



# CASB

Version 2018 R4

## Integrating Forcepoint Web Security

Integration Guide

## Contents

- Introduction on page 2
- Licensing and provisioning on page 2
- Firewall and network access prerequisites on page 5
- Connecting to the Forcepoint CASB portal on page 6
- Configure Content Gateway filtered locations on page 10
- Import the Forcepoint CASB certificate on page 11
- Configuring the protected cloud apps list on page 12
- Setting up and monitoring Forcepoint CASB policies on protected cloud apps on page 16
- Enroll the Forcepoint CASB device on page 19

# Introduction

---

Forcepoint Web Security customers can purchase Forcepoint CASB, then establish an integration that allows policy enforcement to forward requests made to the selected protected cloud apps (referred to as Assets by Forcepoint CASB) directly to Forcepoint CASB.

The integration can be used for:

- Proxy-based 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

Integration is supported for on-premises Web Security, Cloud Web Security, and Hybrid.

# Licensing and provisioning

---

To integrate with Forcepoint CASB, Forcepoint Web Security customers must subscribe to an additional license called Forcepoint Web Security Cloud App Control.

The method for obtaining the App Control license depends on whether you already have a CASB license.

After you receive the license, you will either apply the new subscription key (on-premises and hybrid customers) or verify that the Forcepoint CASB license is listed in your account (cloud customers).

# Obtain the App Control license if you do not have a CASB license

---

If you are a Forcepoint Web Security customer, and you do not have a Forcepoint CASB license, you must obtain 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.

## Steps

- 1) Contact your Forcepoint salesperson to obtain the Forcepoint Web Security Cloud App Control license.

## Result

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 letter with the Forcepoint Web Security Cloud App Control license, Forcepoint CASB API information, and other information.

## Next steps

After you receive the license, you will either apply the new subscription key (on-premises and hybrid customers) or verify that the new license is listed in your account (cloud customers).

# Obtain the App Control license if you have a CASB license

---

If you are a Forcepoint Web Security customer, and you have a Forcepoint CASB license, you must additionally obtain the Forcepoint Web Security Cloud App Control license.

## Steps

- 1) Contact Forcepoint Support to obtain the Forcepoint Web Security Cloud App Control license.

## Result

You will receive a fulfillment letter 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.

## Next steps

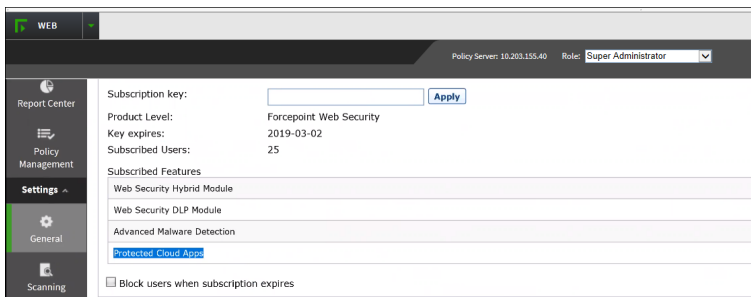
After you receive the license, you will either apply the new subscription key (on-premises and hybrid customers) or verify that the new license is listed in your account (cloud customers).

# Apply the subscription key in the Forcepoint Security Manager

If you are a Forcepoint On-Premises or Hybrid Web Security customer, apply the new subscription key in the Forcepoint Security Manager.

## Steps

- 1) Log on to the Forcepoint Security Manager.
- 2) Go to **General**.
- 3) Paste the subscription key in the **Subscription key** field, then click **Apply**.



## Result

The Forcepoint Security Manager verifies the key syntax, then the Filtering Service attempts to download the Master Database. When this is done, the new CASB Configuration option is available on the **Web > Settings** page.

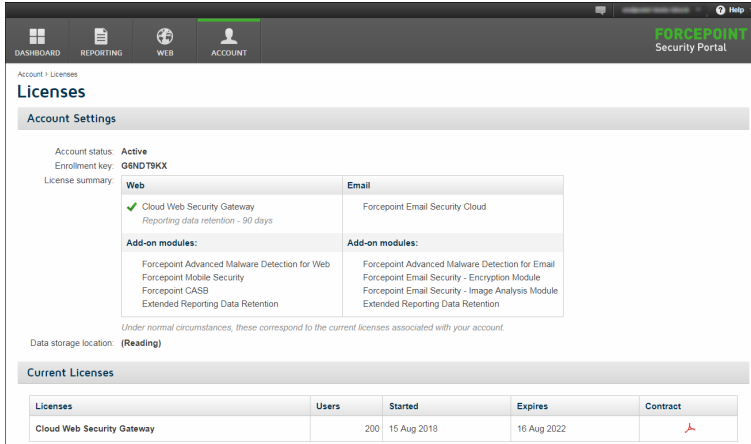
# Verify that the Forcepoint CASB license is listed in the Forcepoint Security Portal

If you are a Forcepoint Web Security Cloud customer, verify that the new Forcepoint CASB license is listed on the Licenses page in the Forcepoint Security Portal.

