Block Executable File Download in SWA

Contents

Introduction

This document describes the process of configuring Secure Web Appliance (SWA) to block downloading executable files.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access ToGraphic User Interface (GUI)of SWA
- Administrative Access to the SWA.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

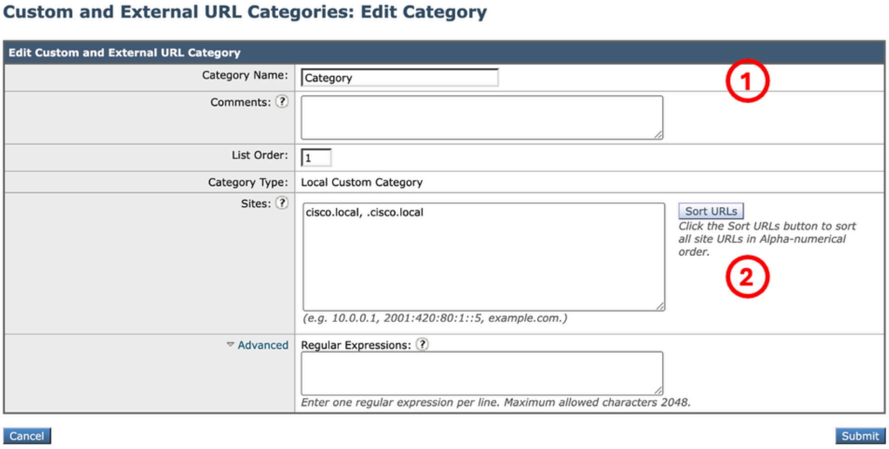
Before you Begin

Cisco SWA can effectively block the download of executable files by inspecting the (Multipurpose Internet Mail Extensions) MIME type of web content. By identifying file types such as application/x-msdownload, application/x-msi and other related MIME types, SWA enforces policies that prevent executable from being delivered to users. In addition to MIME type detection, SWA can leverage file extension filtering, reputation-based analysis, and custom policy rules to further strengthen protection against unwanted or risky downloads. These capabilities help organizations maintain a secure browsing environment and reduce the risk of malware infections.

Tip: SWA cannot identify the MIME type of the file, unless the traffic is decrypted.

application/octet-stream is a generic MIME type used to indicate that a file contains binary data. It does not specify the nature of the file, so it can be used for any file that does not fit a more specific MIME type. This type is commonly assigned to executable files, installers, and other non-text files when the web server cannot determine a more precise type.

Configuration Steps

Step 1. Create a Custom URL Category for the website.	**Step 1.1.**From the GUI Navigate to**Web Security Manage**r and choose**Custom and External URL Categories**. **Step 1.2.**Click**Add Category** to create a new Custom URL Category. **Step 1.3.**Enter**Name**for the new category. **Step 1.4.**Define the domain and/or subdomains of the website that you are trying to block upload traffic (In this example is cisco.local and all its subdomains). **Step 1.5.****Submit**the changes.  Custom and External URL Categories: Edit Category Edit Custom and External URL Category Category Name: Category Comments: List Order: 1 Category Type: Local Custom Category Sites: cisco.local, .cisco.local (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.) Click the Sort URLs button to sort all site URLs in Alpha-numerical order. Advanced Regular Expressions: Enter one regular expression per line. Maximum allowed characters 2048. *Image - Create Custom URL Category* **Tip**: For more information about how to configure Custom URL Categories, kindly visit: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Step 2. Decrypt the traffic for the URL	**Caution**: Decrypting a large number of URLs can lead to performance degradation. **Step 2.1.** From the GUI, Navigate to**Web Security Manager** and choose**Decryption Policies** **Step 2.2.**Click **Add Policy**. **Step 2.3.**Enter**Name** for the new policy.

