Configure Remote Browser Isolation

Remote browser isolation (RBI) is a cloud-based solution that provides zero-trust access to browser-based applications. Remote browser isolation works in conjunction with the secure web gateway (SWG) and Versa Operating System™ (VOS™) cloud-based security features, including malware sandboxing, antivirus, and data loss prevention (DLP), to provide an additional line of defense against zero-day, browser-based attacks.

With remote browser isolation, browsing sessions are executed in remote sandboxed browser containers so that the browsing activity is air-gapped from the client browser and network. Active and harmful content from the website is filtered, and only a safe representation is sent to the client browser. This design restricts the attack surface and prevents malware from breaching the client network, providing protection against zero-day malware. Even if malware infects the remote browser, the sandboxed, unprivileged environment limits the damage. The remote browser session is torn down at the end of the browsing session, preventing the malware from persisting.

You can also configure remote browser isolation to prevent exfiltration of sensitive data and credential theft by either disabling file uploads and form POST activity, or rendering the website in read-only mode.

To enable remote browser isolation, clients must access the the internet through the secure web gateway. You configure security policy rules on the secure web gateway to inspect web traffic. You can redirect sessions of interest, for example, suspicious or unknown URL categories, to the browser isolation service. The browser isolation profiles you configure on the secure web gateways determine the settings to apply to the remote browsing sessions. For example, you can render suspicious websites in read-only mode, or you can create a profile in which file uploads and form POSTs are blocked, and downloads are allowed to be previewed only.

To configure remote browser isolation, you do the following:

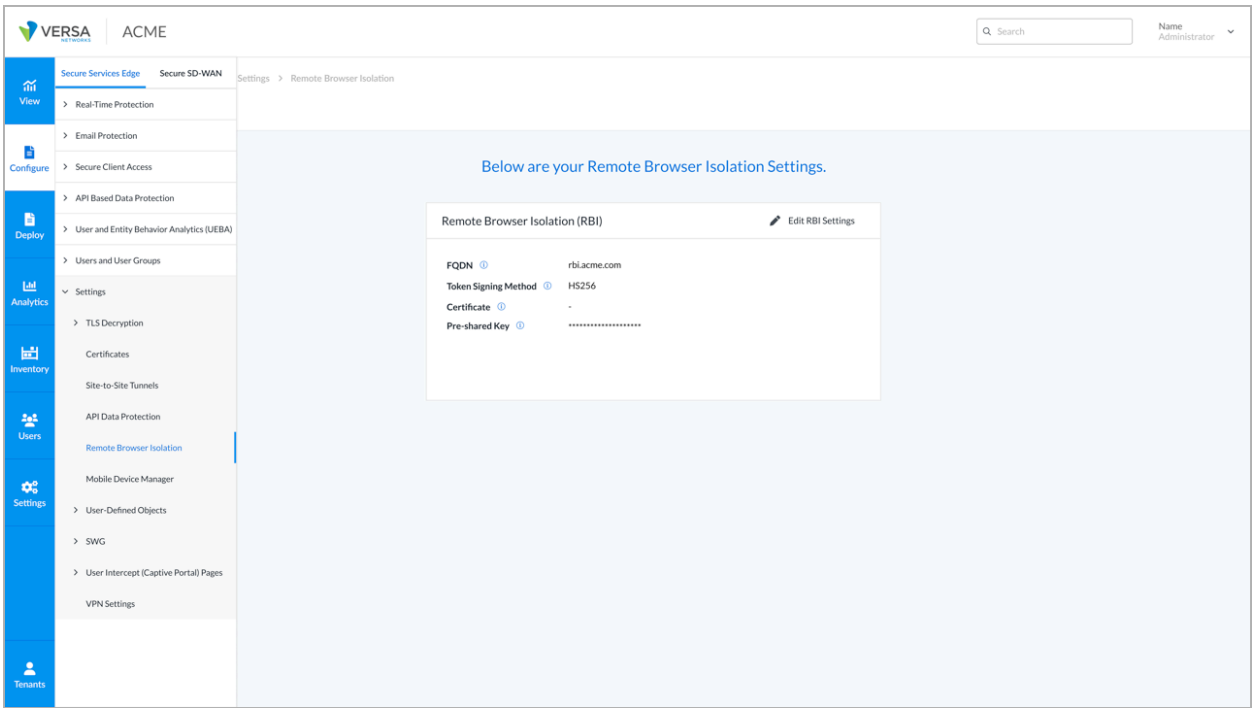
1. Configure the remote browser isolation service location.
2. Configure remote browser isolation profiles.
3. Apply a remote browser isolation profile to an internet protection rule to divert matching sessions to the remote browser isolation service.

