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

Contenu

Introduction

Ce document explique comment configurer et configurer des points d'accès et des contrôleurs de réseau local sans fil (WLC) compatibles LWAPP (Lightweight Access Point Protocol) Cisco, ainsi que Cisco Secure Access Control Server (ACS) à utiliser dans un environnement WLAN authentifié RSA SecurID. Les guides de mise en oeuvre spécifiques à RSA SecurID sont disponibles à l'adresse www.rsasecured.com.

Conditions préalables

Conditions requises

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

- Connaissance des WLC et configuration de leurs paramètres de base.
- Connaissances sur la configuration du profil du client sans fil Cisco à l'aide de l'utilitaire de bureau Aironet (ADU).

- Connaissances fonctionnelles de Cisco Secure ACS.
- Connaître le LWAPP.
- Comprendre de base les services Active Directory (AD) de Microsoft Windows, ainsi que les concepts de contrôleur de domaine et de DNS.**Remarque :** avant de tenter cette configuration, assurez-vous que ACS et le serveur RSA Authentication Manager se trouvent dans le même domaine et que leur horloge système est exactement synchronisée. Si vous utilisez Microsoft Windows AD Services, reportez-vous à la documentation Microsoft pour configurer le serveur ACS et RSA Manager dans le même domaine. Référez-vous à Configurer Active Directory et la base de données des utilisateurs Windows pour obtenir des informations pertinentes.

Components Used

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

- RSA Authentication Manager 6.1
- Agent d'authentification RSA 6.1 pour Microsoft Windows
- Cisco Secure ACS 4.0(1) Build 27**Remarque :** Le serveur RADIUS inclus peut être utilisé à la place de Cisco ACS. Reportez-vous à la documentation RADIUS fournie avec RSA Authentication Manager pour savoir comment configurer le serveur.
- Points d'accès légers et WLC Cisco pour la version 4.0 (version 4.0.155.0)

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

Le système RSA SecurID est une solution d'authentification utilisateur à deux facteurs. Utilisé conjointement avec RSA Authentication Manager et un agent d'authentification RSA, l'authentificateur RSA SecurID exige que les utilisateurs s'identifient à l'aide d'un mécanisme d'authentification à deux facteurs.

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

Les authentificateurs RSA SecurID sont aussi simples à utiliser que la saisie d'un mot de passe. Chaque utilisateur final se voit attribuer un authentificateur RSA SecurID qui génère un code à usage unique. Lors de la connexion, l'utilisateur saisit simplement ce numéro et un code confidentiel secret pour être authentifié avec succès. En outre, les jetons matériels RSA SecurID sont généralement pré-programmés pour être entièrement fonctionnels dès réception.

Cette démonstration Flash explique comment utiliser un périphérique d'authentification RSA secureID : Démo RSA.

Grâce au programme RSA SecurID Ready, les WLC Cisco et les serveurs Cisco Secure ACS prennent en charge l'authentification RSA SecurID immédiatement. Le logiciel RSA Authentication Agent intercepte les demandes d'accès, locales ou distantes, provenant d'utilisateurs (ou de groupes d'utilisateurs) et les dirige vers le programme RSA Authentication Manager pour l'authentification.

Le logiciel RSA Authentication Manager est le composant de gestion de la solution RSA SecurID. Il permet de vérifier les demandes d'authentification et d'administrer de manière centralisée les stratégies d'authentification pour les réseaux d'entreprise. Il fonctionne avec les authentificateurs RSA SecurID et le logiciel RSA Authentication Agent.

Dans ce document, un serveur Cisco ACS est utilisé comme agent d'authentification RSA en installant le logiciel de l'agent dessus. Le WLC est le serveur d'accès au réseau (NAS) (client AAA) qui, à son tour, transfère les authentifications du client à ACS. Le document présente les concepts et la configuration à l'aide de l'authentification client PEAP (Protected Extensible Authentication Protocol).

Pour en savoir plus sur l'authentification PEAP, référez-vous à Cisco Protected Extensible Authentication Protocol.

Configuration

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

Ce document utilise les configurations suivantes :

- Configuration de l'hôte de l'agent
- Configuration de l'agent d'authentification

Configuration de l'hôte de l'agent

Utilisation de Cisco Secure ACS comme serveur RADIUS

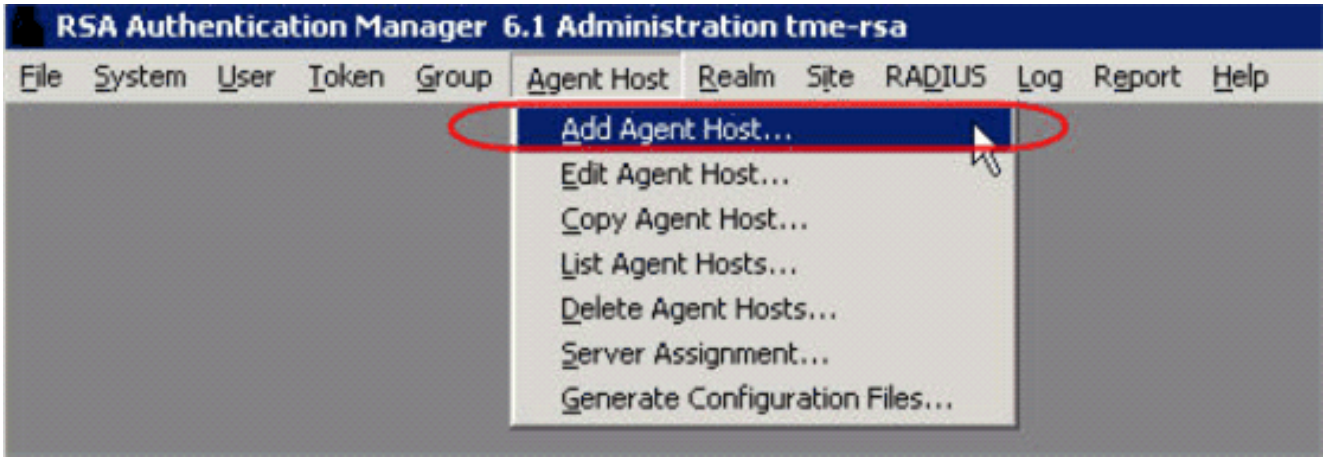
Afin de faciliter la communication entre Cisco Secure ACS et RSA Authentication Manager / RSA SecurID Appliance, un enregistrement d'hôte d'agent doit être ajouté à la base de données RSA Authentication Manager. L'enregistrement Hôte de l'agent identifie Cisco Secure ACS dans sa base de données et contient des informations sur la communication et le chiffrement.

Pour créer l'enregistrement Hôte d'agent, vous avez besoin des informations suivantes :

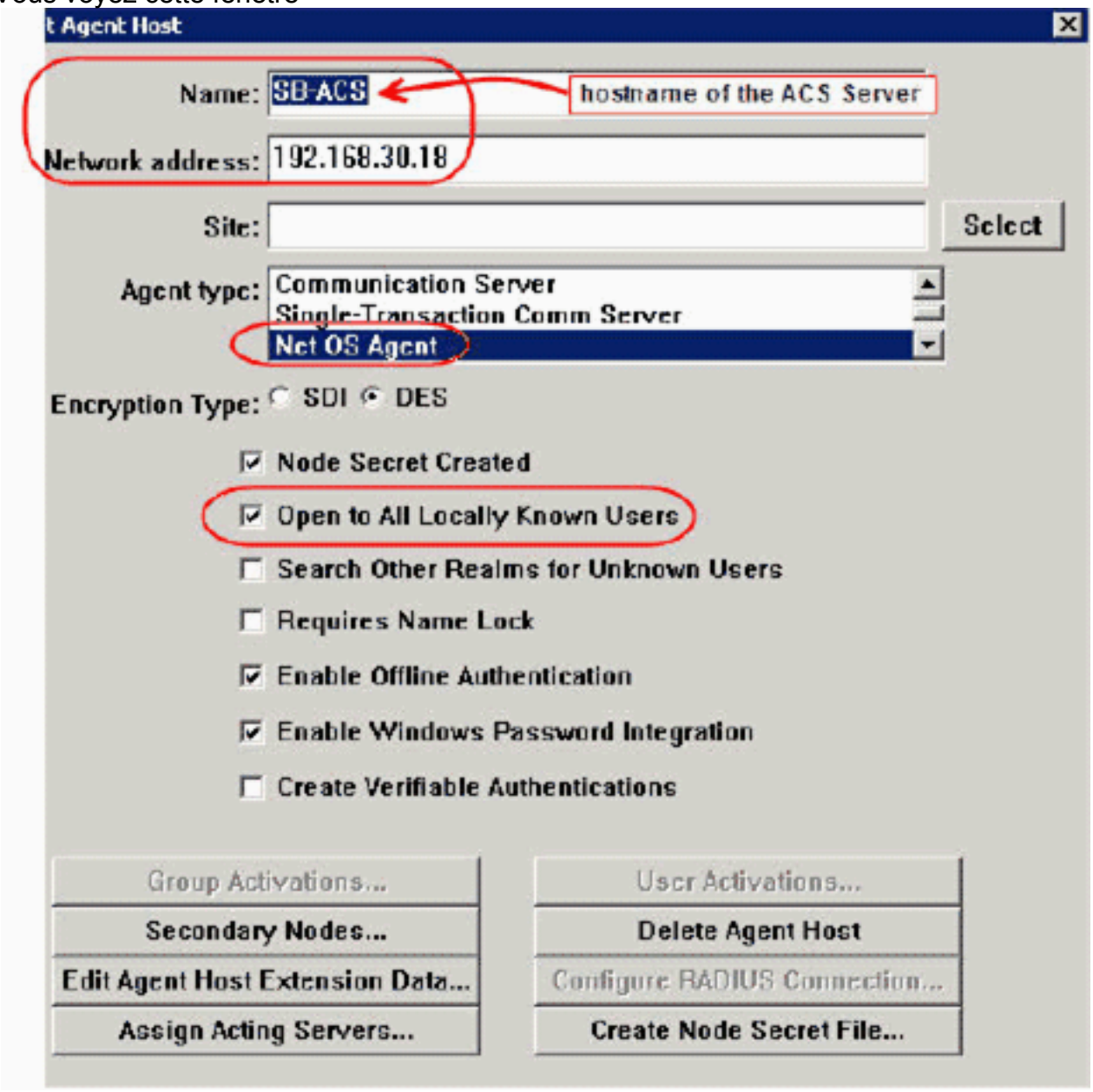
- Nom d'hôte du serveur Cisco ACS
- Adresses IP pour toutes les interfaces réseau du serveur Cisco ACS

