

Konfigurieren der sicheren Webappliance zum Zulassen des Gastzugriffs

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Szenario - Überblick](#)

[Konfigurationsschritte](#)

[Schritt 1: Identifikationsprofil erstellen](#)

[Schritt 2: \(Optional\) Erstellen Sie benutzerdefinierte URL-Kategorien für zulässige und gesperrte URLs](#)

[Schritt 3: Entschlüsselungsrichtlinie für verwaltete Geräte erstellen](#)

[Schritt 4: Entschlüsselungsrichtlinie für nicht verwaltete Geräte erstellen](#)

[Schritt 5: Erstellen einer Zugriffsrichtlinie für verwaltete Geräte](#)

[Schritt 6: Erstellen einer Zugriffsrichtlinie für nicht verwaltete Geräte](#)

[Schritt 7: \(Optional\) Erstellen einer Cisco Datensicherheitsrichtlinie für verwaltete Geräte](#)

[Schritt 8: \(Optional\) Erstellen einer Cisco Datensicherheitsrichtlinie für nicht verwaltete Geräte](#)

[Schritt 9: Speichern der Änderungen](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte beschrieben, mit denen Benutzer, die das Entschlüsselungszertifikat nicht installiert haben, über die Secure Web Appliance (SWA) auf das Internet zugreifen können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Installierte physische oder virtuelle SWA.
- Lizenz aktiviert oder installiert.
- Der Setup-Assistent ist abgeschlossen.
- Administrator-Zugriff auf die grafische Benutzeroberfläche (GUI) von 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.

Szenario - Überblick

Dieser Artikel behandelt ein Szenario der Netzwerkzugriffskontrolle innerhalb des Wi-Fi-Subnetzes 10.10.10.0/24. Die Umgebung besteht aus zwei unterschiedlichen Benutzergruppen, die unterschiedliche Sicherheits- und Zugriffsrichtlinien erfordern:

- **Verwaltete Geräte:** Firmeneigene Laptops, die vollständig authentifiziert sind und auf denen das SWA-Entschlüsselungszertifikat installiert ist. Diese Geräte sind vertrauenswürdig und unterliegen in der Regel den Standard-Zugriffsrichtlinien des Unternehmens.
- **Nicht verwaltete Geräte/Gastgeräte:** Private Laptops und Mobilgeräte ohne Authentifizierung ohne SWA-Entschlüsselungszertifikat

Ziel:

Ziel des Unternehmens ist die Implementierung restriktiver Web-Zugriffsrichtlinien für nicht verwaltete Geräte, die deren Verbindung auf einen bestimmten Teil der zulässigen URLs beschränken und gleichzeitig sicherstellen, dass die Unternehmensressourcen geschützt bleiben.

 **Anmerkung:** Da das Entschlüsselungszertifikat auf den nicht verwalteten Geräten nicht vertrauenswürdig ist, können Sie den HTTPS-Datenverkehr nicht entschlüsseln, und die Aktion muss auf "Pass Through" (Weiterleiten) festgelegt werden.

Konfigurationsschritte

Schritt 1: Erstellen eines Identifikationsprofils	Schritt 1.1: Navigieren Sie in der SWA-GUI zum Web Security Manager, und wählen Sie Identification Profile aus. Schritt 1.2: Klicken Sie auf Identifikationsprofil hinzufügen. Schritt 1.3. Definieren eines Namens für das Profil. Schritt 1.4 (Optional) Definieren Sie die Beschreibung. Schritt 1.5. Wählen Sie Benutzer in Identifizierung und Authentifizierung authentifizieren. Schritt 1.6. Wählen Sie den Active Directory-Bereich
--	--

aus Bereich oder Sequenz auswählen.

Schritt 1.7. Wählen Sie unter Select a Scheme (Schema auswählen) die gewünschten Authentifizierungsprotokolle aus.



Tipp: Wählen Sie in der Liste Schema auswählen nicht die Option Standardauthentifizierung aus.

Schritt 1.8. Aktivieren Sie das Kontrollkästchen für Support Guest-Berechtigungen.

Schritt 1.9. (Optional) Abhängig von Ihrem Design können Sie das Surrogat aktivieren, indem Sie dieselben Surrogateinstellungen auf explizite Weiterleitungsanforderungen anwenden.



Vorsicht: Da Sie den Datenverkehr nicht entschlüsseln können, wählen Sie in der transparenten Bereitstellung nicht Persistent Cookie oder Session Cookie.

Schritt 1.10. Definieren Sie das Subnetz der IP-Adresse in, definieren Sie Mitglieder nach Subnetz.

Schritt 1.11: Senden und bestätigen Sie die Änderungen.

