FORCEPOINT
POWERED BY Raytheon

Forcepoint DLP and Forcepoint CASB

Forcepoint DLP Cloud Applications and Forcepoint CASB Integration Guide

Version 2020 R3

Published 2020

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

Last modified: **20-July-2020**

CONTENTS

Introduction

License Information

Configuring the Forcepoint DLP and Forcepoint CASB connection

Creating and configuring cloud applications

Configuring activity monitoring

Introduction

Forcepoint DLP customers can extend their DLP policies to supported enterprise cloud applications, such as Office 365, G Suite, Box, and ServiceNow, via the DLP Cloud Applications and Forcepoint CASB licenses.

- **Forcepoint DLP Cloud Applications**: Provides the cloud hosted DLP Service (DPS)/DLP Agents, and supports API-based, near real-time analysis, data discovery, and file sharing controls for supported cloud applications.
- **Forcepoint CASB**: Provides real-time inline controls for supported cloud applications using the CASB Cloud Gateway infrastructure (known in this guide as DLP Cloud Proxy) which integrates with the cloud-hosted DLP Cloud Service.

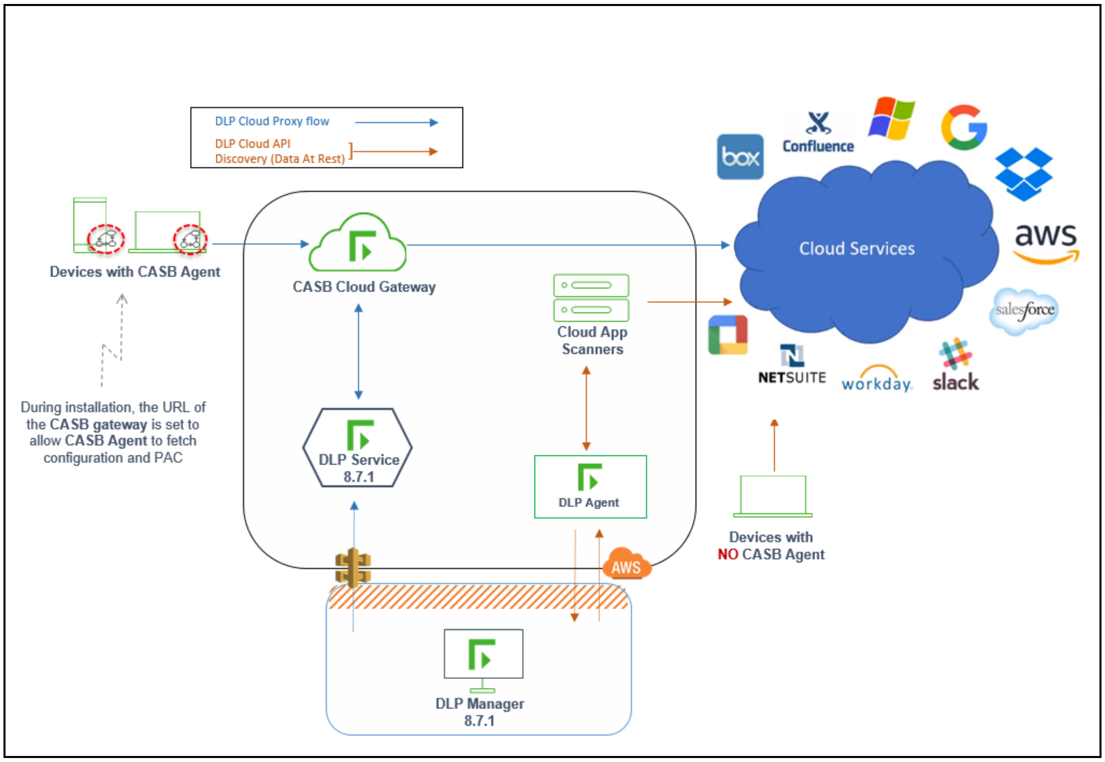
✎ **Note:** Both licenses are required to have the full set of capabilities covering API-based and real-time inline controls for supported cloud applications.

Access to the CASB Portal is provided in both licenses. This guide provides an overview of how to configure the integration between the Forcepoint Security Manager and Forcepoint CASB, and how to configure DLP policies for supported cloud applications.

As highlighted in the diagram below, the integration is achieved via bi-directional communication between the customer-deployed Forcepoint Security Manager server, the cloud-hosted DLP Service/Agents, and Forcepoint CASB cloud infrastructure. Within this guide and the Forcepoint Security Manager user interface, Forcepoint uses the following terms to describe the different interactions with supported cloud applications.

- **DLP Cloud API** (available since Forcepoint DLP 8.5.0): Leveraging an API connection made to the supported cloud application, this option provides near real-time analysis soon after the operation occurs. For example, auditing uploads, downloads, and sharing files.
- **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 supported 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 analysis as the operation 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, in Forcepoint DLP 8.7.1, a new resource type is available, Cloud Application. This means that rules and action plans can be configured to apply to specific applications, such as Office 365.



Additional documentation

The procedures described in this document are covered in more detail in the Administrator Guides for Forcepoint DLP and Forcepoint CASB. We recommend that you have the following documents available when you complete the procedures in this document:

- Forcepoint DLP Administrator Help
- Forcepoint CASB Administration Guide

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.

DLP term	CASB term	Definition
		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/ Forcepoint CASB integration service to scan data at rest on cloud applications.
DLP Agent (DA)	N/A	An agent that enables the system to access the data necessary to analyze specific types of traffic, or the traffic from specific servers.
DLP Cloud API	API Service provider logs Near real-time	A feature that allows the Forcepoint DLP/ Forcepoint CASB integration service to take action soon after a breach occurs on cloud application operations. The file scan is completed in a very specific time frame.
DLP Cloud Proxy	Proxy Real-time	A feature that allows the Forcepoint DLP/ Forcepoint CASB integration service to take immediate action as a breach occurs on cloud application operations.
DLP Cloud Service (DPS)	N/A	The Forcepoint DLP channel 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"

General flow

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

1. Ensure the Forcepoint Security Manager has the DLP Cloud Applications license activated. See "License Information" on page 5 for more information.
2. Using the details in your fulfillment letter, generate a new API access key in Forcepoint CASB. See "Generate an API access key (optional)" on page 6 for more information.
3. In the Forcepoint Security Manager, start the DLP Cloud Service. See "Start the DLP Cloud Service in the Forcepoint Security Manager" on page 9 for more information.
4. Configure your cloud services as required:

a. DLP Cloud Proxy (inline real-time policy enforcement):

    i. Create new assets in the Forcepoint CASB management portal. See "Add an asset in Forcepoint CASB" on page 14 for more information.

    ii. For each asset, configure a custom policy or a quick policy to ensure that the CASB Gateway sends transactions to Forcepoint DLP for analysis. See "Configure a DLP quick policy in Forcepoint CASB" on page 21 or "Configure a DLP custom policy in Forcepoint CASB" on page 23 for more information.

