Konfiguration der Microsoft O365 Tenant-Einschränkung in SWA

Inhalt

Einleitung

In diesem Dokument wird der Konfigurationsvorgang zur Konfiguration der Microsoft O365-Tenant-Einschränkung in einer sicheren Web-Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administratorzugriff auf die SWA.

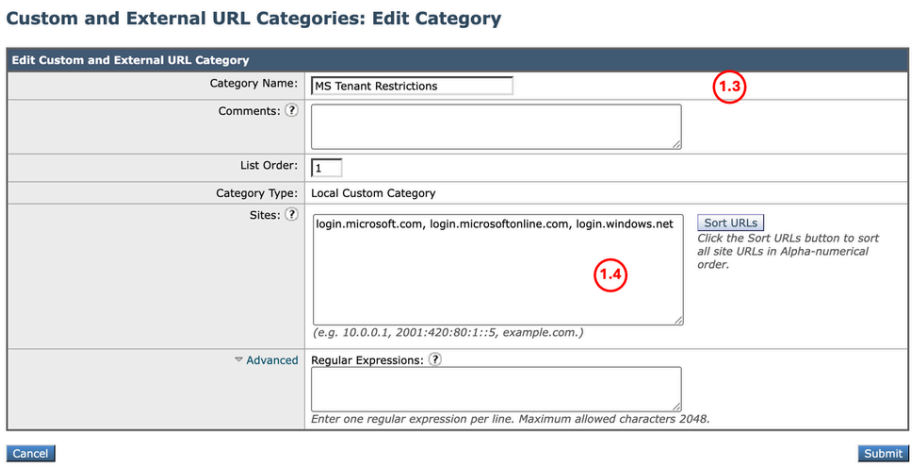
Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurationsschritte

Schritt 1: Erstellen einer	Schritt 1.1. Navigieren Sie in der GUI zu Web Security Manager,

benutzerdefinierten URL-Kategorie für die Website	und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus. Schritt 1.2: Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen. Schritt 1.3: Geben Sie den Namen für die neue Kategorie ein. Schritt 1.4. Definieren Sie diese URLs im Abschnitt Sites: `login.microsoft.com, login.microsoftonline.com, login.windows.net` Schritt 1.5.Senden Sie die Änderungen.  Bild - Benutzerdefinierte URL-Kategorie Tipp: Weitere Informationen zum Konfigurieren benutzerdefinierter URL-Kategorien finden Sie unter: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
Schritt 2: Entschlüsseln des Datenverkehrs	Schritt 2.1. Navigieren Sie in der GUI zum Web Security Manager, und wählen Sie Entschlüsselungsrichtlinien aus. Schritt 2.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 2.3: Geben Sie den Namen für die neue Richtlinie ein. Schritt 2.4. Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll.

Tipp: Wenn Sie die Authentifizierungen für Microsoft-URLs umgangen haben und diese Richtlinie für alle Benutzer konfigurieren, wählen Sie: Alle Identifizierungsprofile > Alle Benutzer

Schritt 2.5. Klicken Sie im Abschnitt Definition der Richtlinienmitglieder auf URL-Kategorien-Links, um die benutzerdefinierte URL-Kategorie hinzuzufügen.

Schritt 2.6. Wählen Sie die URL-Kategorie aus, die in Schritt 1 erstellt wurde.

Schritt 2.7: Klicken Sie auf Senden.

