



Ericom Shield and Forcepoint

Prevent web-borne
malware and
ransomware with zero-
trust browser isolation

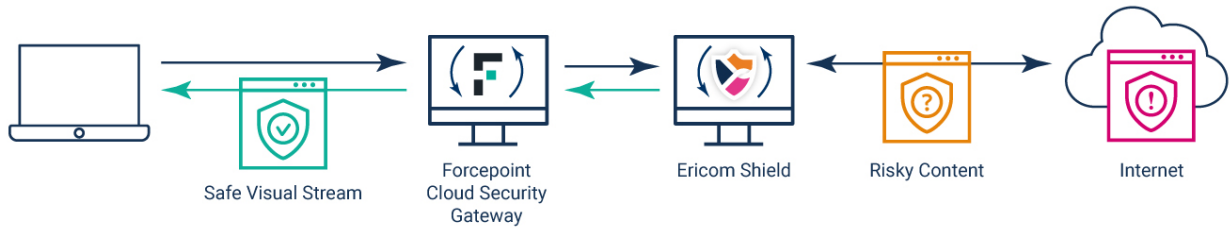
Cloud Security Gateway

Date: July 2020

Solution Overview

Ericom Shield communicates with Forcepoint Cloud Security Gateway via Block Page Redirect to provide isolation-based zero-day malware protection. This technote will explain how to configure Forcepoint Cloud Security Gateway and Ericom Shield.

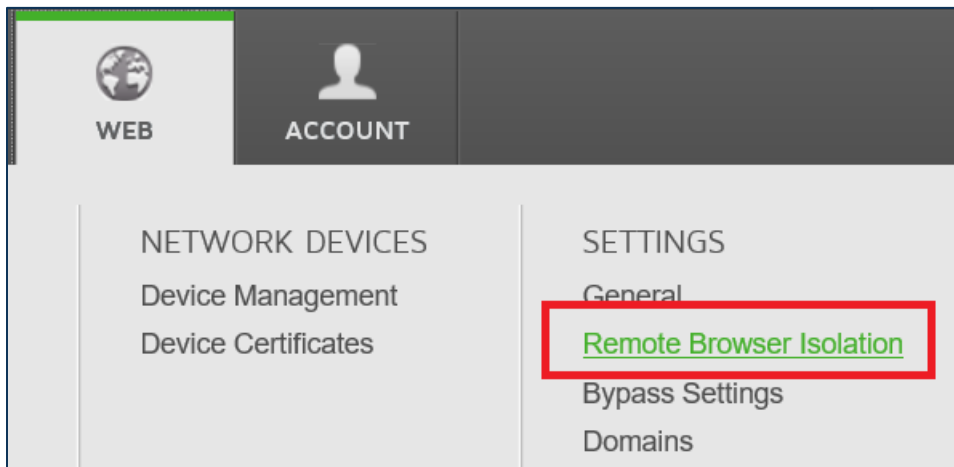
Data flow overview and architectural diagram



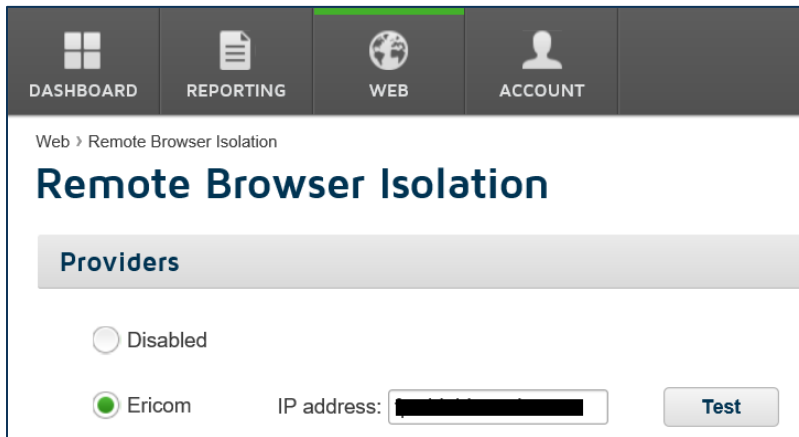
Cloud Security Gateway

Before beginning the configuration, ensure that Forcepoint Cloud Security Gateway can browse successfully to the Internet.

