Guide d'intégration WLC et NAC Guest Server (NGS)

Table des matières

Introduction

Ce document fournit des instructions pour intégrer le NAC Guest Server et les contrôleurs de réseau local sans fil.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Contrôleur LAN sans fil Cisco (WLC) 4.2.61.0
- Catalyst 3560 avec IOS® Version 12.2(25)SEE2
- Cisco ADU version 4.0.0.279
- Serveur invité NAC version 1.0

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Cisco NAC Guest Server est un système complet de mise en service et de création de rapports qui fournit un accès réseau temporaire aux invités, visiteurs, sous-traitants, consultants ou clients. Le serveur invité fonctionne avec l'appareil Cisco NAC ou le contrôleur LAN sans fil Cisco, qui fournit le portail captif et le point d'application pour l'accès invité.

Cisco NAC Guest Server permet à tout utilisateur disposant de privilèges de créer facilement des comptes d'invité temporaires et de parrainer des invités. Cisco NAC Guest Server procède à l'authentification complète des sponsors, c'est-à-dire des utilisateurs qui créent des comptes d'invité, et permet aux sponsors de fournir des informations de compte à l'invité par impression, e-mail ou SMS. L'ensemble de l'expérience, de la création du compte utilisateur à l'accès au réseau invité, est stocké à des fins d'audit et de création de rapports.

Lorsque des comptes d'invité sont créés, ils sont soit provisionnés dans Cisco NAC Appliance Manager (Clean Access Manager), soit stockés dans la base de données intégrée sur Cisco NAC Guest Server. Lorsque vous utilisez la base de données intégrée du serveur invité, les périphériques d'accès réseau externes, tels que le contrôleur LAN sans fil Cisco, peuvent authentifier les utilisateurs par rapport au serveur invité à l'aide du protocole RADIUS (Remote Authentication Dial In User Service).

Le serveur invité Cisco NAC provisionne le compte invité pour la durée spécifiée lors de la création du compte. À l'expiration du compte, le serveur invité supprime le compte directement du Cisco NAC Appliance Manager ou envoie un message RADIUS qui avertit le périphérique d'accès réseau (NAD) de la durée de validité restante du compte avant que le NAD ne doive supprimer l'utilisateur.

Cisco NAC Guest Server fournit une comptabilité d'accès au réseau invité essentielle en consolidant l'ensemble de la piste d'audit, de la création du compte invité à l'utilisation du compte par l'invité, de sorte que les rapports peuvent être exécutés via une interface de gestion centrale.

Concepts d'accès invité

Cisco NAC Guest Server utilise un certain nombre de termes pour expliquer les composants nécessaires pour fournir un accès invité.

Utilisateur invité

L'utilisateur invité est la personne qui a besoin d'un compte d'utilisateur pour accéder au réseau.

Sponsor

Le sponsor est la personne qui crée le compte d'utilisateur invité. Cette personne est souvent un employé de l'entreprise qui fournit l'accès au réseau. Les parrains peuvent être des personnes spécifiques (3) ayant certains rôles, ou tout employé pouvant s'authentifier auprès d'un répertoire d'entreprise tel que Microsoft Active Directory (AD).

Périphérique d'application réseau

Ces périphériques sont les composants de l'infrastructure réseau qui fournissent l'accès au réseau. En outre, les dispositifs d'application de réseau poussent les utilisateurs invités vers un portail captif, où ils peuvent entrer leurs informations de compte d'invité. Lorsqu'un invité entre son nom d'utilisateur et son mot de passe temporaires, le périphérique d'application réseau vérifie ces informations d'identification par rapport aux comptes d'invité créés par le serveur invité.

