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.

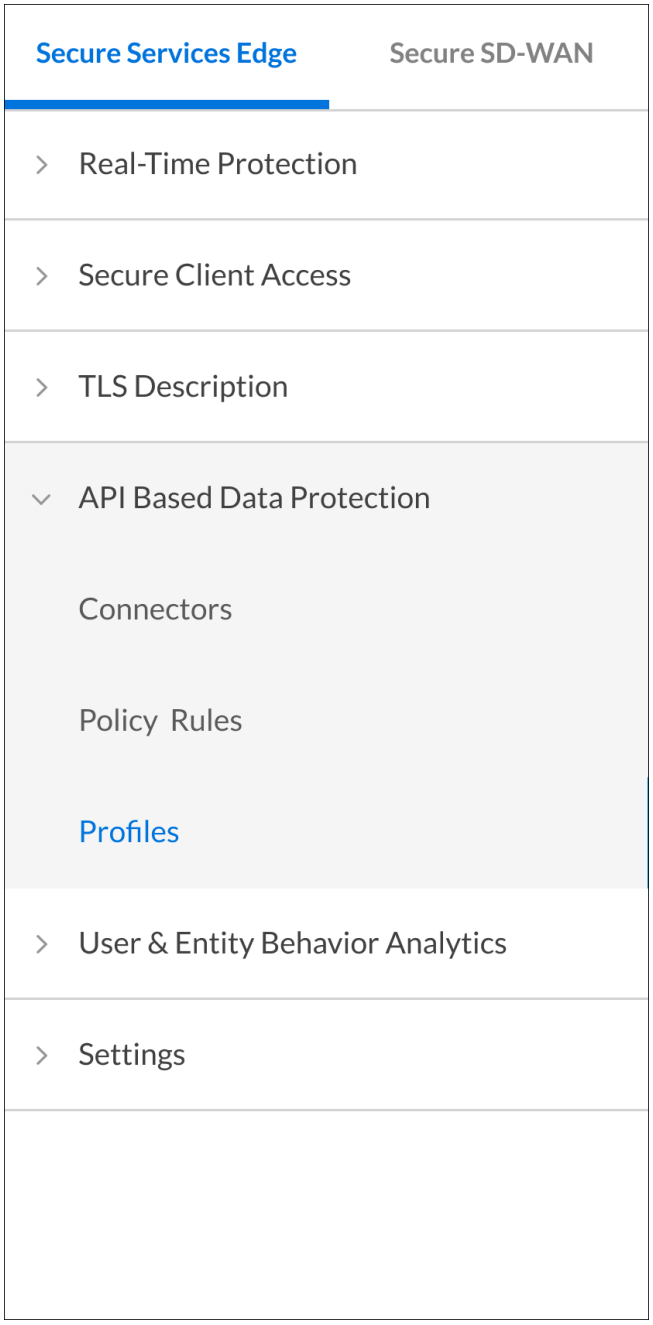
The Versa offline CASB functions monitor user activities, enforce security policies, and provide granular access control for cloud applications. Versa Networks also supports API integration with SaaS and IaaS applications. The API integration uses API calls to SaaS and IaaS applications, inspects user 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.

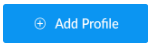
To enforce offline CASB security policies, you create one or more offline CASB profiles, specify match criteria for applications, and then associate offline CASB profiles with an API-based data protection policy for SaaS. For more information, see Configure API-Based Data Protection Policy for SaaS.

