Configura restrizione tenant Microsoft O365 in SWA

Sommario

Introduzione

In questo documento viene descritto il processo di configurazione della limitazione del tenant Microsoft O365 in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'SWA.

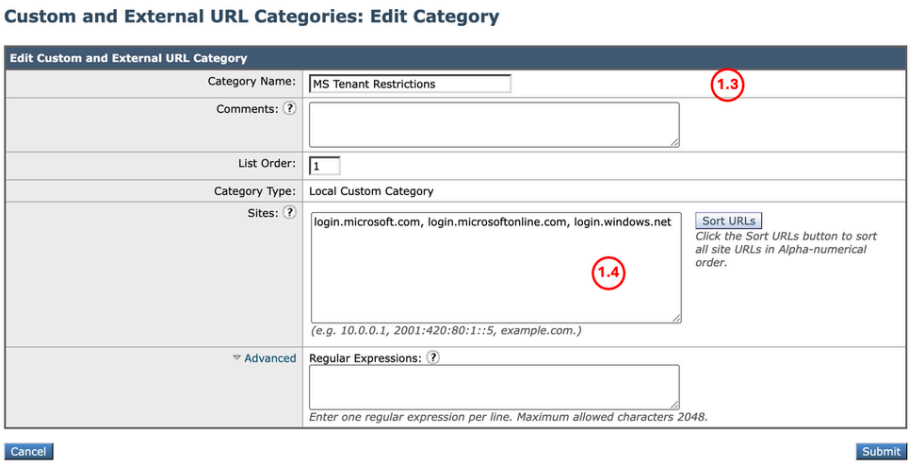
Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura di configurazione

Passaggio 1. Creare una	Passaggio 1.1. Dalla GUI, passare a Web Security Manager e

categoria URL personalizzata per il sito Web.	scegliere Categorie URL personalizzate ed esterne. Passaggio 1.2. Fare clic su Add Category per creare una nuova categoria di URL personalizzati. Passaggio 1.3. Inserire il nome della nuova categoria. Passaggio 1.4. Definire gli URL nella sezione Siti: `login.microsoft.com, login.microsoftonline.com, login.windows.net` Passaggio 1.5.Sottomettere le modifiche.  Immagine - Categoria URL personalizzato Suggerimento: Per ulteriori informazioni su come configurare le categorie URL personalizzate, visitare: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
Passaggio 2. Decriptare il traffico.	Passaggio 2.1. Dalla GUI, passare a Web Security Manager e scegliere Decryption Policies (Criteri di decrittografia) Passaggio 2.2. Fare clic su Aggiungi criterio. Passaggio 2.3. Immettere il nome del nuovo criterio. Passaggio 2.4. Selezionare il profilo di identificazione a cui applicare il criterio.

Suggerimento: Se le autenticazioni per gli URL Microsoft sono state ignorate e si sta configurando questo criterio per Tutti gli utenti, scegliere: Tutti i profili di identificazione > Tutti gli utenti

Passaggio 2.5. Dalla sezione Definizione membri dei criteri, fare clic sui collegamenti Categorie URL per aggiungere la categoria URL personalizzata.

Passaggio 2.6. Selezionare la categoria dell'URL creata nel Passaggio 1.

Passaggio 2.7. Fare clic su Sottometti.

