How to Configure Web Security Appliance Additional Passthrough Settings for the Webex Application

Introduction

This document describes how to configure the Secure Web Appliance (SWA/WSA) bypass policies to ensure proper Cisco Webex application functionality in special deployment conditions.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Async OS for Secure Web Appliance 14.x or higher.
- Administration user access to the Secure Web Appliance Graphic User Interface (GUI).
- Administration user access to the Secure Web Appliance Command Line interface (CLI).

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.

Problem

Based on the Webex public documentation for Network Requirements for Webex Services, proxy server must be configured to allow Webex signaling traffic to access the domains/ URLs listed in the document. The Secure Web Appliance meets the requirements for most environments by enabling the Webex Application Bypass checkbox in bypass settings, however, some additional configurations may be required on Secure Web Appliance to avoid service disruption in the Webex Application. The next steps are recommended for such case scenarios:

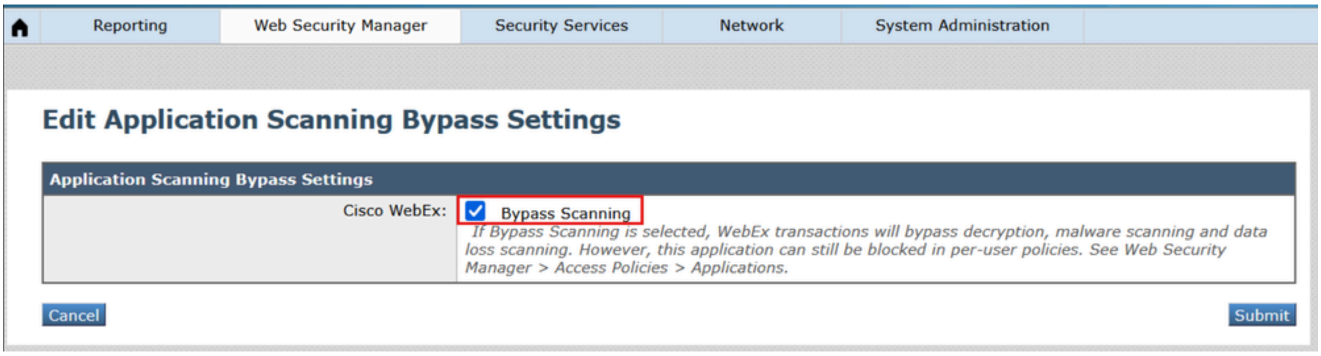
Webex Application Scanning Bypass

The Cisco Webex: Bypass Scanning feature is the first step to enable Webex Application traffic to pass unfiltered through the Secure Web Appliance. It should be enabled in all environments and deployment scenarios where users of the Webex desktop or mobile applications have web traffic proxied through the Secure Web Appliance.

Steps to enable Webex Application Scanning Bypass:

1. In the WSA GUI, browse to **Web Security Manager** > **Bypass Settings** > **Edit Application Bypass Settings.**

2. Check the box for **"Cisco WebEx".**



Edit Application Scanning Bypass Settings

Application Scanning Bypass Settings

Cisco WebEx: ☑ Bypass Scanning

If Bypass Scanning is selected, WebEx transactions will bypass decryption, malware scanning and data loss scanning. However, this application can still be blocked in per-user policies. See Web Security Manager > Access Policies > Applications.

1_wsa_bypass_scanning_settings

3. **Submit** and **Commit** changes

When this setting is enabled, it does not bypass transparent traffic as would be expected once the FQDNs is added to the bypass list on the Secure Web Appliance. Rather, the Webex application traffic is still proxied through the Secure Web Appliance, but it will be passed through on decryption with the decision tag "PASSTHRU_AVC". Below is an example of how this might display in the access logs:

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

Considerations for Unique Environments

There are a few scenarios where additional configurations are required for the Webex app to work when the traffic is proxied through the Secure Web Appliance.

