RSA SecurID Ready with Wireless LAN Controller and Cisco Secure ACS Configuration Example

Inhalt

Einleitung

In diesem Dokument wird erläutert, wie Cisco LWAPP-fähige APs und WLCs (Wireless LAN Controller) sowie der Cisco Secure Access Control Server (ACS) für die Verwendung in einer WLAN-Umgebung mit RSA SecurID-Authentifizierung eingerichtet und konfiguriert werden. RSA SecurID-spezifische Implementierungsleitfäden finden Sie unter www.rsasecured.com.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Kenntnis der WLCs und der Konfiguration der WLC-Basisparameter.
- Informationen zur Konfiguration des Profils des Cisco Wireless Client mithilfe des Aironet Desktop Utility (ADU).

- Verfügen Sie über Fachkenntnisse im Bereich Cisco Secure ACS.
- Grundkenntnisse von LWAPP.
- Grundlegende Kenntnisse der Microsoft Windows Active Directory-Dienste (AD) sowie der Konzepte von Domänencontroller und DNS besitzen.**Hinweis:** Stellen Sie vor dem Versuch dieser Konfiguration sicher, dass der ACS- und der RSA Authentication Manager-Server sich in derselben Domäne befinden und die Systemuhr genau synchronisiert ist. Wenn Sie Microsoft Windows AD Services verwenden, lesen Sie die Microsoft-Dokumentation, um den ACS- und RSA Manager-Server in derselben Domäne zu konfigurieren. Weitere Informationen finden Sie unter Active Directory und Windows-Benutzerdatenbank konfigurieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- RSA Authentication Manager 6.1
- RSA Authentication Agent 6.1 für Microsoft Windows
- Cisco Secure ACS 4.0(1) Build 27**Hinweis:** Der im Lieferumfang enthaltene RADIUS-Server kann anstelle des Cisco ACS verwendet werden. Informationen zur Konfiguration des Servers finden Sie in der RADIUS-Dokumentation, die im RSA Authentication Manager enthalten war.
- Cisco WLCs und Lightweight Access Points für Version 4.0 (Version 4.0.155.0)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Das RSA SecurID-System ist eine Zwei-Faktor-Benutzerauthentifizierungslösung. In Verbindung mit dem RSA Authentication Manager und einem RSA Authentication Agent muss der RSA SecurID-Authentifizierer Benutzer dazu verpflichten, sich mithilfe eines Zwei-Faktor-Authentifizierungsmechanismus zu identifizieren.

Eine ist der RSA SecurID-Code, eine Zufallszahl, die alle 60 Sekunden auf dem RSA SecureID-Authentifizierungsgerät generiert wird. Die andere ist die persönliche Identifikationsnummer (PIN).

RSA SecurID-Authentifizierer sind genauso einfach zu verwenden wie die Eingabe eines Kennworts. Jedem Endbenutzer wird ein RSA SecurID-Authentifizierer zugewiesen, der einen einmaligen Code generiert. Bei der Anmeldung gibt der Benutzer diese Nummer und eine geheime PIN ein, um erfolgreich authentifiziert zu werden. Ein weiterer Vorteil besteht darin, dass RSA SecurID-Hardware-Token in der Regel vorprogrammiert sind, damit sie nach Erhalt voll funktionsfähig sind.

In dieser Flash-Demonstration wird die Verwendung eines sicheren RSA-ID-Authentifizierungsgeräts erläutert: RSA-Demo.

Über das RSA SecurID Ready-Programm unterstützen Cisco WLCs und Cisco Secure ACS-Server die RSA SecurID-Authentifizierung sofort. Die RSA Authentication Agent-Software fängt lokale oder Remote-Zugriffsanfragen von Benutzern (oder Benutzergruppen) ab und leitet diese zur Authentifizierung an das RSA Authentication Manager-Programm weiter.

Die RSA Authentication Manager-Software ist die Verwaltungskomponente der RSA SecurID-Lösung. Sie dient zur Verifizierung von Authentifizierungsanforderungen und zur zentralen Verwaltung von Authentifizierungsrichtlinien für Unternehmensnetzwerke. Es arbeitet mit RSA SecurID-Authentifizierern und der RSA Authentication Agent-Software zusammen.

In diesem Dokument wird ein Cisco ACS-Server als RSA Authentication Agent verwendet, indem die Agent-Software darauf installiert wird. Der WLC ist der Network Access Server (NAS) (AAA-Client), der die Client-Authentifizierungen wiederum an den ACS weiterleitet. Das Dokument veranschaulicht die Konzepte und das Setup mithilfe der PEAP-Clientauthentifizierung (Protected Extensible Authentication Protocol).

Weitere Informationen zur PEAP-Authentifizierung finden Sie unter Cisco Protected Extensible Authentication Protocol.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

In diesem Dokument werden folgende Konfigurationen verwendet:

- Agent-Host-Konfiguration
- Konfiguration des Authentifizierungs-Agenten

Agent-Host-Konfiguration

Verwendung von Cisco Secure ACS als RADIUS-Server

Um die Kommunikation zwischen dem Cisco Secure ACS und der RSA Authentication Manager/RSA SecurID Appliance zu vereinfachen, muss der Datenbank RSA Authentication Manager ein Agent Host-Datensatz hinzugefügt werden. Der Agent Host-Datensatz identifiziert das Cisco Secure ACS in seiner Datenbank und enthält Informationen zur Kommunikation und Verschlüsselung.

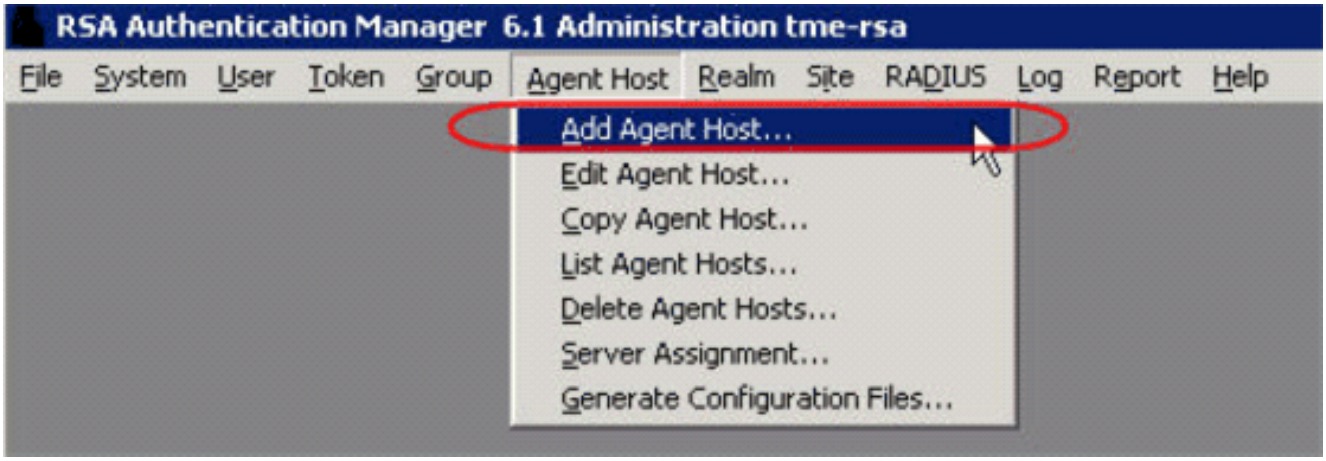
Um den Agent Host-Datensatz zu erstellen, benötigen Sie folgende Informationen:

- Hostname des Cisco ACS-Servers
- IP-Adressen für alle Netzwerkschnittstellen des Cisco ACS Servers