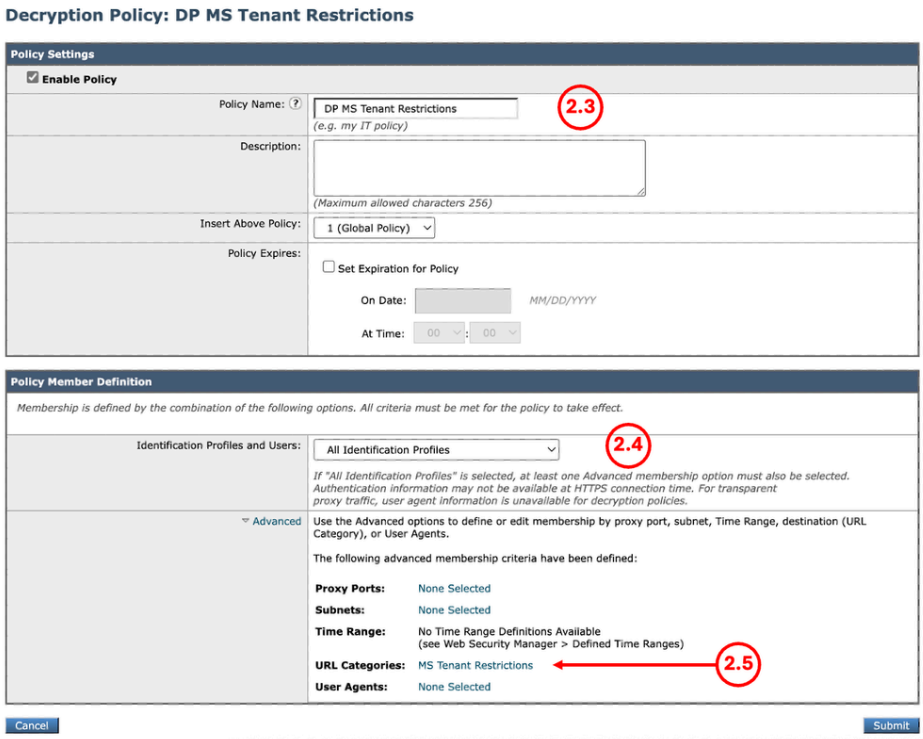
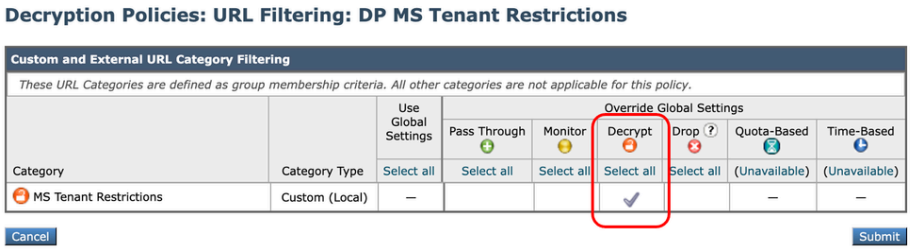


Immagine - Configura criterio di decrittografia

Passaggio 2.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento Filtro URL per il nuovo criterio.

Immagine - Modifica azione filtro URL

	Passaggio 2.9. Scegliere Decrittografa come azione per Categoria URL personalizzato. Passaggio 2.10. Fare clic su Sottometti.  Immagine - Decrittografa la categoria dell'URL personalizzato
Passaggio 3. Creare il profilo di riscrittura HTTP.	Passaggio 3.1. Dalla GUI, passare a Web Security Manager e scegliere HTTP ReWrite Profiles. Passaggio 3.2. Fare clic su Aggiungi profilo. Passaggio 3.3. Immettere il nome del nuovo profilo. Passaggio 3.4. Utilizzare Restrict-Access-To-Tenant per il primo nome intestazione. Passaggio 3.5. Per l'impostazione Restrict-Access-To-Tenants, utilizzare il valore <elenco tenant consentiti>, che deve essere un elenco separato da virgole dei tenant a cui gli utenti possono accedere. Passaggio 3.6. Fare clic su Aggiungi riga Passaggio 3.7. Utilizzare Restrict-Access-Context come secondo nome intestazione. Passaggio 3.8. Per l'impostazione Restrict-Access-Context, utilizzare il valore di un singolo ID directory per specificare il tenant che definisce le restrizioni tenant. Passaggio 3.9. Fare clic su Sottometti.

