Configure CASB Profiles

For supported software information, click here.

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

As more applications move to the cloud, 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 user downloads, uploads, and file sharing.

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

The Versa Operating System™ (VOS™) CASB functions as inline software, leveraging the VOS deep packet inspection (DPI) software to monitor user activity, enforce security policies, and provide granular access control for cloud applications. Versa Networks also supports API integration with SaaS applications. This API integration makes use of API calls to SaaS applications, inspects user activities and contents, enforces security policies, and provides granular access control for SaaS applications. The CASB action can match the risk level and activity of multiple cloud applications, and can allow, deny, or restrict access to shadow IT.

To enforce CASB security policies, you create one or more CASB profiles, specify match criteria for applications, and then associate CASB profiles with an internet protection rule. For Releases 12.1.1 and later, you add CASB rules to configure CASB profiles. You can also add constraint profiles to configure constraints from and to users or user groups. You associate constraint profiles with CASB profiles.

Versa supports both inline CASB and API-Data Protection (API-DP) CASB. The following table compares inline CASB to API-DP CASB and is useful in deciding when to use each of them.

Inline CASB	**API-based Data Protection (CASB)**
~80 SaaS applications, more applications and activities continuously added through security package updates	30+ SaaS/IaaS application connectors, more applica are developed as feature additions

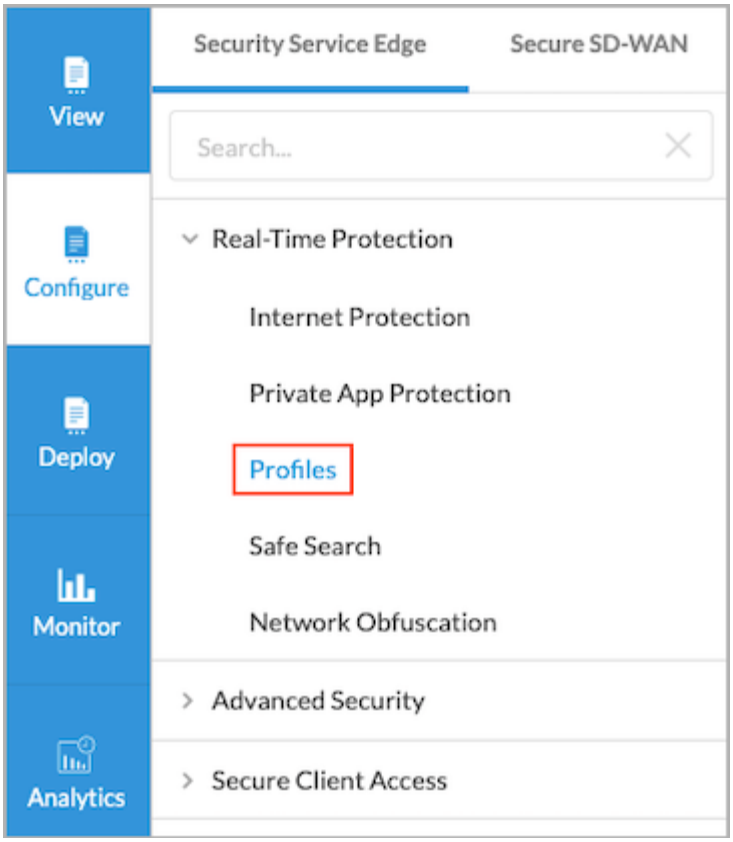
Inline CASB	API-based Data Protection (CASB)
Complements API-DP	Complements inline CASB
Deployed through VOS	Deployed offline, closer to the SaaS application
Granular actions—login, upload, download, video, chat etc.	Very granular app-specific actions—for example, file channel, actions based on a sender/receiver list or g Outlook, etc.
No additional authorization needed because this is a proxy	Needs explicit authorization by an application admin
Operates at the network layer using a reverse proxy mechanism	Operates at the application layer—Uses webhooks, connectors, and works directly as an authorized con IaaS application
Risk classification on a scale of 1–5, from extremely low to extremely high risk	Risk classification does not apply
Use where it is possible to decrypt TLS	Use when the SaaS/IaaS application is certificate pi
Works through the Versa Cloud Gateway or an appliance running VOS, typically through a corporate network	Works even for users who bring their own device (B from outside the corporate network

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

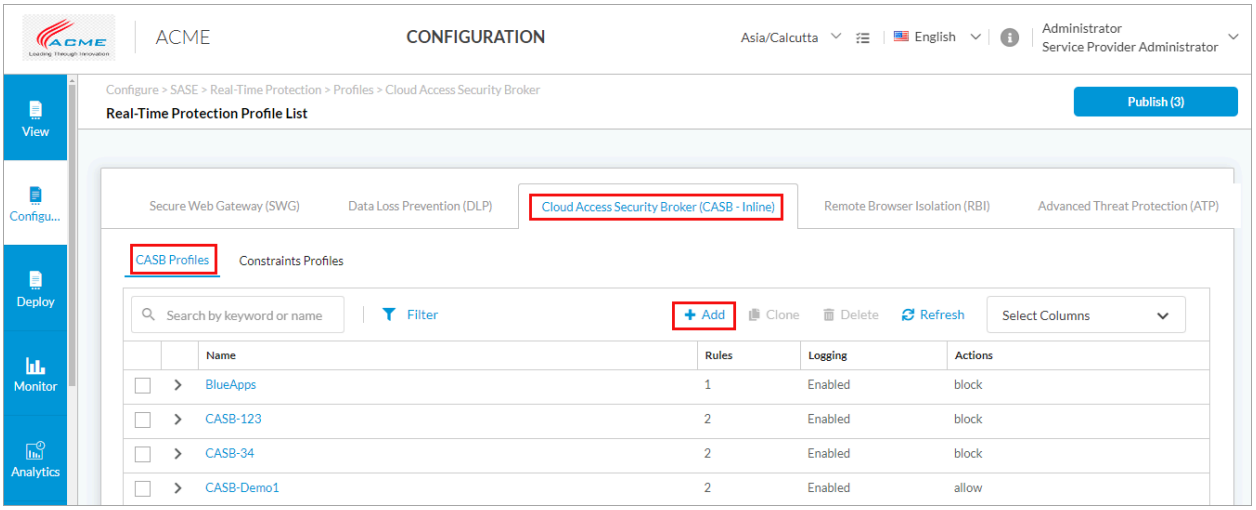
Configure a Custom CASB Profile

For Releases 12.1.1 and later.

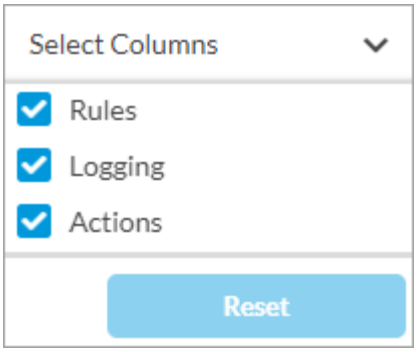
1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



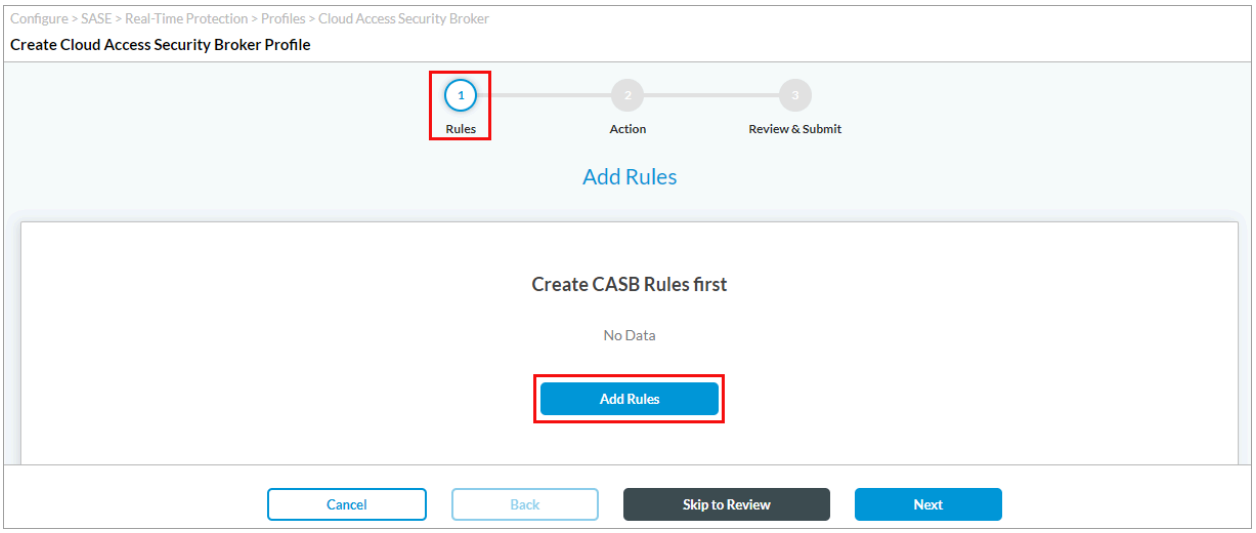
The following screen displays.



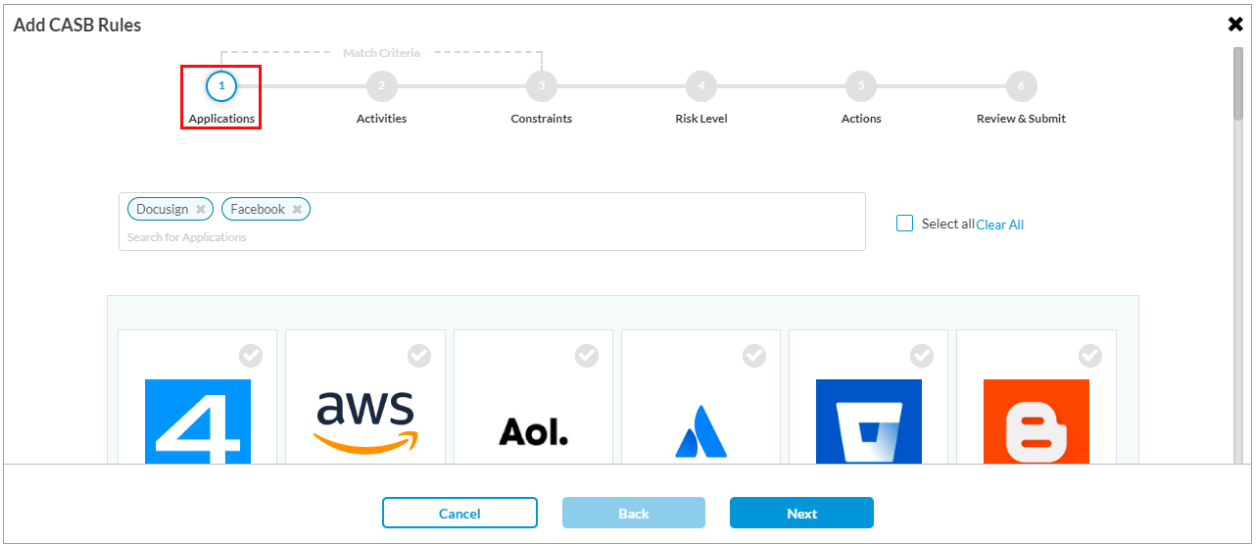
2. Select the Cloud Access Security Broker (CASB Inline) tab.
3. To customize which columns display, click Select Columns, and then click Applications to display or hide the applications. Click Reset to return to the default columns settings.



4. Select the CASB Profiles tab.
5. Click + Add to create a profile. The Create Cloud Access Security Broker Profile screen displays.



6. In Step 1, Rules, click Add Rules to create CASB rules. You must add at least one rule to proceed. The Add CASB Rules screen displays.



7. In Step 1, Applications, select the cloud applications for which you want to configure actions. You can also search for applications to select. The following web-based applications and activities are supported:

Application	Activity
4shared	Download file, login, share, upload file
Amazon AWS	Login
AOL	Login
Atlassian	Login
Bitbucket	Download file, login
Blogger	Download file, upload file
Box.net	Download file, login, search, share, upload file
Craigslist	Login, search
Dailymotion	Like, login, upload file, watch stream
Daum Mail	Download file, search, upload file
DocuSign	Login, upload file
Dropbox	Download file, login, search, share, upload file
eBay	Login, search, upload file
Evernote	Login
Excel Online	Download file, share

Facebook	Download file, login, post, upload file
Facebook Workplace	Login, upload file
Flickr	Upload file
GitHub	Download file, like, login, upload file
Gmail	Download file, send, upload file
Google Accounts	Login
Google Docs	Download file, login, share, upload file
Google Photos	Download file
Google Talk	Audio, video
imo	Audio, audio video, video
Instagram	Like, login, search, share, upload file
Jira	Login, upload file
Join.Me	Upload file
LastPass	Download file, login
Line	Audio, video
LinkedIn	Download file, like, login, post, search, upload file

Mail.ru	Download file, login
Microsoft OneNote	Download file, share
Microsoft Outlook	Download file
Microsoft Teams	Audio, audio video, download file, file transfer, like, search, share, upload file, video
Naver Mail	Download file, share, upload file
Netflix	Login
Office 365	Login
Okta	Login
OneDrive	Download file, login, share, upload file
OneLogin	Login
Pandora	Search
PayPal	Login
Pinterest	Download file, like, login, search, share, upload file
PowerPoint Online	Share
ProtonMail	Search, upload file
Reddit	Like, login, post, upload file

