Exemple de configuration d'un serveur EAP local dans un réseau sans fil unifié Cisco

Contenu

Introduction

Ce document décrit la configuration d'un serveur local Extensible Authentication Protocol (EAP) dans un contrôleur de réseau local sans fil de Cisco (WLC) pour l'authentification des utilisateurs sans fil.

L'authentification EAP locale est une méthode qui permet d'authentifier localement des utilisateurs et des clients sans fil. Il est conçu pour l'usage dans les bureaux distants qui veulent mettre à jour la Connectivité aux clients sans fil quand le système principal devient perturbé ou le serveur d'authentification externe descend. Quand vous activez l'EAP local, le contrôleur sert de serveur d'authentification et de base de données locale des utilisateurs, enlevant de ce fait la dépendance à l'égard un serveur d'authentification externe. L'EAP local récupère des identifiants utilisateurs de la base de données locale des utilisateurs ou de la base de données de partie postérieure de Protocole LDAP (Lightweight Directory Access Protocol) pour authentifier des utilisateurs. L'EAP local prend en charge l'authentification légère d'EAP (LEAP), d'EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), et d'EAP-Transport Layer Security (EAP-TLS) entre le contrôleur et les clients sans fil.

Notez que le serveur local d'EAP n'est pas disponible s'il y a une configuration de serveur RADIUS externe globale dans le WLC. Toutes les demandes d'authentification sont expédiées au RAYON externe global jusqu'à ce que le serveur local d'EAP soit disponible. Si le WLC desserre la Connectivité au serveur RADIUS externe, alors le serveur local d'EAP devient actif. S'il n'y a aucune configuration du serveur RADIUS globale, le serveur local d'EAP devient immédiatement actif. Le serveur local d'EAP ne peut pas être utilisé pour authentifier les clients, qui sont connectés à l'autre WLCs. En d'autres termes, un WLC ne peut pas expédier sa demande d'EAP à un autre WLC pour l'authentification. Chaque WLC devrait avoir sa propre base de données locale de serveur et de personne d'EAP.

Note: Employez ces commandes afin d'arrêter WLC d'envoyer des demandes à un serveur RADIUS externe.

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

Le serveur local d'EAP prend en charge ces protocoles dans la version logicielle de 4.1.171.0 et plus tard :

- LEAP
- EAP-FAST (les deux nom d'utilisateur/mot de passe, et Certificats)
- EAP-TLS

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la façon configurer WLCs et Point d'accès léger (recouvrements) pour le fonctionnement de base
- La connaissance du point d'accès léger Protocol (LWAPP) et des méthodes de sécurité sans fil
- Connaissance de base de l'authentification EAP locale.

Composants utilisés

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

- Windows XP avec la carte adaptateur CB21AG et la version 4.05 de Cisco Secure Services Client
- Contrôleur LAN 4.1.171.0 de radio de Cisco 4400
- Autorité de certification de Microsoft sur le serveur de Windows 2000

Conventions

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

Configurez l'EAP local sur le contrôleur LAN de radio de Cisco

Ce document suppose que la configuration de base du WLC est déjà terminée.

Configuration locale d'EAP

Terminez-vous ces étapes afin de configurer l'EAP local :

1. Ajoutez un utilisateur du réseau local :Du GUI. choisissez la **Sécurité > les utilisateurs du réseau locaux > nouveau**, écrivez le nom d'utilisateur, le mot de passe, l'utilisateur d'invité, l'ID de WLAN, et la description et cliquez sur Apply.Du CLI vous pouvez utiliser la commande de *<description> d'id> du <password> <WLAN de <username> de* ***config netuser add*** :**Note**: Cette commande a été rapportée à une deuxième ligne due aux raisons spatiales.
   ```
   (Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database
   ```

2. Spécifiez la commande de récupération d'identifiant utilisateur.Du GUI, choisissez la **Sécurité > EAP local > authentication priority**. Alors sélectionnez le LDAP, cliquez sur « **<** » le bouton et cliquez sur Apply. Ceci met les identifiants utilisateurs dans la base de données locale d'abord.Du CLI :
   ```
   (Cisco Controller) >config local-auth user-credentials local
   ```

