

Configurer la restriction du service partagé Microsoft O365 dans SWA

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration Steps](#)

[Rapports et journaux](#)

[Journaux](#)

[Rapports](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus de configuration de la restriction du service partagé Microsoft O365 dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface utilisateur graphique (GUI) de SWA
- Accès administratif au SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration Steps

Étape 1 : création d'une catégorie d'URL personnalisée	Étape 1.1. Dans l'interface graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories.
--	---

pour le site Web

Étape 1.2. Cliquez sur Ajouter une catégorie pour créer une nouvelle catégorie d'URL personnalisée.

Étape 1.3. Saisissez le nom de la nouvelle catégorie.

Étape 1.4. Définissez ces URL dans la section Sites :

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

Étape 1.5. Envoyer les modifications

Custom and External URL Categories: Edit Category

The screenshot shows the 'Edit Custom and External URL Category' interface. It includes the following elements:

- Category Name:** MS Tenant Restrictions (highlighted with a red circle 1.3)
- Comments:** A text area with a help icon.
- List Order:** 1
- Category Type:** Local Custom Category
- Sites:** login.microsoft.com, login.microsoftonline.com, login.windows.net (highlighted with a red circle 1.4). A 'Sort URLs' button is next to it. A note below says: 'Click the Sort URLs button to sort all site URLs in Alpha-numerical order.'
- Regular Expressions:** A text area with a help icon. A note below says: 'Enter one regular expression per line. Maximum allowed characters 2048.'
- Buttons:** Cancel and Submit.

Image - Catégorie d'URL personnalisée



Conseil : Pour plus d'informations sur la configuration des catégories d'URL personnalisées, consultez le site : <https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

Étape 2 : déchiffrement du trafic

Étape 2.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Decryption Policies

Étape 2.2. Cliquez sur Add Policy.

Étape 2.3. Entrez le nom de la nouvelle stratégie.

Étape 2.4. Sélectionnez le profil d'identification auquel s'applique la présente politique.



Conseil : Si vous avez ignoré les authentifications pour les URL Microsoft et que vous configurez cette stratégie pour

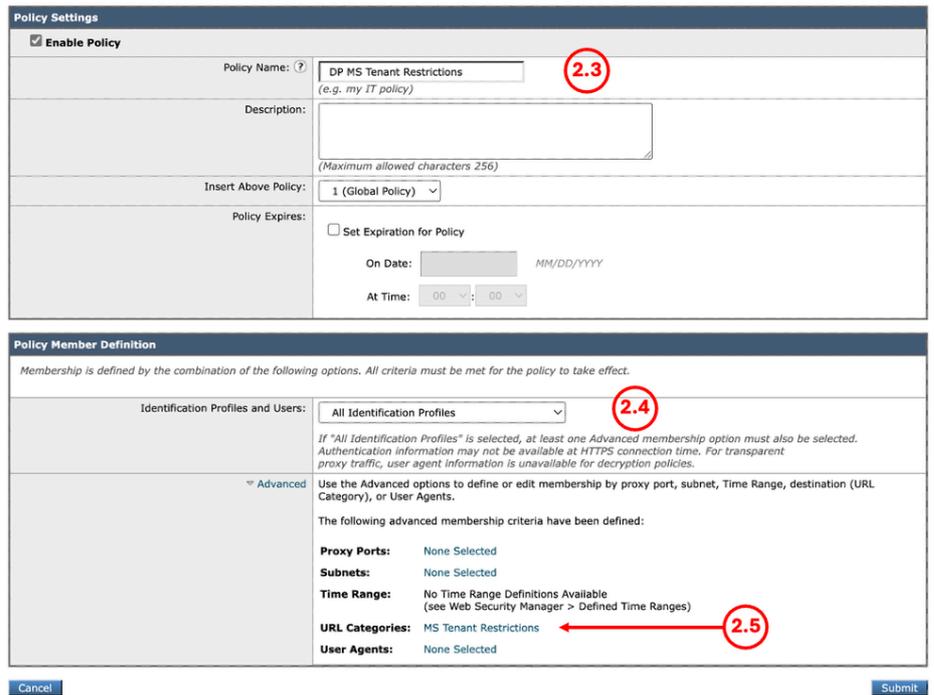
 Tous les utilisateurs, choisissez : Tous les profils d'identification > Tous les utilisateurs

Étape 2.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée.