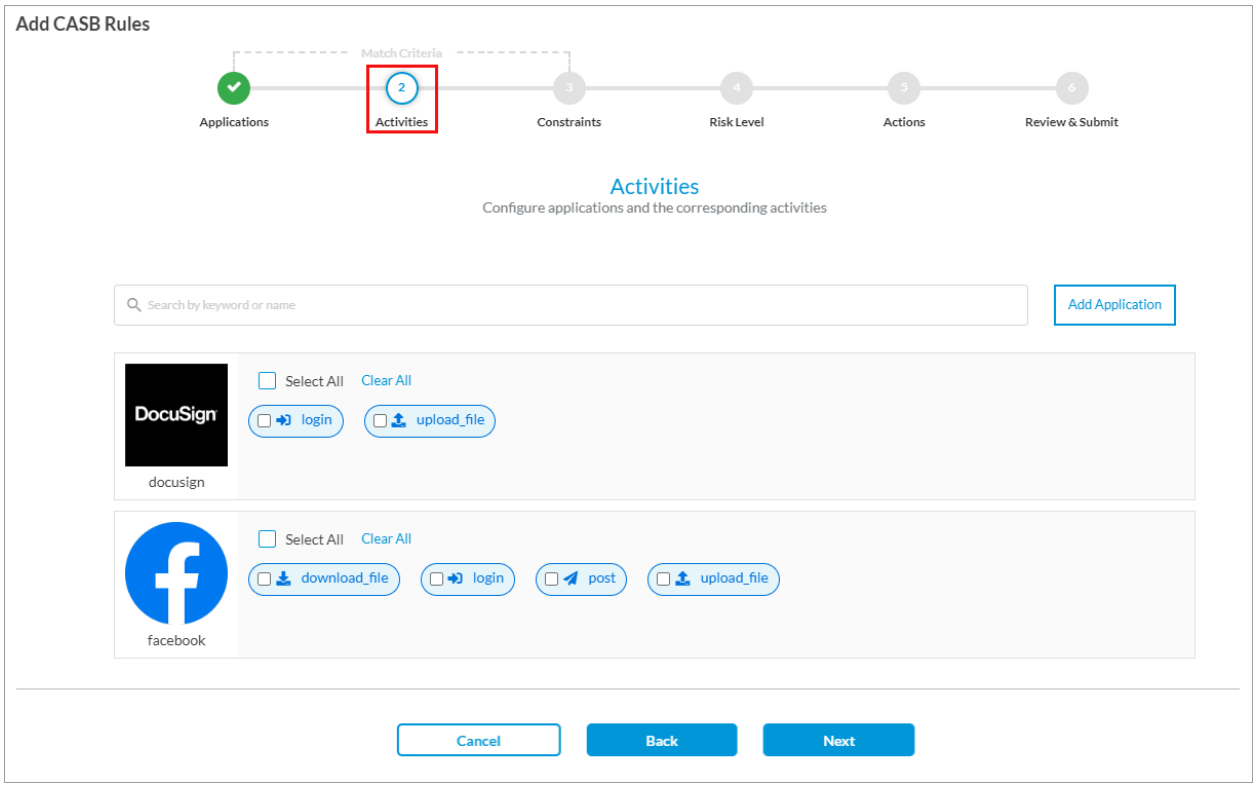
Salesforce	Login, download file
ShareFile.com	Download file, login, search, upload file
SharePoint Online	Search, share
Shopify	Login
Skype	Audio_video, file transfer, like, audio, video
Slack	Download file, like, login, post, search, share, upload file
SlideShare	Login, search, upload file
SoundCloud	Download file, login, search, upload file
SourceForge	Download file, login, search, upload file
Spotify	Like, login, search, upload file
Stack Overflow	Login, search, upload file
Tango	Audio, video
Telegram	Audio
Trello	Search, upload file
Twitch	Login, upload file, watch stream
Twitter	Like, login, post, search, upload file

Viber	Audio, video
Vimeo	Comment, like, search, upload file, watch stream
VMware	Login
Webex	Audio, audio video, login, search, video
WeChat	File transfer
WeTransfer	Download file, share
WhatsApp	Audio, audio video, video
Word Online	Download file, share, upload file
WordPress	Download file, login, upload file
Xero	Login
Yammer	Download file
Yandex	Login
Yandex Mail	Download file
YouTube	Broadcast stream, comment, download file, like, search, share, upload file, watch stream
Zalo	Audio, video
Zoom	Login

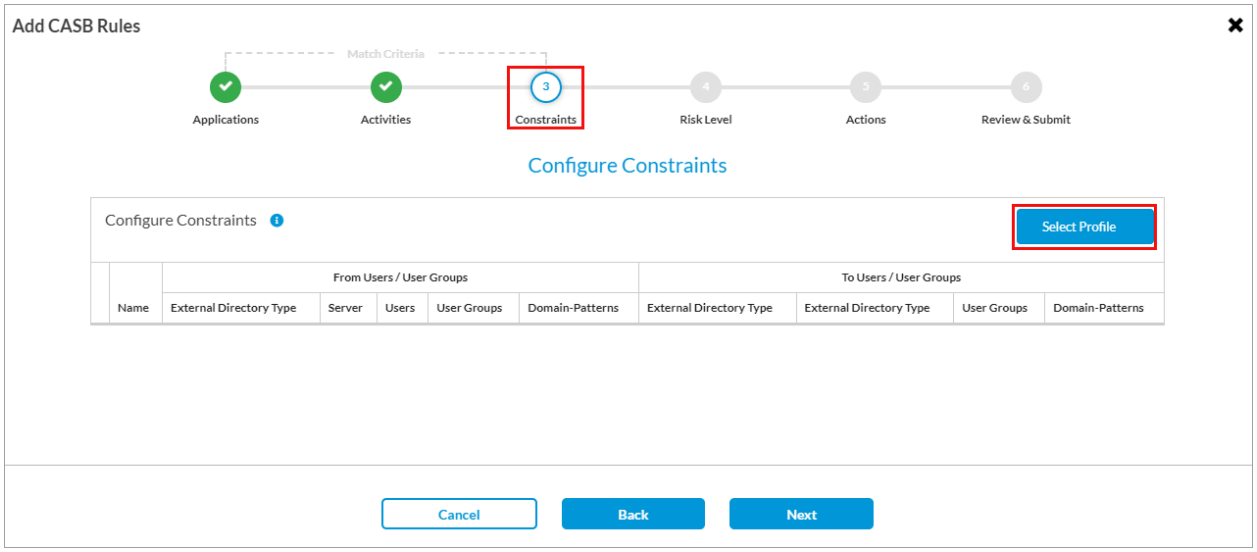
Note: The list shown above is for web-based applications. For mobile applications, a subset of applications are supported, as follows. If an application is not listed in the following table, it is supported as a web-based application and will not work in mobile devices due to certificate pinning.

SaaS Application	Web Activities Supported	Mobile Activities Supported—iOS
Box.net	Yes	Yes
Gmail	Yes	Yes—Send, upload file, download file
Google Accounts	Yes	Yes—Login
Google Docs	Yes	Yes—Upload file, login, share, download file
Gtalk	Yes	Yes—Audio, video
imo	Not applicable	Yes—Audio, video, audio video
Line	Not applicable	Yes—Audio, video
LinkedIn	Yes	Yes—Login, like, upload file, post
Office365	Yes	Yes—Login
Telegram	Not applicable	Yes—Audio
Twitch	Yes	Yes—Login, watch stream
Viber	Yes	Yes—Audio, video
WhatsApp	Yes	Yes—Audio, video, audio video
YouTube	Yes	Yes—Broadcast stream, comment, like, watch str
Zoom	Yes	Yes—Login

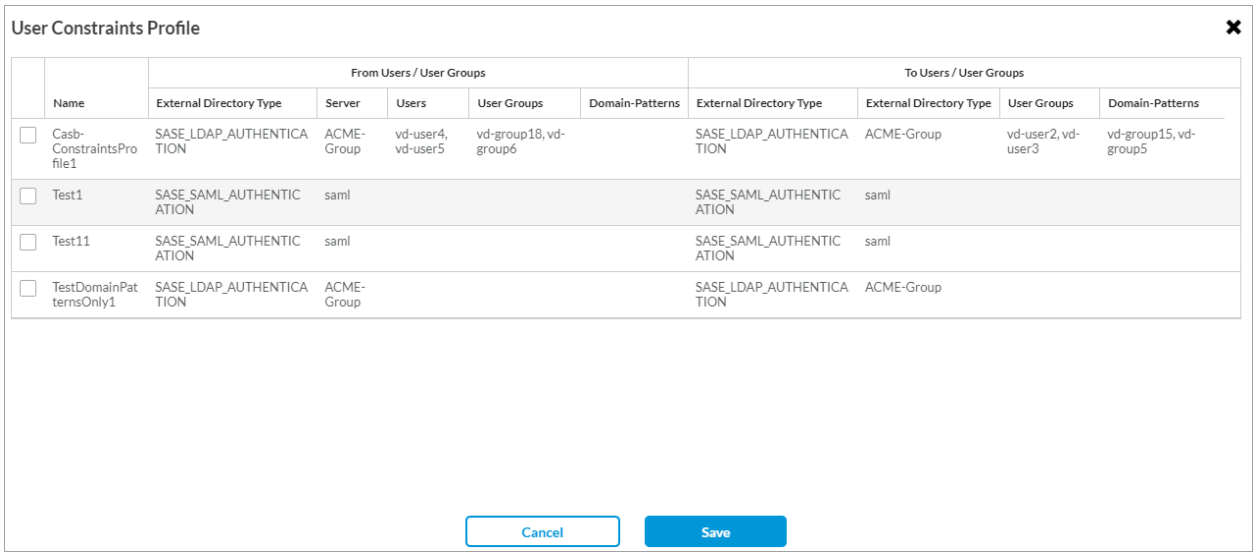
8. Click Next to go to Step 2, Activities. The screen displays the applications that you selected in Step 1, Applications.



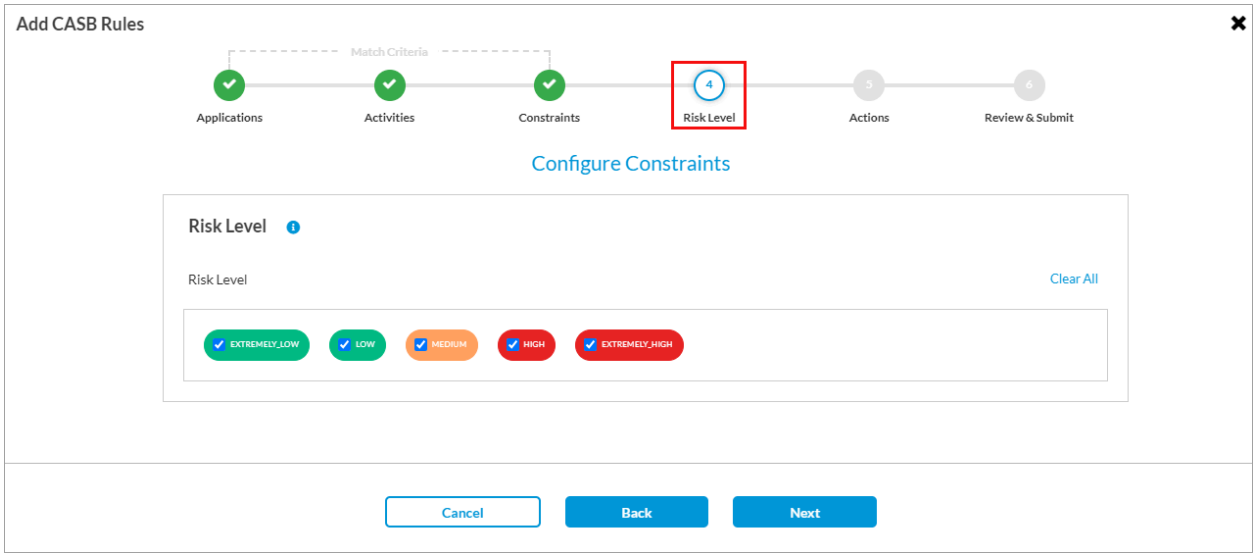
9. To add more applications, click Add Application to select more applications on the Step 1, Application screen.
10. Select the application activities for which you want to configure actions.
11. Click Next to go to Step 3, Constraints to select constraints for applications.



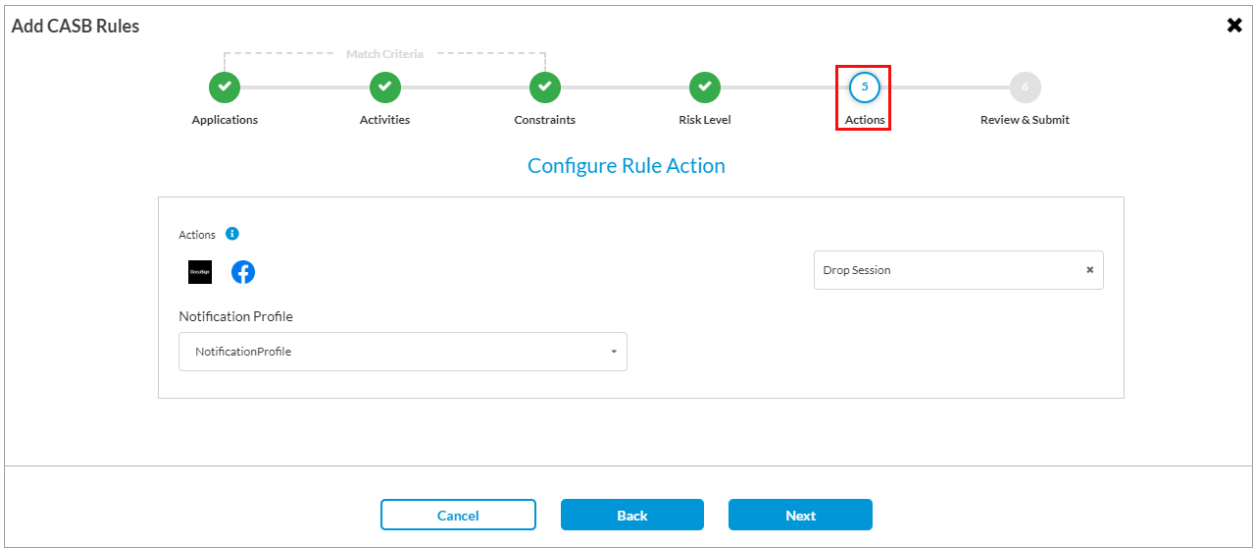
12. Click Select Profile to select a constraint profile. The User Constraints Profile screen displays.



