Exemple de configuration de RSA SecurID avec des contrôleurs de réseau local sans fil et Cisco Secure ACS

Contenu

Introduction

Ce document explique comment installer et configurer le point d'accès léger de Cisco Protocol (LWAPP) - aps capables et contrôleurs LAN Sans fil (WLCs), aussi bien que le Cisco Secure Access Control Server (ACS) à utiliser dans un environnement authentifié par SecurID RSA WLAN. Des guides d'implémentation de SecurID-particularité RSA peuvent être trouvés chez www.rsasecured.com.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de WLCs et comment configurer les paramètres de base WLC.
- La connaissance sur la façon dont configurer le profil du client sans fil de Cisco utilisant Aironet Desktop Utility (ADU).

- Ayez la connaissance fonctionnelle du Cisco Secure ACS.
- Ayez la connaissance de base de LWAPP.
- Ayez la compréhension de base des services de Répertoire actif de Microsoft Windows (AD), aussi bien que le contrôleur de domaine et les concepts de DN.**Remarque:** Avant que vous tentiez cette configuration, assurez-vous que les ACS et le serveur de gestionnaire d'authentification RSA sont dans le même domaine et leur horloge système est exactement synchronisée. Si vous utilisez des services d'AD de Microsoft Windows, référez-vous à la documentation Microsoft serveur pour configurer ACS et RSA gestionnaire dans le même domaine. Référez-vous configurent la base de données de Répertoire actif et d'utilisateur Windows pour information les informations pertinentes.

Composants utilisés

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

- Manager 6.1 d'authentification RSA
- Agent 6.1 d'authentification RSA pour Microsoft Windows
- Construction 27 du Cisco Secure ACS 4.0(1)**Remarque:** Le serveur de RADIUS qui est inclus peut être utilisé au lieu de Cisco ACS. Voyez la documentation de RADIUS qui a été incluse avec le gestionnaire d'authentification RSA sur la façon dont configurer le serveur.
- Cisco WLC et Point d'accès léger pour la version 4.0 (version 4.0.155.0)

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.

Conventions

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

Informations générales

Le système RSA SecurID est une solution à deux facteurs d'authentification de l'utilisateur. Utilisé en même temps que le gestionnaire d'authentification RSA et un agent d'authentification RSA, l'authentificateur RSA SecurID exige des utilisateurs de s'identifier utilisant un mécanisme d'authentification à deux facteurs.

On est le code RSA SecurID, un nombre aléatoire a généré toutes les 60 secondes sur le périphérique d'authentificateur RSA SecureID. L'autre est le numéro d'identification personnel (PIN).

Les authentificateurs RSA SecurID sont aussi simples pour les utiliser en tant qu'écrire un mot de passe. Chaque utilisateur final est assigné un authentificateur RSA SecurID qui génère un code d'un-temps-utilisation. En ouvrant une session, l'utilisateur écrit simplement ce nombre et un PIN de secret à authentifier avec succès. Comme un avantage ajouté, des jetons de matériel RSA SecurID sont habituellement préprogrammés pour être entièrement - fonctionnel sur la réception.

Cette démonstration instantanée explique comment utiliser un périphérique d'authentificateur de secureID RSA : Démonstration RSA.

Par le programme prêt RSA SecurID, les serveurs de Cisco WLC et de Cisco Secure ACS prennent en charge le juste d'authentification RSA SecurID hors de la case. Les demandes d'accès d'interceptions de logiciel agent d'authentification RSA, si les gens du pays ou le distant, des utilisateurs (ou des groupes d'utilisateurs) et les dirige vers le programme de gestionnaire d'authentification RSA pour l'authentification.

Le logiciel de gestionnaire d'authentification RSA est le composant de Gestion de la solution RSA SecurID. Il est utilisé pour vérifier des demandes d'authentification et pour gérer centralement des stratégies d'authentification pour des réseaux d'entreprise. Cela fonctionne en même temps que les authentificateurs RSA SecurID et le logiciel agent d'authentification RSA.

Dans ce document, un serveur ACS de Cisco est utilisé comme agent d'authentification RSA en installant le logiciel agent là-dessus. Le WLC est le serveur d'accès à distance (NAS) (client d'AAA) qui consécutivement en avant les authentifications client à l'ACS. Le document explique les concepts et l'installation utilisant l'authentification client du Protected Extensible Authentication Protocol (PEAP).

Afin de se renseigner sur l'authentification PEAP, référez-vous au Protected Extensible Authentication Protocol de Cisco.

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Ce document utilise les configurations suivantes :

- Configuration d'hôte d'agent
- Configuration d'agent d'authentification

Configuration d'hôte d'agent

Utilisant le Cisco Secure ACS en tant que serveur de RADIUS

Afin de faciliter la transmission entre le Cisco Secure ACS et l'appliance du gestionnaire d'authentification RSA/RSA SecurID, un enregistrement d'hôte d'agent doit être ajouté à la base de données de gestionnaire d'authentification RSA. L'enregistrement d'hôte d'agent identifie le Cisco Secure ACS dans sa base de données et contient des informations sur la transmission et le cryptage.

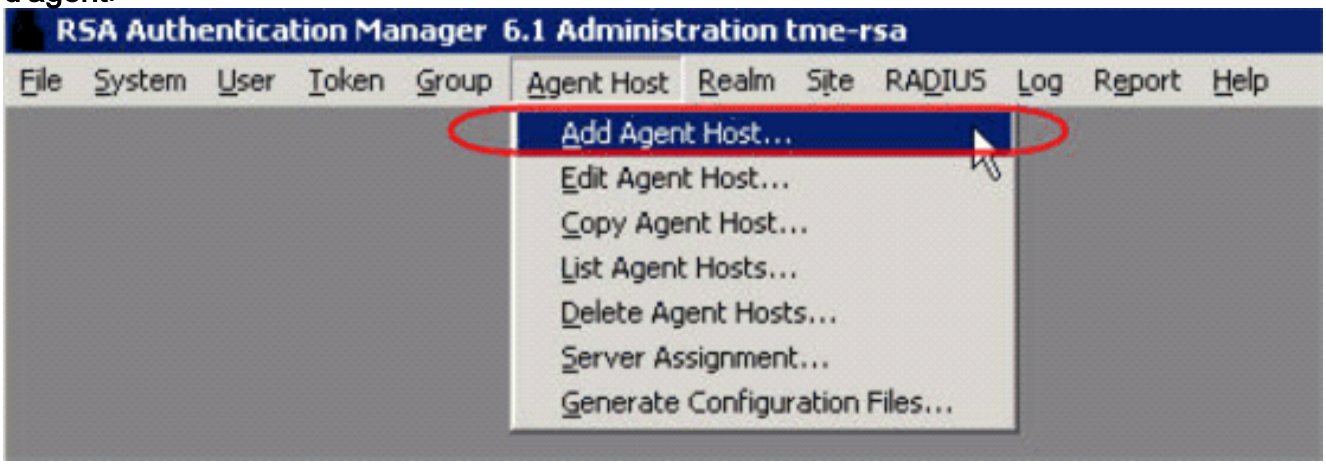
Afin de créer l'enregistrement d'hôte d'agent, vous avez besoin de ces informations :

- Adresse Internet du serveur ACS de Cisco
- Adresses IP pour toutes les interfaces réseau du serveur ACS de Cisco