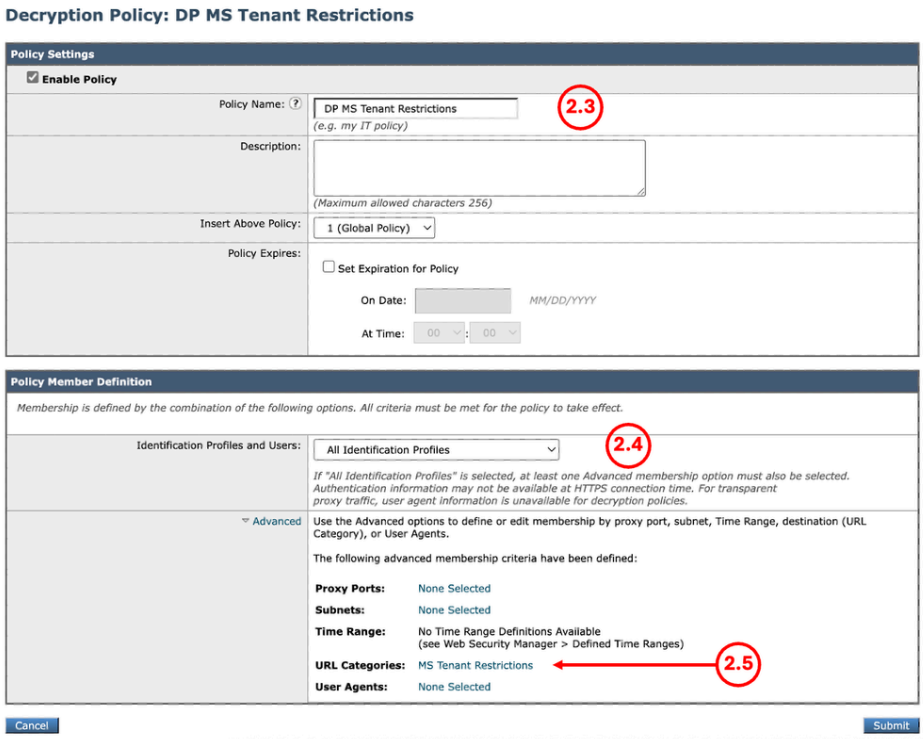
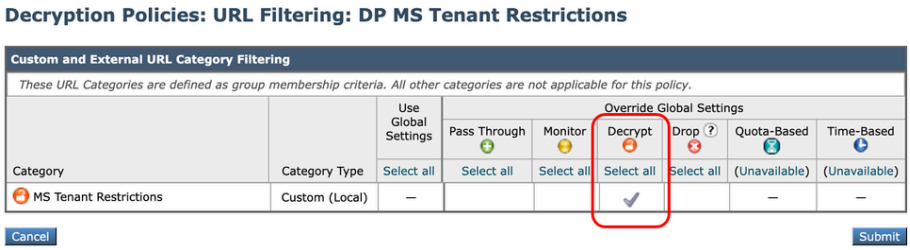


Image: Konfigurieren der Entschlüsselungsrichtlinie

Schritt 2.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung für die neue Richtlinie.

Bild - URL-Filterungsaktion bearbeiten

	Schritt 2.9. Wählen Sie Entschlüsseln als Aktion für die benutzerdefinierte URL-Kategorie aus. Schritt 2.10. Klicken Sie auf Senden.  Bild: Entschlüsseln der benutzerdefinierten URL-Kategorie
Schritt 3: Erstellen eines HTTP-Umschreibprofils	Schritt 3.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie HTTP ReWrite Profiles. Schritt 3.2: Klicken Sie auf Profil hinzufügen. Schritt 3.3: Geben Sie den Namen für das neue Profil ein. Schritt 3.4: Verwenden Sie Restrict-Access-To-Tenants als ersten Header-Namen. Schritt 3.5. Verwenden Sie für die Einstellung Restrict-Access-To-Tenants den Wert <Liste der zulässigen Tenants>. Dabei muss es sich um eine kommagetrennte Liste der Tenants handeln, auf die Benutzer zugreifen dürfen. Schritt 3.6: Klicken Sie auf Zeile hinzufügen Schritt 3.7: Verwenden Sie Restrict-Access-Context als zweiten Header-Namen. Schritt 3.8. Verwenden Sie für die Einstellung Restrict-Access-Context (Zugriffs-Kontext beschränken) den Wert einer einzelnen Verzeichnis-ID, um den Tenant anzugeben, der die Tenant-Einschränkungen definiert. Schritt 3.9: Klicken Sie auf Senden.