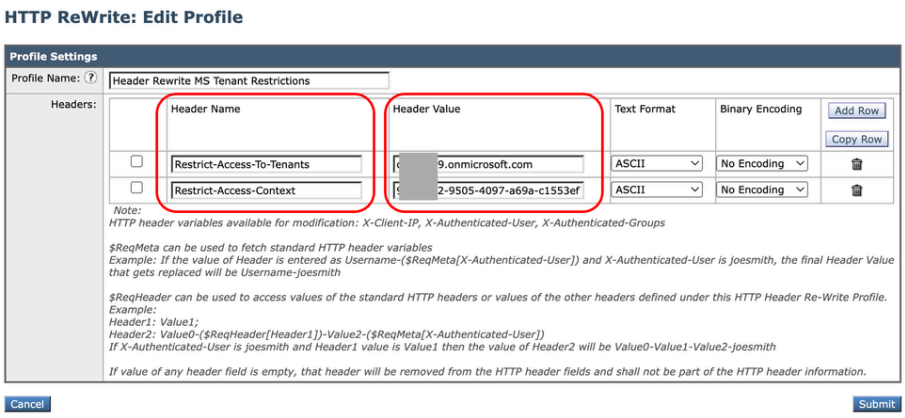
<table>
<tr>
<td></td>
<td>


Immagine - Aggiungi profilo ReWrite HTTP

Suggerimento: Per ulteriori informazioni sulle Restrizioni tenant e su come raccogliere le informazioni sul tenant, visitare: Microsoft Learn - Limita l'accesso a un tenant.
</td>
</tr>
<tr>
<td>Passaggio 4. Creazione dei criteri di accesso.</td>
<td>
Passaggio 4.1. Dalla GUI, passare a Web Security Manager e scegliere Access Policies

Passaggio 4.2. Fare clic su Aggiungi criterio.

Passaggio 4.3. Immettere il nome del nuovo criterio.

Passaggio 4.4. Selezionare il profilo di identificazione a cui applicare il criterio.

Suggerimento: Se le autenticazioni per gli URL Microsoft sono state ignorate e si sta configurando questo criterio per Tutti gli utenti, scegliere: Tutti i profili di identificazione > Tutti gli utenti.

Passaggio 4.5. Dalla sezione Definizione membri dei criteri, fare clic sui collegamenti Categorie URL per aggiungere la categoria URL personalizzata.

Passaggio 4.6. Selezionare la categoria dell'URL creata nel Passaggio 1.