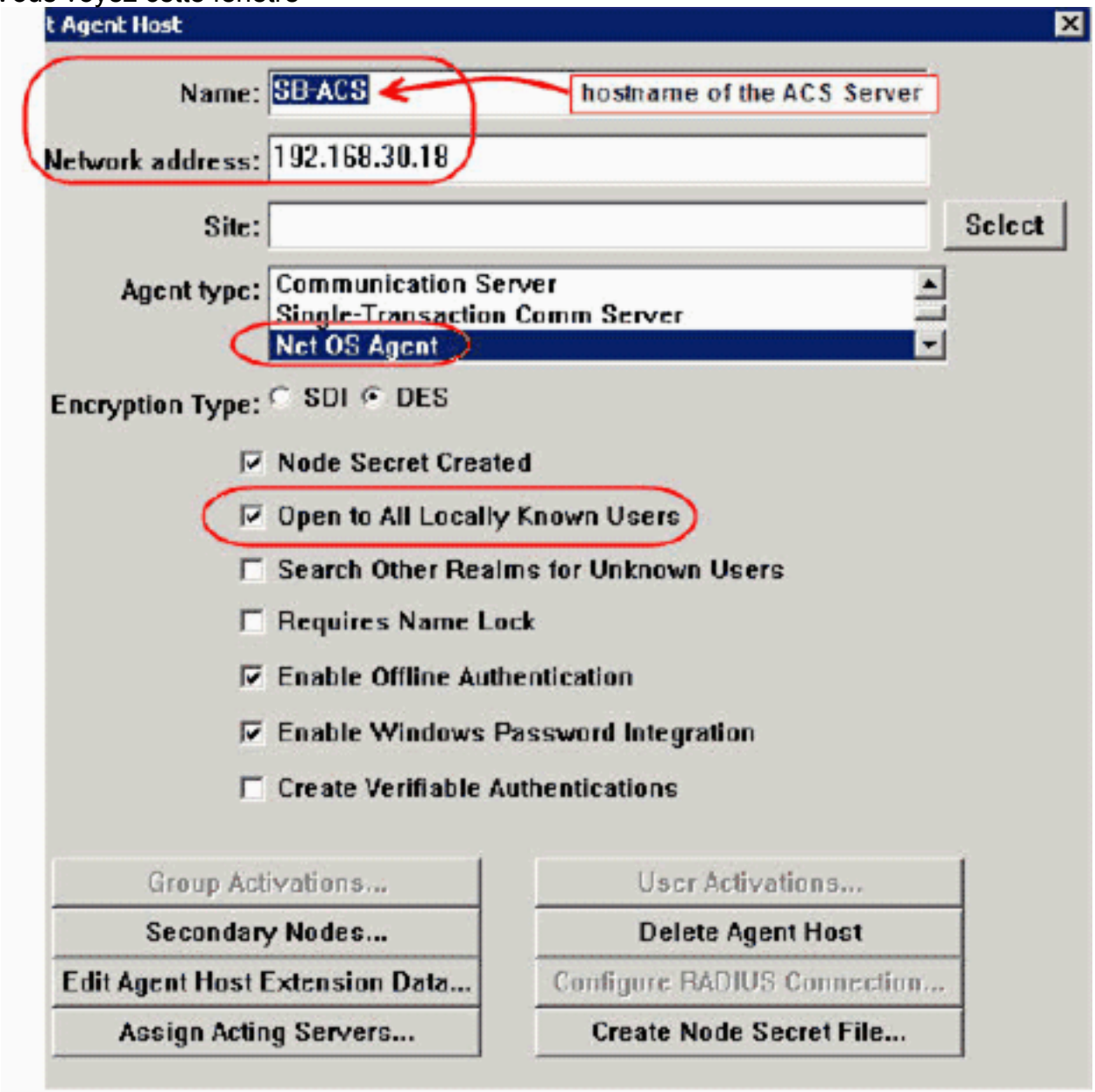
Procédez comme suit :

1. Ouvrez l'application de mode d'hôte de gestionnaire d'authentification RSA.

2. **L'hôte** choisi d'**agent > ajoutent l'hôte d'agent**.



Vous voyez cette fenêtre



:

3. Écrivez l'information correcte pour le nom et l'adresse réseau de serveur ACS de Cisco. Choisissez **NetOS** pour le type d'agent et vérifiez la case à cocher pour **Open à tous les utilisateurs localement connus**.
4. Cliquez sur **OK**.

Utilisant le serveur de RADIUS de Manager 6.1 d'authentification RSA

Afin de faciliter la transmission entre le Cisco WLC et le gestionnaire d'authentification RSA, un enregistrement d'hôte d'agent doit être ajouté à la base de données de gestionnaire d'authentification RSA et à la base de données du serveur de RADIUS. L'enregistrement d'hôte d'agent identifie le Cisco WLC dans sa base de données et contient des informations sur la transmission et le cryptage.

Afin de créer l'enregistrement d'hôte d'agent, vous avez besoin de ces informations :

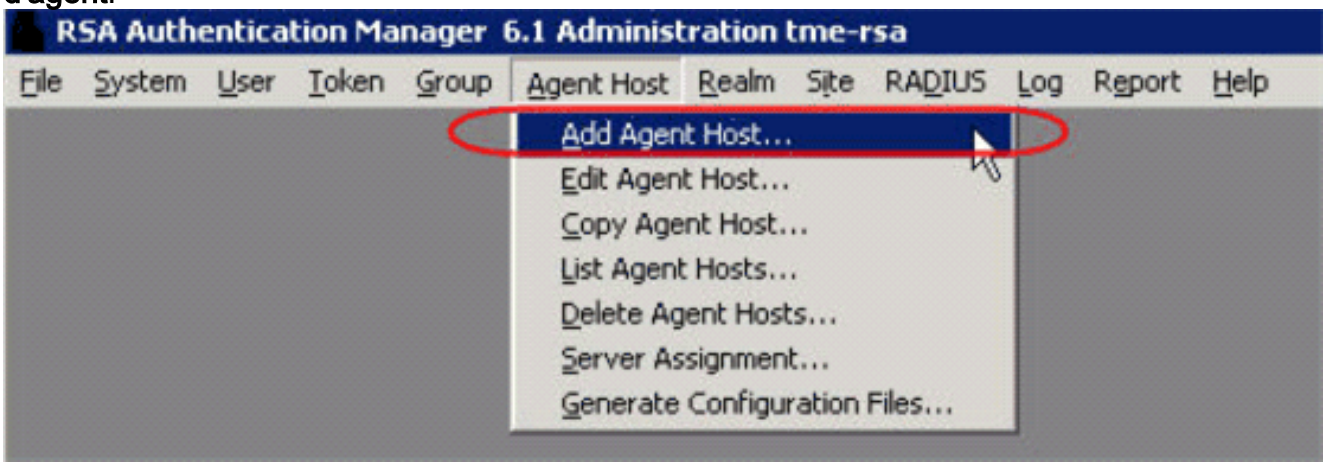
- L'adresse Internet de WLC
- Adresses IP de Gestion du WLC
- Secret de RADIUS, qui doit apparier le secret de RADIUS sur le Cisco WLC

En ajoutant l'enregistrement d'hôte d'agent, le rôle du WLC est configuré en tant que serveur de communication. Cette configuration est utilisée par le gestionnaire d'authentification RSA pour déterminer comment la transmission avec le WLC se produira.

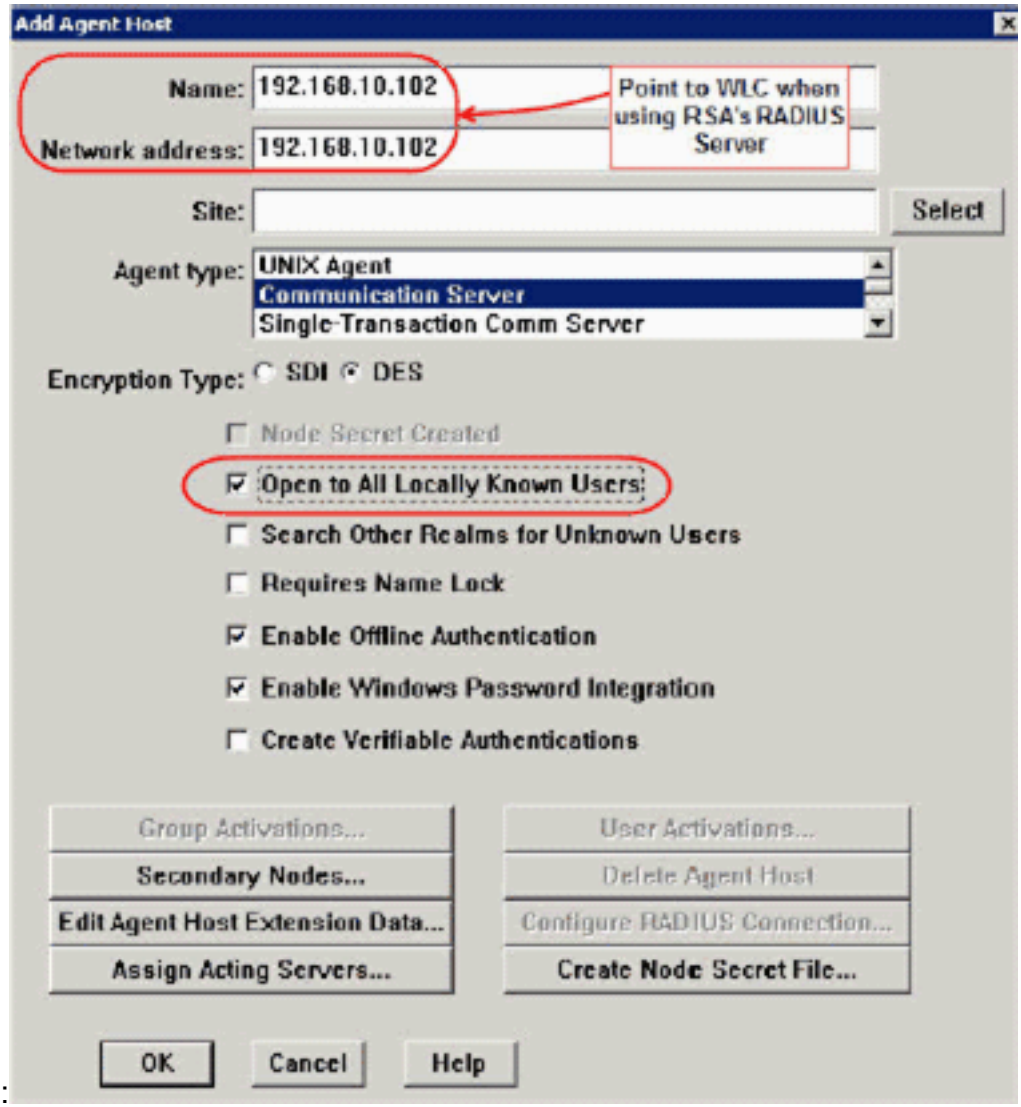
Remarque: Les adresses Internet dans l'appliance du gestionnaire d'authentification RSA/RSA SecurID doivent les résoudre aux adresses IP valides sur le réseau local.

