Configurer la restriction du service partagé Microsoft O365 dans SWA

Table des matières

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.

<table>
<tr>
<td>pour le site Web</td>
<td>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 :

<code>login.microsoft.com, login.microsoftonline.com, login.windows.net</code>

Étape 1.5.Envoyer les modifications

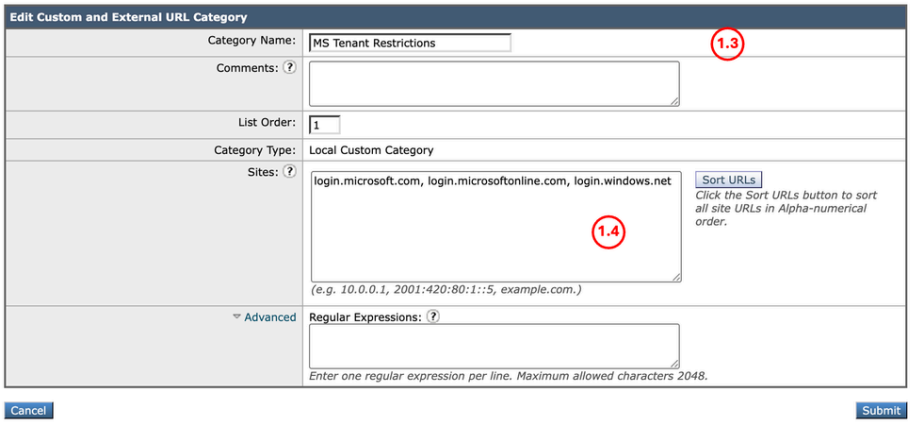
Custom and External URL Categories: Edit Category
 

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</td>
</tr>
<tr>
<td>Étape 2 : déchiffrement du trafic</td>
<td>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</td>
</tr>
</table>

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.