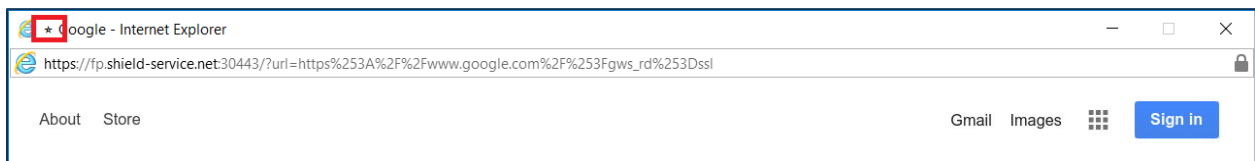
To begin, configure the Remote Browser Isolation setting, under Web | Settings | Remote Browser Isolation. If this option is not present, contact your Forcepoint representative to enable it.



Enter the Ericom Shield address in the IP address field, both DNS name and IP address are supported.



Press the “Test” button to confirm connectivity and an isolated session will open. If the end user notification is enabled in Ericom Shield, a star icon will appear in the browser tab.



Isolation can be verified by viewing the source of the web session and confirming that the original source code is not being downloaded to the local browser (the Ericom Shield code will appear):

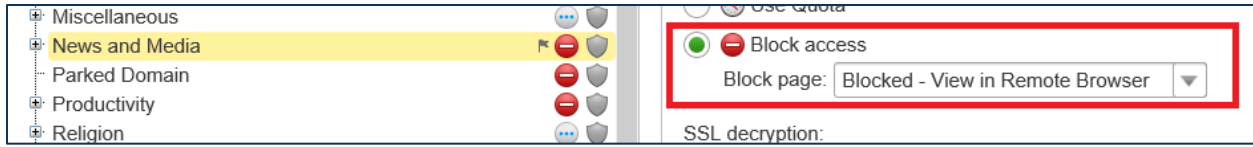
```
<!-- Protected by Ericom Shield -->
</body>
</html>
```

Configuring a Category to use Isolation

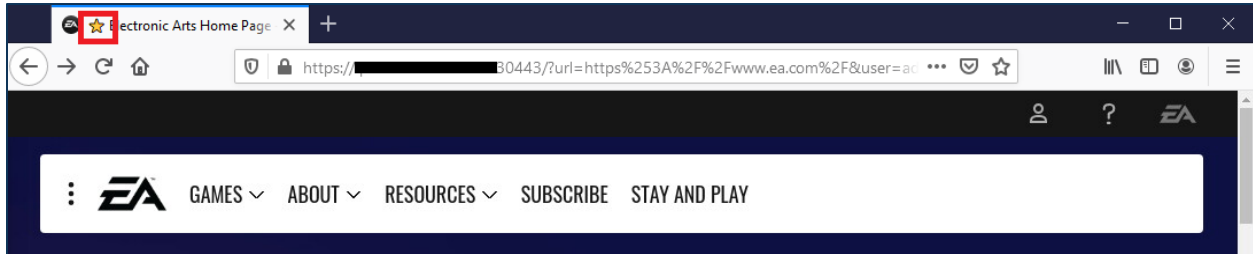
To configure a category to use browser isolation, go to Web | Policies | Web Categories.



Configure a category’s action to “Block access,” and then select the block page that uses isolation. By default, this option is labelled “Blocked – View in Remote Browser”



Wait a few minutes for the settings to propagate throughout Forcepoint Cloud Security Gateway. Navigate to a website that is configured for isolation and a block page will appear. Click “View in Remote Browser” to open the site in Ericom Shield remote browser isolation (enable the end user icon for a visual indicator that the session is isolated):

