Forcepoint

Remote Browser Isolation

23.05

Help

Revision A

Published 12 May 2023

Contents

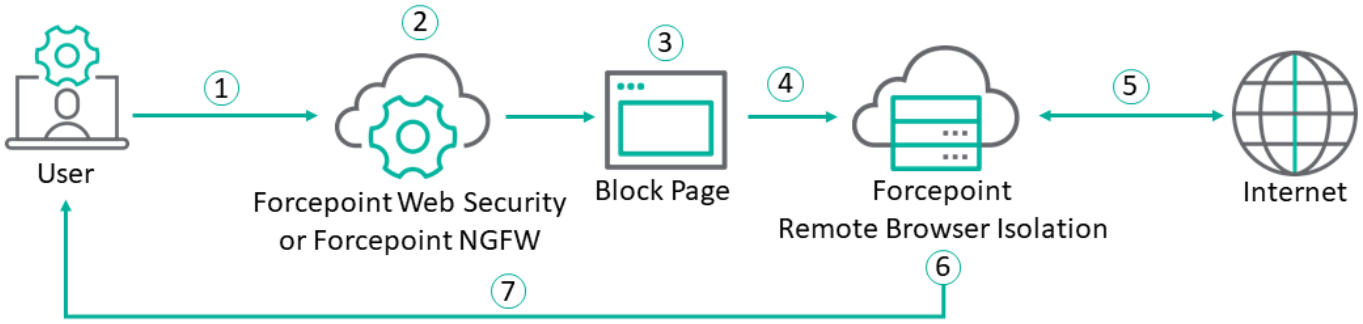
Chapter 1

Introduction

Contents

Forcepoint Remote Browser Isolation (Forcepoint RBI) neutralizes security threats through browser isolation to prevent attacks before they occur. By fully isolating web browser traffic, Forcepoint RBI creates a zero-trust environment that delivers a seamless user experience and eliminates most infections and compromises.

Internet browsing is a major threat carrier that can send unchecked active malicious codes to a user's endpoint machine. Forcepoint RBI prevents these threats by transferring user requests from the local browser to a disposable browser that performs fetch, execute, and render functions remotely. With Forcepoint RBI, active code is never sent to the protected endpoint machines. All web-based instructions are run in an isolated, purposely built virtual machine that removes computer code that could attack the protected endpoint machines.



1. The user submits an HTML request using a standard HTML5 compatible web browser.
2. Your Forcepoint management product — either Forcepoint Next Generation Firewall (Forcepoint NGFW) or Forcepoint Web Security (Cloud, On-Premises, or Hybrid) — checks to see if the requesting web category is blocked by the active web policy.
3. If the web category is blocked, the browser shows a block page to the user instead of the requested webpage. If the block page is configured to automatically redirect the page to the remote browser, then the user does not see the block page (this step is skipped).
4. The web 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 a safe visual stream that eliminates harmful scripts and active content.
7. Forcepoint RBI returns the safe content stream to the user ensuring a safe browsing experience that is isolated from a web attack.

Licensing

Customers require licenses for Forcepoint RBI to configure remote browser isolation in Forcepoint Web Security or Forcepoint Next Generation Firewall (Forcepoint NGFW).

A Forcepoint RBI cloud or on-premises license can be purchased as an add-on to any of the following Forcepoint products:

- Forcepoint Cloud Security Gateway
- Forcepoint Web Security Cloud
- Forcepoint Web Security On-premises or Hybrid
- Forcepoint NGFW

You can select either **RBI Selective**, **RBI Full**, or a combination of both.

- 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.

- 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, and license expiration date. If you purchase an on-premises license, then your fulfillment email also contains a license key file that needs to be uploaded to the Forcepoint RBI Admin Portal when you sign in for the first time.

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, contact Forcepoint Technical Support.

Chapter 2

Getting Started

Contents

To protect against known and unknown malware, Forcepoint Web Security (Cloud, On-Premises, and Hybrid) and Forcepoint NGFW customers configure a block page to redirect websites to Forcepoint RBI.

General workflow:

1) In your Forcepoint management product (Forcepoint NGFW or Forcepoint Web Security Cloud, On-Premises, or Hybrid), 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) In your Forcepoint management product, add the block page to the specific web categories within the user's policy. The initial setup is complete.

3) In the Forcepoint RBI Admin Portal, configure Forcepoint RBI.

Note

If you deploy both Forcepoint Web Security and Forcepoint NGFW within your organization, you can configure the redirection to Forcepoint RBI from either product.

Before you begin

Before you set up the block page for remote browser isolation, review the following requirements.

- Verify that you can connect to the Internet.

- Verify that you have administrator credentials for your Forcepoint products:
  - Forcepoint RBI Admin Portal
  - Forcepoint Cloud Security Gateway if you are integrating with Forcepoint Web Security Cloud.
  - Forcepoint Security Manager if you are integrating with Forcepoint Web Security On-Premises or Hybrid.
  - Forcepoint NGFW Security Management Center (SMC) if you are integrating with Forcepoint NGFW.

  If you do not have administrator credentials, contact Forcepoint Technical Support.
- Verify that the credentials work. Sign in successfully before continuing. If you cannot access the product using your administrator credentials, contact Forcepoint Technical Support.

Note

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

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 outbound connections from the endpoints to Forcepoint RBI through your firewall:
  - *.rbi.forcepoint.com and *.rbi.forcepoint.net: HTTPS port 443
  - Static IP addresses can be added instead of FQDNs for port opening in firewall to integrate with Forcepoint RBI. For details, contact Forcepoint Technical Support.

- Enable third-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 third-party cookies on your endpoints.

For customers using "URL redirect" method of integration:

Deployment mode	RBI service URL
Cloud	`https://<mycompany>.rbi.forcepoint.net/ loader?tenantId=<my_tenant_id>&url=<URL>&username=<USER NAME>`
On-premise	`https://<mycompany>.rbi.forcepoint.com/viewer/loader?tenantId=<my_tenant_id>&url=<URL>&username=<USER NAME>`

Details on service URL and parameters are explained in relevant sections below.

Configuring the redirect for Forcepoint Web Security Cloud

Forcepoint Web Security Cloud customers configure the redirect to Forcepoint RBI through Forcepoint Cloud Security Gateway.

There are two options to redirect user web traffic to Forcepoint RBI:

- Block and Confirm redirect: This option requires that the user confirm the web traffic redirect. When Forcepoint Web Security Cloud detects web traffic to specific configured web categories, it opens a block page in the user's web browser. To view the website, the user clicks a confirmation button on the block page to redirect the web traffic through Forcepoint RBI.
- Automatic redirect: This option redirects the web traffic without intervention by the user. When Forcepoint Web Security Cloud detects web traffic to specific configured web categories, it automatically directs the web traffic through Forcepoint RBI. There are no confirmation steps or block pages in this option.

Add RBI domains to the bypass list

The domains `*rbi.forcepoint.net` and `*rbi.forcepoint.com` are added to the bypass list in the Cloud Portal proxy bypass settings.

Create a custom redirect block page in Forcepoint Cloud Security Gateway

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.

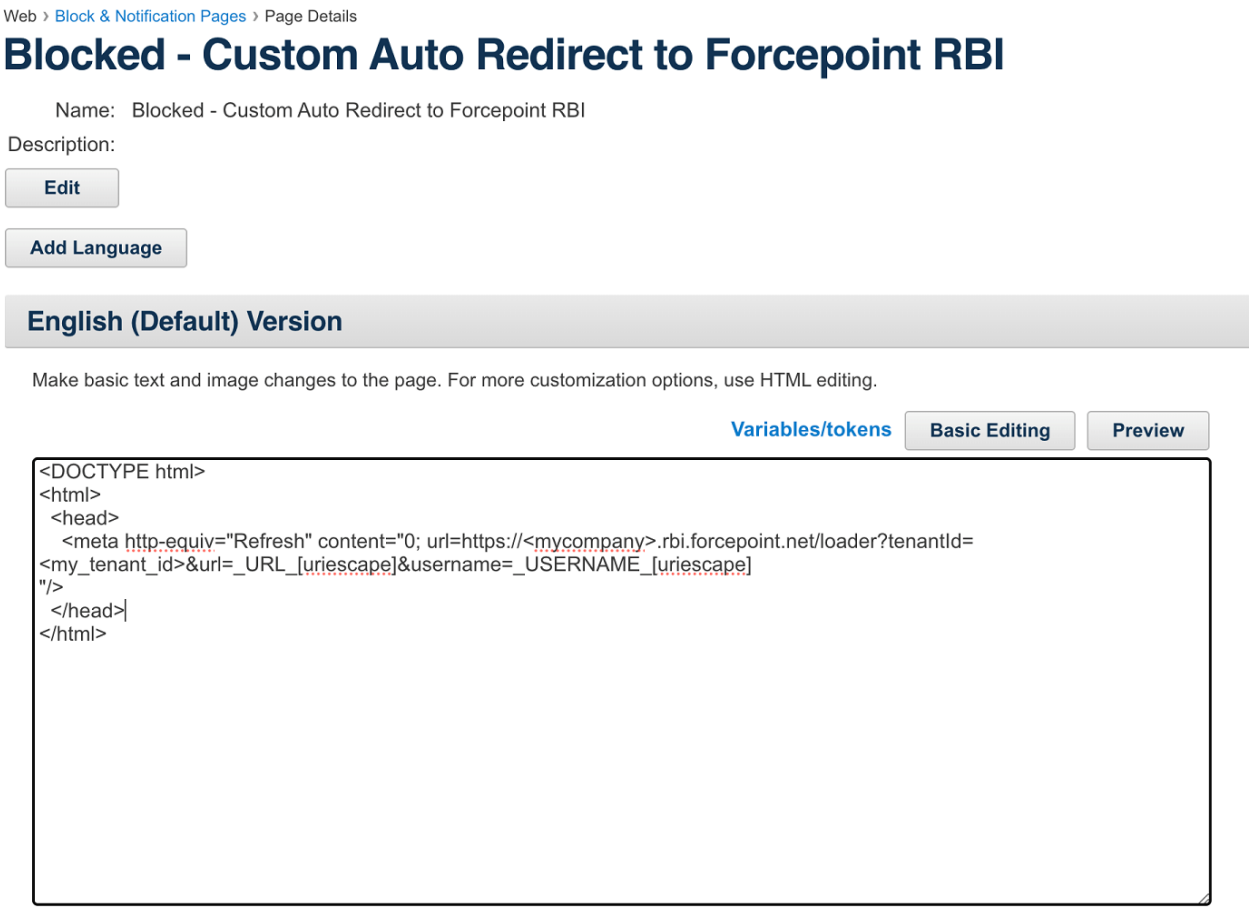
2) Go to **Web** > **Policy Management** > **Block & Notification Pages**.

3) Click **New Page**.

4) On the **New custom page** screen, enter a **Name** and **Description**.

5) Click **Save**.

6) On the **Page Details** page, click **HTML Editing**, then click **Continue** on the dialog box.



7) Replace the default HTML code with the following HTML code:

```
<!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">
                        <img id="title_icon" src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-
resources/notification-pages/icons60/blocked.png" height="60" width="60" class="editable
 image zzNOTIFICATION_ICONxxIMAGEzz" />
                        <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>
```

8) Code continues..

```
</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.net/
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="">
                           <img src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
notification-pages/2020/notification_page_logo_145x35.png" height="35" width="145"
 id="bottom-logo" class="editable image zzNOTIFICATION_BOTTOM_LOGOxxIMAGEzz"/>
                           <span id="footer-text" class="editable text
 zzNOTIFICATION_FOOTERxxTEXTzz" ></span>
                           <div class="clear-float"></div>
                        </div>
                        <div class="clear-float"></div>
                    </div>
                </div>
            </div>
        </div>
        <div class="clear-float"></div>
        <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/notification-pages/
empty.js"></script>
         <!--[if !(IE 6)]>
            <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/notification-pages/
respond.src.js"></script>
         <![endif]-->
        <!-- __DEBUG_INFO__ -->
    </body>
</html>
```

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

```
<div class="span3 "><a class="linkAsButton" href="https://<mycompany>.rbi.forcepoint.net/
loader?tenantId=<my_tenant_id>&url=_URL_[uriescape]&username=_USERNAME_[uriescape]" >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_[uriescape]`: 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 Forcepoint Cloud Security Gateway policy on page 15

Create a custom auto-redirect block page in Forcepoint Cloud Security Gateway

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**.

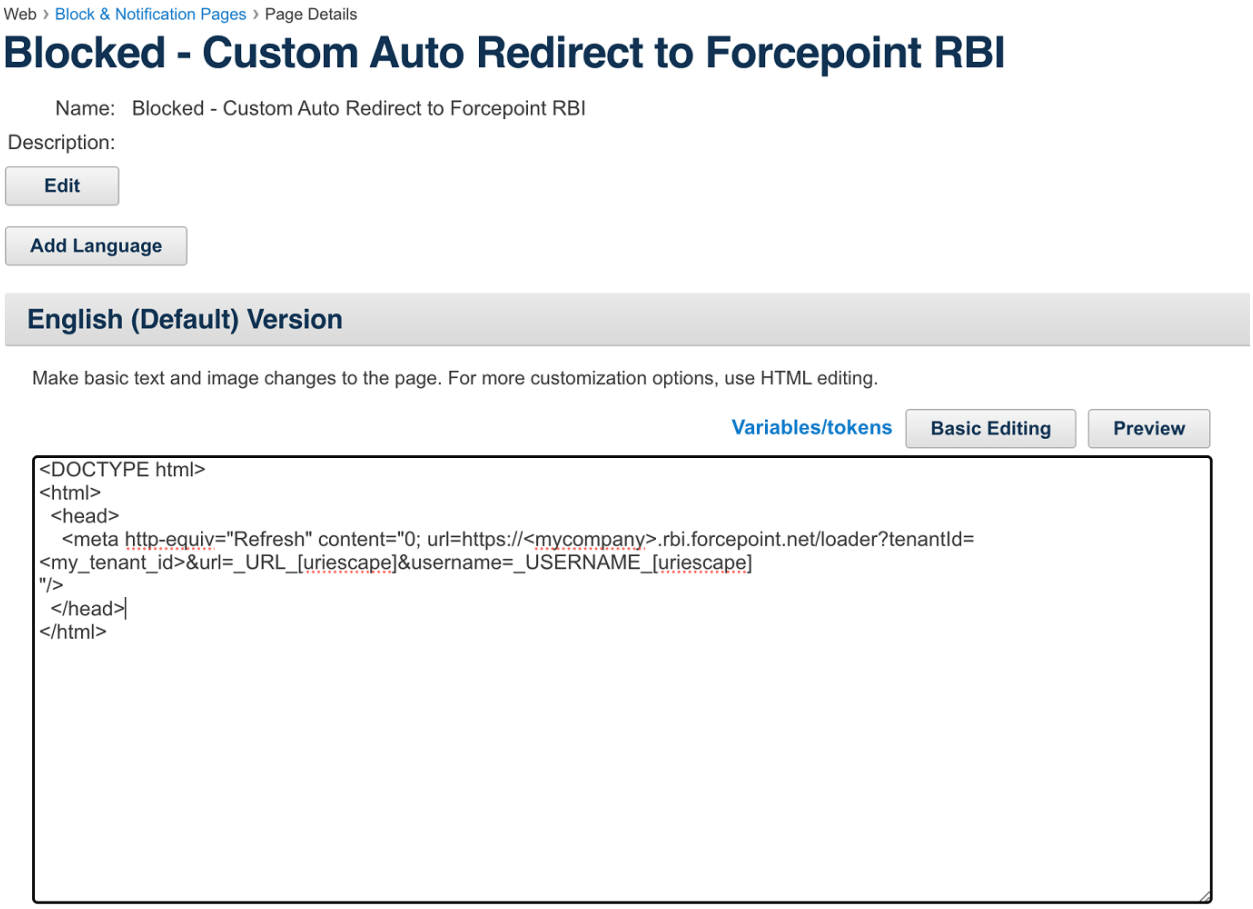
4) On the **New custom page** screen, enter a **Name** and **Description**.

5) Click **Save**.

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

7) Replace the default HTML code with the following HTML code:

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



8) 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.

9) Click **Save**.

Related tasks

Add the custom block page to a Forcepoint Cloud Security Gateway policy on page 15

Add the custom block page to a Forcepoint Cloud Security Gateway 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.

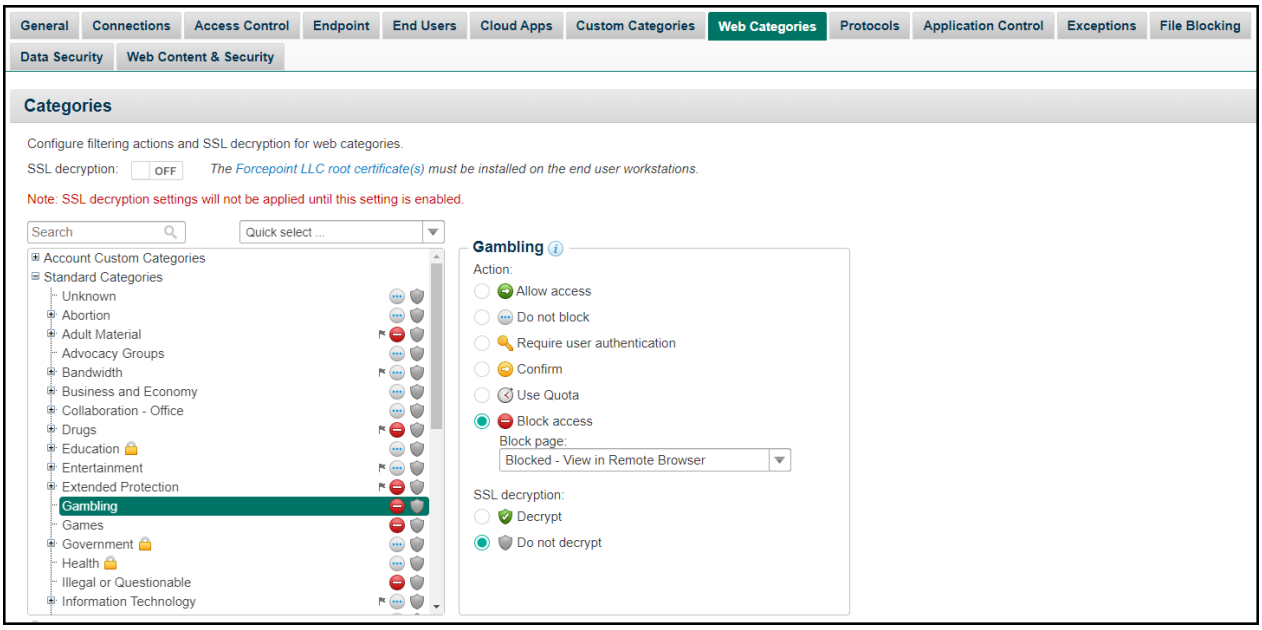
2) Go to **Web** > **Policy Management** > **Policies**.

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 from Forcepoint Cloud Security Gateway on page 16

Verify the redirect from Forcepoint Cloud Security Gateway

Verify that the browser session is isolated based on the redirect block page and configured policy.

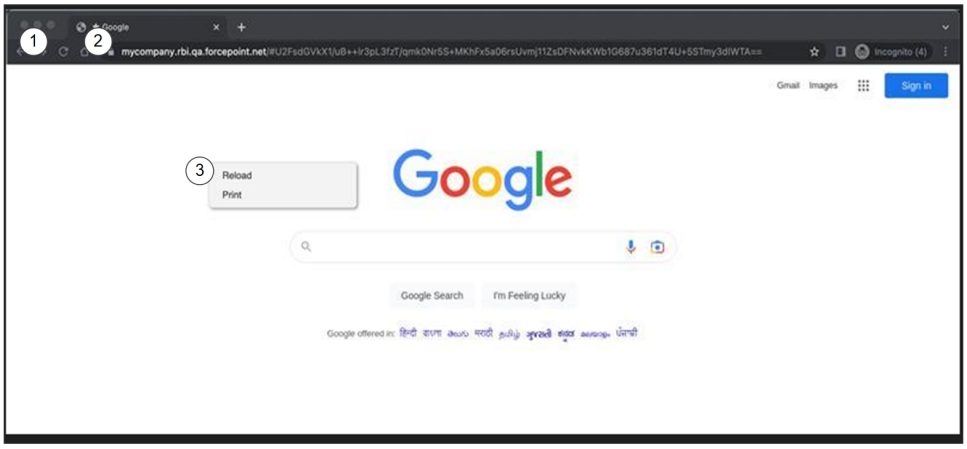
Steps

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.

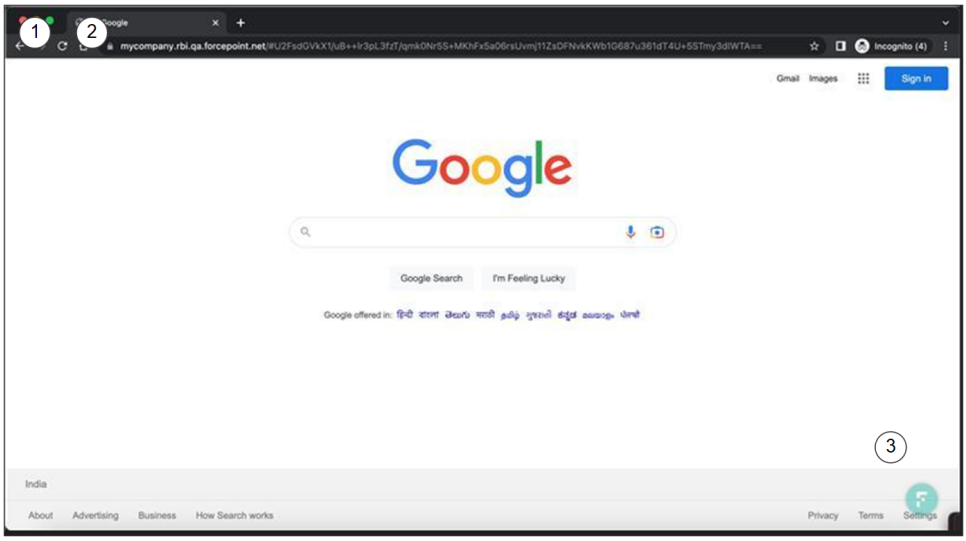
3) Verify that the browser session is going through the remote browser:

Secure Streaming



1. Look for the star. The tab header for the webpage will display a star next to the webpage title.
2. The URL appears as `https://<mycompany>.rbi.forcepoint.net/viewer/#<Encrypted Actual URL>`. The isolated URL is encrypted to restrict user from manipulating the URL and bypassing any proxy restrictions. For more information, see URL Encryption on page 149.
3. Check the right-click menu. The right-click menu contains the options for the remote browser only: **Reload**, **Print**, and **Session Information**.

Secure Rendering



1. Look for the star. The tab header for the webpage will display a star next to the webpage title.
2. The URL appears as `https://<mycompany>.rbi.forcepoint.net/viewer/#<Encrypted Actual URL>`. The isolated URL is encrypted to restrict user from manipulating the URL and bypassing any proxy restrictions. For more information, see URL Encryption on page 149.
3. Check the Forcepoint logo. A Forcepoint logo is visible at the bottom right corner of the browser window. Click this logo to open the menu, then select either **URL Information** (shows the Domain, URL Threat Score, and Category) or **Session Information** (shows the Session ID and IP Address).

Configuring the redirect for Forcepoint Web Security On-Premises

Forcepoint Web Security customers configure the redirect to Forcepoint RBI through the Forcepoint Security Manager.

There are two options to redirect user web traffic to Forcepoint RBI:

- Block and Confirm redirect: This option requires that the user confirm the web traffic redirect. When Forcepoint Web Security detects web traffic to specific configured web categories, it opens a block page in the user's web browser. To view the website, the user clicks a confirmation button on the block page to redirect the web traffic through Forcepoint RBI.
- Automatic redirect: This option redirects the web traffic without intervention by the user. When Forcepoint Web Security detects web traffic to specific configured web categories, it automatically directs the web traffic through Forcepoint RBI. There are no confirmation steps or block pages in this option.

Note

Both options assume that the **Confirm** and **Quota** actions are not currently used in the policy. The procedures in this section override the existing **Confirm** and **Quota** capabilities.

Note

Log traffic entries are shown as **Blocked with confirm option** or **Blocked by quota** in Forcepoint Security Manager, not Forcepoint RBI

Initial configuration in the Forcepoint Security Manager

Before you configure the redirect, complete the initial configuration steps in the Forcepoint Security Manager: add a new filter, specify the FQDN, and add the Forcepoint RBI domain to the SSL decryption bypass.

Steps

1) Sign in to the Forcepoint Security Manager and open the **WEB** module.

2) Go to **Policy Management** > **Filter Components**.

3) On the **Filter Components** page, select **Edit Categories**.

4) Create a new category called **Browser Isolated Sessions**. This new category will be used to create reports based on the sessions that use the Forcepoint RBI redirect URL.

5) Specify the Forcepoint RBI FQDN as a URL for this category. The default URL for Forcepoint RBI is **<mycompany>.rbi.forcepoint.net** where **<mycompany>** is your organization name as defined in the fulfillment letter and shown in the Forcepoint RBI Admin Portal.

6) Add the Forcepoint RBI domain to the SSL decryption bypass:
   a) In the **WEB** module, go to **Settings** > **Scanning** > **Bypass Settings**.
   b) On the **SSL Decryption Bypass** page, add `*.rbi.forcepoint.net` and `*.rbi.forcepoint.com` as a **Destination**.
   c) Click **OK**.
7) Click **Save and Deploy** to deploy the changes to your endpoints.

Configure the TCP ports in Content Gateway Manager

For explicit proxy deployments, customers need to tunnel a port range for websocket traffic from the on-premises proxy to Forcepoint RBI.

Note

For transparent proxy deployments, the websocket traffic goes directly to the Internet and does not need to be tunneled. If you are using a transparent proxy, you do not need to tunnel the port range provided below.

Steps

1) Sign in to the Content Gateway Manager.
2) Go to **Configure** > **Protocols** > **HTTP**.
3) On the **General** tab, add the following port information to the **HTTPS ports** field: **443**.
4) Click **Apply**.

Next steps

For both explicit proxy and transparent proxy deployments, update your firewall rules to allow port 443.

Configure the block and confirm redirect to Forcepoint RBI

Configure the policy to block and confirm one or more web categories.

The confirm action displays a block page with the option to view the website through the Forcepoint RBI isolated browser.

Steps

1) Sign in to the Forcepoint Security Manager and open the **WEB** module.
2) Go to **Policy Management** > **Policies**, then select the relevant policy.
3) On the **Category/Limited Access Filter** tab, select a web category from the left pane.
4) In the right pane, click **Confirm**.
5) Click **OK** to cache the changes.
6) Click **Save and Deploy** to implement the changes.

Next steps

After the policy is configured to block and confirm the web categories, you need to configure the **continueFrame.html** block page to add the **Isolate** button and link to the Forcepoint RBI.

Customize the block and confirm redirect block page

Customize the block and confirm redirect block page to show an Isolate button that links to the Forcepoint RBI redirect URL.

This procedure uses **continueFrame.html** as the block and confirm redirect block page. If you have an appliance-based installation, then Curl is suggested to manage the block page through API requests.

Note

You must have the latest hotfixes installed, if you are on Forcepoint Web Security v8.5.4.

Steps

1) Create a backup copy of the **continueFrame.html** block page. If the Filtering Service resides on a Windows or Linux server, go to the default block page directory. For English, this directory is `Websense/Web Security/BlockPages/en/Default` .
2) For appliance-based installations, get the **continueFrame.html** page. In the terminal, type:

   ```
   curl -k -u admin:{PASSWORD} -X GET https://Cinterface/wse/customblockpage/file/default/en/continueFrame.html > continueFrame.html
   ```

   where `{PASSWORD}` is the password for the admin account.

3) Open **continueFrame.html** and change the Forcepoint RBI URL to the assigned RBI redirect URL (`https://<mycompany>.rbi.forcepoint.net/loader` in the code sample below) and add your Tenant ID (`<my_tenant_id>` in the code sample below).

```
<!-- CONTINUE section -->
    <table class="option">
    <tr>
        <td>
            <form action="https://<mycompany>.rbi.forcepoint.net/loader" method="get"
 target="_top" name="ContinueForm">
                <input type="hidden" name="SD" id="SD">
                <script type="text/javascript">

 document.getElementById('SD').value=Base64.encode('TenantID=<my_tenant_id>'+'&url='+'$*WS_RAWURL*
$'+'&X-Authenticated-User='+'$*WS_USERNAME*$') ;
                </script>
                <input type="submit" value="Isolate" name="" class="ws_btn">
            </form>
        </td>
        <td>
                <span id="continue-text" class="ws_btn_desc">Click <strong>Isolate</strong>
 to view this page for work-related reasons in <strong>Isolated</strong> Browser.<script
 type="text/javascript">writeWarning()</script></span>
        </td>
    </tr>
</table>
```

4) Save the updated file.

5) For appliance-based installations, upload the modified **continueFrame.html** page. In the terminal, type:

```
curl -k -u admin:{PASSWORD} -X PUT -F "file=@continueFrame.html" https://Cinterface/wse/
customblockpage/file/default/en/"
```

where `{PASSWORD}` is the password for the admin account.

Configure the auto-redirect to Forcepoint RBI

Configure the policy to automatically redirect one or more web categories.

The quota action is used to redirect the web traffic automatically through the Forcepoint RBI isolated browser.

Steps

1) Sign in to the Forcepoint Security Manager and open the **WEB** module.

2) Go to **Policy Management** > **Policies**, then select the relevant policy.

3) On the **Category/Limited Access Filter** tab, select a web category from the left pane.

4) In the right pane, click **Quota**.

5) Click **OK** to cache the changes.

6) Click **Save and Deploy** to implement the changes.

Next steps

After the policy is configured to use the Quota option to redirect the web categories, you need to configure the **quotaFrame.html** block page.

Customize the auto-redirect block page

Customize the quota redirect block page to show an Isolate button that links to the Forcepoint RBI redirect URL.

The quota redirect block page is **quotaFrame.html**. If you have an appliance-based installation, then Curl is suggested to manage the block page through API requests.

Note

You must have the latest hotfixes installed, if you are on Forcepoint Web Security v8.5.4.

Steps

1) Create a backup copy of the **quotaFrame.html** block page. If the Filtering Service resides on a Windows or Linux server, go to the default block page directory. For English, this directory is `Websense/Web Security/BlockPages/en/Default` .

2) For appliance-based installations, get the **quotaFrame.html** page. In the terminal, type:

```
curl -k -u admin:{PASSWORD} -X GET https://Cinterface/wse/customblockpage/file/default/en/
quotaFrame.html > quotaFrame.html
```

where `{PASSWORD}` is the password for the admin account.

3) Open **quotaFrame.html** and change the Forcepoint RBI URL to the assigned RBI redirect URL (`https://<mycompany>.rbi.forcepoint.net/loader` in the code sample below) and add your Tenant ID (`<my_tenant_id>` in the code sample below).

```
<td>
    <form action="https://<mycompany>.rbi.forcepoint.net/loader" method="get" target="_top"
 name="QuotaForm">
        <input type="hidden" name="SD" id="SD">
            <script type="text/javascript">

 document.getElementById('SD').value=Base64.encode('TenantID=<my_tenant_id>'+'&url='+'$*WS_RAWURL*
$'+'&X-Authenticated-User='+'$*WS_USERNAME*$') ;
            </script>
        <input type="submit" value="Isolate" name="" class="ws_btn">
    </form>
    <script type="text/javascript">
        document.QuotaForm.submit();
    </script>
</td>
```

4) Save the updated file.

5) For appliance-based installations, upload the modified **quotaFrame.html** page. In the terminal, type:

```
curl -k -u admin:{PASSWORD} -X PUT -F "file=@quotaFrame.html" https://Cinterface/wse/
customblockpage/file/default/en/"
```

where `{PASSWORD}` is the password for the admin account.

Restart Filtering Service

After updating the confirm page, quota page, or both pages, Filtering Service must be restarted.

Steps

1) For Windows, use the Windows Services tool to restart Filtering Service.

2) For Linux, use the /opt/Websense/WebsenseDaemonControl command to restart Filtering Service.

Verify the redirect from Forcepoint Web Security On-Premises

Verify that the browser session is isolated based on the redirect block page and configured policy.

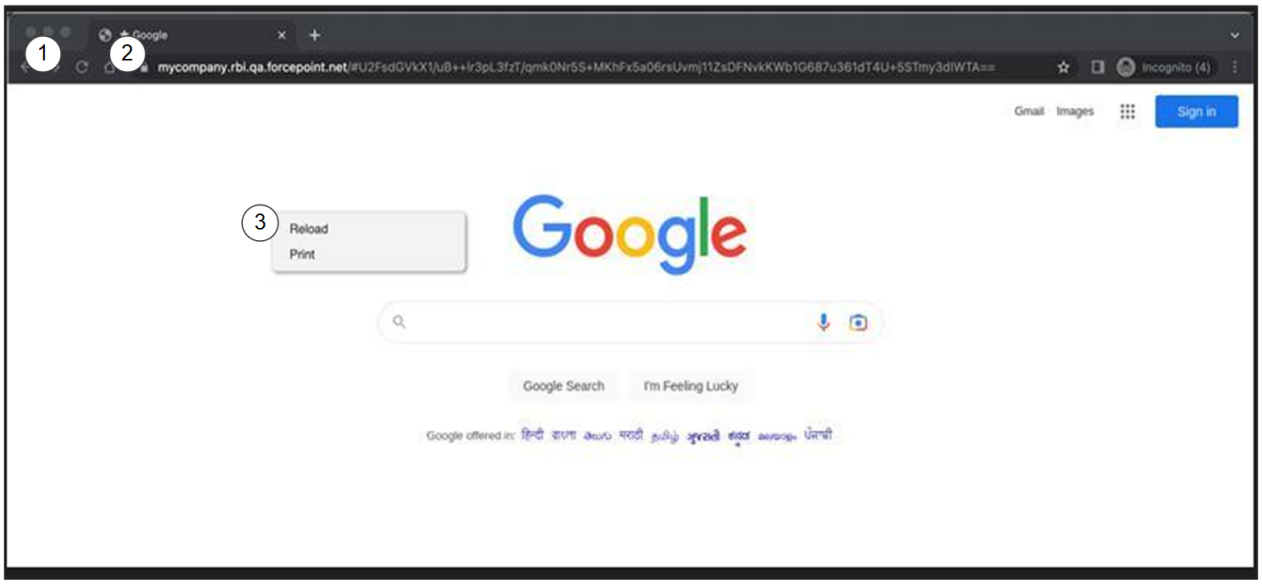
Steps

1) Open an HTML5 compatible browser and go to a webpage that should be blocked per the active policy in Forcepoint Web Security.

2) If you configured the default block page, click **Isolate**. This step is not needed if you created a custom auto-redirect block page.

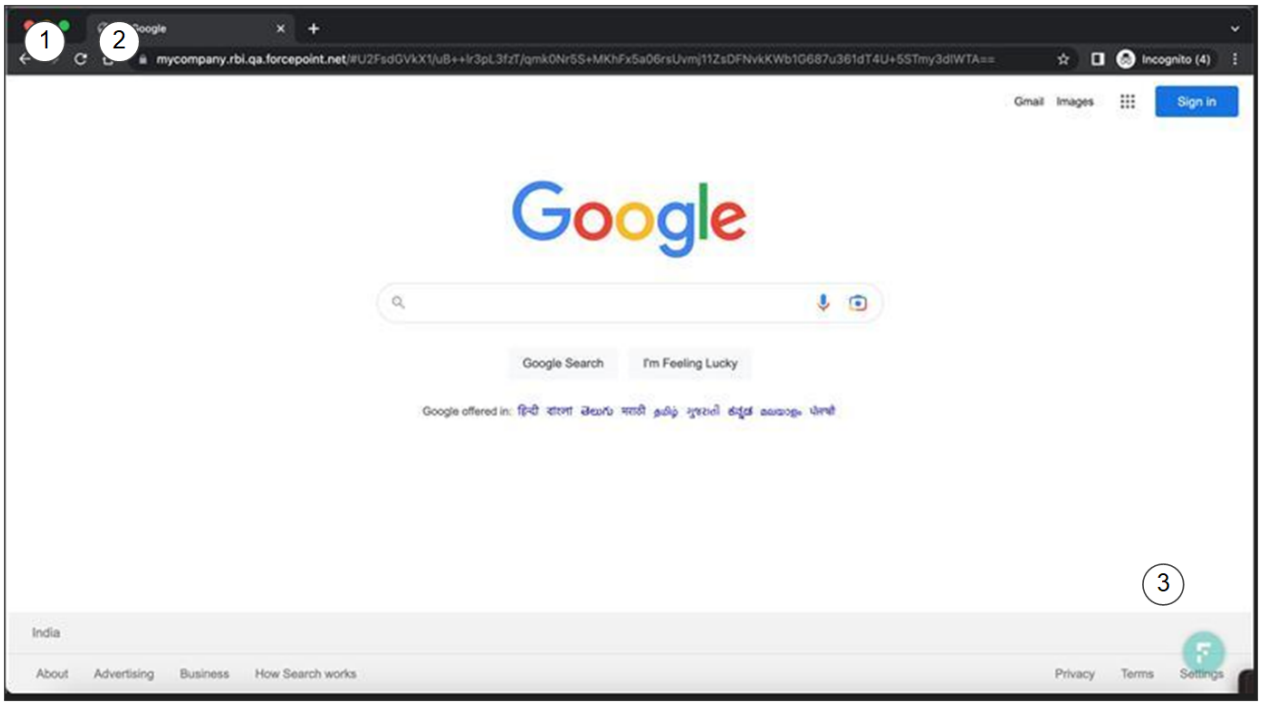
3) Verify that the browser session is going through the remote browser:

Secure Streaming:



1. Look for the star. The tab header for the webpage will display a star next to the webpage title.
2. The URL appears as `https://<mycompany>.rbi.forcepoint.net/viewer/#<Encrypted Actual URL>`. The isolated URL is encrypted to restrict user from manipulating the URL and bypassing any proxy restrictions. For more information, see URL Encryption on page 149.
3. Check the right-click menu. The right-click menu contains the options for the remote browser only: **Reload**, **Print**, and **Session Information**.

Secure Rendering:



1. Look for the star. The tab header for the webpage will display a star next to the webpage title.
2. The URL appears as `https://<mycompany>.rbi.forcepoint.net/viewer/#<Encrypted Actual URL>`. The isolated URL is encrypted to restrict user from manipulating the URL and bypassing any proxy restrictions. For more information, see URL Encryption on page 149.
3. Check the Forcepoint logo. A Forcepoint logo is visible at the bottom right corner of the browser

Configuring the redirect for Forcepoint Web Security Hybrid

Customers cannot customize the functionality of the block pages for Hybrid deployments. Forcepoint needs to customize these block pages.

To enable Forcepoint RBI for Forcepoint Web Security Hybrid, contact Forcepoint Technical Support and request that Support enables the “Customize block page DEBUG section for Hybrid Web” template.

Note

This customization disables the **Confirm** and **Quota** Policy Actions and changes them to **Block-And-Isolate** and **Auto Redirect to Isolate** respectively.

Provide the following information in your request:

- Forcepoint RBI Tenant ID.
- Forcepoint RBI URL.

Note

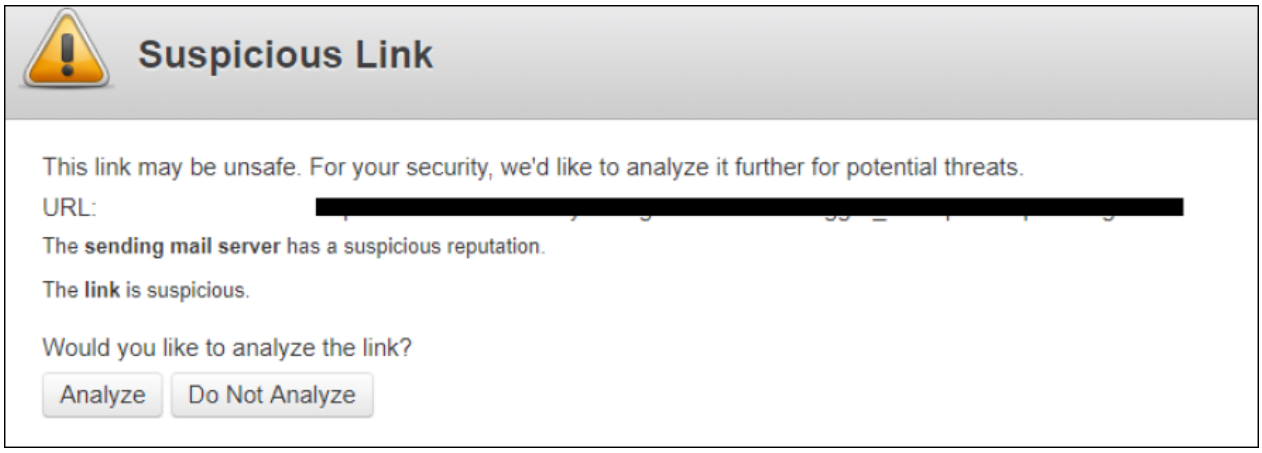
This information can be found in your fulfillment email and in the Forcepoint RBI Admin Portal.

After Technical Support modifies the block page, an isolation action is available for your categories in the Hybrid policy.

Configuring the redirect for Forcepoint Email Security Cloud

Forcepoint RBI communicates with Forcepoint Email Security via Block Page Redirect to provide isolation-based zero-day malware protection.

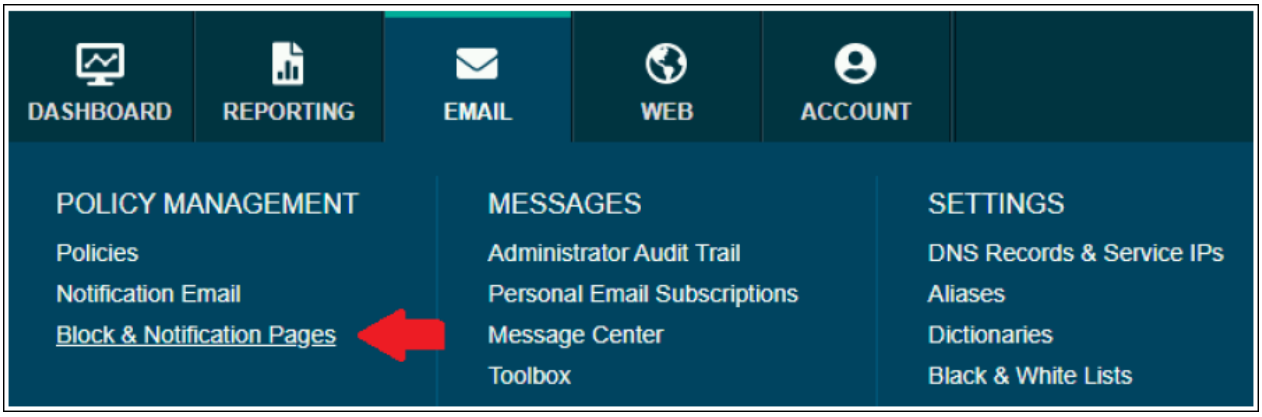
Before beginning the configuration, ensure that Forcepoint Email Security can successfully block suspicious and uncategorized websites. The standard Suspicious Link message will appear like:



Customize the Block and Notification Pages

Steps

1) To begin, go to **Email** and **Block & Notification Pages**:



2) Expand the **URL Sandboxing** section, browser isolation is best used with the **Prompt for Analysis** and **Uncategorized URL** notification pages.

3) Click **HTML Editing**.

4) Edit the code to add the ability to send the URL environment variable to Forcepoint RBI. Here is a sample reference code. Replace <yourrbiaddress> with your Forcepoint RBI URL.

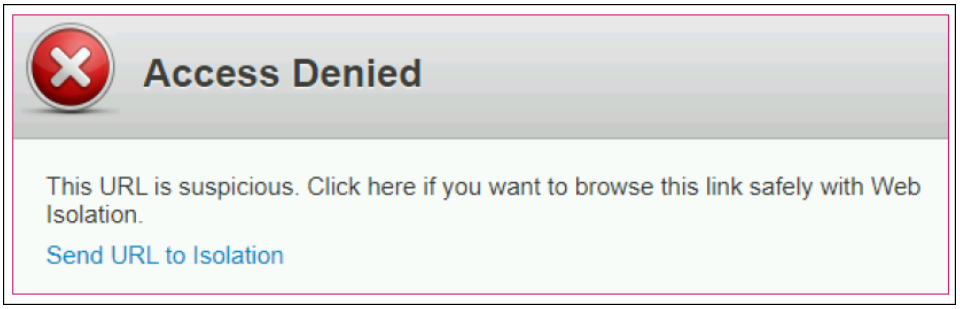
```
<!DOCTYPE html public "-//W3C//DTD HTML 4.0 Transitional//en" "http://www.w3.org/TR/html4/
loose.dtd">
_TEMPLATE_BLOCK_PAGE_HTML_TAG_
<head>
   <meta charset="utf-8"/>
   <base href="_PROTOCOL_://_PORTAL_HOST_NAME_">
   _TEMPLATE_BLOCK_PAGE_META_VIEWPOINT_
   _TEMPLATE_BLOCK_PAGE_HEAD_JS_
   <link 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 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">Access Denied</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">
               <img id="title_icon" src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/
notification-pages/icons60/error.png" height="60_" width="60_" class="editable image
 zzNOTIFICATION_ICONxxIMAGEzz" />
               <span id="notify-title" class="editable text zzNOTIFICATION_TITLExxTEXTzz"
 >Access Denied</span>
               <div id="titleBlink"></div>
```

5) Code continues..