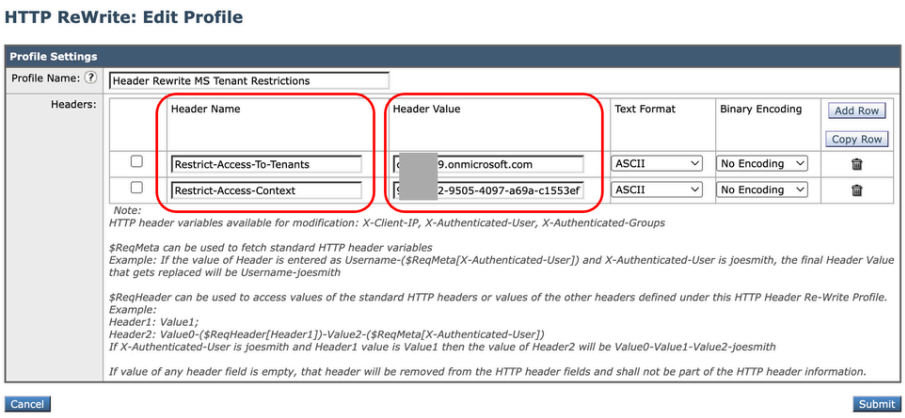
<table>
<tr>
<td></td>
<td>


Bild - HTTP ReWrite-Profil hinzufügen

Tipp: Weitere Informationen zur Mieterbeschränkung und zum Sammeln Ihrer Mieterinformationen finden Sie unter: Microsoft Learn - Beschränken Sie den Zugriff auf einen Tenant.
</td>
</tr>
<tr>
<td>Schritt 4: Erstellen einer Zugriffsrichtlinie</td>
<td>
Schritt 4.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Zugriffsrichtlinien aus.

Schritt 4.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 4.3: Geben Sie den Namen für die neue Richtlinie ein.

Schritt 4.4: Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll.

Tipp: Wenn Sie die Authentifizierungen für Microsoft-URLs umgangen haben und diese Richtlinie für alle Benutzer konfigurieren, wählen Sie: Alle Identifizierungsprofile > Alle Benutzer.

Schritt 4.5: Klicken Sie im Abschnitt Definition der Richtlinienmitglieder auf URL-Kategorien-Links, um die benutzerdefinierte URL-Kategorie hinzuzufügen.

Schritt 4.6: Wählen Sie die URL-Kategorie aus, die in Schritt 1 erstellt wurde.