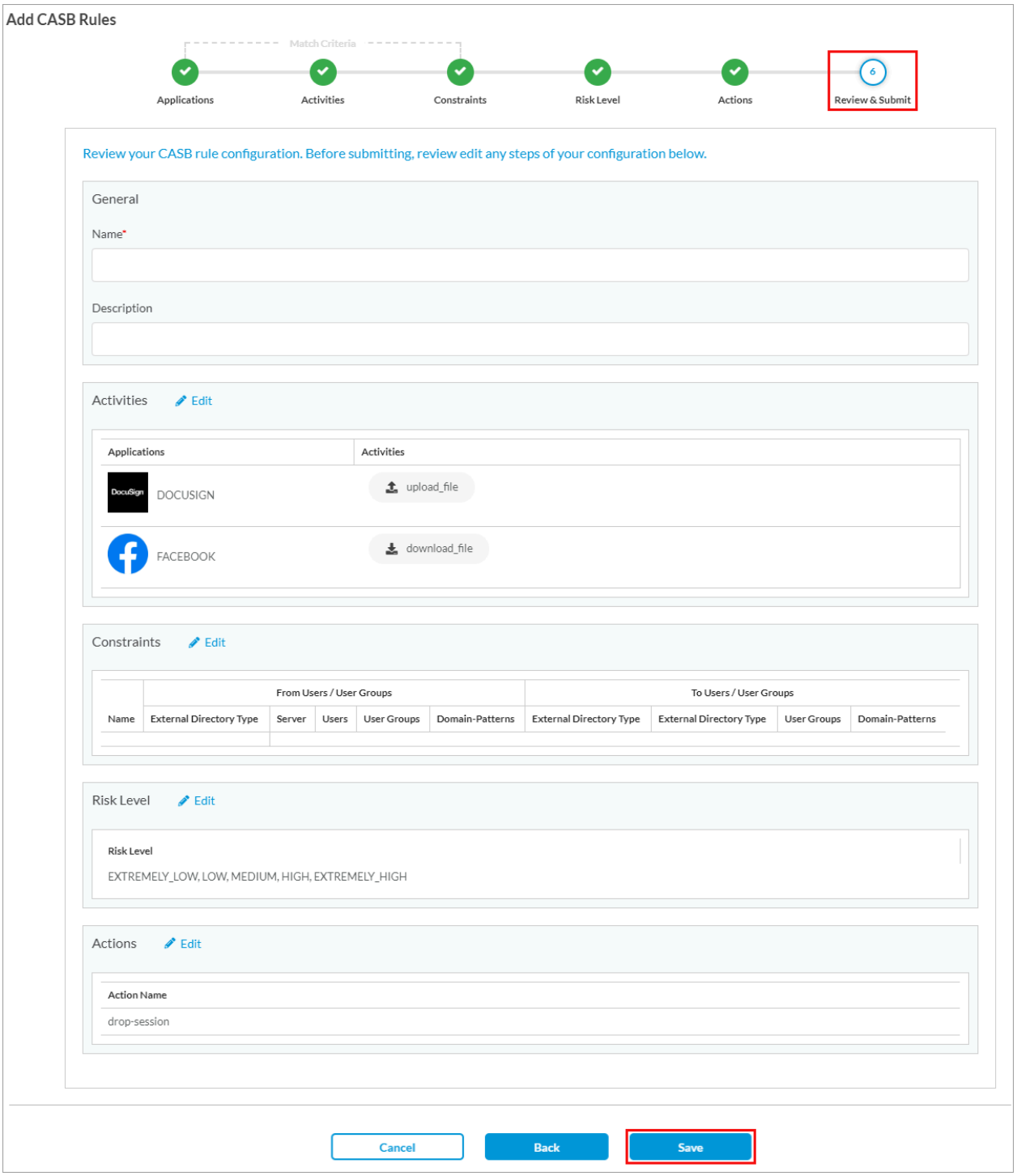
13. Select a constraint profile and click Save. You can select only one constraint profile for a CASB rule. For more information, see Configure Constraint Profiles, below.
14. In the Add CASB Rules screen, click Next to go to Step 4, Risk Level.



15. Select the risk level, which can be Extremely Low, Low, Medium, High, and Extremely High. A color is associated with each risk level.
16. To clear the selections, click Clear All.
17. Click Next to go to Step 5, Actions.

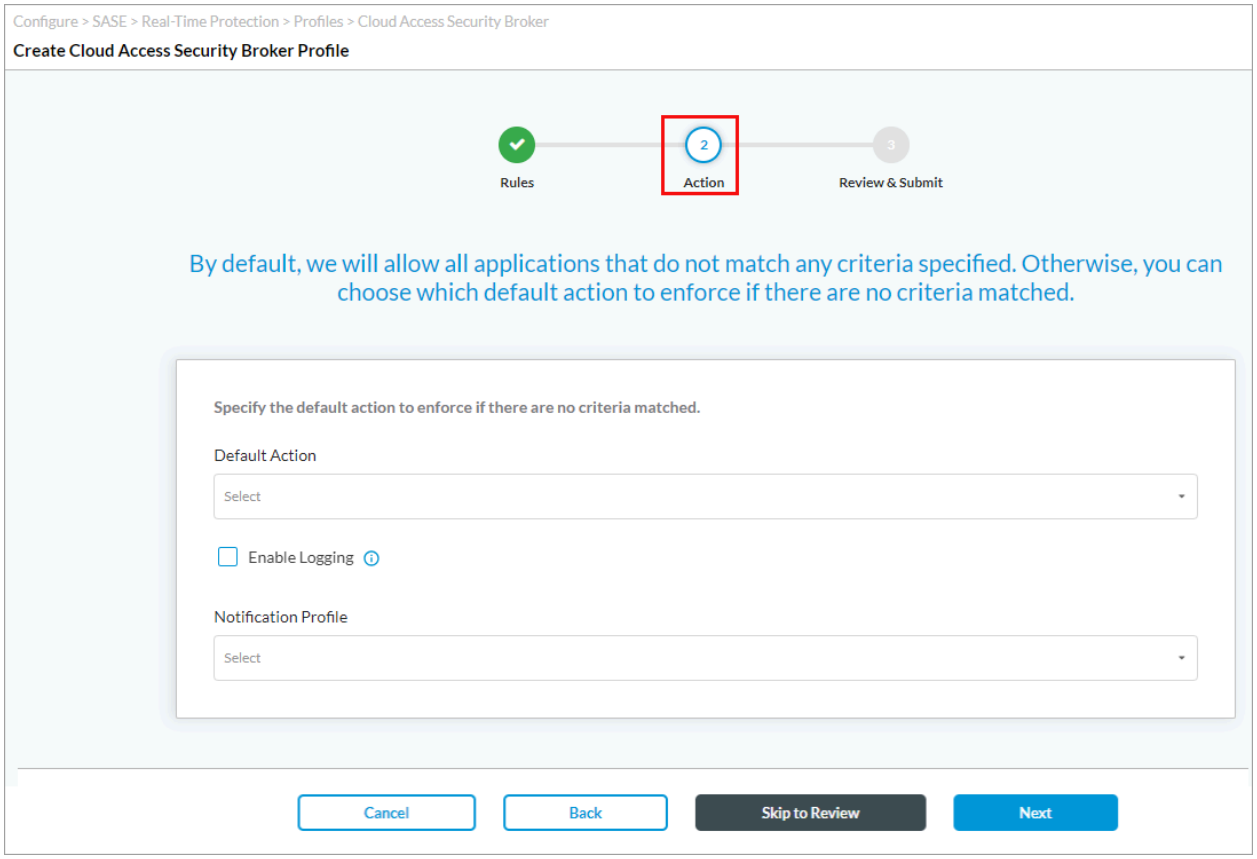


18. In the field on the right, select a predefined or custom action to perform when there are no matching criteria. For more information, see Configure Custom Security Actions. The predefined actions are:
    - Allow—Allow cloud applications.
    - Block—Block cloud applications.
    - Drop Session—Drop cloud application sessions.
19. In the Notification Profile field, select a profile to send email notifications. For more information, see Configure a Notification Profile.
20. Click Next to go to Step 6, Review and Submit.



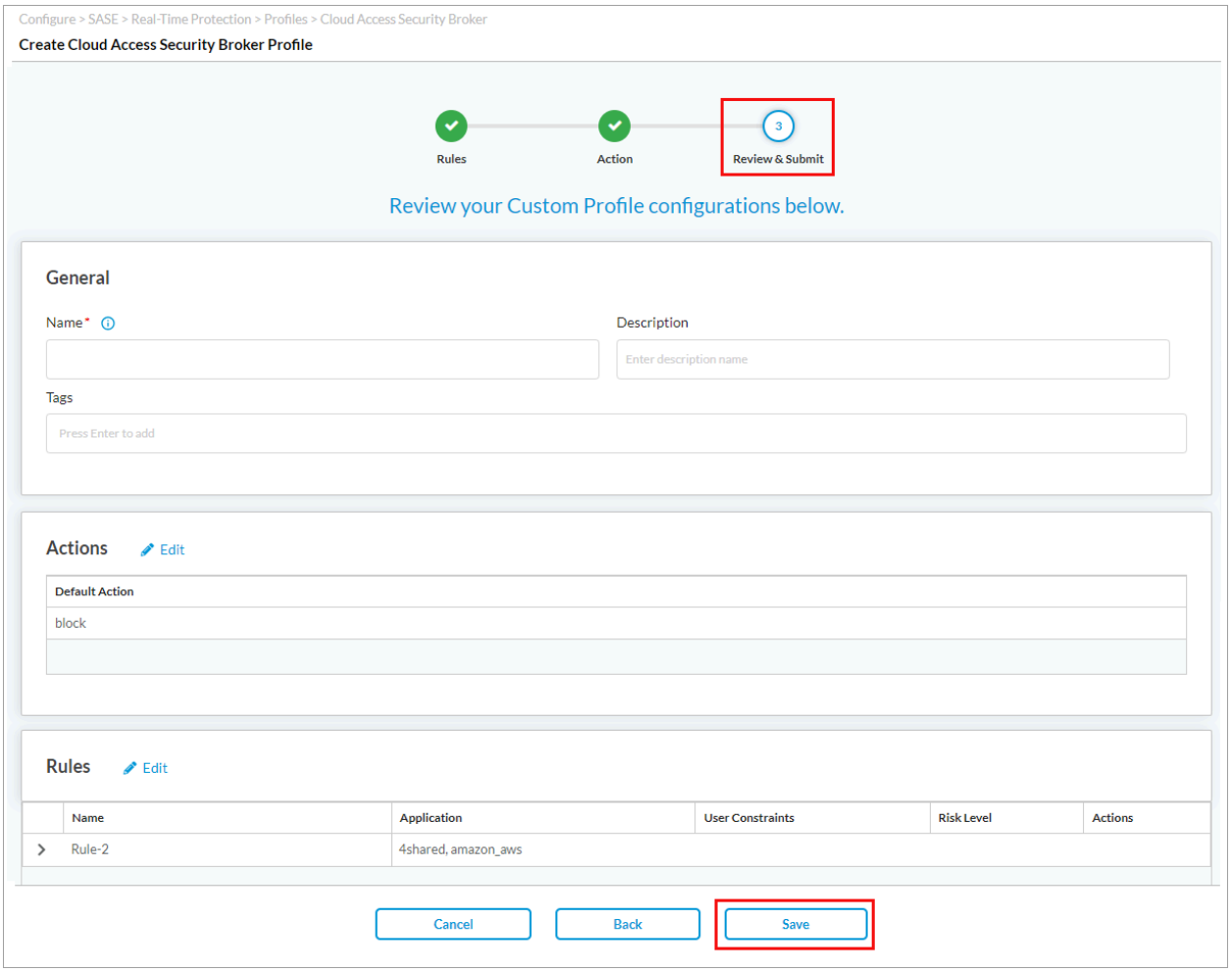
21. In the General section, enter a name for the CASB profile and, optionally, a description and tags.
22. For all other sections, review the information. To make changes, click the Edit icon.
23. Click Save.
24. In the Create Cloud Access Security Broker Profile screen, click Next to go to Step 2, Action, to 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
Default Action	Select the default action to perform when there are no matching criteria: ◦ Allow—Allow cloud applications. ◦ Block—Block cloud applications. ◦ Drop Session—Drop cloud application sessions. ◦ Reject—Reject cloud applications.
Enable Logging	Click to enable CASB logging.
Notification Profile	Select a profile to send email notifications. For more information, see Configure a Notification Profile.

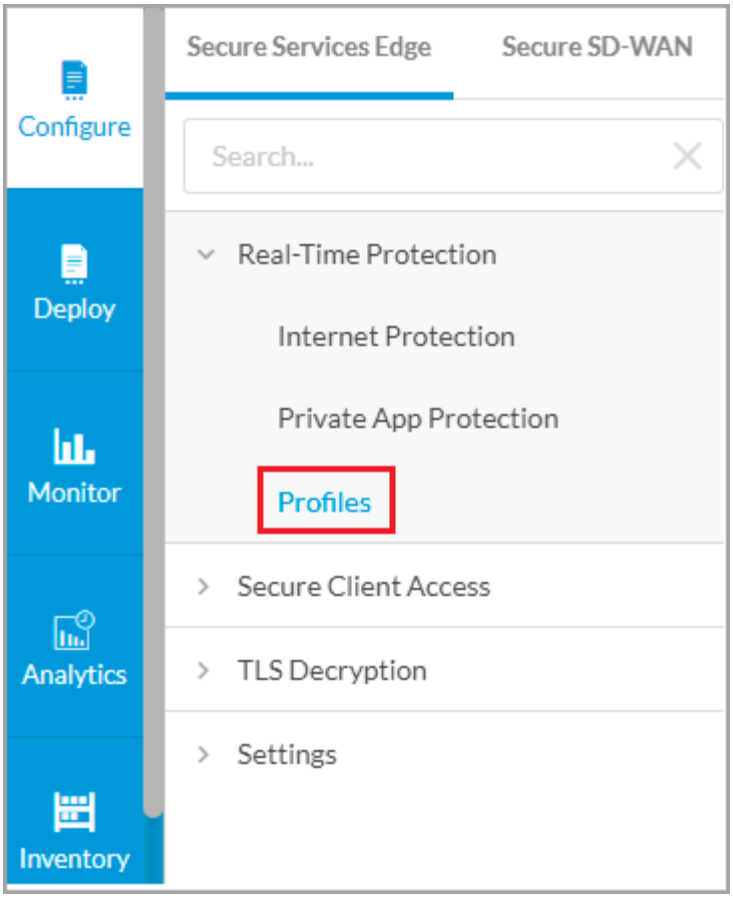
25. Click Next to go to Step 3, Review and Submit.