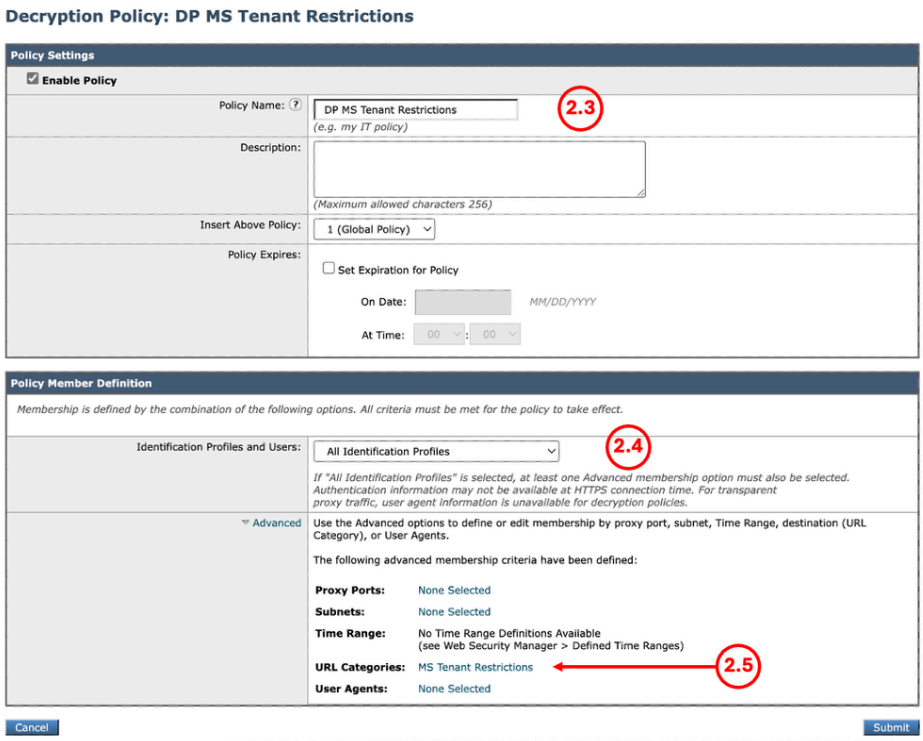


Image - Configurer la stratégie de déchiffrement

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

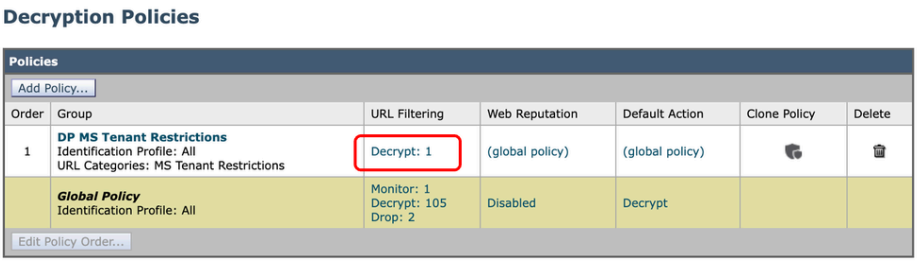


Image - Modifier l'action de filtrage URL

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.* Override Global Settings Category | Category Type | Use Global Settings | Pass Through | Monitor | Decrypt | Drop | Quota-Based | Time-Based Select all | Select all | Select all | Select all | (Unavailable) | (Unavailable) MS Tenant Restrictions | Custom (Local) | – | | | ✓ | | – | – Cancel | Submit Image - Déchiffrer la catégorie d'URL personnalisée
Étape 3 : création du profil de réécriture HTTP	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 Rewrite MS Tenant Restrictions Headers: Header Name | Header Value | Text Format | Binary Encoding | Add Row | Copy Row Restrict-Access-To-Tenants | [redacted]9.onmicrosoft.com | ASCII | No Encoding Restrict-Access-Context | [redacted]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

	Image - Ajouter un profil de réécriture HTTP 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.
Étape 4 : création d'une stratégie d'accès	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 nouvelle stratégie. Étape 4.4. Sélectionnez le profil d'identification auquel s'applique 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.

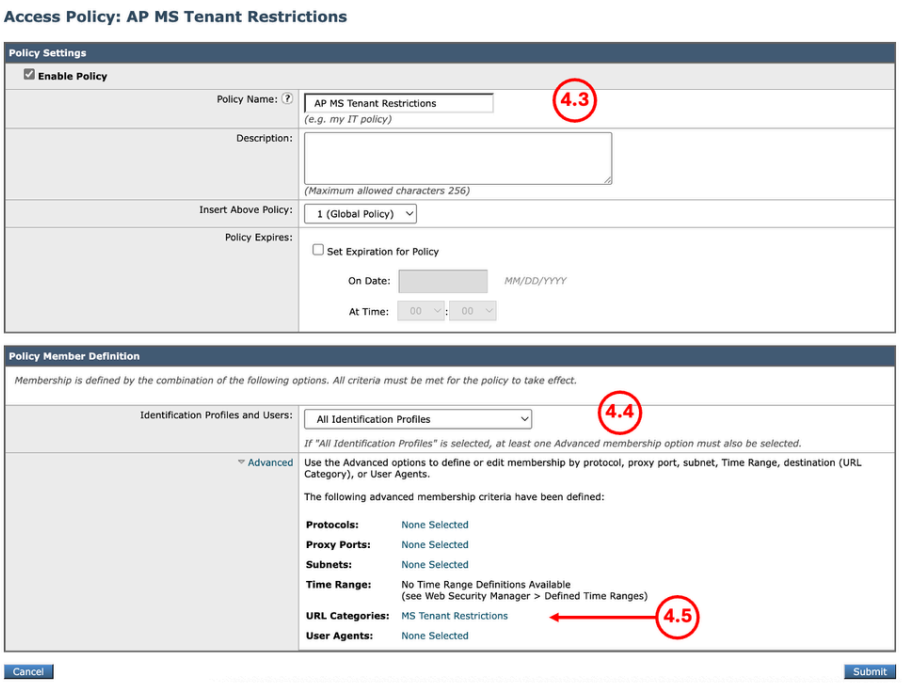


Image - Créer une stratégie d'accès

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.

