Exemple de configuration de l'authentification Web locale du portail invité Identity Services Engine

Contenu

Introduction

Ce document décrit comment configurer l'authentification Web locale (LWA) avec le portail invité Cisco Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Contrôleur LAN sans fil Cisco (WLC)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ISE version 1.4
- WLC version 7.4

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Ce document décrit la configuration de LWA. Cependant, Cisco vous recommande d'utiliser l'authentification Web centralisée (CWA) avec l'ISE dans la mesure du possible. Il y a quelques scénarios où LWA est préférable ou la seule option, c'est donc un exemple de configuration pour ces scénarios.

Configuration

LWA nécessite certaines conditions préalables et une configuration majeure sur le WLC ainsi que quelques modifications nécessaires sur l'ISE.

Avant de les aborder, voici un aperçu du processus LWA avec l'ISE.

Processus LWA avec le portail ISE Guest Portal

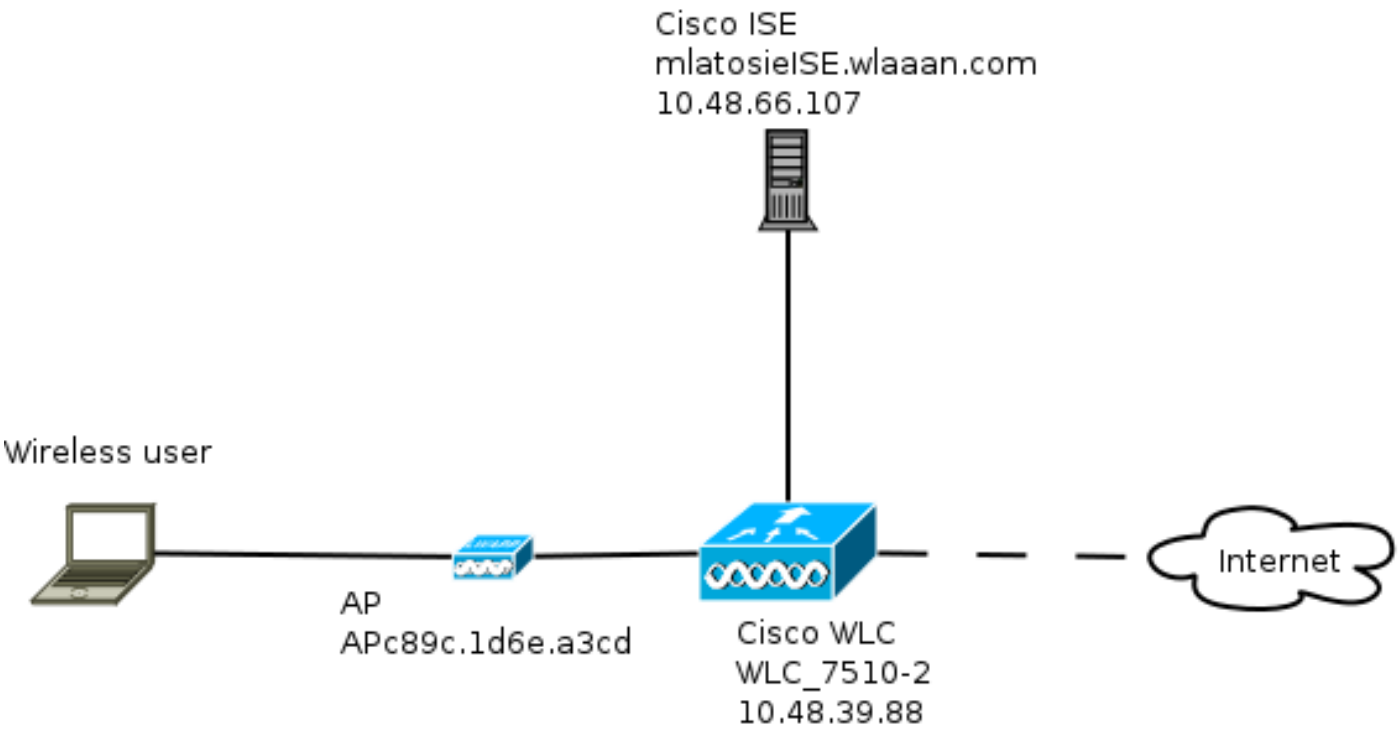
1. Le navigateur essaie de récupérer une page Web.
2. Le WLC intercepte la requête HTTP(S) et la redirige vers l'ISE.
   Plusieurs informations clés sont stockées dans cet en-tête de redirection HTTP. Voici un exemple de l'URL de redirection :
   https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9#&ui-state=dialog?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
   À partir de l'exemple d'URL, vous pouvez voir que l'utilisateur a essayé d'atteindre « yahoo.com. » L'URL contient également des informations sur le nom du réseau local sans fil (WLAN) (mlatosie_LWA) et les adresses MAC du client et du point d'accès (AP). Dans l'exemple d'URL, **1.1.1.1** est le WLC et **mlatosieise.wlaaan.com** est le serveur ISE.
3. La page de connexion de l'invité ISE s'affiche et le nom d'utilisateur et le mot de passe sont saisis.
4. L'ISE effectue l'authentification par rapport à sa séquence d'identité configurée.
5. Le navigateur redirige à nouveau. Cette fois-ci, il envoie des informations d'identification au WLC. Le navigateur fournit le nom d'utilisateur et le mot de passe que l'utilisateur a entrés dans l'ISE sans aucune interaction supplémentaire de la part de l'utilisateur. Voici un exemple de requête GET au WLC.
   GET
   /login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0