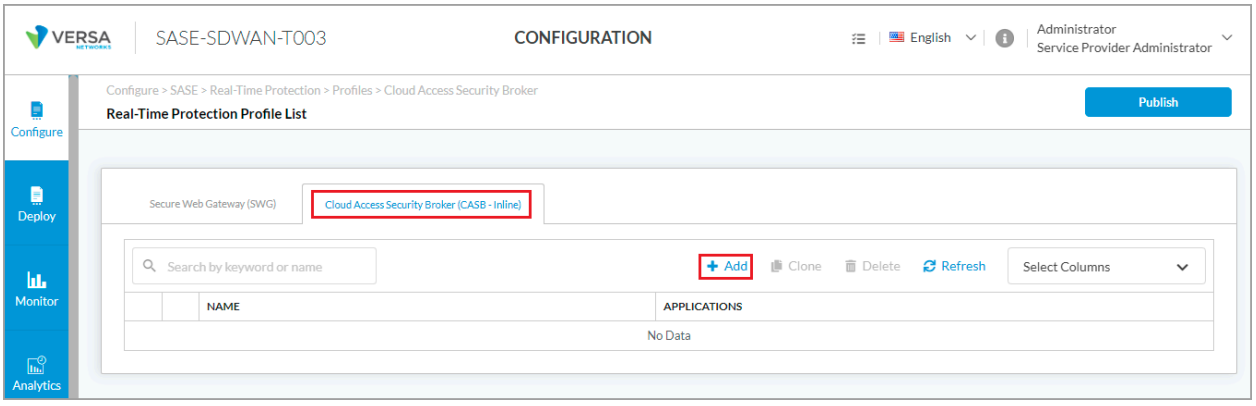
26. In the General section, enter a name for the CASB profile and, optionally, a description and tags.
27. For all other sections, review the information. To make changes, click the Edit icon.
28. Click Save.

Configure a Custom CASB Profile (for Releases 11.4 and Earlier)

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.

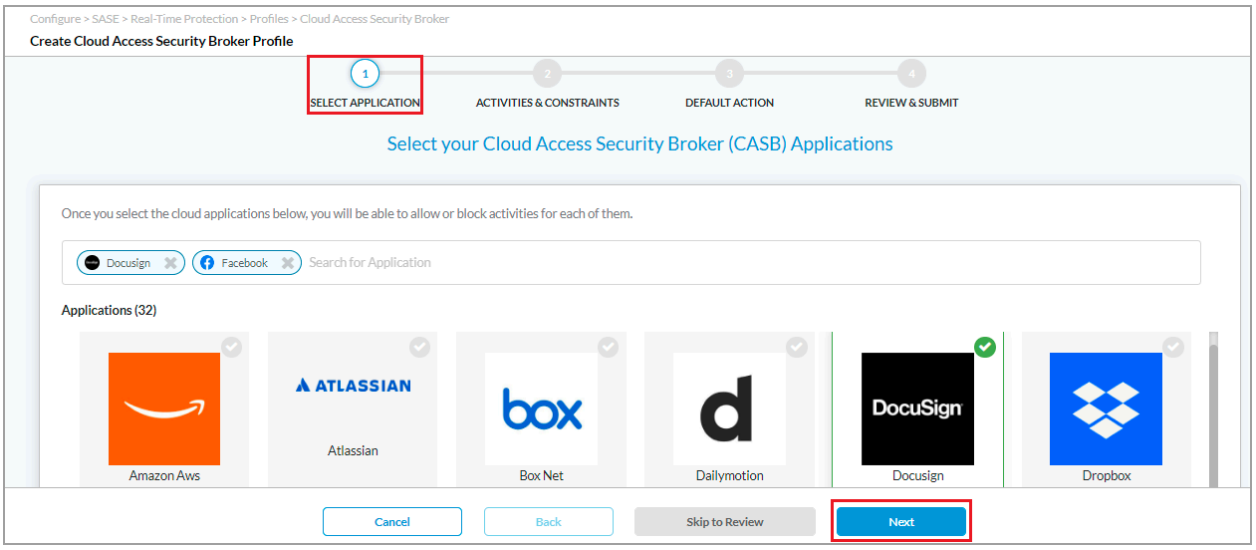


The following screen displays.

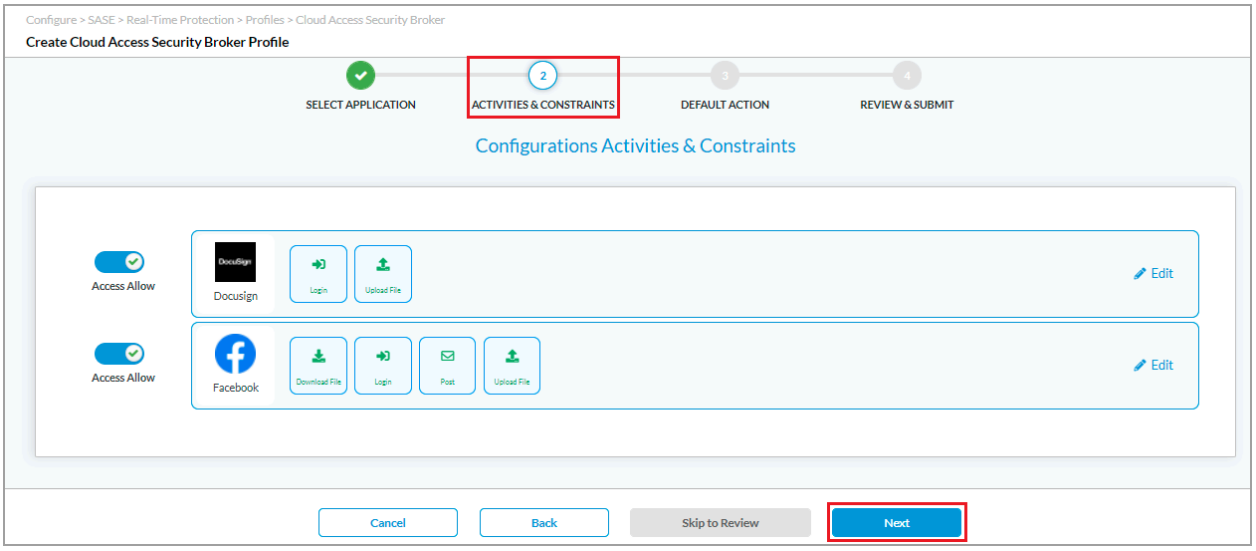


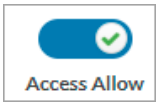
2. Select the Cloud Access Security Broker (CASB Inline) tab.
3. To customize which columns display, click Select Columns and then click Applications to display or hide the applications. Click Reset to return to the default columns settings.

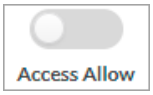
4. Click + Add to create a profile. The Create Cloud Access Security Broker Profile screen displays.



5. In Step 1, Select Application, select the cloud applications for which you want to allow or block activities. You can also search for applications to select.
6. Click Next to go to Step 2, Activities and Constraints, to allow and block activities for the selected cloud applications, or to disable an application.



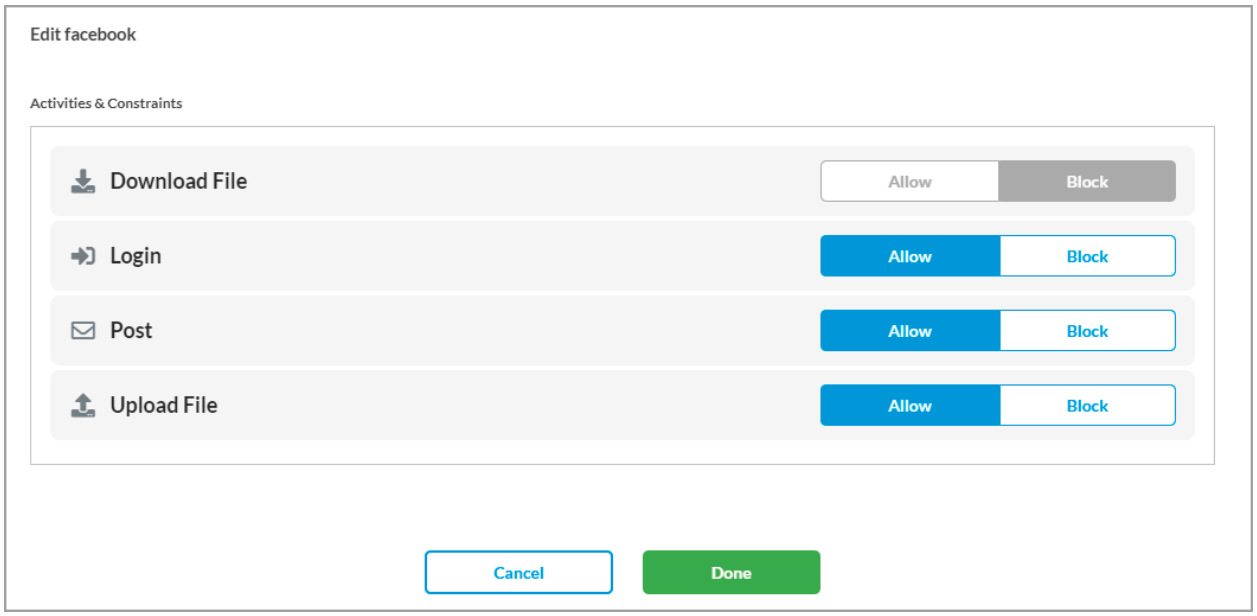
7. By default, the 

Access Allow toggle button for each application is enabled. To bypass CASB processing for an application, click the toggle button. The 

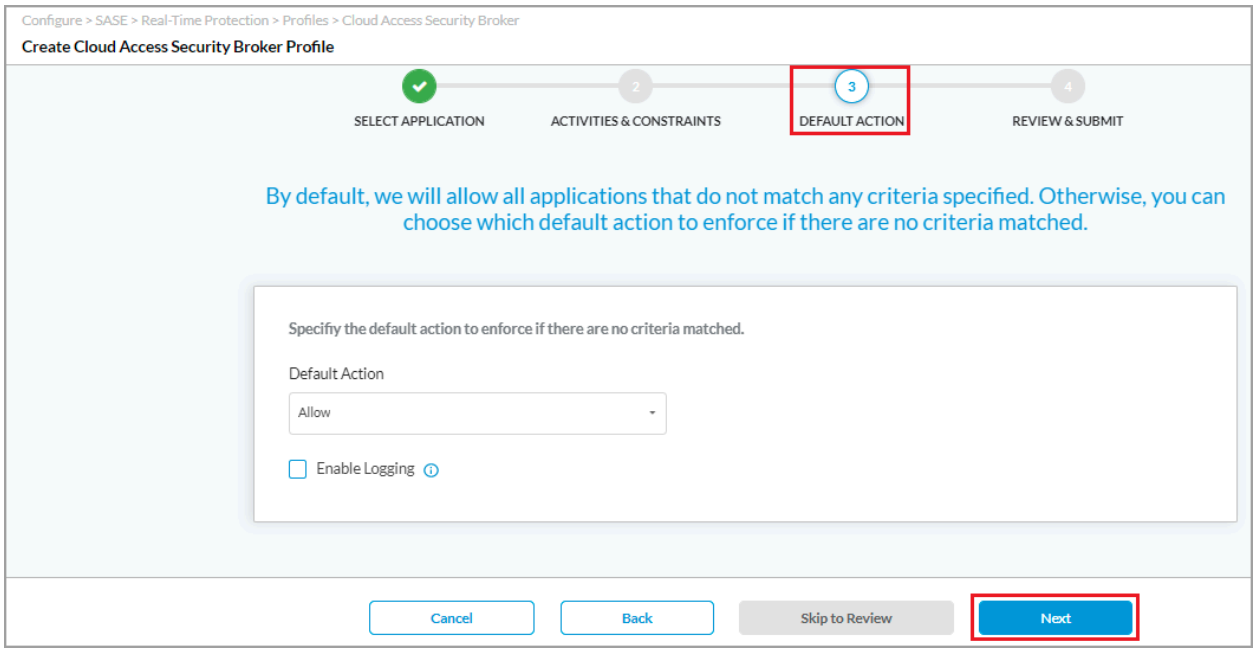
Access Allow button then turns grey.

8. 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 Facebook.