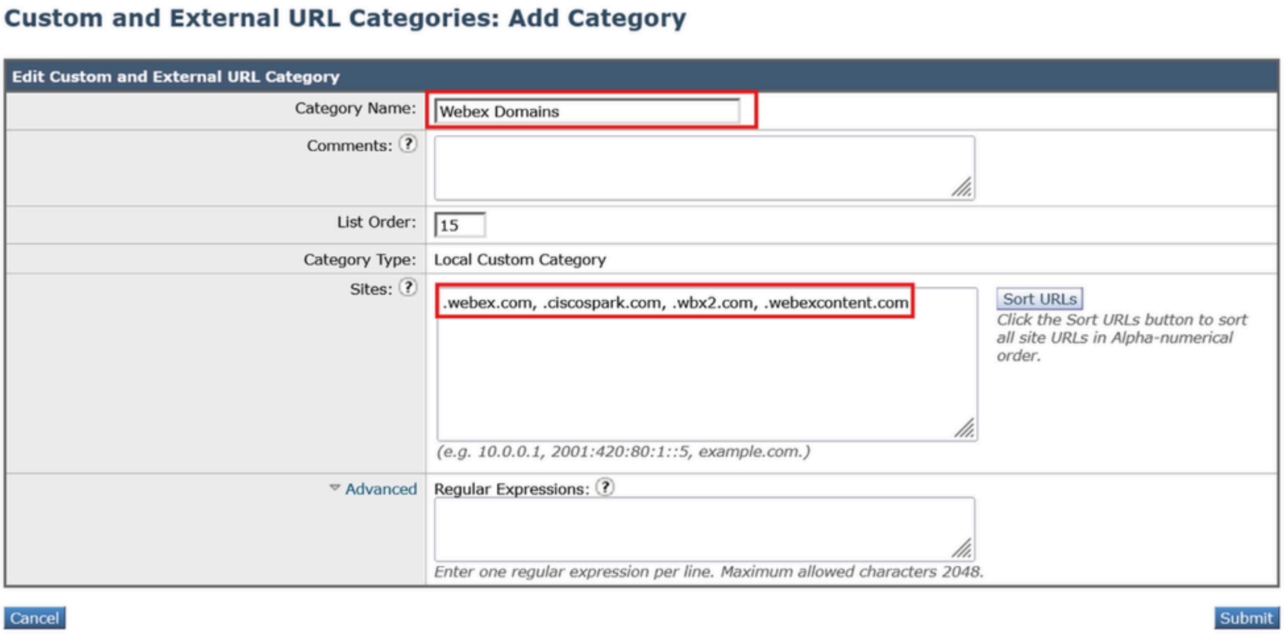
Scenario 1: Webex domains need to be exempted from authentication

This is especially apparent in environments where IP surrogates are not enabled in the Identification Profile, and transparent redirection is used. Based on the existing documentation, the Webex app is capable of NTLMSSP authentication on domain-joined workstations where the proxy is explicitly defined. Otherwise, it is a best practice to configure a custom category for the Webex domains and exempt them from authentication.

Steps to exempt Webex domains from authentication:

1. In the WSA GUI, navigate to **Web Security Manager** > **Custom and External URL Categories** > **Add Category.**
2. Give the new category a name, and place the following domains in the **Sites** section:

   ```
   .webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
   ```



Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name: Webex Domains

Comments:

