



## Configure Offline CASB Profiles



For supported software information, click [here](#).

Offline Cloud Access Security Broker (CASB) is on-premises or cloud-based policy enforcement that secures data between users and cloud applications to comply with corporate and regulatory requirements. Offline CASB applies enterprise security policies when users access cloud-based resources.

As more applications move to the cloud, offline CASB addresses the following challenges to securing data:

- Implement data-centric policies to authorize or control.
- Analyze data access and changes to data stored in software-as-a-service (SaaS) clouds.
- Implement access control for files, applications, and users.
- Identify downloads, uploads, and file sharing done by users.

In addition, offline CASB secures cloud services and access to direct cloud-to-cloud deployments.

The Versa offline CASB functions monitor user activities, enforce security policies, and provide granular access control for cloud applications. Versa Networks also supports API integration with SaaS and IaaS applications. The API integration uses API calls to SaaS and IaaS applications, inspects user activities and content, enforces security policies, and provides granular access control for SaaS applications. The offline CASB action can match the risk level and activity of multiple cloud applications, and it can allow, deny, or restrict access to shadow IT.

To enforce offline CASB security policies, you create one or more offline CASB profiles, specify match criteria for applications, and then associate offline CASB profiles with an API-based data protection policy for SaaS. For more information, see [Configure API-Based Data Protection Policy for SaaS](#).

To use offline CASB, you must use the premium security pack (SPack) Version 1939 or later.

## Configure an Offline CASB Profile

1. Go to Configure > Secure Services Edge > API Based Data Protection > Profiles:

<b>Secure Services Edge</b>	Secure SD-WAN
<hr/>	
> Real-Time Protection	
<hr/>	
> Secure Client Access	
<hr/>	
> TLS Description	
<hr/>	
< API Based Data Protection	
 <b>Connectors</b>	
 <b>Policy Rules</b>	
 <b>Profiles</b>	
<hr/>	
> User & Entity Behavior Analytics	
<hr/>	
> Settings	
<hr/>	

2. Select the Offline Cloud Access Security Broker (CASB) tab. In the CASB Profiles tab, click the  icon.

3. In Step 1, Select Rules screen, select the application for the CASB rule. Each CASB rule can match the activity of multiple cloud applications for which you want to allow or block activities. You can also search for applications to select.

4. By default, the Selected Selected toggle button for each application is enabled. To bypass CASB processing for

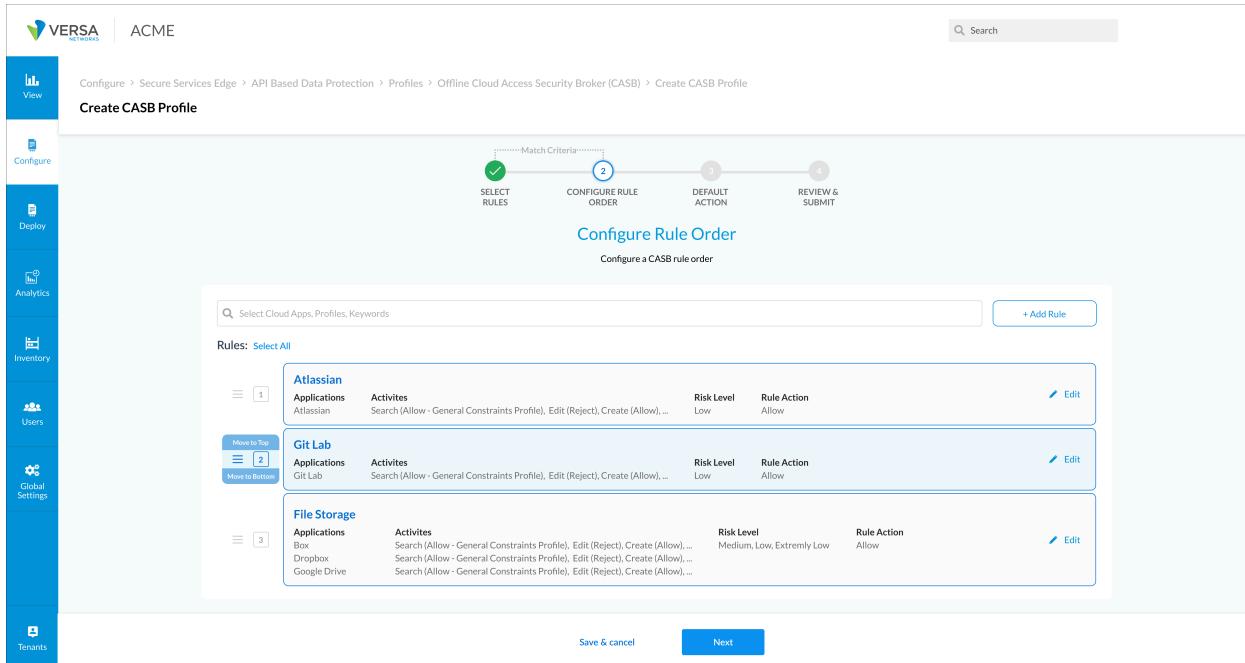
[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_Offline\\_CASB\\_Profi...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Offline_CASB_Profi...)

