

Configuración de Secure Web Appliance para permitir el acceso de invitado

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descripción general del escenario](#)

[Configuration Steps](#)

[Paso 1. Crear perfil de identificación.](#)

[Paso 2. \(Opcional\) Crear las categorías de URL personalizadas para las URL permitidas y bloqueadas](#)

[Paso 3. Crear política de descifrado para dispositivos administrados](#)

[Paso 4. Crear política de descifrado para dispositivos no administrados](#)

[Paso 5. Crear política de acceso para dispositivos administrados](#)

[Paso 6. Crear política de acceso para dispositivos no administrados](#)

[Paso 7. \(Opcional\) Crear la política de seguridad de datos de Cisco para dispositivos administrados](#)

[Paso 8. \(Opcional\) Crear la política de seguridad de datos de Cisco para dispositivos no administrados](#)

[Paso 9. Almacenamiento de los cambios](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos para permitir que los usuarios que no han instalado el certificado de descifrado accedan a Internet a través del dispositivo web seguro (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SWA físico o virtual instalado.
- Licencia activada o instalada.
- El asistente de configuración ha finalizado.
- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general del escenario

En este artículo se aborda un escenario de control de acceso a la red dentro de la subred Wi-Fi 10.10.10.0/24. El entorno consta de dos grupos de usuarios distintos que requieren políticas de acceso y seguridad diferentes:

- Dispositivos gestionados: Portátiles de la empresa totalmente autenticados que tienen instalado el certificado de descifrado SWA. Estos dispositivos son de confianza y, por lo general, están sujetos a las políticas de acceso corporativas estándar.
- Dispositivos no administrados/invitados: Portátiles personales y dispositivos móviles no autenticados y que carecen del certificado de descifrado SWA.

Objetivo:
La empresa pretende implementar políticas de acceso web restrictivas para los dispositivos no gestionados, limitando su conectividad a un subconjunto específico de URL permitidas y garantizando al mismo tiempo que los recursos corporativos permanecen seguros.

 **Nota:** Dado que el certificado de descifrado no es de confianza en los dispositivos no administrados, no puede descifrar el tráfico HTTPS y la acción debe configurarse para que pase a través de él.

Configuration Steps

Paso 1. Crear perfil de identificación.	Paso 1.1. Desde la GUI de SWA, navegue hasta Web Security Manager y seleccione Identification Profile. Paso 1.2. Haga clic en Agregar perfil de identificación. Paso 1.3. Defina un nombre para el perfil. Paso 1.4. (Opcional) Defina la descripción. Paso 1.5. Elija Autenticar usuarios en Identificación y autenticación. Paso 1.6. Elija el rango de Active Directory en Seleccione un rango o una secuencia.
--	--

Paso 1.7. En Select a Scheme, seleccione los protocolos de autenticación deseados.



Consejo: No elija Basic Authentication en la lista Select a Scheme.

Paso 1.8. Active la casilla de verificación para Admitir privilegios de invitado.

Paso 1.9. (Opcional) Dependiendo de su diseño, puede habilitar el sustituto, habilitando la opción Aplicar la misma configuración de sustituto a las solicitudes explícitas de reenvío.



Precaución: Dado que no puede descifrar el tráfico, en la implementación transparente no seleccione Persistent Cookie ni Session Cookie.

Paso 1.10. Defina la subred de direcciones IP en, Definir miembros por subred.

Paso 1.11. Envíe y confirme los cambios.

Imagen: definición del perfil de identificación

Paso 2. (Opcional) Crear las categorías de URL personalizadas para las URL permitidas y bloqueadas

Paso 2.1. Desde la GUI vaya a Web Security Manager y elija Categorías de URL externas y personalizadas.

Paso 2.2. Haga clic en Agregar categoría para crear una nueva categoría de URL personalizada.

Paso 2.3.EnterName para la nueva categoría.

Paso 2.4.Defina el dominio y/o los subdominios de los sitios web a los que desea bloquear el acceso.

Paso 2.5.Envíe los cambios.

Paso 2.6. Utilice los mismos pasos para crear una categoría de URL para el sitio web al que está permitiendo el acceso.

The image contains two screenshots of the 'Custom and External URL Categories: Edit Category' form. Both screenshots have red circles with numbers 2.3 and 2.4 pointing to specific fields. In the top screenshot, the 'Category Name' is 'Blocked WiFi Access' and the 'Sites' field contains 'example.com'. In the bottom screenshot, the 'Category Name' is 'Allowed WiFi Access' and the 'Sites' field contains 'cisco.com'. The form includes fields for 'Category Name', 'Comments', 'List Order', 'Category Type', 'Sites', and 'Regular Expressions'. A 'Sort URLs' button is also present in the 'Sites' field area.

