

* Domain(s) / IP(s) in PAC bypass will go directly (no log in Menlo)
* Domain(s) / IP(s) in SSL bypass will not have user information
* Applications Controls
  + Supported Browsers
  + Non-Browsers / Unsupported browsers
* Exception Rules – policies that overwrites default policy

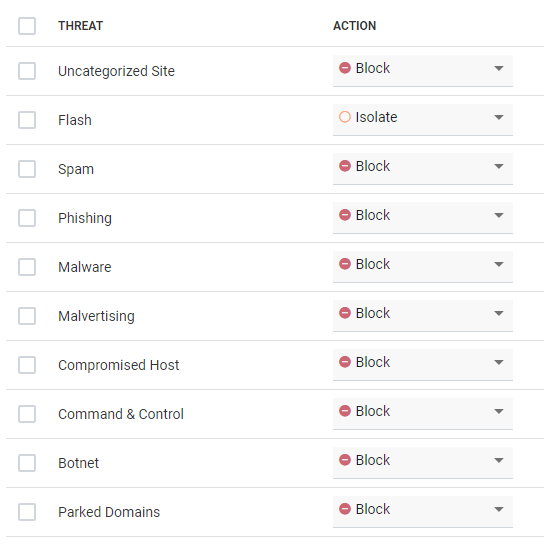
Online checking can be check in the Brightcloud Website for Categorization of the Website

* <https://www.brightcloud.com/tools/url-ip-lookup.php>

Guide to Configure Global Policy

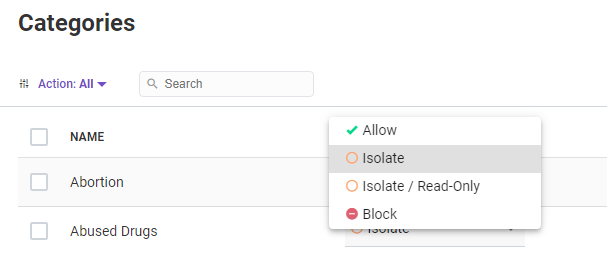
1. For threat category, best practice is to configure block for Spam, Phishing, Malware, Malvertising, Compromised Host, Command & Control, Botnet

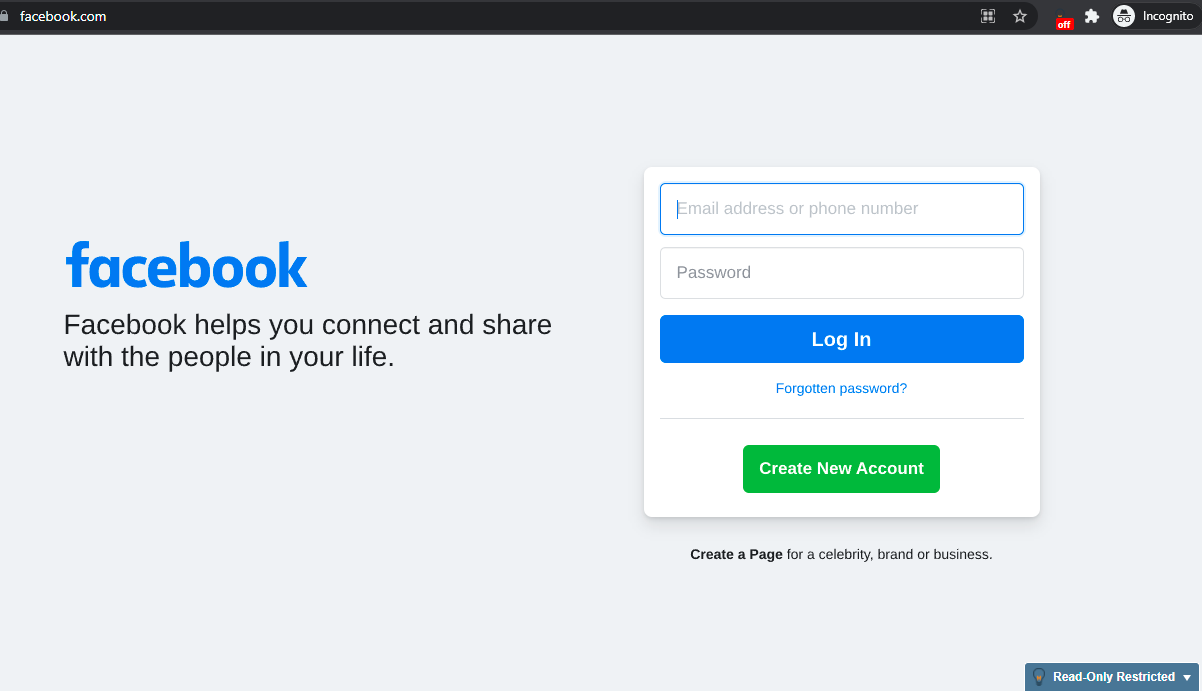
Best practice to Isolate for Uncategorized Site, Flash & Parked Domains



