



Remote Browser Isolation

5.5

Getting Started Guide

© 2022 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.

All other trademarks used in this document are the property of their respective owners.

Published 06 January 2022

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

1 Introduction	5
Licensing	6
Help and support	6
2 Initial setup	7
Before you begin	7
Configuring the redirect to the remote browser	9
3 The Forcepoint RBI Admin Portal	17
Changing your password	18
4 Dashboard	19
Common navigation elements	19
Viewing system details	21
Viewing web security details	22
Viewing network details	26
6 Policy	27
Profiles	28
Settings	32
7 Reports	35
Create a Downloads report	35
Create an Uploads report	36
Create a Browse Activity report	37
8 Integrations	39
Create a new SIEM integration	39
Edit a SIEM profile	41
Delete a SIEM profile	41
9 Product updates	43
What's new?	43
Known and resolved issues	43

Chapter 1

Introduction

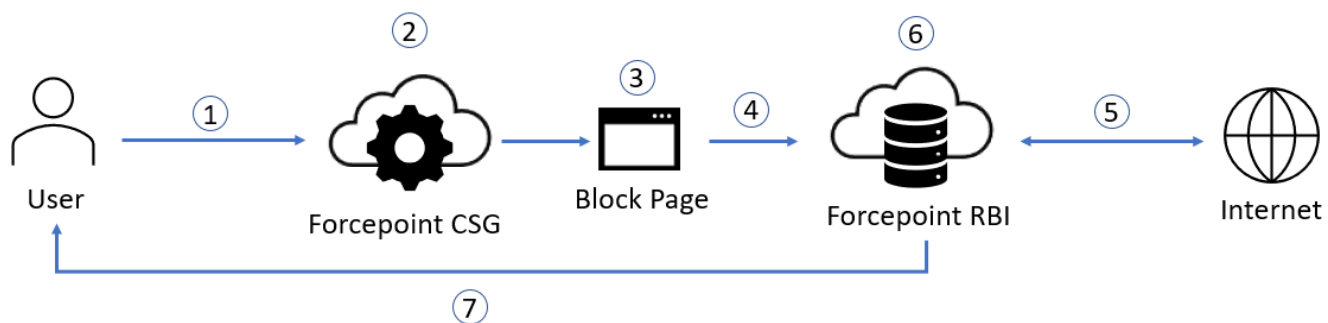
Contents

- [Licensing](#) on page 6
- [Help and support](#) on page 6

Forcepoint Remote Browser Isolation (Forcepoint RBI) neutralizes security threats through browser isolation, preventing attacks before they occur. By transforming all internet content into harmless pixel streams delivered to the endpoint in a seamless user experience, Forcepoint RBI creates a zero trust environment that eliminates most infections and compromises.

Forcepoint RBI works by transferring user requests from the local browser to a remote disposable browser. Internet browsing is a major threat carrier that can send unchecked active malicious codes to a user's endpoint. Forcepoint RBI prevents these threats from the endpoint by performing fetch, execute, and render functions remotely. Forcepoint RBI transforms all the active codes and contents into a visual stream of harmless pixels thereby ensuring a seamless user experience with secure browsing without any security vulnerabilities.

With Forcepoint RBI, active code is never sent to the protected endpoints. All web-based instructions are run in an isolated, purposely built virtual machine where they are transformed into harmless pixels containing no computer code that could attack the protected endpoints.



- 1 The user submits an HTML request using a standard HTML 5 compatible web browser.
- 2 Forcepoint Cloud Security Gateway checks to see if the requesting webpage is blocked by the active web policy.
- 3 If the webpage request is blocked, Forcepoint Cloud Security Gateway shows a block page to the user instead of the requested webpage. The user clicks a button on the block page to view the requested webpage. If the block page is configured to automatically redirect the page to the remote browser, then the workflow skips to step 5.
- 4 The request is sent to Forcepoint RBI.
- 5 Forcepoint RBI executes the web request to the selected webpage in a remote isolated container.
- 6 Forcepoint RBI transforms all code and content into safe pixel streams.
- 7 Forcepoint RBI returns safe pixel streams to the user ensuring a safe browsing experience that is isolated from a web attack.

Licensing

Customers require licenses for both Forcepoint Cloud Security Gateway and Forcepoint Remote Browser Isolation to configure remote browser isolation.

A Forcepoint RBI license can be purchased as an add-on to either Forcepoint Cloud Security Gateway or Forcepoint Web Security Cloud. You can select either **Forcepoint Cloud RBI Selective**, **Forcepoint Cloud RBI Full**, or a combination of both.

- **Forcepoint Cloud RBI Selective:** This license permits 10% of your licensed users to access the Forcepoint RBI remote browser concurrently. This is the most common solution, where you forward uncategorized URLs to Forcepoint RBI.



Note

If users are browsing through the remote browser anonymously, then the number of sessions represents the number of concurrent users.

- **Forcepoint Cloud RBI Full:** This license permits 100% of your licensed users to access the Forcepoint RBI remote browser concurrently. You can choose to redirect all web traffic to Forcepoint RBI for a specific user group, such as a high risk department that requires a higher level of monitoring.

After you order your licenses, Forcepoint sends a fulfillment email that contains the information needed to access the product, including your Tenant ID, access URL, primary administrator credentials, license key, and license expiration date.

Help and support

Access Forcepoint help and support services for assistance and troubleshooting.

Use the [Forcepoint support website](#) to search the knowledge base and product documentation library.

A series of quick training guides, or Hack Stacks, demonstrating how to perform common tasks is available at the Forcepoint Cyber Institute. To view the Hack Stacks, go to:

<https://learn.forcepoint.com/learn/course/forcepoint-remote-browser-isolation/forcepoint-remote-browser-isolation/dashboard>

If you encounter issues with your deployment, raise a case via [Forcepoint Technical Support](#).

Chapter 2

Initial setup

Contents

- [Before you begin](#) on page 7
- [Configuring the redirect to the remote browser](#) on page 9

Forcepoint Cloud Security Gateway can be configured to send websites to Forcepoint RBI through a block page to protect against known and unknown malware.

To send users to the remote browser, configure the block page in Forcepoint Cloud Security Gateway. You can either create a custom block page to give users the option to open the remote browser or create a custom block page to automatically redirect the users to the remote browser.

General workflow:

- 1) Configure the block page to redirect the user to Forcepoint RBI. There are two options:
 - Create a custom block page with a button to open the remote browser: With this option, you create a custom block page with a button that redirects the user's browser to the remote browser. The user must click the redirect button to access the remote browser.
 - Create a custom auto-redirect block page: With this option, you create a custom block page that automatically redirects the user's browser to the remote browser. The user does not need to click a button to redirect.
- 2) Add the block page to the specific web categories within the user's policy on Forcepoint Cloud Security Gateway.
- 3) After the policy is configured in Forcepoint Cloud Security Gateway, the initial setup is complete. To configure Forcepoint RBI, open the Forcepoint RBI Admin Portal.

Before you begin

Before you configure remote browser isolation, review the following requirements.

- Verify that you can connect to the Internet.
- Verify that you have administrator credentials on both Forcepoint Cloud Security Gateway and Forcepoint RBI. If you do not have administrator credentials, contact Forcepoint Support.
- Verify that the credentials work. Sign in to Forcepoint Cloud Security Gateway and Forcepoint RBI successfully before continuing. If you cannot access the product using your administrator credentials, contact Forcepoint Support.



Note

When the primary administrator account (provided in the fulfillment email) signs in to the Forcepoint RBI Admin Portal for the first time, the administrator needs to accept the end user license agreement (EULA) and enter the license key provided in your fulfillment email.

- Add the top-level domain for Forcepoint RBI to the bypass list in Forcepoint Cloud Security Gateway.

System requirements for endpoints

Your endpoints must meet minimum system requirements to work with Forcepoint RBI.

System Requirements

Description	Specification
Processor	Intel i3 2.5GHz or better
RAM	4 GB
Free Disk Space	25 MB

Supported Operating Systems

Operating system	Supported versions
Microsoft Windows	Windows 10
Apple macOS	macOS 10.7 or later

Forcepoint RBI supports all HTML5 compatible web browsers, including Chrome, Edge, Firefox, and Safari.

Configuration for endpoints

Configure the following settings on your endpoints. Your endpoints cannot connect to Forcepoint RBI unless these settings are configured correctly.

- Open the following ports on your endpoints to allow Forcepoint RBI through your firewall:
 - <mycompany>.rbi.forcepoint.com: HTTPS port 443



Note

<mycompany> is your company name as defined in Forcepoint RBI. This information is available in your fulfillment email and the Forcepoint RBI Admin Portal.

- *.rbi.forcepoint.com: TCP port range 30000-32767
- Enable 3rd party cookies on your endpoints. Forcepoint RBI uses cookies to identify the user and set up sessions on the browser.
All browsers using Forcepoint RBI must be configured to allow cookies for `[*.]rbi.forcepoint.com`.



Note

There is a similar, optional setting in the Forcepoint RBI Admin Portal to save cookies on the remote browser for external websites accessed through Forcepoint RBI. The setting on the Admin Portal does not enable 3rd party cookies on your endpoints.