Imagen - Definir categoría de URL personalizada

Paso 3. Crear política de descifrado para dispositivos administrados

Paso 3.1. Desde la GUI, vaya aAdministrador de seguridad web y elijaPolíticas de descifrado

Paso 3.2.Haga clic en Agregar directiva.

Paso 3.3.EnterName para la nueva política.

Paso 3.4. Elija Select One or More Identification Profiles del menú desplegable Identification Profiles and Users.

Paso 3.5.Seleccione el perfil de identificación que se creó en el paso 1.

Paso 3.6. Seleccione Todos los usuarios autenticados.

Paso 3.7.Haga clic en Enviar.

Decryption Policy: WiFi Users DP

Policy Settings

☒ **Enable Policy**

Policy Name:

Description:

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy

On Date:

At Time:

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:

Identification Profile:

Authorized Users and Groups: ☒ All Authenticated Users

☐ Selected Groups and Users (7)
Groups: No groups entered
Users: No users entered

☐ Guests (users failing authentication)

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

Crear política de descifrado para dispositivos administrados

Paso 3.8. En la página Políticas de descifrado, haga clic en el enlace de Filtrado de URL para la nueva política.

Paso 3.9. (Opcional) Puede agregar cualquier categoría de URL personalizado haciendo clic en Seleccionar categorías personalizadas y eligiendo Incluir en política delante de los nombres de categoría

Paso 3.10. Configure la Acción para cada Filtrado de Categoría de URL Personalizado y Externo y Filtrado de Categoría de URL Predefinido.

Paso 3.11. Haga clic en Enviar

Decryption Policies: URL Filtering: WiFi Users DP

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					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	☒	☒	☒	☒	☒	☒	☒

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					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Adult	☒	☒	☒	☒	☒	☒	☒
Advertisements	☒	☒	☒	☒	☒	☒	☒
Alcohol	☒	☒	☒	☒	☒	☒	☒
Arts	☒	☒	☒	☒	☒	☒	☒
Astronomy	☒	☒	☒	☒	☒	☒	☒
Auctions	☒	☒	☒	☒	☒	☒	☒
Business and Industry	☒	☒	☒	☒	☒	☒	☒
Chat and Instant Messaging	☒	☒	☒	☒	☒	☒	☒

Imagen - Configurar acción para política de descifrado

Paso 4.1. Desde la GUI, vaya a Administrador de seguridad web y elija Políticas de descifrado

Paso 4.2. Haga clic en Agregar directiva.

Paso 4.3. EnterName para la nueva política.

Paso 4.4. Elija Select One or More Identification Profiles del menú desplegable Identification Profiles and Users.

Paso 4.5. Seleccione el perfil de identificación que se creó en el paso 1.

Paso 4.6. Seleccione Invitados (usuarios sin autenticación).

Paso 4.7. Haga clic en Enviar.

Paso 4. Crear política de descifrado para dispositivos no administrados

Decryption Policy: WiFi Guest DP

Policy Settings

☒ Enable Policy

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

Description:
(Maximum allowed characters 256)

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 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

Crear política de descifrado para dispositivos no administrados

Paso 4.8. En la página Políticas de descifrado, haga clic en el enlace de Filtrado de URL para la nueva política.

Paso 4.9. (Opcional) Puede agregar cualquier categoría de URL personalizado haciendo clic en Seleccionar categorías personalizadas y eligiendo Incluir en política delante de los nombres de categoría

Paso 4.10. Configure la Acción para cada Filtrado de Categoría de URL Personalizado y Externo y Filtrado de Categoría de URL Predefinido.



Nota: No utilice Decrypt como acción, ya que el certificado de descifrado SWA no es de confianza en los dispositivos no administrados.

Decryption Policies: URL Filtering: WiFi Guest DP

Custom and External URL Category Filtering	
Category	Category Type
Allowed WiFi Access	Custom (Local)
Blocked WiFi Access	Custom (Local)

Predefined URL Category Filtering	
Category	Action
Adult	Drop
Advertisements	Drop
Alcohol	Drop
Arts	Drop
Astrology	Drop
Auctions	Drop
Business and Industry	Drop

Imagen - Acción de descifrado para dispositivos no administrados

Paso 4.11. Desplácese hacia abajo en la sección Uncategorized URLs (Direcciones URL no categorizadas) elija la acción adecuada.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs: Drop

Default Action for Update Categories: Most Restrictive

Imagen: URL sin categoría



Consejo: Desde el punto de vista de la seguridad, es mejor establecer la acción en Drop, en caso de que cualquier URL necesite acceso, puede agregarla en la categoría de URL personalizado asignada a la política.

Paso 4.12. Haga clic en Enviar

Paso 5. Crear política de acceso para dispositivos administrados

Paso 5.1. Desde la GUI, vaya a Administrador de seguridad web y elija Políticas de acceso

Paso 5.2. Haga clic en Agregar directiva.