Procédez comme suit :

1. Ouvrez l'application Mode hôte RSA Authentication Manager.
2. Sélectionnez **Agent Host > Add Agent Host**.



Vous voyez cette fenêtre



:

3. Saisissez les informations appropriées pour le nom du serveur Cisco ACS et l'adresse réseau. Sélectionnez **NetOS** pour le type d'agent et cochez la case **Ouvrir à tous les utilisateurs connus localement**.
4. Click OK.

Utilisation du serveur RADIUS RSA Authentication Manager 6.1

Afin de faciliter la communication entre Cisco WLC et RSA Authentication Manager, un enregistrement d'hôte d'agent doit être ajouté à la base de données RSA Authentication Manager et à la base de données RADIUS Server. L'enregistrement Hôte de l'agent identifie le WLC Cisco dans sa base de données et contient des informations sur la communication et le chiffrement.

Pour créer l'enregistrement Hôte d'agent, vous avez besoin des informations suivantes :

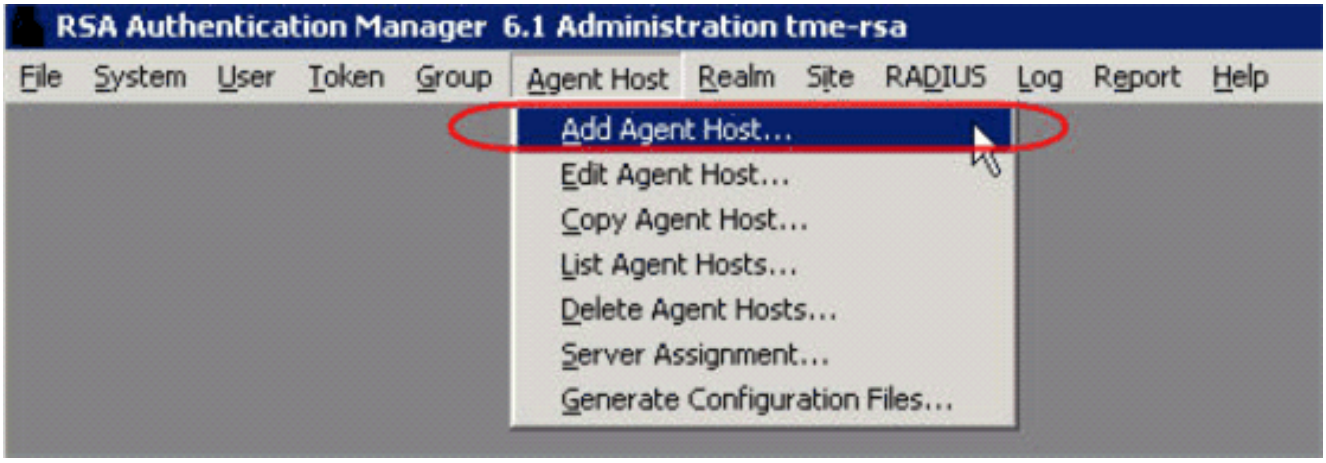
- Nom d'hôte du WLC
- Adresses IP de gestion du WLC
- secret RADIUS, qui doit correspondre au secret RADIUS sur le WLC Cisco

Lors de l'ajout de l'enregistrement d'hôte d'agent, le rôle du WLC est configuré en tant que serveur de communication. Ce paramètre est utilisé par RSA Authentication Manager pour déterminer comment la communication avec le WLC se produira.

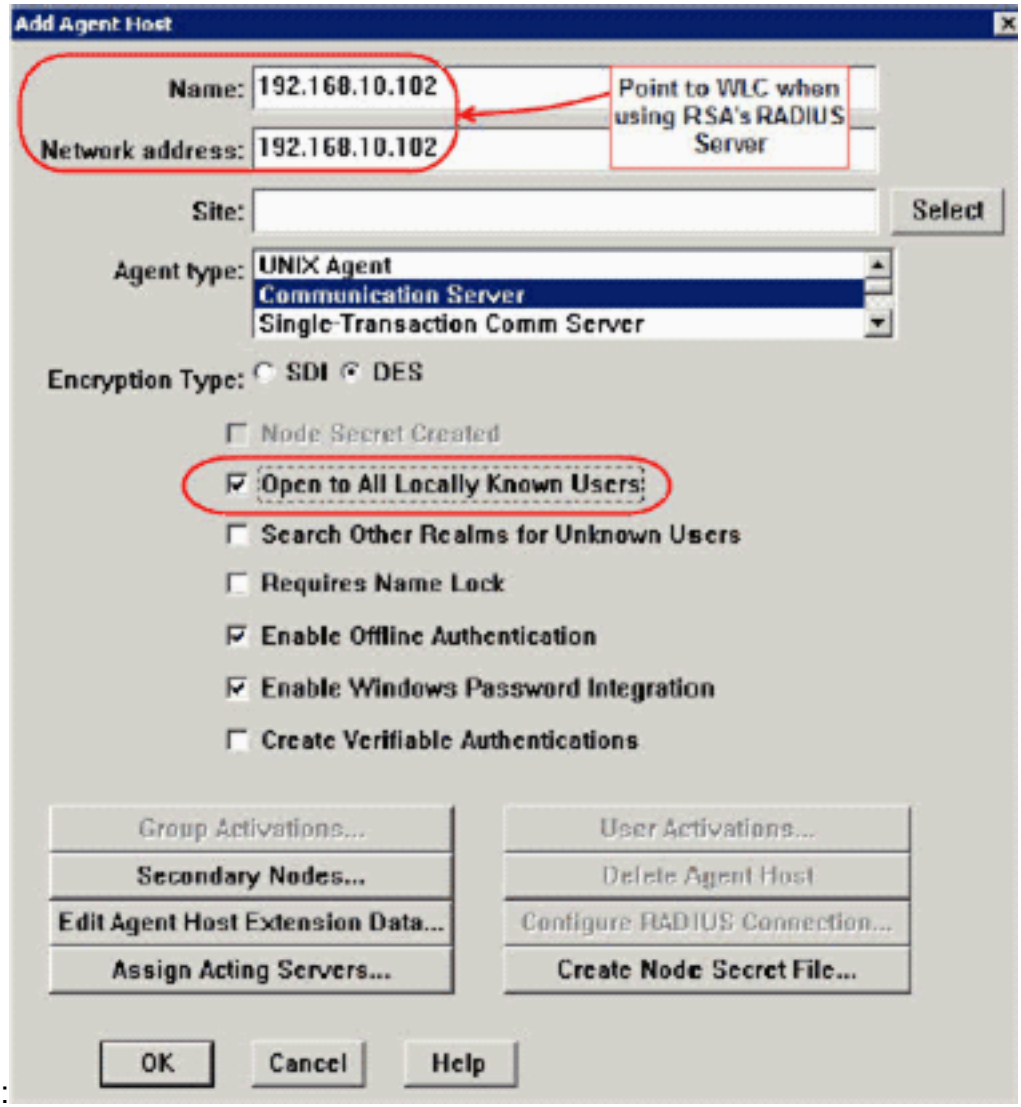
Remarque : les noms d'hôte dans RSA Authentication Manager / RSA SecurID Appliance doivent être résolus en adresses IP valides sur le réseau local.

