

Configure Secure Web Appliance to Allow Guest Access

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Scenario Overview](#)

[Configuration Steps](#)

[Step 1. Create Identification Profile.](#)

[Step 2. \(Optional\) Create the Custom URL Categories for Allowed and Blocked URLs](#)

[Step 3. Create Decryption Policy for Managed Devices](#)

[Step 4. Create Decryption Policy for Unmanaged Devices](#)

[Step 5. Create Access Policy for Managed Devices](#)

[Step 6. Create Access Policy for Unmanaged Devices](#)

[Step 7. \(Optional\) Create Cisco Data Security Policy for Managed Devices](#)

[Step 8. \(Optional\) Create Cisco Data Security Policy for Unmanaged Devices](#)

[Step 9. Saving the Changes](#)

[Related Information](#)

Introduction

This document describes steps to allow users which has not installed the decryption certificate to access the Internet via Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Physical or Virtual SWA Installed.
- License activated or installed.
- The setup wizard is completed.
- Administrative Access to the SWA Graphical User Interface (GUI).

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.

Scenario Overview

This article addresses a network access control scenario within the 10.10.10.0/24 Wi-Fi subnet. The environment consists of two distinct user groups requiring different security and access policies:

- **Managed Devices:** Company-issued laptops that are fully authenticated and have the SWA decryption certificate installed. These devices are trusted and typically subject to standard corporate access policies.
- **Unmanaged/Guest Devices:** Personal laptops and mobile devices that are unauthenticated and lack the SWA decryption certificate.

Objective:

The company aims to implement restrictive web access policies for unmanaged devices, limiting their connectivity to a specific subset of allowed URLs while ensuring that corporate resources remain secure.

 **Note:** Since the Decryption Certificate is not trusted on the unmanaged devices, you cannot decrypt the HTTPS traffic and the action must be set to pass through.

Configuration Steps

<p>Step 1. Create Identification Profile.</p>	<p>Step 1.1. From the SWA GUI, navigate to Web Security Manager and select Identification Profile.</p> <p>Step 1.2. Click Add Identification Profile.</p> <p>Step 1.3. Define a Name for the Profile.</p> <p>Step 1.4. (Optional) Define the Description.</p> <p>Step 1.5. Choose Authenticate Users in Identification and Authentication.</p> <p>Step 1.6. Choose the Active Directory realm from Select a Realm or Sequence.</p> <p>Step 1.7. From Select a Scheme, select the desired authentication protocols.</p> <hr/> <p> Tip: Do not choose Basic Authentication in the Select a Scheme list.</p> <hr/> <p>Step 1.8. Select the check box for Support Guest privileges.</p> <p>Step 1.9. (Optional) Depends on your design, you can enable the Surrogate, by enabling the Apply same surrogate settings to explicit forward requests.</p>
--	---



Caution: Since you cannot decrypt the traffic, in the transparent deployment do not select **Persistent Cookie** or **Session Cookie**.

Step 1.10. Define the IP address subnet in, **Define Members by Subnet**.

Step 1.11. **Submit** and **Commit** the changes.

Image - Define the Identification Profile

Step 2. (Optional) Create the Custom URL Categories for Allowed and Blocked URLs

Step 2.1. From the GUI Navigate to **Web Security Manager** and choose **Custom and External URL Categories**.

Step 2.2. Click **Add Category** to create a new Custom URL Category.

Step 2.3. Enter **Name** for the new category.

Step 2.4. Define the domain and/or subdomains of the websites that you want to block the access.

Step 2.5. **Submit** the changes.

Step 2.6. Use the same steps to create a URL category for the website that you are allowing the access.

Custom and External URL Categories: Edit Category

2.3 → Category Name: Blocked WiFi Access

2.4 → Sites: example.com, example.com

Category Name: Blocked WiFi Access

Comments: ?

List Order: 2

Category Type: Local Custom Category

Sites: ? example.com, example.com

Regular Expressions: ?

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

Cancel Submit

Custom and External URL Categories: Edit Category

2.3 → Category Name: Allowed WiFi Access

2.4 → Sites: cisco.com, cisco.com

Category Name: Allowed WiFi Access

Comments: ?

List Order: 1

Category Type: Local Custom Category

Sites: ? cisco.com, cisco.com

Regular Expressions: ?

