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

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Présentation du scénario

- Objectif

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. Enregistrer les modifications

Autres informations utiles

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 :

- Un SWA physique ou virtuel est installé.

- Une licence est 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.

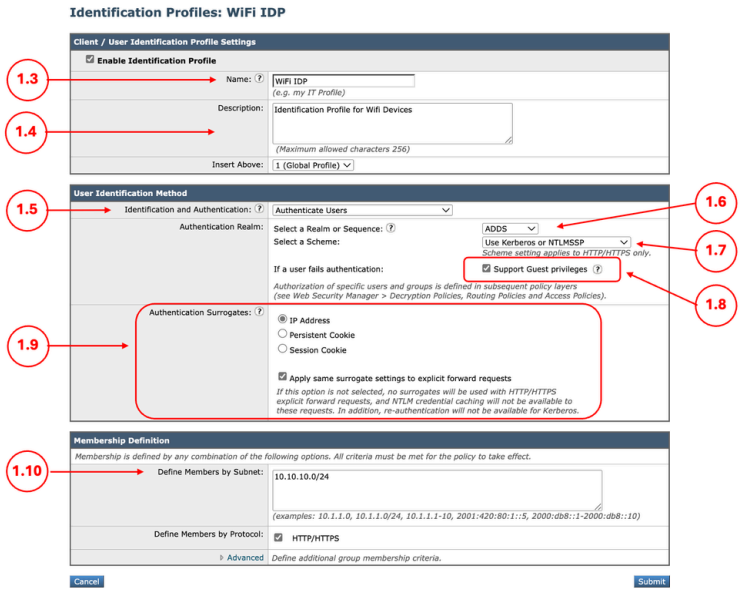
Objectif

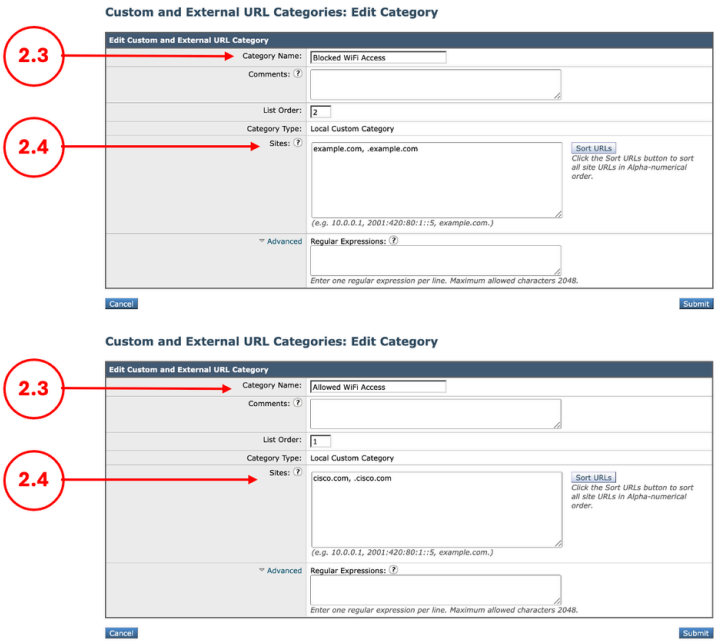
L'entreprise vise à mettre en oeuvre des politiques d'accès Web restrictives pour les périphériques non gérés, en limitant leur connectivité à un sous-ensemble spécifique d'URL autorisées tout en s'assurant que les ressources de l'entreprise restent sécurisées.