```
</div>
            <div class="notify-box">
               <div id="notify-content" class="editable block zzNOTIFICATION_CONTENTxxBLOCKzz">
                  <div class="row">
                     <div class="span9 explanation">This URL is suspicious. Click here if you
 want to browse this link safely with Web Isolation.</div>
                  </div>
                  <div class="row">
                     <div class="span9 explanation"><a
                      href=https://<yourrbiaddress>/loader?
tenantId=<my_tenant_id>&url=_EEPP_FULL_URL_>Send URL to Isolation </a>
                     </div>
                  </div>
               </div>
            </div>
            <div class="" id="footerRow" >
               <div id="footer" class="">
                  <img src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/notification-
pages/2020/notification_page_logo_145x35.png" height="35" width="145" id="bottom-logo"
 class="editable image zzNOTIFICATION_BOTTOM_LOGOxxIMAGEzz"/>
                  <span id="footer-text" class="editable text zzNOTIFICATION_FOOTERxxTEXTzz"
 ></span>
                  <div class="clear-float"></div>
               </div>
               <div class="clear-float"></div>
            </div>
         </div>
      </div>
   </div>
   <div class="clear-float"></div>
   <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/notification-pages/empty.js"></
script>
   <!--[if !(IE 6)]>
   <script src="_PROTOCOL_://_ASSETS_HOST_NAME_/http-resources/notification-pages/
respond.src.js"></script>
   <![endif]-->
   <!-- __DEBUG_INFO__ -->
</body>
</html>
```

6) Click **Save**.

7) Click **Preview** to verify that the HTML code is valid.



The link will not work in Preview mode as it requires an actual website URL to be sent from Forcepoint. Send an email through Forcepoint Email Security with a URL that will be detected as suspicious to trigger the response page. Clicking the link on the actual response page will launch the rewritten URL and send the original URL to browser isolation for safe viewing.

8) To restore the block page back to the original, click on **Revert to Default** and then click **Save**.

Configuring the URL Override for Forcepoint Email Security On-Premises

Forcepoint RBI communicates with Forcepoint Email Security using URL rewriting to provide isolation-based zero-day malware protection.

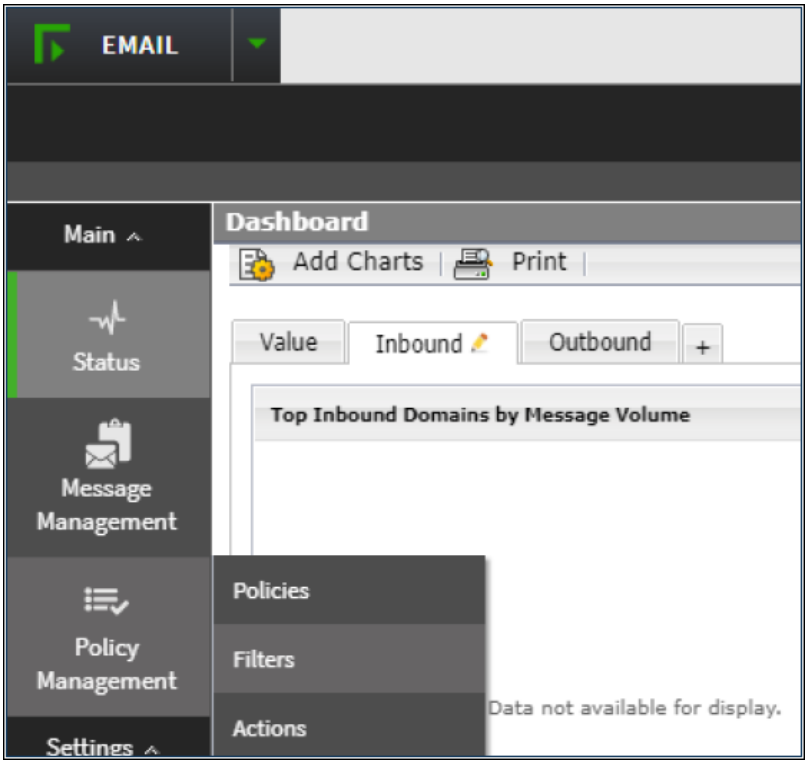
Initial Configuration in the Forcepoint Security Manager

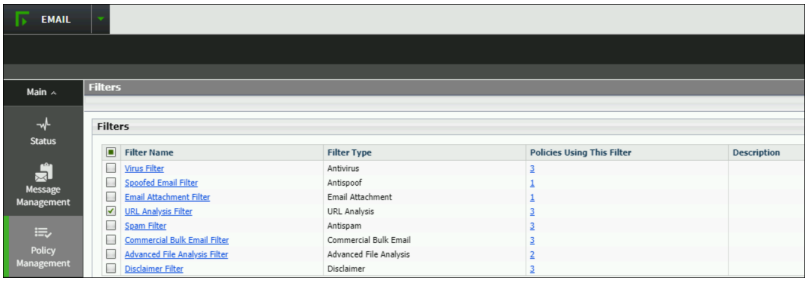
Before beginning this configuration, ensure that Forcepoint Email Security URL Analysis blocking is functional.

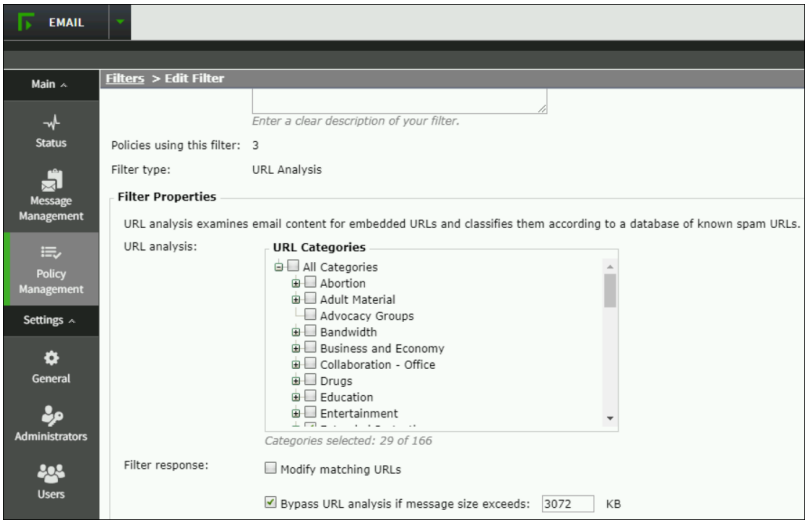
Steps

1) Sign in to the **Forcepoint Security Manager** and open the **EMAIL** module.

2) Go to **Policy Management - Filters - URL Analysis filter**.





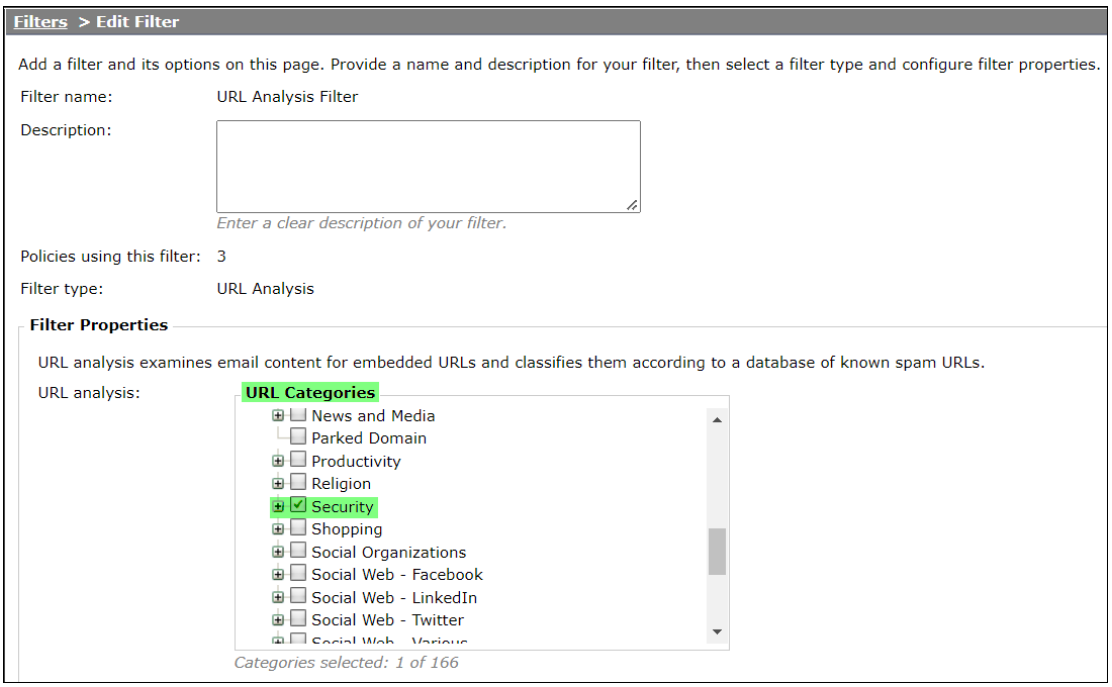


Configure the rewrite URLs for RBI redirection

Select the **Security** URL Category to ensure risky URLs are sent to Forcepoint RBI for isolation.

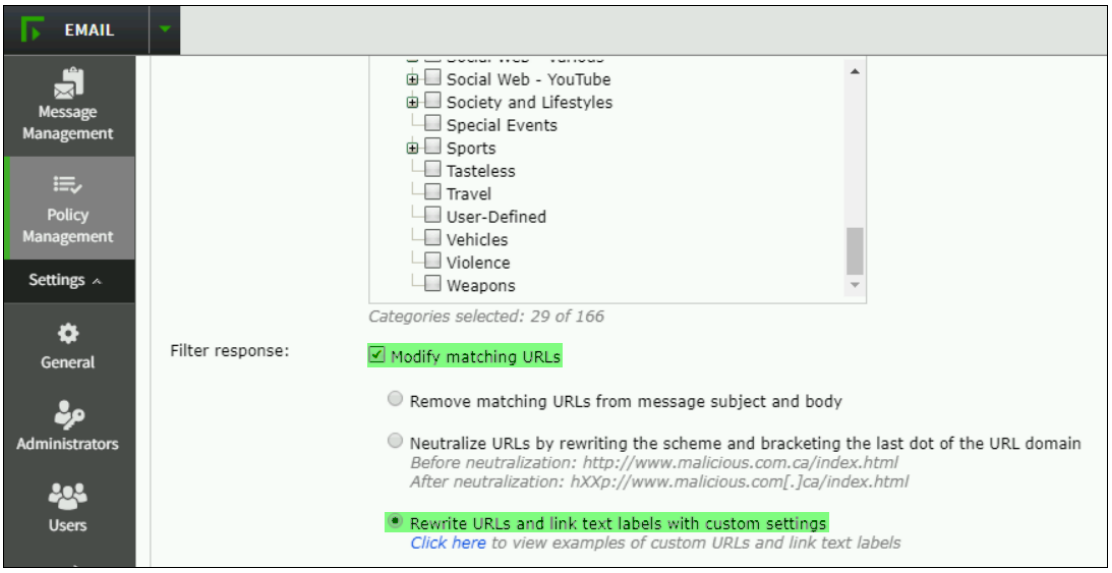
Steps

1) Select **Security** under **URL Categories**.



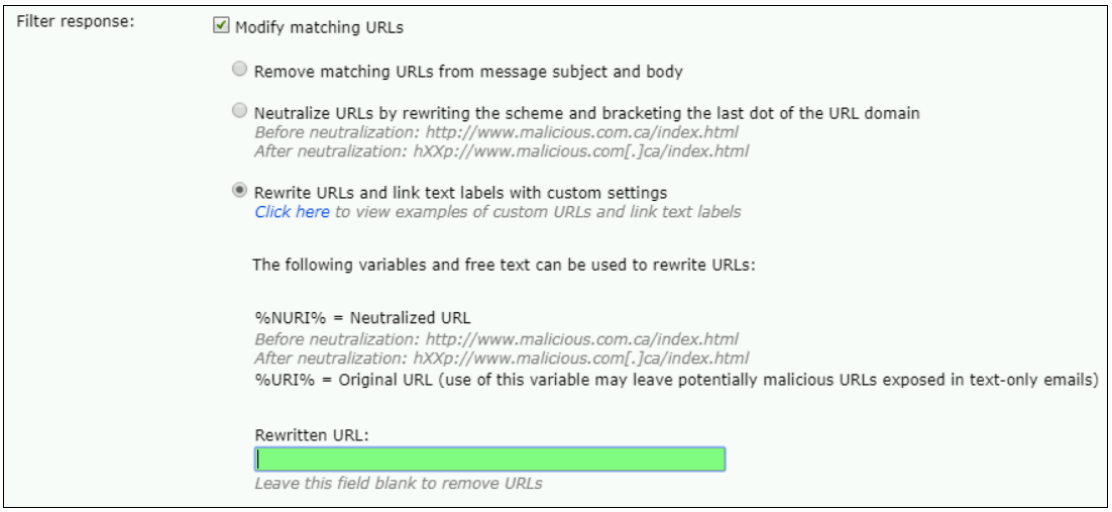
2) Select **Modify matching URLs**.

3) Select **Rewrite URLs and link text labels with custom settings**.

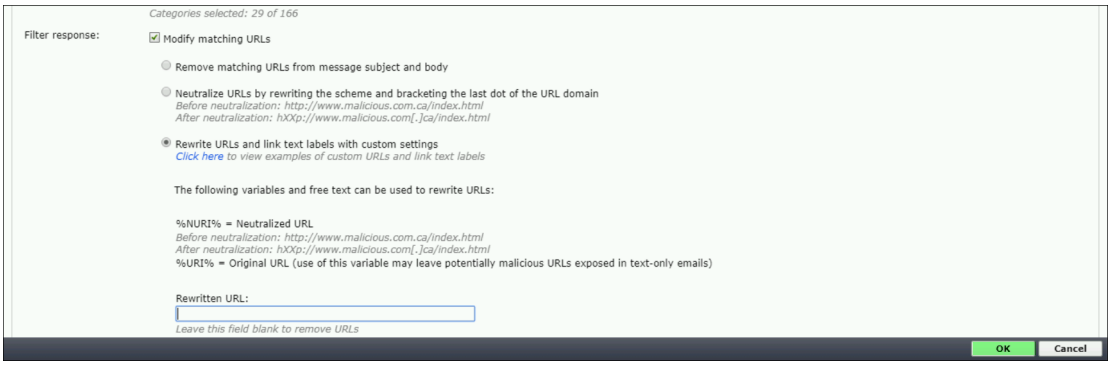


4) In the **Rewritten URL** field, enter the Neutralized URL and the parameter &url=%URI%.

An example for full URL: `https://<mycompany>.rbi.forcepoint.net/loader?tenantId=<my_tenant_id>&url=%URI%`



5) Click **OK**.

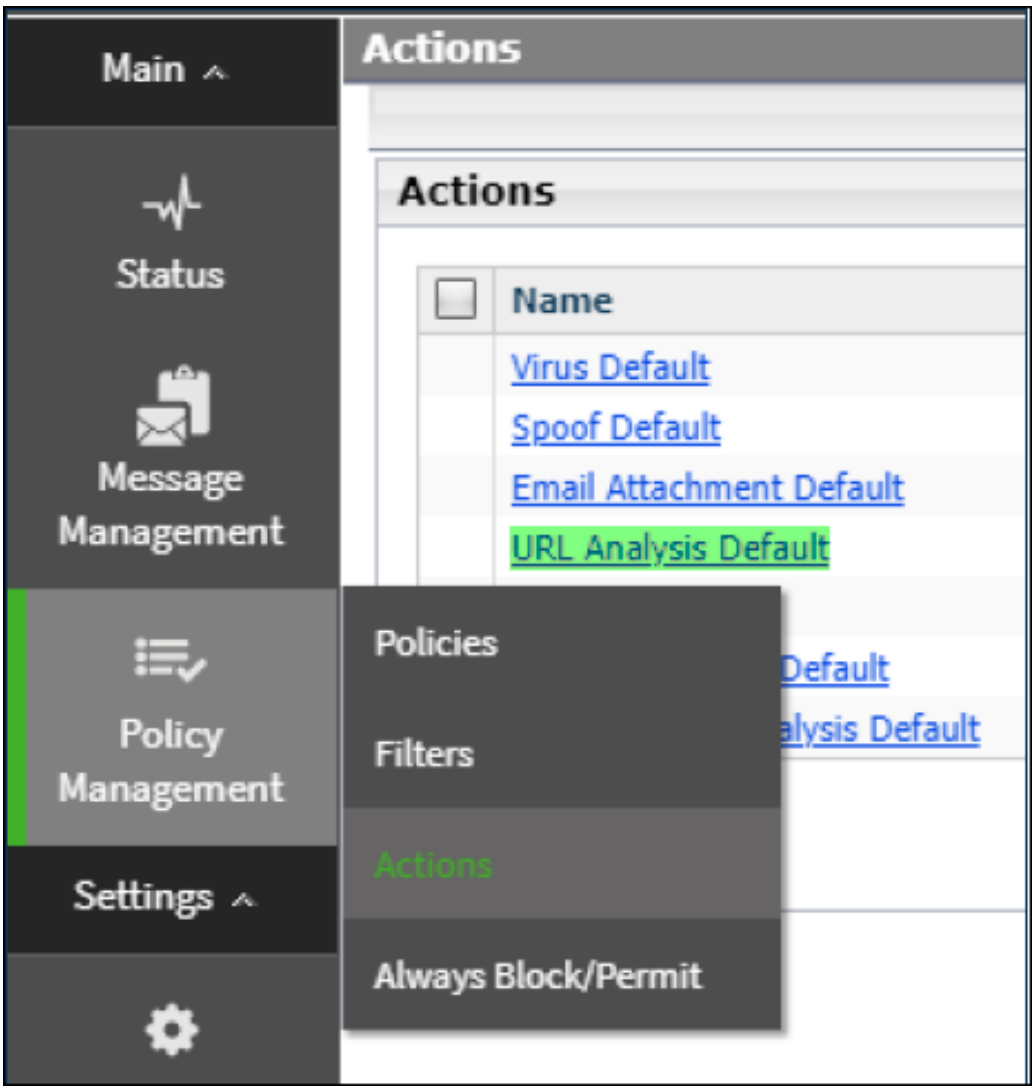


Now any URLs matching **Security** are rewritten with a URL that will send the original URL to Forcepoint RBI.

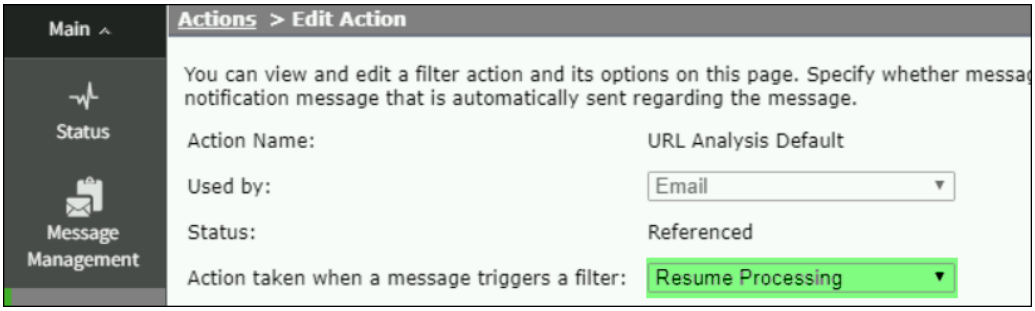
Configure the URL Analysis Action

Steps

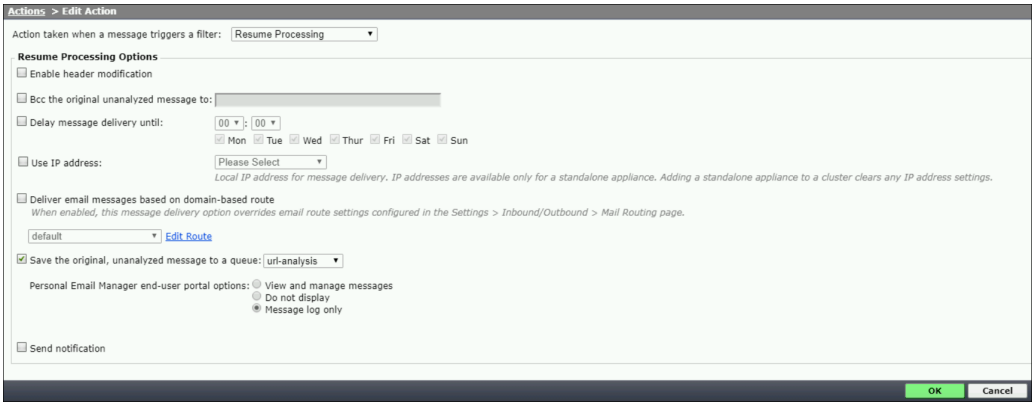
1) Go to **Policy Management - Actions - URL Analysis Default**.



2) Set **Action taken when a message triggers a filter** to **Resume Processing**.



3) Click **OK**.

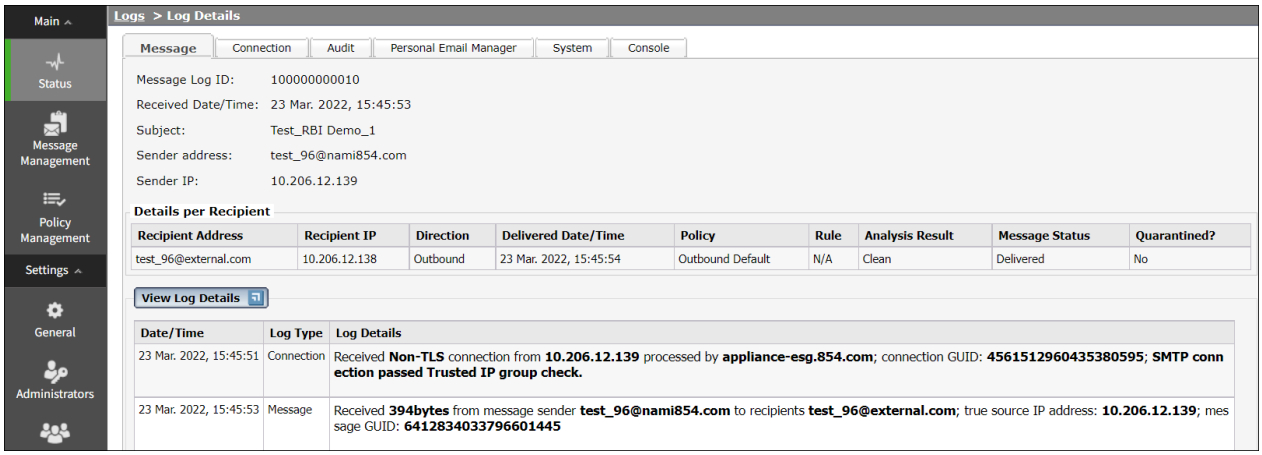


This action will send the email with the rewritten URL to the recipient.

Testing Redirect Links

To test the configuration, send an email through Forcepoint Email Security with a URL that will match the condition for rewriting. The URLs matching the rewriting condition are sent to Forcepoint RBI when clicked on.

A corresponding record of the event can be found under **Status** - **Logs** - **Message** tab.



Configuring the redirect for Forcepoint NGFW

Forcepoint Next Generation Firewall (Forcepoint NGFW) customers configure the redirect in the Forcepoint NGFW Security Management Center (SMC).

There are two options to redirect user web traffic to Forcepoint RBI:

- Confirmation user response: This option requires that the user confirm the web traffic redirect. When Forcepoint NGFW detects web traffic to specific configured web categories, it opens a block page in the user's web browser. To view the website, the user clicks a confirmation button on the block page to redirect the web traffic through Forcepoint RBI.

- Automatic user response: This option redirects the web traffic without intervention by the user. When Forcepoint NGFW detects web traffic to specific configured web categories, it automatically directs the web traffic through Forcepoint RBI. There are no confirmation steps or block pages in this option.

Enable TLS decryption for the Forcepoint NGFW engine

If the Forcepoint NGFW user response will redirect HTTPS websites to Forcepoint RBI, then enable TLS decryption.

This is a high-level procedure to add the CA certificate. For more detailed information about TLS decryption on Forcepoint NGFW, see the *Forcepoint NGFW Product Guide* on the Forcepoint Customer Hub for your version of Forcepoint NGFW.

Steps

1) Open the Forcepoint NGFW engine properties in the management UI.
2) Browse to **Add-Ons/TLS Inspection** in the tree view.
3) Create or import a suitable CA certificate for TLS decryption. Add the certificate in the **Client Protection Certificate Authority** field.
4) Save the engine properties.
5) Import the selected CA certificate to your endpoints as a trusted CA.

Create a custom redirect user response for HTTP and HTTPS websites in Forcepoint NGFW

If you want your users to see a block page and click a link to open the remote browser when they navigate to HTTP and HTTPS websites, then create a new custom user response in Forcepoint NGFW.

For more information about user responses in Forcepoint NGFW, see the *Forcepoint NGFW Product Guide* on the Forcepoint Customer Hub for your version of Forcepoint NGFW.

Steps

1) Sign in to Forcepoint NGFW Security Management Center (SMC).
2) Select **Configuration**.
3) Expand the **Other Elements** branch, then select **Engine Properties**.
4) Right-click **User Responses**, then select **New User Response.**

5) In the **Name** field, enter **Forcepoint Remote Browser Isolation**.

6) Expand **Connection Discarded by Access Rule**.

7) For **Type of Response**, select **Custom HTML**.

8) Paste the following HTML content:

```
<!DOCTYPE html>

<head>
    <title>Connection Not Allowed</title>
</head>

<body>
    <h1>Connection Not Allowed</h1>
    <p style="line-height:1.5;">The connection was not allowed by the corporate security
 policy.
        <br><br>For more information, contact your helpdesk and provide the following
 details:
        <br><br>Source IP Address: <b>{{SrcIP}}</b><br>Destination IP Address:
        <b>{{DstIP}}</b><br>URL: <b>{{Url}}</b><br>URL Category: <b>{{UrlCategory}}</
b><br>Application: <b>{{Application}}</b><br>Rule: <b>{{RuleTag}}</b></p>
    <p>
        <button id="redirect_button">Proceed with RBI</button>
        <script>
            document.getElementById("redirect_button").onclick = function() {
                let tenantId = "<replace with actual tenant ID>"
                let company = "<replace with company part of RBI url>"
                let rbiBaseUrl = ".rbi.forcepoint.net/loader"
                let tenantIdParam = "TenantID=" + tenantId
                let url = "url={{Url}}"
                let user = "X-Authenticated-User={{User}}"
                let urlParamsB64 = "SD=" + btoa(tenantIdParam + "&" + url + "&" + user)
                let rbiRedirUrl = "https://" + company + rbiBaseUrl + "?" + urlParamsB64
                location.replace(rbiRedirUrl)
            };
        </script>
    </p>
</body>

</html>
```

9) Update the company, tenant ID, and username in the URL:

- `<replace with company part of RBI url>`: Required: This information can be found in your fulfillment email and in the Forcepoint RBI Admin Portal.
- `<replace with actual tenant ID>`: Required. This information can be found in your fulfillment email and in the Forcepoint RBI Admin Portal.
- `X-Authenticated-User={{User}}`: Optional. If the username information is removed from the URL, then the username is not recorded in Forcepoint RBI metrics and reports.

Note

If the user response HTML includes `X-Authenticated-User={{User}}`, but the username is not known by Forcepoint NGFW, then the redirected browser connection will show as user **N/A** in the Forcepoint RBI Admin Portal.

10) Expand **URL Not Allowed**.

11) For **Type of Response**, select **Custom HTML**.

12) Copy and paste the same HTML content as mentioned in Step 8.

13) Click **OK**.

Next steps

After you edit the user response, you need to assign it to the web categories in the policy.

Create a custom auto-redirect user response for HTTP and HTTPS websites in Forcepoint NGFW

If your users do not need to see the block page, create a user response to send the HTTP and HTTPS web requests to browser isolation automatically.

For more information about user responses in Forcepoint NGFW, see the *Forcepoint NGFW Product Guide* on the Forcepoint Customer Hub for your version of Forcepoint NGFW.

Steps

1) Sign in to Forcepoint NGFW Security Management Center (SMC).

2) Select **Configuration**.

3) Expand the **Other Elements** branch, then select **Engine Properties**.

4) Right-click **User Responses**, then select **New User Response.**

5) In the **Name** field, enter **Forcepoint Remote Browser Isolation**.

6) Expand **Connection Discarded by Access Rule**.

7) For **Type of Response**, select **Custom HTML**.

8) Paste the following HTML content:

```
<!DOCTYPE html>
<script>
    let tenantId = "<replace with actual tenant ID>"
    let company = "<replace with company part of RBI url>"
    let rbiBaseUrl = ".rbi.forcepoint.net/loader"
    let tenantIdParam = "TenantID=" + tenantId
    let url = "url={{Url}}"
    let user = "X-Authenticated-User={{User}}"
    let urlParamsB64 = "SD=" + btoa(tenantIdParam + "&" + url + "&" + user)
    let rbiRedirUrl = "https://" + company + rbiBaseUrl + "?" + urlParamsB64
    location.replace(rbiRedirUrl)
</script>