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

Cancel Submit

Image - Define Custom URL Category

Step 3. Create Decryption Policy for Managed Devices

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

Step 3.2. Click **Add Policy**.

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

Step 3.4. Choose **Select One or More Identification Profiles** from **Identification Profiles and Users** drop down menu.

Step 3.5. Select the **Identification Profile** that was created in **Step 1**.

Step 3.6. Select **All Authenticated Users**.

Step 3.7. Click **Submit**.

Decryption Policy: WIFI Users DP

Create Decryption Policy for Managed Devices

Step 3.8. In **Decryption Policies** page, click the link from **URL Filtering** for the new policy.

Step 3.9. (Optional) You can add any Custom URL Category by click on **Select Custom Categories** and choose **Include in Policy** in front of the category names

Step 3.10. Configure the Action for each **Custom and External URL Category Filtering** and **Predefined URL Category Filtering**.

Step 3.11. Click **Submit**

Image - Configure Action for Decryption Policy

Step 4. Create Decryption Policy for Unmanaged Devices

Step 4.1. From the GUI, Navigate to **Web Security Manager** and choose **Decryption Policies**

Step 4.2. Click **Add Policy**.

Step 4.3. Enter **Name** for the new policy.

Step 4.4. Choose **Select One or More Identification Profiles** from **Identification Profiles and Users** drop down menu.

Step 4.5. Select the **Identification Profile** that was created in **Step 1**.

Step 4.6. Select **Guests (users failing authentication)**.

Step 4.7. Click **Submit**.

Decryption Policy: WiFi Guest DP

Enable Policy

Policy Name: WiFi Guest DP
(e.g. my IT policy)

Description:

Insert Above Policy: 2 (Global Policy)

Policy Expires:

Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: 00:00:00

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: Select One or More Identification Profiles

Identification Profile: WiFi IDP

Authorized Users and Groups: Add Identification Profile

All Authenticated Users

Selected Groups and Users (?)

Groups: No groups entered

Users: No users entered

Guests (users failing authentication)

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

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: None Selected

User Agents: None Selected

Cancel Submit

Create Decryption Policy for Unmanaged Devices

Step 4.8. In **Decryption Policies** page, click the link from **URL Filtering** for the new policy.

Step 4.9. (Optional) You can add any Custom URL Category by click on **Select Custom Categories** and choose **Include in Policy** in front of the category names

Step 4.10. Configure the Action for each **Custom and External URL Category Filtering** and **Predefined URL Category Filtering**.



Note: Do not use **Decrypt** as the action, since the SWA decryption certificate is not trusted on the unmanaged devices.

Decryption Policies: URL Filtering: WiFi Guest DP

Category	Category Type	Use Global Settings	Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Blocked WiFi Access	Custom (Local)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				

Category	Use Global Settings	Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Adult	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advertisements	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alcohol	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Arts	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Astrology	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auctions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Business and Industry	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Image - Decryption Action for Unmanaged Devices

Step 4.11. Scroll down on the Uncategorized URLs section choose the proper action.

Uncategorized URLs:

Image - Uncategorized URLs

Tip: For the security perspective it is best to set the action to **Drop**, in case any URL needs access, you can add them in the Custom URL Category assigned to the Policy.

Step 4.12. Click **Submit**

Step 5. Create Access Policy for Managed Devices

Step 5.1. From the GUI, Navigate to **Web Security Manager** and choose **Access Policies**

Step 5.2. Click **Add Policy**.

Step 5.3. Enter **Name** for the new policy.

Step 5.4. Choose **Select One or More Identification Profiles** from **Identification Profiles and Users** drop down menu.

Step 5.5. Select the **Identification Profile** that was created in **Step 1**.

Step 5.6. Select **All Authenticated Users**.

Step 5.7. Click **Submit**.

