ワイヤレス LAN コントローラおよび Cisco Secure ACS を使用した RSA SecurID Ready の設定例

目次

概要

このドキュメントでは、RSA SecurID で認証される WLAN 環境で使用するために、Cisco Lightweight Access Point Protocol（LWAPP）対応の AP とワイヤレス LAN コントローラ（WLC）、および Cisco Secure Access Control Server（ACS）を設定する方法を説明します。RSA SecurID 固有の実装ガイドは www.rsasecured.com で確認できます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- WLC に関する知識と WLC の基本的なパラメータの設定方法に関する知識。
- Aironet Desktop Utility（ADU）を使用して Cisco ワイヤレス クライアントのプロファイルを設定する方法に関する知識。
- Cisco Secure ACS に関する実践的な知識があること。

- LWAPP の基本的な知識があること。
- Microsoft Windows Active Directory（AD）のサービスおよびドメイン コントローラと DNS の概念の基本的な知識があること。**注:** この設定を開始する前に、ACS と RSA Authentication Manager サーバが同じドメインにあり、システム クロックが正確に同期していることを確認します。 Microsoft Windows AD サービスを使用している場合は、同じドメインに ACS と RSA Manager サーバを設定するために、Microsoft のマニュアルを参照してください。 関連情報については、「Active Directory と Windows ユーザ データベースの設定」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- RSA Authentication Manager 6.1
- RSA Authentication Agent 6.1 for Microsoft Windows
- Cisco Secure ACS 4.0(1) ビルド 27**注:** 含まれている RADIUS サーバは Cisco ACS の代わりに使用できます。 サーバの設定方法については RSA Authentication Manager に付属している RADIUS の資料を参照してください。
- リリース 4.0（バージョン 4.0.155.0）用の Cisco WLC および Lightweight Access Point

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

RSA SecurID システムは 2 要素ユーザ認証ソリューションです。 RSA SecurID オーセンティケータは、RSA Authentication Manager および RSA Authentication Agent と組み合わせて使用し、ユーザが 2 要素認証機構を使用して自身を識別する必要があります。

要素の 1 つは RSA SecureID オーセンティケータ デバイスで 60 秒ごとに生成される乱数である RSA SecurID コードです。 もう 1 つは、Personal Identification Number（PIN）です。

RSA SecurID オーセンティケータはパスワードの入力と同じくらい簡単に使用できます。 ワンタイム使用コードを生成する RSA SecurID オーセンティケータが各エンド ユーザに割り当てられます。 ログインするとき、正常に認証されるためには、ユーザはこの番号と秘密の PIN を入力します。 RSA SecurID のハードウェア トークンは、通常、配布時に完全に機能するようにプログラム済みであるという長所もあります。

このフラッシュ デモンストレーションは、RSA secureID オーセンティケータ デバイスの使用方法を示しています。 RSA のデモ。

Cisco WLC サーバおよび Cisco Secure ACS サーバは RSA SecurID Ready プログラムを使用して RSA SecurID 認証をサポートするように設定済みです。 RSA Authentication Agent ソフトウェアはユーザ（またはユーザのグループ）からのアクセス要求（ローカルとリモートを問わない

）を代行受信し、認証用に RSA Authentication Manager プログラムに送ります。

RSA Authentication Manager ソフトウェアは、RSA SecurID ソリューションの管理コンポーネントです。 認証要求を検証し、企業ネットワーク向けの認証ポリシーを一元管理するために使用されます。 RSA SecurID オーセンティケータおよび RSA Authentication Agent ソフトウェアと連携して動作します。

このドキュメントでは、エージェント ソフトウェアをインストールすることにより、Cisco ACS サーバを RSA Authentication Agent として使用します。 WLC はネットワーク アクセス サーバ（NAS）（AAA クライアント）であり、次に、クライアント認証を ACS に転送します。 このドキュメントでは、保護拡張認証プロトコル（PEAP）のクライアント認証を使用して概念および設定を説明します。

PEAP の認証については、「Cisco の保護拡張認証プロトコル」を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