List Order: 15

Category Type: Local Custom Category

Sites: .webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

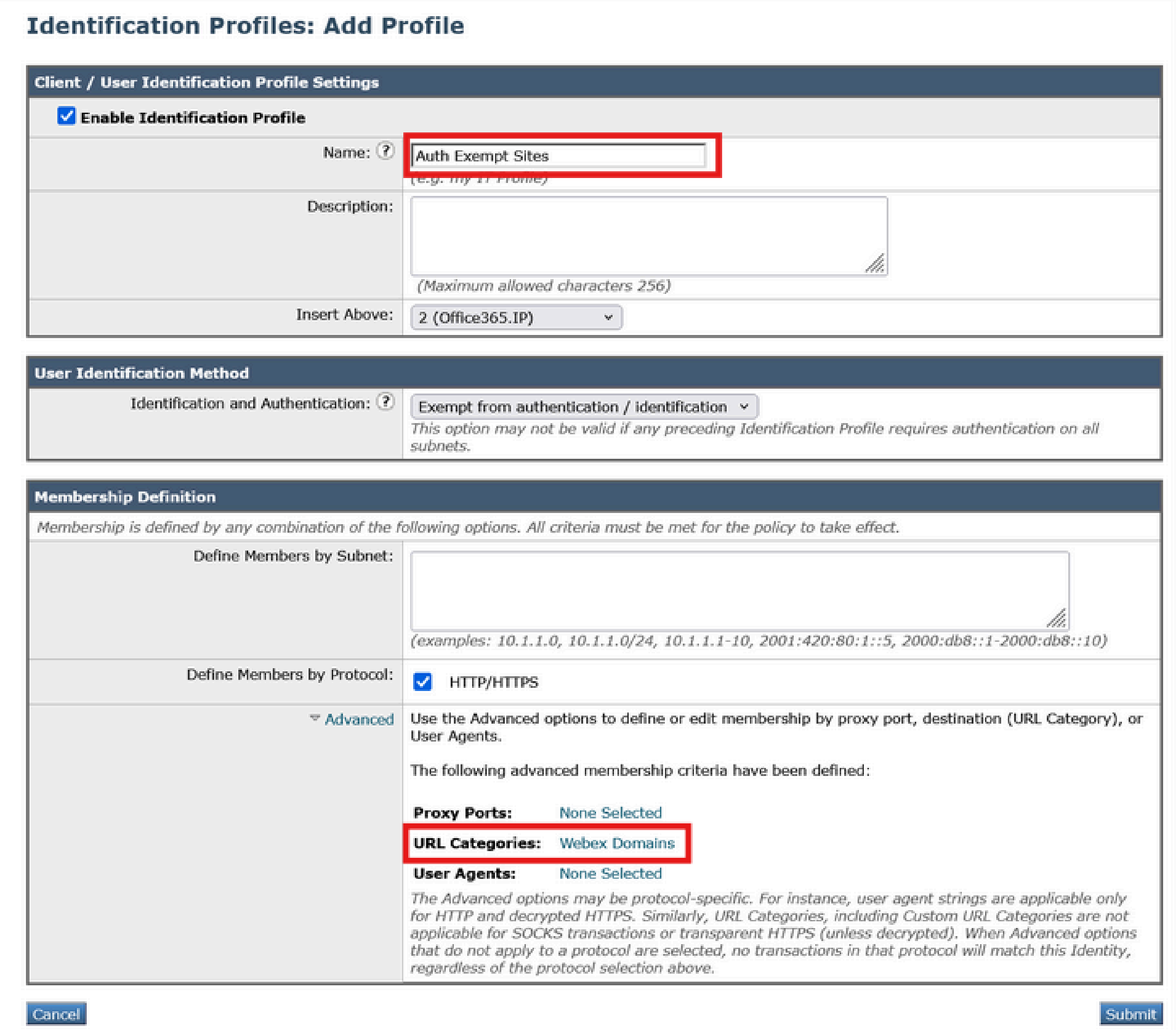
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Advanced Regular Expressions:

Enter one regular expression per line. Maximum allowed characters 2048.

2_wsa_custom_url_category

3. Click **Submit**. Then navigate to **Web Security Manager** > **Identification Profiles** > **Add Identification Profile**
4. Give the new profile a name, and in the **Advanced** section for **URL Categories**, select the new category that was created in step #2



Identification Profiles: Add Profile

Client / User Identification Profile Settings

☑ **Enable Identification Profile**

Name: ?	Auth Exempt Sites (e.g. my IT Profile)
Description:	(Maximum allowed characters 256)
Insert Above:	2 (Office365.IP)

User Identification Method

Identification and Authentication: ?	Exempt from authentication / identification *This option may not be valid if any preceding Identification Profile requires authentication on all subnets.*

Membership Definition

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

Define Members by Subnet:	(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)
Define Members by Protocol:	☑ HTTP/HTTPS
Advanced	Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents. The following advanced membership criteria have been defined: **Proxy Ports:** None Selected **URL Categories:** Webex Domains **User Agents:** None Selected *The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.*

3_wsa_id_profile

5. Ensure the Identification and Authentication in the new profile is set to **Exempt from authentication / identification**
6. **Submit** and **Commit** changes.

Scenario 2: Webex Content domains are not fully honored for decryption bypass.