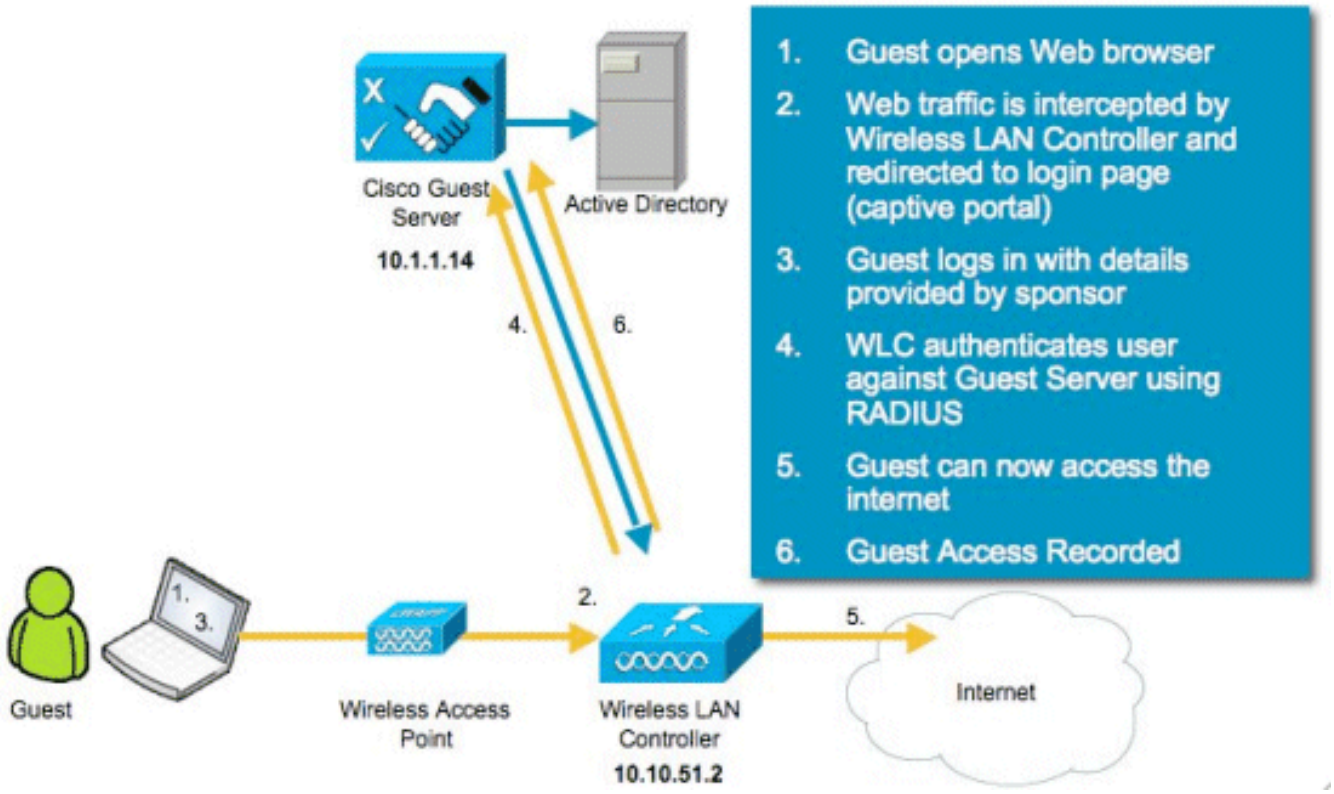
Serveur invité

Il s'agit du serveur invité Cisco NAC, qui rassemble toutes les parties de l'accès invité. Le serveur invité relie ces éléments entre eux : le sponsor qui crée le compte invité, les détails du compte transmis à l'invité, l'authentification de l'invité par rapport au périphérique d'application réseau et la vérification du périphérique d'application réseau de l'invité avec le serveur invité. En outre, le serveur invité Cisco NAC consolide les informations de comptabilité à partir des périphériques d'application du réseau pour fournir un point unique de rapports d'accès invité.

Une documentation détaillée sur NGS est disponible dans CCO.

http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/10/nacguestserver.html

Présentation de la topologie de TP



Configuration du contrôleur LAN sans fil (WLC)

Suivez ces étapes pour configurer le WLC :