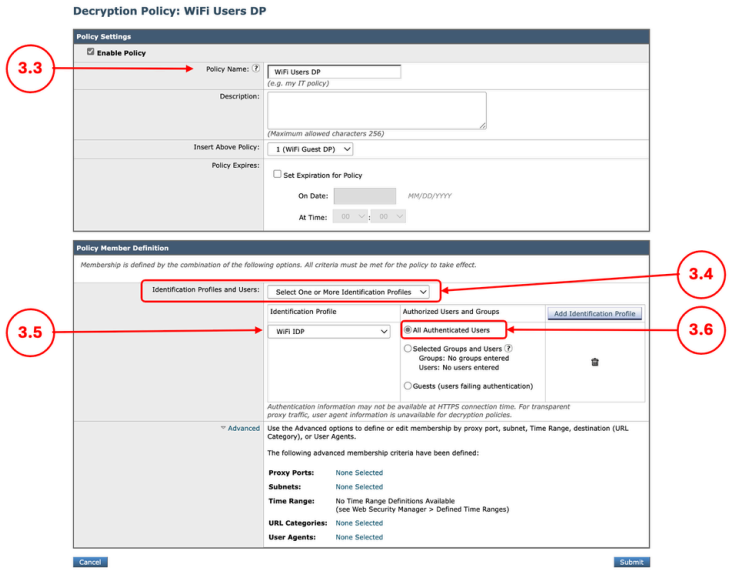
Remarque : Comme le certificat de déchiffrement n'est pas approuvé sur les périphériques non gérés, vous ne pouvez pas déchiffrer le trafic HTTPS et l'action doit être définie pour passer.

Configuration Steps

Étape 1 : création du profil d'identification	1.1. Dans l'interface utilisateur graphique de SWA, accédez à Web Security Manager et sélectionnez Profil d'identification. 1.2. Cliquez sur Add Identification Profile. 1.3. Définir un nom pour le profil. 1.4. (Facultatif) Définissez la description. 1.5. Choisissez Authenticate Users in Identification and Authentication. 1.6. Choisissez le domaine Active Directory dans Sélectionner un domaine ou une séquence. 1.7. Dans Select a Scheme, sélectionnez les protocoles d'authentification souhaités.  Conseil : Ne choisissez pas Basic Authentication dans la liste Select a Scheme. 1.8. Cochez la case des privilèges d'assistance invité. 1.9. (Facultatif) En fonction de votre conception, vous pouvez activer la substitution en activant l'option Appliquer les mêmes paramètres de substitution aux demandes de transfert explicites.  Mise en garde : Comme vous ne pouvez pas déchiffrer le trafic, dans le déploiement transparent ne sélectionnez pas Cookie persistant ou Cookie de session. 1.10. Définissez le sous-réseau d'adresses IP dans, Définir les membres par sous-réseau. 1.11.Envoyer 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	2.1. Dans l'interface graphique, accédez à Web Security Manager et sélectionnez Custom and External URL Categories. 2.2. Cliquez sur Ajouter une catégorie pour créer une nouvelle catégorie d'URL personnalisée. 2.3. Saisissez le nom de la nouvelle catégorie. 2.4. Définissez le domaine et/ou les sous-domaines des sites Web auxquels vous souhaitez bloquer l'accès. 2.5. Soumettre les modifications. 2.6. Suivez les mêmes étapes pour créer une catégorie d'URL pour le site Web auquel vous autorisez l'accès.

	 Image - Définir une catégorie d'URL personnalisée
Étape 3. Création d’une stratégie de déchiffrement pour les périphériques gérés	3.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Decryption Policies 3.2. Cliquez sur Add Policy. 3.3. Saisissez le nom de la nouvelle stratégie. 3.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs. 3.5. Sélectionnez le profil d'identification créé à l'étape 1. 3.6. Sélectionnez Tous les utilisateurs authentifiés. 3.7. Cliquez sur Envoyer.