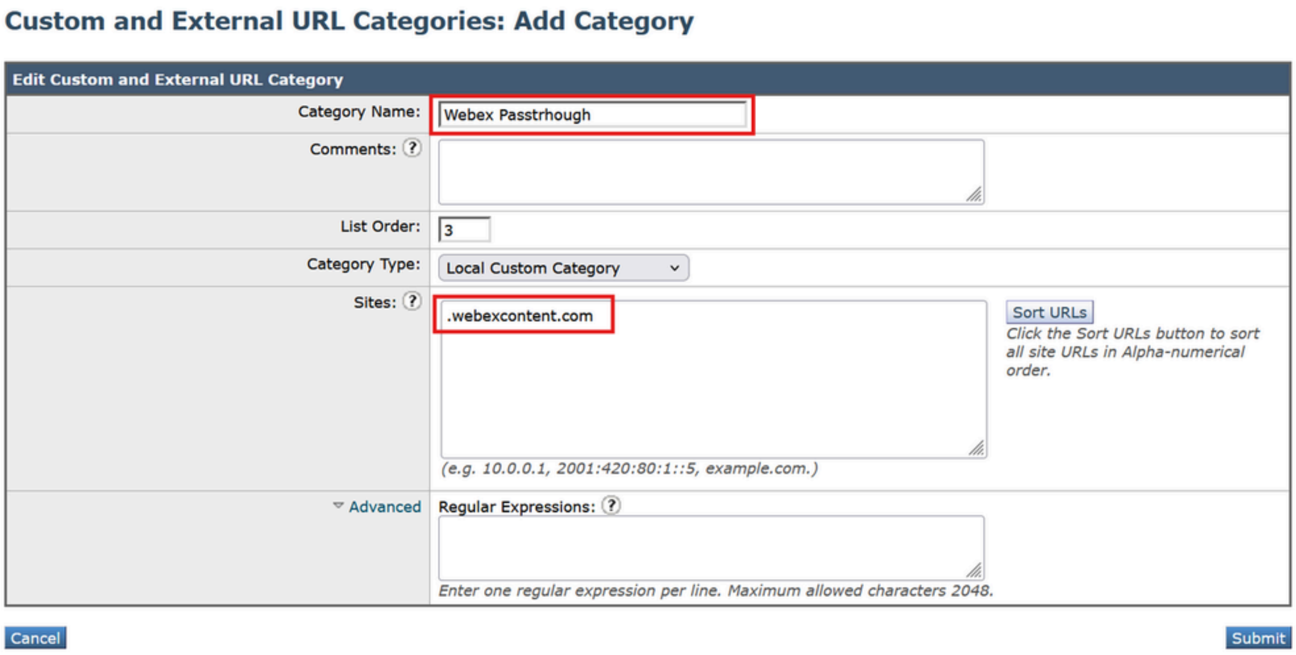
There are a few subdomains related to **webexcontent.com** that do not automatically pass through on decryption when Webex Application Scanning Bypass is enabled. The content served from these domains is trusted by the Webex app when it is decrypted so long as the Secure Web Appliance's decryption certificate is already added to the device's trusted root certificates store, or otherwise signed by an internal certificate authority that is already trusted by the device running the Webex app. However, if the device is unmanaged and the Secure Web Appliance's decryption certificate is not trusted, these domains should be configured to passthrough on decryption.

When transparent redirection deploymeny is in place and there is more than one SWA along client IP spoofing beingused for redirection groups, traffic can be configured to redirect to the Secure Web Appliance based on the destination IP, and similarly the return traffic from the webservers is configured to redirect back through the Secure Web Appliance based on source address. When the Secure Web Appliance is configured to make connections to the webserver using the IP it resolves using DNS lookup, the return traffic may be inadvertently redirected to a different Secure Web Appliance and subsequently dropped. This problem affects not only Webex, but other video streaming applications as well, due to the use of rotating IP addresses on the webservers.

Steps to configure passthrough on decryption for all Webex domains:

1. Ensure **Webex Application Scanning Bypass** is enabled as per instructions above.
2. In the WSA GUI, navigate to **Web Security Manager** > **Custom and External URL Categories** > **Add Category.**
3. Give the new category a name, and place the next domain in the **Sites** section:

```
.webexcontent.com
```