The screenshot shows the 'Identification Profiles: WiFi IDP' configuration page. It is divided into three main sections: 'Client / User Identification Profile Settings', 'User Identification Method', and 'Membership Definition'. Red circles with numbers 1.3 through 1.10 point to specific configuration elements:

- 1.3** points to the 'Enable Identification Profile' checkbox.
- 1.4** points to the 'Name' field, which contains 'WiFi IDP'.
- 1.5** points to the 'Authentication Realm' dropdown menu.
- 1.6** points to the 'Select a Scheme' dropdown menu, which is set to 'Use Kerberos or NTLMSSP'.
- 1.7** points to the 'Support Guest privileges' checkbox, which is checked.
- 1.8** points to the 'Authentication Surrogates' section, which includes radio buttons for 'IP Address', 'Persistent Cookie', and 'Session Cookie'. The 'IP Address' option is selected.
- 1.9** points to the 'Apply same surrogate settings to explicit forward requests' checkbox, which is checked.
- 1.10** points to the 'Define Members by Subnet' field, which contains the IP address '10.10.10.24'.

At the bottom of the page, there are 'Cancel' and 'Submit' buttons.

Bild - Identifikationsprofil definieren

Schritt 2: (Optional) Erstellen Sie benutzerdefinierte URL-Kategorien für zulässige und gesperrte URLs

Schritt 2.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus.

Schritt 2.2. Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen.

Schritt 2.3. EnterName für die neue Kategorie.

Schritt 2.4. Definieren Sie die Domain und/oder Subdomains der Websites, die Sie den Zugriff blockieren möchten.

Schritt 2.5. Senden Sie die Änderungen.

Schritt 2.6. Führen Sie die gleichen Schritte aus, um eine URL-Kategorie für die Website zu erstellen, auf die Sie den Zugriff zulassen.

The image displays two screenshots of the 'Custom and External URL Categories: Edit Category' form. In the top screenshot, the 'Category Name' is 'Blocked WiFi Access', 'List Order' is 2, and 'Sites' are 'example.com, example.com'. In the bottom screenshot, the 'Category Name' is 'Allowed WiFi Access', 'List Order' is 1, and 'Sites' are 'cisco.com, cisco.com'. Red circles with numbers 2.3 and 2.4 point to the 'Category Name' and 'Sites' fields respectively in both screenshots.

Bild: Benutzerdefinierte URL-Kategorie definieren

Schritt 3: Entschlüsselungsrichtlinie für verwaltete Geräte erstellen

Schritt 3.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Entschlüsselungsrichtlinien aus.

Schritt 3.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 3.3. EnterName für die neue Richtlinie.

Schritt 3.4: Wählen Sie mindestens ein

Identifikationsprofil aus dem Dropdown-Menü
Identifikationsprofile und Benutzer aus.

Schritt 3.5. Wählen Sie das in Schritt 1 erstellte
Identifikationsprofil aus.

Schritt 3.6. Wählen Sie Alle authentifizierten Benutzer
aus.

Schritt 3.7: Klicken Sie auf Senden.

Entschlüsselungsrichtlinie für verwaltete Geräte erstellen

Schritt 3.8. Klicken Sie auf der Seite
Entschlüsselungsrichtlinien auf den Link von URL-
Filterung für die neue Richtlinie.

Schritt 3.9. (Optional) Sie können jede
benutzerdefinierte URL-Kategorie hinzufügen, indem
Sie auf Benutzerdefinierte Kategorien auswählen
klicken und In Richtlinie einschließen vor den
Kategorienamen wählen.

Schritt 3.10: Konfigurieren Sie die Aktion für jede
benutzerdefinierte und externe URL-
Kategoriefilterung und vordefinierte URL-
Kategoriefilterung.

Schritt 3.11: Klicken Sie auf Senden

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	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	☒	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

3.9 [Select Custom Categories...](#)

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					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Adult	☒	Select all	Select all	☒	☒	—	—
Advertisements	☒			☒	☒	—	—
Alcohol	☒			☒	☒	—	—
Arts	☒			☒	☒	—	—
Astronomy	☒	☒		☒	☒	—	—
Business and Industry	☒	☒		☒	☒	—	—
Chat and Instant Messaging	☒	☒				—	—

3.10

Image: Aktion für Entschlüsselungsrichtlinie konfigurieren

Schritt 4.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Entschlüsselungsrichtlinien aus.

Schritt 4.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 4.3. Enter Name für die neue Richtlinie.

Schritt 4.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 4.5. Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 4.6. Wählen Sie Gäste (Benutzer, die nicht authentifiziert werden konnten).