Créer une politique de déchiffrement pour les périphériques gérés

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

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

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

3.11. Cliquez sur Envoyer

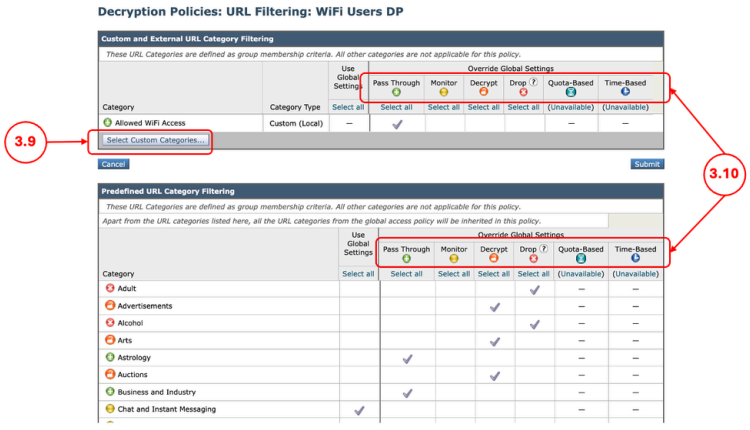
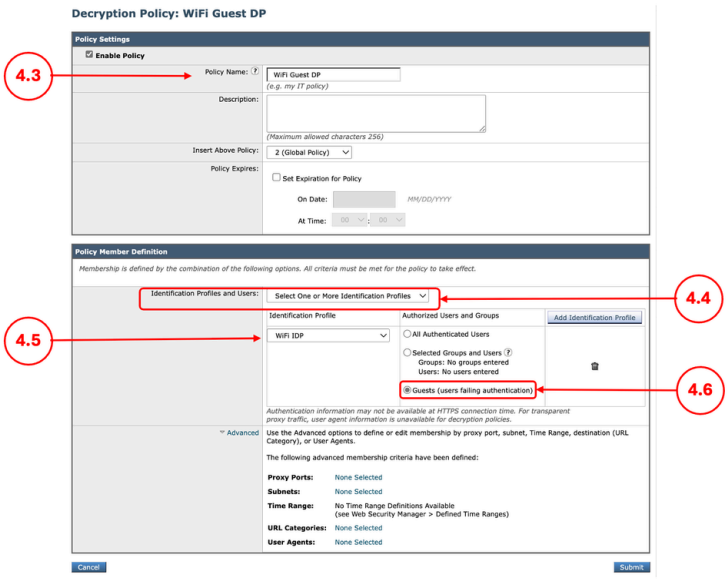
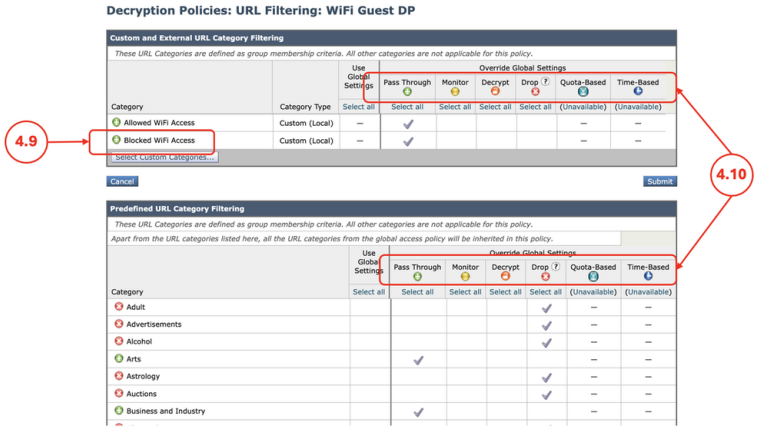


Image - Configurer l'action pour la stratégie de déchiffrement

Étape 4. Création d’une stratégie de déchiffrement pour les périphériques non gérés	4.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Decryption Policies 4.2. Cliquez sur Add Policy. 4.3. Entrez le nom de la nouvelle stratégie. 4.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs. 4.5. Sélectionnez le profil d'identification créé à l'étape 1. 4.6. Sélectionnez Invités (les utilisateurs ne s’authentifient pas). 4.7. Cliquez sur Submit.  Créer une stratégie de déchiffrement pour les périphériques non gérés 4.8. Dans la page Stratégies de décodage, cliquez sur le lien Filtrage des URL pour la nouvelle stratégie de la nouvelle stratégie. 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 4.10. Configurer l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et 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.  Image - Action de déchiffrement pour les périphériques non gérés 4.11. Faites défiler la page jusqu'à la section Uncategory URLs et choisissez l'action appropriée.  Image - URL non classées Conseil : Pour la perspective de sécurité, il est préférable de définir l'action sur Drop. Si une URL nécessite un accès, vous pouvez l'ajouter dans la catégorie d'URL personnalisée attribuée à la stratégie. 4.12. Cliquez sur Envoyer.
Étape 5. Création d'une politique d'accès pour les périphériques gérés	5.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Access Policies 5.2. Cliquez sur Add Policy. 5.3. Saisissez le nom de la nouvelle stratégie. 5.4. Choisissez Sélectionner un ou plusieurs profils

d'identification dans le menu déroulant Profils d'identification et utilisateurs.