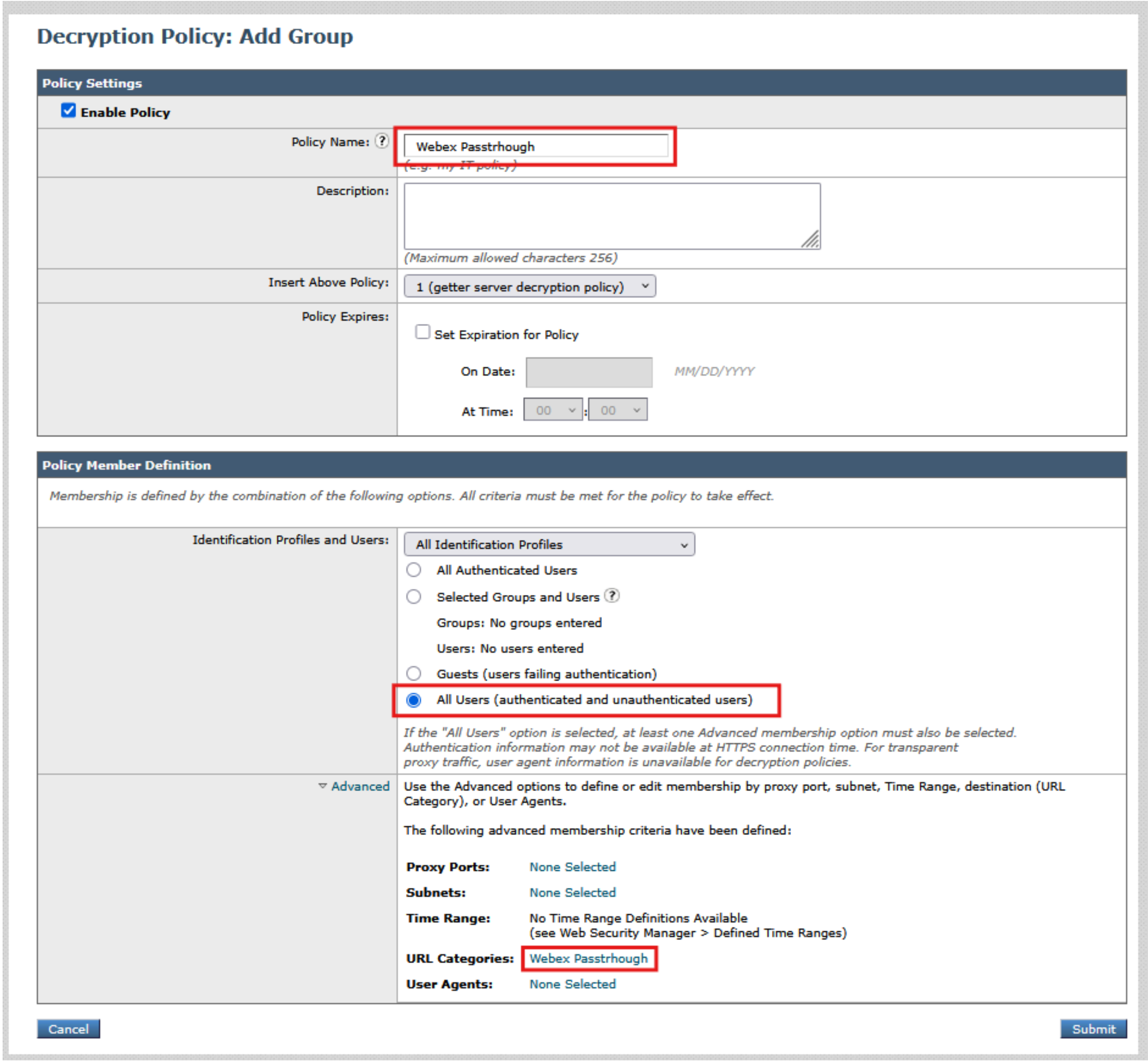
Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name:	Webex Passtrhough
Comments: ?	
List Order:	3
Category Type:	Local Custom Category
Sites: ?	.webexcontent.com (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.) Sort URLs 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.

4_wsa_url_caegory

4. Click **Submit**. Now, navigate to **Web Security Manager** > **Decryption Policies** > **Add Policy**
5. Name the new policy, set **Identification Profiles and Users** to **"All Users",** and in the Advanced section for **URL Categories**, select the new category that was created in step #3



Decryption Policy: Add Group

Policy Settings

☑ **Enable Policy**

Policy Name: Webex Passtrhough

(e.g. my IT policy)

Description:

(Maximum allowed characters 256)

Insert Above Policy: 1 (getter server decryption 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

○ Guests (users failing authentication)

● 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.