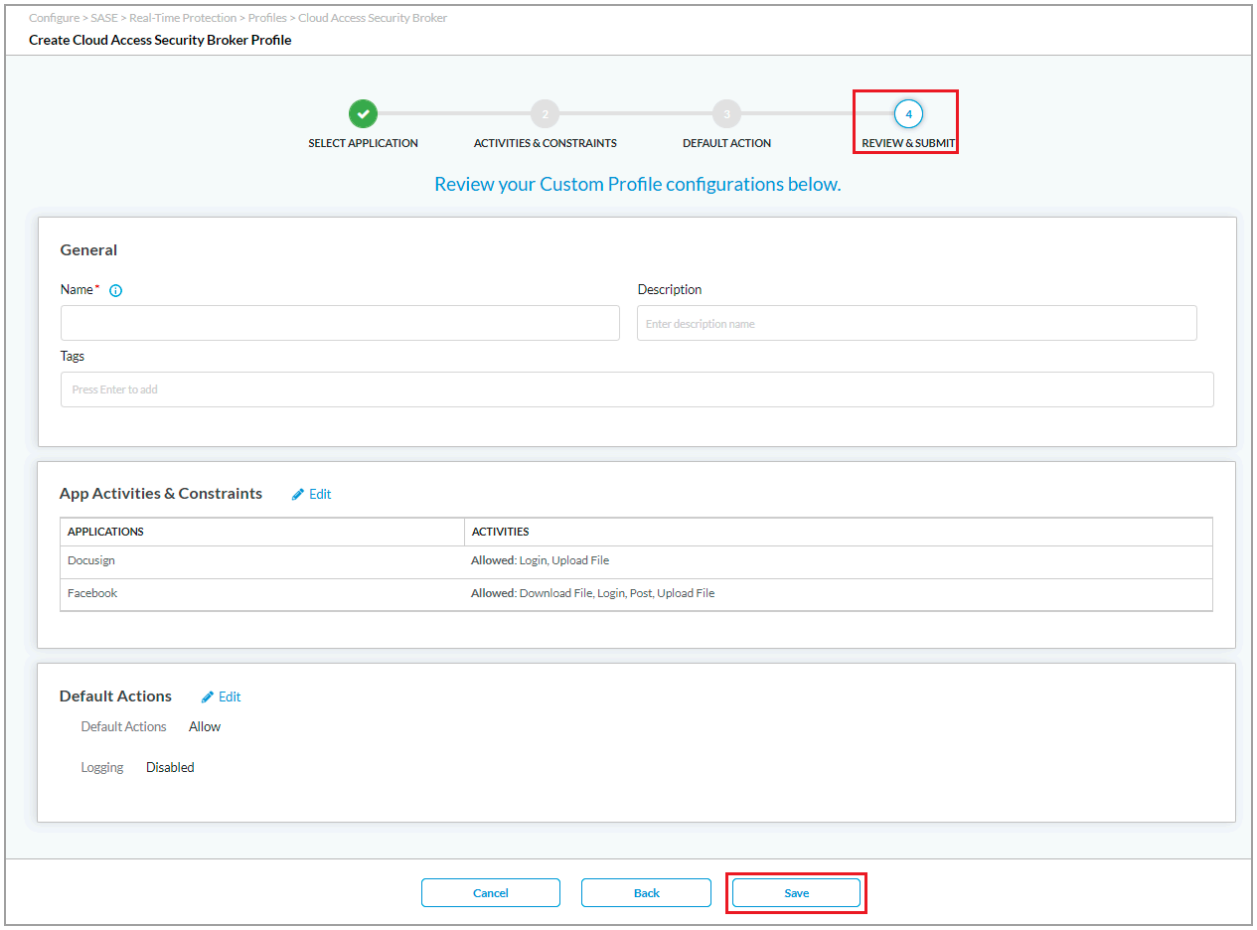


9. Click Done.
10. Click Next to go to Step 3, Default Action, to select the default action to perform when there are no matching criteria. By default, applications that do not match any criteria are allowed. Enter information for the following fields.

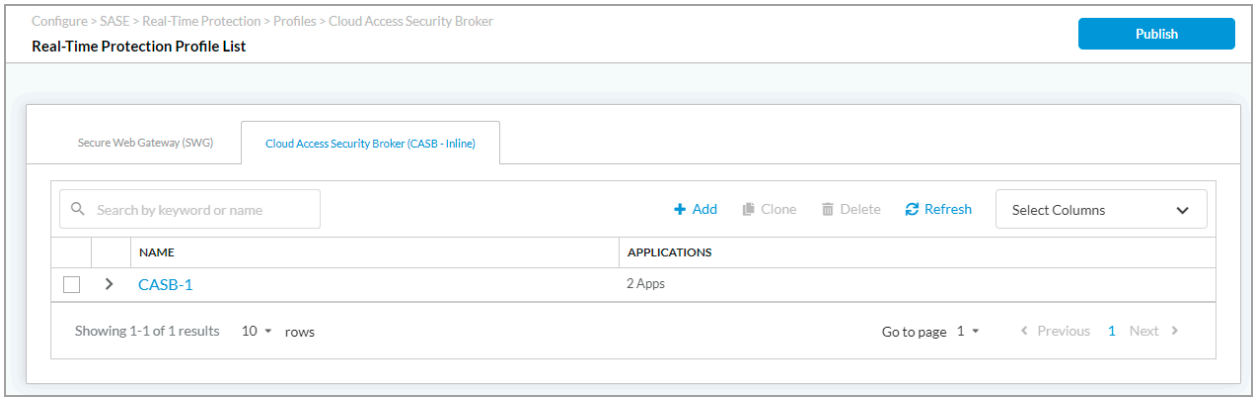


Field	Description
Default Action	Select the default action to perform when there are no matching criteria: ◦ Allow—Allow cloud applications. ◦ Block—Block cloud applications. ◦ Drop Session—Drop cloud application sessions. ◦ Reject—Reject cloud applications.
Enable Logging	Click to enable CASB logging.

11. Click Next to go to Step 4, Review and Submit.



12. In the General section, enter a name for the CASB profile and, optionally, a description and tags.
13. For all other sections, review the information. To make changes, click the Edit icon.
14. Click Save. The CASB profile is displayed in the Cloud Access Security Broker (CASB Inline) tab.



Configure Constraint Profiles

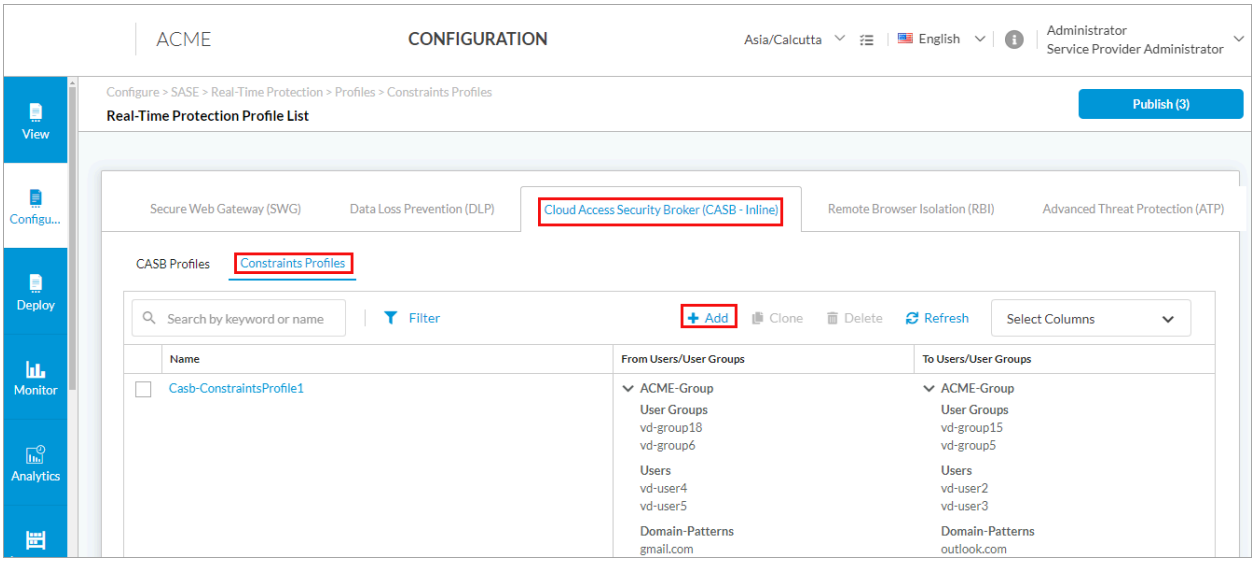
For Releases 12.1.1 and later.

You configure CASB constraint profiles to control which users and groups can access the activities configured in CASB. You can apply the CASB constraint profiles when you configure a CASB profile rule. The following table shows activities and applications that you can configure as a CASB constraint.

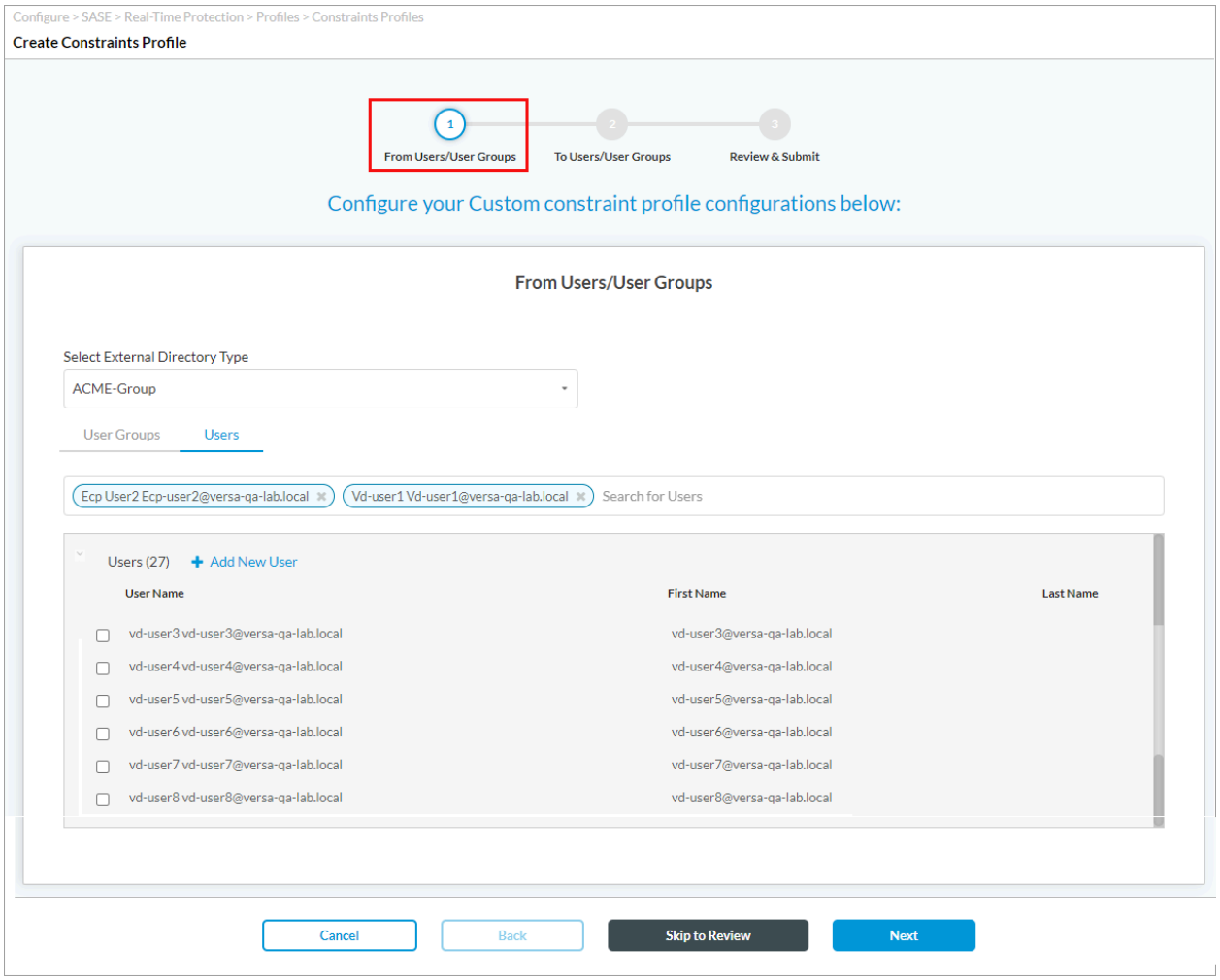
Activity	Description	Applications
Call From User	Users who can initiate a call in the application	MS Teams–audio
Call To User	Users who can receive a call in the application	MS Teams–audio
Send From User	Users who can send content in the application	Outlook
Share From User	Users who can share content in the application	Sharepoint Online
Share To User	Users who can received shared content in the application.	Box, Dropbox, One Drive, Sharepoint Online

To add constraint profiles:

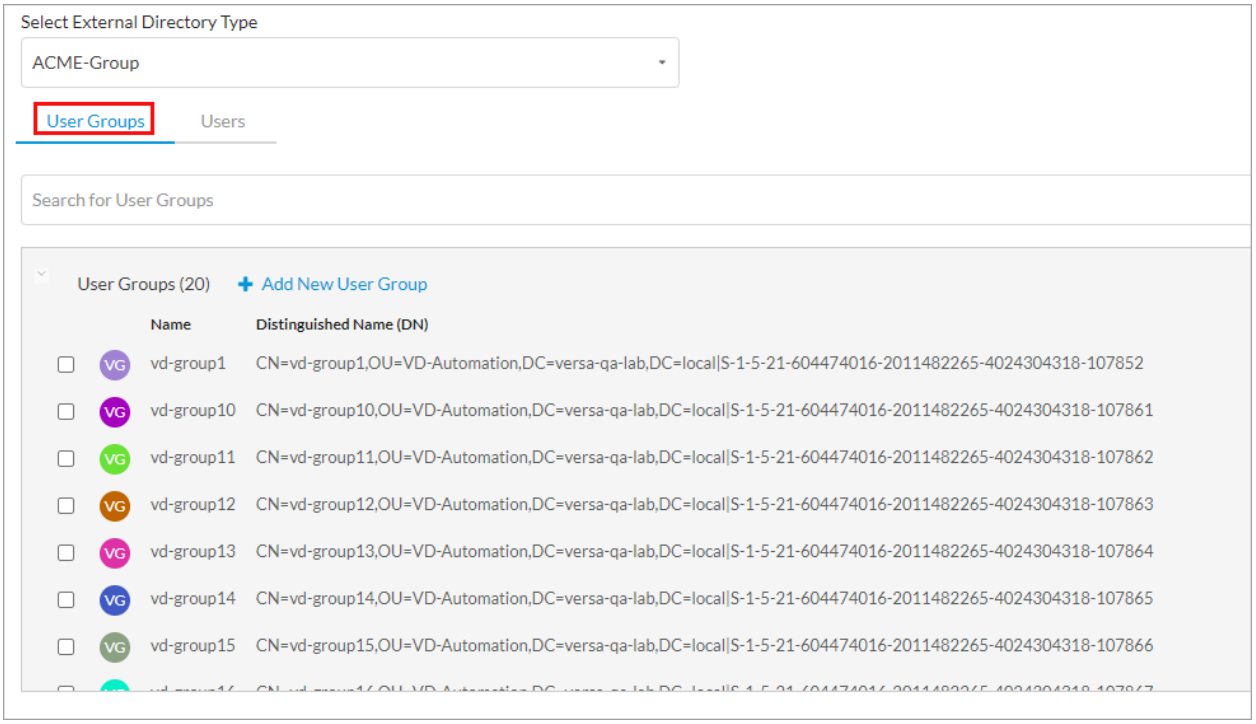
1. In the Cloud Access Security Broker (CASB Inline) tab, select Constraints Profiles.