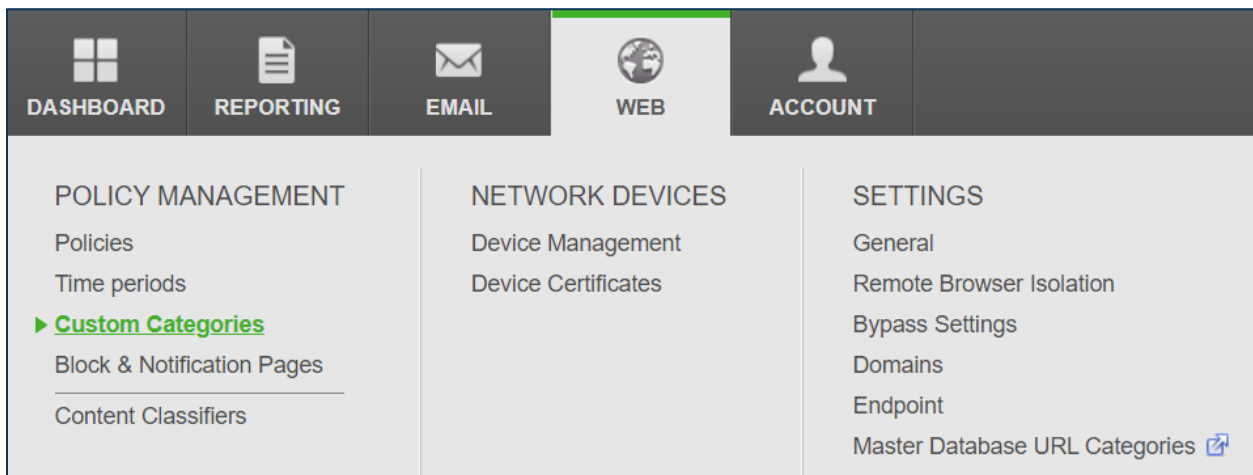


Custom Category for Browser Isolation

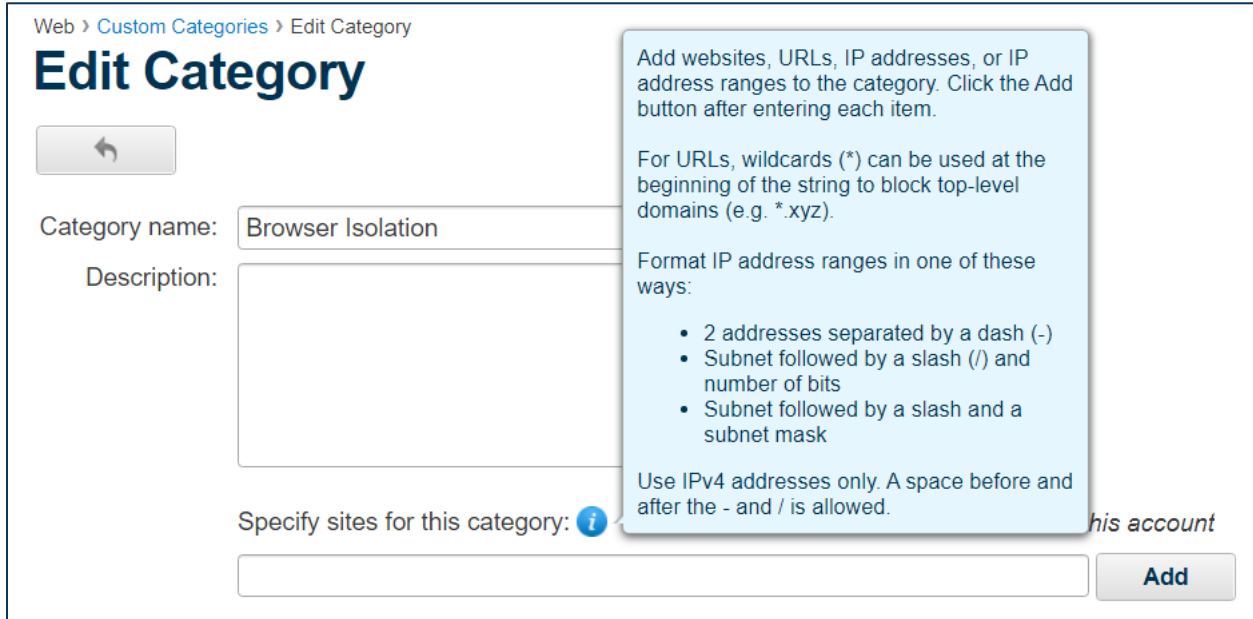
A popular use case for a custom category is to hold risky URLs that are in an allowed category and send them to browser isolation so they cannot be downloaded and cached onto the local browser. By adding the URL to the custom category, it will be recategorized and will adhere to the settings of the new category.

The custom category can also be useful in allowing users to access websites that are in blocked categories. Even though there may be a specific need to access a website in this instance may be risky, opening them in browser isolation ensures that the local browser and device cannot be attacked.