Configuring the redirect to the remote browser

There are two ways to isolate a user's web activity: by clicking a link to the remote browser from a block page or by automatically sending the user to the remote browser.

Create a custom redirect block page

If you want your users to see a block page and click a link to open the remote browser, then create a new custom block page in Forcepoint Cloud Security Gateway.

For more information about block pages, see the *Forcepoint Cloud Security Gateway Help* on the [Forcepoint support website](#).

Steps

- 1) Sign in to Forcepoint Cloud Security Gateway.
- 2) Go to **Web > Policy Management > Block & Notification Pages**.
- 3) Click **New Page**.
- 4) On the **New custom page** screen, enter a **Name** and **Description**.
- 5) Click **Save**.

- 6) Click **HTML Editing**, then click **Continue** on the dialog box.

Web > Block & Notification Pages > Page Details

Blocked - Redirect to Forcepoint RBI

Name: Blocked - Redirect to Forcepoint RBI

Description: Custom block page to redirect the user to Forcepoint RBI. Users click a "View in Remote Browser" button to open the remote browser.

[Edit](#)

[Add Language](#)

English (Default) Version

Make basic text and image changes to the page. For more customization options, use HTML editing.

[Variables/tokens](#) [Basic Editing](#) [Preview](#)

```
</div>
<div class="row lastName">
  <div class="span1 name">Reason</div>
  <div class="span7 explanation wrapURL">_REASON_ </div>
</div>
<div class="row">
  <div class="span5 ">By clicking this button, you agree to open this web page in a third-party remote browser.</div>
  <div class="span3 "><a class="linkAsButton" href="https://<mycompany>.rbi.forcepoint.com/viewer/loader?tenantId=
<my_tenant_id>&url=_URL_[uriescape]&username=_USERNAME_[uriescape]" >View in Remote Browser</a></div>
</div>
<div class="row">
  <div class="span8 explanation">For more information, see your organization's policy on acceptable use of the Internet.
</div>
</div>
</div></div>
<div class="" id="footerRow" >
  <div id="footer" class="">
    
```

- 7) Delete any default HTML code already in the field.

8) Paste the following HTML content:

```

<!DOCTYPE html public "-//W3C//DTD HTML 4.0 Transitional//en" "http://www.w3.org/TR/html4/
loose.dtd">
  _TEMPLATE_BLOCK_PAGE_HTML_TAG_
  <head>
    <meta charset="utf-8"/>
    <base href="_PROTOCOL_://_PORTAL_HOST_NAME_">
    _TEMPLATE_BLOCK_PAGE_META_VIEWPOINT_
    _TEMPLATE_BLOCK_PAGE_HEAD_JS_
    <link rel="stylesheet" href="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
bootstrap/css/bootstrap.css" type="text/css">
    <link rel="stylesheet" href="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
bootstrap/css/bootstrap-responsive.css" type="text/css">
    <link rel="stylesheet" href="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
notification-pages/notification.css" type="text/css">
    <!--[if IE ]>
      <link rel="stylesheet" href="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
notification-pages/notification-ie.css" type="text/css">
      <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/head.js"></script>
    <![endif]-->
    <!--[if IE 6]>
      <link rel="stylesheet" href="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
bootstrap/css/bootstrap-ie6.min.css" type="text/css">
      <link rel="stylesheet" href="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
bootstrap/css/ie.css" type="text/css">
      <link rel="stylesheet" href="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
notification-pages/notification-ie6.css" type="text/css">

      <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/notification-pages/
jquery-1.4.2.min.js"></script>
      <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
ie6_joined_classes.js"></script>
      <script>
        var IEPNGFix = window.IEPNGFix || {};
        IEPNGFix.blankImg = "_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/iepngfix/
blank.gif";
      </script>
      <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/iepngfix/
jquery.iepngfix.js"></script>
    <![endif]-->
    <style id="zzNOTIFICATION_CUSTOM_CSSxxCSSzz"></style>
    <title id="zzNOTIFICATION_HTML_TITLExxPAGE_TITLEzz">Blocked - View in Remote
Browser</title>
  </head>
  <body class="loading" id="_PAGE_INNER_ID">
    <div class="container" id="container">
      <div class="row">
        <div class="span10 offset1" id="notify">
          <div class="notify-title-box">
            
            <span id="notify-title" class="editable text
zzNOTIFICATION_TITLExxTEXTzz">Blocked - View in Remote Browser</span>
            <div id="titleBlink"></div>
          </div>
          <div class="notify-box">
            <div id="notify-content" class="editable block
zzNOTIFICATION_CONTENTxxBLOCKzz"><div class="row">
              <div class="span8 explanation">The Web site you requested is blocked by your
organization.</div>
            </div>
            <div class="row firstName">
              <div class="span1 name">URL</div>
              <div class="span7 explanation">_URL_</div>
            </div>
            <div class="row lastName">
              <div class="span1 name">Reason</div>
              <div class="span7 explanation wrapURL">_REASON_</div>
            </div>
            <div class="row">
              <div class="span5 ">By clicking this button, you agree to open this web page in a third-
party remote browser.</div>
              <div class="span3 "><a class="linkAsButton" href="https://<mycompany>.rbi.forcepoint.com/
viewer/loader?tenantId=<my_tenant_id>&url=_URL_[uriescape]&username=_USERNAME_[uriescape]"
>View in Remote Browser</a></div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </body>
</html>

```

- 9) Go to the following line that contains the redirect URL:

```
<div class="span3 "><a class="linkAsButton" href="https://<mycompany>.rbi.forcepoint.com/viewer/loader?tenantId=<my_tenant_id>&url=_URL_[urunescape]&username=_USERNAME_[urunescape]">View in Remote Browser</a></div>
```

- 10) Update the following information in the URL:

- `<mycompany>`: Required. This information can be found in your fulfillment email and in the Forcepoint RBI Admin Portal.
- `<my_tenant_id>`: Required. This information can be found in your fulfillment email and in the Forcepoint RBI Admin Portal.
- `&username=_USERNAME_[urunescape]`: Optional. If the username information is removed from the URL, then the username is not recorded in Forcepoint RBI metrics and reports.

- 11) Optionally, edit the block page text as needed for your organization.

- 12) Click **Preview** to open the block page in a browser window and review the changes. Update as necessary.

- 13) Click **Save**.

Next steps

After you edit the block page, you need to assign this custom block page to the categories in the policy.

Related tasks

Add the custom block page to a policy on page 14

Create a custom auto-redirect block page

If your users do not need to see the block page, create a custom block page to send the web requests to browser isolation automatically.

For more information about block pages, see the *Forcepoint Cloud Security Gateway Help* on the [Forcepoint support website](#).

Steps

- 1) Sign in to Forcepoint Cloud Security Gateway.
- 2) Go to **Web > Policy Management > Block & Notification Pages**.
- 3) Click **New Page**.
- 4) On the **New custom page** screen, enter a **Name** and **Description**.
- 5) Click **Save**.
- 6) Click **HTML Editing**, then click **Continue** on the dialog box.

- 7) Delete any default HTML code already in the field.
- 8) Paste the following HTML content:

```
<DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Refresh" content="0; url=https://<mycompany>.rbi.forcepoint.com/viewer/
loader?tenantId=<my_tenant_id>&url=_URL_[uriescape]&username=_USERNAME_[uriescape]
"/>
  </head>
</html>
```

Web > Block & Notification Pages > Page Details

Blocked - Custom Auto Redirect to Forcepoint RBI

Name: Blocked - Custom Auto Redirect to Forcepoint RBI
Description: Custom block page to automatically redirect the user to Forcepoint RBI.

[Edit](#)

[Add Language](#)

English (Default) Version

Make basic text and image changes to the page. For more customization options, use HTML editing.

[Variables/tokens](#) [Basic Editing](#) [Preview](#)

```
<DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Refresh" content="0; url=https://<mycompany>.rbi.forcepoint.com/viewer/loader?tenantId=
<my_tenant_id>&url=_URL_[uriescape]&username=_USERNAME_[uriescape]
"/>
  </head>
</html>
```

- 9) Update the company and tenant ID in the URL. The company is shown as `<mycompany>` and the tenant ID is shown as `<my_tenant_id>`. This information is found in your fulfillment email.
- 10) Click **Save**.

