

Blocco dell'accesso degli account consumer di Google nell'area SWA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Report e log](#)

[Log](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il processo di blocco dell'accesso a Google Workspace o Google Consumer Accounts in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

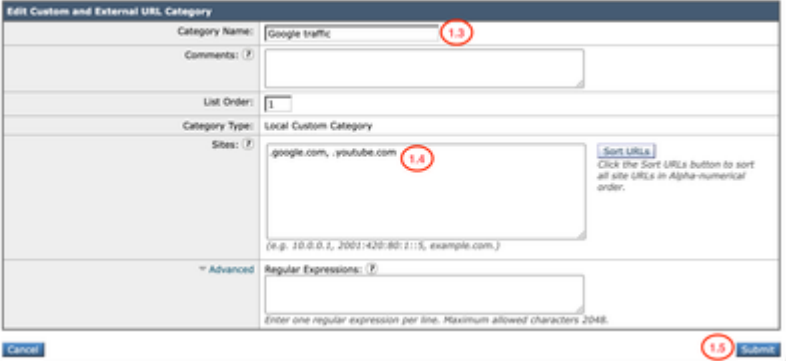

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'SWA.

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.

Configurazione

<p>Passaggio 1. Creare una categoria URL personalizzata per i siti Google.</p>	<p>Passaggio 1.1. Dalla GUI, passare a Web Security Manager e scegliere Custom e External URL Categories.</p> <p>Passaggio 1.2. Fare clic su Add Category (Aggiungi categoria) per creare una nuova categoria di URL personalizzati.</p> <p>Passaggio 1.3. Inserire il nome per la nuova categoria.</p> <p>Passaggio 1.4. Definire gli URL nella sezione Siti:</p> <p>.google.com</p> <p>Passaggio 1.5. Inviare le modifiche.</p> <p>Custom and External URL Categories: Edit Category</p>  <p>Immagine - Categoria URL personalizzato</p> <p> Suggerimento: Per ulteriori informazioni su come configurare le categorie URL personalizzate, visitare: Configurare categorie URL personalizzate in Appliance Web protetta.</p>
<p>Passaggio 2. Decriptare il traffico.</p>	<p>Passaggio 2.1. Dalla GUI, passare a Web Security Manager</p>

e scegliere Decryption Policies.

Passaggio 2.2. Fare clic su Aggiungi criterio.

Passaggio 2.3. EnterName per il nuovo criterio.

Decryption Policy: Google account access

Policy Settings

Enable Policy

Policy Name: Google Traffic Decryption

Description:

Insert Above Policy: 1 (Office365)

Policy Expires:

Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: HH:MM:SS

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 membro criterio, fare clic su URL Classificazioni collegamenti per aggiungere la categoria URL personalizzata.

Passaggio 2.6. Selezionare la categoria URL creata nel passaggio 1.

Passaggio 2.7. Fare clic su Sottometti.

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:

Select One or More Identification Profiles

Identification Profile: No Identification Profile selected

Authorized Users and Groups: Add Identification Profile

Select Identification Profile...

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: Google traffic

User Agents: None Selected

Cancel Submit

Immagine - Configura criterio di decrittografia

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

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Google account access Identification Profile: Global All identified users URL Categories: Google traffic	Decrypt: 1 2.8	{global policy}	{global policy}		

Immagine - Modifica azione filtro URL

Passaggio 2.9. Selezionare Decrittografa come azione per Categoria URL personalizzata.

Passaggio 2.10. Fare clic su Sottometti.

Decryption Policies: URL Filtering: Google account access

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Google traffic	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

3.9 **2.10**

Immagine - Decrittografa la categoria dell'URL personalizzato

Passaggio 3.1. Dalla GUI, selezionare Web Security Manager e scegliere HTTP Rewrite Profiles.

Passaggio 3.2. Fare clic su Aggiungi profilo.

Passaggio 3.3. EnterName per il nuovo profilo.

Passaggio 3.4. Utilizzare X-GoogApps-Allowed-Domains per il nome della prima intestazione.

Passaggio 3.5. Per l'impostazione Restrict-Access-To-Tenant, utilizzare un valore di dominio dell'elenco di tenant consentiti, che deve essere un elenco separato da virgole dei tenant a cui gli utenti sono autorizzati ad accedere.

Passaggio 3. Creare il profilo di riscrittura HTTP.

Passaggio 3.9. Fare clic su Invia.

HTTP Rewrite: Edit Profile

Profile Settings

Profile Name: Google Header Rewrite

Header Name	Header Value	Text Format	Binary Encoding
X-GoogApps-Allowed-Domains	ciroa.com	ASCII	No Encoding

3.4 **3.5**

3.9

Immagine - Aggiungi profilo Rewrite HTTP

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. EnterName per il nuovo criterio.

