Forcepoint

Cloud Security Gateway Integration Guide

Forcepoint Web Security Cloud, Forcepoint DLP, and Forcepoint CASB

Revision A

Published 24 September 2025

Contents

1 Introduction 5
Getting Started 5
Terminology 7
Additional documentation 8

2 License Information 9
Licensing for the Forcepoint CASB and Forcepoint Web Security Cloud integration 9
Licensing for the Forcepoint CASB and Forcepoint DLP integration 11
Update a license in Forcepoint DLP 14
Generate a Forcepoint CASB integration API key 15

3 Integrating Forcepoint CASB and Forcepoint Web Security Cloud 21
General flow 21
Configuring the Forcepoint Web Security Cloud and Forcepoint CASB connection 22
Configure the protected cloud apps list 23
Setting up and monitoring Forcepoint CASB policies on protected cloud apps 25
Managing endpoint enrollment in Forcepoint CASB 27
Verifying the integration 28

4 Integrating Forcepoint DLP and Forcepoint CASB 29
General flow 30
Configuring the Forcepoint DLP and Forcepoint CASB connection 33
Configure single sign-on with Forcepoint CASB 38
Creating and configuring cloud applications 39
Configuring the Cloud API connection 42
Configuring Forcepoint DLP policies for CASB cloud application assets 45
View Forcepoint DLP incidents in the Forcepoint Security Manager 52
View incident information in Forcepoint CASB 53
Configuring Cloud Data Discovery (data at rest) settings 54

5 Integrating Forcepoint DLP and Forcepoint Web Security Cloud 59
General Flow 59
Configuring Data Protection Service connections 61
Configuring a web policy to use Data Protection Service 65
Exporting the Forcepoint Web Security Cloud URL categories 66
Import URL categories to Forcepoint DLP 67
Using URL Categories in DLP policies in the Forcepoint Security Manager 68
Deploy to Data Protection Service 73
View DLP incident reports 74
Verifying the integration 74

Chapter 1

Introduction

Contents

- Getting Started on page 5
- Terminology on page 7
- Additional documentation on page 8

Forcepoint Cloud Security Gateway is an integrated cloud security service that merges web security, network security, and cloud application security into one easy-to- consume service. Forcepoint Cloud Security Gateway protects your business with the following set of products:

- Forcepoint Web Security Cloud
  - Web Security DLP Module
  - Forcepoint DLP Cloud Applications
  - Data Protection Service
  - Advanced Malware Detection
  - Extended Reporting
- Data Protection Service in Forcepoint DLP
- Forcepoint CASB

To fully implement the security features available in Forcepoint Cloud Security Gateway, you must integrate the products so that they communicate and share data. This guide provides the information you need to get started with the integration, as well as the procedures to set up the integrations and configure the products.

Getting Started

This section provides a high-level overview of the Forcepoint Cloud Security Gateway access and integration process. Purchase the Forcepoint Cloud Security Gateway license.

Steps

1) Purchase the Forcepoint Cloud Security Gateway license.

   This license contains the license information for all of the Forcepoint Cloud Security Gateway products: Forcepoint Web Security Cloud, Forcepoint CASB, and Forcepoint DLP Cloud Applications.

   If you purchased the products outside of the Cloud Security Gateway bundle, a separate license is provided for each product. When Forcepoint CASB is purchased, a separate fulfillment email is sent to each customer.

   See *License Information*(mentioned below) for more information about the Forcepoint Cloud Security Gateway license and licensing information if you purchase the products separately.

2) Review your fulfillment email.

   The fulfillment email contains:

   - License information, including the subscription keys for the products
   - Credentials to sign in to the products
   - A JSON file with unique configuration information. This JSON file is used for the Data Protection Service integrations in the Forcepoint Security Manager.

3) Check your Forcepoint Cloud Security Gateway access.

   Verify that you can sign in to the products using the credentials in the fulfillment email:

   a) Sign in to the Forcepoint Cloud Security Gateway Portal to access Forcepoint Web Security Cloud.

   b) Sign in to Forcepoint CASB.

   c) Sign in to the Forcepoint Security Manager to access Forcepoint DLP.

4) Generate your API access keys and secrets in Forcepoint CASB.

   If the API access keys and secrets are not shown in your fulfillment email, or if you need additional API access keys, you can create new keys in Forcepoint CASB. For more information, see *Generate a Forcepoint CASB integration API key* (mentioned below).

   To integrate Forcepoint CASB with Forcepoint Web Security Cloud and Forcepoint DLP Cloud Applications, you need to generate an API access key and API secret for each integration. This key and secret allow Forcepoint CASB to connect to Forcepoint Web Security Cloud and Forcepoint DLP through an API connection.

5) Start the integration process.

   When you start to integrate the products, Forcepoint recommends that you integrate in the following order:

   a) Forcepoint Web Security Cloud and Forcepoint CASB

      With this integration, user requests to selected Protected Cloud Apps are forwarded by the Web Security Cloud proxy to Forcepoint CASB for policy enforcement.

      For more information about setting up this integration and configuring the Protected Cloud Apps, see *Integrating Forcepoint CASB and Forcepoint Web Security Cloud*(mentioned below).

   b) Forcepoint DLP Cloud Applications and Forcepoint CASB

      With this integration, user requests are analyzed depending on the configured cloud app:

      - DLP Cloud Proxy provides immediate, inline activity analysis for cloud applications that connect to Forcepoint CASB through a proxy connection.
      - DLP Cloud API provides near real-time analysis soon after the user operation occurs by connecting to the cloud application through an API connection.
      - Cloud data discovery, or data at rest, provides data discovery and remediation of sensitive data at rest and data shared within sanctioned cloud applications

      For more information about setting up this integration, creating and configuring cloud apps (assets), and configuring Forcepoint CASB policies for DLP, see *Integrating Forcepoint DLP and Forcepoint CASB*(mentioned below).

c) Forcepoint DLP and Forcepoint Web Security Cloud

With this integration, user requests that are considered to represent a potential data security risk are forwarded to Data Protection Service by the cloud proxy. Data Protection Service then determines the risk and returns a response telling the proxy to block or allow the request.
For more information about setting up this integration, see *Integrating Forcepoint DLP and Forcepoint Web Security Cloud*(mentioned below).

Related concepts

License Information on page 9
Generate a Forcepoint CASB integration API key on page 15
Integrating Forcepoint CASB and Forcepoint Web Security Cloud on page 21
Integrating Forcepoint DLP and Forcepoint CASB on page 29
Integrating Forcepoint DLP and Forcepoint Web Security Cloud on page 59

Terminology

Forcepoint CASB and Forcepoint DLP share common features, but sometimes use different terms. The following table maps the terms and definitions for common items you might see in either Forcepoint CASB or Forcepoint DLP.

DLP term	CASB term	Definition
Action/ Action plan	Mitigation	The action that should take place in case of a breach. For example: “Block”, “Permit”.
Case	Incident	An aggregation of incidents (Forcepoint DLP) or alerts (Forcepoint CASB).
Cloud application	Asset	An instance of a cloud service. For example: “My_Company_Box”, “My_Company_AWS”.
Cloud application type	Asset type	A cloud service. For example: “Box”, “AWS”.
Cloud data discovery	Data at rest (DAR)	A feature that allows the Forcepoint DLP Data Agent (DA)/ Forcepoint CASB integration service to scan data at rest on cloud applications.
Cloud service	N/A	A Forcepoint DLP channel.
DLP Data Agent (DA)	N/A	A DLP agent hosted in Forcepoint’s cloud that enables the DLP system to access the data necessary to analyze specific types of traffic, or the traffic from specific servers.

DLP term	CASB term	Definition
DLP Cloud API	API Service provider logs Near real-time	A feature that allows the Forcepoint DLP DA / Forcepoint CASB integration service to take action soon after a breach occurs on cloud application activities. The file scan is completed in a very specific time frame.
DLP Cloud Proxy	Proxy Real-time	A feature that allows the Forcepoint DLP Data Protection Service and Forcepoint CASB solution to take immediate action as a breach occurs on cloud application activities.
Data Protection Service	N/A	The Forcepoint DLP service that enables detection and enforcement of sensitive data breaches on cloud applications.
Event	Activity	A transaction or activity that was monitored and sent for policy analysis.
Incident	Alert	The output of the policy analysis if there is a match in the transaction.
Operation	Action	The atomic action monitored by Forcepoint CASB that an end user completed. For example: “Upload a file”, “Download a file”.

Additional documentation

- Forcepoint DLP v10.4 Administrator Guide
- Forcepoint Web Security Cloud Help
- Forcepoint CASB Administration Guide
- Forcepoint CASB Service Provider API Connection Guide

Chapter 2

License Information

Contents

- Licensing for the Forcepoint CASB and Forcepoint Web Security Cloud integration on page 9
- Licensing for the Forcepoint CASB and Forcepoint DLP integration on page 11
- Update a license in Forcepoint DLP on page 14
- Generate a Forcepoint CASB integration API key on page 15

To enjoy the benefits of the integrations available for the products that are part of Forcepoint Cloud Security Gateway, you need the following licenses. These licenses are automatically included when you purchase the full Forcepoint Cloud Security Gateway package.

- Forcepoint Web Security Cloud Deployment
- Forcepoint Web Security DLP Module
- Forcepoint Web Security Cloud App Control
- Forcepoint DLP Cloud Applications
- Forcepoint CASB

Note

- Customers who already have Forcepoint Web Security Cloud deployment with on-premises Forcepoint Web Security DLP Module can switch to this license. Contact Forcepoint Support for more information.
- Customers with versions of Forcepoint DLP earlier than 8.8.1 who purchase a DLP Cloud Applications license after March 25, 2021, should upgrade to Forcepoint DLP 8.8.1 to enforce policies on DLP Cloud API and Cloud Data Discovery channels.

As part of the fulfillment process, you will receive:

- A new or updated DLP XML license file
- A JSON file with tenant information

Licensing for the Forcepoint CASB and Forcepoint Web Security Cloud integration

For existing Forcepoint CASB and Forcepoint Web Security Cloud customers

Forcepoint recommends that Forcepoint Web Security Cloud customers migrate to Forcepoint Cloud Security Gateway to gain full Forcepoint CASB functionality and unified data protection.

If you choose to only integrate your Forcepoint Web Security Cloud deployment with Forcepoint CASB instead of upgrading to Forcepoint Cloud Security Gateway, you must subscribe to the Forcepoint Web Security Cloud App Control license. Complete one of the following 2 options based on your environment:

- For Forcepoint Web Security customers without a Forcepoint CASB license:
  If you have a Forcepoint Web Security license, but do not have a Forcepoint CASB license, contact your Forcepoint salesperson to obtain the Forcepoint Web Security Cloud App Control license.

  Forcepoint CASB Ops personnel will provision a new Forcepoint CASB instance with the Web Security Cloud App capability enabled. At the end of this process, you will receive a fulfillment email with the Forcepoint Web Security Cloud App Control license.

  Note

  Customers without the Forcepoint CASB suite will incur an additional charge for the Forcepoint Web Security Cloud App Control license.

- For Forcepoint Web Security customers with a Forcepoint CASB license:
  If you currently have both Forcepoint Web Security and Forcepoint CASB licenses, contact Forcepoint Support to obtain the Forcepoint Web Security Cloud App Control license.

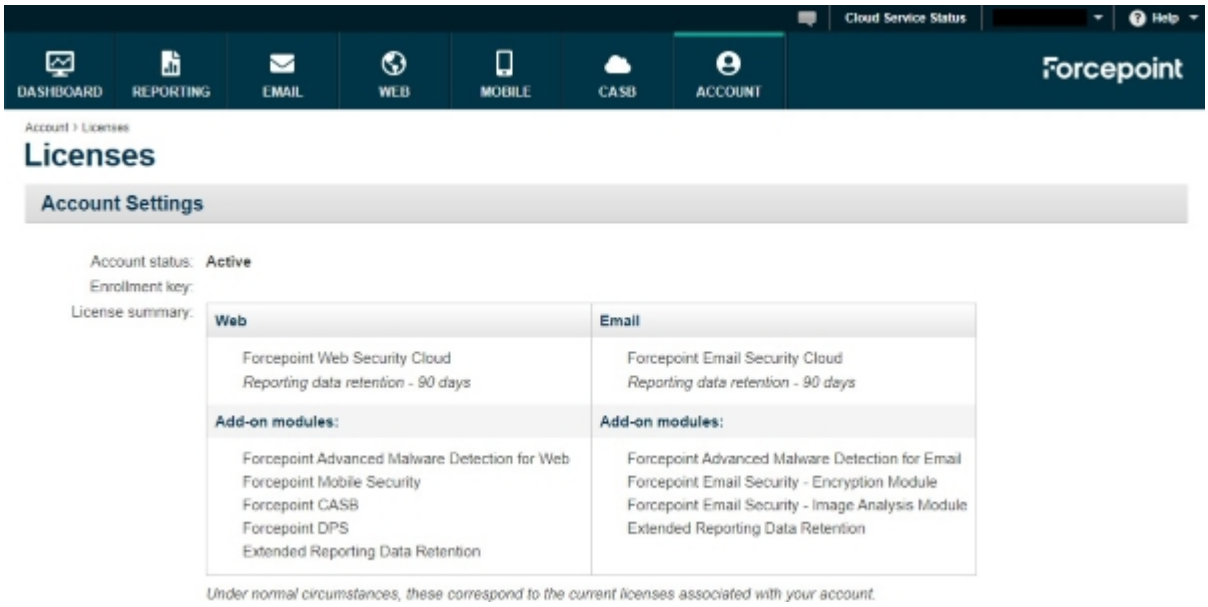
  You will receive a fulfillment email with the Forcepoint Web Security Cloud App Control license. Forcepoint CASB Ops personnel will enable the Web Security Cloud App capability on your relevant Forcepoint CASB instance.

For new Forcepoint Cloud Security Gateway customers

If you purchased the Forcepoint Cloud Security Gateway license, then you received the Forcepoint Web Security Cloud App Control and Forcepoint CASB licenses in the Forcepoint Cloud Security Gateway license. Check your Forcepoint Cloud Security Gateway fulfillment email to verify that these licenses are included.

Check your license on the Forcepoint Cloud Security Gateway Portal

After you receive the license, verify that the new Forcepoint CASB license is listed on the **Account > Licenses** page in the Forcepoint Cloud Security Gateway Portal:



After the license is active, configure the Forcepoint CASB and Forcepoint Web Security Cloud integration. For more information, see *Integrating Forcepoint CASB and Forcepoint Web Security Cloud*.

Related concepts
Integrating Forcepoint CASB and Forcepoint Web Security Cloud on page 21

Licensing for the Forcepoint CASB and Forcepoint DLP integration

For existing Forcepoint CASB and Forcepoint DLP customers

Forcepoint recommends that Forcepoint DLP customers migrate to Forcepoint Cloud Security Gateway, because it integrates the full Forcepoint CASB and Forcepoint Web Security Cloud functionality with Forcepoint DLP to provide unified data protection.

If you only want to integrate your existing Forcepoint DLP deployment with Forcepoint CASB, you can extend their DLP policies to sanctioned enterprise cloud applications, such as Office 365, G Suite, Box, Dropbox, Salesforce, and ServiceNow, via the DLP Cloud Applications or Forcepoint CASB with DLP Cloud Applications licenses.

- **Forcepoint DLP Cloud Applications**: Provides the ability to extend DLP policies to sanctioned cloud applications and supports API-based (offline) activity analysis, data discovery, and file sharing controls for supported cloud applications.
- **Forcepoint CASB with DLP Cloud Applications**: Provides the ability to control access and extend DLP policies to sanctioned cloud applications and supports both inline controls and API-based activity analysis,

data discovery, and file sharing controls for supported cloud applications. It includes integration with the cloud-hosted Data Protection Service.

Access to the Forcepoint CASB Portal is provided in both licenses.

Note

Both Forcepoint CASB and DLP Cloud Applications licenses are required to have the full set of capabilities covering API-based and real-time inline controls for sanctioned cloud applications.

After you purchase DLP Cloud Applications, you receive a fulfillment email that contains a new or updated DLP XML license file that includes DLP Cloud Applications.

If you are upgrading to Forcepoint DLP 8.8:

- Customers upgrading from any Forcepoint DLP version that supports DLP Cloud Applications to Forcepoint Web Security Cloud 8.8.1 must connect to Data Protection Service to support the DLP Cloud Proxy, DLP Cloud API, and Cloud Data Discovery channels. To connect to Data Protection Service, request a JSON file with tenant information from Forcepoint Support. If your Data Security Manager is already connected to Data Protection Service, you do not need a new file or any additional action. For more information, see *Connect Data Protection Service in the Forcepoint Security Manager*, and *Activate DLP Cloud Applications channels after a Forcepoint DLP upgrade*(both mentioned below).
- After upgrading to Forcepoint DLP 8.8.x and adding another license: If you activate Data Protection Service before updating the subscription on the Subscription page for the DLP Manager, the updated license information does not reach Data Protection Service until a new policy configuration is deployed. To resolve this issue, follow the instructions provided in Knowledge Base article 18998.

After you receive the license, you will enter the information in the Forcepoint Security Manager to connect Forcepoint DLP with Forcepoint CASB. For more information, see *Configuring the Forcepoint DLP and Forcepoint CASB connection*(mentioned below).

Related concepts

Connect Data Protection Service in the Forcepoint Security Manager on page 33

Related tasks

Activate DLP Cloud Applications channels after a Forcepoint DLP upgrade on page 38

Related information

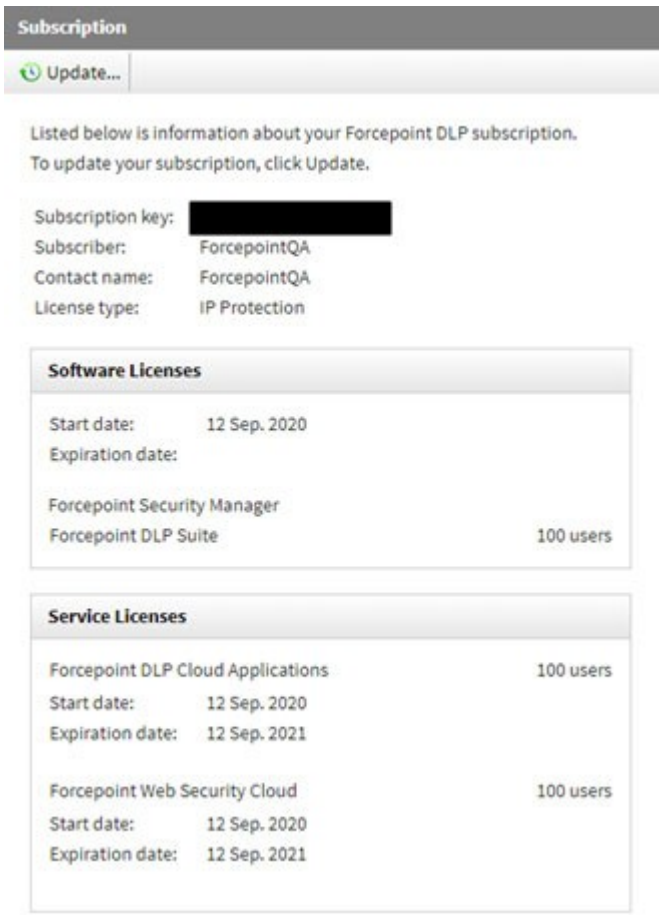
Configuring the Forcepoint DLP and Forcepoint CASB connection on page 33

For new Forcepoint Cloud Security Gateway customers

If you purchased the Forcepoint Cloud Security Gateway license, then you received both of these licenses in the Forcepoint Cloud Security Gateway license. Check your Forcepoint Cloud Security Gateway fulfillment email to verify that these licenses are included.

Check your licenses on the Forcepoint Security Manager

To check that the DLP Cloud Applications and Forcepoint Web Security Cloud licenses are active in the Forcepoint Security Manager, go to **DATA > Settings > General > Subscription**:



If the license is not shown on the Subscription page, update the license. For more information, see *Update a license in Forcepoint DLP*.

Related tasks

Update a license in Forcepoint DLP on page 14

Update a license in Forcepoint DLP

Before you begin

To update your license for this integration:

Steps

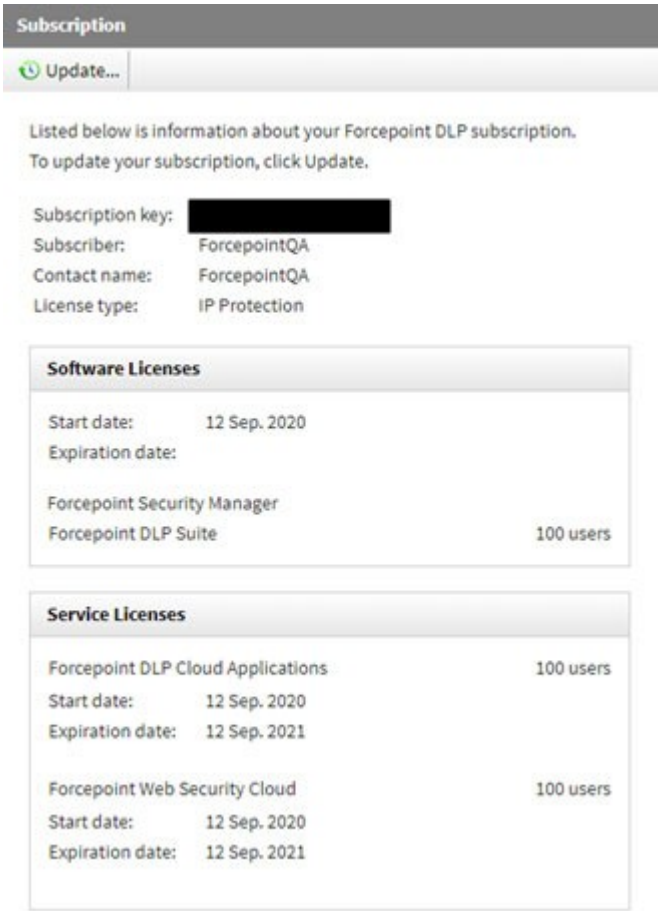
1) In the Forcepoint Security Manager, go to **DATA > Settings > General > Subscription**. The Subscription page displays your current license information.

2) Click **Update**. The Update Subscription window appears.

3) Click **Choose File**, and navigate to the DLP license XML file you received from Forcepoint.

4) Click **OK**. The DLP Manager validates the DLP license XML file, and displays a confirmation message.

5) Click **Continue**. The license information is now updated on the Subscription page.



6) To deploy the license update:
   a) Log out of the Forcepoint Security Manager.

b) Log in to the Forcepoint Security Manager.

c) Return to the Subscription page.

d) Click **Deploy**.