1. Initialisez le contrôleur et le point d'accès.
2. Configurer les interfaces du contrôleur.

3. Configurez RADIUS.
4. Configurez les paramètres WLAN.

Initialisation

Pour la configuration initiale, utilisez une connexion console telle que HyperTerminal et suivez les instructions de configuration pour renseigner les informations de connexion et d'interface. La commande **reset system** lance également ces invites.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_44:36:c3]: WLC
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): admin
Service Interface IP Address Configuration [none][DHCP]: <ENTER>
Enable Link Aggregation (LAG) [yes][NO]:no
Management Interface IP Address: 10.10.51.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.51.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 10.10.51.1
AP Transport Mode [layer2][LAYER3]: layer3
AP Manager Interface IP Address: 10.10.51.3
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.10.5<X>.1):<ENTER>
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: mobile-1
Enable Symmetric Mobility Tunneling: No
Network Name (SSID): wireless-1
Allow Static IP Addresses [YES][no]:<ENTER>
Configure a RADIUS Server now? [YES][no]:<ENTER>
Enter the RADIUS Server's Address: 10.1.1.12
Enter the RADIUS Server's Port [1812]:<ENTER>
Enter the RADIUS Server's Secret: cisco
Enter Country Code (enter 'help' for a list of countries) [US]:<ENTER>
Enable 802.11b Network [YES][no]:<ENTER>
Enable 802.11a Network [YES][no]:<ENTER>
Enable 802.11g Network [YES][no]:<ENTER>
Enable Auto-RF [YES][no]:<ENTER>
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
```

Serveur invité Cisco NAC

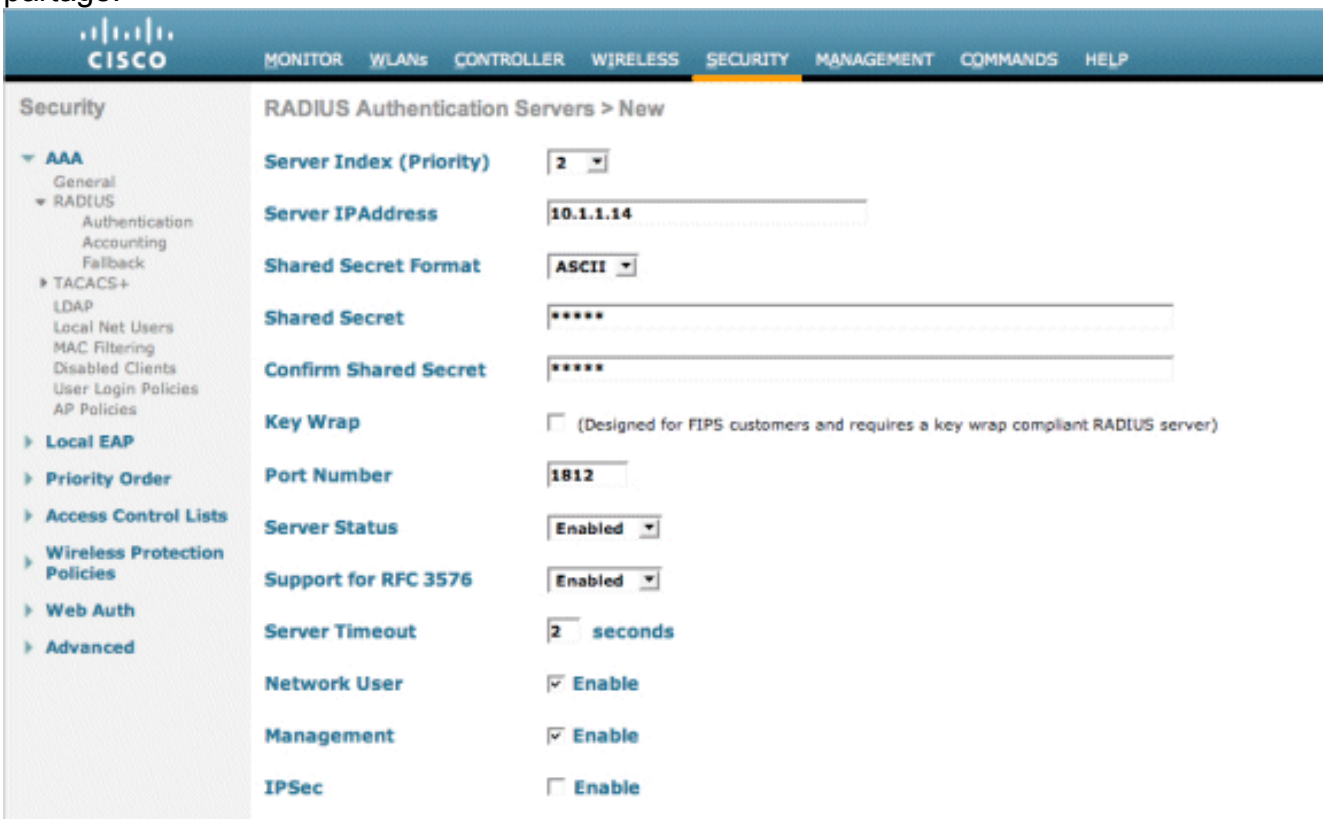
Cisco NAC Guest Server est une solution de mise en service et de création de rapports qui fournit un accès réseau temporaire aux clients tels que les invités, les sous-traitants, etc. Le serveur invité Cisco NAC fonctionne avec les solutions Cisco Unified Wireless Network ou Cisco NAC Appliance. Ce document vous guide tout au long des étapes d'intégration du serveur invité Cisco NAC à un WLC Cisco, qui crée un compte d'utilisateur invité et vérifie l'accès réseau temporaire de l'invité.

Procédez comme suit pour terminer l'intégration :

1. Ajoutez le serveur invité Cisco NAC en tant que serveur d'authentification dans le

WLC.Accédez à votre WLC (https://10.10.51.2, admin/admin) pour le configurer.Choisissez **Security > RADIUS > Authentication**.

Sélectionnez **Nouveau**.Ajoutez l'adresse IP (10.1.1.14) du serveur invité Cisco NAC.Ajoutez le secret partagé.Confirmez le secret partagé.

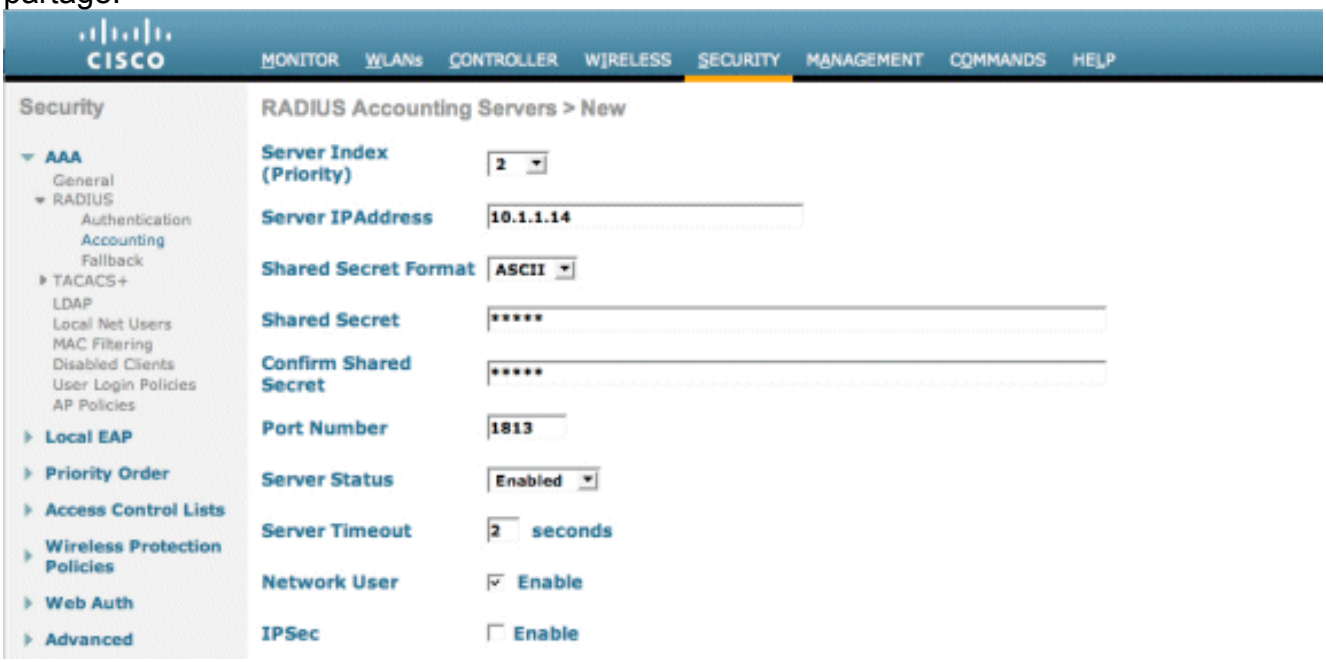


Sélectionnez **Apply**.

2. Ajoutez le serveur invité Cisco NAC en tant que serveur de comptabilité dans le