このドキュメントでは、次の設定を使用します。

- エージェント ホスト設定
- 認証エージェントの設定

エージェント ホスト設定

RADIUS サーバとしての Cisco Secure ACS の使用方法

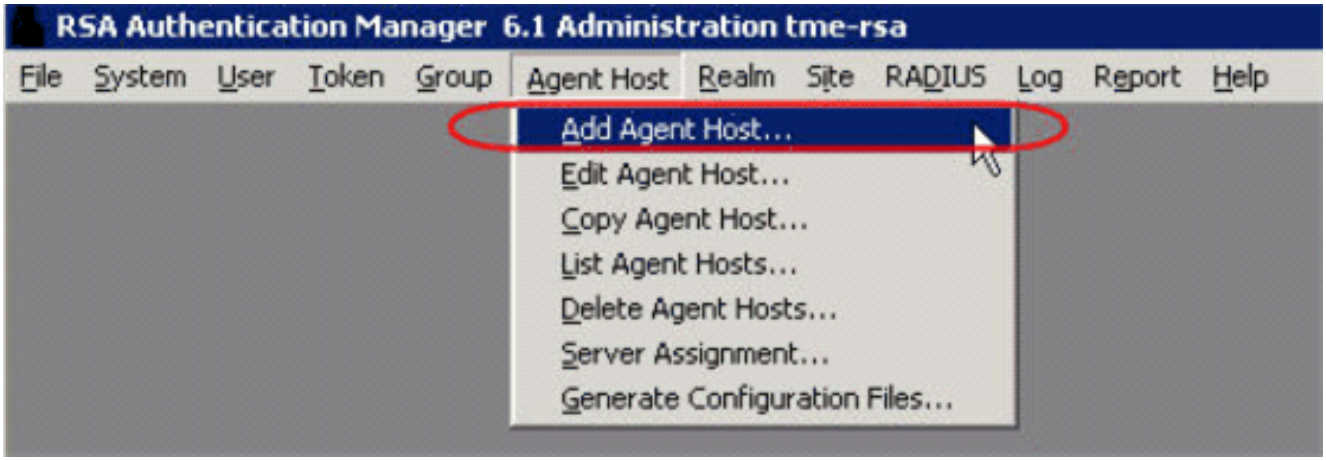
Cisco Secure ACS と RSA Authentication Manager や RSA SecurID アプライアンス間の通信を容易にするためには、RSA Authentication Manager のデータベースにエージェント ホスト レコードを追加する必要があります。 エージェント ホスト レコードでは、データベース内の Cisco Secure ACS を識別し、通信および暗号化に関する情報を格納しています。