Configure the Remote Browser Isolation Service Location

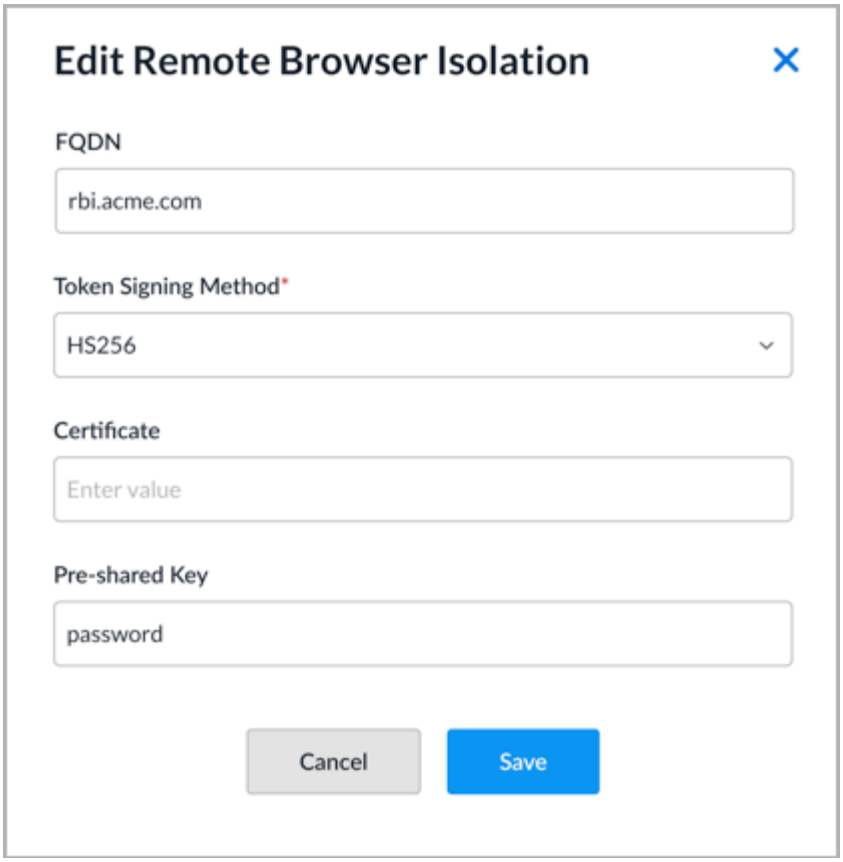
To specify the location to which to redirect sessions that are to be isolated, you configure the location of the remote browser isolation service.

To view and change the remote browser isolation service location:

1. Configure remote browser isolation cluster information for the organization.



2. Enter information for the following fields.



Field	Description
FQDN	Enter the DNS name of the cluster in which the remote browsing sessions are executed.
Token-Signing Method (Required)	Select the method to use to sign the authentication token included in each remote browsing request: ◦ EC256—Certificate-based token signing key ◦ HS256—Preshared key
Certificate	If the token-signing method is EC256, enter the certificate and private key.
Preshared Key (Required)	If the token-signing method is H@256, enter the preshared token-signing key.

