Configurer la restriction du service partagé Microsoft 365 sur 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 de service partagé Microsoft 365 dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

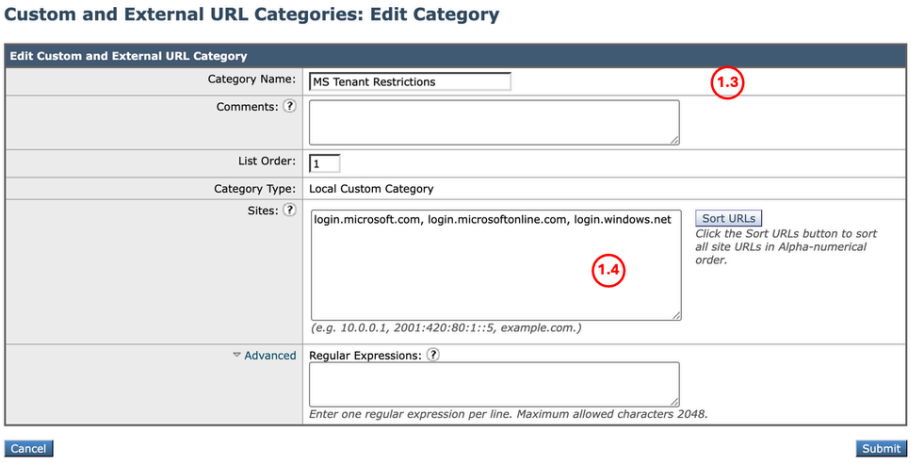
- Privilèges administratifs sur le SWA.
- Connaissance de l'administration SWA.

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. Créer une catégorie d'URL personnalisée pour le site Web	Étape 1.1. Dans l'interface graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories. Étape 1.2. Cliquez sur Add Category pour créer une nouvelle catégorie d'URL personnalisée. Étape 1.3. Entrez 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. Soumettre les modifications  Image - Catégorie d'URL personnalisée Conseil : Pour plus d'informations sur la façon de configurer des catégories d'URL personnalisées, consultez : Configurer des catégories d'URL personnalisées dans l'appareil Web sécurisé
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 stratégie.

Étape 2.4. Sélectionnez le profil d'identification qui doit s'appliquer à cette stratégie.

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.