3. Ajoutez un eap profile :Afin de faire ceci du GUI, choisissez la **Sécurité > EAP local > profils** et cliquez sur New. Quand la nouvelle fenêtre apparaît, introduisez le nom de profil et cliquez sur Apply.Vous pouvez également faire ceci utilisant le **config local-auth eap-profile de** commande CLI **ajoutez le *<profile-name>*.** Dans notre exemple, le nom de profil est Eap-*test*.
   ```
   (Cisco Controller) >config local-auth eap-profile add EAP-test
   ```

4. Ajoutez une méthode à l'eap profile.Du GUI choisissez la **Sécurité > EAP local > profils** et cliquez sur en fonction le nom de profil pour lequel vous voulez ajouter les méthodes d'authentification. Cet exemple utilise le LEAP, l'EAP-FAST, et l'EAP-TLS. Cliquez sur Apply afin de placer les méthodes.Vous pouvez également utiliser la **méthode de config local-auth eap-profile de** commande CLI **ajoutez le *<profile-name> de <method-name>***. En notre exemple de configuration nous ajoutons trois méthodes au l'Eap-test de profil. Les méthodes sont le LEAP, l'EAP-FAST, et l'EAP-TLS dont les noms de méthode sont LEAP*, rapide,* et *tls* respectivement. Cette sortie affiche les commandes de configuration CLI :
   ```
   (Cisco Controller) >config local-auth eap-profile method add leap EAP-test
   (Cisco Controller) >config local-auth eap-profile method add fast EAP-test
   (Cisco Controller) >config local-auth eap-profile method add tls EAP-test
   ```

5. Configurez les paramètres de la méthode d'EAP. Ceci est seulement utilisé pour l'EAP-FAST. Les paramètres à configurer sont :**Clé de serveur (server-key)** — Qualifications de Protected Access de to encrypt/decrypt de clé de serveur (PACs) (dans l'hexadécimal).**Time to Live pour PAC (pac-TTL)** — Place le Time to Live pour le PAC.**ID d'autorité (autorité-id)** — Place l'identifiant d'autorité.**Disposition d'Annonymous (anon-provn)** — Configure si on permet la disposition anonyme. Ceci est activé par défaut.Pour la configuration par le GUI, choisissez la **Sécurité > des paramètres locaux d'EAP > d'EAP-FAST** et des valeurs de l'information écrivez la clé de serveur, le Time to Live pour le PAC, l'ID d'autorité (dans l'hexa), et d'autorité ID.Ce sont les commandes de configuration CLI de les utiliser afin de placer ces paramètres pour l'EAP-FAST :

```
(Cisco Controller) >config local-auth method fast server-key 12345678
(Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID
(Cisco Controller) >config local-auth method fast pac-ttl 10
```

6. Authentification locale d'enable par WLAN :Du GUI choisissez les **WLAN** sur le menu principal et sélectionnez le WLAN pour lequel vous voulez configurer l'authentification locale. Une nouvelle fenêtre apparaît. Cliquez sur la **Sécurité > les** onglets d'**AAA**. Vérifiez l'**authentification EAP locale** et sélectionnez le bon nom d'eap profile du comme indiqué dans cet exemple de menu déroulant :Vous pouvez également émettre la commande de configuration **wlan de *<wlan-id> de <profile-name> d'*enable de gens du pays-auth de config** CLI comme affiché ici :
```
(Cisco Controller) >config wlan local-auth enable EAP-test 1
```
7. Placez les paramètres de degré de sécurité de la couche 2.De l'interface gui, dans le WLAN éditez la fenêtre vont aux onglets de **Sécurité > de couche 2** et ont choisi **WPA+WPA2 du** menu déroulant de degré de sécurité de la couche 2. Sous WPA+WPA2 les paramètres sectionnent, placent le chiffrement WPA à **TKIP** et à chiffrement WPA2 **AES**. Cliquez ensuite sur **Apply**.Du CLI, utilisez ces commandes :
```
(Cisco Controller) >config wlan security wpa enable 1
(Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```
8. Vérifiez la configuration :
```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout ............................. Undefined