エージェント ホスト レコードを作成するには、次の情報が必要です。

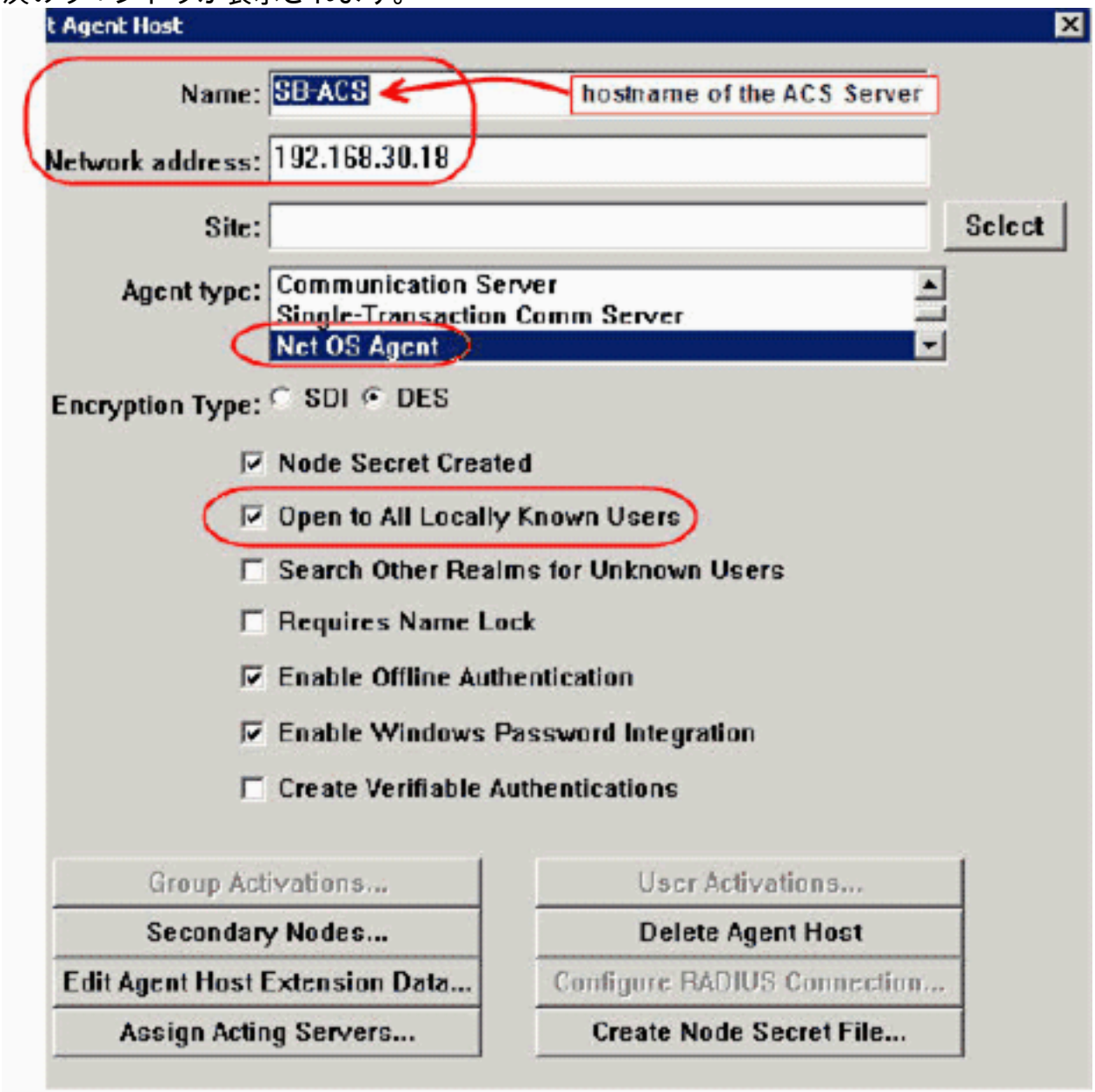
- Cisco ACS サーバのホスト名
- Cisco ACS サーバのすべてのネットワーク インターフェイスの IP アドレス

次の手順を実行します。

1. RSA Authentication Manager のホスト モード アプリケーションを開きます。
2. [Agent Host] > [Add Agent Host] の順に選択します。



次のウィンドウが表示されます。



3. Cisco ACS サーバ名およびネットワーク アドレスの適切な情報を入力します。 エージェント タイプで [NetOS] を選択し、[Open to All Locally Known Users] チェックボックスをオンにします。
4. [OK] をクリックします。

RSA Authentication Manager 6.1 RADIUS サーバの使用方法

Cisco WLC と RSA Authentication Manager の間の通信を容易にするためには、RSA Authentication Manager のデータベースおよび RADIUS サーバ データベースにエージェント ホスト レコードを追加する必要があります。 エージェント ホスト レコードでは、データベース内の Cisco WLC を識別し、通信および暗号化に関する情報を格納しています。

エージェント ホスト レコードを作成するには、次の情報が必要です。

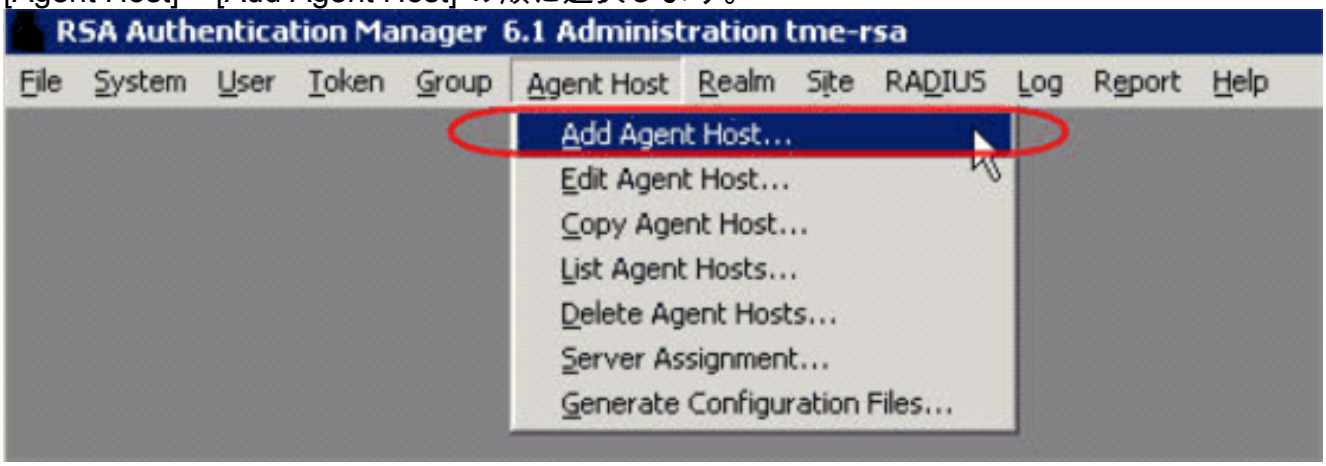
- WLC のホスト名
- WLC の管理 IP アドレス
- Cisco WLC での RADIUS のシークレットと一致する必要がある RADIUS のシークレット

