Configure Upstream Proxy in Secure Web Appliance

Contents

Introduction

This document describes the steps to Configure Upstream Proxy in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SWA administration.
- Basic Networking and Proxy protocols.

Cisco recommends that you have these tools installed:

- Physical or Virtual SWA
- Administrative Access to the SWA Graphical User Interface (GUI)

- Administrative Access to the SWA Command Line Interface (CLI)

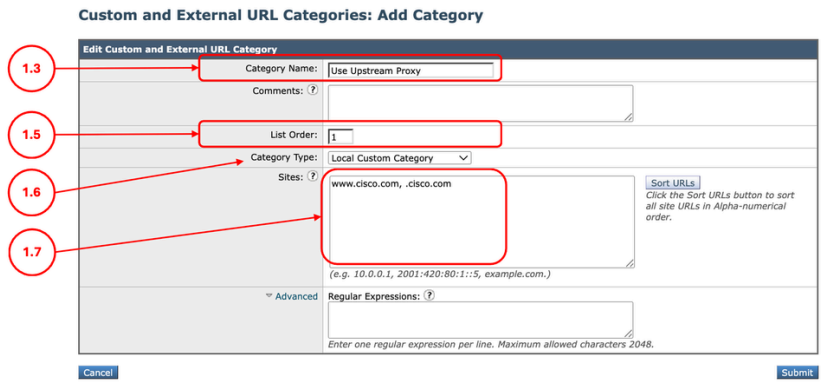
Components Used

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.

Configuring Upstream Proxy

Use these steps to configure an Upstream Proxy in SWA.

Steps	Steps
Step 1. (Optional) Create a Custom URL Category for the URLs **Note**: If you would like to define the upstream proxy for all traffic, you can skip this step.	**Step 1.1.**From**GUI**, Choose**Web Security Manager** and then click **Custom and External URL Categories**. **Step 1.2.**Click**Add Category**to add a Custom URL Category. **Step 1.3.**Assign a unique **CategoryName**. **Step 1.4.** (Optional) Add **Description**. **Step 1.5.** From **List Order**, choose the first category to position on top. **Step 1.6.** From **Category Type**drop-down list, choose **Local Custom Category.** **Step 1.7.** Add desired URLs in the **Sites** Section. **Step 1.8. Submit**.  *Image - Create a Custom URL Category*

Step 2. (Optional) Create an Identification Profile to Use the Upstream Proxy

Note: If you would like to define the upstream proxy for all traffic, you can skip this step.

Step 2.1. From**GUI**, Choose**Web Security Manager** and then click **Identification Profiles**.
Step 2.2. Click**Add Profile**to add a profile.
Step 2.3. Use the**Enable Identification Profile**check box to enable this profile, or to quickly disable it without deleting it.
Step 2.4. Assign a unique profile**Name**.
Step 2.5. (Optional) Add **Description**.
Step 2.6. From the**Insert Above**drop-down list, choose where this profile is to appear in the table.

Step 2.7. If you would like to **not authenticate** the users hitting this policy, In the**User Identification Method**section, choose**Exempt from authentication/ identification,**
else configure the authentication parameters.

Step 2.8. In the **Define Members by Subnet**, leave this field blank to include all Client IP address unless you would like to Pass Through the traffic for a certain IP addresses.

Step 2.9. (**Optional**: If you need to use an upstream proxy for specific users accessing certain websites, complete this step.) From **Advanced** section, choose **Custom URL Categories**, and **Add** the **Custom URL Category** that was created on **Step 1**

Step 2.10. Submit.

