Exemple local portail de configuration d'authentification Web d'invité de Cisco Identity Services Engine

ID de document : 116217

Mis à jour : Nov. 25, 2015

Contribué par Marcin Latosiewicz et Nicolas Darchis, ingénieurs TAC Cisco.

PDF de téléchargement
Copie
Commentaires

Produits connexes

- Réseau local sans fil (WLAN)
- Logiciel Cisco Identity Services Engine

Contenu

[Informations connexes](#)
[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

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

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Contrôleur LAN Sans fil de Cisco (WLC)

[Composants utilisés](#)

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

- Version 1.4 ISE
- Version 7.4 WLC

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Informations générales](#)

Ce document décrit la configuration de LWA. Cependant, Cisco recommande que vous utilisiez l'authentification Web centralisée (CWA) avec l'ISE autant que possible. Il y a quelques scénarios où LWA est préféré ou la seule option, ainsi c'est un exemple de configuration pour ces scénarios.

Configurez

LWA exige certains prerequirements et une configuration importante sur le WLC aussi bien que quelques modifications requis sur l'ISE.

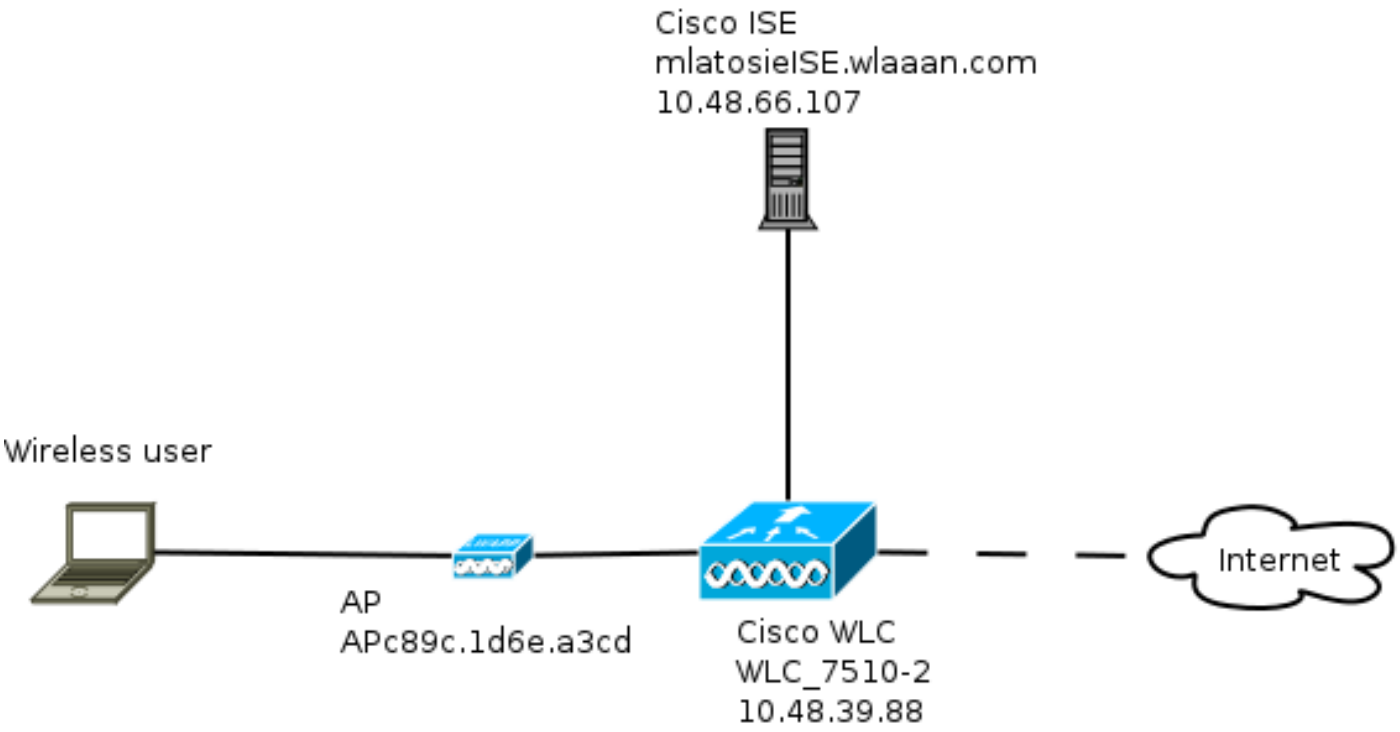
Avant que ceux soient couverts, voici un contour du processus LWA avec l'ISE.