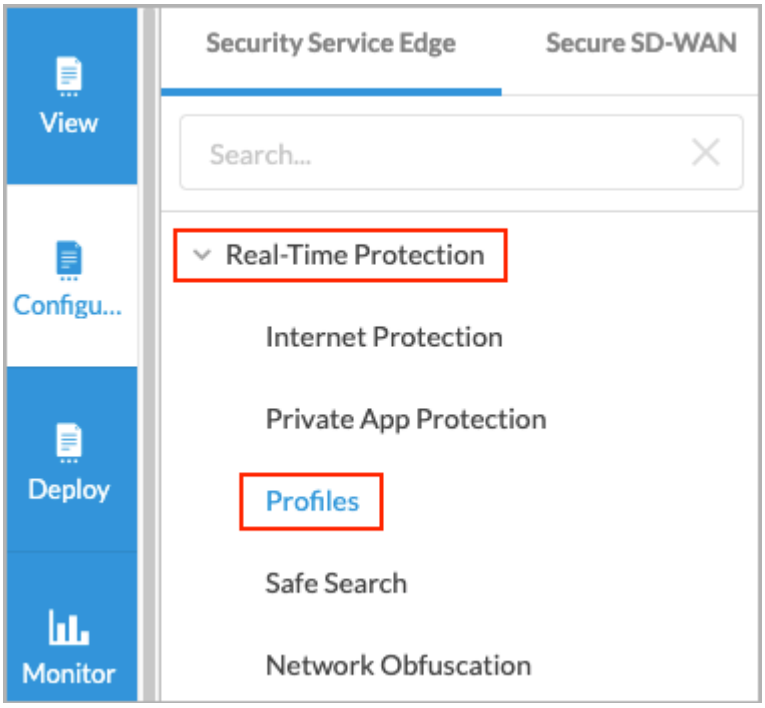
To receive the URL to specify the location to which sessions that are to be isolated are redirected, isolate.versanow.net, contact Versa Networks.

Configure Remote Browser Isolation Profiles

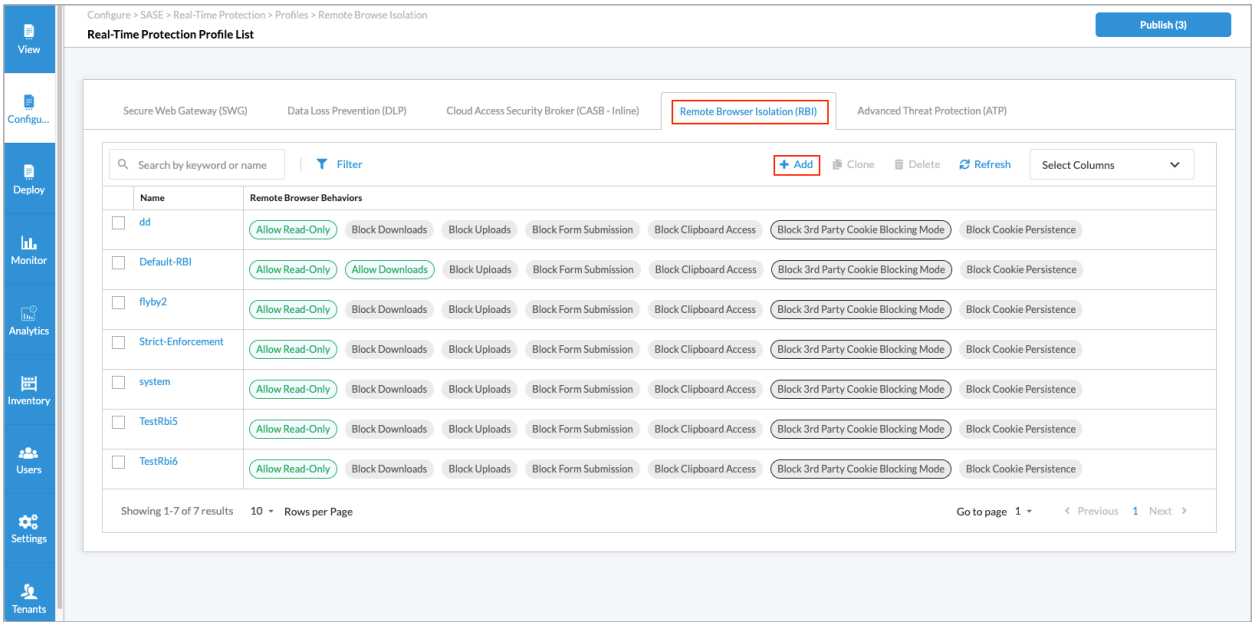
You configure a remote browser isolation profile to define the settings to apply to isolated browsing sessions.

