

Configurar Restrição de Locatário do Microsoft O365 em SWA

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Relatórios e registros](#)

[Logs](#)

[Relatórios](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o processo de configuração da Restrição de Usuário do Microsoft O365 no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface gráfica do usuário (GUI) do SWA
- Acesso administrativo ao SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuration Steps

Etapa 1. Crie uma Categoria	Etapa 1.1. Na GUI, navegue até Web Security Manager e escolha
-----------------------------	---

de URL Personalizada para o site.

Custom and External URL Categories.

Etapa 1.2. Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada.

Etapa 1.3. Digite Nome para a nova categoria.

Etapa 1.4. Defina esses URLs na seção Sites:

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

Etapa 1.5. Envie as alterações.

Custom and External URL Categories: Edit Category

Category Name: MS Tenant Restrictions

Comments: ?

List Order: 1

Category Type: Local Custom Category

Sites: ? 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

Imagem - Categoria de URL personalizada



Tip: Para obter mais informações sobre como configurar categorias de URL personalizadas, acesse: <https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

Etapa 2. Descriptografe o tráfego.

Etapa 2.1. Na GUI, navegue até o Web Security Manager e escolha Políticas de descriptografia

Etapa 2.2. Clique em Add Policy.

Etapa 2.3. Digite Nome para a nova política.

Etapa 2.4. Selecione o Perfil de identificação ao qual você precisa que essa política se aplique.



Tip: Se você tiver ignorado as Autenticações para URLs da Microsoft e estiver configurando esta política para Todos os usuários, escolha: Todos os perfis de identificação > Todos os usuários

Etapa 2.5. Na seção Definição de membro de política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada.

Etapa 2.6. Selecione a Categoria de URL que foi criada na Etapa 1.

Etapa 2.7. Clique em Submit.

Decryption Policy: DP MS Tenant Restrictions

Policy Settings

☒ **Enable Policy**

Policy Name: 2.3
(e.g. my IT policy)

Description:
(Maximum allowed characters 256)

Insert Above Policy:

1 (Global Policy)

Policy Expires:

☐ Set Expiration for Policy

On Date: 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

2.4

If "All Identification Profiles" 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.

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:

MS Tenant Restrictions

2.5

User Agents:

None Selected

Cancel

Submit

Imagem - Configurar política de descryptografia

Etapa 2.8. Na página Políticas de descryptografia, clique no link de Filtragem de URL para a nova 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...						

Imagem - Editar ação de filtragem de URL

Etapa 2.9. Escolha Descriptografar como a ação para Categoria de URL Personalizada.

Etapa 2.10. Clique em Submit.

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

Cancel Submit

Imagem - Descriptografar a categoria de URL personalizada

Etapa 3.1. Na GUI, navegue até o Web Security Manager e escolha HTTP ReWrite Profiles.

Etapa 3.2. Clique em Add Profile.

Etapa 3.3. Digite Name para o novo perfil.

Etapa 3.4. Use Restrict-Access-To-Tenants para o primeiro Nome do Cabeçalho.

Etapa 3.5. Para a configuração Restrict-Access-To-Tenants, use um valor de <lista de espaços permitidos>, que deve ser uma lista separada por vírgulas dos espaços que os usuários têm permissão para acessar.

Etapa 3.6. Clique em Adicionar linha

Etapa 3.7. Use Restrict-Access-Context como o segundo Header Name.

Etapa 3.8. Para a configuração Restrict-Access-Context, use o valor de um único ID de diretório para especificar o espaço que está definindo as restrições de espaço.

Etapa 3.9. Clique em Submit.

Etapa 3. Criar Perfil de Regravação HTTP.

HTTP ReWrite: Edit Profile

Profile Settings

Profile Name:

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.

Imagem - Adicionar perfil de gravação HTTP



Tip: Para obter mais informações sobre Restrição de Locatário e como coletar suas informações de locatário, acesse: [Microsoft Learn - Restringir o acesso a um espaço.](#)

Etapa 4. Criar Política de Acesso.



Tip: Se tiver ignorado as Autenticações para URLs da Microsoft e estiver configurando esta política para Todos os usuários, escolha: Todos os perfis de identificação > Todos os usuários.

Etapa 4.5. Na seção Definição de membro de política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada.

Etapa 4.6. Selecione a Categoria de URL que foi criada na Etapa 1.

Etapa 4.7. Clique em Submit.

Access Policy: AP MS Tenant Restrictions

Policy Settings

☒ **Enable Policy**

Policy Name: (4.3)
(e.g. my IT policy)

Description:
(Maximum allowed characters 256)

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

Imagem - Criar política de acesso

Etapa 4.8. Na página Access Policies, certifique-se de que a ação da filtragem de URL esteja definida como Monitor.

Etapa 4.9. Clique no link em HTTP ReWrite Profile para adicionar o Perfil do Cabeçalho HTTP 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		

Imagem - Propriedades da política de acesso

Etapa 4.10. Escolha os perfis de regravação HTTP, criados na Etapa [3].

Access Policies: Edit HTTP ReWrite Profile

Profile Settings

Profiles: ☒ Use Global Settings
☐ None
 (4.10)

Imagem - Adicionar perfil de regravação HTTP

Etapa 4.11. Clique em Submit.

Etapa 4.12. Confirmar alterações.

Relatórios e registros

Logs

Você pode adicionar um campo personalizado aos logs de acesso ou aos logs W3C para exibir o nome do perfil de gravação do cabeçalho HTTP.

Especificador de Formato em Logs de Acesso	Campo Log nos Logs W3C	Descrição
%]	x-http-rewrite-profile-name	Nome do perfil de gravação do cabeçalho HTTP.

Relatórios

Você pode gerar o relatório de Rastreamento da Web para exibir os relatórios do tráfego pelo nome da política de acesso.

Siga estas etapas para gerar os relatórios:

Etapas 1. Na GUI, selecione Reporting e escolha Web Tracking.

Etapas 2. Escolha o intervalo de tempo desejado.

Etapas 3. Clique no link Avançado para pesquisar transações usando critérios avançados.

Etapas 4. Na seção Política, selecione Filtrar por política e digite o nome da Política de acesso que foi criada anteriormente.

Etapas 5. Clique em Pesquisar para revisar o relatório.

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 3 Search transactions using advanced criteria.

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

Imagem - Relatório de rastreamento da Web

Informações Relacionadas

- [Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Guia de instalação do Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco](#)
- [Use as práticas recomendadas de dispositivos da Web seguros](#)
- [Configurar firewall para dispositivo seguro da Web](#)
- [Configurar certificado de descryptografia no aplicativo da Web seguro](#)
- [Configurar e solucionar problemas de SNMP em SWA](#)
- [Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server](#)
- [Habilitar canal/vídeo específico do YouTube e bloquear o restante do YouTube no SWA](#)
- [Entender o formato do registro de acesso HTTPS no Secure Web Appliance](#)
- [Acessar logs do dispositivo da Web seguro](#)
- [Ignorar autenticação no Secure Web Appliance](#)
- [Bloquear o tráfego no Secure Web Appliance](#)
- [Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.