エージェント ホスト レコードを追加するとき、WLC のロールは、通信サーバとして設定されます。 この設定は、RSA Authentication Manager によって、WLC との通信方法を指定するために使用されます。

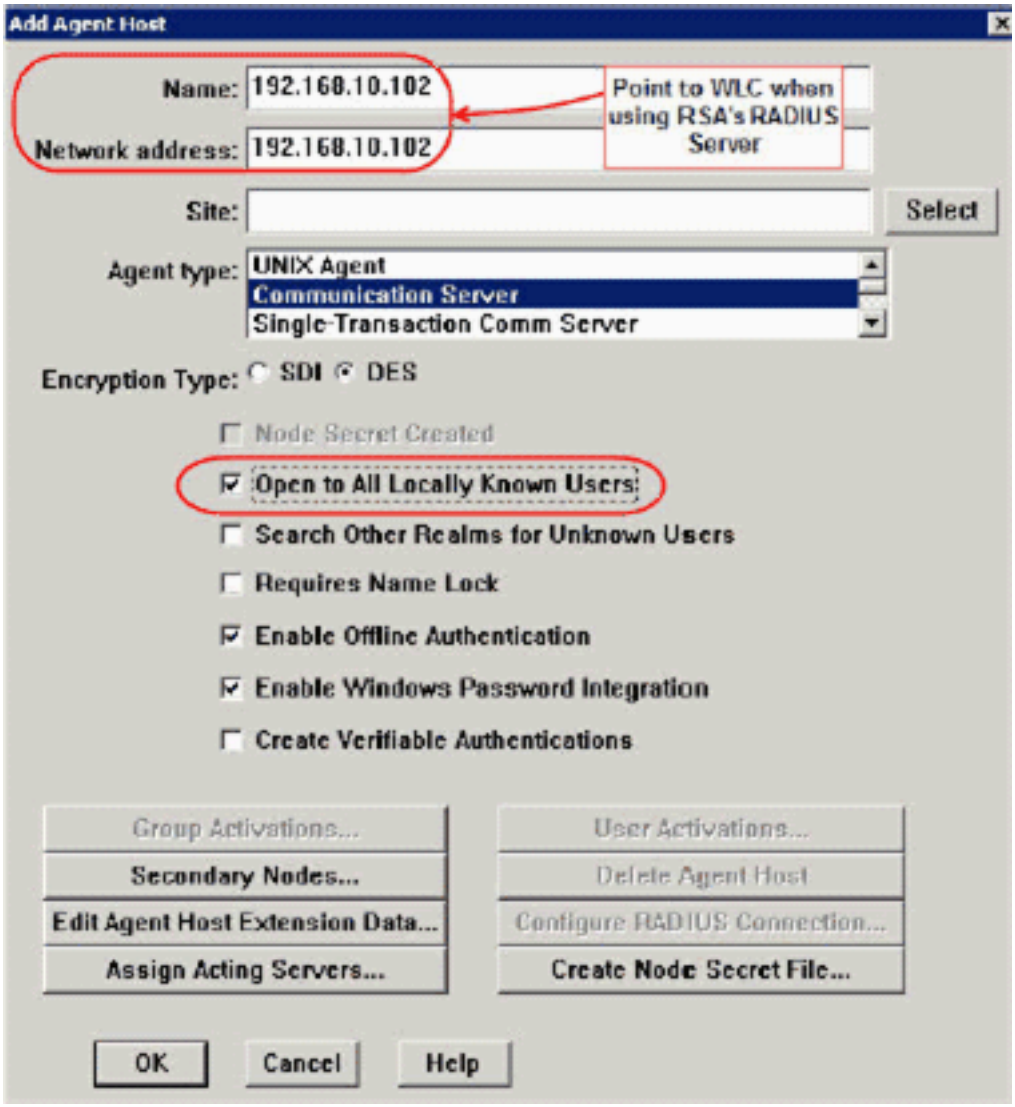
注: RSA Authentication Manager と RSA SecurID のアプライアンス内のホスト名は、ローカル ネットワークの有効な IP アドレスに解決される必要があります。