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

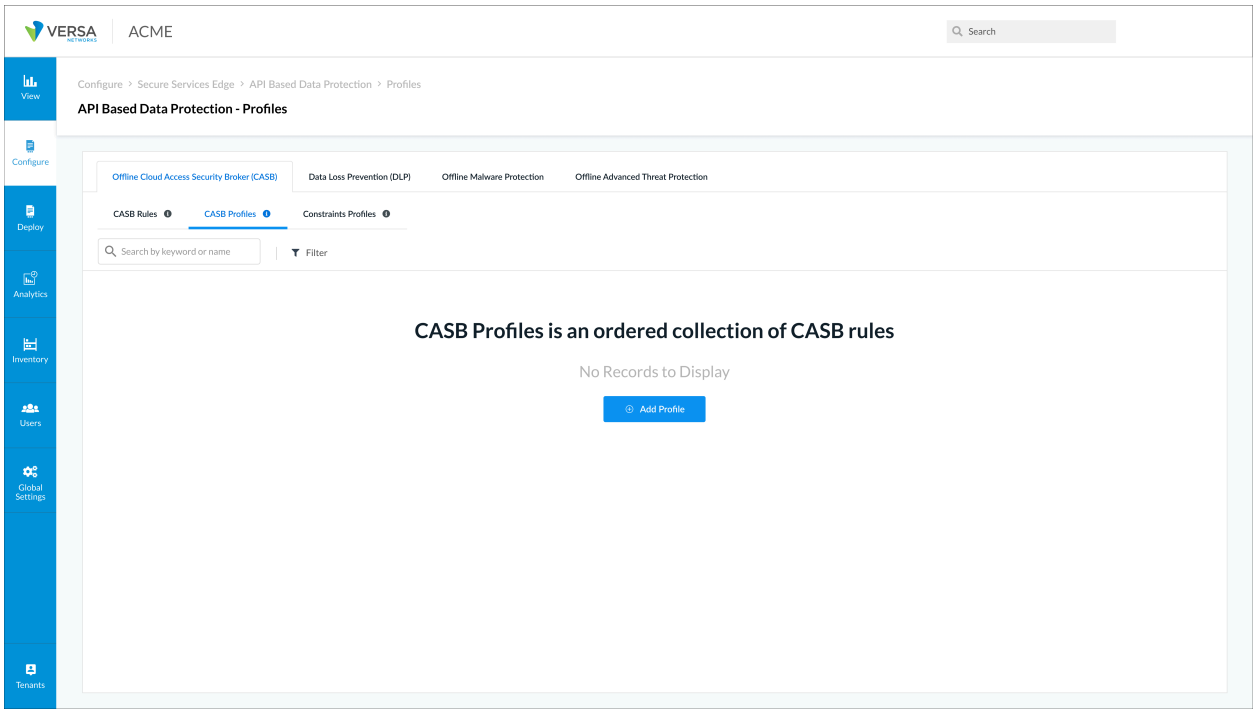
Configure an Offline CASB Profile

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

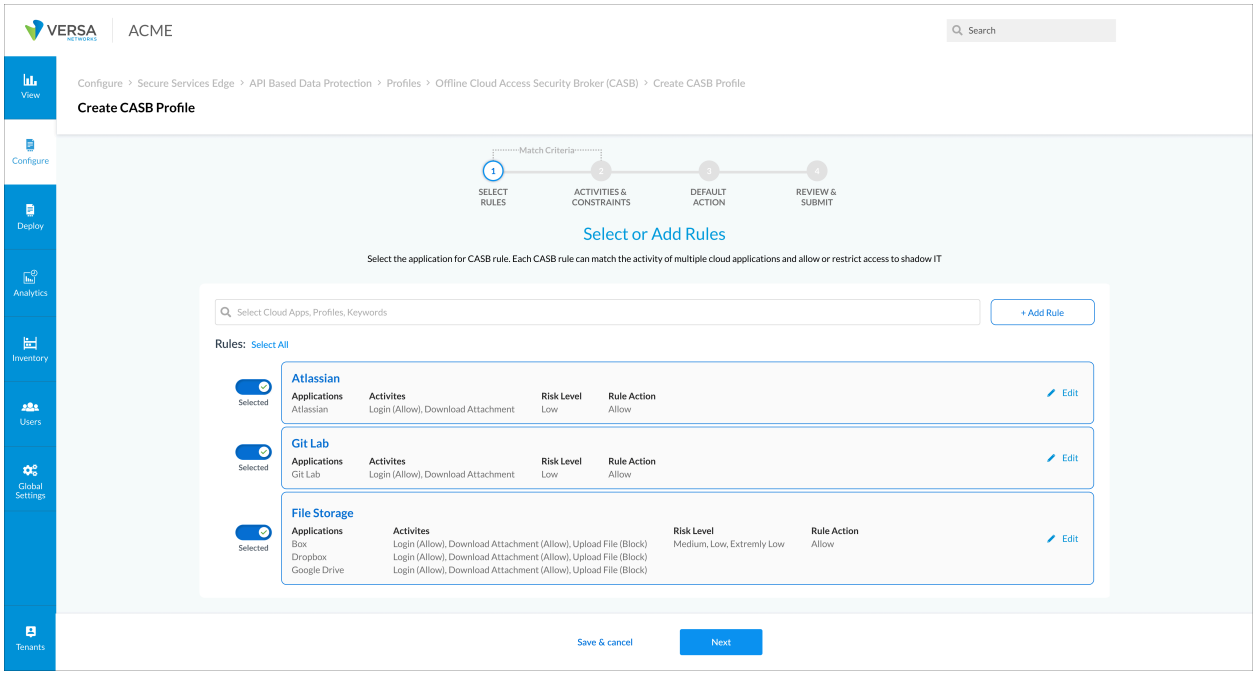


2. Select the Offline Cloud Access Security Broker (CASB) tab. In the CASB Profiles tab, click the 

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 

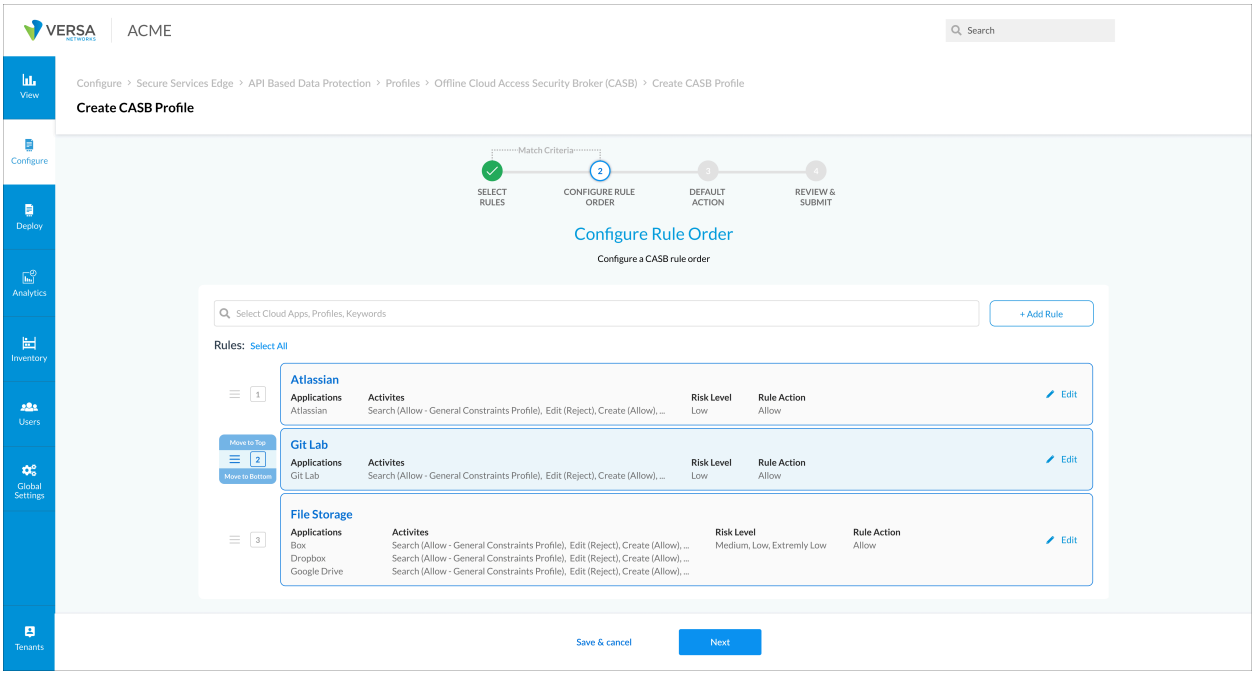
Selected toggle button for each application is enabled. To bypass CASB processing for