Updated: Wed, 23 Oct 2024 08:38:55 GMT

Copyright © 2024, Versa Networks, Inc.

an application, click the toggle button. The Unselected Unselected button then turns grey.

5. Click  Edit to allow or block the activities of an application. In the Edit popup window, click the toggle button to allow or block application activities. For example, you can allow or block file download, login, post, or file upload for Box.
6. Click Next.
7. In Step 2, Configure Rule Order screen, configure the CASB rule order and click Next.



The screenshot shows the 'Create CASB Profile' screen in the Versa Networks interface. The left sidebar includes icons for View, Configure, Deploy, Analytics, Inventory, Users, Global Settings, and Tenants. The main area shows the 'Configure Rule Order' step, which is the second step in the process. The flow consists of four steps: SELECT RULES (green checkmark), CONFIGURE RULE ORDER (blue circle with number 2), DEFAULT ACTION (grey circle with number 3), and REVIEW & SUBMIT (grey circle with number 4). The 'CONFIGURE RULE ORDER' section displays a table of rules:

Rule	Application	Activities	Risk Level	Rule Action	Action
1	Atlassian	Search (Allow - General Constraints Profile), Edit (Reject), Create (Allow), ...	Low	Allow	
2	Git Lab	Search (Allow - General Constraints Profile), Edit (Reject), Create (Allow), ...	Low	Allow	
3	File Storage	Search (Allow - General Constraints Profile), Edit (Reject), Create (Allow), ... Search (Allow - General Constraints Profile), Edit (Reject), Create (Allow), ... Search (Allow - General Constraints Profile), Edit (Reject), Create (Allow), ...	Medium, Low, Extremely Low	Allow	

Buttons at the bottom include 'Save & cancel' and 'Next'.

8. In Step 3, Default Action screen, select the default action to perform when there are no matching criteria. By default, applications that do not match any criteria are allowed. Enter information for the following fields.

Field	Description
Rule Action	Select the default action to perform when there are no matching criteria: <ul style="list-style-type: none"> <li>◦ Allow—Allow cloud applications.</li> <li>◦ Block—Block cloud applications.</li> </ul>
Logging Profile	Select a logging profile.
Set as Default	Click to set the action as the default action.

9. Click Next.
10. In Step 4, Review and Submit screen, review the information.

**VERSACLOUD** ACME

Configure > Secure Services Edge > API Based Data Protection > Profiles > Offline Cloud Access Security Broker (CASB) > Create CASB Profile

### Create CASB Profile

Match Criteria

SELECT RULES ✓

CONFIGURE RULE ORDER ✓

DEFAULT ACTION ✓

REVIEW & SUBMIT 4

#### Configure Default Action

When there is no action matched within the specified rules in this profile, the following default action will apply.

##### General

Customize Profile Name  
CASB Profile 3

Description  
Input Description

##### Actions

Default Action: Allow | Logging Profile: - | Set as Default: Yes

##### Rule

Order	Rule Name	Applications	Activities	Risk Level	Rule Action
1	Atlassian	Atlassian	Login (Alert), Download (Allow)	Low	Allow
2	Git Lab	GitLab	Login (Alert)	Low	Allow
3	File Storage	Box	Search(Allow - General Constraints Profile), File Share (Remove: blacklisted user), Upload File (Allow)	Medium, Low	Extremely Low
	Dropbox	Dropbox	Search(Allow), Login (Alert), File Share (Remove: blacklisted user), Upload File (Allow)		Allow
	Google Drive	Google Drive	Search(Allow), Login (Alert), File Share (Remove: blacklisted user), Upload File (Allow)		Allow

Save & cancel Back Save

11. In the General section, enter a name for the offline CASB profile and, optionally, a description.
  12. For all other sections, review the information. To make changes, click the  Edit icon.
  13. Click Save to create a profile. The API-Based Data Protection Profile screen displays.

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_Offline\\_CASB\\_Profil...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Offline_CASB_Profil...)  
Updated: Wed, 23 Oct 2024 08:38:55 GMT  
Copyright © 2024, Versa Networks, Inc.