Configured EAP profiles:
    Name ........................................ EAP-test
      Certificate issuer ....................... cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No
      Enabled methods ........................... leap fast tls
      Configured on WLANs ....................... 1

EAP Method configuration:
    EAP-FAST:
--More-- or (q)uit
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 43697369f10000000000000000000
      Authority Information ..................... CiscoA-ID
```
Vous pouvez voir des paramètres spécifiques de 1 wlan avec la commande *<wlan d'id> de show wlan* :
```
(Cisco Controller) >show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... austinlab
Network Name (SSID).............................. austinlab
```

```
Status..................................... Disabled
MAC Filtering.............................. Disabled
Broadcast SSID............................. Enabled
AAA Policy Override........................ Disabled
Number of Active Clients................... 0
Exclusionlist Timeout...................... 60 seconds
Session Timeout............................ 1800 seconds
Interface.................................. management
WLAN ACL................................... unconfigured
DHCP Server................................ Default
DHCP Address Assignment Required........... Disabled
Quality of Service......................... Silver (best effort)
WMM........................................ Disabled
CCX - AironetIe Support.................... Enabled
CCX - Gratuitous ProbeResponse (GPR)....... Disabled
Dot11-Phone Mode (7920).................... Disabled
Wired Protocol............................. None
--More-- or (q)uit
IPv6 Support............................... Disabled
Radio Policy............................... All
Local EAP Authentication................... Enabled (Profile 'EAP-test')
Security

   802.11 Authentication:.................. Open System
   Static WEP Keys......................... Disabled
   802.1X.................................. Disabled
   Wi-Fi Protected Access (WPA/WPA2)....... Enabled
      WPA (SSN IE)......................... Enabled
         TKIP Cipher....................... Enabled
         AES Cipher........................ Disabled
      WPA2 (RSN IE)........................ Enabled
         TKIP Cipher....................... Disabled
         AES Cipher........................ Enabled
                                                    Auth Key Management
         802.1x............................ Enabled
         PSK............................... Disabled
         CCKM.............................. Disabled
   CKIP ..................................... Disabled
   IP Security............................... Disabled
   IP Security Passthru...................... Disabled
   Web Based Authentication.................. Disabled
--More-- or (q)uit
   Web-Passthrough........................... Disabled
   Conditional Web Redirect.................. Disabled
   Auto Anchor............................... Disabled
   Cranite Passthru.......................... Disabled
   Fortress Passthru......................... Disabled
   H-REAP Local Switching.................... Disabled
   Infrastructure MFP protection............. Enabled
                                         (Global Infrastructure MFP Disabled)
   Client MFP................................ Optional
   Tkip MIC Countermeasure Hold-down Timer... 60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

Il y a d'autres paramètres d'authentification locale qui peuvent être configurés, en particulier le temporisateur actif de délai d'attente. Ce temporisateur configure la période l'où l'EAP local est après tout les serveurs utilisés de RAYON ont manqué.Du GUI, choisissez la **Sécurité > EAP local > général** et placez la valeur temporelle. Cliquez ensuite sur **Apply**.Du CLI, émettez ces commandes :

```
(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
```

```
in seconds.
(Cisco Controller) >config local-auth active-timeout 60
```

Vous pouvez vérifier la valeur à laquelle ce temporisateur est installé quand vous émettez la commande de **show local-auth config**.

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout ............................. 60

Configured EAP profiles:
    Name ........................................ EAP-test
... Skip
```

9. Si vous devez générer et charger le manuel PAC, vous pouvez utiliser le GUI ou le CLI.Du GUI, les **COMMANDES** choisies du menu principal et ont choisi le **fichier de téléchargement de la** liste dans le côté droit. **PAC** choisi **(laisser-passer de Protected Access) du** type de fichier menu déroulant. Entrez tous les paramètres et cliquez sur en fonction le **téléchargement**.Du CLI, sélectionnez ces commandes :

```
(Cisco Controller) >transfer upload datatype pac
(Cisco Controller) >transfer upload pac ?

username     Enter the user (identity) of the PAC

 (Cisco Controller) >transfer upload pac test1 ?