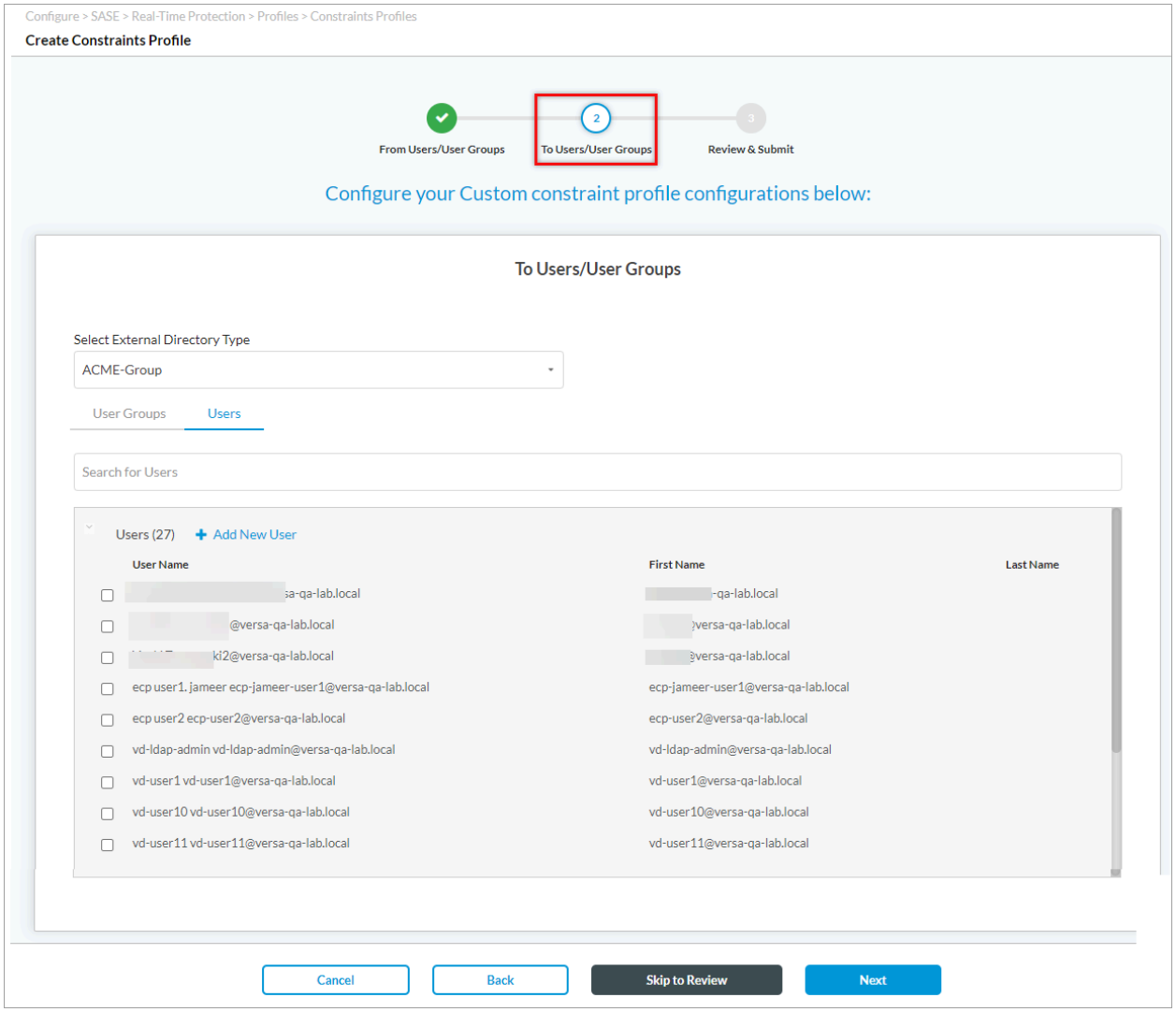
2. Click + Add. The Create Constraints Profile screen displays. In Step 1, From Users/User Groups, configure a custom constraint profile.



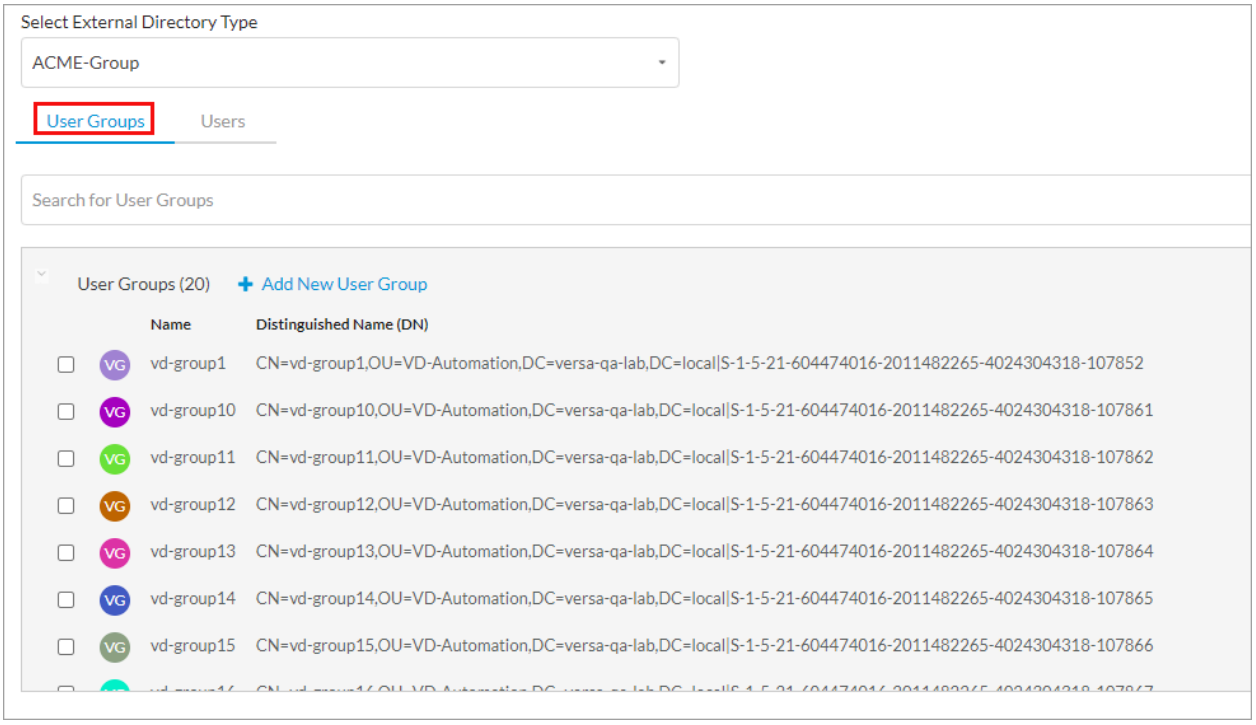
3. Select the external directory type, and then add users in the Users Tab.
4. Select the User Groups tab, and then select user groups.



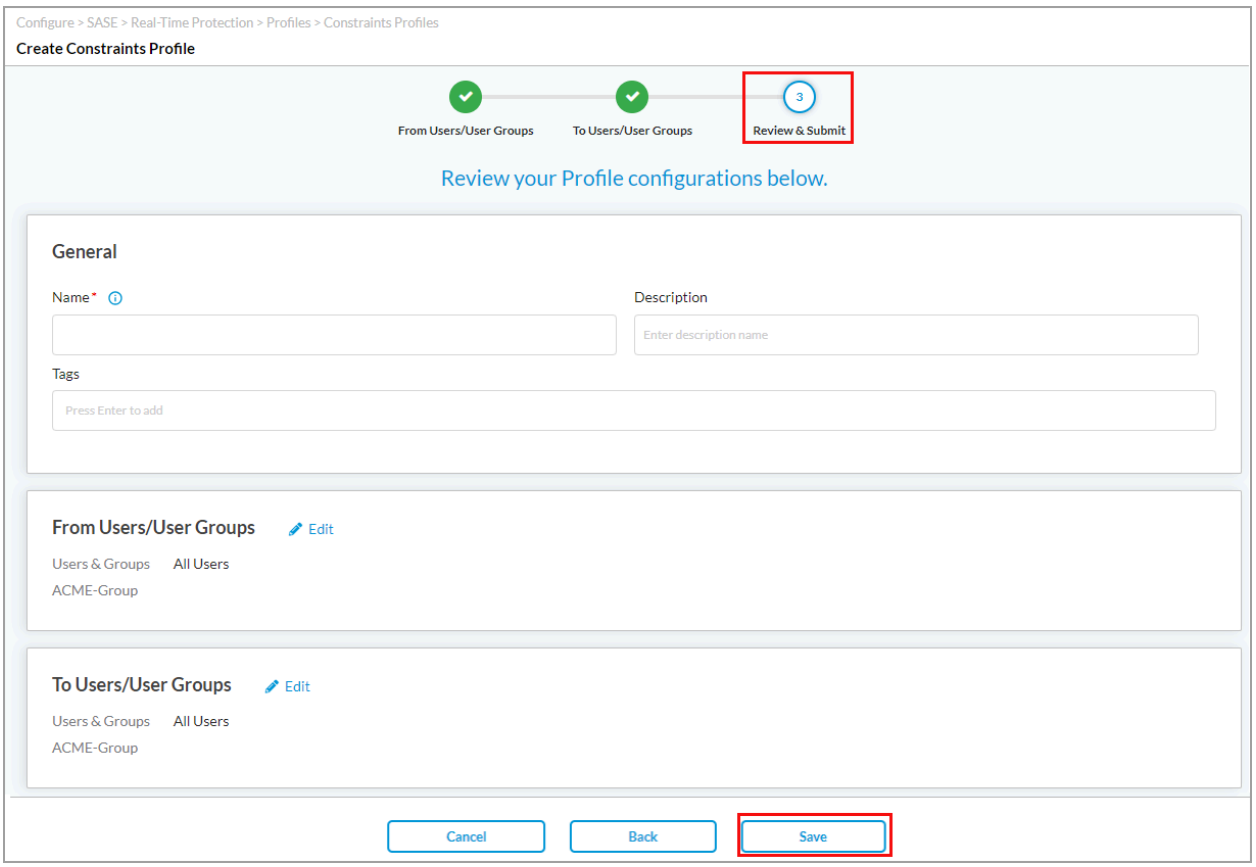
5. Click Next to go to Step 2, To Users/User Groups screen.



6. Select the external directory type, and then add users in the Users Tab.
7. Select the User Groups tab, and then select user groups.



8. Click Next to go to Step 3, Review and Submit.



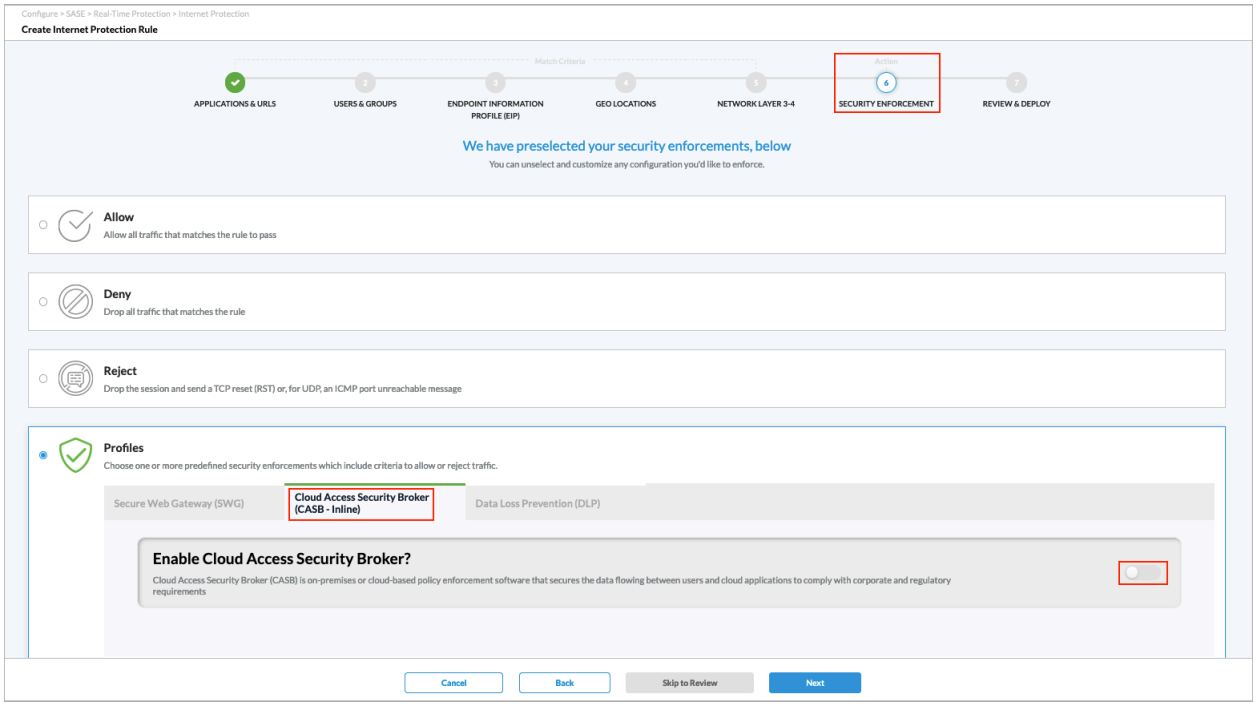
9. In the General section, enter a name for the constraints profile and, optionally, a description and tags.
10. For all other sections, review the information. To make changes, click the Edit icon.
11. Click Save.