Encore une fois, l'URL d'origine (**yahoo.com**), le nom d'utilisateur (**mlatosie@cisco.com**) et le mot de passe (**ityh**) sont inclus.
Note: Bien que l'URL soit visible ici, la demande réelle est soumise via SSL (Secure Sockets Layer), qui est indiqué par HTTPS, et est difficile à intercepter.

6. Le WLC utilise RADIUS afin d'authentifier ce nom d'utilisateur et ce mot de passe par rapport à l'ISE et autorise l'accès.
7. L'utilisateur est redirigé vers le portail spécifié. Référez-vous à la section "**Configurer ISE externe comme URL de webauth »** de ce document pour plus d'informations.

Diagramme du réseau

Cette figure décrit la topologie logique des périphériques utilisés dans cet exemple.



Prérequis pour la configuration

Pour que le processus LWA fonctionne correctement, un client doit pouvoir obtenir les éléments suivants :

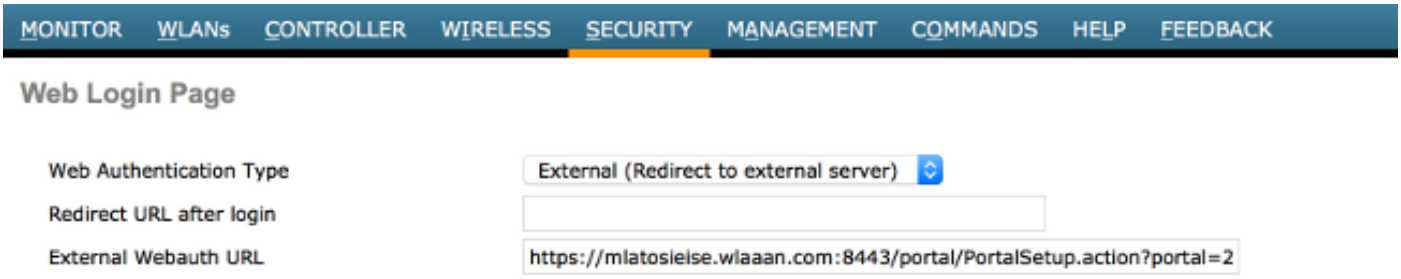
- Configuration de l'adresse IP et du masque de réseau
- Route par défaut
- Serveur DNS (Domain Name System)

Tous ces éléments peuvent être fournis avec DHCP ou la configuration locale. La résolution DNS doit fonctionner correctement pour que le LWA fonctionne.