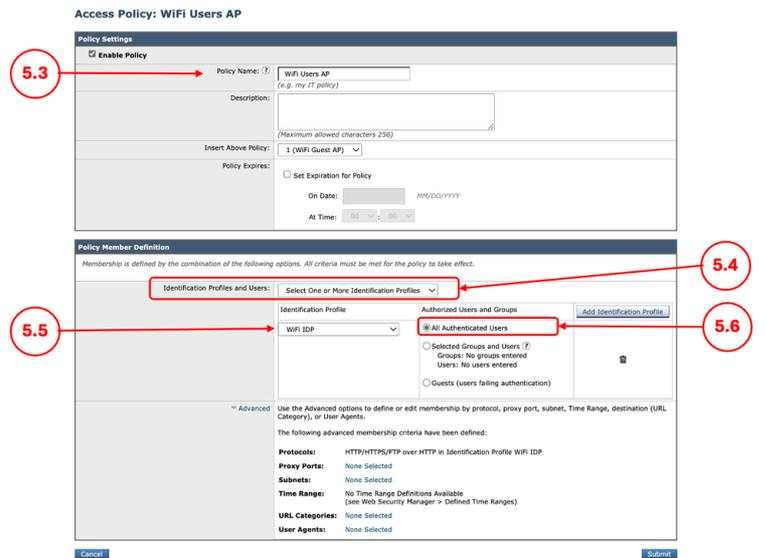


Image - Access Policy for Managed Devices

Step 5.8. In **Access Policies** page, click the link from **URL Filtering** for the new policy.

Step 5.9. (Optional) You can add any Custom URL Category by click on **Select Custom Categories** and choose **Include in Policy** in front of the category names

Step 5.10. Configure the Action for each **Custom and External URL Category Filtering** and **Predefined URL Category Filtering**.

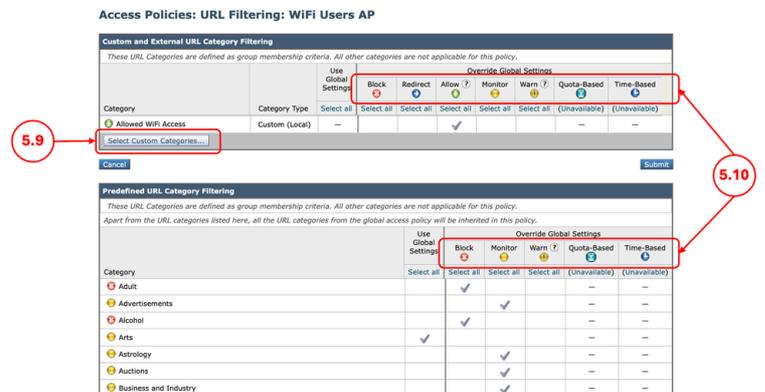


Image - Access Policy URL Filtering for Managed Devices

Step 5.11. Click **Submit**.

Step 6. Create Access Policy for Unmanaged Devices

Step 6.1. From the GUI, Navigate to **Web Security Manager** and choose **Access Policies**

Step 6.2. Click **Add Policy**.

Step 6.3. Enter **Name** for the new policy.

Step 6.4. Choose **Select One or More Identification**

Profiles from **Identification Profiles and Users** drop down menu.

Step 6.5. Select the **Identification Profile** that was created in **Step 1**.

Step 6.6. Select **Guests (users failing authentication)**.

Step 6.7. Click **Submit**.

Access Policy: WiFi Guest AP

Policy Settings

Enable Policy

Policy Name: WiFi Guest AP (A.g. my IT policy)

Description:

Insert Above Policy: 2 (Global Policy)

Policy Expires:

Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: HH:MM:SS

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: Select One or More Identification Profiles

Identification Profile: WiFi IDP

Authorized Users and Groups: All Authenticated Users Selected Groups and Users (?)

Groups: No groups entered

Users: No users entered

Guests (users failing authentication)

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: HTTP/HTTPS/FTP over HTTP in Identification Profile WiFi IDP

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (See Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Buttons: Cancel, Submit

Image - Access Policy for Unmanaged Devices

Step 6.8. In **Access Policies** page, click the link from **URL Filtering** for the new policy.

Step 6.9. (Optional) You can add any Custom URL Category by click on **Select Custom Categories** and choose **Include in Policy** in front of the category names

Step 6.10. Configure the Action for each **Custom and External URL Category Filtering** and **Predefined URL Category Filtering**.