1. For categories, the global policy can be set to Allow, Isolate, Isolate /Read-Only and Block

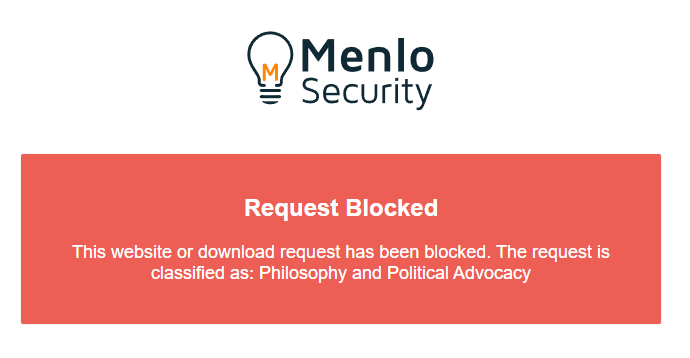
The Read-Only will allow the page in Isolate mode but with the key-in parameter greyed out.



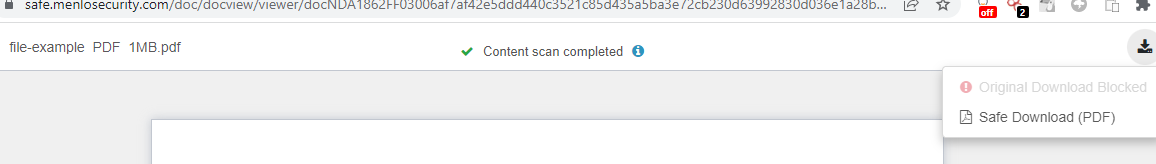


For Block Feature, would receive the notification when trying to login to the Website

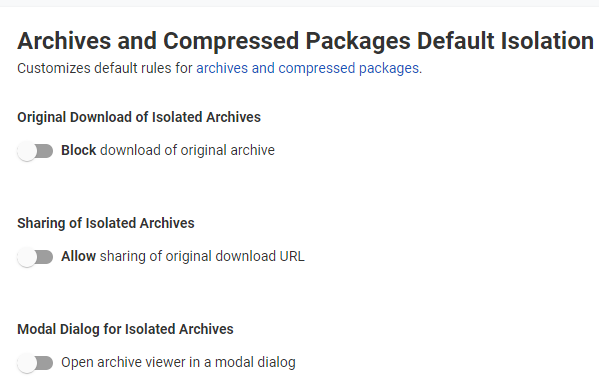
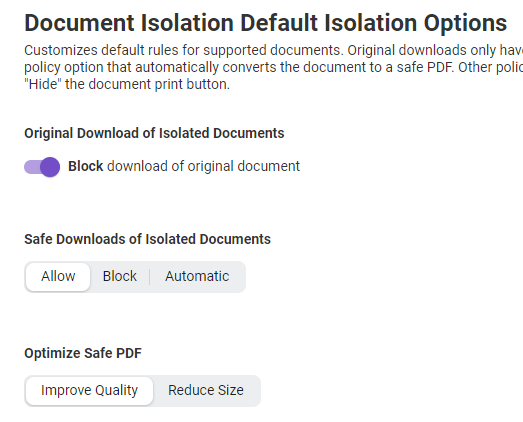
The Block page can be customized.