Paso 5.3. EnterName para la nueva política.

Paso 5.4. Elija Select One or More Identification Profiles del menú desplegable Identification Profiles and Users.

Paso 5.7.Haga clic en Enviar.

Imagen - Política de acceso para dispositivos administrados

Paso 5.10. Configure la Acción para cada Filtrado de Categoría de URL Personalizado y Externo y Filtrado de Categoría de URL Predefinido.

[illegible]

Imagen - Filtrado de URL de política de acceso para dispositivos administrados

Paso 5.11. Haga clic en Enviar.

Paso 6.1. Desde la GUI, vaya a Administrador de seguridad web y elija Políticas de acceso

Paso 6.2. Haga clic en Agregar directiva.

Paso 6.3. EnterName para la nueva política.

Paso 6.4. Elija Select One or More Identification Profiles del menú desplegable Identification Profiles and Users.

Paso 6.5. Seleccione el perfil de identificación que se creó en el paso 1.

Paso 6.6. Seleccione Invitados (usuarios sin autenticación).

Paso 6.7. Haga clic en Enviar.

Paso 6. Crear política de acceso para dispositivos no administrados

Imagen - Política de acceso para dispositivos no administrados

Paso 6.8. En la página Access Políticas, haga clic en el enlace de URL Filtering para la nueva política.

Paso 6.9. (Opcional) Puede agregar cualquier categoría de URL personalizado haciendo clic en Seleccionar categorías personalizadas y eligiendo Incluir en política delante de los nombres de categoría

Paso 6.10. Configure la Acción para cada Filtrado de Categoría de URL Personalizado y Externo y Filtrado de Categoría de URL Predefinido.

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	Select all	Select all	Select all	Select all
Blocked WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	Select all	Select all	Select all	Select all
Select Custom Categories...										

6.9

6.10

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	Select all	Select all	Select all	Select all	Select all	
Advertisements	Select all	Select all	Select all	Select all	Select all	Select all	
Alcohol	Select all	Select all	Select all	Select all	Select all	Select all	
Arts	Select all	Select all	Select all	Select all	Select all	Select all	
Astrology	Select all	Select all	Select all	Select all	Select all	Select all	
Auctions	Select all	Select all	Select all	Select all	Select all	Select all	
Business and Industry	Select all	Select all	Select all	Select all	Select all	Select all	
Chat and Instant Messaging	Select all	Select all	Select all	Select all	Select all	Select all	

Imagen - Filtrado de URL de política de acceso para dispositivos no administrados

Paso 6.11. Desplácese hacia abajo en la sección Uncategorized URLs (URL sin categorizar) elija la acción adecuada.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs: **Block**

Default Action for Update Categories: **Most Restrictive**

6.11

Imagen: URL sin categoría de política de acceso

 Consejo: Desde el punto de vista de la seguridad, es mejor establecer la acción en Block (Bloquear). En caso de que cualquier URL necesite acceso, puede agregarla en la categoría de URL personalizado asignada a la política.

Paso 6.12. Haga clic en Enviar

Paso 7. (Opcional) Crear política de seguridad de datos de Cisco para dispositivos administrados

 Nota: Si no desea filtrar el tráfico de carga para los dispositivos administrados, puede omitir este paso.

Paso 7.1. Desde la GUI, vaya a Web Security Manager y elija Cisco Data Security.

Paso 7.2. Haga clic en Agregar directiva.

Paso 7.3. Enter Name para la nueva política.

Paso 7.4. Elija Select One or More Identification Profiles del menú desplegable Identification Profiles and Users.

Paso 7.5. Seleccione el perfil de identificación que se creó en el paso 1.

Paso 7.6. Seleccione Todos los usuarios autenticados.

Paso 7.7. Haga clic en Enviar.

Cisco Data Security Policy: Add Group

Policy Settings

☒ Enable Policy

Policy Name:

Description:

Insert Above Policy:

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:

Identification Profile:

Authorized Users and Groups: ☒ All Authenticated Users

☐ Selected Groups and Users (?)

☐ Groups: No groups entered

☐ Users: No users entered

☐ Guests (users failing authentication)

[Add Identification Profile](#)

[Cancel](#) [Submit](#)

Imagen - Política de seguridad de datos de Cisco para dispositivos administrados

Paso 7.8. En la página Cisco Data Security Policies, haga clic en el enlace de Filtrado de URL para la nueva política.

Paso 7.9. (Opcional) Puede agregar cualquier categoría de URL personalizado haciendo clic en Seleccionar categorías personalizadas y eligiendo Incluir en política delante de los nombres de categoría

Paso 7.10. Configure la Acción para cada Filtrado de Categoría de URL Personalizado y Externo y Filtrado de Categoría de URL Predefinido.