Associate a CASB Profile with a SASE Internet Protection Rule

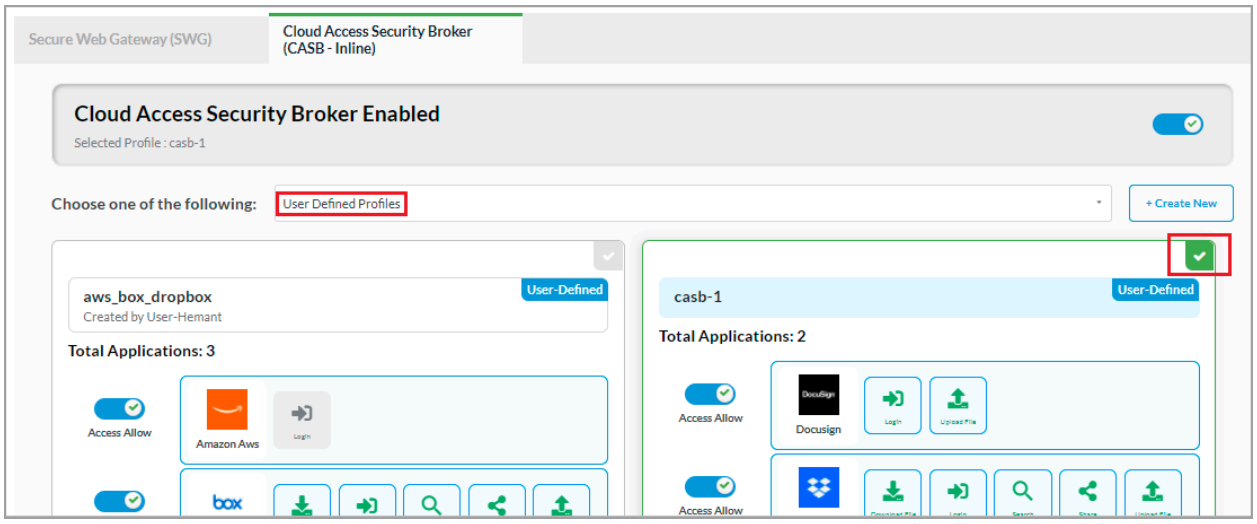
To allow or deny traffic, you associate a CASB profile with a SASE internet protection rule. CASB secures the data flowing between users and cloud applications in order to comply with corporate and regulatory requirements.

To associate a CASB profile with a SASE internet protection rule:

1. Go to Configure > Real-Time Protection > Internet Protection.
2. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays. For more information, see Configure SASE Internet Protection Rules.
3. Select the Security Enforcement screen, and then select Profiles.
4. Select the Cloud Access Security Broker (CASB Inline) tab, and then enable CASB.



5. Select User-Defined Profiles, and then select the CASB profile to associate with the internet protection rule.



6. Review and then deploy the internet protection rule.

Configure IPS-Based CASB

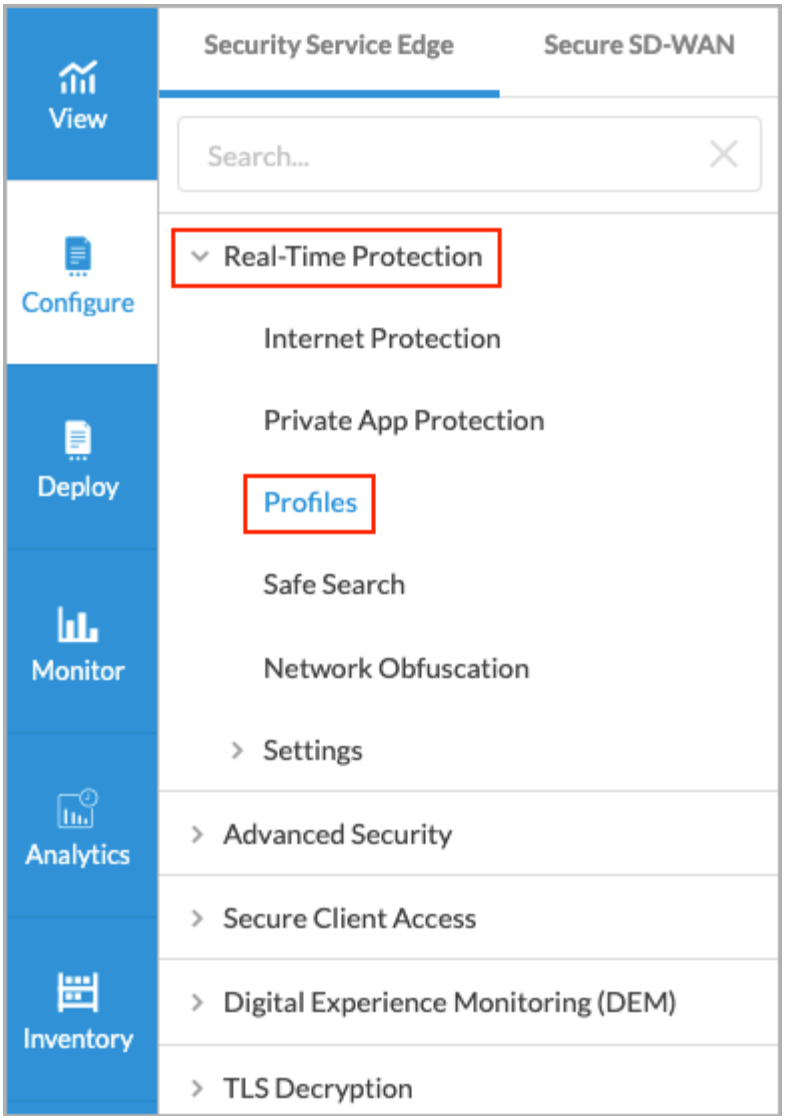
For Releases 12.1.1 and later.

You can use IPS-based signatures with CASB to protect against known threats and prevent malicious access attempts. IPS identifies malicious activity using signatures, which are rules for matching suspicious software or patterns in an application's traffic and are stored in a database of known threats.

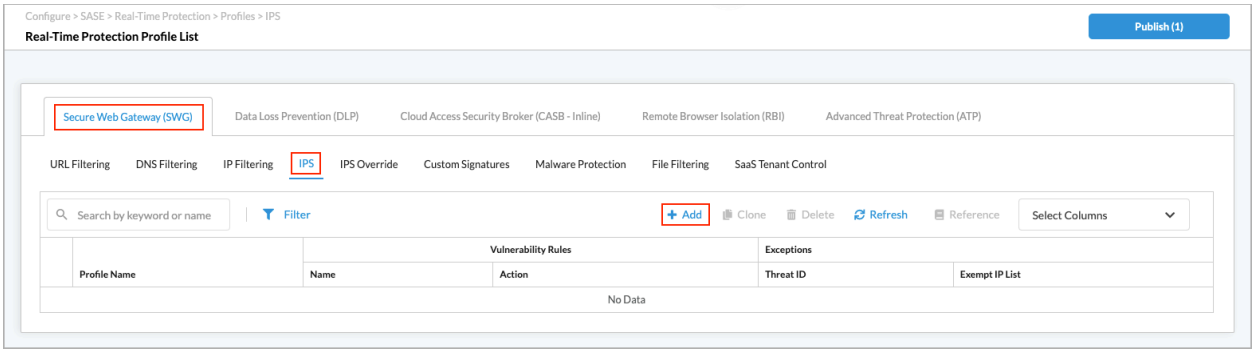
To load the IPS signatures for use with CASB, create an IPS profile with app-activity as the class type and alert as the predefined action. You then use this user-defined IPS profile along with a CASB profile in an access-policy rule, such as an internet protection rule or a private application protection rule.

To create an IPS profile for use with CASB:

1. Go to Configure > Real-Time Protection > Profiles.

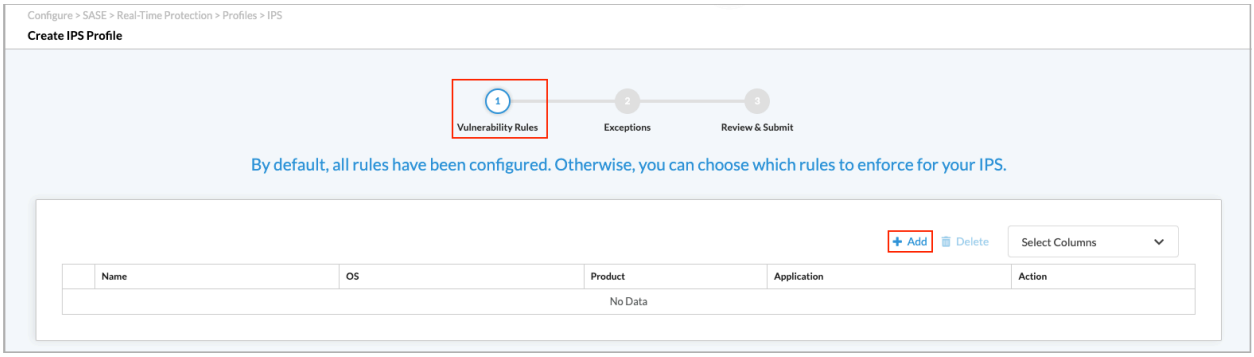


The following screen displays.



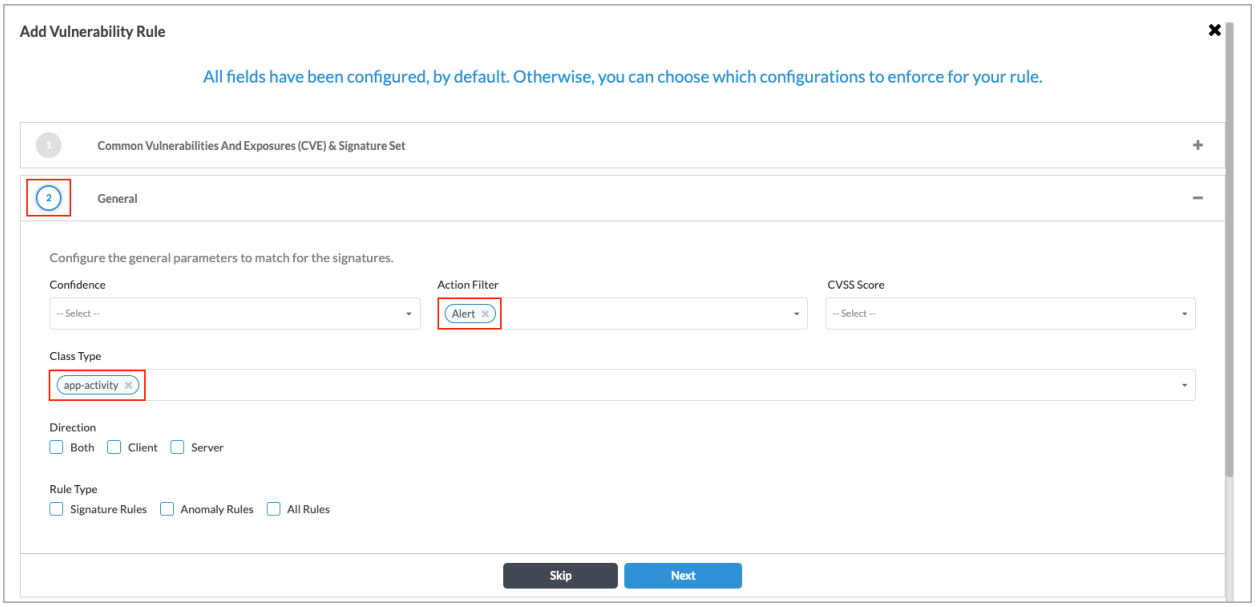
2. Select Secure Web Gateway (SWG) in the horizontal menu bar, then select IPS in the submenu bar.

3. Click the + Add icon to create a new IPS profile. The following screen displays.



4. Select Step 1, Vulnerability Rules, then click the + Add icon. The Add Vulnerability Rule screen displays with Section 1, Common Vulnerabilities and Exposures (CVE) and Signature Set selected by default.
5. Select Section 2, General, then enter information for the following fields.

   Note: This example shows only the steps needed to configure the IPS profile for use with CASB. For complete information about configuring user-defined IPS profiles, see Configure Custom IPS-Filtering Profiles.



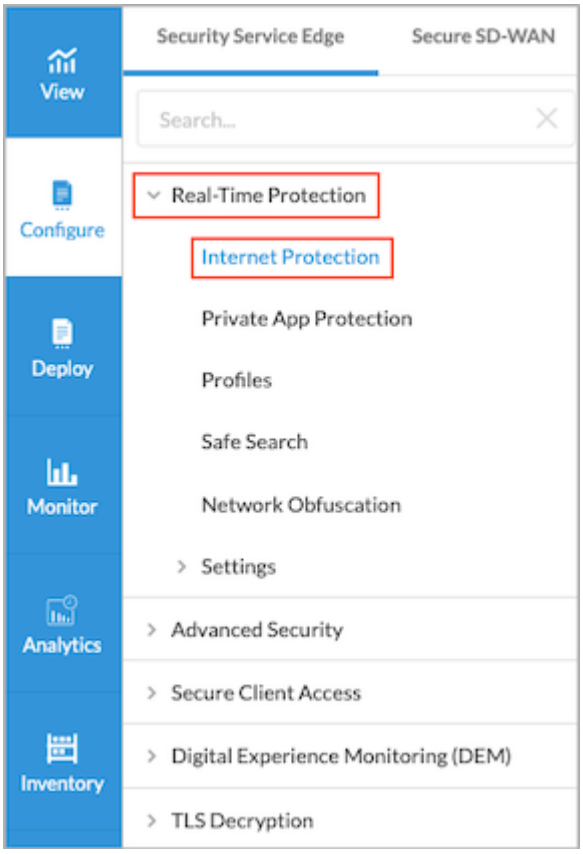
Field	Description
Action Filter	Select Alert.
Class Type	Select app-activity.