次の手順を実行します。

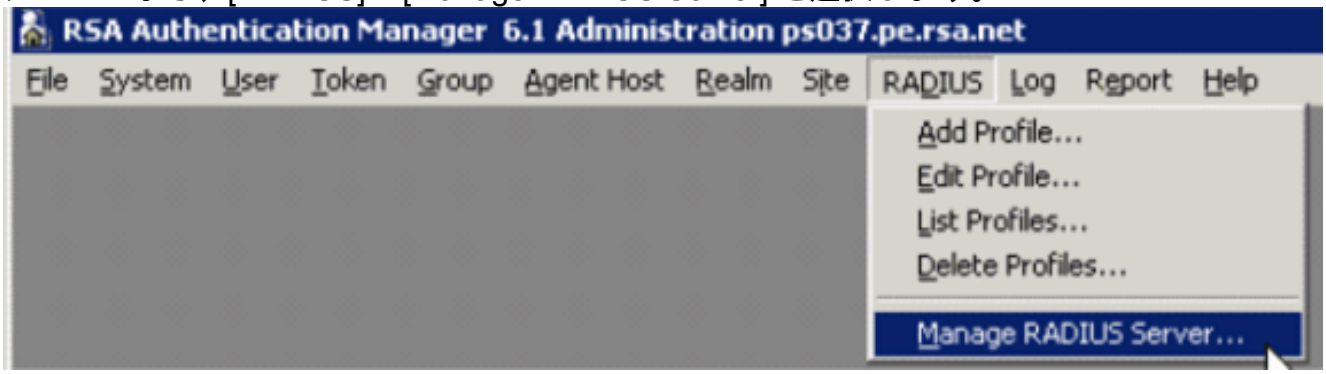
1. RSA Authentication Manager のホスト モード アプリケーションを開きます。
2. [Agent Host] > [Add Agent Host] の順に選択します。