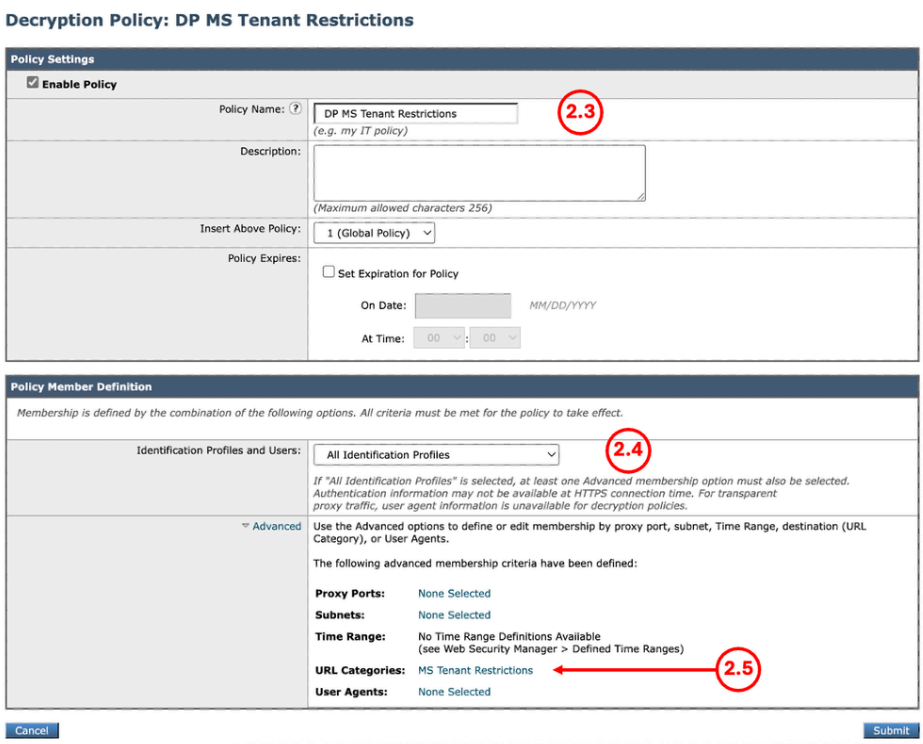


Image - Configurer la stratégie de déchiffrement

Étape 2.8. Dans la page Decryption Policies, cliquez sur le lien du filtrage d'URL qui a été créé à l'étape 1.

<table>
<tr>
<td></td>
<td>
Decryption Policies
Policies
Add Policy...
<table>
<tr><th>Order</th><th>Group</th><th>URL Filtering</th><th>Web Reputation</th><th>Default Action</th><th>Clone Policy</th><th>Delete</th></tr>
<tr><td>1</td><td>DP MS Tenant Restrictions
Identification Profile: All
URL Categories: MS Tenant Restrictions</td><td>Decrypt: 1</td><td>(global policy)</td><td>(global policy)</td><td></td><td></td></tr>
<tr><td></td><td>Global Policy
Identification Profile: All</td><td>Monitor: 1
Decrypt: 105
Drop: 2</td><td>Disabled</td><td>Decrypt</td><td></td><td></td></tr>
</table>
Edit Policy Order...
Image - Modifier l'action de filtrage URL

Étape 2.9. Choisissez Decrypt comme action pour Custom URL Category.

Étape 2.10. Cliquez sur Envoyer.

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.
<table>
<tr><th></th><th></th><th>Use Global Settings</th><th colspan="6">Override Global Settings</th></tr>
<tr><th></th><th></th><th></th><th>Pass Through</th><th>Monitor</th><th>Decrypt</th><th>Drop</th><th>Quota-Based</th><th>Time-Based</th></tr>
<tr><th>Category</th><th>Category Type</th><th>Select all</th><th>Select all</th><th>Select all</th><th>Select all</th><th>Select all</th><th>(Unavailable)</th><th>(Unavailable)</th></tr>
<tr><td>MS Tenant Restrictions</td><td>Custom (Local)</td><td>–</td><td></td><td></td><td>✓</td><td></td><td>–</td><td>–</td></tr>
</table>
Cancel Submit
Image - Déchiffrer la catégorie d'URL personnalisée
</td>
</tr>
<tr>
<td>Étape 3 : création d'un profil de réécriture HTTP</td>
<td>
Étape 3.1. Dans l’interface 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.
</td>
</tr>
</table>

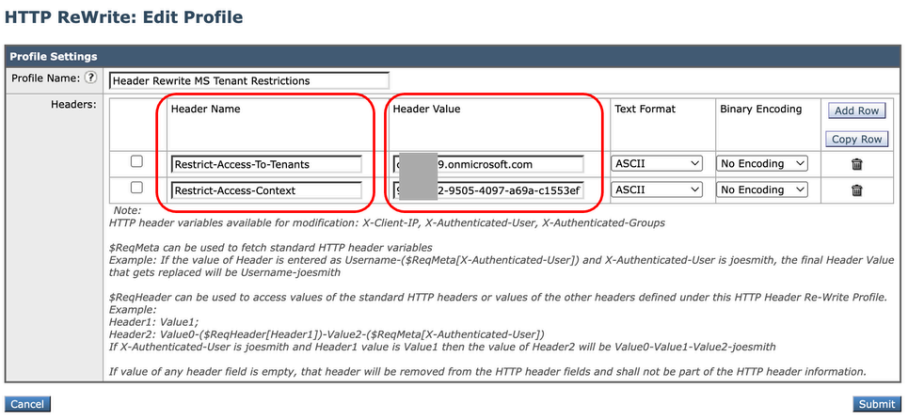
<table>
<tr>
<td></td>
<td>


Image - Ajouter un profil de réécriture HTTP

Conseil : Pour plus d'informations sur la restriction des locataires et sur la façon de collecter vos informations de locataire, consultez : Apprentissage Microsoft - Restreindre l'accès à un locataire
</td>
</tr>
<tr>
<td>Étape 4 : création d’une stratégie d’accès</td>
<td>
Étape 4.1. À partir de l’interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Access Policies.