Related tasks

Add the custom block page to a policy on page 14

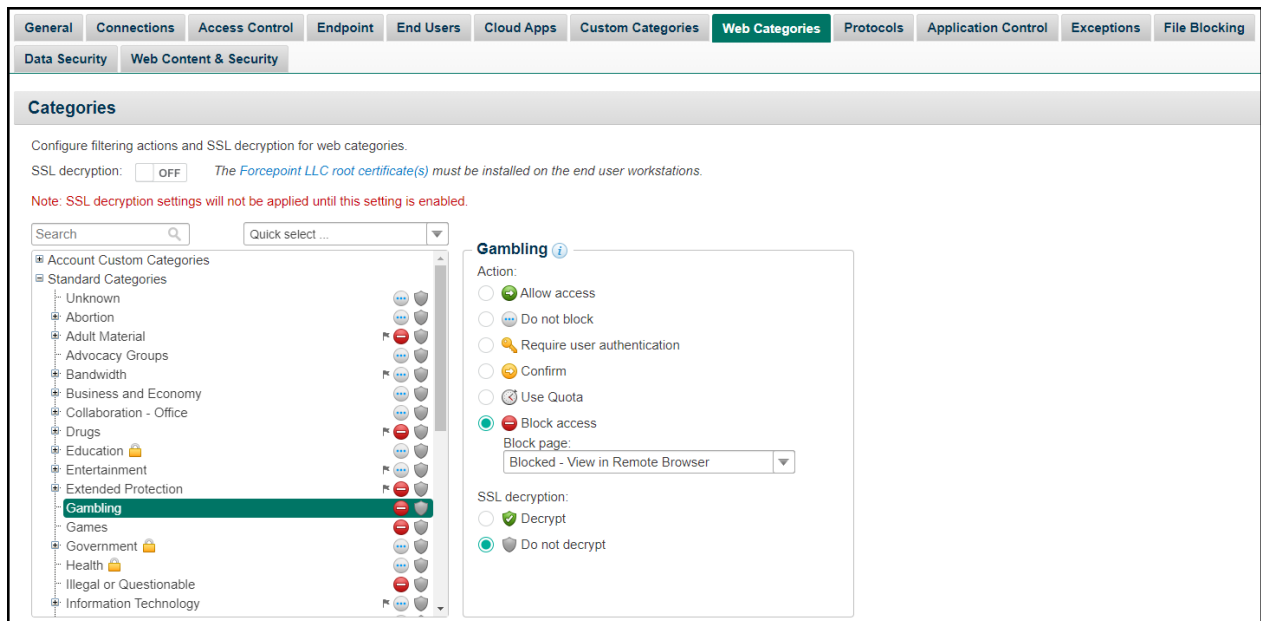
Add the custom block page to a policy

Add the custom block page a policy's web categories. When a user tries to connect to a webpage associated with the web category, the browser opens the custom block page.

For more information about creating or updating a policy, see the *Forcepoint Cloud Security Gateway Help* on the [Forcepoint support website](#).

Steps

- 1) Sign in to Forcepoint Cloud Security Gateway.
- 2) Go to **Web > Policy Management > Policies**.
- 3) Select your policy.
- 4) Click **Web Categories**.
- 5) Select the categories in the left panel, then choose **Block access** from the right pane.
- 6) In the **Block** page drop-down menu, select the custom block page for remote browser isolation.



- 7) Click **Save**.

Related tasks

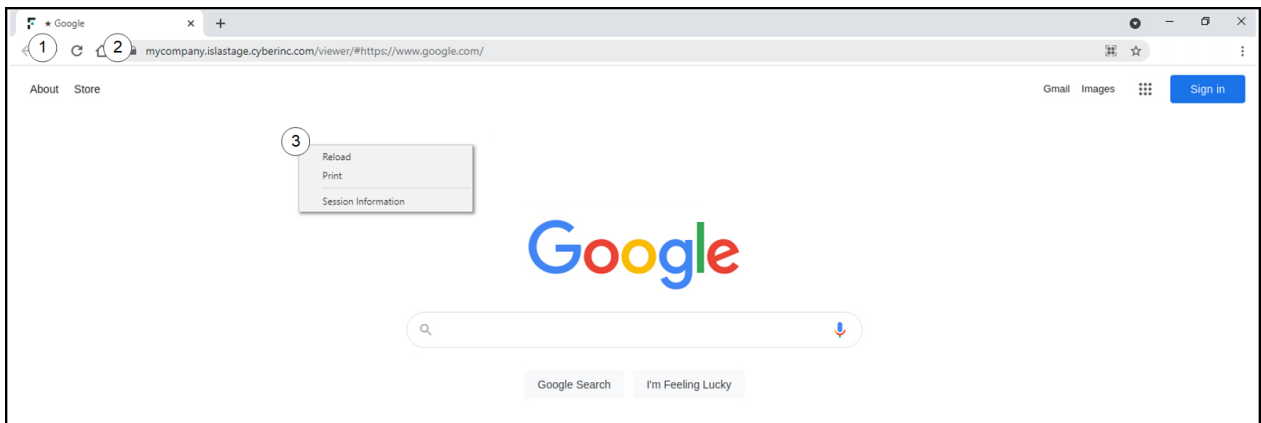
Verify the redirect to Forcepoint Remote Browser Isolation on page 15

Verify the redirect to Forcepoint Remote Browser Isolation

After Forcepoint Cloud Security Gateway redirects the user to Forcepoint RBI, verify that the browser session is isolated.

Steps

- 1) Open an HTML5 compatible browser and go to a webpage that should be blocked per the active policy in Forcepoint Cloud Security Gateway.
- 2) If you configured the default block page, click **View in Remote Browser**. This step is not needed if you created a custom auto-redirect block page.
- 3) Verify that the browser session is going through the remote browser:



- 1 Look for the star. The tab header for the webpage will display a star next to the webpage title.
- 2 Check the URL. The URL will contain the domain for the remote browser. For example, the URL for `https://www.google.com` would appear as `https://<mycompany>.rbi.forcepoint.com/viewer/#https://www.google.com/`.
- 3 Check the right-click menu. The right-click menu will only contain the options for the remote browser: **Reload**, **Print**, and **Session Information**.

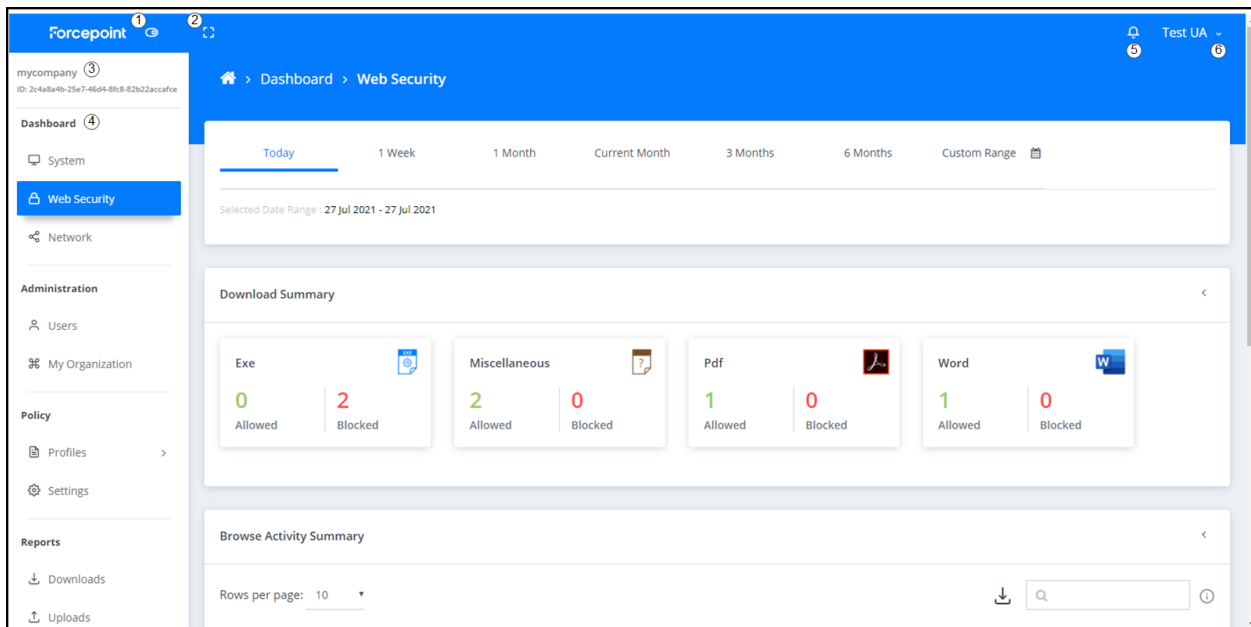
Chapter 3

The Forcepoint RBI Admin Portal

Contents

- [Changing your password](#) on page 18

The Admin Portal provides a cloud-based interface to manage the Forcepoint RBI configuration and view user and browser activities.



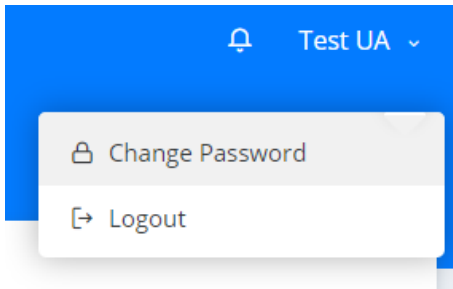
- 1 Hide/Show Menu: Click this button to hide the left navigation menu. Click the button again to open the menu.
- 2 Full Screen: Click this button to open Forcepoint RBI in full screen mode. Click the button again to return to normal size.
- 3 Company information: Shows the name of the organization (as defined by the **Display Name** under **My Organization**) and the Tenant ID created when you purchased Forcepoint RBI.
- 4 Navigation menu: The Admin Portal menu is divided into five sections:
 - **Dashboard:** View information about the users and endpoints connected to Forcepoint Remote Browser Isolation.
 - **Administration:** Configure the users, roles, and organization details.
 - **Policy:** Configure the remote browser isolation policy.
 - **Reports:** Configure and view reports.
 - **Integrations:** Configure integrations with third-party security information and event management (SIEM) solutions.
- 5 Show notifications: Click this button to show recent system notifications.
- 6 User menu: Click the name of the user to open the user menu and either change your password or logout.