## Steps

- 1) Log on to the Forcepoint Security Portal.
- 2) Browse to **Account > Licenses**.

3) Verify that the Forcepoint CASB license is listed.



**Next steps**

After the license is active, the new Forcepoint CASB configuration option is available on the **Protected Cloud Apps** page (**Web > Settings > Protected Cloud Apps**).

# Firewall and network access prerequisites

Forcepoint CASB and Forcepoint Web Security integration is based on 2 network connections.

- HTTPS connection between the Forcepoint Security Manager and the Forcepoint CASB management portal for distributing the configuration.
- HTTP tunnel between the Content Gateway and the Forcepoint CASB proxy for traffic forwarding.

If the Forcepoint Security Manager and/or the on-premises Content Gateway are behind your network firewall or any other network access control system, you must configure the following rules.

HTTPS connection between Forcepoint Security Manager and Forcepoint CASB portal	HTTPS connection between Content Gateway and Forcepoint CASB proxy
<p>Allow outbound connection on TCP port 443 (HTTPS) from the FSM to the Internet.</p> <p>If a more specific rule is required, allow the connection to one of the following:</p> <ul style="list-style-type: none"> <li>■ For the US Forcepoint CASB portal: my.skyfence.com</li> <li>■ For the EU Forcepoint CASB portal: my-eu1.skyfence.com</li> </ul>	<p>Allow outbound connection on TCP port 8081 from the Content Gateway to the Internet.</p> <p>If a more specific rule is required, contact Forcepoint Support to receive the relevant Forcepoint CASB proxy information.</p>

# Connecting to the Forcepoint CASB portal

To connect to the Forcepoint CASB portal, you must have an Access key ID and API key secret.

If the CASB API information is not available in the fulfillment letter, you can generate a new API access key in the Forcepoint CASB management portal.

- For Forcepoint On-Premises or Hybrid Web Security customers, you must connect to the Forcepoint CASB portal in the Forcepoint Security Manager.
- For Forcepoint Web Security Cloud customers, you must connect to the Forcepoint CASB portal in the Forcepoint Security Portal.

## Related tasks

[Connect to the Forcepoint CASB portal in the Forcepoint Security Manager on page 7](#)

[Connect to the Forcepoint CASB portal in the Forcepoint Security Portal on page 9](#)

## Generate an API access key

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

### Steps

- 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**.



- 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**.

The screenshot shows the 'Add API access key' configuration page. Under the 'Permissions' section, the 'Web Security' checkbox is checked under the 'Read' column. The 'Enable key' checkbox is also checked. The 'Access key ID' field is highlighted with a red bar. The 'Client Access' section has 'Allow access from everywhere' selected. The 'Back' and 'Done' buttons are at the bottom right.

- 6) Click **Done**.

## Next steps

Use the API access key when you connect to the Forcepoint CASB portal.

# Connect to the Forcepoint CASB portal in the Forcepoint Security Manager

For Forcepoint On-Premises or Hybrid Web Security customers, you must connect to the Forcepoint CASB portal in the Forcepoint Security Manager.

## Before you begin

If your fulfillment letter did not include an API access key, generate one in the Forcepoint CASB management portal.



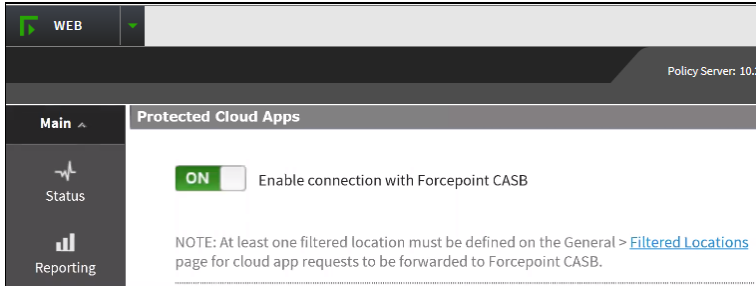
### Important

The Forcepoint Security Manager requires Internet access to successfully connect to the Forcepoint CASB portal (on port TCP 443). If the Forcepoint Security Manager is behind a proxy or firewall, configure the **Use proxy server or firewall** option in the Forcepoint Security Manager (**Settings > General > Database Download**). For more information, see the section about firewall and network access prerequisites.

## Steps

- 1) Log on to the Forcepoint Security Manager.
- 2) Go to **Web > Settings > CASB Configuration > Protected Cloud Apps**.

