

Configurar la restricción de arrendatario de Microsoft O365 en SWA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Informes y registros](#)

[Registros](#)

[Informes](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de configuración de Configure Microsoft O365 Tenant Restriction in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz gráfica de usuario (GUI) de SWA
- Acceso administrativo al 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.

Configuration Steps

Paso 1. Crear una categoría de URL personalizada para el sitio web.

Paso 1.1. Desde la GUI vaya a Web Security Manager y elija Custom and External URL Categories.

Paso 1.2. Haga clic en Agregar categoría para crear una nueva categoría de URL personalizada.

Paso 1.3. Introduzca Nombre para la nueva categoría.

Paso 1.4. Defina estas URL en la sección Sitios:

login.microsoft.com, login.microsoftonline.com, login.windows.net

Paso 1.5. Envíe los cambios.

Custom and External URL Categories: Edit Category

Category Name: MS Tenant Restrictions (1.3)

Comments: ?

List Order: 1

Category Type: Local Custom Category

Sites: ? (1.4)
login.microsoft.com, login.microsoftonline.com, login.windows.net
Sort URLs
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced Regular Expressions: ?
Enter one regular expression per line. Maximum allowed characters 2048.

Cancel Submit

Imagen - Categoría de URL personalizado



Consejo: Para obtener más información sobre cómo configurar categorías de URL personalizadas, visite: <https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

Paso 2. Descifrar el tráfico.

Paso 2.1. Desde la GUI, navegue hasta Web Security Manager y elija Políticas de descifrado

Paso 2.2. Haga clic en Agregar directiva.

Paso 2.3. Introduzca Name para la nueva política.

Paso 2.4. Seleccione el perfil de identificación al que necesita que se aplique esta política.



Consejo: Si ha omitido las autenticaciones para URL de Microsoft y está configurando esta directiva para todos los usuarios, elija: Todos los perfiles de identificación > Todos los usuarios

Paso 2.5. En la sección Definición de miembro de política, haga clic en los enlaces Categorías de URL para agregar la categoría de URL personalizado.

Paso 2.6. Seleccione la categoría de URL que se creó en el Paso 1.

Paso 2.7. Haga clic en Enviar.

Decryption Policy: DP MS Tenant Restrictions

Imagen - Configurar política de descifrado

Paso 2.8. En la página Políticas de descifrado, haga clic en el enlace de Filtrado de URL para la nueva política.

Decryption Policies

Policies						
Add Policy...						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DP MS Tenant Restrictions Identification Profile: All URL Categories: MS Tenant Restrictions	Decrypt: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 1 Decrypt: 105 Drop: 2	Disabled	Decrypt		
Edit Policy Order...						

Imagen - Editar acción de filtrado de URL

Paso 2.9. Elija Decrypt como la acción para Custom URL Category.

Paso 2.10. Haga clic en Enviar.

Decryption Policies: URL Filtering: DP MS Tenant Restrictions

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					Quota-Based (Unavailable)	Time-Based (Unavailable)
			Pass Through Select all	Monitor Select all	Decrypt Select all	Drop Select all	Drop ? Select all		
MS Tenant Restrictions	Custom (Local)	—			✓			—	—

Cancel Submit

Imagen - Descifrar la categoría de URL personalizado

Paso 3.1. Desde la GUI, navegue hasta Web Security Manager y elija HTTP ReWrite Profiles.

Paso 3.2. Haga clic en Agregar perfil.

Paso 3.3. Introduzca Name para el nuevo perfil.

Paso 3.4. Use Restrict-Access-To-Tenants para el primer Nombre de encabezado.

Paso 3.5. Para la configuración Restrict-Access-To-Tenants, utilice un valor de <lista de arrendatarios permitidos>, que debe ser una lista separada por comas de los arrendatarios a los que los usuarios pueden acceder.

Paso 3.6. Haga clic en Agregar fila

Paso 3.7. Utilice Restrict-Access-Context como segundo nombre de encabezado.

Paso 3.8. Para la configuración Restrict-Access-Context, utilice el valor de un ID de directorio único para especificar el arrendatario que está definiendo las restricciones de arrendatario.

Paso 3.9. Haga clic en Enviar.

Paso 3. Crear perfil de reescritura HTTP.

HTTP ReWrite: Edit Profile

Profile Settings

Profile Name: ? Header Rewrite MS Tenant Restrictions

Header Name	Header Value	Text Format	Binary Encoding	
☐ Restrict-Access-To-Tenants	9.onmicrosoft.com	ASCII	No Encoding	
☐ Restrict-Access-Context	2-9505-4097-a69a-c1553ef	ASCII	No Encoding	

Note:
HTTP header variables available for modification: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups

\$ReqMeta can be used to fetch standard HTTP header variables
Example: If the value of Header is entered as Username-{\$ReqMeta[X-Authenticated-User]} and X-Authenticated-User is joesmith, the final Header Value that gets replaced will be Username-joesmith

\$ReqHeader can be used to access values of the standard HTTP headers or values of the other headers defined under this HTTP Header Re-Write Profile.
Example:
Header1: Value1;
Header2: Value0-{\$ReqHeader(Header1)}-Value2-{\$ReqMeta[X-Authenticated-User]}
If X-Authenticated-User is joesmith and Header1 value is Value1 then the value of Header2 will be Value0-Value1-Value2-joesmith
If value of any header field is empty, that header will be removed from the HTTP header fields and shall not be part of the HTTP header information.