Configurer le WLC

Configurer l'ISE externe en tant qu'URL Webauth globalement

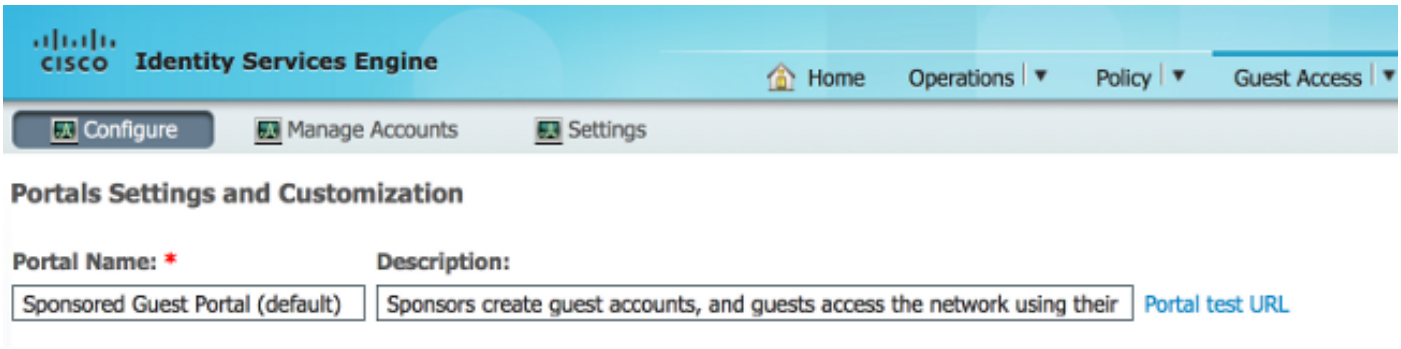
Sous **Sécurité > Authentification Web > Page de connexion Web**, vous pouvez accéder à ces informations.



Note: Cet exemple utilise une URL Webauth externe et provient de ISE version 1.4. Si vous avez une version différente, consultez le guide de configuration afin de comprendre ce qui doit être configuré.

Il est également possible de configurer ce paramètre par WLAN. Il se trouve ensuite dans les paramètres de sécurité WLAN spécifiques. Celles-ci remplacent le paramètre global.

Afin de trouver l'URL correcte pour votre portail spécifique, choisissez **ISE > Guest Policy > Configure > votre portail spécifique**. Cliquez avec le bouton droit de la souris sur le lien à partir de l'URL de test du portail et choisissez l'**emplacement du lien de copie**.



Dans cet exemple, l'URL complète est : https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9

Configurer les listes de contrôle d'accès (ACL)

Pour que l'authentification Web fonctionne, le trafic autorisé doit être défini. Déterminez si des listes de contrôle d'accès FlexConnect ou normales doivent être utilisées. Les points d'accès FlexConnect utilisent des listes de contrôle d'accès FlexConnect, tandis que les points d'accès qui utilisent la commutation centralisée utilisent des listes de contrôle d'accès normales.

Afin de comprendre dans quel mode fonctionne un point d'accès particulier, **sans fil > points d'accès** et choisissez le **nom du point d'accès > Mode AP** dans la liste déroulante. Un déploiement type est **local** ou **FlexConnect**.

Sous **Sécurité > Listes de contrôle d'accès,** choisissez **Listes de contrôle d'accès FlexConnect** ou **Listes de contrôle d'accès**.Dans cet exemple, tout le trafic UDP a été autorisé afin d'autoriser spécifiquement l'échange DNS et le trafic vers l'ISE (10.48.66.107).

General

Access List Name FLEX_GUEST

Deny Counters 634752

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	Any	Any	Any	208398
2	Permit	10.48.66.107 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	32155
3	Permit	0.0.0.0 / 0.0.0.0	10.48.66.107 / 255.255.255.255	TCP	Any	Any	Any	Any	24532

Cet exemple utilise FlexConnect, de sorte que FlexConnect et les listes de contrôle d'accès standard sont définis.