- 3) Switch **Enable connection with Forcepoint CASB** to **ON** to enable the feature.



- 4) Click **Connect to Forcepoint CASB**.

- 5) Complete the fields using the CASB API information received in the fulfillment letter you received from Forcepoint.

- Access key ID
- API key secret
- Service URL:
  - For the US Forcepoint CASB portal: <https://my.skyfence.com>
  - For the EU Forcepoint CASB portal: <https://my-eu1.skyfence.com>

**Connect to Forcepoint CASB**

Enter your Forcepoint CASB credentials provided in the fulfillment letter to connect to Forcepoint CASB.

Access key ID:

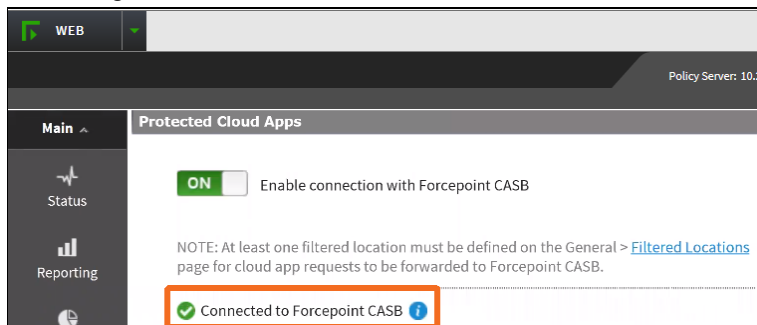
API key secret:

Service URL:

- 6) Click **Connect** to generate a secure connection to Forcepoint CASB.

## Result

A message shows that the connection is successful. Also, a list of all available cloud apps is provided.



### Related concepts

Firewall and network access prerequisites on page 5



# Connect to the Forcepoint CASB portal in the Forcepoint Security Portal

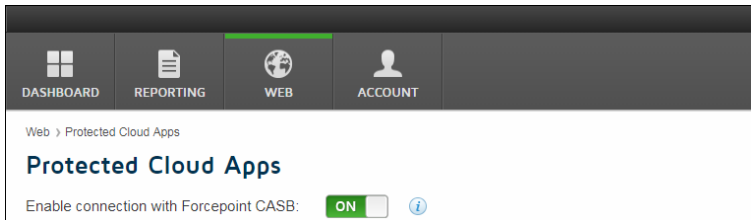
For Forcepoint Web Security Cloud customers, you must connect to the Forcepoint CASB portal in the Forcepoint Security Portal.

## Before you begin

If your fulfillment letter did not include an API access key, generate one in the Forcepoint CASB management portal.

## Steps

- 1) Log on to the Forcepoint Security Portal.
- 2) Go to **Web > Settings > Protected Cloud Apps**.
- 3) Switch **Enable connection with Forcepoint CASB** to **ON** to enable the feature.



- 4) Click **Connect to Forcepoint CASB**.
- 5) Complete the fields using the CASB API information received in the fulfillment letter you received from Forcepoint.
  - Access key ID
  - API key secret
  - Service URL:
    - For the US Forcepoint CASB portal: <https://my.skyfence.com>
    - For the EU Forcepoint CASB portal: <https://my-eu1.skyfence.com>

**Connect to Forcepoint CASB**

Enter your Forcepoint CASB credentials provided in the fulfillment letter to connect to Forcepoint CASB.

Access key ID:

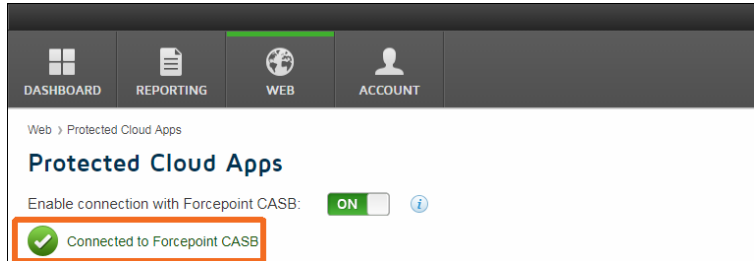
API key secret:

Service URL:

- 6) Click **Connect** to generate a secure connection to Forcepoint CASB.

## Result

A message shows that the connection is successful. Also, a list of all available cloud apps is provided.



# Configure Content Gateway filtered locations

The Forcepoint CASB service requires a list of the egress points from which traffic should be expected.



### Important

This information is only relevant for Forcepoint On-Premises or Hybrid Web Security customers.



### Note

Hybrid Web Security customers do not need to configure the egress points here if their Hybrid environment's public egress IP address of the Content Gateways are already configured.