Processus LWA avec le portail d'invité ISE

1. Les essais de navigateur pour chercher une page Web.
2. Le WLC intercepte la demande de HTTPS et la réoriente à l'ISE.
   Plusieurs les informations principales sont enregistrés du fait le HTTP réorientent l'en-tête.
   Voici un exemple de l'URL de réorientation :
   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/
   De l'URL d'exemple, vous pouvez voir que l'utilisateur jugé pour atteindre « yahoo.com. » L'URL contient également des informations sur le nom du réseau local sans fil (WLAN) (mlatosie_LWA), et les adresses MAC de client et de Point d'accès (AP). Dans l'URL d'exemple, 1.1.1.1 **est les** WLC, et mlatosieise.wlaaan.com **est le** serveur ISE.
3. L'utilisateur est présenté avec la page de connexion d'invité ISE et écrit le nom d'utilisateur et mot de passe.
4. L'ISE exécute l'authentification contre son ordre configuré d'identité.
5. Le navigateur réoriente de nouveau. Cette fois, il soumet des qualifications au WLC. Le navigateur fournit le nom d'utilisateur et mot de passe que l'utilisateur a écrit dans l'ISE sans n'importe quelle interaction supplémentaire de l'utilisateur. Voici une demande GET d'exemple au WLC.
   OBTENEZ
   /login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
   De nouveau, tous l'URL d'original (**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 au-dessus de Secure Sockets Layer (SSL), qui est indiqué par HTTPS, et est difficile d'intercepter.
6. Le WLC emploie RADIUS afin d'authentifier que nom d'utilisateur et mot de passe contre l'ISE et permet l'accès.
7. L'utilisateur est réorienté au portail spécifié. Référez-vous « **configurent ISE externe à la** section **comme de webauth URL » de** ce pour en savoir plus de document.

Diagramme du réseau

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



Conditions préalables à la configuration

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

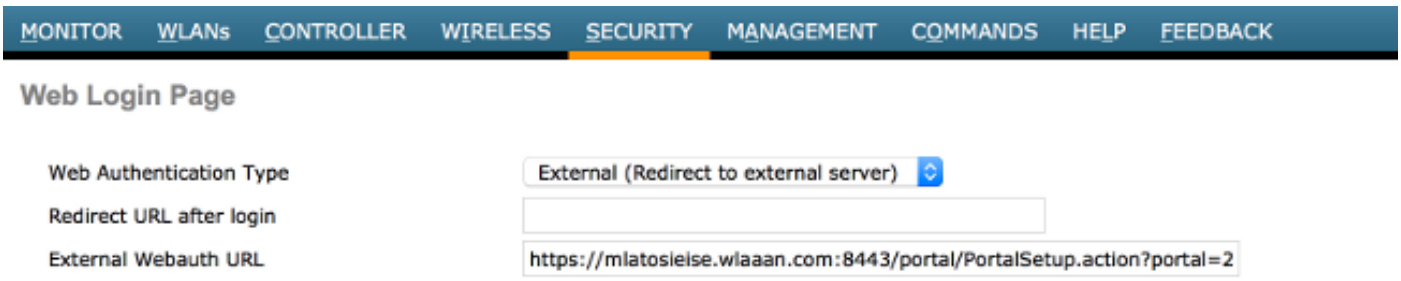
- Adresse IP et configuration de netmask
- Default route
- Serveur de Système de noms de domaine (DNS)

Toute la ces derniers peut être équipée de DHCP ou de configuration locale. La résolution de DN doit fonctionner correctement pour que le LWA fonctionne.

Configurez le WLC

Configurez l'ISE externe comme URL de Webauth globalement

Sous la **Sécurité > le Web authentiques > page Web Login**, vous pouvez accéder à ces informations.