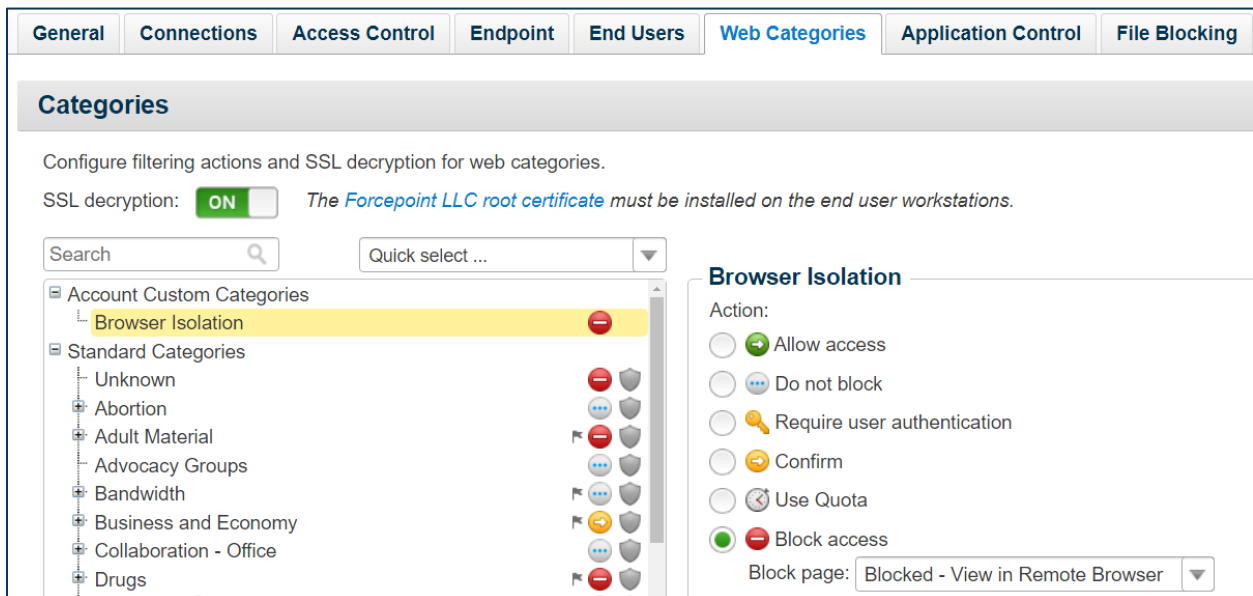
To add a custom category, use the Forcepoint admin console and go to Web | Custom Categories



Add the websites that will be included in this category. Click on the information icon for instructions on how to format URLs and IP addresses.



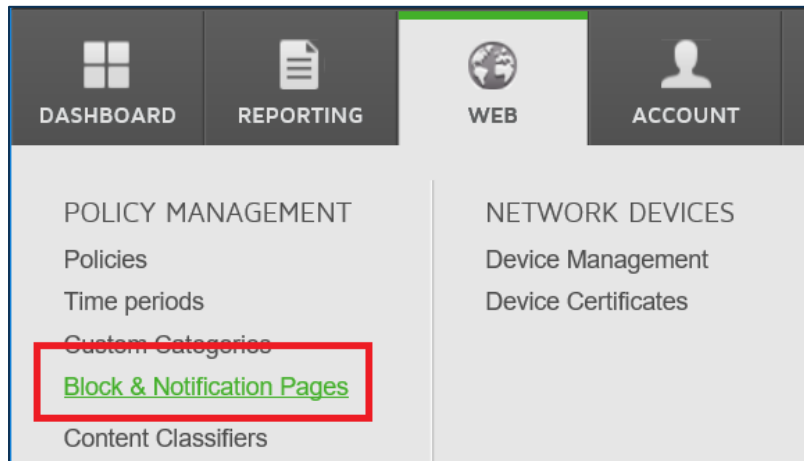
Save the settings and go Policies | Web Categories | click the Browser Isolation category, set the Action to “Block access,” and select the browser isolation option.



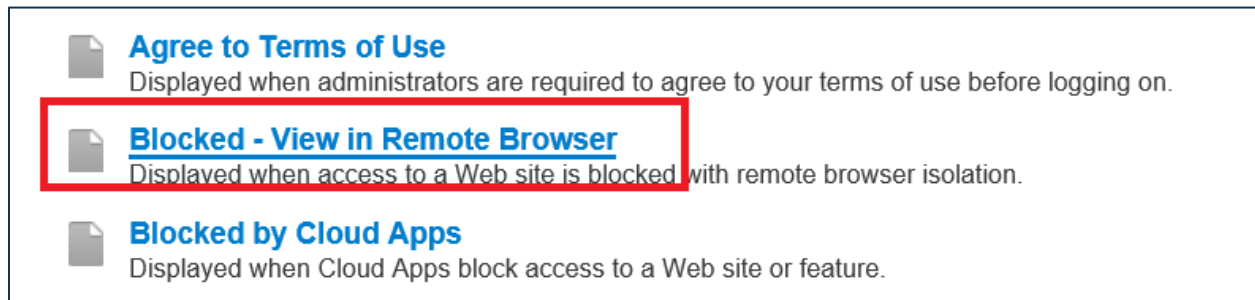
Click Save and wait a few minutes for the setting to propagate in the cloud before testing.

