

# Configurazione di Secure Web Appliance per consentire l'accesso guest

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica dello scenario](#)

[Procedura di configurazione](#)

[Passaggio 1. Creazione del profilo di identificazione.](#)

[Passaggio 2. \(Facoltativo\) Creazione di categorie di URL personalizzati per gli URL consentiti e bloccati](#)

[Passaggio 3. Creazione dei criteri di decrittografia per i dispositivi gestiti](#)

[Passaggio 4. Creazione dei criteri di decrittografia per i dispositivi non gestiti](#)

[Passaggio 5. Creazione dei criteri di accesso per i dispositivi gestiti](#)

[Passaggio 6. Creazione dei criteri di accesso per i dispositivi non gestiti](#)

[Passaggio 7. \(Facoltativo\) Creazione di criteri di sicurezza dei dati Cisco per dispositivi gestiti](#)

[Passaggio 8. \(Facoltativo\) Creazione di criteri di sicurezza dei dati Cisco per dispositivi non gestiti](#)

[Passaggio 9. Salvataggio delle modifiche](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come consentire agli utenti che non hanno installato il certificato di decrittografia di accedere a Internet tramite Secure Web Appliance (SWA).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SWA fisico o virtuale installato.
- Licenza attivata o installata.
- Installazione guidata completata.
- Accesso amministrativo all'interfaccia grafica (GUI) 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.

## Panoramica dello scenario

Questo articolo descrive uno scenario di controllo dell'accesso alla rete all'interno della subnet Wi-Fi 10.10.10.0/24. L'ambiente è costituito da due gruppi di utenti distinti che richiedono regole di protezione e di accesso diverse:

- Dispositivi gestiti: Notebook aziendali completamente autenticati e con il certificato di decrittografia SWA installato. Questi dispositivi sono affidabili e sono in genere soggetti alle policy di accesso aziendali standard.
- Dispositivi non gestiti/guest: Notebook personali e dispositivi mobili non autenticati e privi del certificato di decrittografia SWA.

Obiettivo:

L'obiettivo dell'azienda è implementare policy di accesso al Web restrittive per i dispositivi non gestiti, limitando la connettività a un sottoinsieme specifico di URL consentiti e garantendo al contempo la sicurezza delle risorse aziendali.

---

 Nota: Poiché il certificato di decrittografia non è considerato attendibile sui dispositivi non gestiti, non è possibile decrittografare il traffico HTTPS e l'azione deve essere impostata in modo da consentirne la trasmissione.

---

## Procedura di configurazione

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passaggio 1. Creare il profilo di identificazione. | <p>Passaggio 1.1. Dalla GUI SWA, passare a Web Security Manager e selezionare Identification Profile (Profilo di identificazione).</p> <p>Passaggio 1.2. Fare clic su Aggiungi profilo di identificazione.</p> <p>Passaggio 1.3. Definire un nome per il profilo.</p> <p>Passaggio 1.4. (Facoltativo) Definire la descrizione.</p> <p>Passaggio 1.5. Scegliere Autentica utenti in Identificazione e autenticazione.</p> <p>Passaggio 1.6. Scegliere il realm di Active Directory da Selezionare un realm o una sequenza.</p> |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Passaggio 1.7. Da Selezionare uno schema, selezionare i protocolli di autenticazione desiderati.



Suggerimento: Non scegliere Autenticazione di base nell'elenco Selezionare uno schema.

Passaggio 1.8. Selezionare la casella di controllo Privilegi Guest di supporto.

Passaggio 1.9. (Facoltativo) A seconda del progetto, è possibile abilitare il surrogato abilitando Applica le stesse impostazioni del surrogato alle richieste di inoltro esplicite.



Attenzione: Poiché non è possibile decrittografare il traffico, nella distribuzione trasparente non selezionare Cookie persistente o Cookie di sessione.

Passaggio 1.10. Definire la subnet di indirizzi IP in, Definire i membri in base alla subnet.

Passaggio 1.11. Sottomettere e confermare le modifiche.

Immagine - Definizione del profilo di identificazione

Passaggio 2. (Facoltativo)  
Creazione di categorie di URL  
personalizzati per gli URL consentiti

Passaggio 2.1. Dalla GUI, passare a Web Security Manager e scegliere Categorie URL personalizzate ed esterne.

e bloccati

- Passaggio 2.2.Fare clic su Aggiungi categoria per creare una nuova categoria di URL personalizzati.
- Passaggio 2.3.Inserire il nome della nuova categoria.
- Passaggio 2.4.Definire il dominio e/o i sottodomini dei siti Web a cui si desidera bloccare l'accesso.
- Passaggio 2.5.Inviare le modifiche.
- Passaggio 2.6. Per creare una categoria URL per il sito Web a cui si desidera consentire l'accesso, attenersi alla stessa procedura.