Procédez comme suit :

1. Ouvrez l'application Mode hôte RSA Authentication Manager.
2. Sélectionnez **Agent Host > Add Agent Host**.

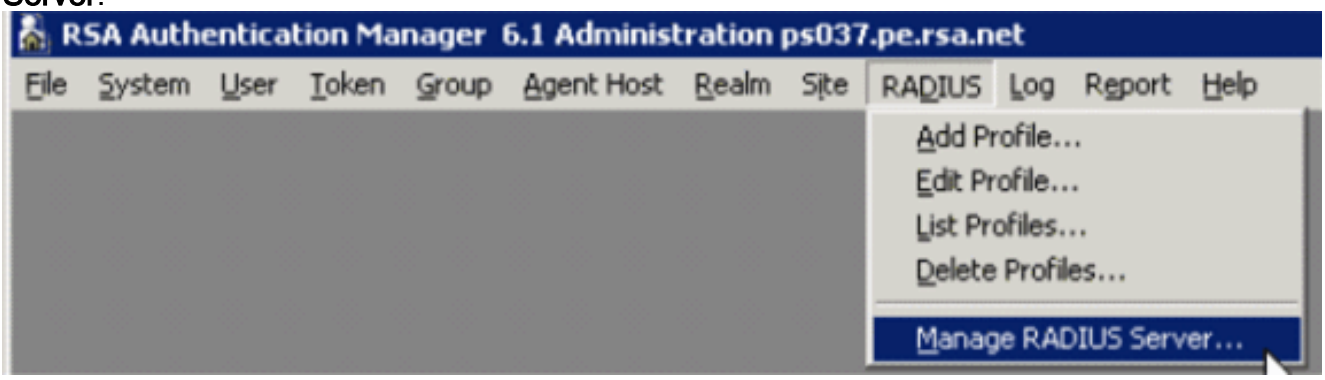


Vous voyez cette fenêtre



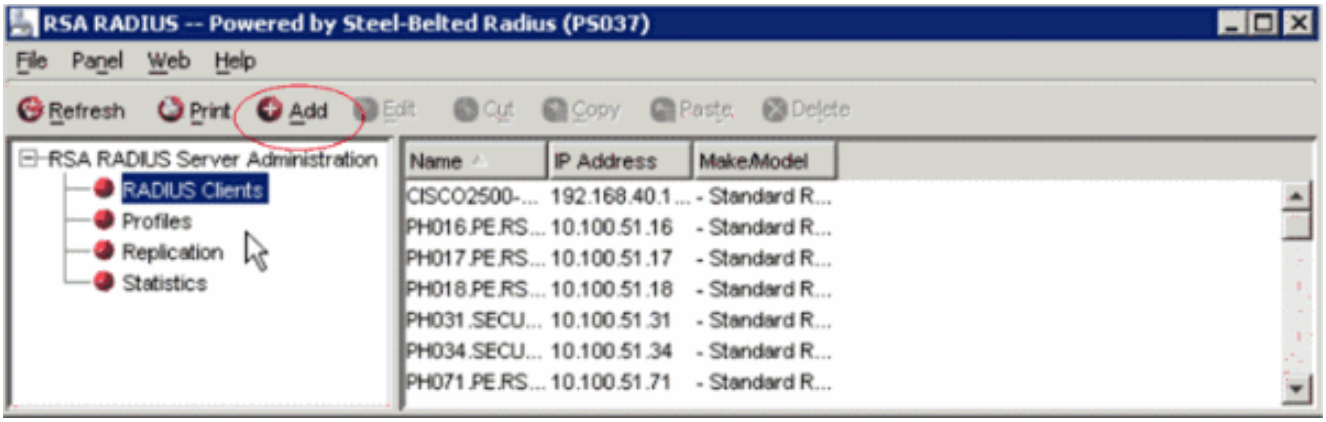
:

3. Saisissez les informations appropriées pour le nom d'hôte du WLC (un nom de domaine complet résolvable, si nécessaire) et l'adresse réseau. Choisissez **Communication Server** pour le type d'agent et cochez la case **Ouvrir à tous les utilisateurs connus localement**.
4. Click OK.
5. Dans le menu, sélectionnez **RADIUS > Manage RADIUS Server**.

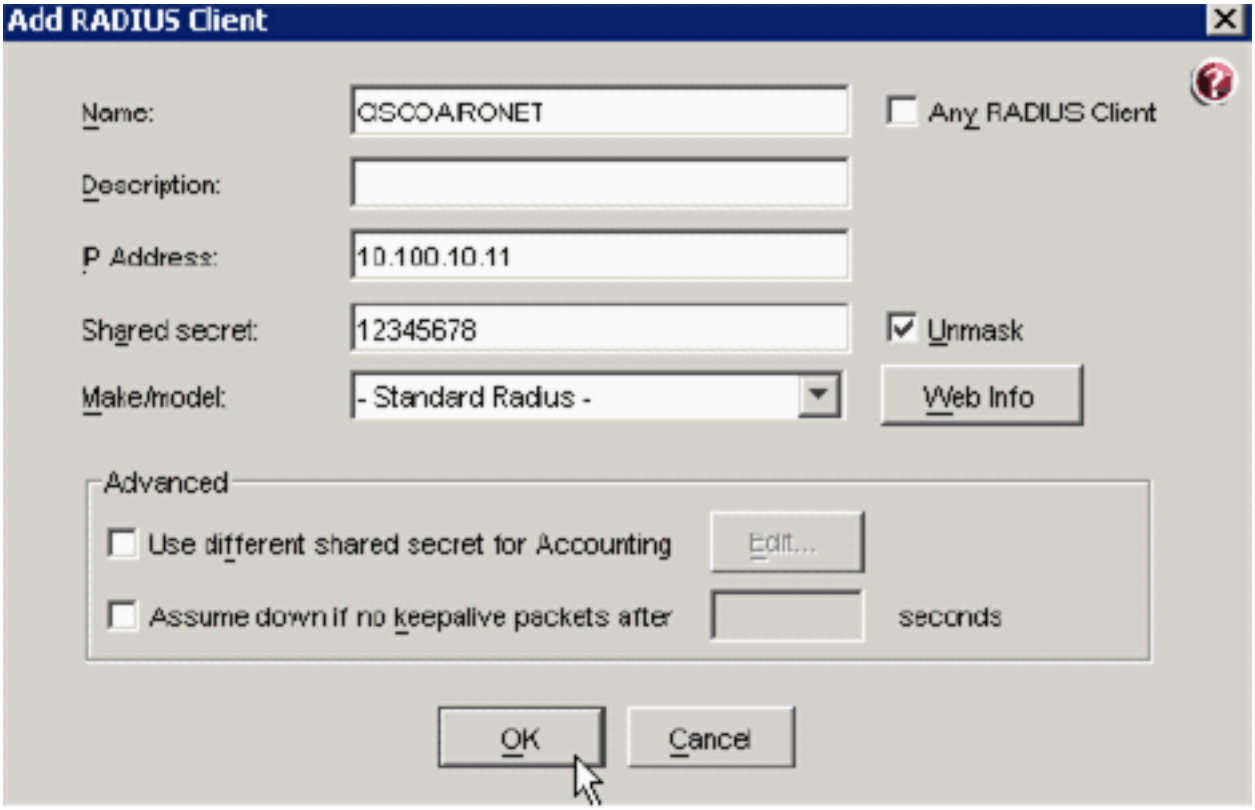


Une nouvelle fenêtre d'administration s'ouvre.

6. Dans cette fenêtre, sélectionnez **Clients RADIUS**, puis cliquez sur **Ajouter**.



7. Entrez les informations appropriées pour le WLC Cisco. Le secret partagé doit correspondre au secret partagé défini sur le WLC
Cisco.