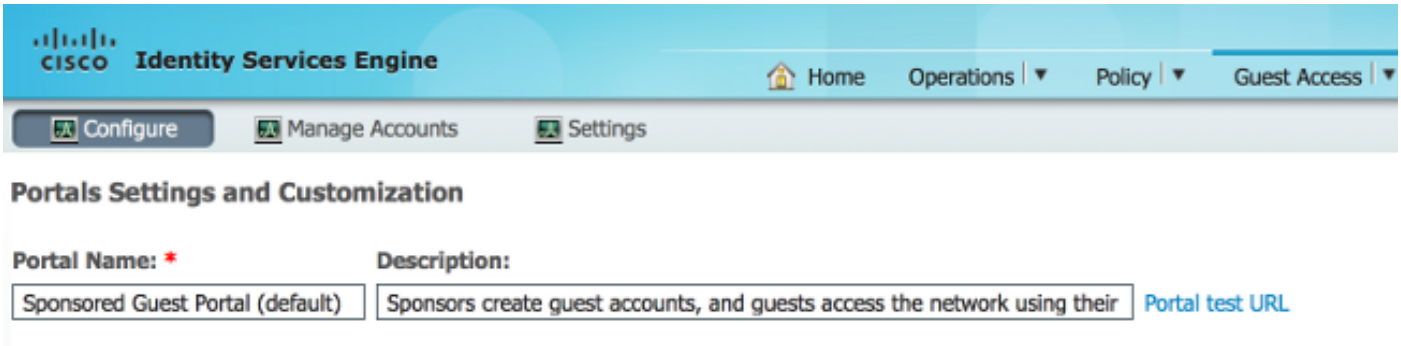


Note: Cet exemple utilise un URL externe de Webauth et a été pris de la version 1.4 ISE. Si vous avez une différente version, consultez le guide de configuration afin de comprendre ce

qui devrait être configuré.

Il est également possible de configurer ce par-WLAN de établissement. Il est alors dans les configurations spécifiques de Sécurité WLAN. Ceux ignorent le paramètre général.

Afin de découvrir l'URL correct pour votre portail spécifique, choisissez **ISE > stratégie d'invité > configurent > votre portail de particularité**. Cliquez avec le bouton droit le lien « de l'URL portail de test » et choisissez l'**emplacement de lien de copie**.



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

Configurez le Listes de contrôle d'accès (ACL)

Pour que l'authentification Web fonctionne, le trafic permis devrait être défini. Déterminez si FlexConnect ACLs ou ACLs normal devrait être utilisé. FlexConnect aps utilisent FlexConnect ACLs, alors que les aps qui utilisent la normale centralisée ACLs d'utilisation de commutation.

Afin de comprendre dans quel mode AP particulier actionne, choisissez la **radio > les Points d'accès** et choisissez la liste déroulante de **nom AP > de mode AP**. Un déploiement typique est des **gens du pays** ou **FlexConnect**.

Sous la **Sécurité > les listes de contrôle d'accès,** choisissez **FlexConnect ACLs** ou **ACLs**. Dans cet exemple, on a permis au tout le trafic UDP afin de permettre spécifiquement l'échange de DN et trafiquer à 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, ainsi FlexConnect et ACLs standard sont définis.

Ce comportement est documenté dans l'ID de bogue Cisco CSCue68065 en ce qui concerne des