You can proceed with the required steps to connect and configure Data Protection Service.

Generate a Forcepoint CASB integration API key

To set up the Forcepoint CASB connections to Forcepoint DLP and Forcepoint Web Security Cloud, you need to generate an API access key and secret in the Forcepoint CASB management portal for each connection.

Important

Do not delete the auto-generated keys in Forcepoint CASB. If you delete these keys, Data Protection Services will no longer work and Forcepoint will need to re- provision the integration.

Generate the API key for Forcepoint DLP and Forcepoint CASB integration

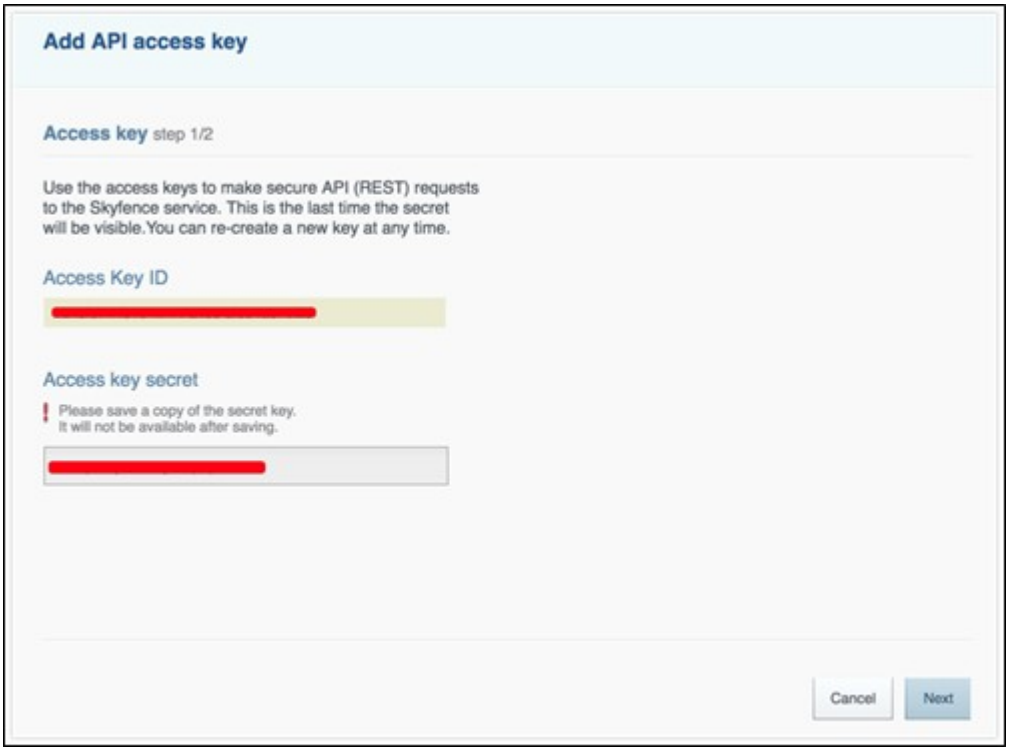
Steps

1) Log on to the Forcepoint CASB management portal.

2) Go to Settings > Access Management > API.

3) Under API Status, click Enable API Access.

4) Click Add API Access Key and write down the Access Key ID and Access key secret.



Note

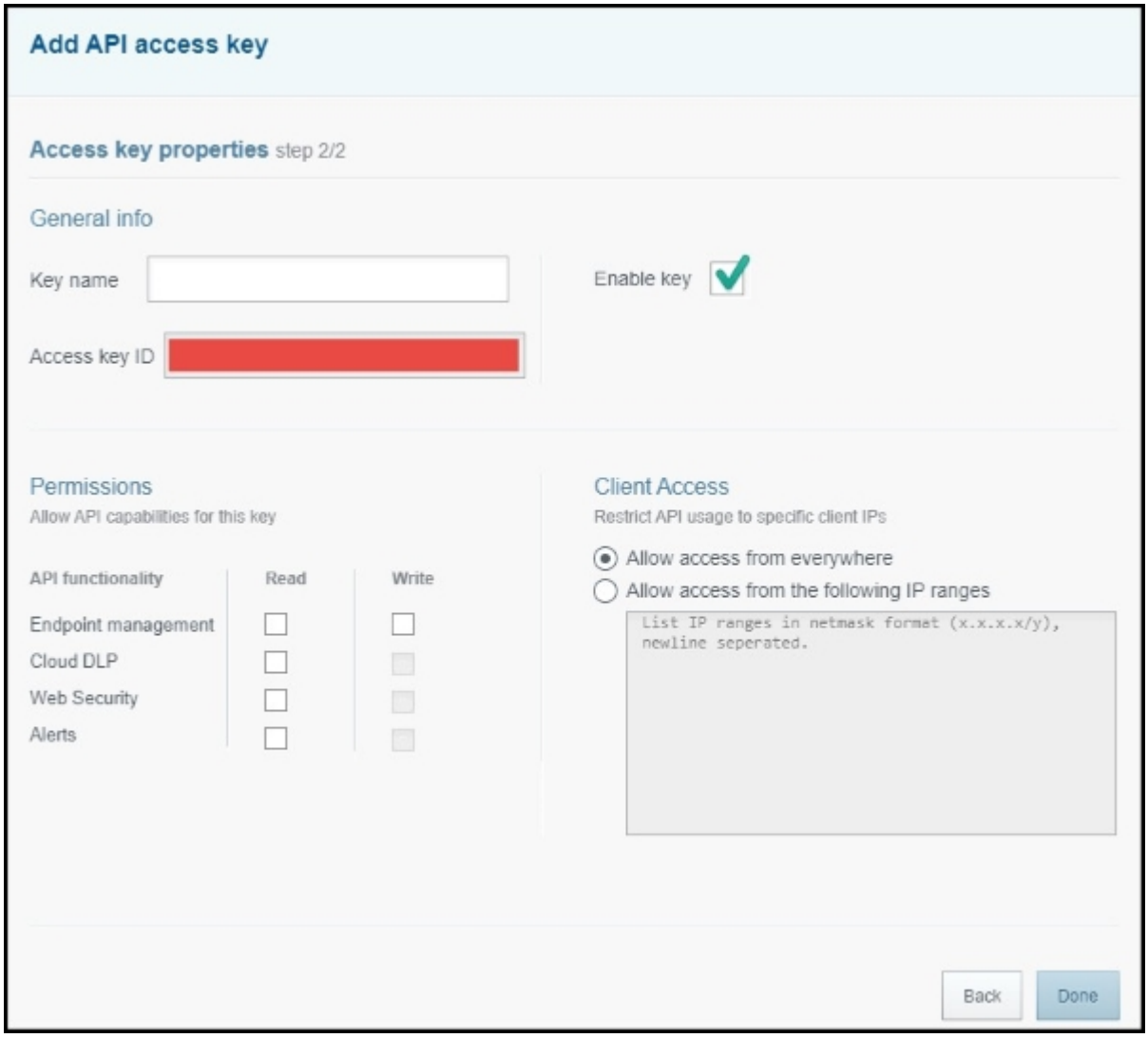
Save a copy of the access key secret. After you save the API access key, you will not be able to access the secret again.

5) Click **Next** and complete the following steps to configure the key:

   a) Type a new **Key name**.

   b) Make sure the **Enable key** option is checked.

c) Select the **Read** permission for **Cloud DLP**.



6) Click **Done**.

Use this API access key to configure your Forcepoint Web Security Cloud integration with Forcepoint CASB. See *Activate the connection with Forcepoint CASB in the Forcepoint Security Manager*(mentioned below).

Related tasks

Activate the connection with Forcepoint CASB in the Forcepoint Security Manager on page 35

Generate the API key for Forcepoint Web Security Cloud and Forcepoint CASB integration

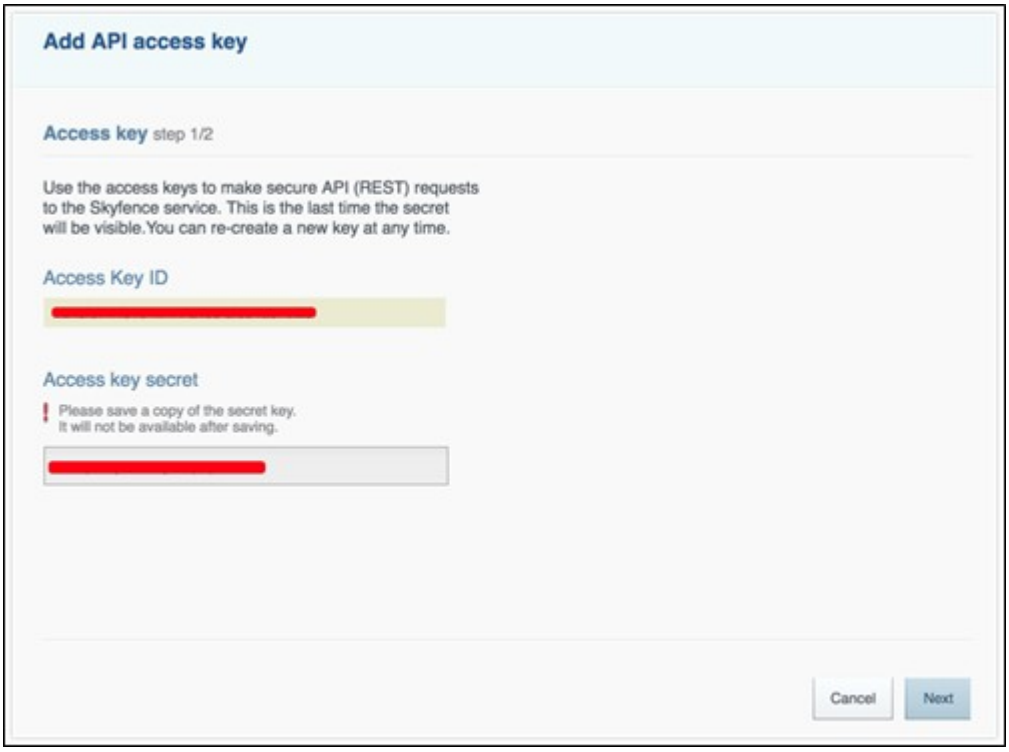
Steps

1) Log on to the Forcepoint CASB management portal.

2) Go to **Settings > Access Management > API**.

3) Under **API Status**, click **Enable API Access**.

4) Click **Add API Access Key** and write down the **Access Key ID** and **Access key secret**.



Note

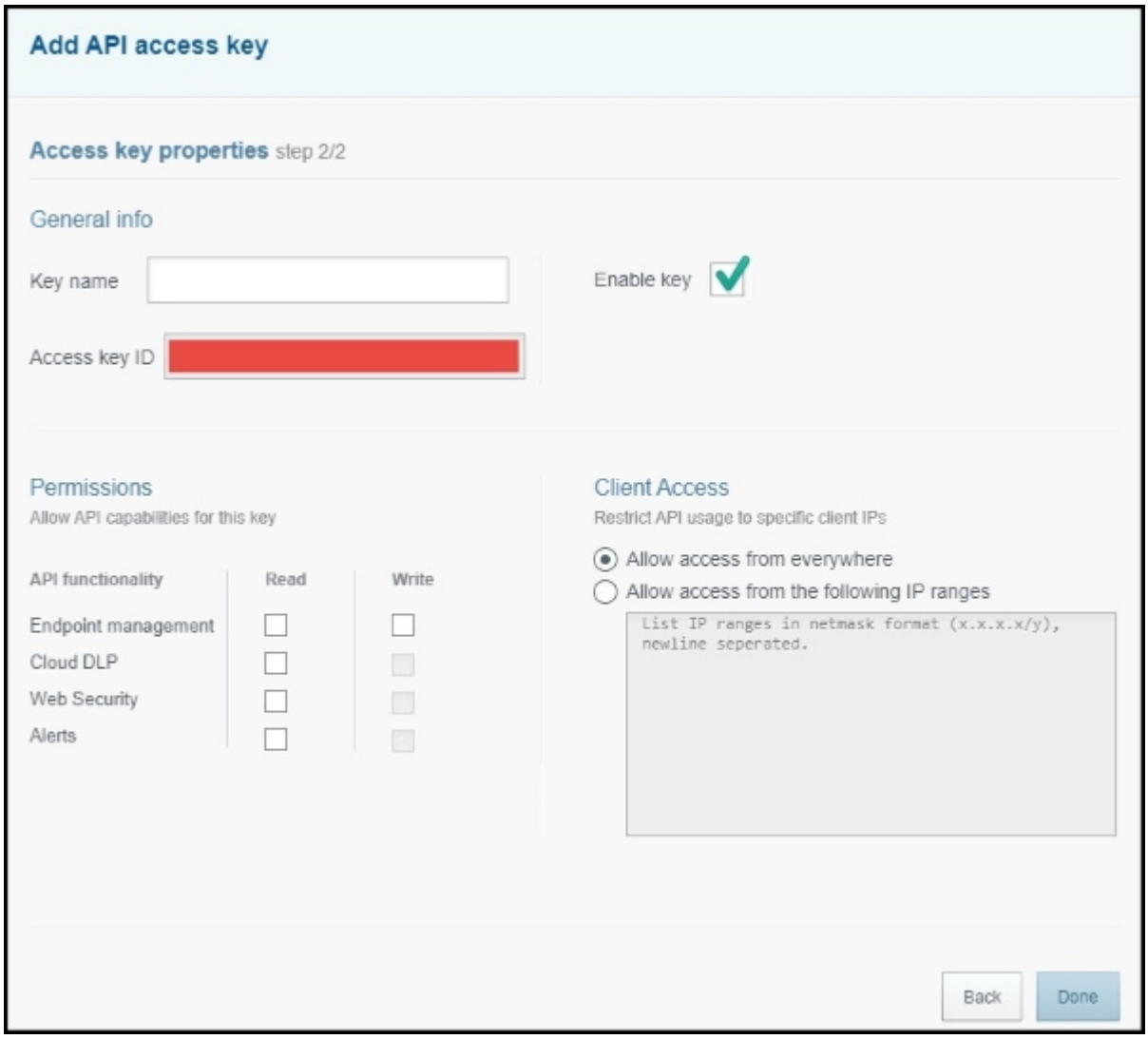
Save a copy of the access key secret. After you save the API access key, you will not be able to access the secret again.

5) Click **Next** and complete the following steps to configure the key:

   a) Type a new **Key name**.

   b) Make sure the **Enable key** option is checked.

c) Select the **Read** permission for **Web Security**.



6) Click **Done**.

Use this API access key to configure your Forcepoint Web Security Cloud integration with Forcepoint CASB. See *Configuring the Forcepoint Web Security Cloud and Forcepoint CASB connection* (mentioned below).

Related tasks

Configuring the Forcepoint Web Security Cloud and Forcepoint CASB connection on page 22

Chapter 3

Integrating Forcepoint CASB and Forcepoint Web Security Cloud

Contents

- General flow on page 21
- Configuring the Forcepoint Web Security Cloud and Forcepoint CASB connection on page 22
- Configure the protected cloud apps list on page 23
- Setting up and monitoring Forcepoint CASB policies on protected cloud apps on page 25
- Managing endpoint enrollment in Forcepoint CASB on page 27
- Verifying the integration on page 28

This chapter provides an overview of how to configure the integration between the Forcepoint Web Security Cloud and Forcepoint CASB. Customers can integrate these products either as part of a Forcepoint Cloud Security Gateway deployment, or if the two products are purchased separately (outside of a Forcepoint Cloud Security Gateway deployment).

The Forcepoint Web Security Cloud and Forcepoint CASB integration allows policy enforcement to forward requests made to the selected protected cloud apps (referred to as Assets by Forcepoint CASB) directly to Forcepoint CASB for:

- Real-time activity visibility
- Anomaly detection with user behavior analysis (UBA) and risk assessment
- Real-time mitigation
- Security information and event management (SIEM) and Active Directory (AD) integration

General flow

Before starting this integration, verify that you have purchased the required licenses.

- If you purchased Forcepoint Cloud Security Gateway, the Forcepoint Web Security Cloud App Control and Forcepoint CASB licenses are automatically included in the Forcepoint Cloud Security Gateway license.
- If you purchased Forcepoint Web Security Cloud and Forcepoint CASB separately, make sure that you have the two licenses (Forcepoint Web Security Cloud App Control and Forcepoint CASB) before you start the integration.

After you complete the purchase and receive your fulfillment email from Forcepoint, follow the steps below:

1) Log on to the Forcepoint Cloud Security Gateway portal using the credentials in your fulfillment email.

2) Fully set up and configure Forcepoint Cloud Security Gateway using the Setup Wizard.

3) Generate your API access key and secret in Forcepoint CASB. For more information, see *Generate a Forcepoint CASB integration API key* (mentioned below). If this information was provided in your fulfillment letter, then you do not need to create a new key.

4) Configure the connection in the Forcepoint Cloud Security Gateway Portal, also referred to as the cloud portal. For more information, see *Configuring the Forcepoint Web Security Cloud and Forcepoint CASB connection* (mentioned below).

5) Configure the protected cloud apps list in the cloud portal. For more information, see *Configure the protected cloud apps list* (mentioned below).

6) View and configure Forcepoint CASB policies that relate to protected cloud apps. For more information, see *Setting up and monitoring Forcepoint CASB policies on protected cloud apps* (mentioned below).

Related concepts

Generate a Forcepoint CASB integration API key on page 15

Related tasks

Configuring the Forcepoint Web Security Cloud and Forcepoint CASB connection on page 22
Configure the protected cloud apps list on page 23
Setting up and monitoring Forcepoint CASB policies on protected cloud apps on page 25

Configuring the Forcepoint Web Security Cloud and Forcepoint CASB connection

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

To protect cloud app usage via Forcepoint CASB:

Steps

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

2) Set the **Enable connection with Forcepoint CASB** toggle switch to **ON**.

3) Enter the connection details:
   - The **Access key ID** created in Forcepoint CASB.
   - The **Access key secret** created in Forcepoint CASB.
     For more information about creating the key ID and secret, see *Generate theAPI key for Forcepoint Web Security Cloud and Forcepoint CASB integration* (mentioned below).
   - Service URL:
     - For the US Forcepoint CASB portal: **https://my.skyfence.com**
     - For the EU Forcepoint CASB portal: **https://my-eu1.skyfence.com**
     - For the UK Forcepoint CASB portal: **https://my-uk.skyfence.com**
       When you enter the Service URL, make sure you use **https** instead of http and do not add a slash (/) to the end. If you include the slash, the Service URL will not work correctly.

4) Click **Connect**.

Related tasks
Generate the API key for Forcepoint Web Security Cloud and Forcepoint CASB integration on page 18

Signing in to Forcepoint CASB from the Forcepoint Cloud Security Gateway Portal

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

To log on to Forcepoint CASB from the Forcepoint Cloud Security Gateway Portal, click the **CASB** option available in the toolbar. Users with account level **Modify configuration** permissions are logged on to the portal. (See Configuring permissions in the Forcepoint Cloud Security Gateway Portal Help.) All other users are required to provide login credentials to access the portal.

If you encounter an authorization error when you try to access Forcepoint CASB from the Forcepoint Cloud Security Gateway Portal, make sure that the account logged on to the portal has an account in Forcepoint CASB with the same email address.

Configure the protected cloud apps list

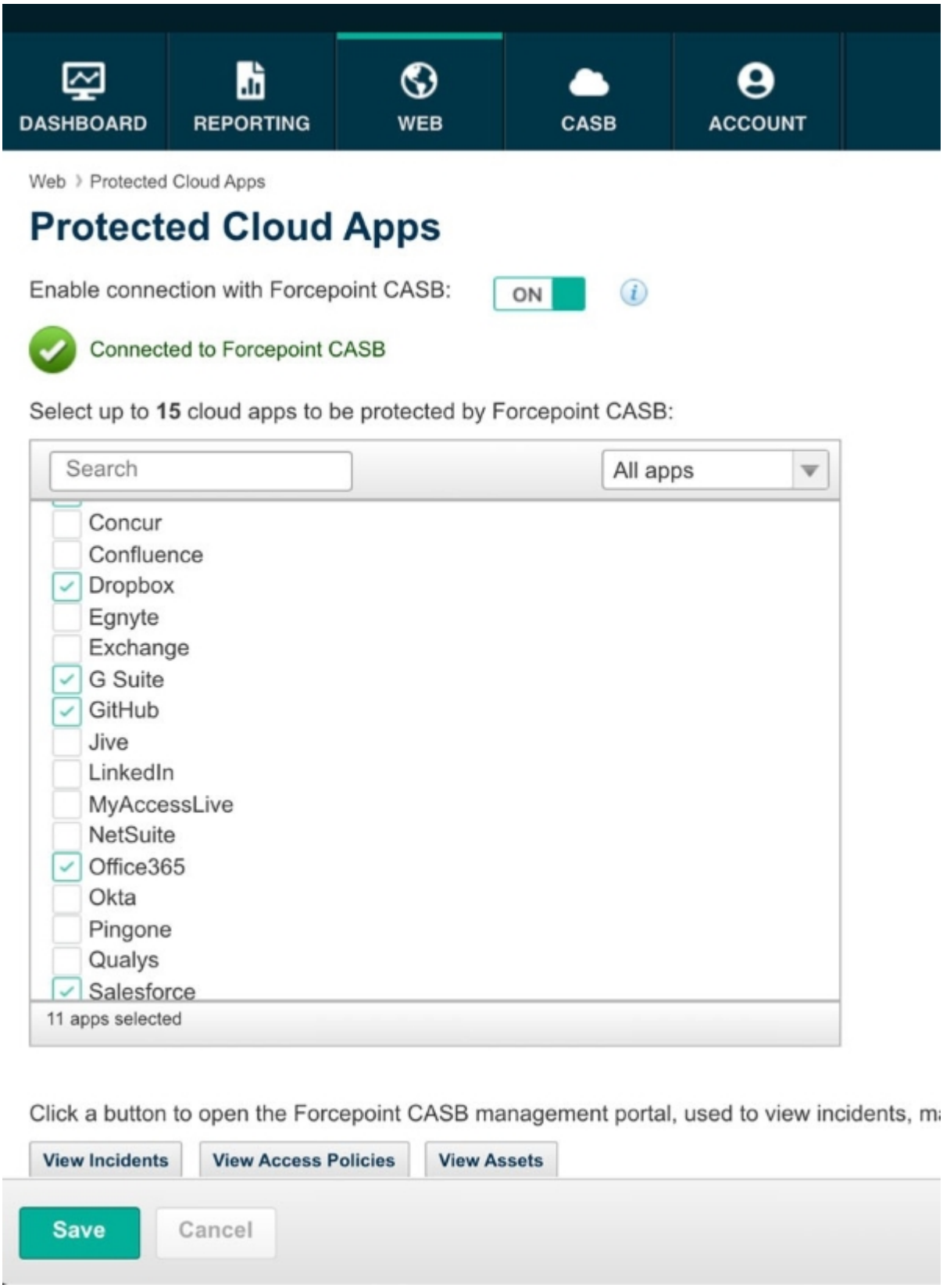
Steps

1) In the cloud portal, go to **Web > Settings > Protected Cloud Apps**.