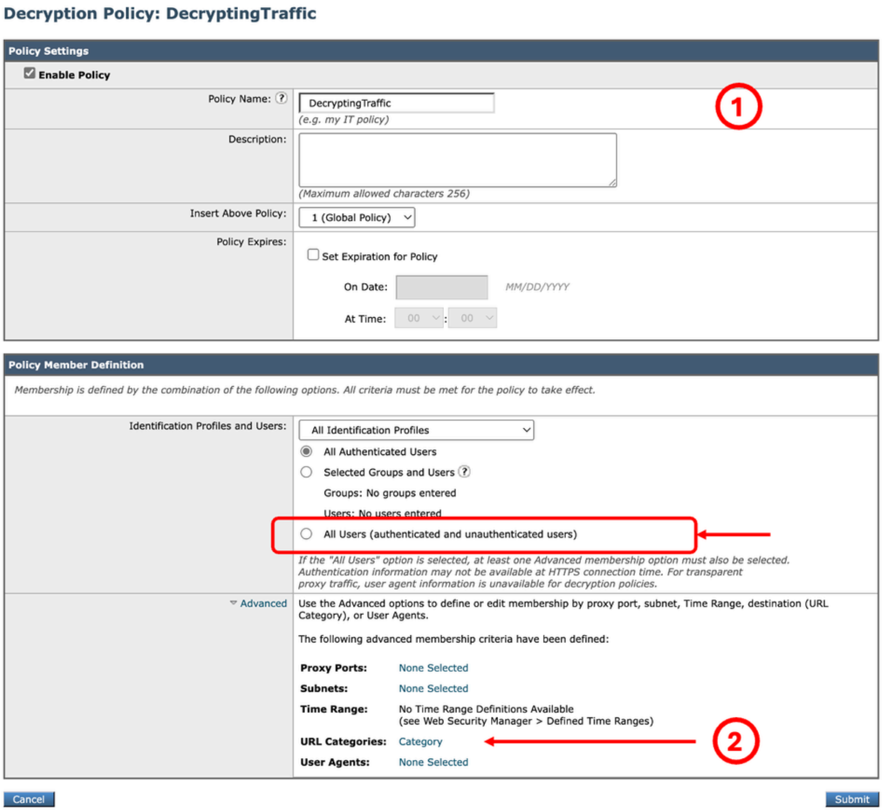
Step 2.4.(Optional) Select the**Identification Profile** that you need this policy applies to.

Tip: (Optional) If you want to apply the policy for all users even if they are not authenticated, choose **All Users (authenticated and unauthenticated users)**.

Step 2.5. From**Policy Member Definition** section, Click **URL Categories**links to add the Custom URL Category.

Step 2.6. Select the URL Category that was created in**Step 1**.

Step 2.7. Click**Submit**.



Decryption Policy: DecryptingTraffic

Policy Settings

☑ Enable Policy

Policy Name: DecryptingTraffic
(e.g. my IT policy)

Description:
(Maximum allowed characters 256)

Insert Above Policy: 1 (Global Policy)

Policy Expires: □ Set Expiration for Policy
On Date: MM/DD/YYYY
At Time: 00 : 00

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: All Identification Profiles
● All Authenticated Users
○ Selected Groups and Users
Groups: No groups entered
Users: No users entered
○ All Users (authenticated and unauthenticated users)
If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

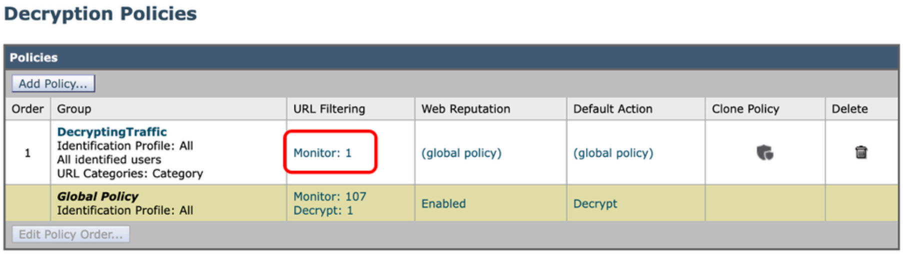
Advanced: Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected
Subnets: None Selected
Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)
URL Categories: Category
User Agents: None Selected

Image - Create a Decryption Policy

Step 2.8. In**Decryption Policies** page, click the link from**URL Filtering** for the new policy.



Decryption Policies

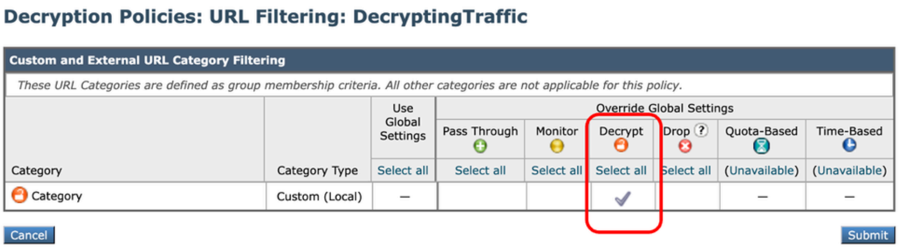
Policies

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	**DecryptingTraffic** Identification Profile: All All identified users URL Categories: Category	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		

Image - Select the URL Filtering

Step 2.9. Choose**Decrypt** as the action for Custom URL Category.