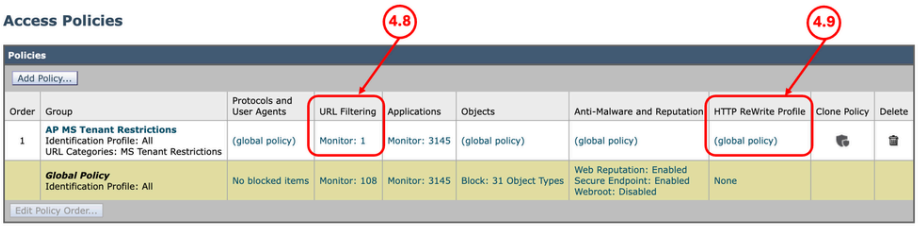


Image - Propriétés de la stratégie d'accès

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

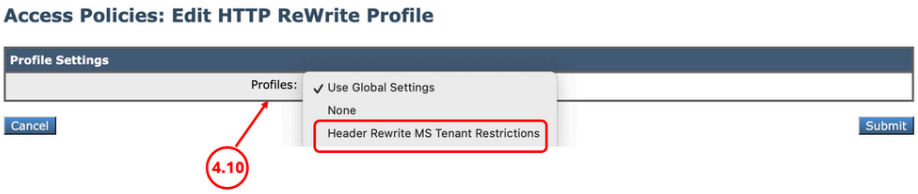


Image - Ajouter un profil de réécriture HTTP

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 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.

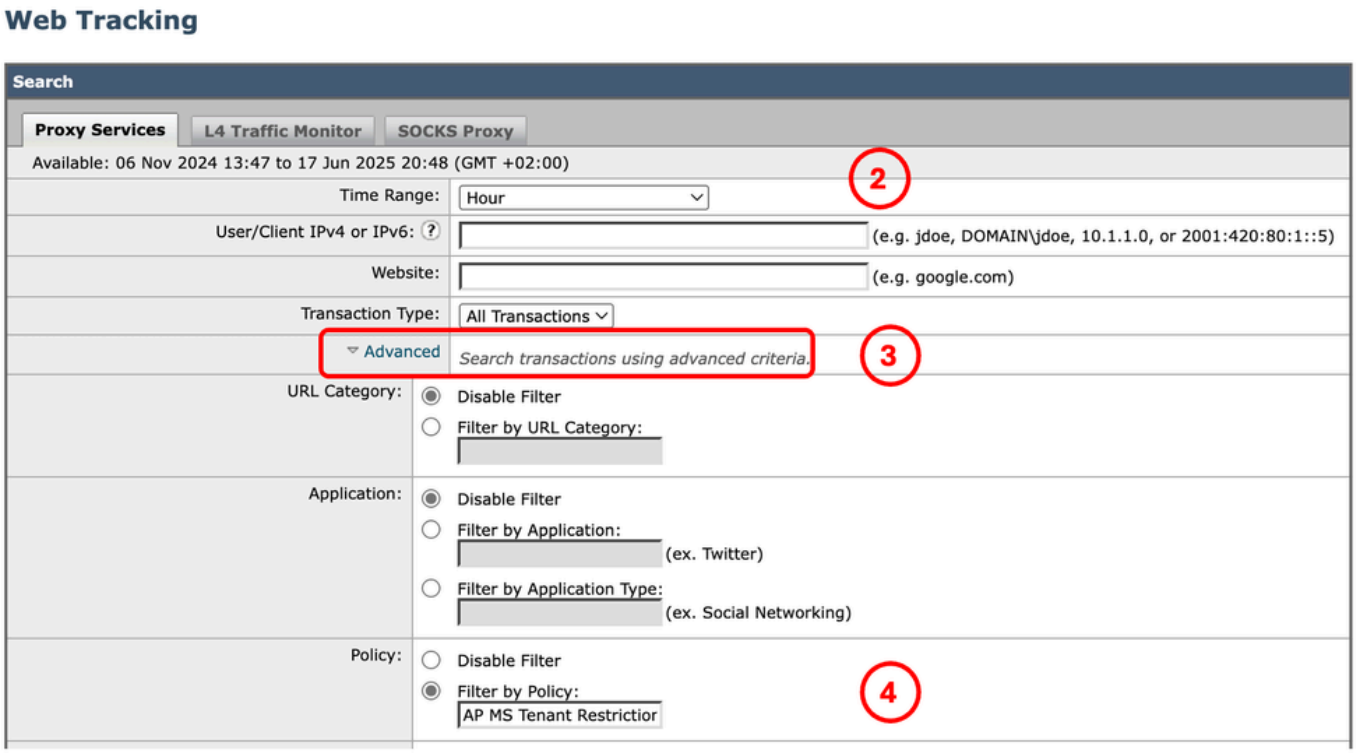


Image - Rapport de suivi Web

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.