully' with a 'Change connection' link. There is a toggle switch for 'Activity import enabled' which is currently 'on'. Below this are 'Test connection' and 'Delete connection' buttons. The 'Web connection' section has a description: 'Used to retrieve service configuration for configuration settings review'. It contains three input fields: 'User Name' with the value 'admin@forcepoint.com', 'Password' which is masked with dots, and 'Login URL (Optional)' with the value 'https://app.box.com/login'. At the bottom of this section are 'Test Web Connection' and 'Save Connection Settings' buttons.

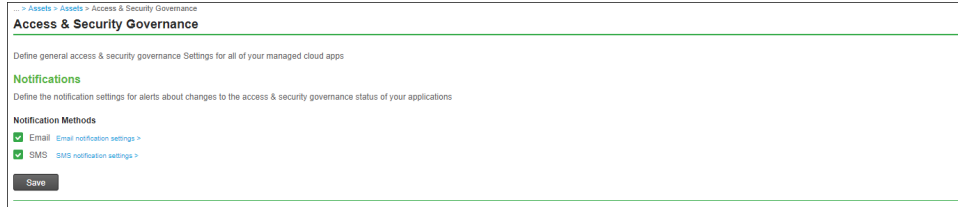
The account credentials should have full administrative permissions. Alternatively, for a description of a sufficient but more restrictive permission set, see the *Forcepoint CASB Service Provider API Connection Guide*.

If the asset API uses a token (rather than credentials), paste it into the **Password** field. For both connections, **Login URL** is necessary only if a non-default URL is used (for example, if your organization uses single sign-on or a customized URL).

2. Click **Save Connection Settings**.
3. You can receive automatic updates upon scans, including the information marked in the Access & Security Governance dashboard as **New**.

To receive these updates, if you haven't yet done this:

- a. Configure a [Governance notification](#).
- b. Go to **Settings > Access & Security Governance** and enable the notification:




This is a global setting for all access & security governance-enabled assets.

## Configuring an API connection

Forcepoint CASB leverages the API offered by the cloud service to audit and monitor user activity, scan and classify stored files, provide information about sharing, apply corrective (mitigation) actions, and compare security settings to regulations and industry standards.

---

 **Note:** Connecting Forcepoint CASB to a cloud service's API must be performed using an Administrator account that has access to all users' and administrators' folders in the account.

---

1. In Forcepoint CASB, go to **Settings > Resources > Assets > asset > Asset Governance**.

Asset Governance

---

**API connection**

Used to retrieve activity logs, scan files at rest, and retrieve user lists. Forcepoint does not store the user credentials

✓ Credentials added successfully [Change connection](#)

on  off Activity import enabled ⓘ

[Test connection](#)

[Delete connection](#)

---

**Web connection**

Used to retrieve service configuration for configuration settings review

User Name

Password

Login URL (Optional)

[Test Web Connection](#) [Save Connection Settings](#)


2. By default, Forcepoint CASB creates an API connection with read and write permissions. This allows you to both audit the activity and assign mitigation actions that require write access to the asset, such as Quarantine, Remove sharing permissions, and Keep a safe copy.

If this is an Office 365 asset, you can configure the connection to allow read-only access to the asset's data. Read-only access allows activity auditing and data classification, but only supports the Audit Only mitigation action.

To select the read-only permission:

- a. Open the drop-down menu above the **Set connection** button and select **Request read-only connection**.

---


 **Note:** This option is only available before the connection is set. After the connection is set, the drop-down menu is disabled.

Read-only access only supports the Audit Only mitigation action. If you have policies in this asset that are set to another mitigation action, Forcepoint CASB displays a message stating that those policies' mitigation actions will reset to

---



---

 **Audit Only.** If you wish to keep the other mitigation actions, click **Cancel** to keep the read-write permission.

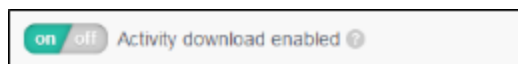
---

3. Under **API connection**, click **Set connection**. A new browser window opens and displays the log in page for the cloud service.
4. On the cloud service's log in page, enter your administrator login credentials. Forcepoint CASB automatically requests that the service generate a token with a set of permissions. These permissions will be presented by the cloud service. You can review and accept these. Note that the required permissions are a subset of the admin capabilities limited to the minimal requirements for Forcepoint CASB functionality.
5. Review the required credentials, then click the button to grant access. The cloud service window closes.
6. In Forcepoint CASB, return to the cloud service asset's settings page (**Settings > Resources > Assets > asset > Asset Governance**), if you are not there already.
7. Forcepoint CASB displays the message **Credentials added successfully** if the API connection accepts the administrator login credentials.
8. Click **Test connection** under API connection to test the connection. Forcepoint CASB connects to the cloud service through the API and attempts to retrieve the user list, data classification download, and activity download.

If this is an Office 365 asset, you can select the **Check encryption** check box to check the connection to the key management service (in this case Azure Key Vault). For more information about setting up a key management service, see "[Managing your key management services](#)" on page 213.

If the connection test fails, Forcepoint CASB is not connected to the cloud service through the API. Verify that you are connecting with an account that has administrator privileges.

9. Click **on** to enable activity download.



10. After this is completed, Forcepoint CASB imports all users' audited activities from the cloud service.

# Customizing access enforcement

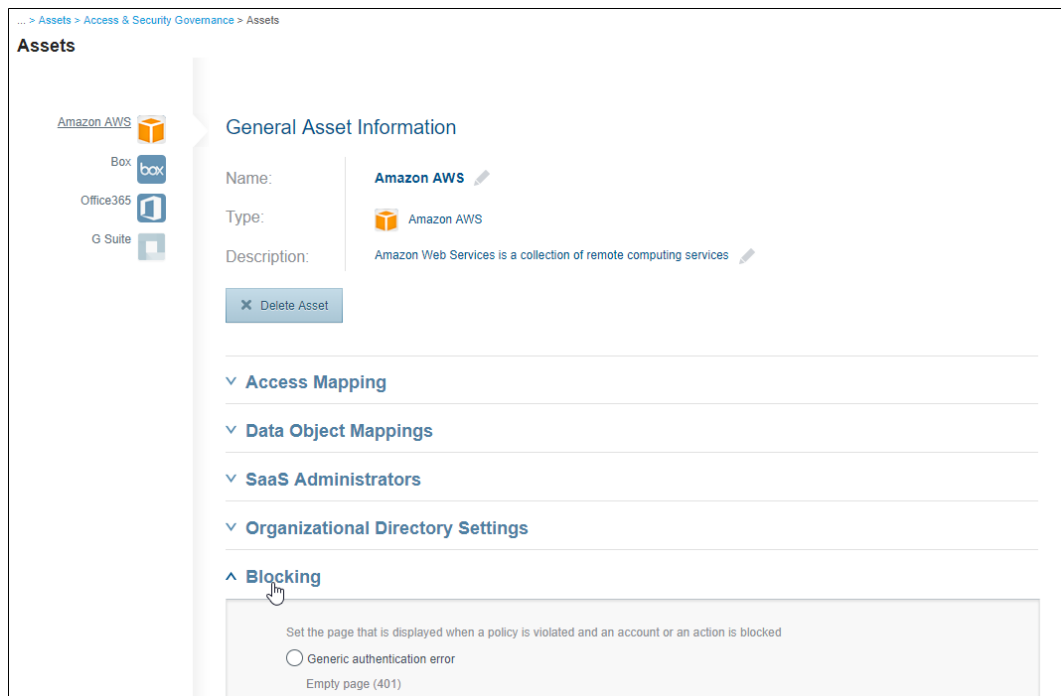
Various Forcepoint CASB features include enforcement by blocking activities or accounts, or by requiring verification for activities or accounts. For each managed service asset, you can customize Forcepoint CASB behavior in these scenarios.

## Customizing account and activity blocking

Various Forcepoint CASB features include enforcement by blocking activities or accounts. You can customize what appears in browsers, for blocked accounts and for block activities.