To configure a remote browser isolation profile:

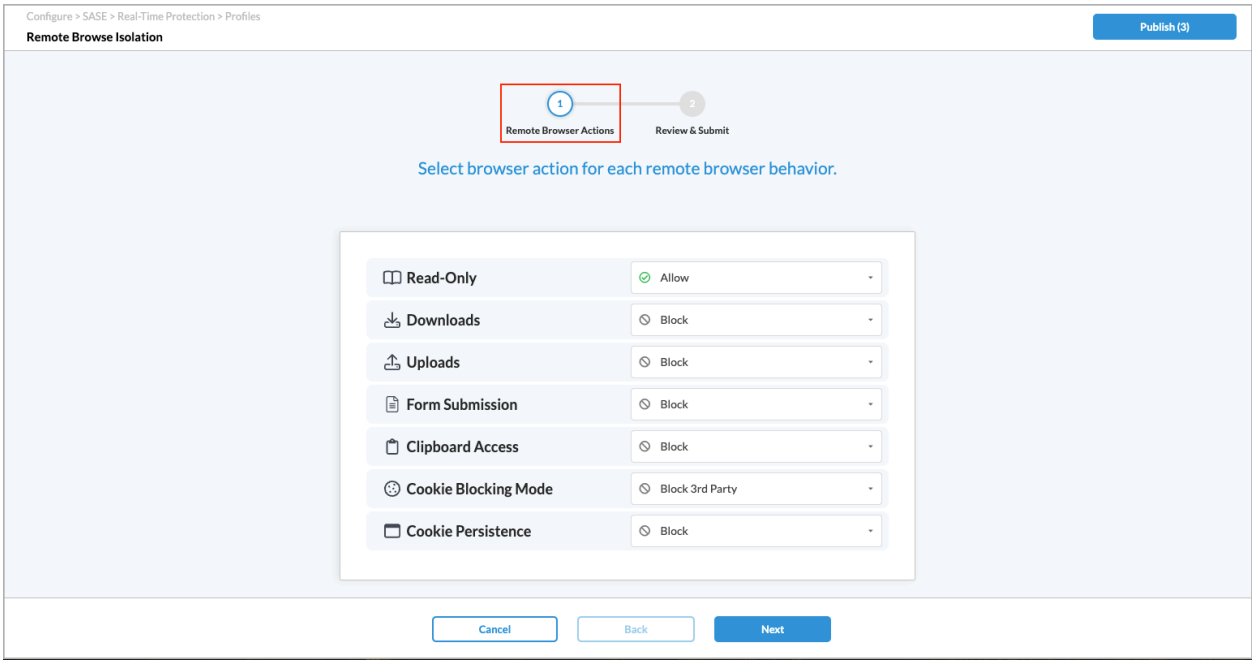
1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