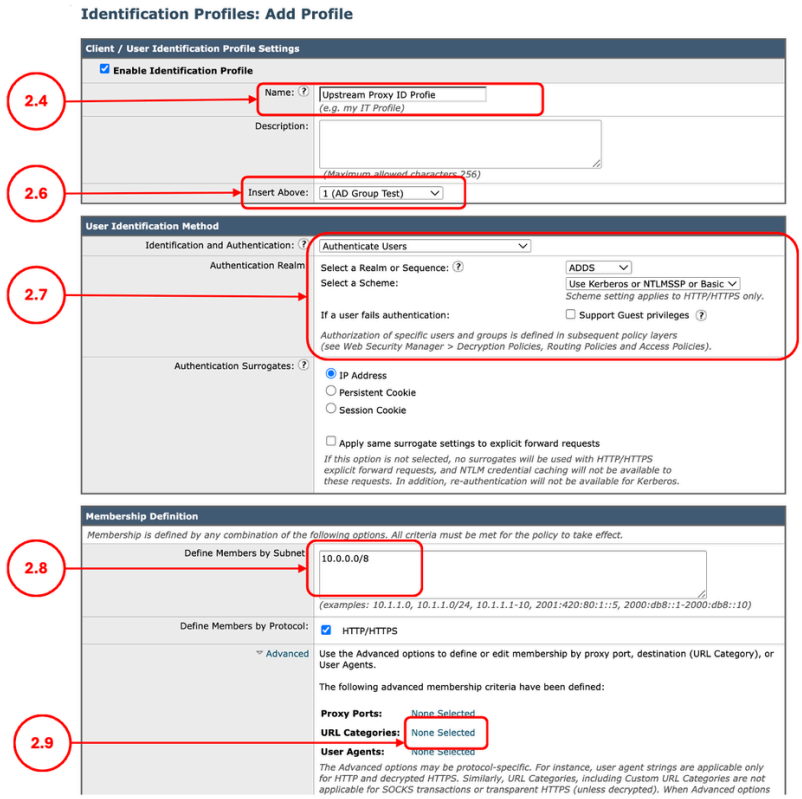
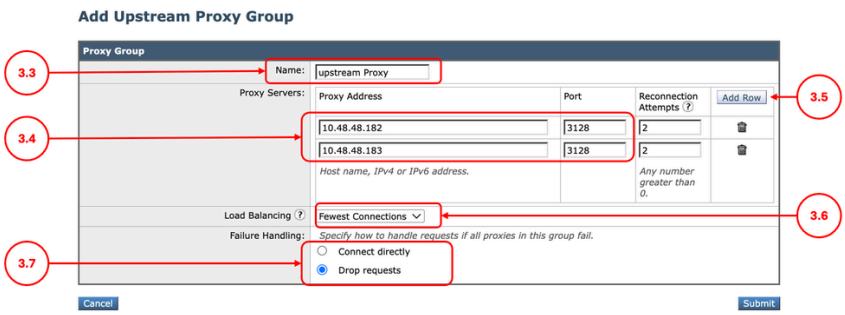


Image - Create an Identification Profile

Step 3. Create the Upstream Proxy

Step 3.1. From**GUI**, Choose**Network** and then click **Upstream Proxy**.

	Step 3.2. Click**Add Group**. **Step 3.3.**Assign a unique**Name**. **Step 3.4.** Define the **Proxy Address** and **Port Number**. **Step 3.5.** (**Optional**) If you have more than one Upstream Proxy, click **Add Row** to define the next Proxy. **Step 3.6.** (**Optional**) If you entered more than one Upstream Proxy from the **Load Balancing section**, define the desired Load Balancing method, • **None (failover)**: The Web Proxy directs transactions to one external proxy in the group. It tries to connect to the proxies in the order they are listed. If one proxy cannot be reached, the Web Proxy attempts to connect to the next one in the list. • **Fewest connections**: The Web Proxy keeps track of how many active requests are with the different proxies in the group and it directs a transaction to the proxy currently servicing the fewest number of connections. • **Hash based**:Least recently used. The Web Proxy directs a transaction to the proxy that least recently received a transaction if all proxies are currently active. This setting is similar to round robin except the Web Proxy also takes into account transactions a proxy has received by being a member in a different proxy group. That is, if a proxy is listed in multiple proxy groups, the “least recently used” option is less likely to overburden that proxy. • **Round robin**: The Web Proxy cycles transactions equally among all proxies in the group in the listed order. **Step 3.7.** Choose the **Failure Handling** option depends on your internal policy. • **Connect directly**:Send the requests directly to their destination servers. • **Drop requests**:Discard the requests without forwarding them. **Step 3.8. Submit**.  *Image - Add Upstream Proxy Group*
Step 4. (Optional) Upload the	**Step 4.1.**From**GUI**, Choose**Network** and then click**Certificate**