Changing your password

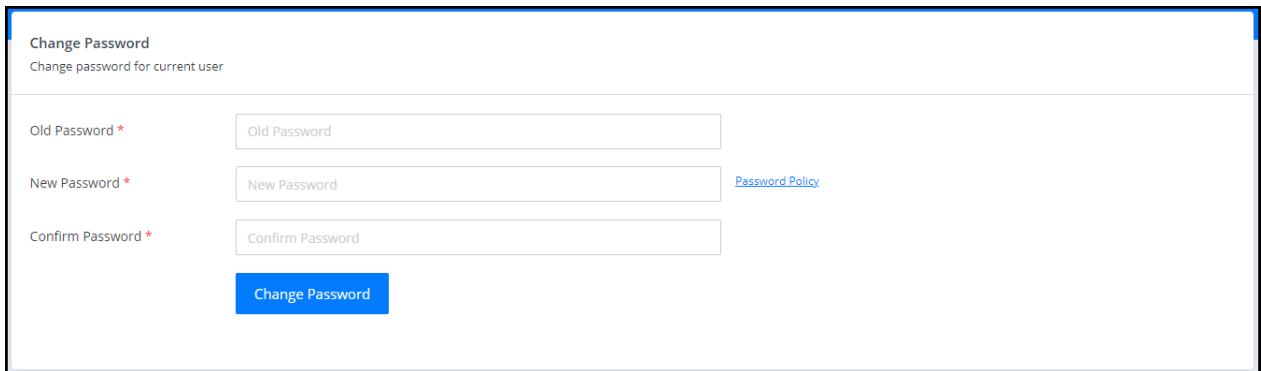
To change your password, open the user menu at the top of the Admin Portal.

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) At the top of the Admin Portal, click the user name to open the user menu.



- 3) Click **Change Password**.
- 4) Enter your current password in the **Old Password** field.
- 5) Enter your new password in the **New Password** field, then enter it a second time in the **Confirm Password** field.

A screenshot of the 'Change Password' form. The title is 'Change Password' with a subtitle 'Change password for current user'. There are three input fields: 'Old Password *', 'New Password *', and 'Confirm Password *'. Each field has a placeholder text matching its label. To the right of the 'New Password' field is a blue link labeled 'Password Policy'. At the bottom of the form is a blue button labeled 'Change Password'.

- 6) Click **Change Password**.

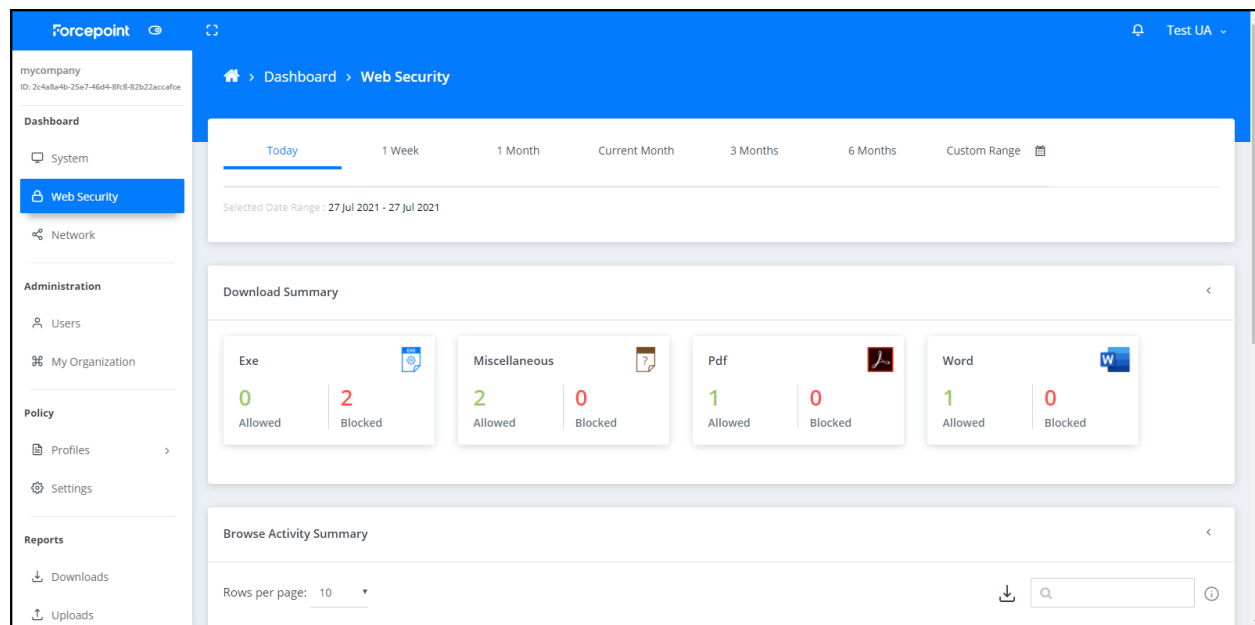
Chapter 4

Dashboard

Contents

- Common navigation elements on page 19
- Viewing system details on page 21
- Viewing web security details on page 22
- Viewing network details on page 26

The **Dashboard** section provides interactive, real-time graphical information about the status and activity in Forcepoint RBI.



Dashboard tabs

Tab	Description
System	Provides system license and active session details.
Web Security	Provides comprehensive information about the range of threats encountered by Forcepoint RBI. The Web Security tab opens by default when you sign in to Forcepoint RBI.
Network	Provides usage statistics for each user, browser type, and browsing category.

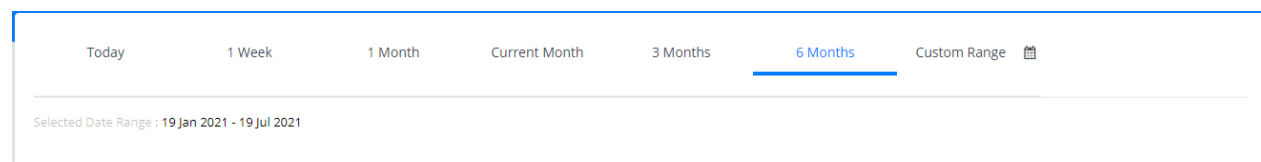
Common navigation elements

Each dashboard contains information within widgets. These widgets have common navigation elements, such as selecting the date range and changing the size of the widget.

Selecting the date range

For Web Security and Network widgets, you can select a specific time frame for the metrics shown within the widget.

The date range selector is located at the top of the dashboard screen. Select the date range, then view the metrics in the individual widgets.

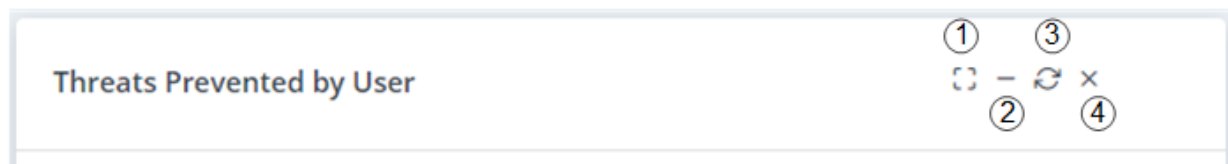


- Today: Shows metrics for the current date.
- 1 Week: Shows metrics for the past week from the current date.
- 1 Month: Shows metrics for the past month from the current date.
- Current Month: Shows metrics from the first day of the current month to the current date.
- 3 Months: Shows metrics for the past three months from the current date.
- 6 Months: Shows metrics for the past six months from the current date.
- Custom Range: If you do not want to use one of the default date ranges, you can select a specific start and end date.

Changing the size of the widget

Each widget contains a menu to resize the widget or refresh the data.

To open the menu, click the < icon in the top-right corner of the widget:



- 1 Full window: Click this option to change the size of the widget to take over the full browser window. The widget will be the only visible object in the browser window until you click the button to return to normal size.
- 2 Minimize: Click this option to show only the title area of the widget. The chart is not shown when the widget is minimized.
- 3 Refresh: Click this option to update the data shown in the chart. If new data have been added since the last time you refreshed, the chart is updated with the new data.
- 4 Close: Click this option to hide the menu and return to the original < icon.

Viewing system details

The **System** dashboard provides information about the Forcepoint RBI license and the active users.

The screenshot shows the Forcepoint System dashboard. The left sidebar contains navigation links for mycompany, Dashboard, System (selected), Web Security, Network, Administration (Users, My Organization), Policy (Profiles, Settings), and Reports (Downloads, Uploads). The main content area is titled 'Dashboard > System' and contains two widgets: 'Licensing Details' and 'Active Sessions'.