To customize the appearance for blocked accounts and for block activities:

1. In Forcepoint CASB, go to **Settings > Resources > Assets > asset > Blocking:**



2. Select one:

- ▶ **Generic authentication error:** Forcepoint CASB sends a 401 error, and the browser displays a page accordingly.
- ▶ **Custom page:** Forcepoint CASB displays a custom page. For each of **Blocked**

**account page** and **Blocked action page**, you can use Forcepoint CASB's default page (contains message **Your account has been blocked. Please contact your administrator**), or **Browse** to upload your own HTML page. To use the Forcepoint CASB default page as a basis for changes, **Download** and edit it. To revert to the Forcepoint CASB default page, click **Restore default**.

The screenshot shows a configuration window titled "Set the page that is displayed when a policy is violated and an account or an action is blocked". It contains two radio buttons: "Generic authentication error" (with subtext "Empty page (401)") and "Custom page file upload" (which is selected). Below the "Custom page file upload" option, it says "Choose the file that will be displayed". There are two columns of file selection controls. The left column is for the "Blocked account page" and shows a text input with "block\_account.html" and a "Browse" button. Below it are links for "Download file" and "Restore default". The right column is for the "Blocked action page" and shows a text input with "block\_action.html" and a "Browse" button. Below it are also links for "Download file" and "Restore default". At the bottom of the window is a "Save Blocking Parameters" button.

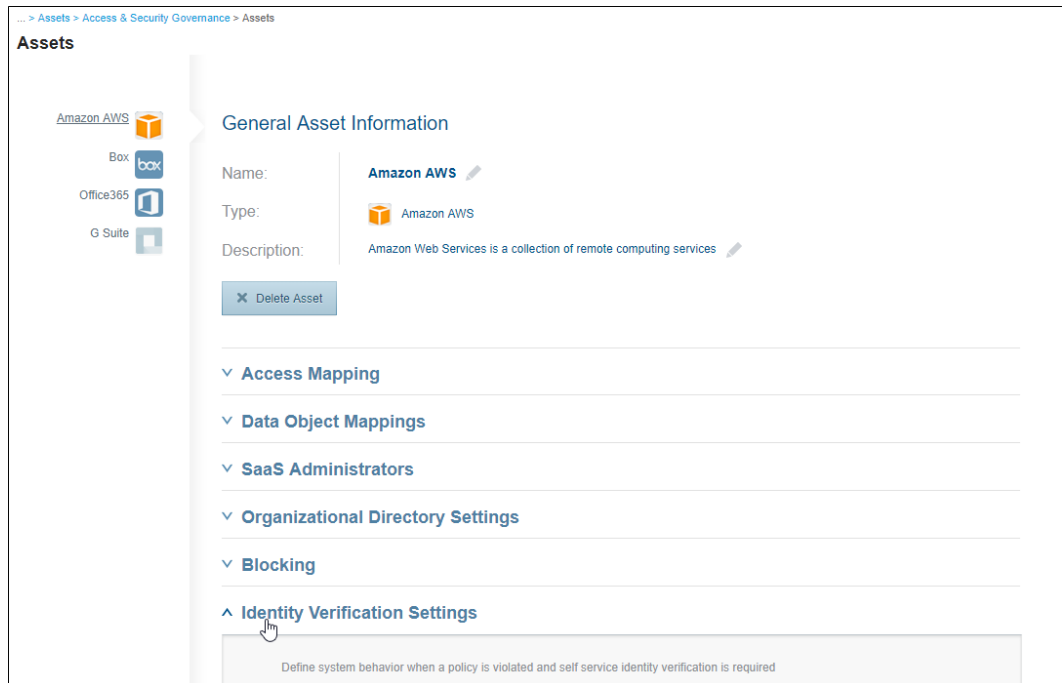
3. Click **Save Blocking Parameters**.

## Customizing identity verification

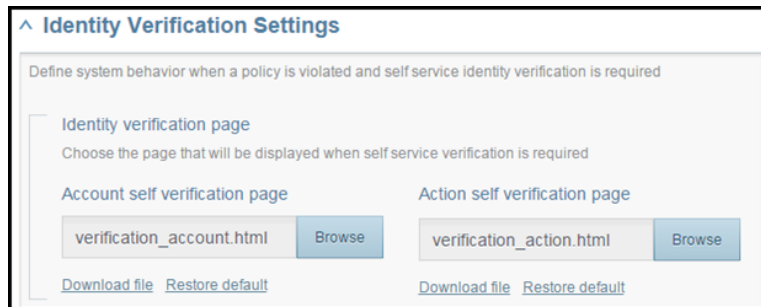
Various Forcepoint CASB features include security enforcement by requiring identity verification. Forcepoint CASB sends the user a verification code and blocks access until the user enters that code. You can customize how the code is sent, identity expiration, and the page presented to the user for verification.

To customize identity verification behavior:

1. In Forcepoint CASB, go to **Settings > Resources > Assets > asset > Identity Verification Settings**:



2. Optionally customize the identity verification page that will be presented to users:



For each of **Account self-verification page** and **Action self-verification page**, you can **Download** and customize the content and style of the verification page. Then **Browse** to upload it.

To revert to the Forcepoint CASB default page, click **Restore default**.

3. Under **Notification Type**, select how verification codes are sent to users (**Email** and/or **SMS**), and how many times a user can request a code before being blocked until the following day:

**Notification Type**  
Choose the type of notification that will be sent and the maximum number that can be sent per day

Email [Notification settings](#)

SMS [Notification settings](#)

Allow up to  notifications in 24 hours

Email and SMS messages are as configured in [Notifications](#).

4. Configure whether and after how much time verification expires:

**Identity verification expiration**  
Define how long the user device remains unblocked after self service verification

User device remains unblocked forever

Custom expiration period

Identity verification expiration  h  m

[Save self service settings](#)

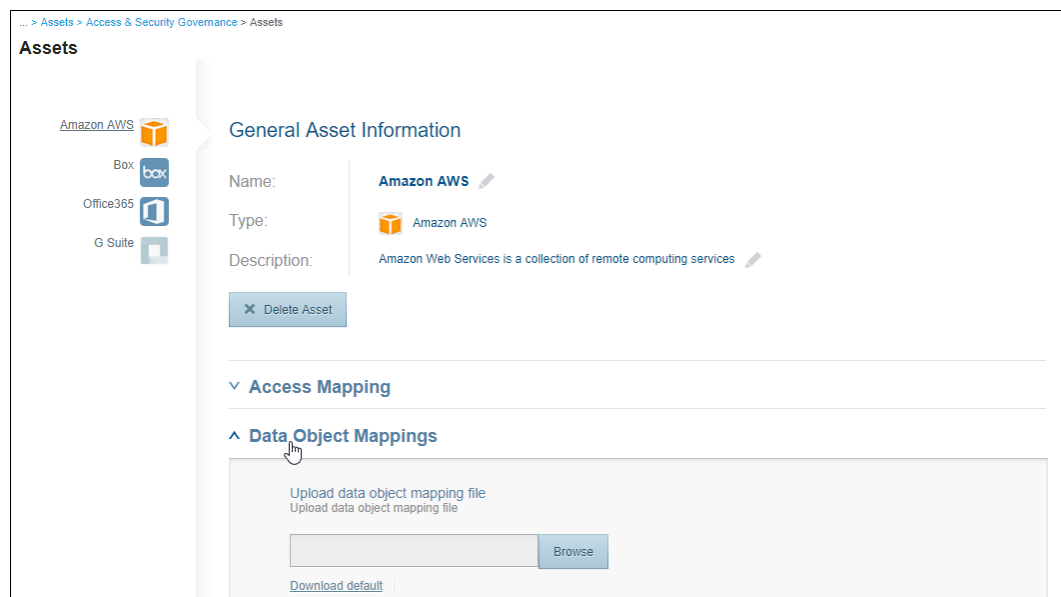
5. Click **Save self-service settings**.