</html>
```

9) Update the company, tenant ID, and username in the URL:

- `<replace with company part of RBI url>`: Required: This information can be found in your fulfillment email and in the Forcepoint RBI Admin Portal.
- `<replace with actual tenant ID>`: Required. This information can be found in your fulfillment email and in the Forcepoint RBI Admin Portal.
- `X-Authenticated-User={{User}}`: Optional. If the username information is removed from the URL, then the username is not recorded in Forcepoint RBI metrics and reports.

Note

If the user response HTML includes `X-Authenticated-User={{User}}`, but the username is not known by Forcepoint NGFW, then the redirected browser connection will show as user **N/A** in the Forcepoint RBI Admin Portal.

10) Expand **URL Not Allowed**.

11) For **Type of Response**, select **Custom HTML**.

12) Copy and paste the same HTML content as mentioned in Step 8.

13) Click **OK**.

Next steps

After you edit the user response, you need to assign it to the web categories in the policy.

Create a rule to allow access to Forcepoint RBI

Depending on your firewall policy, you might need to add a rule to allow clients to access Forcepoint RBI using Port 443 (TCP).

Before you begin

Before you create the rule, create a custom TCP service named **rbi-streaming** with a Destination port **443**.

Depending on your Forcepoint RBI deployment type, you might need to create two rules: one rule to allow endpoints to access the Forcepoint RBI Admin Portal and one rule to allow endpoints to access the Forcepoint RBI remote container. Regardless of the deployment type, the endpoints need HTTPS and rbi-streaming access with the Forcepoint RBI service.

Steps

1) Sign in to Forcepoint NGFW Security Management Center (SMC).
2) Select **Configuration**.
3) Find your NGFW policy under the **Policies** branch and open it for editing.
4) On the **IPv4 Access** tab, add a new Access rule with the following values:
   - **Source**: Select an element matching the clients in your network intending to use Forcepoint RBI, or create a new element to represent them (such as **rbi-clients**).
   - **Destination**: *.rbi.forcepoint.com and *.rbi.forcepoint.net.
   - **Service**: **HTTPS** and the custom **rbi-streaming** service.
   - **Action**: Allow.
5) Save the policy.

Add the user response to a Forcepoint NGFW policy

Triggering the redirection to Forcepoint RBI requires two rules: one rule with a Continue action to trigger the user response and one rule blocking client access to specific URL categories.

This topic covers the procedure to create the rule with a Continue action and assign the user response to that rule, and the rule with a Discard action. For information about creating a rule (or rules) to block access to specific URL categories, see the *Forcepoint NGFW Product Guide* on the Forcepoint Customer Hub for your version of Forcepoint NGFW.

Steps

1) Sign in to Forcepoint NGFW Security Management Center (SMC).

2) Select **Configuration**.

3) Find your NGFW policy under the **Policies** branch and open it for editing.

4) On the **IPv4 Access** tab, add a new rule with the following values:
   - **Source**: Select an element matching the clients in your network intending to use Forcepoint RBI, or create a new element to represent them (such as **rbi-clients**).
   - **Destination**: **ANY**
   - **Service**: **HTTP** and **HTTPS (with decryption)**
   - **Action**: **Continue**

5) After the rule is created, right-click the **Action** cell for the rule, then select **Edit Options**.

6) On the **Select Rule Action Options** screen's **General** tab, turn **Deep Inspection** to **Off**.

7) On the **Response** tab, enable **Override Settings Inherited from Continue Rule(s)**, then click **Select**.

8) On the **Select User Response** screen, select the Forcepoint RBI redirect user response, then click **Select**.

9) On the policy's **IPv4 Access** tab, the new action information is shown in the **Action** cell for the selected rule.

10) Add a new rule after the Continue rule with the following values:
   - **Source**: Same as the Continue rule above.
   - **Destination**: **ANY**
   - **Service**: The **URL Category** where you want to apply the Forcepoint RBI redirect user response.
   - **Action**: **Discard**

11) Click **Save and Install** to install the policy to your Forcepoint NGFW engine.

Verify the redirect from Forcepoint NGFW

Verify that the browser session is isolated based on the redirect block page and configured policy.

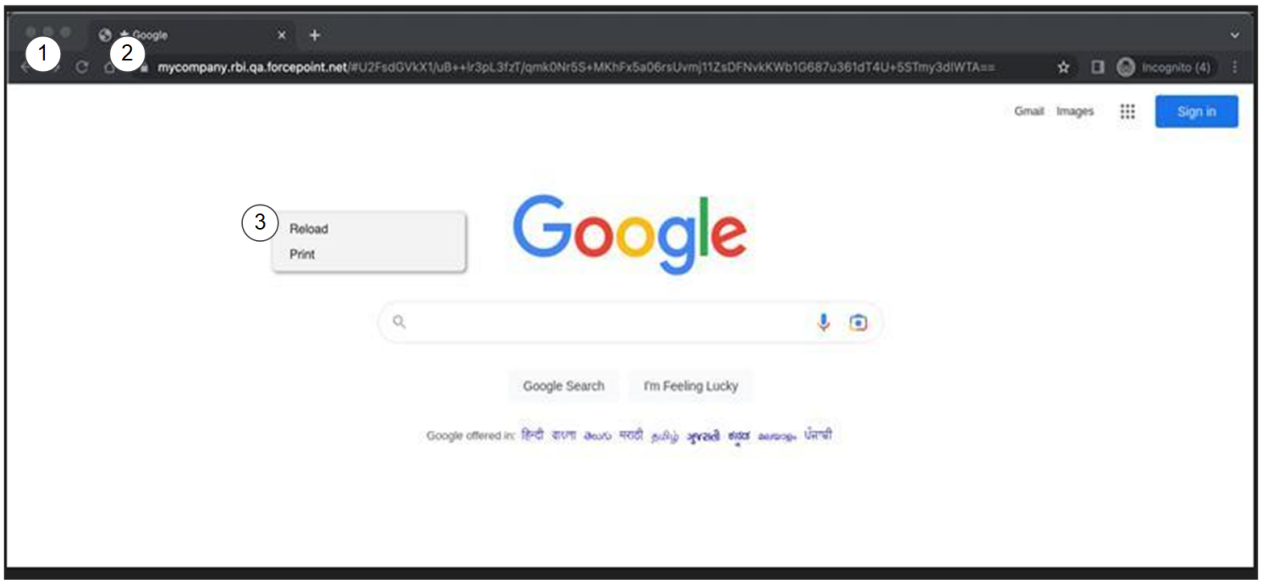
Steps

1) Open an HTML5 compatible browser and go to a webpage that should be blocked per the active policy in Forcepoint NGFW Security Management Center (SMC).

2) If you configured the default block page, click **You may continue using Browser Isolation**. This step is not needed if you created a custom auto-redirect block page.

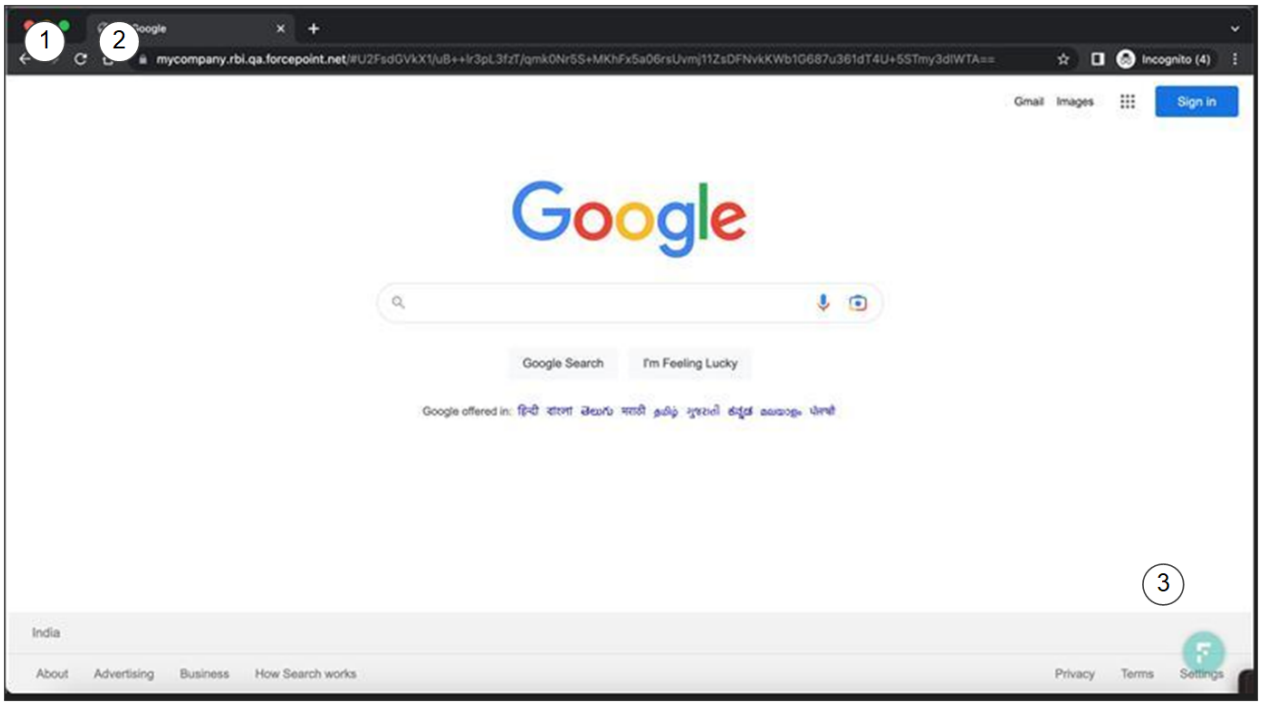
3) Verify that the browser session is going through the remote browser:

Secure Streaming:



1. Look for the star. The tab header for the webpage will display a star next to the webpage title.
2. The URL appears as `https://<mycompany>.rbi.forcepoint.net/viewer/#<Encrypted Actual URL>`. The isolated URL is encrypted to restrict user from manipulating the URL and bypassing any proxy restrictions. For more information, see URL Encryption on page 149.
3. Check the right-click menu. The right-click menu contains the options for the remote browser only: **Reload**, **Print**, and **Session Information**.

Secure Rendering:



1. Look for the star. The tab header for the webpage will display a star next to the webpage title.
2. The URL appears as `https://<mycompany>.rbi.forcepoint.net/viewer/#<Encrypted Actual URL>`. The isolated URL is encrypted to restrict user from manipulating the URL and bypassing any proxy restrictions. For more information, see URL Encryption on page 149.
3. Check the Forcepoint logo. A Forcepoint logo is visible at the bottom right corner of the browser

Configuring Forcepoint RBI (On-premises Deployment) in proxy chaining mode with Forcepoint Content Gateway for full isolation

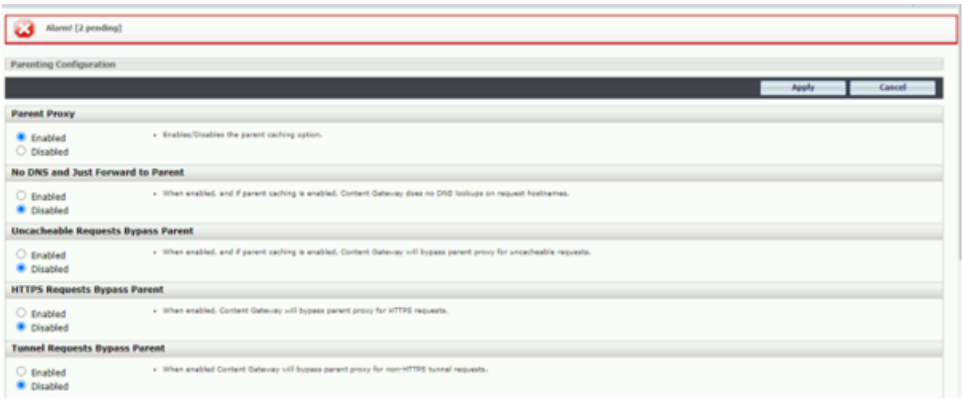
1) In this scenario, Content Gateway, a component of Forcepoint Web Security, is the upstream proxy for Endpoint and the Forcepoint RBI proxy is configured as the upstream proxy (parent proxy).

2) To enable proxy chaining, the Forcepoint RBI proxy component is deployed as part of the Forcepoint RBI deployment (See the Forcepoint RBI deployment guide to enable the Forcepoint RBI proxy.)

3) Before configuring proxy chaining, login to a Forcepoint RBI terminal session, navigate to `/var/nfs/squidfiles/rbi-proxy/` and locate the Forcepoint RBI Proxy Certificate.

4) Copy the certificate content from `squid-ca-cert-key.pem` and save it to the local machine in `.crt` format. It will later be added as Root CA in the Forcepoint Content Gateway Manager.

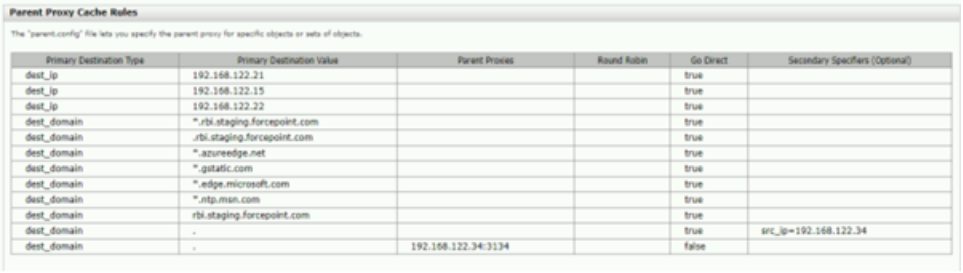
5) To configure proxy chaining for Content Gateway, open Forcepoint Content Gateway Manager.
   a) Select **Configure** > **Content Routing**
   b) Select **Hierarchies**.
   c) In the **Parent Proxy** section, select **Enabled**.
   d) Continue as indicated in the following screen shot.



6) Under **Parent Proxy Cache Rules**, configure the following.
   a) Content Gateway Manager, Forcepoint Security Manager, Forcepoint RBI Domain (Wildcard) to go Direct.
   b) azureedge.net, gstatic.com, edge.microsoft.com, ntp.microsoft.com to go Direct.

c) All traffic (*) with source IP of RBC Cluster Browsing Nodes to go Direct.

d) All traffic (*) to redirect to Forcepoint RBI Proxy as Parent Proxy.



Parent Proxy Cache Rules

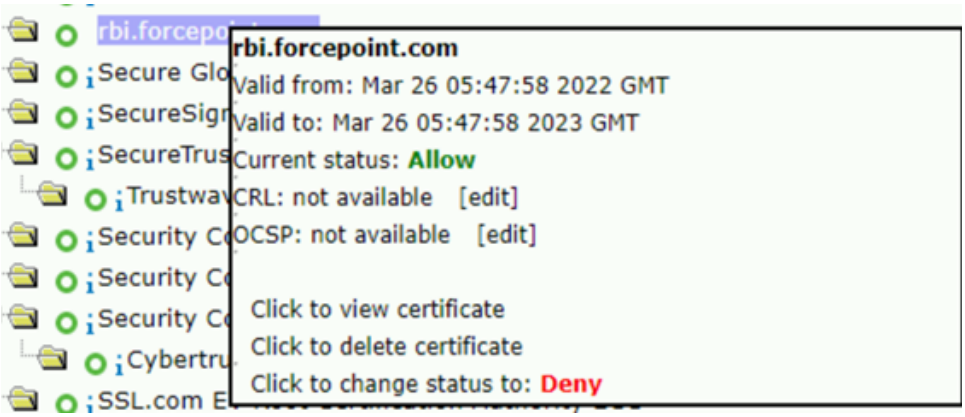
The "parent.config" file lets you specify the parent proxy for specific objects or sets of objects.

Primary Destination Type	Primary Destination Value	Parent Proxies	Round Robin	Go Direct	Secondary Specifiers (Optional)
dest_ip	192.168.122.21			true	
dest_ip	192.168.122.15			true	
dest_ip	192.168.122.22			true	
dest_domain	*.rbi.staging.forcepoint.com			true	
dest_domain	.rbi.staging.forcepoint.com			true	
dest_domain	*.azureedge.net			true	
dest_domain	*.gstatic.com			true	
dest_domain	*.edge.microsoft.com			true	
dest_domain	*.ntp.msn.com			true	
dest_domain	rbi.staging.forcepoint.com			true	
dest_domain	.			true	src_ip=192.168.122.34
dest_domain	.	192.168.122.34:3134		false	

7) Navigate to **Configure** > **SSL** > **Certificates** > **Add Root CA**.

a) Click on Choose file and select the Forcepoint RBI Proxy `.crt` file created earlier. Once the Root CA is added, it displays under Certificate Authorities.

b) Select the certificate that you have saved and change the status to **Allow**, as shown in the following image:



8) Login to the Forcepoint RBI Super admin Portal.

a) Go to **Organization**

b) Edit the respective Organization

c) Go to the **Proxy Details** section and disable URL redirection.

9) On the Forcepoint RBI Admin Portal.

a) Go to **My Organization**

b) Scroll down to the **Authentication** section.

c) Under **End user Authentication Level**, select **Authenticated under End user**.

10) Configure the endpoints with Proxy bypass to Forcepoint RBI RBC Cluster Browsing Nodes i.e., rbchost-192-168-122-34.rbi.forcepoint.net, rbchost-192-168-122-35.rbi.staging.forcepoint.com, etc.

When the configuration is complete, Forcepoint RBI can be used in a Proxy chaining mode for Full Isolation.

Note

Web URLs that are part of Desktop applications must be added to Forcepoint Content Gateway proxy bypass or configured in Parent Proxy Cache Rules to Go direct.

Configuring Forcepoint RBI (Cloud Deployment) in proxy chaining mode with Forcepoint Content Gateway for full isolation

The following steps provide a procedure to configure Forcepoint RBI cloud in proxy chaining mode for full isolation.

1) Cloud Ops team shares the Cloud RBI Proxy information via fulfillment email. The email contains the RBI proxy certificate to be installed in the Forcepoint Content Gateway Manager. The fulfillment email also includes Cloud RBI proxy host and port details.

2) Save the RBI proxy certificate to the local machine in `.crt` format and then, add the RBI proxy certificate as Root CA in the Forcepoint Content Gateway Manager.

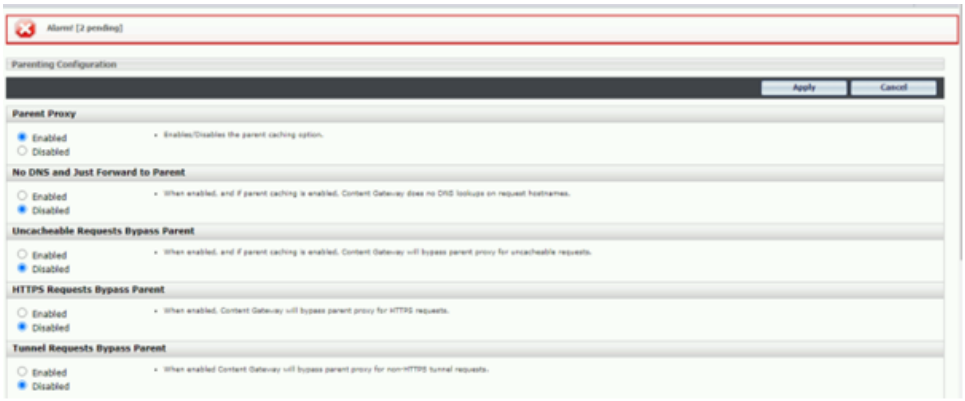
3) To configure proxy chaining for Content Gateway, open Forcepoint Content Gateway Manager and perform the following steps:

   a) Select **Configure** > **Content Routing**.

   b) Select **Hierarchies**.

   c) In the **Parent Proxy** section, select **Enabled**.

   d) Continue as indicated in the following screen shot.



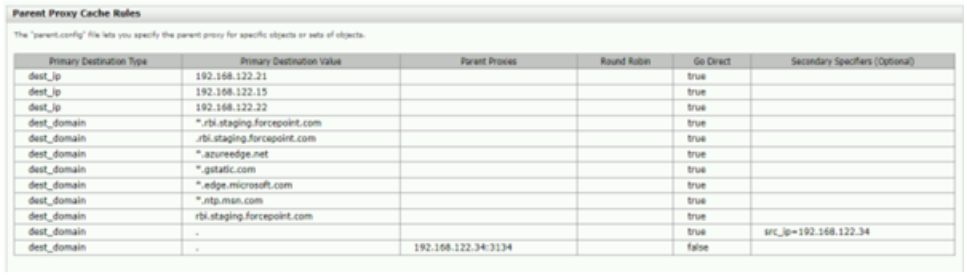
4) Under **Parent Proxy Cache Rules**, configure the following.

   a) Content Gateway Manager, Forcepoint Security Manager, Forcepoint RBI Domain (Wildcard) to go Direct.

   b) azureedge.net, gstatic.com, edge.microsoft.com, ntp.microsoft.com to go Direct.

   c) All traffic (*) with source IP of RBC Cluster Browsing Nodes to go Direct.

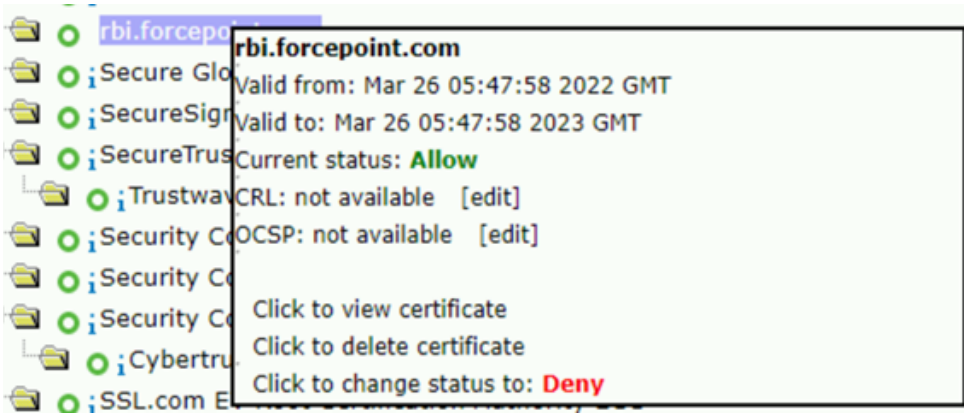
   d) All traffic (*) to redirect to Forcepoint RBI Proxy as Parent Proxy.



5) Navigate to **Configure** > **SSL** > **Certificates** > **Add Root CA**.

   a) Click on Choose file and select the Forcepoint RBI Proxy `.crt` file created earlier. Once the Root CA is added, it displays under Certificate Authorities.

   b) Select the certificate that you have saved and change the status to **Allow**, as shown in the following image:

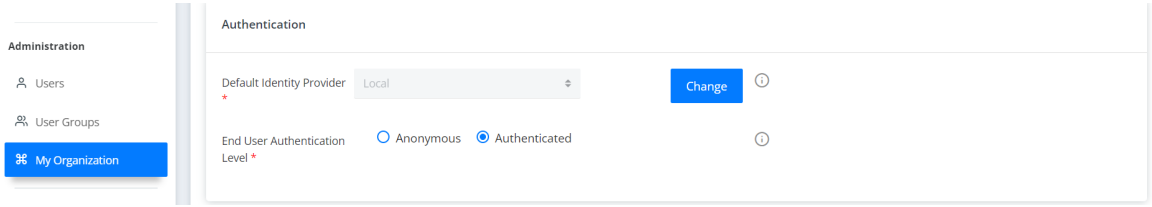


6) On the Forcepoint RBI Admin Portal.

   a) Go to **My Organization**

   b) Scroll down to the **Authentication** section.

   c) In **End user Authentication Level**, select **Authenticated**.



When the configuration is complete, Forcepoint RBI can be used in a Proxy chaining mode for Full Isolation.

Note

Web URLs that are part of Desktop applications must be added to Forcepoint Content Gateway proxy bypass or configured in Parent Proxy Cache Rules to Go direct.

Integrating Forcepoint DLP with RBI

Forcepoint DLP can be integrated with RBI to have Forcepoint DLP policies applied while browsing in isolation.

Integrating On-premises Forcepoint RBI and Forcepoint DLP for File upload use case

Configuration steps for Integrating Forcepoint On-premises Proxy and Forcepoint DLP (Onbox Integration) with On-premises Forcepoint Remote Browser isolation in Proxy chaining mode for Forcepoint DLP for File uploads use case.

Following points must be considered, before you begin working the configuration steps:

1) Proxy chaining should be configured between Forcepoint On-premises Proxy, Forcepoint DLP (Onbox Integration), and Forcepoint RBI. Refer section *Configure Forcepoint RBI (On-premises Deployment) in Proxy chaining mode with Forcepoint WSG for Full isolation* to configure proxy chaining between Forcepoint On-premises Proxy and Forcepoint Remote browser isolation. Also, in this scenario Forcepoint On-premises Proxy and DLP (Onbox integration) will be configured as downstream proxy to RBI.

2) Ensure that the Forcepoint RBI proxy component is deployed as part of Forcepoint RBI deployment. For details refer the Forcepoint RBI On-premises deployment guide to deploy the Forcepoint RBI component.

3) This integration requires enabling TLS 1.2 on Forcepoint RBI. Forcepoint RBI is by default configured with TLS 1.3.

4) To enable TLS 1.2 on Forcepoint RBI, follow below steps. Login to respective clusters Master to run below steps.

   a) Uninstall ingress from Forcepoint RBI.

   Note

   If there are 2 separate clusters configured for Forcepoint RBI admin portal and RBC Cluster, follow the steps on both the clusters.

   ```
   helm uninstall ingress-nginx -n ingress-nginx
   ```

   b) Install Ingress.

   ```
   helm install ingress-nginx ingress-nginx/ingress-nginx -n ingress-nginx --version 3.35.0
   ```

   c) Patch Ingress

   ```
   kubectl patch svc -n ingress-nginx ingress-nginx-controller -p '{"spec": {"type":
    "NodePort", "externalIPs":["IP_Address_of_the_Master"]}}'
   ```

5) SSL decryption bypass for rbi domain for e.g., *.rbi.forcepoint.net should not be set in the Forcepoint Security Manager. For On premises DLP-RBI integration it is required that the HTTPS traffic to RBI is not bypassed for SSL decryption.

6) Proxy bypass should be configured for RBC cluster nodes FQDNs. For e.g., rbchost-192-168-122-1.rbi.forcepoint.net, rbchost-192-168-122-2.rbi.forcepoint.net.

Related concepts

Configuring Forcepoint RBI (On-premises Deployment) in proxy chaining mode with Forcepoint Content Gateway for full isolation on page 42

DLP Policy visibility and control for File Uploads

Forcepoint DLP is known the world over as the industry leading Data Loss Protection solution. With Proxy chaining, Forcepoint RBI sessions provide the visibility for Monitoring and Protection of DLP File Upload Policies.

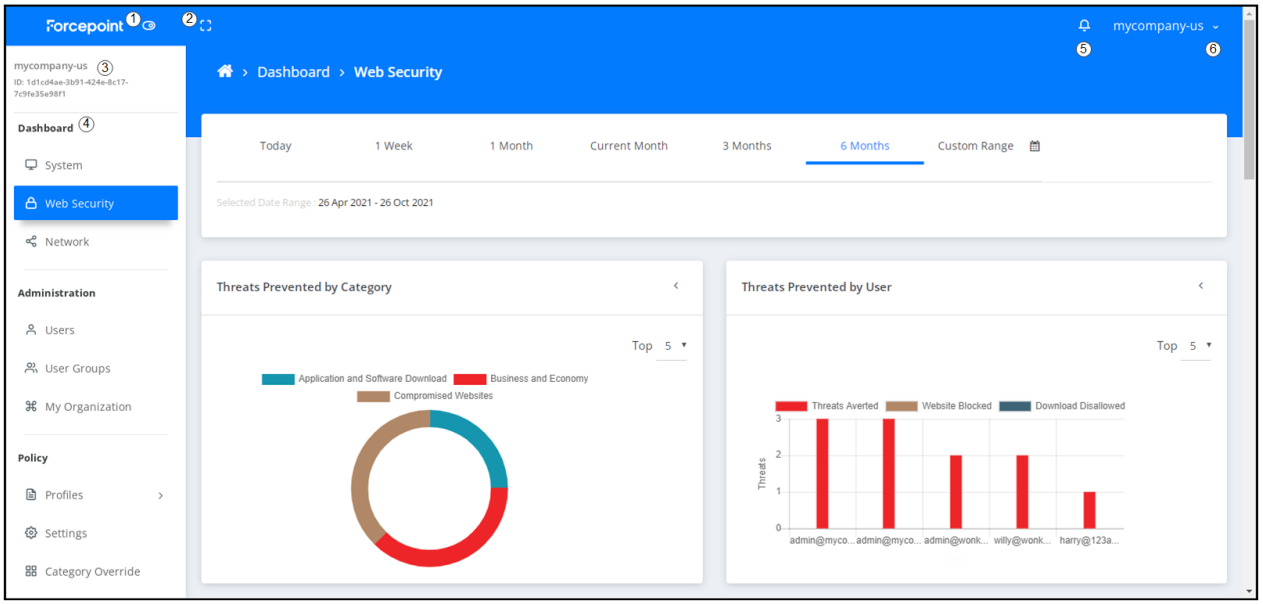
On setups, that have the DLP agent installed on endpoints, while browsing in isolation, if an effort is made to upload a file containing sensitive content, then the DLP policy will be automatically applied for such file uploads.

Chapter 3

The Forcepoint RBI Admin Portal

Contents

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 RBI.
   - **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.

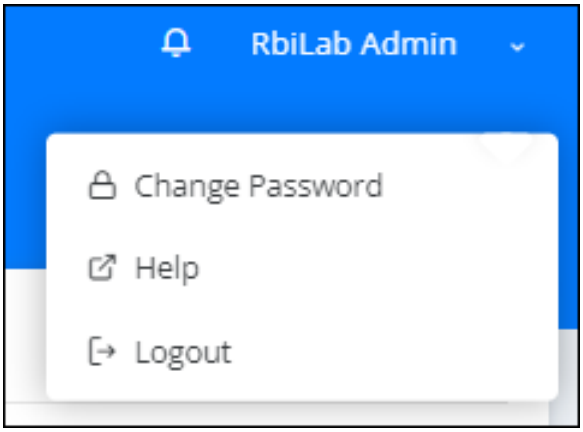
Changing your password

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

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

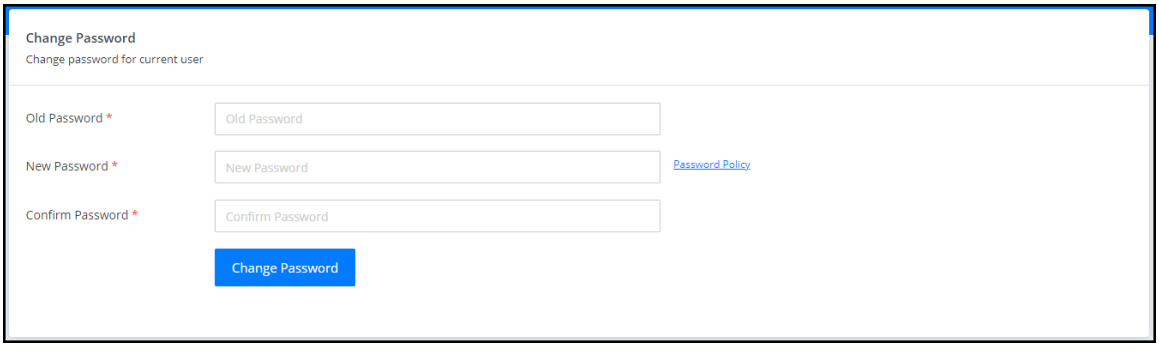
2) At the top of the Admin Portal, click the user name to open the user menu.



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.



6) Click **Change Password**.

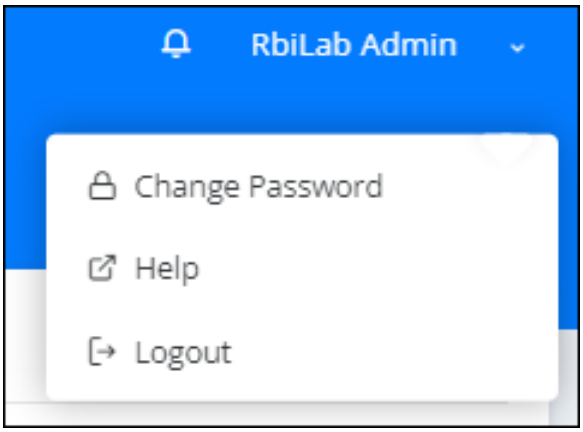
Help

The Forcepoint RBI help guide can be accessed through the user menu at the top of the Admin Portal.

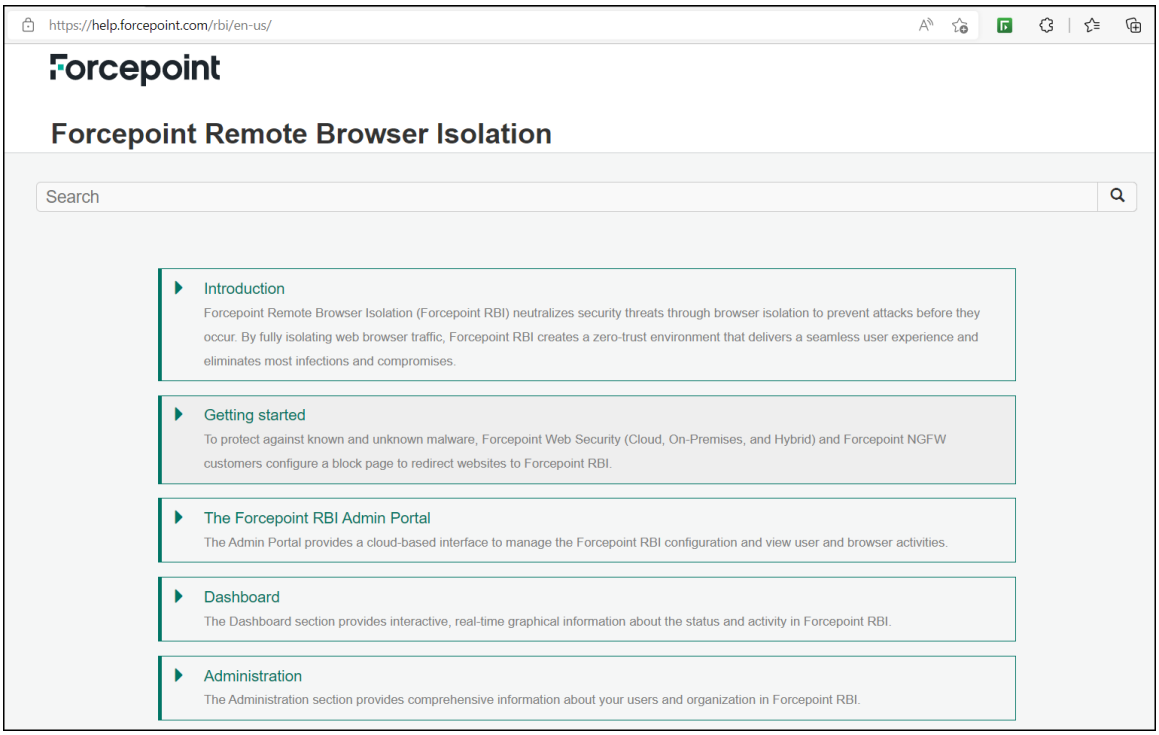
Steps

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 **Help** to open the Forcepoint RBI help guide.

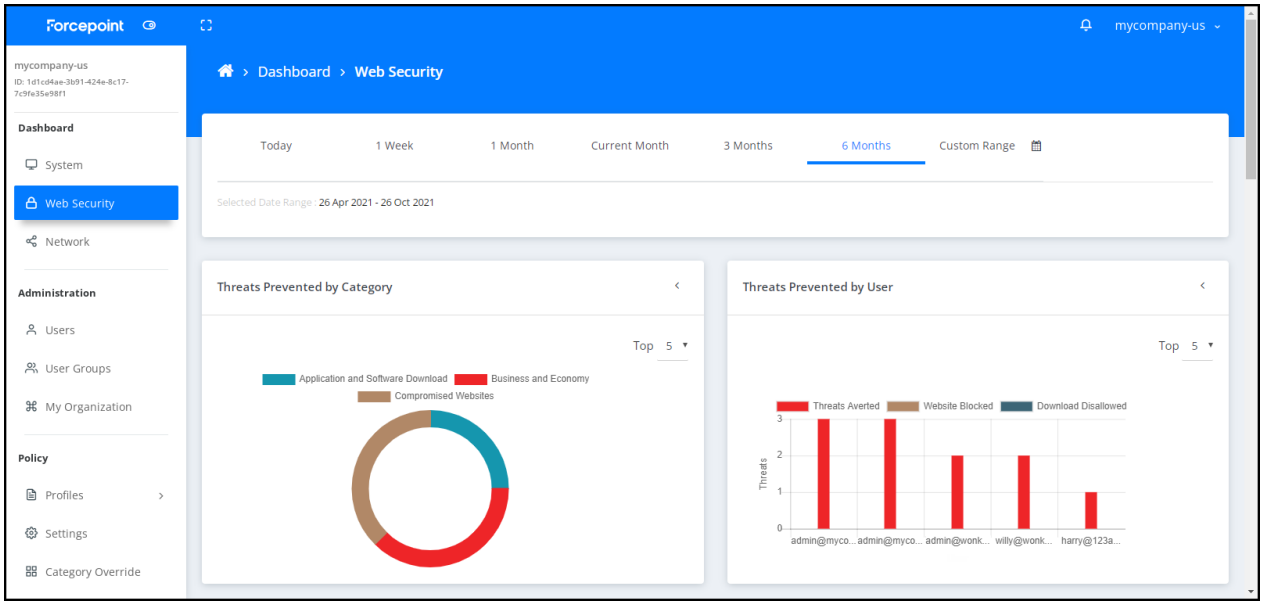


Chapter 4

Dashboard

Contents

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.

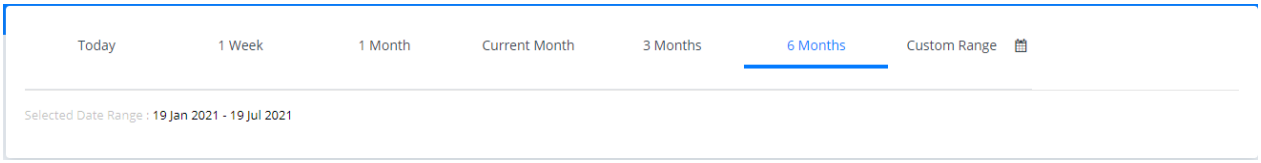
Common navigation elements

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.

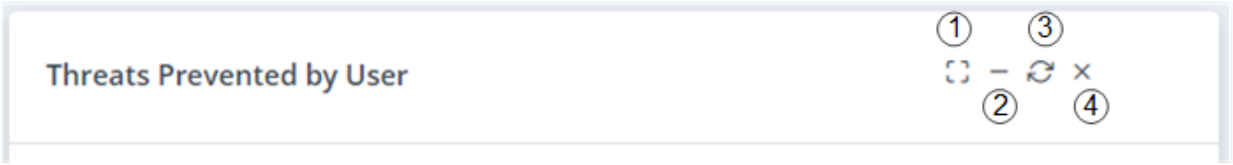


- Today: Shows metrics for the current date.
- 1 Week: Shows metrics for the past week from the current date.
- 1 Month: Shows metrics for the past month from the current date.
- Current Month: Shows metrics from the first day of the current month to the current date.
- 3 Months: Shows metrics for the 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.

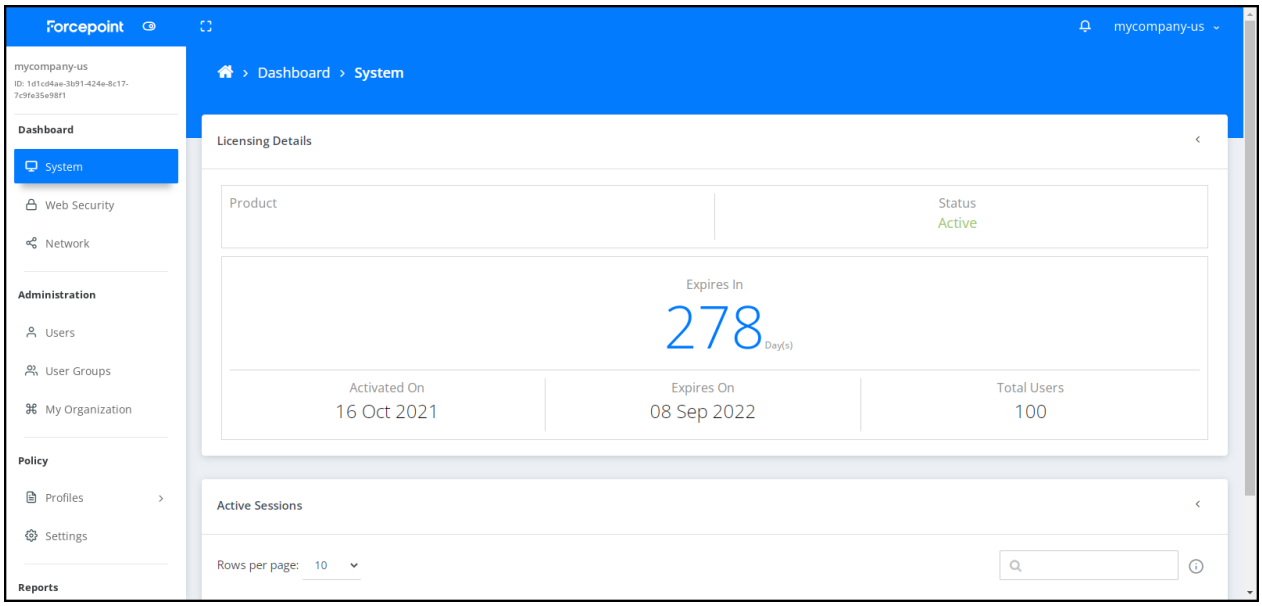
To open the menu, click the < icon in the top-right corner of the widget:



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 sessions.



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.
License	(On-Premises Forcepoint RBI only) Enter or update the License key provided by Forcepoint when you purchase or renew a license.

Update the license key

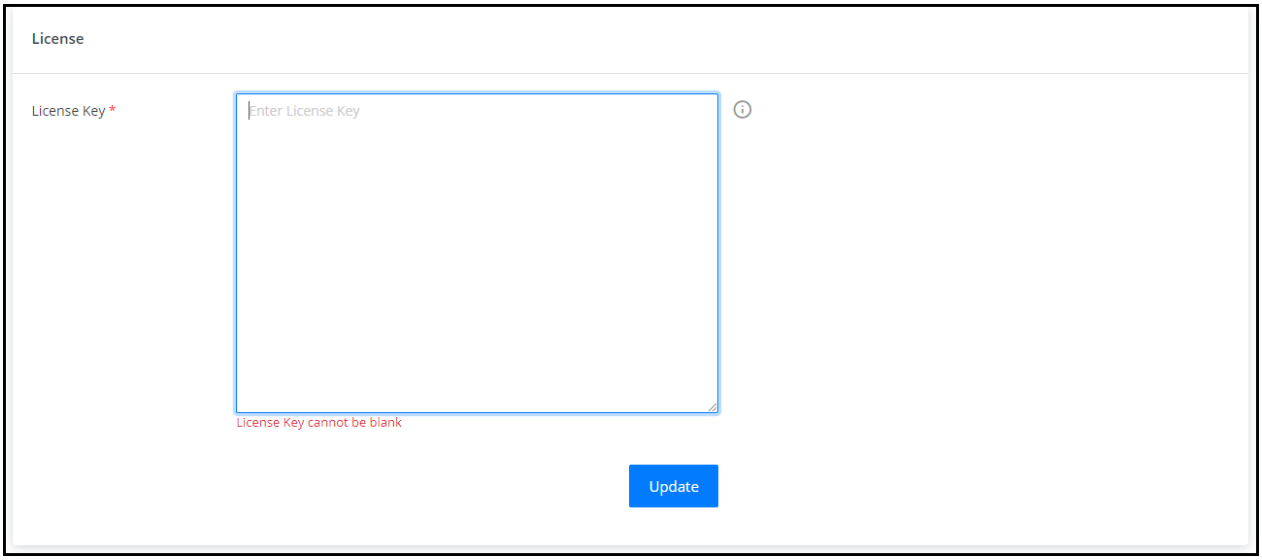
For on-premises Forcepoint RBI deployments only. If you have purchased or upgraded your license, update the license key on the System dashboard.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Dashboard** > **System**.

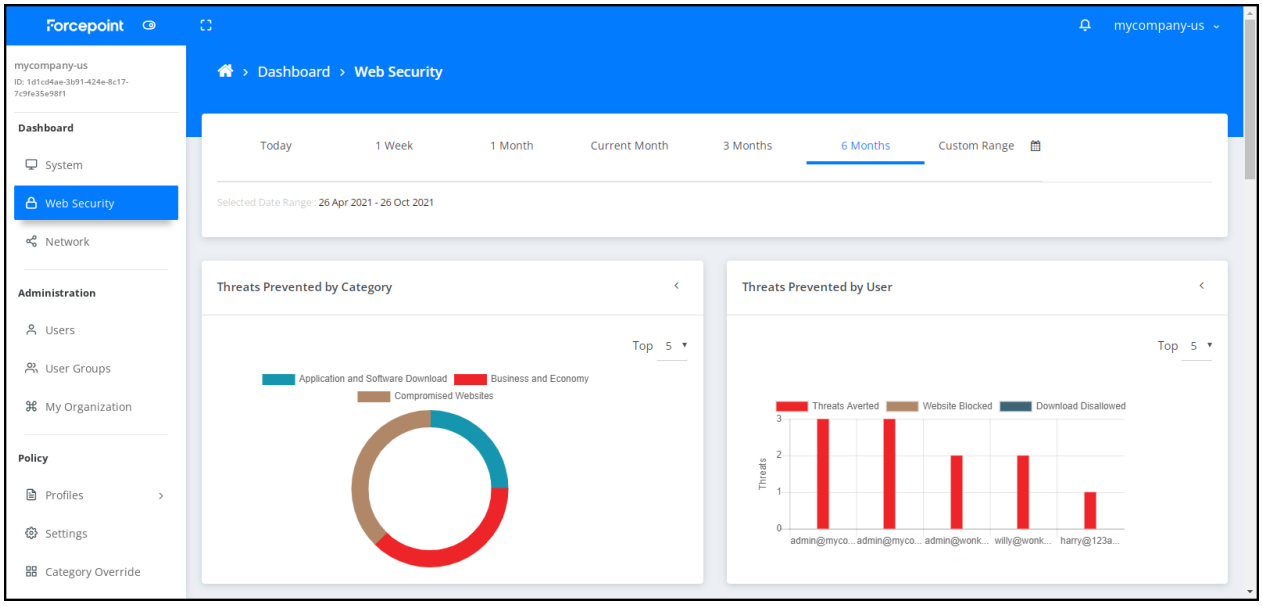
3) Go to the **License** section.



4) Enter the license key, then click **Update**.

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
Threats Prevented by Category	Shows information about the threats prevented for each threat category. By default, the categories are defined in the Forcepoint Threat Intelligence Service (FTIS), which is enabled under Policy Settings.

Widget	Description
Threats Prevented by User	Shows information about the threats prevented per user. The users are defined under the Administration section in the left navigation menu.
Security Threat Summary	Shows information for all browsed sites where the threat score exceeded the allowable level set by the administrator. By default, the categories are defined in the Forcepoint Threat Intelligence Service (FTIS), which is enabled under Policy Settings.
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 CDR conversion or malware scanning check (blocked).
Upload Summary	Shows the count for all file types that were either uploaded successfully by the user (allowed) or were not uploaded when the file failed the CDR conversion, or DLP policy is enforced (blocked).
Browse Activity Summary	Shows the cumulative browsing activity and security events per user.