Access Policies: URL Filtering: WiFi Guest AP

Custom and External URL Category Filtering

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

Category	Category Type	Use Global Settings	Override Global Settings						
			Block	Redirect	Allow (?)	Monitor	Warn (?)	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	--	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Blocked WiFi Access	Custom (Local)	--	✓			✓			

Buttons: Cancel, Submit

Predefined URL Category Filtering

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

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Override Global Settings					
		Block	Monitor	Warn (?)	Quota-Based	Time-Based	
Adult	Select all	✓					
Advertisements	Select all	✓					
Alcohol	Select all	✓					
Arts	Select all	✓					
Astrology	Select all	✓					
Auctions	Select all	✓					
Business and Industry	Select all		✓				
Chat and Instant Messaging	Select all	✓					

Image - Access Policy URL Filtering for Unmanaged Devices

Step 6.11. Scroll down on the Uncategorized URLs section choose the proper action.



Image - Access Policy Uncategorized URLs

Tip: For the security perspective it is best to set the action to **Block**, in case any URL needs access, you can add them in the Custom URL Category assigned to the Policy.

Step 6.12. Click **Submit**

Step 7.1. From the GUI, Navigate to **Web Security Manager** and choose **Cisco Data Security**.

Step 7.2. Click **Add Policy**.

Step 7.3. Enter **Name** for the new policy.

Step 7.4. Choose **Select One or More Identification Profiles** from **Identification Profiles and Users** drop down menu.

Step 7.5. Select the **Identification Profile** that was created in **Step 1**.

Step 7.6. Select **All Authenticated Users**..

Step 7.7. Click **Submit**.

Step 7. (Optional) Create Cisco Data Security Policy for Managed Devices

Note: If you do not want to filter the upload traffic for managed devices, you can skip this step.

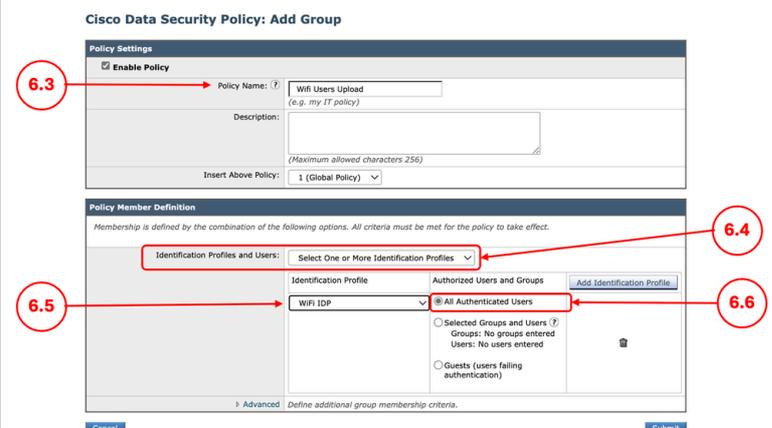


Image - Cisco Data Security Policy for Managed Devices

Step 7.8. In **Cisco Data Security Policies** page, click the link from **URL Filtering** for the new policy.

Step 7.9. (Optional) You can add any Custom URL Category by click on **Select Custom Categories** and choose **Include in Policy** in front of the category names

Step 7.10. Configure the Action for each **Custom and External URL Category Filtering** and **Predefined URL Category Filtering**.

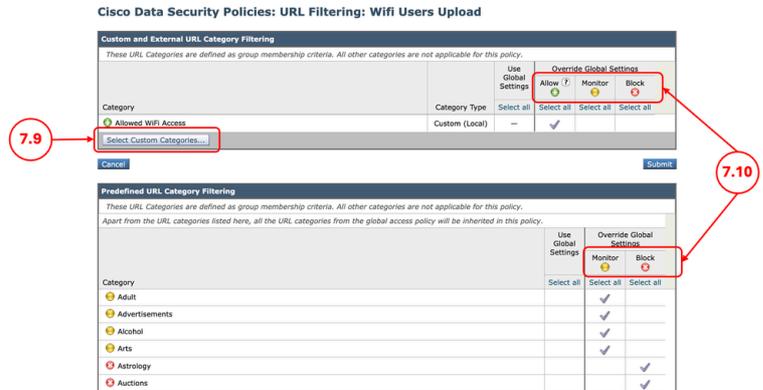


Image - Upload Action for Managed Devices

Step 7.11. Click **Submit**.

