

# Configure Warn Rule Action

## Contents

- [Introduction](#)
- [Overview](#)
- [Duration of Access](#)
- [Activity Report Overview](#)
- [Destination List Restrictions](#)
- [Enabling HTTPS Inspection](#)
- [Creating a Custom Warn Page](#)
- [Conclusion](#)

## Introduction

This document describes a comprehensive understanding of the Warn rule action feature, its configuration, and associated restrictions within Cisco Umbrella.

## Overview

When a user attempts to access a website categorized under the Warn category in Cisco Umbrella, they encounter a Warn page. To proceed, users must click through the Warn page.

Test

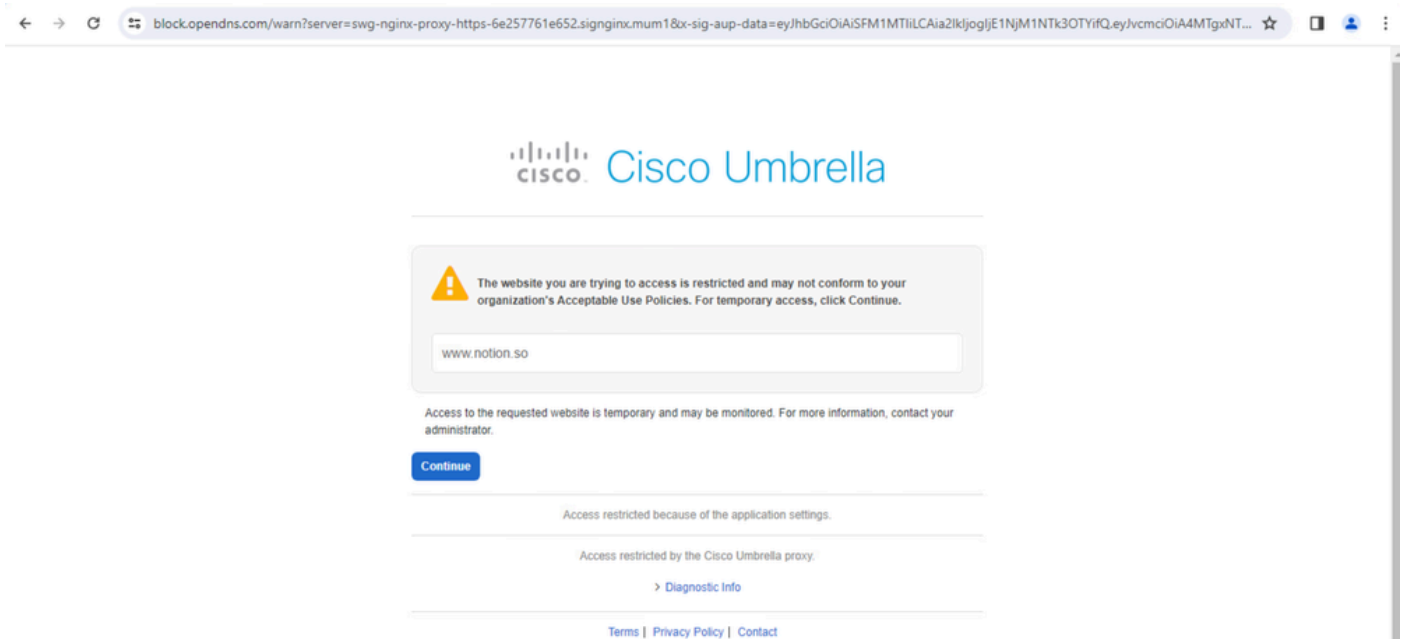
Contains2 Rules

Last ModifiedMar 21, 2024

Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration
<div></div> 1	Test1	<div></div> Warn	1 Anyconnect Roaming Client...	70 Applications ...	Any Day, Any Time No additional configuration applied Protected File Bypass Disabled Umbrella Block and Warn Page (Inherited)



## Duration of Access

Upon clicking through the Warn page, access to the requested destination is granted for a limited duration of one hour. After this period, the Warn page reappears, requiring users to click through again for continued access.

## Activity Report Overview

Warn page interactions are logged within Umbrella's activity reports, providing administrators with insights into user interactions and warnings triggered by the Warn rule action feature.

4 Total		Viewing activity from Mar 14, 2024 4:06 PM to Mar 15, 2024 4:06 PM				Page: 1	Results per page: 50	1 - 4 of 4	<	>
Request	Identity	Policy or Ruleset Identity	Destination	Destination IP	Internal IP	External IP	Action	>		
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		192.168.1.95	123.63.117.88	Allowed	...		
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		192.168.1.95	123.63.117.88	Allowed	...		
WEB	DESKTOP-CSC	DESKTOP-CSC	https://www.notion.so/help/guides/category/ai		192.168.1.95	123.63.117.88	Allowed - Warn Page	...		