an application, click the toggle button. The

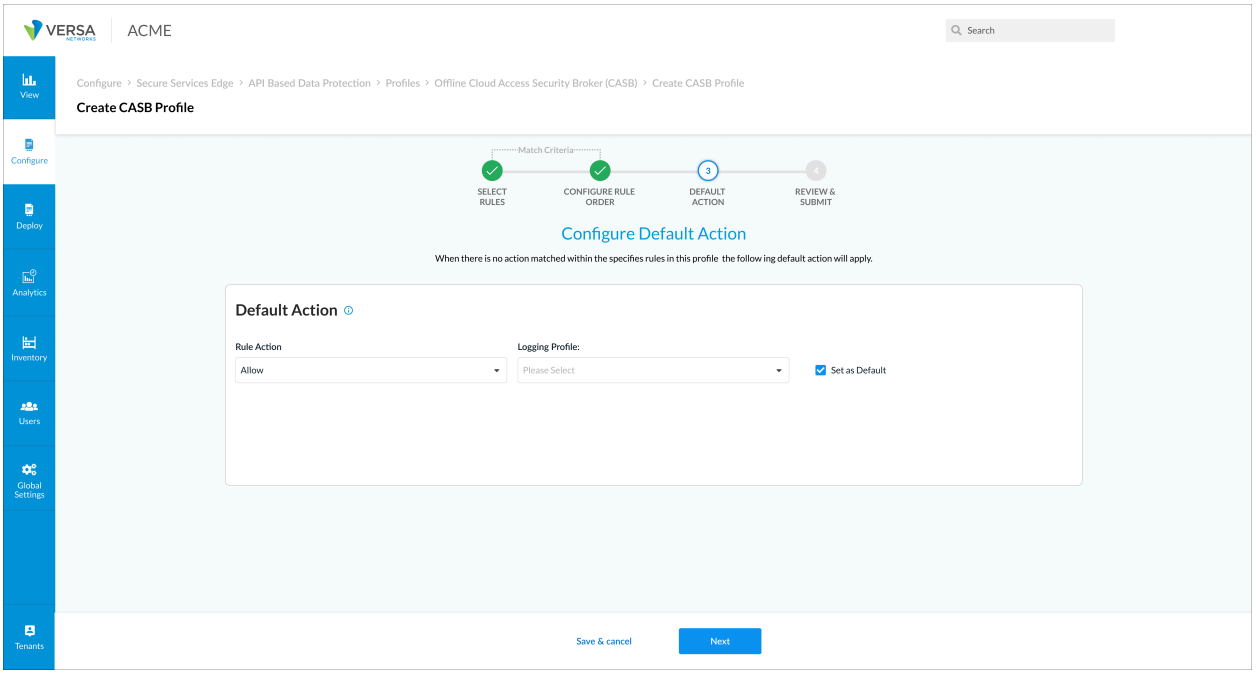
Unselected button then turns grey.

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.

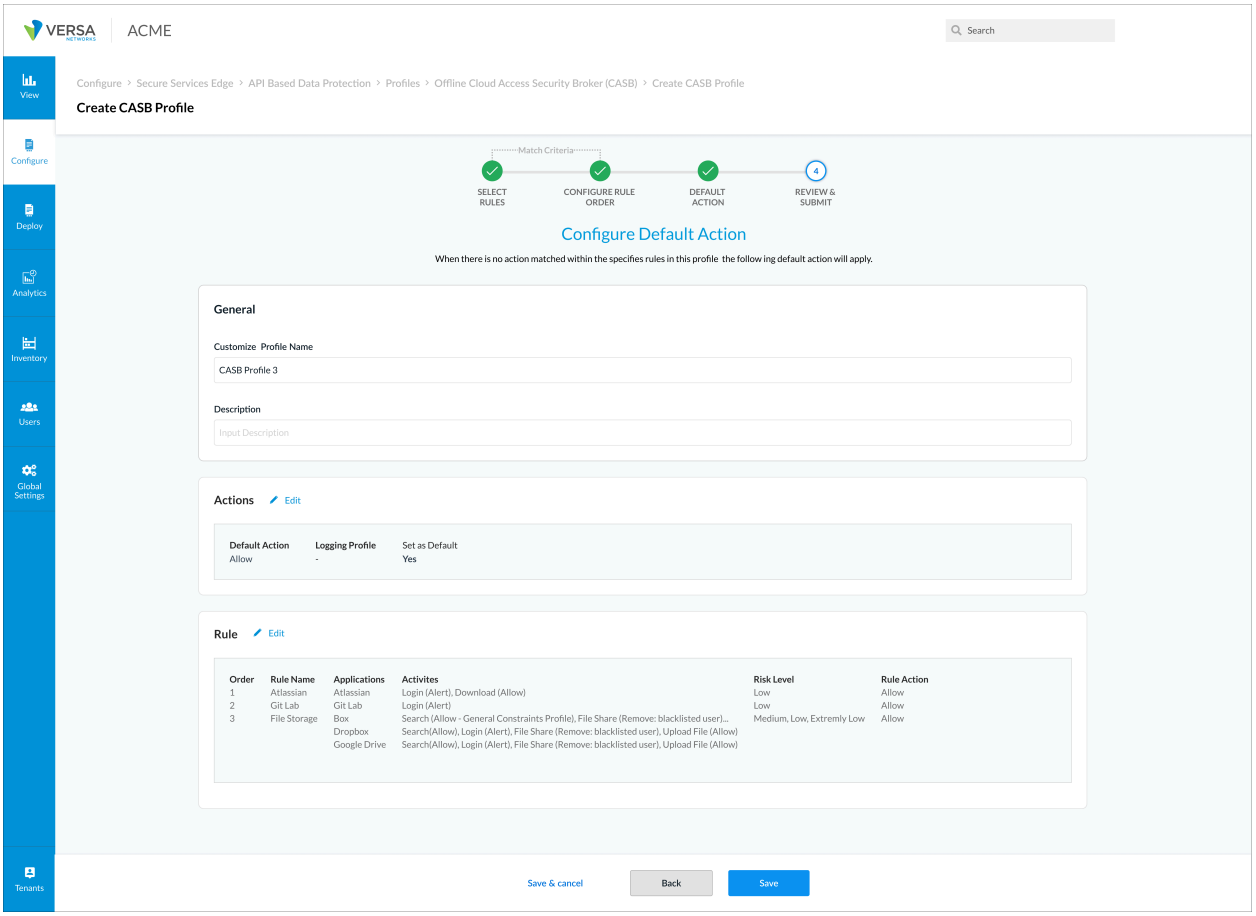


8. In Step 3, Default Action screen, select the default action to perform when there are no matching criteria. By default, applications that do not match any criteria are allowed. Enter information for the following fields.

