

Konfiguration der Microsoft O365 Tenant-Einschränkung in SWA

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte](#)

[Berichte und Protokolle](#)

[Protokolle](#)

[Berichterstellung](#)

[Zugehörige Informationen](#)

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.

Custom and External URL Categories: Edit Category

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.

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:

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: Konfigurieren der Entschlüsselungsrichtlinie

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

Decryption Policies

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		

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.

Decryption Policies: URL Filtering: DP MS Tenant Restrictions

Custom and External URL Category Filtering								
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>								
Category	Category Type	Use Global Settings	Override Global Settings					
		Select all	Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
MS Tenant Restrictions	Custom (Local)	—	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Buttons: Cancel, Submit

Bild: Entschlüsseln der benutzerdefinierten URL-Kategorie

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 kommasetrennte 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.

Schritt 3: Erstellen eines HTTP-Umschreibprofils

HTTP ReWrite: Edit Profile

Profile Settings

Profile Name: ?

Headers:	Header Name	Header Value	Text Format	Binary Encoding	
<input type="checkbox"/>	<input type="text" value="Restrict-Access-To-Tenants"/>	<input type="text" value="9.onmicrosoft.com"/>	ASCII	No Encoding	<input type="button" value="Add Row"/>
<input type="checkbox"/>	<input type="text" value="Restrict-Access-Context"/>	<input type="text" value="2-9505-4097-a69a-c1553ef"/>	ASCII	No Encoding	<input type="button" value="Copy Row"/>

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.

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.](#)

Schritt 4: Erstellen einer Zugriffsrichtlinie



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

- Schritt 4.1. 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.
- 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.

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

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.

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)	<input type="button" value="Clone"/>	<input type="button" value="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		

Bild - Eigenschaften der Zugriffsrichtlinie

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

Access Policies: Edit HTTP ReWrite Profile

Profile Settings

Profiles:

(4.10)

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.

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 Restrictor 4

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.