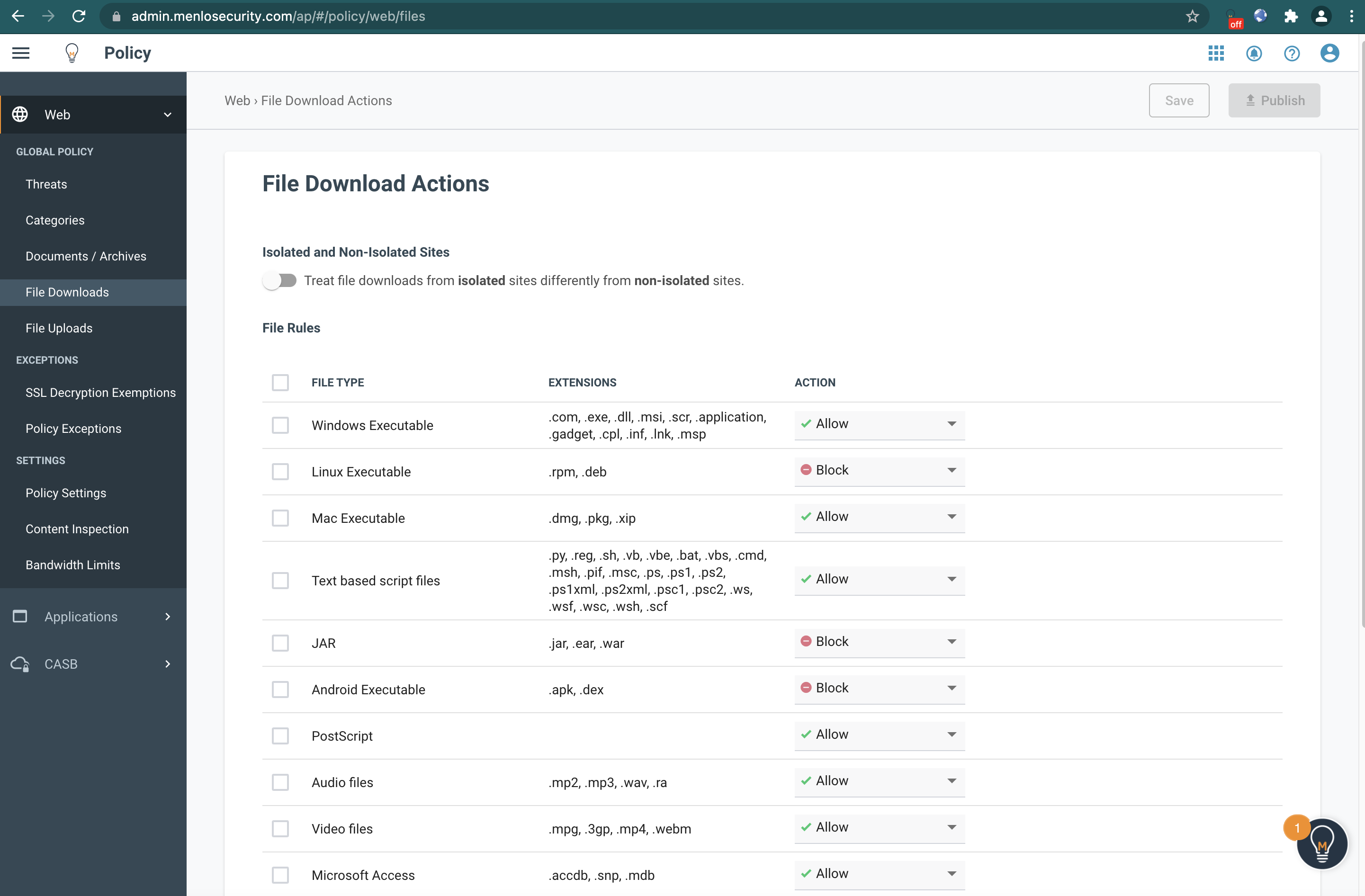
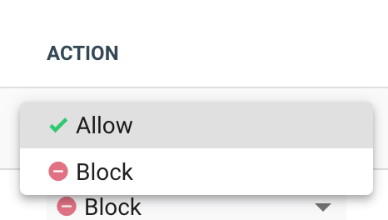
1. For Documents / Archives Tab, Isolation also can be applied in which the document / archive would be open in an isolation platform while the AV proceed with the scanning



Both Document and Archive can be configured to allow or block to download original file. If the original option configured to block, this button would be greyed out.