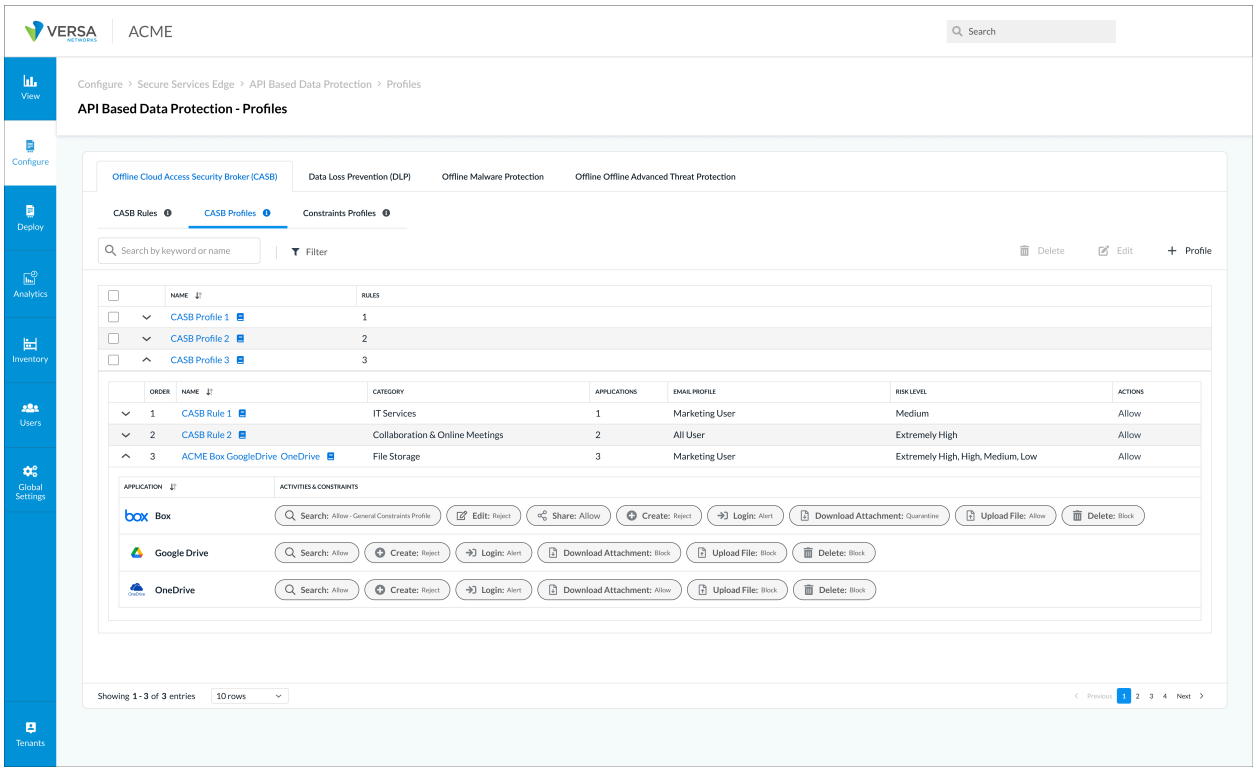


Field	Description
Rule Action	Select the default action to perform when there are no matching criteria: ◦ Allow—Allow cloud applications. ◦ Block—Block cloud applications.
Logging Profile	Select a logging profile.
Set as Default	Click to set the action as the default action.

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

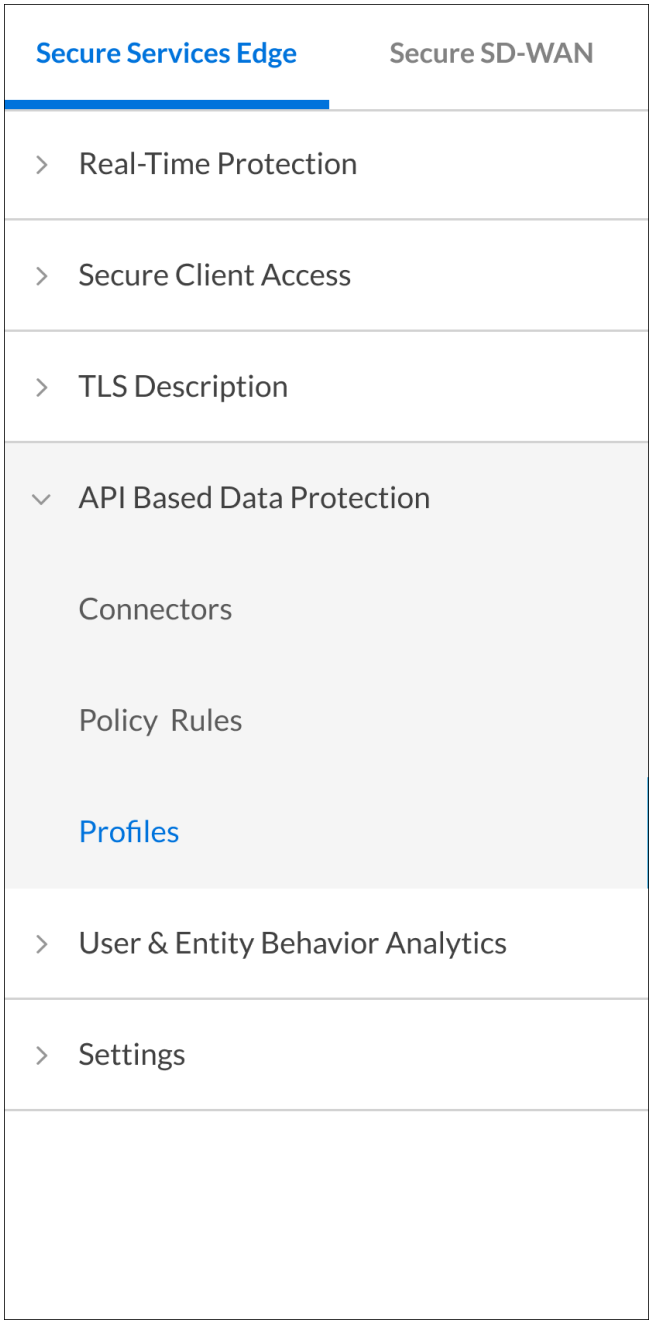


11. In the General section, enter a name for the offline CASB profile and, optionally, a description.
12. For all other sections, review the information. To make changes, click the Edit icon.
13. Click Save to create a profile. The API-Based Data Protection Profile screen displays.