Procédez comme suit :

1. Ouvrez l'application de mode d'hôte de gestionnaire d'authentification RSA.
2. **L'hôte** choisi d'**agent > ajoutent l'hôte d'agent**.

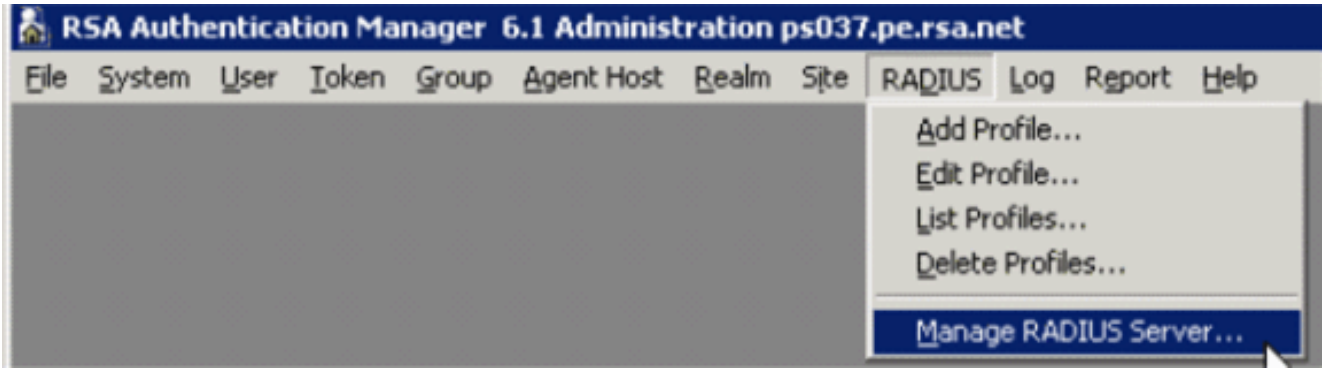


Vous voyez cette fenêtre



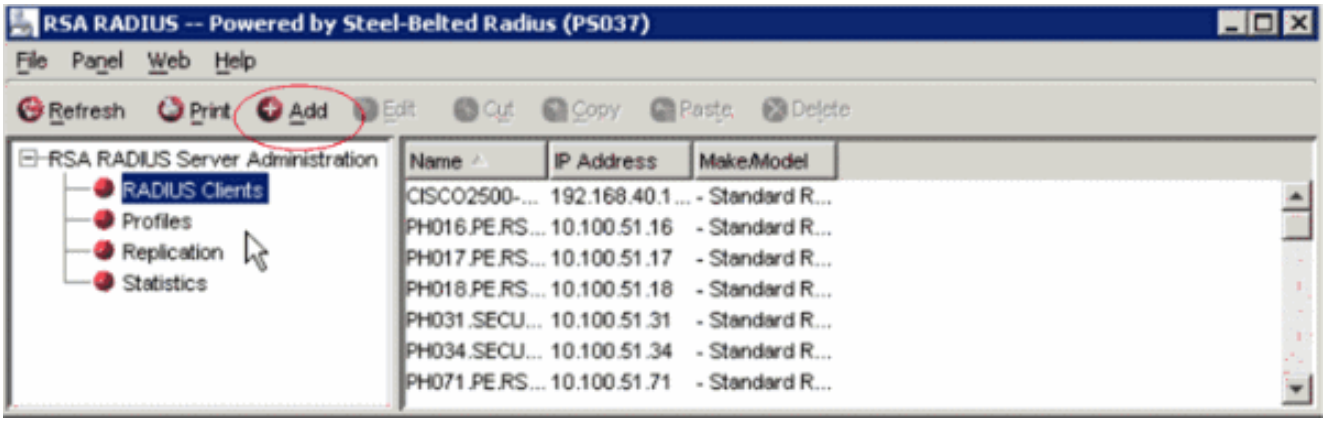
:

3. Écrivez l'information correcte pour l'adresse Internet WLC (un FQDN résoluble, s'il y a lieu) et l'adresse réseau. Choisissez le **serveur de communication** pour le type d'agent et vérifiez la case à cocher pour **Open à tous les utilisateurs localement connus**.
4. Cliquez sur **OK**.
5. Du menu, **RADIUS** choisi > **gèrent le serveur de RADIUS**.

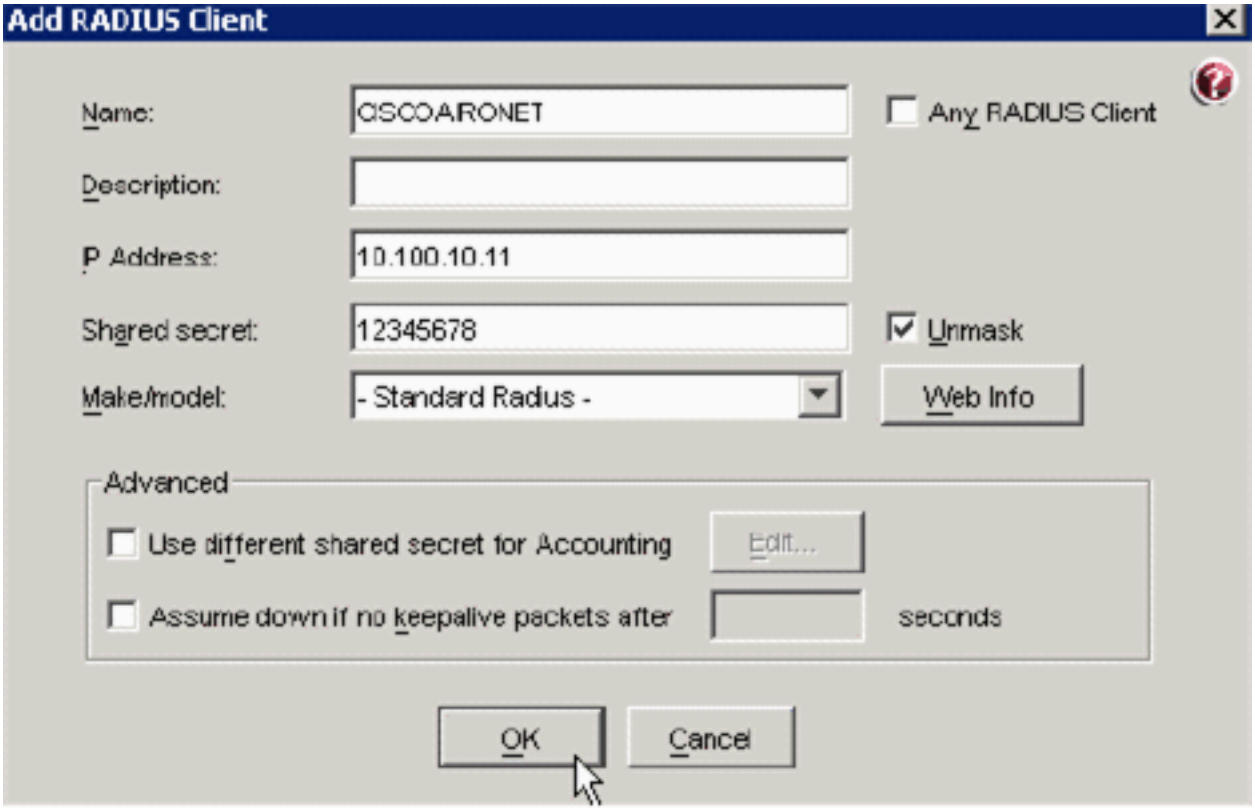


Une nouvelle fenêtre de gestion s'ouvre.

6. Dans cette fenêtre, les **clients RADIUS** choisis, cliquent sur Add alors.



7. Écrivez l'information correcte pour le Cisco WLC. Le secret partagé doit apparier le secret partagé défini sur le Cisco
WLC.