    iii. Check that the assets are shown in the Forcepoint Security Manager with an **OK** status. See "View the list of Cloud Applications" on page 13 for more information.

    iv. Configure one or more DLP rules using **Destination > Cloud Service > DLP Cloud Proxy**.

    v. Configure one or more DLP action plans using DLP Cloud Proxy operations. See "Configure an action plan with cloud application resources" on page 23 for more information.

b. DLP Cloud API:

    i. Add new cloud applications in the Forcepoint Security Manager, or define new assets in Forcepoint CASB. See "Add a cloud application in the Forcepoint Security Manager" on page 14 or "Add an asset in Forcepoint CASB" on page 14 for more information.

    ii. Check that the assets are shown in the Forcepoint Security Manager with an **OK** status. See "View the list of Cloud Applications" on page 13 for more information.

    iii. For each asset, configure a custom policy or a quick policy to ensure that the CASB Gateway sends transactions to Forcepoint DLP for analysis. See "Configure a DLP quick policy in Forcepoint CASB" on page 21 or "Configure a DLP custom policy in Forcepoint CASB" on page 23 for more information.

    iv. Configure one or more DLP rules using **Destination > Cloud Service > DLP Cloud API**.

    v. Configure one or more DLP action plans using DLP Cloud API operations. See "Configure an action plan with cloud application resources" on page 23 for more information.

c. Cloud data discovery:

    i. Add new cloud applications in the Forcepoint Security Manager, or define new assets in Forcepoint CASB. See "Add a cloud application in the Forcepoint Security Manager" on page 14 or "Add an asset in Forcepoint CASB" on page 14 for more information.

    ii. Check that the assets are shown in the Forcepoint Security Manager with an **OK** status. See "View the list of Cloud Applications" on page 13 for more information.

    iii. Create a discovery scan in the Forcepoint Security Manager. See "Enable cloud data discovery (data at rest) in the Forcepoint Security Manager" on page 18 for more information.

License Information

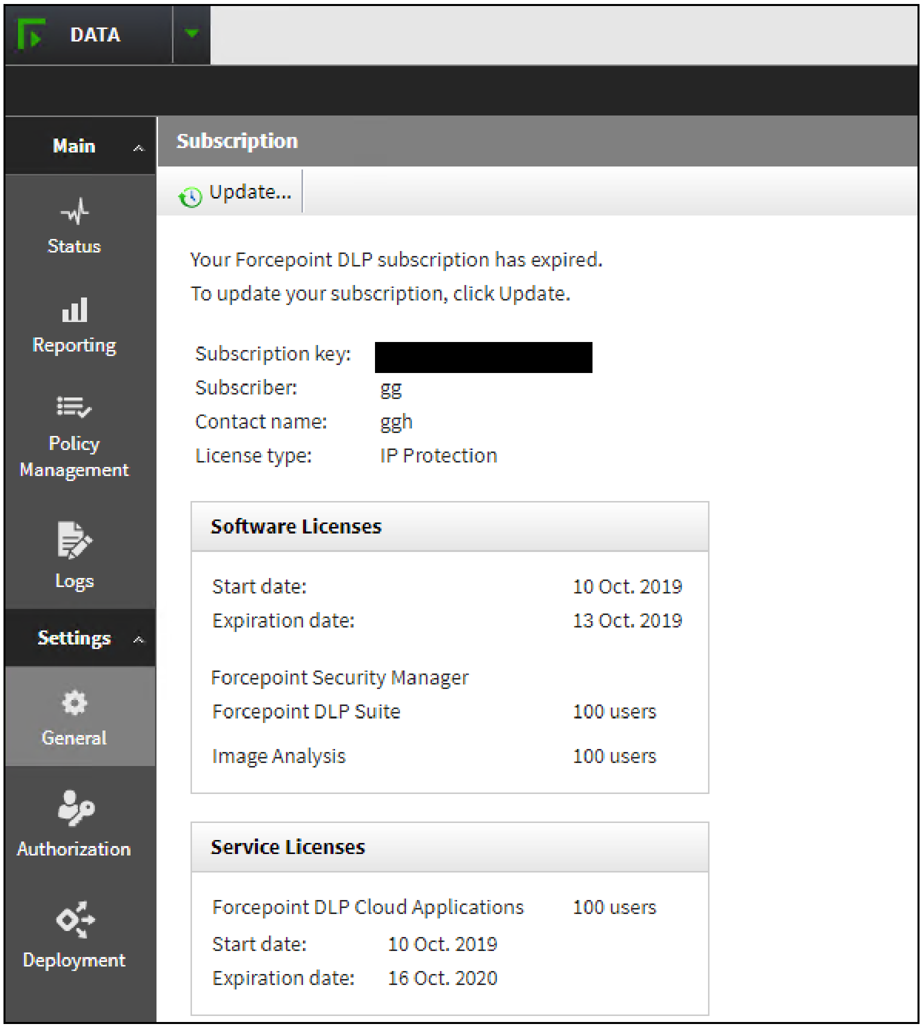
After DLP Cloud Applications has been ordered, you will receive:

1. A new or updated DLP XML license file that includes DLP Cloud Applications.
2. A fulfillment communication that includes the following information:
   - The access key ID
   - The access key secret
   - The service URL

✎ **Note:** If you did not receive the access key ID and secret in a fulfillment letter, you can generate the key in Forcepoint CASB (if you have access to Forcepoint CASB). See "Generate an API access key (optional)" on the next page for more information.

After you receive the license, you will enter the information in the Forcepoint Security Manager to connect Forcepoint DLP with Forcepoint CASB. See "Start the DLP Cloud Service in the Forcepoint Security Manager" on page 9 for more information.

To check that the DLP Cloud Applications license is active in the Forcepoint Security Manager, go to **Settings > General > Subscription**:



Your Forcepoint DLP subscription has expired.
To update your subscription, click Update.

Subscription key:	[redacted]
Subscriber:	gg
Contact name:	ggh
License type:	IP Protection

Software Licenses

Start date:	10 Oct. 2019
Expiration date:	13 Oct. 2019
Forcepoint Security Manager	
Forcepoint DLP Suite	100 users
Image Analysis	100 users

Service Licenses

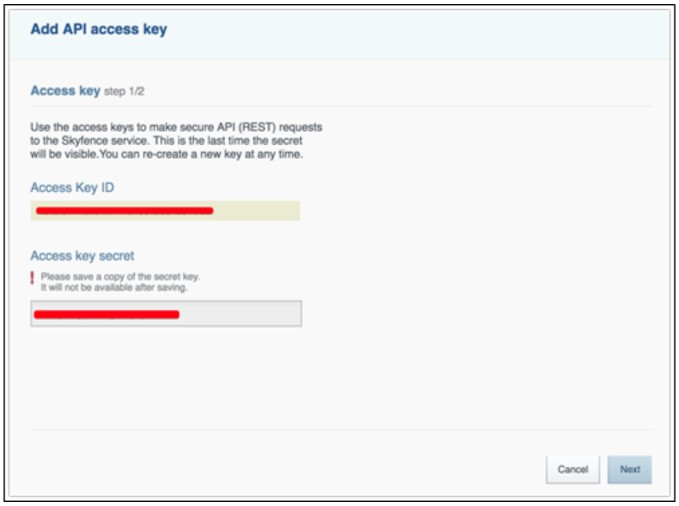
Forcepoint DLP Cloud Applications		100 users
Start date:	10 Oct. 2019	
Expiration date:	16 Oct. 2020	

Under **Service Licenses**, verify that the **Forcepoint DLP Cloud Applications** license is shown. To integrate with Forcepoint CASB, Forcepoint DLP customers must have the Forcepoint DLP Cloud Applications license.