2. Select the Remote Browser Isolation (RBI) tab, and then click + Add.



3. In the Remote Browser Isolation screen, select the remote browser behavior actions.

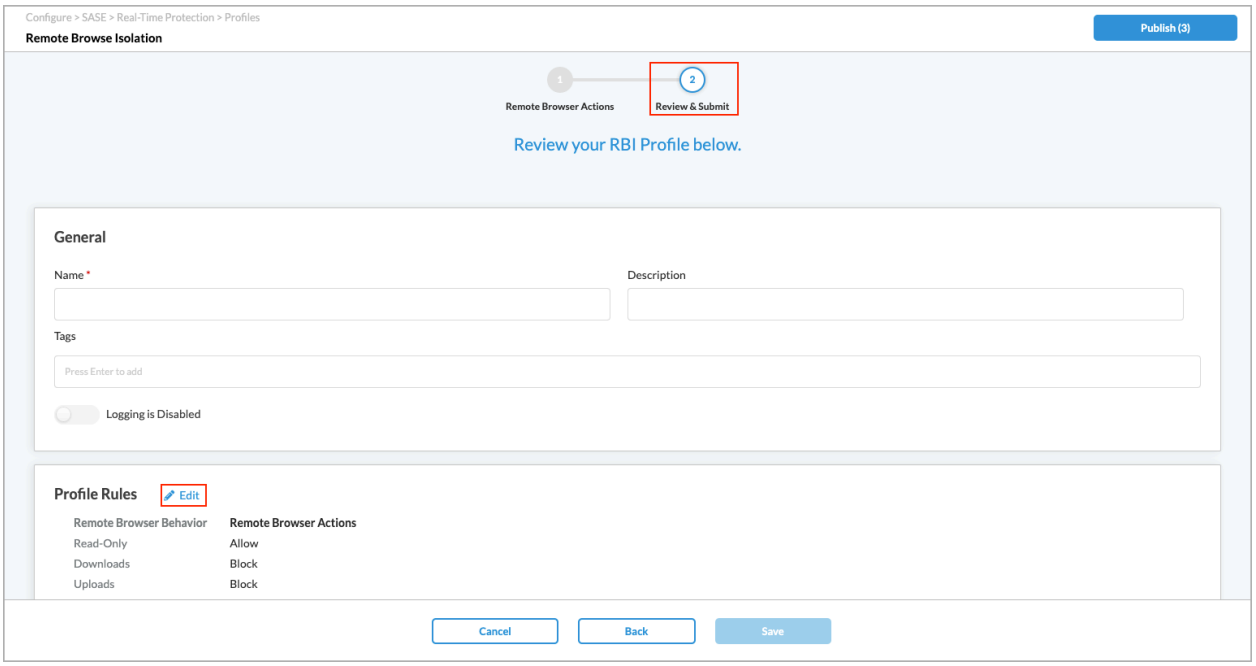


Field	Description
Read Only	Render the website in read-only mode, and prevent the user from interacting with the website. The user cannot upload or download files, fill and submit HTML

Field	Description
	forms, or perform other actions on the website. When you enable read-only mode, all other settings in the RBI profile are ignored. *Default:* Allow
Downloads	Select the behavior for file downloads: ◦ Allow—Allow file downloads to the client browser. If you allow file download, Versa's malware sandboxing software scans the files to ensure that they are clean. ◦ Block—Block file downloads. ◦ Preview—Files cannot be downloaded to the client browser. The user can preview in PDF format any files that can be converted to PDF, such as Office 365 and Google documents. If you allow file preview, Versa's malware sandboxing software scans the files to ensure that they are clean. *Default:* Block
Uploads	Select the behavior for file uploads: ◦ Allow—Allow file uploads. If you allow file upload, Versa DLP service scans the files to enforce DLP policies. ◦ Block—Block file uploads. *Default:* Block
Form Submission	Select the behavior for form submission: ◦ Allow—Allow submission of HTML forms. ◦ Block—Users cannot fill in and submit HTML forms. *Default:* Block
Clipboard Access	Select whether the user is allowed to copy content from the browser to the system clipboard or from the

Field	Description
	system clipboard to the browser: ◦ Allow—Allow clipboard access. ◦ Block—Deny clipboard access.
Cookie Blocking Mode	Select whether the user's cookies persist across browsing sessions. If cookies are allowed to persist, website settings, such as user preferences and shopping cart contents, are restored when the user visits the website again. ◦ Allow—Cookies persist. ◦ Block—Cookies do not persist. ◦ Block Third-Party Cookies—Allow first-party cookies, and block third-party cookies. *Default:* Block Third-Party Cookies
Cookie Persistence	Select the cookie-blocking setting: ◦ Allow—Allow first-party cookies (cookies that belong to the website that the user is remote browsing), and allow third-party cookies (cookies belong to different websites or domains). ◦ Block—Block all cookies. *Default:* Block

