

Configurer l'appliance Web sécurisée pour autoriser l'accès invité

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Présentation du scénario](#)

[Configuration Steps](#)

[Étape 1 : création du profil d'identification](#)

[Étape 2. \(Facultatif\) Créez les catégories d'URL personnalisées pour les URL autorisées et bloquées](#)

[Étape 3. Création d'une stratégie de déchiffrement pour les périphériques gérés](#)

[Étape 4. Création d'une stratégie de déchiffrement pour les périphériques non gérés](#)

[Étape 5. Création d'une politique d'accès pour les périphériques gérés](#)

[Étape 6. Création d'une stratégie d'accès pour les périphériques non gérés](#)

[Étape 7. \(Facultatif\) Créer une stratégie de sécurité des données Cisco pour les périphériques gérés](#)

[Étape 8. \(Facultatif\) Créer une stratégie de sécurité des données Cisco pour les périphériques non gérés](#)

[Étape 9. Enregistrement des modifications](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes à suivre pour permettre aux utilisateurs qui n'ont pas installé le certificat de déchiffrement d'accéder à Internet via l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SWA physique ou virtuel installé.
- Licence activée ou installée.
- L'Assistant de configuration est terminé.
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Présentation du scénario

Cet article traite d'un scénario de contrôle d'accès au réseau dans le sous-réseau Wi-Fi 10.10.10.0/24. L'environnement se compose de deux groupes d'utilisateurs distincts nécessitant des politiques de sécurité et d'accès différentes :

- Périphériques gérés : Ordinateurs portables de l'entreprise entièrement authentifiés et sur lesquels le certificat de déchiffrement SWA est installé. Ces périphériques sont fiables et généralement soumis aux politiques d'accès standard de l'entreprise.
- Périphériques non gérés/invités : Ordinateurs portables et périphériques mobiles personnels non authentifiés et ne disposant pas du certificat de déchiffrement SWA.

Objectif:

L'entreprise vise à mettre en oeuvre des politiques d'accès Web restrictives pour les périphériques non gérés, en limitant leur connectivité à un sous-ensemble spécifique d'URL autorisées tout en s'assurant que les ressources de l'entreprise restent sécurisées.

 Remarque : Comme le certificat de déchiffrement n'est pas approuvé sur les périphériques non gérés, vous ne pouvez pas déchiffrer le trafic HTTPS et l'action doit être définie pour passer.

Configuration Steps

Étape 1 : création du profil d'identification	Étape 1.1. Dans l'interface utilisateur graphique de SWA, accédez à Web Security Manager et sélectionnez Profil d'identification. Étape 1.2. Cliquez sur Add Identification Profile. Étape 1.3. Définissez un nom pour le profil. Étape 1.4. (Facultatif) Définissez la description. Étape 1.5. Choisissez Authenticate Users in Identification and Authentication. Étape 1.6. Choisissez le domaine Active Directory dans Sélectionner un domaine ou une séquence. Étape 1.7. Dans Sélectionner un schéma,
---	--

sélectionnez les protocoles d'authentification souhaités.

 Conseil : Ne choisissez pas Basic Authentication dans la liste Select a Scheme.

Étape 1.8. Activez la case à cocher des privilèges d'assistance invité.

Étape 1.9. (Facultatif) Selon votre conception, vous pouvez activer le substitut en activant l'option Appliquer les mêmes paramètres de substitution aux demandes de transfert explicites.

 Mise en garde : Puisque vous ne pouvez pas déchiffrer le trafic, dans le déploiement transparent ne sélectionnez pas Cookie persistant ou Cookie de session.

Étape 1.10. Définissez le sous-réseau d'adresses IP dans Define Members by Subnet.

Étape 1.11. Soumettre et valider les modifications

Image - Définir le profil d'identification

Étape 2. (Facultatif) Créez les catégories d'URL personnalisées pour les URL autorisées et bloquées

Étape 2.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Custom and External URL Categories.

Étape 2.2. Cliquez sur Ajouter une catégorie pour

créer une nouvelle catégorie d'URL personnalisée.

Étape 2.3.EnterName pour la nouvelle catégorie.

Étape 2.4.Définissez le domaine et/ou les sous-domaines des sites Web auxquels vous souhaitez bloquer l'accès.

Étape 2.5.Envoyez les modifications.

Étape 2.6. Utilisez les mêmes étapes pour créer une catégorie d'URL pour le site Web auquel vous autorisez l'accès.