Web Security Summary	Shows the page protection metrics for isolated web pages.

View metrics for threats prevented per category

The **Threats Prevented by Category** panel shows the number of threats prevented for each category. The categories are defined in the policy.

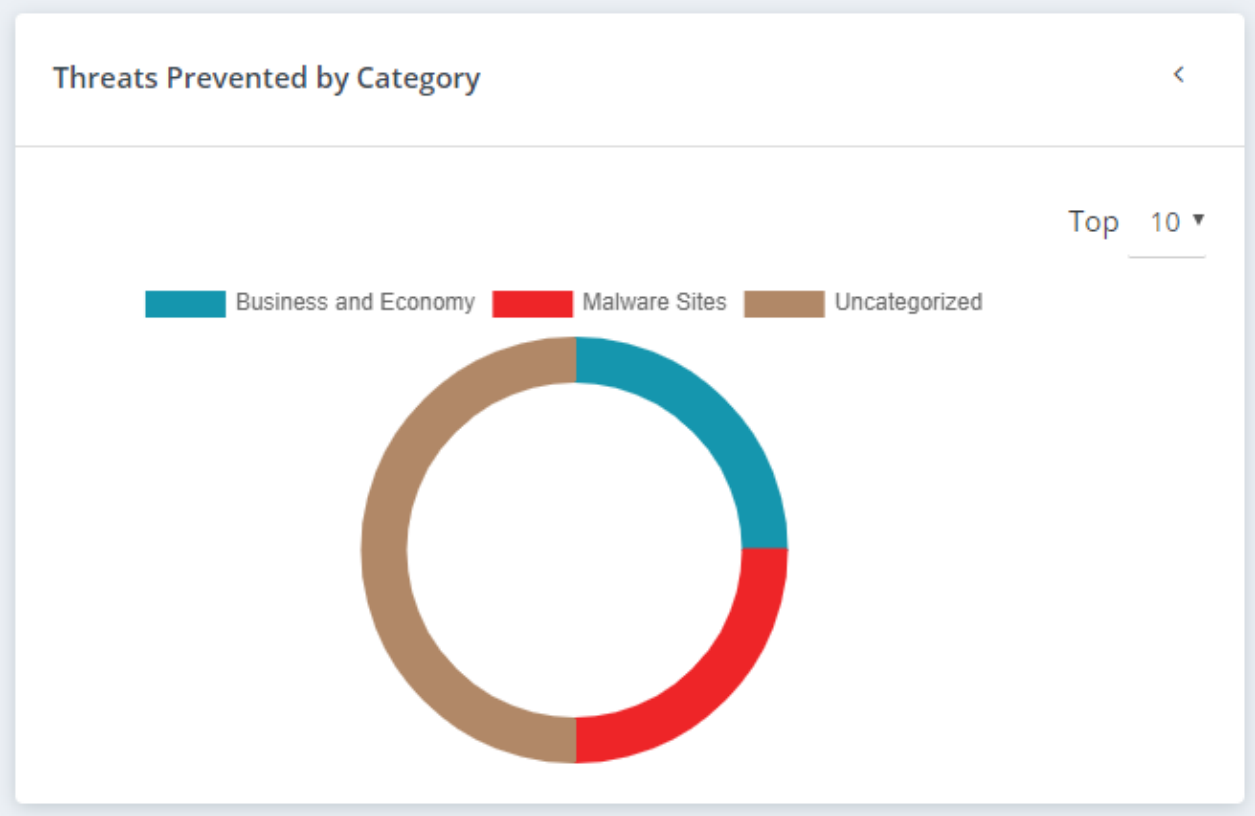
Steps

1) Sign in to Forcepoint Remote Browser Isolation.

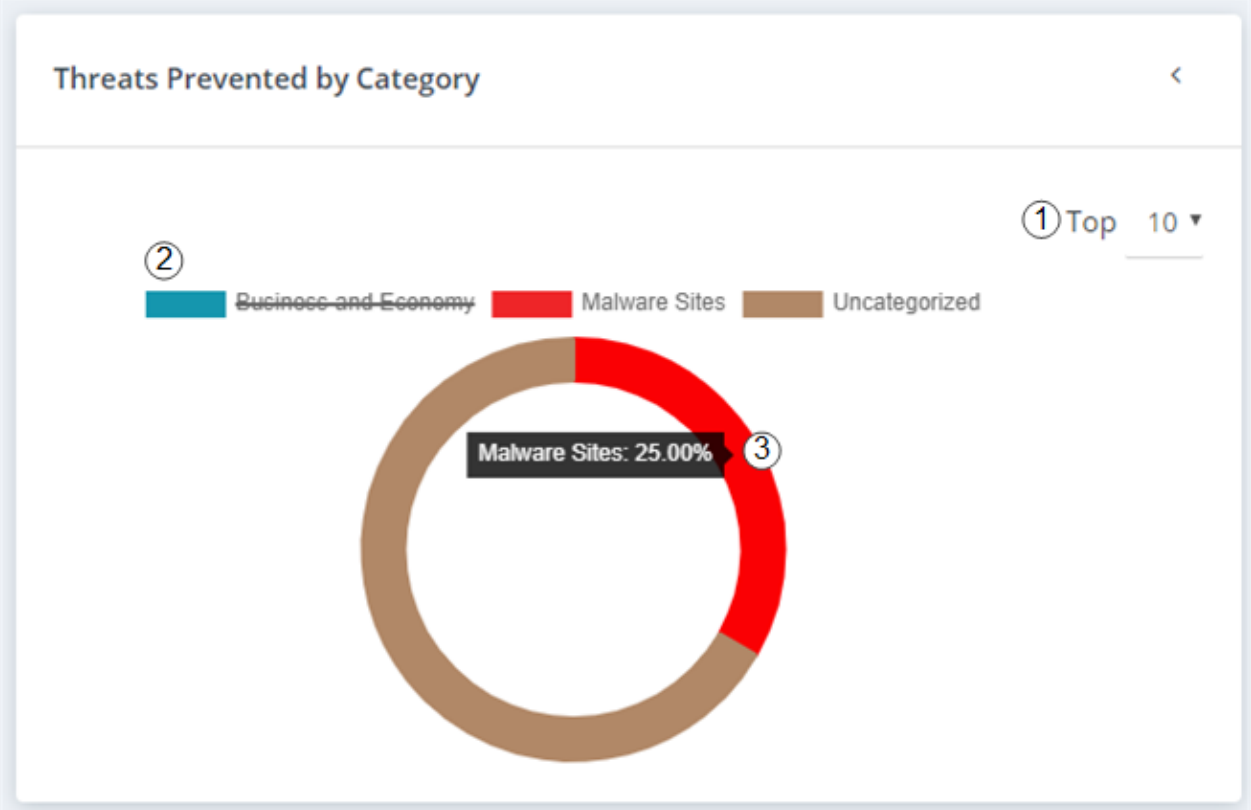
2) Go to **Dashboard** > **Web Security**.

3) Select the data range for the dashboard.

4) Go to the **Threats Prevented by Category** panel. This panel shows a chart with the categories that contain the most threats that were prevented by Forcepoint Remote Browser Isolation.



5) To change the metrics display:



1. Click the **Top** drop-down menu to show either the Top 5, 10, or 15 prevented threats.
2. Click the category name above the chart to remove that category 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 categories by percentage.

View metrics for threats prevented per user

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

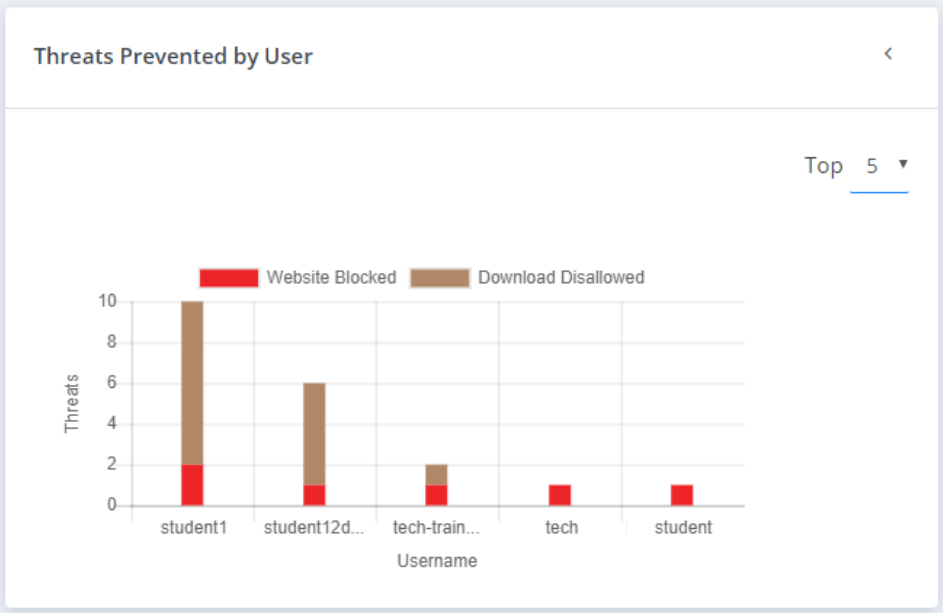
Steps

1) Sign in to Forcepoint Remote Browser Isolation.

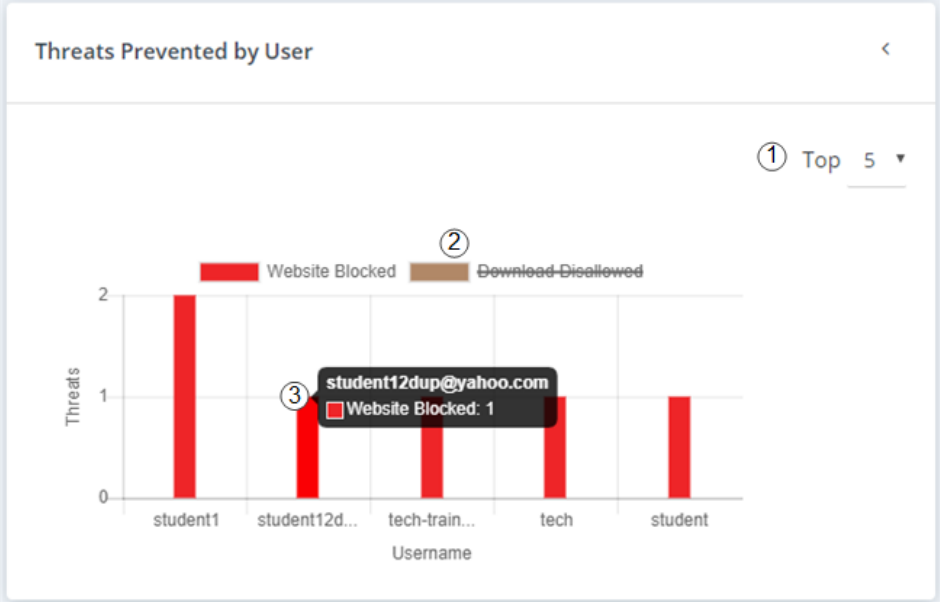
2) Go to **Dashboard** > **Web Security**.

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.

View the security threat summary

The **Security Threat Summary** shows information for all browsed sites where the threat score exceeded the allowable level set by the administrator.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Dashboard** > **Web Security**.

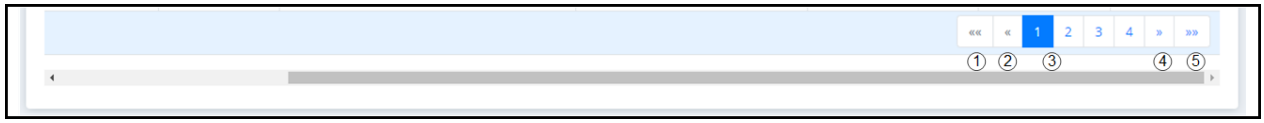
3) Select the data range for the dashboard.

4) Go to the **Security Threat Summary** panel.

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, Date, IP address, Source URL, Web Category, and Threat Score.

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 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.

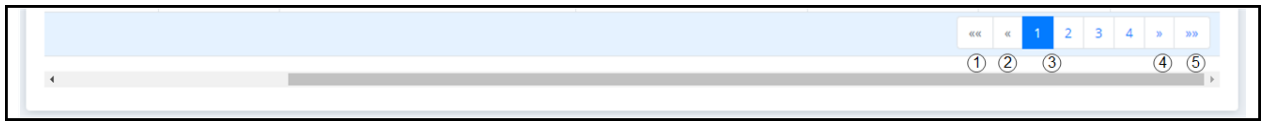
4) Go to the **Download Summary** widget. The summary chart shows the file types for each file that has been either **Allowed** or **Blocked**.

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 upload summary

The **Upload Summary** shows the count for all file types that were either uploaded successfully by the user (allowed) or were not uploaded when the file failed the CDR conversion, or a DLP policy is enforced (blocked).

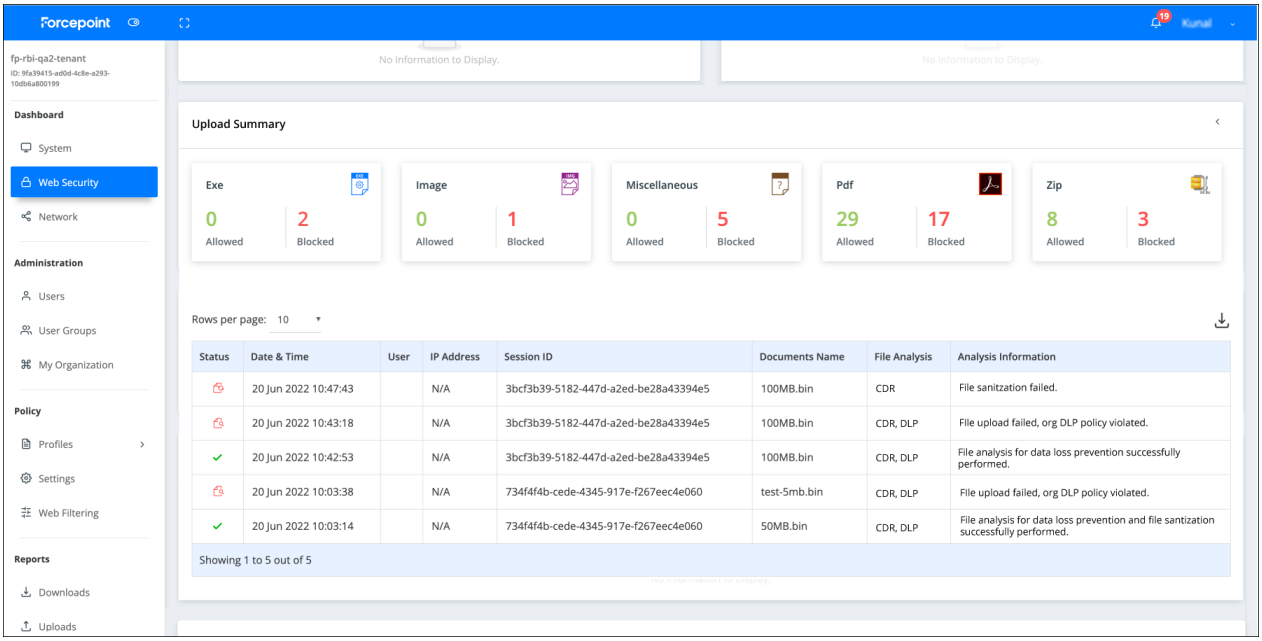
Steps

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 **Upload Summary** widget. The summary chart shows the file types for each file that was either **Allowed** or **Blocked**.

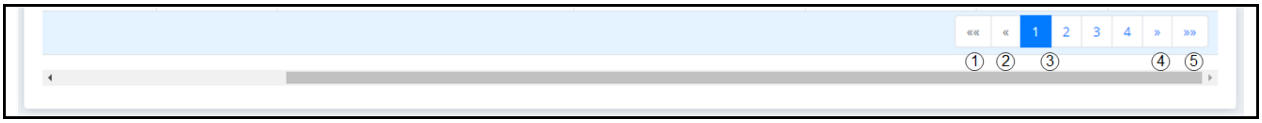


5) To see more details about a specific file type, click the file type icon. A table opens under the chart.

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**.

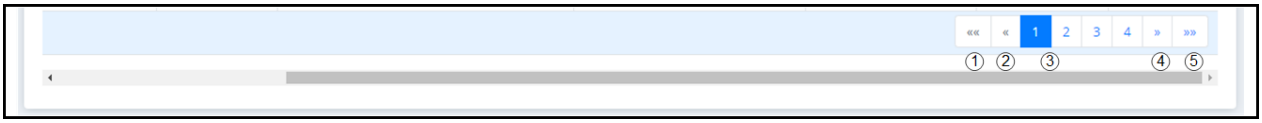
3) Select the data range for the dashboard.

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 the web security summary

The **Web Security Summary** widget displays the page protection metrics for isolated web pages.

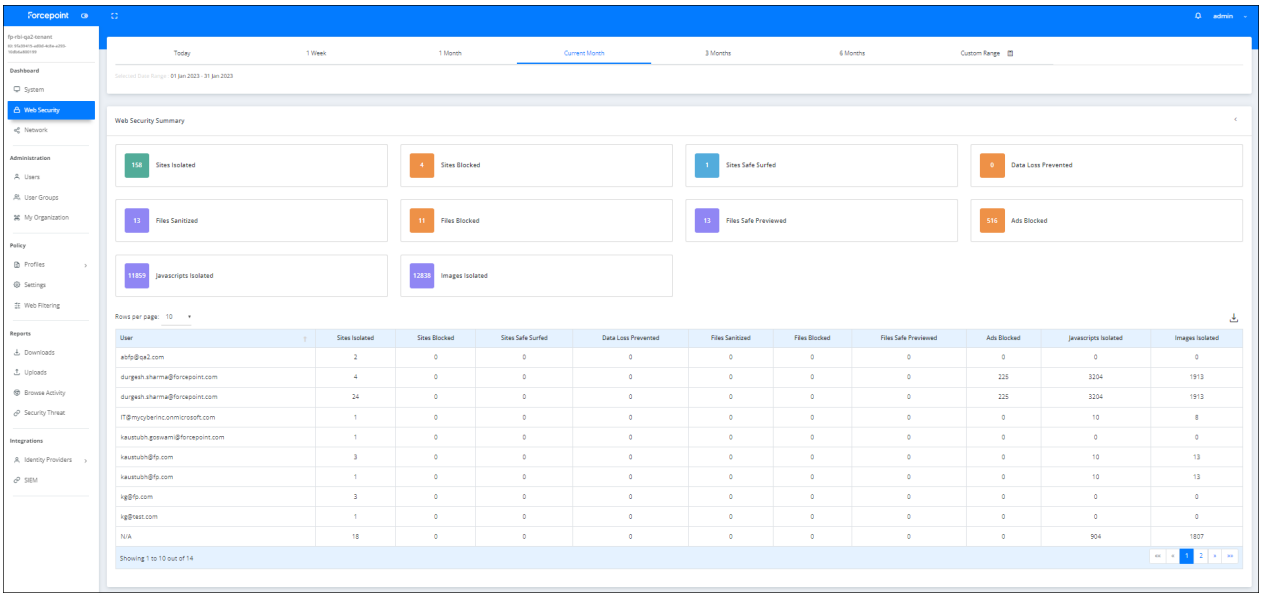
Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Dashboard** > **Web Security**.

3) Select the data range for the dashboard.

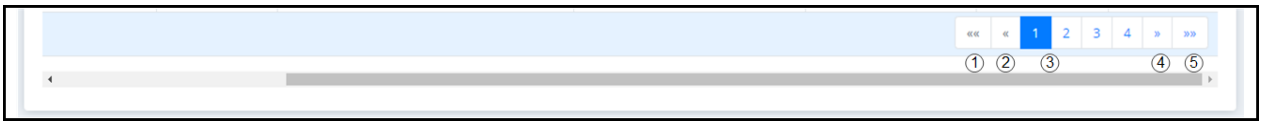
4) Go to the **Web Security Summary** widget. The summary chart displays the statistical data for each security event types.



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.

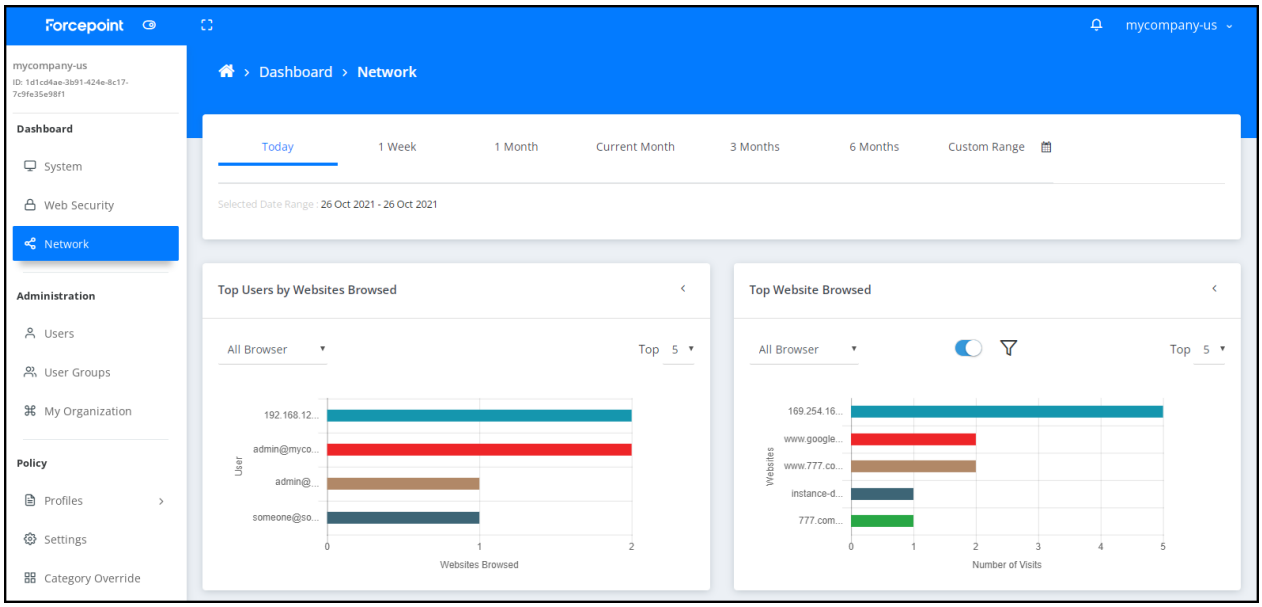
6) Below the table, you can choose the following options to navigate through the table.



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.

Viewing network details

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



Network Widgets

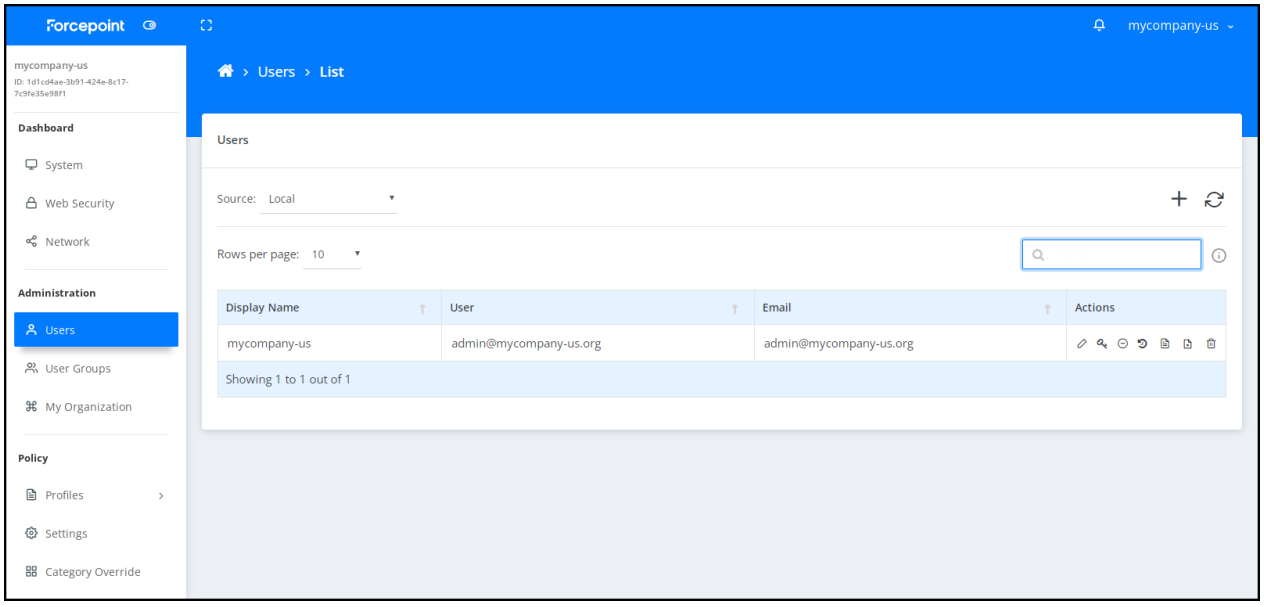
Widgets	Description
Top Users by Websites Browsed	Shows information about the number of websites browsed per user. You can choose to see the top 5, 10, or 15 users and you can choose to view the users for all browsers or a specific browser.
Top Website Browsed	Shows information about the number of visits 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 5

Administration

Contents

The **Administration** section provides comprehensive information about your users and organization in Forcepoint RBI.

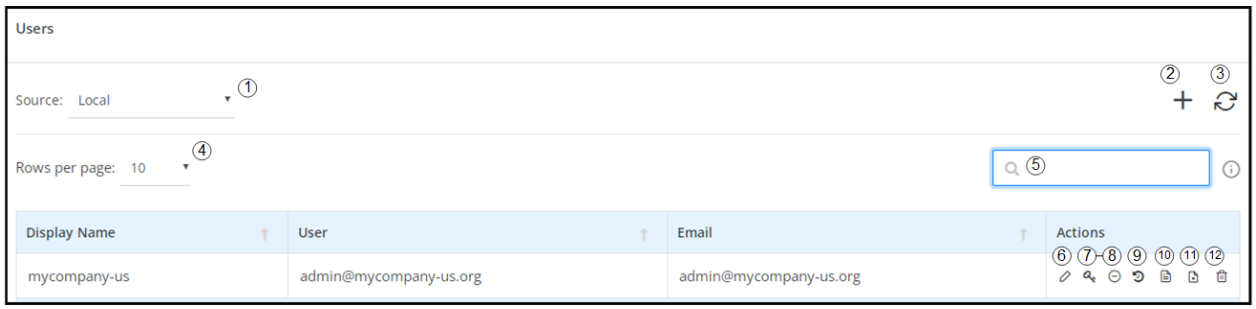


Administration tabs

Tab	Description
Users	Provides a list of all users in Forcepoint RBI. From this tab, you can create new users, modify user details, disable and enable users, and delete users.
User Groups	Provides a list of all user groups in Forcepoint RBI. A user groups is a set of specific users that share a specific policy.
My Organization	Provides comprehensive information about the Forcepoint RBI instance for your organization. From this tab, you can view and modify the active policy, logo image file, and license.

Users

The **Users** tab provides a list of all users in Forcepoint RBI. From this tab, you can create new users, modify user details, disable and enable users, and delete users.



1. Choose to display the user list by the directory source: either **Local** (users created in Forcepoint RBI) or a user directory provided through a configured LDAP, SAML or Proxy Authentication identity provider (configured under Integrations).
2. Add a new user.
3. Refresh the user list.
4. Choose to show either 10, 25, 50, or 100 rows in the table per page.
5. Search the user list for a specific user. You can search on the Display Name, Username, or Email.
6. View or edit user details.
7. Reset the password.
8. Disable or enable the user.
9. Open the Browse Activity report for the user.
10. Associate (assign) or dissociate (unassign) one or more policies. This option allows administrators to enable specific policies for specific users instead of having a specific policy enabled for all users.
11. Anonymize the user's record. Selecting this option removes identifying information about the user from their activities in Forcepoint RBI.
12. Delete the user.

Create a new user

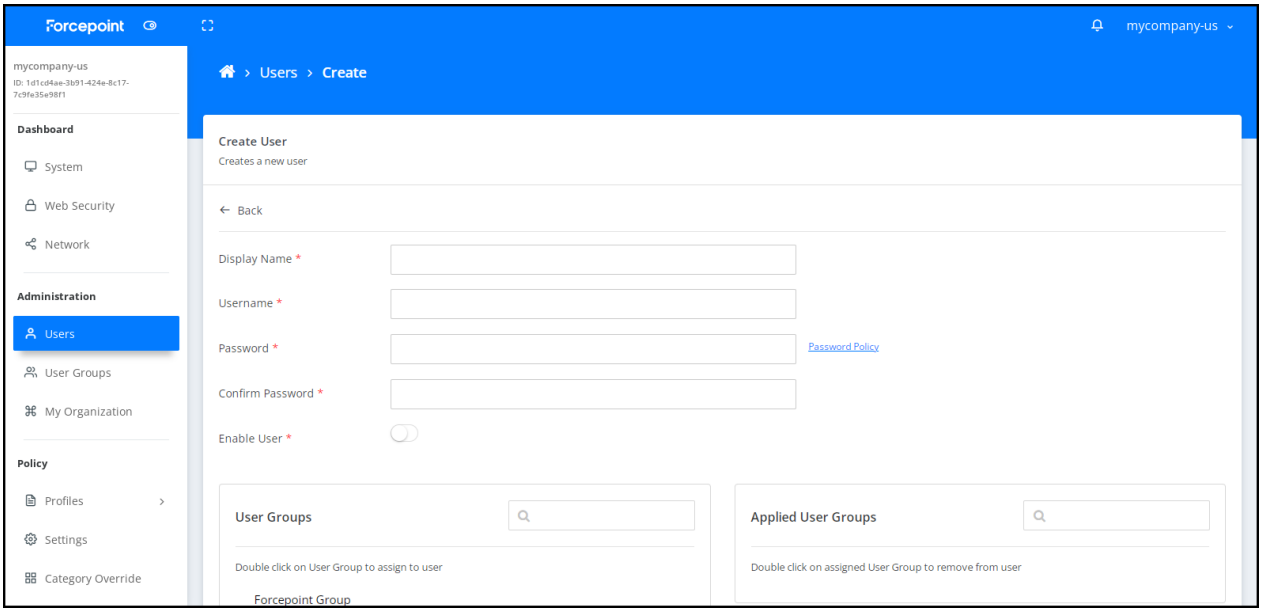
Add new Users or Administrators through the Users page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **Users**.

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



4) Enter the user details:

- **Display name** (required): The name shown for the user within Forcepoint RBI. The display name is shown in the top right corner of the Admin Portal and the Dashboard widgets.
- **Username** (required): The email address of the user. The user will use this username to sign in to Forcepoint RBI.
- **Password** (required): The password used to sign in to Forcepoint RBI. The password must contain the following:
  - Minimum length of 8 characters
  - Maximum length of 20 characters
  - At least one uppercase letter
  - At least one lowercase letter
  - At least one number (0-9)
  - At least one special character: ! @ # $ % & ? = [ ] < > { }
- **Confirm Password** (required): Enter the password a second time to verify that you entered the correct password.
- **Enable User** (required): Select this toggle to enable the user. If you do not enable the user, then they cannot sign in using these credentials.

5) Under **User Groups**, double-click the group name, then click **Confirm** to add the user group to the user account. The user groups are defined under **Administration** > **User Groups.**

6) To remote a user group, double-click the group name under **Applied User Groups**, then click **Confirm**.

7) Under **Roles**, double-click a role, then click **Confirm** to add the role to the user account. When a role has been added to the user account, it is shown under **Applied roles**.

   In this release, there are three available roles:

   - **Admin**: Allows the viewing and editing of all administrative pages within the organization. The Admin role allows you can create, edit, and delete users; manage the policy; and configure and create reports. Admins can access the Forcepoint RBI Admin Portal, but cannot browse. If you want to allow an Administrator to use the isolated browser, then assign both an Admin role (either Admin or Admin - Read Only) and a User role.
   - **Admin - Read Only**: Allows the viewing of the Dashboard and Reports pages only. With the Admin - Read Only role, you can interact with the Dashboard widgets and generate, print, and download reports.
   - **User**: Allows isolated browsing only. With the User role, you cannot sign into or access the Forcepoint RBI Admin Portal.

   Note

   Accounts introduced through LDAP or SAML default to the User role and have no access to the Admin Portal.

8) To remote a role, double-click the role under **Applied roles**, then click **Confirm**.

9) Click **Save**.

Edit user details

Edit the details for a User or an Administrator on the Users page.

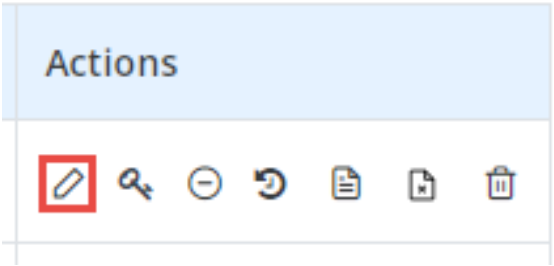
You cannot change the **Username** or **Password** on this screen.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **Users**.

3) In the user table, click the pencil icon in the **Actions** column.



4) Edit the **Display Name**, then click **Save**.

5) To change user group settings:

   a) Add a new user group: Double-click the group name under **User Groups**, then click **Confirm**.

b) Remove a user group: Double-click the role under **Applied User Groups**, then click **Confirm**.

6) To change roles:

a) Add a new role: Double-click a role under **Roles**, then click **Confirm**.

b) Remove a role: Double-click the role under **Applied roles**, then click **Confirm**.

Note

You do not need to click **Save** after you update the user group or role. The updates are saved automatically.

Reset a user password

Reset the password for a user on the Users page.

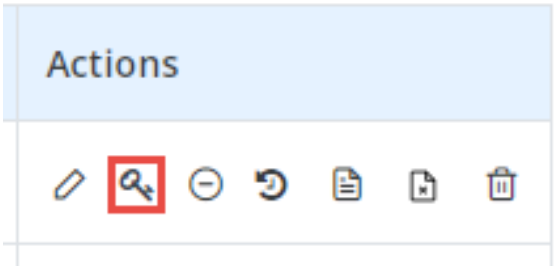
This page allows you to reset the password for a user. A user can change their own password in Forcepoint RBI using the **Change Password** option under the menu in the top right corner of the Admin Portal.

Steps

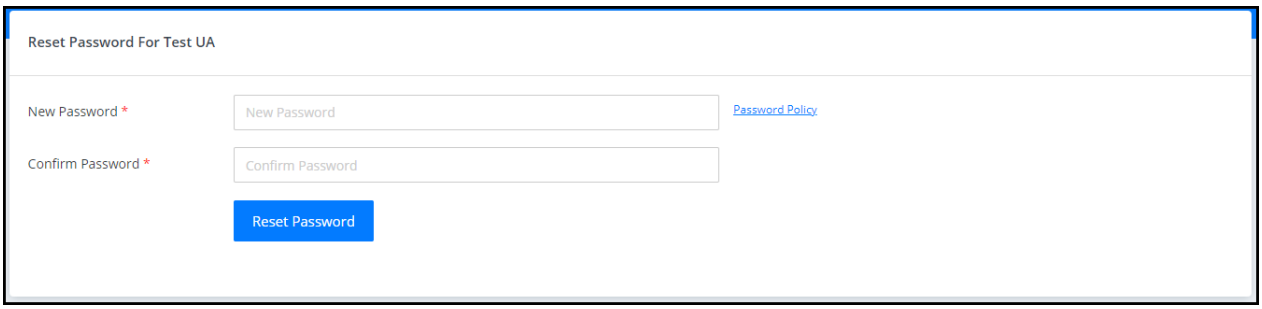
1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **Users**.

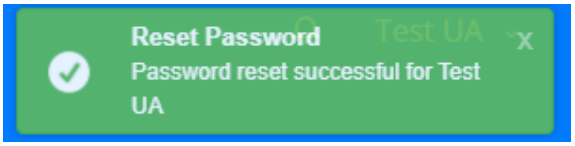
3) In the user table, click the key icon in the **Actions** column.



4) On the **Reset Password** screen, enter the **New Password**, then enter it a second time in the **Confirm Password** field.



5) Click **Reset Password**. Forcepoint RBI opens the Users page again and shows a confirmation message.



Forcepoint RBI sends a notification email to the email address (Username) associated with the user.

Disable and enable a user

Disable or enable a user on the Users page.

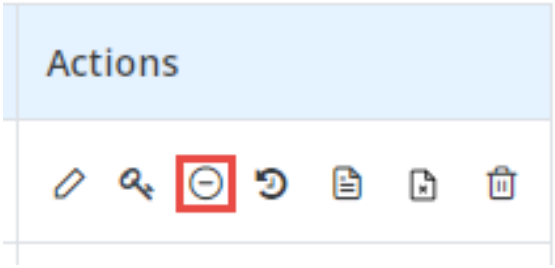
You disable and enable a user through the same icon. Click the icon once to disable an enabled user, or click it to enable a disabled user.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

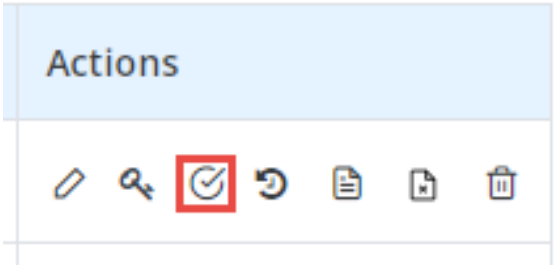
2) Go to **Administration** > **Users**.

3) In the user table, click the circle icon in the **Actions** column.



4) Click **Confirm** when asked if you want to disable the user.

5) The icon changes to show that the user is disabled.



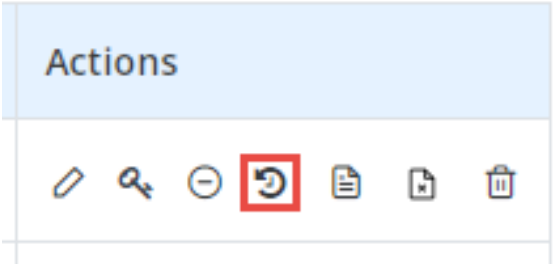
6) To enable a disabled user, click the icon again, then confirm.

View user browsing history

Open the Browse Activity Report for a user from the Users page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.
2) Go to **Administration** > **Users**.
3) In the user table, click the history clock icon in the **Actions** column.



4) On the **Browse Activity** screen, select the report filters, then click **Generate Report**.

Related tasks
Create a Browse Activity report on page 113

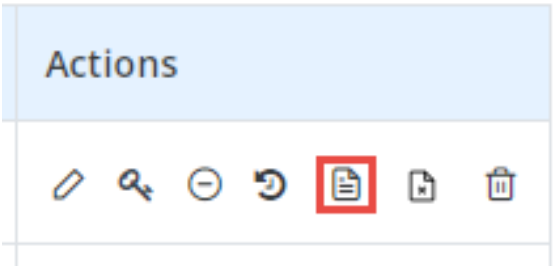
Associate or dissociate a policy for a user

Associate (assign) or dissociate (unassign) a policy for a specific user on the Users page.

A user can have one associated policy profile only. If the user has an associated policy and you try to associate another policy, then the old policy will be dissociated.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.
2) Go to **Administration** > **Users**.
3) In the user table, click the file icon in the **Actions** column.



4) On the **User Policy Association** page, locate the policy in the table, then click the toggle in the **Actions** column.
   - Policy is associated with the user:
   - Policy is not associated with the user:

   Note

   If you try to associate a policy when the user already has an associated policy, then a confirmation message displays. Click **Confirm** to associate the new policy and dissociate the old policy.

5) To configure or view the policy, click the pencil icon in the **Actions** column.

Anonymize a user record

Remove personal information from a user record through the Users page.

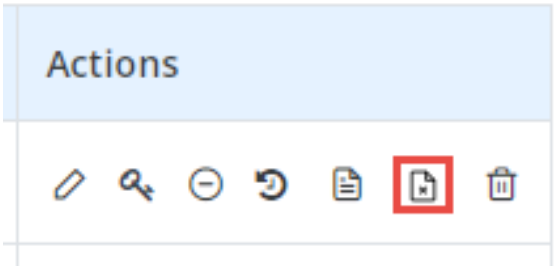
In support of the General Data Protection Regulation (GDPR), Forcepoint RBI can remove personal information from a user's record so that browsing activity is not tied to the specific user.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **Users**.

3) In the user table, click the delete file icon in the **Actions** column.



4) Click **Confirm** when asked if you want to anonymize the user record. When the user record is anonymized, Forcepoint RBI removes user-specific personal information from all records related to browsing activity.

Delete a user

Delete an Administrator or User account on the Users page.

When you delete a user, they are removed permanently from Forcepoint RBI. You cannot retrieve a user record after it is deleted.

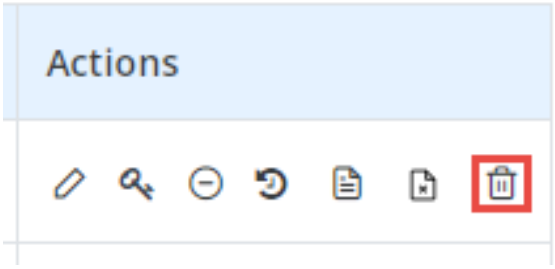
Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **Users**.

3) From the **Source** drop-down list, select a directory source to display the list of users in the user table.

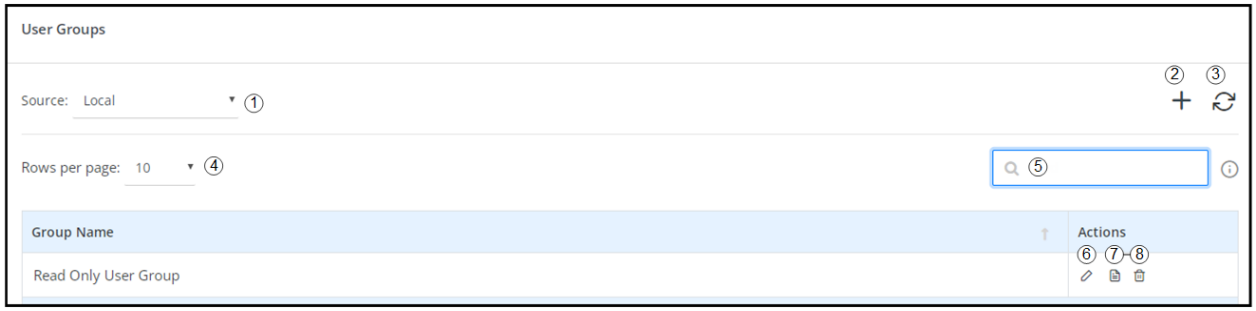
4) In the user table, click the trashcan icon in the **Actions** column.



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

User Groups

The **User Groups** tab provides a list of all user groups in Forcepoint RBI. From this tab, you can create new groups, modify group details, associate or dissociate a policy for each group, and delete groups.



1. Choose to display the user group list by the directory source: either **Local** (users created in Forcepoint RBI) or a user directory provided through a configured LDAP, SAML or Proxy Authentication identity provider (configured under Integrations).
2. Add a new user group.
3. Refresh the user group list.
4. Choose to show either 10, 25, 50, or 100 rows in the table per page.
5. Search the user group list for a specific group.
6. View or edit user group details.
7. Associate (assign) or dissociate (unassign) a policy for the user group. This option allows administrators to enable specific policies for specific groups instead of having a specific policy enabled for all groups.
8. Delete the user group.

Create a new user group

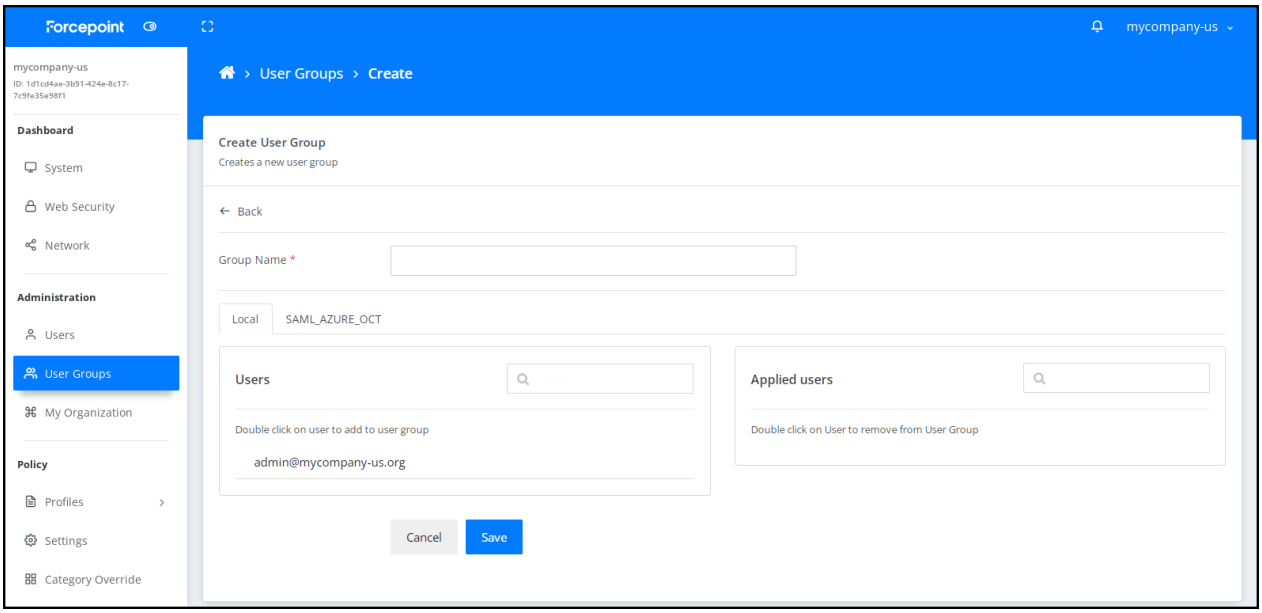
Add new user group through the User Groups page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **User Groups**.

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



4) Enter the **Group name** (required).

5) Under **Users**:

   a) Select the user directory. By default, Forcepoint RBI displays the **Local** directory. If you have configured an LDAP or SAML directory (**Integrations** > **Identity Providers**) and want to add users from those directories, select the relevant tab.

   b) Add users to the group. Double-click the user name, then click **Confirm** to add the user to the group. When the user is added to the group, it is shown under **Applied users**.

6) To remote a user from the group, double-click the group name under **Applied users**, then click **Confirm**.

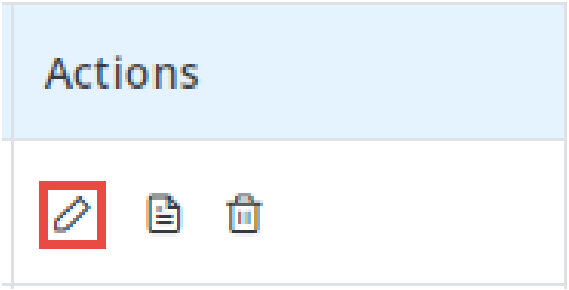
7) Click **Save**.

Edit user group details

Edit the details for a user group on the Users page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.
2) Go to **Administration** > **User Groups**.
3) In the user group table, click the pencil icon in the **Actions** column.



4) Edit the **Group Name**, then click **Save**.
5) To change the users assigned to the group:
   a) Select the preferred user directory tab. **Local** is the default directory.
   b) Add a new user: Double-click the group name under **Users**, then click **Confirm**.
   c) Remove a user: Double-click the role under **Applied users**, then click **Confirm**.

Note

You do not need to click **Save** after you update the users. The updates are saved automatically.

Associate or dissociate a policy for a user group

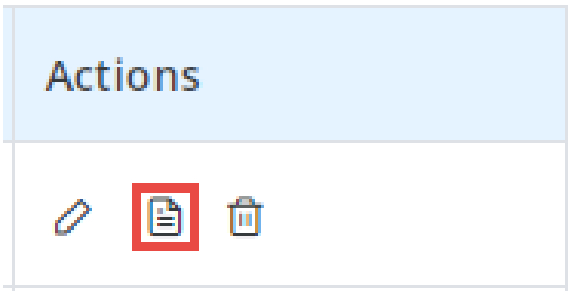
Associate (assign) or dissociate (unassign) a policy for a specific group on the User Groups page.

A user group can have one associated policy profile only. If the group has an associated policy and you try to associate another policy, then the old policy will be dissociated.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.
2) Go to **Administration** > **User Groups**.

3) In the user groups table, click the file icon in the **Actions** column.



4) On the **User Group Policy Association** page, locate the policy in the table, then click the toggle in the **Actions** column.

- Policy is associated with the user:
- Policy is not associated with the user:

Note

If you try to associate a policy when the group already has an associated policy, then a confirmation message displays. Click **Confirm** to associate the new policy and dissociate the old policy.

5) To configure or view the policy, click the pencil icon in the **Actions** column.

Delete a user group

Delete a user group on the User Groups page.

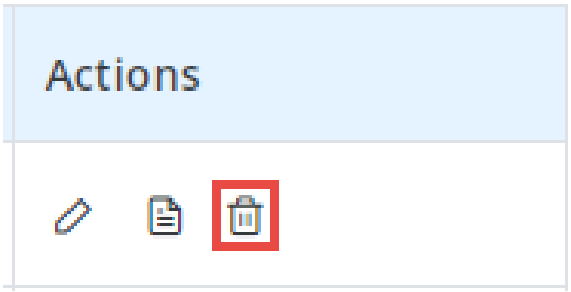
When you delete a user group, it is removed permanently from Forcepoint RBI. You cannot retrieve a user group record after it is deleted.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **User Groups**.

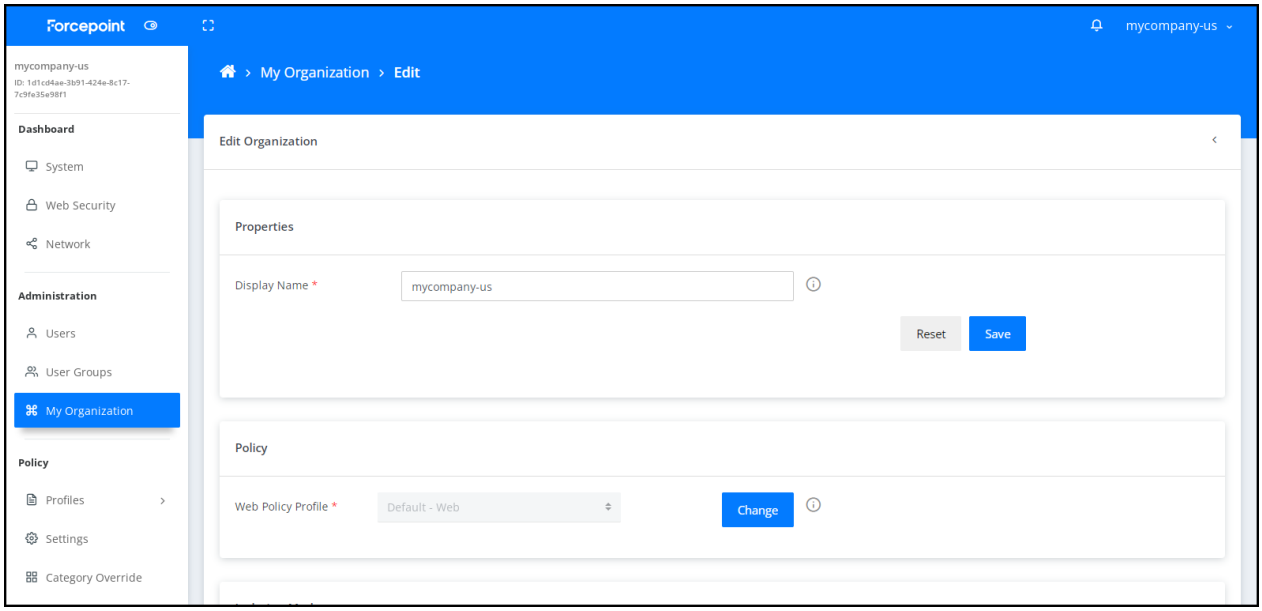
3) In the user group table, click the trashcan icon in the **Actions** column.



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

My Organization

The **My Organization** tab provides comprehensive information about the Forcepoint RBI instance for your organization. From this tab, you can view and modify the active policy, logo image file, and license.



My Organization Widgets

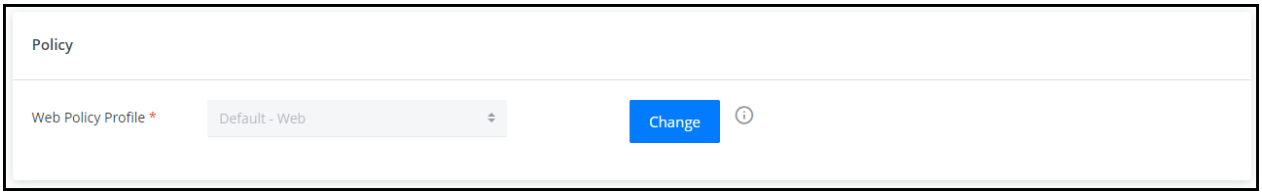
Widgets	Description
Properties	Shows the **Display Name** for your organization.
Policy	Shows the active policy profile.
Isolation Mode	Enables or disables **Smart isolation**, which intelligently switches between Secure Streaming and Secure Rendering based on the content and the FTIS real-time threat score.