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

5.6. Sélectionnez Tous les utilisateurs authentifiés.

5.7. Cliquez sur Envoyer.

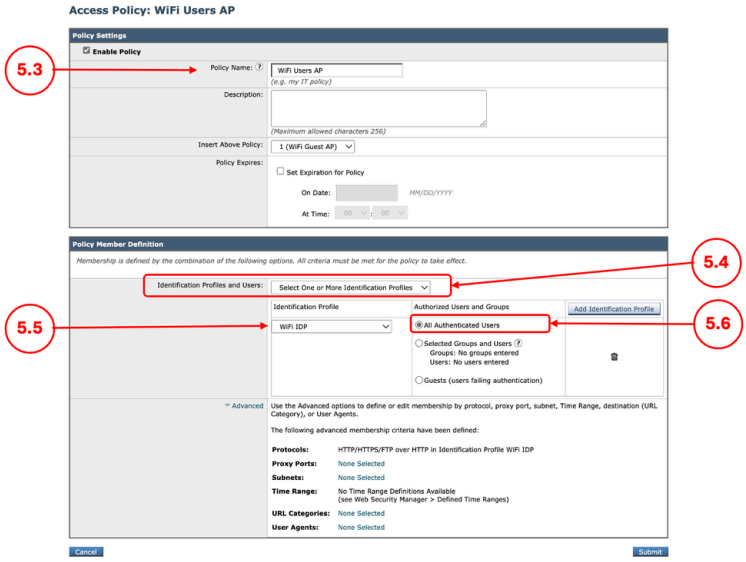
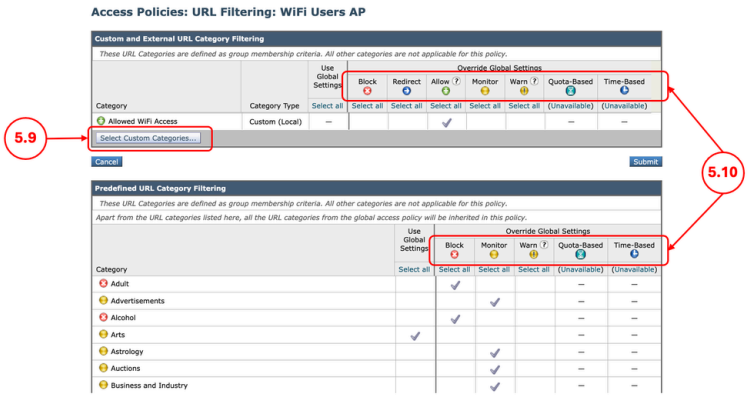


Image - Stratégie d'accès pour les périphériques gérés

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

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

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

	 Image - Filtrage des URL de stratégie d'accès pour les périphériques gérés 5.11. Cliquez sur Envoyer.
Étape 6. Création d’une stratégie d’accès pour les périphériques non gérés	6.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Access Policies 6.2. Cliquez sur Add Policy. 6.3. Saisissez le nom de la nouvelle stratégie. 6.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs. 6.5. Sélectionnez le profil d'identification créé à l'étape 1. 6.6. Sélectionnez Invités (les utilisateurs ne s'authentifient pas). 6.7. Cliquez sur Submit.