# Updating Forcepoint CASB asset data

Forcepoint continuously researches service application behavior, and from time to time might provide customers with asset data updates to improve the Forcepoint CASB product's ability to monitor asset user activities. In some cases, you can request custom changes to asset data from Forcepoint professional services.

To install an asset data update:

1. In Forcepoint CASB, go to **Settings > Resources > Assets > asset > Data Object Mappings**:



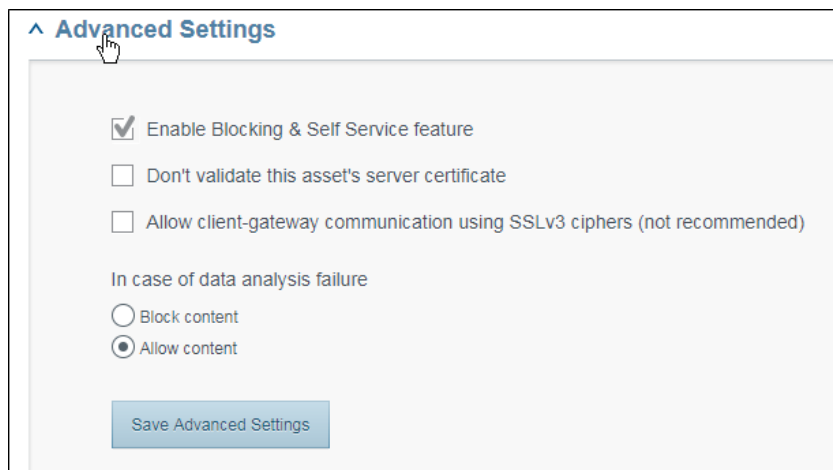
2. **Browse** to and upload the asset update file.
3. Click **Save mapping file**.

# Configuring a custom asset

Forcepoint CASB can monitor uncommon assets such as homegrown organizational service applications, with limited feature functionality.

To add a custom asset, [create the asset as usual](#), and in the **Add Asset** window select **Protect custom app**. Configure relevant asset settings.

Some additional settings that might be relevant to custom assets appear in the asset Settings page, under **Advanced Settings**:



The screenshot shows the 'Advanced Settings' section of the asset configuration interface. It features a header with an expand/collapse icon and the text 'Advanced Settings'. Below the header are three checkboxes: 'Enable Blocking & Self Service feature' (checked), 'Don't validate this asset's server certificate' (unchecked), and 'Allow client-gateway communication using SSLv3 ciphers (not recommended)' (unchecked). Underneath these is a section titled 'In case of data analysis failure' with two radio buttons: 'Block content' (unchecked) and 'Allow content' (checked). At the bottom of the settings area is a 'Save Advanced Settings' button.

- ▶ If the service application doesn't present a proper certificate, select **Don't validate this asset's server certificate**.
- ▶ If the service application uses the non-secure SSLv3, select **Allow client-gateway communication using SSLv3 ciphers**.



# CHAPTER 13

## Setting up Gateway Enforcement

*Forcepoint CASB | 2021 R4 | Updated: December 19, 2021*

For cloud user activities to go through the [Forcepoint CASB gateway](#), connections from browsers and other client applications need to go through the Forcepoint CASB gateway. To implement this, reverse proxy and endpoint routing solutions are available.

Reverse proxy provides a secure solution by disabling non-gateway connections to cloud assets. However, non-browser client applications, such as most Office 365 desktop applications and most mobile client applications, can only access their native server URL. If only reverse proxy is used, these applications will not work. Endpoint routing provides a good solution for controlled organizational devices, including for applications that do not support URL changes, but does not disable non-gateway connections from other devices. A comprehensive solution recommended in many cases is to use both types of solutions in parallel (supported by Forcepoint CASB): Implement reverse proxy as the primary enforcement method, and distribute the Forcepoint CASB endpoint routing solutions as needed for applications that cannot otherwise be directed to the Forcepoint CASB gateway.

This chapter discusses the following:

Setting up reverse proxy (IdP Proxy) .....	290
Setting up endpoint routing solutions .....	305
Blocking unmanaged service applications .....	314



# Setting up reverse proxy (IdP Proxy)

---

For [reverse proxy enforcement](#), configure cloud service applications to accept service requests for the relevant account(s) only from the Forcepoint CASB gateway. This can be done for each service application either by IP restriction (configure accounts to accept service requests only from the gateway's IP address; not available for all service applications) or by IdP proxy as explained in this section.

## IdP proxy overview

For any cloud application that has been configured as a [managed asset](#), you can configure the application to authenticate users by an external single sign-on Identity Provider (SSO IdP; a third-party IdP, which might already be configured for your organization, or Forcepoint CASB can itself be the IdP), and configure the IdP to redirect via Forcepoint CASB. Upon authentication, the IdP redirects the connection (with identity assertion) via Forcepoint CASB. For Office 365, the flow is slightly different, in that even before IdP authentication, browser connections are redirected via Forcepoint CASB.

End-users will need to log only into the IdP, as usual with such single sign-on systems. Instead of then redirecting to the cloud service, you'll configure the IdP to automatically redirect to Forcepoint CASB, with no impact on user experience. You can additionally configure the cloud service to accept only such connections, or, for gradual deployment, you can choose to allow non-gateway connections as well. To support these two options, Forcepoint CASB provides the following two IdP Proxy modes:

- ▶ **Limited Integration:** The IdP redirects via Forcepoint CASB, but the service application does not enforce such connections. Forcepoint CASB functions as a transparent proxy, passing on the original authentication token which is addressed to the service application. The service application is configured to trust authentication originating from the IdP.

Limited Integration has the following advantages over Proxy Enforcement:

- ▶ Simpler configuration, and easier to revert from if necessary.
- ▶ For gradual deployment, for the service application to continue accepting also connections that do not go through Forcepoint CASB. This is relevant if the service application does not enable configuring multiple IdP accounts (as is the case for most service applications) but the IdP can be configured to use the same certificate for two accounts addressed to the same service application.
- ▶ **Proxy Enforcement:** The IdP addresses its response to the Forcepoint CASB gateway; the Forcepoint CASB gateway accepts the authentication from the IdP, then re-signs the response with its own certificate. The service application accepts only such authentication

signed by the Forcepoint CASB gateway.

Proxy Enforcement provides complete reverse proxy enforcement.

Rather than use a third-party IdP, you can use [Forcepoint CASB itself as a single sign-on IdP](#). This simplifies some configuration of IdP Proxy.

## Using Forcepoint CASB as a single sign-on identity provider

Instead of using a third-party IdP, Forcepoint CASB itself can be used as a single sign-on IdP. Users sign into Forcepoint CASB's IdP page with their organizational domain credentials, and Forcepoint CASB authenticates users to the service application by their email address (more precisely, by the Active Directory property [mapped to Account Email](#), usually **mail**).

For Forcepoint CASB management server performance or high-availability considerations, a separate, external Forcepoint CASB instance can be dedicated for IdP, or, for simpler configuration, use the main organizational Forcepoint CASB.

Forcepoint CASB as IdP is not supported for Office 365.


To configure Forcepoint CASB as an IdP:

1. Make sure that a relevant Active Directory (**not** static directory file) is [configured](#).
2. In Forcepoint CASB, go to **Settings > Forcepoint IDP**:

... > Access & Security Governance > Assets > Forcepoint IDP

### Forcepoint IDP

The Forcepoint CASB Identity Provider enables you to provide single sign-on to managed cloud assets and enforce proxy usage

Name:  Forcepoint CASB

---

### Login Page

To change the default login page, upload an HTML file here. Download the default HTML for more information

ForcepointIDP\_login.html

[Download](#) [Restore Default](#)

---

### Security Settings

Enable persistent login  
Allow users to access their approved assets without re-entering their credentials

Expiration time is  hours

Block after  failed login attempts by a user from the same IP for  minutes

3. Under **Login Page**:

- ▶ Customize the current login page: Click **Download** to save a copy of the current login page, then customize the content and style. Click **Browse** to upload it.
- ▶ Upload a new login page: To use a different login page, click **Browse** to upload the file. The login page must be in HTML format.
- ▶ Use the default login page: If you are using a custom login page, you can return to using the default login page by clicking **Restore Default**.