Imagen - Agregar perfil de reescritura HTTP



Consejo: Para obtener más información sobre Restricción de arrendatario y cómo recopilar su información de arrendatario, visite: [Microsoft Learn: restringir el acceso a un arrendatario.](#)

Paso 4. Crear política de acceso.



Consejo: Si ha omitido las Autenticaciones para URL de Microsoft y está configurando esta directiva para Todos los usuarios, elija: Todos los perfiles de identificación > Todos los usuarios.

Paso 4.1. Desde la GUI, navegue hasta Web Security Manager y elija Access Policies

Paso 4.2. Haga clic en Agregar directiva.

Paso 4.3. Introduzca Name para la nueva política.

Paso 4.4. Seleccione el perfil de identificación al que necesita que se aplique esta política.

Paso 4.5. En la sección Definición de miembro de política, haga clic en los enlaces Categorías de URL para agregar la categoría de URL personalizado.

Paso 4.6. Seleccione la categoría de URL que se creó en el Paso 1.

Paso 4.7. Haga clic en Enviar.

Access Policy: AP MS Tenant Restrictions

Policy Settings

☒ **Enable Policy**

Policy Name: (4.3)

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: (4.4)

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

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: None Selected

Proxy Ports: None Selected

Subnets: None Selected

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

URL Categories: MS Tenant Restrictions (4.5)

User Agents: None Selected

Imagen - Crear política de acceso

Paso 4.8. En la página Access Policies, asegúrese de que la acción de URL Filtering está establecida en Monitor.

Paso 4.9. Haga clic en el enlace en HTTP ReWrite Profile para agregar el HTTP Header Profile a esta política.

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP MS Tenant Restrictions Identification Profile: All URL Categories: MS Tenant Restrictions	(global policy)	Monitor: 1 (4.8)	Monitor: 3145	(global policy)	(global policy)	(global policy) (4.9)	Clone	Delete
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 3145	Block: 31 Object Types	Web Reputation: Enabled Secure Endpoint: Enabled Webroot: Disabled	None		

Imagen - Propiedades de directiva de acceso

Paso 4.10. Elija los perfiles de reescritura HTTP, creados en el paso [3].

Access Policies: Edit HTTP ReWrite Profile

Profile Settings

Profiles: ☒ Use Global Settings

(4.10)

Imagen - Agregar perfil de reescritura HTTP

Paso 4.11. Haga clic en Enviar.

Paso 4.12. Registrar cambios.

Informes y registros

Registros

Puede agregar un campo personalizado a los registros de acceso o a los registros de W3C para ver el nombre del perfil de reescritura del encabezado HTTP.

Especificador de formato en registros de acceso	Campo Log (Registro) en Registros W3C	Descripción
%]	x-http-rewrite-profile-name	Nombre del perfil de reescritura del encabezado HTTP.

Informes

Puede generar un informe de seguimiento web para ver los informes del tráfico por el nombre de la directiva de acceso.

Siga estos pasos para generar los informes:

Paso 1. En la GUI, seleccione Reporting y elija Web Tracking.

Paso 2. Elija el rango de tiempo deseado.

Paso 3. Haga clic en el enlace Avanzado para buscar transacciones utilizando criterios avanzados.

Paso 4. En la sección Política, seleccione Filtrar por Política y escriba el nombre de la Política de acceso que se creó anteriormente.

Paso 5. Haga clic en Buscar para revisar el informe.

Web Tracking

Search

Proxy Services | L4 Traffic Monitor | SOCKS Proxy

Available: 06 Nov 2024 13:47 to 17 Jun 2025 20:48 (GMT +02:00)

Time Range: (2)

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type:

☒ Advanced Search transactions using advanced criteria. (3)

URL Category: ☒ Disable Filter
☐ Filter by URL Category:

Application: ☒ Disable Filter
☐ Filter by Application: (ex. Twitter)
☐ Filter by Application Type: (ex. Social Networking)

Policy: ☐ Disable Filter
☒ Filter by Policy: (4)

Imagen: informe de seguimiento web

Información Relacionada

- [Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Guía de instalación de Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco](#)
- [Uso de las prácticas recomendadas de Secure Web Appliance](#)
- [Configuración del firewall para el dispositivo web seguro](#)
- [Configurar certificado de descifrado en dispositivo web seguro](#)
- [Configuración y solución de problemas de SNMP en SWA](#)
- [Configuración de registros de inserción de SCP en un dispositivo web seguro con Microsoft Server](#)
- [Habilitar canal/vídeo específico de YouTube y bloquear el resto de YouTube en SWA](#)
- [Comprensión del formato de registro de acceso HTTPS en el dispositivo web seguro](#)
- [Acceder a registros de appliances web seguros](#)
- [Omitir autenticación en dispositivo web seguro](#)
- [Bloqueo del tráfico en el 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).