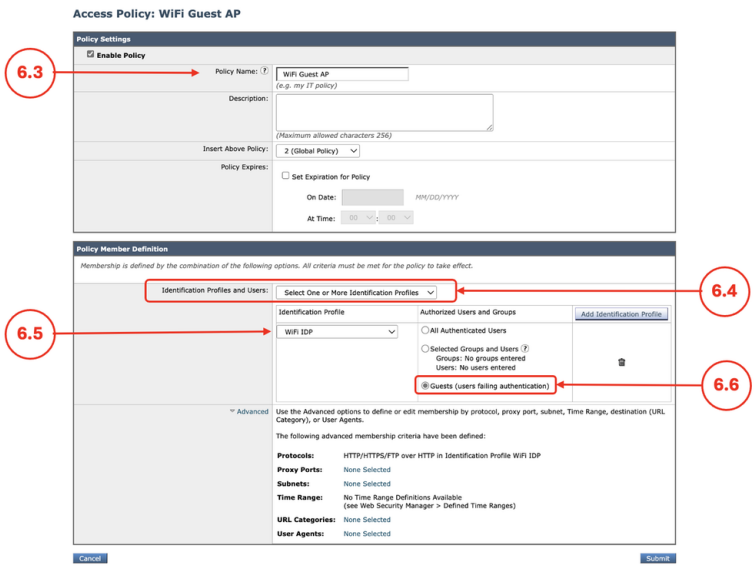


Image - Stratégie d'accès pour les périphériques non gérés

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

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

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

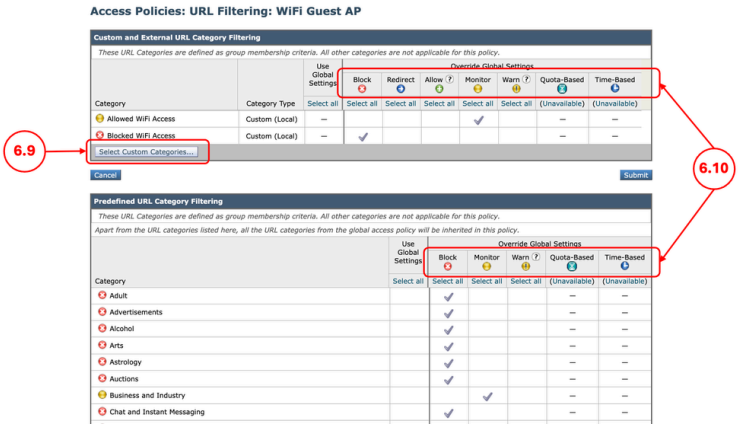


Image - Filtrage des URL de stratégie d'accès pour les périphériques non gérés

6.11. Faites défiler la section des URL non classées pour choisir l'action appropriée.



Image - URL non classées de stratégie d'accès

Conseil : Pour la sécurité, il est préférable de définir l'action sur Bloquer. Si une URL nécessite un accès, vous pouvez l'ajouter dans la catégorie d'URL personnalisée attribuée à la stratégie.

6.12. Cliquez sur Envoyer

Étape 7. (Facultatif) Créer une stratégie 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.