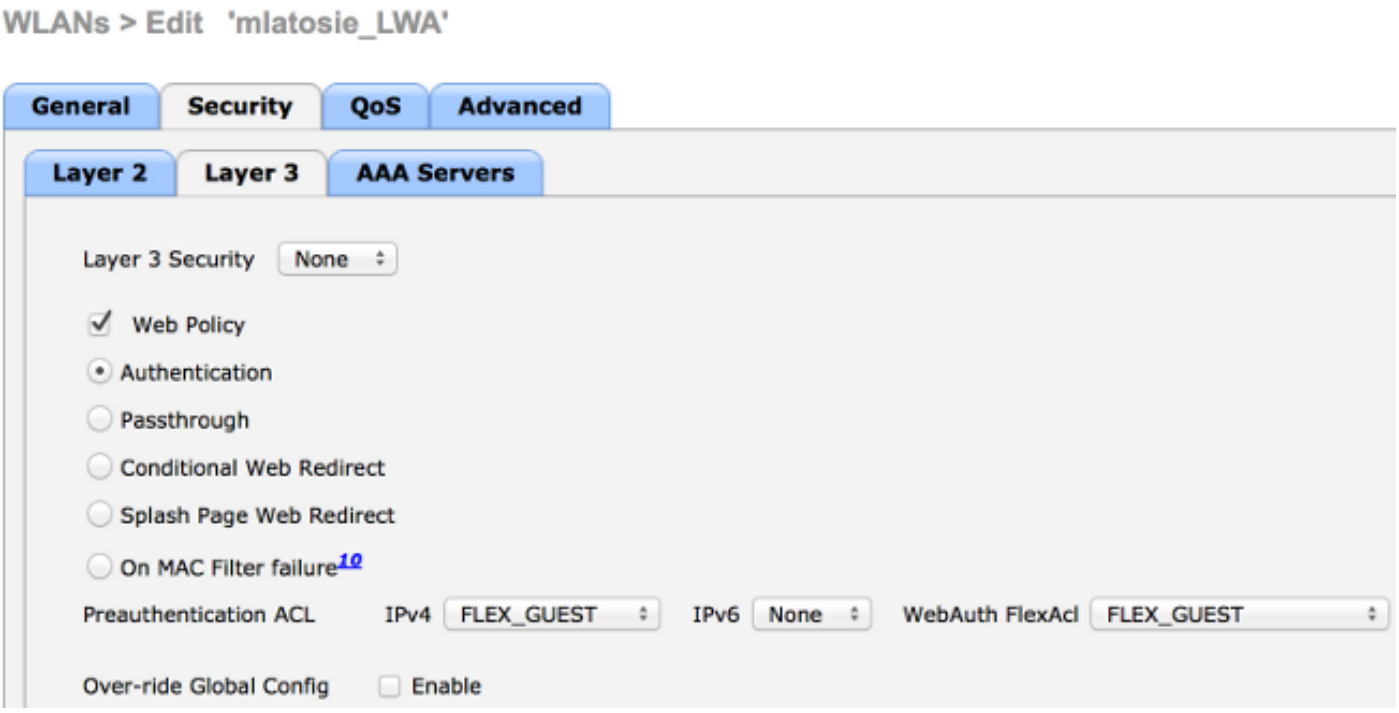
contrôleurs WLC 7.4. On ne l'exige plus sur WLC 7.5 où vous n'avez besoin seulement désormais de FlexACL et d'aucun ACL standard

Configurez l'Identifiant SSID (Service Set Identifier) pour LWA

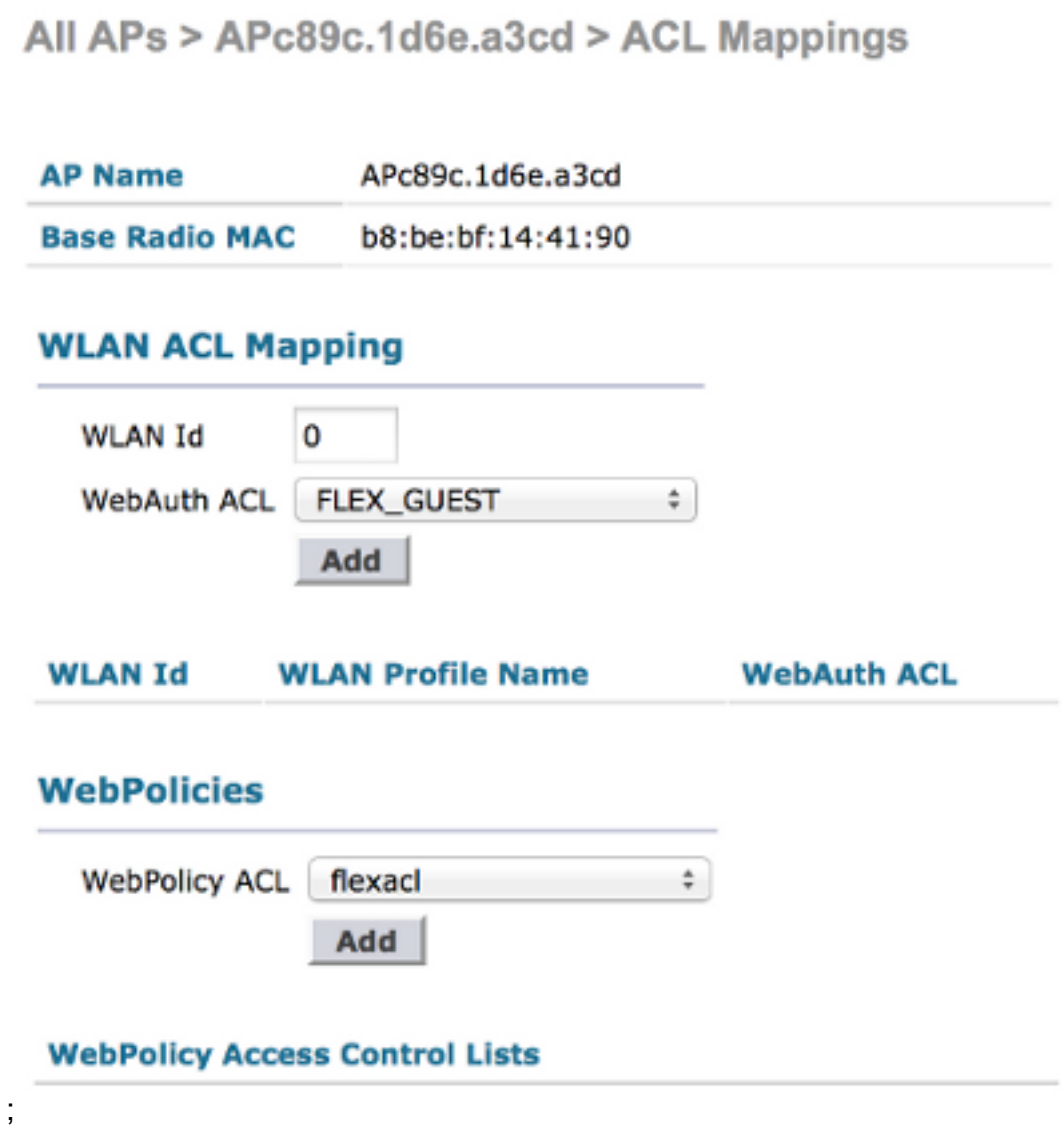
Sous des **WLAN,** choisissez l'**ID de WLAN** pour éditer.