The image displays two screenshots of the 'Custom and External URL Categories: Edit Category' web interface. Both screenshots show a form with fields for 'Category Name', 'Comments', 'List Order', 'Category Type', 'Sites', and 'Regular Expressions'. In the top screenshot, the 'Category Name' is 'Blocked WiFi Access' and the 'Sites' field contains 'example.com'. In the bottom screenshot, the 'Category Name' is 'Allowed WiFi Access' and the 'Sites' field contains 'cisco.com'. Red circles with numbers 2.3 and 2.4 are overlaid on the screenshots, pointing to the 'Category Name' and 'Sites' fields respectively. A 'Sort URLs' button is also visible in the bottom right of the 'Sites' field in both screenshots.

Image - Définir une catégorie d'URL personnalisée

Étape 3. Création d'une stratégie de déchiffrement pour les périphériques gérés

Étape 3.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Decryption Policies

Étape 3.2.Cliquez sur Add Policy.

Étape 3.3.EnterName pour la nouvelle stratégie.

Étape 3.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs.

Étape 3.5.Sélectionnez le profil d'identification créé à l'étape 1.

Étape 3.6. Sélectionnez Tous les utilisateurs authentifiés.

Étape 3.7. Cliquez sur Envoyer.

Decryption Policy: WiFi Users DP

Policy Settings

☒ Enable Policy

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

Description:

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

Identification Profile: WiFi IDP

Authorized Users and Groups

☒ All Authenticated Users

☐ Selected Groups and Users (7)
Groups: No groups entered
Users: No users entered

☐ Guests (users failing authentication)

Add Identification Profile

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

Créer une politique de déchiffrement pour les périphériques gérés

Étape 3.8. Dans la page Stratégies de décodage, cliquez sur le lien du filtrage des URL pour la nouvelle stratégie.

Étape 3.9. (Facultatif) Vous pouvez ajouter n'importe quelle catégorie d'URL personnalisée en cliquant sur Sélectionner des catégories personnalisées et en choisissant Inclure dans la stratégie devant les noms de catégorie

Étape 3.10. Configurez l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et pour chaque filtrage de catégorie d'URL prédéfinie.

Étape 3.11. Cliquez sur Submit

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	Select all	(Unavailable)	(Unavailable)

3.9

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							
Alcohol							
Arts							
Astrology							
Auctions							
Business and Industry							
Chat and Instant Messaging							

3.10

Image - Configurer l'action pour la stratégie de déchiffrement

Étape 4.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Decryption Policies

Étape 4.2.Cliquez sur Add Policy.

Étape 4.3.EnterName pour la nouvelle stratégie.

Étape 4.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs.

Étape 4.5.Sélectionnez le profil d'identification créé à l'étape 1.

Étape 4.6. Sélectionnez Invités (les utilisateurs ne s'authentifient pas).

Étape 4.7.Cliquez sur Envoyer.

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

☒ Guests (users failing authentication)

4.3

4.4

4.5

4.6

Créer une stratégie de déchiffrement pour les périphériques non gérés

Étape 4.8. Dans la page Stratégies de décodage, cliquez sur le lien du filtrage des URL pour la nouvelle stratégie.

Étape 4.9. (Facultatif) Vous pouvez ajouter n'importe quelle catégorie d'URL personnalisée en cliquant sur Sélectionner des catégories personnalisées et en choisissant Inclure dans la stratégie devant les noms de catégorie

Étape 4.10. Configurez l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et pour chaque filtrage de catégorie d'URL prédéfinie.



Remarque : N'utilisez pas Decrypt comme action, car le certificat de déchiffrement SWA n'est pas approuvé sur les périphériques non gérés.

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)

Cancel Submit

4.9

4.10

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					
		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)

Cancel Submit

Image - Action de déchiffrement pour les périphériques non gérés

Étape 4.11. Faites défiler la section des URL non classées vers le bas et choisissez l'action appropriée.

Uncategorized URLs

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

Uncategorized URLs: Drop

Default Action for Update Categories: Most Restrictive

Cancel Submit

4.11

Image - URL non classées



Conseil : Pour la perspective de la sécurité, il est préférable de définir l'action sur Drop, dans le cas où une URL a besoin d'un accès, vous



pouvez les ajouter dans la catégorie d'URL personnalisée assignée à la politique.

Étape 4.12. Cliquez sur Submit

Étape 5.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Access Policies

Étape 5.2. Cliquez sur Add Policy.

Étape 5.3. EnterName pour la nouvelle stratégie.

Étape 5.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs.

Étape 5.5. Sélectionnez le profil d'identification créé à l'étape 1.