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

7.2. Cliquez sur Add Policy.

7.3. Entrez le nom de la nouvelle stratégie.

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

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

7.6. Sélectionner tous les utilisateurs authentifiés.

7.7. Cliquez sur Submit.

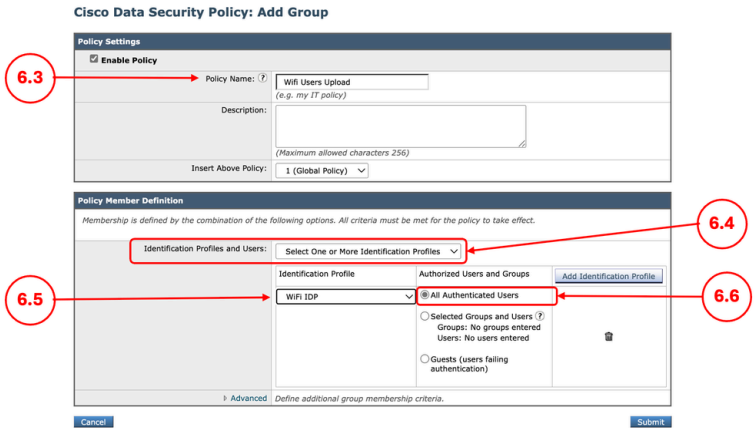


Image - Politique de sécurité des données Cisco pour les périphériques gérés

	7.8. Dans la page Cisco Data Security Policies, cliquez sur le lien URL Filtering pour la nouvelle stratégie. 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 7.10. Configurer l'action pour chaque filtrage de catégorie d'URL personnalisée et externe et chaque filtrage de catégorie d'URL prédéfinie.  Image - Action de téléchargement pour les périphériques gérés 7.11. Cliquez sur Envoyer.
Étape 8. (Facultatif) Créer une stratégie 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.	8.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et sélectionnez Cisco Data Security. 8.2. Cliquez sur Add Policy. 8.3. Entrez le nom de la nouvelle stratégie. 8.4. Choisissez Sélectionner un ou plusieurs profils d'identification dans le menu déroulant Profils d'identification et utilisateurs. 8.5. Sélectionnez le profil d'identification créé à l'étape 1. 8.6. Sélectionner tous les utilisateurs authentifiés. 8.7. Cliquez sur Submit.

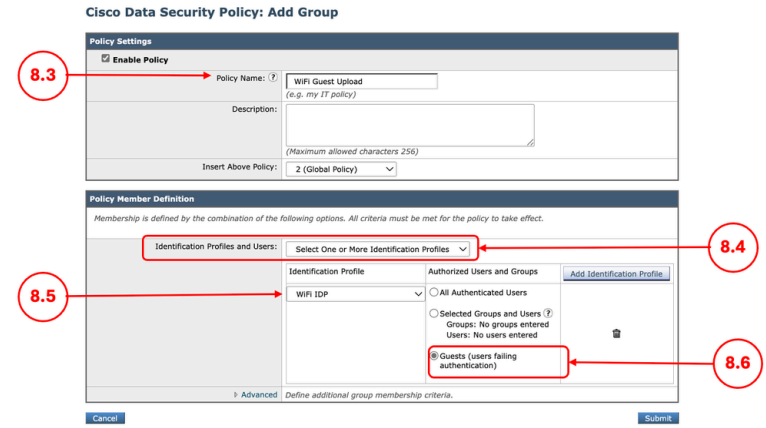


Image - Politique de sécurité des données Cisco pour les périphériques non gérés

8.8. Dans la page Cisco Data Security Policies, cliquez sur le lien URL Filtering pour la nouvelle stratégie.

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

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

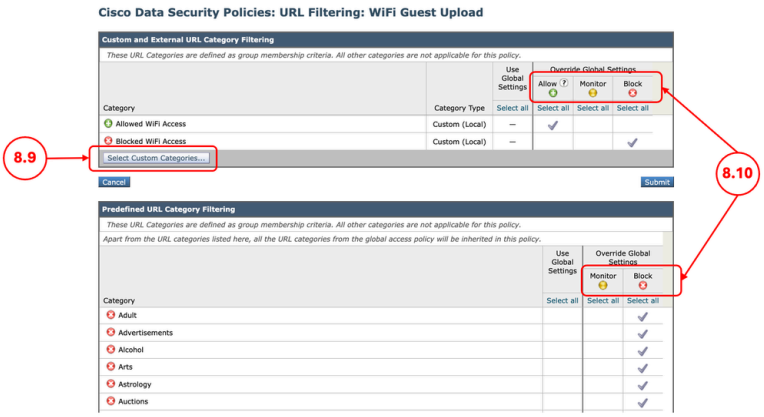


Image - Action de téléchargement pour les périphériques non gérés

8.11. Faites défiler la section des URL non classées pour choisir l'action appropriée.

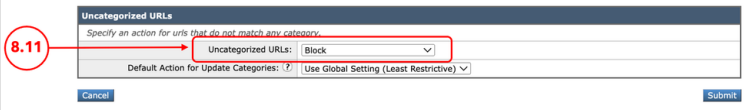


	Image - Action de téléchargement pour les URL non classées Conseil : Pour la sécurité, il est préférable de définir l'action sur Bloquer. Si une URL nécessite un accès, vous pouvez l'ajouter dans la catégorie d'URL personnalisée attribuée à la stratégie. 8.12. Cliquez sur Envoyer
Étape 9. Enregistrer les modifications	9.1. Valider les modifications

Autres informations utiles

- 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.