次のウィンドウが表示されます。

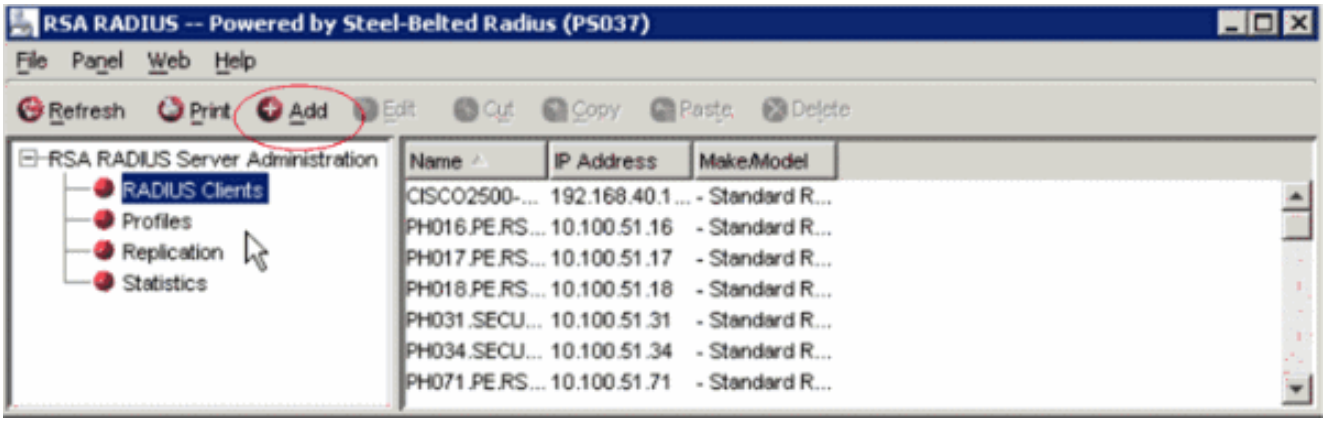


3. WLC のホスト名（必要な場合、解決可能な FQDN）とネットワーク アドレスの適切な情報を入力します。 エージェント タイプで [Communication Server] を選択し、[Open to All Locally Known Users] チェックボックスをオンにします。
4. [OK] をクリックします。
5. メニューから、[RADIUS] > [Manage RADIUS Server] を選択します。