Viewing the Block Appearance

To view the template of the default isolation block page, go to Web | Block & Notification Pages



Click on General | Blocked – View in Remote Browser to view and edit the default page.



To create a custom, click on “New Page” button at the “Block & Notification Pages” screen:



Add the custom code to a new page. This will automatically become an available option in the Block Page selection list.

NOTE: In the default block page, the Ericom Shield URL will be updated automatically if the Remote Browser setting changes. In custom pages, this must be updated manually if the Ericom Shield address changes.

Set Block Page to Auto-redirect

In cases where the end user does not need to see the block page and the web request should automatically go to Ericom Shield, create a custom page with the following code:

```
<DOCTYPE html>

<html>

  <head>

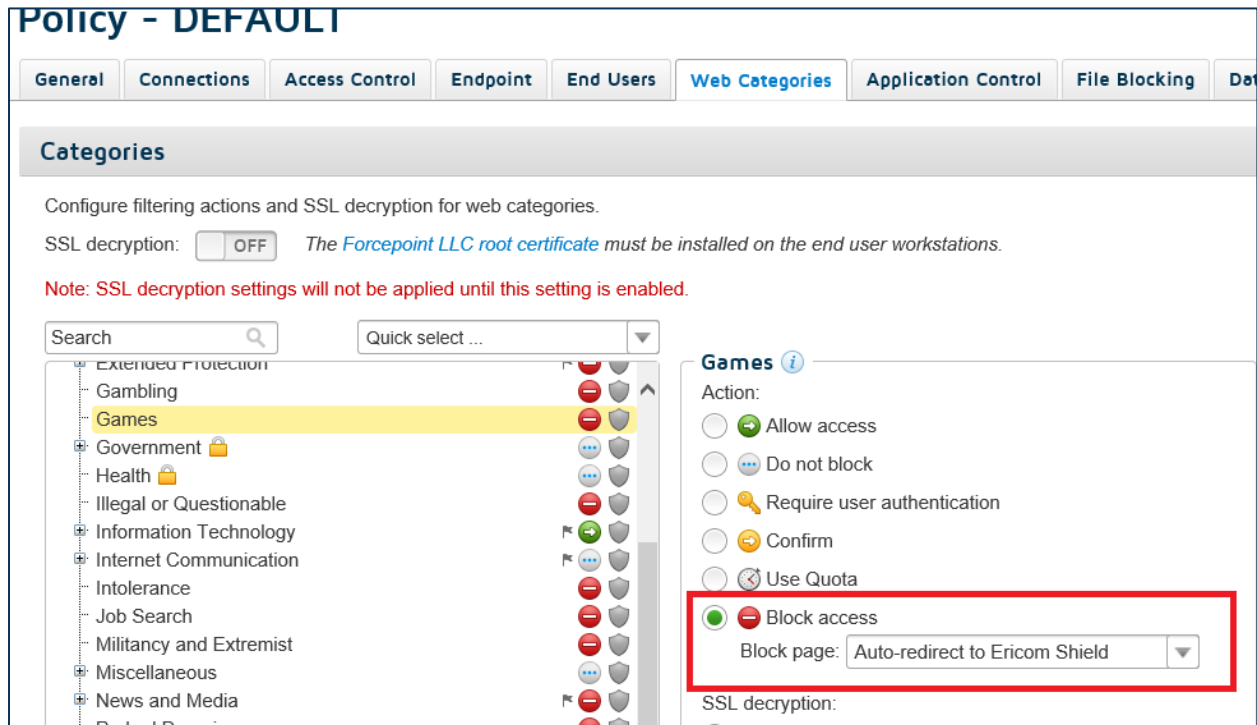
    <meta http-equiv="Refresh" content="0; url=https://<yourtenant>.shield-
service.net:30443/?url=_URL_&user=_USERNAME_[urlescape]"/>

  </head>

</html>
```

Manually enter your Ericom Shield URL in place of <https://<yourtenant>.shield-service.net:30443>

Once saved, the custom page will appear in the list of available "Block access" options:



Policy - DEFAULT

General | Connections | Access Control | Endpoint | End Users | **Web Categories** | Application Control | File Blocking | Data

Categories

Configure filtering actions and SSL decryption for web categories.