<validity>     Enter the PAC validity period (days)

(Cisco Controller) >transfer upload pac test1 60 ?

<password>     Enter a password to protect the PAC

 (Cisco Controller) >transfer upload pac test1 60 cisco123

(Cisco Controller) >transfer upload serverip 10.1.1.1

(Cisco Controller) >transfer upload filename manual.pac

(Cisco Controller) >transfer upload start

Mode......................................... TFTP
TFTP Server IP............................... 10.1.1.1
TFTP Path.................................... /
TFTP Filename................................ manual.pac
Data Type.................................... PAC
PAC User..................................... test1
PAC Validity................................. 60 days
PAC Password................................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

Autorité de certification de Microsoft

Afin d'utiliser la version 2 d'EAP-FAST et l'authentification d'EAP-TLS, le WLC et tous périphériques de client doivent avoir un certificat valide et doivent également connaître le certificat

public de l'autorité de certification.

Installation

Si le Windows 2000 Server n'a pas déjà des services d'autorité de certification installés, vous devez les installer.

Terminez-vous ces étapes afin de lancer l'autorité de certification de Microsoft sur un Windows 2000 Server :

1. Du panneau de configuration, choisissez l'**Add/Remove Programs**. : :
2. **Add/Remove Windows Components** choisi du côté gauche.
3. **Services de certificat de** contrôle.Passez en revue cet avertissement avant que vous poursuiviez :
4. Sélectionnez que le type d'autorité de certification vous veulent installer. Afin de créer une autorité autonome simple, **racine autonome** choisie **CA.**
5. Écrivez les informations nécessaires au sujet de l'autorité de certification. Ces informations créent un certificat auto-signé pour votre autorité de certification. Souvenez-vous le nom CA que vous utilisez.L'autorité de certification enregistre les Certificats dans une base de données. Cet exemple utilise l'installation par défaut proposée par Microsoft :
6. Utilisation de services d'autorité de certification de Microsoft le serveur Web IIS Microsoft afin de créer et gérer des Certificats de client et serveur. Il doit redémarrer le service IIS pour ceci :Le Microsoft Windows 2000 Server installe maintenant le nouveau service. Vous devez avoir votre CD d'installation de Windows 2000 Server afin d'installer des composants de nouveau Windows.L'autorité de certification est maintenant installée.

Installez le certificat dans le contrôleur LAN de radio de Cisco

Afin d'utiliser la version 2 et l'EAP-TLS d'EAP-FAST sur le serveur local d'EAP d'un contrôleur LAN Sans fil de Cisco, suivez ces trois étapes :

1. Installez le certificat de périphérique sur le contrôleur LAN Sans fil.
2. Téléchargez un certificat de CA de constructeur au contrôleur LAN Sans fil.
3. Configurez le contrôleur LAN Sans fil pour utiliser l'EAP-TLS.

Notez que dans l'exemple présenté dans ce document, le serveur de contrôle d'accès (ACS) est installé sur le même hôte que la Microsoft Active Directory et l'autorité de certification de Microsoft, mais la configuration devrait être identique si le serveur ACS est sur un serveur différent.

Installez le certificat de périphérique sur le contrôleur LAN Sans fil

Procédez comme suit :

1. . Terminez-vous ces étapes afin de générer le certificat pour importer au WLC :Allez à **http://<serverIpAddr>/certsrv**.Choisissez la **demande un certificat** et cliquez sur Next.Choisissez la **demande avancée** et cliquez sur Next.Choisissez **soumettent une demande de certificat à ce CA utilisant une forme** et cliquent sur Next.Choisissez le **serveur Web** pour le modèle de certificat et écrivez les informations pertinentes. Marquez alors les clés comme **exportables**.Vous recevez maintenant un certificat que vous devez installer dans votre

ordinateur.