Configuration authentique de Web

Appliquez le même ACLs qui ont été définis dans l'étape précédente et activez l'authentification Web.



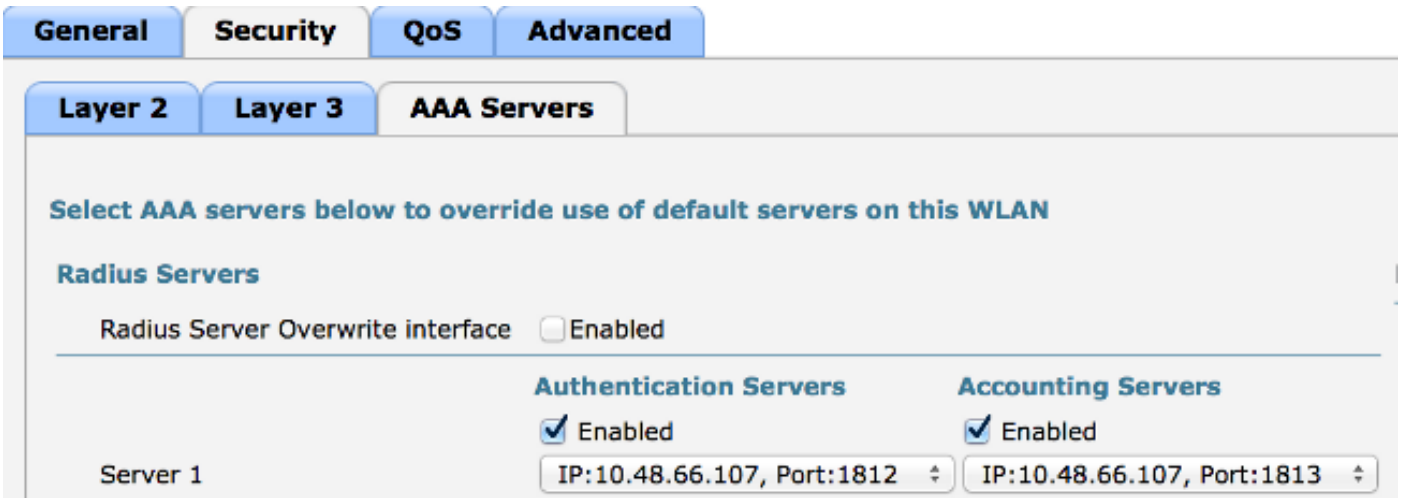
Note: Si la caractéristique de la commutation locale de FlexConnect est utilisée, la cartographie d'ACL doit être ajoutée au niveau AP. Ceci peut être trouvé à la **radio > aux Points d'accès.** Choisissez le **nom** approprié **> FlexConnect AP > WebAuthentication externe ACLs**.