8. Click OK.

Configuration de l'agent d'authentification

Ce tableau représente la fonctionnalité RSA Authentication Agent 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

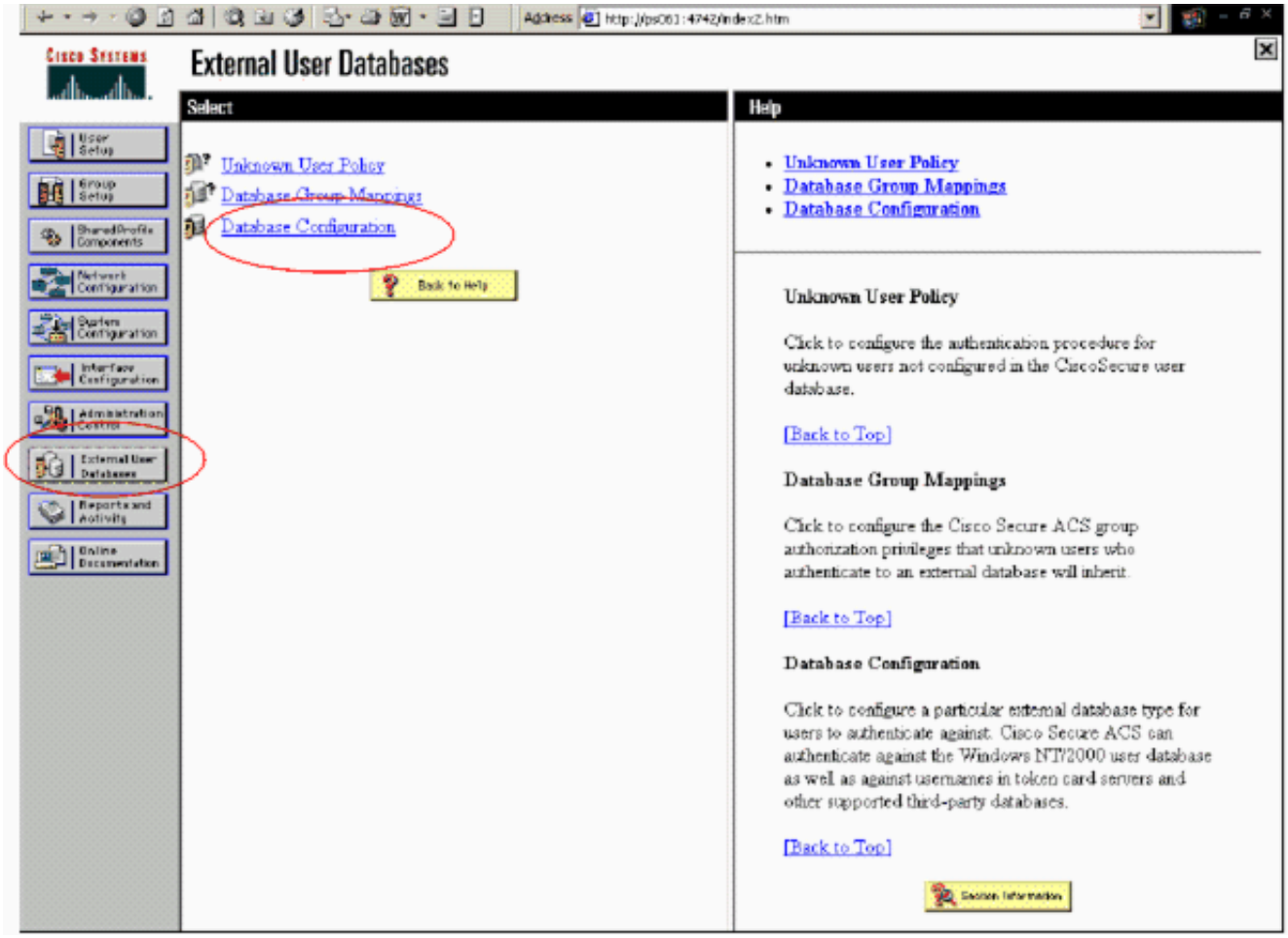
Remarque : Reportez-vous à la documentation RADIUS fournie avec RSA Authentication Manager pour savoir comment configurer le serveur RADIUS, s'il s'agit du serveur RADIUS qui sera utilisé.

Configurer Cisco ACS

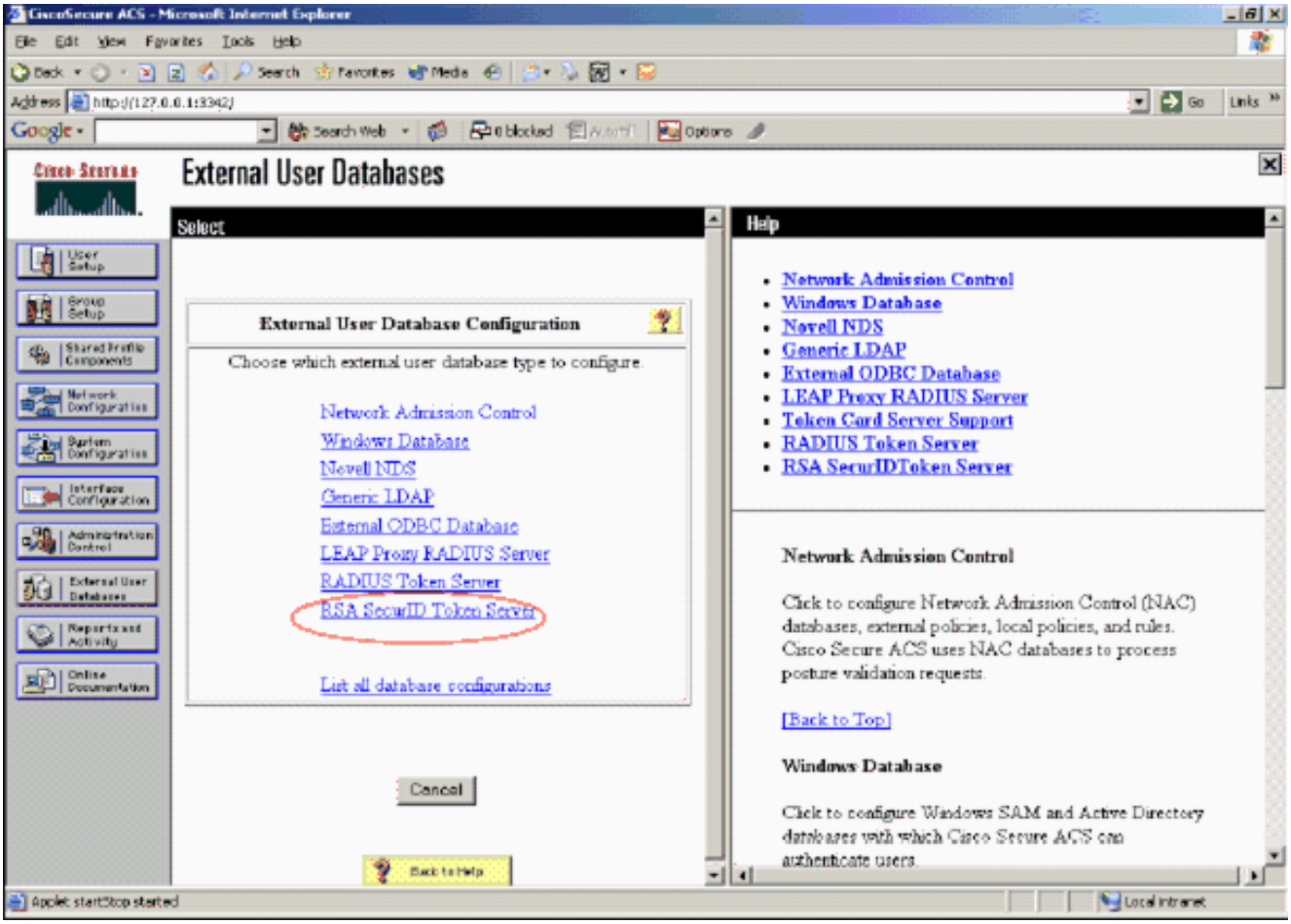
Activer l'authentification RSA SecurID

Cisco Secure ACS prend en charge l'authentification RSA SecurID des utilisateurs. Complétez ces étapes afin de configurer Cisco Secure ACS pour authentifier les utilisateurs avec Authentication Manager 6.1 :