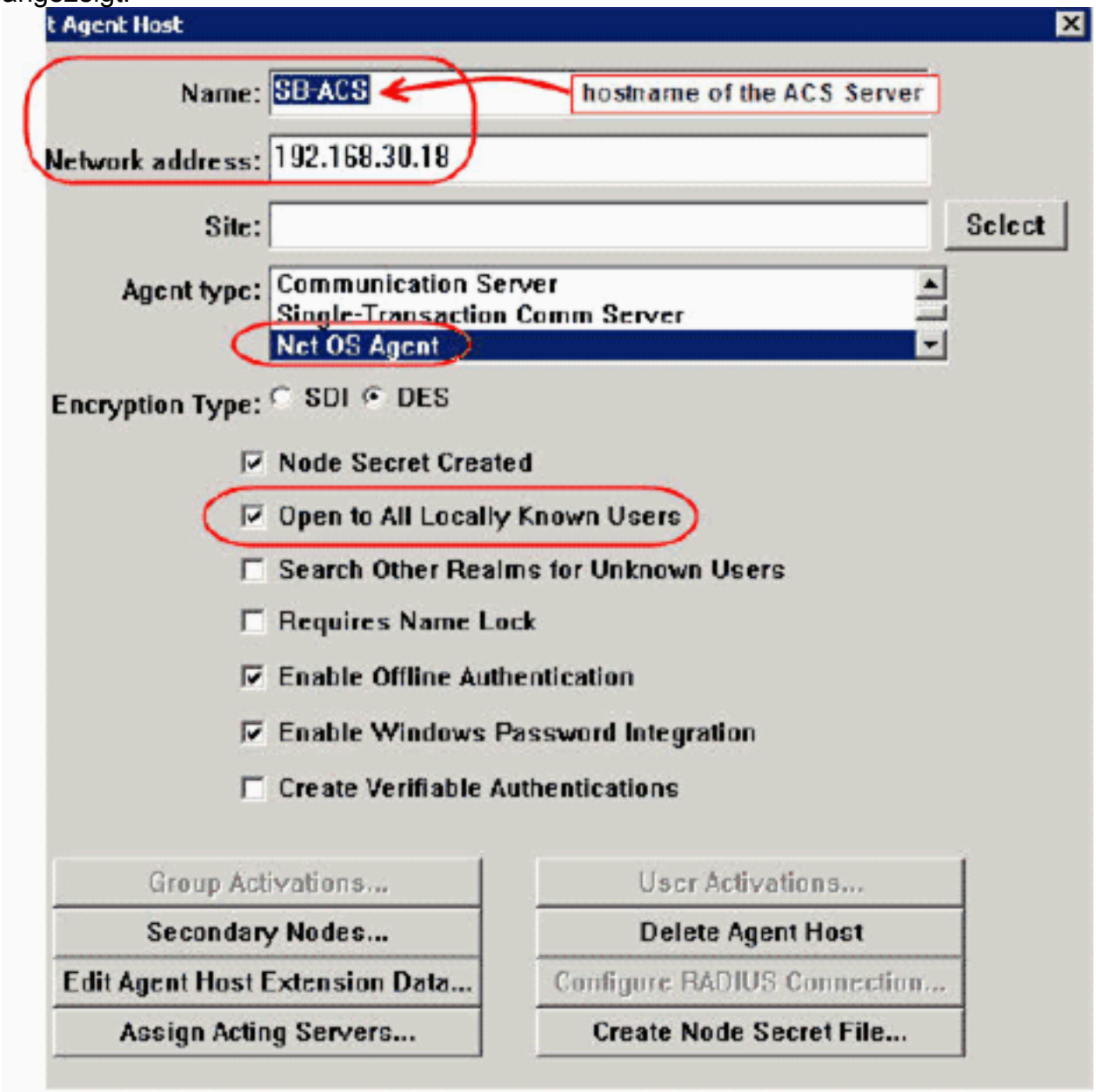
Führen Sie diese Schritte aus:

1. Öffnen Sie die Anwendung RSA Authentication Manager Host Mode.
2. Wählen Sie **Agent-Host > Agent-Host hinzufügen**

aus.



Dieses Fenster wird angezeigt:



3. Geben Sie die entsprechenden Informationen für den Cisco ACS-Servernamen und die Netzwerkadresse ein. Wählen Sie **NetOS** als Agent-Typ aus, und aktivieren Sie das Kontrollkästchen **Open to All Locally Known Users**.
4. Klicken Sie auf **OK**.

Verwenden des RSA Authentication Manager 6.1 RADIUS-Servers

Um die Kommunikation zwischen dem Cisco WLC und dem RSA Authentication Manager zu vereinfachen, muss der Datenbank des RSA Authentication Manager und der RADIUS Server ein Agent Host-Datensatz hinzugefügt werden. Der Agent Host-Datensatz identifiziert den Cisco WLC in seiner Datenbank und enthält Informationen zur Kommunikation und Verschlüsselung.

Um den Agent Host-Datensatz zu erstellen, benötigen Sie folgende Informationen:

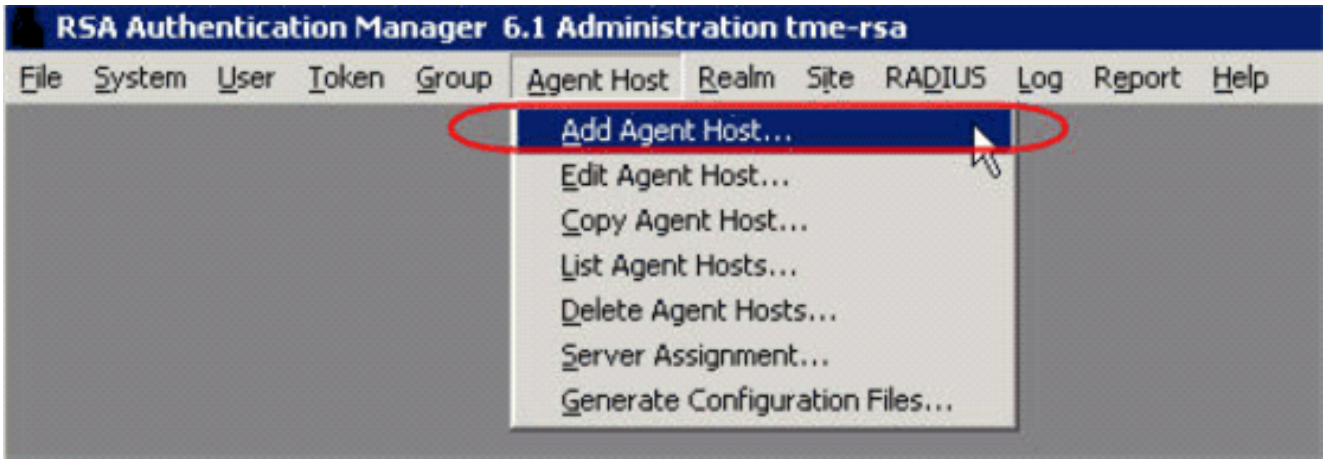
- WLC-Hostname
- Management-IP-Adressen des WLC
- geheim RADIUS, der mit dem geheimen RADIUS-Schlüssel auf dem Cisco WLC übereinstimmen muss

Beim Hinzufügen des Agent Host Record wird die Rolle des WLC als Kommunikationsserver konfiguriert. Diese Einstellung wird vom RSA Authentication Manager verwendet, um die Kommunikation mit dem WLC zu bestimmen.

Hinweis: Hostnamen im RSA Authentication Manager/RSA SecurID Appliance müssen auf gültige IP-Adressen im lokalen Netzwerk aufgelöst werden.

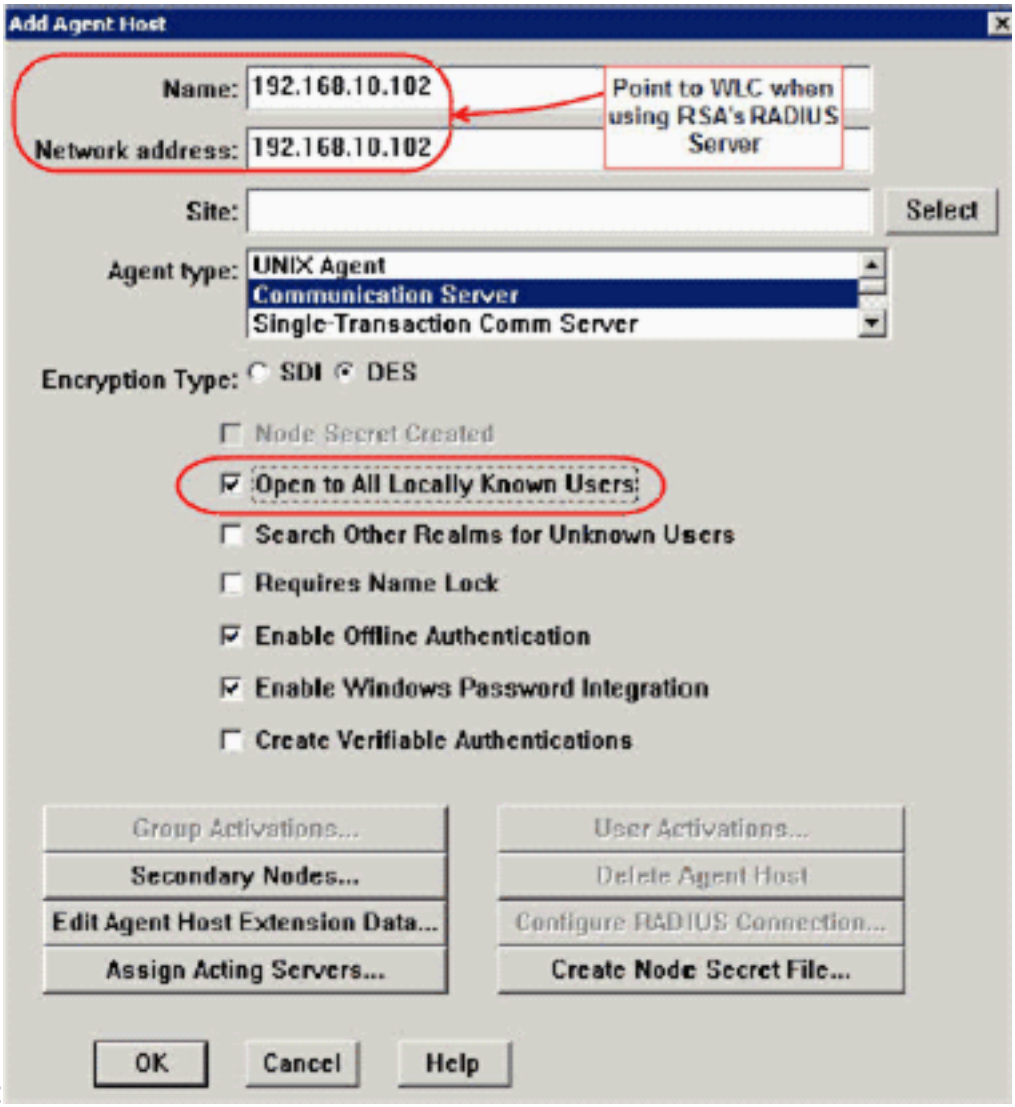
Führen Sie diese Schritte aus:

1. Öffnen Sie die Anwendung RSA Authentication Manager Host Mode.
2. Wählen Sie **Agent-Host > Agent-Host hinzufügen aus**.