Ce comportement est documenté dans l'ID de bogue Cisco CSCue68065 en ce qui concerne les contrôleurs WLC 7.4. Il n'est plus nécessaire sur WLC 7.5 où vous n'avez besoin que d'une FlexACL et plus d'une ACL standard

Configurer le SSID (Service Set Identifier) pour LWA

Sous **WLAN,** sélectionnez l'**ID WLAN** à modifier.

Configuration de l'authentification Web

Appliquez les mêmes listes de contrôle d'accès que celles définies à l'étape précédente et activez l'authentification Web.

WLANs > Edit 'mlatosie_LWA'

General | Security | QoS | Advanced

Layer 2 | Layer 3 | AAA Servers

Layer 3 Security None

Web Policy

Authentication

Passthrough

Conditional Web Redirect

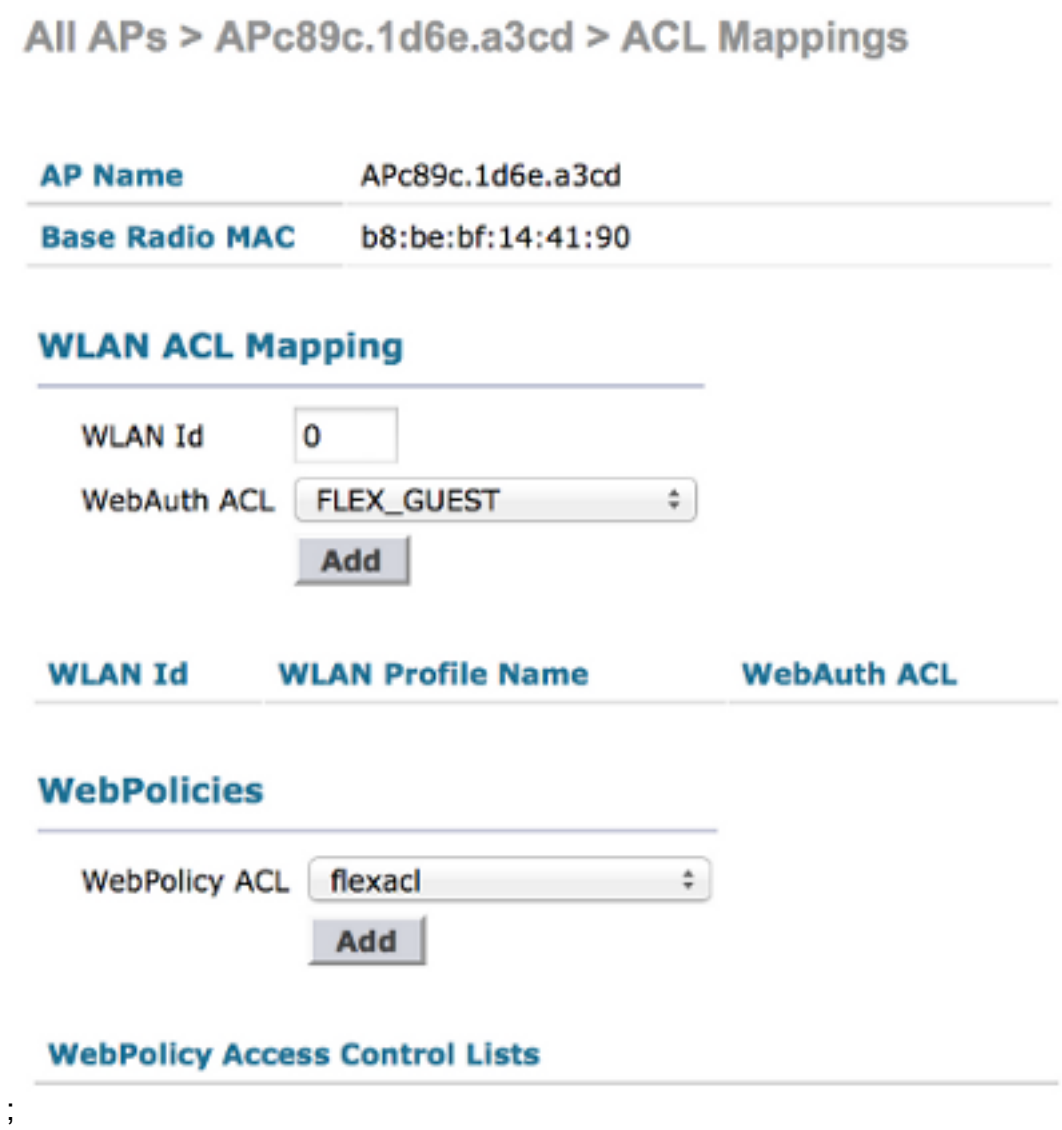