Step 8. (Optional) Create Cisco Data Security Policy for Unmanaged Devices

 **Note:** If you do not want to filter the upload traffic for unmanaged devices, you can skip this step.

Step 8.1. From the GUI, Navigate to **Web Security Manager** and choose **Cisco Data Security**.

Step 8.2. Click **Add Policy**.

Step 8.3. Enter **Name** for the new policy.

Step 8.4. Choose **Select One or More Identification Profiles** from **Identification Profiles and Users** drop down menu.

Step 8.5. Select the **Identification Profile** that was created in **Step 1**.

Step 8.6. Select **All Authenticated Users**..

Step 8.7. Click **Submit**.

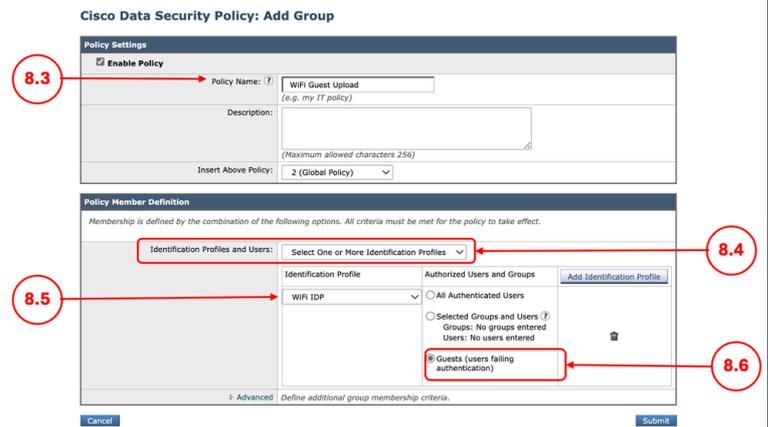


Image - Cisco Data Security Policy for Unmanaged Devices

Step 8.8. In **Cisco Data Security Policies** page, click the link from **URL Filtering** for the new policy.

Step 8.9. (Optional) You can add any Custom URL Category by click on **Select Custom Categories** and choose **Include in Policy** in front of the category names

Step 8.10. Configure the Action for each **Custom and External URL Category Filtering** and **Predefined URL Category Filtering**.

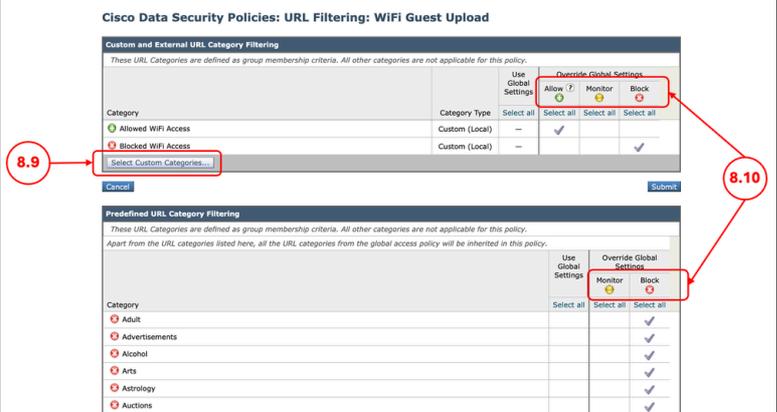


Image - Upload Action for Unmanaged Devices

Step 8.11. Scroll down on the Uncategorized URLs section choose the proper action.



Image - Upload Action for Uncategorized URLs

Tip: For the security perspective it is best to set the action to **Block**, in case any URL needs access, you can add them in the Custom URL Category assigned

	 to the Policy.
	Step 8.12. Click Submit
Step 9. Saving the Changes	Step 9.1. Commit the changes

Related Information

- [User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - LD \(Limited Deployment\) - Troubleshooti...](#)
- [Block Executable File Download in SWA](#)
- [Block Upload Traffic in Secure Web Appliance](#)
- [Block Traffic in Secure Web Appliance](#)
- [Bypass Authentication in Secure Web Appliance](#)
- [Configure Microsoft O365 Tenant Restriction in SWA](#)
- [Configure Secure Web Appliance Initial Setup](#)
- [Bypass Microsoft Updates Traffic in Secure Web Appliance](#)