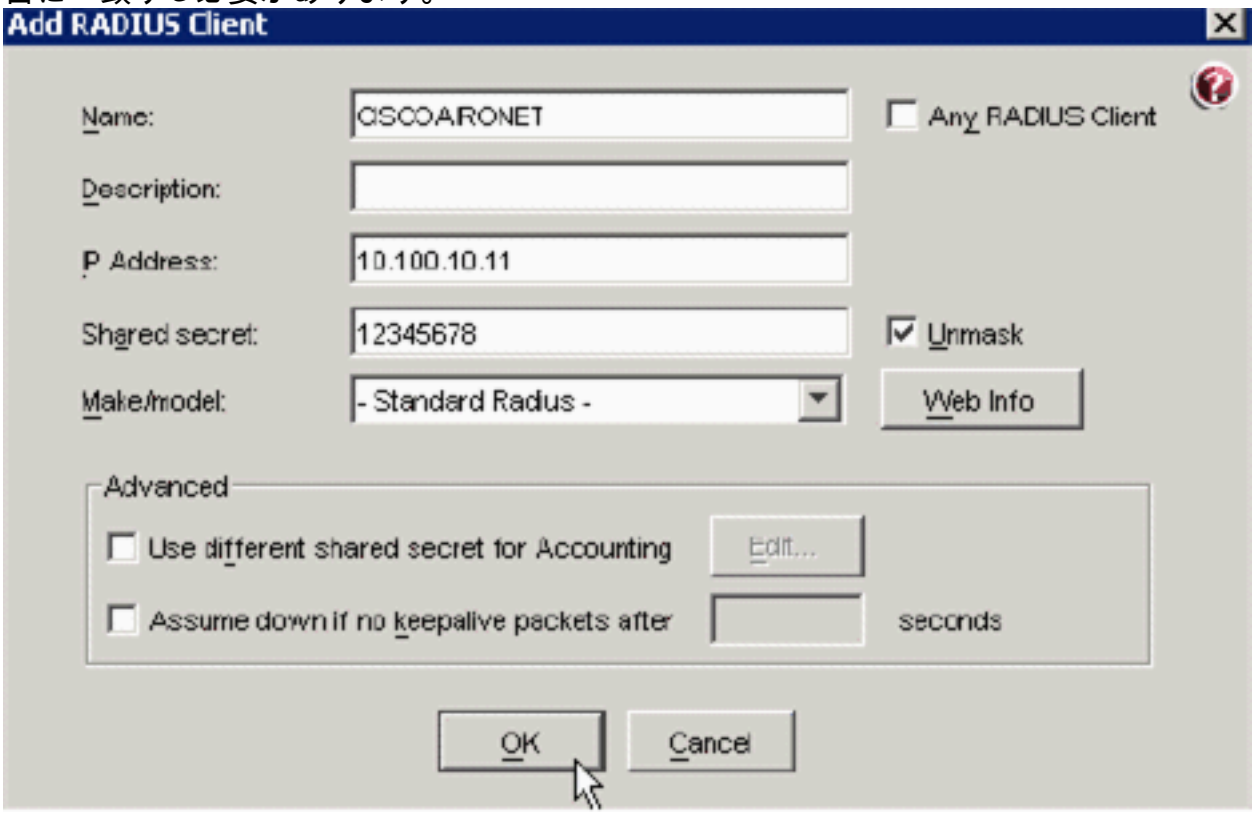


新しい管理ウィンドウが開きます。

6. このウィンドウで、[RADIUS Clients] を選択し、[Add] をクリックします。



7. Cisco WLC の適切な情報を入力します。 共有秘密は、Cisco WLC に定義されている共有秘密に一致する必要があります。



8. [OK] をクリックします。

認証エージェントの設定

次の表は、ACS の RSA Authentication Agent 機能を表しています。

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

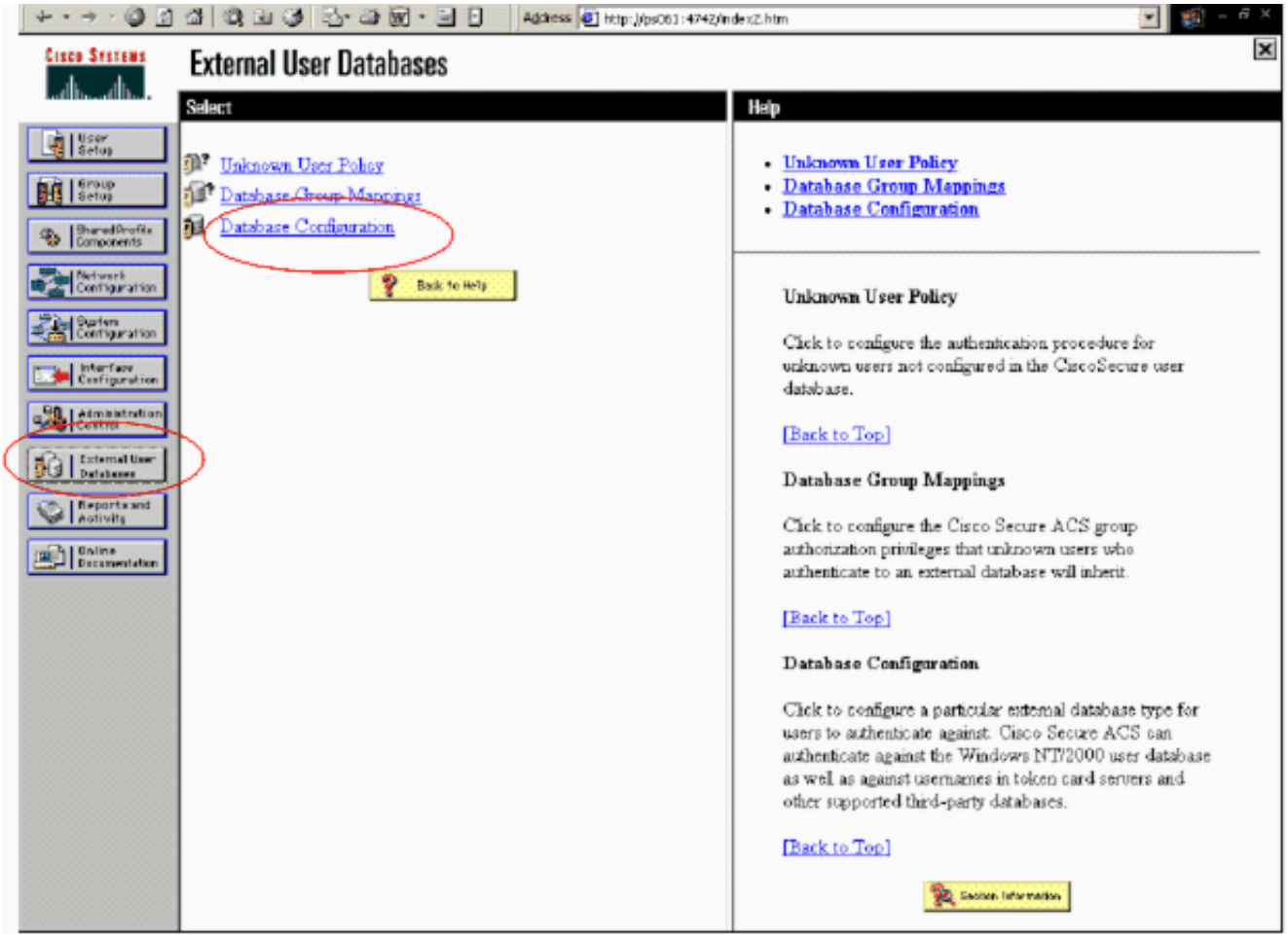
注: これが使用される RADIUS サーバである場合、RADIUS サーバの設定方法については、RSA Authentication Manager に付属している RADIUS のマニュアルを参照してください。