Licensing Details

- License Status: Active
- Entitled Features: Core
- Expires In: 157 Days(s)
- Activated On: 30 Jun 2021
- Expires On: 31 Dec 2021
- Total Users: 300

Active Sessions

Rows per page: 10

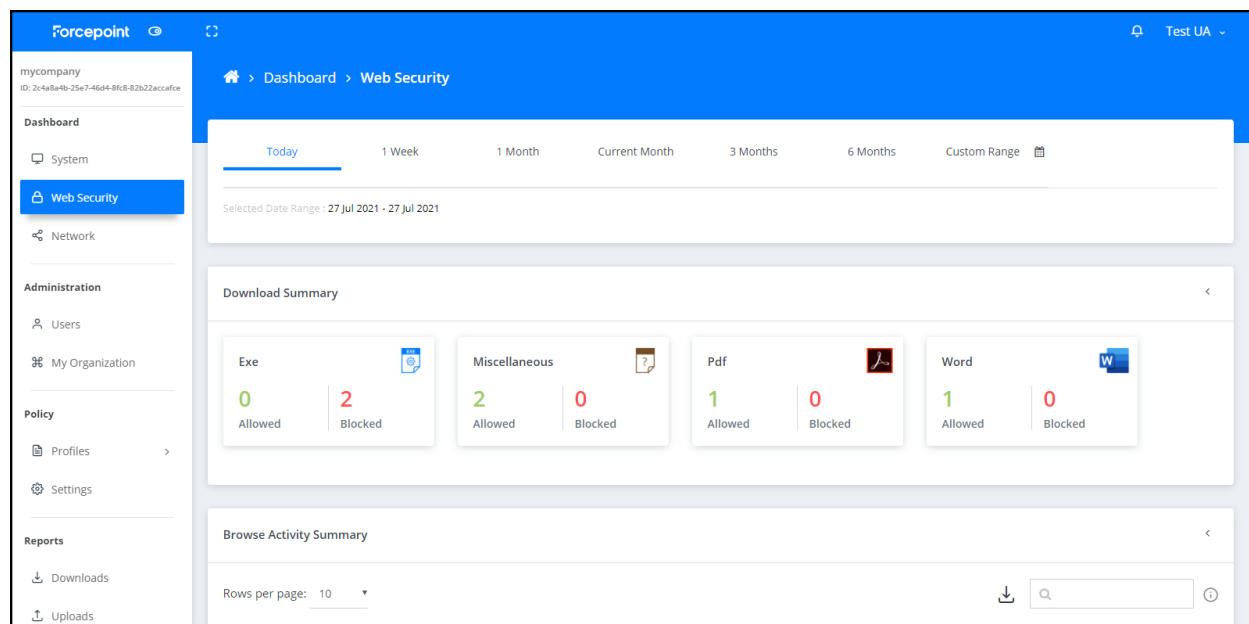
Start Date & Time	Username	Session ID	Appliance Name	Node Id	Device Details
26 Jul 2021 12:32:51	student12dup@yahoo.com	90fac94c-fd46-479d-be7a-9002e24b8f5c	stage-rbc-us-west-2-01	1004	Windows OS (10), Chrome browse

System Widgets

Widget	Description
Licensing Details	Shows information about the current license.
Active Sessions	Shows detailed information about the current active sessions of the users with isolated browsing sessions.

Viewing web security details

The **Web Security** dashboard provides comprehensive information about a range of threats encountered by Forcepoint RBI.



Web Security Widgets

Widget	Description
Download Summary	Shows the count for all file types that were either downloaded successfully by the user (allowed) or were not downloaded when the file failed the malware scanning check (blocked).
Browse Activity Summary	Shows the cumulative browsing activity and security events per user.
Threats Prevented by User	Shows information about the threats prevented per user.

View the download summary

The **Download Summary** shows the count for all file types that were either downloaded successfully by the user (allowed) or were not downloaded when the file failed the malware scanning check (blocked).

Steps

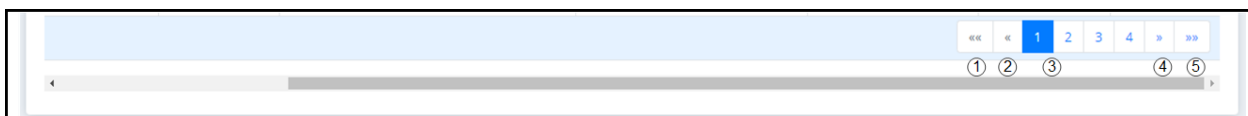
- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Dashboard > Web Security**.
- 3) Select the data range for the dashboard.
- 4) Go to the **Download Summary** widget. The summary chart shows the file types for each file that has been either **Allowed** or **Blocked**.

- 5) To see more details about a specific file type, click the file type icon. A table opens under the chart.
- 6) Above the table, you can choose the following options to change the visible metrics or download the table data.



- 1 Select the number of rows to show in the table. You can select to show either 10, 25, 50, or 100 rows.
- 2 Download the table data as a CSV file.
- 3 Search the table data for specific keywords. You can search on Username only.

- 7) Below the table, you can choose the following options to navigate through the table.



- 1 Go to the first page.
- 2 Go to the next page.
- 3 Go to a specific page.
- 4 Go to the next page.
- 5 Go to the last page.

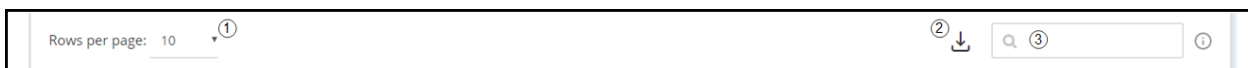
View the browse activity summary

The **Browse Activity Summary** shows the cumulative browsing activity and security events per user.

Steps

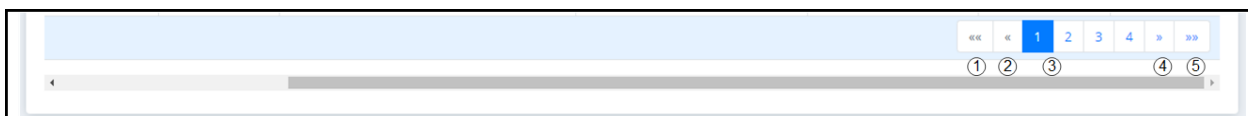
- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Dashboard > Web Security**.
- 3) Select the data range for the dashboard.
- 4) Go to the **Browse Activity Summary** widget.

- 5) Above the table, you can choose the following options to change the visible metrics or download the table data.



- 1 Select the number of rows to show in the table. You can select to show either 10, 25, 50, or 100 rows.
- 2 Download the table data as a CSV file.
- 3 Search the table data for specific keywords. You can search on Username only.

- 6) Below the table, you can choose the following options to navigate through the table.



- 1 Go to the first page.
- 2 Go to the next page.
- 3 Go to a specific page.
- 4 Go to the next page.
- 5 Go to the last page.

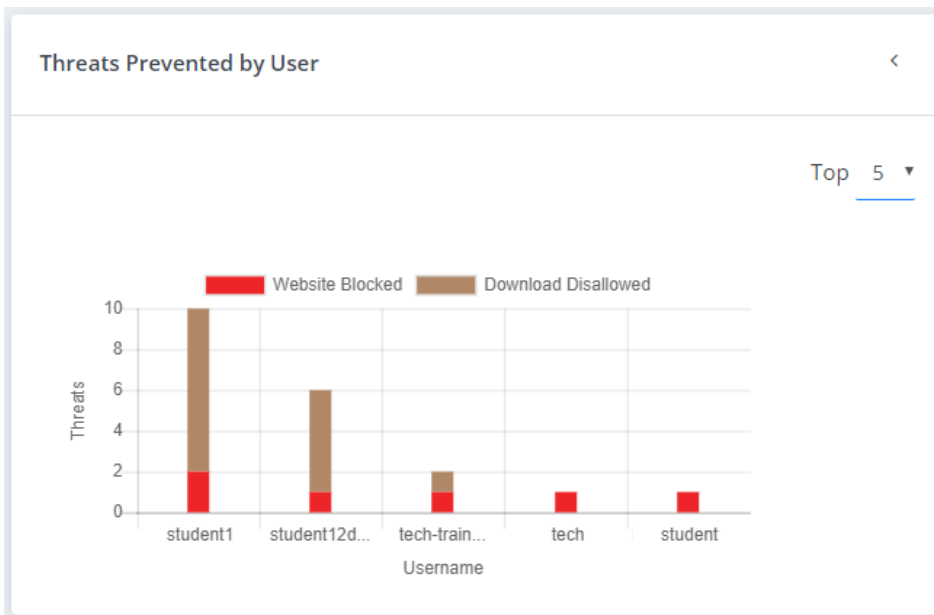
View metrics for threats prevented per user

The **Threats Prevented by Category** widget shows the number of threats prevented for each user.