Schritt 4.7: Klicken Sie auf Senden.

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: 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)

4.3

4.4

4.5

4.6

Schritt 4: Entschlüsselungsrichtlinie für nicht verwaltete Geräte erstellen

Schritt 4.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung für die neue Richtlinie.

Schritt 4.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 4.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.



Anmerkung: Verwenden Sie nicht Entschlüsseln als Aktion, da das SWA-Entschlüsselungszertifikat auf den nicht verwalteten Geräten nicht vertrauenswürdig ist.

Decryption Policies: URL Filtering: WiFi Guest 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	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Blocked WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

4.9 → Blocked WiFi Access

4.10 → Decrypt

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					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Adult	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Advertisements	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Alcohol	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Arts	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Astrology	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Auctions	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Business and Industry	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Image - Entschlüsselungsaktion für nicht verwaltete Geräte

Schritt 4.11. Blättern Sie im Abschnitt Nicht kategorisierte URLs nach unten, und wählen Sie die gewünschte Aktion aus.

Uncategorized URLs

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

Uncategorized URLs: Drop

Default Action for Update Categories: Most Restrictive

4.11 → Drop

Bild - Nicht kategorisierte URLs



Tipp: Aus sicherheitstechnischer Sicht ist es am



besten, die Aktion auf Drop festzulegen. Falls eine URL Zugriff benötigt, können Sie sie in der benutzerdefinierten URL-Kategorie hinzufügen, die der Richtlinie zugewiesen ist.

Schritt 4.12: Klicken Sie auf Senden

Schritt 5.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Zugriffsrichtlinien.

Schritt 5.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 5.3. Enter Name für die neue Richtlinie.

Schritt 5.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 5.5. Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 5.6. Wählen Sie Alle authentifizierten Benutzer aus.

Schritt 5.7: Klicken Sie auf Senden.

Schritt 5: Erstellen einer Zugriffsrichtlinie für verwaltete Geräte

Image - Zugriffsrichtlinie für verwaltete Geräte

Schritt 5.8. Klicken Sie auf der Seite Access Policies (Zugriffsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie.

Schritt 5.9. (Optional) Sie können jede

benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 5.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

Custom and External URL Category Filtering	
Category	Category Type
Allowed WiFi Access	Custom (Local)
Select Custom Categories...	

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
Adult	☐	☐	☐	☐	☐	☐
Advertisements	☐	☒	☒	☐	☐	☐
Alcohol	☐	☐	☒	☐	☐	☐
Arts	☐	☒	☐	☐	☐	☐
Astroslogy	☐	☐	☒	☐	☐	☐
Auctions	☐	☐	☒	☐	☐	☐
Business and Industry	☐	☐	☒	☐	☐	☐

Bild - URL-Filterung für Zugriffsrichtlinien für verwaltete Geräte

Schritt 5.11: Klicken Sie auf Senden.

Schritt 6: Erstellen einer Zugriffsrichtlinie für nicht verwaltete Geräte

Schritt 6.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Zugriffsrichtlinien.

Schritt 6.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 6.3. Enter Name für die neue Richtlinie.

Schritt 6.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 6.5. Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 6.6. Wählen Sie Gäste (Benutzer, die nicht authentifiziert werden konnten).

Schritt 6.7: Klicken Sie auf Senden.

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:

Protocols: 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

Image - Zugriffsrichtlinie für nicht verwaltete Geräte

Schritt 6.8. Klicken Sie auf der Seite Access Policies (Zugriffsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie.

Schritt 6.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 6.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

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	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Blocked WiFi Access	Custom (Local)	Select all	Select all	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	Block	Monitor	Warn	Quota-Based	Time-Based
Adult	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
Alcohol	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
Astronomy	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
Business and Industry	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

Bild - URL-Filterung für Zugriffsrichtlinien für nicht verwaltete Geräte

Schritt 6.11. Blättern Sie im Abschnitt Nicht kategorisierte URLs nach unten, und wählen Sie die gewünschte Aktion aus.

Bild - Zugriffsrichtlinien Nicht kategorisierte URLs



Tipp: Aus sicherheitstechnischer Sicht ist es am besten, die Aktion auf Blockieren festzulegen. Falls eine URL Zugriff benötigt, können Sie sie der Richtlinie zugewiesenen benutzerdefinierten URL-Kategorie hinzufügen.

Schritt 6.12. Klicken Sie auf Senden

Schritt 7: (Optional) Erstellen einer Cisco Datensicherheitsrichtlinie für verwaltete Geräte



Anmerkung: Wenn Sie den Upload-Datenverkehr nicht nach verwalteten Geräten filtern möchten, können Sie diesen Schritt überspringen.