Authentication	Configures the default identity provider and end user authentication level.
Customize Logo	Upload a custom logo to show for blocked rendered sites.
API Keys	Generate API Key from RBI admin portal to access the RBI APIs.

Change the web policy profile

If you have more than one policy profile, you can change your active web policy profile on the My Organizations page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.
2) Go to **Administration** > **My Organization**.
3) Go to the **Policy** section. This section shows the current active web policy profile.



4) Click **Change**.
5) Open the drop-down menu and select the policy profile.
6) Click **Save**.

Configure the isolation mode

Choose to enable Smart Isolation to automatically switch between Secure Streaming and Secure Rendering, or disable Smart Isolation to set the switching threshold manually.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.
2) Go to **Administration** > **My Organization**.
3) Go to the **Isolation Mode** section.

4) By default, **Smart Isolation** is set to **Enabled**. When Smart Isolation is enabled, Forcepoint RBI decides the isolation mode (either Secure Rendering or Secure Streaming) automatically based on the web page content and the FTIS real-time threat score.

5) To manually decide which isolation mode to use, click the toggle to set **Smart Isolation** to **Disabled**.

Move the blue selector icon to the threat score, or click the specific threat score, then click **Confirm** to verify the new threat score threshold. By default, the threat score threshold is set to **80**. If the threat score for the web page is above the threshold, then Forcepoint RBI uses Secure Streaming. If the threat score is below the threshold, then Forcepoint RBI uses Secure Rendering.

Note

The changes are saved automatically. You do not need to click **Save.**

Related concepts

Secure Streaming and Secure Rendering isolation modes on page 81

Secure Streaming and Secure Rendering isolation modes

Forcepoint RBI offers two rendering modes: Secure Streaming and Secure Rendering.

- Secure Streaming: This mode converts website content into a visual stream of content. The browser experience is close to standard browsing (rendering the page contents outside of Forcepoint RBI), but the browser shows a custom right-click menu instead of the standard browser menu and does not display all custom fonts. This is the safest isolation mode, but uses a high amount of network bandwidth.
- Secure Rendering: This mode removes executable code, like JavaScript, and delivers only the HTML and CSS for a page to the local browser to render with native DOM rendering. The browsing experience is close to standard browsing — the browser shows the standard browser right-click menu and uses native fonts to provide a better experience to end users when they view the page through the isolated browser.

In Forcepoint RBI, you can choose to use Secure Streaming, Secure Rendering, or Smart Isolation, which automatically switches between streaming and rendering based on several factors, including the threat level of the website and its content. Smart Isolation is powered by the Forcepoint Threat Intelligence Service (FTIS), a cloud-based service that provides real-time data on security threat metrics.

Related concepts

Override Isolation Mode on page 101

Related tasks
Configure the isolation mode on page 80

Configure end user authentication

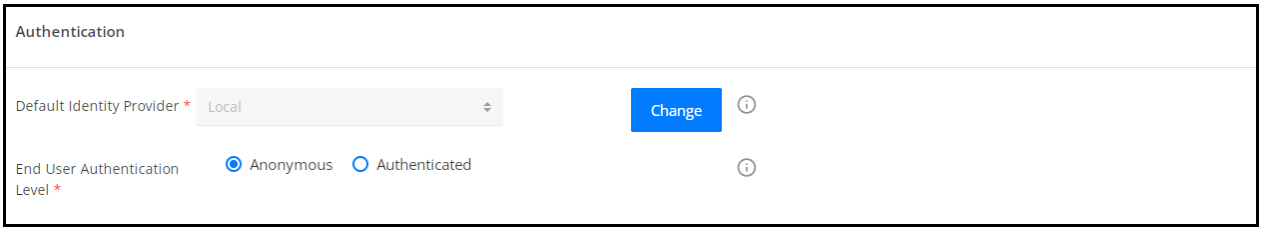
Select the mode of authentication for Forcepoint Remote Browser Isolation users. You can choose to authenticate users locally or through a third-party identity provider.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Administration** > **My Organization**.

3) Go to the **Authentication** section.



4) To change the **Default Identity Provider**, click **Change**, then select your preferred identity provider from the drop-down list. **Local** is the default identity provider for all accounts created in Forcepoint RBI under **Administration** > **Users**. Other identity providers are shown here if they were created and configured under **Integrations** > **Identity Providers**.

5) To change the **End User Authentication Level**, select one of the following options:
   - **Anonymous**: Allows users to browse without authenticating with Forcepoint RBI.
   - **Authenticated**: Allows only authenticated users to browse. Users must sign in to Forcepoint RBI before browsing.

Enable RBI Admins to self-generate API Key

RBI admins can generate the API Key to access Forcepoint RBI APIs from the RBI admin portal. This capability provides a secure way of generating the API Key over older means of having the Forcepoint technical support share the API Keys over email channels. RBI admins can create, edit, as well as delete API keys from the RBI admin portal as explained in the procedure below:

Create API Key

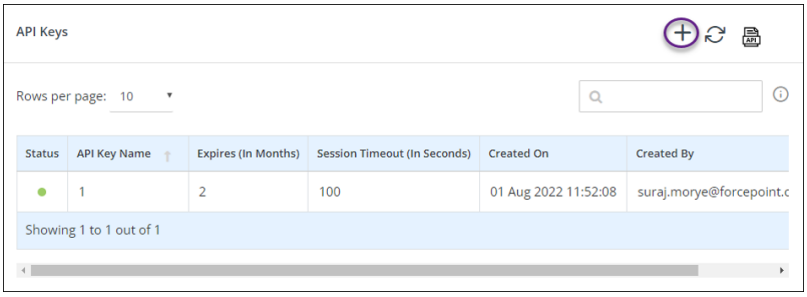
Steps

1) Sign in to Forcepoint Remote Browser Isolation (Forcepoint RBI).

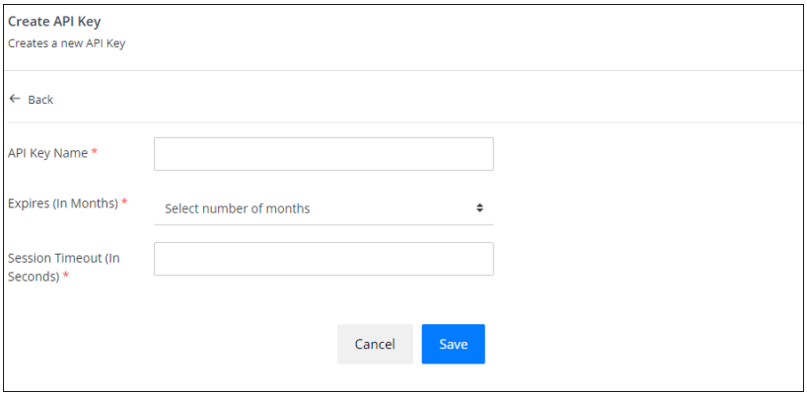
2) Go to **Administration** > **My Organization**.

3) Scroll to the **API Keys** section.

4) Click the + sign as shown below.



5) The **Create API Key** dialog box is displayed as follows:



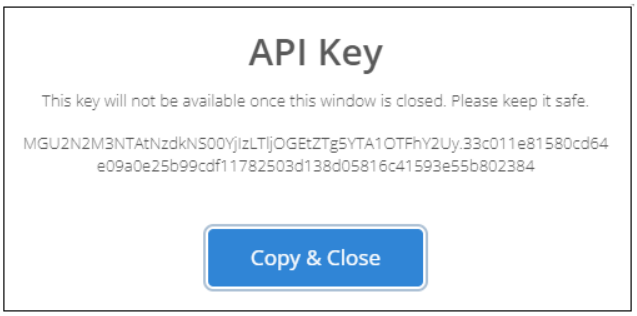
6) Enter the following details:

   a) **API Key Name**: Represents the API Key name.

   b) **Expires (In Months)**: Key validity period.

   c) **Session Timeout (In Seconds)**: API session timeout.

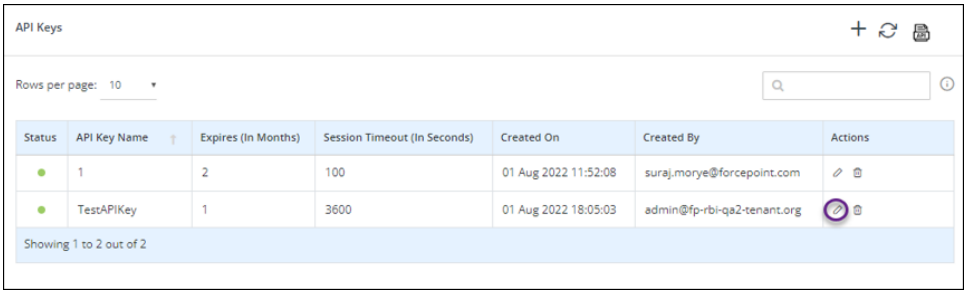
7) The generated API Key is displayed in a new dialog box. Using the **Copy & Close** option, copy the API Key for later use. An example is shown below.



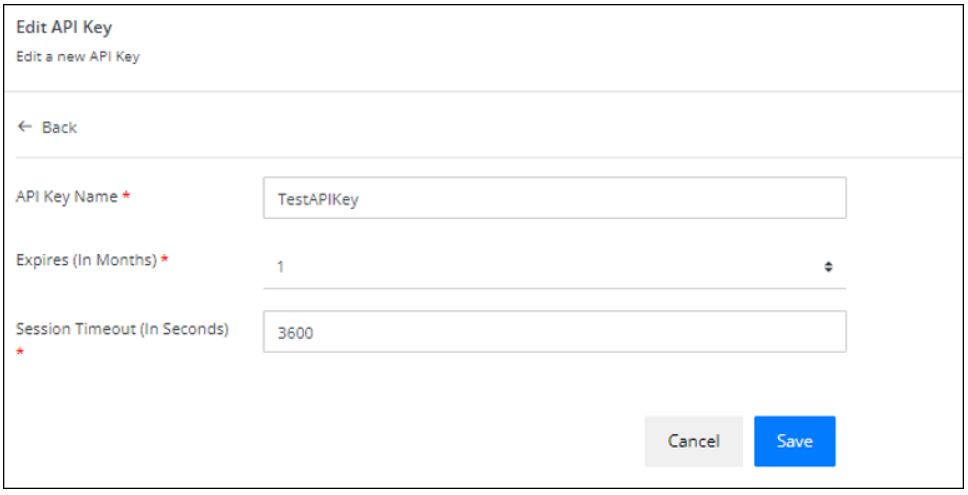
Edit API Key

Steps

1) An API Key, previously created can be modified using the **Edit** option as shown below:



2) On clicking the icon following edit dialog box is opened:

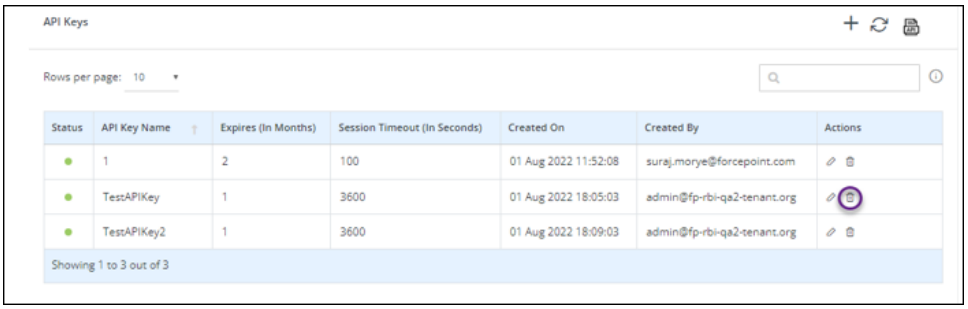


3) Post making the required changes, click **Save** to save the changes.

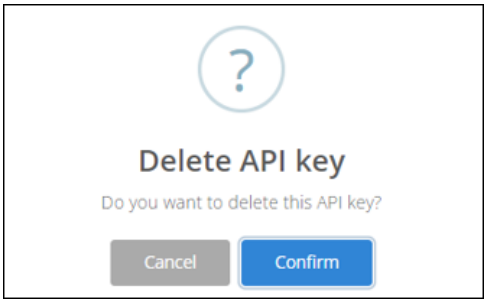
Delete API Key

Steps

1) An existing API Key, can be deleted by selecting the Delete option as shown below:



2) On clicking the icon, the following confirmation dialog is displayed:

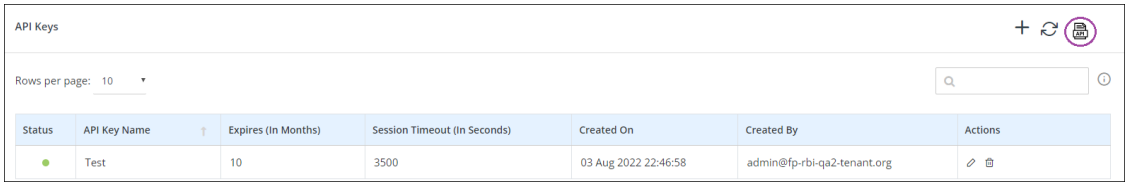


3) Click **Confirm**, to delete the selected API Key.

API Reference Guide

The API Reference Guide can be accessed through the API Keys Widget.

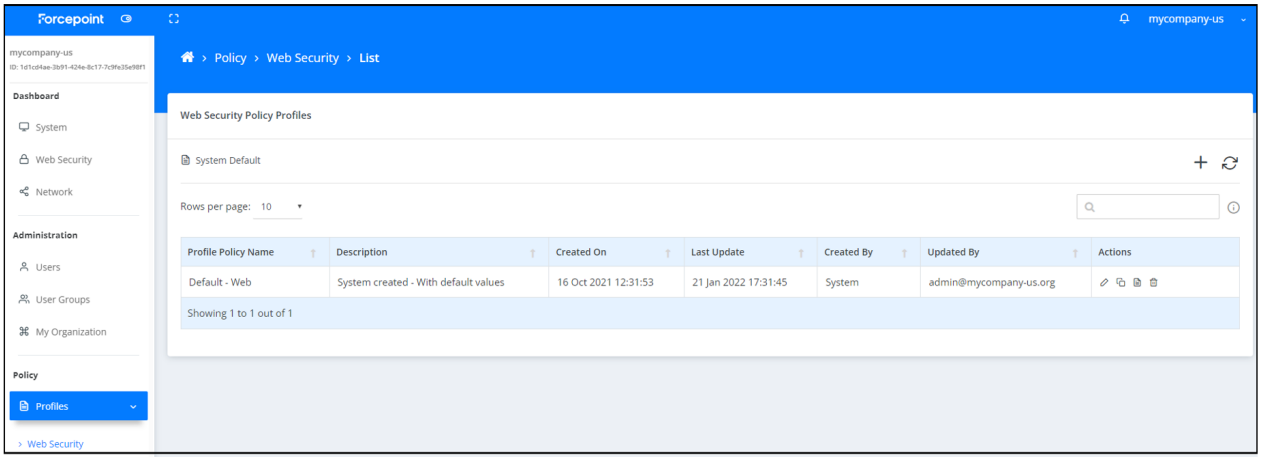
To access the API Reference Guide, Click icon as shown below.



Chapter 6
Policy

Contents

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

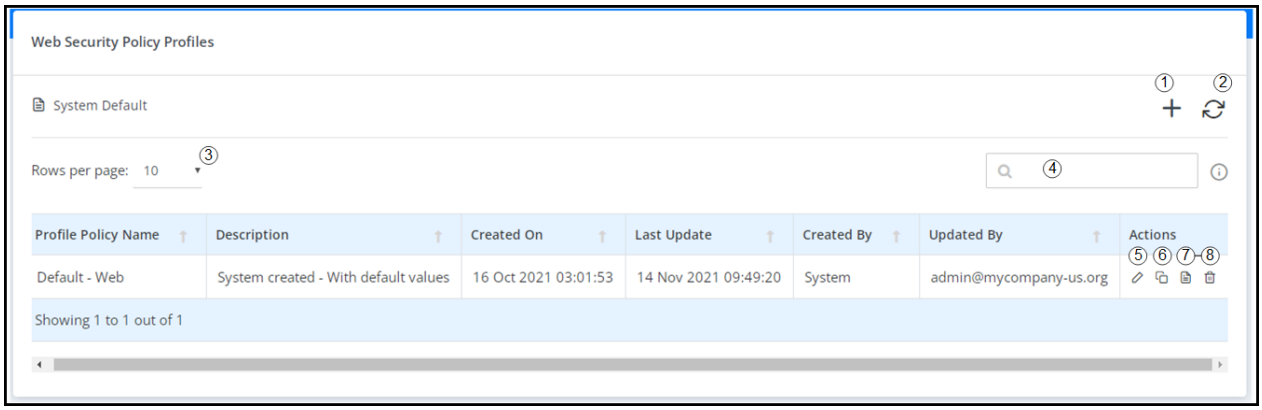


Policy tabs

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.
Category Override	Provides the ability to change the category associated with a website. This feature is available for standalone Forcepoint RBI deployments only.

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. Select the users and user groups to associate (assign) with the policy profile or dissociate (unassign) from the policy profile.
8. Delete the profile.

Create a new policy profile

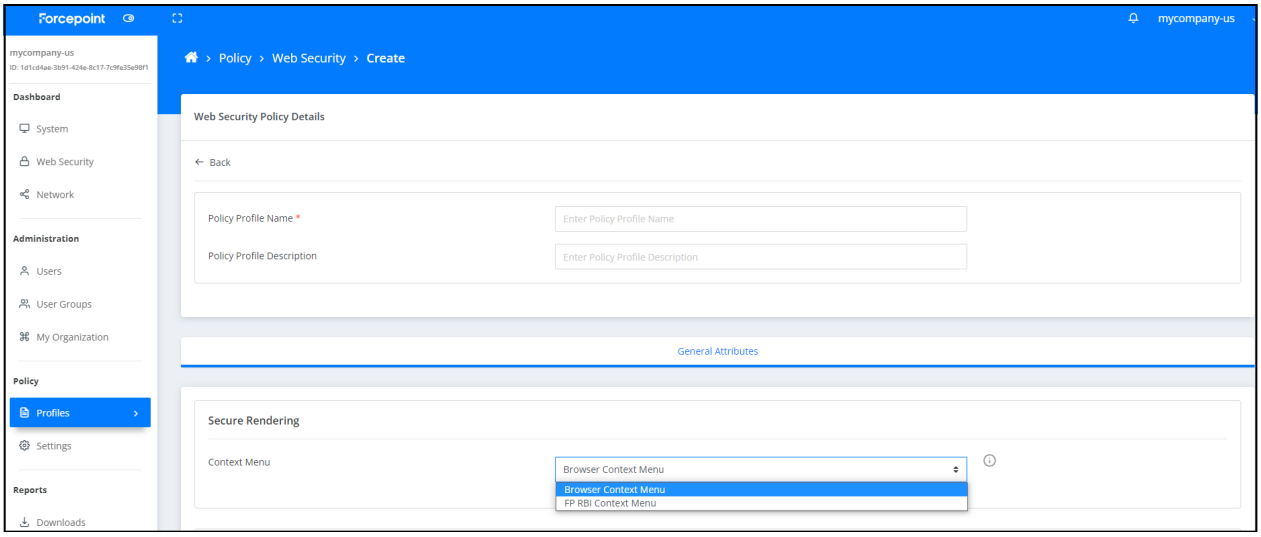
Forcepoint RBI comes with one default Web Security Policy profile. You can create more policy profiles through the **Profile** settings page.

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 **Secure Rendering**, select the **Context Menu** type from the drop-down menu. Select the **Browser Context Menu** for more native browsing experience. Select the **FP RBI Context Menu** for stricter security control.

Note

Forcepoint recommends the use of the FP RBI Context Menu when CDR is enabled. Enable the Browser Context Menu when necessary for productivity application shortcuts. The Browser Context Menu's Save As option will bypass RBI's CDR file processing and should only be used on trusted sources.

6) Under **Clipboard Control**, click the toggle switch to disable the **Endpoint to Remote Browser** option.

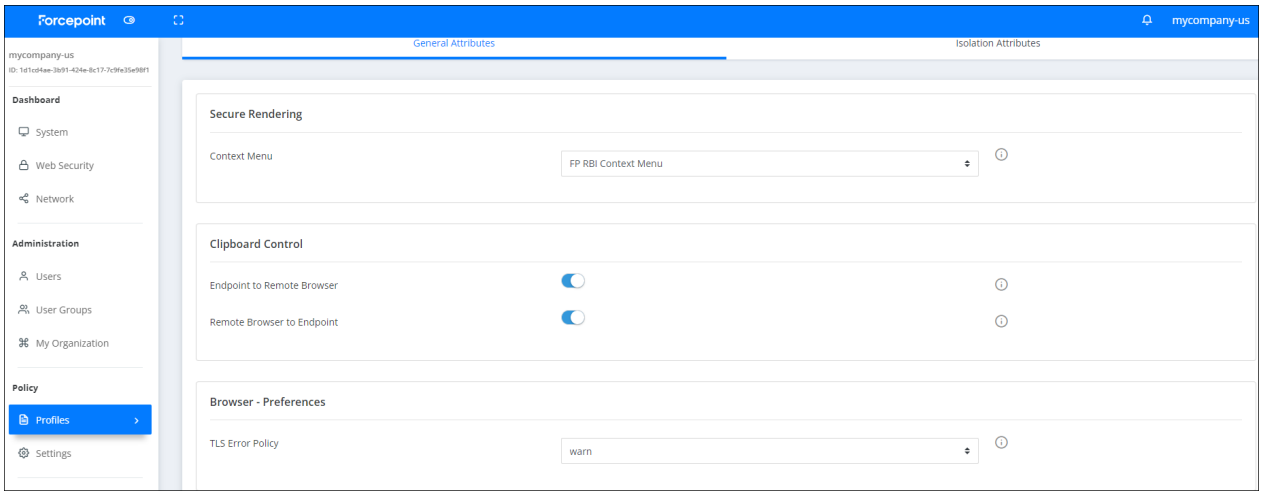
Note

Endpoint to Remote Browser option is enabled by default. It allows users to perform copy and paste action from endpoint to remote browser. The maximum number of characters that can be copied and pasted is 7000.

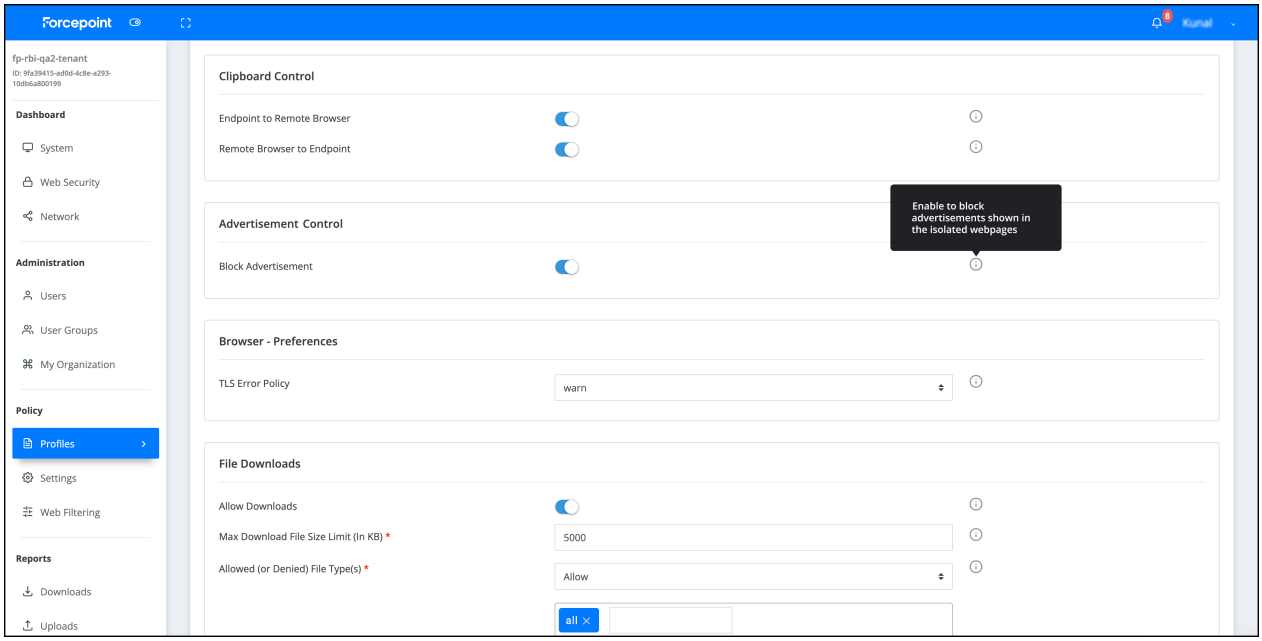
Click the toggle switch to disable the **Remote Browser to Endpoint** option.

Note

Remote Browser to Endpoint option is also enabled by default. It allows users to perform copy and paste action from remote browser to endpoint.



7) Under **Advertisement Control**, click the toggle switch to enable or disable the **Block Advertisement** option.



Note

a) By default, the **Block Advertisement** option is disabled.

b) When this option is enabled, the advertisements are blocked on the isolated page.

c) To display the number of ads that are blocked for a user, the **Ads Blocked** column is added in the table under the **Browse Activity Summary** section, in the **Dashboard** > **Web Security** tab.

8) 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.

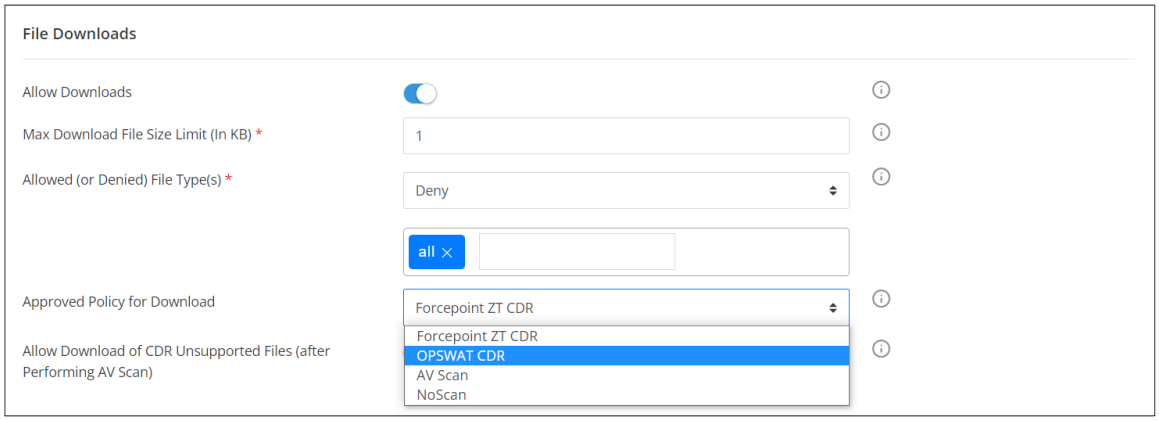
9) Under **File Downloads**, enter the relevant information:

- **Allow Downloads**: Enable this option to allow users to download files.
- **Max Download File Size Limit (in KB)**: Enter the maximum file size for downloads in kilobytes. The maximum allowed file size is 50000 KB (50 MB).
- **Allowed (or Denied) file type(s)**: Choose to **Allow** or **Deny** specific file types from downloading. Leave **all** as the only option to allow or deny all file types, or enter one or more file types into the field (**all** will be ignored if at least one file type is listed). For example, if you enter **.exe,.doc**, then EXE and DOC file types only will be allowed or denied.
- **Approved Policy for Download**: Choose the file download policy option:
  - **Forcepoint ZT CDR**: During download, files will be scanned and sanitized using Forcepoint ZT CDR technology.
  - **OPSWAT CDR**: During download, files will be scanned and sanitized using the OPSWAT Deep CDR technology.
  - **AV Scan**: File downloads are scanned by antivirus only.
  - **NoScan**: File downloads are not scanned.

Note

OPSWAT CDR option is visible in the file download policy even if, it is not configured. If RBI administrator selects this option, an error message is displayed saying the configuration is not saved. For more information about OPSWAT Configuration, see Settings on page 98.

- **Allow Downloads of CDR Unsupported Files after Performing AV Scan**: After performing AV Scan, enable this option to download files that are not supported by OPSWAT or Forcepoint ZT CDR. If you do not want to download the files, disable this option.



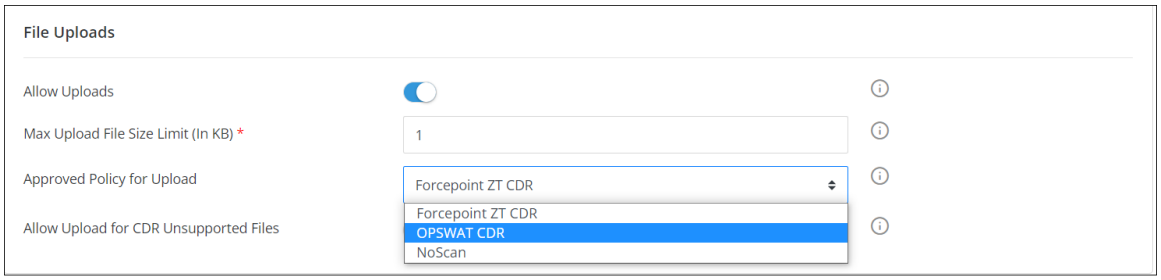
10) Under **File Uploads**, enter the relevant information:

- **Allow Uploads**: Enable this option to allow users to upload files.
- **Max Upload File Size Limit (in KB)**: Enter the maximum file size for individual uploads in kilobytes. The maximum allowed file size is 400000 KB (400 MB).
- **Approved Policy for Upload**: Choose the file upload policy option:
  - **Forcepoint ZT CDR**: During upload, files will be scanned and sanitized using Forcepoint ZT CDR technology.
  - **OPSWAT CDR**: During upload, files will be scanned and sanitized using OPSWAT Deep CDR technology.
  - **NoScan**: File uploads are not scanned.

Note

OPSWAT CDR option is visible in the file upload policy even if, it is not configured. If RBI administrator selects this option, an error message is displayed saying the configuration is not saved. For more information about OPSWAT Configuration, see Settings on page 98.

- **Allow Upload for CDR Unsupported Files**: Enable this option to upload files that are not supported by OPSWAT or Forcepoint ZT CDR.



11) Under **Printing**, click the toggle switch to enable or disable the printing option.

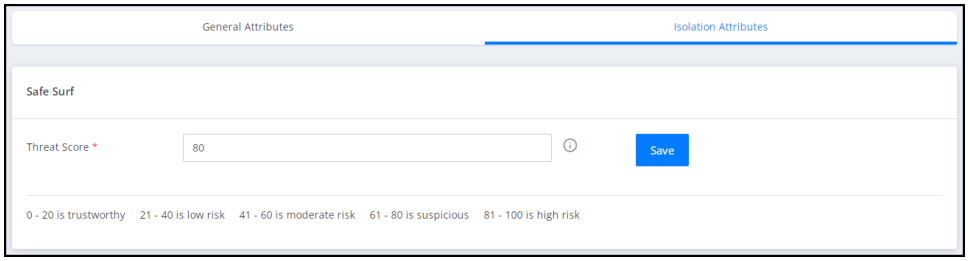
Note

a) By default, the printing option is disabled.

b) When this option is enabled, a user or user group can perform a print action.

c) When this option is disabled, a user or user group cannot perform a print action. If a user or user group tries to perform a print action, an error message that states *"Print action is restricted by your organization's policy. Please contact your administrator for more information"* is displayed.

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



13) In the **Safe Surf** section, select the **Threat Score** threshold. If the threat score for a web page is more than the threshold, then the page is rendered in a 'read-only' mode where hyperlinks and navigation work, but entering data into text fields and file uploads and downloads are not allowed.

14) Click **Save**.

15) (Standalone Forcepoint RBI deployments only) Configure Categories Selection:

a) In the **Categories Selection** section, click the **+** icon. A new row is added to the table.

b) In the **Category** column, enter the category name.

c) Select whether the category should be **Isolated** or **Blocked**.

d) In the **Action** column, click the save icon.

16) (Standalone Forcepoint RBI deployments only) Configure URL Selection:

a) In the **URL Selection** section, click the **+** icon. A new row is added to the table.

b) In the **URL** column, enter the full URL for the website.

c) Select whether the URL should be **Isolated** or **Blocked**.

d) In the **Action** column, click the save icon.

Related concepts
Content Disarm and Reconstruction on page 151

Edit a policy profile

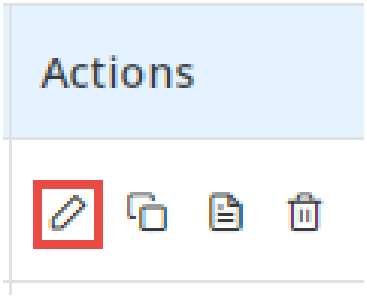
After a policy is created, you can edit the information for an existing policy through the Profiles settings page.

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

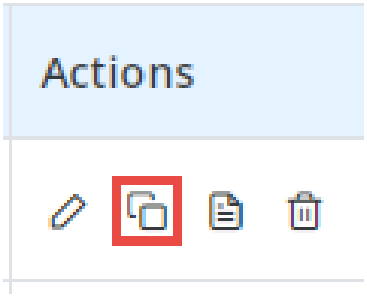
Duplicate a policy profile to copy the information from existing profile into a new profile.

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**.

Associate or dissociate a policy profile

In a policy profile, associate (assign) or dissociate (unassign) users or user groups.

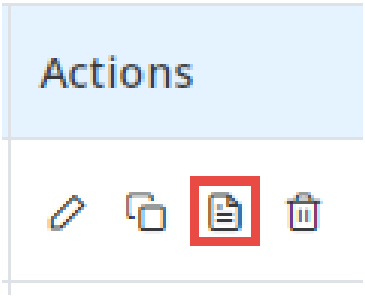
A user group can have one associated policy profile only. If the group has an associated policy and you try to associate another policy, then the old policy will be dissociated.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Policy** > **Profiles** > **Web Security**.

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



4) On the **Policy Profiles Association** page, select either the **Users** or **User Group** tab.

5) Select the **Source**. This can be either **Local** or a configured third-party Identity Provider.

6) Locate the user or user group in the table, then click the toggle in the **Associate/Dissociate** column.
   - User is associated with the policy profile:
   - User is not associated with the policy profile:

Note

If you try to associate a policy when the group already has an associated policy, then a confirmation message displays. Click **Confirm** to associate the new policy and dissociate the old policy.

Delete a policy profile

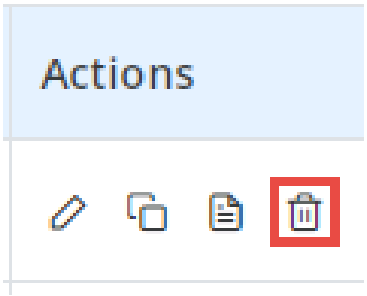
Delete a policy profile if it is no longer needed. You can delete any user-created profile, but you cannot delete the default Web Security policy profile.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Policy** > **Profiles** > **Web Security**.

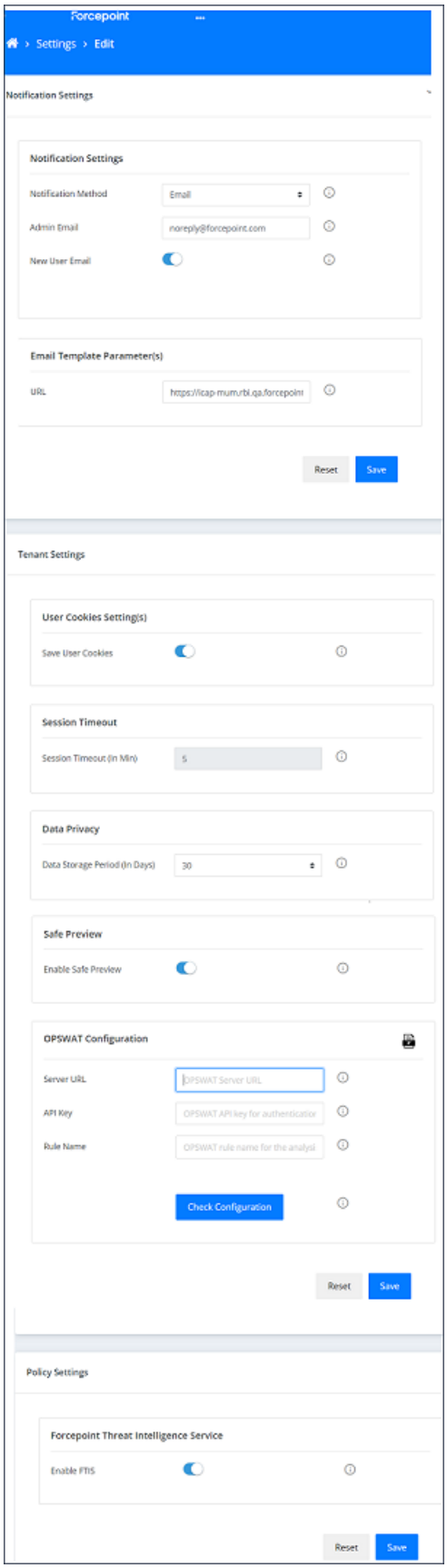
3) In the profile table, click the trashcan icon in the **Actions** column.



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

Configure notification, tenant, policy, override isolation mode, and override user agent settings under the Policy section:


Forcepoint
Settings › Edit
Notification Settings
Notification Settings
Notification Method
Email
Admin Email
noreply@forcepoint.com
New User Email
Email Template Parameter(s)
URL
https://icap-mum.rbi.qa.forcepoint
Reset
Save
Tenant Settings
User Cookies Setting(s)
Save User Cookies
Session Timeout
Session Timeout (In Min)
5
Data Privacy
Data Storage Period (In Days)
30
Safe Preview
Enable Safe Preview
OPSWAT Configuration
Server URL
OPSWAT Server URL
API Key
OPSWAT API key for authentication
Rule Name
OPSWAT rule name for the analysis
Check Configuration
Reset
Save
Policy Settings
Forcepoint Threat Intelligence Service
Enable FTIS
Reset
Save

Settings Widgets

Widgets	Description
Notification Settings	Configures the settings for sending notifications to Forcepoint RBI administrators. You can choose to send notifications over email, or choose to send no notifications.
Email Template Parameter(s)	Configures the URL from where administrators can make all necessary configurations in Forcepoint RBI. You must configure this field with the tenant URL (`https://<mycompany>rbi.forcepoint.net`). **Note** You can set this parameter one time only. After it is saved, you cannot edit it.
User Cookies Setting(s)	Saves cookies for external websites accessed through Forcepoint RBI to ensure accessibility and user experience. Anonymous user cookies are not saved. **Note** This setting is applicable for signed in users only. Forcepoint RBI v5.5 only allows anonymous users.
Session Timeout	Indicates the time in minutes of inactivity before Forcepoint RBI terminates the session.
Data Privacy	Configures the number of days that user-identifiable data should be stored.

Safe Preview	Enables or disables the Safe Preview mode, that allows a user to safely preview a file in a pop-up window before the user can download the file.
	
	Note
	- You must disable the Safe Preview mode to allow a user to directly download a file without the need to safe preview the file.
	- The user must have the pop-ups feature enabled in the browser for the Safe Preview mode to function properly.
	- This mode is enabled by default.
	- The Safe Preview mode is supported only for the following file formats:
	  - Image Files (jpg, jpeg, png, gif, tiff, ai, and raw)
	  - Microsoft 365 documents (xls, xlsb, xlsx, xltx, xlsm, ppt, pptx, pptm, pot, potm, doc, docx, dot, dotm, dotx and xml)
	  - Microsoft Visio (vsdx)
	  - OpenOffice Documents (odt, ods and odp)
	  - Portable Document Format (pdf)
	  - Rich Text Format (rtf)

Widgets	Description
OPSWAT Configuration	Configures OPSWAT Content Disarm and Reconstruction to support sanitization and reconstruction of files during file download or upload policy. **Note** ■ To fetch the list of static IPs to be whitelisted, click the IP icon. For more information about Forcepoint RBI static IP list per region, see Knowledge Base article 40786 . ■ File sanitization for password protected files is not supported in the current release.