## Steps

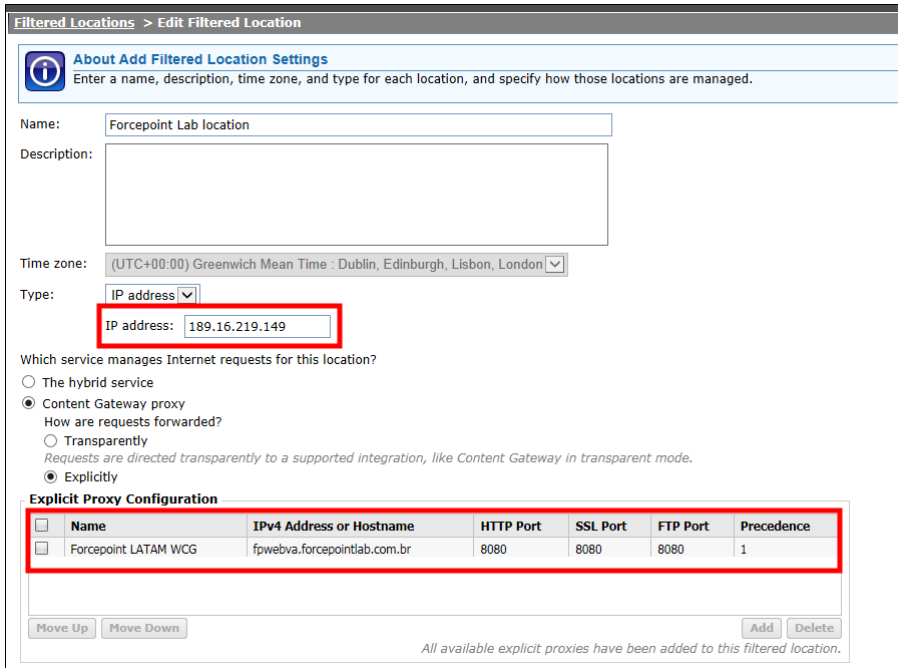
- 1) Log on to the Forcepoint Security Manager.
- 2) Go to **Settings > General > Filtered Locations**.



### Tip

You can also use the link at the top of the Protected Cloud Apps page (**Web > Settings > CASB Configuration > Protected Cloud Apps**).

### 3) Add a list of all locations where Internet traffic is managed by an instance of Content Gateway.



**Filtered Locations > Edit Filtered Location**

**About Add Filtered Location Settings**  
Enter a name, description, time zone, and type for each location, and specify how those locations are managed.

Name: Forcepoint Lab location

Description:

Time zone: (UTC+00:00) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Type: IP address

IP address: 189.16.219.149

Which service manages Internet requests for this location?

The hybrid service

Content Gateway proxy

How are requests forwarded?

Transparently  
*Requests are directed transparently to a supported integration, like Content Gateway in transparent mode.*

Explicitly

**Explicit Proxy Configuration**

<input type="checkbox"/>	Name	IPv4 Address or Hostname	HTTP Port	SSL Port	FTP Port	Precedence
<input type="checkbox"/>	Forcepoint LATAM WCG	fpwebva.forcepointlab.com.br	8080	8080	8080	1

Move Up Move Down Add Delete

*All available explicit proxies have been added to this filtered location.*

## Result

After the egress IP addresses are added to the Filtered Locations list, Forcepoint CASB adds the IP addresses to a list of allowed IP addresses. When a request for a selected cloud app is proxied through an instance of Content Gateway and the request is forwarded to Forcepoint CASB, the user will not be able to connect to that cloud app if the egress IP of that Content Gateway is not in the allowed IP list.

# Import the Forcepoint CASB certificate

Forcepoint provides a certificate authority (CA) certificate to every Forcepoint Web Security customer. This certificate must be uploaded to each Content Gateway server machine and must be installed on each client.



### Important

This information is only relevant for Forcepoint On-Premises or Hybrid Web Security customers.

The certificate (casb\_ssl\_ca.crt) is automatically downloaded to the Manager folder (usually C:\Program Files (x86)\ Websense\Web Security\Manager).