4. Click Next.
5. In the Review and Submit screen, click Submit.

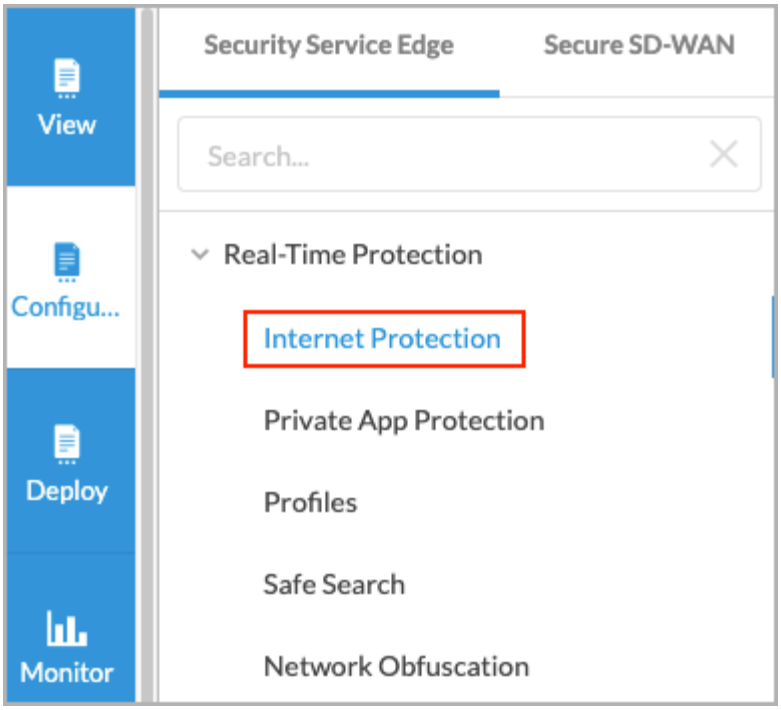


Associate a Remote Browser Isolation Profile with a Security Internet Protection Rule

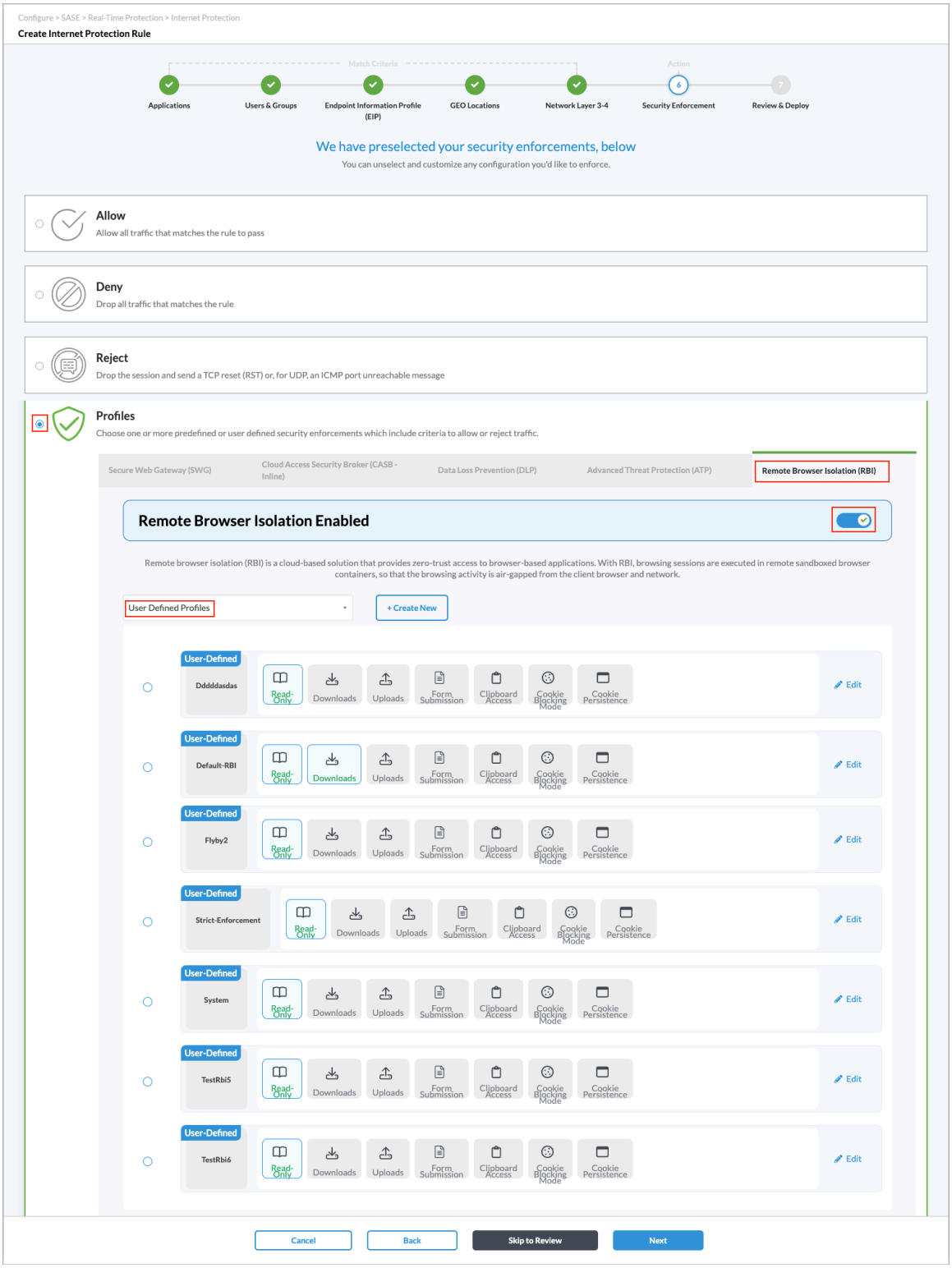
To enforce remote browser isolation, you create one or more internet protection rules with the required match conditions and associate the RBI profile with the rule.