Forcepoint Threat Intelligence Service	Enables the Forcepoint Threat Intelligence Service (FTIS) to power Safe Surf, Smart Isolation, Smart Redirection, and category-based policies.
Override Isolation Mode	Selects the type of isolation mode for a category, or a URL to override the isolation mode that is determined by FTIS.
Override User Agent	Configures the user agent to use for rendering a URL. The configured user agent overrides the user agent that is selected by default for the URL.

Override Isolation Mode

The override isolation mode feature allows administrators to manually select the type of isolation mode for a URL.

The type of isolation mode selected for a URL overrides the isolation mode that is determined by Forcepoint Threat Intelligence Services. The isolation modes that are available to select are secure rendering and secure streaming.

Note

1) This feature is valid even if the Smart Isolation mode is in enabled or disabled state.

2) This feature is not applicable for web applications and their isolation mode cannot be overridden.

Related concepts

Secure Streaming and Secure Rendering isolation modes on page 81

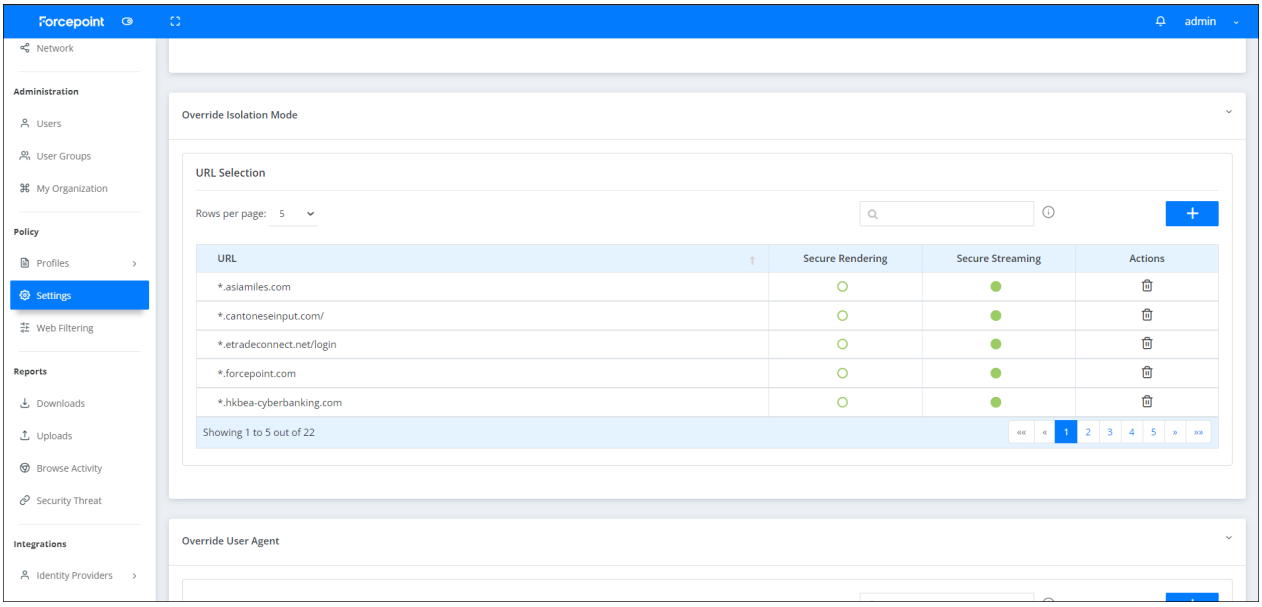
URL Selection

Choose the type of isolation mode for a URL to override the default isolation mode of the URL.

Steps

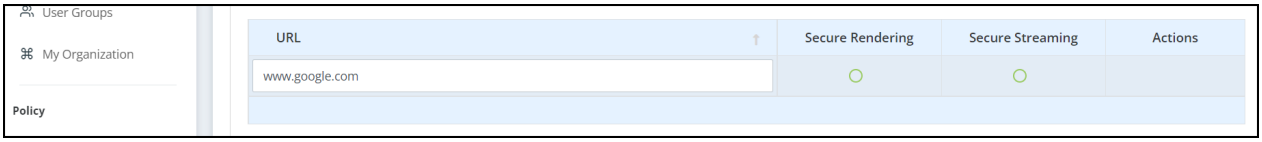
1) Sign in to Forcepoint Remote Browser Isolation.

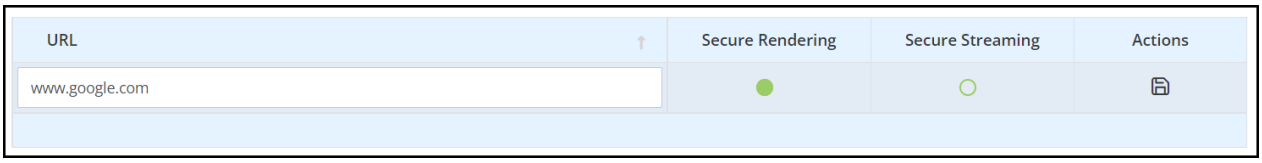
2) Go to **Policy** > **Settings**.



3) In the **Override Isolation Mode** section, under **URL Selection**, Click the **+** icon.

4) Enter the URL name in the **URL** field, and then select either **Secure Rendering** or **Secure Streaming**.





5) Click the **Save** icon under the **Actions** column.

Override User Agent

The override user agent feature allows an administrator to manually configure a user agent to use for rendering a URL, or URLs.

The user agent that is configured for a URL, overrides the default user agent for the URL that is selected by default. This helps to fix rendering issue of the URL by using a more appropriate user agent.

Note

You can choose to configure multiple URLs to use a same user agent or configure multiple URLs to use different user agent.

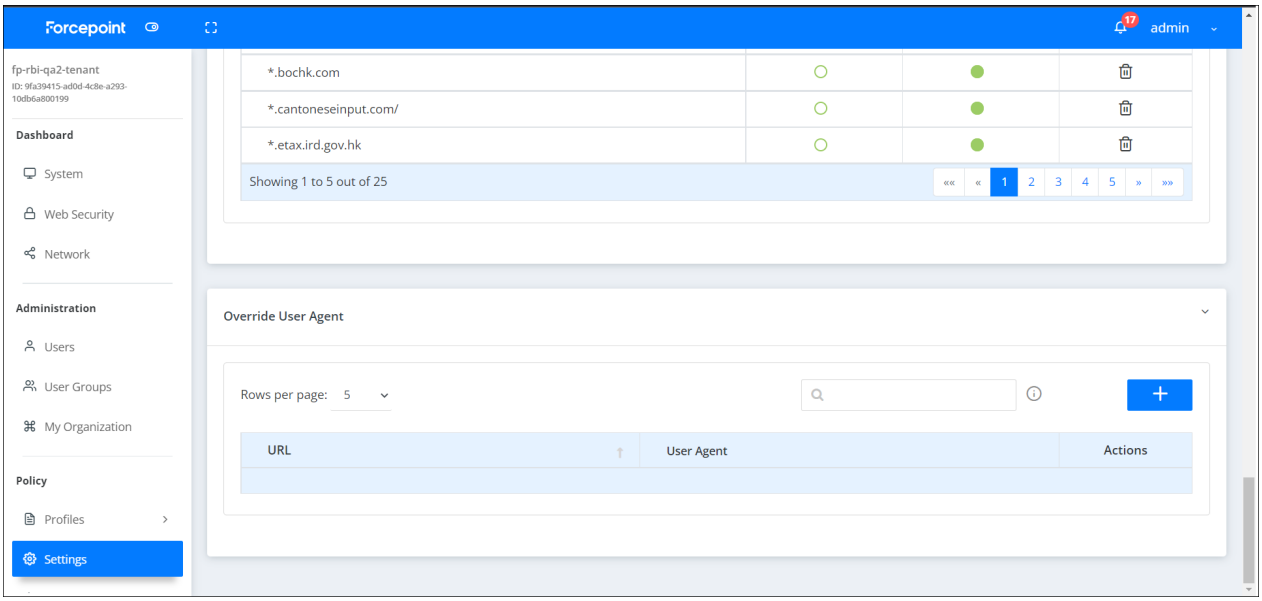
Configure a User Agent

Configure a user agent for a URL from the Policy settings page.

Steps

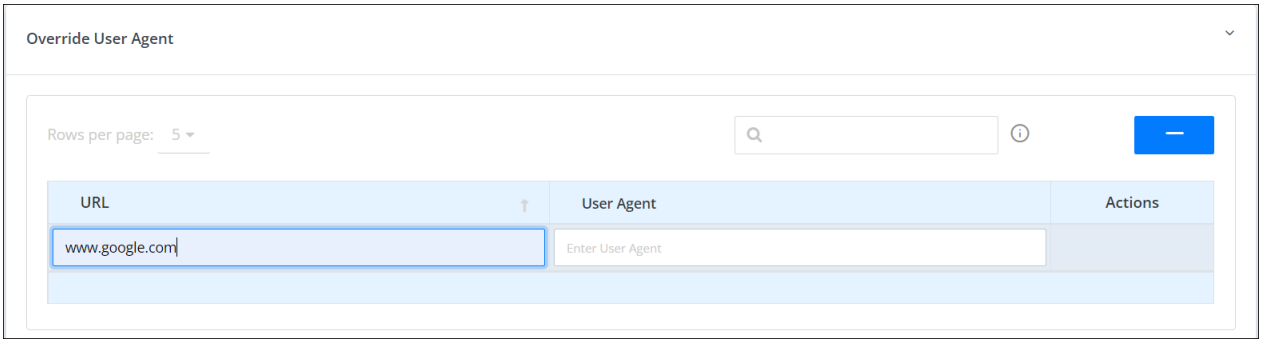
1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to the **Policy** > **Settings** page.

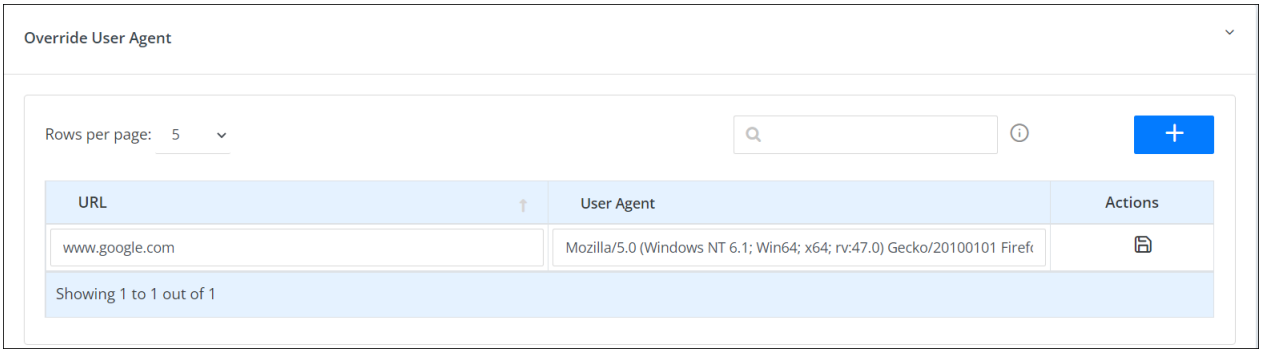


3) In the **Override User Agent** section, click the **+** icon.

4) Enter the URL name in the field, in the **URL** column.



5) Enter the preferred user agent string in the field, in the **User Agent** column.



6) Click the **Save** icon in the **Actions** column.

Edit a User Agent

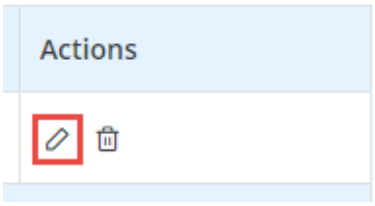
Edit a user agent for a URL from the Policy settings page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to the **Policy** > **Settings** page.

3) In the **Override User Agent** section, click the **Pencil** icon in the **Actions** column.



4) Edit the user agent as needed.

5) Click the **Save** icon in the **Actions** column.

Delete a Configured User Agent

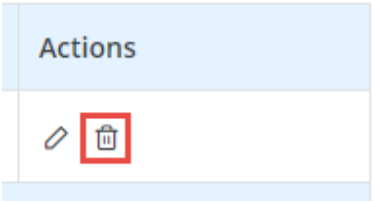
Delete a configured user agent from the Policy settings page. You can delete any user-configured user agent.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to the **Policy** > **Settings** page.

3) In the **Override User Agent** section, click the **Trashcan** icon in the **Actions** column.



4) Click the **Confirm** button.

Web Filtering

To enable Forcepoint Remote Browser Isolation customers to control web access within the Remote Browser Isolation sessions, web filtering feature is added. The following Web filtering features are available for both FRBIF (Forcepoint RBI Full) and FRBIS (Forcepoint RBI Selective) customers:

- Block URL and Categories
- Category Override
- Trust URL and Categories are available in RBI Cloud and On-prem proxy chaining.

Note

For URL redirect connection, Trust URL and Categories are not available for both FRBIF and FRBIS subscriptions.

Note

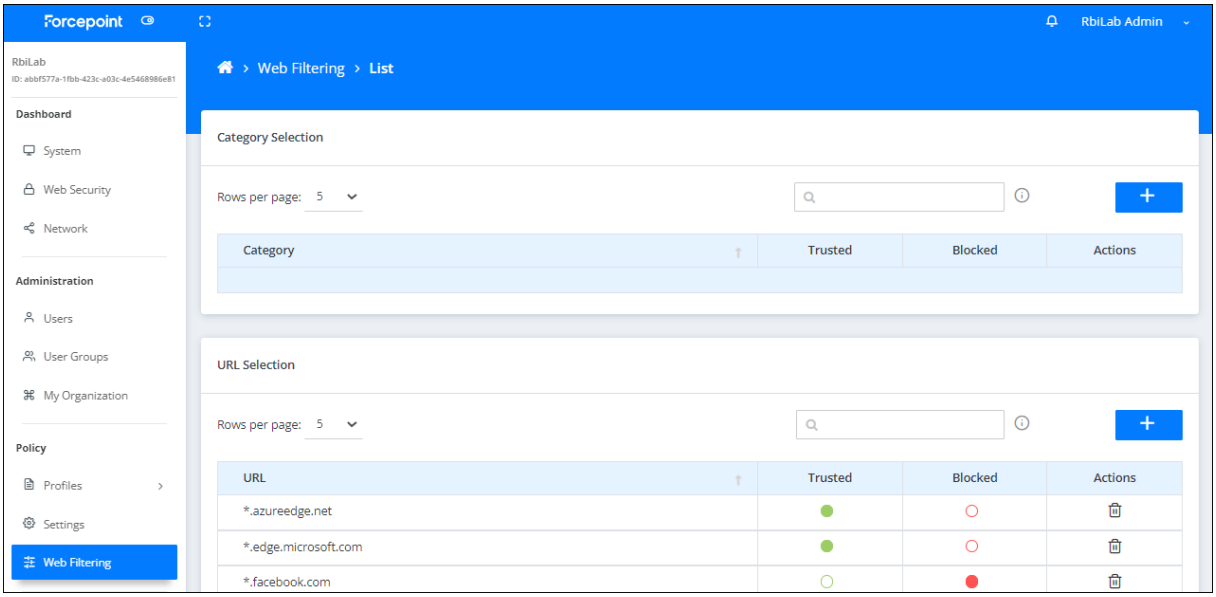
For rendering a trusted webpage correctly, make sure to add all the URL's or domains requested from the web page in the Trusted URL's list.

Category Selection

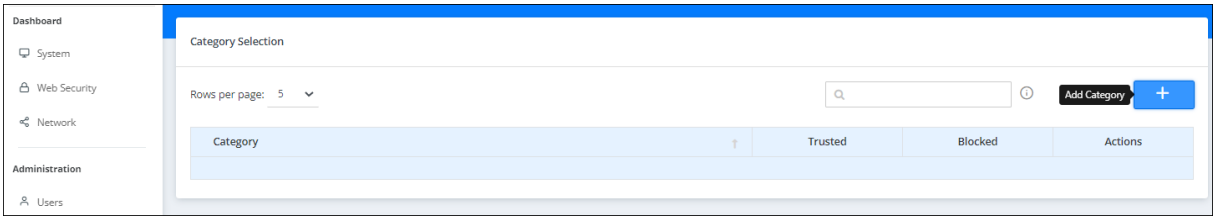
Steps

1) Sign in to Forcepoint Remote Browser Isolation.

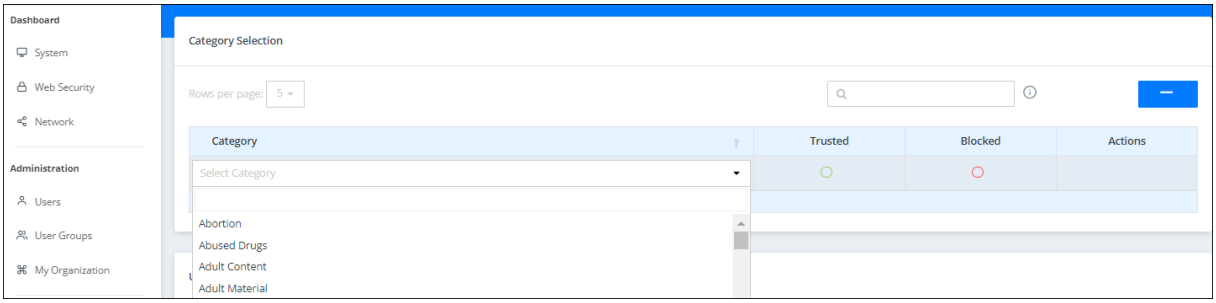
2) Go to **Policy** > **Web Filtering**.

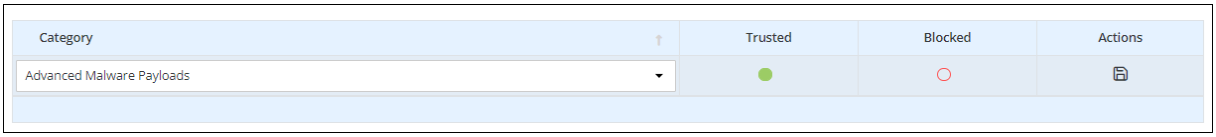


3) Click **+ Add Category** under **Category Selection**.



4) Select the suitable category available under **Category** drop down list and select either **Trusted** or **Blocked**.





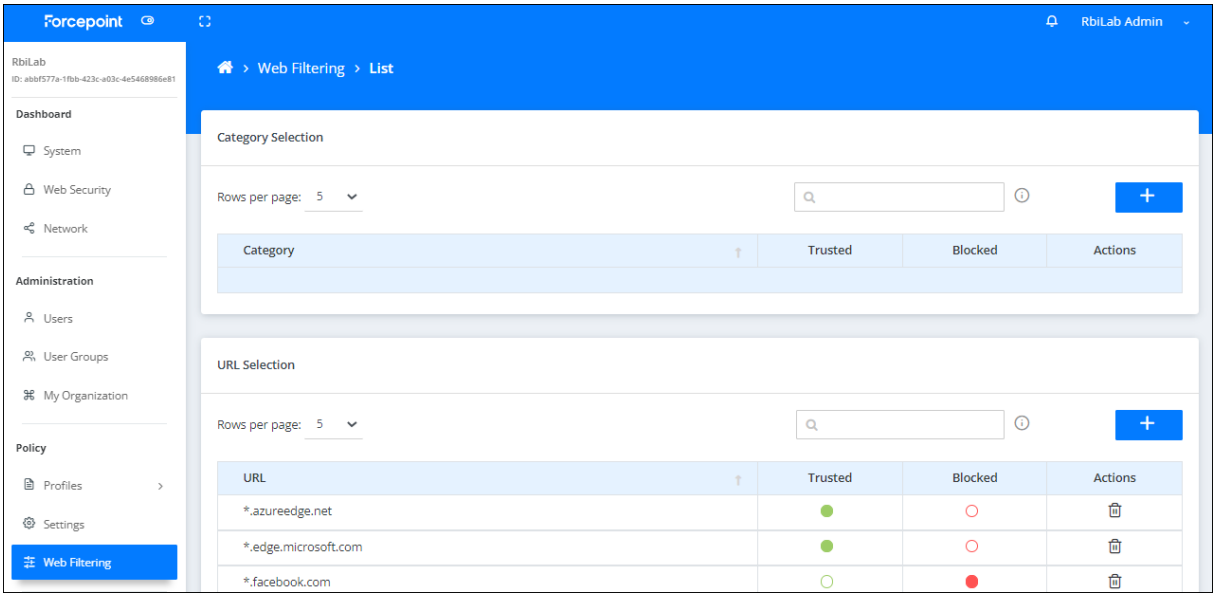
5) Click **Save**.

URL Selection

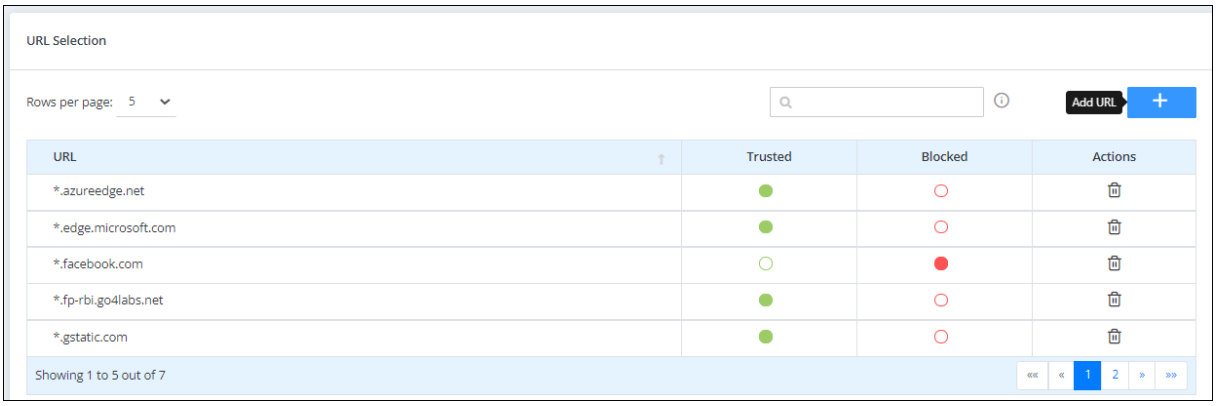
Steps

1) Sign in to Forcepoint Remote Browser Isolation.

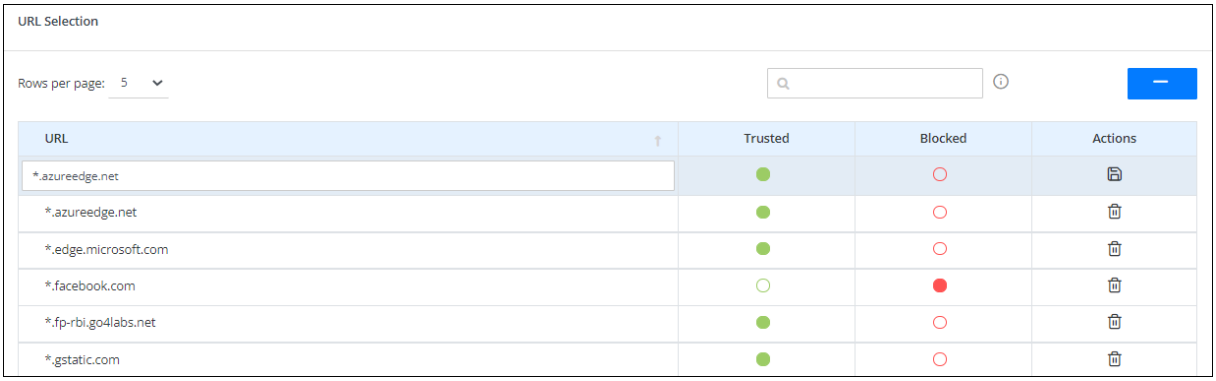
2) Go to **Policy** > **Web Filtering**.



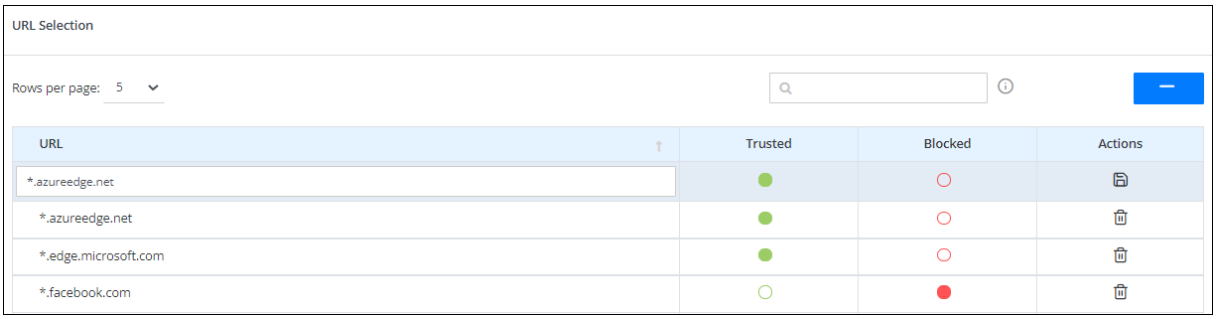
3) Click **+ Add URL** under **URL Selection**.



4) Enter the complete or partial URL under **URL**.



5) Select either **Trusted** or **Blocked**.



6) Click **Save**.

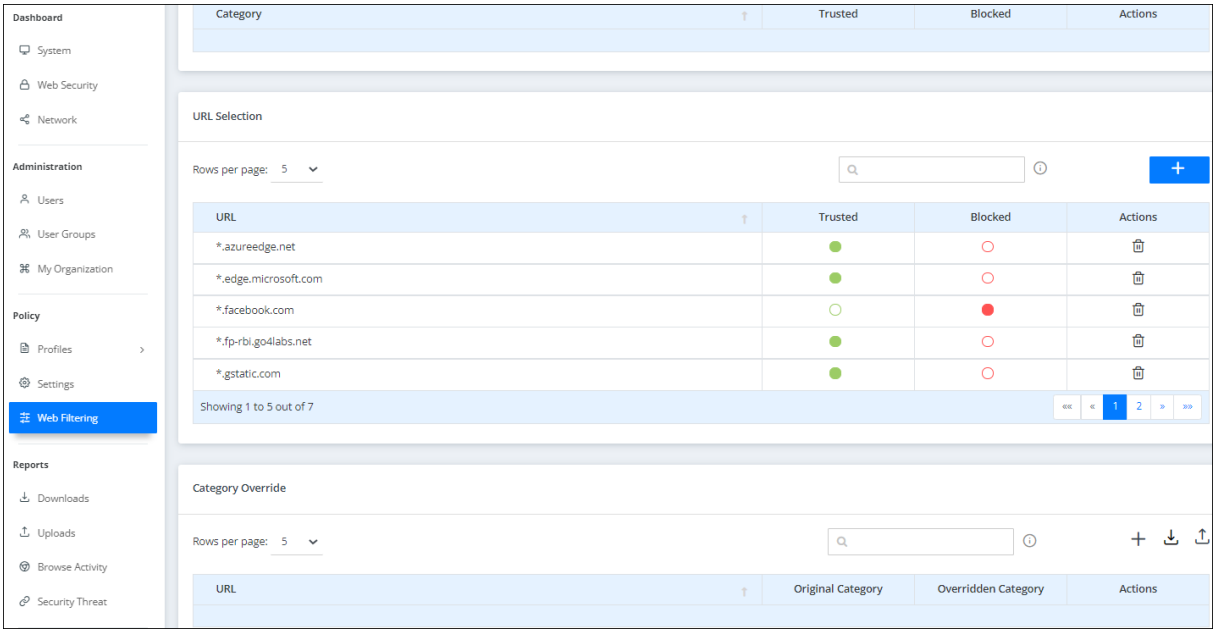
Category Override

The Forcepoint Threat Intelligence Services provide full website categorization for popular websites and allows administrators to block selected categories. The category override feature allows administrators to re-classify certain websites as a different category. The new category provided by the administrator overrides the category determined by Forcepoint Threat Intelligence Services.

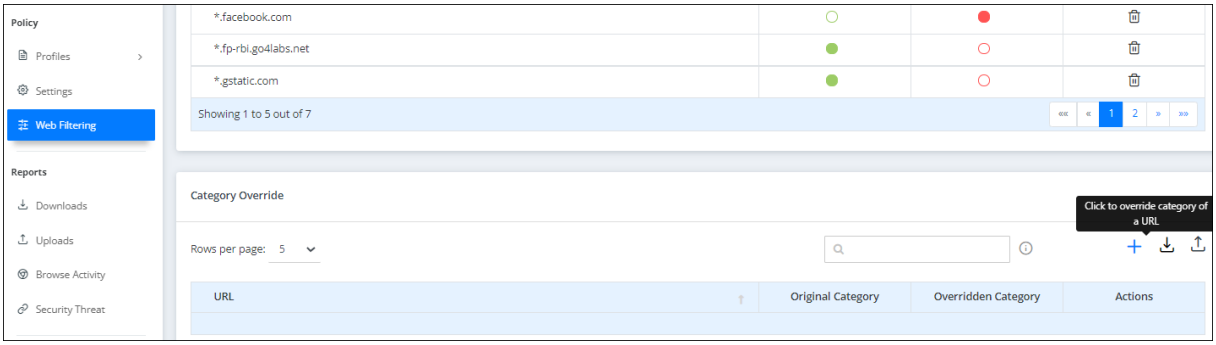
Steps

1) Sign in to Forcepoint Remote Browser Isolation.

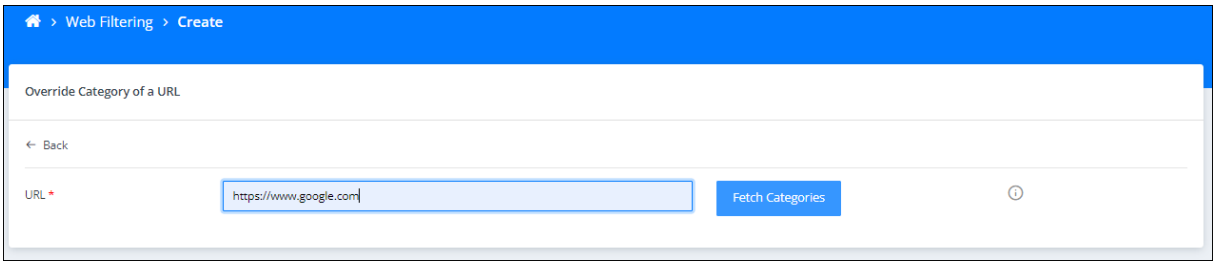
2) Go to **Policy** > **Web Filtering**.



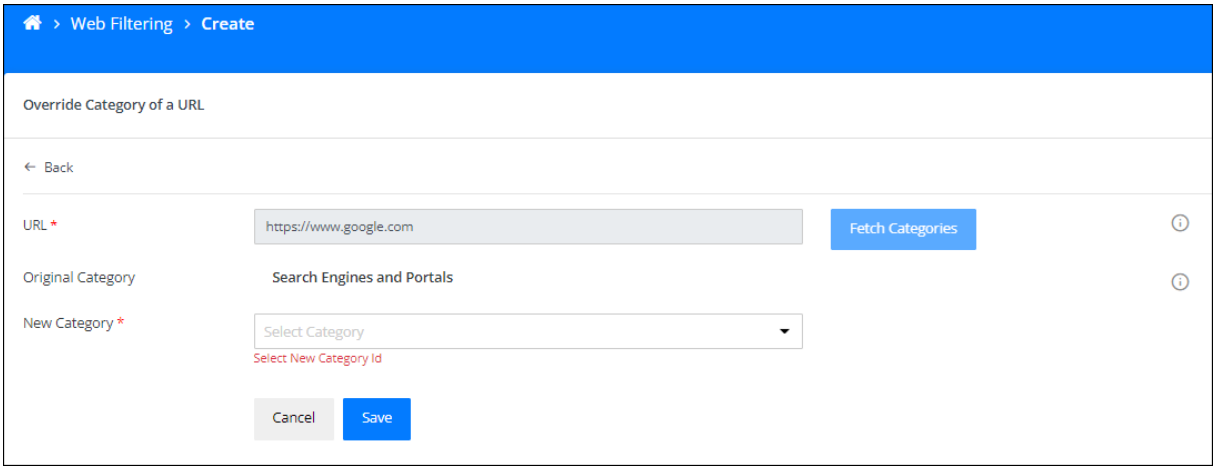
3) Click **+ Create Category Override** under **Category Override**



4) Enter the website address in the **URL** field, then click **Fetch Categories**.



5) The **Original Category** is shown, along with the **New Category** to be entered. Select a **New Category** to replace the original category.



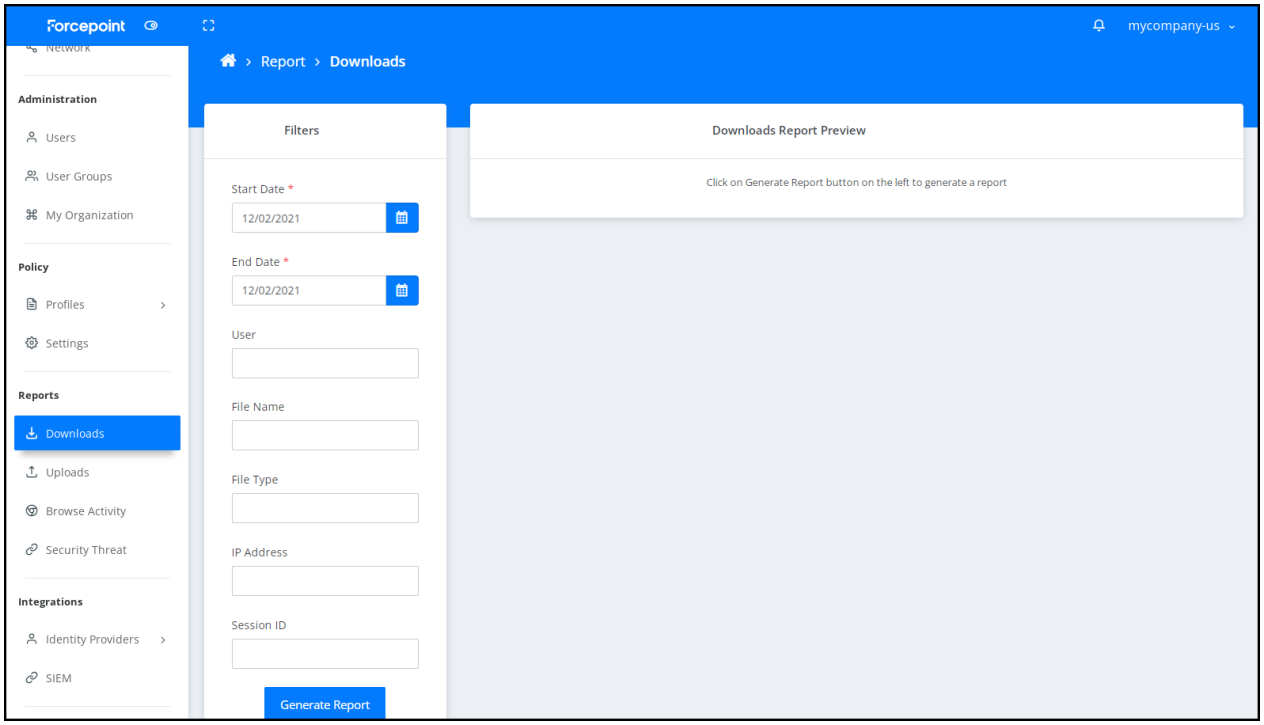
6) Click **Save**.

Chapter 7

Reports

Contents

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



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.
Security Threat	Generate a report that shows the threat score for each website viewed through the remote browser.

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**.
3) Select the report filters:
   - Start Date (required)
   - End Date (required)
   - User
   - 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**.
3) Select the report filters:
   - Start Date (required)
   - End Date (required)
   - User
   - 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**.
3) Select the report filters:
   - Start Date (required)
   - End Date (required)
   - User
   - Category
   - IP Address
   - Session ID
   - Rendering Status
   - Client Browser
4) Click **Generate Report**.

Create a Security Threat report

The Security Threat report shows the threat score for each website viewed through the remote browser.

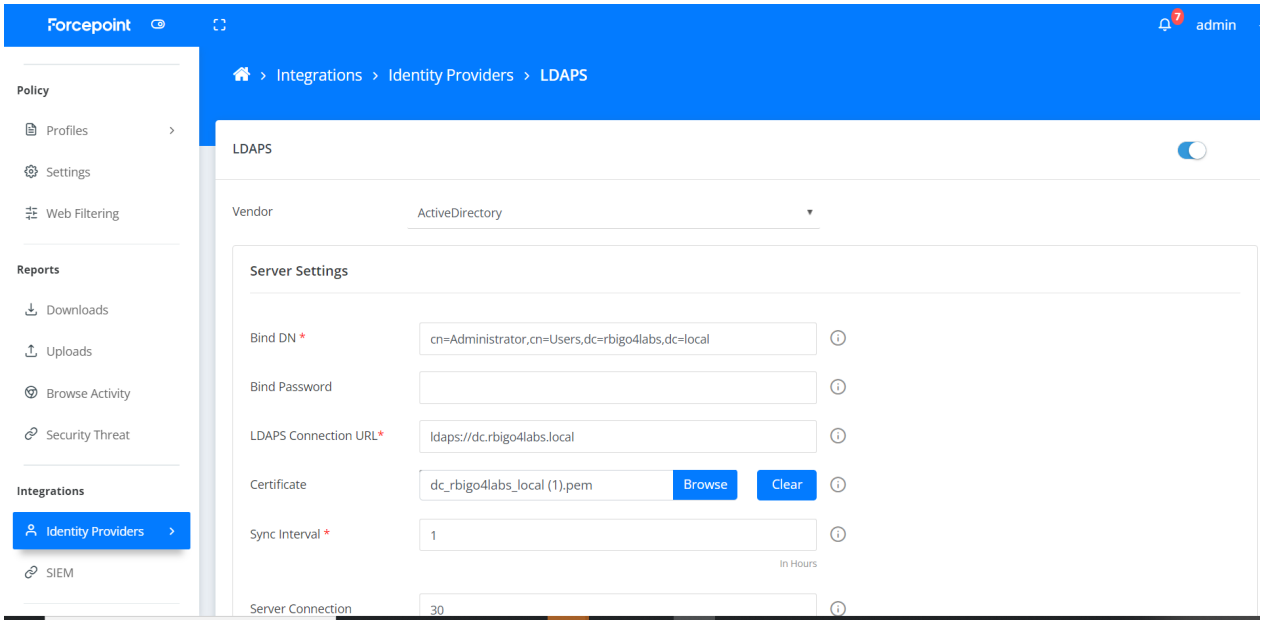
Steps

1) Sign in to Forcepoint Remote Browser Isolation.
2) Go to **Reports** > **Security Threat**.
3) Select the report filters:
   - Start Date (required)
   - End Date (required)
   - User
   - IP Address
   - Session ID
4) Click **Generate Report**.
5) To modify the report:

Chapter 8
Integrations

Contents

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



Integrations tabs

Tab	Description
Identity Providers	Configure an identity provider connection for user authentication.
SIEM	Configure an integration with a security information and event management (SIEM) solution to monitor security events, ensure appropriate action, and generate centralized reports.
DLP	Configure an integration with Data Loss Prevention (DLP), so that the DLP policies are applied to RBI isolated sessions to prevent data loss.

Identity Providers

The **Identity Providers** tab allows the ability to connection to an identity provider. After you configure or set up the connection here, you can select the identity provider as the authentication mode for users or user groups.

The supported identity providers are:

- LDAP/LDAPS
- SAML
- Proxy Authentication

Note

For stricter security control, LDAP and Proxy Authentication integration are not available for cloud tenants, but are available only for on-premises customers.

Before integrating an identity provider with Forcepoint RBI, the administrator needs to perform the following tasks:

1) Finalize the users by creating the usernames.
2) Create user groups and add the users to their respective groups.
3) Create binding or service accounts that will sync Active Directory with Forcepoint RBI.
4) Record the organizational path.

Related tasks

Configure the LDAP/LDAPS connection on page 116
Create a new SAML profile on page 119
Sign into Forcepoint RBI using a SAML profile on page 121
Edit a SAML profile on page 121
Download SP metadata on page 122
Delete a SAML profile on page 122
Configure the Proxy Authentication on page 123

LDAP/LDAPS

The **Lightweight Directory Access Protocol (LDAP)** or **Secure LDAP (LDAPS)** based identity provider allows user authentication by validating a username and password combination with the directory server that stores information about the user, user group and permissions. For example, Microsoft Active Directory Servers.

Note

Only LDAPS connection is supported for Cloud RBI tenants.

Configure the LDAP/LDAPS connection

Integrate Active Directory either through an LDAP or LDAPS connection.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Integrations** > **Identity Providers** > **LDAP**.
To configure LDAPS connection, Go to **Integrations** > **Identity Providers** > **LDAPS**.

3) By default, **ActiveDirectory** is selected in the **Vendor** drop-down menu.

4) Click the toggle switch to enable the configuration (**LDAP** or **LDAPS**).

5) Configure the **Server Settings**:

Parameter	Values	Description
Bind DN	CN=Administrator, CN=Users, DC=pnq, DC=aps	Required parameter. The usernames that will be used for searching and requesting authentication.
Bind Password		Password used by the LDAP user specified in the Bind DN.
Connection URL	LDAP/LDAPS	Required parameter. The hostname or IP address of the Active Directory server. **Note:** LDAP connection is not available for cloud tenants.
Certificate		Configure the CA client certificate for LDAPS. **Note:** This is not applicable for LDAP connection.
Start TLS	Enabled/Disabled	Enable or disable LDAP over SSL/TLS.
Sync Interval (In Hours)	Default value is 1 hour	Required parameter. The time in hours to wait between directory updates.
Server Connection Timeout (In Seconds)	Default value is 30 seconds.	Required parameter. The duration in seconds that Forcepoint RBI waits before considering the Active Directory server is unreachable.

6) Click **Check Connection** to verify that the connection to the **Connection URL** works.

7) Configure the **LDAP Schema**:

Parameter	Values	Description
Base DN	DC=pnq, DC=aps	Required parameter. Proper base for the Active Directory where Forcepoint RBI starts searching the directory structure.
Base DN	CN=John.Smith, CN=Users, DC=MyDomain, DC=com	Starting point to look for a user.
Group Base DN	"CN=Users, CN=Builtin, DC=MyDomain, DC=com"	Starting point to look for a group.

8) Configure the **User Schema**:

Parameter	Values	Description
Contact Number Attribute	CN=Telephone-number	Contact number of the user.
Display Name Attribute	cn=Display-Name	Required parameter. The user attribute whose value is the display name.
Email Attribute	cn=E-Mail-Address	Required parameter. The user attribute whose value is the email address.
Filter	(&objectCategory=person) (objectClass=user))	Required parameter. Select the users that match the filter. This can be used to limit the number of users with access to Forcepoint RBI.
Fixed ID Attribute	sAMAccountName	Required parameter. This is a fixed attribute in LDAP. It is used to search user/group in the database and based on the availability of a match, the user or user groups are updated or created.
Group Member Attribute	memberOf	Required parameter. This attribute defines the members of users in the user group.
User Attribute	sAMAccountName or userPrincipalName	Required parameter. The attribute whose values match with the username part of the credential entered by the users when logging into Forcepoint RBI.

9) Configure the **Group Schema**:

Parameter	Values	Description
Filter	(&objectCategory=group)	Required parameter. Criteria to filter or limit the number of groups that are imported to Forcepoint RBI.
Fixed ID Attribute	cn for OpenLDAP, name for AD	Required parameter. This is a fixed attribute in LDAP. It is used to search user groups in the database and based on the availability of a match, the user groups are updated or created.
Name Attribute	cn for OpenLDAP, name for AD	Required parameter. Select the groups that match the filter.

10) Click **Sync Now** to sync the settings and click **Update** to save the Active Directory settings.

SAML

The **Security Assertion Markup Language (SAML)** based identity provider allows user authentication by transferring identity data between two parties, that is an identity provider and a service provider.

Identity Provider: It performs the authentication and passes the identity data of the user and authorization level to the service provider. For example, Okta.

Service Provider: It trusts the identity provider and in turn authorizes the user to access the requested resource. For example, Salesforce.

Create a new SAML profile

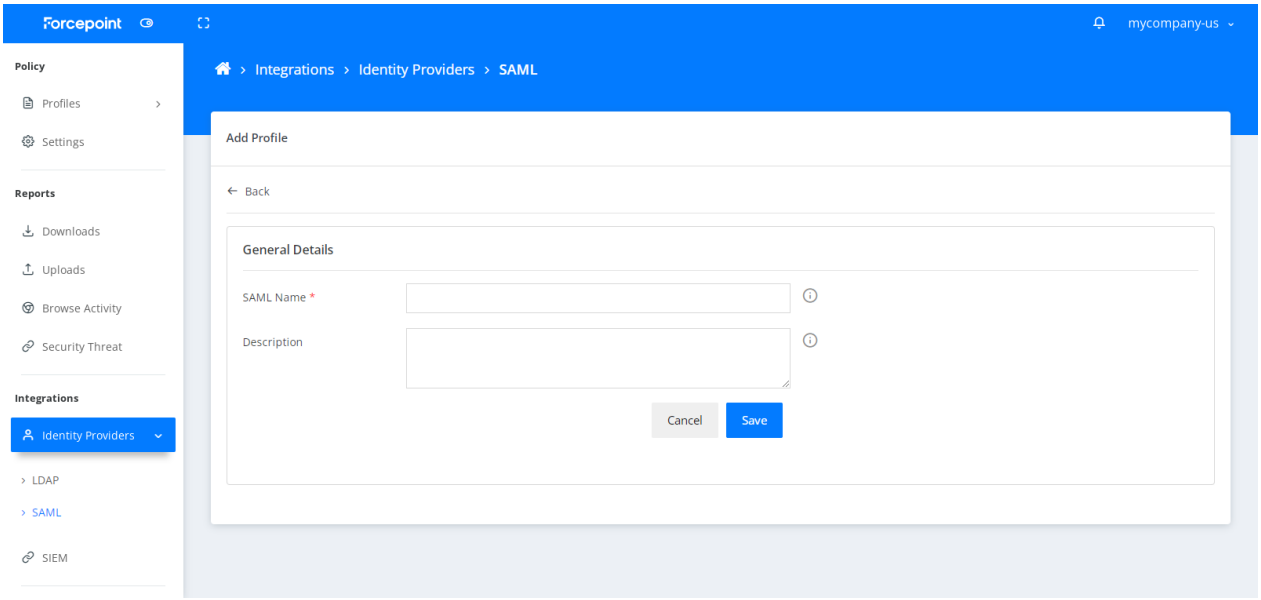
Create new SAML profiles through the SAML Identity Providers page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Integrations** > **Identity Providers** > **SAML**.

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



4) Enter the **SAML Name** and **Description**.

Note

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

5) Click **Save**. The profile is saved and it opens with the **Edit Profile** page.

Note

After the initial profile is saved, two additional read-only fields are shown in the **General Details** section: **ACS URL** (the URL location where the SAML assertion is sent with an HTTP POST) and **Logout Response URL** (the URL location on the service provider where the identity provider sends its sign out response).

6) In the **IdP Metadata** section, select the **IdP Metadata** option from the drop-down menu. This selection defines how Forcepoint RBI gets the SAML identity provider metadata.

7) After you select the **IdP Metadata** option, complete the other fields in this section. Some fields are only available with specific **IdP Metadata** options:

- **IdP Metadata File**: The SAML metadata file from the identity provider. This field is available if you selected **IdP Metadata File** from the **IdP Metadata** drop-down menu. After you provide the metadata file, the other fields auto-populate.
- **IdP Metadata URL**: The SAML metadata URL from the identity provider. This field is available if you selected **IdP Metadata URL** from the **IdP Metadata** drop-down menu. After you provide the URL, click **Get Metadata** to auto-populate the other fields.
- **IdP Certificate**: The SAML identity provider certificate.
- **End-point URL**: The SAML identity provider endpoint URL to which the SAML authentication request is sent.
- **Issuer URL**: A unique identity provider identifier where the security assertion originated.
- **Single Log-out URL**: The SAML URL for logging out of the identity provider.:

8) Click **Save**.

9) A pop-up window displays asking if you want to download the SP metadata. Click **Yes** to download the **SPMetadata.xml** file. If you click **No**, you can download the metadata file later from the SAML Profiles page.

10) Use the **SPMetadata.xml** file to configure the identity provider.

Sign into Forcepoint RBI using a SAML profile

After you configure the SAML profile, users can select the SAML profile when they sign into Forcepoint RBI.

Steps

1) On the Forcepoint Remote Browser Isolation sign in page, open the top drop-down menu and select the SAML profile.

2) Click **SAML Sign In**.

3) The sign in screen for the identity provider opens. For example, if you selected an Okta SAML profile, then the Okta sign in page opens.

4) Enter the credentials, then click the sign in button.

5) If the authentication is successful, then the account signs into the Forcepoint RBI Admin Portal.

Edit a SAML profile

After a SAML profile is created, you can edit the information for an existing profile through the SAML Identity Providers page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Integrations** > **Identity Providers** > **SAML**.

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

4) Edit the profile as needed.

5) Click **Save**.

Download SP metadata

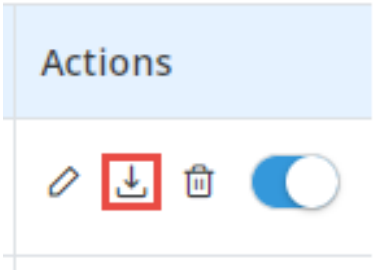
Service Provider (SP) metadata contains the information needed to interact with the identity providers. If you did not save the SP metadata file when you created the SAML profile, you can download it at any time from the SAML Profiles page.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Integrations** > **Identity Providers** > **SAML**.

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



4) A **SPMetadata.xml** file is downloaded to your browser's Downloads folder.

5) Use the **SPMetadata.xml** file to configure the identity provider.

Delete a SAML profile

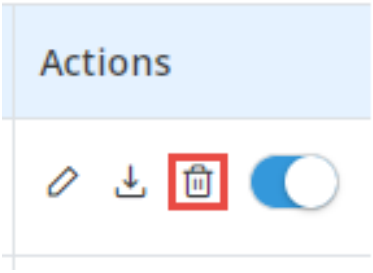
Delete a SAML profile if it is no longer needed. You can delete any user-created profile.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to **Integrations** > **Identity Providers** > **SAML**.

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.

Proxy Authentication

The proxy authentication-based identity provider option enables the X-Header authentication for a tenant.

Hence, RBI authentication is not required for the tenant when the traffic is redirected from Forcepoint Web Security to Forcepoint Remote Browser Isolation.

Note

1) The users who are authenticated by using the X-header authentication can now access the RBI session without the need to login again to Forcepoint RBI.

2) The users that are created via proxy authentication cannot login into Admin Portal as an admin user.

3) In case the Proxy Authentication option is enabled and the user information is not sent to Forcepoint RBI. The user is displayed with the RBI login page.