Generate an API access key (optional)

If you do not have an API access key, you can generate one in the Forcepoint CASB management portal.

1. Log on to the Forcepoint CASB management portal.
2. Go to **Settings > API**.
3. Enable API Access at the top of the page.
4. Click **Add API Access Key** and write down the **Access Key ID** and **Access key secret**.



Add API access key

Access key step 1/2

Use the access keys to make secure API (REST) requests to the Skyfence service. This is the last time the secret will be visible.You can re-create a new key at any time.

Access Key ID

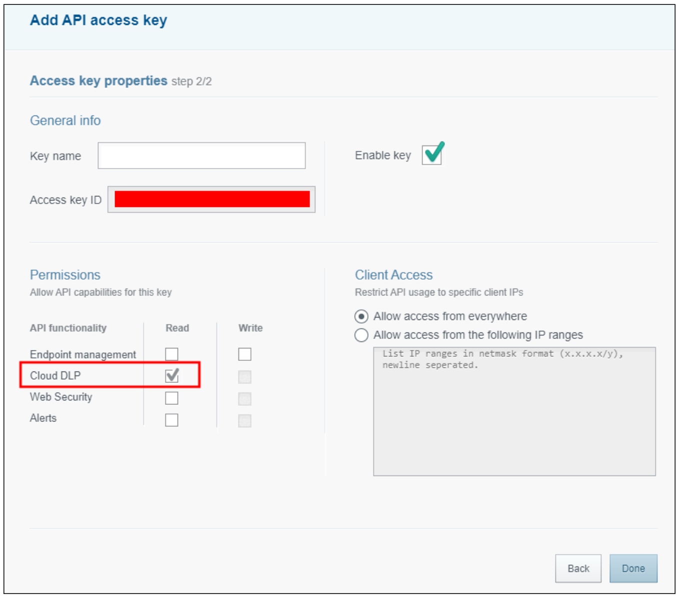
[redacted]

Access key secret

! Please save a copy of the secret key. It will not be available after saving.

[redacted]

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**.



Add API access key

Access key properties step 2/2

General info

Key name

Enable key ☑

Access key ID [redacted]

Permissions

Allow API capabilities for this key

API functionality	Read	Write
Endpoint management	□	□
Cloud DLP	☑	□
Web Security	□	□
Alerts	□	□

Client Access

Restrict API usage to specific client IPs

● Allow access from everywhere

○ Allow access from the following IP ranges

List IP ranges in netmask format (x.x.x.x/y), newline seperated.

6. Click **Done**.

Use this API access key in the Forcepoint Security Manager when you configure the DLP Cloud Service.

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 (DPS) / DLP Cloud Proxy
- Forcepoint Security Manager to DLP Agent (DA) / 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 the following ports:

- For DLP Cloud Proxy:
  - Port 443
- For DLP Cloud API:
  - Port 443
  - Ports 17500-17515
- For Cloud Data Discovery:
  - Port 443
  - Ports 17500-17515

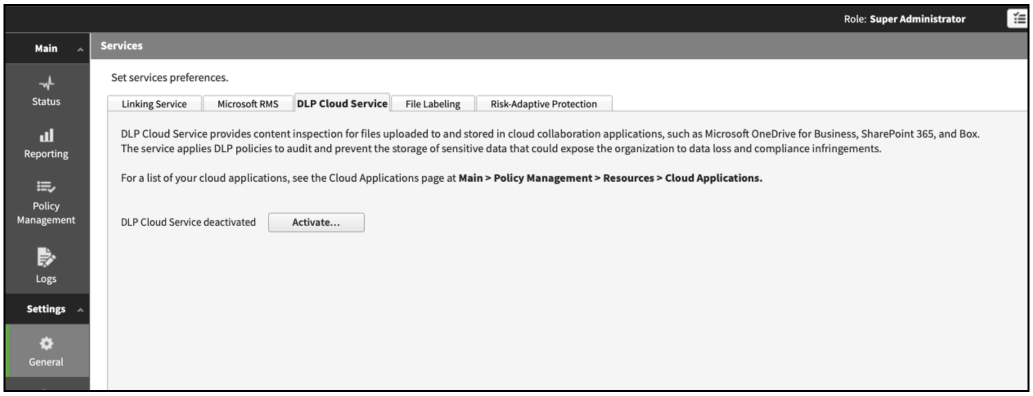
Port 443 must be open to allow communication between the Forcepoint Security Manager and Forcepoint CASB management portal IP addresses. Ports 17500-17515 must be open for DLP Cloud API and Cloud Data Discovery to allow communication between the Forcepoint Security Manager and the DA.

Start the DLP Cloud Service in the Forcepoint Security Manager

Use the **DLP Cloud Service** tab of the **Settings > General > Services** page to connect, disconnect, and configure the DLP Cloud Service.

Note: For users familiar with versions of Forcepoint DLP lower than 8.7.1, most of the functionality that used to be available in **Settings > Services > CASB** is now on this page. This is the only place where you can define DLP Cloud API applications. You can also launch the Forcepoint CASB management portal.

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



Set services preferences.