2) From the list of cloud apps, select which apps to protect in Forcepoint CASB. You can select up to the maximum number of apps that your CASB license covers.

Use the scrollbar, or begin typing the name of an app in the Search field. To view only the apps that are currently selected, set the search menu drop-down menu to **Selected apps**.

This list of cloud apps is populated based on the available cloud apps (assets) in Forcepoint CASB. If an asset is updated, added, or removed in the Forcepoint CASB portal, the change is reflected in this list.



3) Click **Save**.

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

Note

Forwarding the selected app requests from the endpoint machines to the cloud proxy is handled like any other traffic. This is based on your Forcepoint Web Security Cloud implementation.

Setting up and monitoring Forcepoint CASB policies on protected cloud apps

Forcepoint CASB has a few preset dashboards for setting and customizing Forcepoint CASB predefined policies on the protected cloud apps, in addition to an Incidents reporting dashboard. These dashboards can be accessed directly from the Forcepoint Cloud Security Gateway Portal.

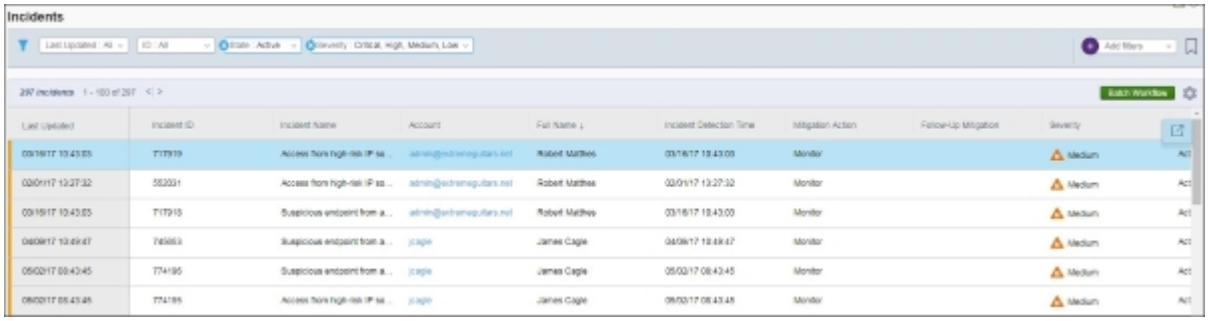
To access these Forcepoint CASB dashboards from the cloud portal:

1) Go to **Web > Settings > Protected Cloud Apps**.

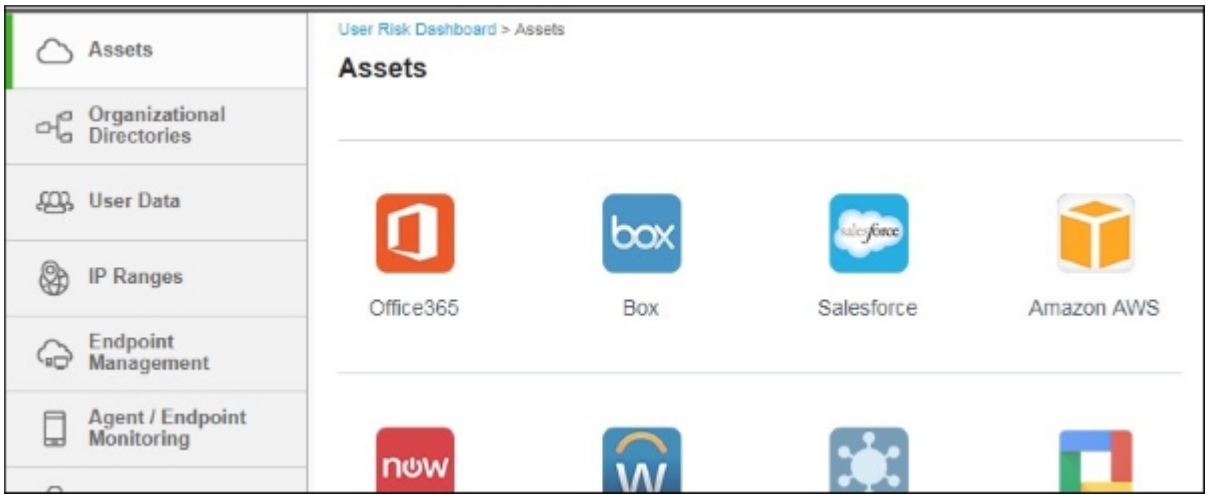
2) Click one of the buttons beneath the app selection box to open the relevant page in Forcepoint CASB:

- **View Incidents**: Open the Forcepoint CASB incident log (**Audit & Protect > Incidents**) to view incidents such as alerts and policy violations.
  Forcepoint CASB 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.

  You can view the Incidents log and filter the results according to various parameters. Forcepoint CASB provides many different ways to view incidents, including by user and by asset.

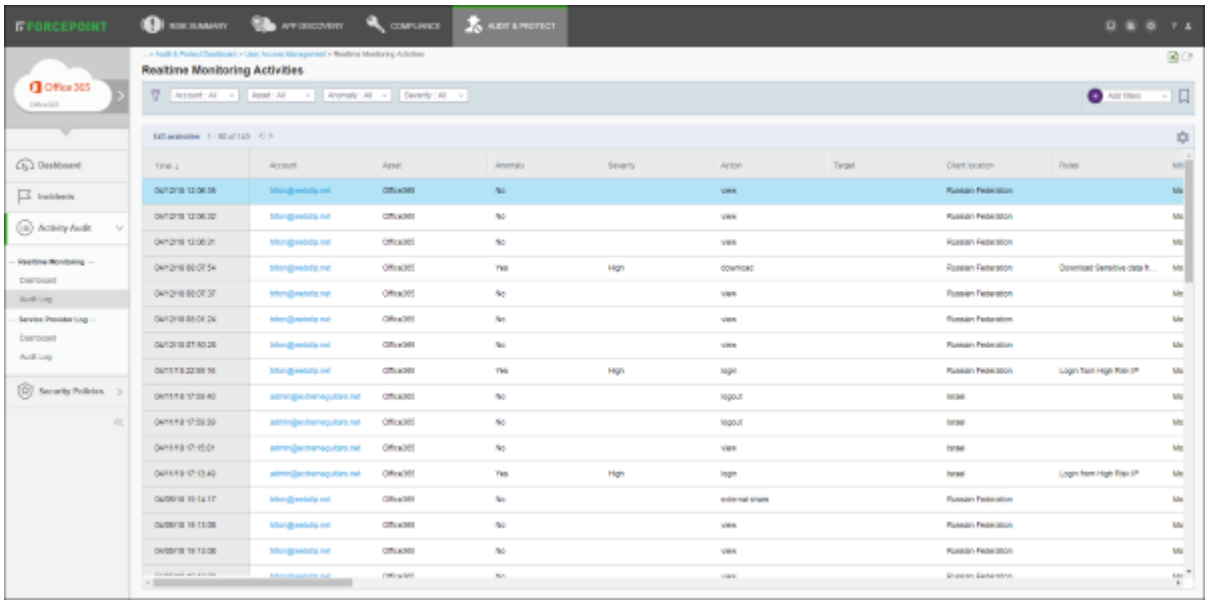


- **View Access Policies**: Manage and configure user access policies for cloud apps within your Forcepoint CASB account. This button opens **Audit & Protect > Security Policies > User Access Management** (per selected asset).
  You can configure access policies to managed assets without needing to rely on the native permission systems for the app, which in some cases can be limited or insecure. Forcepoint CASB includes several pre-configured simple access policies that can be enabled and in some cases further configured.
- **View Assets**: Manage settings for the cloud apps protected by Forcepoint CASB. This button opens **Settings > Assets**.
  The Assets page is a Settings dashboard where you can add more assets (also known as apps) to monitor with Forcepoint CASB, edit an asset's configuration, or remove an asset.

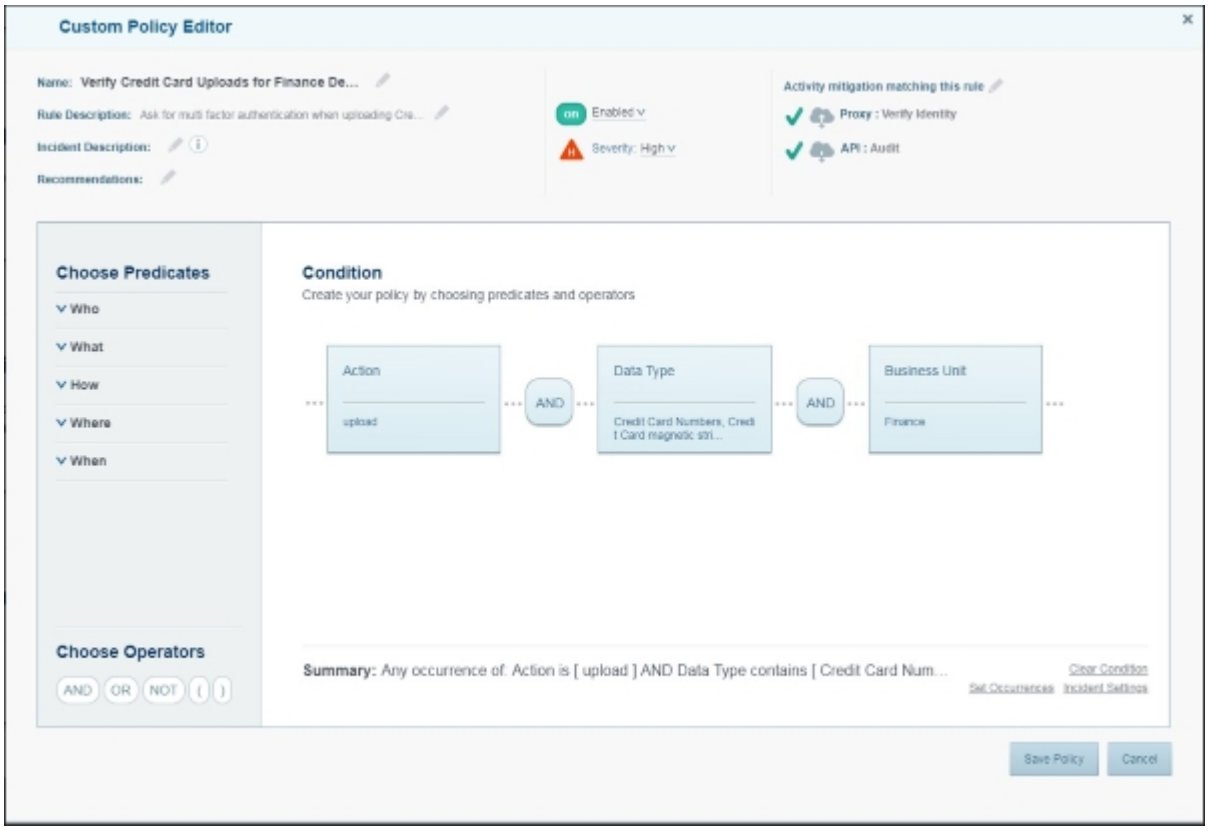


In addition to those quick access Forcepoint CASB dashboards available from the Forcepoint Cloud Security Gateway portal, more dashboards are available from the Forcepoint CASB management portal, including:

- **Audit & Protect > Activity Audit > Realtime Monitoring > Audit Log**(available for all assets or a selected asset):
  For protected apps, Forcepoint CASB can identify activity details such as data object, source locations, and actions (e.g., password change or data modification). All the activities and their details can be seen in this dashboard. Filtered activity lists can be exported for further analysis and compliance.



- **Audit & Protect > Security Policies > Custom Policy Editor** (per selected asset):
  Forcepoint CASB gives you the ability to create custom policies to be triggered by granularly defined custom conditions. These conditions consist of configured generic and asset-specific parameters (predicates) separated by Boolean operators (AND / OR / NOT).



Managing endpoint enrollment in Forcepoint CASB

The following Forcepoint CASB features require that Forcepoint CASB knows which devices are managed by the organization:

- The Endpoint Management Access Policy
- Custom policies based on managed devices
- An Analytics dashboard filter that displays access from managed devices
- Analytics activity logs that 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.

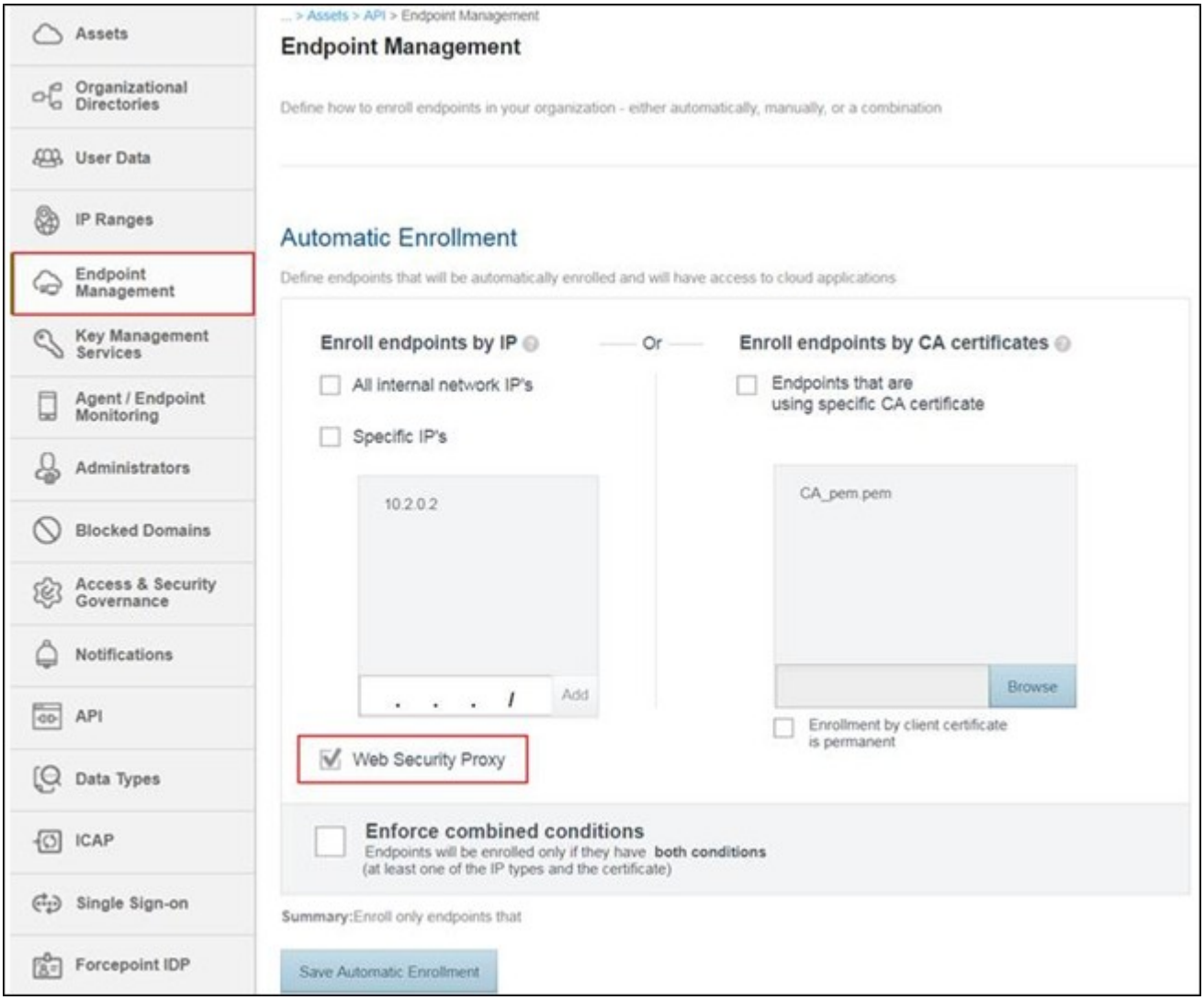
You can configure the enrollment criteria that define how Forcepoint CASB determines whether an endpoint is organizationally managed.

With the Forcepoint Web Security Cloud and Forcepoint CASB integration, a new option called **Web Security Proxy** is available in Forcepoint CASB:

Steps

1) In the Forcepoint CASB management portal, go to **Settings > Endpoints > Endpoint Management**.

2) Under the **Automatic Enrollment** section, select **Web Security Proxy**.



With this option enabled, Forcepoint CASB regards all traffic coming from Forcepoint Web Security Cloud as coming from managed devices.

Verifying the integration

When the Forcepoint Web Security Cloud and Forcepoint CASB integration is completed and working correctly, user requests to protected cloud apps are forwarded to CASB by policy enforcement. These requests generate log data that can then be viewed in the Report Center.

To confirm that transactions have been forwarded from cloud web to Forcepoint CASB, use the **Reporting > Report Center > Transaction Viewer**. In the **Attributes** list, under **Cloud Apps**, drag **Cloud App Forwarded** to the Filters field and define the filter to include records with that attribute. See the Cloud Security Portal Admin Guide for details on Using the Transaction Viewer to define continue defining your report.

The results will display all of the user requests that were forwarded to Forcepoint CASB for enforcement.

Chapter 4

Integrating Forcepoint DLP and Forcepoint CASB

Contents

- General flow on page 30
- Configuring the Forcepoint DLP and Forcepoint CASB connection on page 33
- Configure single sign-on with Forcepoint CASB on page 38
- Creating and configuring cloud applications on page 39
- Configuring the Cloud API connection on page 42
- Configuring Forcepoint DLP policies for CASB cloud application assets on page 45
- View Forcepoint DLP incidents in the Forcepoint Security Manager on page 52
- View incident information in Forcepoint CASB on page 53
- Configuring Cloud Data Discovery (data at rest) settings on page 54

This chapter provides an overview of how to configure the integration between Forcepoint DLP and Forcepoint CASB, and how to configure DLP policies for sanctioned cloud applications.

The integration is achieved via multi-directional communication between the customer-deployed Forcepoint Security Manager server, the cloud-hosted Data Protection Service and DLP agents, and Forcepoint CASB cloud infrastructure. Within this chapter and the Forcepoint Security Manager user interface, Forcepoint uses the following terms to describe the different interactions with sanctioned cloud applications.

- **DLP Cloud API** (available from Forcepoint DLP 8.5.0): Leveraging an API connection made to the supported cloud application, this option provides near real-time activity analysis soon after the operation occurs. For example, uploads, downloads, and sharing activity.
- **Cloud Data Discovery**, also known as data at rest (DAR) (available since Forcepoint DLP 8.6.0): Data discovery and remediation of sensitive data at rest and data shared within sanctioned cloud applications. This capability also leverages an API connection to each supported cloud application.
- **DLP Cloud Proxy** (available from Forcepoint DLP 8.7.1): For cloud applications that connect to Forcepoint CASB through a proxy connection, this option provides immediate, inline activity analysis as the activity occurs.

DLP Cloud API protection enables action plans that occur shortly after an operation, such as placing a file in quarantine. DLP Cloud Proxy protection enables real-time DLP scanning of operations and content moving to or from the cloud, with real-time mitigation, such as blocking. To this end, as of Forcepoint DLP 8.7.1, a new resource type is available, Cloud Applications. This means that rules and action plans can be configured to apply to specific applications, such as Box.

Note

When Forcepoint Web Security Cloud is integrated with Forcepoint CASB and Forcepoint DLP, a user request that includes both a request to a protected cloud application and potential data loss is forwarded by the cloud proxy to Forcepoint CASB. Forcepoint CASB then forwards it to Forcepoint DLP.

General flow

To fully integrate Forcepoint DLP and Forcepoint CASB, complete the following steps:

Steps

1) Ensure the Forcepoint Security Manager has the DLP Cloud Applications license activated. If you purchased the Forcepoint Cloud Security Gateway license, the DLP Cloud Applications license is included. For more information, see *License Information* (mentioned below).

2) Generate your API access key and secret in Forcepoint CASB. For more information, see *Generate a Forcepoint CASB integration API key* (mentioned below).

3) Ensure your network is configured to enable connectivity between the Forcepoint Security Manager and the Forcepoint CASB service. For more information, see *Firewall and network access prerequisites* (mentioned below).

4) Configure the connection between Forcepoint DLP and Forcepoint CASB in the Forcepoint Security Manager using the API access key and secret. For more information, see *Activate the connection with Forcepoint CASB in the Forcepoint Security Manager* (mentioned below).

5) Connect to Data Protection Service. To connect between the DLP Manager and Data Protection Service, upload the JSON file received in your fulfillment email to the Data Protection Service tab. For more information, see *Connect Data Protection Service in the Forcepoint Security Manager* (mentioned below).

6) Create user accounts for single sign-on with Forcepoint CASB. For more information, see *Configure single sign-on with Forcepoint CASB* (mentioned below).

7) Configure DLP Cloud Proxy:

   a) For each new or existing Forcepoint CASB asset you want to apply DLP policies to, you need to configure a Forcepoint CASB quick policy to ensure that the CASB Gateway sends transactions to Forcepoint DLP for analysis. For more information, see *Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage* (mentioned below).

   b) Check that the assets are shown in the Forcepoint Security Manager with an **OK** status. For more information, see *View the list of cloud applications* (mentioned below).

   c) Configure one or more DLP rules for DLP Cloud Applications (**DATA Policy Management > Manage DLP Policies > Policy rule > Destination > DLP Cloud Applications).**For more information, see *Configure DLP policies for cloud applications in the Forcepoint Security Manager*, page (mentioned below).

   d) Configure one or more DLP action plans using cloud application resources. For more information, see *Configure an action plan with cloud application resources* (mentioned below).

8) Configure DLP Cloud API:

   a) For DLP Cloud API setup, Forcepoint recommends that you configure existing cloud applications or add new cloud applications through the Forcepoint Security Manager as this automatically creates and configures Forcepoint CASB cloud application assets. For more information, see *Add a cloud application in the Forcepoint Security Manager* (mentioned below).

   Alternatively, you can create and configure a new Forcepoint CASB asset in Forcepoint CASB, which will then sync with the Forcepoint Security Manager. For more information, see *Add an asset in Forcepoint CASB* and *Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage* (mentioned below).

   b) Check that the Forcepoint CASB assets are shown as cloud applications in the Forcepoint Security Manager with an OK status. For more information, see *View the list of cloud applications* (mentioned below).

   c) Configure DLP Cloud API policies for cloud applications in the Forcepoint Security Manager (**DATA > Policy Management > Manage DLP Policies > Policy rule > Destination > DLP Cloud Applications**). For more information, see *Configure DLP policies for cloud applications in the Forcepoint Security Manager* (mentioned below).

   d) Configure one or more DLP action plans using DLP Cloud API operations. For more information, see *Configure an action plan with cloud application resources* (mentioned below).