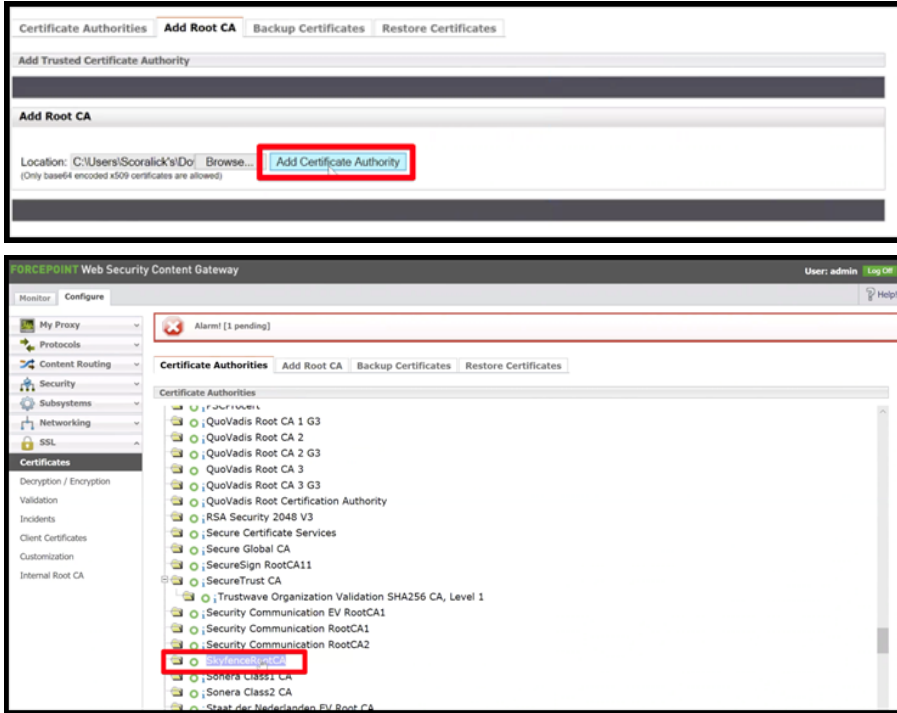


### Note

The Forcepoint CASB proxy runs on port 8081. Content Gateway requires outbound communication access on port 8081 in order to reach the Forcepoint CASB proxy and forward the relevant traffic. For more information, see "Firewall and network access prerequisites".

## Steps

- 1) Upload the certificate to each Content Gateway server machine and install on each client.



### Related concepts

Firewall and network access prerequisites on page 5

# Configuring the protected cloud apps list

The method for selecting which apps you want to be monitored by Forcepoint CASB depends on whether you are a Forcepoint On-Premises or Hybrid Web Security customer using the Forcepoint Security Manager, or whether you are a Forcepoint Web Security Cloud customer using the Forcepoint Security Portal.

### Related tasks

Configure the protected cloud apps list in the Forcepoint Security Manager on page 13

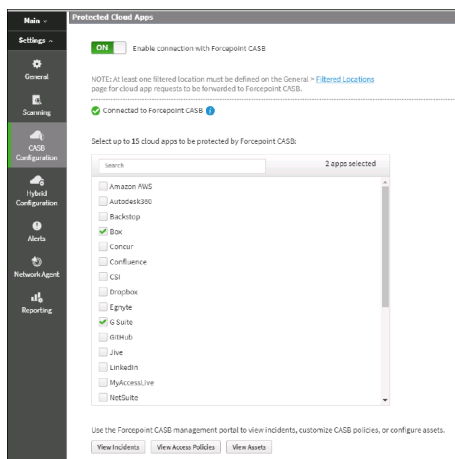
Configure the protected cloud apps list in the Forcepoint Security Portal on page 14

# Configure the protected cloud apps list in the Forcepoint Security Manager

For Forcepoint On-Premises or Hybrid Web Security customers, you must select which apps you want to be monitored by Forcepoint CASB in the Forcepoint Security Manager.

## Steps

- 1) Log on to the Forcepoint Security Manager.
- 2) Go to **Web > Settings > CASB Configuration > Protected Cloud Apps**.
- 3) Select the apps that should be monitored by Forcepoint CASB.  
You are limited by the number of apps for which your Forcepoint CASB license is valid.



Requests to the selected applications are forwarded to and monitored by Forcepoint CASB. Forwarding occurs (as of v8.5.5) only if the policy being applied has been configured to Forward traffic to Forcepoint CASB. The action code **Protected cloud app request forwarded** is applied to requests to the managed applications when the requests are forwarded to Forcepoint CASB.



### Important

Selections are sent to Forcepoint CASB. The number of selections is provided at the top of the selection list. If the maximum number of cloud apps has been selected (based on your license), no additional selection can be made. Deselect a cloud app to select a new one.

- 4) (Added with v8.5.5) The list of selected apps can be used by all policies or applied to a specified subset of policies. Use the selections to **Forward traffic to Forcepoint CASB**:
  - a) For **All policies** (the default) to forward all user requests to any of the selected apps to Forcepoint CASB for enforcement.
  - b) **Per policy** to select the policies that should use the list of selected apps when the policy is enforced.

- 5) When **Per policy** is selected, the **Forward to Forcepoint CASB** column provides the complete list of existing policies. Use the arrows to move selected policies for which protected cloud apps should not be applied to the **Do Not Forward to Forcepoint CASB** column.

Use the arrows to move policies from one list to the other.