4) Any user that is created via proxy authentication can be deleted from the **Administration** > **Users** tab.

5) This option is available only for on-premises tenants, for whom RBI proxy is enabled.

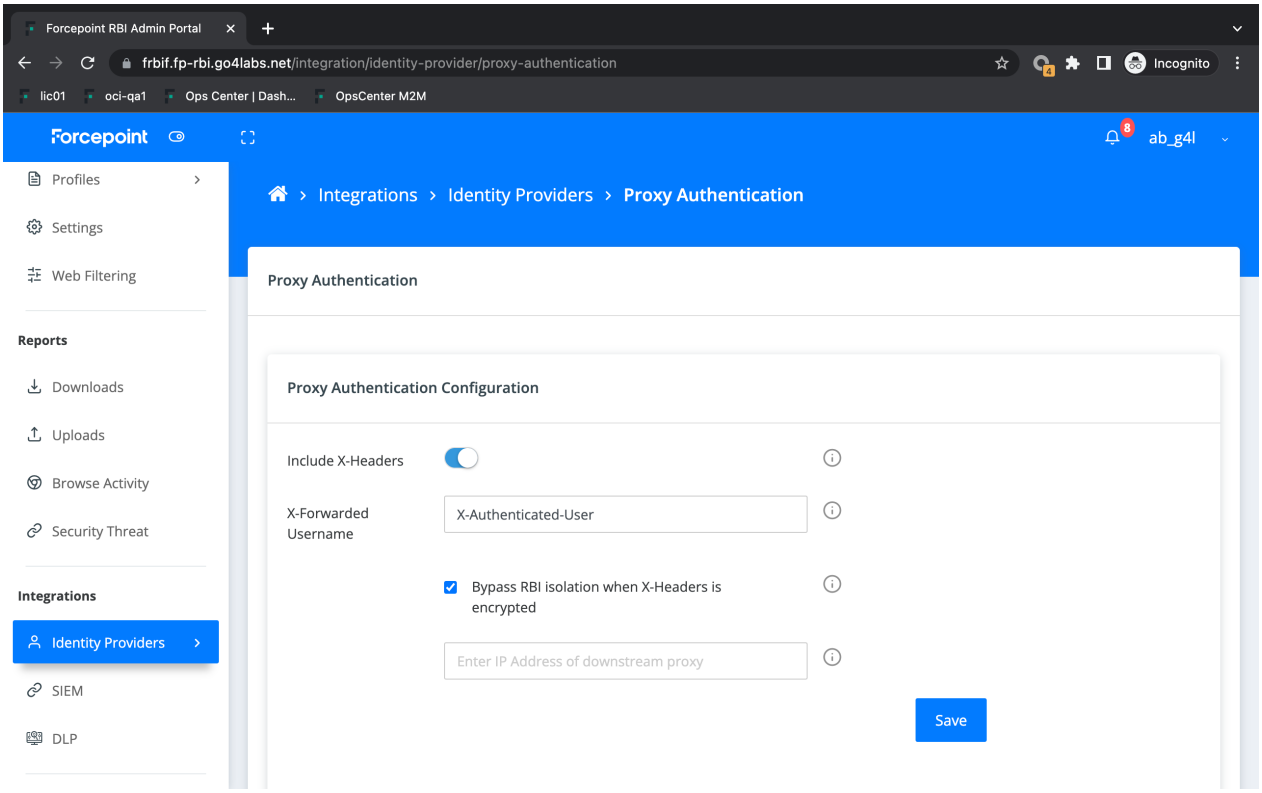
Configure the Proxy Authentication

On the **Proxy Authentication** page, you can configure the X-Header authentication settings. Before an administrator configures the **Proxy Authentication**, the administrator must ensure there are no active session for the tenant.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to the **Integrations > Identity Providers > Proxy Authentication** page.



3) Click the **Include X-Headers** toggle switch to enable or disable the X-Header authentication via proxy chaining for incoming traffic requests.

Note

In the proxy chain, incoming traffic request is from the child (downstream) proxy when RBI is the parent (upstream) proxy.

4) Enter the username value to use for the X-Header authentication in the **X-Forwarded Username** field.

5) Select the option **Bypass RBI isolation when X-header is encrypted** to enable isolation bypass when downstream proxy has SSL decryption turned off.

This option is disabled by default.

6) Type the IP address of the downstream proxy.

Note

- If the IP address does not match, user is prompted for authentication.
- For multiple IP addresses, comma (,) is used as a separator.

7) Click the **Save** button.

SIEM Integration

When Forcepoint RBI is used in an enterprise environment to secure the browser activities of users, administrators can monitor and view the user activities in a SIEM server.

Integrating Forcepoint RBI with the enterprise SIEM allows administrators to:

- Monitor security events and ensure appropriate action
- Troubleshoot deployment issues
- Generate centralized reports

Create a new SIEM integration

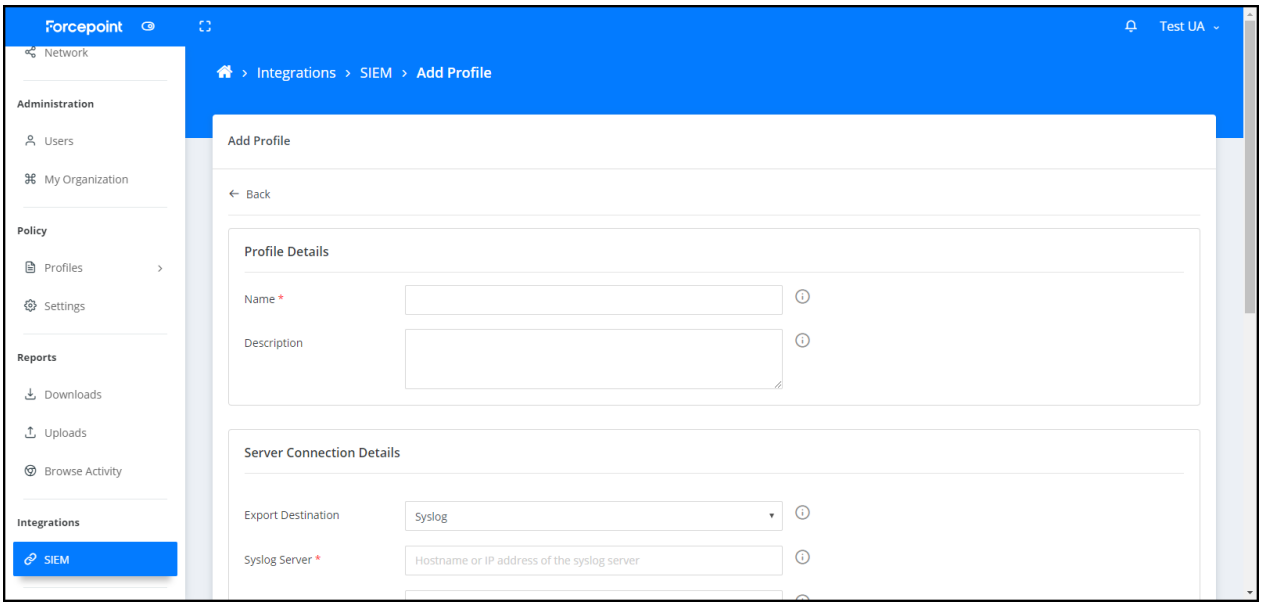
Create a new profile to connect Forcepoint RBI to a SIEM tool.

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**

   a) For **Export Destination**, **Syslog** is the only option and is selected by default.

b) In the **Syslog Server** field, enter the host name or the IP address of the Syslog server. This field is required.

c) In the **Server Port** field, enter the port number of the server. This field is required

d) Select the **Transport Protocol**. **UDP** is selected by default.

e) Click **Check Connection** to verify that Forcepoint RBI can connect to the Syslog server.

6) Under **Log Details**:

a) For **Log Format**, **JSON** is the only option and is selected by default.

b) Select the **Log Level**.

c) 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

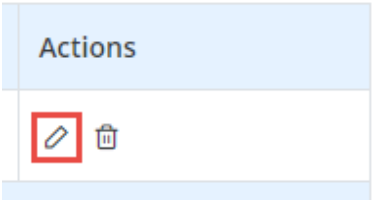
After the SIEM profile is created, you can edit the information through the SIEM settings page.

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

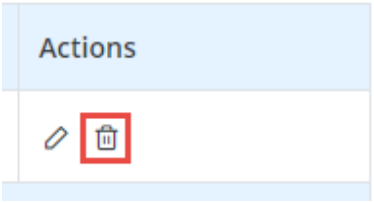
Delete a SIEM profile if it is no longer needed. You can delete any user-created profile.

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.

DLP Integration

Forcepoint RBI can be integrated with Data Loss Prevention (DLP), so that the DLP policies are applied to RBI isolated sessions to prevent data loss.

The DLP policies are applicable for both the file upload and HTTP post actions in the RBI isolated sessions. The **Data Leakage Prevented** column is available in the table under the **Browse Activity Summary** section, in the **Dashboard** > **Web Security** tab. This column displays the number of incidents for both the HTTP Post and file uploads that are blocked by DLP policies for the user.

Note

1) RBI only supports analysis of files uploaded in isolated sessions as per the file size limit supported by DLP. For more information on DLP file size limit, refer to the **Forcepoint DLP Supported File Formats and Size Limits** documentation.

2) In case the error message that states "*Your request has been blocked to prevent the loss or theft of potentially sensitive data. Please refresh, if the page is unresponsive*" is displayed persistently. Please ensure to remove any restricted data that is shared in the current window.

The integration of Forcepoint RBI with DLP is done either by using the ICAP protocol for On-premises Forcepoint RBI or by ICAPS protocol for Cloud Forcepoint RBI.

Note

1) Forcepoint RBI is the ICAP client and DLP is the ICAP server.

2) The source (username or endpoint name), and destination URL of the RBI isolated sessions are sent to DLP.

3) When Proxy Authentication is enabled in RBI admin portal, and is used along with WCG configured in *Integrated Windows Authentication* mode and *Send user authentication to parent proxy* is enabled in WCG, then the *Username* is displayed in DLP console against the DLP incidents. If WCG-RBI integration is not configured for Proxy Authentication via X-Authenticated-user header, then the *Username* information will not be displayed in DLP console against the DLP incidents.

4) Forcepoint Security Manager is used to create user-level policies for DLP. The Username field has restriction that, it must contain only numbers and letters. RBI local username is an email address. Hence, if RBI authentication is used for DLP integration, the user-level policy cannot be applied.

Before you integrate DLP with Forcepoint RBI, make sure that the following requirements are met:

- The DLP Protector component is configured.

  Note

  The DLP-Protector/ICAP server is exposed over public IP Address and is accessible to RBI RBC cluster for port 1344 and 11344. A secure tunnel is configured using stunnel for Forcepoint DLP Protector ICAP communication. For more information, see Knowledge Base article 36918 .

- Forcepoint on-premises proxy (WCG) is configured to proxy chain the request to Forcepoint RBI.

  Note

  For more details on proxy chaining, refer to *Configuring Forcepoint RBI (Onpremises Deployment) in Proxy chaining mode with Forcepoint Content Gateway for Full isolation* section.

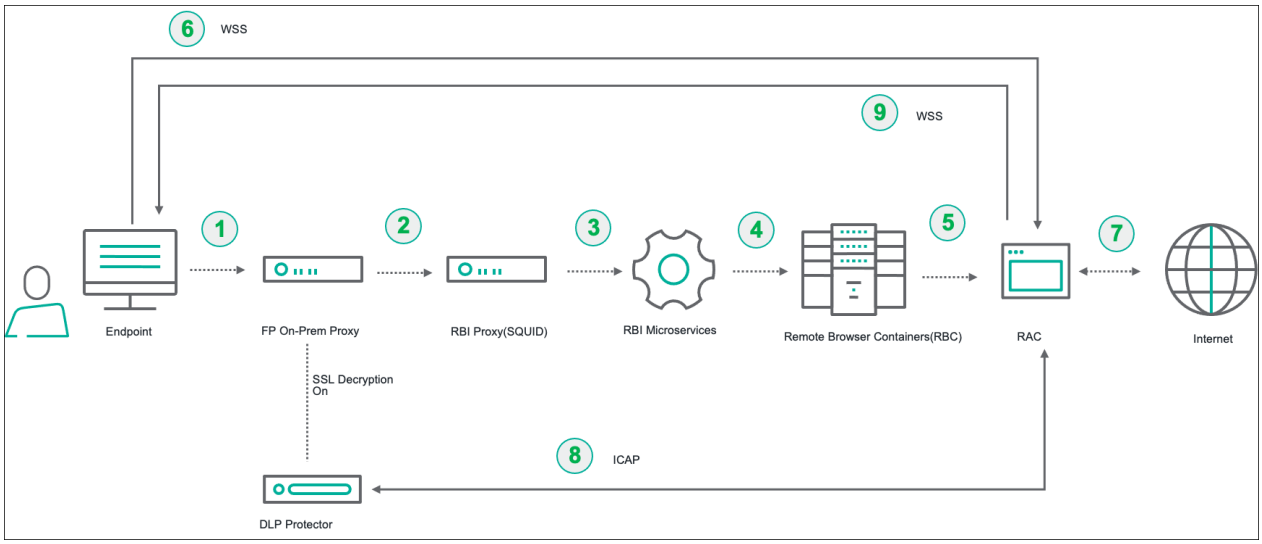
  Note

  For Cloud RBI proxy chaining, refer to *Configuring Forcepoint RBI (Cloud Deployment) in proxy chaining mode with Forcepoint Content Gateway for full isolation* section.

- The SSL decryption bypass for the RBI domain is configured in WCG. For example, *rbi.forcepoint.net.

Data Flow Diagram

DLP- RBI Integration- HTTP Post



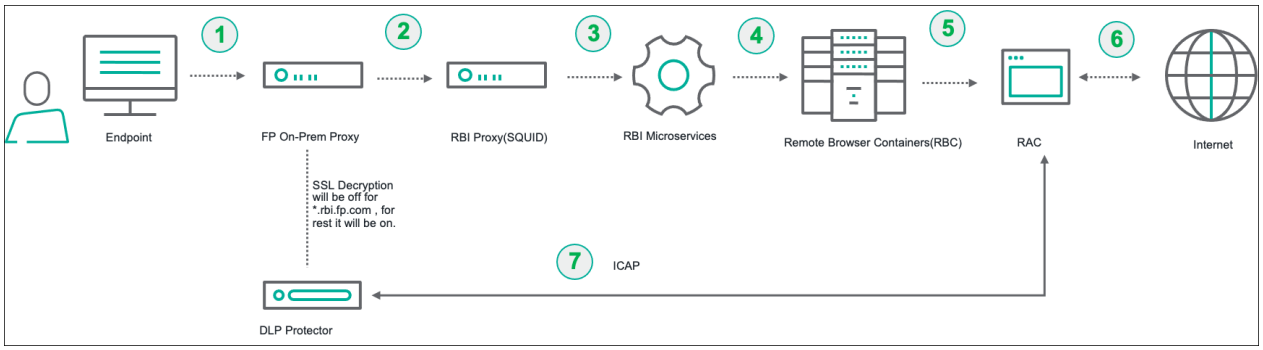
1. The user system is configured to point to Forcepoint WCG proxy, and the web requests are sent to WCG proxy.
2. The WCG proxy is configured to redirect all web requests to Forcepoint RBI proxy (parent proxy).
3. Forcepoint RBI proxy redirects the request to RBI microservices for user authentication and session initiation.
4. The user is assigned a RBI session in the Remote Browser Container cluster.
5. Each user is assigned a unique Remote Access Container (RAC) for remote browsing.
6. Once the user is assigned an unique RAC, the communication between the End user and the Remote browser container (RBC) happens over a Secured Web Socket connection (WSS)
7. The Web resource that is browsed by the end user is executed in the RAC.

   Note

   If a user does a HTTP post it is executed in the RAC, but the RAC is configured to redirect all HTTP posts to DLP Protector via ICAP protocol for evaluating against DLP policies.

8. The DLP evaluates the HTTP post request that is received from the RAC against the DLP policy. After the evaluation is completed the DLP responds with appropriate action as defined in the DLP policy (Block/Allow).
9. If the RAC receives the response from the DLP to block the HTTP post, RBI will block the HTTP post and notify the end user regarding the block action through RBI Nav bar notification.

DLP- RBI Integration- File Upload



1. The user system is configured to point to Forcepoint WCG proxy, and the web requests are sent to WCG proxy.
2. The WCG proxy is configured to redirect all web requests to Forcepoint RBI proxy (parent proxy).
3. Forcepoint RBI proxy redirects the request to RBI microservices for user authentication and session initiation.
4. The user is assigned a RBI session in the Remote Browser Container cluster.
5. Each user is assigned an unique Remote Access Container (RAC) for remote browsing.
6. The Web resource browsed by the end user is executed in the RAC.

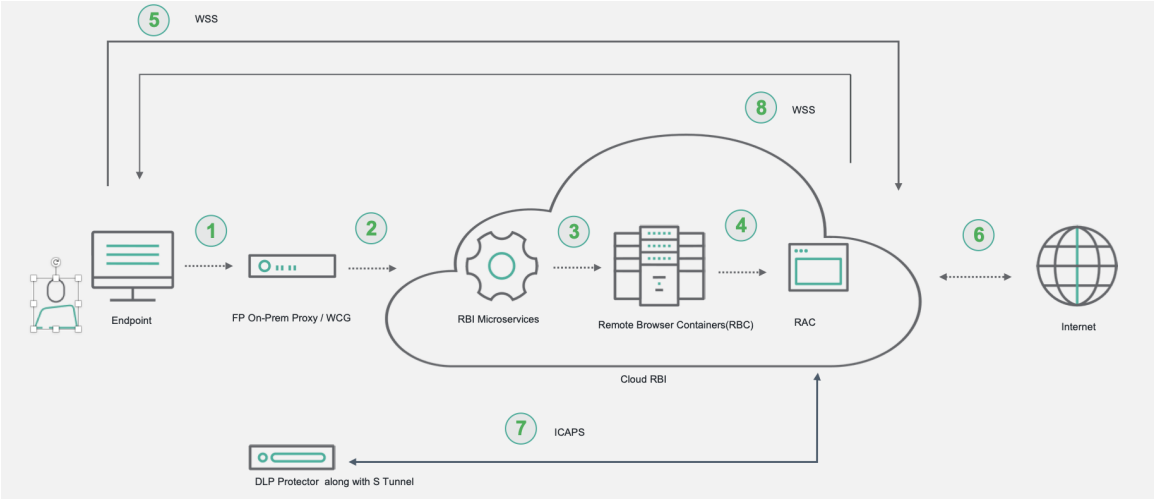
Note

1) The RAC is configured to redirect all file uploads to DLP Protector via ICAP/ICAPS protocol for evaluating against DLP policies.

2) If a user uploads a file through RBI, the file is first uploaded to RBI and is processed through CDR, and then sent to DLP protector for evaluating against DLP policies.

7. The DLP evaluates the file upload request that is received from the RAC against the DLP policy. After the evaluation is completed the DLP responds with appropriate action as defined in the DLP policy (Block/Allow). If the RAC receives the response from the DLP to block the file upload, RBI will block the file upload and notify the end user regarding the block action through RBI Nav bar notification.

On-prem DLP-ICAPS and RBI Cloud Integration



1. The user system is configured to point to the Web Security Cloud proxy or Web Security on-premises proxy, and the web requests are sent to the Web Security Cloud proxy/Web Security on-premises proxy.
2. The Forcepoint Cloud RBI consists of RBI Microservices, Remote Browser Container cluster, and RAC. The Web Security Cloud proxy/Web Security on-premises proxy redirects the request to RBI microservices for user authentication and session initiation.
3. The user is assigned an RBI session in the Remote Browser Container cluster.
4. Each user is assigned a unique Remote Access Container (RAC) for remote browsing.
5. Once the user is assigned a unique RAC, the communication between the End user and the Remote browser container (RBC) happens over a Secured Web Socket connection (WSS).
6. The Web resource that is browsed by the end user is executed in the RAC.

   Note

   Forcepoint Cloud RBI is configured to redirect all file uploads and HTTP posts to the DLP Protector via ICAPS protocol for evaluating against DLP policies.

7. The DLP evaluates the HTTP post/file uploads request that is received from the RAC against the DLP policy. After evaluation is completed, DLP responds with appropriate action as defined in the DLP policy (Block/Allow).
8. If the RAC receives the response from the DLP to block the HTTP post/file uploads, RBI will block the HTTP post/file uploads and notify the end user regarding the block action through RBI Nav bar notification.

Related concepts

Configuring Forcepoint RBI (On-premises Deployment) in proxy chaining mode with Forcepoint Content Gateway for full isolation on page 42

Configuring Forcepoint RBI (Cloud Deployment) in proxy chaining mode with Forcepoint Content Gateway for full isolation on page 44

Configure DLP Integration

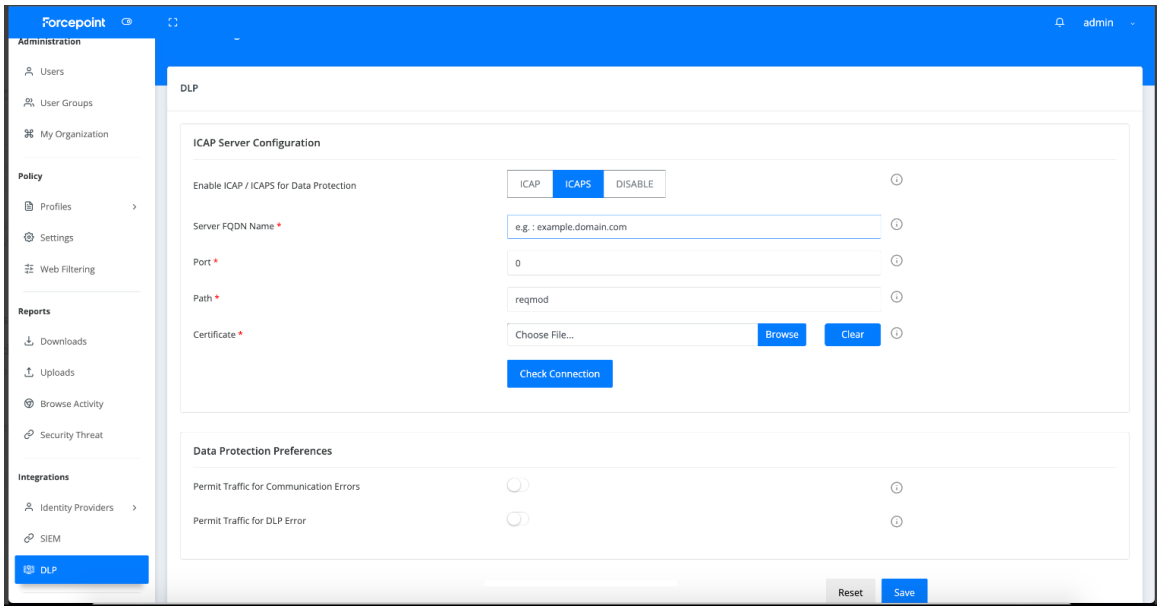
On the DLP page, do either of the following:

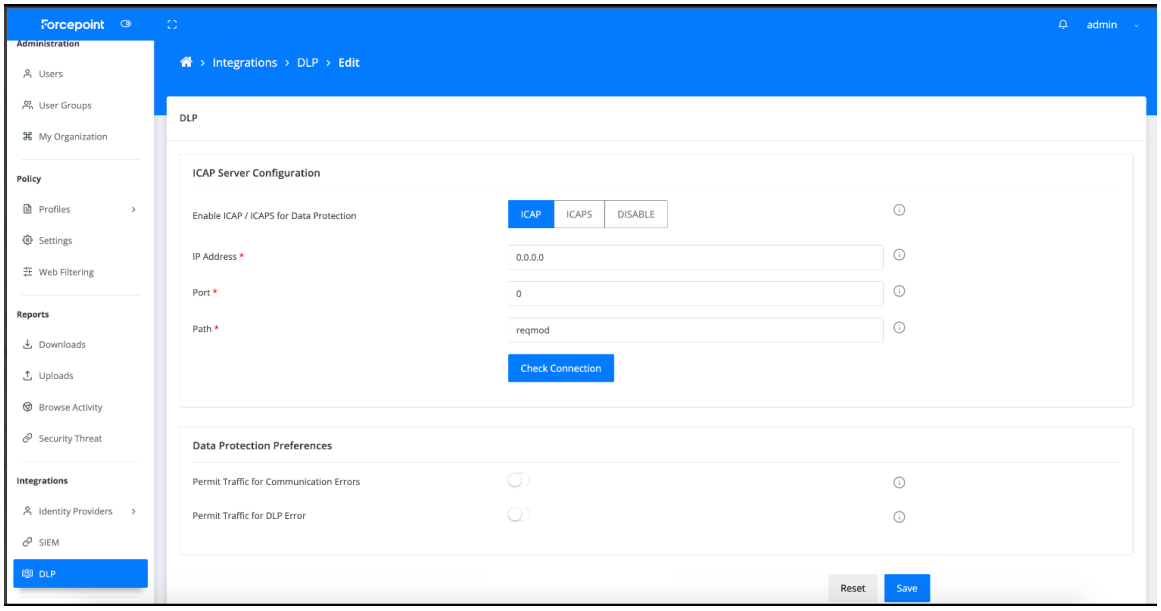
- For On-premise Forcepoint RBI, configure the ICAP or ICAPS protocol settings to allow DLP integration.
- For Forcepoint Cloud RBI, configure only the ICAPS protocol settings to allow DLP integration.

Steps

1) Sign in to Forcepoint Remote Browser Isolation.

2) Go to the **Integrations** > **DLP** page.





3) Under **ICAP Server Configuration**, click either **ICAP** or **ICAPS** option in the **Enable ICAP/ICAPS for Data Protection** to enable data protection.
To disable the data protection, select the **DISABLE** option.

4) For the ICAP server, enter the IP address in the **IP Address** field.
For the ICAPS server, enter the FQDN server name in the **Server FQDN Name** field.

5) Enter the port number of the ICAP/ICAPS server in the **Port** field

6) Enter the path value of the ICAP/ICAPS server in the **Path** field.

7) Browse the CA client certificate for ICAPS server.

Note

This is not applicable for ICAP server.

8) Click the **Check Connection** button to verify that Forcepoint RBI can connect to the ICAP/ICAPS server.

9) Under **Data Protection Preferences**, enable the **Permit Traffic for Communication Errors** toggle switch to allow traffic when there is a communication error. By default, this option is disabled.

Note

The communication error can occur due to one of the following reasons:

- DLP is not able to analyze files. For example, due to timeout.
- ICAP communication error.

10) Under **Data Protection Preferences**, enable the **Permit Traffic for DLP Error** toggle switch to allow traffic when DLP fails to analyze a file that exceeds maximum size limit. By default, this option is disabled.

Files are not uploaded when the toggle is disabled and shows an appropriate message to the user. However, once you enable the toggle, files are uploaded without showing any error to the user. The user can view the analyzed information both in upload reports and in the upload summary under **Web Security**.

11) Click the **Save** button.

Chapter 9

Localization Support

The Forcepoint RBI focuses on ensuring a seamless end user experience, where RBI delivered content matches the experience of the local web browser. This includes ensuring our international customers enjoy RBI in their native language and with locale specific keyboard support.

The Forcepoint RBI supports following while browsing in isolation:

- Localized rendering of web content
- Localized keyboard input
- Localized RBI messages (which includes localized FAB button tooltips)

Currently, following language locales have support for localized rendering, keyboard type-in, and end user notifications.

- Arabic
- Chinese (simplified)
- Chinese (traditional)
- German
- Hebrew
- Spanish
- Turkish

Additionally, localized rendering is supported for the following languages:

- Dutch
- French
- Italian
- Japanese
- Korean
- Portuguese (Brazil)
- Russian

Chapter 10

Product Updates

Contents

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.

On-prem OPSWAT CDR Integration Support

On-premises OPSWAT CDR is integrated with Cloud RBI to support automatic file sanitization for files downloaded or uploaded during an RBI session. RBI admins can enable OPSWAT CDR directly from the RBI Admin Portal, for more information, see Create a new policy profile on page 88.

Note

File sanitization for password protected files is not supported in the current release.

Previous updates

New features and product updates added in earlier releases.

On-prem DLP-ICAPS integration for RBI Cloud

On-prem DLP-ICAPS can now be integrated with Cloud RBI to ensure that data loss is prevented in RBI isolated sessions. It is recommended to use a secured ICAP protocol (ICAPS), which is a SSL/TLS encrypted ICAP-based communication, to integrate Cloud RBI with DLP. For more details, see Configure DLP Integration on page 131.

RBI architectural updates

Currently, the remote browsing container communicates with the control center located in the same region that of the container. As a result, roaming users might experience some latency while browsing.

With this new architecture, remote browsing container can communicate with control center located in any region after registering with that particular control center. For roaming users, browsing experience will significantly improve as the users will be assigned a session nearest to their region, based on Geo latency.

For more information regarding the list of Geo-location PoP available to RBI users, see Knowledge Base article 41549 .

Note

The new architecture is available only for RBI cloud deployment.

Some of the key advantages of the new architecture:

- Better Performance: Improves the browsing experience for roaming users.
- Security: For a secured approach, RBI administrator can open only port 443 instead of port range 30000 to 32767.
- Compliance: Post architectural update, RBI continues to be GDPR compliant.

Post the configuration change, new customers will use the `*rbi.forcepoint.net` service URL. Existing customers can continue using the `*rbi.forcepoint.com` service URL. Also, existing Block page customizations will continue to function as before once the Port 443 and Bypass rules are set as follows:

- Port 443 is required to be opened to access RBI service. Make sure, port 443 is open for both `*rbi.forcepoint.com` and `*rbi.forcepoint.net`, and for static IP address range if the RBI service is referred via the static IP address range.
- For cloud customers, add `*rbi.forcepoint.net` as an additional domain to the bypass list in the Cloud Portal proxy bypass settings.
- For on-premises customer, add `*.rbi.forcepoint.net` to SSL Decryption Bypass in the Forcepoint Security Manager (FSM).

Proxy Chaining Support for Cloud RBI

Proxy chaining mode is now supported with Cloud RBI for full isolation. For more information, see Configuring Forcepoint RBI (Cloud Deployment) in proxy chaining mode with Forcepoint Content Gateway for full isolation on page 44.

Configure trusted sites in Cloud RBI

Trusted site options is now enabled in Web Filtering for RBI cloud in proxy chaining mode. For more information, see Web Filtering on page 105.

LDAPS support for RBI Cloud

LDAPS is a secure Lightweight Directory Access Protocol (LDAP) based identity provider that allows user authentication. For more information about configuring LDAPS connection, see Configure the LDAPS connection.

Note

Cloud RBI tenant supports only LDAPS connection.

Additional File Formats now Supported for Safe Preview

Forcepoint RBI now supports additional file formats for **Safe Preview**. For more details, refer to the **Settings** section.

Related concepts

Settings on page 98

Deprecated support for Override Isolation Mode for Categories

For both cloud and on-premises environments, Forcepoint RBI has removed the support for overriding the isolation mode for a category.

Existing users who have configured this setting for a category, upon Forcepoint RBI upgrade the configured setting is removed and the default configuration is used.

Note

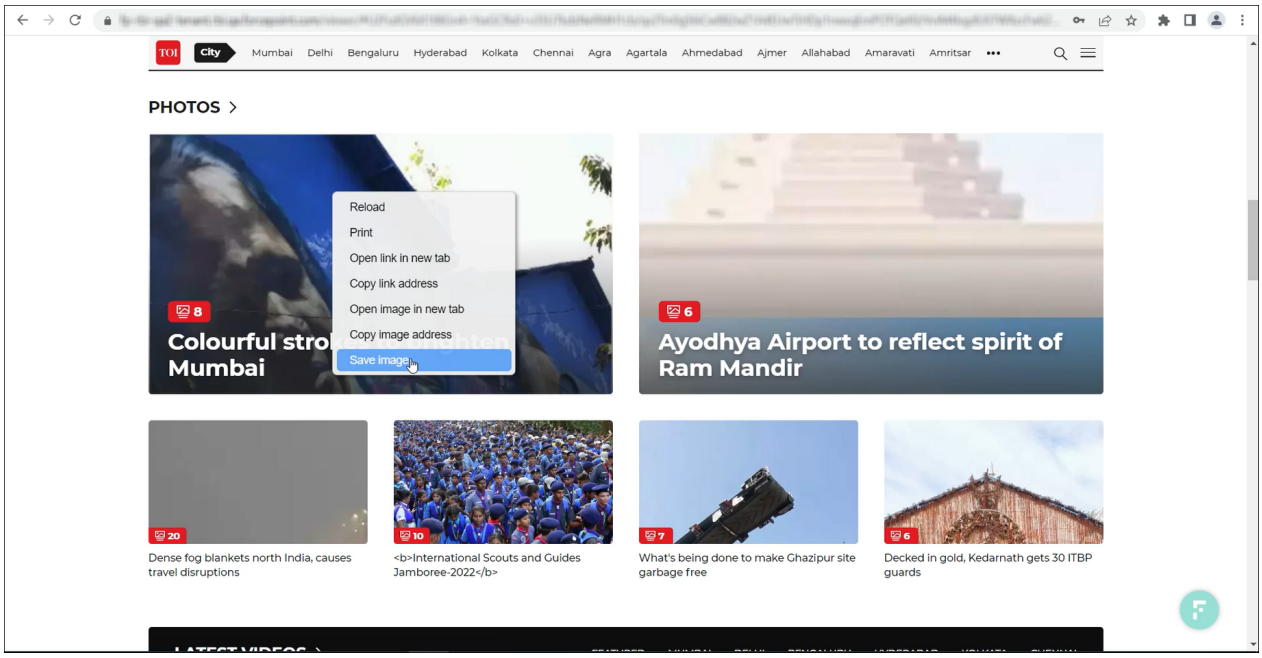
Forcepoint RBI will continue to have support for overriding the isolation mode of a URL.

Support for secure image download

Forcepoint RBI now allow end-users to securely download images from an isolated web page by using the **Save Image** option in the **RBI context** menu. When an end-user chooses to download an image by using the **Save Image** option, the RBI file download policy is applied to the image file.

An administrator can configure the **File Downloads** setting to allow or block the download of a type of image file. For more information about the setting, refer to the *Create a new policy profile* section.