   Important

   If you upgraded to Forcepoint DLP 8.8.1 and already have a DLP Cloud Applications license supporting DLP Cloud API and Cloud Data Discovery, make sure to connect to Data Protection Service as described in *Activate DLP Cloud Applications channels after a Forcepoint DLP upgrade* (mentioned below).

9) Configure Cloud Data Discovery:

   a) For Cloud Data Discovery setup, Forcepoint recommends that you configure existing cloud applications or add new cloud applications through the Forcepoint Security Manager as this automatically creates and configures Forcepoint CASB cloud application assets. For more information, see *Add a cloud application in the Forcepoint Security Manager* (mentioned below).

   Alternatively, you can create and configure a new Forcepoint CASB asset in Forcepoint CASB, which will then sync with the Forcepoint Security Manager. For more information, see *Add an asset in Forcepoint CASB* and *Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage* (mentioned below).

   b) Check that the Forcepoint CASB assets are shown as cloud applications in the Forcepoint Security Manager with an OK status. For more information, see *View the list of cloud applications* (mentioned below).

   c) Enable Cloud Data Discovery. Forcepoint recommends that you enable Cloud Data Discovery in the Forcepoint Security Manager. Alternatively, you can configure data at rest discovery in Forcepoint CASB. For more information, see *Enable Cloud Data Discovery in the Forcepoint Security Manager* and *Configure data at rest discovery in Forcepoint CASB* (mentioned below).

   d) Add a Cloud Data Discovery policy. Before you create a Cloud Data Discovery scan, make sure that you have created at least one Discovery Policy in the Forcepoint Security Manager (**Policy Management > Discovery Policies > Manage Policies**). For more information, see Creating Discovery Policies in the Forcepoint DLP Administrator Help

e) Add a Cloud Data Discovery scan. Forcepoint recommends that you add and configure a Cloud Data Discovery scan in the Forcepoint Security Manager. Alternatively, you can configure a data classification scan policy in Forcepoint CASB. For more information, see *Add a Cloud Data Discovery scan in the Forcepoint Security Manager* (mentioned below).

Important

If you upgraded to Forcepoint DLP 8.8.1 and already have a DLP Cloud Applications license supporting DLP Cloud API and Cloud Data Discovery, make sure to connect to Data Protection Service as described in *Activate DLP Cloud Applications channels after a Forcepoint DLP upgrade* (mentioned below).

10) View Forcepoint DLP incident details in the Forcepoint Security Manager and Forcepoint CASB:

a) View Forcepoint DLP incident information in the Forcepoint Security Manager. For more information, see *View Forcepoint DLP incidents in the Forcepoint Security Manager* (mentioned below).

b) View additional incident information in Forcepoint CASB. For more information, see *View incident information in Forcepoint CASB* (mentioned below).

Related concepts

License Information on page 9
Generate a Forcepoint CASB integration API key on page 15
Firewall and network access prerequisites on page 33
Connect Data Protection Service in the Forcepoint Security Manager on page 33
Configure single sign-on with Forcepoint CASB on page 38
View the list of cloud applications on page 39
View Forcepoint DLP incidents in the Forcepoint Security Manager on page 52
View incident information in Forcepoint CASB on page 53

Related tasks

Activate the connection with Forcepoint CASB in the Forcepoint Security Manager on page 35
Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage on page 45
Configure DLP policies for cloud applications in the Forcepoint Security Manager on page 48
Configure an action plan with cloud application resources on page 50
Add a cloud application in the Forcepoint Security Manager on page 40
Add an asset in Forcepoint CASB on page 41
Activate DLP Cloud Applications channels after a Forcepoint DLP upgrade on page 38
Enable Cloud Data Discovery in the Forcepoint Security Manager on page 54
Configure data at rest discovery in Forcepoint CASB on page 56
Add a Cloud Data Discovery scan in the Forcepoint Security Manager on page 57

Configuring the Forcepoint DLP and Forcepoint CASB connection

Firewall and network access prerequisites

Forcepoint CASB and Forcepoint DLP integration is based on the following HTTPS network connections:

- Forcepoint Security Manager to the Forcepoint CASB management portal
- Forcepoint Security Manager to DLP Service / DLP Cloud Proxy
- Forcepoint Security Manager to DLP Agent / CASB Cloud App Scanners

If the Forcepoint Security Manager is behind your network firewall or any other network access control system, you must allow connections on port 443.

If you want to allow specific Forcepoint CASB portal IP addresses for security reasons, see the list of IP addresses in Knowledge Base article 19105.

Connect Data Protection Service in the Forcepoint Security Manager

To benefit from the integration of the cloud channels with Forcepoint CASB, you must first connect the DLP Manager to Data Protection Service, which is responsible for the enforcement of DLP policies on cloud web traffic and cloud applications.

In the DATA module of the Forcepoint Security Manager, use the Data Protection Service tab of the **Settings > General > Services** page to connect to Data Protection Service. Uploading tenant information is part of the connection process.

Data Protection Service:

- Enables enforcement of DLP rules that protect cloud applications, with Forcepoint CASB integration for all cloud channels (DLP Cloud Proxy, DLP Cloud API, and Data Discovery).
- Protects data over web traffic through integration with Forcepoint Web Security Cloud.

First, Data Protection Service must be connected. This is done by uploading the Data Protection Service JSON file either received in the fulfillment email as part of the onboarding process or requested from Forcepoint Technical Support.

Important

If you upgraded to Forcepoint DLP 8.8.1 and added another license, you must update the subscription on the Subscriptions page of the DLP Manager before activating Data Protection Service, or the new license information will not reach Data Protection Service until a new policy configuration is deployed. In the event you have connected Data Protection Service before updating the subscription, you can resolve the issue by following the instructions in this article.

1) Click **Select File**, and in the dialog box that appears, click **Choose File**. Browse to the JSON file you received from Forcepoint, and then click **OK**. The file is uploaded to the server, and the information begins to appear in the Connection area of the Data Protection Service tab.

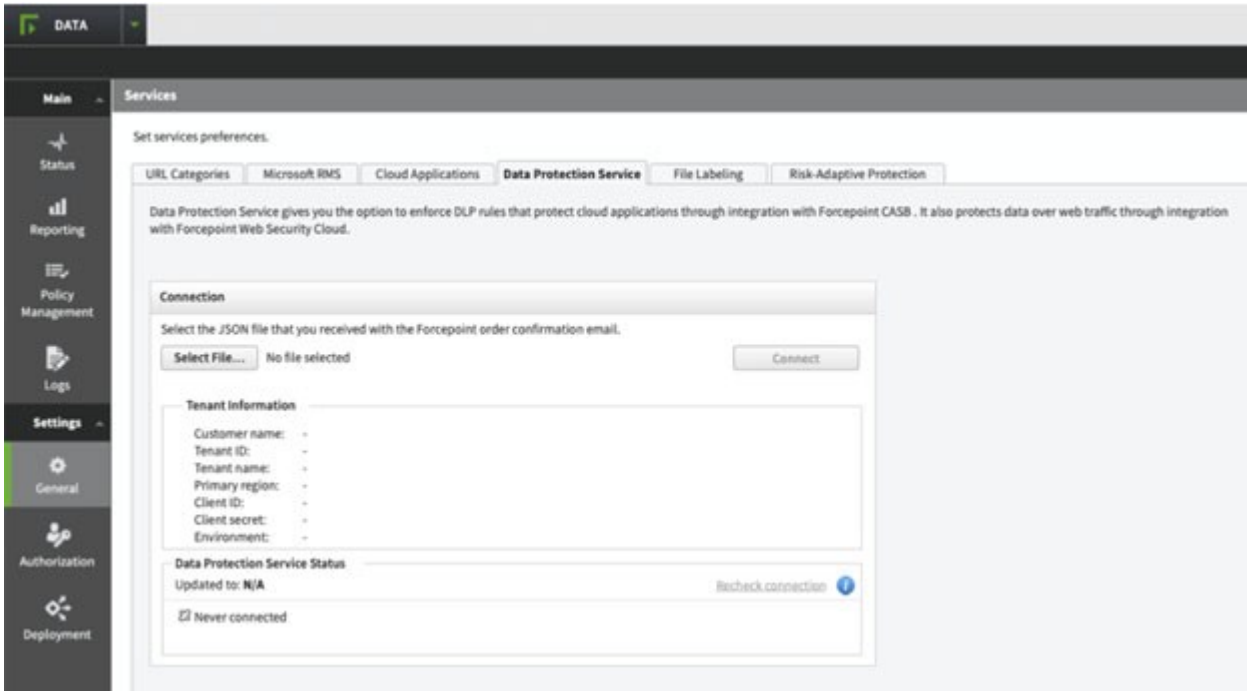
2) Verify that the correct **Customer Name** is shown in the Forcepoint Security Manager. If the Customer Name is incorrect, contact Forcepoint Technical Support.

3) Click **Connect** to establish the connection with Data Protection Service.

4) Click **OK** at the bottom of the screen to complete the process.

When the connection is active, the **Connect** button turns into a **Disconnect** button, enabling disconnection of Data Protection Service from Forcepoint DLP.

In the Data Protection Service Status area, upon successful connection, the status is marked as “Connected successfully”, the time and date of the connection is displayed, and the **Recheck connection link** is enabled. This link is used to check the connection status in the event of problems. If an error is returned upon checking the connection, the status is listed as “Failed to connect”.



Error handling

- If Data Protection Service shows the status “Failed to connect”, the module is temporarily unavailable. Click **Connect** or **Recheck Connection** to try to connect again. If the problem continues, contact Forcepoint Technical Support.
- If the JSON file is uploaded for the first time, and when you click **Connect** the connection fails, the status shown is “Never connected”. This is because the Forcepoint Security Manager has never successfully connected to the Data Protection Service. In this case, it is probable that a Data Protection Service was not created. Contact Forcepoint Technical Support for assistance.
- If you receive the following message in the Data Protection Service Status area:
  This service is not connected to Forcepoint CASB. Incident reporting and policy enforcement will be affected for cloud channels. See “Explain this page” for more information.

  This means that there is a connection issue, and DLP Cloud API and Cloud Data Discovery channels will not enforce DLP policies, and the DLP Cloud Proxy channel might not report incidents to the Forcepoint Security

Manager. See Viewing Deployment Status in the Forcepoint DLP Administrator Guide for more information on error handling.

- When you contact Forcepoint Technical Support, you can share the following files to help troubleshoot the issue:
  - %DSS_HOME%tomcat\logs\dlp\dlp-all.log
  - %DSS_HOME%mediator\logs\mediator.out

  The default location for %DSS_HOME% is C:\Program Files (x86)\Websense\Data Security\. If you cannot find these files at the default location, check with your Forcepoint Security Manager administrator.

Activate the connection with Forcepoint CASB in the Forcepoint Security Manager

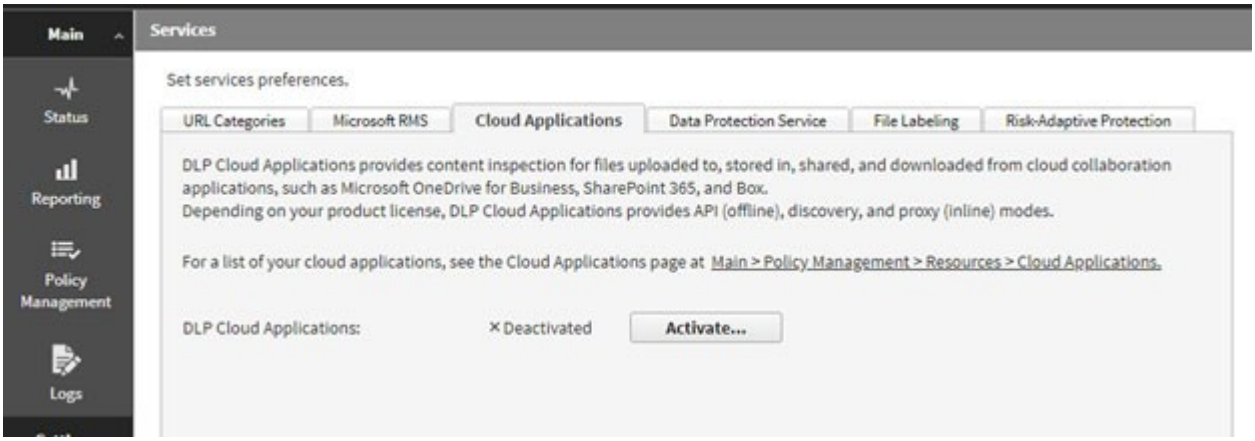
Use the **Cloud Applications** tab of the **Settings > General > Services** page to connect, disconnect, and configure the CASB service.

Steps

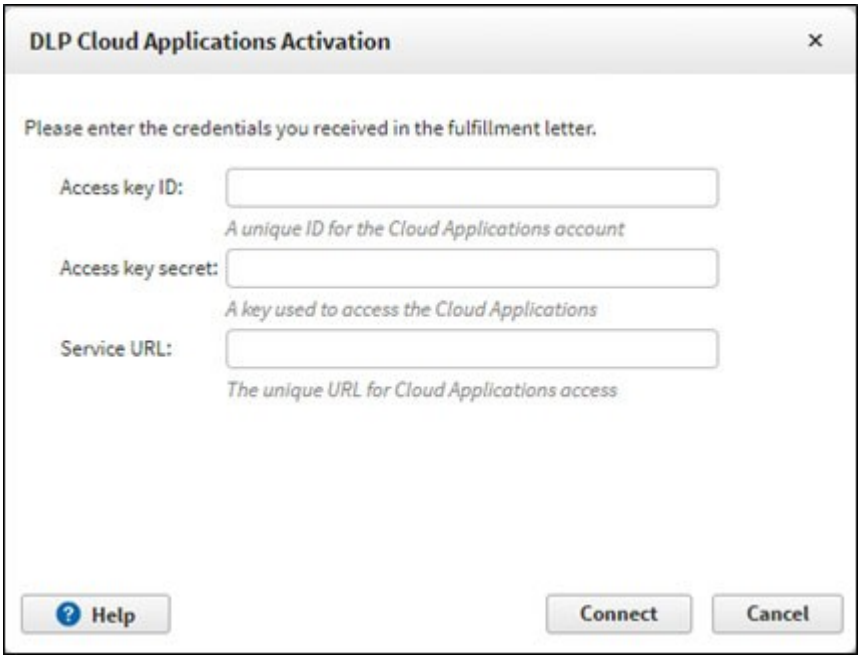
1) In the Forcepoint Security Manager, go to **DATA > Settings > General > Services**, then select the **Cloud Applications** tab.

Note

The Cloud Applications tab is visible only if the Forcepoint DLP Cloud Applications license appears on the Subscription page.



2) Click **Activate**. The **DLP Cloud Applications Activation** dialog box is displayed.



3) Enter the connection details:

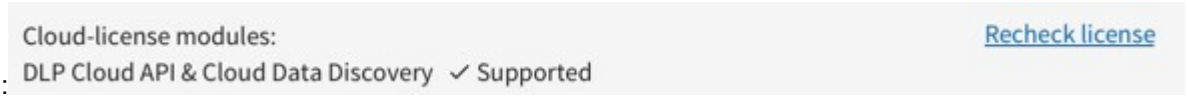
- The **Access key ID** created in Forcepoint CASB.
- The **Access key secret** created in Forcepoint CASB.
  For more information about creating the key ID and secret, see *Generate the API key for Forcepoint DLP and Forcepoint CASB integration* (mentioned below).
- Service URL:
  - For the US Forcepoint CASB portal: **https://my.skyfence.com**
  - For the EU Forcepoint CASB portal: **https://my-eu1.skyfence.com**
  - For the UK Forcepoint CASB portal: **https://my-uk.skyfence.com**

When you enter the Service URL, make sure you use **https** instead of http and do not add a slash (/) to the end. If you include the slash, the Service URL will not work correctly.

4) Click **OK**. The connection process is initiated. This might take some time to complete.

5) To deploy all the configured changes, click **Deploy**.

6) Upon successful activation, a list of supported modules is displayed:

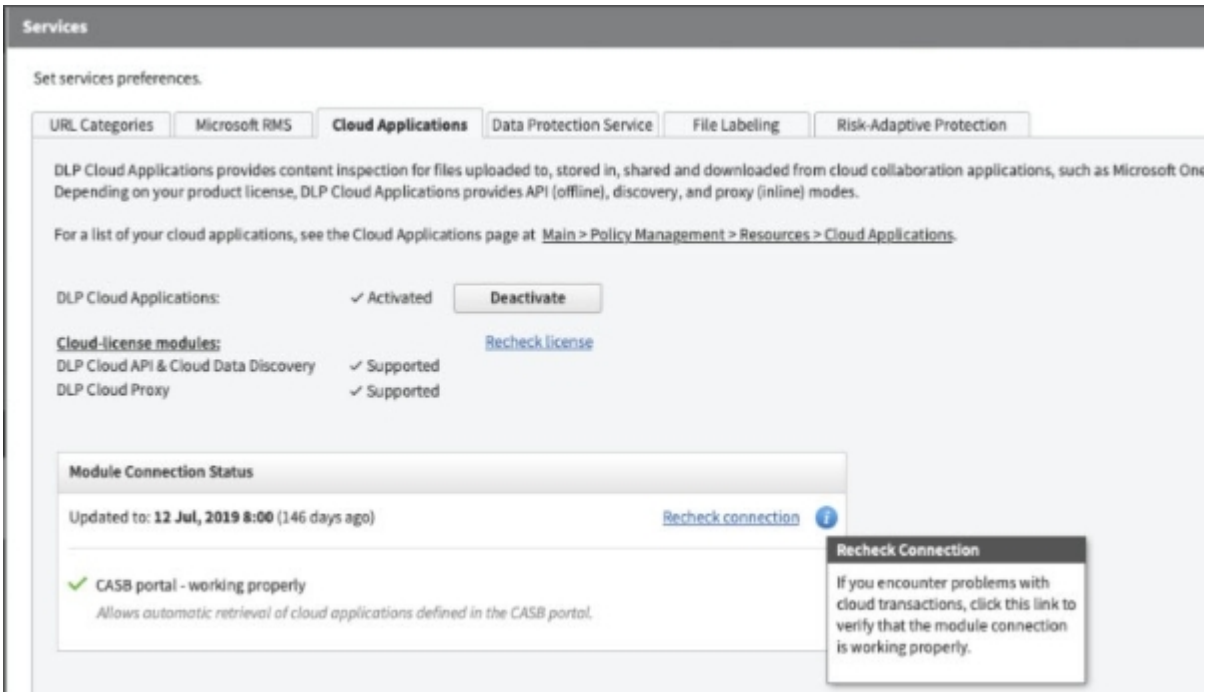


Note

The process might take a while, or might not be updated if you recently upgraded your licenses. Click the **Recheck license** link to get the most updated information.

7) The **Module Connection Status** section also appears on the page, indicating the connection status of the CASB Portal. In this section, you can do the following:

Click **Recheck connection** if the information shown is not up to date or the connection is not working properly.



After the connection is established between Forcepoint DLP and Forcepoint CASB, you can:

- Create an asset in the Forcepoint Security Manager. For more information, see *Add a cloud application in the Forcepoint Security Manager* (mentioned below).
- Create an asset in Forcepoint CASB. For more information, see *Add an asset in Forcepoint CASB* (mentioned below).
- Configure a Cloud Proxy or Cloud API policy in the Forcepoint Security Manager. For more information, see *Configure DLP policies for cloud applications in the Forcepoint Security Manager* (mentioned below).
- Configure a Cloud Proxy or Cloud API policy in Forcepoint CASB. For more information, see *Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage* (mentioned below).
- Configure and run a discovery scan in the Forcepoint Security Manager. For more information, see *Enable Cloud Data Discovery in the Forcepoint Security Manager* (mentioned below).
- Configure and run a discovery scan in Forcepoint CASB. For more information, see *Enable Cloud Data Discovery in the Forcepoint Security Manager* (mentioned below).

Related tasks

Generate the API key for Forcepoint DLP and Forcepoint CASB integration on page 15
Add a cloud application in the Forcepoint Security Manager on page 40
Add an asset in Forcepoint CASB on page 41
Configure DLP policies for cloud applications in the Forcepoint Security Manager on page 48
Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage on page 45
Enable Cloud Data Discovery in the Forcepoint Security Manager on page 54

Activate DLP Cloud Applications channels after a Forcepoint DLP upgrade

After you upgrade Forcepoint DLP, you must recheck the license and components to make sure that everything is working properly, and then redeploy the configuration to Data Protection Service.

If you do not complete these actions, the integration with Forcepoint CASB will not be activated after the upgrade, even though you are connected to the Forcepoint CASB portal. When you are done, you can verify that your cloud channels are being analyzed by Data Protection Service.

Recheck the license

1) In the Forcepoint Security Manager, go to **DATA > Settings > General > Services**, then select the **Cloud Applications** tab. The DLP Cloud Proxy license status is **Unknown**.

2) Click **Recheck license**. The status changes to **Supported**.

Connect to Data Protection Service or verify existing connection

To connect, request a new unique JSON file from Forcepoint Technical Support in order to successfully connect to Data Protection Service post-upgrade. Upload the JSON file and check the connection status. For more information on how to connect and to check connection status, see *Connect Data Protection Service in the Forcepoint Security Manager* (mentioned below).

Verify analysis by Data Protection Service

1) Deploy a policy configuration to Data Protection Service.

2) Go to the incident report for either the DLP Cloud API or Cloud Data Discovery channel, and verify that the **Analyzed by** field displays “Data Protection Service”.

For more information, see the knowledge article “Confirming successful switch from Data Agent to Data Protection Service”.

Related concepts
Connect Data Protection Service in the Forcepoint Security Manager on page 33

Configure single sign-on with Forcepoint CASB

The Forcepoint Security Manager allows users to open the Forcepoint CASB portal using a **Launch CASB Portal** button.

To open the Forcepoint CASB portal using the **Launch CASB Portal** button, the user logged on to the Forcepoint Security Manager must have an account with the same email address in Forcepoint CASB. When you set up user accounts in the Forcepoint Security Manager and Forcepoint CASB, make sure that the accounts for each user have the same email address.

If you encounter an authorization error when you try to access Forcepoint CASB from the Forcepoint Security Manager, make sure that the account logged on to the Forcepoint Security Manager has an account in Forcepoint CASB with the same email address.