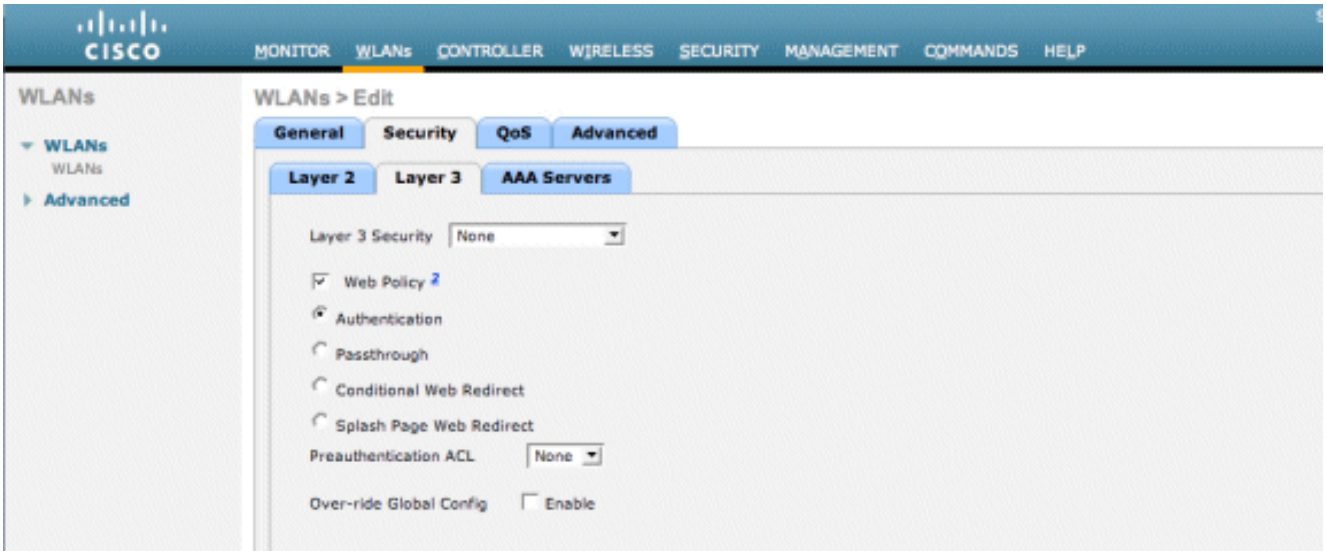
WLC.Choisissez **Security > RADIUS > Accounting**.

Sélectionnez **Nouveau**.Ajoutez l'adresse IP (10.1.1.14) du serveur invité Cisco NAC.Ajoutez le secret partagé.Confirmez le secret partagé.

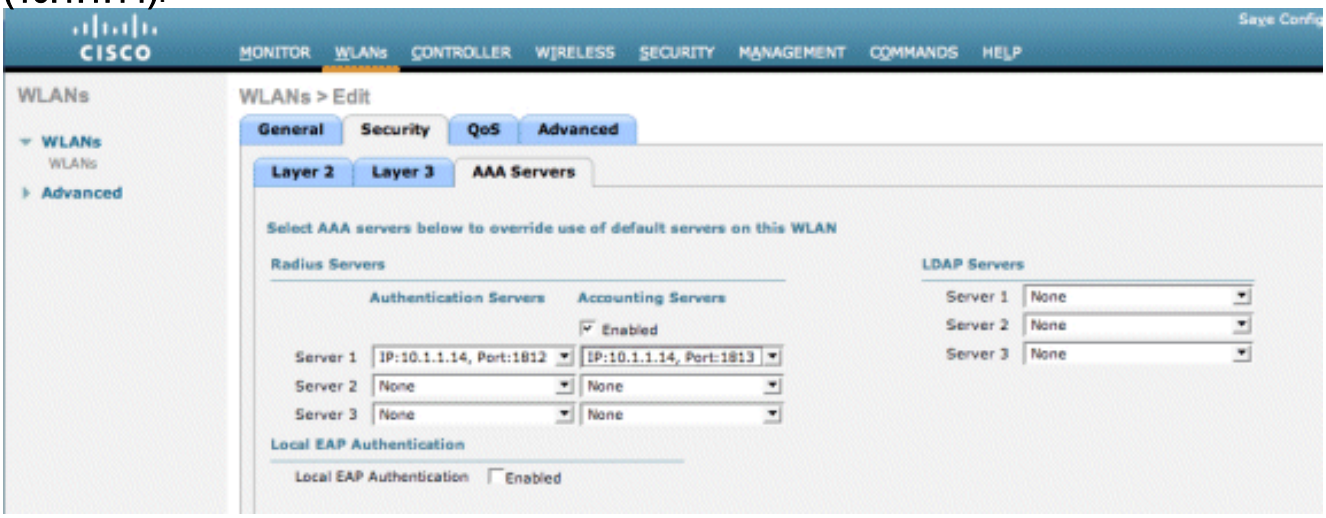


Sélectionnez **Apply**.

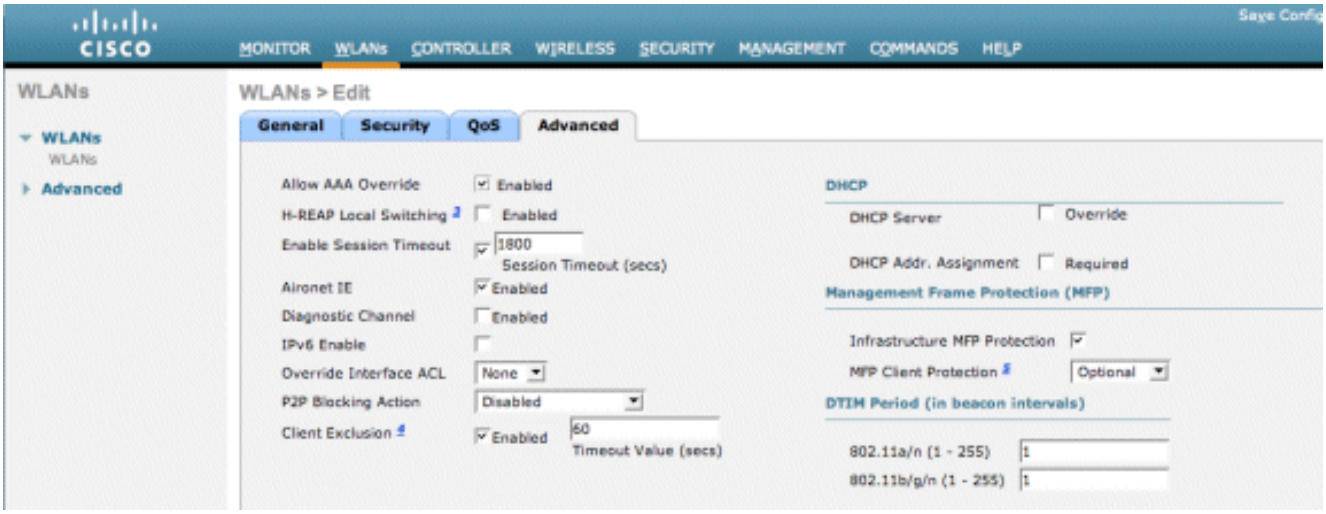
3. Modifiez le WLAN (wireless-x) pour utiliser le serveur invité NAC.Modifiez le WLAN (wireless-x).Sélectionnez l'onglet Security .Modifiez la sécurité de couche 2 sur **None** et la sécurité de couche 3 pour utiliser l'**authentification Web**.



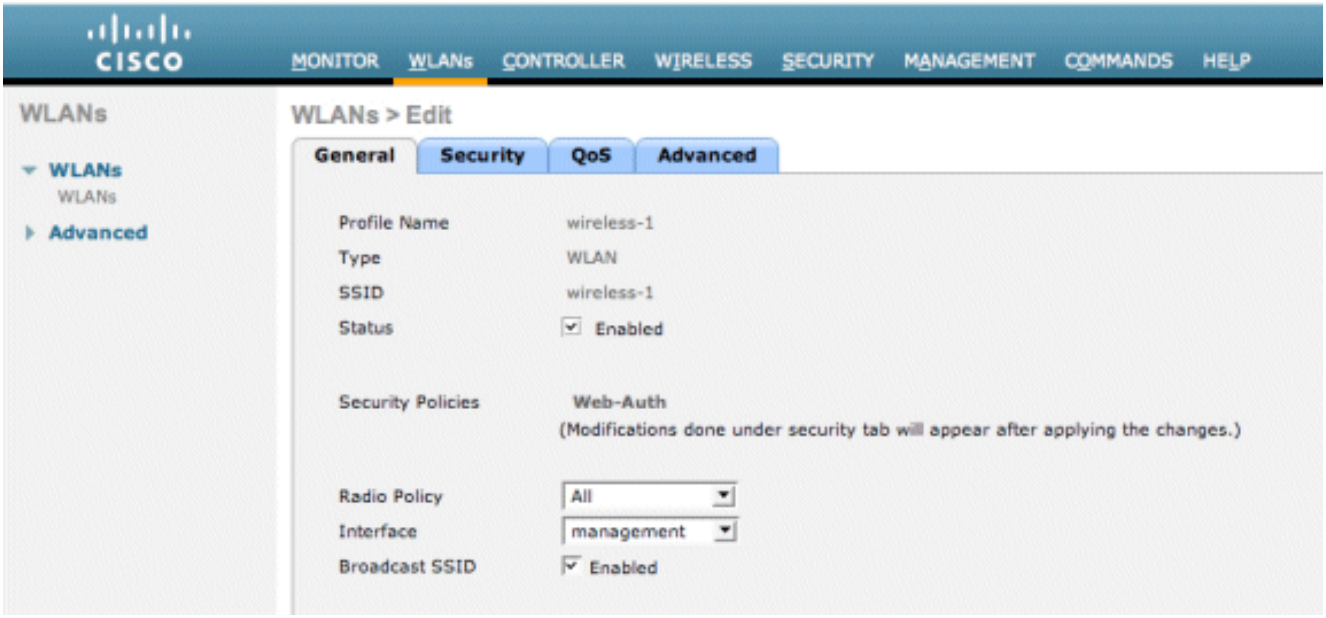
Sélectionnez **AAA Servers** sous l'onglet Security.Dans la zone Server 1, sélectionnez le **serveur RADIUS (10.1.1.14)**.Dans la zone Serveur 1, sélectionnez le **serveur Accounting (10.1.1.14)**.



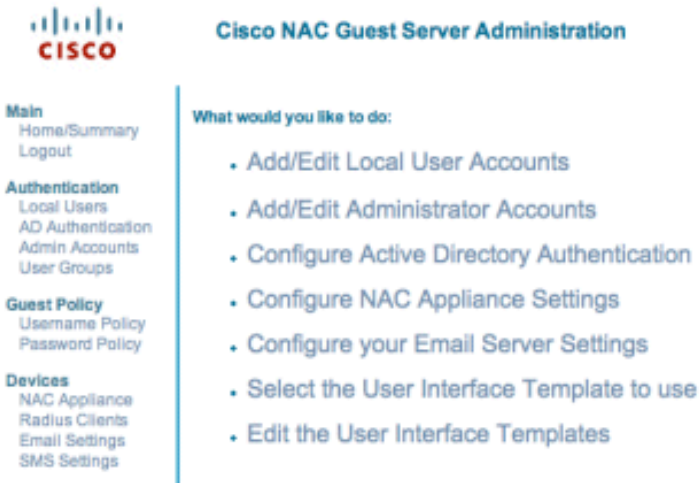
Sélectionnez l'onglet **Avancé**.Activez **Allow AAA Override**. Cela permet de définir le délai d'expiration de la session par client à partir de l'appliance invité
NAC.



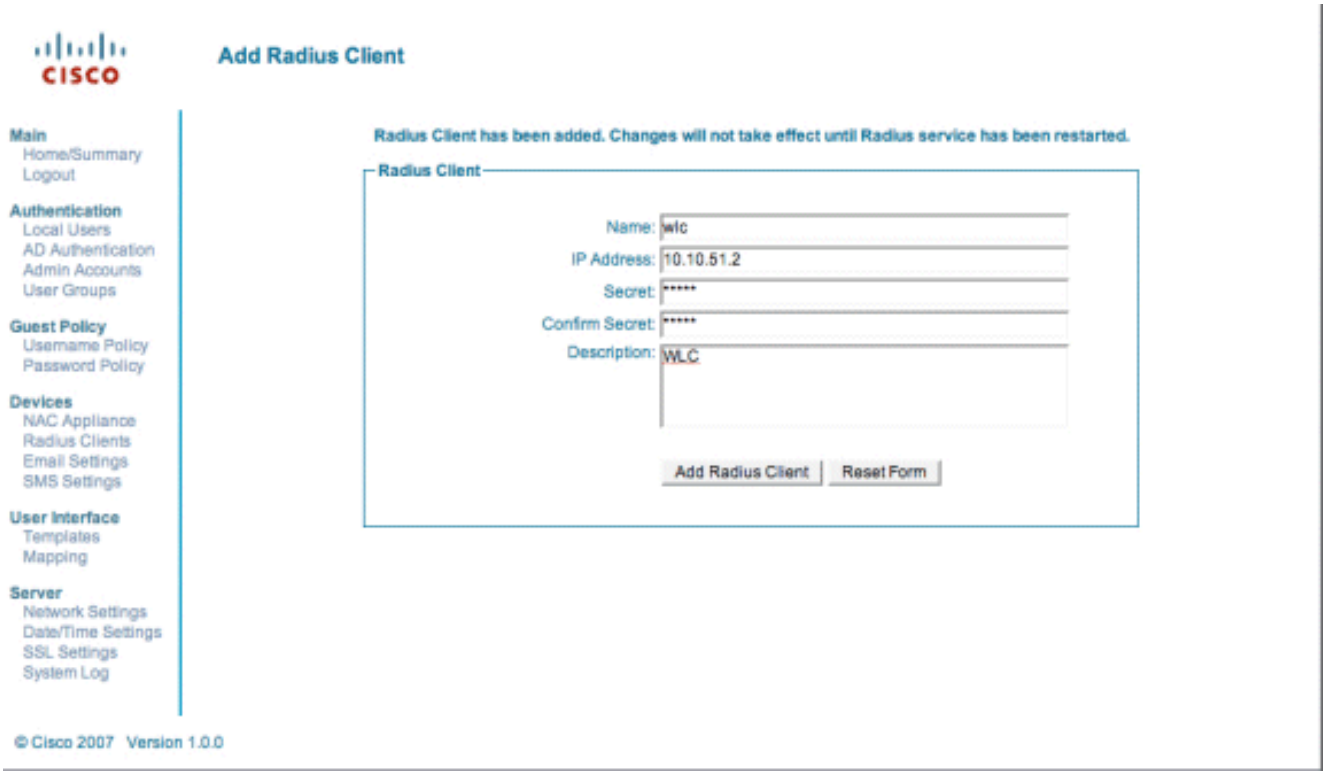
Remarque : lorsque la **substitution AAA** est activée sur le SSID, la durée de vie restante de l'utilisateur invité sur NGS est poussée vers le WLC comme délai d'expiration de session au moment de la connexion de l'utilisateur invité.Choisissez **Apply** pour enregistrer votre configuration