8. Cliquez sur **OK**.

Configuration d'agent d'authentification

Cette table représente la fonctionnalité d'agent d'authentification RSA d'ACS :

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS, Both
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

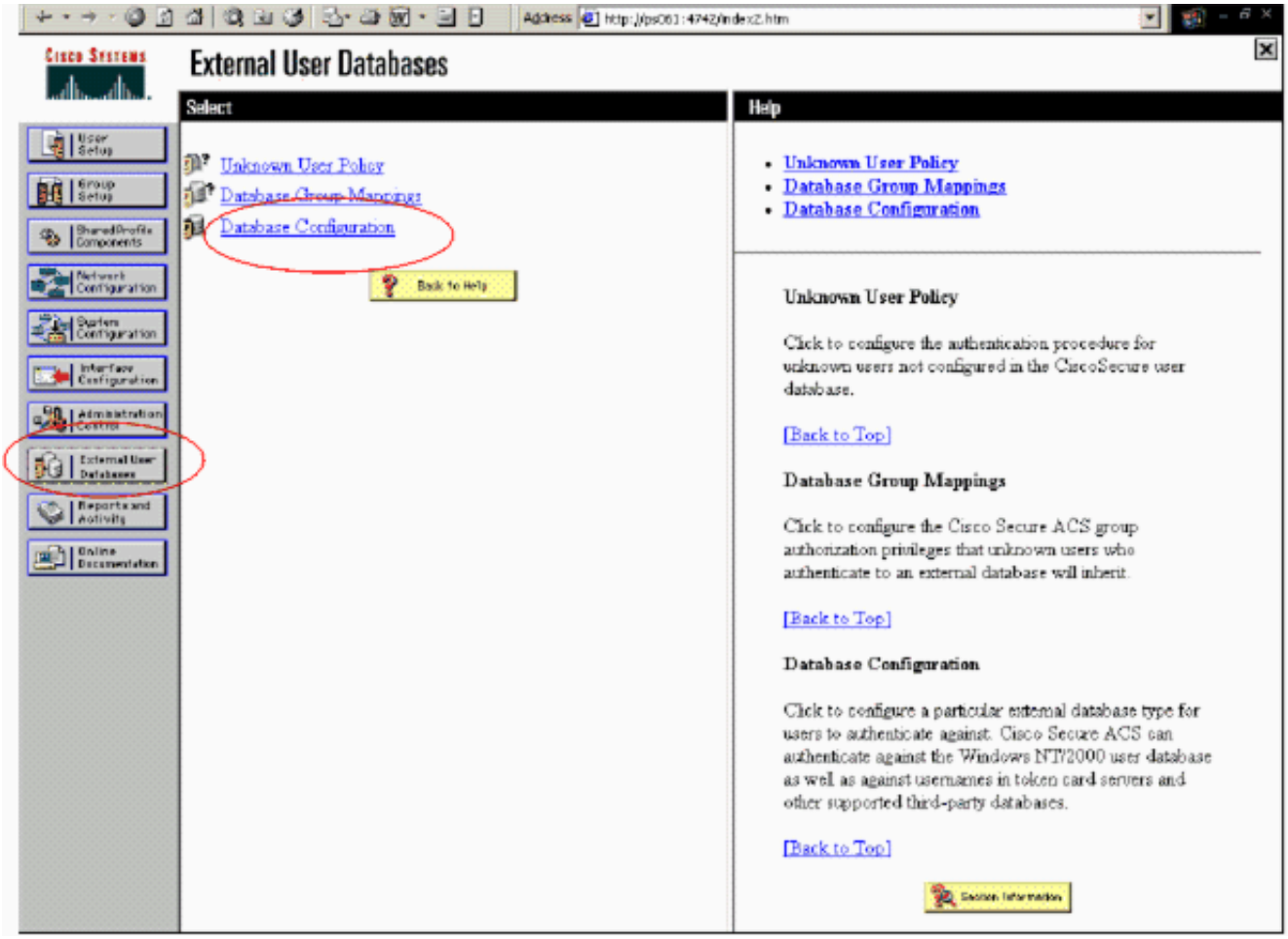
Remarque: Voyez la documentation de RADIUS qui a été incluse avec le gestionnaire d'authentification RSA sur la façon dont configurer le serveur de RADIUS, si c'est le serveur de RADIUS qui sera utilisé.

Configurez Cisco ACS

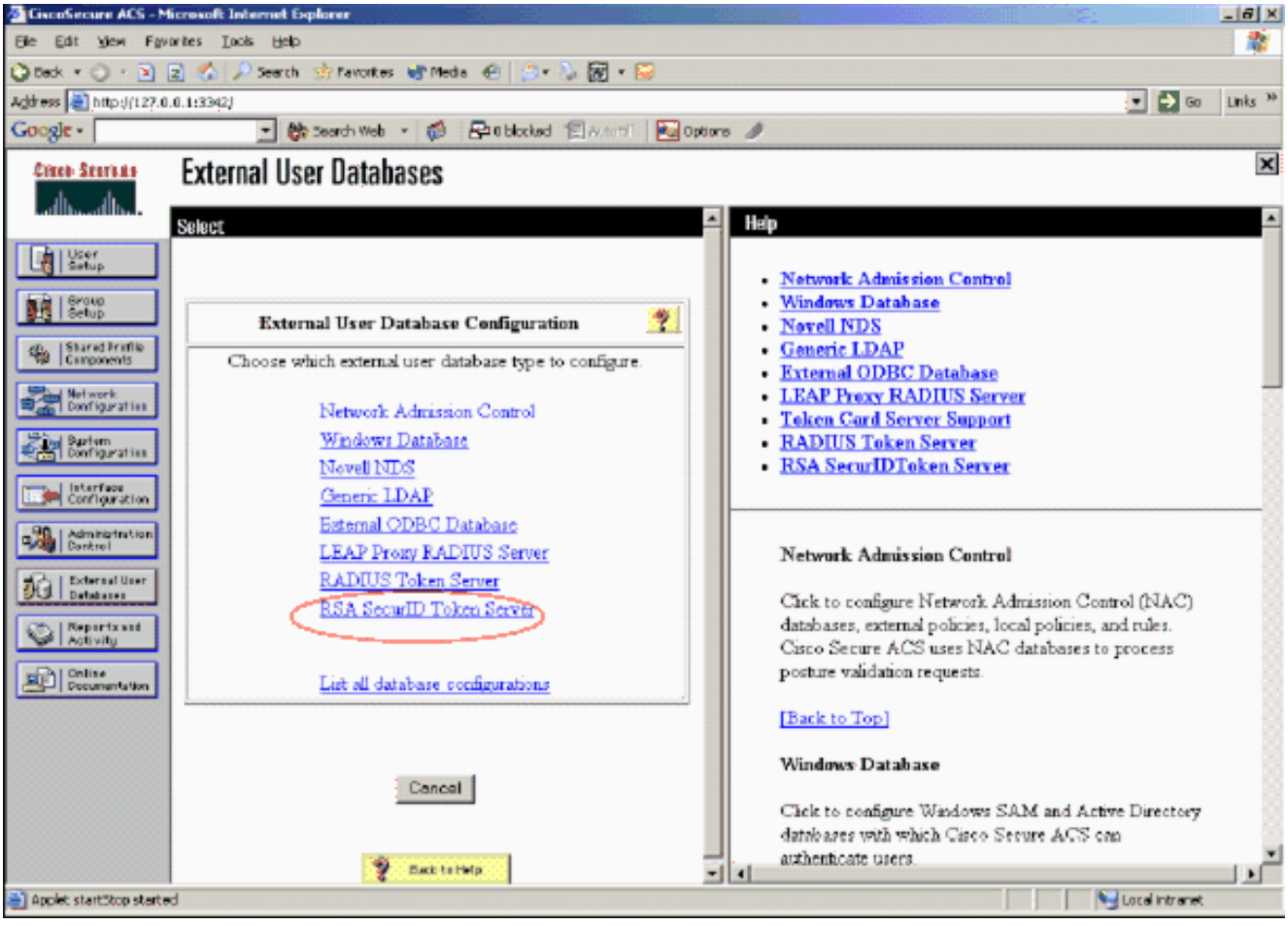
Lancez l'authentification RSA SecurID

Le Cisco Secure ACS prend en charge l'authentification RSA SecurID des utilisateurs. Terminez-vous ces étapes afin de configurer le Cisco Secure ACS pour authentifier des utilisateurs avec le Manager 6.1 d'authentification :