Schritt 4.7: Klicken Sie auf Senden.
</td>
</tr>
</table>

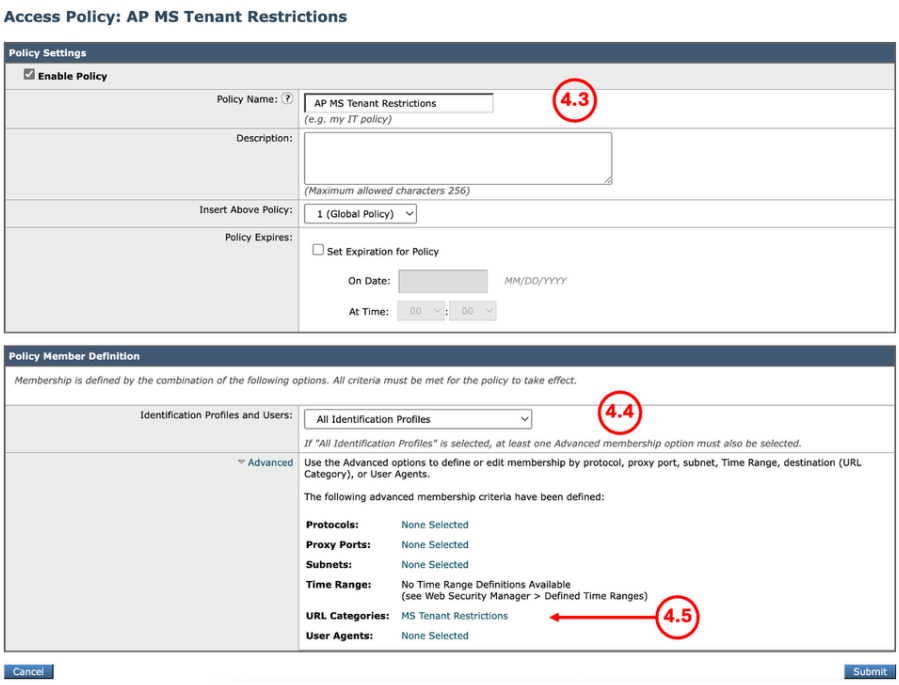


Bild: Erstellen einer Zugriffsrichtlinie

Schritt 4.8. Stellen Sie auf der Seite Access Policies (Zugriffsrichtlinien) sicher, dass die Aktion der URL-Filterung auf Monitor (Überwachen) festgelegt ist.

Schritt 4.9: Klicken Sie auf den Link im HTTP ReWrite Profile, um dieser Richtlinie das HTTP-Header-Profil hinzuzufügen.

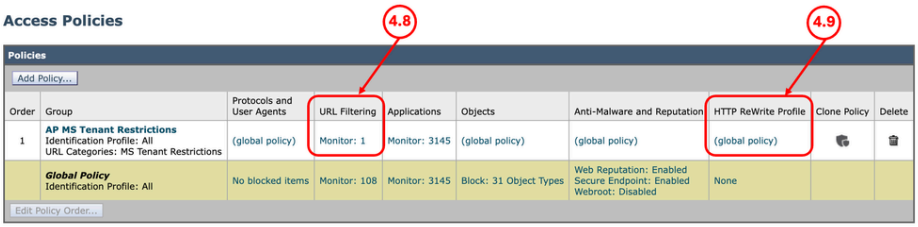


Bild - Eigenschaften der Zugriffsrichtlinie

Schritt 4.10. Wählen Sie die HTTP ReWrite Profiles, die in Schritt [3] erstellt wurden.

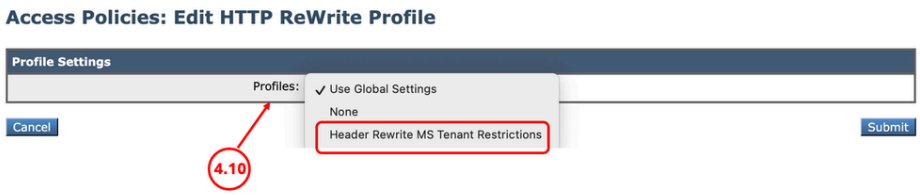


Bild - HTTP ReWrite-Profil hinzufügen

Schritt 4.11: Klicken Sie auf Senden.

Schritt 4.12: Änderungen bestätigen.

Berichte und Protokolle

Protokolle

Sie können den Zugriffsprotokollen oder den W3C-Protokollen ein benutzerdefiniertes Feld hinzufügen, um den Namen des HTTP-Header-Umschreibprofils anzuzeigen.

Formatangabe in Zugriffsprotokollen	Protokollfeld in W3C-Protokollen	Beschreibung
%]	x-http-rewrite-profilname	Profilname für HTTP-Header umschreiben.

Berichterstellung

Sie können einen Web Tracking-Bericht generieren, um die Berichte des Datenverkehrs nach dem Namen AccessPolicy anzuzeigen.

Gehen Sie folgendermaßen vor, um Berichte zu erstellen:

Schritt 1. Wählen Sie in der GUI Reporting aus, und wählen Sie Web Tracking.

Schritt 2. Wählen Sie den gewünschten Zeitraum.

Schritt 3: Klicken Sie auf den Link Erweitert, um Transaktionen nach erweiterten Kriterien zu suchen.

Schritt 4. Wählen Sie im Abschnitt Policy (Richtlinie) die Option Filter by Policy (Nach Richtlinie filtern) aus, und geben Sie den Namen der Zugriffsrichtlinie ein, die zuvor erstellt wurde.

Schritt 5: Klicken Sie auf Suchen, um den Bericht zu überprüfen.