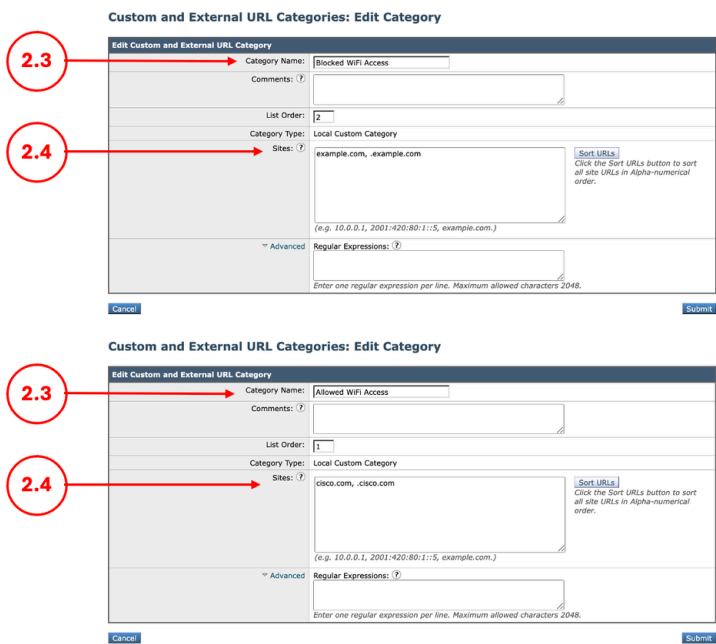


Immagine - Definisci categoria URL personalizzata

Passaggio 3. Creazione dei criteri di decrittografia per i dispositivi gestiti

- Passaggio 3.1. Dalla GUI, passare a Web Security Manager e selezionare Decryption Policies (Criteri di decrittografia)
- Passaggio 3.2. Fare clic su Aggiungi criterio.
- Passaggio 3.3.EnterName per il nuovo criterio.
- Passaggio 3.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.
- Passaggio 3.5.Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 3.6. Selezionare Tutti gli utenti autenticati.

Passaggio 3.7. Fare clic su Sottometti.

Decryption Policy: WiFi Users DP

**Policy Settings**

☒ Enable Policy

Policy Name: WiFi Users DP  
(e.g. my IT policy)

Description: (Maximum allowed characters 255)

Insert Above Policy: 1 (WiFi Guest DP)

Policy Expires: ☐ Set Expiration for Policy  
On Date: MM/DD/YYYY  
At Time: HH:MM:SS

**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

WiFi IDP

Authorized Users and Groups

☒ All Authenticated Users

☐ Selected Groups and Users (Groups: No groups entered, Users: No users entered)

☐ Guests (users failing authentication)

**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: None Selected  
User Agents: None Selected

Cancel Submit

Crea criterio di decrittografia per dispositivi gestiti

Passaggio 3.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 3.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 3.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

Passaggio 3.11. Fare clic su Invia

Decryption Policies: URL Filtering: WiFi Users DP

**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                 | Pass Through | Monitor    | Decrypt    | Drop       | Quota-Based   | Time-Based    |
|---------------------|----------------|-------------------------------------|--------------|------------|------------|------------|---------------|---------------|
| Allowed WiFi Access | Custom (Local) | <input checked="" type="checkbox"/> | Select all   | Select all | Select all | Select all | (Unavailable) | (Unavailable) |

Cancel Submit

**Predefined URL Category Filtering**

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

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

| Category                   | Use Global Settings                 | Pass Through                        | Monitor                             | Decrypt                             | Drop                                | Quota-Based                         | Time-Based                          |
|----------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Adult                      | <input checked="" type="checkbox"/> | Select all                          | Select all                          | Select all                          | Select all                          | (Unavailable)                       | (Unavailable)                       |
| Advertisements             | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Alcohol                    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Arts                       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Astronomy                  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Auctions                   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Business and Industry      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Chat and Instant Messaging | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Immagine - Configura azione per criterio di decrittografia

Passaggio 4. Creazione dei criteri di decrittografia per i dispositivi non gestiti

Passaggio 4.1. Dalla GUI, passare a Web Security Manager e selezionare Decryption Policies (Criteri di decrittografia)

Passaggio 4.2. Fare clic su Aggiungi criterio.

Passaggio 4.3. EnterName per il nuovo criterio.

Passaggio 4.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.