Decryption Certificate

Note: If the Upstream Proxy is not decrypting the traffic or its CA server is already trusted in the SWA, you can skip this step

Management.

Step 4.2. From the **Certificate Management** section, click **Manage Trusted Root Certificates**.

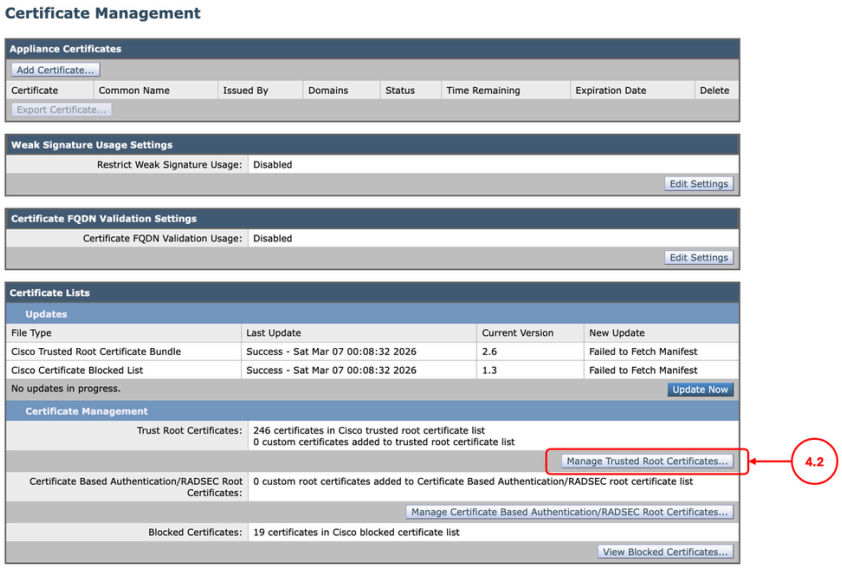


Image - Manage Trusted Root Certificate

Step 4.3. Submit and **Commit** changes.

Caution: If both root and intermediate CA certificates are required, upload the root CA certificate first, then click Submit and Commit. After the commit completes, import the intermediate CA certificate, and again submit and commit the changes.

Step 5. Configure the Routing Policy

Step 5.1. From**GUI**, Choose**Web Security Manager** and then click **Routing Policy**.

Step 5.2. (**Optional**) If you would like to use the upstream proxy for specific users or websites, click **Add Policy**, and select the Identification Profile that you created on **Step 2**.