Étape 5.6. Sélectionnez Tous les utilisateurs authentifiés.

Étape 5.7. Cliquez sur Envoyer.

Étape 5. Création d'une politique d'accès pour les périphériques gérés

Image - Stratégie d'accès pour les périphériques gérés

Étape 5.8. Dans la page Access Policies, cliquez sur le lien de filtrage URL pour la nouvelle stratégie.

Étape 5.9. (Facultatif) Vous pouvez ajouter n'importe quelle catégorie d'URL personnalisée en cliquant sur Sélectionner des catégories personnalisées et en

choisissant Inclure dans la stratégie devant les noms de catégorie

Étape 5.10. Configurez l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et pour chaque filtrage de catégorie d'URL prédéfinie.

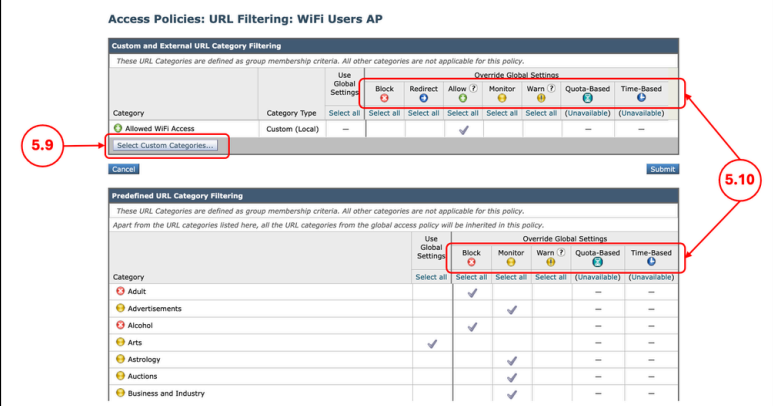


Image - Filtrage des URL de stratégie d'accès pour les périphériques gérés

Étape 5.11. Cliquez sur Submit.

Étape 6.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Access Policies

Étape 6.2.Cliquez sur Add Policy.

Étape 6.3.EnterName pour la nouvelle stratégie.

Étape 6.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs.

Étape 6.5.Sélectionnez le profil d'identification créé à l'étape 1.

Étape 6.6. Sélectionnez Invités (les utilisateurs ne s'authentifient pas).

Étape 6.7.Cliquez sur Envoyer.

Étape 6. Création d'une stratégie d'accès pour les périphériques non gérés

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 (?)

☒ 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

Schedulers: 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 - Stratégie d'accès pour les périphériques non gérés

Étape 6.8. Dans la page Access Policies, cliquez sur le lien de filtrage URL pour la nouvelle stratégie.

Étape 6.9. (Facultatif) Vous pouvez ajouter n'importe quelle catégorie d'URL personnalisée en cliquant sur Sélectionner des catégories personnalisées et en choisissant Inclure dans la stratégie devant les noms de catégorie

Étape 6.10. Configurez l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et pour chaque filtrage de catégorie d'URL prédéfinie.

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)

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	Block	Monitor	Warn (?)	Quota-Based	Time-Based
Adult	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Advertisements	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Alcohol	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Arts	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Astrology	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Auctions	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Business and Industry	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Chat and Instant Messaging	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Cancel Submit

Image - Filtrage des URL de stratégie d'accès pour les périphériques non gérés

Étape 6.11. Faites défiler la section des URL non classées vers le bas et choisissez l'action appropriée.

Image - URL non classées de stratégie d'accès

 **Conseil :** Pour la perspective de sécurité, il est préférable de définir l'action sur Block, dans le cas où une URL a besoin d'un accès, vous pouvez les ajouter dans la catégorie d'URL personnalisée assignée à la politique.

Étape 6.12. Cliquez sur Submit

Étape 7. (Facultatif) Création de la politique de sécurité des données Cisco pour les périphériques gérés

 **Remarque :** Si vous ne souhaitez pas filtrer le trafic de téléchargement pour les périphériques gérés, vous pouvez ignorer cette étape.

Étape 7.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Cisco Data Security.

Étape 7.2. Cliquez sur Add Policy.

Étape 7.3. EnterName pour la nouvelle stratégie.

Étape 7.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs.

Étape 7.5. Sélectionnez le profil d'identification créé à l'étape 1.

Étape 7.6. Sélectionnez Tous les utilisateurs authentifiés.

Étape 7.7. Cliquez sur Envoyer.