Creating and configuring cloud applications

DLP Cloud Applications uses the resource type: **Cloud Applications**. These resources are listed in the **DLP Policy Management > Resources > Cloud Applications** screen after Forcepoint DLP establishes a successful connection with Forcepoint CASB. All DLP Cloud Proxy resources are defined in Forcepoint CASB, but are shown in Forcepoint DLP automatically. For DLP Cloud API, you can add, edit, or remove any application defined in Forcepoint CASB for this purpose. DLP Cloud Proxy applications are not editable at this time.

View the list of cloud applications

The Forcepoint Security Manager Cloud Applications resource screen shows a list of all configured cloud applications. To open the cloud applications list, open the Forcepoint Security Manager, then go to **DATA > Policy Management > Resources> Cloud Applications.**

By default, the table shows:

- **Application Name**: The unique name given to the specific cloud application.
  Click the Application Name to open the cloud application's **Properties** screen, where you can edit the cloud application settings.

  Note

  You cannot edit cloud applications that are only defined for DLP Cloud Proxy. You can only edit the properties for cloud applications defined for both DLP Cloud API and Cloud Data Discovery.

- **Application Type**: The name of the cloud application. The application type can be shared by multiple cloud applications in Forcepoint DLP.
- **Description**: The short description given to the cloud application.
- **DLP Cloud API Status**: The API connection needs to be manually configured for the specific cloud application on the cloud application's **Properties** screen. If an API connection has been successfully configured with the cloud application, the status is **OK**. If there is an issue with the connection, the appropriate message is shown. Move the mouse over the status message to see more information.
- **DLP Cloud Proxy Status**: If the application supports a proxy connection, the status is **OK**. If the application does not support a proxy connection, the status is **NA**. If there is an issue with the connection, the appropriate message is shown. Move the mouse over the status message to see more information.
- **Cloud Data Discovery Status**: The Cloud Data Discovery connection needs to be manually configured for the specific cloud application on the cloud application's **Properties** screen. If an API connection has been successfully configured with the cloud application, the status is **OK**. If there is an issue with the connection, the appropriate message is shown. Move the mouse over the status message to see more information.

If you want to view the cloud application in Forcepoint CASB, click the **Launch CASB Portal** button to open the Forcepoint CASB management portal.

Add a cloud application in the Forcepoint Security Manager

For Forcepoint DLP to apply both DLP and discovery policies to Forcepoint CASB cloud application assets, the cloud applications must be listed and configured correctly in the Forcepoint Security Manager Cloud Applications resource list.

DLP Cloud Proxy usage requires that both existing and new Forcepoint CASB assets have a quick policy enabled and activated in Forcepoint CASB before they can be used within the Forcepoint Security Manager. For more information, see *Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage* (mentioned below). This step is not required for DLP Cloud API and data discovery configuration, because new cloud application entries and settings can be configured directly in the Forcepoint Security Manager through the Cloud Application resource list using the following procedure:

1) In the Forcepoint Security Manager, go to **DATA > Policy Management > Resources > Cloud Applications**.
2) Click **Add**.
3) In the **Add DLP Cloud API Application** window, select an available cloud application, then click **OK**.
4) On the cloud application's **Properties** screen, configure the cloud application settings.
5) To deploy all the configured changes, click **Deploy**.

For information about configuring the API connection for the cloud application, see *Configure the cloud application connection in the Forcepoint Security Manager* (mentioned below).

For information about configuring the Cloud Data Discovery settings for the cloud application, see *Configuring Cloud Data Discovery (data at rest) settings* (mentioned below).

Related concepts
Configuring Cloud Data Discovery (data at rest) settings on page 54

Related tasks
Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage on page 45
Configure the cloud application connection in the Forcepoint Security Manager on page 42

Edit a cloud application in the Forcepoint Security Manager

Steps

1) In the Forcepoint Security Manager, go to **DATA > Policy Management>Resources > Cloud Applications.**
2) Click the **Application Name** for the cloud application.

3) On the cloud application's **Properties** screen, configure the API connection settings for the cloud application.

4) To deploy all the configured changes, click **Deploy**.

Note

Applications in use for DLP Cloud Proxy *only* are not links, because they cannot be edited. For applications defined as both DLP Cloud API and DLP Cloud Proxy, click the application name to open the cloud application's **Properties** screen. Only DLP Cloud API properties can be edited here.

Add an asset in Forcepoint CASB

Steps

1) In Forcepoint CASB, go to **Settings > Resources > Assets**.

2) Click **Add Asset**.

3) Select the relevant asset type, then click **Next**.

4) Type an **Asset Name** and **Description**, then click **Add**.

Next steps

After the asset is saved in Forcepoint CASB, it is visible in Forcepoint DLP in the Forcepoint Security Manager (**DATA > Policy Management > Resources > Cloud Applications**).

You can now configure the API connection to the cloud application. For more information, see *Configure a cloud application API connection in Forcepoint CASB* (mentioned below).

Related tasks

Configure a cloud application API connection in Forcepoint CASB on page 43

Edit an asset in Forcepoint CASB

Steps

1) In Forcepoint CASB, go to **Settings > Resources > Assets**.

2) Select the asset.

3) On the asset information page, you can edit or configure all settings for the asset.

   For more information about editing and configuring an asset in Forcepoint CASB, see the "Managing Service Assets" chapter in the Forcepoint CASB Administration Guide.

Delete an asset in Forcepoint CASB

Steps

1) In Forcepoint CASB, go to **Settings > Resources > Assets**.

2) Select the asset.

3) On the asset information page, click the **Delete Asset** button.

   When you delete the asset in Forcepoint CASB, the corresponding cloud application in Forcepoint DLP is also deleted.

Configuring the Cloud API connection

DLP Cloud API requires an API connection between the cloud application and Forcepoint CASB. This API connection can be configured in Forcepoint DLP or Forcepoint CASB. When you configure the connection to the cloud application, you must use an administrator account with elevated privileges. For more information about which cloud applications are supported and the account requirements for those supported cloud applications, see the Forcepoint CASB Service Provider API Connection Guide.

Configure the cloud application connection in the Forcepoint Security Manager

Steps

1) In the Forcepoint Security Manager, go to **DATA > Policy Management>Resources > Cloud Applications.**

2) In the cloud applications table, click the **Application Name**.

   The **Cloud Application Properties** screen opens to allow configuration of the selected application.

   - Pop-up blockers might prevent this screen from opening. If this occurs, disable the pop-up blocker and try again.
   - It might take a while for the screen to open. Wait for the screen to load, then complete the steps below. Do not close the screen while it is still loading.

3) On the **General** tab, click **Configure Connection**.

   The Forcepoint CASB service uses the connection to retrieve activity logs, scan files at rest, and retrieve user lists. It does not store the user credentials. For more information about account requirements, see the Forcepoint CASB Service Provider API Connection Guide .

4) Open the **DLP Cloud Service** tab. In the **DLP Cloud API** section:

   a) Select **Enable activity import** to allow the Forcepoint CASB service to access and import user activity logs for the selected cloud application.

b) For Office 365 and Box assets, select **Unshare parent folder** to remove the sharing permissions for a sensitive file's parent folder. Select this option to remove sharing permissions when sensitive files inherit sharing permissions from a parent folder in the hierarchy. This removes the sharing permissions for the affected folders and all files located in them. This option applies only if one of the unshare actions is selected in the action plan of the DLP policy.

5) Open the **General** tab. In the **Mitigation Settings** section, configure an **Archive folder** within the selected cloud service for files moved or copied in response to a DLP incident. The archive folder must reside on the scanned asset, so the path needs to match the browser URL.

6) Under **Quarantine Notes**, optionally configure messages that can replace quarantined files and explain to users that files have been moved.

7) Click **Test Connection** to verify activity download, data classification, and the validity of the archive folder.

8) To save the changes and return to the cloud applications list, click **OK**.

- The new application is added to the cloud applications list, which shows the application name, type, description, and status.
- You can edit the cloud application's properties by clicking the **Application Name.**

The new application is added to the cloud applications list even if configuration is canceled before this step is completed. Open the cloud application's **Properties** screen to finish configuration if necessary.

9) To deploy all the configured changes, click **Deploy**.

Note

If you are logged on to the Forcepoint Security Manager, but want to edit the cloud application in Forcepoint CASB, click the **Launch CASB Portal** button to open the Forcepoint CASB management portal.

Configure a cloud application API connection in Forcepoint CASB

If you prefer to set up the API connection in Forcepoint CASB instead of the Forcepoint Security Manager, follow these steps:

Steps

1) In Forcepoint CASB, go to **Settings > Resources > Assets**.

2) Select the cloud application (asset) from the list.

3) Expand the **Asset Governance** section.

4) Under **API connection**, click **Set connection**.

5) Forcepoint CASB opens the cloud application logon page. Log on to the account using an administrator account. For more information about account requirements, see the Forcepoint CASB Service Provider API Connection Guide.

6) The cloud application shows a page with the permissions that Forcepoint CASB is requesting. Approve the request to close this page and log on to the account.

7) In Forcepoint CASB, the API connection section shows **Credentials added successfully** if the connection succeeded. If the connection failed, re-enter the credentials.

8) Click **Test connection** to verify that Forcepoint CASB can successfully connect to the cloud application.

9) Click the **Activity import** button to enable or disable the setting.

- If data at rest scanning is disabled, this setting is shown as **Activity import disabled** and the **off** button is highlighted.
- If data at rest scanning is enabled, this setting is shown as **Activity import enabled** and the **on** button is highlighted.

Forcepoint CASB downloads the activities through the configured API connection. This process might take up to 24 hours.

10) Expand the **Data Classification** section.

11) Enter an **Archive folder path**. This path is needed for some API mitigation rules, such as **Remove sharing permissions**, **Keep a safe copy**, and **Quarantine**. The archive folder must reside on the scanned asset, so the path needs to match the browser URL.

12) Click Save archive folder settings.

13) When you select the Quarantine mitigation in an API policy, you have the option of leaving a note where the sensitive file was located. You can customize the note here.

To edit the current note:

a) Click the download icon next to the format icon (docx, xlsx, pptx, pdf, or txt).

b) Open the downloaded note, edit the text, and save the file

c) Click the upload icon, browse to the file, then click **Open**.

To upload a new note:

a) Click the upload icon, browse to the file, then click **Open**.

To restore the note to the default:

a) Click the restore icon.

b) Confirm that you want to restore the default note.

14) Click **Save quarantine note settings**.

After the API connection is set in Forcepoint CASB, the connection is also visible in the Forcepoint Security Manager (**DATA > Policy Management > ResourcesCloud Applications**) under the **Cloud API Status** column in the cloud applications table.

Configuring Forcepoint DLP policies for CASB cloud application assets

After the Forcepoint CASB and Forcepoint DLP integration is complete, Forcepoint CASB can be configured to send data for specified cloud application assets to the DLP Cloud Proxy or DLP Cloud API for content inspection and the enforcement of either Forcepoint DLP policies or Forcepoint CASB policies.

This Integration Guide focuses on the enforcement of Forcepoint DLP policies for Forcepoint CASB cloud application assets. For more information about configuring Forcepoint CASB custom policies to use the Forcepoint DLP predicate, see the Forcepoint CASB Administration Guide.

This section walks through the following configuration steps:

- Forcepoint CASB portal: Enable Forcepoint DLP content inspection for each Forcepoint CASB cloud application asset. See *Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage* (mentioned below).
- Forcepoint Security Manager: Configure Forcepoint DLP policy rules for active cloud application assets. See *Configure DLP policies for cloud applications in the Forcepoint Security Manager* (mentioned below).
- Forcepoint Security Manager: Configure one or more action plans with cloud application resources. See *Configure an action plan with cloud application resources* (mentioned below).

After this configuration is complete, the cloud application incidents are captured in incident reports.

Related tasks

Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage on page 45
Configure DLP policies for cloud applications in the Forcepoint Security Manager on page 48
Configure an action plan with cloud application resources on page 50

Configure Forcepoint CASB cloud application assets for Forcepoint DLP policy usage

After the Forcepoint DLP and Forcepoint CASB integration is configured and the DLP Cloud Application license is active in Forcepoint CASB, a new Forcepoint Data Security DLP policy is added to the Data Leak Prevention quick policies list in the Forcepoint CASB management portal.

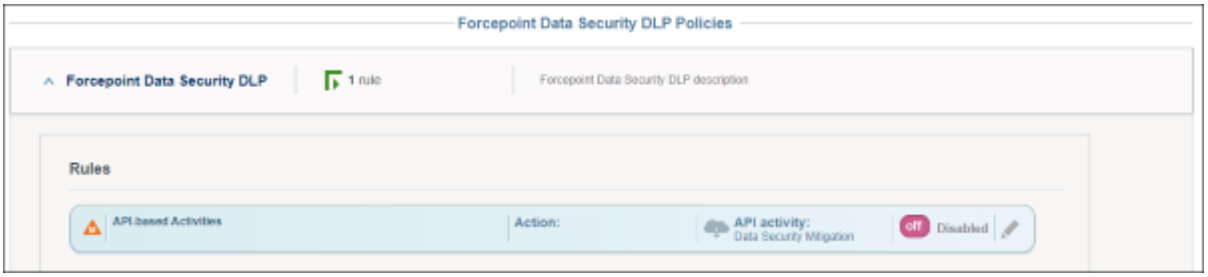
Enable and configure this policy to define which user activities should be monitored:

Steps

1) In Forcepoint CASB, go to **Audit & Protect > Security Policies > Data Leak Prevention**.

2) Select the cloud application (asset) from the list above the Dashboard.

3) Expand the **Forcepoint Data Security DLP** policy.
This policy is automatically set up with rules depending on the cloud application connection settings:



4) Click the edit icon on the right side end of the rule.

5) Edit the rule:

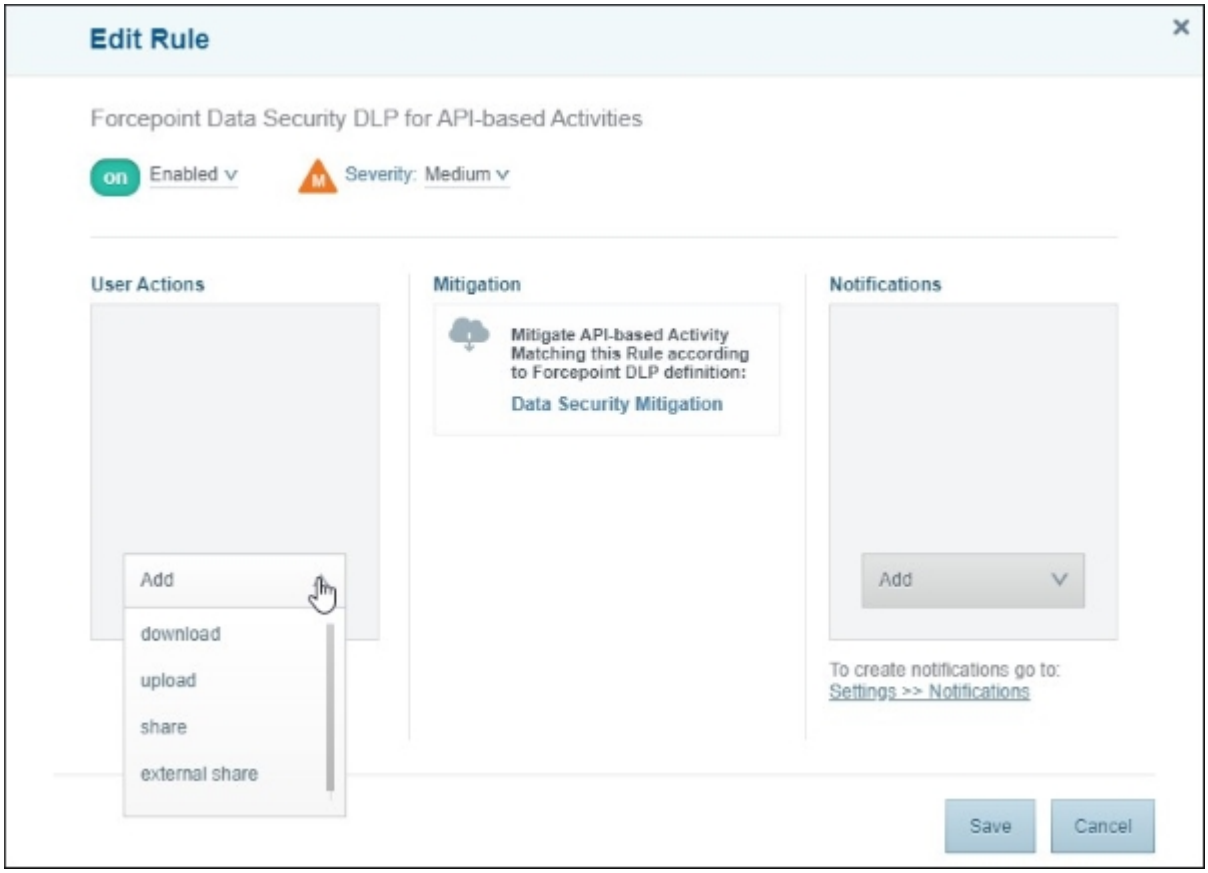
   a) Change the rule status to **Enabled**. When the status is Enabled, the **on** button is shown.
   If you want to disable the rule again, change the status to **Disabled**. When the status is Disabled, the **off** button is shown.

   b) Select the **Severity**.

c) Select the **User Actions** to be flagged for this rule. You must select at least one action for the rule to work.

If a user performs an action that matches the action selected here, Forcepoint CASB performs the selected mitigation.

- For API-based activities, you can select **download**, **upload**, **share**, and **external share**.
- For Proxy-based activities, you can select **download** and **upload**.



d) Create and configure **Notifications** for this rule. For more information about notifications, see the "Configuring notifications" section in the Forcepoint CASB Administration Guide.

Note

The Mitigation (**Data Security Mitigation**) is set in Forcepoint DLP on the Forcepoint Security Manager. When **Data Security Mitigation** is selected as the mitigation, the policy uses the Action Plan configured on the Forcepoint Security Manager.

6) Click **Save**.

Important

If you create custom policies for Forcepoint DLP in Forcepoint CASB, Forcepoint recommends that you disable the Data Leak Prevention security policy. If you have active custom policies and an active Data Leak Prevention policy, then the Data Leak Prevention policy takes precedence over the custom policies. This might cause reporting issues with the custom policies.

Configure DLP policies for cloud applications in the Forcepoint Security Manager

When configuring DLP Cloud policy rules, you must select **DLP Cloud Applications** as the destination, and you must select one or both of the DLP Cloud Applications channels – **DLP Cloud API** and **DLP Cloud Proxy**.

Steps

1) In the Forcepoint Security Manager, go to **DATA > Policy Management>Manage DLP Policies.**

2) Expand a policy in the tree view and click a rule, then select **Edit** or **Add > Rule**.

3) On the **Policy Rule** page, configure the rule through the **General**, **Condition**, **Severity & Action**, **Source**, and **Destination** tabs. Configuring a rule for a cloud application is similar to any DLP rule, but requires specific configuration settings in the **Severity & Action** and **Destination** tabs (see steps 3 and 4 below). For more information about creating a policy rule, see the Forcepoint DLP Administrator Guide.

4) On the **Severity & Action** tab, select an action from the **Action Plan** drop-down menu. Click the button to the right of the drop-down menu to open the **Action Plan Details** page.

   On the **Data Loss Prevention** tab, in the **Cloud Applications Channels** section, select the actions for the available operations.

   - For DLP Cloud Proxy, you can select the following actions:
     - **Permit**: Allow the operation.
     - **Block**: Block the operation.
   - For DLP Cloud API, you can select the following actions:
     - **Permit**: Allow the operation.
     - **Safe copy**: Save a copy of the file to a cloud archive that is accessible only to administrators.
     - **Quarantine**: Save the file in a quarantine folder defined in the CASB portal.
     - **Quarantine with note**: Quarantine the file and leave a message in place of the original file.
     - **Unshare external**: Remove sharing permission for external addresses.
     - **Unshare all**: Remove all sharing permissions from the file.

5) On the **Destination** tab, in the **DLP Cloud Applications** section, select **DLP Cloud API**, **DLP Cloud proxy**, or both. For each channel, select at least one cloud application (or **All**) and at least one operation, as follows:

   a) Click **Edit**.

   b) Select one or more cloud applications in the **Available Elements** list.

   If you want to use all of the cloud applications, leave this as **All** and then continue with step 5e to select an operation.

   (Forcepoint DLP 8.9 and above) If you have an Office 365 cloud application, then you can choose to monitor OneDrive, SharePoint, Teams, or Other. Select Other to monitor Office 365 applications that are not part of OneDrive, SharePoint, or Teams.

   c) Click the right arrow button to move the selected cloud applications to the **Selected Elements** list.

   d) Click **OK**. The cloud applications are now shown in the box under the channel name.

e) Select user operations to monitor: For DLP Cloud API these include **File uploading/attaching**, **File downloading**, **External file-sharing**, and **Unrecognized file-sharing**. For DLP Cloud Proxy operations include **File uploading/attaching** or **File downloading**.

6) Click **Next** to show a summary of the rule.