Passaggio 4.5. Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 4.6. Selezionare Guests (errori di autenticazione degli utenti).

Passaggio 4.7. Fare clic su Sottometti.

Decryption Policy: WiFi Guest DP

**Policy Settings**

☒ Enable Policy

Policy Name: WiFi Guest DP  
(e.g. my IT policy)

Description:

Insert Above Policy: 2 (Global Policy)

Policy Expires:

☐ Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: 00:00:00

**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: WiFi IDP

Authorized Users and Groups: Add Identification Profile

☐ All Authenticated Users

☐ Selected Groups and Users (Groups: No groups entered Users: No users entered)

☒ Guests (users failing authentication)

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

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: None Selected

User Agents: None Selected

Cancel Submit

Crea criterio di decrittografia per dispositivi non gestiti

Passaggio 4.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 4.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 4.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.



Nota: Non utilizzare Decrypt come azione, poiché il certificato di decrittografia SWA non è attendibile sui dispositivi non gestiti.

#### Decryption Policies: URL Filtering: WiFi Guest DP

| Category            | Category Type  | Use Global Settings | Pass Through | Monitor | Decrypt | Drop | Quota-Based | Time-Based |
|---------------------|----------------|---------------------|--------------|---------|---------|------|-------------|------------|
| Allowed WiFi Access | Custom (Local) | —                   | ✓            | —       | —       | —    | —           | —          |
| Blocked WiFi Access | Custom (Local) | —                   | —            | —       | —       | —    | —           | —          |

| Category              | Use Global Settings | Pass Through | Monitor | Decrypt | Drop | Quota-Based | Time-Based |
|-----------------------|---------------------|--------------|---------|---------|------|-------------|------------|
| Adult                 | —                   | —            | —       | —       | ✓    | —           | —          |
| Advertisements        | —                   | —            | —       | —       | ✓    | —           | —          |
| Alcohol               | —                   | —            | —       | —       | ✓    | —           | —          |
| Arts                  | —                   | —            | —       | —       | —    | —           | —          |
| Astroslogy            | —                   | —            | —       | —       | ✓    | —           | —          |
| Auctions              | —                   | —            | —       | —       | ✓    | —           | —          |
| Business and Industry | —                   | —            | —       | —       | —    | —           | —          |

Immagine - Azione di decrittografia per dispositivi non gestiti

Passaggio 4.11. Scorrere verso il basso la sezione URL non classificati e scegliere l'azione appropriata.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs: Drop

Default Action for Update Categories: Most Restrictive

Immagine - URL non classificati



Suggerimento: Per motivi di sicurezza, è consigliabile impostare l'azione su Elimina, nel caso in cui un URL richieda l'accesso, è possibile aggiungerlo nella Categoria URL personalizzato assegnata al criterio.

Passaggio 4.12. Fare clic su Submit

Passaggio 5. Creazione dei criteri di accesso per i dispositivi gestiti

Passaggio 5.1. Dalla GUI, passare a Web Security Manager e scegliere Access Policies (Policy di accesso)

Passaggio 5.2. Fare clic su Aggiungi criterio.

Passaggio 5.3. EnterName per il nuovo criterio.

Passaggio 5.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.

Passaggio 5.5. Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 5.6. Selezionare Tutti gli utenti autenticati.

Passaggio 5.7. Fare clic su Sottometti.

Access Policy: WiFi Users AP

**Policy Settings**

☒ Enable Policy

Policy Name: WiFi Users AP  
(e.g. my IT policy)

Description: (Maximum allowed characters 256)

Insert Above Policy: 1 (WiFi Guest AP)

Policy Expires: ☐ Set Expiration for Policy  
On Date: MM/DD/YYYY  
At Time: HH:MM:SS

**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: WiFi IDP

Authorized Users and Groups: ☒ All Authenticated Users  
☐ Selected Groups and Users (?)  
Groups: No groups entered  
Users: No users entered  
☐ Guests (users failing authentication)

**Advanced**

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: HTTP/HTTPS/FTP over HTTP in Identification Profile WiFi IDP

Proxy Ports: None Selected

Subnets: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

Time Range: None Selected

URL Categories: None Selected

User Agents: None Selected

Cancel Submit

Immagine - Criteri di accesso per dispositivi gestiti

Passaggio 5.8. Nella pagina Criteri di accesso, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 5.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 5.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

Access Policies: URL Filtering: WiFi Users AP

**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: Allowed WiFi Access

Category Type: Custom (Local)

Use Global Settings: ☐

Block: ☐ Redirect: ☐ Allow: ☒ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Cancel Submit

**Predefined URL Category Filtering**

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

Category: Adult

Use Global Settings: ☐

Block: ☒ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Cancel Submit

Immagine - Filtro URL criteri di accesso per dispositivi gestiti



Passaggio 5.11. Fare clic su Submit (Invia).