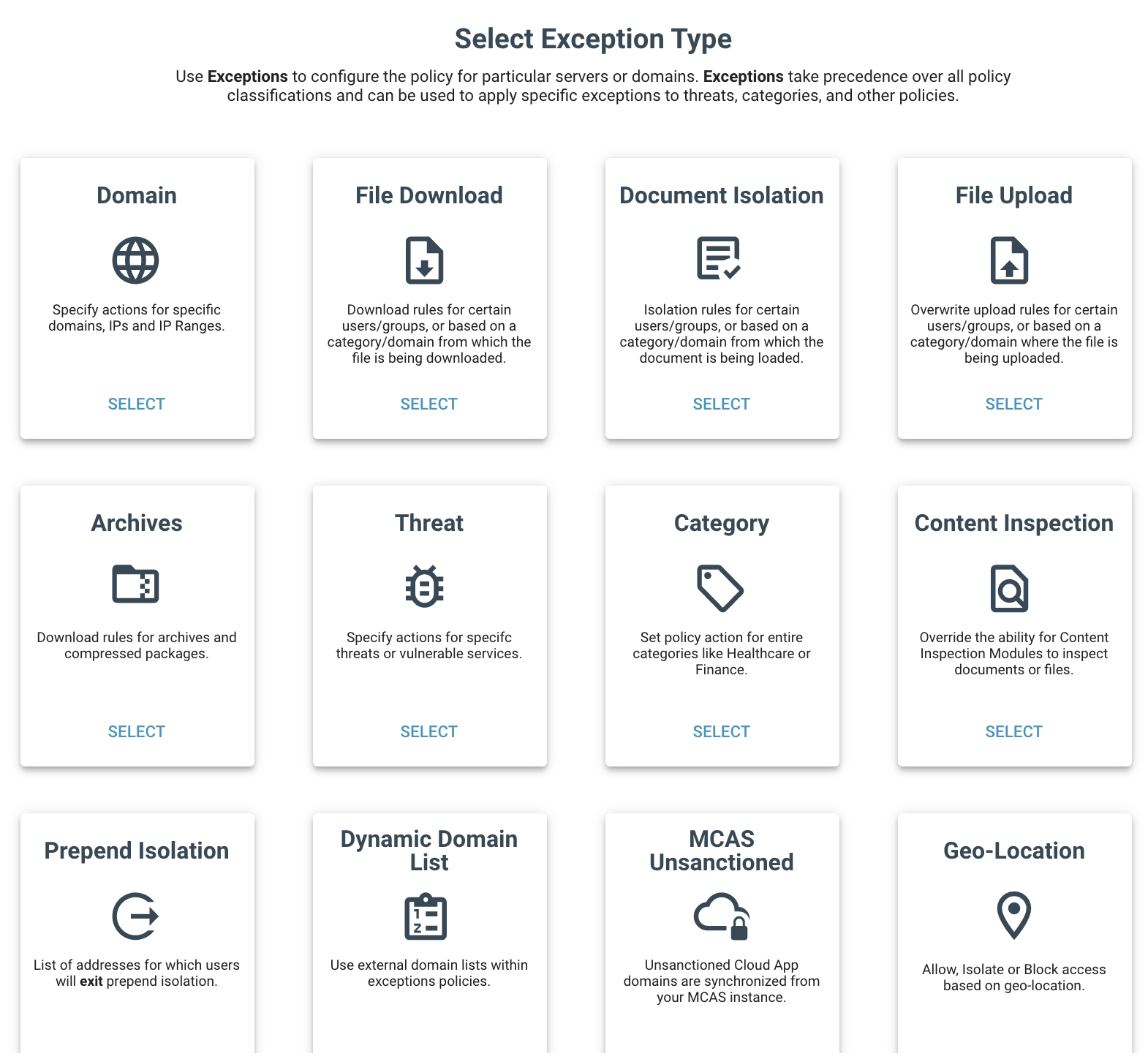


1. For File Control can be configure to allow or block file upload and download



**Exceptions**

2 types of exception can be applied to specific user / groups. Exception rules will take precedence over the global policy. So, if the global policy define isolate read only for the category website but require to allow 1 website of the same category to be configured in isolate to key in the parameter. Hence, the policy will be applied in isolate for that URL but the rest of the website in the same category will be in isolate read-only.