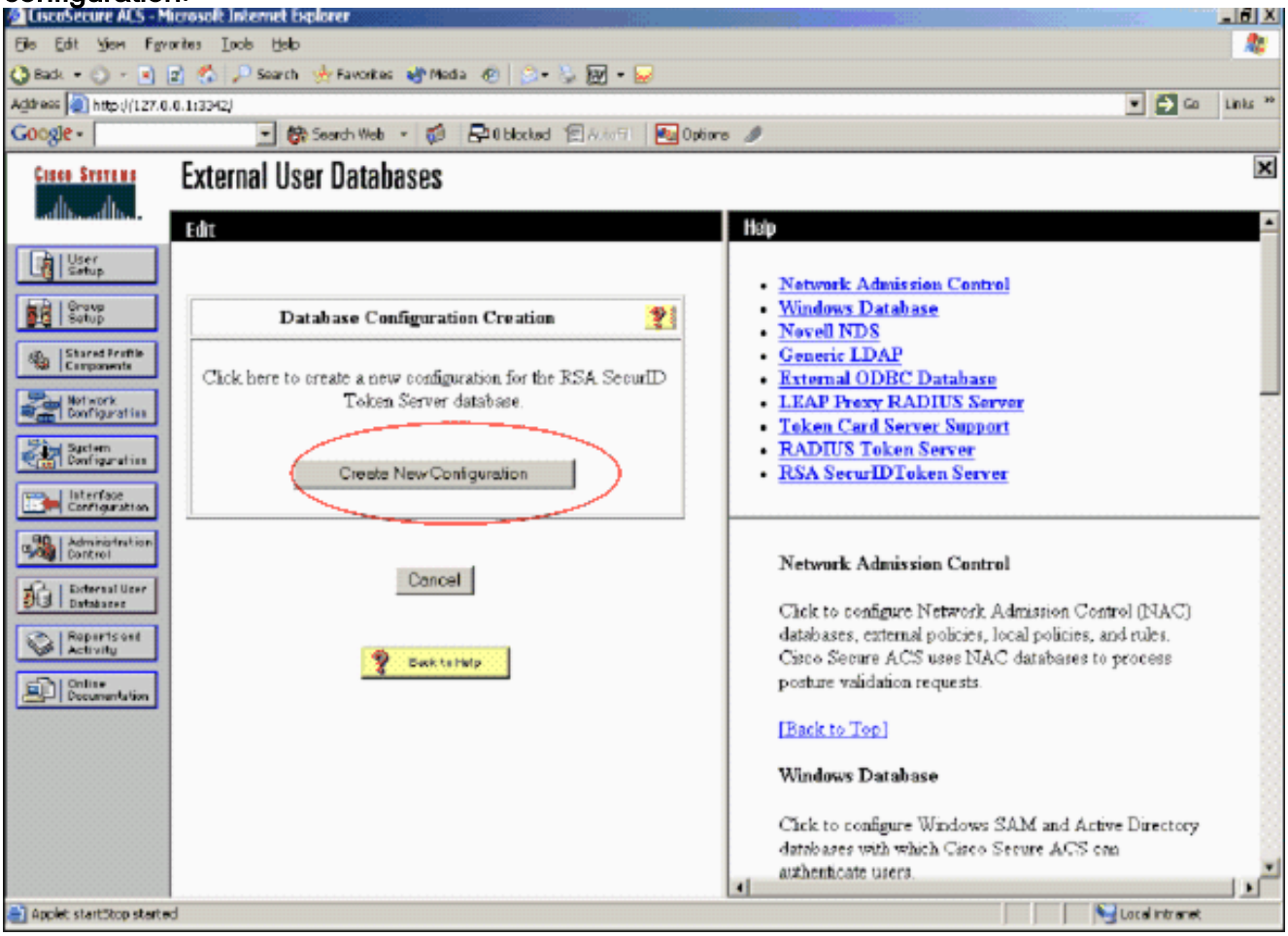
1. Installez l'agent d'authentification RSA 5.6 ou plus tard pour Windows sur le même système que le serveur de Cisco Secure ACS.
2. Vérifiez la Connectivité en exécutant la fonction de test d'authentification de l'agent d'authentification.
3. Copiez le fichier aceclnt.dll à partir du **répertoire de gestionnaire \ prog d'authentification de la Sécurité de** c:\Program Files\RSA de serveur RSA **\ RSA** sur le **répertoire de** c:\WINNT\system32 du serveur ACS.
4. Dans la barre de navigation, **base de données d'utilisateur externe de** clic. Puis, **configuration de base de données de** clic dans la page de base de données externe.



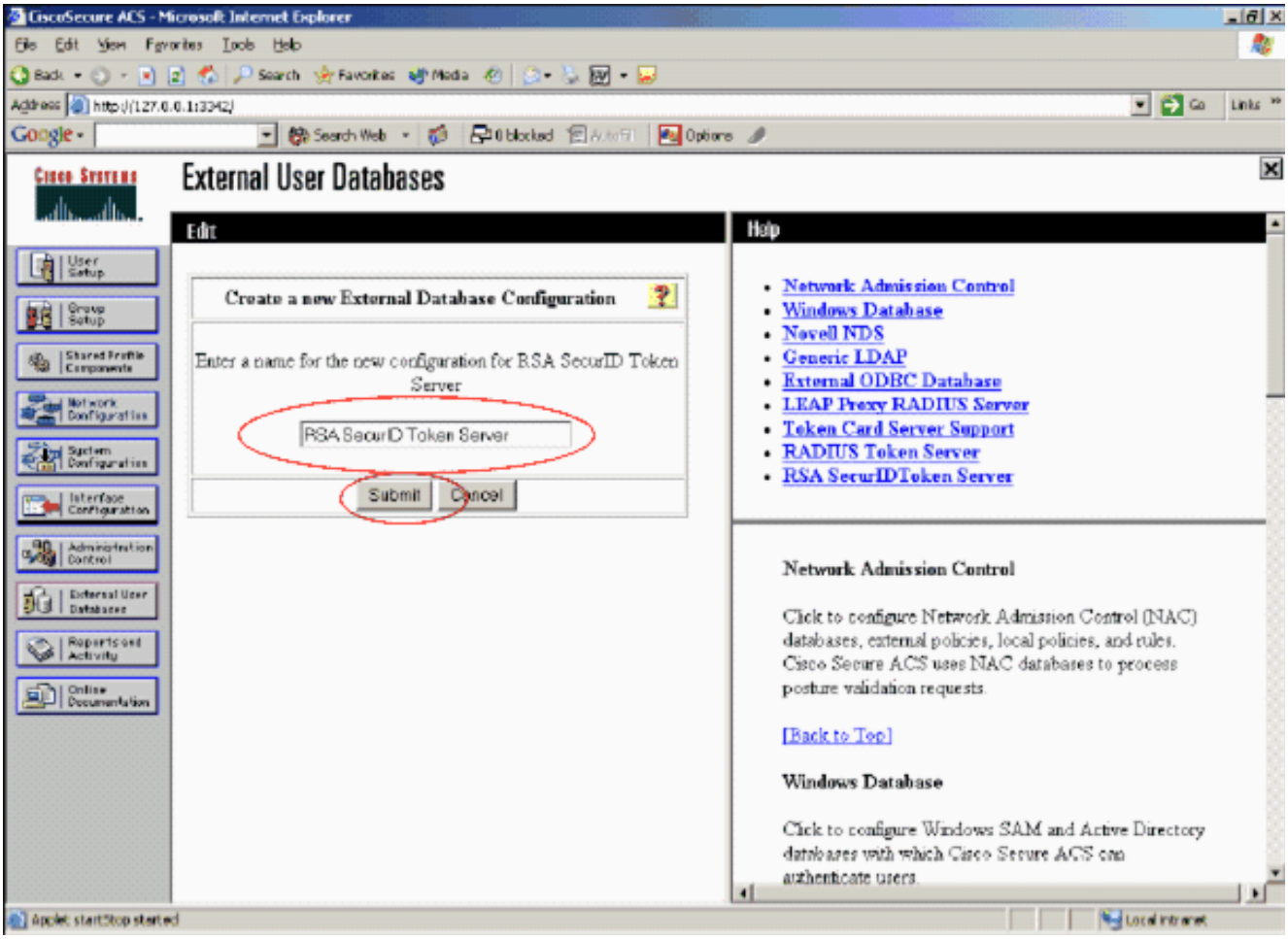
5. Dans la page de configuration de base de données d'utilisateur externe, **serveur de jetons du** clic **RSA SecurID**.



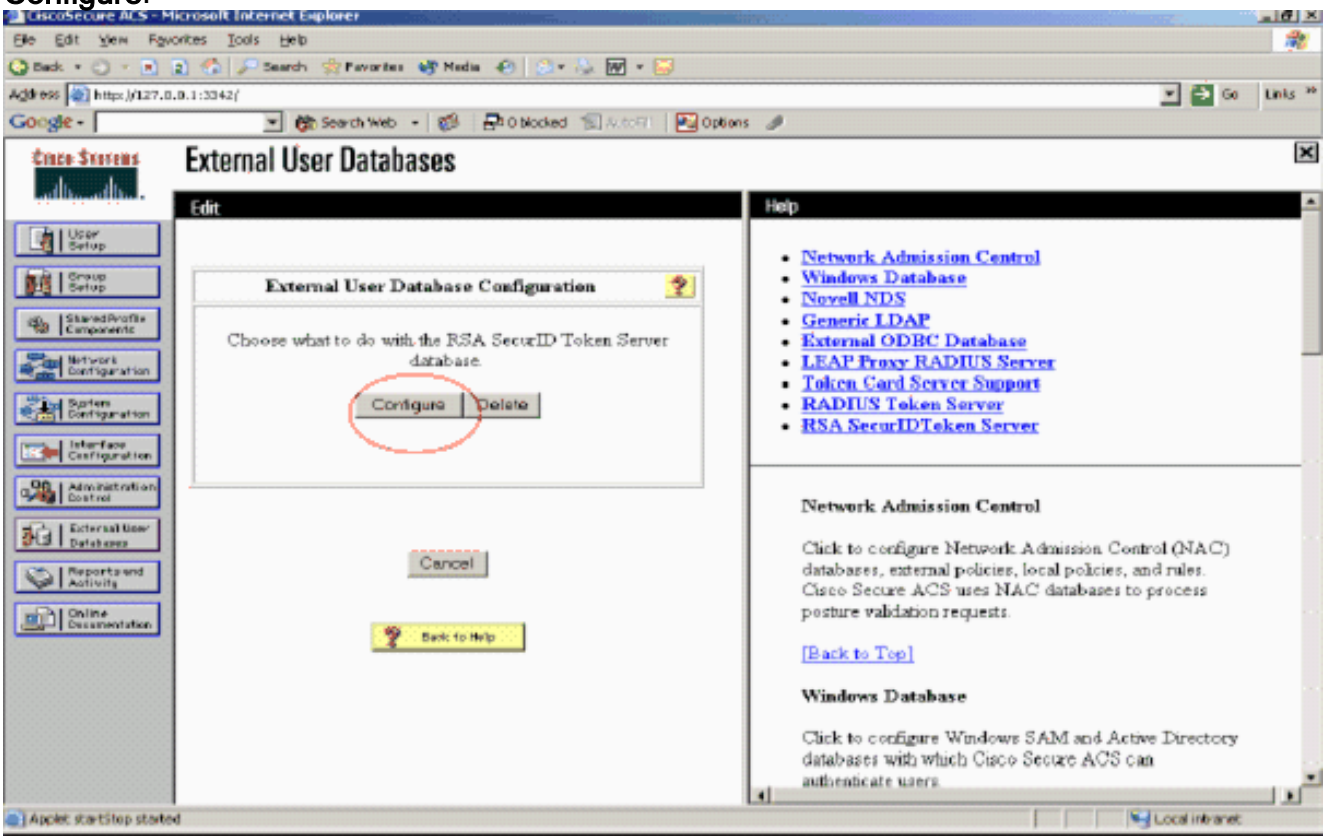
6. Le clic **créent la nouvelle configuration**.