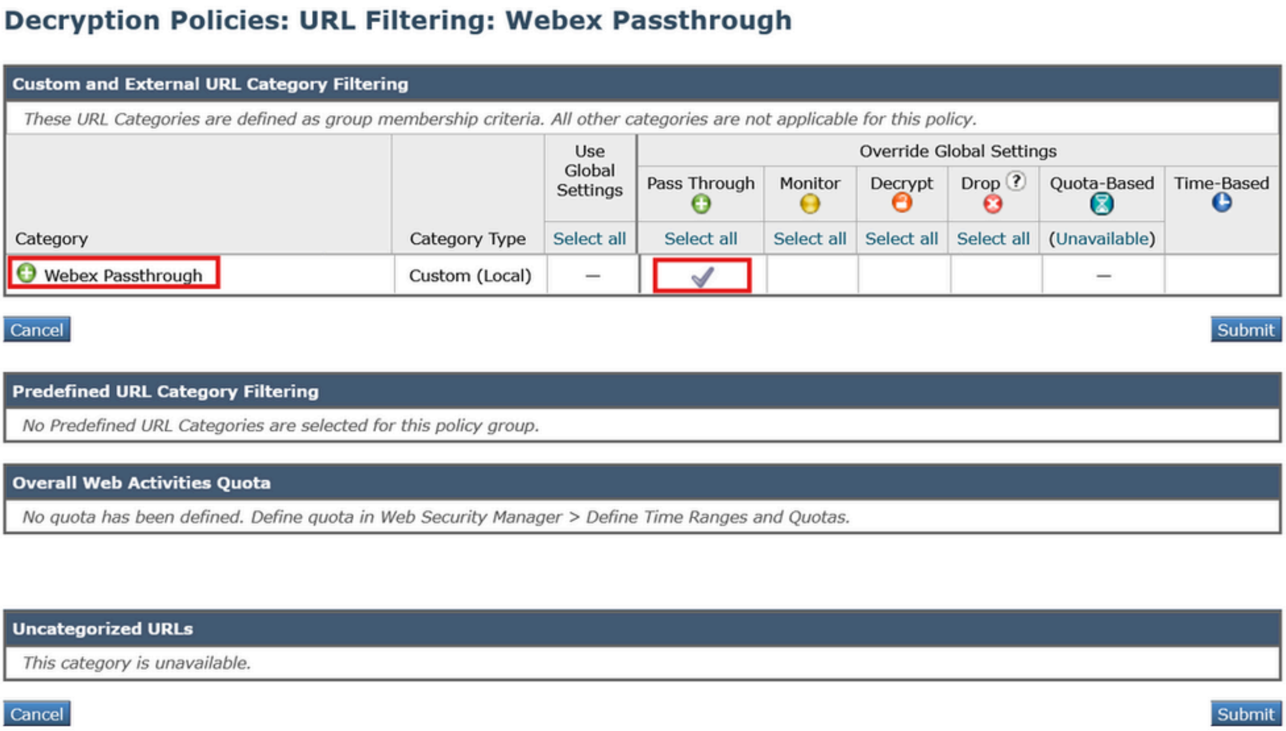
Advanced: Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

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:	Webex Passtrhough
User Agents:	None Selected

5_wsa_decryption_policy

6. Click **Submit**. Then, click on the **URL Filtering** section and set the custom category that was created in step #3 to **"Pass Through".**



Decryption Policies: URL Filtering: Webex Passthrough

Custom and External URL Category Filtering

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

			Override Global Settings					
		Use 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)	
Webex Passthrough	Custom (Local)	—	✓				—	

Predefined URL Category Filtering

No Predefined URL Categories are selected for this policy group.

Overall Web Activities Quota

No quota has been defined. Define quota in Web Security Manager > Define Time Ranges and Quotas.

Uncategorized URLs

This category is unavailable.

6_wsa_url_filtering

7. **Submit** and **Commit** the changes.

If multiple Secure Web Appliances are deployed for transparent redirection and client IP spoofing is enabled, there are two solutions to this:

1. Set the outgoing and return WCCP services to load balance based on client address rather than server address.
2. In the WSA CLI, set **advancedproxyconfig** > **DNS** > "**Find web server by**" to always use the client-supplied IP address on connections to the webserver (options 2 and 3). More information about this setting can be found in the DNS section of the Use Secure Web Appliance Best Practices guide.

Verification

When the passthrough settings complete, Webex traffic will be processed on the access logs as Pass through as per policies:

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

Review and monitor the webex application, if any slowness or service disruption is reported, review the access logs one more time and validate all webex-side traffic is processed correctly.

Related Information

- Network Requirements for Webex Services

- Use Secure Web Appliance Best Practices