;

Configuration du serveur d'Authentification, autorisation et comptabilité (AAA)

Dans cet exemple, les serveurs d'authentification et de comptabilité indiquent le serveur précédent-défini ISE.



Note: Les par défaut sous l'**onglet Avancé** n'ont pas besoin d'être ajoutés.

Configurez l'ISE

La configuration ISE se compose de plusieurs étapes.

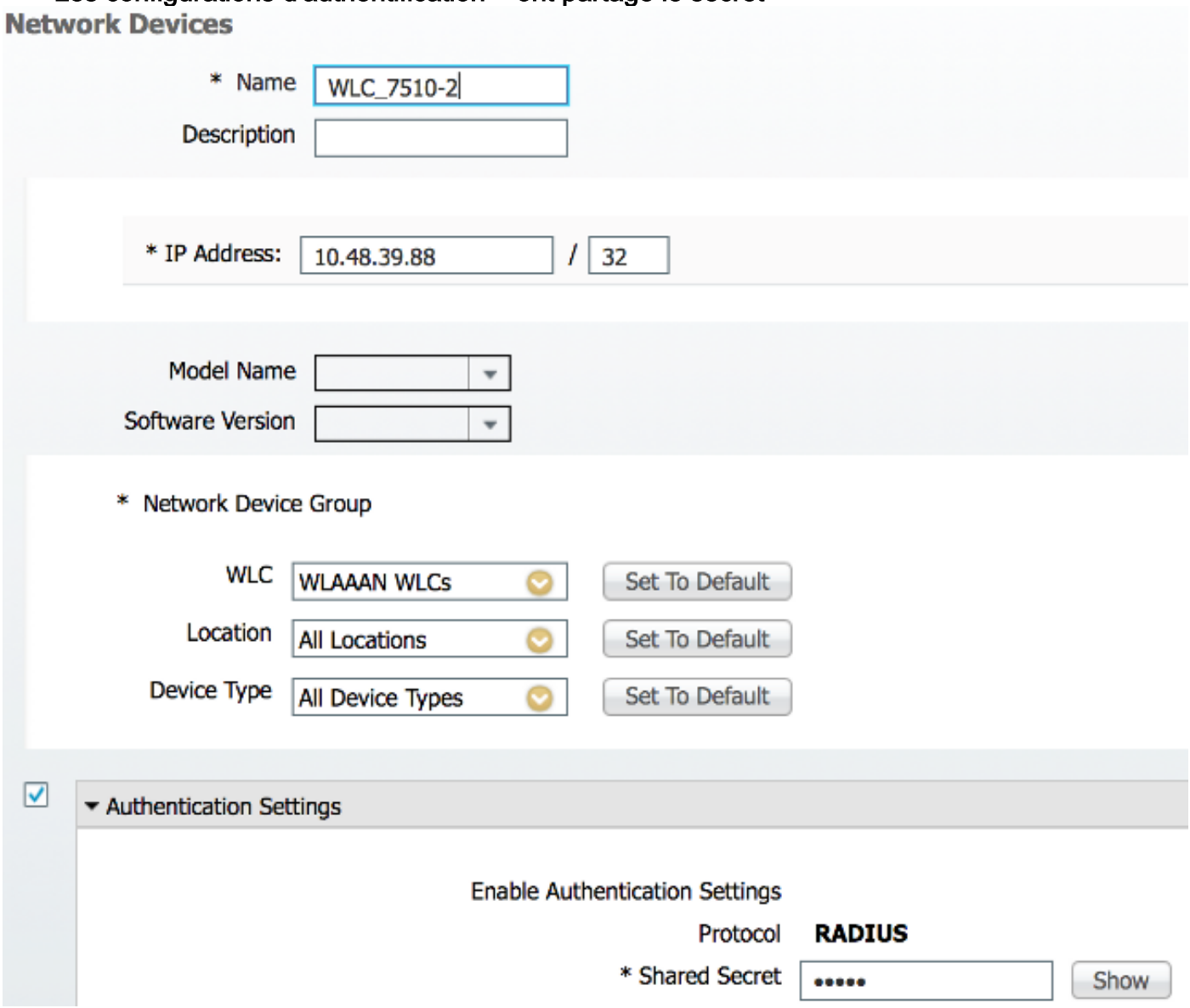
D'abord, définissez le périphérique comme périphérique de réseau.