7. Écrivez un nom, puis cliquez sur Submit.

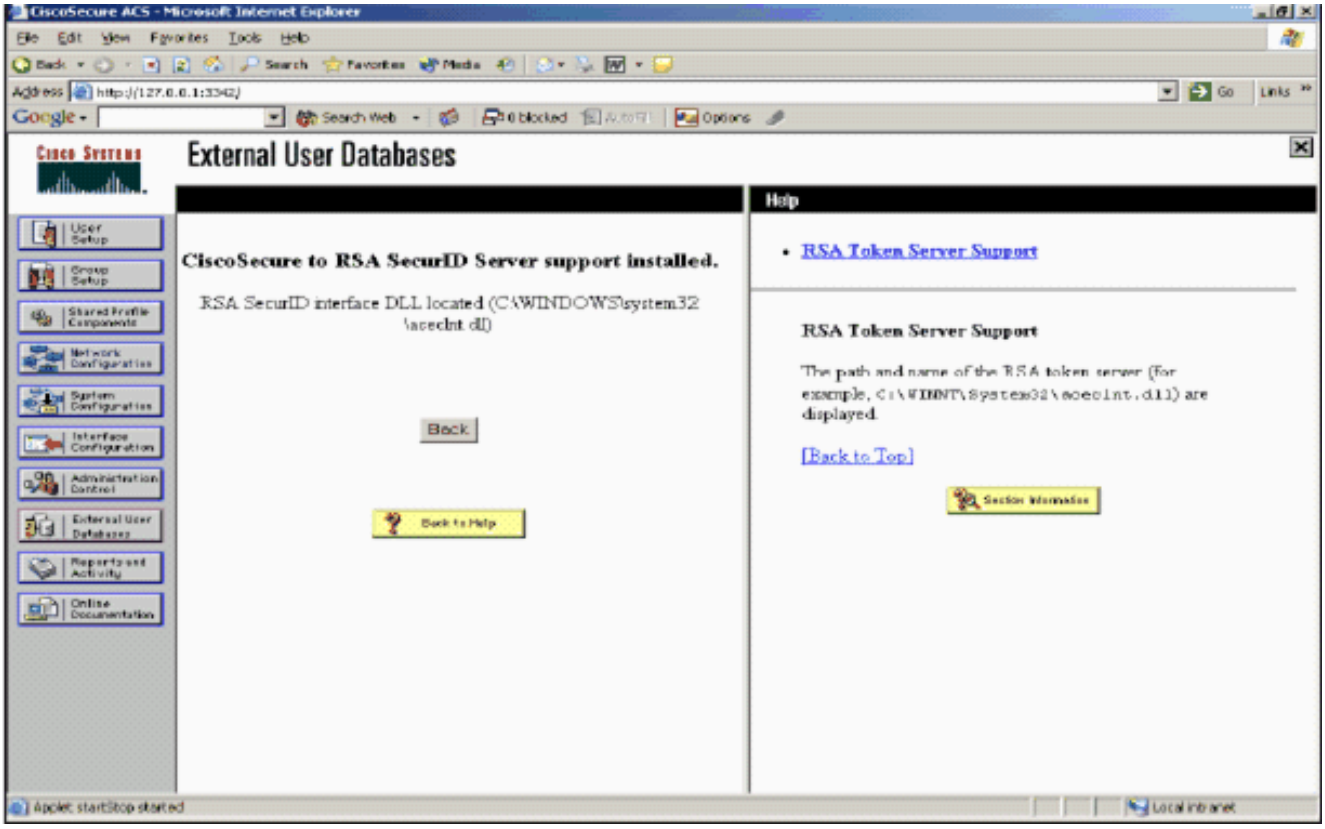


8. Cliquez sur **Configure**.



Le Cisco Secure ACS affiche le nom du serveur de jetons et du chemin au DLL d'authentificateur. Ces informations confirment que le Cisco Secure ACS peut entrer en contact avec l'agent d'authentification RSA. Vous pouvez ajouter la base de données d'utilisateur externe RSA SecurID à votre stratégie inconnue d'utilisateur ou assigner des

comptes utilisateurs spécifiques pour utiliser cette base de données pour l'authentification.

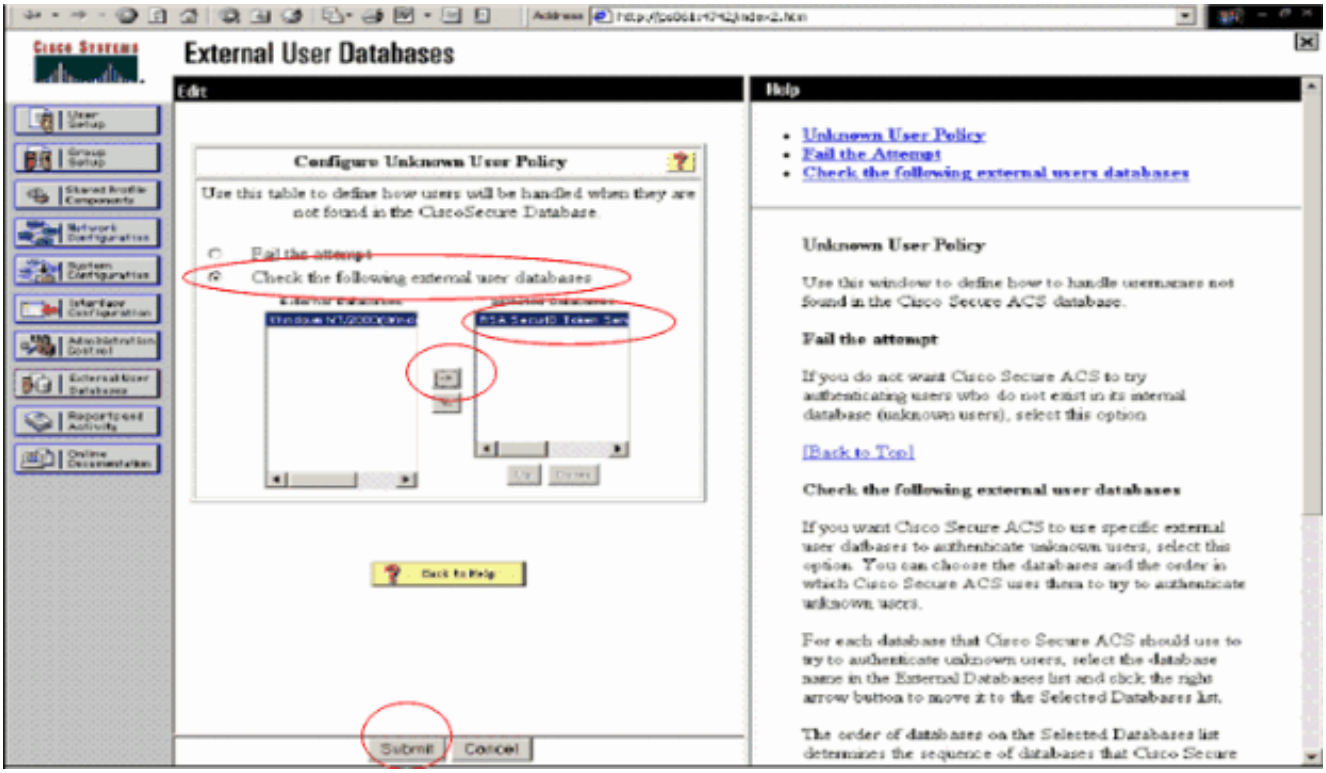


Ajoutez/configurez l'authentification RSA SecurID à votre stratégie inconnue d'utilisateur

Procédez comme suit :

1. Dans la barre de navigation ACS, **base de données d'utilisateur externe de** clic **> stratégie inconnue d'utilisateur**.