Étape 2.6. Sélectionnez la catégorie d'URL créée à l'étape 1.

Étape 2.7. Cliquez sur Submit.

Decryption Policy: DP MS Tenant Restrictions



Policy Settings

Enable Policy

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

Description:

(Maximum allowed characters 256)

Insert Above Policy:

Policy Expires: Set Expiration for Policy

On Date: MM/DD/YYYY

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: **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.

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: MS Tenant Restrictions **2.5**

User Agents: None Selected

Image - Configurer la stratégie de déchiffrement

Étape 2.8. Dans la page Stratégies de décodage, cliquez sur le lien du filtrage des URL pour la nouvelle stratégie.

Decryption Policies



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		

Image - Modifier l'action de filtrage URL

Étape 2.9. Choisissez Décrypter comme action pour la catégorie d'URL personnalisée.

Étape 2.10. Cliquez sur 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	Decryption	Drop	Quota-Based	Time-Based	
MS Tenant Restrictions	Custom (Local)	Select all	Select all	Select all	Select all <input checked="" type="checkbox"/>	Select all	(Unavailable)	(Unavailable)

Cancel Submit

Image - Déchiffrer la catégorie d'URL personnalisée

Étape 3.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez HTTP ReWrite Profiles.

Étape 3.2. Cliquez sur Add Profile.

Étape 3.3. Entrez le nom du nouveau profil.

Étape 3.4. Utilisez Restrict-Access-To-Tenants pour le premier nom d'en-tête.

Étape 3.5. Pour le paramètre Restrict-Access-To-Tenants, utilisez la valeur <allowed tenant list>, qui doit être une liste séparée par des virgules des locataires auxquels les utilisateurs sont autorisés à accéder.

Étape 3.6. Cliquez sur Add Row

Étape 3.7. Utilisez Restrict-Access-Context comme deuxième nom d'en-tête.

Étape 3.8. Pour le paramètre Restrict-Access-Context, utilisez la valeur d'un ID de répertoire unique pour spécifier le service partagé qui définit les restrictions du service partagé.

Étape 3.9. Cliquez sur Submit.

HTTP ReWrite: Edit Profile

Profile Settings

Profile Name:

Header Name	Header Value	Text Format	Binary Encoding	
<input type="checkbox"/> Restrict-Access-To-Tenants	<input type="text" value="9.onmicrosoft.com"/>	ASCII	No Encoding	
<input type="checkbox"/> Restrict-Access-Context	<input type="text" value="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.

Cancel Submit

Étape 3 : création du profil de réécriture HTTP

	<p>Image - Ajouter un profil de réécriture HTTP</p> <hr/> <p> Conseil : Pour plus d'informations sur la restriction des locataires et sur la façon de collecter les informations sur les locataires, veuillez consulter : Apprentissage Microsoft - Restreindre l'accès à un service partagé.</p> <hr/>
Étape 4 : création d'une stratégie d'accès	<p>Étape 4.1. À partir de l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Access Policies</p> <p>Étape 4.2. Cliquez sur Add Policy.</p> <p>Étape 4.3. Entrez le nom de la nouvelle stratégie.</p> <p>Étape 4.4. Sélectionnez le profil d'identification auquel s'applique cette stratégie.</p> <hr/> <p> Conseil : Si vous avez ignoré les authentifications pour les URL Microsoft et que vous configurez cette stratégie pour Tous les utilisateurs, choisissez : Tous les profils d'identification > Tous les utilisateurs.</p> <hr/> <p>Étape 4.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée.</p> <p>Étape 4.6. Sélectionnez la catégorie d'URL créée à l'étape 1.</p> <p>Étape 4.7. Cliquez sur Submit.</p>

Access Policy: AP MS Tenant Restrictions

Policy Settings

Enable Policy

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

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:

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: 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:

User Agents: None Selected

Image - Créer une stratégie d'accès

Étape 4.8. Dans la page Access Policies, assurez-vous que l'action du filtrage d'URL est définie sur Monitor.