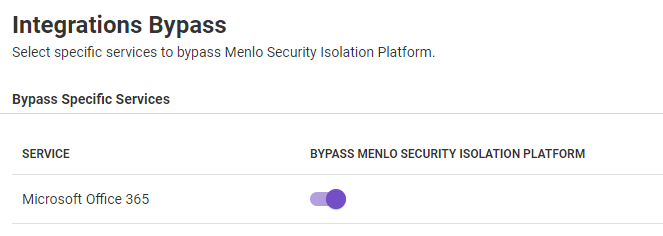
****

The policy exception can be applied to specific user / groups

The group feature must be configured 1st to sync to the AD

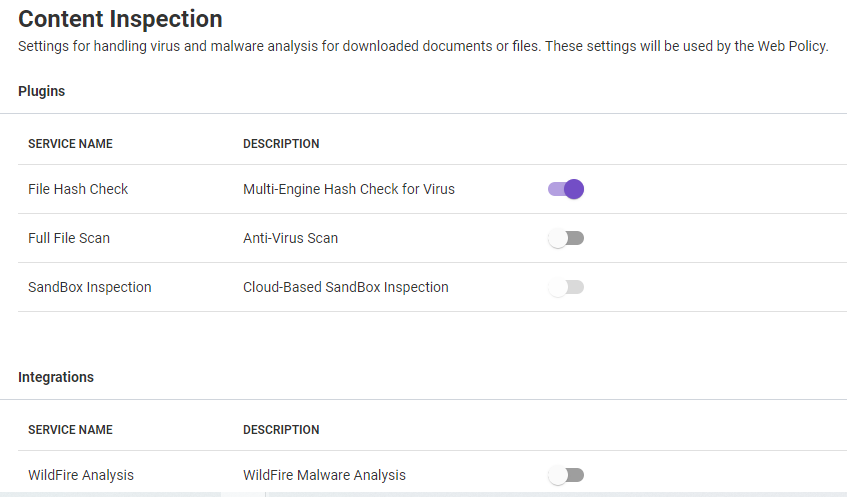
SSL Exemption Decryption

For this feature, Menlo have integration bypass to bypass all Microsoft Office 365



Content Inspection

The setting for SSL Content Inspection can be configured



**What is a 'split session'?**

A split session occurs can occur when there are conflicting policies between dependent sites, i.e., when a site that is currently in isolation requests information from a non-isolated site or vice versa.  This happens because cookies that are set by isolated sites are stored in one of Menlo's Disposable Virtual Containers, but cookies set by non-isolated sites are stored in the browser on a user's local machine.

**What are the possible symptoms of a split session (i.e., conflicting policies)?**

* Cookie errors are displayed
* The connection appears to loop
* A white screen or blank page is displayed in the browser
* The browser screen locks
* HTTP-403 Forbidden Error
* SSO Login fails

**How can I prevent split sessions/conflicting policy scenarios?**

* If appropriate, change the configuration so that all the interdependent sites have the same isolation policy (e.g., the originating and referenced sites are both Allowed).
* Consider switching on the  **direct\_on\_allow** feature. This will assist with situations where the user is going from an Isolated site to an Allowed site but not from an Allowed to an Isolated site. This feature is enabled by default for newer tenants, but you may need to request it for older tenants. Please contact Customer Success for further information on this feature.

**What does Menlo use cookies for?**

Most websites use cookies to function correctly and therefore Menlo needs to support cookies so that these sites can function as expected when handled by Menlo.

**Where are the cookies stored?**

Menlo has a cookie database which is stored outside the **Disposable Virtual Container (DVC)**. These cookies are attached to a specific browser session.

**How are cookies protected?**

Cookies are associated with a specific user session; they are automatically encrypted and attached to the user's browsing session once the user has authenticated.  A user cannot access another user's cookies.

**How are cookies removed?**

Cookies are removed when they are deleted from the local browser or when they expire.

**How are cookies used in user authentication?**

* When a user enters valid login details, they are authenticated and a **safeview-id** cookie is created which is unique for that user's credentials and browser connection.
* A different cookie **\_sc\_token**is set when using proxy mode.

For sites that are Allowed, the Security Policy does not include **\*.menlosecurity.com** which means the user may have issues using reCAPTCHA as it will block the generation of a session cookie when the site redirects to **safe.menlosecurity.com**.

How to Use Wireshark to Identify a List of Domains Connected via MSIP

1. Capture the **PCAP** file using Wireshark
2. Start **Wireshark**.
3. Open the PCAP capture file.
4. Enter the following query into the display filter, using the relevant port number for the configuration in the environment being investigated:

**Using SAML SSO on Port 3131**

http.request.method == "CONNECT" and tcp.port==3131

**Using Menlo Authentication on Port 3129**

http.request.method == "CONNECT" and tcp.port==3129

Technologies that are Currently Unsupported or have Known Limitations

**Flash**

Flash is no longer supported in isolation.

Menlo Support Policy for Adobe Flash After it Reaches End of Support in December 2020

**WebGL**

WebGL is supported in isolation from 2.81.0.

**WebRTC**

WebRTC is a browser native communication API for voice calling, video chat, and file sharing.  It is currently not supported in isolation.

**Web Sockets**

Sites that use web sockets are supported in isolation but is not supported in proxy mode (allow).  WS:// will not work via MSIP but WSS:// will work when matching a SSL Exception Rule.

**Browser Extensions**

Browser extensions are currently not supported in isolation.  Many extensions may work as intended since they operate on the DOM tree, but there is a possibility that some extensions will break.

**Client Certificate-Based Authentication**

Client certificate-based authentication does not work in isolation.  However, it will work when matching an SSL Exception Rule.

**ActiveX / Silverlight**

Neither ActiveX nor Silverlight works in isolation.  Both technologies are now deprecated.

**Java**

Java applets are not supported and will not function in isolation.

**SOCKS**

SOCKS is not supported. Menlo Security operates an HTTP proxy service for web isolation and an SMTP proxy service for email isolation.