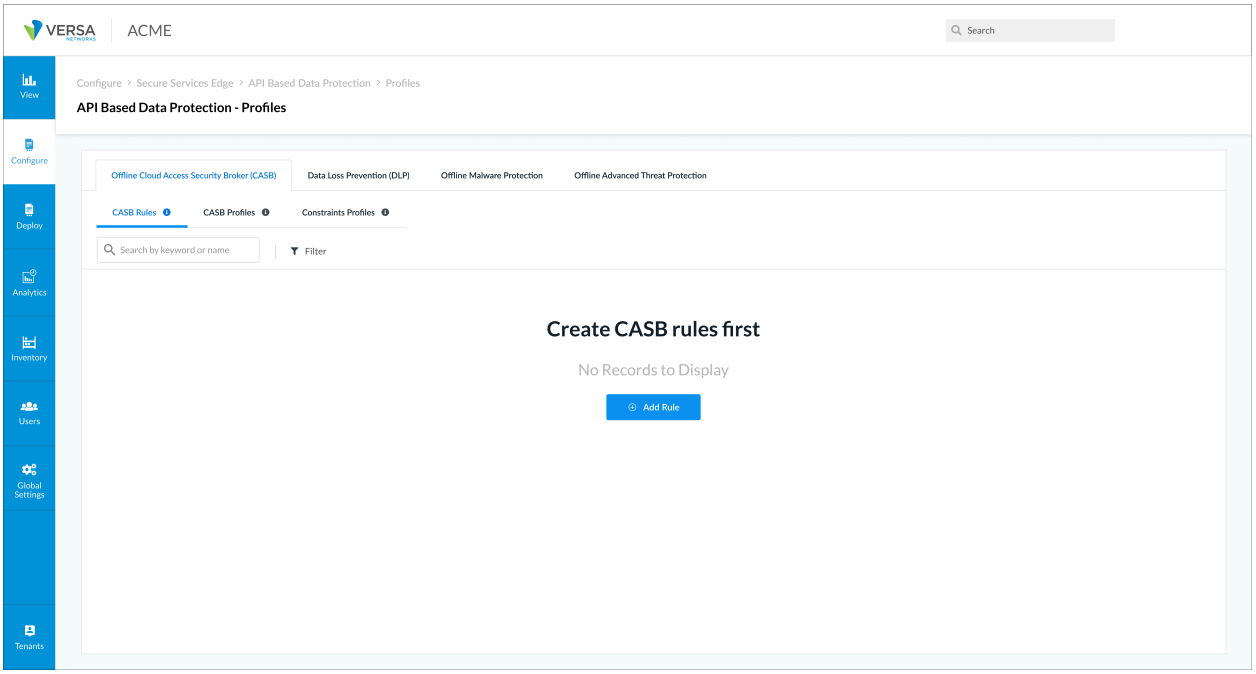
Configure CASB Rules

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

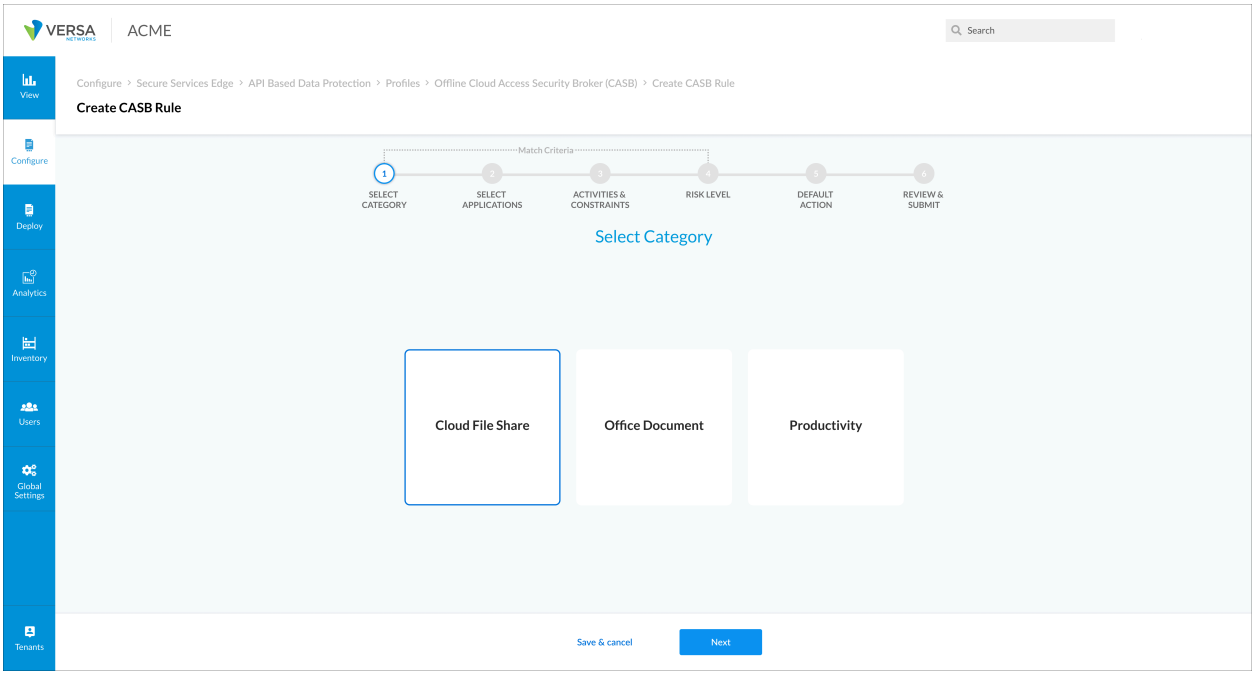


2. Select the Offline Cloud Access Security Broker (CASB) tab. In the CASB Rules tab, click 

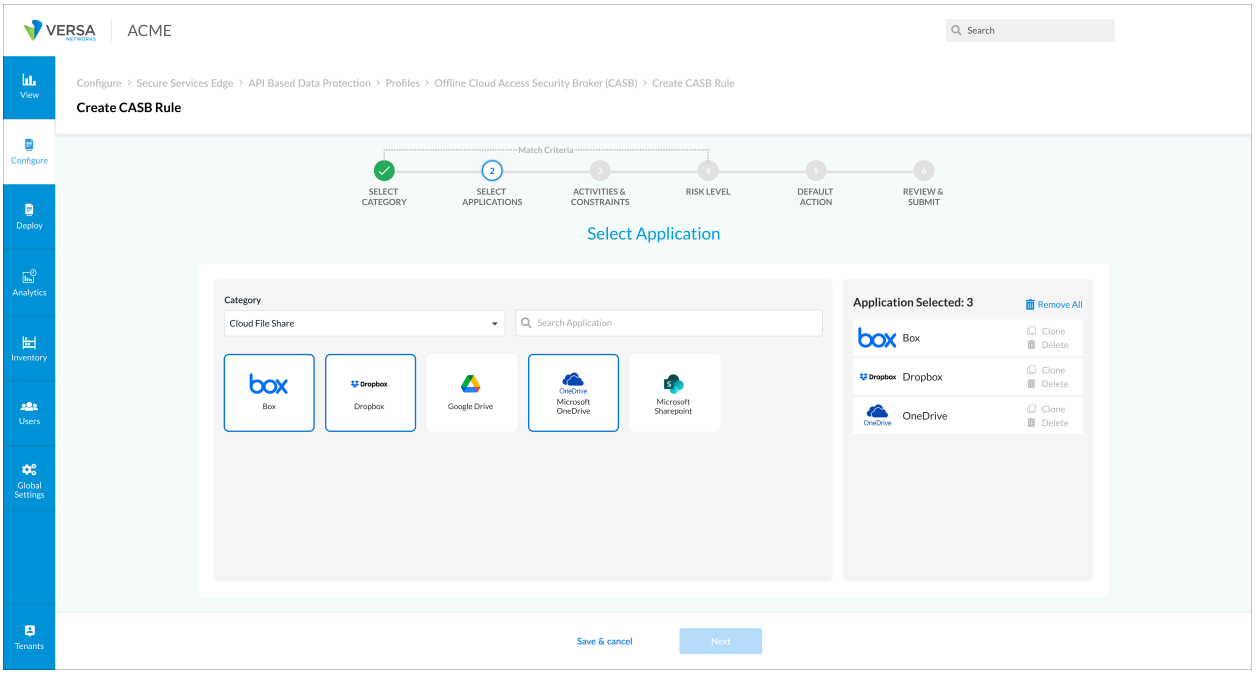
.