## Configure CASB Rules

1. Go to Configure > Secure Services Edge > API Based Data Protection > Profiles.

The screenshot shows a sidebar navigation menu with the following structure:

- Secure Services Edge** (highlighted in blue)
- Secure SD-WAN**
- > Real-Time Protection
- > Secure Client Access
- > TLS Description
- ▽ API Based Data Protection
  - Connectors
  - Policy Rules
- Profiles** (highlighted in blue)
- > User & Entity Behavior Analytics
- > Settings

2. Select the Offline Cloud Access Security Broker (CASB) tab. In the CASB Rules tab, click .

Configure > Secure Services Edge > API Based Data Protection > Profiles

**API Based Data Protection - Profiles**

Offline Cloud Access Security Broker (CASB) Data Loss Prevention (DLP) Offline Malware Protection Offline Advanced Threat Protection

CASB Rules Constraints Profiles

Search by keyword or name Filter

Create CASB rules first

No Records to Display

Add Rule

- In Step 1, Select Category screen, select the application category for the CASB rule and click Next.

Configure > Secure Services Edge > API Based Data Protection > Profiles > Offline Cloud Access Security Broker (CASB) > Create CASB Rule

**Create CASB Rule**

Match Criteria

1 SELECT CATEGORY 2 SELECT APPLICATIONS 3 ACTIVITIES & CONSTRAINTS 4 RISK LEVEL 5 DEFAULT ACTION 6 REVIEW & SUBMIT

Select Category

Cloud File Share Office Document Productivity

Save & cancel Next

- In Step 2, Select Applications screen, select the application for the CASB rule. Each CASB rule can match the activity of multiple cloud applications for which you want to allow or block activities.

5. Click Next.
6. In Step 3, Activities and Constraints screen, configure applications and allow and block activities for the selected cloud applications, or disable an application.

7. By default, the  Access Allow toggle button for each application is enabled. To disable all access to an

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_Offline\\_CASB\\_Profil...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Offline_CASB_Profil...)

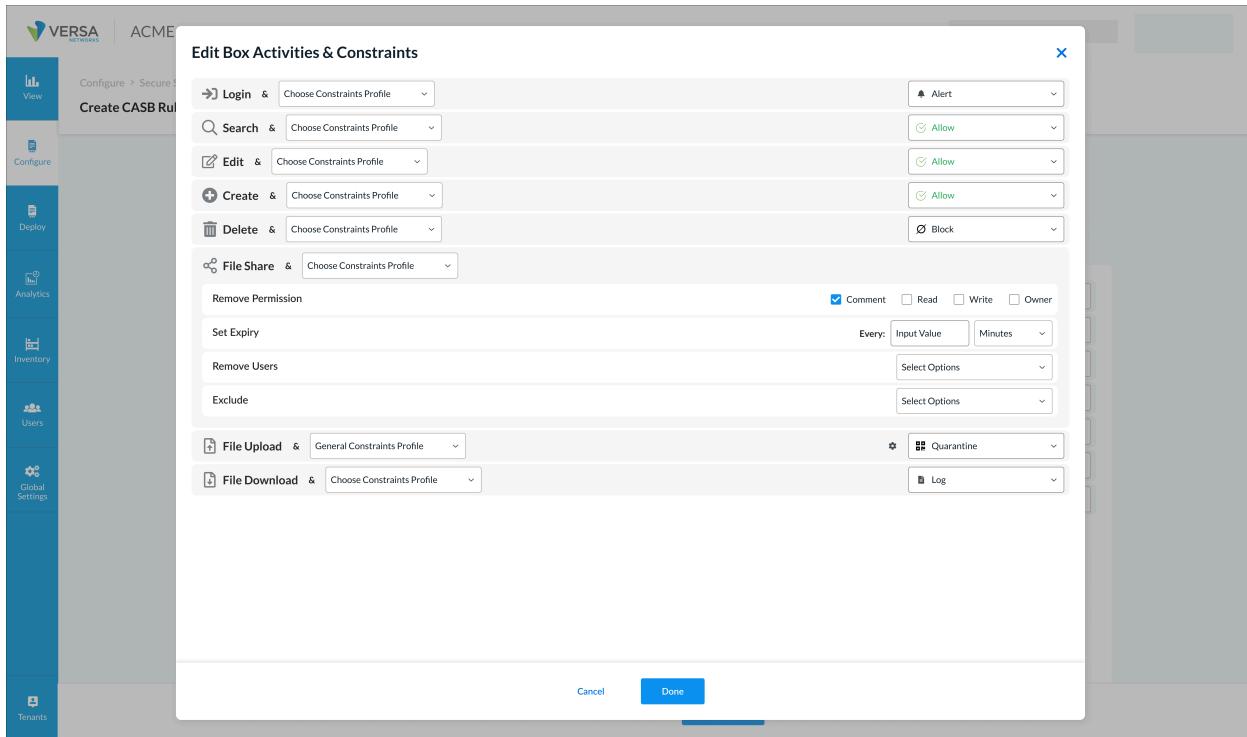
Updated: Wed, 23 Oct 2024 08:38:55 GMT

Copyright © 2024, Versa Networks, Inc.



application, click the toggle button. The access allow button then turns **Access Blocked** Access Blocked and grey.