2. Terminez-vous ces étapes afin de récupérer le certificat du PC :Ouvrez un navigateur Internet Explorer et choisissez les **outils > les options Internet > le contenu**.**Certificats de** clic.Sélectionnez le certificat nouvellement installé du menu déroulant.**Exportation de** clic.Cliquez sur Next deux fois et choisissez **oui l'exportation la clé privée**. Ce format est le PKCS#12 (format .PFX).Choisissez Enable la **protection forte**.Tapez un mot de passe.Archivez-le dans un fichier <tme2.pfx>.
3. Copiez le certificat dans le format PKCS#12 sur n'importe quel ordinateur où vous faites installer Openssl afin de le convertir en format PEM.

```
(Cisco Controller) >transfer upload datatype pac
(Cisco Controller) >transfer upload pac ?

username     Enter the user (identity) of the PAC

 (Cisco Controller) >transfer upload pac test1 ?

<validity>     Enter the PAC validity period (days)

(Cisco Controller) >transfer upload pac test1 60 ?

<password>     Enter a password to protect the PAC

 (Cisco Controller) >transfer upload pac test1 60 cisco123

(Cisco Controller) >transfer upload serverip 10.1.1.1

(Cisco Controller) >transfer upload filename manual.pac

(Cisco Controller) >transfer upload start

Mode..................................................... TFTP
TFTP Server IP........................................... 10.1.1.1
TFTP Path................................................ /
TFTP Filename............................................ manual.pac
Data Type................................................ PAC
PAC User................................................. test1
PAC Validity............................................. 60 days
PAC Password............................................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

4. Téléchargez le certificat converti de périphérique de formatage PEM sur le WLC.

```
(Cisco Controller) >transfer download datatype eapdevcert

(Cisco Controller) >transfer download certpassword password
!--- From step 3. Setting password to <cisco123> (Cisco Controller) >transfer download
filename tme2.pem

(Cisco Controller) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Vendor Dev Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ tme2.pem

This may take some time.
```

```
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

5. Une fois que redémarré, vérifiez le certificat.

```
(Cisco Controller) >show local-auth certificates

Certificates available for Local EAP authentication:

Certificate issuer ............................ vendor
  CA certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
  Device certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT
```

Téléchargez un certificat de CA de constructeur au contrôleur LAN Sans fil

Procédez comme suit :

1. Terminez-vous ces étapes afin de récupérer le certificat de CA de constructeur :Allez à **http://<serverIpAddr>/certsrv**.Choisissez **récupèrent le certificat de CA** et cliquent sur Next.Choisissez le certificat de CA.Clic **DER encodé**.Cliquez sur en fonction le **certificat de CA de téléchargement** et sauvegardez le certificat comme **rootca.cer**.
2. Convertissez le constructeur que le CA du format DER dans le format PEM avec l'**openssl x509 - dans rootca.cer - informent DER - rootca.pem - commande PEM d'outform**.Le fichier de sortie est rootca.pem dans le format PEM.
3. Téléchargez le certificat de CA de constructeur :

```
(Cisco Controller) >transfer download datatype eapcacert

(Cisco Controller) >transfer download filename ?

<filename>     Enter filename up to 16 alphanumeric characters.

(Cisco Controller) >transfer download filename rootca.pem

(Cisco Controller) >transfer download start ?

(Cisco Controller) >transfer download start

Mode.......................................... TFTP
Data Type..................................... Vendor CA Cert
TFTP Server IP................................ 10.1.1.12
TFTP Packet Timeout........................... 6
TFTP Max Retries.............................. 10
TFTP Path..................................... /
TFTP Filename................................. rootca.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.

Certificate installed.
```

```
Reboot the switch to use new certificate.
```

Configurez le contrôleur LAN Sans fil pour utiliser l'EAP-TLS

Procédez comme suit :

Du GUI, choisissez la **Sécurité > EAP local > profils**, choisissez le profil et vérifiez ces configurations :

- Le certificat local exigé est activé.
- Le certificat client exigé est activé.
- L'émetteur de certificat est constructeur.
- Le contrôle contre des Certificats CA est activé.