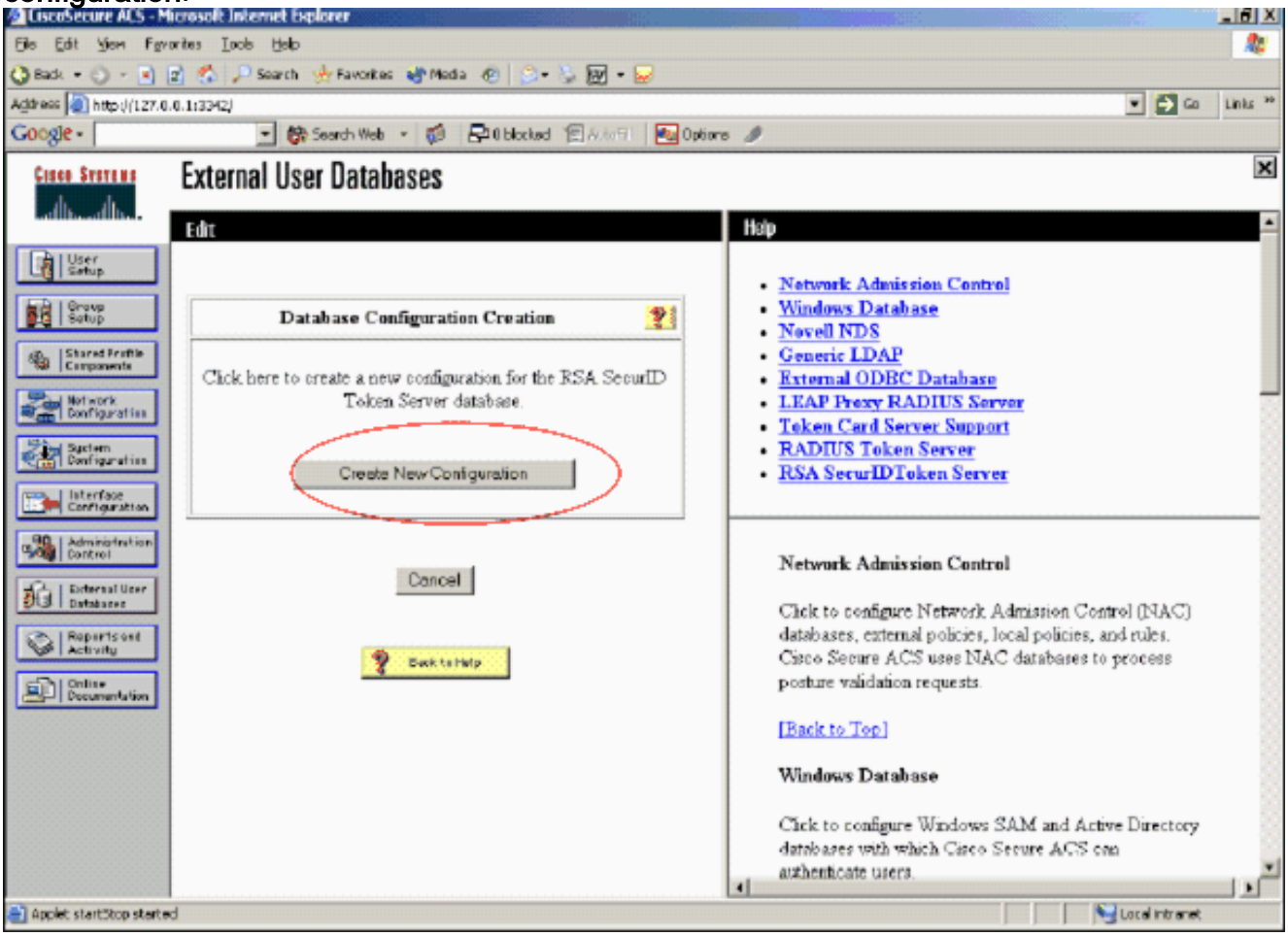
1. Installez RSA Authentication Agent 5.6 ou version ultérieure pour Windows sur le même système que le serveur Cisco Secure ACS.
2. Vérifiez la connectivité en exécutant la fonction Test Authentication de l'agent d'authentification.
3. Copiez le fichier aceclnt.dll du répertoire **c:\Program Files\RSA Security\RSA Authentication Manager\prog** du serveur RSA vers le répertoire **c:\WINNT\system32** du serveur ACS.
4. Dans la barre de navigation, cliquez sur **Base de données utilisateur externe**. Ensuite, cliquez sur **Configuration de base de données** dans la page Base de données externe.



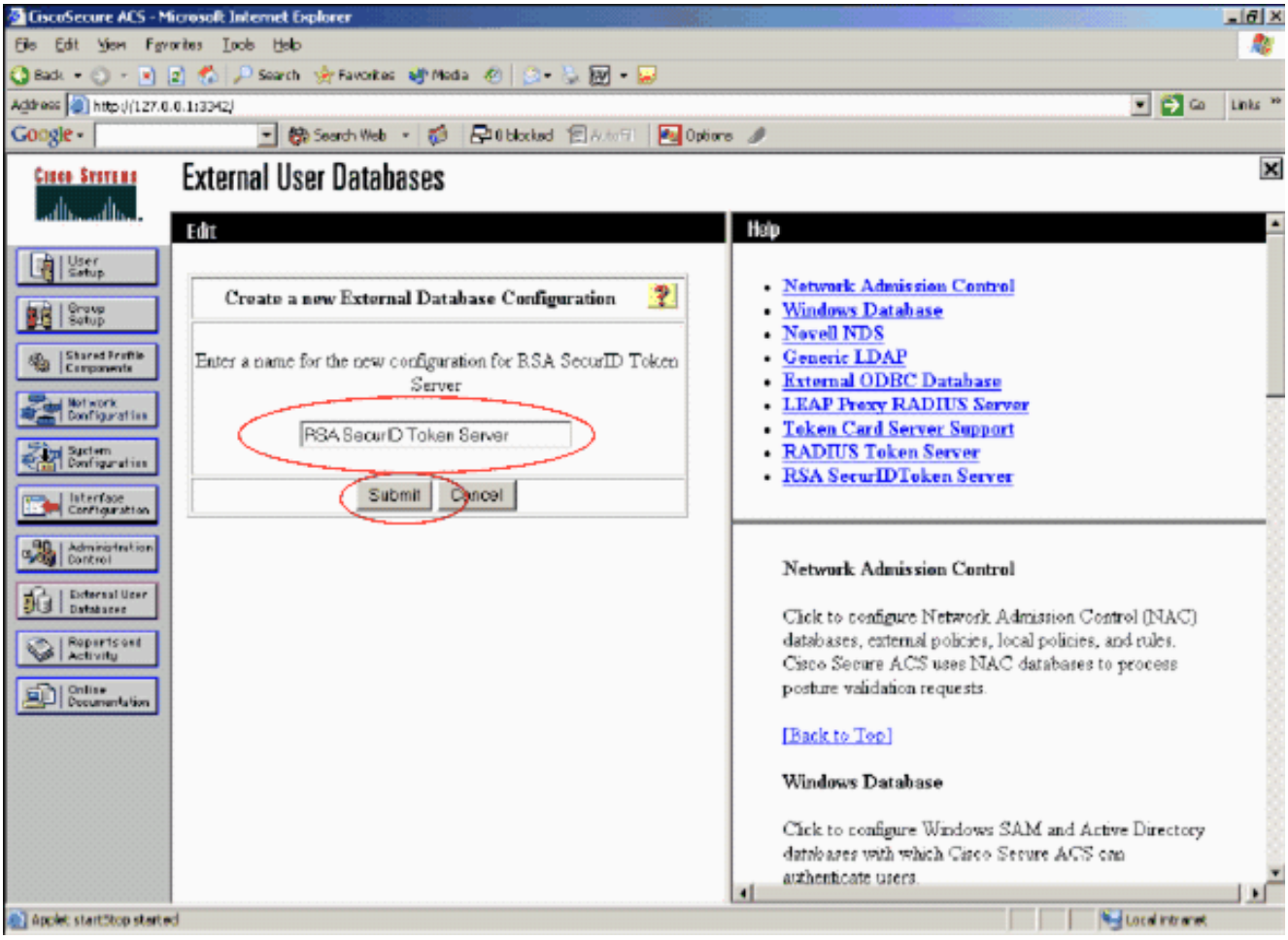
5. Dans la page Configuration de la base de données des utilisateurs externes, cliquez sur **RSA SecurID Token Server**.



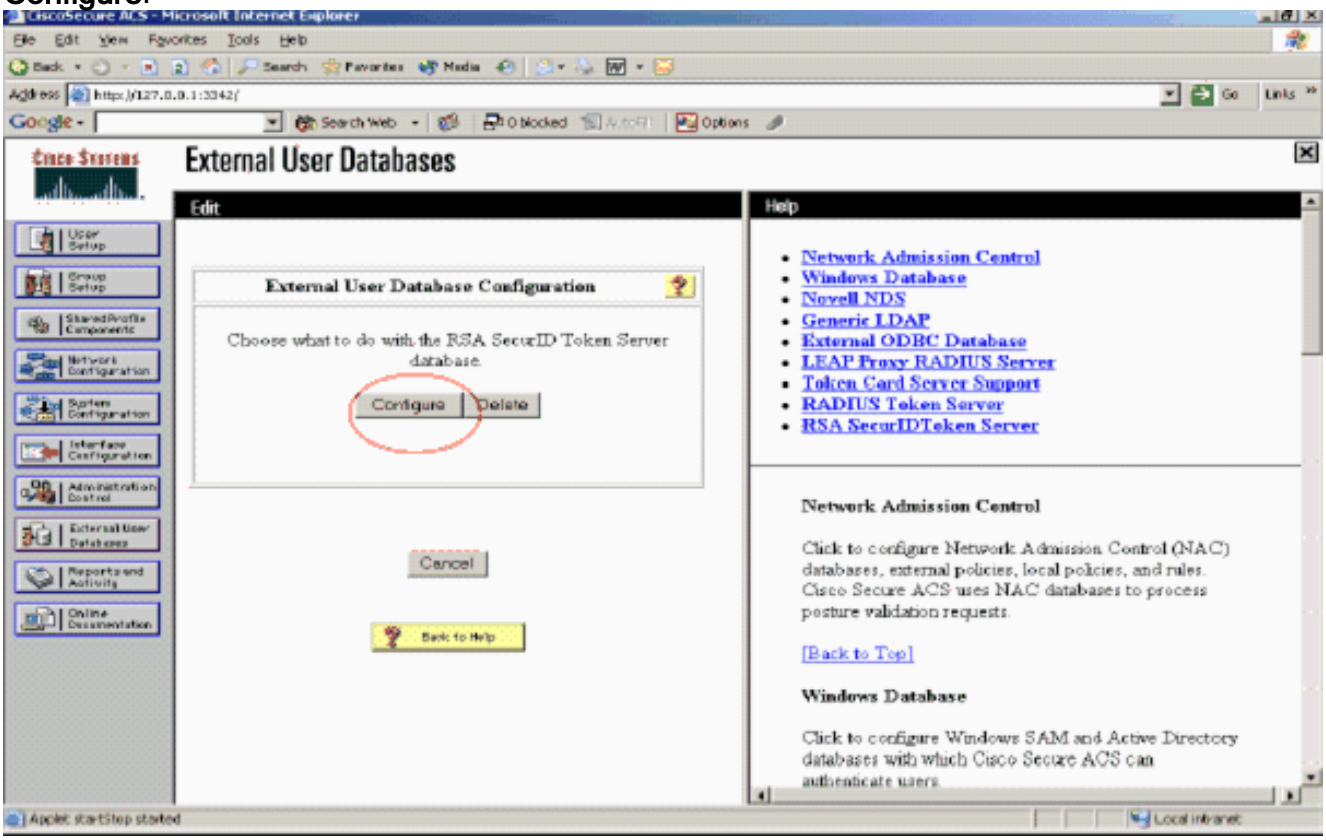
6. Cliquez sur **Créer une configuration**.