Splash Page Web Redirect

On MAC Filter failure[10]

Preauthentication ACL IPv4 FLEX_GUEST IPv6 None WebAuth FlexAcl FLEX_GUEST

Over-ride Global Config Enable

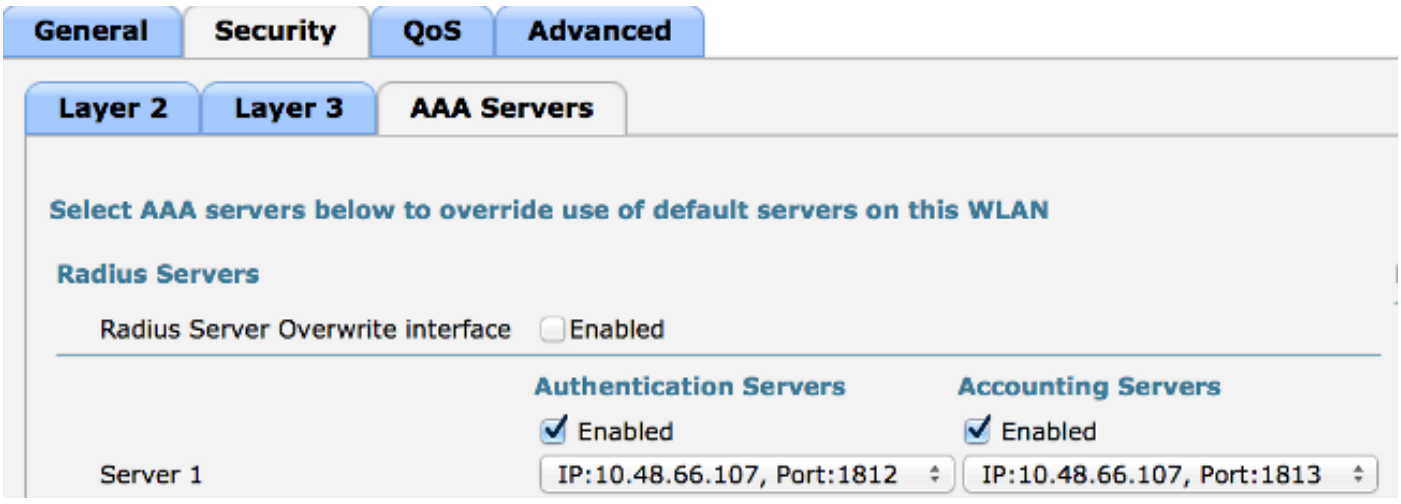
Note: Si la fonctionnalité de commutation locale de FlexConnect est utilisée, le mappage des listes de contrôle d'accès doit être ajouté au niveau du point d'accès. Vous pouvez le trouver sous **Wireless > Access Points.** Choisissez le **nom** approprié **AP > FlexConnect > External WebAuthentication ACL**.



;

Configuration du serveur AAA (Authentication, Authorization and Accounting)

Dans cet exemple, les serveurs d'authentification et de comptabilité pointent vers le serveur ISE précédemment défini.