Step 2.10. Click**Submit**.



Decryption Policies: URL Filtering: DecryptingTraffic

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

		Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
Category	Category Type	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Category	Custom (Local)	—			✓		—	—

Image - Set Decrypt as Action

Step 3. Block the Executable Files

Step 3.1. From the GUI, Navigate to**Web Security Manager** and choose**Access Policies**.

Step 3.2. Click**Add Policy**.

Step 3.3. Enter**Name** for the new policy.

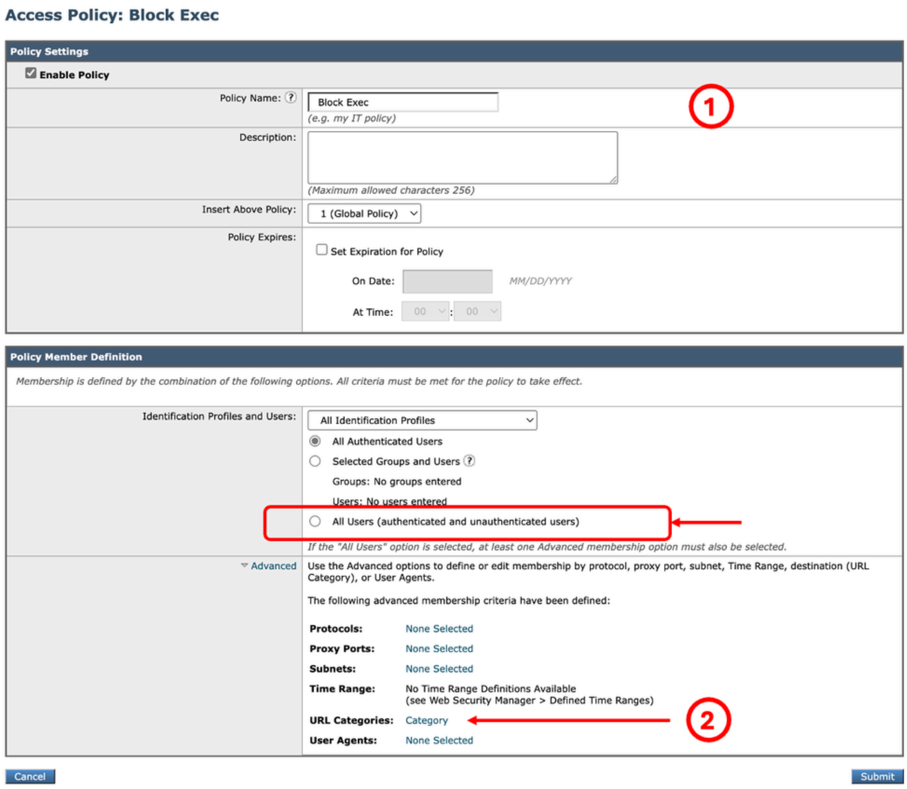
Step 3.4.(Optional) Select the**Identification Profile** that you need this policy applies to.

Tip: (Optional) If you want to apply the policy for all users even if they are not authenticated, choose **All Users (authenticated and unauthenticated users)**.

Step 3.5. From**Policy Member Definition** section, Click **URL Categories** links to add the Custom URL Category.

Step 3.6. Select the URL Category that was created in**Step 1**.

Step 3.7. Click**Submit**.



Access Policy: Block Exec

Policy Settings

☑ Enable Policy

Policy Name: ?	Block Exec (e.g. my IT policy)
Description:	(Maximum allowed characters 256)
Insert Above Policy:	1 (Global Policy)
Policy Expires:	☐ Set Expiration for Policy On Date: MM/DD/YYYY At Time: 00 : 00

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:	All Identification Profiles ● All Authenticated Users ○ Selected Groups and Users ? Groups: No groups entered Users: No users entered ○ All Users (authenticated and unauthenticated users) If the "All Users" option is selected, at least one Advanced membership option must also be selected.
▿ Advanced	Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined:

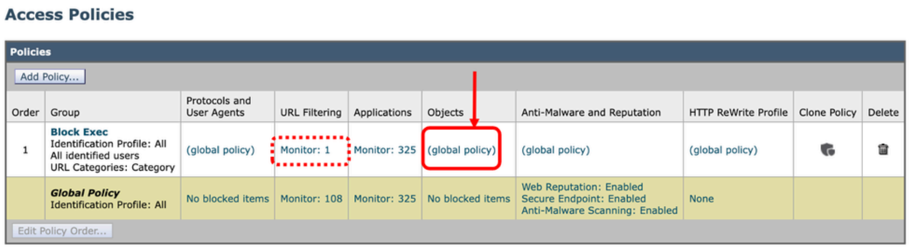
Protocols:	None Selected
Proxy Ports:	None Selected
Subnets:	None Selected
Time Range:	No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
URL Categories:	Category
User Agents:	None Selected

Image - Access Policy

Tip: For the reporting purpose, It is best to choose a name that is not same as any other Access/Decryption Policies.