Image - Politique de sécurité des données Cisco pour les périphériques gérés

Étape 7.8. Dans la page Stratégies de sécurité des données Cisco, cliquez sur le lien du filtrage des URL pour la nouvelle stratégie.

Étape 7.9. (Facultatif) Vous pouvez ajouter n'importe quelle catégorie d'URL personnalisée en cliquant sur Sélectionner des catégories personnalisées et en choisissant Inclure dans la stratégie devant les noms de catégorie

Étape 7.10. Configurez l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et pour chaque filtrage de catégorie d'URL prédéfinie.

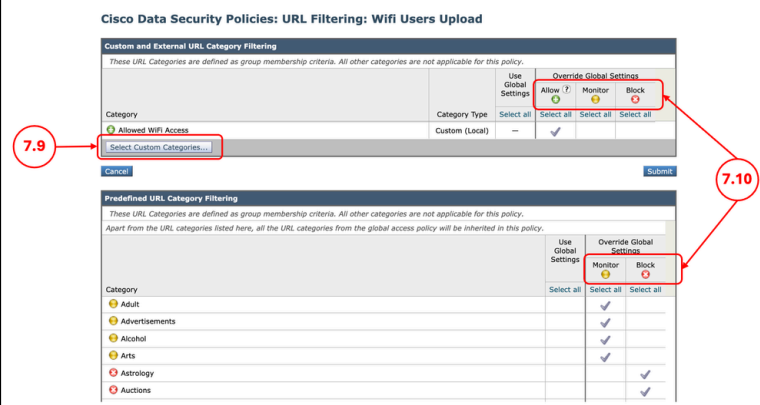


Image - Action de téléchargement pour les périphériques gérés

Étape 7.11. Cliquez sur Submit.

Étape 8. (Facultatif) Création d'une politique de sécurité des données Cisco pour les périphériques non gérés

 Remarque : Si vous ne souhaitez pas filtrer le trafic de téléchargement pour les périphériques non gérés, vous pouvez ignorer cette étape.

Étape 8.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Cisco Data Security.

Étape 8.2. Cliquez sur Add Policy.

Étape 8.3. EnterName pour la nouvelle stratégie.

Étape 8.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs.

Étape 8.5. Sélectionnez le profil d'identification créé à l'étape 1.

Étape 8.6. Sélectionnez Tous les utilisateurs authentifiés.

Étape 8.7. Cliquez sur Envoyer.

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)

[Advanced](#) Define additional group membership criteria.

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

Image - Politique de sécurité des données Cisco pour les périphériques non gérés

Étape 8.8. Dans la page Stratégies de sécurité des données Cisco, cliquez sur le lien du filtrage des URL pour la nouvelle stratégie.

Étape 8.9. (Facultatif) Vous pouvez ajouter n'importe quelle catégorie d'URL personnalisée en cliquant sur Sélectionner des catégories personnalisées et en choisissant Inclure dans la stratégie devant les noms de catégorie

Étape 8.10. Configurez l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et pour chaque filtrage de catégorie d'URL prédéfinie.

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
		Allow	Monitor
Allowed WiFi Access	Custom (Local)	☒	☐
Blocked WiFi Access	Custom (Local)	☐	☒

[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
	Monitor	Block
Adult	☐	☒
Advertisements	☐	☒
Alcohol	☐	☒
Arts	☐	☒
Astronomy	☐	☒
Auctions	☐	☒

Image - Action de téléchargement pour les périphériques non gérés

Étape 8.11. Faites défiler la section des URL non classées vers le bas et choisissez l'action appropriée.

Uncategorized URLs

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

Uncategorized URLs:

Default Action for Update Categories:

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

	Image - Action de téléchargement pour les URL non classées  Conseil : Pour la perspective de sécurité, il est préférable de définir l'action sur Block, dans le cas où une URL a besoin d'un accès, vous pouvez les ajouter dans la catégorie d'URL personnalisée assignée à la politique. Étape 8.12. Cliquez sur Submit
Étape 9. Enregistrement des modifications	Étape 9.1. Valider les modifications

Informations connexes

- [Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - LD \(Limited Deployment\) - Troubleshooti...](#)
- [Bloquer le téléchargement de fichiers exécutables dans SWA](#)
- [Bloquer le trafic de téléchargement dans l'appliance Web sécurisée](#)
- [Bloquer le trafic dans l'appliance Web sécurisée](#)
- [Contourner l'authentification dans l'appliance Web sécurisée](#)
- [Configurer la restriction du service partagé Microsoft O365 dans SWA](#)
- [Configuration initiale de Secure Web Appliance](#)
- [Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.