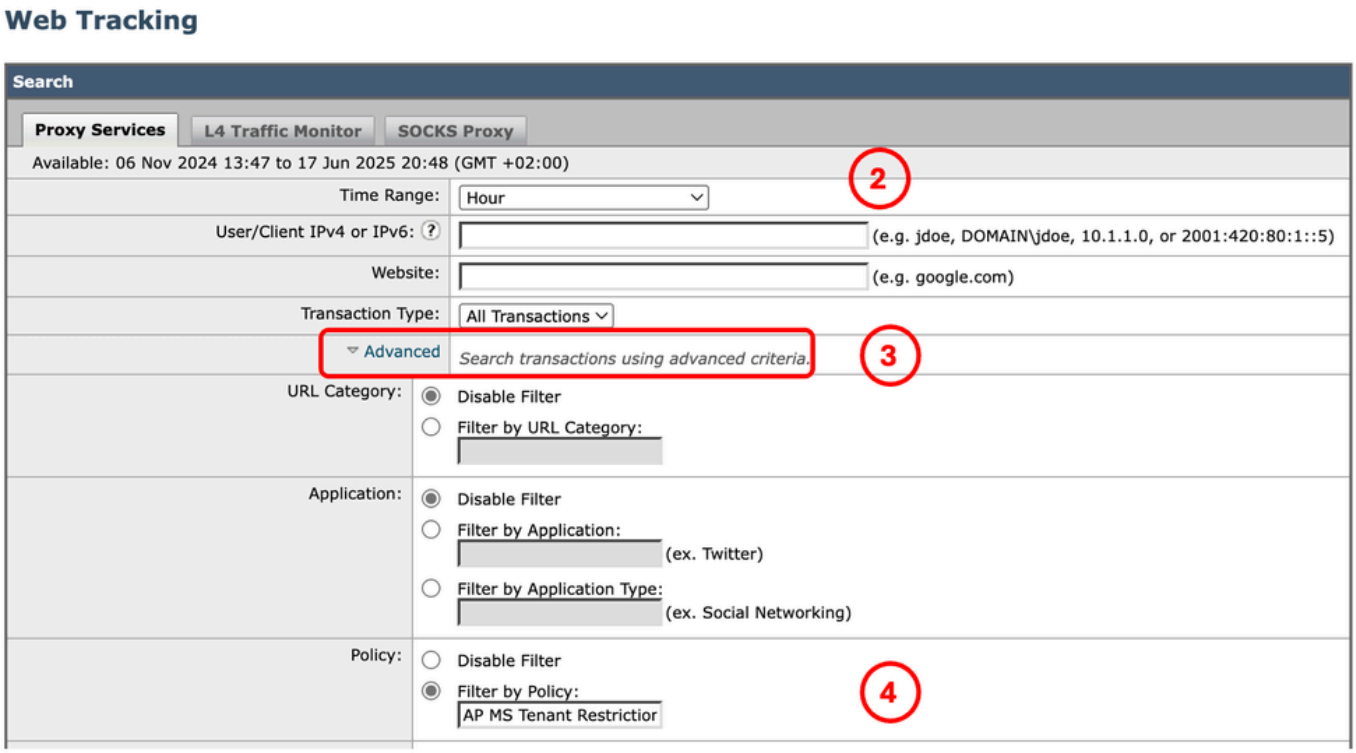


Bild - Web-Tracking-Bericht

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance
- Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance
- Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco
- Best Practices für sichere Web-Appliances
- Firewall für sichere Web-Appliance konfigurieren
- Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren
- SNMP in SWA konfigurieren und Fehlerbehebung dafür durchführen
- Konfigurieren von SCP-Push-Protokollen in der sicheren Web-Appliance mit Microsoft Server
- Aktivierung bestimmter YouTube-Kanäle/Videos und Blockierung sonstiger YouTube-Inhalte in SWA
- HTTPS-Zugriffsformat in sicherer Web-Appliance
- Zugreifen auf Protokolle der sicheren Web-Appliance
- Umgehen der Authentifizierung in einer sicheren Web-Appliance
- Blockieren von Datenverkehr in einer sicheren Web-Appliance

- Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.