8. Click the  Edit icon to allow or block the activities of an application. In the Edit popup window, enter information for the following fields.



Fields	Description
Login	Select an action to take when a login is attempted: <ul style="list-style-type: none"><li>◦ Alert</li><li>◦ Log</li></ul>
Search	Select an action to take when a search is attempted.
Edit	Select an action to take when an edit is attempted.
Create	Select an action.
Delete	Select the delete actions.
File Share	Select the file permissions to set for shared files:

Fields	Description
	<ul style="list-style-type: none"> <li>◦ Remove Permissions—Select to remove comment, read, write, and owner permissions.</li> <li>◦ Remove Users—Select the option to remove users: <ul style="list-style-type: none"> <li>▪ All users</li> <li>▪ Domain profiles</li> <li>▪ User profiles</li> <li>▪ External users</li> <li>▪ Selected users</li> </ul> </li> <li>◦ Set expiry—Enter an expiry time in minutes, after which access is expired.</li> <li>◦ Exclude—Select exclude options.</li> </ul>
File Upload	<p>Select an action to take when a file is uploaded:</p> <ul style="list-style-type: none"> <li>◦ Legal hold</li> <li>◦ Quarantine</li> <li>◦ Remove</li> </ul>
File Download	<p>Select an action to take when a file is downloaded:</p> <ul style="list-style-type: none"> <li>◦ Alert</li> <li>◦ Log</li> </ul>

9. Click Next.
10. In Step 4, Risk Level screen, select the risk level and click Next.

Configure > Secure Services Edge > API Based Data Protection > Profiles > Offline Cloud Access Security Broker (CASB) > Create CASB Rule

**Create CASB Rule**

Match Criteria

RISK LEVEL

**Risk Level**

Risk Level

Disable All

Extremely High (1)

High (1)

Medium (1)

Low (1)

Extremely Low (1)

Save & cancel      Next

- In Step 5, Default Action screen, select the default action to perform when there are no matching criteria. By default, applications that do not match any criteria are allowed. Enter information for the following fields.

Configure > Secure Services Edge > API Based Data Protection > Profiles > Offline Cloud Access Security Broker (CASB) > Create CASB Rule

**Create CASB Rule**

Match Criteria

RISK LEVEL

**Configure Default Action**

When there is no action matched within the specified rules in this profile, the following default action will apply.

**Default Action**

Rule Action

Allow

Email Profile

Marketing User

Save & cancel      Next

Field	Description
Rule Action	Select the default action to perform when there are no matching criteria: o Allow—Allow cloud applications.
Email Profile	Enter an email profile.

12. Click Next.
13. In Step 6, Review and Submit screen, review the configuration.

The screenshot shows the 'Create CASB Rule' configuration page. The 'General' section contains the rule name 'ACME Box GoogleDrive OneDrive' and a description 'Box, Dropbox, OneDrive'. The 'Actions' section shows 'Rule Action' set to 'Allow' and 'Email Profile' set to 'Marketing User'. The 'App Activities & Constraints' section lists activities for Box, Dropbox, and OneDrive. The sidebar on the left includes icons for View, Configure, Deploy, Analytics, Inventory, Users, Global Settings, and Tenants.

14. In the General section, enter a name for the rule name and, optionally, a description.
15. For all other sections, review the information. To make changes, click the Edit icon.
16. Click Save to create a profile. The API-Based Data Protection Profile screen displays.

	NAME	CATEGORY	APPLICATIONS	EMAIL PROFILE	RISK LEVEL	ACTIONS
<input type="checkbox"/>	CASB Rule 1	IT Services	1	Marketing User	Medium	Allow
<input type="checkbox"/>	CASB Rule 2	Collaboration & Online Meetings	2	All User	Extremely High	Allow
<input type="checkbox"/>	ACME Box GoogleDrive OneDrive	File Drive	3	Marketing User	Extremely High, High, Low	Allow

APPLICATION ACTIVITIES & CONSTRAINTS

Box	Search: Allow - General Constraints Profile	Edit: Reject	File Share: Remove Blacklisted user	Create: Reject	Login: Allow	File Upload Quarantine - General Constraints Profile	Delete: Block
Google Drive	Search: Allow	Create: Reject	Login: Alert	Upload File: Quarantine	Delete: Block		
OneDrive	Search: Allow	Create: Reject	Login: Allow	Upload File: Block	Delete: Block		

## Supported Software Information

Releases 11.1.1 and later support all content described in this article.

## Additional Information

[Configure CASB Profiles](#)

[Configure SASE Internet Protection Rules](#)

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_Offline\\_CASB\\_Profiles](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Offline_CASB_Profiles)

Updated: Wed, 23 Oct 2024 08:38:55 GMT

Copyright © 2024, Versa Networks, Inc.