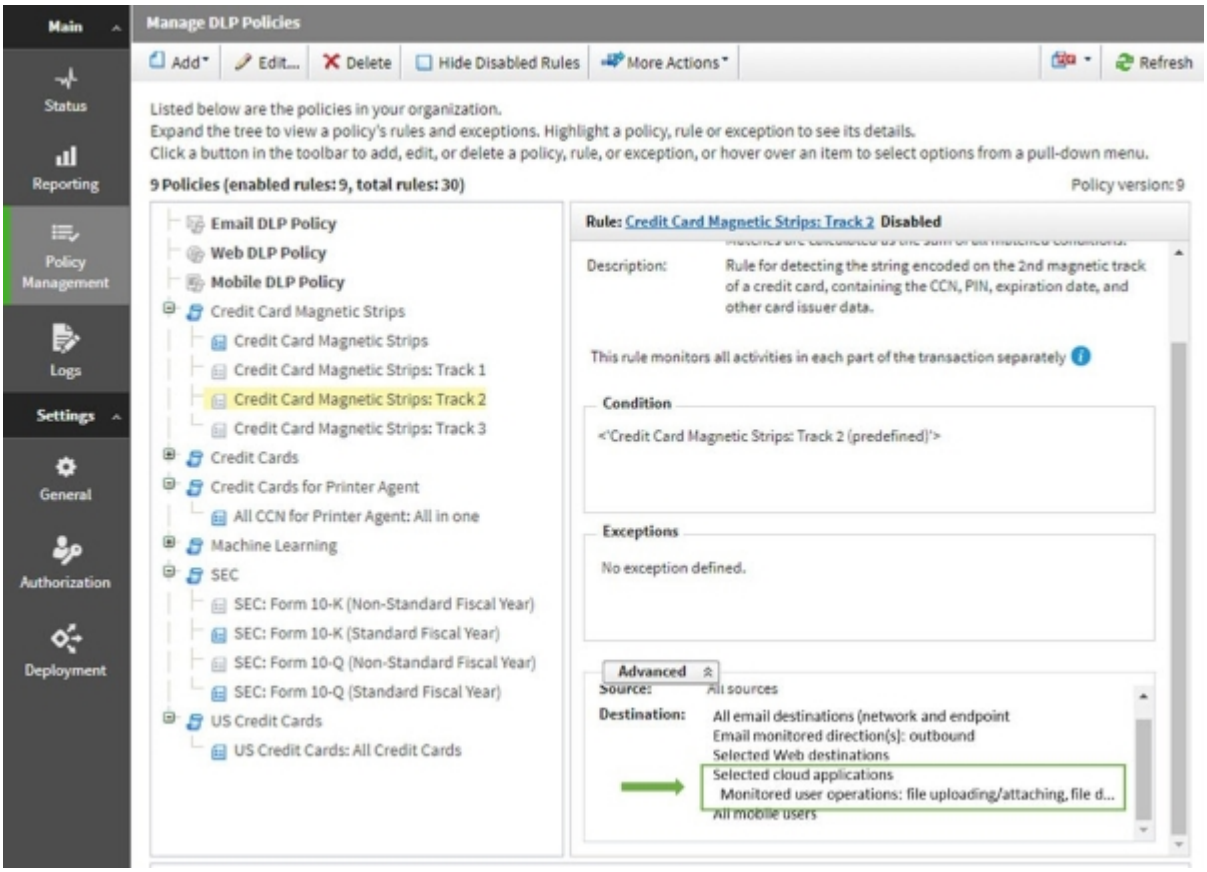
7) Click **Finish** to save the rule.

8) To deploy all the configured changes, click **Deploy**.

Note

If you do not want to monitor certain operations for DLP Cloud API, you must configure this in Forcepoint CASB.

In the **Manage DLP Policies** screen, the rule summary (right pane) shows whether **DLP Cloud Applications** are selected as a **Destination**.



Configure an action plan with cloud application resources

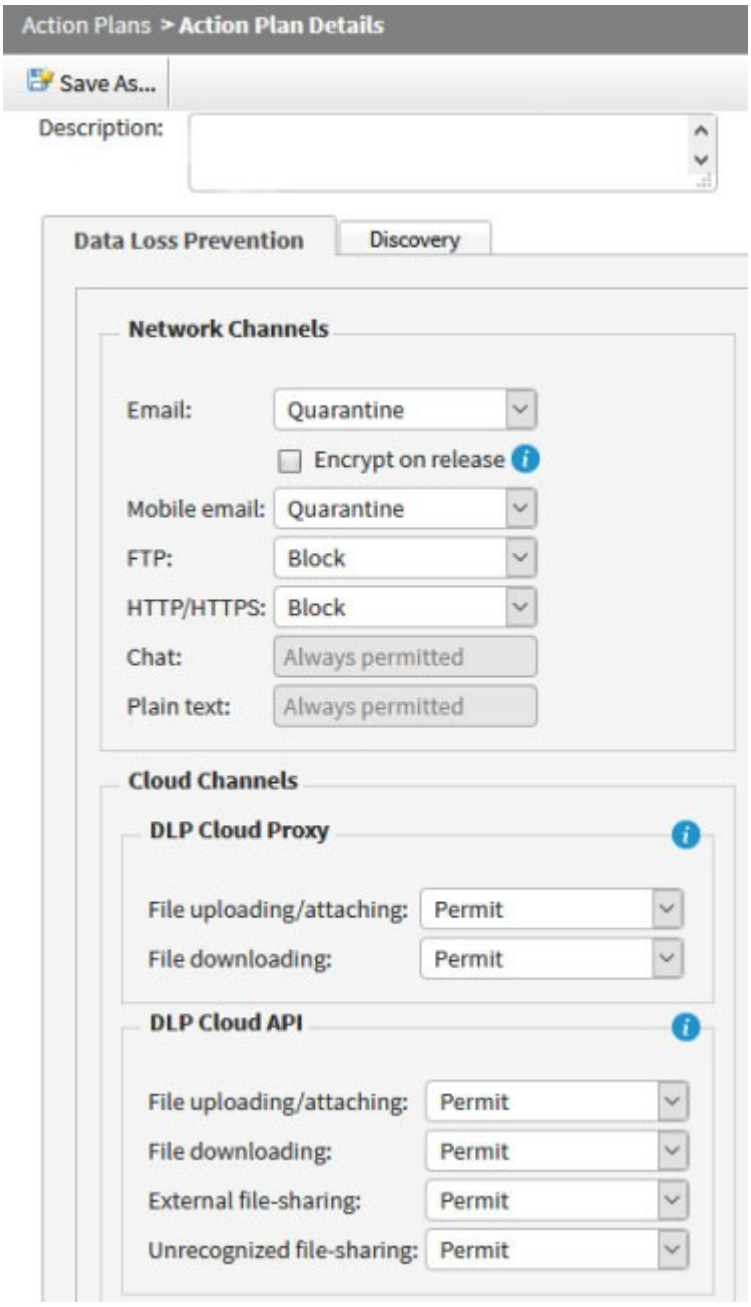
Steps

1) In the Forcepoint Security Manager, go to **DATA > Policy Management>Resources > Action Plans.**

2) Click **New**.

3) On the **Action Plan Details** page, type a **Name** and **Description** for the action plan.

4) On the **Data Loss Prevention** tab, in the **Cloud Applications Channels** section, select the actions for the available operations.
   - For DLP Cloud Proxy, you can select the following actions:
     - **Permit**: Allow the operation.
     - **Block**: Block the operation.
   - For DLP Cloud API, you can select the following actions:
     - **Permit**: Allow the operation.
     - **Safe copy**: Save a copy of the file to a cloud archive that is accessible only to administrators.
     - **Quarantine**: Save the file in a quarantine folder defined in the CASB portal.
     - **Quarantine with note**: Quarantine the file and leave a message in place of the original file.
     - **Unshare external**: Remove sharing permission for external addresses.
     - **Unshare all**: Remove all sharing permissions from the file.



5) Click **OK**.

6) To deploy all the configured changes, click **Deploy**.

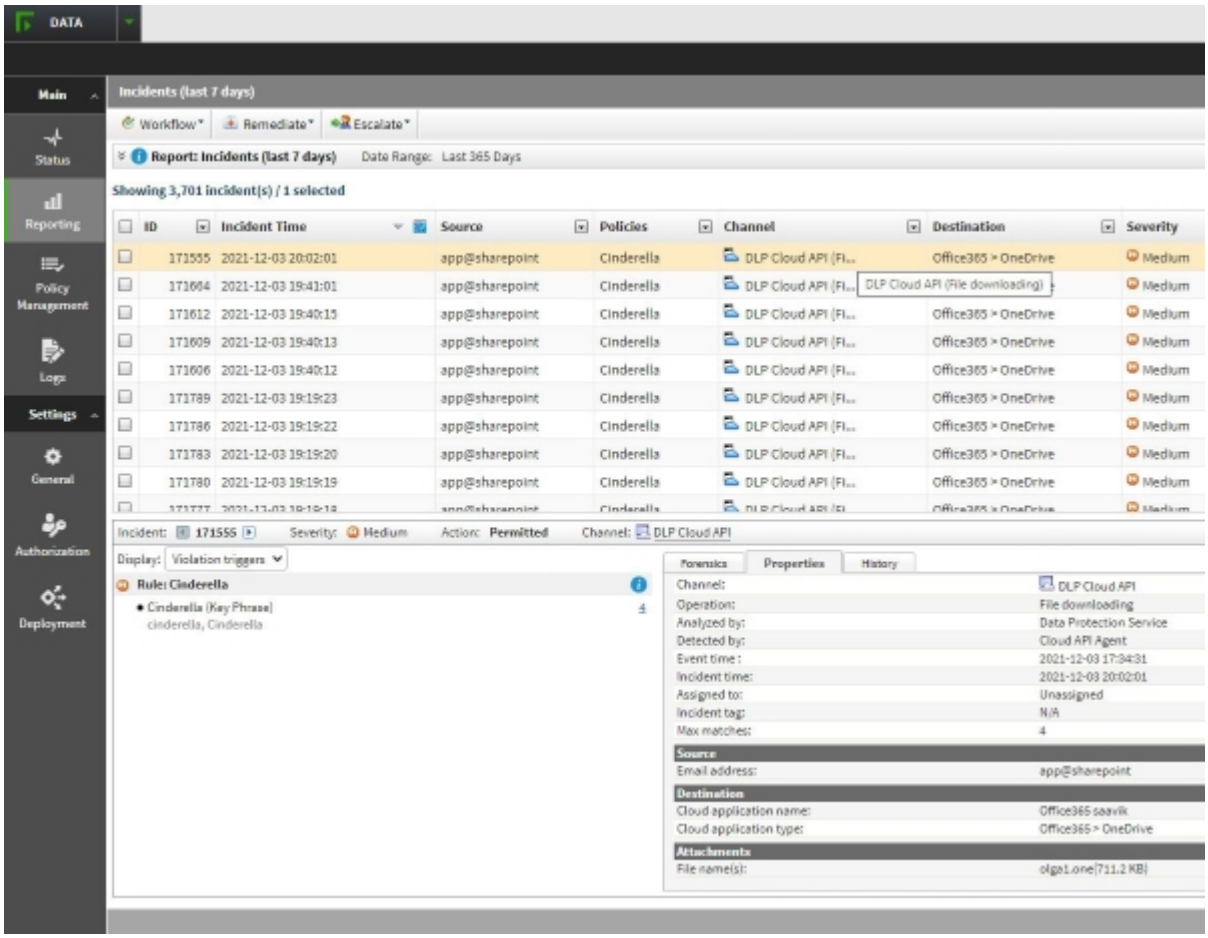
View Forcepoint DLP incidents in the Forcepoint Security Manager

Viewing and managing reports for the **DLP Cloud Applications** feature is the same as for the on-premises DLP. The main change involves what is displayed for a DLP incident:

- Action (expected)
- Channel (operation)
- Cloud application name
- Cloud application type

Note

If the **Destination > Cloud application type** property displays **Office 365 - unknown application**, it means that the Office 365 application type was not recognized by the Cloud Agent. In this case, the enforcement is done according to the selected option **Office 365 > Other** in the policy management.



View incident information in Forcepoint CASB

When a DLP policy is triggered, additional transaction details are captured and shown in the corresponding Forcepoint CASB Audit Log and Incidents screens.

To view the Audit Log for a DLP Cloud Proxy activity:

1) In Forcepoint CASB, go to **Audit & Protect > Activity Audit > Realtime Monitoring > Audit Log**.

2) Select the cloud application (asset) from the list above the Dashboard.

3) In the Rules column, look for a rule that matches the policy you created or enabled.

4) If you want to only show the activities that match the DLP rules:
   a) Click the **Add filters** plus (+) sign.

   b) Select **Rules** from the list. A new Rules filter is added to the top of the audit log.

c) Open the **Rules** drop-down menu and select the rule (or rules) you want to show.

To view the Audit Log for a DLP Cloud API activity:

1) In Forcepoint CASB, go to **Audit & Protect > Activity Audit > Service Provider Log > Audit Log**.

2) Select the cloud application (asset) from the list above the Dashboard.

3) In the Rules column, look for a rule that matches the policy you created or enabled.

4) If you want to only show the activities that match the DLP rules:
   a) Click the **Add filters** plus (+) sign.

   b) Select **Rules** from the list. A new Rules filter is added to the top of the audit log.

   c) Open the **Rules** drop-down menu and select the rule (or rules) you want to show.

For more information about Forcepoint CASB audit logs, see the “Investigating activity logs” section in the Forcepoint CASB Administration Guide.

Configuring Cloud Data Discovery (data at rest) settings

After you create the cloud application and set up the API connection, you can enable Cloud Data Discovery (data at rest) to run Discovery Scans.

Enable Cloud Data Discovery in the Forcepoint Security Manager

Steps

1) In the Forcepoint Security Manager, go to **DATA > Policy Management>Resources > Cloud Applications.**

2) In the cloud applications table, click the **Application Name**.
   The **Cloud Application Properties** screen opens to allow configuration of the selected application.
   - Pop-up blockers might prevent this screen from opening. If this occurs, disable the pop-up blocker and try again.
   - It might take a while for the screen to open. Wait for the screen to load, then complete the steps below. Do not close the screen while it is still loading.

3) If you have not already configured the connection to the cloud service, click **Configure Connection**on the **General** tab.

   The Forcepoint CASB service uses the connection to retrieve activity logs, scan files at rest, and retrieve user lists. It does not store the user credentials.

4) Open the **DLP Cloud Service** tab. In the **DLP Cloud Data Discovery** section:

   a) Select **Enable data at rest discovery** to activate the data at rest discovery scan for this cloud application.

   b) Under **Scan Path > Folder Path**, enter the full URL of the storage folder to be scanned. By default, all folders and files in the drive path are 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.

   c) For Office 365 and Box assets, select **Unshare parent folder** to remove the sharing permissions for a sensitive file's parent folder. Select this option to remove sharing permissions when sensitive files inherit sharing permissions from a parent folder in the hierarchy. This removes the sharing permissions for the affected folders and all files located in them. This option applies only if one of the unshare actions is selected in the action plan of the DLP Discovery policy.

   d) For Office 365, Box, Dropbox, and G Suite assets, select **Scan by sharing status** to scan files with a specific 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).

5) To scan files with specific file extensions only, click the **Scan by File Extension** button in the **DLP Cloud Data Discovery** section.

   a) To scan files with specific file extensions either:

      - Enter the file extensions into the large text field separated by commas (e.g., “.doc,.docx”), or
      - Click the **File Extensions** button to select predefined categories. On the **File Extensions** screen, select the predefined categories to include in the scan. When a category is selected, the file extensions are shown in the right-side column. The bold categories are the default categories.

      To include all files with extensions, leave the field empty. The field shows **All extensions** to let the user know that all files with extensions are included in the scan. Note that this might increase the scan time significantly.

   b) To add the default file extensions, click **Set to Default Extensions**.This adds the default extension predefined categories (marked on the **File Extensions** screen in bold: Word processing, Spreadsheet, Presentation, Mail, and Archive).

   c) To scan files that do not have a file extension, select **Include files with no extension**.

d) To sort the extensions alphabetically, select one of the two sort buttons: **Sort A to Z or Sort Z to A**.

6) Open the **General** tab. In the **Mitigation Settings** section, configure an **Archive folder** within the selected cloud service for files moved or copied in response to a DLP incident. The archive folder must reside on the scanned asset, so the path needs to match the browser URL.

7) Under **Quarantine Notes**, optionally configure messages that can replace quarantined files and explain to users that files have been moved.

8) Click **Test Connection** to verify that the message file can be copied to the cloud application.

9) To save the changes and return to the cloud applications list, click **OK**.

- The new application is added to the cloud applications list, which shows the application name, type, description, and status.
- You can edit the cloud application's properties by clicking the **Application Name.**

The new application is added to the cloud applications list even if configuration is canceled before this step is completed. Open the cloud application's **Properties** screen to finish configuration if necessary.

10) To deploy all the configured changes, click **Deploy**.

Note

If you are logged on to the Forcepoint Security Manager, but want to edit the cloud application in Forcepoint CASB, click the **Launch CASB Portal** button to open the Forcepoint CASB management portal.

Configure data at rest discovery in Forcepoint CASB

If you prefer to enable and configure data at rest discovery in Forcepoint CASB instead of the Forcepoint Security Manager, follow these steps:

Steps

1) In Forcepoint CASB, go to **Settings > Resources > Assets**.

2) Select the cloud application (asset) from the list. The asset must have a configured API connection. For more information, see *Configure a cloud application API connection in Forcepoint CASB* (mentioned below).

3) Expand the **Data Classification** section.

4) Enter an **Archive folder path**. This path is needed for some data at rest policies, such as **Remove sharing permissions**, **Keep a safe copy**, and **Quarantine**. The archive folder must reside on the scanned asset, so the path needs to match the browser URL.

5) Click **Save archive folder settings**.

6) When you select the Quarantine mitigation in a data at rest policy, you have the option of leaving a note where the sensitive file was located. You can customize the note here.

   To edit the current note:

   a) Click the download icon next to the format icon (docx, xlsx, pptx, pdf, or txt).

   b) Open the downloaded note, edit the text, and save the file

   c) Click the upload icon, browse to the file, then click **Open**.

   To upload a new note:

   a) Click the upload icon, browse to the file, then click **Open**.

   To restore the note to the default:

   a) Click the restore icon.

   b) Confirm that you want to restore the default note.

7) Click **Save quarantine note settings**.

Related tasks

Configure a cloud application API connection in Forcepoint CASB on page 43

Create a Cloud Data Discovery policy in the Forcepoint Security Manager

Before you create a Cloud Data Discovery scan, make sure that you have created at least one Discovery Policy in the Forcepoint Security Manager (**Policy Management > Discovery Policies > Manage Policies**). For more information, see Creating Discovery Policies in the Forcepoint DLP Administrator Help.

Add a Cloud Data Discovery scan in the Forcepoint Security Manager

Use the **Cloud Discovery Scan Properties** page in the Data Security module of the Forcepoint Security Manager to create or edit a Cloud Data Discovery scan.
To access the Cloud Discovery Scan Properties page:

1) In the Forcepoint Security Manager, go to **DATA > Policy Management > Discovery Policies > Cloud Data Discovery Scans > Cloud Discovery Scan Properties**.

2) Click **New** in the toolbar at the top of the content pane on the Cloud Discovery Scans page to add a new scan. A Cloud Discovery Scan Properties page is shown.

To create or edit a scan:

1) Enter or update a **Scan name** and **Description** for the scan.

2) Select **Enable scan** to enable the Cloud Data Discovery scan.

3) Choose a cloud application from the drop-down list for the new scan.
The Cloud Application field lists all unassigned cloud applications created from the CASB Service page (e.g., Dropbox-Test Instance).

   Only applications that support Cloud Data Discovery are shown in the drop-down list. Cloud data discovery is enabled for all supported assets in the CASB portal. To disable Cloud Data Discovery, go to the CASB portal and modify the relevant asset. Each cloud application can be assigned to only one scan.

   Note that you cannot change the Cloud application name when you edit the scan.

4) Use the **Discovery Policies** section to determine which policies to apply during the scan.
Do one of the following:
   - Select **All discovery policies** to prompt Forcepoint DLP to search for data that matches the rules in all deployed policies.
   - Select **Selected policies** to apply only certain policies in this scan, then select the policies to apply.

5) To save the changes and return to the Cloud Discovery Scans page, click **OK**.

6) To deploy all the configured changes, click **Deploy**.

Chapter 5

Integrating Forcepoint DLP and Forcepoint Web Security Cloud

Contents

- General Flow on page 59
- Configuring Data Protection Service connections on page 61
- Configuring a web policy to use Data Protection Service on page 65
- Exporting the Forcepoint Web Security Cloud URL categories on page 66
- Import URL categories to Forcepoint DLP on page 67
- Using URL Categories in DLP policies in the Forcepoint Security Manager on page 68
- Deploy to Data Protection Service on page 73
- View DLP incident reports on page 74
- Verifying the integration on page 74

Customers licensed for Cloud Security Gateway (or Forcepoint Web Security Cloud and Forcepoint Web Security DLP Module) can extend their existing enterprise DLP policies to web traffic analyzed and protected through the Forcepoint cloud proxy infrastructure. This includes support for advanced data classification technologies, such as structured and unstructured data fingerprinting and the use of web categories to build targeted DLP policies and enrich incident records.

The integration between Forcepoint DLP and Forcepoint Web Security Cloud is available as of Forcepoint DLP 8.8 and the October 2020 release of Forcepoint Web Security Cloud. The integration enables Forcepoint Web Security Cloud to use the Forcepoint DLP policy engine to analyze and apply rules to traffic enforced by Forcepoint Web Security Cloud.

Forcepoint Web Security Cloud can be configured to send user web requests that are considered potential security risks to the Data Protection Service for further review and evaluation. With this integration, enterprise data security, including blocking and monitoring data loss, is handled by the Data Protection Service rather then by the cloud proxy. The cloud proxy continues to handle web traffic.

General Flow

Make sure you received the following items in your fulfillment email from Forcepoint as part of the onboarding process:

- A Forcepoint DLP license XML file.
- A JSON file with tenant information.

Integrate Forcepoint DLP with Forcepoint Web Security Cloud by following these steps.

Steps

1) Configure the Data Protection Service connections.
   a) Configure Data Protection Service in the Forcepoint DLP.
      - Update your license by uploading the license XML file to the Subscription page (**Settings > General > Subscription**). See *Update a license in Forcepoint DLP* (mentioned below).
      - Connect between the DLP Manager and Data Protection Service, as described in *Connect Forcepoint DLP to Data Protection Service*, (mentioned below) by uploading the JSON tenant information to the Data Protection Service tab (**Settings > General > Services**).

   b) Configure Data Protection Service in the Forcepoint Cloud Security Gateway Portal (also called the cloud portal). See *Connect Forcepoint Web Security Cloud to Data Protection Service*, (mentioned below).

2) Configure policies to be enforced by Forcepoint Web Security Cloud. See *Configuring a web policy to use Data Protection Service* (mentioned below).

3) Export URL categories from Forcepoint Web Security Cloud. See *Exporting the Forcepoint Web Security Cloud URL categories* (mentioned below).

4) Map and use URL categories in Forcepoint DLP.
   a) Import URL categories from Forcepoint Web Security Cloud. See *Import URL categories to Forcepoint DLP* (mentioned below).

   b) View and update URL categories. See *Viewing and updating URL categories* (mentioned below).

   c) Manage URL categories in rule destinations. See *Using URL Categories in DLP policies in the Forcepoint Security Manager* (mentioned below).

5) Deploy the configuration to Data Protection Service and begin receiving incidents in the DLP Manager. See *Deploy to Data Protection Service* (mentioned below).

6) View incident reports using Data Protection Service. See *View DLP incident reports* (mentioned below).

Related concepts

Exporting the Forcepoint Web Security Cloud URL categories on page 66
Viewing and updating URL categories on page 68
Deploy to Data Protection Service on page 73
View DLP incident reports on page 74

Related tasks

Update a license in Forcepoint DLP on page 14
Connect Forcepoint DLP to Data Protection Service on page 61
Connect Forcepoint Web Security Cloud to Data Protection Service on page 63
Configuring a web policy to use Data Protection Service on page 65
Import URL categories to Forcepoint DLP on page 67

Related information
Using URL Categories in DLP policies in the Forcepoint Security Manager on page 68

Configuring Data Protection Service connections

Data Protection Service connects to both Forcepoint DLP and Forcepoint Web Security Cloud.