6. Complete creating the profile as shown in Configure Custom IPS-Filtering Profiles.

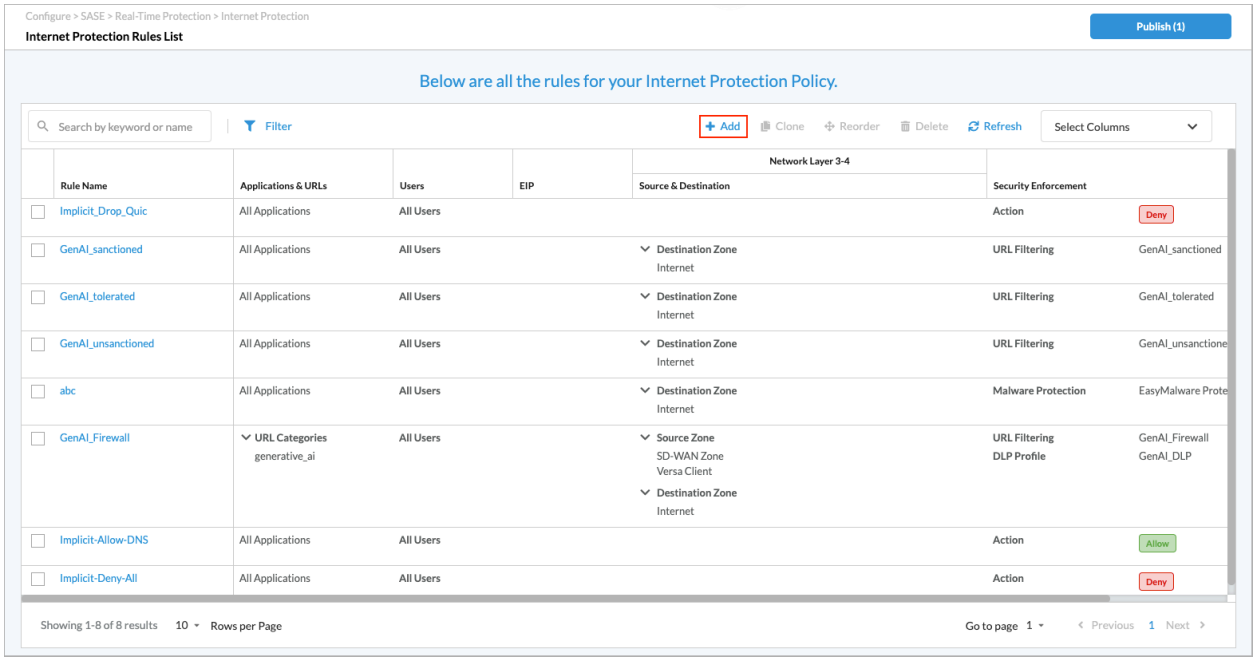
To use the IPS profile in an access-policy rule:

Note: The following procedure uses an internet protection policy rule.

1. Go to Configure > Real-Time Protection > Internet Protection.

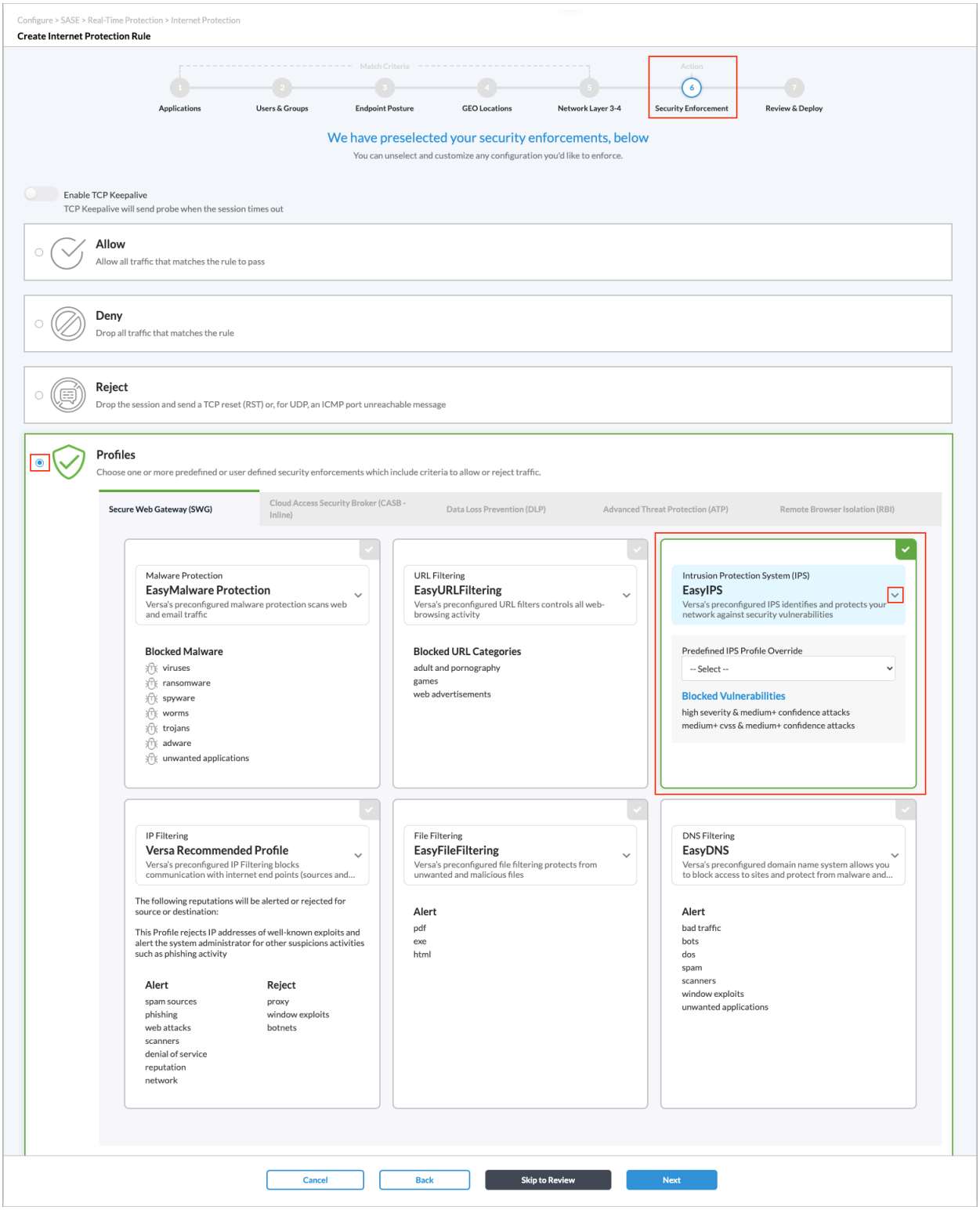


The following screen displays.

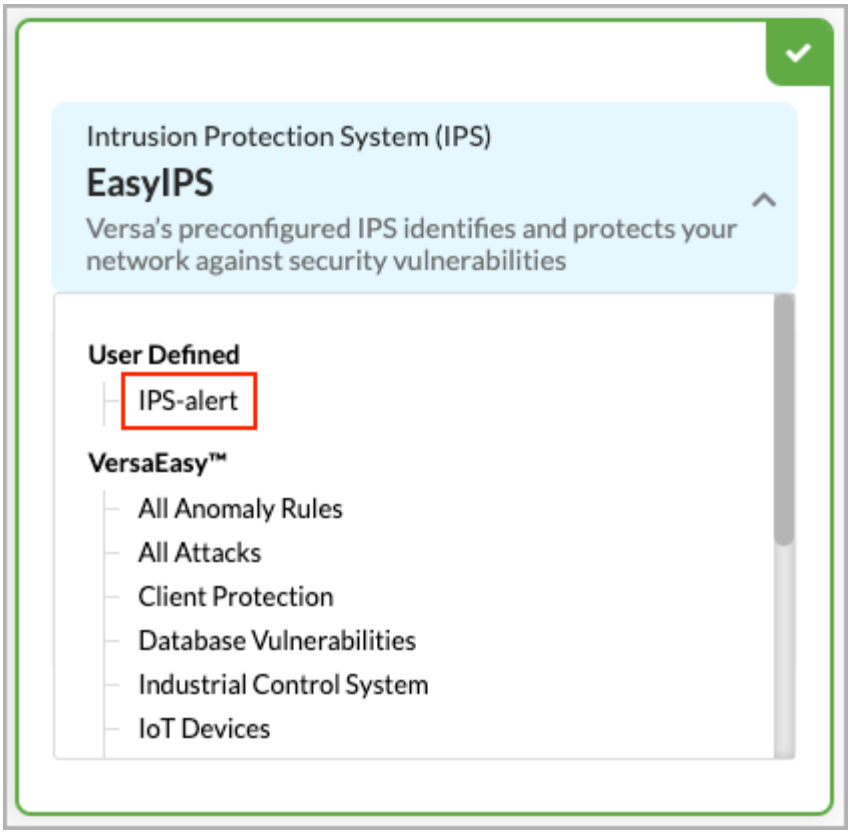


2. Click the + Add icon. The Create Internet Protection Rule screen displays.
3. Select Step 6, Security Enforcement.

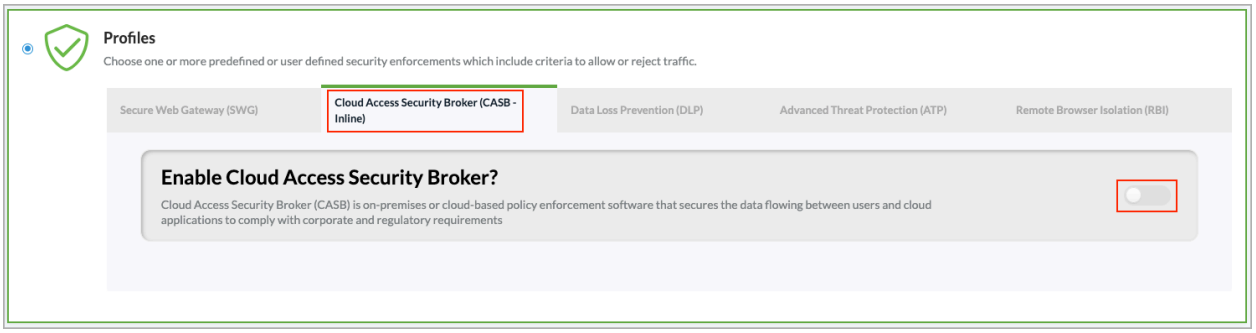
   Note: This example shows only the steps needed to configure the security enforcement for an internet protection rule. For complete information about configuring internet protection rules, see Configure SASE Internet Protection Rules.



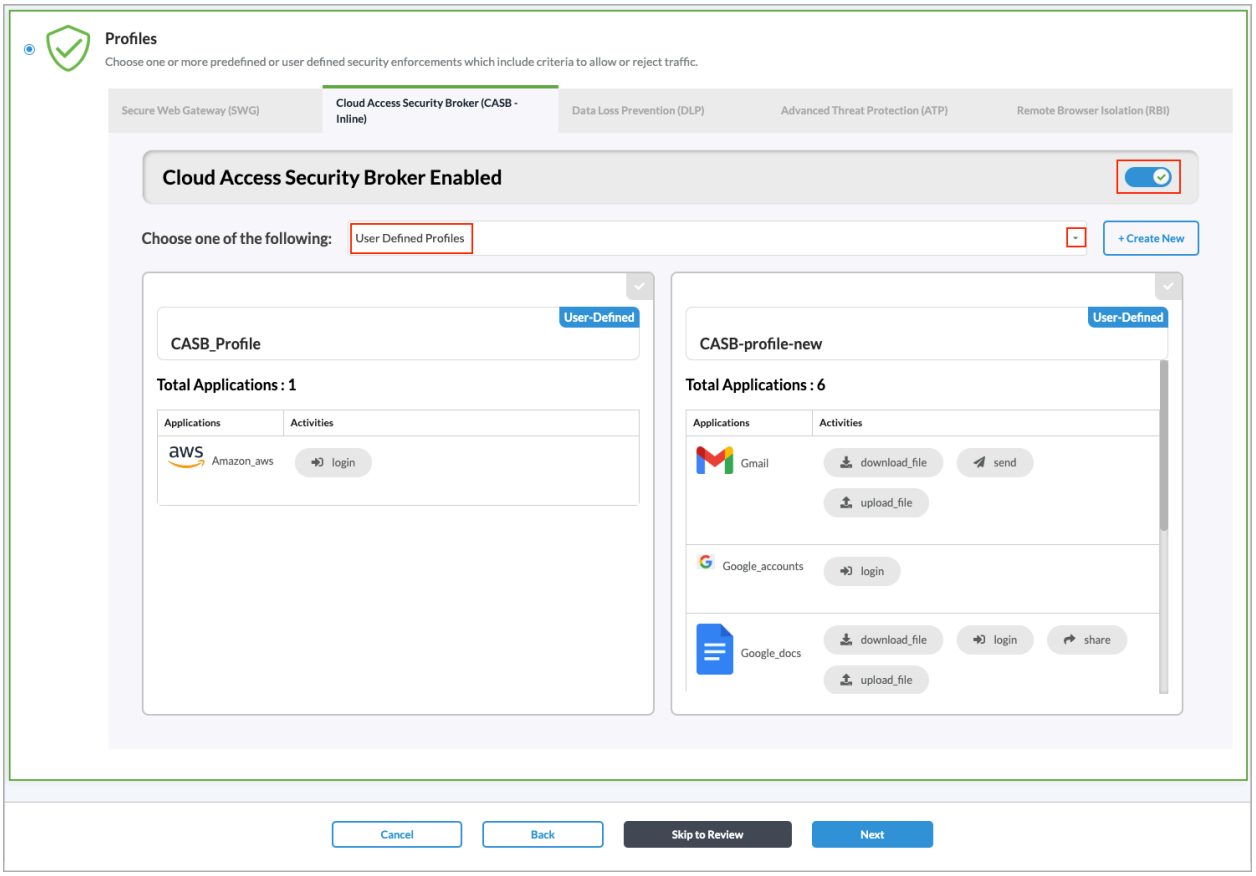
4. Select the Profiles section of the Security Enforcement screen, then select the Secure Web Gateway (SWG) tab and the Intrusion Protection System (IPS) panel. The Easy IPS profile is selected by default.
5. Click the down arrow in the IPS panel to display all available IPS profiles.



6. Select the user-defined profile you created. In this example, the profile is named IPS-alert.
7. Next, select the Cloud Access Security Broker (CASB-inline) tab in the Profiles section.



8. Click the slider to enable CASB.



9. In the field labeled "Choose one of the following," select User Defined Profiles.
10. Select one of the user-defined CASB profiles that are displayed.
11. Complete creating the profile as shown in Configure SASE Internet Protection Rules.

Supported Software Information

Releases 11.2.1 and later support all content described in this article, except:

- Release 12.1.1 adds support for constraint profiles; CASB profiles support CASB rules; IPS-based CASB.

Additional Information

Configure Offline CASB Profiles
Configure SASE Private Application Protection Rules
Configure SASE Internet Protection Rules
Configure SASE Secure Client Access Rules
Configure SASE User-Defined Objects