To associate a remote browser isolation 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 Remote Browser Isolation (RBI) tab.
5. Click the slider bar to enable Remote Browser Isolation.

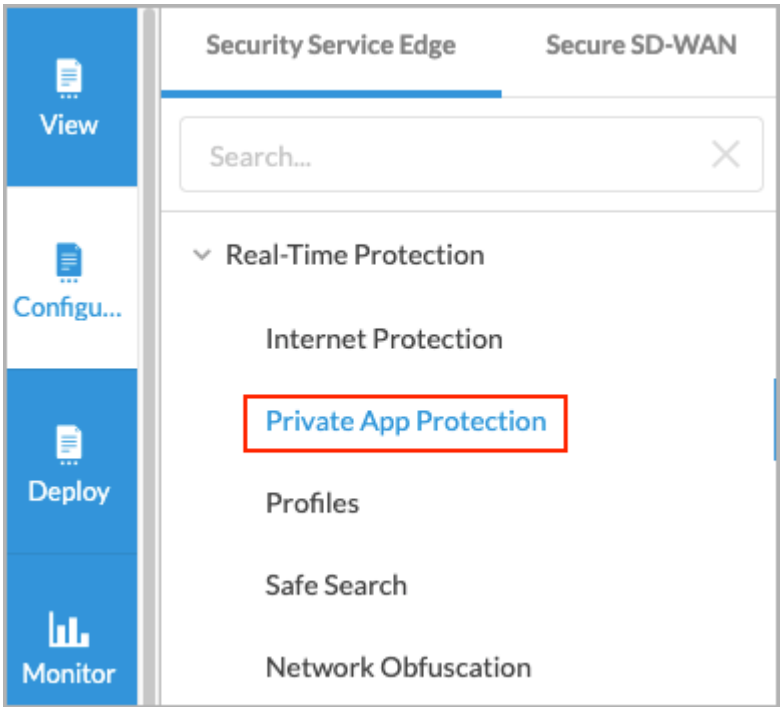
6. Select User Defined or Predefined.
7. Click a profile to associate the profile with the rule.
8. Click Next.
9. In the Review & Deploy, review your selections, and make any needed updates.
10. Click Save.

Associate a Remote Browser Isolation Profile with a Security Private Application Protection Rule