SSL decryption: OFF *The Forcepoint LLC root certificate must be installed on the end user workstations.*

Note: SSL decryption settings will not be applied until this setting is enabled.

Search: Quick select:

Category	Action	SSL Decryption
Extended Protection	Block access	Off
Gambling	Block access	Off
Games	Block access	Off
Government	Block access	Off
Health	Block access	Off
Illegal or Questionable	Block access	Off
Information Technology	Block access	Off
Internet Communication	Block access	Off
Intolerance	Block access	Off
Job Search	Block access	Off
Militancy and Extremist	Block access	Off
Miscellaneous	Block access	Off
News and Media	Block access	Off
Parked Domain	Block access	Off

Games ⓘ

Action:

- Allow access
- Do not block
- Require user authentication
- Confirm
- Use Quota
- Block access**

Block page:

SSL decryption:

Website categories that have this page enabled will automatically go to the configured Ericom Shield service.

Adding User Name Attribute to Ericom Shield Reports

To add the user name to the Shield session for reporting purposes, add the following parameter:
&user=_USERNAME_[uriescape]

Example code:

```
<meta http-equiv="Refresh" content="0; url=https://your-service-url.shield-service.net:30443/?url=_URL_&user=_USERNAME_[uriescape]" />
```

The user name passed from Forcepoint will appear in the Shield reports:

Time	User Name	Display Name	Profile	Client IP	Domain	Mode	Matched Reason
Apr 10, 2020, 10:44:20 AM	admin		All	.90	www.cnn.com	shield	Default Policy

Configuration for Crystal rendering mode

To use Ericom Shield Crystal rendering mode with Forcepoint Cloud Security Gateway, configure the following:

- Go to Policy | File Blocking tab | File Extensions
- Click Add Extensions
- Add File Extensions: jpeg, jpg, gif, png, css, woff2
- Set Rule State: Enabled

Web > Policies > DEFAULT > Edit File Extensions

Edit File Extensions

File Extensions
Enter file extensions separated by commas (for example, gz,cad,js)

Rule State

Enabled
 Disabled

- Blocking Options: set the categories that will be allowed for Crystal rendering.

Blocking Options

Block all files
 Block all files over KB
 Category specific blocking

Block files in certain categories over KB

Standard Categories

- Unknown
- Abortion
- Adult Material
- Advocacy Groups

Action

Allow access
 Do not block
 Block access

Click Advanced Options

And set:

- Block Page: Access Blocked (if not already set)

Block Page

Press "Save" and the rule set will be added.

File Extensions

Add file extensions, then define how they are blocked by categories, groups, and users.

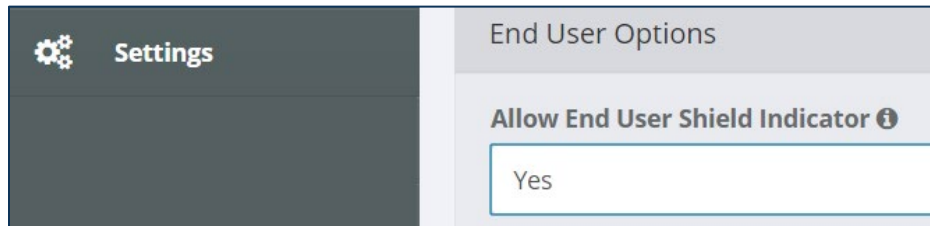
State	Extension Set	Filter	Block Page	Delete Rule
✓	jpeg.jpg,gif,png,css,woff2	1 categories	Access Blocked	✗

NOTE: Crystal rendering mode is currently in technical preview, contact Ericom for release status.

Ericom Shield Configuration

End user notification

Configure the following setting in Ericom Shield's admin console to allow the End User Shield indicator:



When enabled, an icon will appear in the browser tab to indicate that the session is isolated.



By default, this is disabled to provide a seamless and transparent experience for the end user.

About Ericom

Ericom Software provides businesses with secure access to the web and corporate applications, in the cloud and on-premises, from any device or location. Leveraging innovative isolation capabilities and multiple secure access technologies, Ericom's solutions ensure that devices and applications are protected from cybersecurity threats, and users can connect to only the specific resources they are authorized to access.