WLAN.



4. Vérifiez si le contrôleur est ajouté en tant que client Radius dans le serveur invité Cisco NAC.Accédez à NAC Guest Server (https://10.1.1.14/admin) pour configurer ce paramètre.**Remarque :** vous obtenez la page Administration si vous spécifiez /admin dans l'URL.

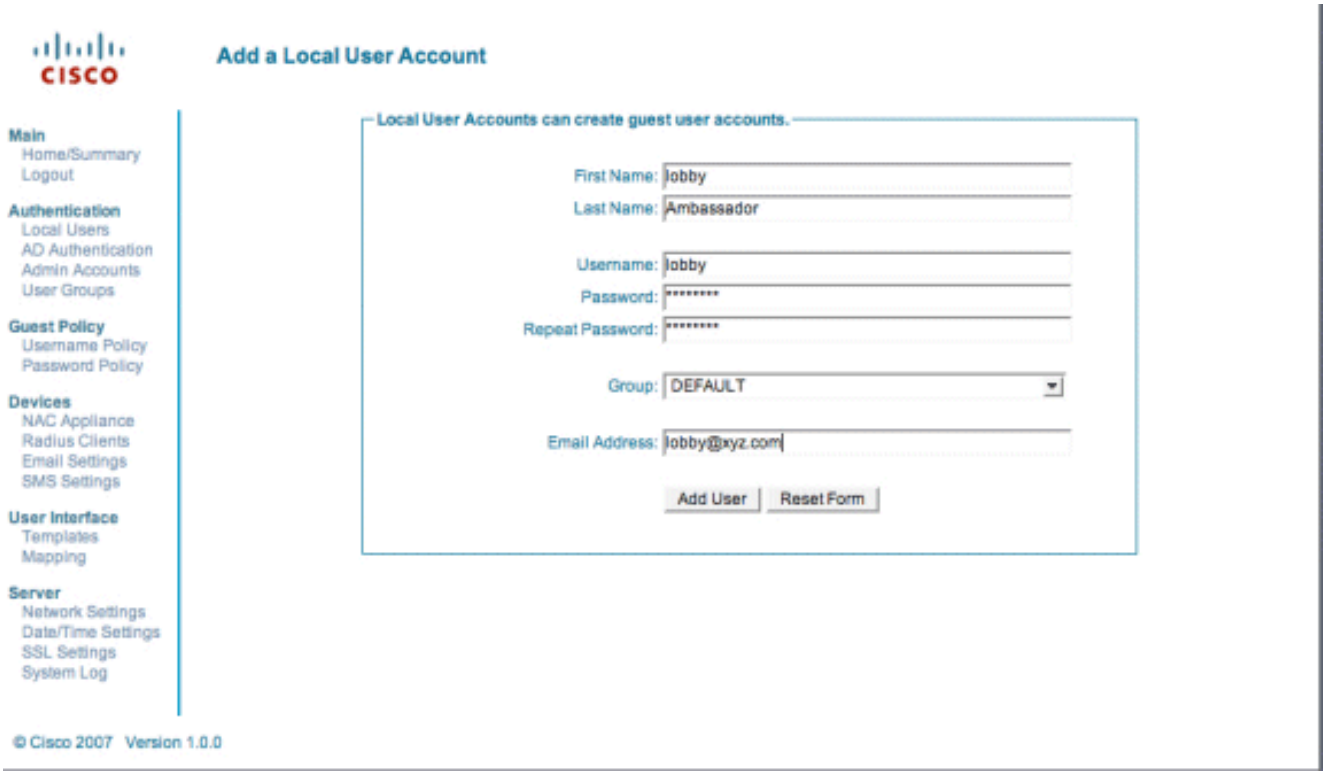


Sélectionnez **Radius Clients**.Sélectionnez **Ajouter un rayon**.Saisissez les informations du client Radius :Entrez un nom : nom du système WLC.Entrez l'adresse IP : adresse IP du WLC **(10.10.51.2)**.Entrez le même secret partagé que celui que vous avez entré à l'étape 1.Confirmez votre secret partagé.Saisissez une description.Choisissez **Add Radius Client**.



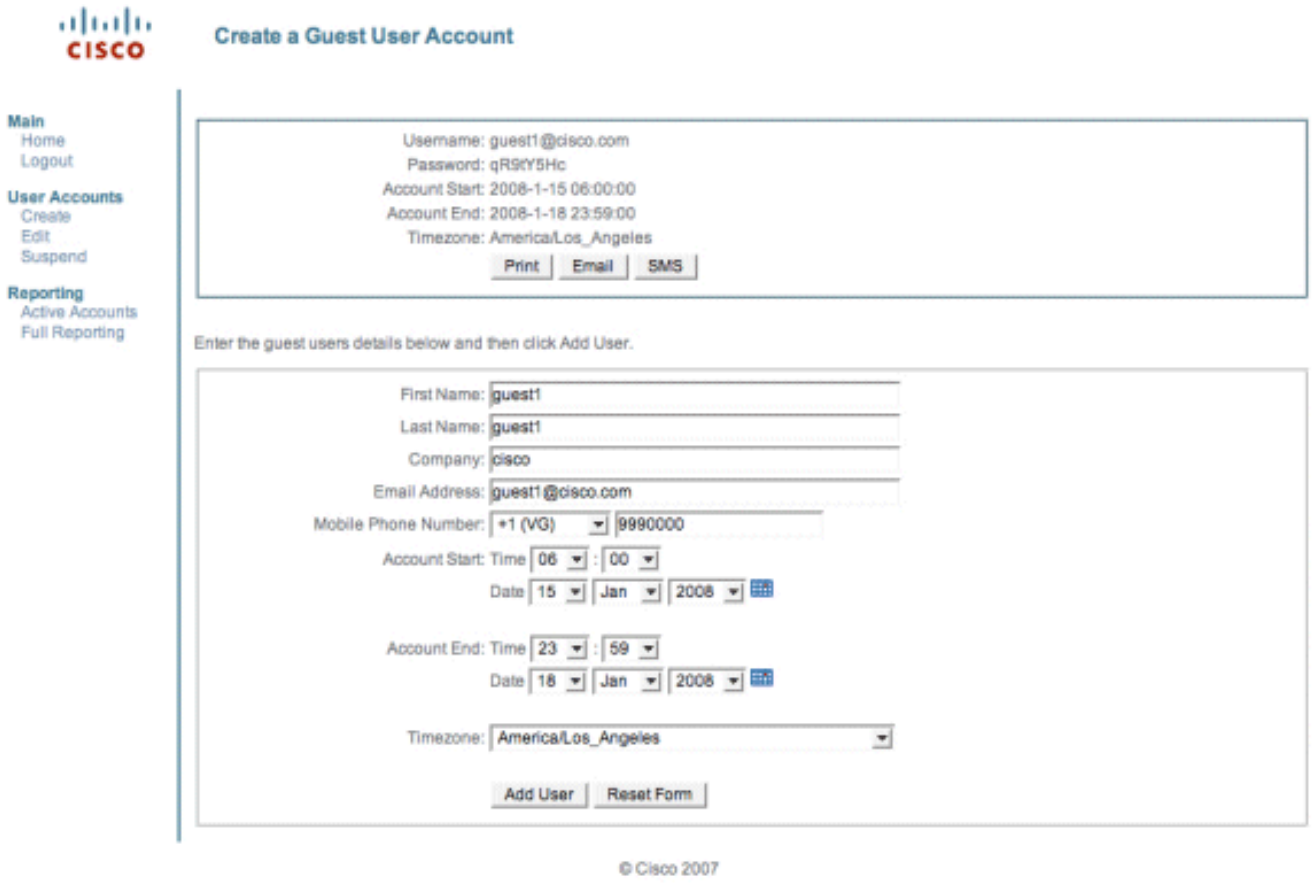
Redémarrez le service Radius afin que les modifications prennent effet.Sélectionnez **Radius Clients**.Choisissez **Restart** dans la zone Restart
Radius.

5. Créez un utilisateur local, c'est-à-dire Lobby Ambassador, dans le serveur invité Cisco NAC.Sélectionnez **Utilisateurs locaux**.Sélectionnez **Ajouter un utilisateur**.**Remarque :** vous devez renseigner tous les champs.Entrez un prénom : **hall**.Entrez un nom : **Ambassador**.Saisissez Nom d'utilisateur : **lobby**.Entrez un mot de passe : **password**.Laissez le groupe par **défaut**.Saisissez l'adresse e-mail : **lobby@xyz.com**.Sélectionnez **Ajouter un utilisateur**.