Étape 4.9. Cliquez sur le lien du profil de réécriture HTTP pour ajouter le profil d'en-tête HTTP à cette stratégie.

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	Monitor: 3145	(global policy)	(global policy)	(global policy)		
	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		

Image - Propriétés de la stratégie d'accès

Étape 4.10. Choisissez les profils HTTP ReWrite, créés à l'étape [3].

Access Policies: Edit HTTP ReWrite Profile

Profile Settings

Profiles: Use Global Settings

None

Header Rewrite MS Tenant Restrictions

Image - Ajouter un profil de réécriture HTTP

Étape 4.11. Cliquez sur Submit.

Étape 4.12. Valider les modifications

Rapports et journaux

Journaux

Vous pouvez ajouter un champ personnalisé aux journaux d'accès ou aux journaux W3C pour afficher le nom du profil de réécriture de l'en-tête HTTP.

Spécificateur de format dans les journaux d'accès	Champ Log dans les journaux W3C	Description
%]	x-http-rewrite-profile-name	Nom du profil de réécriture d'en-tête HTTP.

Rapports

Vous pouvez générer un rapport de suivi Web pour afficher les rapports du trafic en fonction du nom AccessPolicy.

Pour générer les rapports, procédez comme suit :

Étape 1. Dans l'interface utilisateur graphique, sélectionnez Reporting et choisissez Web Tracking.

Étape 2. Choisissez la plage horaire souhaitée.

Étape 3. Cliquez sur le lien Avancé pour rechercher des transactions à l'aide de critères avancés.

Étape 4. Dans la section Stratégie, sélectionnez Filtrer par stratégie et tapez le nom de la stratégie d'accès qui a été créée précédemment.

Étape 5. Cliquez sur Rechercher pour consulter le rapport.

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:	Hour 2
User/Client IPv4 or IPv6: ?	<input type="text"/> (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)
Website:	<input type="text"/> (e.g. google.com)
Transaction Type:	All Transactions ▾
3 ▾ Advanced Search transactions using advanced criteria.	
URL Category:	<input checked="" type="radio"/> Disable Filter <input type="radio"/> Filter by URL Category: <input type="text"/>
Application:	<input checked="" type="radio"/> Disable Filter <input type="radio"/> Filter by Application: <input type="text"/> (ex. Twitter) <input type="radio"/> Filter by Application Type: <input type="text"/> (ex. Social Networking)
Policy:	<input type="radio"/> Disable Filter <input checked="" type="radio"/> Filter by Policy: <input type="text"/> AP MS Tenant Restrictior 4

Image - Rapport de suivi Web

Informations connexes

- [Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance](#)
- [Guide d'installation de l'appliance virtuelle Cisco Secure Email and Web](#)
- [Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco](#)
- [Utilisation des meilleures pratiques de sécurisation des appliances Web](#)
- [Configurer le pare-feu pour l'appliance Web sécurisée](#)
- [Configurer le certificat de déchiffrement dans l'appareil Web sécurisé](#)
- [Configuration et dépannage du protocole SNMP dans SWA](#)
- [Configuration des journaux de transmission SCP dans l'appliance Web sécurisée avec Microsoft Server](#)
- [Activer une chaîne/vidéo YouTube spécifique et bloquer le reste de YouTube dans SWA](#)
- [Comprendre le format de journal d'accès HTTPS dans l'appliance Web sécurisée](#)
- [Accéder aux journaux de l'appliance Web sécurisée](#)
- [Contourner l'authentification dans l'appliance Web sécurisée](#)
- [Bloquer le trafic dans l'appliance Web sécurisée](#)

- [Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.