Schritt 7.1: Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Cisco Data Security.

Schritt 7.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 7.3. EnterName für die neue Richtlinie.

Schritt 7.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 7.5. Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 7.6. Wählen Sie Alle authentifizierten Benutzer aus.

Schritt 7.7: Klicken Sie auf Senden.

Bild - Cisco Datensicherheitsrichtlinie für verwaltete Geräte

Schritt 7.8: Klicken Sie auf der Seite Cisco Data

Security Policies (Cisco Datensicherheitsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie.

Schritt 7.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 7.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

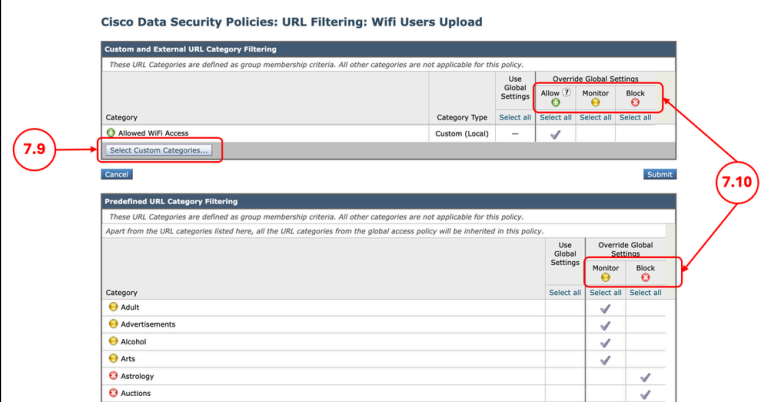


Image - Upload-Aktion für verwaltete Geräte

Schritt 7.11: Klicken Sie auf Senden.

Schritt 8: (Optional) Erstellen einer Cisco Datensicherheitsrichtlinie für nicht verwaltete Geräte

 Anmerkung: Wenn Sie den Upload-Datenverkehr nicht nach nicht verwalteten Geräten filtern möchten, können Sie diesen Schritt überspringen.

Schritt 8.1: Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Cisco Data Security.

Schritt 8.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 8.3. EnterName für die neue Richtlinie.

Schritt 8.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 8.5. Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 8.6. Wählen Sie Alle authentifizierten Benutzer aus.

Schritt 8.7: Klicken Sie auf Senden.

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 (?) ☒ Guests (users failing authentication)

Bild - Cisco Datensicherheitsrichtlinie für nicht verwaltete Geräte

Schritt 8.8: Klicken Sie auf der Seite Cisco Data Security Policies (Cisco Datensicherheitsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie.

Schritt 8.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 8.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

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	Use Global Settings	Override Global Settings
Allowed WiFi Access	Custom (Local)	☒	☐
Blocked WiFi Access	Custom (Local)	☒	☐

Predefined URL Category Filtering

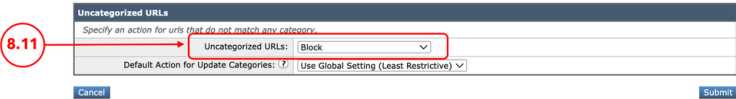
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

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
Adult	☒	☐
Advertisements	☒	☐
Alcohol	☒	☐
Arts	☒	☐
Astrology	☒	☐
Auctions	☒	☐

Image - Upload-Aktion für nicht verwaltete Geräte

Schritt 8.11. Blättern Sie im Abschnitt Nicht kategorisierte URLs nach unten, und wählen Sie die gewünschte Aktion aus.

	 Bild - Aktion für nicht kategorisierte URLs hochladen  Tipp: Aus sicherheitstechnischer Sicht ist es am besten, die Aktion auf Blockieren festzulegen. Falls eine URL Zugriff benötigt, können Sie sie der Richtlinie zugewiesenen benutzerdefinierten URL-Kategorie hinzufügen. Schritt 8.12: Klicken Sie auf Senden
Schritt 9: Speichern der Änderungen	Schritt 9.1. Bestätigen Sie die Änderungen.

Zugehörige Informationen

- [Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - LD \(begrenzte Bereitstellung\) - Fehlerbehebung...](#)
- [Download ausführbarer Dateien in SWA blockieren](#)
- [Upload-Verkehr in sicherer Web-Appliance blockieren](#)
- [Blockieren von Datenverkehr in einer sicheren Web-Appliance](#)
- [Umgehen der Authentifizierung in einer sicheren Web-Appliance](#)
- [Konfiguration der Microsoft O365 Tenant-Einschränkung in SWA](#)
- [Ersteinrichtung der sicheren Webappliance konfigurieren](#)
- [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.