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

Passaggio 4.5. Dalla sezione Definizione del membro dei criteri, fare clic su URL Categorieslinks (Categorie URL) per aggiungere la Categoria URL personalizzata.

Passaggio 4.6. Selezionare la categoria URL creata nel passaggio 1.

Passaggio 4.7. Fare clic su Sottometti.

Passaggio 4. Creare i criteri di accesso.

Access Policy: Google account access

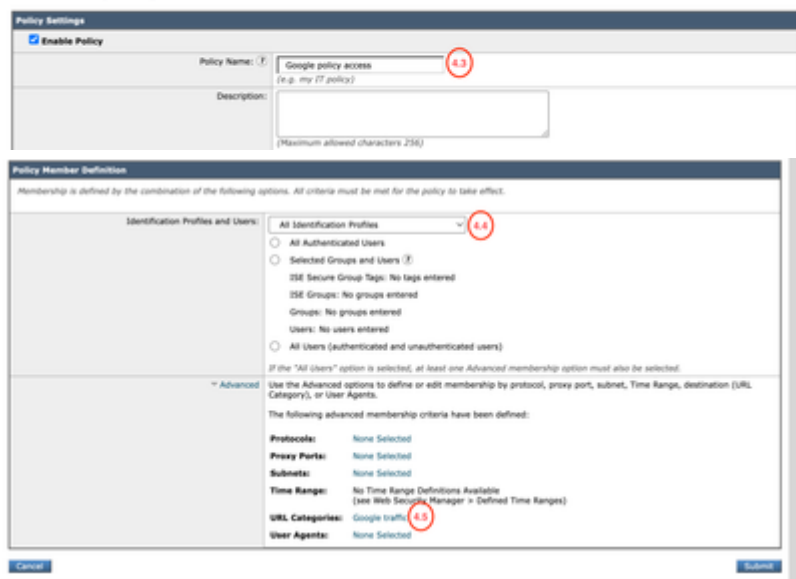



Immagine - Crea criteri di accesso

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

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

Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	C
(global policy)	Monitor: 4.8	Restrict: 1 Monitor: 320	(global policy)	(global policy)	Google rewrite 4.9	

	<p>Immagine - Proprietà criteri di accesso</p> <p>Passaggio 4.10. Scegliere i profili di riscrittura HTTP, creati nel passaggio [3].</p>  <p>Immagine - Aggiungi profilo ReWrite HTTP</p> <p>Passaggio 4.11. Fare clic su Sottometti.</p> <p>Passaggio 4.12. CommitChanges.</p>
--	---

Report e log

Log

È possibile aggiungere campi personalizzati 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.

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 Web Tracking.

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

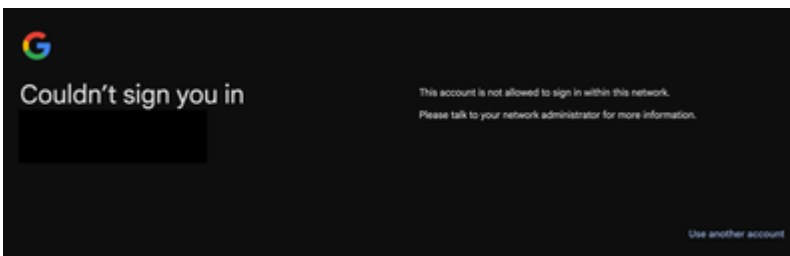
accesso creato in precedenza.

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

The screenshot shows the 'Search' section of a Proxy Services configuration page. The interface includes several filter fields: 'Time Range' (set to 'Hour'), 'User/Client IPv4 or IPv6', 'Website', 'Transaction Type' (set to 'All Transactions'), and 'Advanced' filters. The 'Advanced' filters are expanded to show 'URL Category', 'Application', and 'Policy'. The 'Policy' filter is selected and set to 'Filter by Policy: Google account access'. Red circles highlight the 'Time Range' dropdown, the 'Current Criteria: Policy: Google account access' text, and the 'Filter by Policy: Google account access' text.

Verifica

Una volta completata la configurazione della restrizione del dominio Google, l'utente può accedere solo agli account che si trovano nel dominio configurato nel profilo Header Rewrite nel passo 3. Se l'utente tenta di accedere a un account in un dominio diverso o a un account Google personale diverso, l'accesso viene limitato con questo avviso:



Informazioni correlate

[Definizione di categorie URL personalizzate in WSA](#)

[Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance](#)

[Configura certificato di decrittografia in Appliance Web sicura](#)

[Riscrittura intestazione HTTP WSA](#)

[Blocca l'accesso ai conti dei consumatori \(documentazione di Google\)](#)

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).