Passaggio 4.7. Fare clic su Sottometti.
</td>
</tr>
</table>

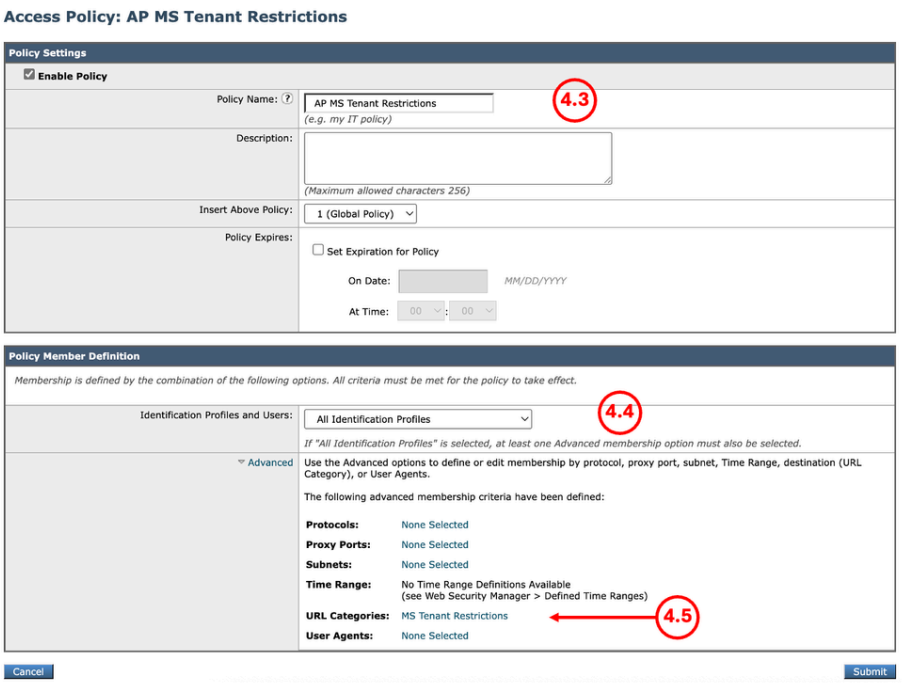


Immagine - Crea criteri di accesso

Passaggio 4.8. Nella pagina Criteri di accesso, verificare che l'azione del filtro URL sia impostata su Monitor.

Passaggio 4.9. Fare clic sul collegamento in Profilo di riscrittura HTTP per aggiungere il profilo di intestazione HTTP al criterio.

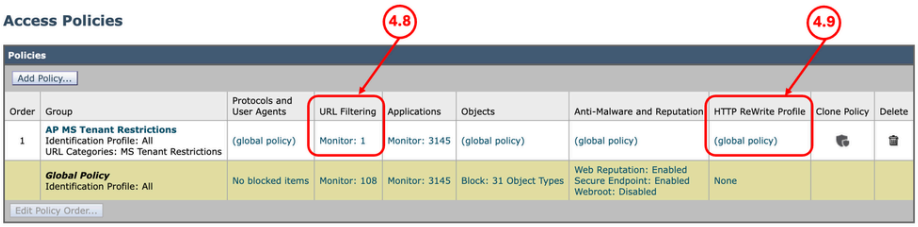


Immagine - Proprietà criteri di accesso

Passaggio 4.10. Scegliere i profili di riscrittura HTTP, creati nel passaggio [3].

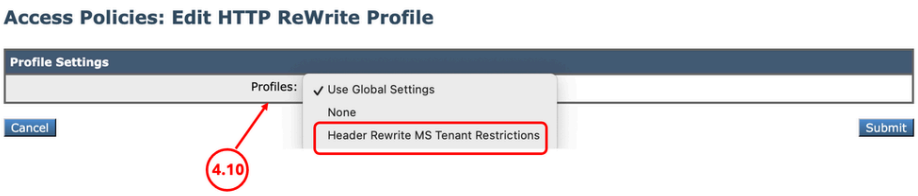


Immagine - Aggiungi profilo ReWrite HTTP

Passaggio 4.11. Fare clic su Sottometti.

Passaggio 4.12. Esecuzione del commit delle modifiche.

Report e log

Log

È possibile aggiungere un campo personalizzato ai log degli accessi o ai log W3C per visualizzare il nome del profilo di riscrittura dell'intestazione HTTP.

Identificatore formato nei log degli accessi	Campo di log nei log W3C	Descrizione
%]	x-http-rewrite-profile-name	Nome profilo di riscrittura intestazione HTTP.

Creazione di report

È possibile generare un report di verifica Web per visualizzare i report del traffico in base al nome del criterio di accesso.

Per generare i rapporti, effettuare le operazioni riportate di seguito.

Passaggio 1. Dalla GUI, selezionare Reporting e scegliere Tracciamento Web.

Passaggio 2. Scegliere l'intervallo di tempo desiderato.

Passaggio 3. Fare clic sul collegamento Avanzate per cercare le transazioni utilizzando criteri avanzati.

Passaggio 4. Nella sezione Criterio selezionare Filtra per criterio e digitare il nome del criterio di accesso creato in precedenza.

Passaggio 5. Fare clic su Cerca per esaminare il report.