Étape 4.2. Cliquez sur Add Policy.

Étape 4.3. Entrez le nom de la stratégie.

Étape 4.4. Sélectionnez le profil d'identification qui doit s'appliquer à cette stratégie.

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

Étape 4.6. Sélectionnez la catégorie d'URL créée à l'étape 1.

Étape 4.7. Cliquez sur Submit.
</td>
</tr>
</table>

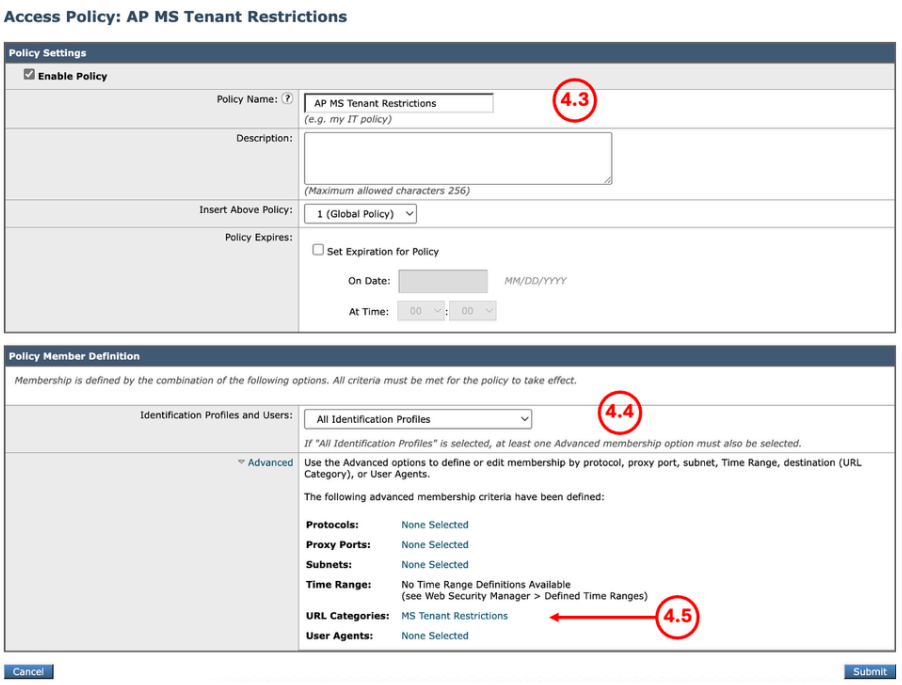


Image - Créer une stratégie d'accès

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 dans Profil de réécriture HTTP pour ajouter le profil d'en-tête HTTP à cette stratégie.

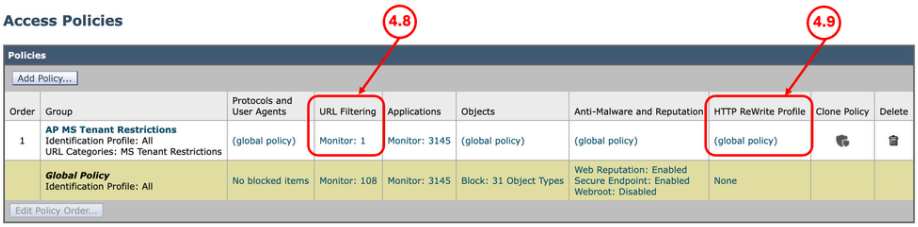


Image - Propriétés de la stratégie d'accès

Étape 4.10. Choisissez les profils de réécriture HTTP, créés à l'étape 3.