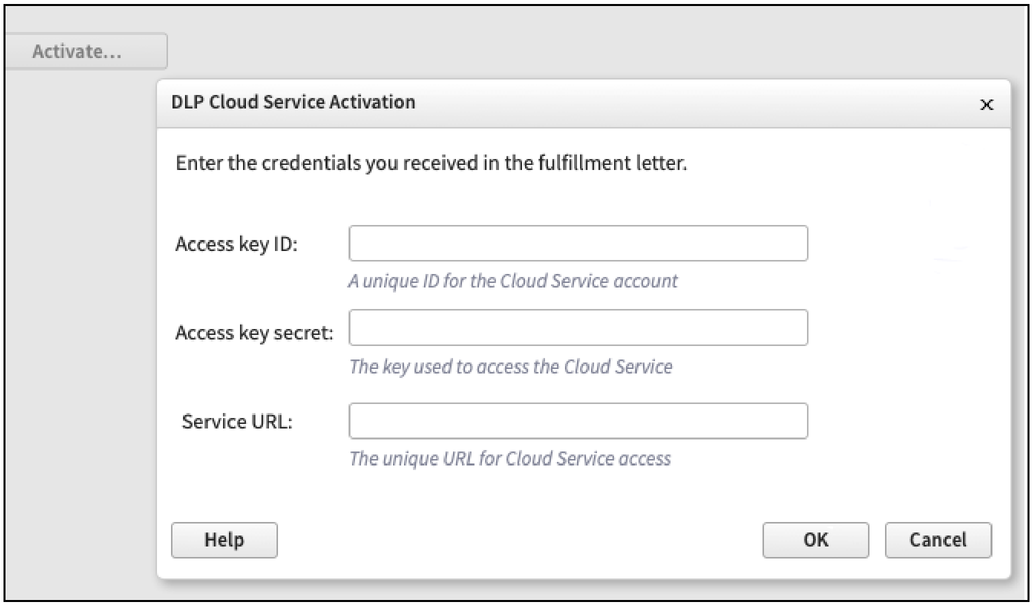
DLP Cloud Service provides content inspection for files uploaded to and stored in cloud collaboration applications, such as Microsoft OneDrive for Business, SharePoint 365, and Box. The service applies DLP policies to audit and prevent the storage of sensitive data that could expose the organization to data loss and compliance infringements.

For a list of your cloud applications, see the Cloud Applications page at **Main > Policy Management > Resources > Cloud Applications.**

DLP Cloud Service deactivated

Note: The DLP Cloud Service tab is shown only if the Forcepoint Security Manager has an XML file with the DLP Cloud Applications license.

2. Click **Activate**. The **DLP Cloud Service Activation** dialog box opens:


Activate...

DLP Cloud Service Activation

Enter the credentials you received in the fulfillment letter.

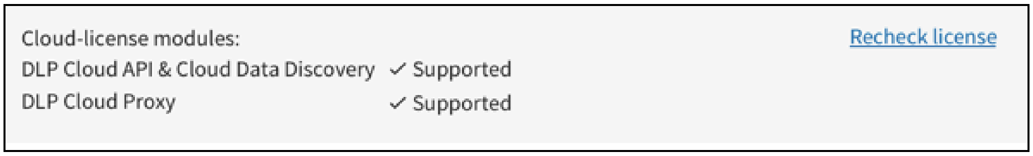
Access key ID: *A unique ID for the Cloud Service account*

Access key secret: *The key used to access the Cloud Service*

Service URL: *The unique URL for Cloud Service access*

3. Enter the following information from the Forcepoint CASB fulfillment letter:
   a. The **Access key ID**
   b. The **Access key secret** for the account
   c. The **Service URL**
4. Click **OK**.

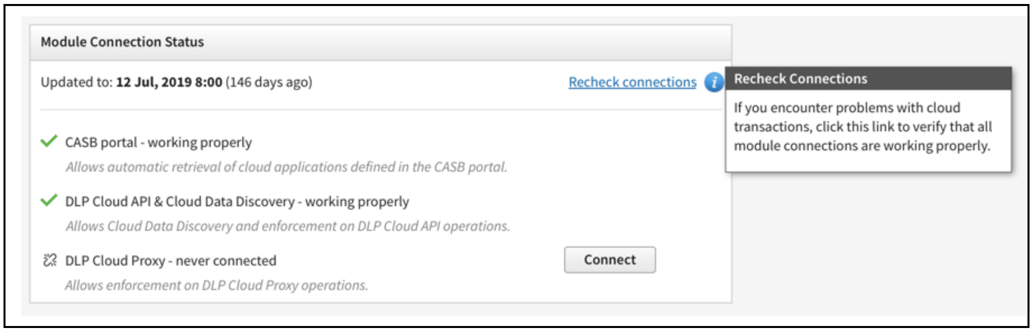
   The connection process is initiated. This might take some time to complete.
5. Upon successful activation, a list of supported DLP Cloud Service modules is shown:


Cloud-license modules:

DLP Cloud API & Cloud Data Discovery	✓ Supported
DLP Cloud Proxy	✓ Supported

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.

6. The **Module Connection Status** section on this page indicates the connection status for each DLP Cloud Service module. In this section, you can do the following:
   - Click **Recheck connections** if the information shown is not up to date or the connection is not working properly.
   - Click **Connect** to connect a module that has never before been activated (for example, if you upgraded your Forcepoint DLP version, or added a new license).



Module Connection Status

Updated to: **12 Jul, 2019 8:00** (146 days ago)

Recheck Connections

If you encounter problems with cloud transactions, click this link to verify that all module connections are working properly.

✓ CASB portal - working properly

Allows automatic retrieval of cloud applications defined in the CASB portal.

✓ DLP Cloud API & Cloud Data Discovery - working properly

Allows Cloud Data Discovery and enforcement on DLP Cloud API operations.

DLP Cloud Proxy - never connected

Allows enforcement on DLP Cloud Proxy operations.

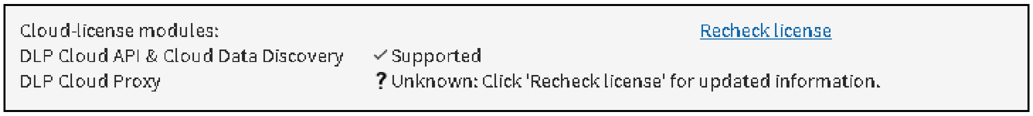
After the connection is established between Forcepoint DLP and Forcepoint CASB, you can:

- Create an asset in the Forcepoint Security Manager. See "Add a cloud application in the Forcepoint Security Manager" on page 14 for more information.
- Create an asset in Forcepoint CASB. See "Add an asset in Forcepoint CASB" on page 14 for more information.
- Configure a Cloud API or Cloud Proxy policy in the Forcepoint Security Manager. See "Configure DLP policies in the Forcepoint Security Manager" on page 17 for more information.
- Configure a Cloud API or Cloud Proxy policy in Forcepoint CASB. See "Configure a DLP custom policy in Forcepoint CASB" on page 23 for more information.
- Configure and run a discovery scan in the Forcepoint Security Manager. See "Enable cloud data discovery (data at rest) in the Forcepoint Security Manager" on page 18 for more information.
- Configure and run a discovery scan in Forcepoint CASB. See "Enable data at rest discovery in Forcepoint CASB" on page 19 for more information.

Activate the DLP Cloud Proxy feature 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. Otherwise, the DLP Cloud Proxy feature will not be activated after the upgrade, even though you are connected to the Forcepoint CASB portal.