Puis, assurez-vous que les règles d'authentification et d'autorisation qui facilitent cet échange existent.

Définissez le périphérique de réseau

Sous la **gestion > les ressources de réseau > les périphériques de réseau**, remplissez ces champs :

- Nom du périphérique
- Adresse IP de périphérique
- **Les configurations d'authentification > ont partagé le secret**

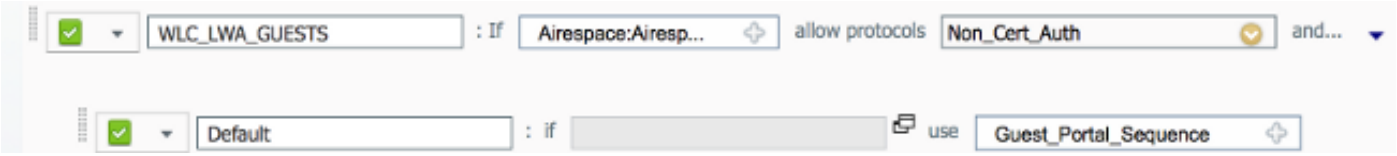


Configurez la stratégie d'authentification

Sous la **stratégie > l'authentification**, ajoutez une nouvelle stratégie d'authentification.

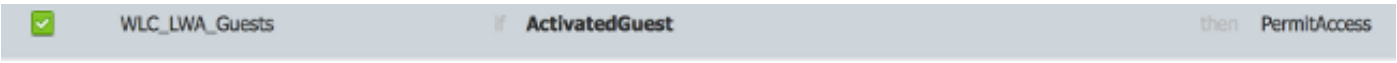
Cet exemple utilise ces paramètres :

- Nom : **WLC_LWA_Guests**
- Condition : **Airespace : Airespace-WLAN-id.** Cette condition apparie l'ID de WLAN de 3, qui est l'ID du **mlatosie_LWA** WLAN qui a été précédemment défini sur le WLC.
- il {facultatif} permet les Protocoles d'authentification qui n'exigent pas le certificat **Non_Cert_Auth**, mais les par défaut peuvent être utilisés.
- Guest_Portal_Sequence, qui définit que les utilisateurs sont les utilisateurs local-définis d'invités.



Configurez la stratégie et le résultat d'autorisation

Sous la **stratégie > l'autorisation,** définissez une nouvelle stratégie. Ce peut être une stratégie très de base, comme :

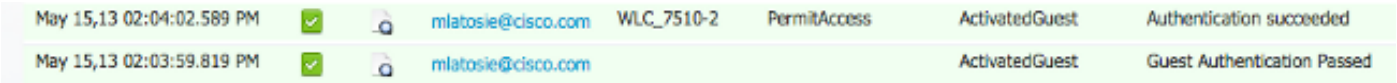


Cette configuration dépend de la configuration globale de l'ISE. Cet exemple est à bon escient simplifié.

Vérifiez

Sur l'ISE, les administrateurs peuvent surveiller et dépanner des sessions vivantes sous des **exécutions > des authentifications**.

Deux authentifications devraient être vues. La première authentification est du portail d'invité sur l'ISE. La deuxième authentification est livré comme une demande d'accès du WLC à l'ISE.



Vous pouvez cliquer sur l'icône d'**état de détail d'authentification** afin de vérifier que des stratégies et les stratégies d'authentification d'autorisation ont été choisie.

Sur le WLC, un administrateur peut surveiller des clients sous le **moniteur > le client**.

Voici un exemple d'un client qui a authentifié correctement :

Dépannez

Cisco recommande que vous vous exécutiez mette au point au moyen du client autant que possible.

Par le CLI, ceux-ci met au point fournissent les 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 du Cisco WLC 7.x
- Support et documentation techniques - Cisco Systems

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Nov. 25, 2015
ID de document : 116217