#### Important

Filtering Service handles all user requests to a cloud app if the policy being applied is not configured to **Forward to Forcepoint CASB**.

- 6) Click **Save**.

## Result

Any request to the selected cloud apps is forwarded by Forcepoint Web Security service to, and monitored by, Forcepoint CASB.



#### Note

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

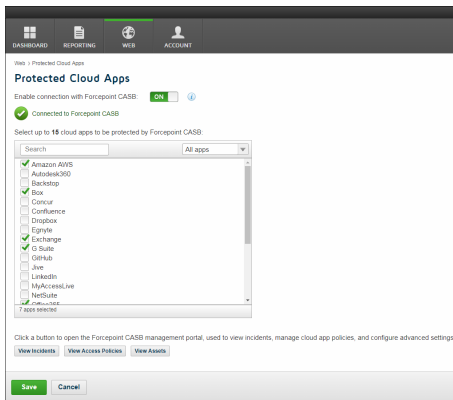
# Configure the protected cloud apps list in the Forcepoint Security Portal

For Forcepoint Web Security Cloud customers, you must select which apps you want to be monitored by Forcepoint CASB in the Forcepoint Security Portal.

## Steps

- 1) Log on to the Forcepoint Security Portal.
- 2) Go to **Web > Settings > Protected Cloud Apps**.

- 3) Select the apps that should be monitored by Forcepoint CASB.  
You are limited by the number of apps for which your Forcepoint CASB license is valid.



Requests to the selected applications are forwarded to and monitored by Forcepoint CASB. Forwarding occurs (as of v8.5.5) only if the policy being applied has been configured to Forward traffic to Forcepoint CASB. The action code **Protected cloud app request forwarded** is applied to requests to the managed applications when the requests are forwarded to Forcepoint CASB.



### Important

Selections are sent to Forcepoint CASB. The number of selections is provided at the top of the selection list. If the maximum number of cloud apps has been selected (based on your license), no additional selection can be made. Deselect a cloud app to select a new one.

- 4) (Added with v8.5.5) The list of selected apps can be used by all policies or applied to a specified subset of policies. Use the selections to **Forward traffic to Forcepoint CASB**:
- For **All policies** (the default) to forward all user requests to any of the selected apps to Forcepoint CASB for enforcement.
  - Per policy** to select the policies that should use the list of selected apps when the policy is enforced.
- 5) When **Per policy** is selected, the **Forward to Forcepoint CASB** column provides the complete list of existing policies. Use the arrows to move selected policies for which protected cloud apps should not be applied to the **Do Not Forward to Forcepoint CASB** column.  
Use the arrows to move policies from one list to the other.



### Important

Filtering Service handles all user requests to a cloud app if the policy being applied is not configured to **Forward to Forcepoint CASB**.

- 6) Click **Save**.

## Result

Any request to the selected cloud apps is forwarded by Forcepoint Web Security service to, and monitored by, Forcepoint CASB.

**Note**

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

There are different dashboards available in the Forcepoint Security Manager and in the Forcepoint CASB management portal.

## Dashboards in the Forcepoint Security Manager

In the Forcepoint Security Manager, you can use dashboards to view incidents, access policies, and assets.

### View incidents

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.

#### Steps

- 1) Log on to the Forcepoint Security Manager.
- 2) Below the apps list, click **View Incidents**.

Last Updated	Incident ID	Incident Name	Account	Full Name	Incident Detection Time	Mitigation Action	Follow-Up Mitigation	Severity
03/16/17 10:43:03	717919	Access from high-risk IP so...	admin@extremegulars.net	Robert Matthes	03/16/17 10:43:03	Monitor		Medium
02/01/17 13:27:32	552031	Access from high-risk IP so...	admin@extremegulars.net	Robert Matthes	02/01/17 13:27:32	Monitor		Medium
03/16/17 10:43:03	717918	Suspicious endpoint from a...	admin@extremegulars.net	Robert Matthes	03/16/17 10:43:03	Monitor		Medium
04/09/17 10:49:47	745953	Suspicious endpoint from a...	j.cage	James Cage	04/09/17 10:49:47	Monitor		Medium
05/02/17 08:43:45	774196	Suspicious endpoint from a...	j.cage	James Cage	05/02/17 08:43:45	Monitor		Medium
05/02/17 08:43:45	774195	Access from high-risk IP so...	j.cage	James Cage	05/02/17 08:43:45	Monitor		Medium

The **Audit & Protect > Incidents** table (available for all assets or a selected asset) opens.