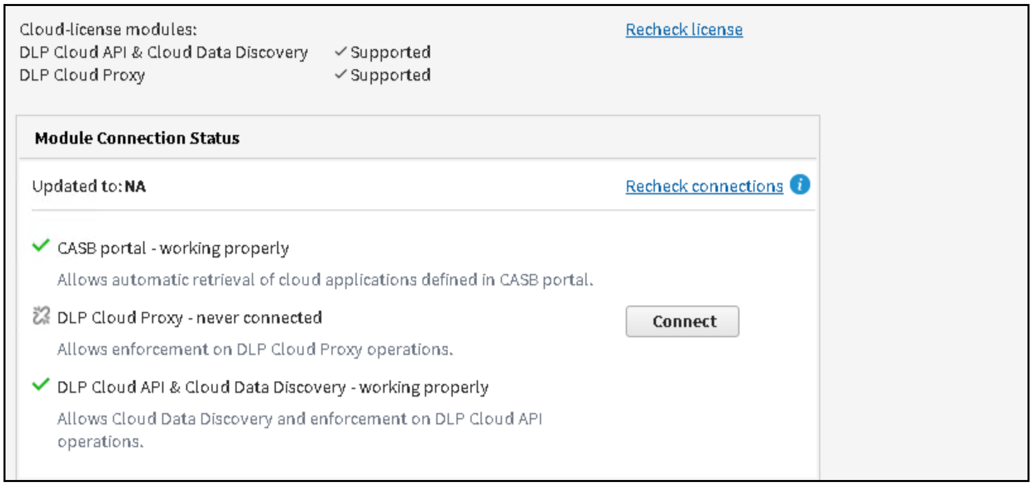
1. In the Forcepoint Security Manager, go to **DATA > Settings > General > Services**, then select the **DLP Cloud Service** tab. The DLP Cloud Proxy license status is **Unknown**.

   Cloud-license modules: Recheck license
   DLP Cloud API & Cloud Data Discovery ✓ Supported
   DLP Cloud Proxy ? Unknown: Click 'Recheck license' for updated information.

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

   Under the **Module Connection Status** section, the DLP Cloud Proxy now shows a **never connected** status.

   Cloud-license modules: Recheck license
   DLP Cloud API & Cloud Data Discovery ✓ Supported
   DLP Cloud Proxy ✓ Supported

   Module Connection Status

   Updated to: **NA** Recheck connections

   ✓ CASB portal - working properly
   Allows automatic retrieval of cloud applications defined in CASB portal.

   DLP Cloud Proxy - never connected
   Allows enforcement on DLP Cloud Proxy operations.

   ✓ DLP Cloud API & Cloud Data Discovery - working properly
   Allows Cloud Data Discovery and enforcement on DLP Cloud API operations.

3. Click **Connect**. The DLP Cloud Proxy status should now be **working properly**.

Creating and configuring cloud applications

The new DLP Cloud Service requires a new 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 Cloud Applications 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 **CASB Properties** page, where you can edit the cloud application settings.

  > **Note:** You cannot edit DLP Cloud Proxy properties. You can only edit the properties for cloud applications defined for both DLP Cloud API and cloud data discovery. Cloud applications that are only defined for DLP Cloud Proxy cannot be edited.

- **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. If an API connection has been successfully configured with the 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. If an API connection has been successfully configured with the 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.

Creating new cloud applications

Before you can analyze the content from a cloud application, you must first create the cloud application record in Forcepoint DLP, or the equivalent asset in Forcepoint CASB. If a cloud application that supports a proxy connection is created in Forcepoint CASB, it is automatically synced to Forcepoint DLP.

Add a cloud application in the Forcepoint Security Manager

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. In the **CASB Properties** window, configure the cloud application settings.

   For information about configuring the API connection for the cloud application, see "Configure the cloud application API connection in the Forcepoint Security Manager" on the next page.

   For information about configuring the cloud data discovery settings for the cloud application, see "Configuring cloud data discovery scan settings" on page 18.

Edit a cloud application in the Forcepoint Security Manager

1. In the Forcepoint Security Manager, go to **DATA > Policy Management > Resources > Cloud Applications**.
2. Click the **Application Name** for the cloud application.
3. In the **CASB Properties** window, configure the API connection settings for the cloud application.

✎ **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 CASB Properties page. Only DLP Cloud API properties can be edited here.

Add an asset in Forcepoint CASB

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**.

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. See "Configure a cloud application API connection in Forcepoint CASB" on the next page for more information.

Edit an asset in Forcepoint CASB

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

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.

Configure the cloud application API connection in the Forcepoint Security Manager

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 CASB portal opens in a new tab to allow configuration of the selected application.

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

   The DLP Cloud Service uses the connection to retrieve activity logs, scan files at rest, and retrieve user lists. It does not store the user credentials.

4. Under **Service Type**, in the **API Based CASB** section, specify whether or not to **Enable activity import** and allow the DLP Cloud Service to access and import user activity logs for the selected cloud application.
5. In the **Mitigation Settings** section, configure an **Archive folder** within the selected cloud application for files moved or copied in response to a DLP incident. A Drive email entry field is available for applications that need to know a user's identity for copying files to the archive folder.
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 that the message file can be copied to the cloud application.
8. To save the changes and return to the DLP Cloud Services tab, click **OK**.
    - The new application is added to the cloud applications list, which shows the application name, type, description, and status.
    - The Edit link opens the properties in a new CASB window, which can be used to update configuration for the application.

   The new application is added to the cloud applications list even if configuration is canceled before this step is completed. Use the Edit link to finish configuration if necessary.
9. If needed, click **Return to the Security Manager**.

   This functionality can be used to exit the CASB portal at any point and continue working in the Forcepoint Security Manager.

✎ **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

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.

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

Configure DLP policies in the Forcepoint Security Manager

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

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 (**General**, **Condition**, **Severity & Action**, and **Source** tabs). Configuring a rule for a cloud application is similar to any DLP rule. For more information, see the *Forcepoint DLP Administrator Guide*.
4. On the **Destination** tab, in the **DLP Cloud Service** section, select **DLP Cloud API**, **DLP Cloud Proxy**, or both.

   If you select **DLP Cloud API**, all cloud applications configured in Forcepoint DLP are automatically included in the rule.

   If you select **DLP Cloud Proxy**, you must also select at least one cloud application and at least one operation:

   a. Under **DLP Cloud Proxy**, click the **Edit** button.