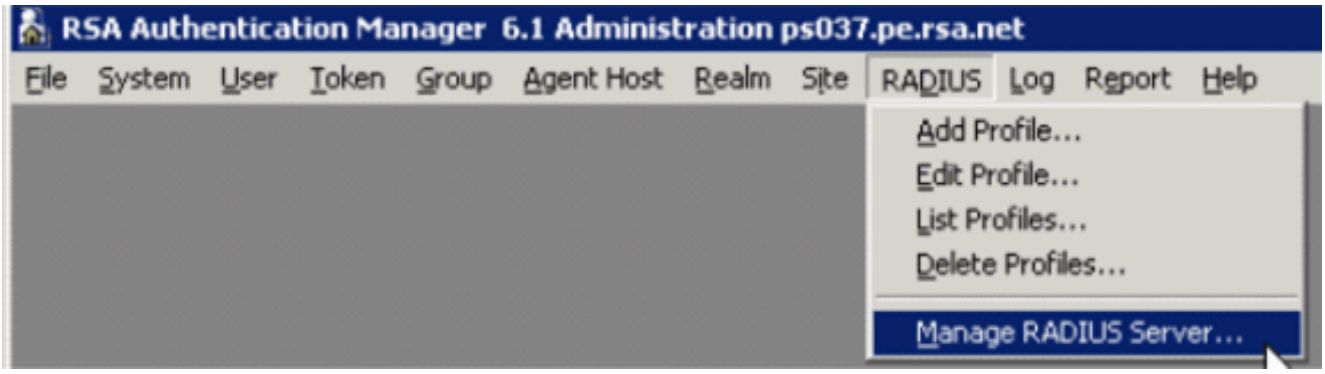


Dieses Fenster wird

angezeigt:

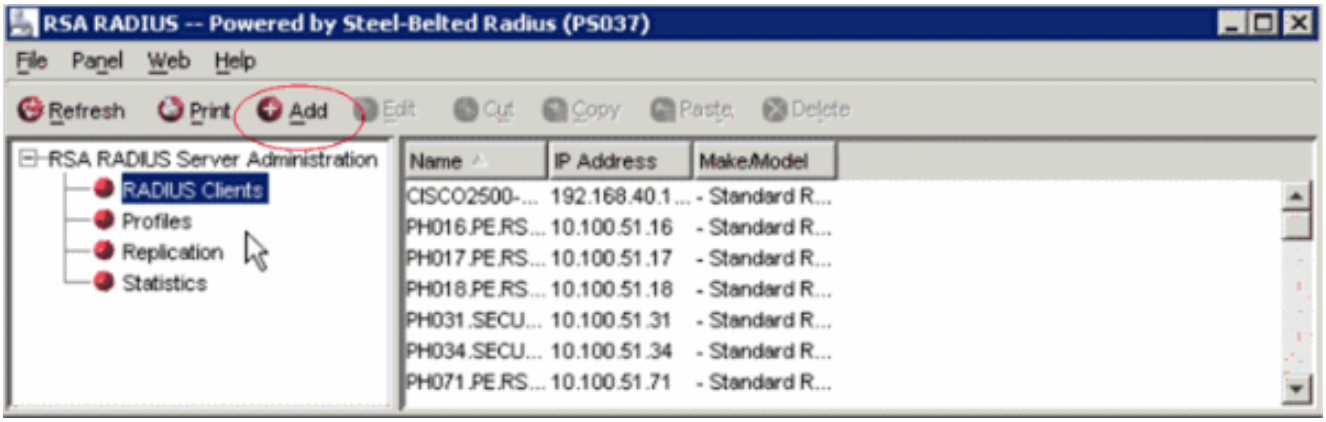


3. Geben Sie die entsprechenden Informationen für den WLC-Hostnamen (ggf. einen auflösbaren FQDN) und die Netzwerkadresse ein. Wählen Sie **Communication Server** als Agent-Typ aus, und aktivieren Sie das Kontrollkästchen **Open to All Locally Known Users (Für alle lokal bekannten Benutzer öffnen)**.
4. Klicken Sie auf **OK**.
5. Wählen Sie im Menü **RADIUS > RADIUS-Server verwalten aus**.

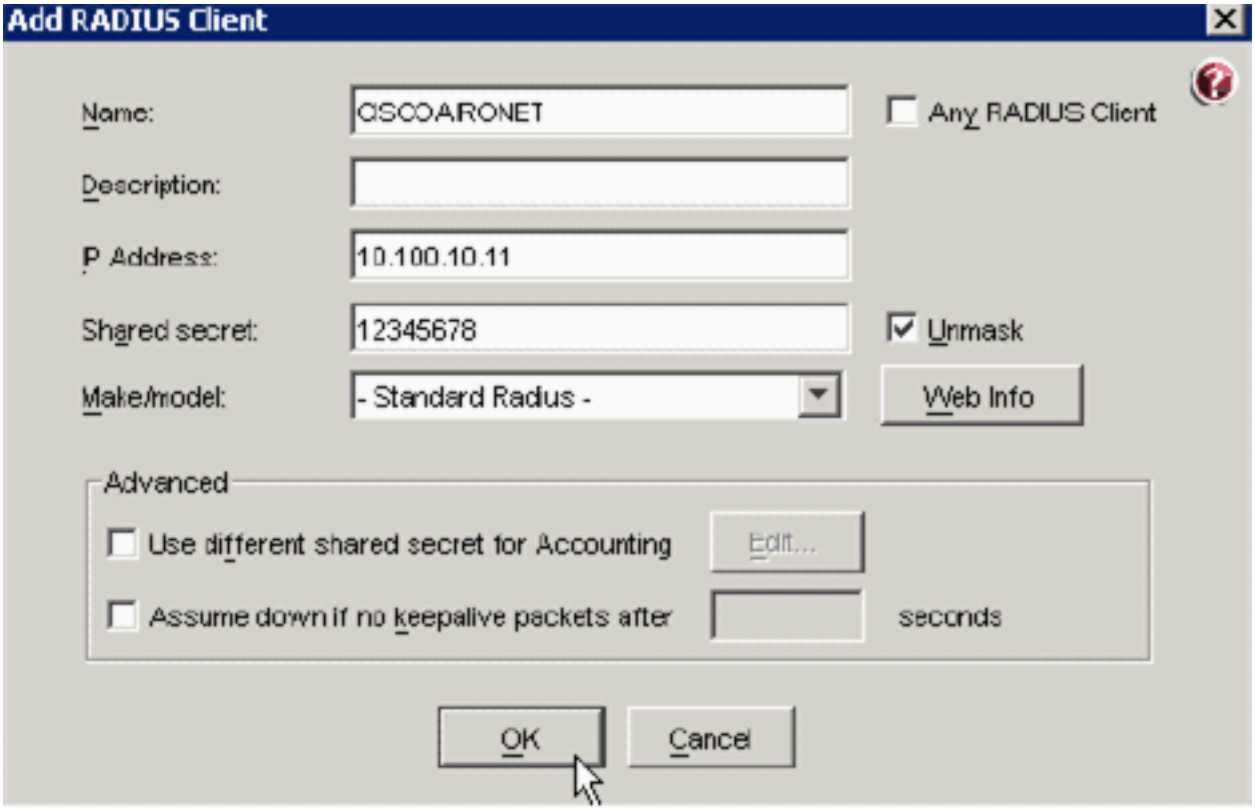


Ein neues Verwaltungsfenster wird geöffnet.

6. Wählen Sie in diesem Fenster **RADIUS Clients aus**, und klicken Sie dann auf **Hinzufügen**.



7. Geben Sie die entsprechenden Informationen für den Cisco WLC ein. Der gemeinsame geheime Schlüssel muss mit dem auf dem Cisco WLC definierten gemeinsamen geheimen Schlüssel
übereinstimmen.