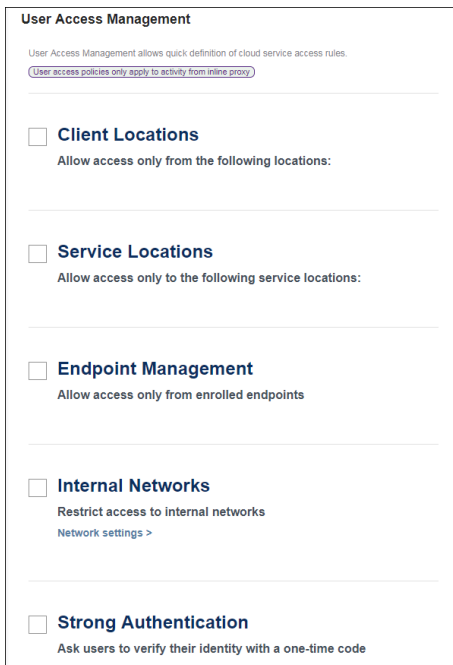
# View access policies

You can configure access policies to managed assets without needing to rely on the apps' native permission systems, which in some cases can be limited or insecure.

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

## Steps

- 1) Log on to the Forcepoint Security Manager.
- 2) Below the apps list, click **View Access Policies**.



The screenshot shows the 'User Access Management' configuration page. At the top, it states 'User Access Management allows quick definition of cloud service access rules.' Below this, a note indicates 'User access policies only apply to activity from inline proxy.' The page lists five policy options, each with an unchecked checkbox:

- Client Locations**  
Allow access only from the following locations:
- Service Locations**  
Allow access only to the following service locations:
- Endpoint Management**  
Allow access only from enrolled endpoints
- Internal Networks**  
Restrict access to internal networks  
Network settings >
- Strong Authentication**  
Ask users to verify their identity with a one-time code

The **Audit & Protect > Security Policies > User Access Management** table (per selected asset) opens.

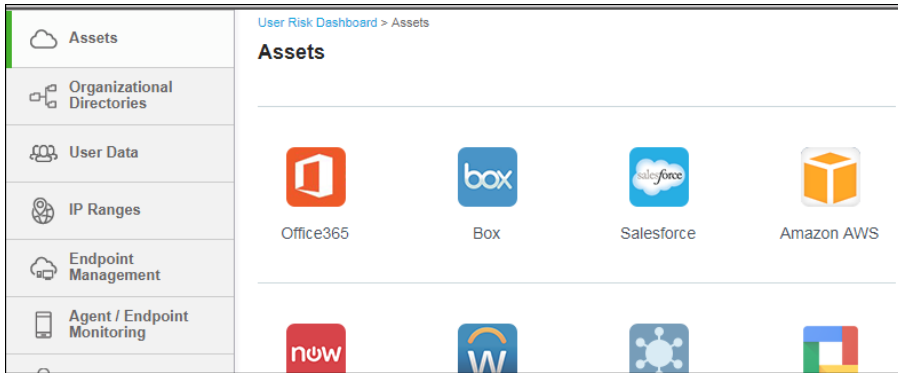
# View assets

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.

## Steps

- 1) Log on to the Forcepoint Security Manager.

- Below the apps list, click **View Assets**.



The **Settings > Assets** view opens.

## Dashboards in the Forcepoint CASB management portal

In the Forcepoint CASB management portal, you can use dashboards to view audit logs or to create a custom policy.

### View audit logs

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.

### Steps

- Log on to the CASB management portal.
- Go to **Audit & Protect > Activity Audit > Realtime Monitoring > Audit Log**. This option is available for all assets or a selected asset.

Time	Account	Asset	Anomaly	Severity	Action	Target	Client location	Rules
04/12/18 12:00:35	it@office365.net	Office365	No		view		Russian Federation	MS
04/12/18 12:00:32	it@office365.net	Office365	No		view		Russian Federation	MS
04/12/18 12:00:31	it@office365.net	Office365	No		view		Russian Federation	MS
04/12/18 08:07:54	it@office365.net	Office365	Yes	High	download		Russian Federation	Download Sensitive Data #
04/12/18 08:07:37	it@office365.net	Office365	No		view		Russian Federation	MS
04/12/18 08:07:24	it@office365.net	Office365	No		view		Russian Federation	MS
04/12/18 07:50:28	it@office365.net	Office365	No		view		Russian Federation	MS
04/11/18 22:56:16	it@office365.net	Office365	Yes	High	login		Russian Federation	Login from High Risk IP
04/11/18 17:59:40	admin@gethomeragular.net	Office365	No		logout		Israel	MS
04/11/18 17:59:39	admin@gethomeragular.net	Office365	No		logout		Israel	MS
04/11/18 17:59:01	admin@gethomeragular.net	Office365	No		view		Israel	MS
04/11/18 17:13:49	admin@gethomeragular.net	Office365	Yes	High	login		Israel	Login from High Risk IP
04/05/18 19:14:17	it@office365.net	Office365	No		external share		Russian Federation	MS
04/05/18 19:13:09	it@office365.net	Office365	No		view		Russian Federation	MS
04/05/18 19:13:08	it@office365.net	Office365	No		view		Russian Federation	MS
04/05/18 19:13:07	it@office365.net	Office365	No		view		Russian Federation	MS