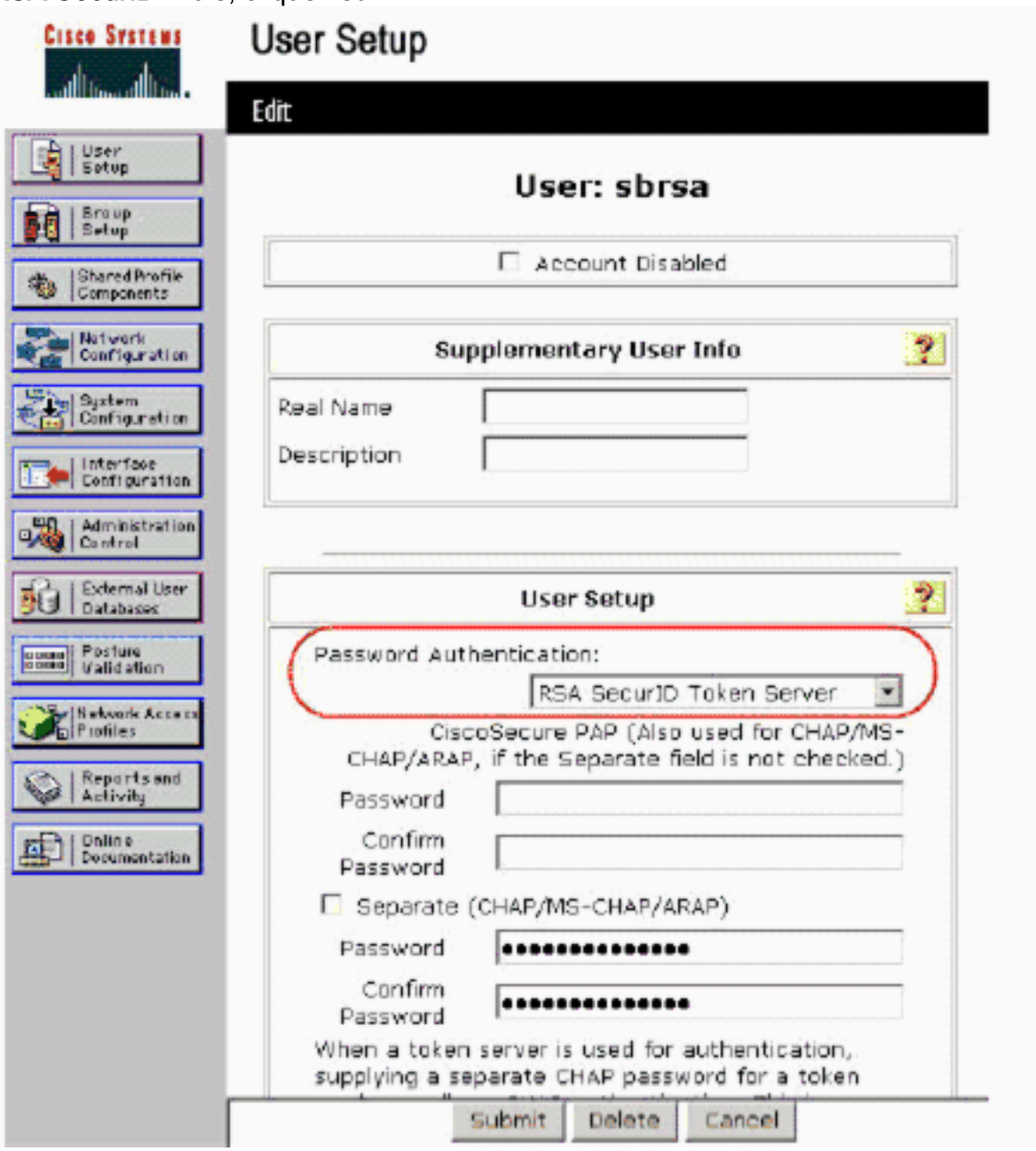
2. Dans la page **inconnue de stratégie d'utilisateur**, le **contrôle** choisi les **bases de données d'utilisateur externe suivantes**, **serveur de jetons du** point culminant **RSA SecurID** et la déplacent dans la case sélectionnée de bases de données. Puis, cliquez sur **Submit**.



Ajoutez/configurez l'authentification RSA SecurID pour des comptes utilisateurs spécifiques

Procédez comme suit :

1. Cliquez sur User Setup du GUI principal d'admin ACS. Écrivez le nom d'utilisateur et cliquez sur Add (ou sélectionnez un utilisateur existant que vous souhaitez modifier).
2. Sous l'authentification d'installation utilisateur > de mot de passe, choisissez le **serveur de jetons RSA SecurID**. Puis, cliquez sur **Submit**.

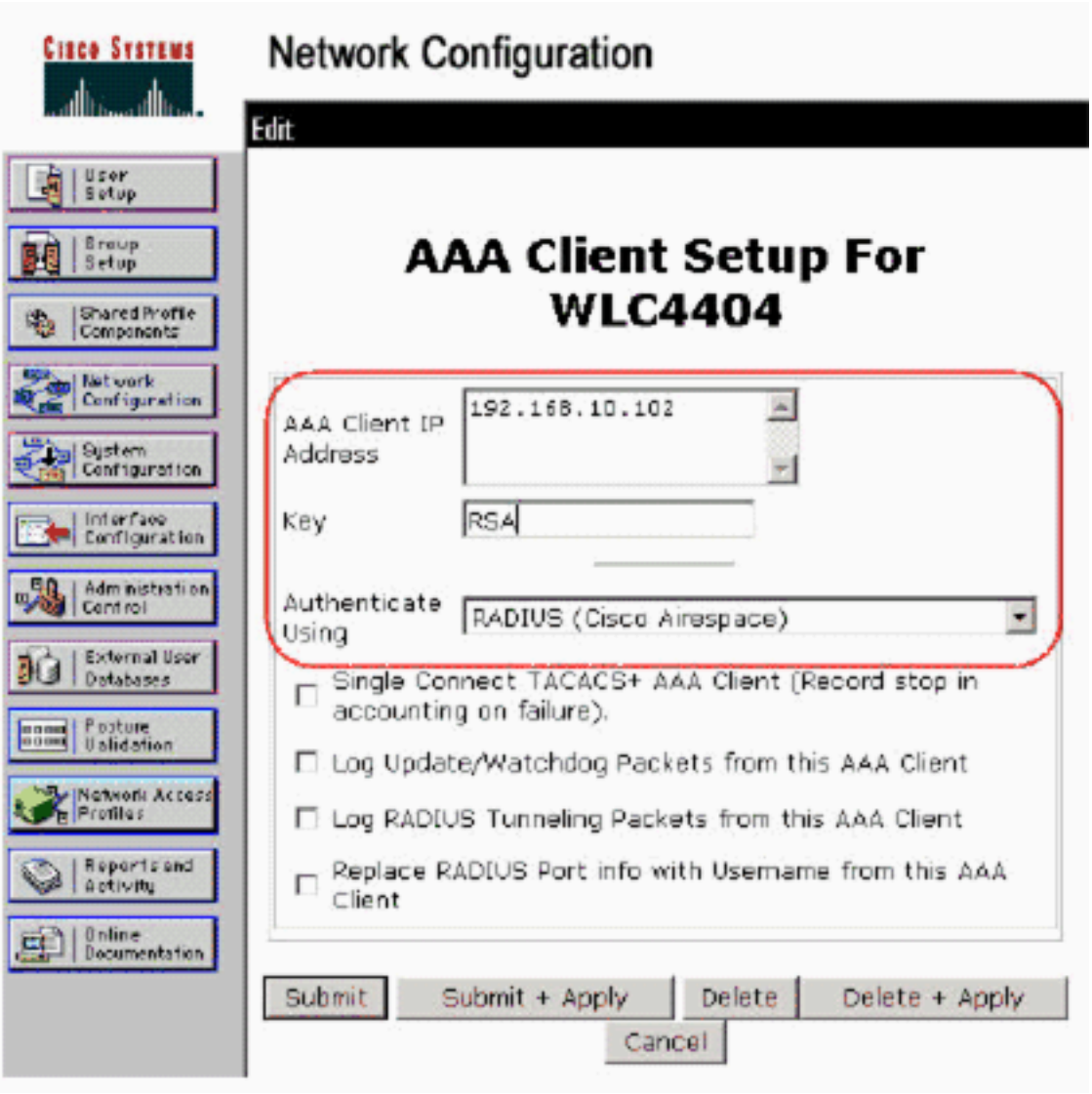


[Ajoutez un client RADIUS à Cisco ACS]

Le serveur ACS de Cisco installent aura besoin des adresses IP du WLC pour servir de le NAS pour expédier des authentifications du client PEAP à l'ACS.