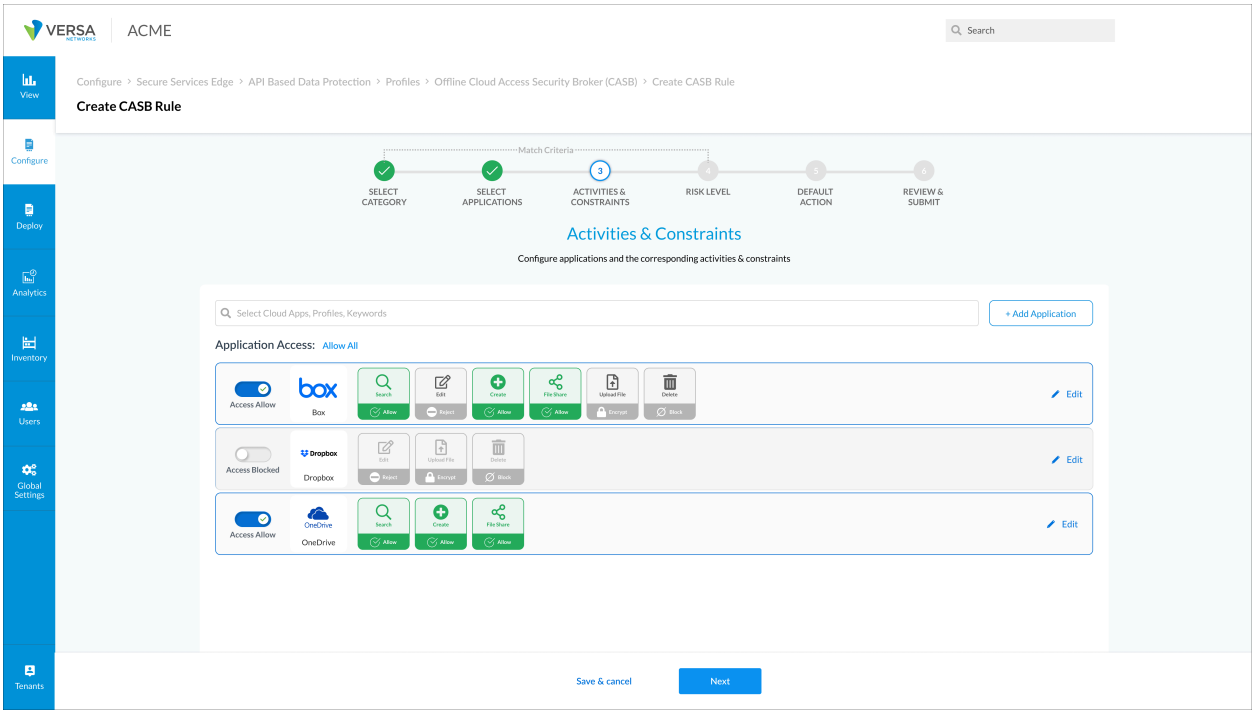
3. In Step 1, Select Category screen, select the application category for the CASB rule and click Next.

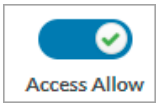


4. In Step 2, Select Applications screen, select the application for the CASB rule. Each CASB rule can match the activity of multiple cloud applications for which you want to allow or block activities.



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 

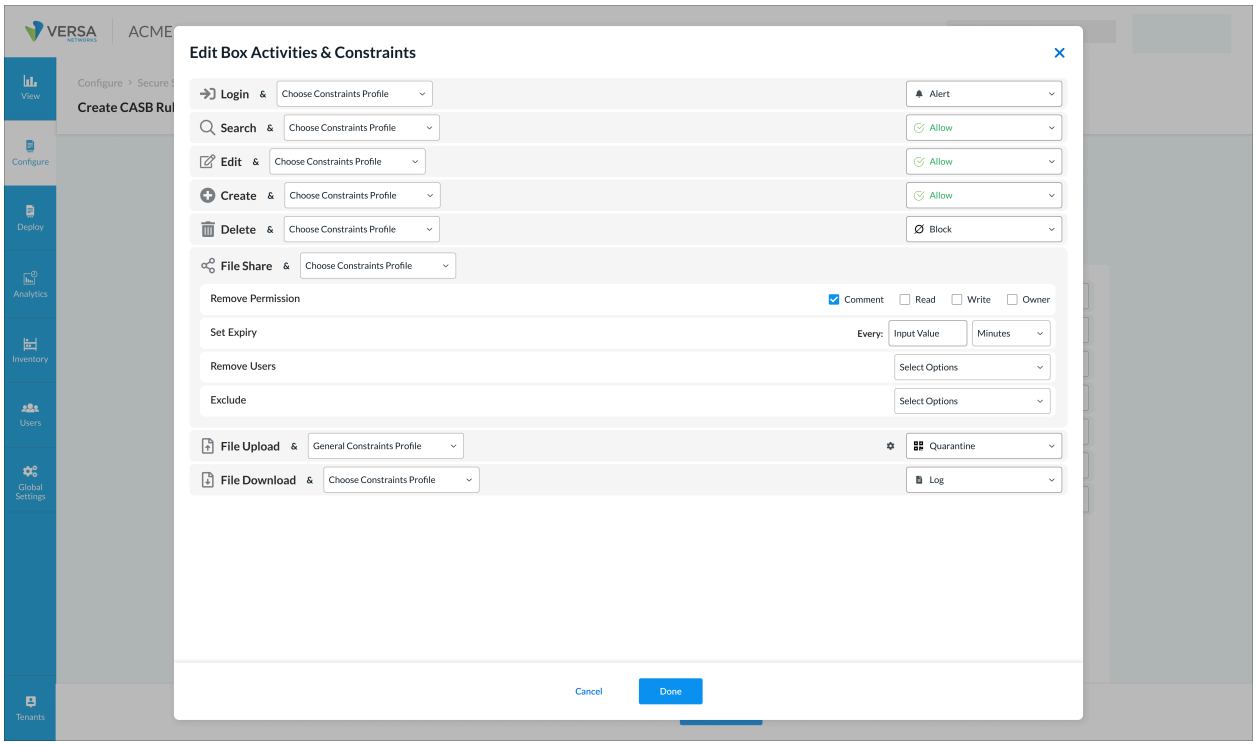
Access Allow toggle button for each application is enabled. To disable all access to an

application, click the toggle button. The access allow button then turns 

Access Blocked and grey.