Step 3.8. In**Access Policies** page, make sure the**URL Filtering** action is set to Monitor.

Step 3.9. In**Access Policies** page, click the link from **Objects** for the new policy.



Access Policies

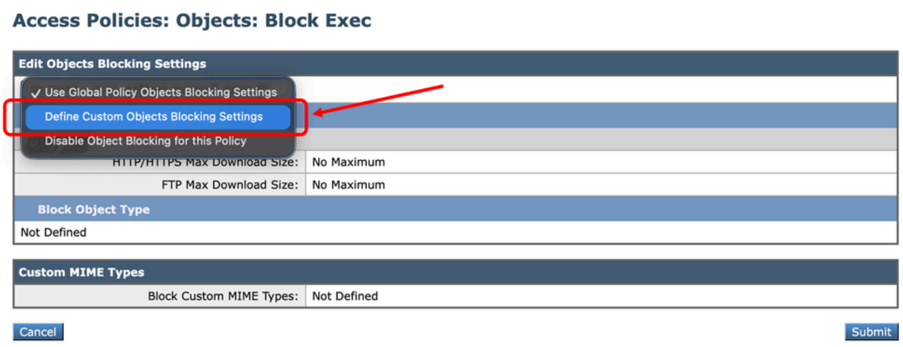
Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	**Block Exec** Identification Profile: All All identified users URL Categories: Category	(global policy)	Monitor: 1	Monitor: 325	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 325	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

Image - Select the Objects

Image - Select the URL Filtering

Step 3.10. From the drop down menu choose **Define Custom Objects Blocking Settings**.



Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

✓ Use Global Policy Objects Blocking Settings
Define Custom Objects Blocking Settings
Disable Object Blocking for this Policy