7. Entrez un nom, puis cliquez sur **Soumettre**.

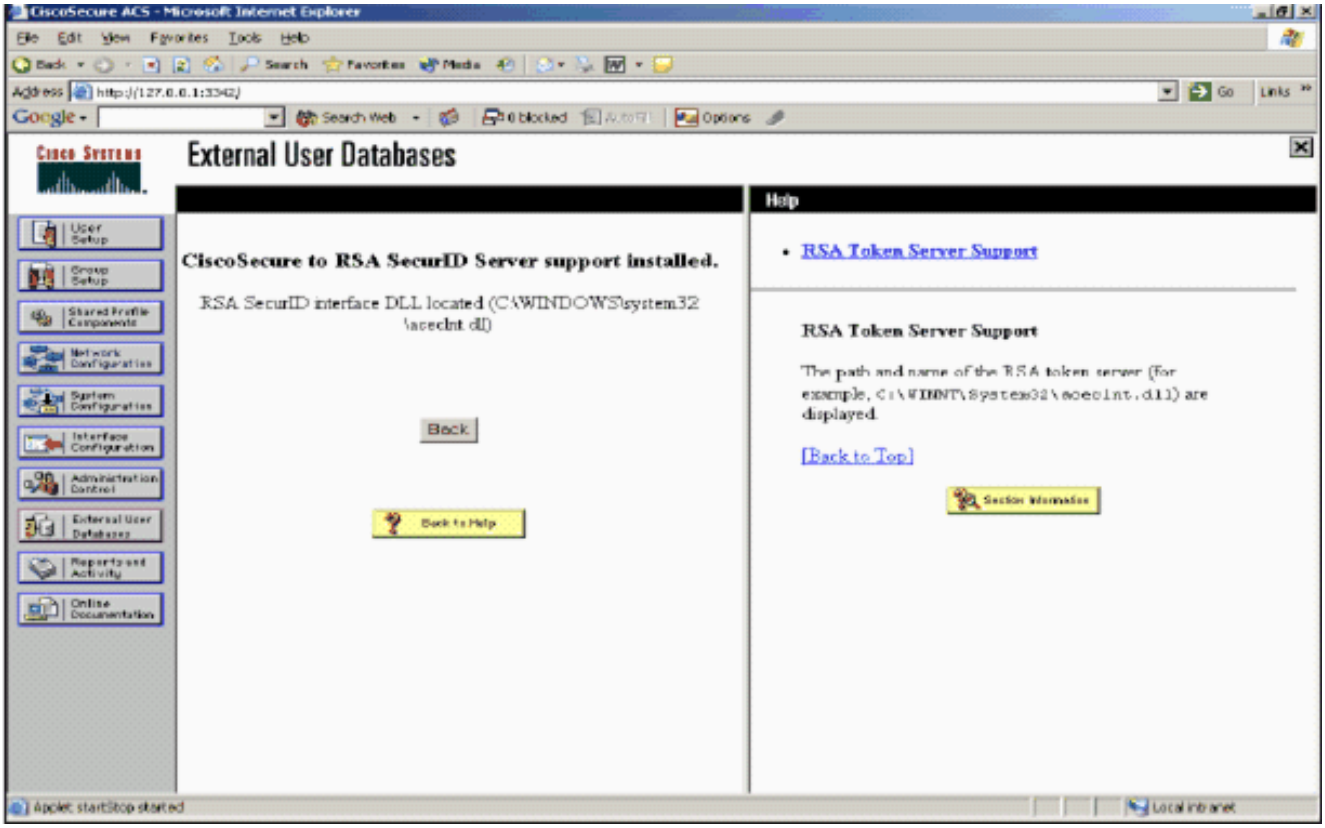


8. Cliquez sur **Configure**.



Cisco Secure ACS affiche le nom du serveur de jetons et le chemin d'accès à la DLL de l'authentificateur. Ces informations confirment que Cisco Secure ACS peut contacter l'agent d'authentification RSA. Vous pouvez ajouter la base de données utilisateur externe RSA SecurID à votre stratégie d'utilisateur inconnu ou affecter des comptes d'utilisateur

spécifiques à utiliser cette base de données pour l'authentification.

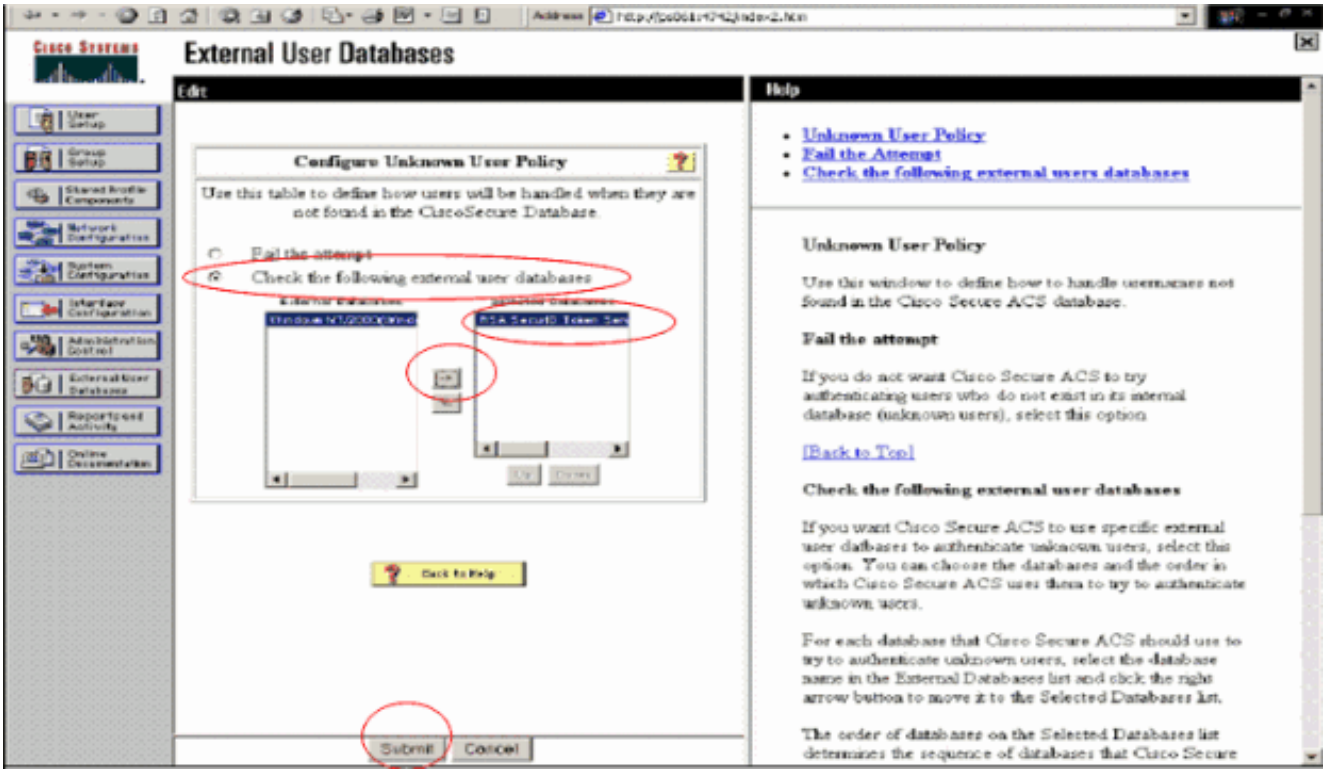


Ajouter/configurer l'authentification RSA SecurID à votre stratégie utilisateur inconnue

Procédez comme suit :

1. Dans la barre de navigation ACS, cliquez sur **Base de données utilisateur externe > Stratégie utilisateur inconnue**.