Click **Save Login Page**.

4. Under **Security Settings**, click **Enable persistent login** to set a defined **Expiration time**. You can also define values for temporarily blocking access after a set number of failed login attempts.

Click **Save Security Settings**.

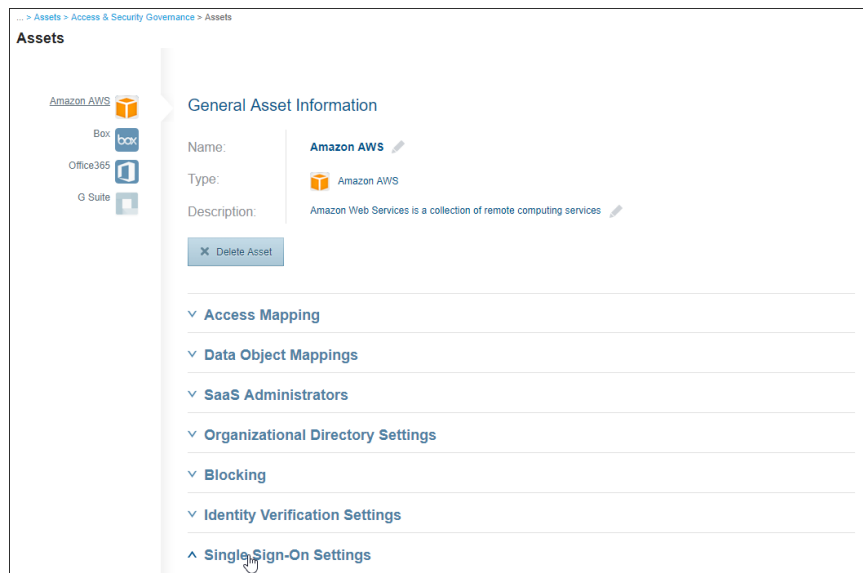
5. Select how Forcepoint CASB should sign its responses:

- ▶ **Forcepoint CASB self signed key pair**: Use a certificate automatically-generated for the organization.

- ▶ **Custom key pair:** Use a provided certificate. Click **Browse** to upload a certificate PFX file in Base 64 (not binary) format, and provide the **password**.

Click **Save Key Pair**.

6. For each service application that should accept single sign-on:
  - a. Make sure that Active Directory users are properly [mapped for the service application](#).
  - b. In the service application’s administration site, configure your organizational account for single sign-on from an IdP, including:
    - i. The service application’s single sign-on configuration settings will require either an IdP metadata file or manually-provided IdP URLs. You can find both of these in Forcepoint CASB at **Settings > Resources > Assets > asset > Single Sign-On Settings > Cloud Application IDP Settings**:



Either copy the **Manual Configuration** URLs to the service application’s administration site, or **Download SAML Metadata**, then upload it to the service application’s administration site.

- ii. For the service application to trust the IdP, it requires the IdP’s public key certificate. In Forcepoint CASB, in the above page, **Download IDP Certificate**, then upload it to the service application’s administration site.
- c. In Forcepoint CASB, in the above page, scroll down to **General Settings** and provide:

**General Settings**

Provide required information about the managed cloud asset for the Skyfence identity provider. Look for this information under the Single Sign On Settings in the cloud application

Application's Login URL ?

Default Relay State ?

Entity ID ?

Save General Settings

- ▶ **Application's Login URL** (required): The service application's login URL for single sign-on.  
If you're using an external Forcepoint CASB instance for the IdP, when you later on configure IdP Proxy you'll be directed to change this field's value to the relevant Forcepoint CASB URL.
- ▶ **Default Relay State**: The URL of the service application page that the user should be presented with upon successful authentication. To send the user to the last-accessed page, leave empty or enter a slash ( / ) depending on service application syntax requirements.
- ▶ **Entity ID**: If required by service application, provide the required string.

Click **Save General Settings**.

- d. Under **Active Directories**, specify one or more [configured organizational directories](#) to use for authenticating users for this service application.

Click **Save Active Directories**.

- e. Under **SAML Attributes**, provide additional attributes that are required by some service applications (notably, AWS).

Single sign-on is now active. To test, go to the **Single Sign-On URL** that appears under **Cloud Application IDP Settings** above. Make the URL available to end users, such as by linking to it from an organizational portal.

## Configuring IdP proxy

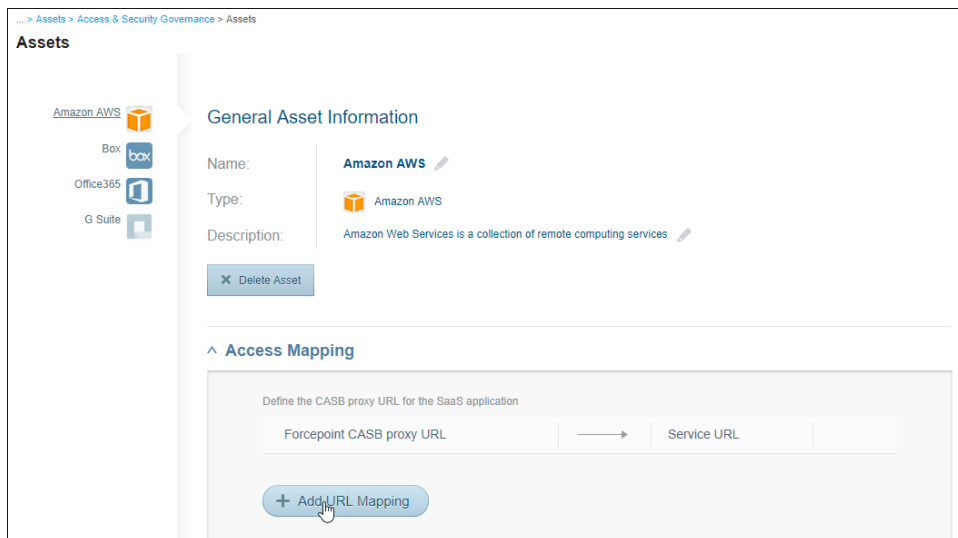
You can configure IdP Proxy in either of two modes: [Limited Integration or Proxy Enforcement](#).

To configure IdP Proxy for Office 365, you'll need to follow a [different procedure](#).

Limited Integration requires that the IdP be either Forcepoint CASB itself (not an external Forcepoint CASB instance) or an IdP that supports separating the redirection destination from the final authentication recipient, so that it can mark its response as addressed to the service application but redirect the connection to the Forcepoint CASB gateway.

To configure IdP Proxy for a service application, in either of the above modes:

1. Make sure that single sign-on [via Forcepoint CASB as IdP](#) or via a third-party IdP is fully configured for the service application.
2. Make sure that the service application is configured as a [managed asset](#).
3. Configure an asset-specific gateway address to be mapped to the service application's address:
  - a. In Forcepoint CASB, go to **Settings > Resources > Assets > asset > Access Mapping > Add URL Mapping**:



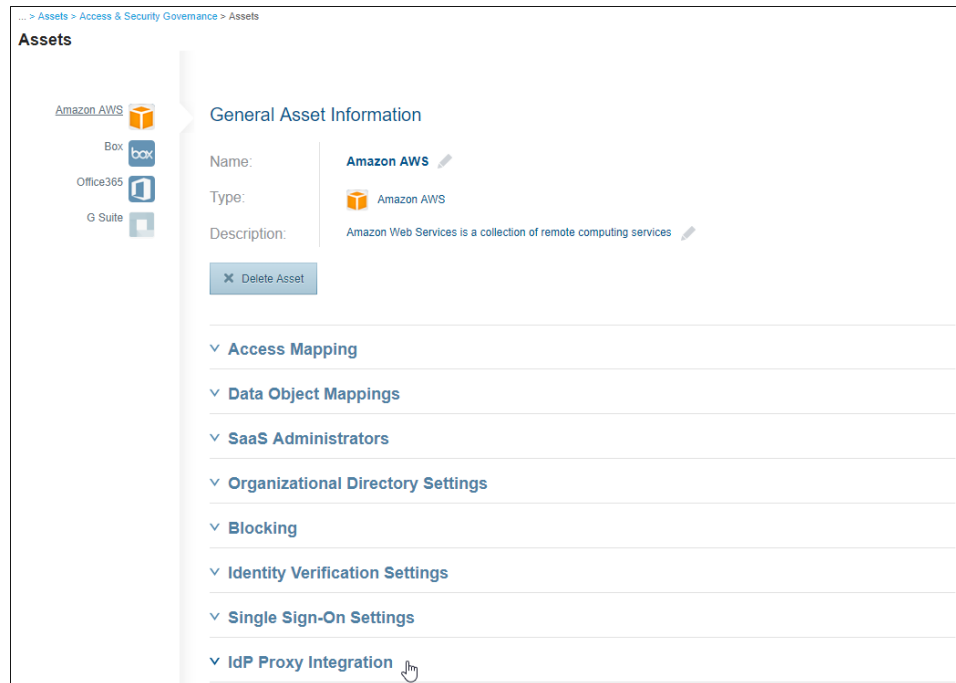
- b. Configure the URL mapping:

The screenshot shows a dialog box titled "URL Mapping". It has a close button (X) in the top right corner. The dialog contains two input fields: "Forcepoint CASB proxy URL" which includes a text input box and a dropdown menu, and "Service URL" which is a simple text input box. At the bottom right of the dialog are two buttons: "Save" and "Cancel".

- ▶ By **Forcepoint CASB proxy URL**, type an asset-specific prefix and select the relevant gateway from the list.
- ▶ By **Service URL**, type the service application's URL.

Click **Save**.

4. In Forcepoint CASB, go to **Settings > Resources > Assets > asset > IdP Proxy Integration**:



For the following settings, you can click **Use a Wizard**, or just set them on this page.

5. Select the IdP Proxy mode: **IdP Integration** or **IdP Integration with Anti-bypass**:



^ IdP Proxy Integration

Use a Wizard OR Change integration settings manually

Enable IdP Proxy Integration using a SAML-based corporate single-sign-on service.

Disabled  
No integration with WS-Federation. Users will not be automatically directed to the CASB gateway

IdP Integration  
Use corporate single sign-on to automatically direct users to the CASB gateway. This mode enables a gradual CASB rollout by retaining the option to access the cloud application directly.

**Choose Identity Provider**  
This Identity Provider will be used for authentication

Choose Identity Provider ▾

IdP Integration with Anti-bypass  
Use corporate single sign-on to automatically direct users to the CASB gateway. All users will be forced to access the cloud application through the CASB Proxy.

Save IdP Proxy Integration Settings

6. Select the **Identity Provider**. If the IdP is a separate Forcepoint CASB instance, select **CASB External**. If the IdP is the same Forcepoint CASB you're working on (local), select **Forcepoint CASB**.
7. For IdP Integration with Anti-bypass mode only:
  - a. Unless you selected **Forcepoint CASB** (local; in which case the IdP's certificate is already known), provide Forcepoint CASB with the IdP's public key:
    - i. Obtain the IdP's public key certificate file; it should be available for download from the IdP's page for the service application.
    - ii. Back in Forcepoint CASB, under **Identity Provider's Signing Certificate**

provide the IdP's public key file:

**Identity Provider's Signing Certificate** ?

This is the Identity Provider's public key. The proxy uses it to verify the authenticity of SAML requests

Identity Provider Certificate File

- b. For IdP Integration with Anti-bypass mode only, Select how Forcepoint CASB should re-sign authentication responses:

**Signing Key Pair** ?

Key pair that will be used by the proxy to sign outgoing SAML requests to the cloud application.

Forcepoint CASB self signed key pair Use this option to generate a self signed key pair

Custom key pair Use this option to upload a custom key pair PFX file

Key File

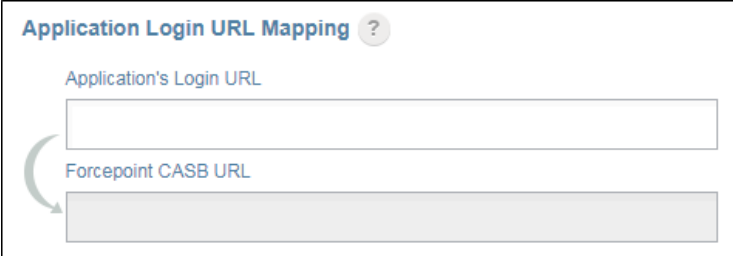
Password

- ▶ **Forcepoint CASB self-signed key pair:** Use a certificate automatically-generated for this service application asset.
- ▶ **Custom key pair:** Provide a certificate. Click **Browse** to upload a certificate PFX file in Base 64 (not binary) format, and provide its **password**.

For Forcepoint CASB IdP Proxy to be effectively enforced, the certificate should be different than the certificate used by the IdP.

- c. Click **Save IdP Proxy Integration Settings**, then click **Download Signing Certificate**.
- d. Upload this certificate file that you downloaded from Forcepoint CASB to the service application's administrative portal, in its single sign-on settings, as the IdP's public key.
8. Unless you selected **Forcepoint CASB** (local; in which case the application login URL is known from Forcepoint CASB IdP settings):

- a. Copy the service application's URL for single-sign on by IdPs.
- b. Paste the SSO login URL into Forcepoint CASB under **Application Login URL Mapping > Application's Login URL:**



The screenshot shows a configuration window titled "Application Login URL Mapping" with a help icon. It contains two text input fields. The top field is labeled "Application's Login URL" and the bottom field is labeled "Forcepoint CASB URL". A grey curved arrow points from the top field to the bottom field, indicating a mapping or auto-generation process.

- c. Click outside the URL field to auto-generate a mapped **Forcepoint CASB URL**.
- d. Copy the above **Forcepoint CASB URL** to the IdP's administration site for the service application as the service provider's single-sign on / Login / Assertion Consumer Service (ACS) URL.

If the IdP is an external instance of Forcepoint CASB, enter it in the external Forcepoint CASB at **Settings > Resources > Assets > asset > Single Sign-On Settings > General Settings > Application's Login URL**, and click **Save General Settings**.

9. Click **Save IdP Proxy Integration Settings**.

IdP proxy is now active.

## Configuring IdP proxy for Office 365

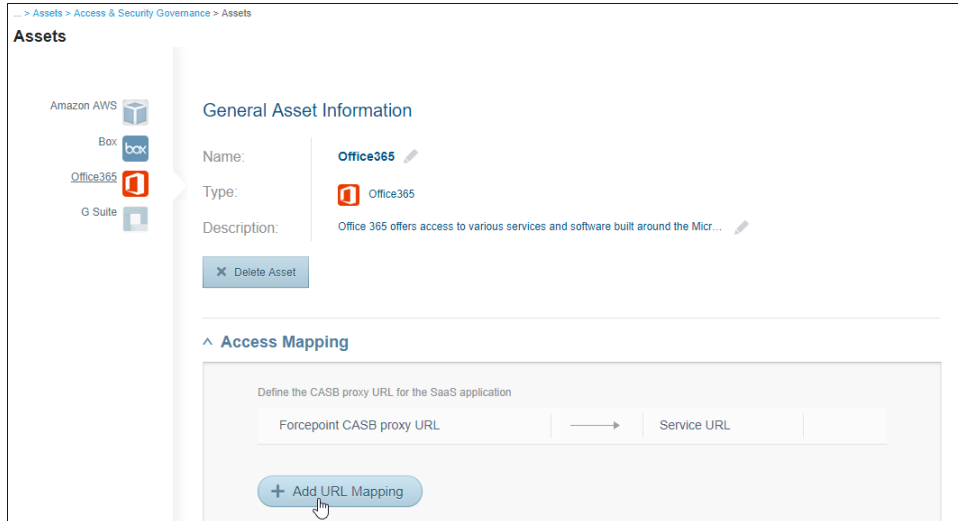
To enable browser communications with Office 365 to go through Forcepoint CASB, Office 365 must accept authentication only from an IdP (for example, Okta or Microsoft ADFS), and the IdP should be accessed via Forcepoint CASB. Forcepoint CASB is then effectively a transparent reverse proxy in front of the IdP.