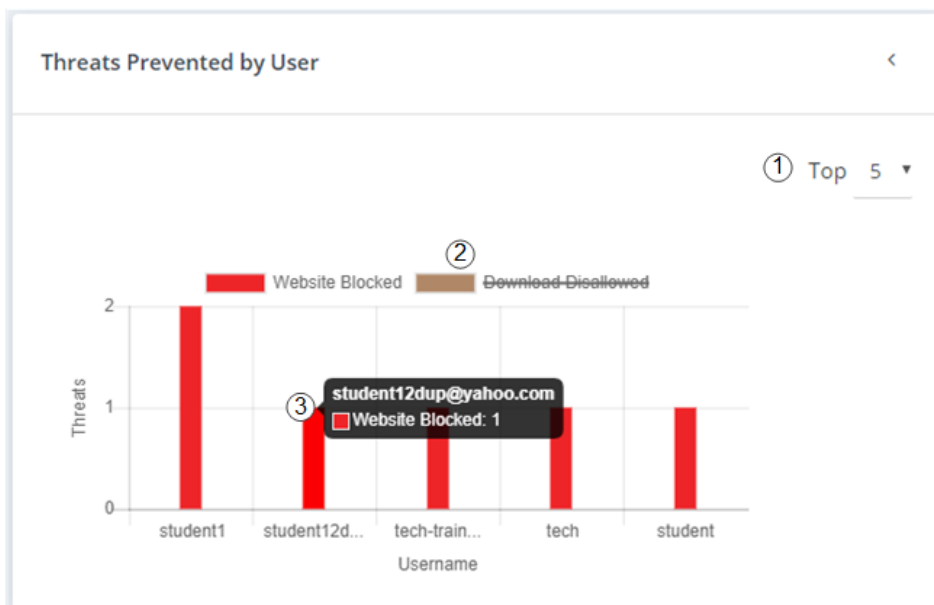
Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Dashboard > Web Security**.
- 3) Select the data range for the dashboard.

- 4) Go to the **Threats Prevented by User** widget. This widget shows a chart with the number of threats prevented per user.



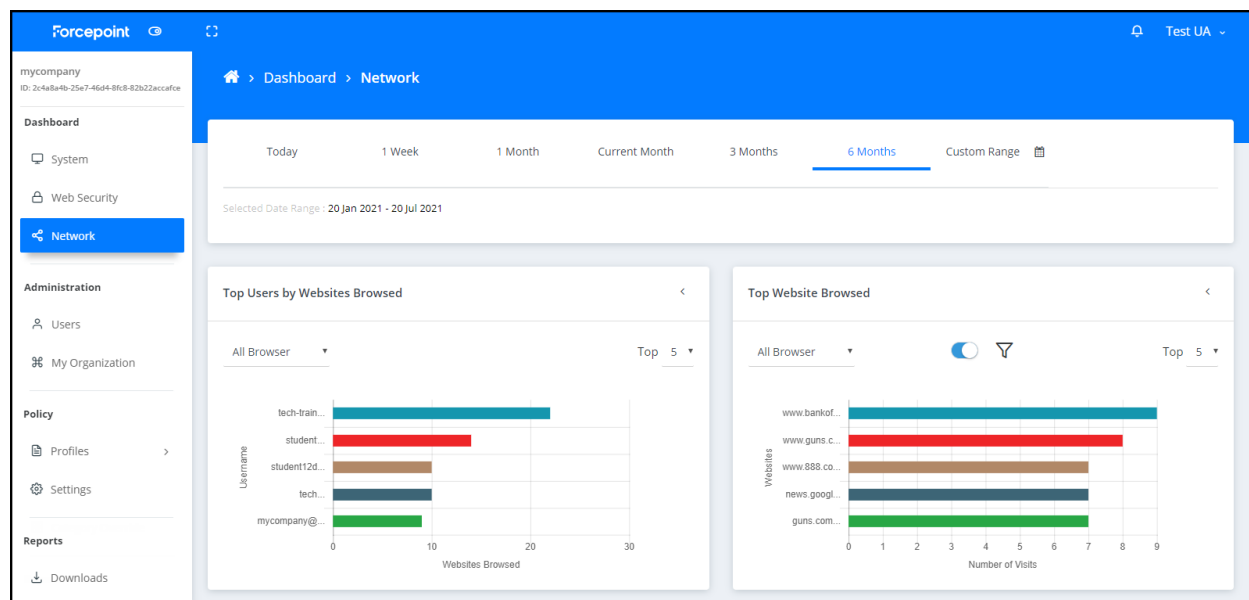
- 5) To change the metrics display:



- 1 Click the **Top** drop-down menu to show either the top 5, 10, or 15 users.
- 2 Click the threat type above the chart to remove that threat type from the chart. Click it again to add it back to the chart.
- 3 Hover your mouse over the chart to show a breakdown of the number of threats per threat type for that user.

Viewing network details

The **Network** dashboard provides usage statistics for each user, browser type, and browsing category.



Network Widgets

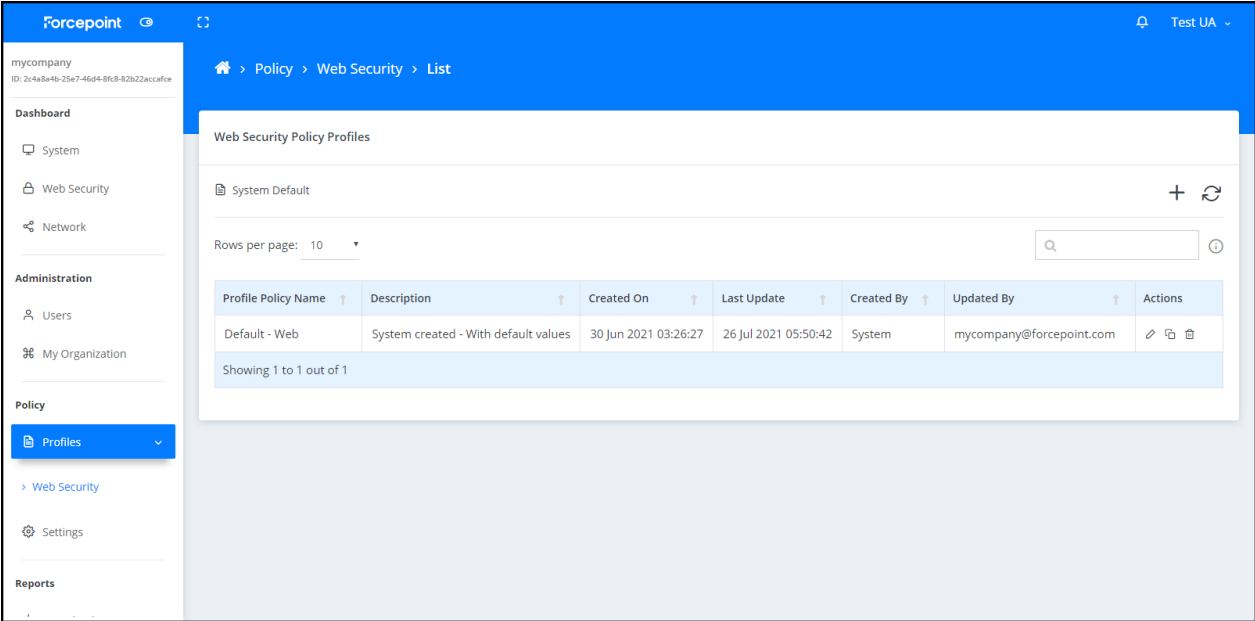
Widgets	Description
Top Users by Websites Browsed	Shows information about the number of websites browsed per user. You can choose to see the top 5, 10, or 15 users and you can choose to view the users for all browsers or a specific browser.
Top Website Browsed	Shows information about the number of visits per browsed website. You can choose to see the top 5, 10, or 15 users and you can choose to view the users for all browsers or a specific browser. Also, you can filter out specific URLs.
Sessions by Browser Type	Shows the total number of remote browser sessions per browser.
Users by Browser Type	Shows the total number of unique users per browser.

Chapter 6

Policy

Contents	
■	Profiles on page 28
■	Settings on page 32

The **Policy** section provides comprehensive information about your policy profiles.

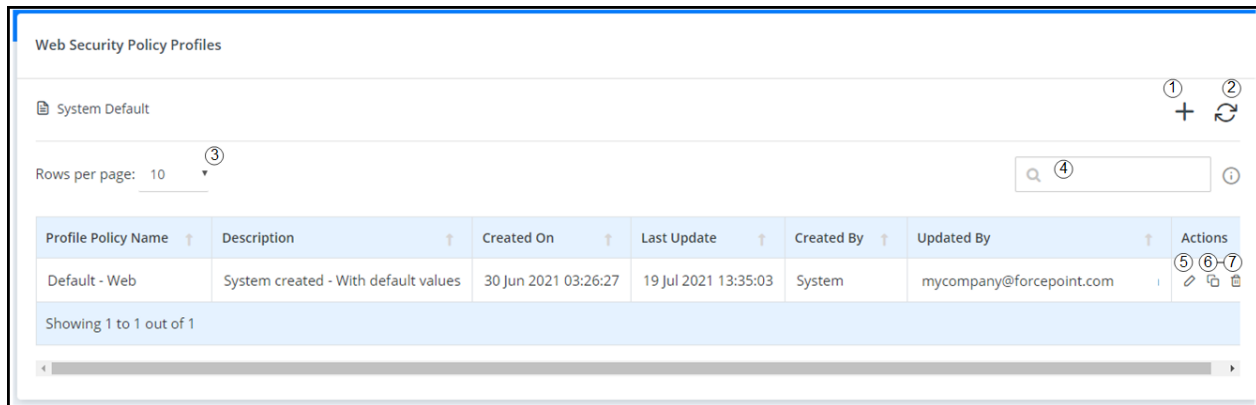


Policy tabs

Tab	Description
Profiles	Provides comprehensive information about the policy profiles configured for your organization. From this tab, you can create new profiles, or view, edit, delete, and duplicate existing profiles.
Settings	Provides comprehensive information about the Forcepoint RBI settings. From this tab, you can view and modify the settings for the email template parameters, notifications, and user cookies.