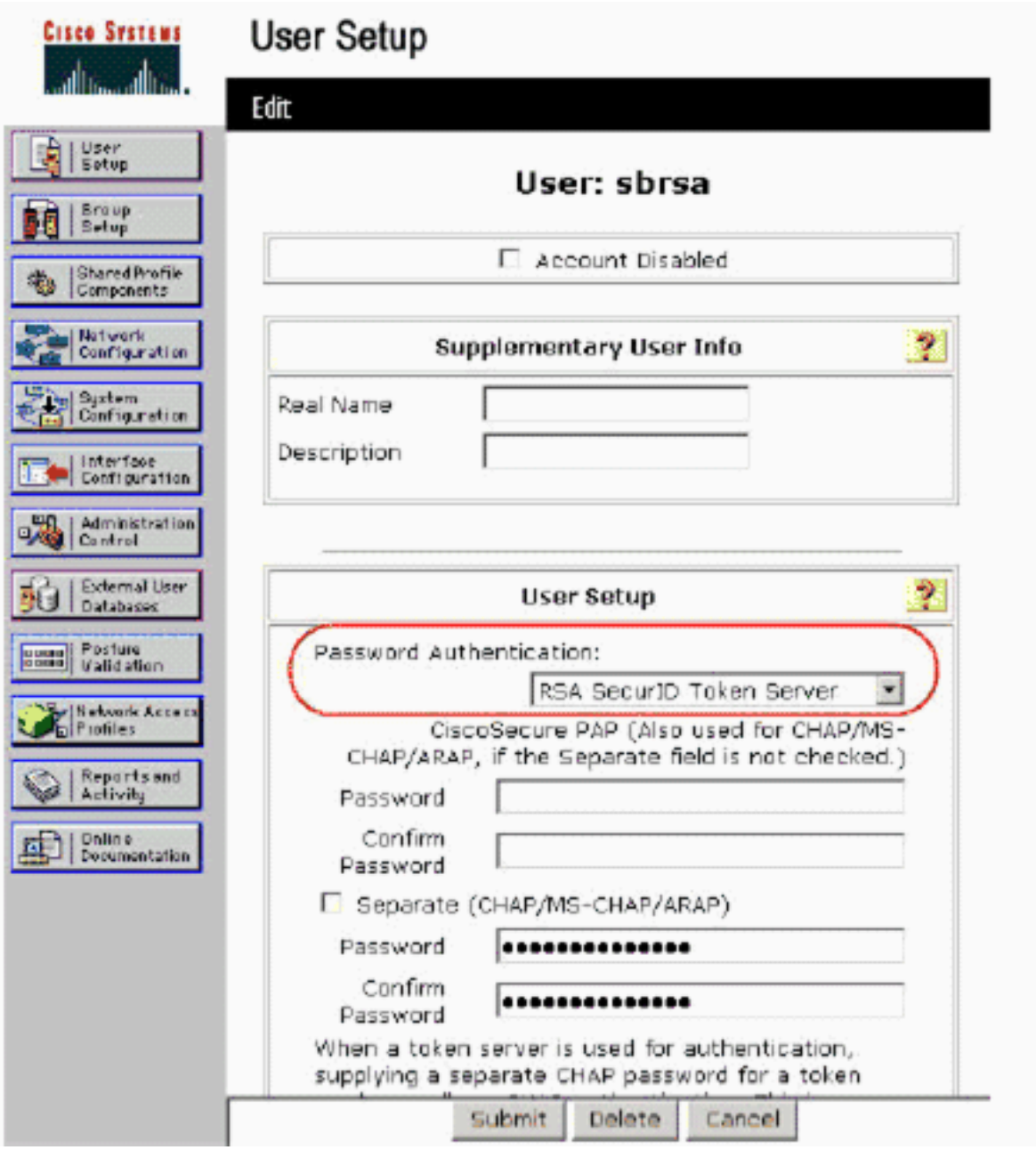
2. Dans la page **Stratégie utilisateur inconnu**, sélectionnez **Vérifier les bases de données utilisateur externes suivantes**, mettez en surbrillance **RSA SecurID Token Server** et déplacez-la dans la zone Bases de données sélectionnées. Puis, cliquez sur **Submit**.



Ajouter/configurer l'authentification RSA SecurID pour des comptes d'utilisateurs spécifiques

Procédez comme suit :

1. Cliquez sur **User Setup** dans l'interface utilisateur principale d'ACS Admin. Entrez le nom d'utilisateur et cliquez sur **Ajouter** (ou sélectionnez un utilisateur existant que vous souhaitez modifier).
2. Sous User Setup > Password Authentication, sélectionnez **RSA SecurID Token Server**. Puis, cliquez sur **Submit**.

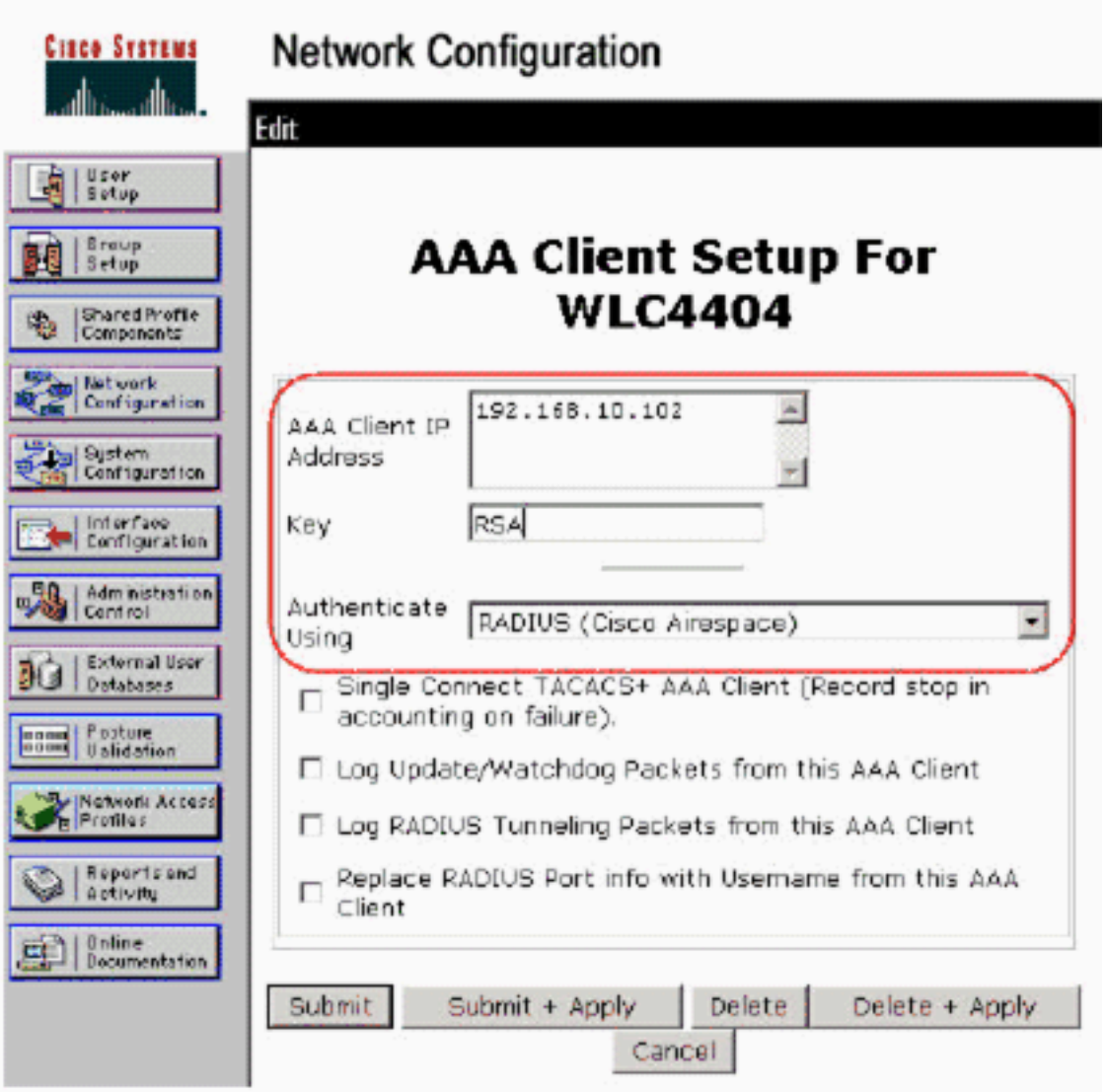


Ajouter un client RADIUS dans Cisco ACS

L'installation du serveur Cisco ACS aura besoin des adresses IP du WLC pour servir de NAS pour transférer les authentifications PEAP client à ACS.