6. Connectez-vous en tant qu'utilisateur local et créez un compte invité.Accédez au serveur invité NAC (https://10.1.1.14), connectez-vous avec le nom d'utilisateur/mot de passe que vous avez créé à l'étape 5, puis configurez ceci
:

Sélectionnez **Créer** pour un compte d'utilisateur invité.**Remarque :** vous devez renseigner tous les champs.Saisissez un prénom.Saisissez un nom.Saisissez la société.Saisissez l'adresse e-mail.**Remarque :** l'adresse e-mail est le nom d'utilisateur.Saisissez la date de fin du compte : **Heure**.Sélectionnez **Ajouter un utilisateur**.



7. Connectez-vous au WLAN invité et connectez-vous en tant qu'utilisateur invité.Connectez votre client sans fil au WLAN invité (sans fil-x).Ouvrez le navigateur Web pour être redirigé vers la page Web-Auth Login.**Remarque :** vous pouvez également taper **https://1.1.1.1/login.html** pour être redirigé vers la page de connexion.Saisissez le nom d'utilisateur invité que vous avez créé à l'étape 6.Saisissez le mot de passe généré automatiquement à l'étape 6.Établissez une connexion Telnet avec le WLC et vérifiez que le délai d'attente de session a été défini avec la commande **show client detail**.Lorsque le délai de session expire, le client invité est déconnecté et votre requête ping s’arrête.