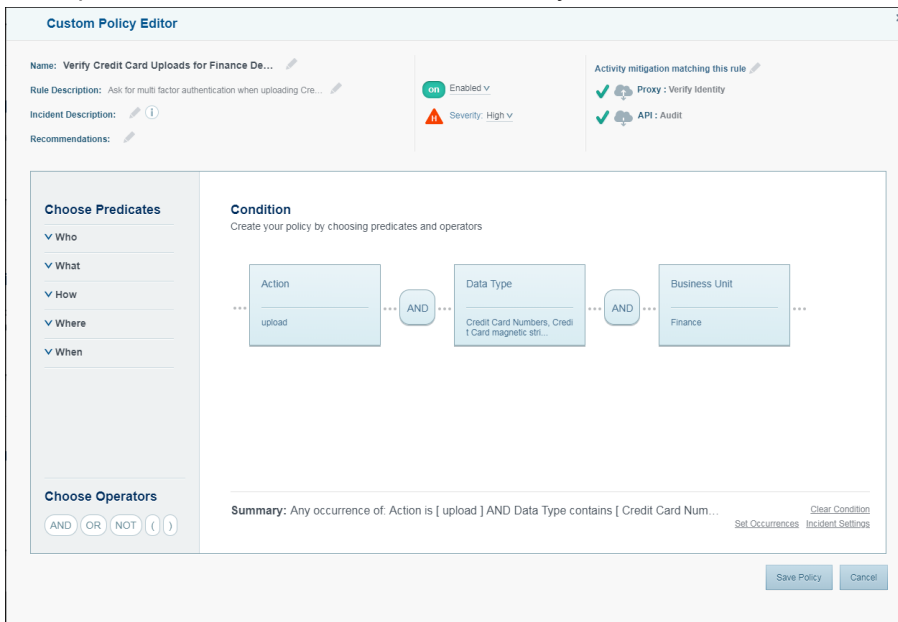
# Create a custom policy

Forcepoint CASB gives you the ability to create custom policies to be triggered by granularly defined custom conditions.

Conditions are configured as Boolean logical phrases (AND / OR / NOT) of configured values of generic and asset-specific parameters (predicates). A variety of predicates are available.

## Steps

- 1) Log on to the CASB management portal.
- 2) Go to **Audit & Protect > Security Policies > Custom Policy Editor**.  
This option is available for a selected asset only.



# Enroll the Forcepoint CASB device

Some Forcepoint CASB features require Forcepoint CASB to know which devices are managed by the organization. Enrolling source devices with Forcepoint CASB enables Forcepoint CASB to know that they are managed by the organization.

You must enroll source devices if you use any of the following features:

- The Endpoint Management Access Policy
- Custom policies based on managed devices
- An Analytics dashboard filter that shows access from managed devices
- Analytics activity logs that show whether source devices are managed or not

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

## Steps

- 1) Log onto the Forcepoint CASB management portal.
- 2) Go to **Settings > Endpoint Management**.
- 3) Under the **Automatic Enrollment** section, select **Web Security Proxy**.

The screenshot displays the Forcepoint CASB management portal interface. On the left, a sidebar menu lists various settings categories, with 'Endpoint Management' highlighted in a red box. The main content area is titled 'Endpoint Management' and includes a sub-section for 'Automatic Enrollment'. This section allows users to define endpoints for automatic enrollment. It features two columns: 'Enroll endpoints by IP' and 'Enroll endpoints by CA certificates'. Under 'Enroll endpoints by IP', there are checkboxes for 'All internal network IP's' and 'Specific IP's'. A text input field contains '10.2.0.2' and an 'Add' button. Under 'Enroll endpoints by CA certificates', there is a checkbox for 'Endpoints that are using specific CA certificate' and a 'Browse' button. A checkbox for 'Enrollment by client certificate is permanent' is also present. At the bottom of the configuration area, there is a checkbox for 'Enforce combined conditions' with a sub-note: 'Endpoints will be enrolled only if they have both conditions (at least one of the IP types and the certificate)'. A 'Summary' section at the bottom indicates 'Enroll only endpoints that' and a 'Save Automatic Enrollment' button is located at the bottom left of the main content area. A red box highlights the 'Web Security Proxy' checkbox, which is checked.

## Result

Forcepoint CASB regards all traffic coming from Forcepoint Web Security as coming from managed devices.