HTTP/HTTPS Max Download Size:	No Maximum
FTP Max Download Size:	No Maximum

Block Object Type

Not Defined

Custom MIME Types

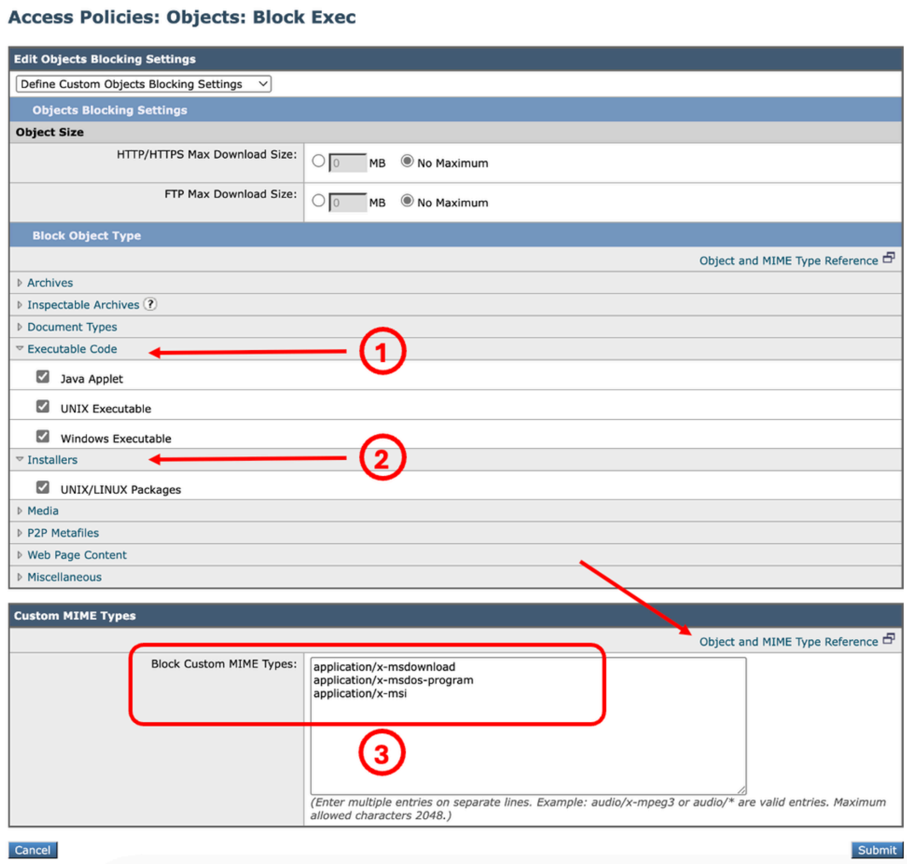
Block Custom MIME Types:	Not Defined

Image – Define Custom Objects

Step 3.11. Click**Executable Code** to select the types of Objects you want to block.

Step 3.12. Click **Installers** to select the types of Objects you want to block.

Step 3.13. Additionally you can enter the MIME types of the files you want to block in the **Custom MIME Types** section.



Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

Define Custom Objects Blocking Settings

Objects Blocking Settings

Object Size

HTTP/HTTPS Max Download Size:	○ 0 MB ● No Maximum
FTP Max Download Size:	○ 0 MB ● No Maximum

Block Object Type

Object and MIME Type Reference

- Archives
- Inspectable Archives
- Document Types
- Executable Code
  - ☑ Java Applet
  - ☑ UNIX Executable
  - ☑ Windows Executable
- Installers
  - ☑ UNIX/LINUX Packages
- Media
- P2P Metafiles
- Web Page Content
- Miscellaneous

Custom MIME Types

Object and MIME Type Reference

Block Custom MIME Types:

```
application/x-msdownload
application/x-msdos-program
application/x-msi
```

(Enter multiple entries on separate lines. Example: audio/x-mpeg3 or audio/* are valid entries. Maximum allowed characters 2048.)