You can configure IdP Proxy for Office 365 in either of two modes: [Limited Integration or Proxy Enforcement](#).

To configure IdP Proxy for Office 365, in either of the above modes:

1. Make sure that single sign-on via a third-party IdP such as ADFS is fully configured for Office 365.
2. Make sure that Office 365 is configured as a [managed asset](#).
3. Configure an asset-specific gateway address to be mapped to Office 365's address:

- a. In Forcepoint CASB, go to **Settings > Resources > Assets > Office 365 > Access Mapping > Add URL Mapping**:



- b. Configure the URL mapping:

The screenshot shows a 'URL Mapping' dialog box. It has a title bar with 'URL Mapping' and a close button. The dialog contains two input fields: 'Forcepoint CASB proxy URL' and 'Service URL'. The 'Forcepoint CASB proxy URL' field has a dropdown menu next to it. At the bottom right of the dialog, there are two buttons: 'Save' and 'Cancel'.

- ▶ By **Forcepoint CASB proxy URL**, type an asset-specific prefix and select the relevant gateway from the list.
- ▶ By **Service URL**, type Office 365's URL.

Click **Save**.

4. In Forcepoint CASB, go to **Settings > Resources > Assets > Office 365 > IdP Proxy Integration**:

**^ IdP Proxy Integration**

Integrate Forcepoint CASB as a proxy in front of the organizational single sign-on IdP (Identity Provider, such as Microsoft ADFS) This enables browser communications with Office 365, from managed and unmanaged endpoints, to go through Skyfence.

**Disabled**  
No integration with WS-Federation. Users will not be automatically directed to the CASB gateway.

**IdP Integration**  
Use corporate single sign-on to automatically direct users to the CASB gateway. This mode enables a gradual CASB rollout by retaining the option to access the cloud application directly.

**IdP Integration with Anti-bypass**  
Use corporate single sign-on to automatically direct users to the CASB gateway. All users will be forced to access the cloud application through the CASB Proxy.

Save IdP Proxy Integration Settings

5. Select the IdP Proxy mode: **IdP Integration** or **IdP Integration with Anti-bypass**:
6. In step **3**, provide your organizational domain:

**To configure IdP Proxy:**

1. Make sure that single sign-on via a third-party IdP (for example, ADFS) is fully configured for Office 365.
2. Make sure that URL Mapping (above) is configured.
3. Enter your organizational domain (for example, acme.com):

Save

7. For IdP Integration with Anti-bypass mode only, Select how Forcepoint CASB should re-sign authentication responses:

**Signing Key Pair** ?  
 Key pair that will be used by the proxy to sign outgoing SAML requests to the cloud application.

**Forcepoint CASB self signed key pair** Use this option to generate a self signed key pair

**Custom key pair** Use this option to upload a custom key pair PFX file

Key File

Password

- ▶ **Forcepoint CASB self-signed key pair:** Use a certificate automatically-generated for this service application asset.
- ▶ **Custom key pair:** Provide a certificate. Click **Browse** to upload a certificate PFX file in Base 64 (not binary) format, and provide its **password**.

For Forcepoint CASB IdP Proxy to be effectively enforced, the certificate should be different than the certificate used by the IdP.

8. [Download](#) and run the Windows Azure Active Directory Module for Windows PowerShell.

9. In PowerShell, run:

```
Connect-MsolService
```

At the prompt, provide your Office 365 administrative account.

10. Copy the command that appears in Forcepoint CASB under step 7, replace **output.xml** with a convenient location to save the output file, and run the command in PowerShell.

11. In Forcepoint CASB, in step 7 (in Limited integration) or 8 (in Proxy Enforcement) click **Browse** and upload the output XML file.

12. If your organization uses Kerberos authentication, authentication from organizational endpoints needs to be directly to the IdP's URL. For this, expand **advanced settings** and select **Bypass Skyfence for passive login on desktops**:

Hide advanced settings

Bypass Skyfence for passive login on desktops

The integration with Kerberos may require additional configuration of the IdP. Please contact Forcepoint support for assistance.

13. If your organization's Office 365 login URL is non-standard, under **advanced settings** provide it.
14. Click **Save IdP Proxy Integration Settings**.
15. Copy the command now displayed below and run it in PowerShell.
16. If your IdP enables IdP-initiated access (not relevant for ADFS):
  - a. Under **Application Login URL Mapping > Application's Login URL** provide the service application's URL for single sign-on login by IdP, and click outside to auto-generate a mapped **Forcepoint CASB URL**.
  - b. Do one of the following:
    - ▶ If the IdP portal includes an Office 365 link with an editable Office 365 URL, change the URL to the Forcepoint CASB Office 365 IdP proxy URL.
    - ▶ Otherwise, hide or otherwise prevent use of the default link to Office 365, and create a new SAML 2.0 application icon with the Forcepoint CASB Office 365 IdP proxy URL.

IdP proxy is now active.

# Setting up endpoint routing solutions

---

Deploy endpoint routing solutions to the managed devices within your organization to route all asset connections from these devices through the Forcepoint CASB gateway.

For routing on Windows and Mac endpoints, implement endpoint routing either with the Forcepoint CASB Security Service agent (also known as the Forcepoint CASB Endpoint agent), or by distributing a PAC file through GPO distribution. See "[Deploying the Forcepoint CASB Security Service](#)" below and "[Automated PAC file distribution](#)" on page 309 for more information.

All provided routing solutions have extremely low resource impacts and provide a seamless user experience.

## Deploying the Forcepoint CASB Security Service

The recommended method of endpoint routing for desktop endpoints is installing the Forcepoint CASB Security Service on organizational endpoints. The Forcepoint CASB Security Service (also known as the Forcepoint CASB Endpoint agent) automatically routes connections from all browsers and applications on an endpoint to their destinations via the Forcepoint CASB gateway. The Forcepoint CASB Security Service has an extremely low resource impact and merges its routing functionality with existing organizational proxy settings to provide a seamless user experience. The service is maintained with a watchdog service.

## Installing the Forcepoint CASB Security Service (Attended)

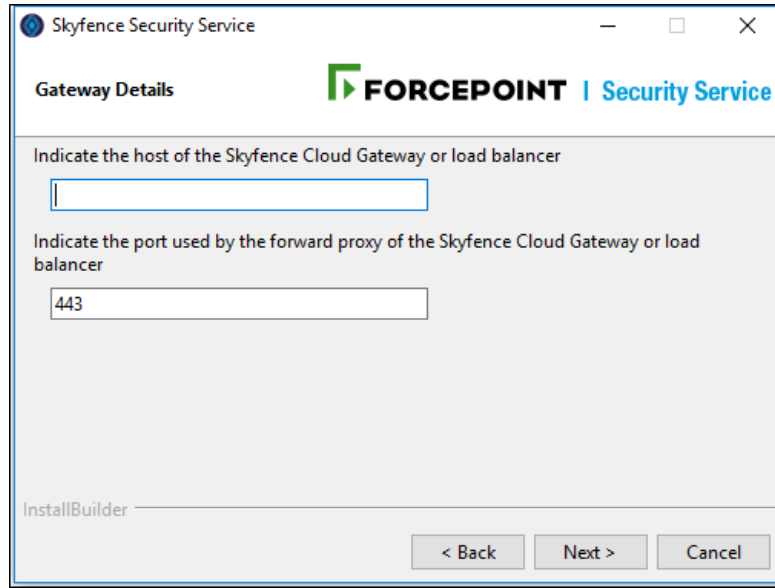
To install the Forcepoint CASB Security Service on a Windows or Mac endpoint:

1. In Forcepoint CASB, go to **Settings > Tools and Agents**.
2. Under the **Endpoint Agents** section, download the package that matches your requirements: Windows 32-bit, Windows 64-bit, or MacOS.
3. Complete one of the following OS-specific tasks:
  - ▶ On **Windows**: As an Administrator, run the Forcepoint CASB Security Service installer.
  - ▶ On **Mac**: As an Administrator, install the application bundle from the DMG, then run the following file inside the installed application bundle:

**SkyfenceSecurityServiceInstall<ver>.app/Contents/MacOS/osx-intel**



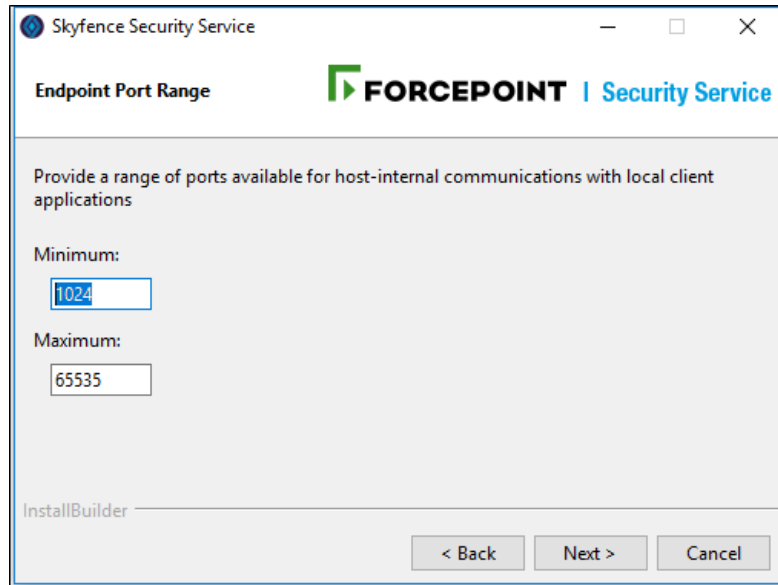
4. Continue through the wizard. Depending on the browser type, you might be directed to close the browser.
5. On the **Gateway Details** wizard page, provide the name (not IP) address of the organizational Forcepoint CASB gateway, and its listening port (usually **443**).



The screenshot shows a window titled "Skyfence Security Service" with a "Gateway Details" wizard page. The page features the Forcepoint Security Service logo. It contains two input fields: the first is for the host address, and the second is for the port, with "443" entered. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

If you are not sure what the gateway address is, in Forcepoint CASB go to **Settings > Tools and Agents**. In the **Endpoint Agents** section, the gateway address is listed under the Desktop agents.

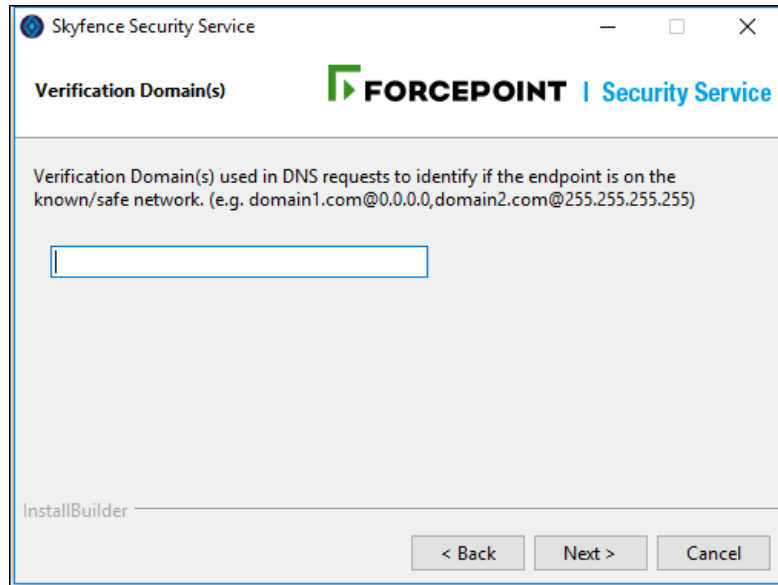
6. On the **Endpoint Port Range** page, provide a range of ports that the Forcepoint CASB Security Service can use for host-internal communications with local client applications.



Providing a range enables fallback when ports are unavailable. To avoid conflicts with other known ports in use, provide other ports.

7. On the **Verification Domain(s)** screen, enter one or more domains to be used in DNS requests to identify if the endpoint machine is on a known, or safe, network. Separate the domains with a comma. For example, `domain1.com@0.0.0.0,domain2.com@255.255.255.255`.

This step is optional depending on your PAC file retrieval method. Verification domains are required if you are retrieving the PAC file dynamically using WPAD and need to verify that the endpoint is on a trusted network by matching the DNS name to the known address. If you are not using WPAD to retrieve the PAC file, you do not need to complete this screen.



8. Complete the wizard.

The Forcepoint CASB Security Service is now installed on the endpoint. If you find that a specific endpoint application is not being properly directed via the gateway, perform [troubleshooting](#).

## Deploying the Forcepoint CASB Security Service via CLI (Silent)

To centrally deploy the Forcepoint CASB Security Service, you can use an automated distribution system such as Active Directory Group Policy to distribute the installer, then:

► **Windows:** Run as an Administrator:

```
SkyfenceSecurityServiceInstall_<ver>_<os>.exe --mode unattended -
-gwHost <gw> --gwPort <port> --minListeningPort <minport> --
maxListeningPort <maxport> [--disablePac 1] [--prefix <location>]
```

► **Mac:** Run:

```
sudo SkyfenceSecurityServiceInstall_
<version>.app/Contents/MacOS/installbuilder.sh --
mode unattended --gwHost <gw> --gwPort <port> --
minListeningPort <minport> --maxListeningPort <maxport> [--
disablePac 1] [--prefix <location>]
```

where

<gw> is the name (not IP) address of the organizational Forcepoint CASB gateway.

<port> is the organizational Forcepoint CASB gateway's listening port (usually 443).

<minport> and <maxport> define a range of ports that the Forcepoint CASB Security Service can use for host-internal communications with local client applications. Providing a range enables fallback when ports are unavailable; to avoid conflicts with other known ports in use, exclude those ports. If the Forcepoint CASB Security Service will be using an [externally-distributed PAC file](#) rather than one retrieved from Forcepoint, it must use only a single fixed listening port, so <minport> and <maxport> must be the same.

Include **--disablePac 1** for the Forcepoint CASB Security Service to use an [externally-distributed PAC file](#) rather than one retrieved from Forcepoint CASB.

<location> (optional) is the installation directory. If omitted, the Forcepoint CASB Security Service is installed in:

- ▶ **Windows:** C:\Program Files (x86)\SkyfenceSecurityService
- ▶ **Mac:** Applications\SkyfenceSecurityService

For example:

```
SkyfenceSecurityServiceInstall_4.1.1.465_windows_x64.exe -mode  
unattended -gwHost acme.skyfencenet.com -gwPort 443 -minListeningPort  
1024 -maxListeningPort 1031
```

Firefox and Safari browsers that were open during the Forcepoint CASB Security Service installation will not be affected until they are restarted.

## Removing the Forcepoint CASB Security Service via CLI

To remove the Forcepoint CASB Security Service:

- ▶ **Windows:** Run the following as an Administrator from the installation directory of Forcepoint CASB Security Service:

```
uninstall.exe --mode unattended
```

- ▶ **Mac:** Run:

```
sudo /Applications/SkyfenceSecurityService/uninstall.app/Content  
s/MacOS/installbuilder.sh --mode unattended
```

## Automated PAC file distribution

An alternative method of endpoint routing for desktop endpoints is distributing a Forcepoint CASB PAC file via an automated distribution system such as Active Directory Group Policy. Endpoint

browsers route connections to asset destinations via the Forcepoint CASB gateway. Non-browser client applications are not affected by the PAC file.