Profiles

The **Profiles** tab provides a list of the policy profiles configured for your organization. From this tab, you can create new profiles, or view, edit, delete, and duplicate existing profiles.



- 1 Add a new policy profile.
- 2 Refresh the list of profiles.
- 3 Choose to show either 10, 25, 50, or 100 rows in the table per page.
- 4 Search the list for a specific policy profile. You can search on the Profile Policy Name or Description.
- 5 View profile details.
- 6 Duplicate the profile.
- 7 Delete the profile.

Create a new policy profile

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Policy > Profiles > Web Security**.

- 3) Click the **+** icon above the table to open the **Create Profile** screen.

- 4) Enter the **Policy Profile Name** and **Policy Profile Description**.



Note

The **Policy Profile Name** is required. The profile cannot be saved without a name.

- 5) Under **Browser – Clipboard**, click the **Clipboard** button to enable the **Browser Clipboard** feature.
- Enabling the ability of a user to access the clipboard for copy and paste operations.
 - Disabling the ability of a user to access the clipboard for copy and paste operations.
 - Numerical entry fields are also available to set maximum limits on data size for both ingress and egress directions in the clipboard.
- 6) Under **Browser – Preferences**, select the **TLS Error Policy** type from the drop-down menu. The TLS Error Policy specifies the behavior of the Isolation browser when it navigates to a website with an invalid TLS certification.
- 7) Under **File Downloads**, click **Allow Downloads**, then enter the relevant information in the fields.
- 8) Under **File Uploads**, click **Allow Uploads** to allow file uploads, then enter the **Max Upload File Size Limit**.
- 9) Under **Printing**, enter the number of allowed prints from the printer.
- a) In the **Max Default Print Paper Size** field, enter the number of allowed prints from the printer.
 - b) Select the **Default Print Paper Size** from the drop-down menu.

- 10) Click **Save**. The profile is saved and it opens with a new tab: **Isolation Attributes**.

General Attributes | Isolation Attributes

URL Selection

Rows per page: 5

URL	Isolated	Blocked	Action
www.amazon.in	○	●	🗑️
www.audacityteam.org	○	●	🗑️

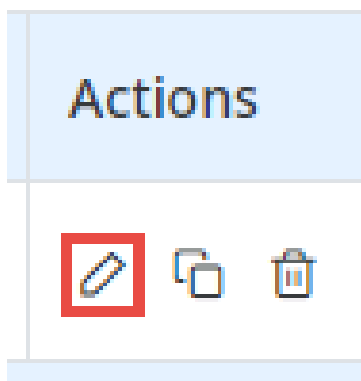
Showing 1 to 2 out of 2

- 11) In the **URL Selection** section, click the **+** icon. A new row is added to the table.
- 12) In the **URL** column, enter the full URL for the website.
- 13) Select whether the URL should be **Isolated** or **Blocked**.
- 14) In the **Action** column, click the save icon.

Edit a policy profile

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Policy > Profiles > Web Security**.
- 3) In the profile table, click the pencil icon in the **Actions** column.



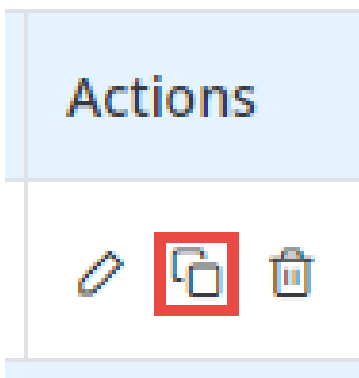
- 4) Edit the profile as needed.

- 5) Click **Save**.

Duplicate a policy profile

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Policy > Profiles > Web Security**.
- 3) In the profile table, click the duplicate icon in the **Actions** column.



The policy details page opens with the same configuration information as the existing policy. The **Policy Profile Name** has **- copy** added to the end.

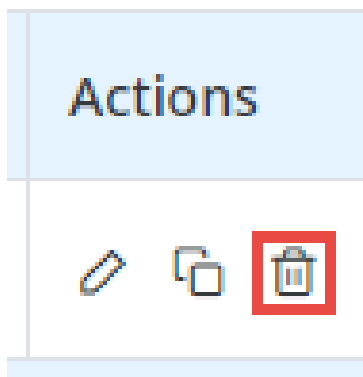
- 4) Edit the profile as needed.
- 5) Click **Save**.

Delete a policy profile

Steps

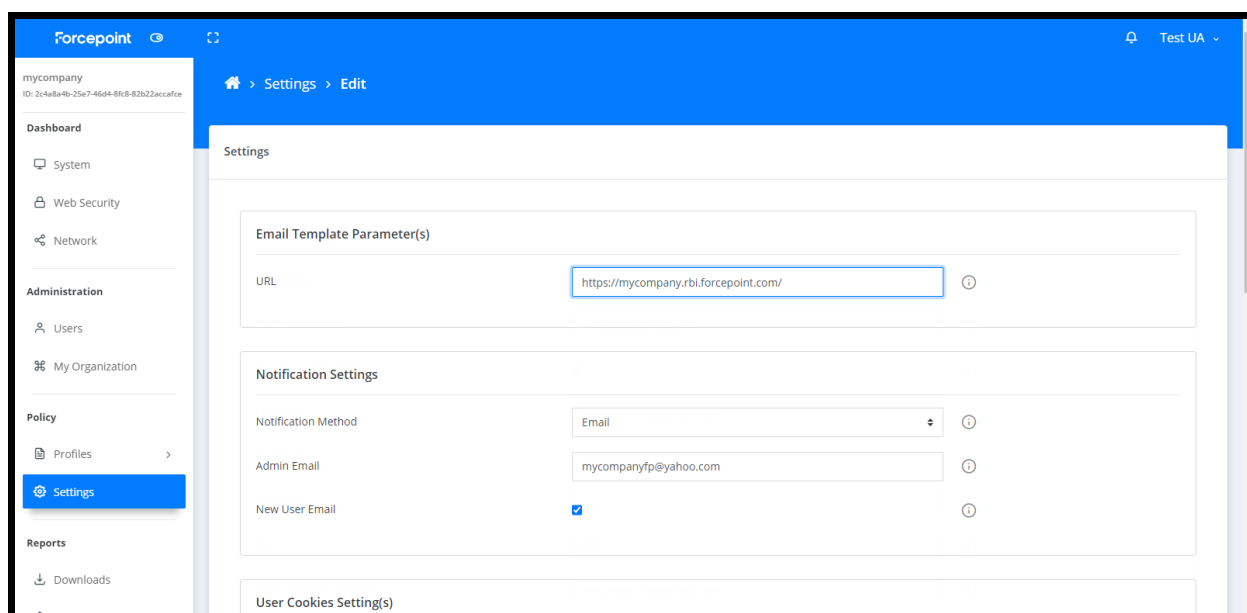
- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Policy > Profiles > Web Security**.

- 3) In the profile table, click the trashcan icon in the **Actions** column.




- 4) Click **Confirm** when asked if you want to delete the profile. The profile is deleted from the system and removed from the table.

Settings



Settings Widgets

Widgets	Description
Email Template Parameter(s)	<p>Configures the URL from where administrators can make all necessary configurations in Forcepoint RBI. You must configure this field with the tenant URL (<code>https://<mycompany>rbi.forcepoint.com</code>).</p> <div> <div></div> <div> <p>Note</p> <p>You can set this parameter one time only. After it is saved, you cannot edit it.</p> </div> </div>

Widgets	Description
Notification Settings	Configures the email notification settings to send email notifications to the list of email addresses in a comma-separated value (CSV) format.
User Cookies Setting(s)	<p>Saves cookies for external websites accessed through Forcepoint RBI to ensure accessibility and user experience. Anonymous user cookies are not saved.</p> <div>Note<p>This setting is applicable for signed in users only. Forcepoint RBI v5.5 only allows anonymous users.</p></div>

Chapter 7

Reports

Contents

- Create a Downloads report on page 35
- Create an Uploads report on page 36
- Create a Browse Activity report on page 37

The **Reports** section provides comprehensive reports about the downloads, uploads, and browsing activities of your users.

The screenshot shows the Forcepoint web interface. On the left is a navigation sidebar with categories: Dashboard, System, Web Security, Network, Administration (Users, My Organization), Policy (Profiles, Settings), Reports (Downloads, Uploads, Browse Activity), and Integrations (SIEM). The 'Downloads' option under Reports is highlighted. The main content area is titled 'Report > Downloads'. It features a 'Filters' panel on the left with input fields for 'Start Date' (07/27/2021), 'End Date' (07/27/2021), 'Username', 'File Name', 'File Type', 'IP Address', and 'Session ID'. A 'Generate Report' button is at the bottom of the filters. To the right is a 'Downloads Report Preview' box with the text: 'Click on Generate Report button on the left to generate a report'.

Reports tabs

Tab	Description
Downloads	Generate a report that shows the file downloads per user.
Uploads	Generate a report that shows the file uploads per user.
Browse Activity	Generate a report that shows the web browsing activity per user.

Create a Downloads report

The Downloads report shows detailed information about the files downloaded during a remote browser session.

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Reports > Downloads**.