8. Klicken Sie auf **OK**.

Konfiguration des Authentifizierungs-Agenten

Diese Tabelle stellt die RSA Authentication Agent-Funktionalität von ACS dar:

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

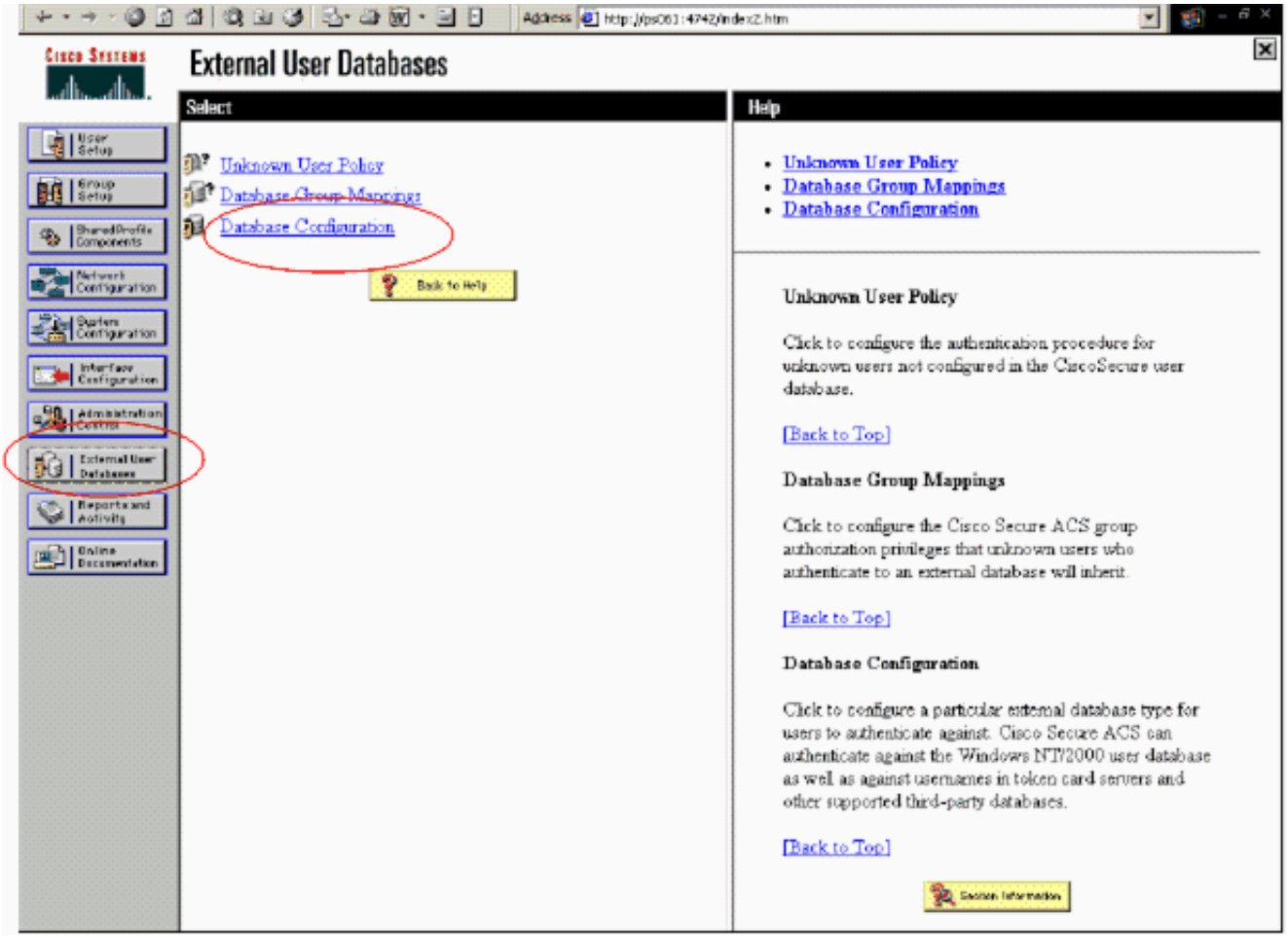
Hinweis: In der im RSA Authentication Manager enthaltenen RADIUS-Dokumentation finden Sie Informationen zur Konfiguration des RADIUS-Servers, sofern es sich um den RADIUS-Server handelt, der verwendet wird.

Konfigurieren von Cisco ACS

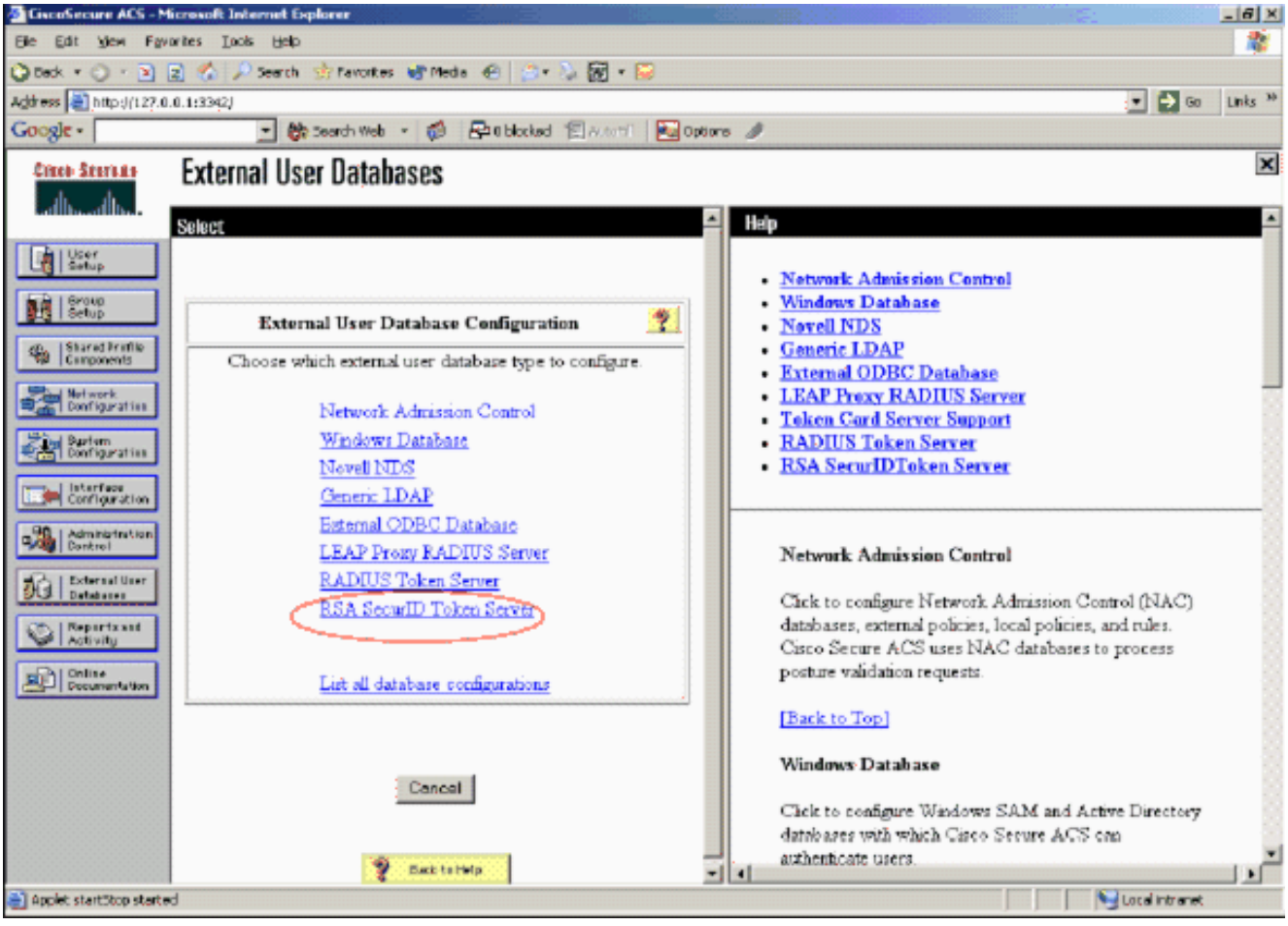
Aktivieren der RSA SecurID-Authentifizierung

Cisco Secure ACS unterstützt die RSA SecurID-Authentifizierung von Benutzern. Gehen Sie wie folgt vor, um Cisco Secure ACS für die Authentifizierung von Benutzern mit Authentication Manager 6.1 zu konfigurieren:

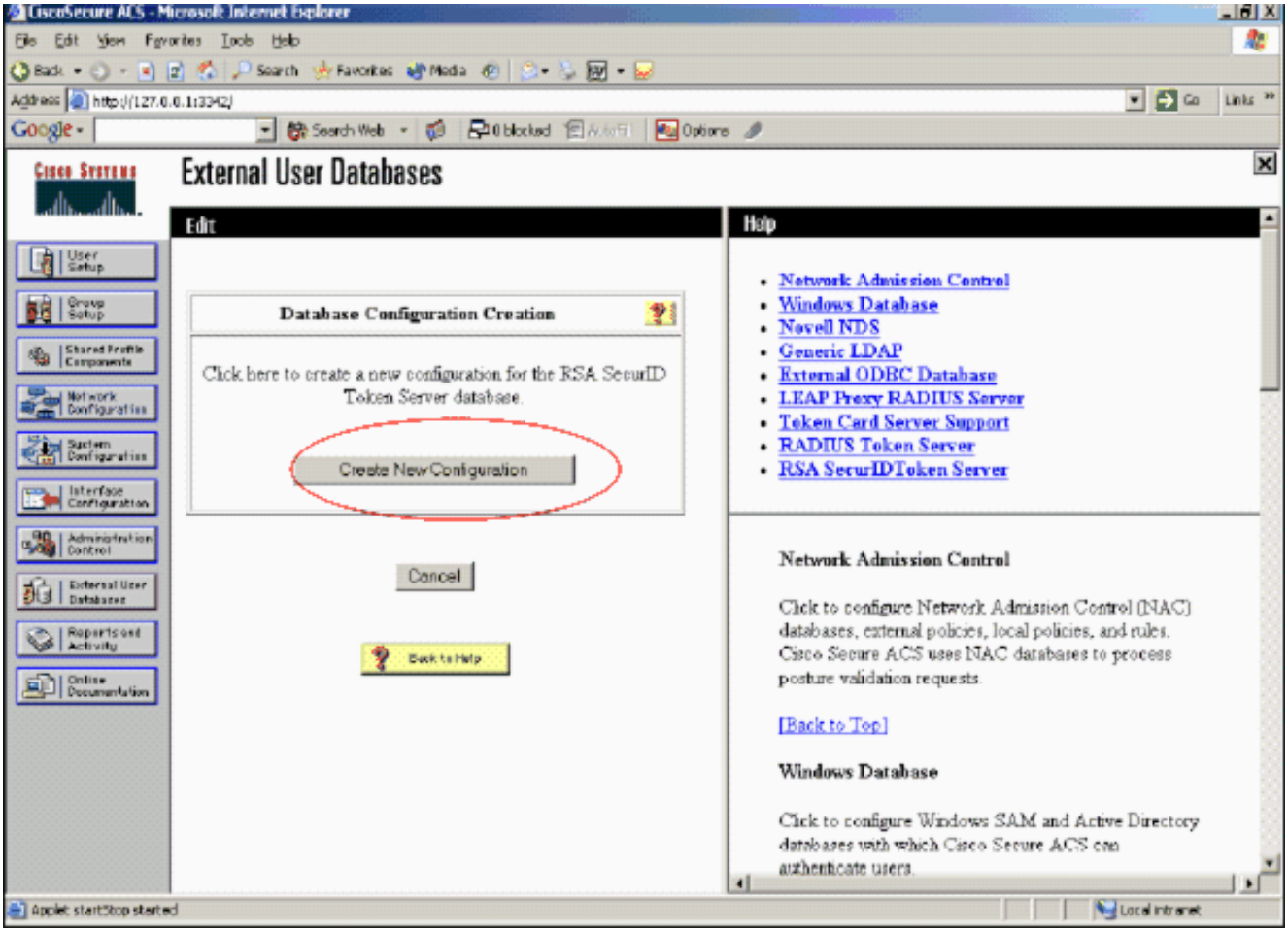
1. Installieren Sie den RSA Authentication Agent 5.6 oder höher für Windows auf demselben System wie der Cisco Secure ACS-Server.
2. Überprüfen Sie die Konnektivität, indem Sie die Testauthentifizierungsfunktion des Authentifizierungs-Agenten ausführen.
3. Kopieren Sie die Datei "aceclnt.dll" aus dem Verzeichnis **c:\Program Files\RSA Security\RSA Authentication Manager\prog** des RSA-Servers in das **c:\WINNT\system32** Verzeichnis des ACS-Servers.
4. Klicken Sie in der Navigationsleiste auf **Externe Benutzerdatenbank**. Klicken Sie dann auf der Seite Externe Datenbank auf **Datenbankkonfiguration**.



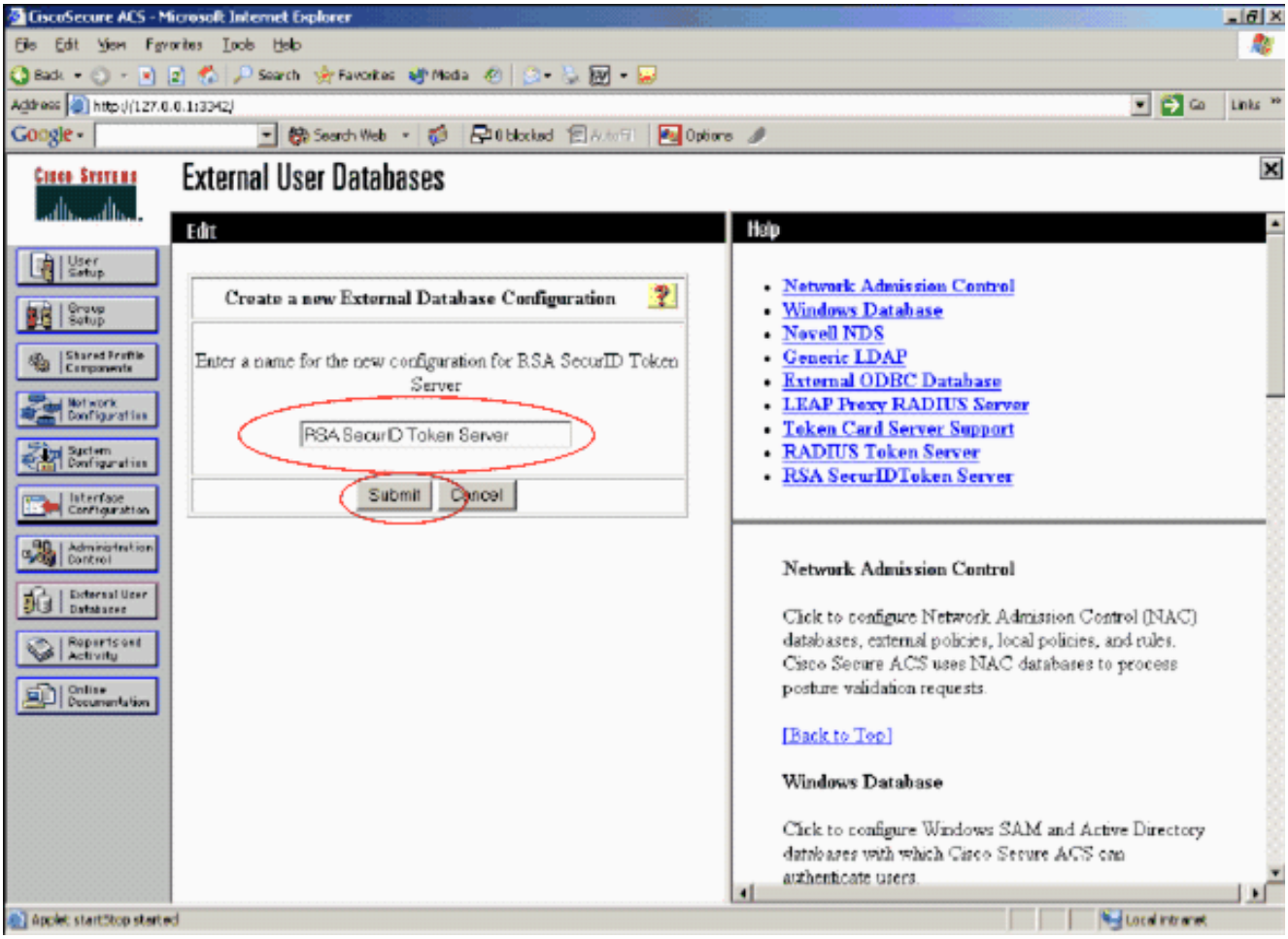
5. Klicken Sie auf der Seite Konfiguration der externen Benutzerdatenbank auf **RSA SecurID Token Server**.



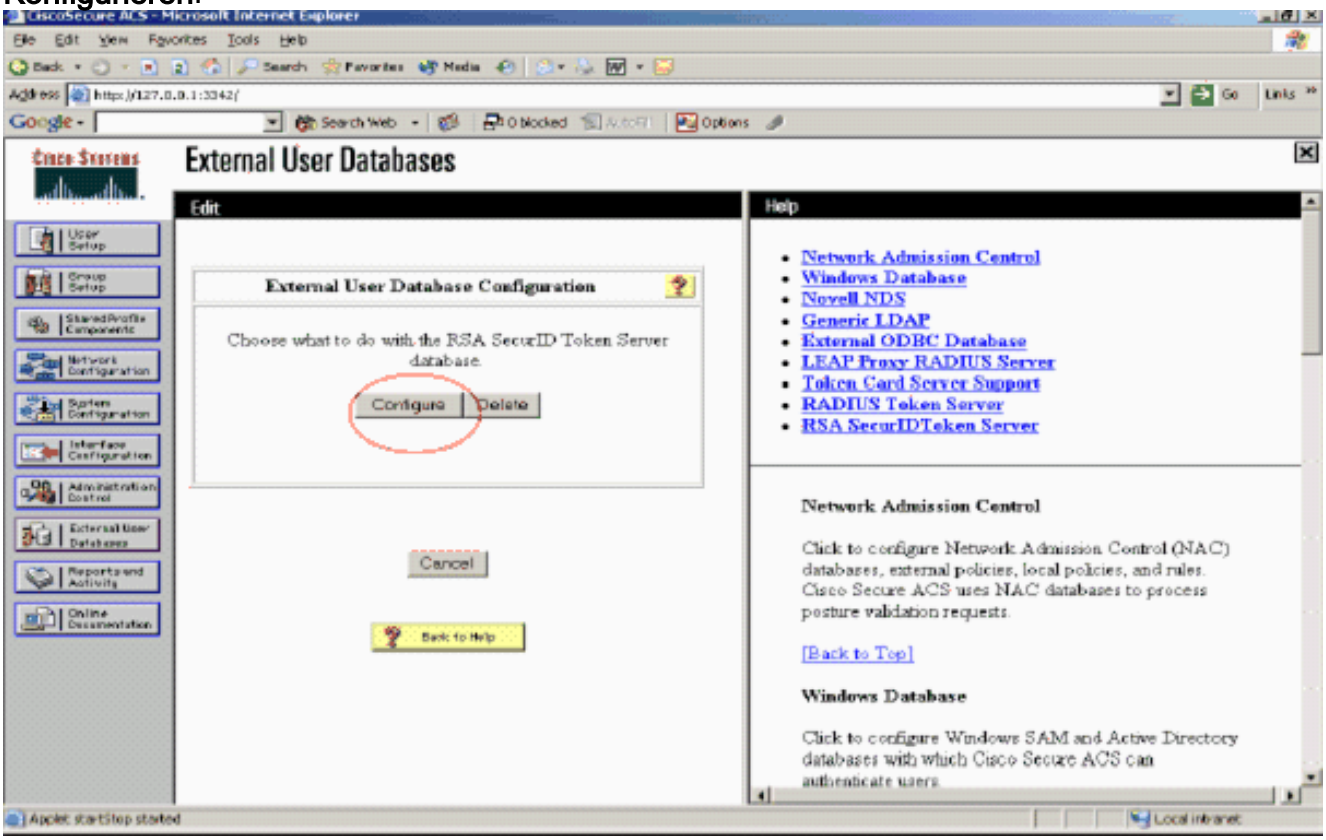
6. Klicken Sie auf **Neue Konfiguration erstellen**.