Installez le certificat d'autorité de certification sur le périphérique de client

Téléchargez et installez un certificat de CA de racine pour le client

Le client doit obtenir un certificat de CA de racine d'un serveur d'autorité de certification. Il y a plusieurs méthodes que vous pouvez employer pour obtenir un certificat client et pour l'installer sur l'ordinateur Windows XP. Afin de saisir un certificat valide, l'utilisateur de Windows XP doit être ouvert une session utilisant leur user-id et doit avoir une connexion réseau.

Un navigateur Web sur le client de Windows XP et une connexion câblée au réseau ont été utilisés pour obtenir un certificat client du serveur privé d'autorité de certification racine. Cette procédure est utilisée pour obtenir le certificat client d'un serveur d'autorité de certification de Microsoft :

1. Utilisez un navigateur Web sur le client et indiquez le navigateur le serveur d'autorité de certification. Afin de faire ceci, entrez dans **http://IP-address-of-Root-CA/certsrv**.
2. Procédure de connexion utilisant **Domain_Name \ user_name**. Vous devez ouvrir une session utilisant le nom d'utilisateur de la personne qui est d'utiliser le client de XP.
3. Sur la fenêtre bienvenue, choisissez **récupèrent un certificat de CA** et cliquent sur Next.
4. **Certificat de CA du codage Base64** choisi et du **téléchargement**.
5. Sur le certificat délivré la fenêtre, clic **installent ce certificat** et cliquent sur Next.
6. Choisissez **automatiquement choisi la mémoire de certificat** et cliquez sur Next, pour le message réussi d'importation.
7. Connectez à l'autorité de certification pour récupérer le certificat d'autorité de certification :
8. Cliquez sur **Download CA certificate**.
9. Afin de vérifier que le certificat d'autorité de certification est correctement installé, Internet Explorer ouvert et choisir des **outils > des options Internet > le contenu > des Certificats**.Dans l'Autorité de certification racine approuvée, vous devriez voir votre autorité nouvellement installée de certification :

Générez un certificat client pour un périphérique de client

Le client doit obtenir un certificat d'un serveur d'autorité de certification pour que le WLC

authentifie un client d'EAP-TLS WLAN. Il y a plusieurs méthodes que vous pouvez employer afin d'obtenir un certificat client et l'installer sur l'ordinateur Windows XP. Afin de saisir un certificat valide, l'utilisateur de Windows XP doit être ouvert une session utilisant leur user-id et doit avoir une connexion réseau (une connexion câblée ou une connexion WLAN avec la Sécurité de 802.1x désactivée).

Un navigateur Web sur le client de Windows XP et une connexion câblée au réseau sont utilisés pour obtenir un certificat client du serveur privé d'autorité de certification racine. Cette procédure est utilisée pour obtenir le certificat client d'un serveur d'autorité de certification de Microsoft :

1. Utilisez un navigateur Web sur le client et indiquez le navigateur le serveur d'autorité de certification. Afin de faire ceci, entrez dans **http://IP-address-of-Root-CA/certsrv**.
2. Procédure de connexion utilisant **Domain_Name \ user_name**. Vous devez ouvrir une session utilisant le nom d'utilisateur de la personne qui utilise le client de XP. (Le nom d'utilisateur obtient encastré dans le certificat client.)
3. Sur la fenêtre bienvenue, choisissez la **demande un certificat** et cliquez sur Next.
4. Choisissez la **demande avancée** et cliquez sur Next.
5. Choisissez **soumettent une demande de certificat à ce CA utilisant une forme** et cliquent sur Next.
6. Sur la forme avancée de demande de certificat, choisissez le modèle de certificat comme **utilisateur**, spécifiez la taille de clé en tant que **1024** et cliquez sur Submit.
7. Sur le certificat délivré la fenêtre, clic **installent ce certificat**. Ceci a comme conséquence l'installation réussie d'un certificat client sur le client de Windows XP.
8. **Certificat** choisi d'**authentification client**.Le certificat client est maintenant créé.
9. Afin de vérifier que le certificat est installé, allez à l'Internet Explorer et choisissez les **outils > les options Internet > le contenu > les Certificats**. Dans l'onglet personnel, vous devriez voir le certificat.