8. Click the 

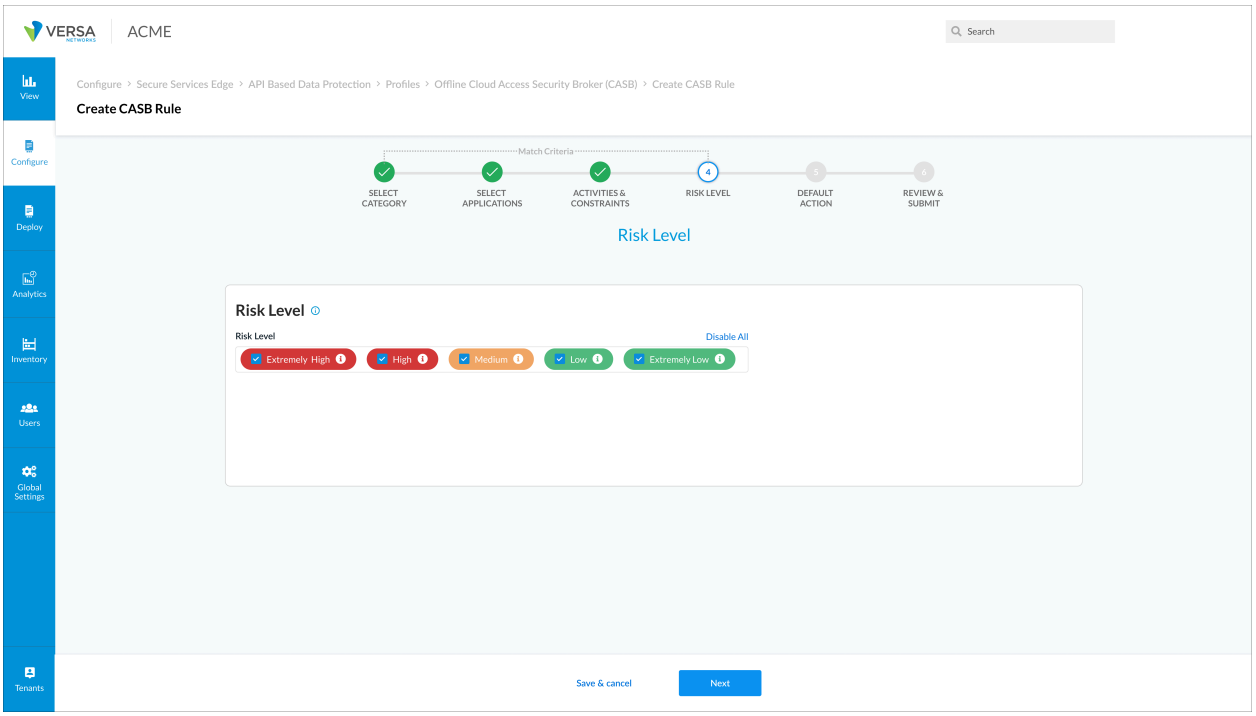
Edit icon to allow or block the activities of an application. In the Edit popup window, enter information for the following fields.



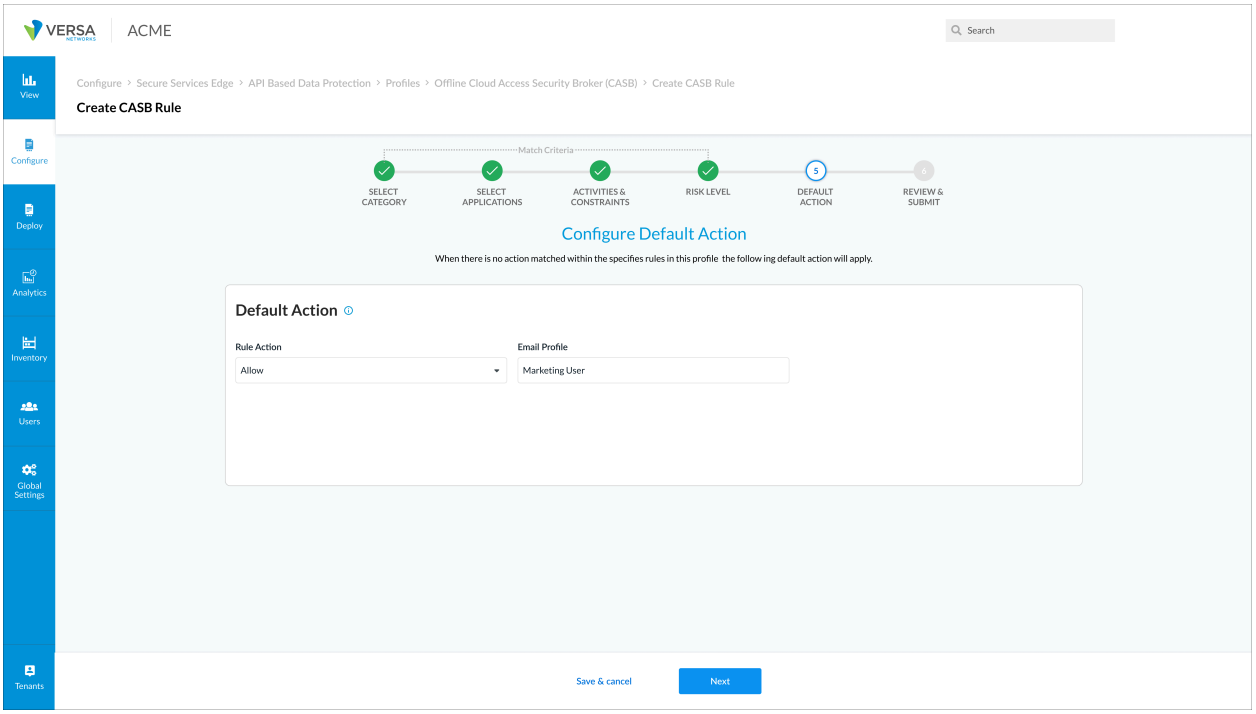
Fields	Description
Login	Select an action to take when a login is attempted: ◦ Alert ◦ Log
Search	Select an action to take when a search is attempted.
Edit	Select an action to take when an edit is attempted.
Create	Select an action.
Delete	Select the delete actions.
File Share	Select the file permissions to set for shared files:

Fields	Description
	◦ Remove Permissions—Select to remove comment, read, write, and owner permissions. ◦ Remove Users—Select the option to remove users: ▪ All users ▪ Domain profiles ▪ User profiles ▪ External users ▪ Selected users ◦ Set expiry—Enter an expiry time in minutes, after which access is expired. ◦ Exclude—Select exclude options.
File Upload	Select an action to take when a file is uploaded: ◦ Legal hold ◦ Quarantine ◦ Remove
File Download	Select an action to take when a file is downloaded: ◦ Alert ◦ Log