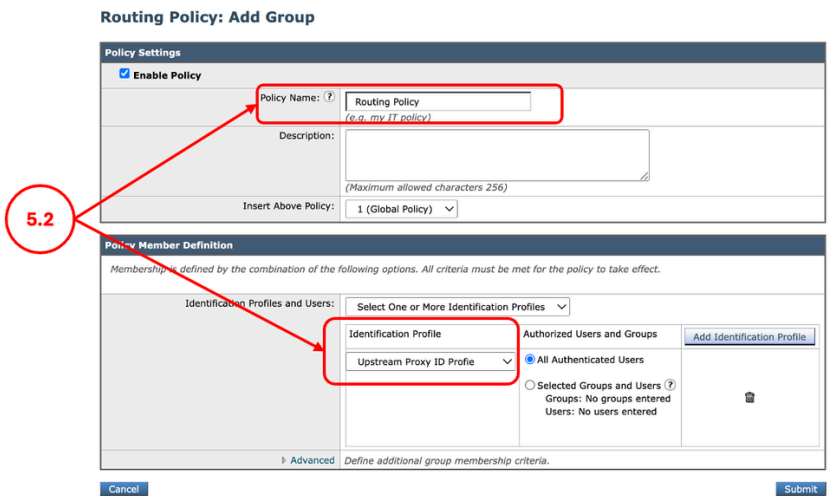


Image - Adding ID Profile to Routing Policy

Step 5.3. For the desired conditions, that you would like to use the upstream proxy, click on Routing Destination link and select the Upstream Proxy Group you created on **Step 3**.

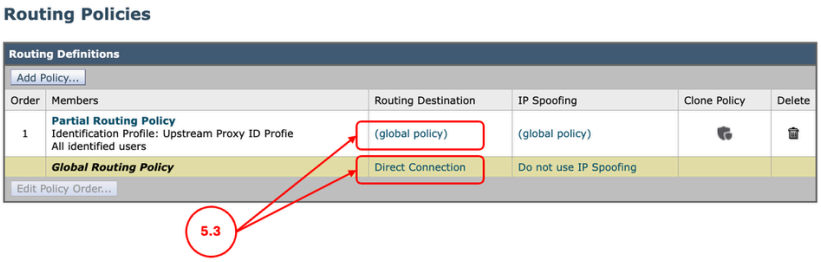


Image - Configuring Routing Destination

Note: If you would like all the traffic using upstream proxy, from the **Global Routing Policy,** select the desired Upstream Proxy.

Step 5.4. Submit and **Commit** the changes.

Step 6. (Optional) Configuring the Upstream Proxy Unresponsive Timeout Settings

Tip: It is recommended not to modify these values unless you fully understand their behavior and potential impact.

Step 6.1. Log in to the CLI and run **advancedproxyconfig**

Step 6.2. Select **MISCELLANEOUS**

Step 6.3. Press Enter until you see **Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds).** you can configure the minimum amount of time, SWA waits to retry the upstream proxy that was previously declared **Sick**. The default value is 10 seconds.

Step 6.4. Press Enter to proceed to the next setting. When defining the **maximum idle timeout for checking an unresponsive upstream proxy,** note that if this timeout value is reached before the configured number of **reconnection attempts** is exhausted (**Step 3**), the SWA consider the upstream proxy offline.

	Step 6.7. Keep pressing Enter, until you exit the wizard, run **commit** to save the changes.

Logging

Accesslogs

In the Accesslogs, the traffic that was routed to upstream proxy are shown as **DEFAULT_PARENT** followed by the name of the upstream proxy. here is an example:

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

Proxylogs

From the proxylogs, you can verify the health status of the upstream proxies.

Tip: You can filter for **peer** to review the logs related to the upstream proxy.

Here are some examples, since we configured the Reconnecting Attempts on **Step 3** to two times, after two failure connecting to the upstream proxy, the upstream proxy is declared dad and SWA removes this upstream proxy from the list until the proxy process is restarted.

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

Note: If the upstream proxy does not respond to TCP SYN requests, fails to return an HTTP response code, or returns an HTTP 504 (Gateway Timeout) response, the SWA considers the upstream proxy unavailable and changes its status from **Healthy** to **Sick**.

Tip: The SWA considers an upstream proxy healthy if it returns a VIA header.

Related Information

- User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance

- Configure Custom URL Categories in Secure Web Appliance - Cisco
- How To Exempt Office 365 Traffic From Authentication and Decryption on Cisco Web Security Appliance (WSA) - Cisco
- Use Secure Web Appliance Best Practices - Cisco
- Block Traffic in Secure Web Appliance
- Block Upload Traffic in Secure Web Appliance
- Block Executable File Download in SWA
- Bypass Microsoft Updates Traffic in Secure Web Appliance
- Bypass Authentication in Secure Web Appliance - Cisco