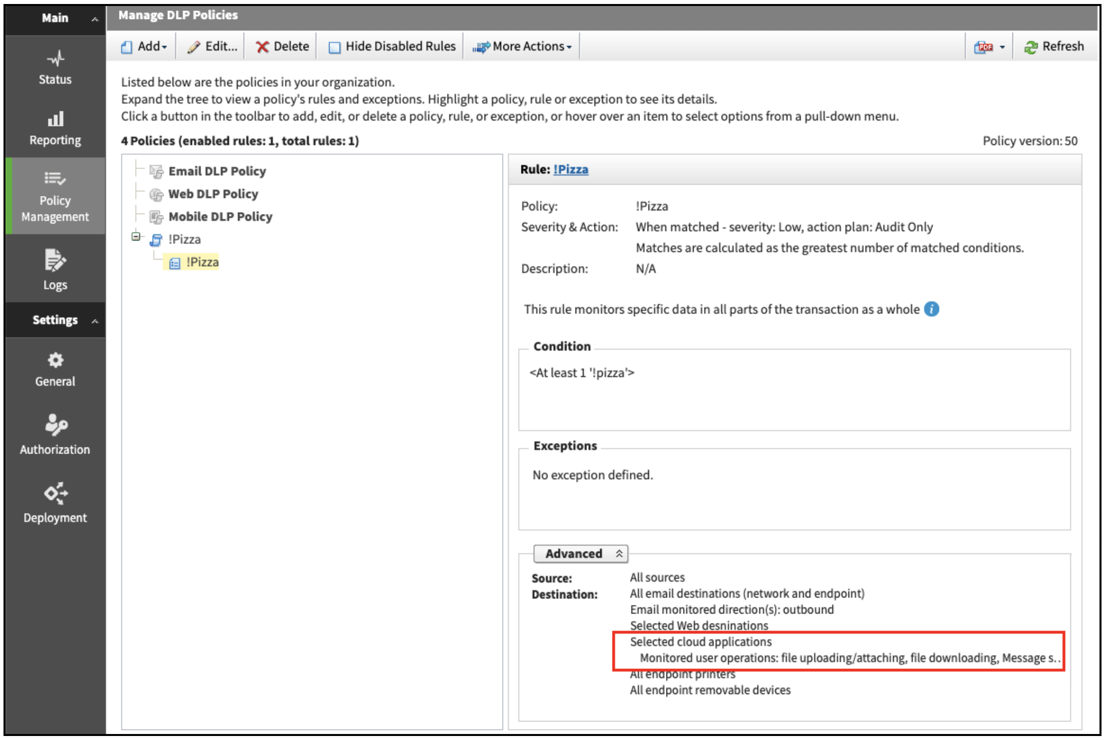
   b. Select one or more cloud applications in the **Available Elements** list.

   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 **DLP Cloud Proxy**.

   e. Select one or both of the operations: **File uploading/attaching** or **File downloading**.
5. Click **Next** to show a summary of the rule.
6. Click **Finish** to save the rule.

In the Manage DLP Policies screen, the rule summary (right pane) shows whether the cloud application is selected as a Destination.



Listed below are the policies in your organization.
Expand the tree to view a policy's rules and exceptions. Highlight a policy, rule or exception to see its details.
Click a button in the toolbar to add, edit, or delete a policy, rule, or exception, or hover over an item to select options from a pull-down menu.

4 Policies (enabled rules: 1, total rules: 1) Policy version: 50

Rule: !Pizza

Policy: !Pizza
Severity & Action: When matched - severity: Low, action plan: Audit Only
Matches are calculated as the greatest number of matched conditions.
Description: N/A

This rule monitors specific data in all parts of the transaction as a whole

<At least 1 '!pizza'>

No exception defined.

Source: All sources
Destination: All email destinations (network and endpoint)
Email monitored direction(s): outbound
Selected Web desninations
Selected cloud applications
Monitored user operations: file uploading/attaching, file downloading, Message s..
All endpoint printers
All endpoint removable devices

Configuring cloud data discovery scan 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 (data at rest) in the Forcepoint Security Manager

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 CASB portal opens in a new tab to allow configuration of the selected application.

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

The DLP Cloud Service uses the connection to retrieve activity logs, scan files at rest, and retrieve user lists. It does not store the user credentials.

4. In the **Data at Rest** section:

    a. Mark the **Enable data at rest discovery** check box to activate the data at rest discovery scan for this cloud application.

    b. Enter the folder path you want scanned.

    c. Click **Excluded Subfolders** to specify any subfolders you want excluded from the scan.

5. In the **Mitigation Settings** section, configure an **Archive folder** within the selected cloud application for files moved or copied in response to a DLP incident. A Drive email entry field is available for applications that need to know a user's identity for copying files to the archive folder.

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 that the message file can be copied to the cloud application.

8. To save the changes and return to the DLP Cloud Service tab, click **OK**.

    - The new application is added to the cloud applications list, which shows the application name, type, description, and status.
    - The Edit link opens the properties in a new CASB window, which can be used to update configuration for the application.

    The new application is added to the cloud applications list even if configuration is canceled before this step is completed. Use the Edit link to finish configuration if necessary.

9. If needed, click **Return to the Security Manager**.

    This functionality can be used to exit the CASB portal at any point and continue working in the Security Manager.

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.

Enable data at rest discovery in Forcepoint CASB

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. 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.

5. Expand the **Data Classification** section.
6. 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.
7. Click **Save archive folder settings**.
8. 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.
9. Click **Save quarantine note settings**.

Configuring activity monitoring

To enable the capture of sensitive content in Forcepoint CASB and the analysis of this content in Forcepoint DLP, you must create a new DLP policy or edit an existing policy to add a DLP rule. You can do this in one or more of the following ways:

- Configure a **Forcepoint Data Security DLP** quick policy
- Create a custom policy with the **Forcepoint DLP** predicate
- Configure a **Forcepoint DLP Scan** data classification policy

To analyze sensitive content from the Forcepoint CASB assets in Forcepoint DLP, you must complete the following steps in the Forcepoint Security Manager:

- Configure the policy rules
- Configure an action plan with cloud application resources

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

Configure a DLP quick policy in Forcepoint CASB

Note: You must have Forcepoint DLP v8.7.1 or higher installed for this feature to work with DLP Cloud Proxy. DLP Cloud API is supported on Forcepoint v8.5 and higher.

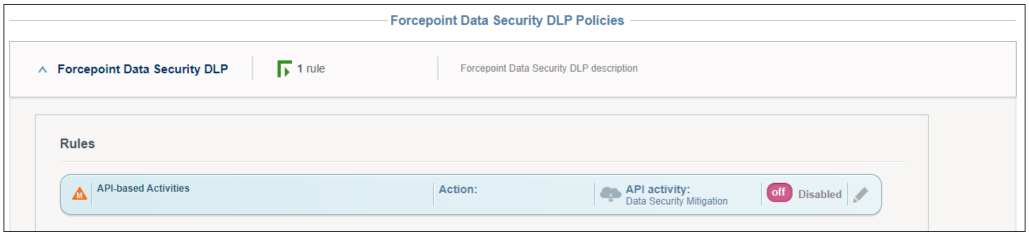
After the Forcepoint DLP and Forcepoint CASB license is active, a new Forcepoint Data Security DLP policy is added to the Data Leak Prevention quick policies list in the Forcepoint CASB management portal.

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

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:

   - If a DLP Cloud API connection is set, an **API activity** rule is shown.
   - If a DLP Cloud Proxy connection is set, a **Proxy activity** rule is shown.