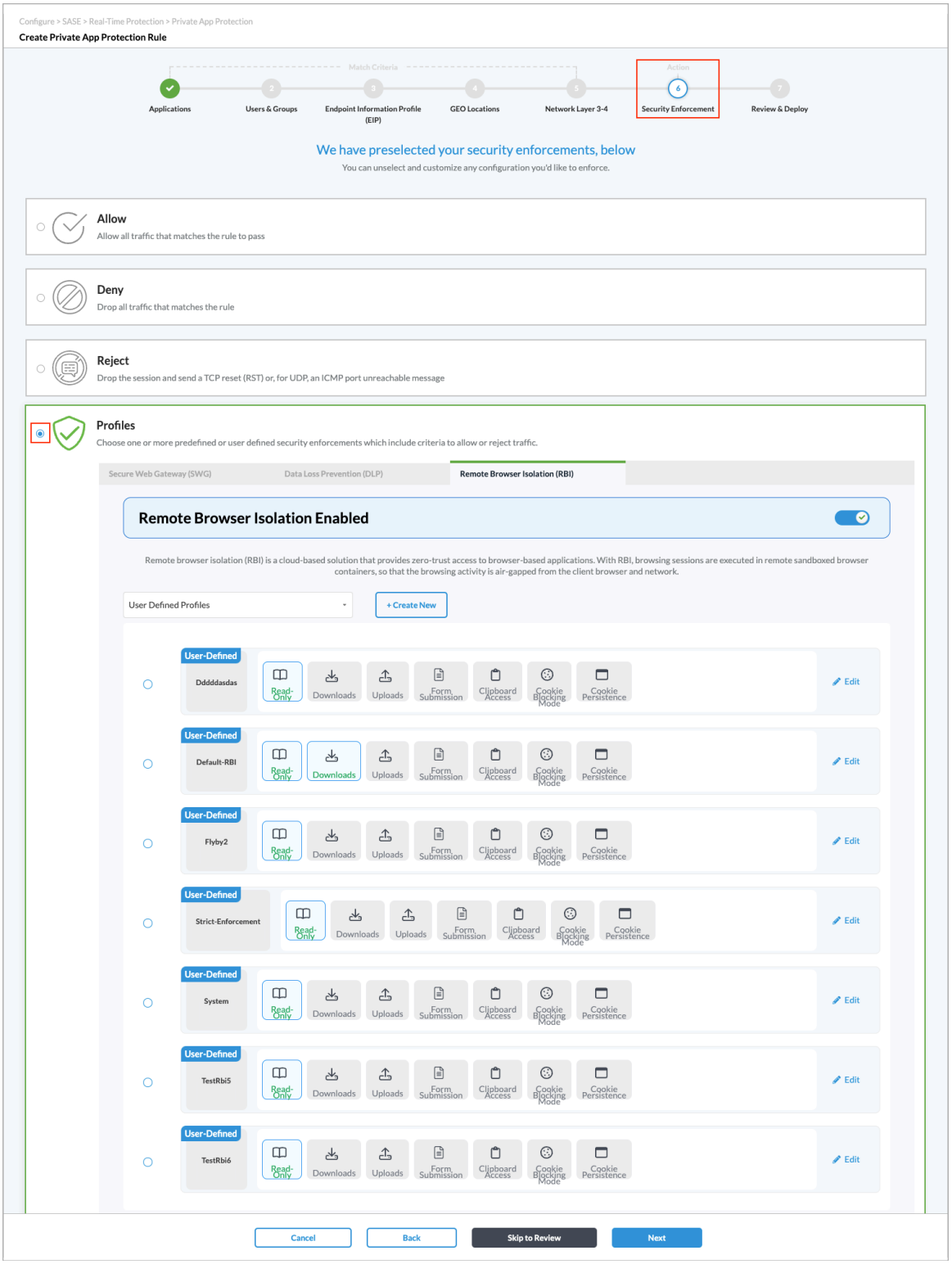
To enforce remote browser isolation, you create one or more private application protection rules with the required match conditions and associate the RBI profile with the rule.

To associate a remote browser isolation profile with a private application protection rule:

1. Go to Configure > Real-Time Protection > Private Application Protection.



2. In the Private Application Protection Rules List screen, click + Add to create a rule. The Create Private Application Protection Rule screen displays.
3. Select the Security Enforcement screen, and then select Profiles.



4. Select the Remote Browser Isolation (RBI) tab.
5. Click the slider bar to enable Remote Browser Isolation.

6. Select User Defined or Predefined.
7. Click a profile to associate the profile with the rule.
8. Click Next.
9. In the Review & Deploy, review your selections and make any needed updates.
10. Click Save.

Additional Information

Configure SASE Internet Protection Rules