Each of these steps requires you to upload the configuration file provided by Forcepoint in the fulfillment email you received. This file provides the information needed to connect both products to Data Protection Service.

Important

Make sure you update your subscription before connecting to Data Protection Service. If you connected first, the new license is not reaching Data Protection Service. To resolve this issue, follow the instructions provided in this article.

Connect Forcepoint DLP to Data Protection Service

Forcepoint DLP and Data Protection Service are connected on the DLP in the Data Protection Service tab (**General > Services > Data Protection Service**), as follows:

1) Click **Select File**, and in the dialog box that appears, click **Choose File**, and browse to the JSON file you received from Forcepoint, and then click **OK**.
   The file is uploaded to the server, and the information begins to appear in the Connection area of the Data Protection Service tab.

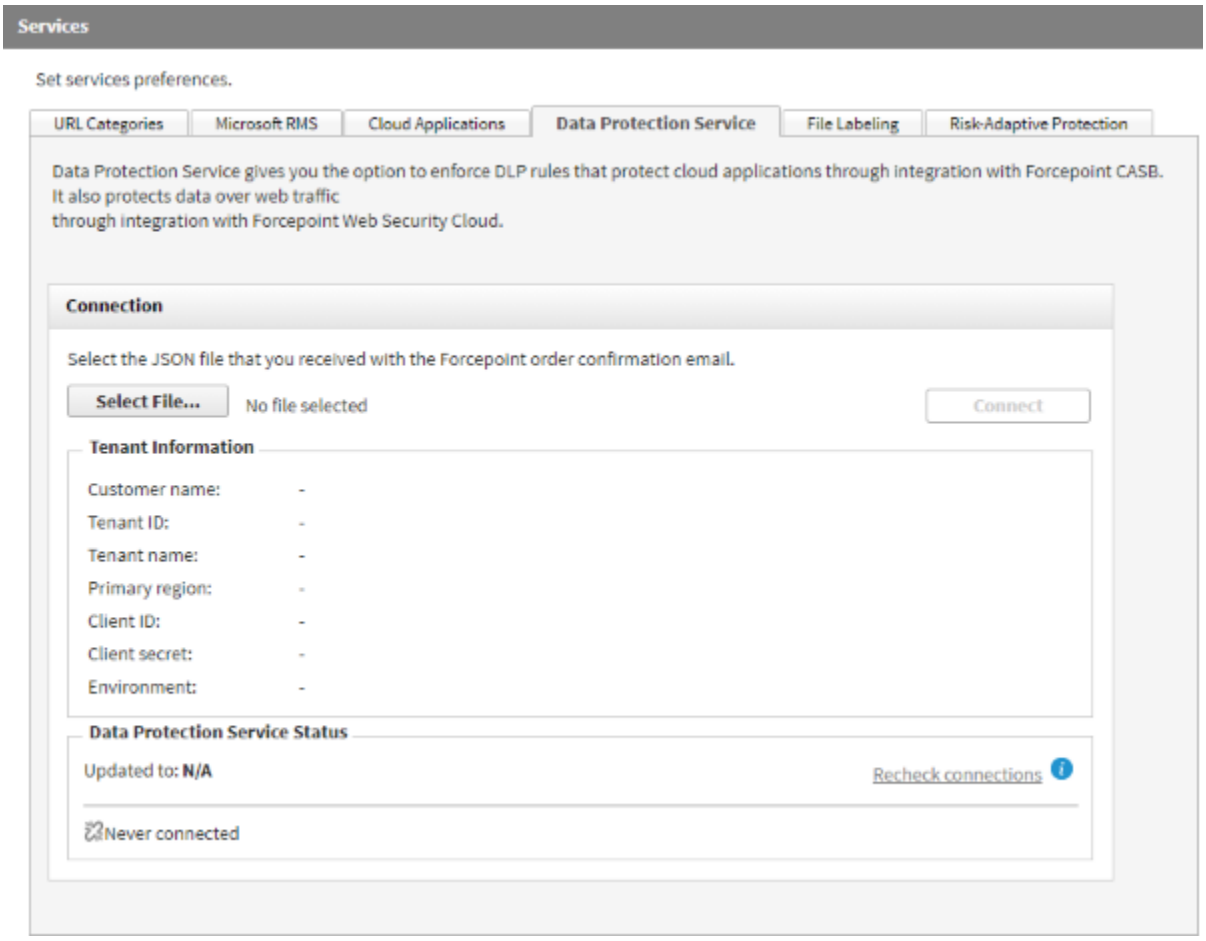
2) Click **Connect** to establish the connection with Data Protection Service.

3) Click **OK** at the bottom of the screen to complete the process.

4) To deploy all the configured changes, click **Deploy**.

When the connection is active, the Connect button turns into a Disconnect button, enabling disconnection of Data Protection Service from Forcepoint DLP.

In the Data Protection Service Status area, upon successful connection, the status is marked as **Connected successfully**, the time and date of the connection is displayed, and the **Recheck connection** link is enabled. This link is used to check the connection status in the event of problems. If an error is returned upon checking the connection, the status is listed as **Failed to connect**.



Upon successful connection, you can see Data Protection Service on the System Modules page (Service on the Settings > Deployment > System Modules). See *Deploy to Data Protection Service* (mentioned below).

Error handling

- If Data Protection Service shows the status **Failed to connect**, the module is temporarily unavailable. Click **Connect** or **Recheck Connection** to try to connect again. If the problem continues, contact Forcepoint Technical Support.
- If the JSON file is uploaded for the first time, and when you click **Connect** the connection fails, the status shown is “Never connected”. This is because the Forcepoint Security Manager has never successfully connected to the Data Protection Service. In this case, it is probable that a Data Protection Service was not created. Contact Forcepoint Technical Support for assistance.
- When you contact Forcepoint Technical Support, you can share the following files to help troubleshoot the issue:
  - %DSS_HOME%tomcat\logs\dlp\dlp-all.log
  - %DSS_HOME%mediator\logs\mediator.out

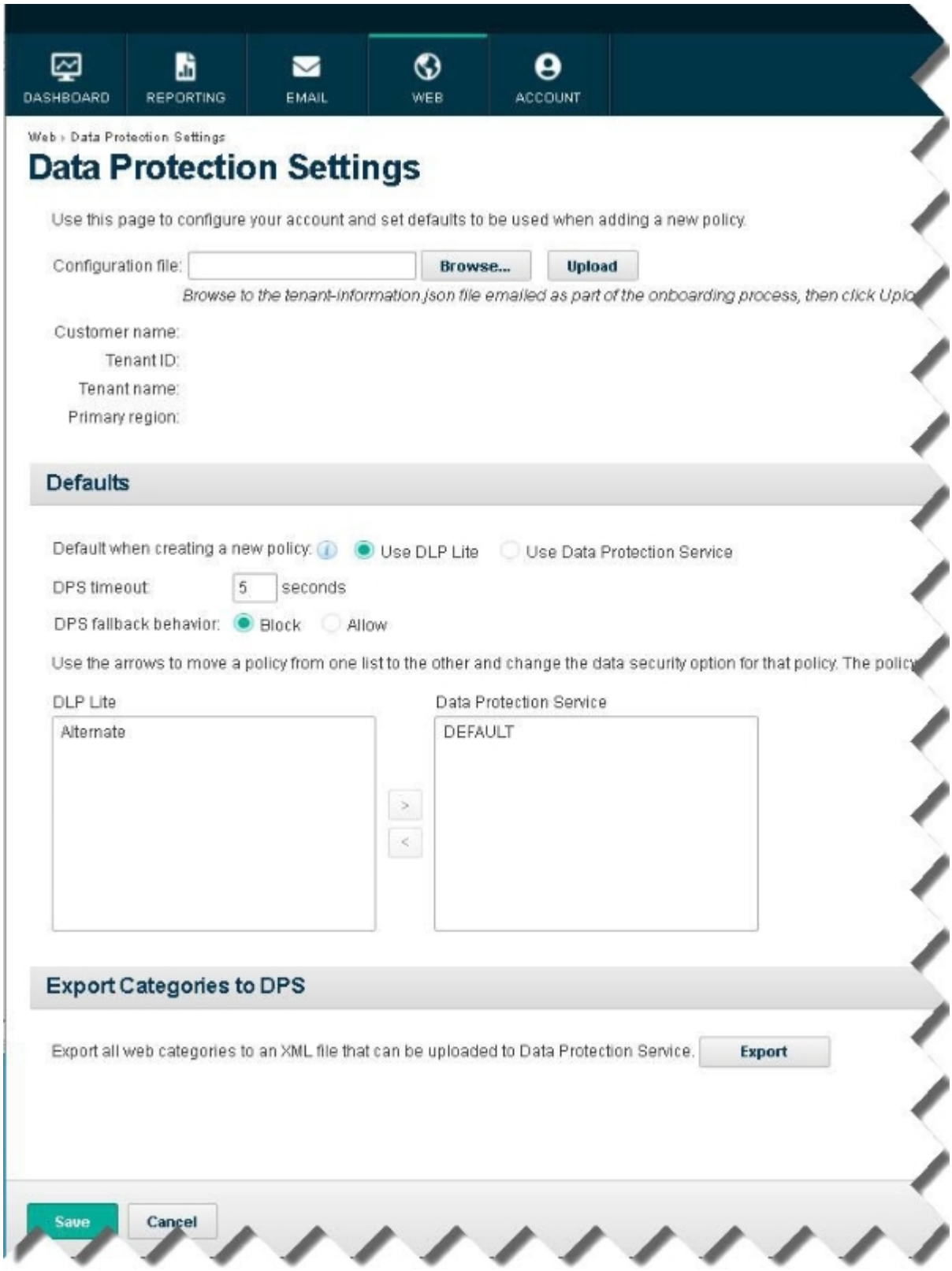
  The default location for %DSS_HOME% is C:\Program Files (x86)\Websense\Data Security\. If you cannot find these files at the default location, check with your Forcepoint Security Manager administrator.

Related concepts

Deploy to Data Protection Service on page 73

Connect Forcepoint Web Security Cloud to Data Protection Service

Use the **Web > Settings > Data Protection Settings** page of the Forcepoint Cloud Security Gateway Portal, also referred to as the cloud portal, to enable and configure the integration with Data Protection Service and Forcepoint DLP.



Upload the configuration file provided by Forcepoint in the fulfillment email you received. This file provides the information needed to connect the cloud service to Data Protection Service and is the same file used when configuring Data Protection Service in the Data module of the on-premises Forcepoint Security Manager.

1) Click **Browse**, then locate and select the JSON file you received from Forcepoint. The filename appears in the Configuration file entry.

2) Click **Upload**.
When the upload is successful, the remaining fields are automatically populated.

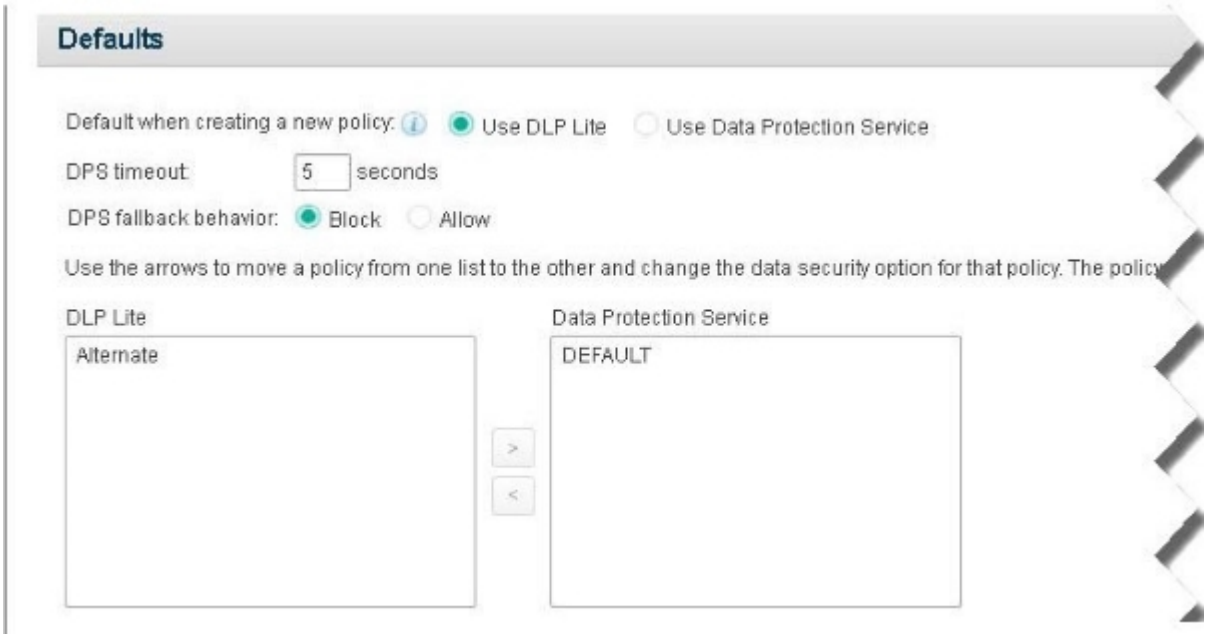
3) Verify that the correct **Customer Name** is shown in the Forcepoint Security Manager. If the Customer Name is incorrect, contact Forcepoint Technical Support.

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

The remainder of the options on the page are used to configure data security for cloud web policies.

Configuring a web policy to use Data Protection Service

Use the **Defaults** section of **Web > Settings > Data Protection Settings** to configure the default values that will be used to define how data security is handled in new web policies.



Steps

1) Select the option to be used, by default, when adding a policy.

   - When **Use DLP Lite** is selected, a Data Security tab is available when a web policy is added.
     When a policy uses DLP Lite, basic data protection is provided by the cloud proxy. A Data Security tab appears when adding a new policy.
   - When **Use Data Protection Service** is selected, a Data Protection tab is available when adding a new policy. Defaults set here are used to populate the new tab, but the default values can be changed. See Data Protection Tab in cloud help for more information.
     When a policy uses Data Protection Service, enterprise data protection is provided and handled by Forcepoint DLP through the data protection service.

     User requests considered to represent a potential data security risk are forwarded to Data Protection Service by the cloud proxy. Data Protection Service then determines the risk and returns a response telling the proxy to block or allow the request.

     When a user is not identified, Data Protection Service returns specific allow or block instructions only if a DLP policy for all sources exists. If all DLP policies apply to specific users or groups, no match is found and the proxy allows the request.

     Important

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

2) Accept the default provided or enter a new value for **DPS timeout**. This value determines the length of time, in seconds, that the cloud service waits for a response from Data Protection Service after sending an inspection request.

3) Select **Block** or **Allow** as the **DPS fallback behavior** if a timeout or other error occurs. If a response from Data Protection Service is not received within the time configured in **DPS timeout**, the user request will be blocked or allowed based on this setting.

4) Use the tables to change the data security selection for existing policies.

   Each list contains the existing policies that currently use the data security option indicated in the table heading. Use the arrows to move selected polices from one list to the other. When the changes are saved, the policies are updated to include the new data security type.

   Note

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

Exporting the Forcepoint Web Security Cloud URL categories

The URL categories used by cloud web policy enforcement must be used in Forcepoint DLP policies. Master database categories, account-level custom categories, and policy-level custom categories are all eligible for use by DLP.

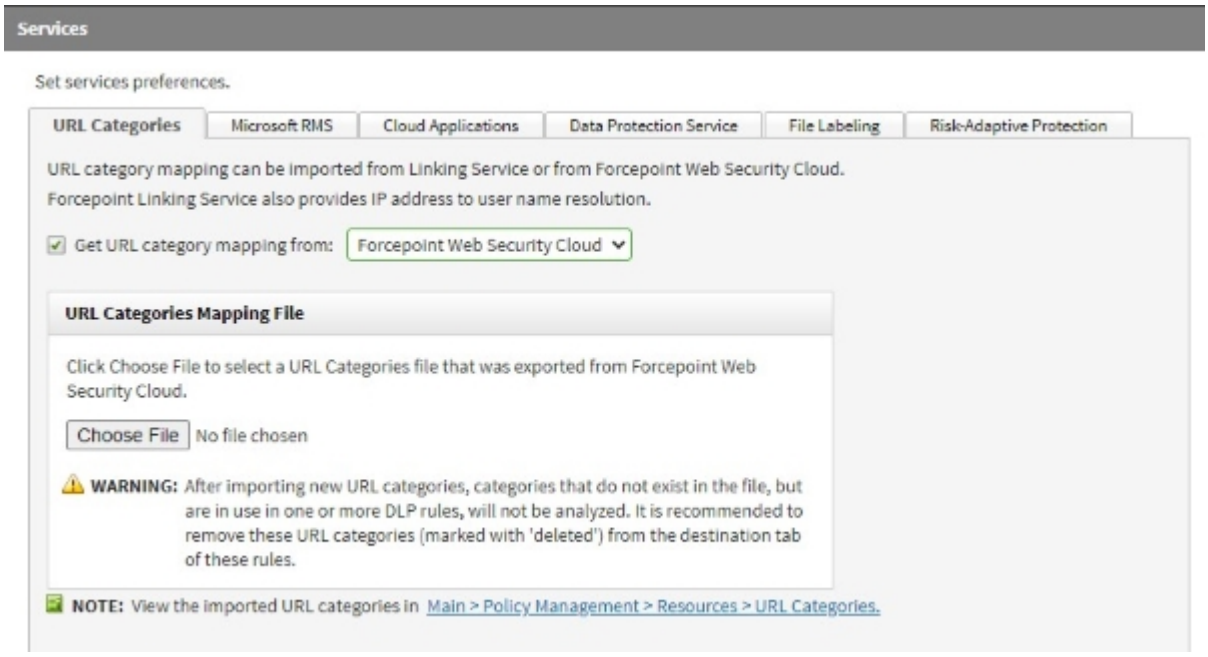
On the **Web > Settings > Data Protection Settings** page of the cloud portal, click **Export** in the **Export Categories to DPS** section to create an xml file containing all web categories, including Master Database categories, account-level custom categories, and policy-level custom categories. This file can then be uploaded to Data Protection Service and the categories can be used when defining Forcepoint DLP policies.

The **Export** button is not available for users with **View Configuration** web permissions.

Import URL categories to Forcepoint DLP

After the Data Protection Service is activated, you can then import cloud URL categories previously exported from Forcepoint Web Security Cloud. This is done using the XML file with a list of categories created in the export process from Forcepoint Web Security Cloud. See *Exporting the Forcepoint Web Security Cloud URL categories* (mentioned below).

In the URL Categories tab (**Settings > General > Services > URL Categories**), select **Get URL category mapping from**, and then, from the drop-down, select Forcepoint Web Security Cloud. For more information on using Linking Service, see the Forcepoint DLP Administrator Guide.



Importing from Forcepoint Web Security Cloud:

Steps

1) Click **Choose File**, and browse to the location of the XML file with the URL categories.

2) Select the file, and then click **OK**. The file is uploaded to the server.

3) Repeat as many times as needed (multiple files can be uploaded, one by one).

Important

- If you previously worked with Linking Service, and thus already have URL categories in your rules, and now want to import URL categories using an XML file, note that categories imported via XML from Forcepoint Web Security Cloud will override the existing rules. This can cause missing categories or conflicts, and it is highly recommended that you review your rules after importing new URL categories and make sure they are using valid categories.
- If any of the following properties are missing for a URL category in the XML file, the DLP manager ignores the category, and it is not added to the database nor is it listed in the Security Manager:
  - Name
  - Predefined/Custom
  - Parent (note that “root” is a valid value)
- If a URL category is corrupted (for example, is missing an ID number), it is recommended that you remove it from the XML file before uploading.