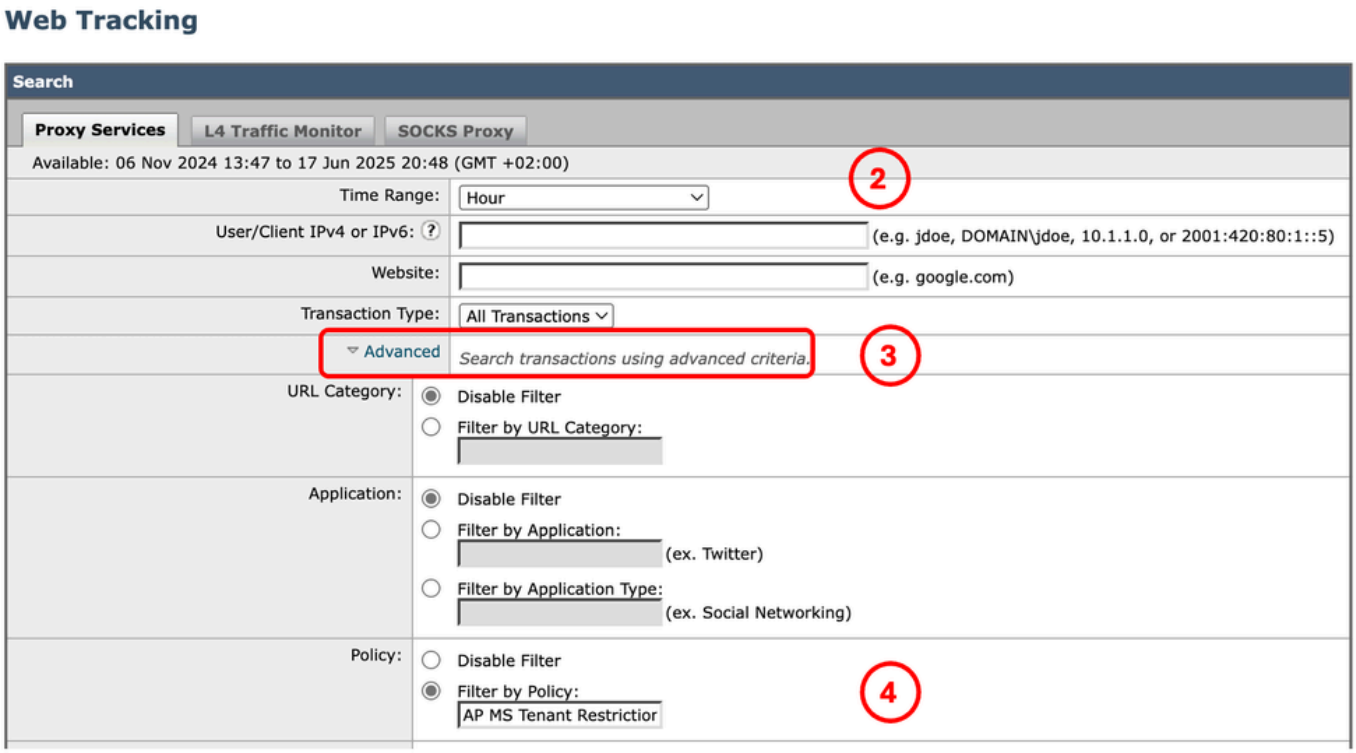


Immagine - Report di verifica Web

Informazioni correlate

- Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance
- Guida all'installazione di Cisco Secure Email e Web Virtual Appliance
- Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco
- Utilizzare le procedure ottimali per Secure Web Appliance
- Configurare il firewall per Secure Web Appliance
- Configura certificato di decrittografia in Appliance Web sicura
- Configurazione e risoluzione dei problemi di SNMP in SWA
- Configurazione dei log di push SCP in Secure Web Appliance con Microsoft Server
- Abilita canale/video YouTube specifico e blocca resto di YouTube in SWA
- Informazioni sul formato HTTPS Accesslog in Secure Web Appliance
- Accesso ai registri protetti di Web Appliance
- Ignora autenticazione in Secure Web Appliance
- Blocca il traffico in Secure Web Appliance
- Ignora traffico aggiornamenti Microsoft in Secure Web Appliance

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).