Passaggio 6.1. Dalla GUI, passare a Web Security Manager e scegliere Access Policies (Policy di accesso)

Passaggio 6.2. Fare clic su Aggiungi criterio.

Passaggio 6.3. EnterName per il nuovo criterio.

Passaggio 6.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.

Passaggio 6.5. Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 6.6. Selezionare Guests (errori di autenticazione degli utenti).

Passaggio 6.7. Fare clic su Sottometti.

Passaggio 6. Creazione dei criteri di accesso per i dispositivi non gestiti

Access Policy: WiFi Guest AP

**Policy Settings**

☒ Enable Policy

Policy Name: WiFi Guest AP (e.g., my IT policy)

Description:

Insert Above Policy: 2 (Global Policy)

Policy Expires:

☐ Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: HH:MM:SS

**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: WiFi IDP

Authorized Users and Groups

☐ All Authenticated Users

☐ Selected Groups and Users (?)

Groups: No groups entered

Users: No users entered

☒ Guests (users failing authentication)

**Advanced**

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:

Protocol: HTTP/HTTPS/FTP over HTTP in Identification Profile WiFi IDP

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Cancel Submit

Immagine - Criteri di accesso per dispositivi non gestiti

Passaggio 6.8. Nella pagina Criteri di accesso, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 6.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 6.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

Access Policies: URL Filtering: WiFi Guest AP

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 |            |            |            |            |             |
|---------------------|----------------|---------------------|--------------------------|------------|------------|------------|------------|-------------|
|                     |                |                     | Block                    | Redirect   | Allow      | Monitor    | Warn       | Quota-Based |
| Allowed WiFi Access | Custom (Local) | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  |
| Blocked WiFi Access | Custom (Local) | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  |

6.9

6.10

Predefined URL Category Filtering

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

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

| Category                   | Use Global Settings | Override Global Settings |            |            |            |            |             |            |
|----------------------------|---------------------|--------------------------|------------|------------|------------|------------|-------------|------------|
|                            |                     | Block                    | Redirect   | Allow      | Monitor    | Warn       | Quota-Based | Time-Based |
| Adult                      | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |
| Advertisements             | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |
| Alcohol                    | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |
| Arts                       | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |
| Astrotology                | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |
| Auctions                   | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |
| Business and Industry      | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |
| Chat and Instant Messaging | Select all          | Select all               | Select all | Select all | Select all | Select all | Select all  | Select all |

Immagine - Filtro URL criteri di accesso per dispositivi non gestiti

Passaggio 6.11. Scorrere verso il basso la sezione URL non classificati e scegliere l'azione appropriata.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs: Block

Default Action for Update Categories: Most Restrictive

6.11

Immagine - URL non classificati nei criteri di accesso

 Suggerimento: Per motivi di sicurezza, è consigliabile impostare l'azione su Blocca, nel caso in cui un URL richieda l'accesso, è possibile aggiungerlo nella Categoria URL personalizzato assegnata al criterio.

Passaggio 6.12. Fare clic su Submit (Invia)

Passaggio 7. (Facoltativo)  
Creazione di criteri di sicurezza dei dati Cisco per dispositivi gestiti

 Nota: Se non si desidera filtrare il traffico di caricamento per i dispositivi gestiti, è possibile ignorare questo passaggio.

Passaggio 7.1. Dalla GUI, passare a Web Security Manager e scegliere Cisco Data Security.

Passaggio 7.2. Fare clic su Aggiungi criterio.

Passaggio 7.3. EnterName per il nuovo criterio.

Passaggio 7.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.

Passaggio 7.5. Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 7.6. Selezionare Tutti gli utenti autenticati.

Passaggio 7.7. Fare clic su Sottometti.

**Cisco Data Security Policy: Add Group**

**Policy Settings**

☒ Enable Policy

Policy Name:

Description:

Insert Above Policy:

**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:

Identification Profile:

Authorized Users and Groups: ☒ All Authenticated Users

☐ Selected Groups and Users (Groups: No groups entered Users: No users entered)

☐ Guests (users failing authentication)

[Add Identification Profile](#)

[Cancel](#) [Submit](#)

Immagine - Criterio di sicurezza dei dati Cisco per dispositivi gestiti

Passaggio 7.8. Nella pagina Criteri di sicurezza dei dati Cisco, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 7.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 7.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per il filtro predefinito delle categorie di URL.