7. Geben Sie einen Namen ein, und klicken Sie dann auf **Senden**.

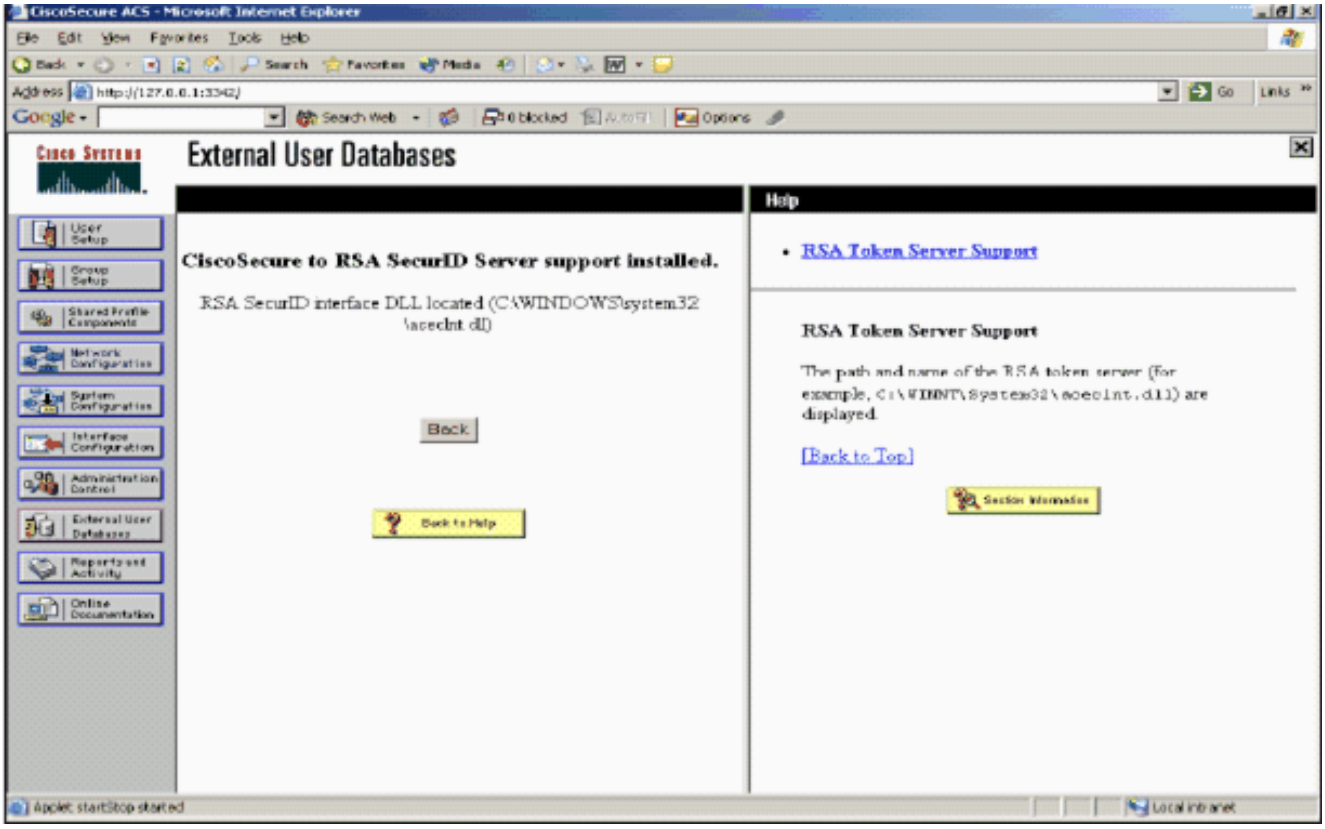


8. Klicken Sie auf **Konfigurieren**.



Cisco Secure ACS zeigt den Namen des Tokenservers und den Pfad zur Authentifizierer-DLL an. Diese Informationen bestätigen, dass Cisco Secure ACS den RSA Authentication Agent kontaktieren kann. Sie können die externe RSA SecurID-Benutzerdatenbank Ihrer Unbekannten Benutzerrichtlinie hinzufügen oder bestimmte Benutzerkonten zuweisen, um

diese Datenbank für die Authentifizierung zu verwenden.

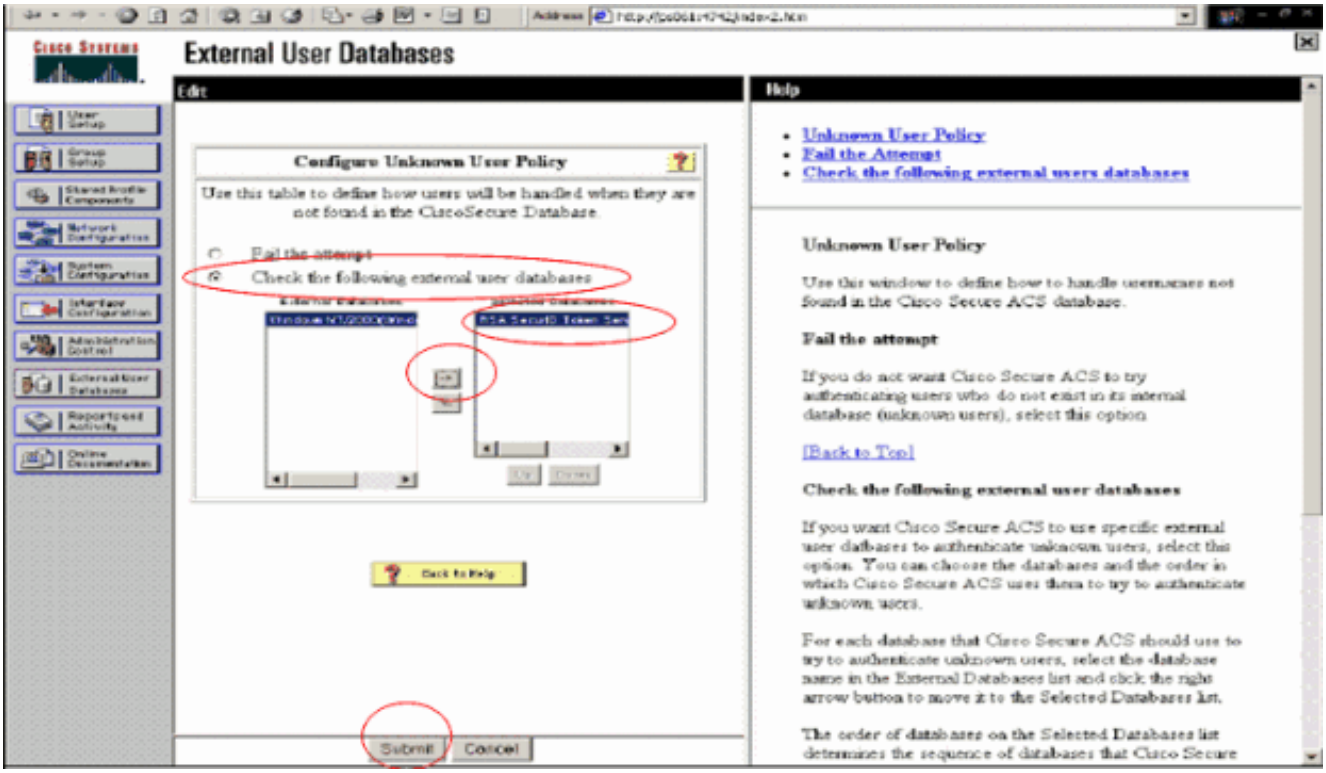


Hinzufügen/Konfigurieren der RSA SecurID-Authentifizierung zu Ihrer unbekannten Benutzerrichtlinie

Führen Sie diese Schritte aus:

1. Klicken Sie in der ACS-Navigationsleiste auf **Externe Benutzerdatenbank > Unbekannte Benutzerrichtlinie**.

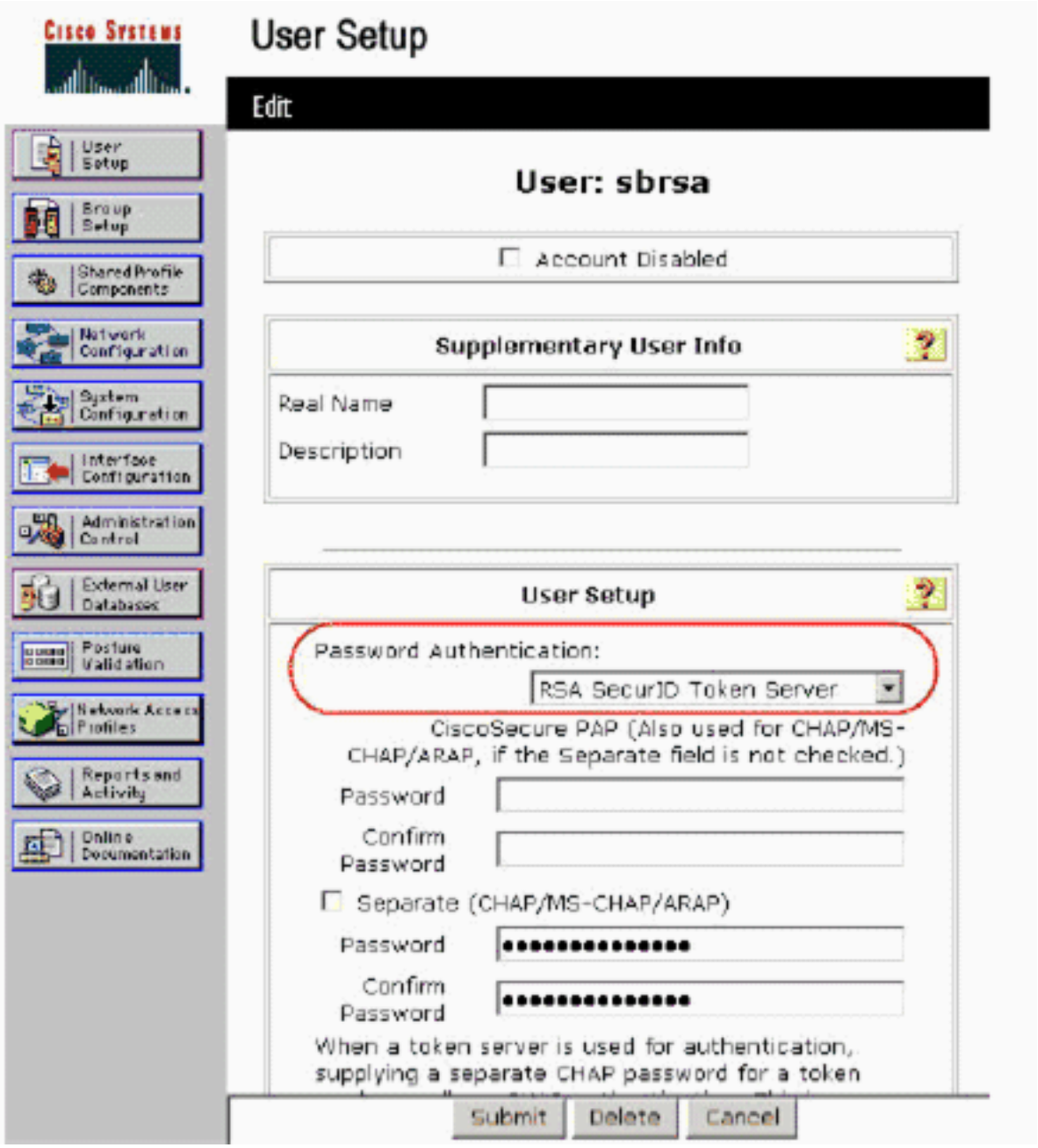
2. Wählen Sie auf der Seite **Unbekannte Benutzerrichtlinie die Option Folgende externe Benutzerdatenbanken überprüfen**, **RSA SecurID Token Server** markieren und in das Feld Ausgewählte Datenbanken verschieben aus. Klicken Sie anschließend auf **Senden**.



Hinzufügen/Konfigurieren der RSA SecurID-Authentifizierung für bestimmte Benutzerkonten

Führen Sie diese Schritte aus:

1. Klicken Sie in der Hauptbenutzeroberfläche des ACS Admin auf **User Setup** (Benutzereinrichtung). Geben Sie den Benutzernamen ein, und klicken Sie auf **Hinzufügen** (oder wählen Sie einen vorhandenen Benutzer aus, den Sie ändern möchten).
2. Wählen Sie unter User Setup > Password Authentication (Benutzereinrichtung > Kennwortauthentifizierung) die Option **RSA SecurID Token Server aus**. Klicken Sie anschließend auf **Senden**.



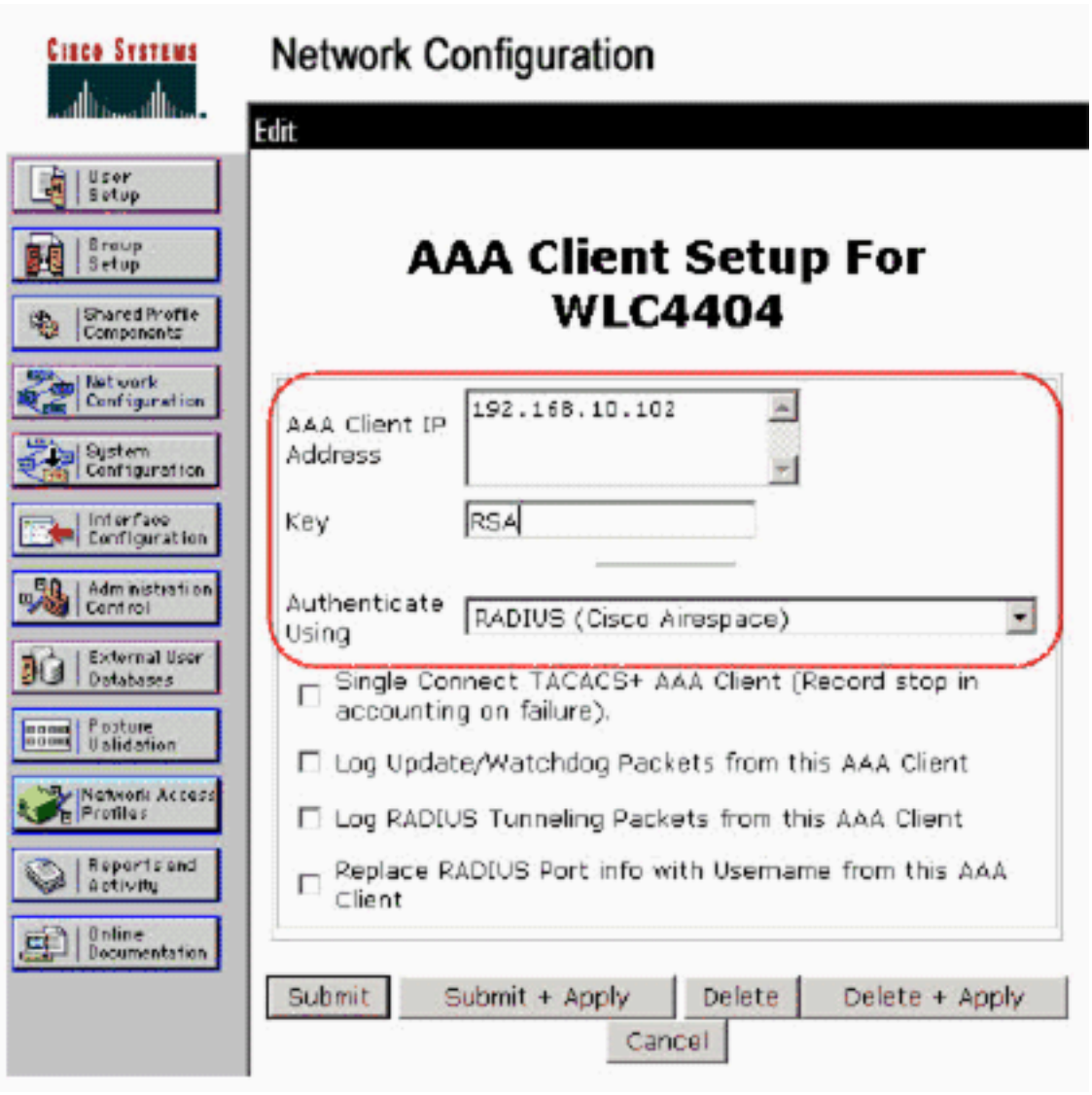
Hinzufügen eines RADIUS-Clients in Cisco ACS

Die Cisco ACS-Serverinstallation benötigt die IP-Adressen des WLC, um als NAS für die Weiterleitung von Client-PEAP-Authentifizierungen an den ACS zu dienen.