To download an image, right-click on the image and select the **Save Image** option.



Related tasks

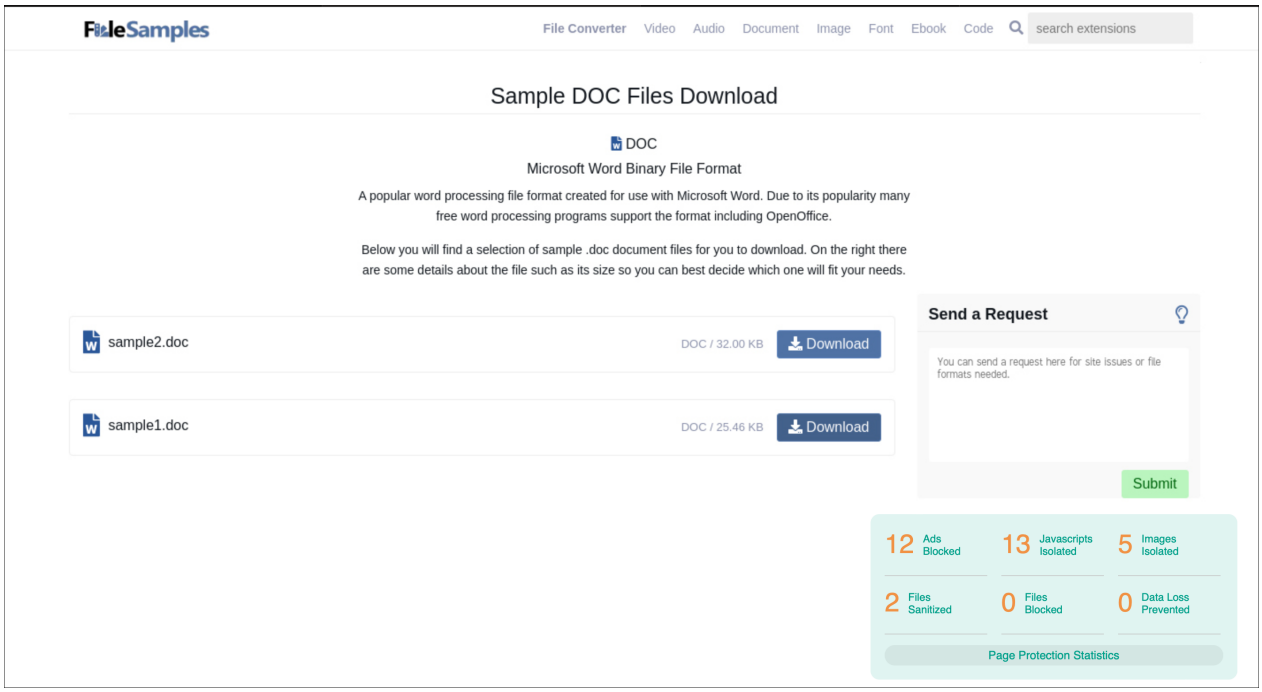
Create a new policy profile on page 88

RBI protection metrics for isolated web pages

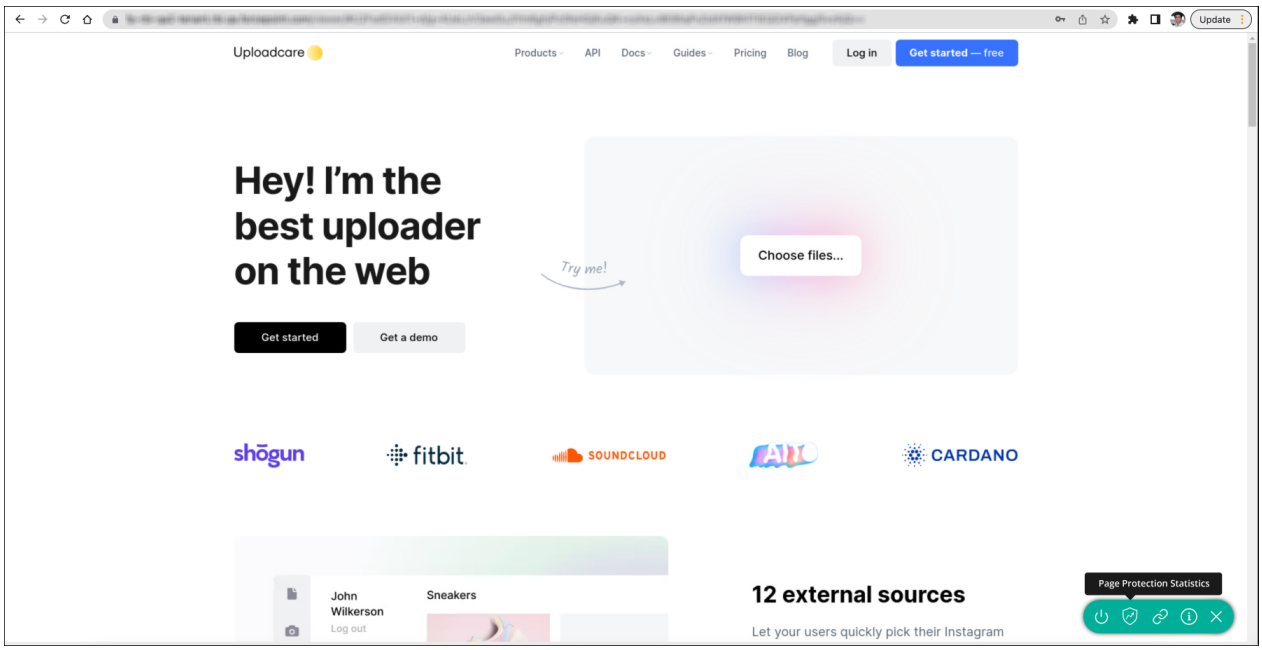
Forcepoint RBI now displays protection metrics for an isolated web page to both administrators and end-users. The protection metrics contains information about the security events for the isolated web pages.

An administrator can view the protection metrics in the **Web Security Summary** widget, on the **Dashboard** > **Web Security** page. For more details, refer to the **View the Web Security Summary** section.

An end-user can view the protection metrics in the **Page Protection Statistics** card.



To access the **Page Protection Statistics** card, click the **Page Protection Statistics** option in the **RBI FAB** menu on the isolated web page.



Related tasks

View the web security summary on page 64

Mobile Rendering Support

Forcepoint RBI now supports the mobile rendering feature.

The mobile rendering feature has the following benefits:

- When a user accesses RBI by using a mobile device, a mobile version of the browsed webpage is rendered. If the mobile version of the browsed webpage is not available, the desktop version of the browsed webpage is rendered.
- It ensures the organization's security is not compromised when RBI users browse through links by using a mobile device.

Note

1) The RBI license is applicable to all mobile device users.

2) For a mobile device:
   - The supported browsers are Safari and Chrome.
   - The supported operating systems are Android and iOS.

3) The webpage that is rendered on a mobile device only supports the basic functions scrolling, clicking and typing.

Spanish Locale Support

Forcepoint Remote Browser Isolation now supports localized rendering, keyboard type-in, and end user notifications in Spanish Locale.

Override User Agent

For cloud and on-premises environments, the override user agent feature allows administrators to manually configure a user agent for rendering a URL. The user agent that is configured for a URL, overrides the user agent that is selected by default for the URL. For more details, refer to the *Override User Agent* section.

Related concepts

Override User Agent on page 103

Print Control

The administrator can now choose to manually enable or disable the printing option for a tenant with ease. This helps to prevent data leak via printing. For more details, refer to *Create a new policy profile* section.

Note

The restriction of maximum size of file that can be printed is removed, that is there is no file size limit for printing a file.

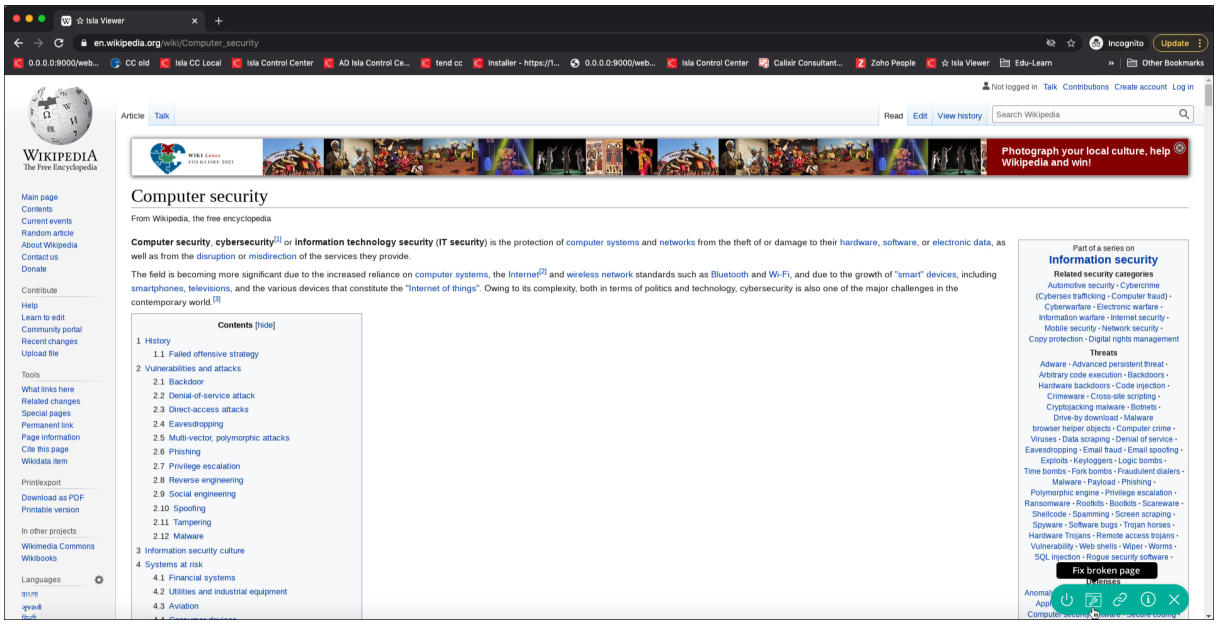
Related tasks

Create a new policy profile on page 88

Fix Rendering Issues

Forcepoint RBI now allows end-users to fix web page rendering issues by themselves in RBI isolated sessions.

To fix web page rendering issues, an end-user can click the **Fix Broken Page** option in the **RBI FAB** menu.



Note

The web page rendering issue is fixed for the end-user only, and not for the complete tenant.

Block Advertisement

Forcepoint RBI now supports Ad Block, and this can be enabled by using the **Block Advertisement** option. The administrator can choose to enable or disable the **Block Advertisement** option. When this option is enabled, the unwanted advertisements are blocked and this results in lower bandwidth usage, which facilitates more responsive web browsing experience for a user. For more details, refer to *Create a new policy profile* section.

Note

1) By default, this option is disabled.

2) To display the number of ads that are blocked for a user, the **Ads Blocked** column is added in the table under the **Browse Activity Summary** section, in the **Dashboard** > **Web Security** tab.

Related tasks
Create a new policy profile on page 88

Proxy Authentication

The administrator can now configure the proxy authentication-based identity provider option for a tenant. This allows seamless one-time authentication for Forcepoint Web Security with Forcepoint Remote Browser Isolation, via proxy chaining. For more details, refer to *Proxy Authentication* section.

Related concepts
Proxy Authentication on page 123

DLP Integration

Forcepoint RBI can now be integrated with DLP to ensure that data loss is prevented in RBI isolated sessions. The integration of Forcepoint RBI with DLP is done by using the ICAP protocol. For more details, refer to *DLP* section.

Note

1) The **Data Leakage Prevented** column is available in the table under the **Browse Activity Summary** section, in the **Dashboard** > **Web Security** tab. This column displays the number of incidents for both HTTP Post and file uploads that are blocked by DLP policy for the user.

2) This feature is only available for on-premises RBI and on-premises DLP protector.

Related concepts
DLP Integration on page 127

Upload Summary

The new **Upload Summary** widget is added in the **Dashboard** > **Web Security** tab. The **Upload Summary** widget shows the count for all file types that were either uploaded successfully by the user (allowed) or were not uploaded when the file failed the CDR conversion, or a DLP policy is enforced (blocked).

Safe Preview

The administrator can now choose to enable or disable the Safe Preview mode. When this mode is enabled, a user can download a file only after the file is safely previewed in a pop-up window. The administrator must disable the Safe Preview mode to allow a user to directly download a file without the need to safe preview the file.

Note

This mode is enabled by default.

Override Isolation Mode

For cloud and on-premises environments, the override isolation mode feature allows administrators to manually select the type of isolation mode for a category, or a URL. The type of isolation mode selected by the administrator for a category, or a URL overrides the isolation mode that is determined by Forcepoint Threat Intelligence Services. For more details, refer to the *Override Isolation Mode* section.

Related concepts

Override Isolation Mode on page 101

Turkish Locale Support

The Forcepoint Remote Browser Isolation now supports localized rendering, keyboard type-in, and end user notifications in Turkish Locale.

CDR for file uploads

Forcepoint's Zero Trust CDR removes any potential malicious content from a document or image file by removing executable content (like Macros) and sanitizing images to prevent steganography and links to external content. With RBI 22.07 release, CDR scan is supported for both File Upload and download. RBI admins can now enable or disable CDR scan for File Upload directly from the RBI Admin Portal. For more details, refer the section *Create a new policy profile*.

Related tasks

Create a new policy profile on page 88

German locale support

The Forcepoint Remote Browser Isolation now supports localized rendering, keyboard type-in, and end user notifications in German Locale.

API key self-generation

API key self-generation feature allows RBI admins to generate the API Key to access RBI APIs from the RBI Admin Portal. For more details, refer the section *Enable RBI Admins to self-generate API key*.

Related concepts
Enable RBI Admins to self-generate API Key on page 82

Deprecation of Smart Redirection

Feature to redirect links back to proxy or gateway is deprecated in this release. From RBI 22.07 release onwards, any links clicked from an isolated page will continue to open in isolation. This is done primarily to prevent accidental violation of configured RBI policy when the request gets redirected back to proxy from an isolated session. To ensure while browsing in isolation user is not able to access any sites blocked by proxy or gateway policy, it is advised to configure blocked URLs and category as explained in section *Web Filtering*.

Related concepts
Web Filtering on page 105

Localization Support

The Forcepoint Remote Browser Isolation now supports localization in Arabic locale which includes localized rendering, type-in, and end user notifications.

Web Filtering Block Feature Enabled Universally

The below Web Filtering features will be now available to both FRBIF (Forcepoint RBI Full) and FRBIS (Forcepoint RBI Selective) customers.

- URL and Category Blocking
- Category Override

The URL and Category trust will continue to be available only to FRBIF subscriptions using non-URL redirect integrations.

Subscription Agreement Updated

The Terms and Conditions of the subscription agreement have been updated. Administrators will now need to accept the updated subscription agreement (EULA) before they can access the Forcepoint Remote Browser Isolation Admin Portal.

Managing Policies and Settings via APIs

The Forcepoint Remote Browser Isolation now supports managing policies and settings via APIs for ease of use. To obtain an API key, and for more information, contact Forcepoint Technical Support.

Localized Keyboard Support

The keyboard localization feature allows users to type in a locale set on their keyboard during an isolated session.

Note

The localized keyboard now supports Chinese-Simplified, and Chinese-Traditional in addition to Hebrew language.

Localized RBI Messages

When the browser locale is set to Chinese-Simplified (zh-CN), Chinese-Traditional (zh-TW), Hebrew (he, and he-IL), the context menu and end user notifications are translated into the locale in which the page is being rendered.

Note

The context menu and end user notifications are displayed in English if the browser locale is not supported.

Static IP Address Support

Static IP addresses can be now added instead of FQDNs for port opening in firewall to integrate with Forcepoint RBI. For details, contact Forcepoint Technical Support.

Localized Keyboard Support

The keyboard localization feature allows users to type in a locale set on their keyboard during an isolated session.

Note

The localized keyboard currently supports Hebrew language only.

ICAP and ICAPS Integration Support

ICAP or ICAPS can now be used to integrate with cloud tenant of Forcepoint RBI.

Note

ICAPS integration is more secure than ICAP integration.

Forcepoint RBI Integration with Email Security

For cloud and on-premises environments, Forcepoint RBI Integration with Email Security allows users to browse email links safely and prevent phishing and other malicious link attacks. Additionally, users of email security can now safely download files from isolated email links using CDR.

Rendering Isolated Pages in End User Browser's Locale

Forcepoint RBI now renders the isolated pages based on the endpoint browser's locale.

Forcepoint RBI supports the following browser locales:

- Arabic
- Chinese (traditional)
- Chinese (simplified)
- Dutch
- English
- French
- German
- Hebrew
- Italian
- Japanese
- Korean
- Portuguese (Brazil)
- Russian

Note

The isolated pages will be rendered in English if the browser locale is not supported.

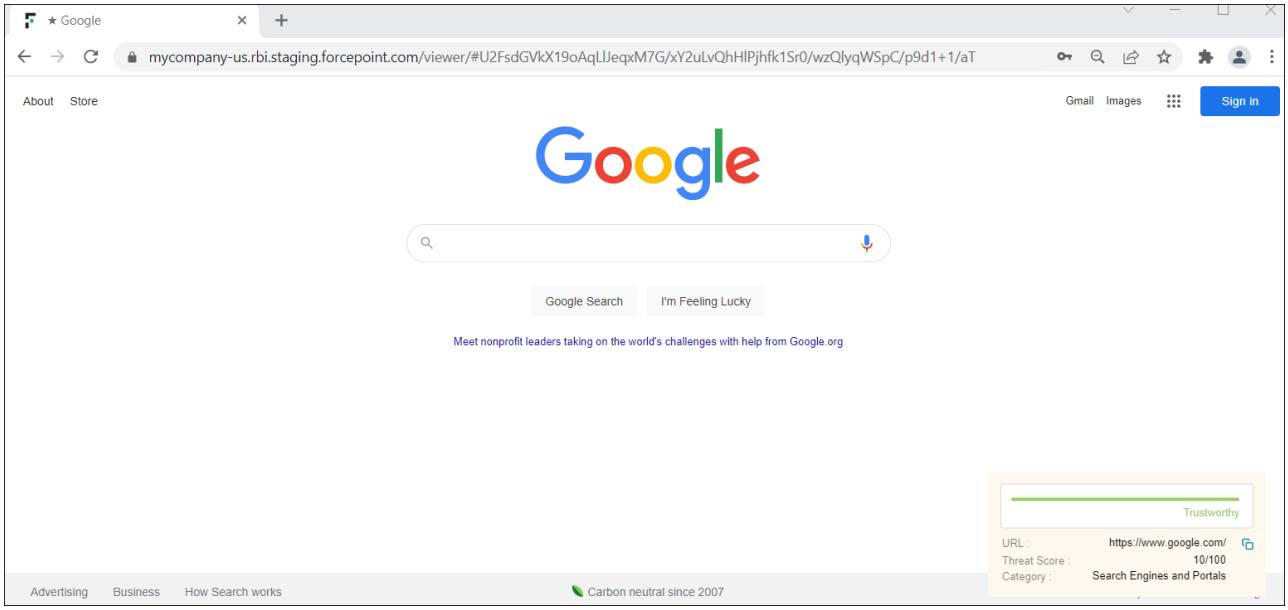
TLS 1.3 Exclusive Support

TLS 1.1 and TLS 1.2 both have known vulnerabilities. As a security-centric solution, we will deprecate support for TLS 1.1 and TLS 1.2 to ensure users are not exposed to these vulnerabilities. Forcepoint RBI will now exclusively support TLS 1.3.

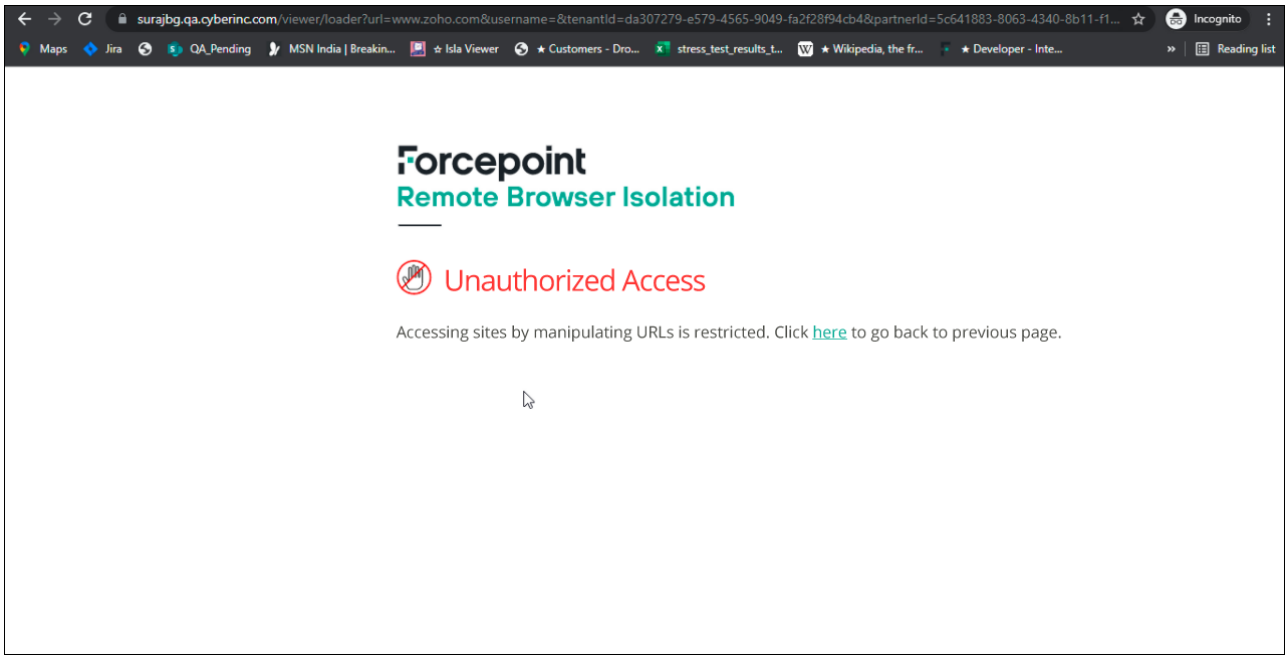
URL Encryption

Users are restricted from manipulating URLs in the address bar to bypass the proxy restrictions. All users will have this setting enabled by default. This feature is applicable only to URL redirect integrations.

- Isolated URLs will appear encrypted in the address bar. The floating action button (FAB) displays the actual URL and enables the user to copy it.



- Any attempt to modify the address bar URL will redirect the user to the Forcepoint RBI custom block page.



Note

The URL Encryption has no impact on the existing Forcepoint Web Gateway integrations.

Clipboard Control

Clipboard Control allows administrators to restrict copy and paste operation from the endpoint to the remote browser and vice versa.

Related tasks

Create a new policy profile on page 88

ICAP Integration

Forcepoint RBI now supports ICAP integration in addition to URL redirect. An ICAP integration provides a more secure connection to the RBI service and avoids the need for customized block pages for a more seamless end user experience.

Smart isolation

Smart isolation provides automatic switching of the render mode based on destination risk analysis.

Forcepoint RBI has two render mode capabilities:

- Secure Streaming: Visual steam of remote browser content. The safest mode, but uses high network bandwidth.

- Secure Rendering: Executable code like JavaScript is removed. HTML and CSS are delivered to the local browser to render with native DOM render. Fast native-like performance.

Typically, an Admin user must decide up front which rendering mode best suits their environment and business security needs. With Smart Isolation, Forcepoint RBI dynamically chooses the most appropriate rendering mode based on the destination URL Threat score.

Smart Isolation is powered by the FTIS engine; however, the auto switching of rendering mode is not solely decide by the FTIS engine. There are other factors internal to this feature, such as content and connectivity, that decide the suitable rendering mode to ensure optimum user experience is delivered to the end user making it a truly "smart" feature.

Related tasks
Configure the isolation mode on page 80

Content Disarm and Reconstruction

Content Disarm and Reconstruction (CDR) removes malicious content from a document or image.

Forcepoint's Zero Trust CDR removes any potential malicious content from a document or image file by removing executable content (like Macros) and sanitizing images to prevent steganography and links to external content. This "disarms" the file in a preventative manner. CDR does not rely on detection — all potential threat vectors are disarmed. The file is reconstructed to resemble the original file as closely as possible before it is delivered to the end user. File Downloads are disabled by default; however, CDR is the default action when File Downloads are enabled.

Supported File Types: For the most up-to-date list of supported file types, see the Deep Secure FAQ.

For file types that are not supported, Forcepoint RBI falls back to an AntiVirus scan of the file. A patience page is displayed while a file is been processed by CDR. The original file is not stored or accessible to customer within an RBI session.

Secure Rendering

Secure Rendering removes potentially malicious executable content, like JavaScript, and delivers the HTML and CSS to the local browser.

Typically, Forcepoint RBI uses secure streaming, which steams a sequence of images or pixels of an isolated website to the end user's browser. This is a highly secure delivery mechanism to deliver web content, but it tends to be a high consumer of network bandwidth because it is a stream of images. With "Secure Rendering", Forcepoint RBI disarms a website of potentially malicious executable content like JavaScript files, and delivers HTML and CSS to the end user's browser. The local browser can then render the page using its DOM, which provides a native responsive user experience.

Safe Surf

Safe Surf turns a webpage into a read-only like mode where hyperlinks and navigation work, but entering data into text fields and file uploads and downloads do not work.

Safe Surf is recommended for URLs that are classified as high risk. With Safe Surf, passwords and other user data cannot be shared or exposed within a Forcepoint RBI session.

Smart Redirection (Deprecated)

Smart Redirection automatically manages website navigation within a Forcepoint RBI session, ensuring customers remain protected when an end user clicks a link within their session.

When Forcepoint RBI renders the webpage and creates links based on the setting for this attribute, Forcepoint RBI prefixes the actual link with the Forcepoint RBI domain if navigation is to be retained within the session. For example, if the setting is set to **None**, Forcepoint RBI always prefixes the links with `*.fp.rbi.forcepoint.com/viewer/#`. You can choose between ensuring all navigation within the session remains within the session and ensuring that all external links are processed by Forcepoint Secure Web Gateway to make sure that policies are not bypassed.

Authentication

Forcepoint RBI provides two modes for connecting to the Forcepoint RBI service: Authenticated mode and Anonymous mode.

- Authenticated Mode: Use this mode when you have integrated your Identity Provider with Forcepoint RBI. End users sign in to the service and are identifiable in Forcepoint RBI logs. Policies can be applied to users and user groups in authenticated mode.
- Anonymous Mode: Use this mode if you want your end users to remain anonymous. End users can browse web sites through a Forcepoint RBI session, but they are not identifiable in Forcepoint RBI logs. Policies are applied to all anonymous users. You cannot apply policies to specific users or user groups.

On-Premises Deployment

Forcepoint RBI can be installed and deployed on the hardware infrastructure within your organization.

Standalone Forcepoint RBI

Forcepoint RBI can now be purchased as a standalone product.

Forcepoint RBI was previously available only as an add-on to previously purchased Forcepoint products. Starting in this release, Forcepoint RBI can be purchased as a standalone product.

Forcepoint Next Generation Firewall integration

Forcepoint RBI integrates with Forcepoint Next Generation Firewall (Forcepoint NGFW) with URL forwarding to the Forcepoint RBI service from custom user responses.

Related concepts

Configuring the redirect for Forcepoint NGFW on page 34

Forcepoint Web Security On-Premises integration

Forcepoint RBI integrates with Forcepoint Web Security On-Premises with URL forwarding to the Forcepoint RBI service from custom block pages.

Related concepts
Configuring the redirect for Forcepoint Web Security On-Premises on page 18

Forcepoint Web Security Hybrid integration

Forcepoint RBI integrates with Forcepoint Web Security with URL forwarding to the Forcepoint RBI service from custom block pages.

Note

Forcepoint Web Security Hybrid customers cannot modify the block pages. Contact Forcepoint Support to enable the custom block pages.

Related concepts
Configuring the redirect for Forcepoint Web Security Hybrid on page 25

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-2023

This link requires a Forcepoint Support account.