Forcepoint Data Security DLP Policies

Forcepoint Data Security DLP | 1 rule | Forcepoint Data Security DLP description

Rules

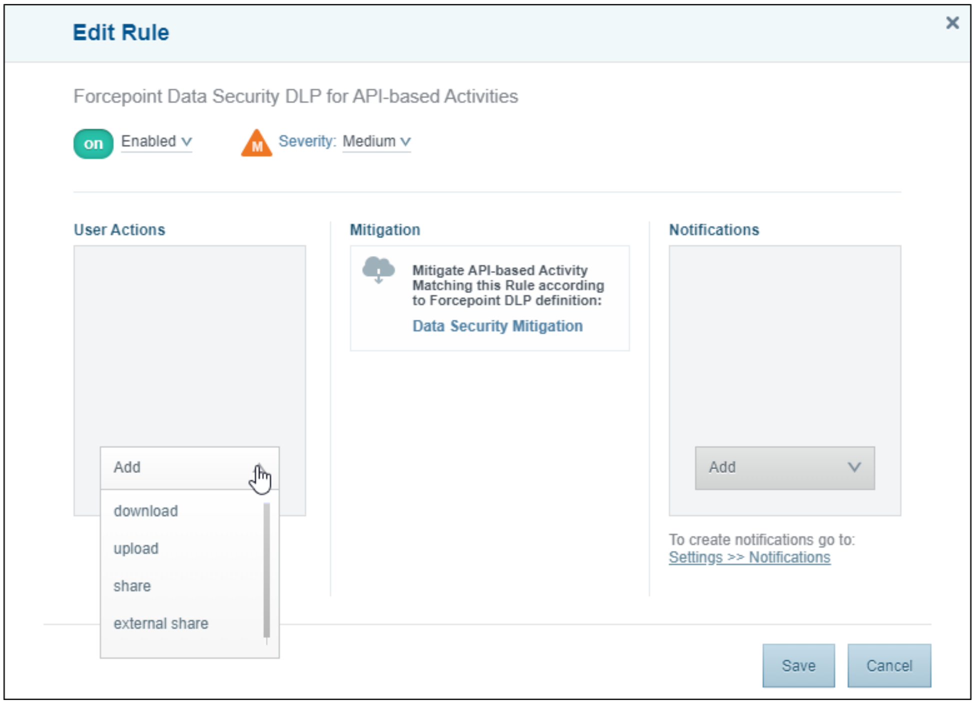
M | API-based Activities | Action: | API activity: Data Security Mitigation | off Disabled

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**.



Edit Rule

Forcepoint Data Security DLP for API-based Activities

on Enabled | M Severity: Medium

User Actions

Add
- download
- upload
- share
- external share

Mitigation

Mitigate API-based Activity Matching this Rule according to Forcepoint DLP definition: Data Security Mitigation

Notifications

Add

To create notifications go to: Settings >> Notifications

Save | Cancel

   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 is set in Forcepoint DLP on the Forcepoint Security Manager.

6. Click **Save**.

Configure a DLP custom policy in Forcepoint CASB

Note: You must have Forcepoint DLP v8.7.1 or higher installed for this feature to work for DLP Cloud Proxy. DLP Cloud API works with Forcepoint DLP v8.5 and higher.

To configure a custom policy for Forcepoint DLP analysis, you must select the **Forcepoint DLP** predicate. You can create a DLP custom policy for DLP Cloud Proxy and DLP Cloud API.

1. In Forcepoint CASB, go to **Audit & Protect > Security Policies > Custom Policy Editor**.
2. Select the cloud application (asset) from the list above the Dashboard.
3. Click **Add Policy**.
4. Create a new custom policy. For more information about creating and configuring a custom policy, see the “Configuring custom access policies” section in the *Forcepoint CASB Administration Guide*.
5. Select the **Forcepoint DLP** predicate located under the **What** drop-down menu.
6. Select the **Action** predicate located under the What drop-down menu.
   - For DLP Cloud Proxy, select either the **download** or **upload** action.
   - For DLP Cloud API, select the **download**, **upload**, **share**, or **external share** action.
7. When you select Forcepoint DLP as a predicate, a new mitigation action is available: **Data Security Mitigation**. If you select this option, the enforcement is done according to the policy's action plan configured in Forcepoint DLP. If you select a different mitigation action, the enforcement is done according to the custom rule created here.
8. Click **Save Policy**.

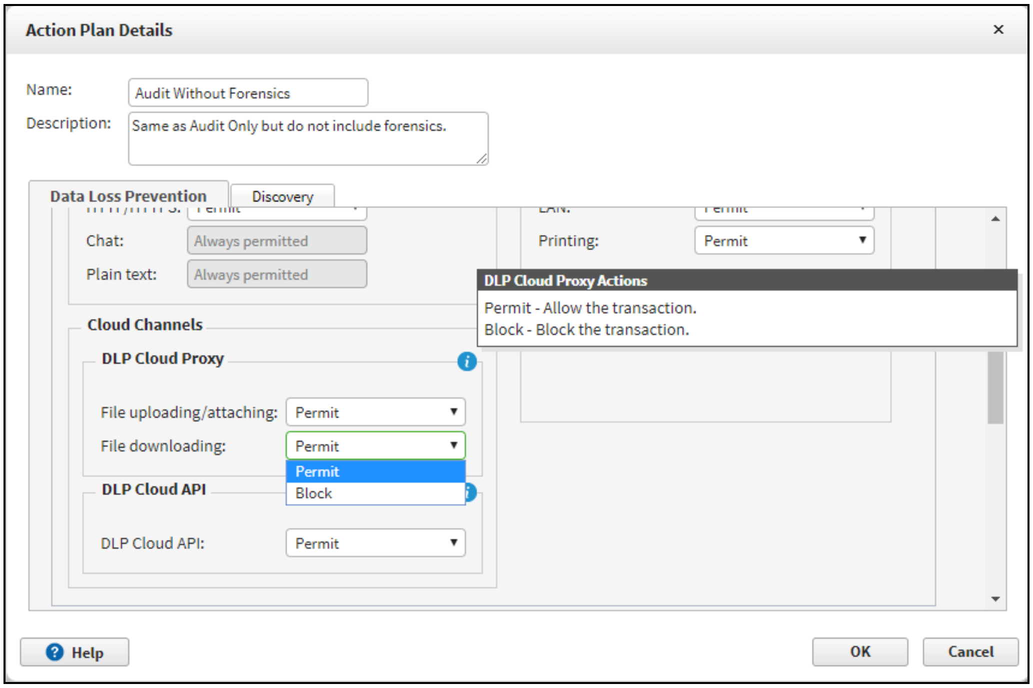
Configure an action plan with cloud application resources

The DLP Cloud Proxy option is only available if you are using Forcepoint DLP 8.7.1 with the **Forcepoint DLP Cloud Applications** license. The DLP Cloud API option is available if you are using Forcepoint DLP 8.5 and higher with the Forcepoint DLP Cloud Applications license. If you do not have this license, you will not see the **Cloud Channels** section.

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 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 all**: Remove all sharing permissions from the file.



Name: Audit Without Forensics

Description: Same as Audit Only but do not include forensics.