Führen Sie diese Schritte aus:

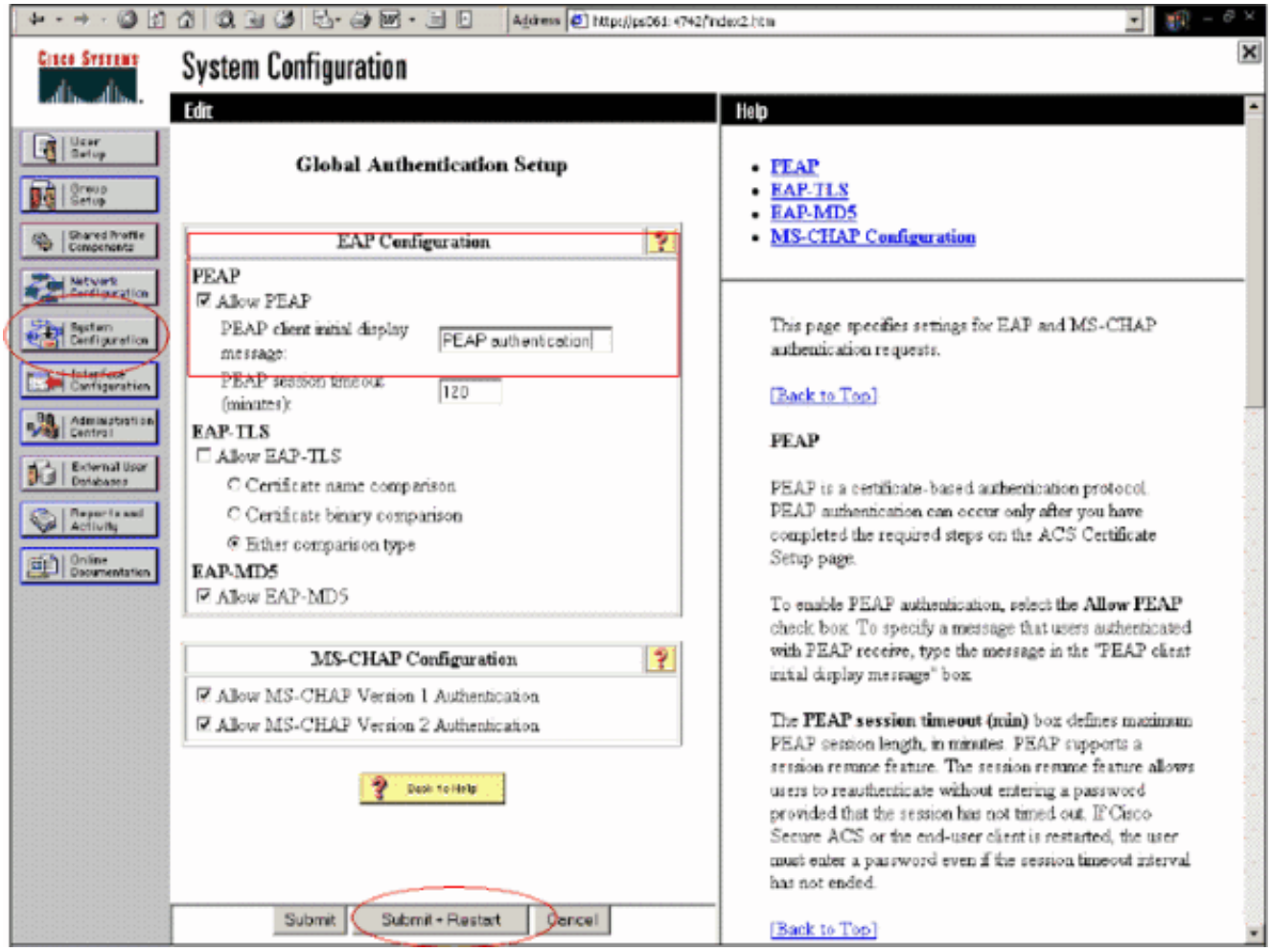
1. Fügen Sie unter **Netzwerkkonfiguration** den AAA-Client für den zu verwendenden WLC hinzu bzw. bearbeiten Sie ihn. Geben Sie den gemeinsamen geheimen Schlüssel (gemeinsam mit WLC) ein, der zwischen dem AAA-Client und dem ACS verwendet wird. Wählen Sie für diesen AAA-Client **Authentication Using > RADIUS (Cisco Air)** aus. Klicken Sie dann auf

Senden +



Übernehmen.

2. Beantragen und installieren Sie ein Serverzertifikat von einer bekannten, vertrauenswürdigen Zertifizierungsstelle wie der RSA Keon Certificate Authority.Weitere Informationen zu diesem Prozess finden Sie in der Dokumentation, die im Lieferumfang von Cisco ACS enthalten ist. Wenn Sie RSA Certificate Manager verwenden, können Sie den Implementierungsleitfaden für RSA Keon Aironet als zusätzliche Hilfe anzeigen. Sie müssen diese Aufgabe erfolgreich abschließen, bevor Sie fortfahren können.**Hinweis:** Sie können auch selbst signierte Zertifikate verwenden. Informationen zur Verwendung dieser Funktionen finden Sie in der Dokumentation zu Cisco Secure ACS.
3. Aktivieren Sie unter **Systemkonfiguration > Globales Authentifizierungs-Setup** das Kontrollkästchen **PEAP-**Authentifizierung **zulassen**.



Konfigurieren der Cisco Wireless LAN Controller-Konfiguration für 802.1x

Führen Sie diese Schritte aus:

1. Stellen Sie eine Verbindung zur Befehlszeilenschnittstelle des WLC her, um den Controller so zu konfigurieren, dass er für die Verbindung mit dem Cisco Secure ACS-Server konfiguriert werden kann.
2. Geben Sie den Befehl **config radius auth ip-address** vom WLC ein, um einen RADIUS-Server für die Authentifizierung zu konfigurieren.**Hinweis:** Geben Sie beim Testen mit dem RADIUS-Server des RSA Authentication Manager die IP-Adresse des RADIUS-Servers des RSA Authentication Manager ein. Wenn Sie mit dem Cisco ACS-Server testen, geben Sie die IP-Adresse des Cisco Secure ACS-Servers ein.
3. Geben Sie den Befehl **config radius auth port** vom WLC ein, um den UDP-Port für die Authentifizierung anzugeben. Die Ports 1645 oder 1812 sind standardmäßig sowohl im RSA Authentication Manager als auch im Cisco ACS-Server aktiv.
4. Geben Sie den Befehl **config radius auth secret** vom WLC ein, um den gemeinsamen geheimen Schlüssel auf dem WLC zu konfigurieren. Dies muss mit dem in den RADIUS-Servern für diesen RADIUS-Client erstellten gemeinsamen geheimen Schlüssel übereinstimmen.
5. Geben Sie den Befehl **config radius auth enable** vom WLC ein, um die Authentifizierung zu aktivieren. Geben Sie bei Bedarf den Befehl **config radius auth disable** ein, um die Authentifizierung zu deaktivieren. Beachten Sie, dass die Authentifizierung standardmäßig deaktiviert ist.
6. Wählen Sie die entsprechende Layer-2-Sicherheitsoption für das gewünschte WLAN am

WLC aus.

7. Verwenden Sie die Befehle **show radius auth statistics** und **show radius summary**, um zu überprüfen, ob die RADIUS-Einstellungen korrekt konfiguriert sind.**Hinweis:** Die Standard-Timer für EAP Request-Timeout sind niedrig und müssen möglicherweise geändert werden. Dies kann mit dem Befehl **config advanced eap request-timeout *<seconds>*** erfolgen. Es kann auch helfen, das Timeout für Identitätsanfragen entsprechend den Anforderungen anzupassen. Dies kann mithilfe des Befehls **config Advanced Eap Identity-Request-Timeout *<seconds>*** erfolgen.

802.11 Wireless-Client-Konfiguration

Eine ausführliche Erklärung zur Konfiguration der Wireless-Hardware und der Client-Komponente finden Sie in der Dokumentation von Cisco.

Bekannte Probleme

Dies sind einige der bekannten Probleme bei der RSA SecureID-Authentifizierung:

- RSA-Software-Token. Der neue Pin-Modus und der nächste Tokencode-Modus werden bei Verwendung dieser Form der Authentifizierung mit XP2 nicht unterstützt. (BEHOBEN als Ergebnis von ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Wenn Ihre ACS-Implementierung älter ist oder Sie den oben genannten Patch nicht haben, kann sich der Client erst authentifizieren, wenn der Benutzer von "Enabled;New PIN Mode" auf "Enabled" (Aktiviert) wechselt. Dies können Sie erreichen, indem Sie den Benutzer eine Nicht-Wireless-Authentifizierung durchführen lassen oder die RSA-Anwendung "Testauthentifizierung" verwenden.
- 4-stellige/alphanumerische PINs verweigern. Wenn ein Benutzer im New Pin-Modus gegen die PIN-Richtlinie verstößt, schlägt der Authentifizierungsprozess fehl, und der Benutzer weiß nicht, wie oder warum. Wenn ein Benutzer gegen die Richtlinie verstößt, wird ihm in der Regel eine Meldung gesendet, dass die PIN abgelehnt wurde, und er wird erneut aufgefordert, die PIN-Richtlinie anzuzeigen (z. B. wenn die PIN-Richtlinie 5-7 Ziffern umfasst, der Benutzer jedoch 4 Ziffern eingibt).

Zugehörige Informationen

- Dynamische VLAN-Zuordnung mit WLCs auf der Grundlage von ACS zu Active Directory Group Mapping - Konfigurationsbeispiel
- Client VPN over Wireless LAN mit WLC-Konfigurationsbeispiel
- Konfigurationsbeispiele für die Authentifizierung auf Wireless LAN-Controllern
- EAP-FAST-Authentifizierung mit Wireless LAN-Controllern und Konfigurationsbeispiel für einen externen RADIUS-Server
- Konfigurationsbeispiel für Wireless-Authentifizierungstypen auf festem ISR über SDM
- Beispiele für Wireless-Authentifizierungstypen in einem festkonfigurierten ISR
- Cisco Protected Extensible Authentication Protocol
- EAP-Authentifizierung mit RADIUS-Server
- Technischer Support und Dokumentation für Cisco Systeme