The screenshot shows the Forcepoint Remote Browser Isolation interface. On the left is a navigation sidebar with categories: Dashboard, System, Web Security, Network, Administration (Users, My Organization), Policy (Profiles, Settings), Reports (Downloads, Uploads, Browse Activity), and Integrations (SIEM). The 'Downloads' option under Reports is highlighted. The main content area is titled 'Report > Downloads'. It features a 'Filters' panel on the left with input fields for Start Date (07/27/2021), End Date (07/27/2021), Username, File Name, File Type, IP Address, and Session ID. A 'Generate Report' button is at the bottom of the filters. To the right is a 'Downloads Report Preview' section with a message: 'Click on Generate Report button on the left to generate a report'.

- 3) Select the report filters:
 - Start Date (required)
 - End Date (required)
 - Username
 - File Name
 - File Type
 - IP Address
 - Session ID
- 4) Click **Generate Report**.

Create an Uploads report

The Uploads report shows detailed information about the files uploaded during a remote browser session.

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Reports > Uploads**.

The screenshot shows the Forcepoint Remote Browser Isolation interface. On the left is a navigation sidebar with categories: Dashboard, System, Web Security, Network, Administration (Users, My Organization), Policy (Profiles, Settings), Reports (Downloads, Uploads, Browse Activity), and Integrations (SIEM). The 'Uploads' option under Reports is highlighted. The main content area is titled 'Report > Uploads'. It features a 'Filters' panel on the left with input fields for 'Start Date' (07/27/2021), 'End Date' (07/27/2021), 'Username', 'File Name', 'IP Address', and 'Session ID'. A 'Generate Report' button is at the bottom of the filters. To the right is an 'Uploads Report Preview' box with the text: 'Click on Generate Report button on the left to generate a report'.

3) Select the report filters:

- Start Date (required)
- End Date (required)
- Username
- File Name
- IP Address
- Session ID

4) Click **Generate Report**.

Create a Browse Activity report

The Browse Activity report shows the websites viewed during a remote browsing session.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Reports > Browse Activity**.

The screenshot shows the Forcepoint web interface. The top navigation bar is blue with the Forcepoint logo and a user profile icon labeled 'Test UA'. The left sidebar is white with a blue header 'Dashboard' and several menu items: System, Web Security, Network, Administration (Users, My Organization), Policy (Profiles, Settings), Reports (Downloads, Uploads, Browse Activity), and Integrations (SIEM). The 'Browse Activity' item is highlighted with a blue background. The main content area has a blue header 'Report > Browse Activity'. Below this is a 'Filters' section with the following fields: Start Date (07/27/2021), End Date (07/27/2021), Username, IP Address, Session ID, Rendering Status (All), and Client Browser (All). A blue 'Generate Report' button is at the bottom of the filters. To the right of the filters is a 'Browse Activity Report Preview' section with a message: 'Click on Generate Report button on the left to generate a report'.

3) Select the report filters:

- Start Date (required)
- End Date (required)
- Username
- IP Address
- Session ID
- Rendering Status
- Client Browser

4) Click **Generate Report**.

Chapter 8

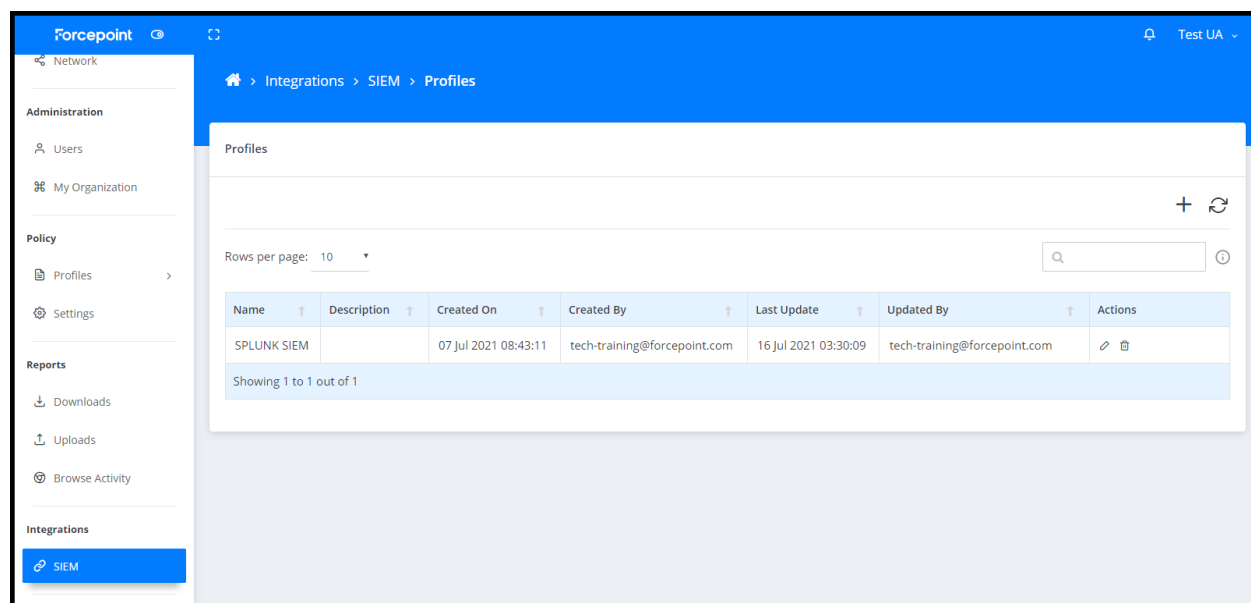
Integrations

Contents

- [Create a new SIEM integration](#) on page 39
- [Edit a SIEM profile](#) on page 41
- [Delete a SIEM profile](#) on page 41

The **Integrations** section allows you to set up and configure integrations with third-party solutions.

Currently, there is only one integration available in Forcepoint RBI: **SIEM**. This integration allows you to set up and configure an integration with a security information and event management (SIEM) solution to monitor security events, ensure appropriate action, and generate centralized reports



Create a new SIEM integration

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Integrations > SIEM**.

- 3) Click the **+** icon above the table to open the **Create Profile** screen.

- 4) Under **Profile Details**, enter the **Name** and **Description**.



Note

The **Name** is required. The profile cannot be saved without a name.

- 5) Under **Server Connection Details**

- For **Export Destination**, **Syslog** is the only option and is selected by default.
- In the **Syslog Server** field, enter the host name or the IP address of the Syslog server. This field is required.
- In the **Server Port** field, enter the port number of the server. This field is required
- Select the **Transport Protocol**. **UDP** is selected by default.
- Click **Check Connection** to verify that Forcepoint RBI can connect to the Syslog server.

- 6) Under **Log Details**:

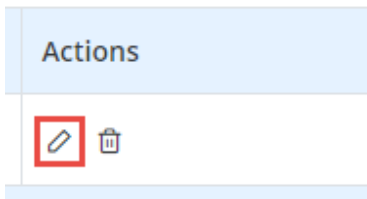
- For **Log Format**, **JSON** is the only option and is selected by default.
- Select the **Log Level**.
- Select the **Events** that need to be logged. You can select one or more types of events in this field.

- 7) Click **Add**.

Edit a SIEM profile

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Integrations > SIEM**.
- 3) In the profile table, click the pencil icon in the **Actions** column.

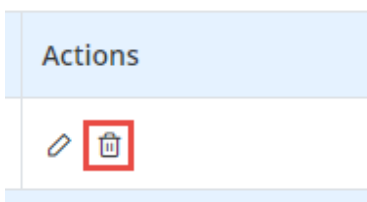


- 4) Edit the profile as needed.
- 5) Click **Save**.

Delete a SIEM profile

Steps

- 1) Sign in to Forcepoint Remote Browser Isolation.
- 2) Go to **Integrations > SIEM**.
- 3) In the profile table, click the trashcan icon in the **Actions** column.



- 4) Click **Confirm** when asked if you want to delete the profile. The profile is deleted from the system and removed from the table.

Product updates

Contents

- [What's new?](#) on page 43
- [Known and resolved issues](#) on page 43

Details of new and updated features, as well as known and resolved issues for Forcepoint Remote Browser Isolation.

What's new?

New features and product updates added during the most recent release.

Introducing Forcepoint Remote Browser Isolation version 5.5

This is the first release of Forcepoint Remote Browser Isolation (Forcepoint RBI) developed by Forcepoint. In this version, Forcepoint Remote Browser Isolation integrates with Forcepoint Cloud Security Gateway to redirect users to the remote browser powered by Forcepoint RBI.

To set up the integration between Forcepoint Cloud Security Gateway and Forcepoint RBI:

- 1) Configure a custom block page to redirect the user to the Forcepoint RBI remote browser.
- 2) Add the block page to the specific web categories within the user's policy on Forcepoint Cloud Security Gateway.
- 3) After the policy is configured in Forcepoint Cloud Security Gateway, you can configure Forcepoint RBI through the Forcepoint RBI Admin Portal.

Known and resolved issues

Refer to the Forcepoint Knowledge Base for details of current known issues and former issues that have been resolved.

For details of resolved and known issues, see the article: <https://support.forcepoint.com/s/article/Resolved-and-known-issues-for-Forcepoint-Remote-Browser-Isolation-2021>

This link requires a Forcepoint Support account.