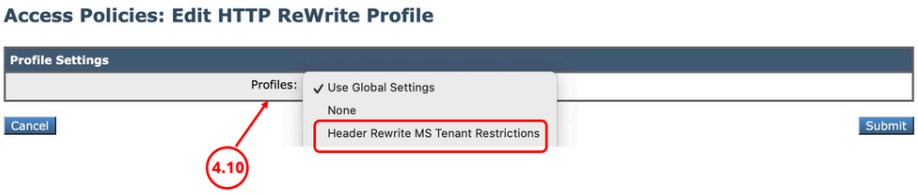


Image - Ajouter un profil de réécriture HTTP

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 de la stratégie d'accès.

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.

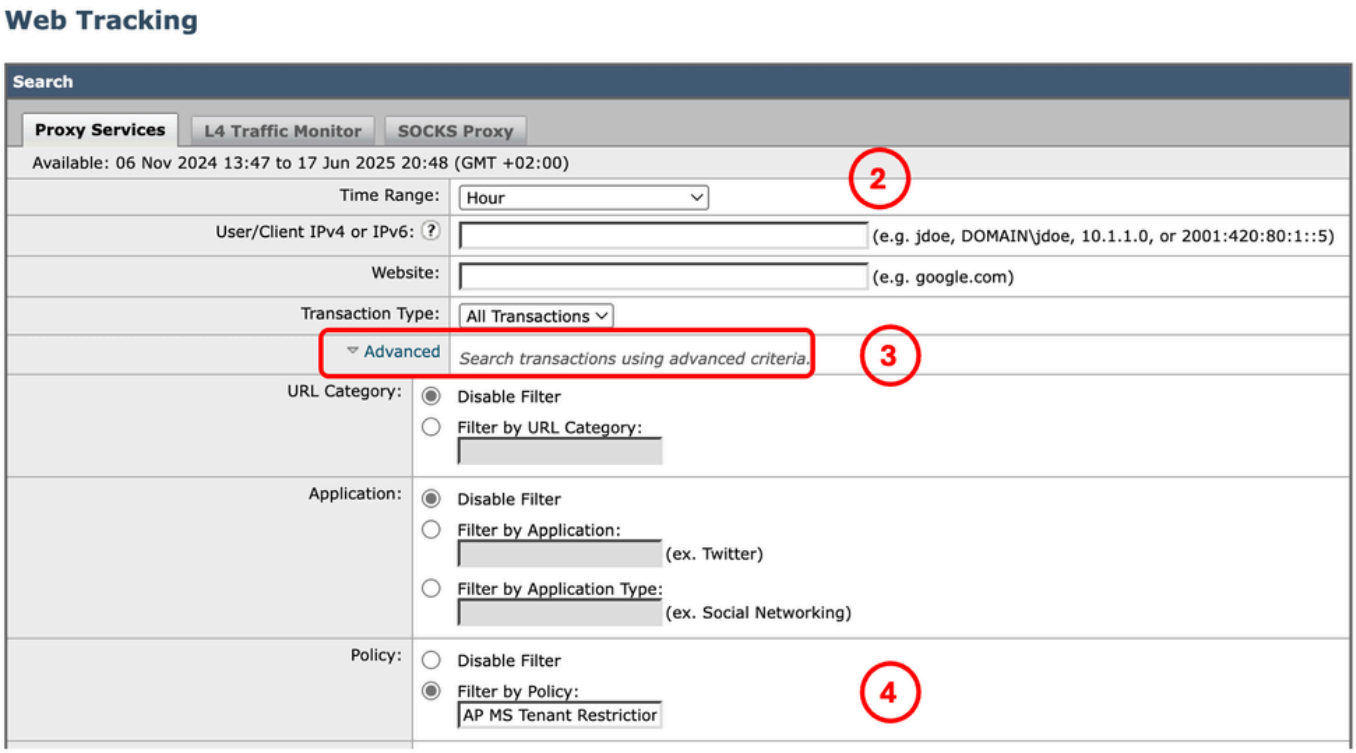


Image - Rapport de suivi Web

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.