EAP-TLS avec le Cisco Secure Services Client sur le périphérique de client

Procédez comme suit :

1. Le WLC, par défaut, annonce le SSID, ainsi on lui affiche dans la liste de réseaux de création de SSID balayé. Afin de créer un profil réseau, vous pouvez cliquer sur le SSID dans la liste (entreprise) et le clic **créent le réseau**.Si l'infrastructure WLAN est configurée avec l'émission SSID désactivée, vous devez manuellement ajouter le SSID. Afin de faire ceci, cliquez sur Add sous des périphériques d'Access et écrivez manuellement le SSID approprié (par exemple, entreprise). Configurez le comportement actif de sonde pour le client. C'est-à-dire, où le client sonde activement pour son SSID configuré. Spécifiez **recherchent activement ce périphérique d'accès** après que vous écriviez le SSID sur la fenêtre de périphérique d'Access d'ajouter.**Note**: Les configurations de port ne permettent pas des modes entreprises (802.1X) si les configurations d'authentification EAP ne sont pas des premières configurées pour le profil.
2. Le clic **créent le réseau** afin de lancer la fenêtre de profil réseau, qui te permet pour associer (ou configuré) le SSID choisi avec un mécanisme d'authentification. Assignez un nom descriptif pour le profil.**Note**: La plusieurs Sécurité WLAN tape et/ou le SSID peut être associé sous ce profil d'authentification.

3. Activez l'authentification et vérifiez la méthode d'EAP-TLS. Cliquez sur Configure alors afin de configurer des propriétés d'EAP-TLS.
4. Sous le résumé de configuration réseau, le clic **modifient** afin de configurer l'EAP/configurations de qualifications.
5. Spécifiez **activent l'authentification**, choisissent l'**EAP-TLS** sous Protocol, et choisissent le **nom d'utilisateur** comme identité.
6. Spécifiez l'**utilisation simple se connectent des qualifications** pour utiliser des qualifications de login pour l'authentification de réseau. Cliquez sur Configure pour installer des paramètres d'EAP-TLS.
7. Afin d'avoir une configuration sécurisée d'EAP-TLS que vous devez vérifier le certificat de serveur de RAYON. Afin de faire ceci, le contrôle **valident le certificat de serveur**.
8. Afin de valider le certificat de serveur de RAYON, vous devez fournir les informations de Cisco Secure Services Client afin de recevoir seulement le certificat droit. Choisissez le **client > a fait confiance que les serveurs > gèrent les serveurs de confiance par utilisateur courant**.
9. Donnez un nom pour la règle et vérifiez le nom du certificat de serveur.La configuration d'EAP-TLS est de finition.
10. Connectez au profil réseau Sans fil. Le Cisco Secure Services Client demande l'ouverture de session utilisateur :Le Cisco Secure Services Client reçoit le certificat de serveur et le vérifie (la règle configurée et l'autorité de certification étant installé). Il demande alors le certificat pour l'utiliser pour l'utilisateur.
11. Après que le client authentifie, choisissez le **SSID** sous le profil dans l'onglet de réseaux de gérer et cliquez sur l'**état** pour questionner des détails de connexion.La fenêtre de détails de connexion fournit des informations sur le périphérique de client, l'état de la connexion et les statistiques, et la méthode d'authentification. L'onglet de détails de WiFi fournit des détails sur l'état de la connexion de 802.11, qui inclut le RSSI, le canal de 802.11, et l'authentification/cryptage.

Commandes de débogage

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Ces commandes de débogage peuvent être utilisées au WLC pour surveiller la progression de l'échange d'authentification :

- **enable d'événements de debug aaa**
- **enable de détail de debug aaa**
- **enable d'événements de debug dot1x**
- **enable d'états de debug dot1x**
- **enable d'événements de debug aaa local-auth eap**OU
- **debug aaa all enable**

Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.1
- Support de technologie WLAN
- Support et documentation techniques - Cisco Systems