Related concepts

Exporting the Forcepoint Web Security Cloud URL categories on page 66

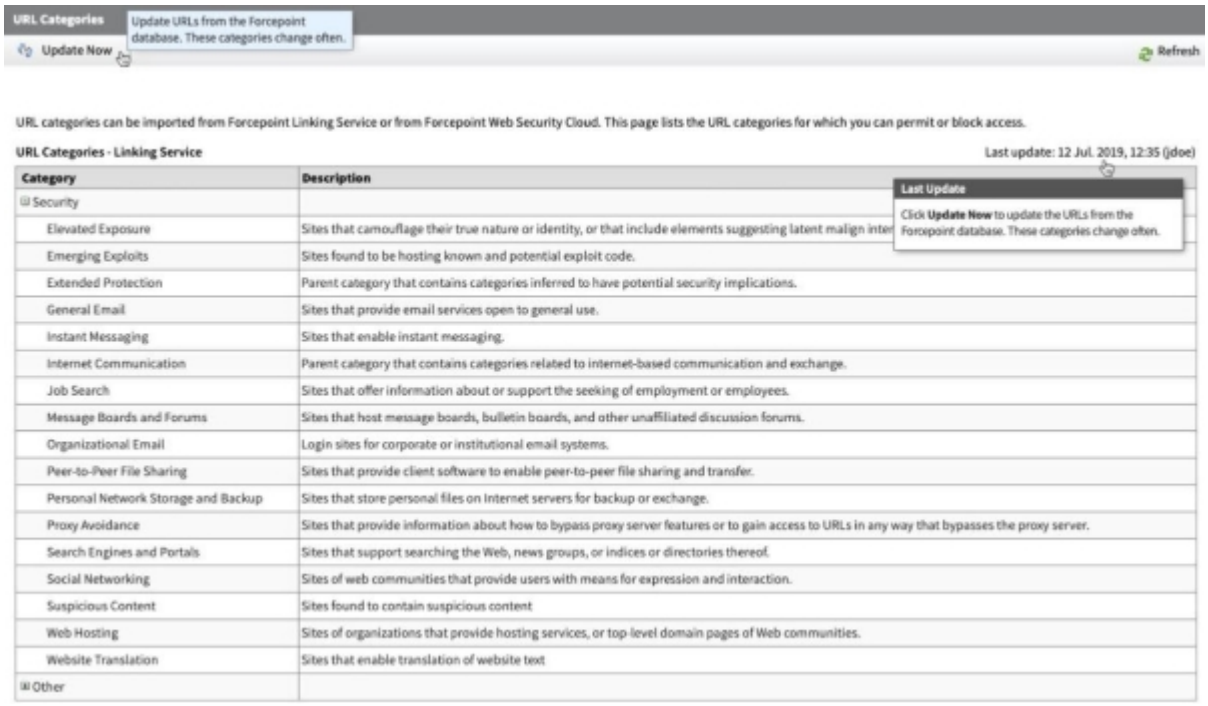
Using URL Categories in DLP policies in the Forcepoint Security Manager

Viewing and updating URL categories

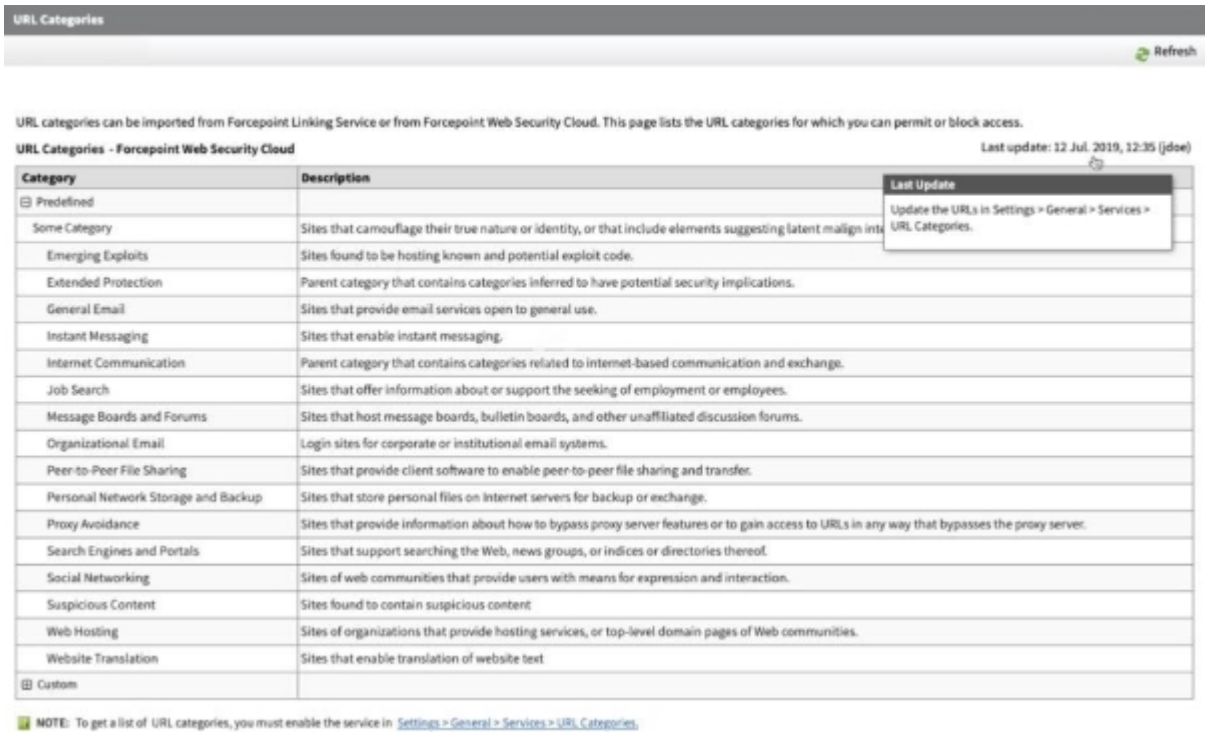
Viewing and updating URL categories (**Policy Management > Resources > URL Categories**) is different depending on whether you imported the categories using Linking Service or from Forcepoint Web Security Cloud, using an XML file.

For example, if the categories were uploaded using Linking Service, there is an **Update Now** button at the top of the screen that imports an updated list of categories from the cloud. If you perform an update, and categories you use in your rules have been deleted, they do not automatically disappear from your system, but they will no longer be analyzed. In this case, an alert is displayed, recommending that you manually delete the URL categories from destination tab of the rules.

The time and date of the last update is displayed, as well as the name of the administrator who performed the update.



If you imported the URL categories from Forcepoint Web Security Cloud, there is no update button. A tooltip in the time and date of the last update includes an instruction that updates can be performed using the XML import method.

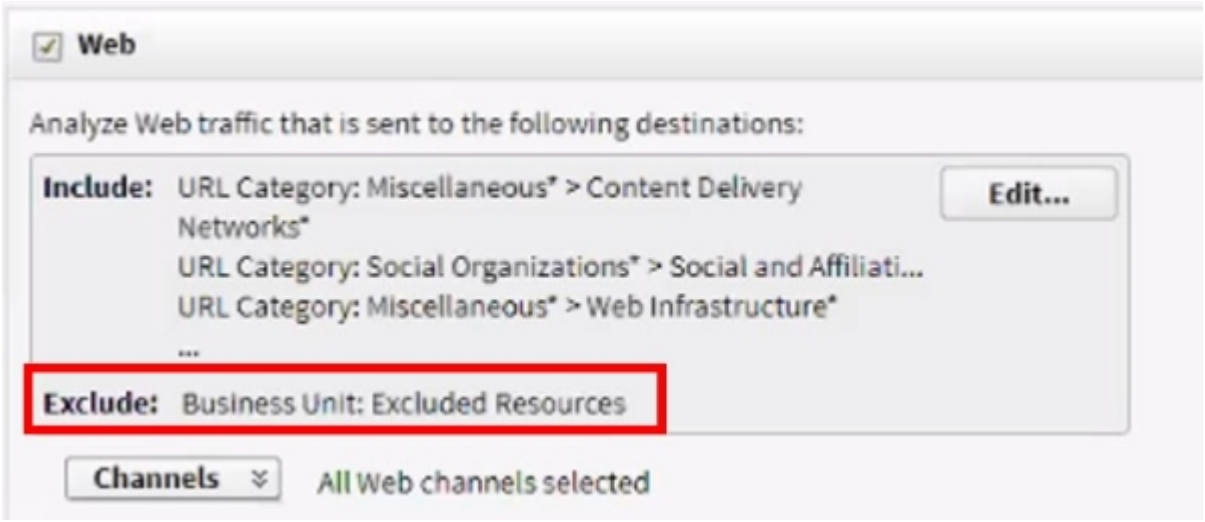


URL categories imported from Forcepoint Web Security Cloud are also indicated as either predefined or custom categories.

URL categories in rule destinations

Adding a URL category to a rule destination

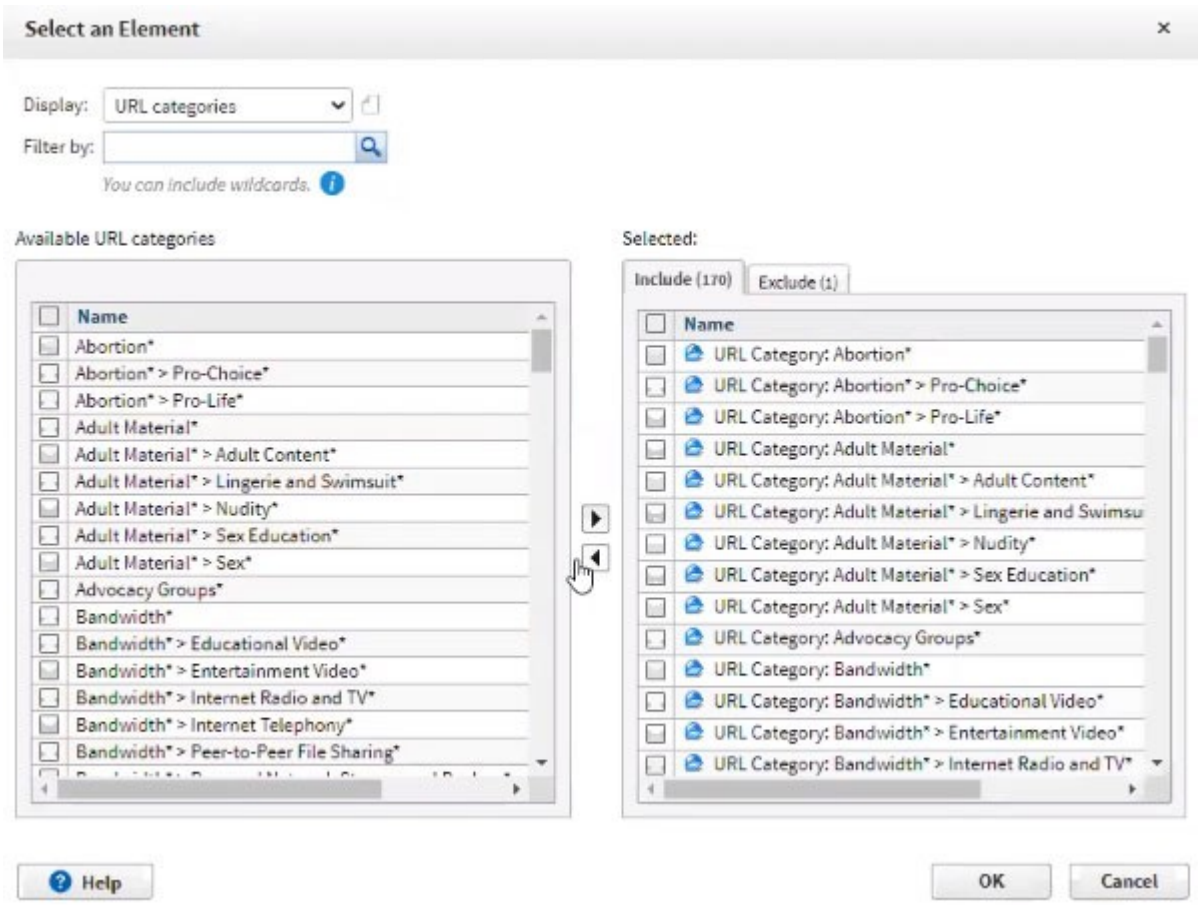
1) In the Destination tab (**Policy Management > Policy Rule > Destination**), click**Edit** in the web traffic destination area:



Note

When creating a custom policy, in the rule's destination, for the Web channel, by default there is a “Business Unit: Excluded Resources” list in the **Exclude** section, which defines trusted domains that should not be tracked. If you want to track one of these domains, remove it from the **Excluded Resources** on the **Policy Management> Resources> Business Unit** page.

The Select an Element window appears:



2) Select **URL Categories** from the **Display** drop-down to view all the categories imported from Forcepoint Web Security Cloud, which are marked by asterisks (*).

3) Move categories to the **Selected > Included** tab as needed, to enforce them.

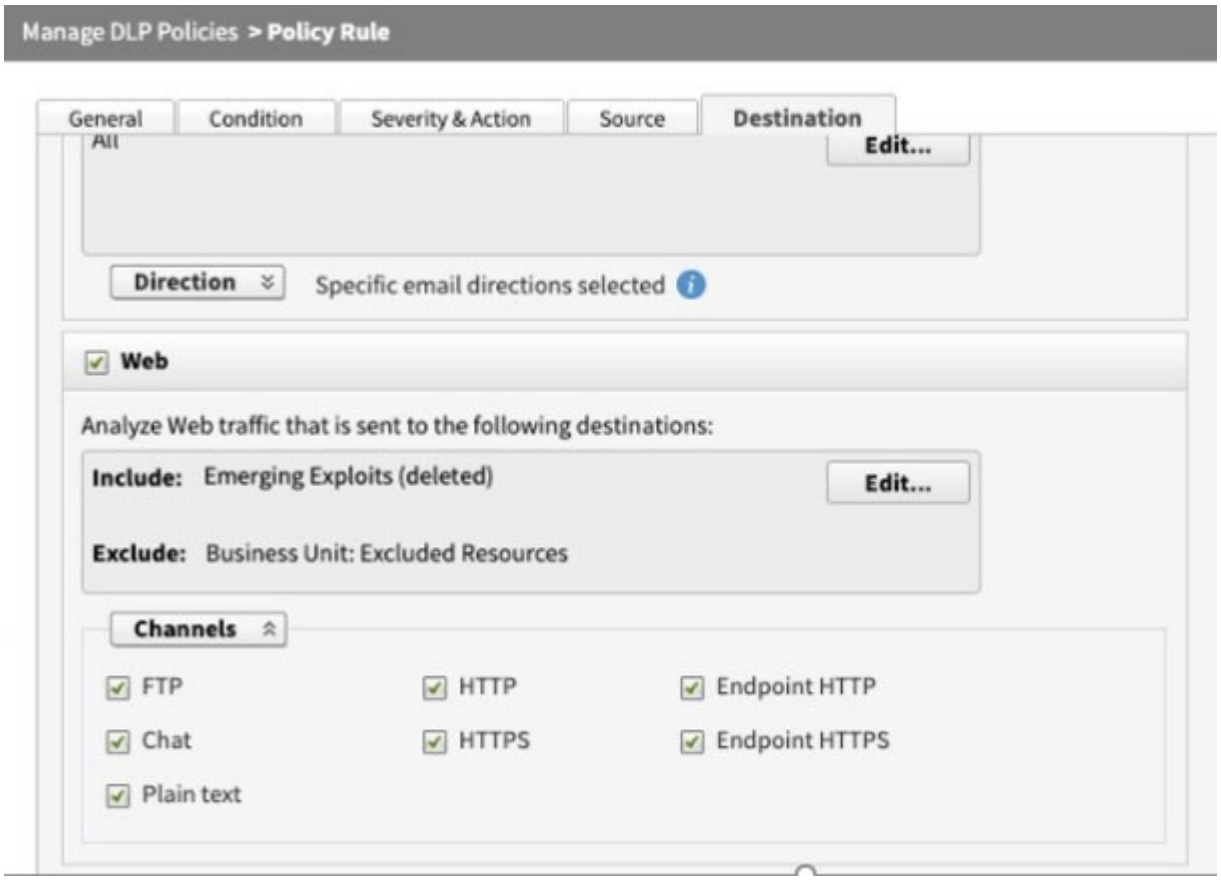
4) Click **OK**.

5) To deploy all the configured changes, click **Deploy**.

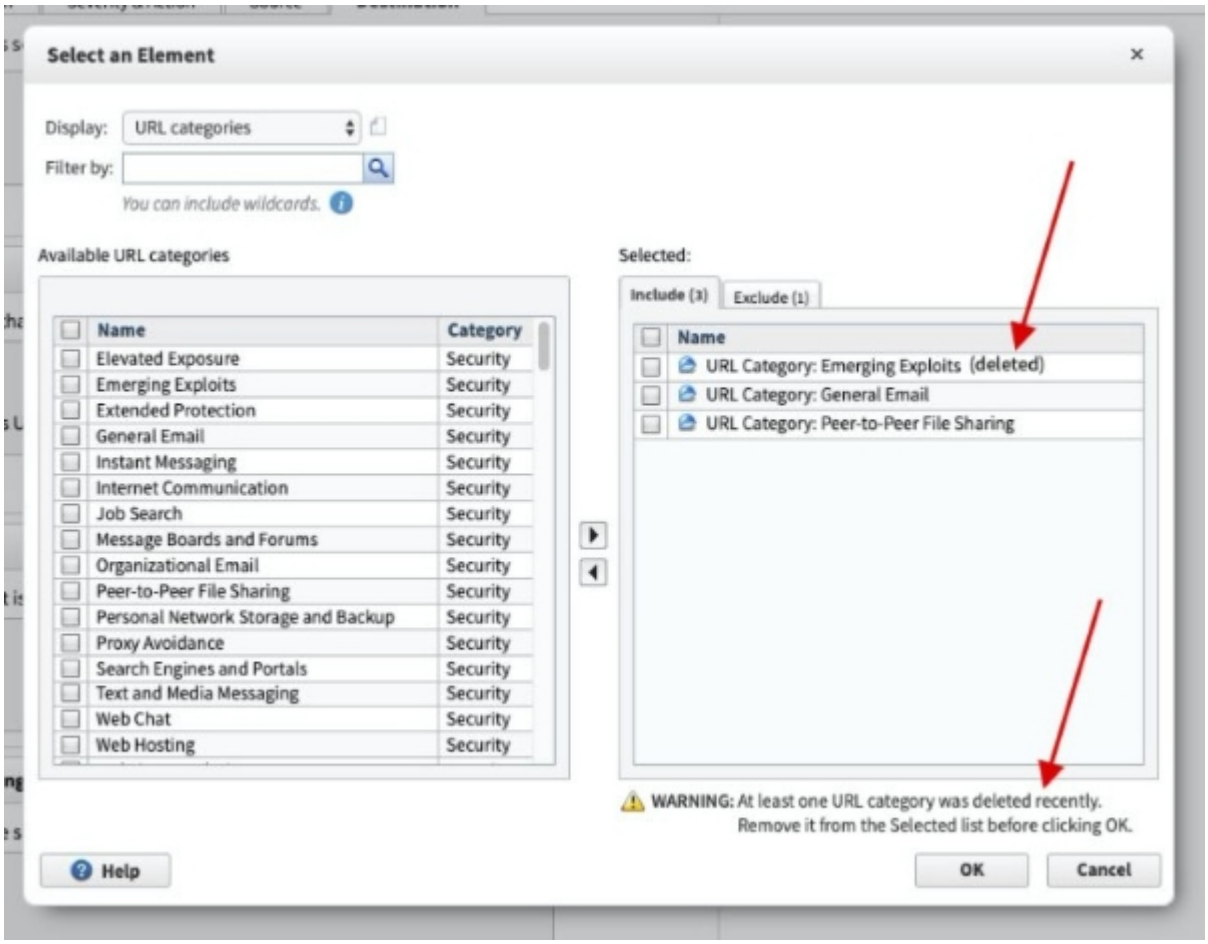
Deleted URL categories

When URL categories are imported (either using Linking Service or the Forcepoint Web Security Cloud XML file), the current URL categories list is deleted, and the new list is saved to the database. URL categories that were used in a rule and now do not exist anymore, are shown as deleted (**Policy Management > Policy Rule > Destination**).

The deleted status as it appears in the Destination tab:

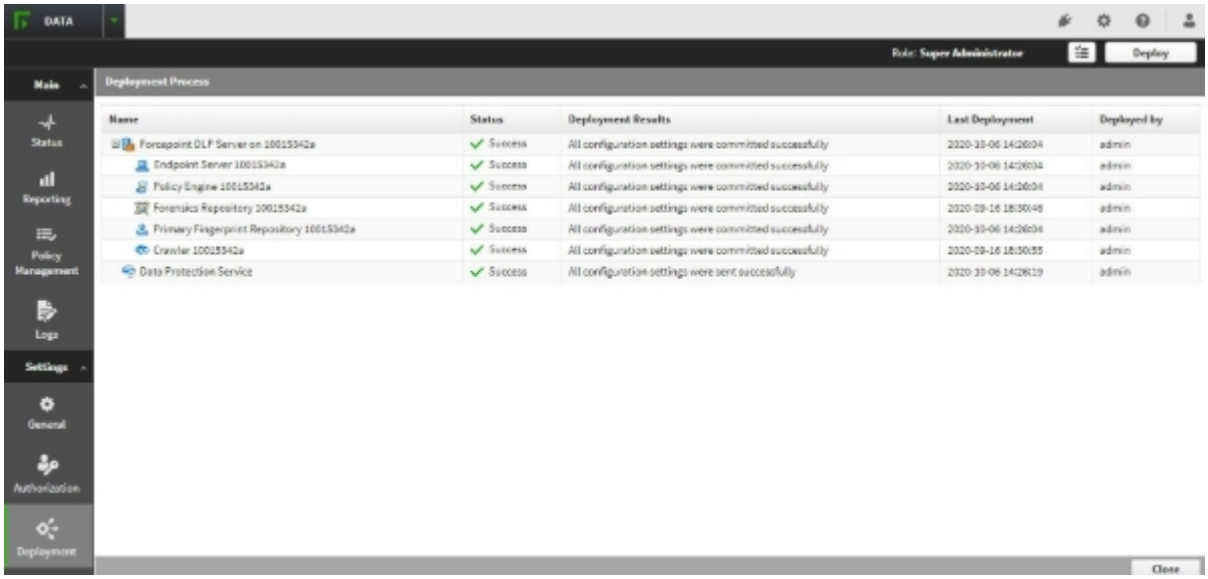


The deleted status of categories as it appears in the selection screen:

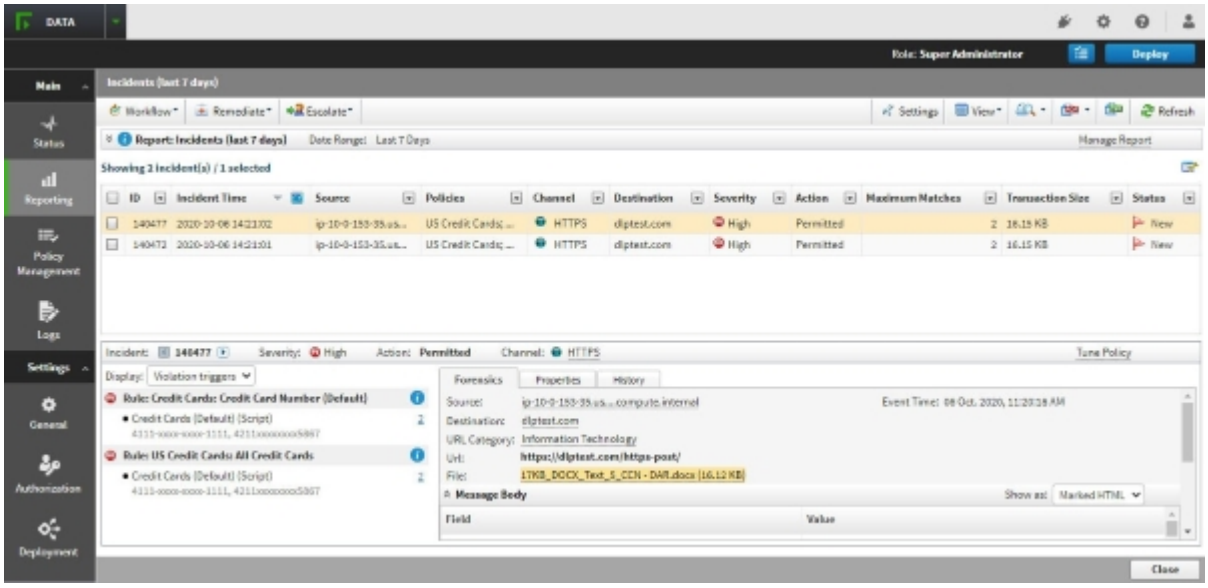


Deploy to Data Protection Service

Deploy the configuration to Data Protection Service by clicking **Deploy**, and begin receiving incidents in the DLP Manager.



View DLP incident reports



Viewing and managing reports for the **web traffic is** the same as for the on-premises DLP. The main change involves what is displayed for a DLP incident:

- **Source:** User email or login name
- **Destination:** Host name and URL categories

> **Note**
>
> URL Categories imported from Forcepoint Web Security Cloud are marked with an asterisk (*), while URL Categories mapped using Linking service are not.

- **Channel:** HTTP or HTTPS

Verifying the integration

When the Forcepoint DLP and Forcepoint Web Security Cloud integration is completed and working correctly, web traffic will appear in the DLP incident reports.