Note: Les valeurs par défaut de l'onglet **Avancé** ne doivent pas être ajoutées.

Configurer ISE

La configuration ISE se compose de plusieurs étapes.

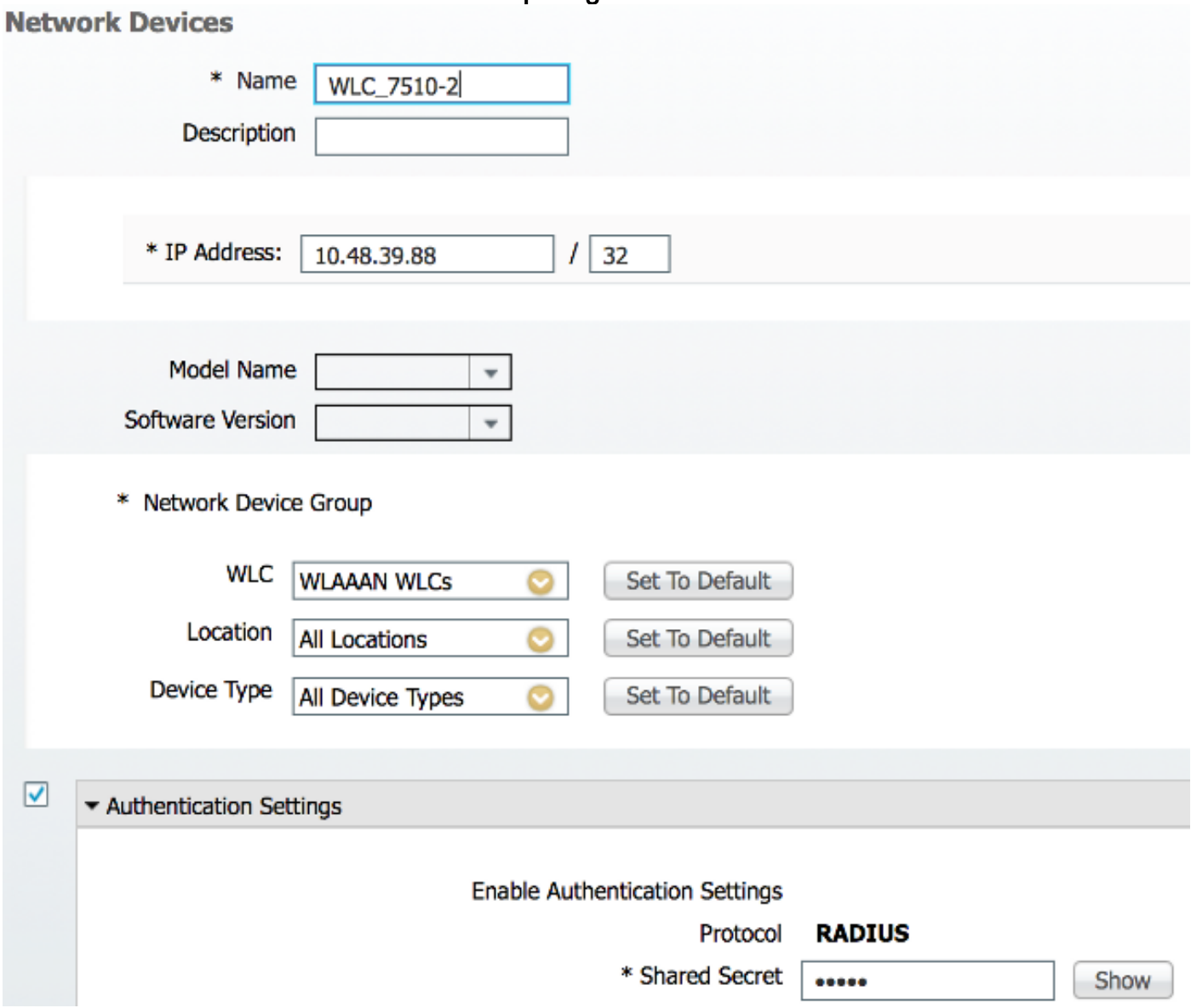
Définissez d'abord le périphérique en tant que périphérique réseau.