Chat: Always permitted

Plain text: Always permitted

Printing: Permit

DLP Cloud Proxy Actions

Permit - Allow the transaction.

Block - Block the transaction.

Cloud Channels

DLP Cloud Proxy

File uploading/attaching: Permit

File downloading: Permit

Permit

Block

DLP Cloud API

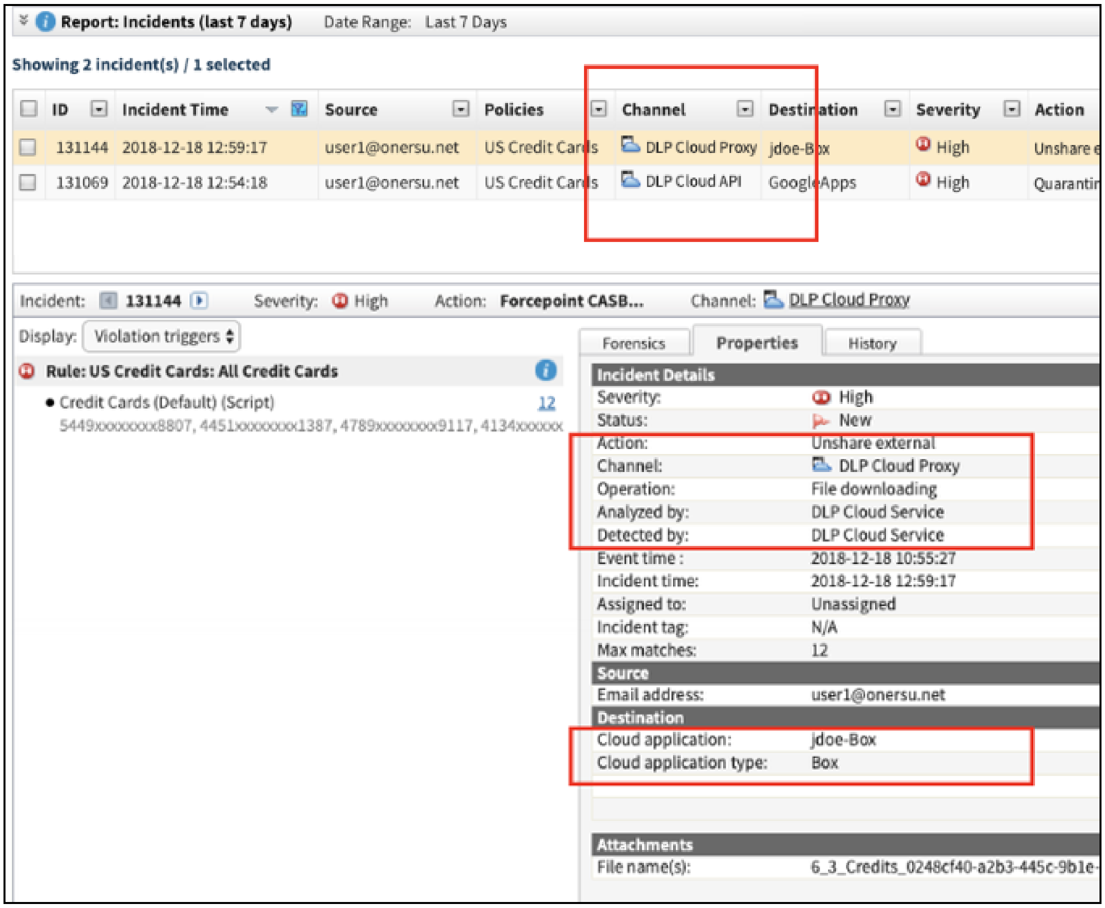
DLP Cloud API: Permit

5. Click **OK**.

View DLP Cloud Services in an incident report in the Forcepoint Security Manager

The new DLP Cloud Services feature has not changed any of the functionality of viewing and managing reports, but has changed the information shown for a DLP incident:

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



Report: Incidents (last 7 days)   Date Range: Last 7 Days

Showing 2 incident(s) / 1 selected

ID	Incident Time	Source	Policies	Channel	Destination	Severity	Action
131144	2018-12-18 12:59:17	user1@onersu.net	US Credit Cards	DLP Cloud Proxy	jdoe-Box	High	Unshare e
131069	2018-12-18 12:54:18	user1@onersu.net	US Credit Cards	DLP Cloud API	GoogleApps	High	Quarantir

Incident: **131144**   Severity: High   Action: **Forcepoint CASB...**   Channel: DLP Cloud Proxy

Display: Violation triggers

Rule: US Credit Cards: All Credit Cards

- Credit Cards (Default) (Script) 12

5449xxxxxxxx8807, 4451xxxxxxxx1387, 4789xxxxxxxx9117, 4134xxxxxx

Incident Details	
Severity:	High
Status:	New
Action:	Unshare external
Channel:	DLP Cloud Proxy
Operation:	File downloading
Analyzed by:	DLP Cloud Service
Detected by:	DLP Cloud Service
Event time :	2018-12-18 10:55:27
Incident time:	2018-12-18 12:59:17
Assigned to:	Unassigned
Incident tag:	N/A
Max matches:	12
Source	
Email address:	user1@onersu.net
Destination	
Cloud application:	jdoe-Box
Cloud application type:	Box
Attachments	
File name(s):	6_3_Credits_0248cf40-a2b3-445c-9b1e-

View incident information in Forcepoint CASB

The new DLP Cloud Services feature has not changed any of the functionality of viewing and managing incidents in Forcepoint CASB. When a DLP policy is triggered, the activity is shown in the corresponding Audit Log and Incident record.

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. For example, if

you enabled the DLP quick policy, the **Forcepoint Data Security DLP for API-based Activities** rule is shown.

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. For example, if you enabled the DLP quick policy, the **Forcepoint Data Security DLP for API-based Activities** rule is shown.
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*.

To view a DLP Cloud incident:

1. In Forcepoint CASB, go to **Audit & Protect > Incidents**.
2. Select the cloud application (asset) from the list above the Dashboard.
3. In the Incidents log, select an incident record to see the detailed information about the incident and the list of activities connected to this incident record.

For more information about incidents in Forcepoint CASB, see the "Monitoring and Investigating Alerts and Incidents" chapter in the *Forcepoint CASB Administration Guide*.

Add a cloud data discovery scan in the Forcepoint Security Manager

Use the **DATA > Policy Management > Discovery Policies > Cloud Discovery Scans > Cloud Discovery Scan Properties** page in the Data Security module of the Forcepoint Security Manager to

Use the Cloud Discovery Scan Properties page in the Data Security module of the Forcepoint Security Manager to create or edit a cloud discovery scan.

To access the Cloud Discovery Scan Properties page:

1. In the Forcepoint Security Manager, go to **DATA > Policy Management > Discovery Policies > Cloud 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. Mark **Enable scan** to enable the cloud 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 data at rest are shown in the drop-down list. Data at rest is enabled for all supported assets in the CASB portal. To disable Data at rest, 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**.