Cisco Data Security Policies: URL Filtering: Wifi Users Upload

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		
			Allow	Monitor	Block
☒ Allowed Wifi Access	Custom (Local)	☒	☒	☐	☐

[Select Custom Categories...](#)

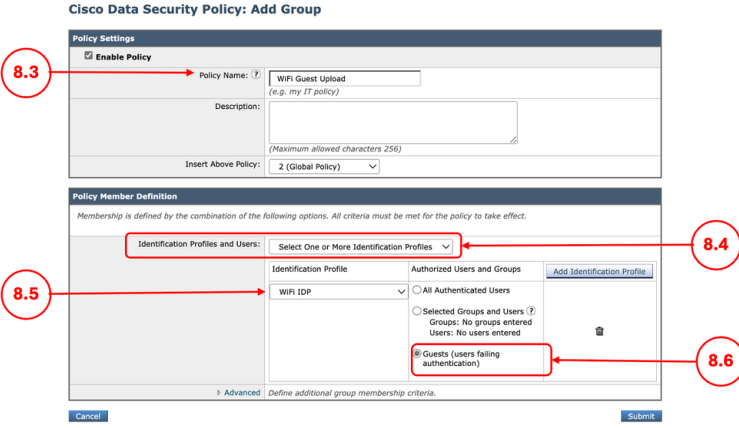
Predefined URL Category Filtering

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	
		Monitor	Block
☒ Adult	☒	☒	☐
☒ Advertisements	☒	☒	☐
☒ Alcohol	☒	☒	☐
☒ Arts	☒	☒	☐
☒ Astrology	☒	☒	☐
☒ Auctions	☒	☒	☐

Imagen: acción de carga para dispositivos administrados

	Paso 7.11. Haga clic en Enviar.
Paso 8. (Opcional) Crear la política de seguridad de datos de Cisco para dispositivos no administrados  Nota: Si no desea filtrar el tráfico de carga para los dispositivos no administrados, puede omitir este paso.	Paso 8.1. Desde la GUI, vaya a Web Security Manager y elija Cisco Data Security. Paso 8.2. Haga clic en Agregar directiva. Paso 8.3. Enter Name para la nueva política. Paso 8.4. Elija Select One or More Identification Profiles del menú desplegable Identification Profiles and Users. Paso 8.5. Seleccione el perfil de identificación que se creó en el paso 1. Paso 8.6. Seleccione Todos los usuarios autenticados. Paso 8.7. Haga clic en Enviar.  Imagen - Política de seguridad de datos de Cisco para dispositivos no administrados Paso 8.8. En la página Cisco Data Security Policies, haga clic en el enlace de Filtrado de URL para la nueva política. Paso 8.9. (Opcional) Puede agregar cualquier categoría de URL personalizado haciendo clic en Seleccionar categorías personalizadas y eligiendo Incluir en política delante de los nombres de categoría Paso 8.10. Configure la Acción para cada Filtrado de Categoría de URL Personalizado y Externo y Filtrado de Categoría de URL Predefinido.

Cisco Data Security Policies: URL Filtering: WiFi Guest Upload

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	Select all	Override Global Settings		
			Use Global Settings	Allow	Monitor
Allowed WiFi Access	Custom (Local)	Select all	☒	☐	☐
Blocked WiFi Access	Custom (Local)	Select all	☐	☒	☒

8.9 8.10

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	Select all	Override Global Settings	
		Monitor	Block
Adult	Select all	☒	☒
Advertisements	Select all	☒	☒
Alcohol	Select all	☒	☒
Arts	Select all	☒	☒
Astrology	Select all	☒	☒
Auctions	Select all	☒	☒

Imagen: acción de carga para dispositivos no administrados

Paso 8.11. Desplácese hacia abajo en la sección Uncategorized URLs (URL sin categorizar) elija la acción adecuada.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs:

Default Action for Update Categories:

8.11

Imagen: acción de carga para URL no categorizadas



Consejo: Desde el punto de vista de la seguridad, es mejor establecer la acción en Block (Bloquear). En caso de que cualquier URL necesite acceso, puede agregarla en la categoría de URL personalizado asignada a la política.

Paso 8.12. Haga clic en Enviar

Paso 9. Almacenamiento de los cambios

Paso 9.1. Realice los cambios

Información Relacionada

- [Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - LD \(implementación limitada\) - Solución de problemas...](#)
- [Bloquear la descarga de archivos ejecutables en SWA](#)
- [Bloquear la carga de tráfico en el dispositivo web seguro](#)
- [Bloqueo del tráfico en el dispositivo web seguro](#)
- [Omitir autenticación en dispositivo web seguro](#)
- [Configurar la restricción de arrendatario de Microsoft O365 en SWA](#)

- [Configuración de la configuración inicial del dispositivo web seguro](#)
- [Omitir tráfico de actualizaciones de Microsoft en dispositivo web seguro](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).