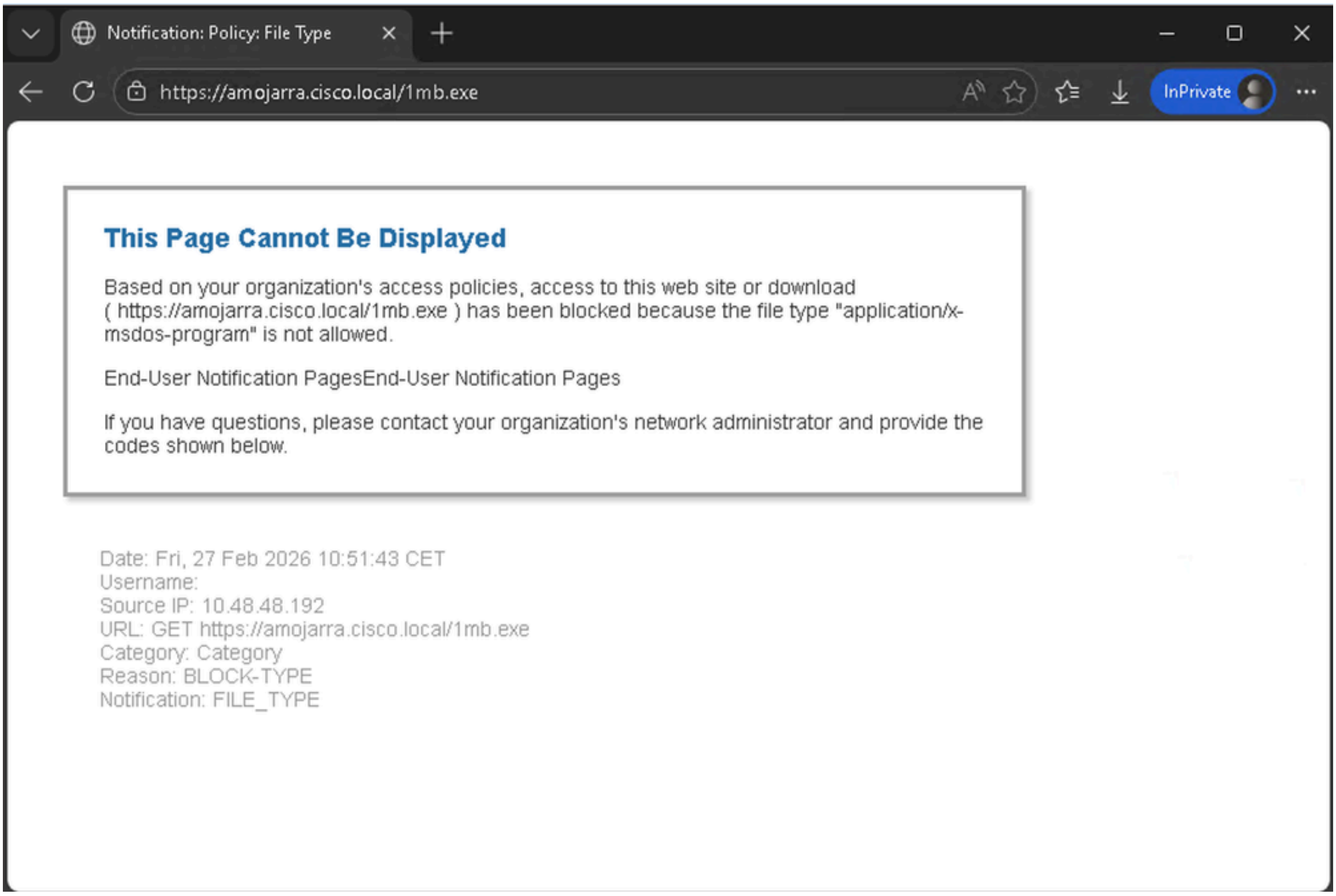
Image - Configuring Objects to Block

Tip: To view the list of the MIME types, click **Object and MIME Type Reference**.

	Step 3.14.Submit. **Step 3.15.Commit** changes.

Validation of File Extension Blocking

In this example, when a user tries to download an executable file, this warning page is displayed:



Notification: Policy: File Type
https://amojarra.cisco.local/1mb.exe
InPrivate

This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site or download (https://amojarra.cisco.local/1mb.exe) has been blocked because the file type "application/x-msdos-program" is not allowed.

End-User Notification PagesEnd-User Notification Pages

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Fri, 27 Feb 2026 10:51:43 CET
Username:
Source IP: 10.48.48.192
URL: GET https://amojarra.cisco.local/1mb.exe
Category: Category
Reason: BLOCK-TYPE
Notification: FILE_TYPE

Image - Blocking Notification Page

Tip: To configure End User Notification (EUN) page, from the GUI navigate to **Security Services** and click **End-User Notification** and modify the **End-User Notification Pages** section.

From the access logs, you can see two log lines related to the traffic.

The first log line is related to the Decryption Policy (Name: **DecryptingTraffic**) that is decrypting the Traffic. The action is **DECRYPT_CUSTOMCAT**

The second Access Log line is related to the Access Policy (Name: **Block_Exec**) that we created in Step.3. The action is **BLOCK_ADMIN_FILE_TYPE**

Policy	Access Log

Decryption Policy	1772186569.823 182 10.48.48.192 **TCP_MISS_SSL/200** 39 CONNECT **tunnel://amojarra.cisco.local:443/** - DIRECT/amojarra.cisco.local - **DECRYPT_CUSTOMCAT_7-DecryptingTraffic**-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"-",-,"-","-","-","-","-","-","-",1.71,0,-,"-","-",-,"-",-,-,"-","-",-,-,"-",-,-> - -
Access Policy	1772186576.735 2242 10.48.48.192 **TCP_DENIED_SSL/403** 0 GET **https://amojarra.cisco.local:443/1mb.exe** - DIRECT/amojarra.cisco.local application/x-msdos-program **BLOCK_ADMIN_FILE_TYPE_12-Block_Exec**-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",ns,0,"-",0,0,0,-,"-",-,-,-,"-",-,-,"-","-",-,-,"nc",-,"-","-","-","Unknown","Unknown","-","-",0.00,0,-,"Unknown","-",-,"-",-,-,"-","-",-,-,"-",-,-> - -

Related Information

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Cisco Secure Email and Web Virtual Appliance Installation Guide
- Configure Custom URL Categories in Secure Web Appliance - Cisco
- Use Secure Web Appliance Best Practices
- Configure Firewall for Secure Web Appliance
- Configure Decryption Certificate in Secure Web Appliance
- Configure and Troubleshoot SNMP in SWA
- Configure SCP Push Logs in Secure Web Appliance with Microsoft Server
- Enable Specific YouTube Channel/Video and Block Rest of YouTube in SWA
- Understand HTTPS Accesslog Format in Secure Web Appliance
- Access Secure Web Appliance Logs
- Bypass Authentication in Secure Web Appliance
- Block Traffic in Secure Web Appliance
- Bypass Microsoft Updates Traffic in Secure Web Appliance