## Configuring automated PAC file distribution

To configure [automated PAC file distribution](#):

1. Make sure that the Forcepoint CASB management server is configured with an [appropriate PAC file](#).
2. In Forcepoint CASB, go to **Settings > Endpoints > Agent/Endpoint Monitoring** and check **Enable Proxy Auto Configuration (PAC)**:

... > Access & Security Governance > Assets > Agent / Endpoint Monitoring

**Agent / Endpoint Monitoring**

Enable Mobile Agent Configuration

**Mobile configuration URL**  
Distribute the link below to mobile users that need to install the agent on their device. The link leads to a page with deployment instructions  
(No Installation Guides URLs)

Save Configuration

**Enable Proxy Auto Configuration (PAC)**  
Forcepoint CASB automatically creates a new PAC file based on your current file and the new CASB settings

**1 Current proxy configuration file**  
The location of the current PAC file

Default file

Remote URL

Local file  
 Browse

**2 New proxy configuration file**  
Download the merged PAC file  
(No PAC URLs)

Save Configuration

3. Under **New proxy configuration file**, download the PAC file.
4. Using standard distribution systems, distribute the PAC file to organizational endpoints and configure browsers to use it.

## PAC file management

Both methods of [desktop routing](#) use a PAC file that is produced by the organizational Forcepoint CASB to define per-asset routing to Forcepoint CASB. If your organization already uses a distributed PAC file for other purposes, this PAC file needs to be merged with the Forcepoint CASB PAC file.

The Forcepoint CASB Security Service automatically performs this merging, so for Forcepoint CASB Security Service in most cases you do not need to do anything with PAC files. However, in some cases, you might choose to externally perform the merging and/or distribution.

You can either manually merge the PAC files, or you can submit the PAC files to Forcepoint CASB for automatic merging, then use the merged output for manual download and distribution or for automatic retrieval by the Forcepoint CASB Security Service.

## Automatic PAC file merging

You can externally manage PAC file merging.

To provide the organizational PAC file to Forcepoint CASB to be automatically merged with its PAC file, you can either upload a static organizational PAC file, or you can point Forcepoint CASB to a location for continuous updating.

To configure automatic PAC file merging:

1. In Forcepoint CASB, go to **Settings > Endpoints > Agent/Endpoint Monitoring** and check **Enable Proxy Auto Configuration (PAC)**:

... > Access & Security Governance > Assets > Agent / Endpoint Monitoring

### Agent / Endpoint Monitoring

Enable Mobile Agent Configuration

**Mobile configuration URL**  
Distribute the link below to mobile users that need to install the agent on their device. The link leads to a page with deployment instructions  
(No Installation Guides URLs)

Save Configuration

---

**Enable Proxy Auto Configuration (PAC)**  
Forcepoint CASB automatically creates a new PAC file based on your current file and the new CASB settings

**1 Current proxy configuration file**  
The location of the current PAC file

Default file

Remote URL

Local file

**2 New proxy configuration file**  
Download the merged PAC file  
(No PAC URLs)

Save Configuration

2. Under **Current proxy configuration file**, select one of the following:
  - ▶ **Default file:** Don't merge anything into the Forcepoint CASB PAC file.
  - ▶ **Remote URL:** Periodically get the organizational PAC file from this URL and merge it into the Forcepoint CASB PAC file.

- ▶ **Local file:** Merge the uploaded PAC file into the Forcepoint CASB PAC file.

3. Click **Save Configuration**.

The PAC file is now ready to be used by the [Forcepoint CASB Security Service](#) or for [distribution](#).

## Manually merging PAC files

You can manually merge the organizational PAC file with the Forcepoint CASB PAC file, then distribute the merged file to endpoints. You will need to merge the PAC files again any time you add services as managed assets or there are any changes to asset domains.

The merged PAC file must include routing for all domains of all cloud services that are Forcepoint CASB assets. The address that the PAC file should point to depends on whether the PAC file will be on endpoints running the Forcepoint CASB Security Service or not:

- ▶ On endpoints **not** running the Forcepoint CASB Security Service, point to the (optional) organizational Forcepoint Web Security Gateway.
- ▶ On endpoints running the Forcepoint CASB Security Service, point to **127.0.0.1:<port>**, where <port> is the Forcepoint CASB Security Service's listening port.

For the Forcepoint CASB Security Service to use a manually distributed PAC file, it must be [installed via CLI](#) with **--disablePac 1** and with a single listening port (i.e., **--minListeningPort** must be the same as **--maxListeningPort**).

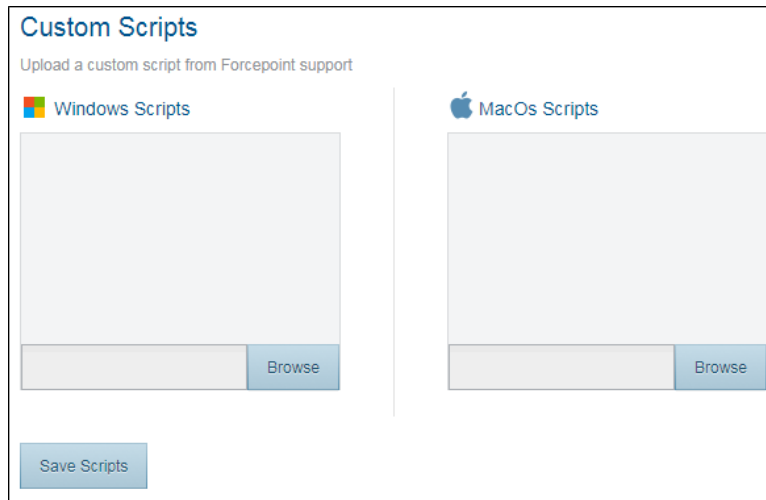
## Testing and troubleshooting endpoint routing solutions

To check whether connections to an asset are being properly routed from a Windows or Mac endpoint through the Forcepoint CASB gateway, verify that when connected to the asset, the presented certificate is for the Forcepoint CASB gateway.

If you find that on Windows or Mac endpoints running the Forcepoint CASB Security Service, a specific endpoint application is not being properly directed via the gateway, it is possible that the Forcepoint CASB Security Service cannot properly monitor that application. In this case, you will need to create a custom script to get the application to use the PAC file. Forcepoint CASB support can assist in creating this script.

After you have created the script:

1. In Forcepoint CASB, go to **Settings > Endpoints > Agent/Endpoint Monitoring**.
2. Under **Custom Scripts**, upload the script under the relevant OS (Windows or Mac):



3. Click **Save Scripts**. The script will run every few minutes on endpoints running the Forcepoint CASB Security Service.



# Blocking unmanaged service applications

With [endpoint routing](#), you can block users from accessing unmanaged service applications, by specifying domain addresses to be blocked.

To block a domain:

1. In Forcepoint CASB, go to **Settings > Organizational Network > Domains**:

User Risk Dashboard > Assets > Domains

## Domains

### Internal domains

Please specify the domains owned by your organization (example format: mycompany.com). All users detected by Forcepoint CASB from the Internal domains are classified as Internal Users. All users outside of these domains are classified as External Users. This classification is used during Data Classification to determine if files are shared internally or externally and can be used to restrict file access to external users.

Enter line-separated domains list

Save

---

### Blocked domains

Please specify the domains that users should not access (example format: restrictedcloudservice.com). This list is used by the Endpoint Agent to restrict access to unauthorized domains.

- support.photobucket.com
- press.spotify.com
- e1.boxcdn.net
- community.igniterealtime.org
- developer.spotify.com

Save

2. Under **Blocked domains**, type the domain address(es) to block. Each domain address must be on a separate line.
3. Click **Save**.

To allow access to a blocked domain:

1. Select the domain address and press the Delete key.
2. Click **Save**.