**Cisco Data Security Policies: URL Filtering: Wifi Users Upload**

**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:

[Select Custom Categories...](#)

[Cancel](#) [Submit](#)

**Predefined URL Category Filtering**

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

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

| Category       | Use Global Settings                 | Override Global Settings            |
|----------------|-------------------------------------|-------------------------------------|
|                | Select all                          | Monitor Block                       |
| Adult          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Advertisements | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Alcohol        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Arts           | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Astrology      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Auctions       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Immagine - Azione di caricamento per dispositivi gestiti

Passaggio 7.11. Fare clic su Sottometti.

Passaggio 8. (Facoltativo)  
Creazione di criteri di sicurezza dei

Passaggio 8.1. Dalla GUI, passare a Web Security Manager e scegliere Cisco Data Security.

dati Cisco per dispositivi non gestiti

 Nota: Se non si desidera filtrare il traffico di caricamento per i dispositivi non gestiti, è possibile ignorare questo passaggio.

Passaggio 8.2. Fare clic su Aggiungi criterio.

Passaggio 8.3. EnterName per il nuovo criterio.

Passaggio 8.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.

Passaggio 8.5. Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 8.6. Selezionare Tutti gli utenti autenticati.

Passaggio 8.7. Fare clic su Sottometti.

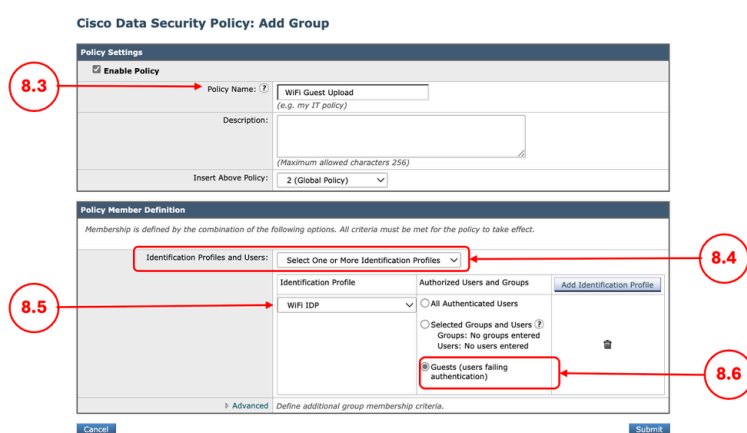


Immagine - Criterio di sicurezza dei dati Cisco per dispositivi non gestiti

Passaggio 8.8. Nella pagina Criteri di sicurezza dei dati Cisco, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 8.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 8.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

# Cisco Data Security Policies: URL Filtering: WiFi Guest Upload

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  | Select all | Override Global Settings            |                          |                                     |
|---------------------|----------------|------------|-------------------------------------|--------------------------|-------------------------------------|
|                     |                |            | Use Global Settings                 | Allow                    | Monitor                             |
| Allowed WiFi Access | Custom (Local) | Select all | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            |
| Blocked WiFi Access | Custom (Local) | Select all | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Predefined URL Category Filtering

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

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

| Category       | Select all | Override Global Settings |                          |                                     |
|----------------|------------|--------------------------|--------------------------|-------------------------------------|
|                |            | Use Global Settings      | Monitor                  | Block                               |
| Adult          | Select all | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Advertisements | Select all | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Alcohol        | Select all | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Arts           | Select all | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Astrology      | Select all | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Auctions       | Select all | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Immagine - Azione di caricamento per dispositivi non gestiti

Passaggio 8.11. Scorrere verso il basso la sezione URL non classificati e scegliere l'azione appropriata.

Uncategorized URLs

Specify an action for urls that do not match any category.

Immagine - Azione di caricamento per URL non classificati



Suggerimento: Per motivi di sicurezza, è consigliabile impostare l'azione su Blocca, nel caso in cui un URL richieda l'accesso, è possibile aggiungerlo nella Categoria URL personalizzato assegnata al criterio.

Passaggio 8.12. Fare clic su Submit (Invia)

Passaggio 9. Salvataggio delle modifiche

Passaggio 9.1. Eseguire il commit delle modifiche

## Informazioni correlate

- [Guida per l'utente di AsyncOS 15.0 for Cisco Secure Web Appliance - LD \(installazione limitata\) - Risoluzione dei problemi...](#)
- [Blocca download file eseguibile in SWA](#)
- [Blocca il traffico di caricamento in Secure Web Appliance](#)
- [Blocca il traffico in Secure Web Appliance](#)
- [Ignora autenticazione in Secure Web Appliance](#)
- [Configura restrizione tenant Microsoft O365 in SWA](#)
- [Configura installazione iniziale di 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).