Ensuite, assurez-vous que les règles d'authentification et d'autorisation qui prennent en charge cet échange existent.

Définir le périphérique réseau

Sous **Administration > Network Resources > Network Devices**, renseignez les champs suivants :

- Nom du périphérique
- Adresse IP du périphérique
- **Paramètres d'authentification > Secret partagé**

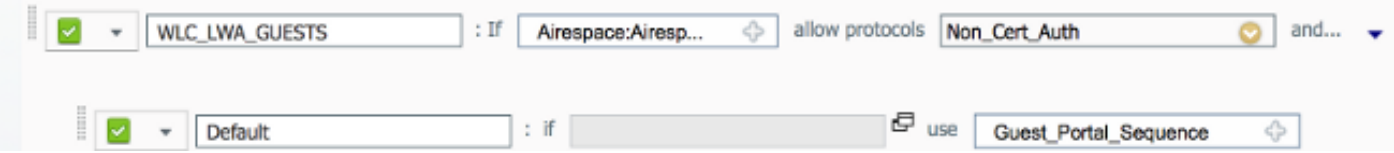


Configurer la stratégie d'authentification

Sous **Policy > Authentication**, ajoutez une nouvelle stratégie d'authentification.

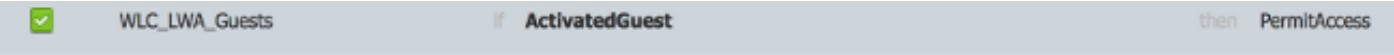
Cet exemple utilise les paramètres suivants :

- Name : **WLC_LWA_Invités**
- Condition : **Airespace : Airespace-Wlan-Id.** Cette condition correspond à l'ID WLAN de 3, qui est l'ID du WLAN **mlatosie_LWA** précédemment défini sur le WLC.
- {facultatif} Il autorise les protocoles d'authentification qui ne nécessitent pas le certificat **Non_Cert_Auth**, mais les valeurs par défaut peuvent être utilisées.
- Guest_Portal_Sequence, qui définit que les utilisateurs sont des utilisateurs invités définis localement.



Configurer la stratégie et le résultat d'autorisation

Sous **Stratégie > Autorisation,** définissez une nouvelle stratégie. Il peut s'agir d'une politique de base, telle que :

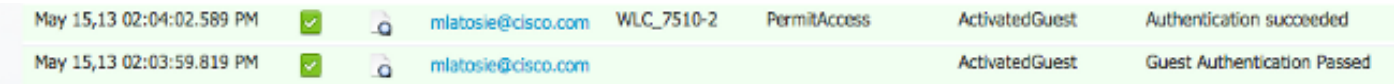


Cette configuration dépend de la configuration globale de l'ISE. Cet exemple est volontairement simplifié.

Vérification

Sur ISE, les administrateurs peuvent surveiller et dépanner les sessions en direct sous **Operations > Authentications**.

Deux authentifications doivent être vues. La première authentification provient du portail invité de l'ISE. La deuxième authentification est fournie sous la forme d'une demande d'accès du WLC à l'ISE.



Vous pouvez cliquer sur l'icône **Rapport détaillé d'authentification** afin de vérifier quelles stratégies d'autorisation et d'authentification ont été sélectionnées.

Sur le WLC, un administrateur peut surveiller les clients sous **Monitor > Client**.

Voici un exemple de client qui s'est authentifié correctement :

Dépannage

Cisco vous recommande d'exécuter des débogages par le biais du client autant que possible.

Grâce à l'interface de ligne de commande, ces débogages fournissent des informations utiles :

```
debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

Informations connexes

- Guide de configuration de Cisco ISE 1.x
- Guide de configuration de Cisco WLC 7.x
- Support et documentation techniques - Cisco Systems