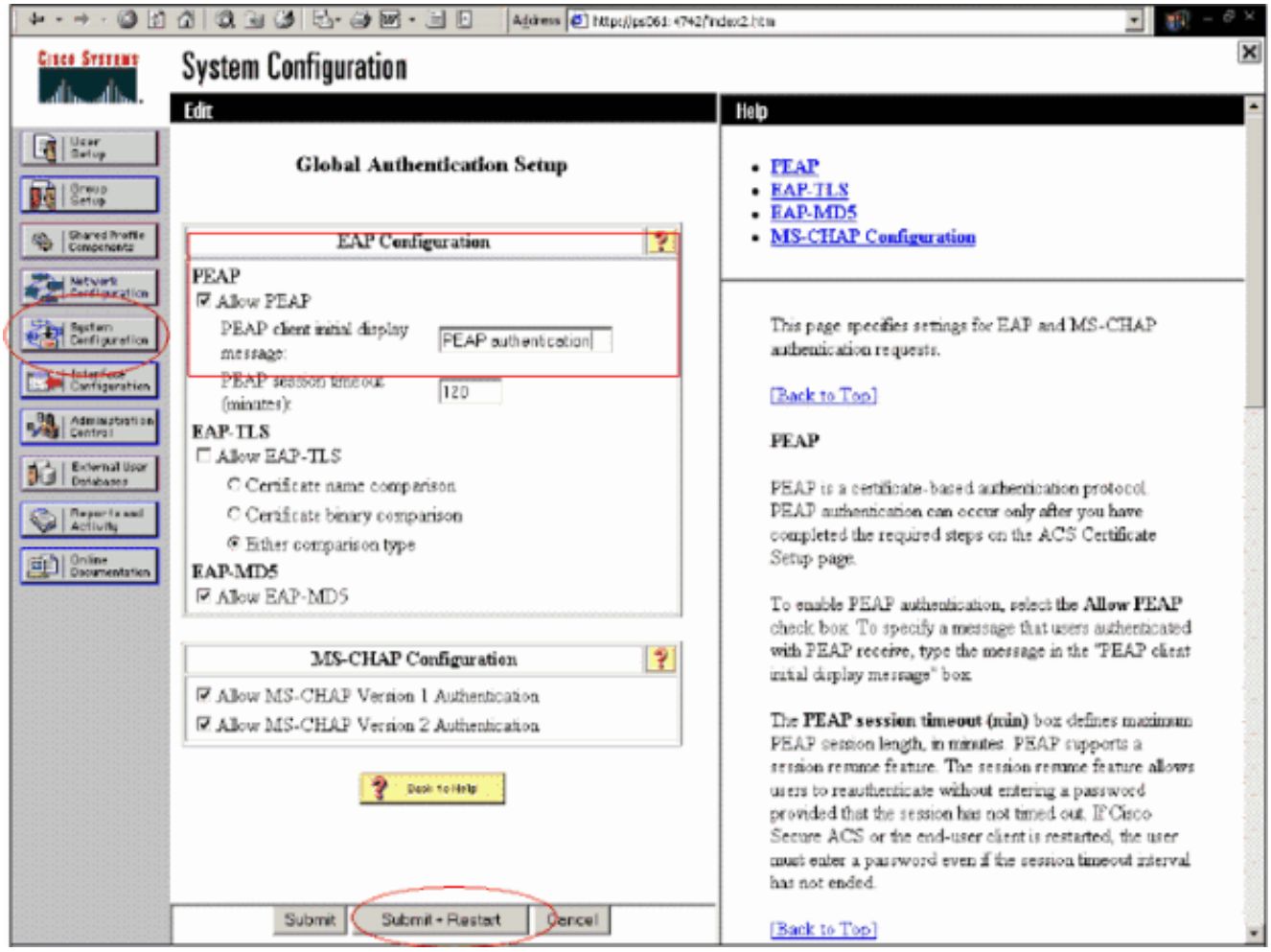
Procédez comme suit :

1. Sous la **configuration réseau**, ajoutez/éditez le client d'AAA pour le WLC qui sera utilisé. Introduisez » la clé secrète « partagée (commune à WLC) qui est utilisée entre le client d'AAA et l'ACS. Choisi **authentifiez utilisant > RADIUS (Cisco Airespace)** pour ce client d'AAA. Puis, cliquez sur Submit **+**



appliquez.

2. Appliquez pour et installez un certificat de serveur d'une autorité de certification connue et de confiance telle que l'autorité de certification RSA Keon.Pour plus d'informations sur ce processus, référez-vous à la documentation qui se transporte avec Cisco ACS. Si vous utilisez le gestionnaire de certificat RSA, vous pouvez visualiser le guide d'implémentation d'Aironet RSA Keon pour l'aide supplémentaire. Vous devez avec succès se terminer cette tâche avant que vous continuiez.**Remarque:** des Certificats Auto-signés peuvent également être utilisés. Référez-vous à la documentation de Cisco Secure ACS sur la façon dont utiliser ces derniers.
3. Sous la **configuration système > l'installation globale d'authentification**, vérifient la case à cocher pour l'authentification **Allow PEAP**.



Configurez la configuration Sans fil de contrôleur LAN de Cisco pour le 802.1x

Procédez comme suit :

1. Connectez à l'interface de ligne de commande du WLC pour configurer le contrôleur ainsi il peut être configuré pour se connecter au serveur de Cisco Secure ACS.
2. Sélectionnez la commande **authentique d'IP address de rayon de config du** WLC de configurer un serveur de RADIUS pour l'authentification.**Remarque:** Quand vous testez avec le serveur de RADIUS de gestionnaire d'authentification RSA, écrivez l'adresse IP du serveur de RADIUS du gestionnaire d'authentification RSA. Quand vous testez avec le serveur ACS de Cisco, écrivez l'adresse IP du serveur de Cisco Secure ACS.
3. Sélectionnez la commande **authentique de port de rayon de config du** WLC de spécifier le port UDP pour l'authentification. Les ports 1645 ou 1812 sont en activité par défaut dans le gestionnaire d'authentification RSA et le serveur ACS de Cisco.
4. Sélectionnez la **commande secret authentique de rayon de config du** WLC de configurer le secret partagé sur le WLC. Ceci doit apparier le secret partagé créé dans les serveurs de RADIUS pour ce client RADIUS.
5. Sélectionnez la commande de **config radius auth enable du** WLC d'activer l'authentification. Une fois désiré, sélectionnez la commande de **config radius auth disable** de désactiver l'authentification. Notez que l'authentification est désactivée par défaut.
6. Sélectionnez l'option appropriée de degré de sécurité de la couche 2 pour le WLAN désiré au WLC.
7. Utilisez les commandes de **show radius auth statistics** et de **show radius summary** de vérifier que les configurations de RADIUS sont correctement configurées.**Remarque:** Les minuteurs

par défaut pour le request-timeout d'EAP sont bas et pourraient devoir être modifiés. Ceci peut être fait utilisant la commande de *<seconds>* de ***request-timeout de config advanced eap***. Il pourrait également aider à tordre le délai d'attente de demande d'identité basé sur les conditions requises. Ceci peut être fait utilisant la commande de *<seconds> d'identité-demande-****délai d'attente de config advanced eap***.

Configuration de client sans fil de 802.11

Pour une explication détaillée de la façon configurer votre suppliant Sans fil de matériel et de client, référez-vous à la diverse Documentation Cisco.

Problèmes identifiés

Ce sont certaines des questions réputées avec l'authentification RSA SecureID :

- Jeton de logiciel RSA. Le nouveau mode Pin et les prochains modes de Tokencode ne sont pas pris en charge à l'aide de cette forme d'authentification avec XP2. (RÉPARÉ en raison d'ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Si votre implémentation ACS est plus ancienne ou vous n'avez pas le correctif ci-dessus, le client ne pourra pas authentifier jusqu'à ce que les transitions d'utilisateur de « aient activé ; Nouveau mode PIN » « à activer ». Vous pouvez accomplir ceci en ayant l'utilisateur vous terminez une authentification de non-radio, ou à l'aide de l'application RSA de « test d'authentification ».
- Refusez 4 chiffres/broches alphanumériques. Si un utilisateur en nouveau mode Pin va contre la stratégie PIN, la procédure d'authentification échoue, et l'utilisateur est inconscient de la façon dont ou de pourquoi. Typiquement, si un utilisateur va contre la stratégie, ils seront envoyés à un message que le PIN a été rejeté et être incité de nouveau tout en affichant à l'utilisateur de nouveau ce qu'est la stratégie PIN (par exemple, si la stratégie PIN est 5-7 chiffres, pourtant l'utilisateur écrit 4 chiffres).

Informations connexes

- Exemple de configuration d'une affectation de VLAN dynamique avec des contrôleurs de réseau local sans fil en fonction du mappage du groupe ACS au groupe Active Directory
- Exemple de configuration d'un VPN client sur un réseau local sans fil avec WLC
- Exemples de configuration de l'authentification sur des contrôleurs de réseau local sans fil
- Exemple de configuration d'authentification EAP-FAST avec des contrôleurs de réseau local sans fil et un serveur RADIUS externe
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe via SDM
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe
- Protected Extensible Authentication Protocol de Cisco
- Authentification EAP avec le serveur RADIUS
- Support et documentation techniques - Cisco Systems