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

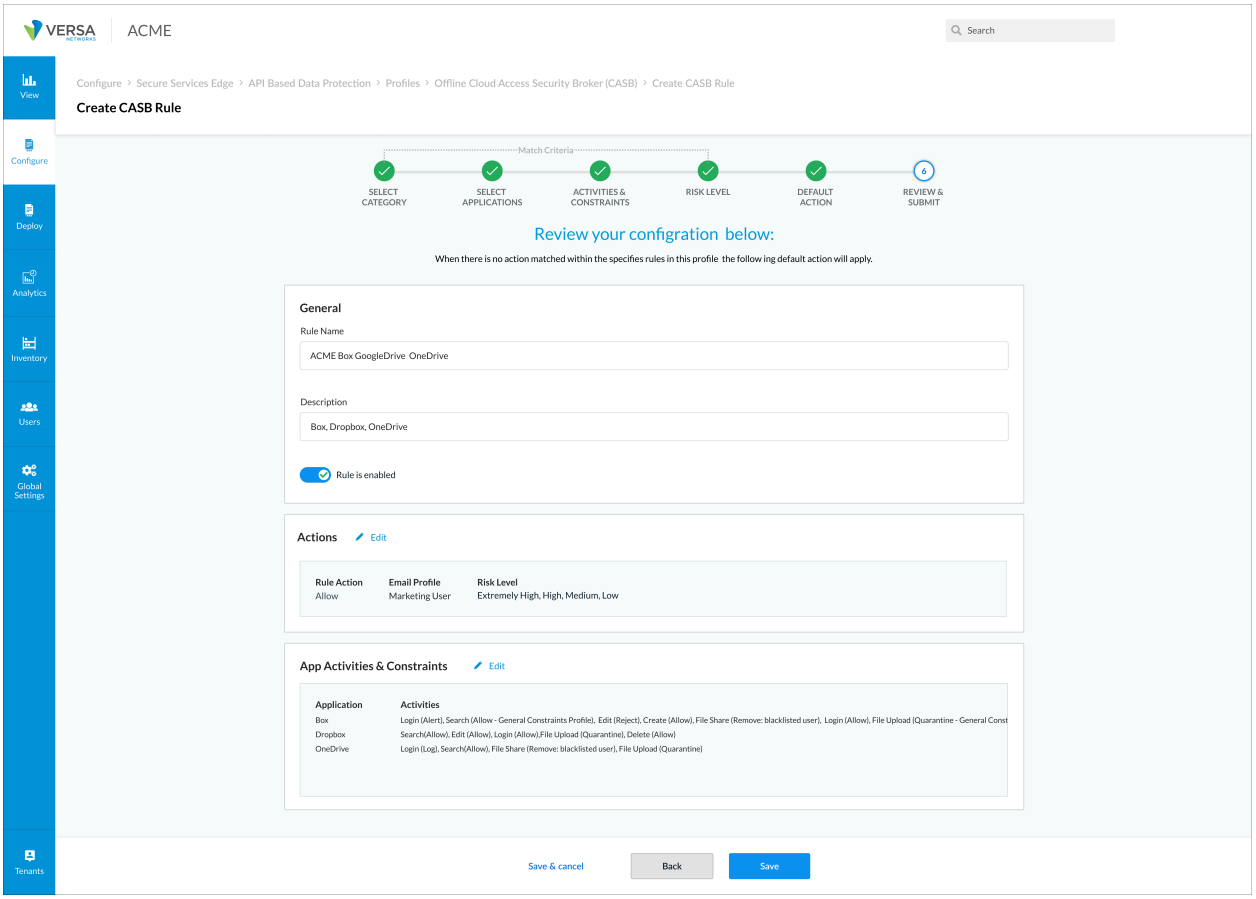


11. In Step 5, Default Action screen, select the default action to perform when there are no matching criteria. By default, applications that do not match any criteria are allowed. Enter information for the following fields.

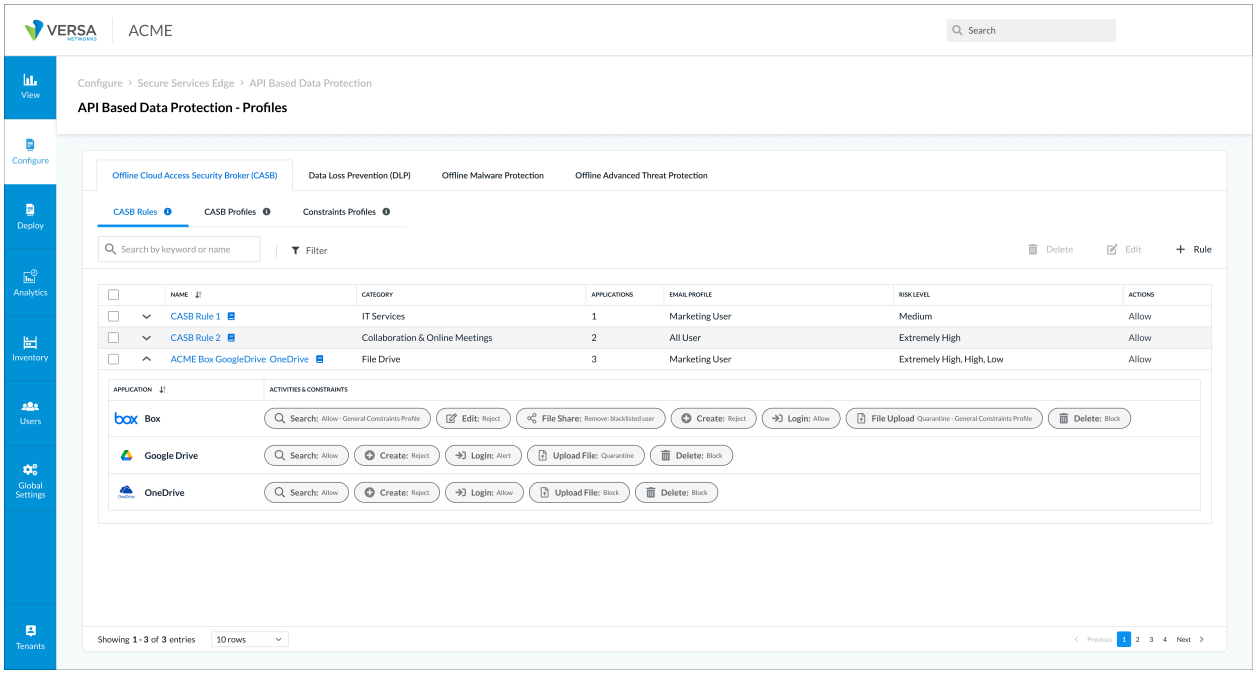


Field	Description
Rule Action	Select the default action to perform when there are no matching criteria: ◦ Allow—Allow cloud applications.
Email Profile	Enter an email profile.

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



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.



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