4 Total	Viewing activity from Mar 14, 2024 4:06 PM to Mar 15, 2024 4:06 PM	Page: 1	Results per page: 50	1 - 4 of 4	< >	Action ● Allowed – Warn Page Displayed
Request	Identity	Policy or Ruleset Identity ⓘ	Destination	Destination IP	Insert IP	Time Mar 15, 2024 4:03 PM
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		19 ...	Ruleset or Rule Test
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		19 ...	↳ Rule Name Test1
WEB	DESKTOP-CSC	DESKTOP-CSC	https://www.notion.so/help/guides/category/ai		19 ...	
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		19 ...	
						Identity DESKTOP-CSC Lab - 123.63.117.88 Policy or Ruleset Identity DESKTOP-CSC Internal IP Address 192.168.1.95 External IP Address 123.63.117.88 Destination https://www.notion.so/help/guides/category/ai Hostname www.notion.so Categories Application Warn, Online Document Sharing and Collaboration Dispute Categorization Public Application Notion AI Application Category Generative AI Content Type text/html File Action (Remote Browser Isolation) - Total Size in Bytes 1083

## Destination List Restrictions

Enabling the Warn page feature restricts access to Destination Lists. Users are unable to select the Destination List option for websites categorized under Warn.

## Enabling HTTPS Inspection

To enforce the Warn page feature effectively, HTTPS Inspection must be enabled within Cisco Umbrella. HTTPS Inspection decrypts and inspects HTTPS traffic, enabling Umbrella to enforce Warn pages for encrypted connections.

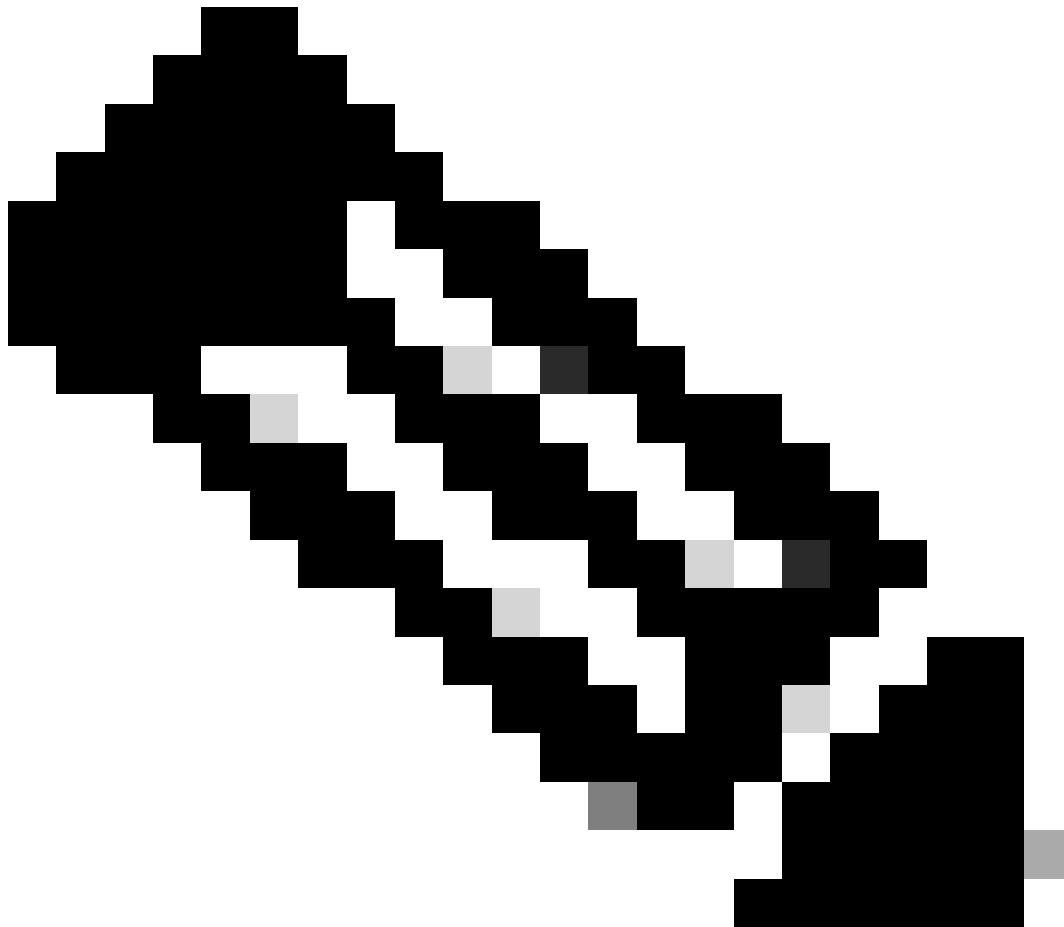
HTTPS Inspection	Enabled	Edit
------------------	---------	------

## Creating a Custom Warn Page

Administrators have the option to create a custom Warn page with personalized messaging. This custom Warn page can be selected when adding rules to a ruleset, providing users with a tailored warning experience.

For detailed instructions on creating a custom Warn page and further information on Warn rule action configuration, please refer to the official documentation: [Create Custom Warn Page](#).

---



**Note:** Any selective decryption list exceptions impact the ability of the proxy to enforce certain policies and features, the warn page is one of them.

---

## Conclusion

Understanding the Warn rule action configuration and associated restrictions is essential for implementing effective security policies within Cisco Umbrella. By leveraging Warn pages and HTTPS Inspection, organizations can enhance their security posture and ensure safe browsing experiences for users.