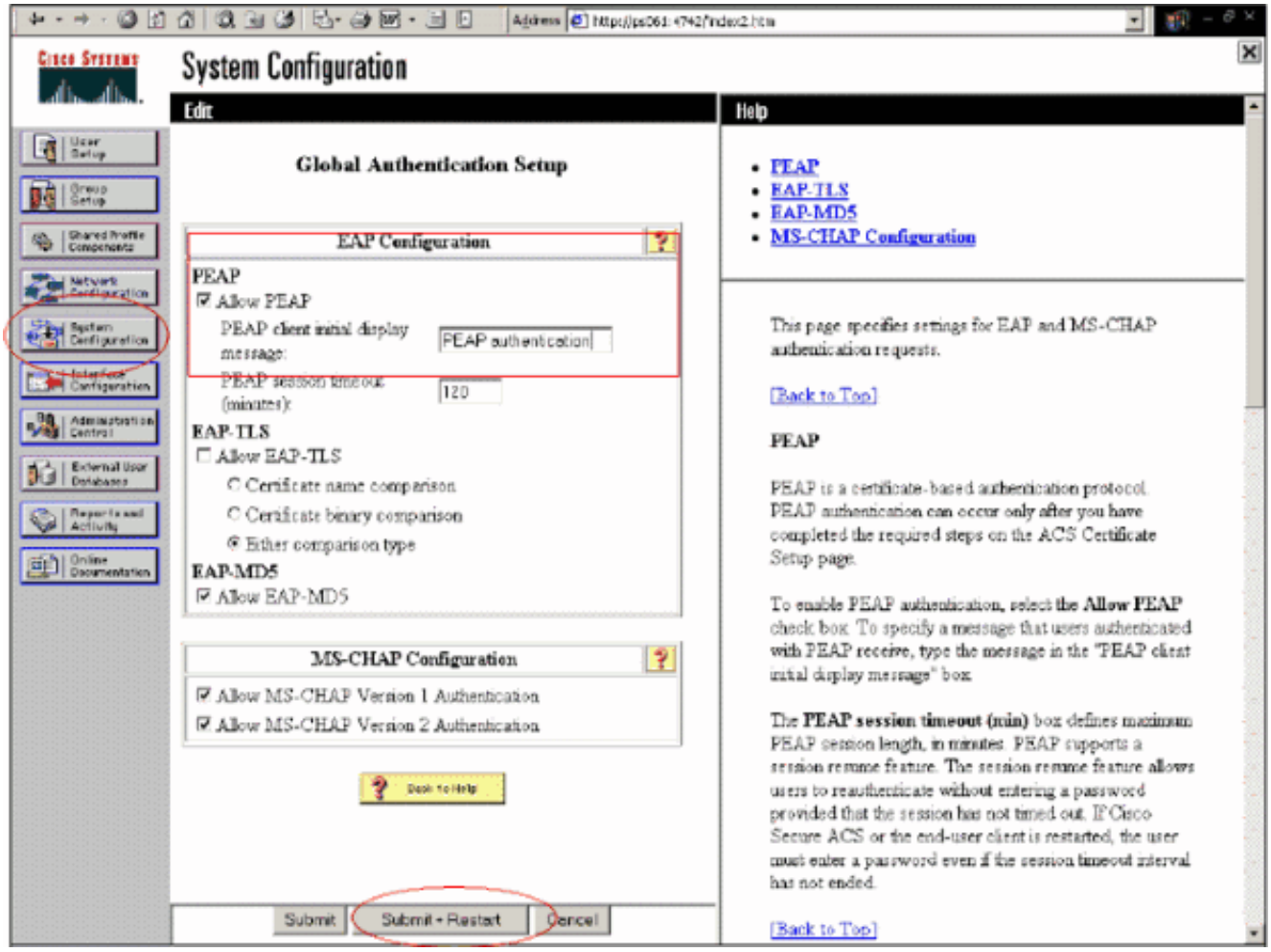
Procédez comme suit :

1. Sous **Configuration du réseau**, ajoutez/modifiez le client AAA pour le WLC qui sera utilisé. Entrez la clé " secrète partagée " (commune à WLC) qui est utilisée entre le client AAA et ACS. Sélectionnez **Authentifier à l'aide de > RADIUS (Cisco Airespace)** pour ce client AAA. Ensuite, cliquez sur **Soumettre +**



Appliquer.

2. Demandez et installez un certificat de serveur auprès d'une autorité de certification connue et fiable, telle que RSA Keon Certificate Authority.Pour plus d'informations sur ce processus, reportez-vous à la documentation fournie avec Cisco ACS. Si vous utilisez RSA Certificate Manager, vous pouvez consulter le guide de mise en oeuvre RSA Keon Aironet pour obtenir de l'aide supplémentaire. Vous devez terminer cette tâche avant de continuer.**Remarque :** Les certificats auto-signés peuvent également être utilisés. Reportez-vous à la documentation de Cisco Secure ACS pour savoir comment les utiliser.
3. Sous **Configuration système > Configuration de l'authentification globale**, cochez la case **Autoriser l'**authentification
PEAP.



Configuration du contrôleur LAN sans fil Cisco pour 802.1x

Procédez comme suit :

1. Connectez-vous à l'interface de ligne de commande du WLC pour configurer le contrôleur afin qu'il puisse être configuré pour se connecter au serveur Cisco Secure ACS.
2. Entrez la commande **config radius auth ip-address** à partir du WLC pour configurer un serveur RADIUS pour l'authentification.**Remarque :** lorsque vous effectuez un test avec le serveur RADIUS de RSA Authentication Manager, saisissez l'adresse IP du serveur RADIUS de RSA Authentication Manager. Lorsque vous effectuez un test avec le serveur Cisco ACS, saisissez l'adresse IP du serveur Cisco Secure ACS.
3. Entrez la commande **config radius auth port** à partir du WLC pour spécifier le port UDP pour l'authentification. Les ports 1645 ou 1812 sont actifs par défaut dans RSA Authentication Manager et sur le serveur Cisco ACS.
4. Entrez la commande **config radius auth secret** à partir du WLC pour configurer le secret partagé sur le WLC. Cette valeur doit correspondre au secret partagé créé dans les serveurs RADIUS pour ce client RADIUS.
5. Entrez la commande **config radius auth enable** à partir du WLC pour activer l'authentification. Si vous le souhaitez, entrez la commande **config radius auth disable** pour désactiver l'authentification. Notez que l'authentification est désactivée par défaut.
6. Sélectionnez l'option de sécurité de couche 2 appropriée pour le WLAN souhaité au niveau du WLC.
7. Utilisez les commandes **show radius auth statistics** et **show radius summary** pour vérifier que les paramètres RADIUS sont correctement configurés.**Remarque :** Les temporisateurs par

défaut pour le délai d'attente de la requête EAP sont faibles et peuvent devoir être modifiés. Pour cela, utilisez la commande **config advanced eap request-timeout** ***<secondes>.*** Il peut également aider à ajuster le délai d'attente de la demande d'identité en fonction des besoins. Pour cela, utilisez la commande **config advanced eap identity-request-timeout** ***<secondes>.***

Configuration du client sans fil 802.11

Pour obtenir une explication détaillée de la configuration de votre matériel sans fil et de votre client supplicant, reportez-vous à la documentation Cisco.

Problèmes identifiés

Voici quelques-uns des problèmes connus liés à l'authentification RSA SecureID :

- Jeton logiciel RSA. Les nouveaux modes Pin et Next Tokencode ne sont pas pris en charge lors de l'utilisation de cette forme d'authentification avec XP2. (FIXE suite à ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Si votre implémentation ACS est plus ancienne ou si vous n'avez pas le patch ci-dessus, le client ne pourra pas s'authentifier tant que l'utilisateur ne passera pas de “ Activé ; Nouveau mode PIN ” à “ Activé ”. Pour ce faire, vous pouvez demander à l'utilisateur de terminer une authentification non sans fil ou utiliser l'authentification “ test ” application RSA.
- Refuser les codes PIN alphanumériques à 4 chiffres. Si un utilisateur en mode Nouvelle broche va à l'encontre de la stratégie PIN, le processus d'authentification échoue et l'utilisateur ignore comment et pourquoi. En règle générale, si un utilisateur va à l'encontre de la stratégie, il reçoit un message indiquant que le code PIN a été rejeté et qu'il est invité à nouveau tout en indiquant à l'utilisateur quel est le code PIN (par exemple, si la stratégie de code PIN est composée de 5 à 7 chiffres, l'utilisateur entre toutefois 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
- Cisco Protected Extensible Authentication Protocol
- Authentification EAP avec le serveur RADIUS
- Support et documentation techniques - Cisco Systems