```
(Cisco Controller) >show client detail 00:13:e8:b7:5e:dd
Client MAC Address.............................. 00:13:e8:b7:5e:dd
Client Username ................................ podx@cisco.com
AP MAC Address.................................. 00:17:df:a6:e5:f0
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:17:df:a6:e5:ff
Channel......................................... 60
IP Address...................................... 10.1.1.22
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 59
Client CCX version.............................. 4
Client E2E version.............................. 1
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Enabled
U-APSD Support.................................. Disabled
Mobility State.................................. Local
--More-- or (q)uit
(Cisco Controller) >
```

Remarque : pour configurer l'authentification Web à partir du contrôleur LAN sans fil, WLC vers le serveur invité NAC (NGS), vous devez utiliser l'authentification en mode PAP sur les propriétés d'authentification Web. Si la stratégie d'authentification Web est définie sur CHAP,

l'authentification échoue car CHAP n'est pas pris en charge avec NGS.

Informations connexes

- Cisco NAC Appliance - Guide d'installation et de configuration de Clean Access Manager, version 4.1(3)
- Prise en charge du commutateur Cisco NAC et du contrôleur LAN sans fil
- Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0
- (Vidéo) Intégration de Cisco ISE (Identity Services Engine) et WLC (Wireless LAN Controller)
- NAC (Clean Access) : configuration de l'accès invité
- Guide de déploiement : Cisco Guest Access Using the Cisco Wireless LAN Controller, Release 4.1
- Assistance et documentation techniques - Cisco Systems

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.