Cisco ACS の設定

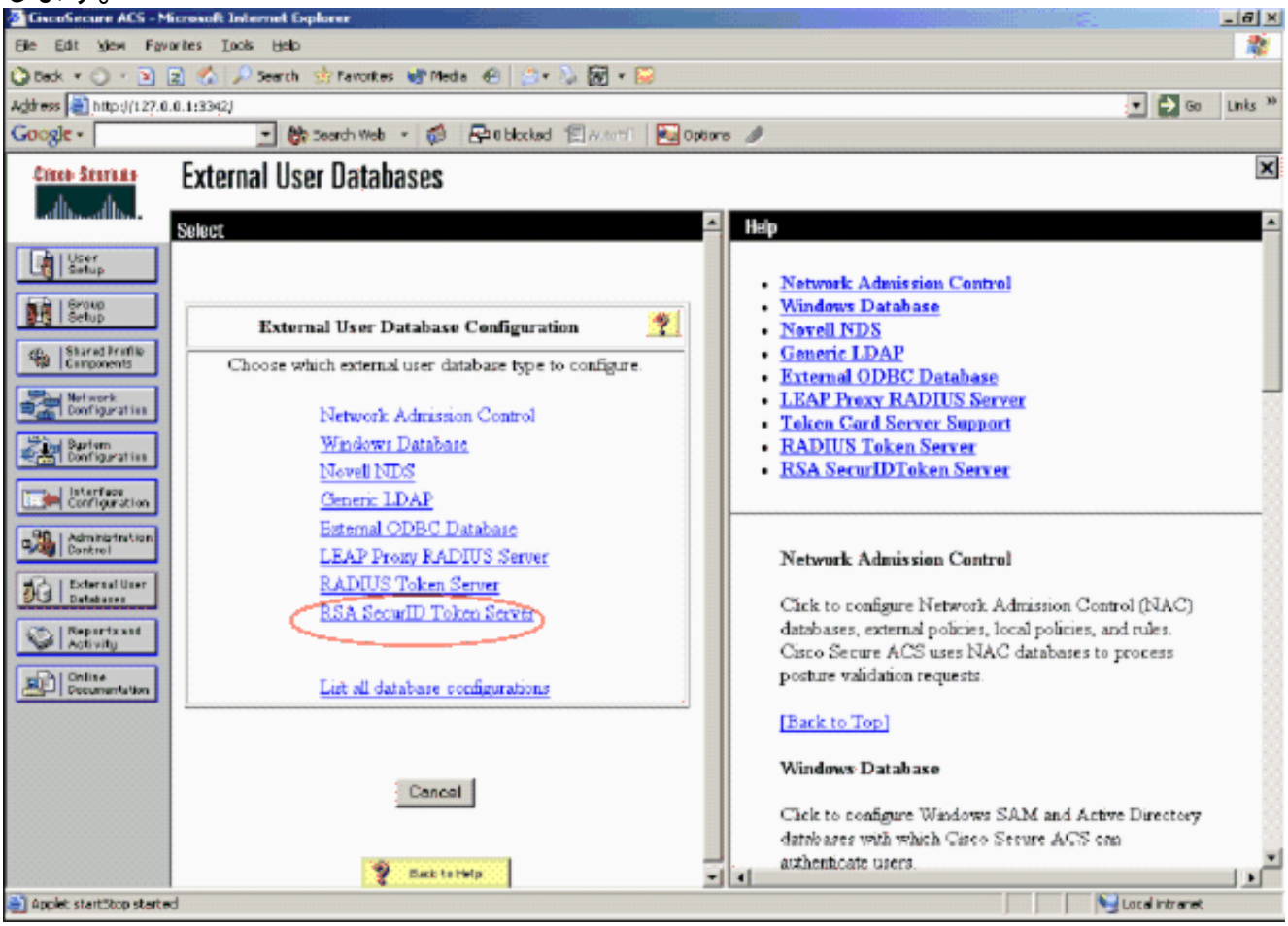
RSA SecurID Authentication のアクティブ化

Cisco Secure ACS では、ユーザの RSA SecurID 認証をサポートしています。 Certificate Manager 6.1 を使用してユーザを認証するように Cisco Secure ACS を設定するには、次の手順を実行してください。

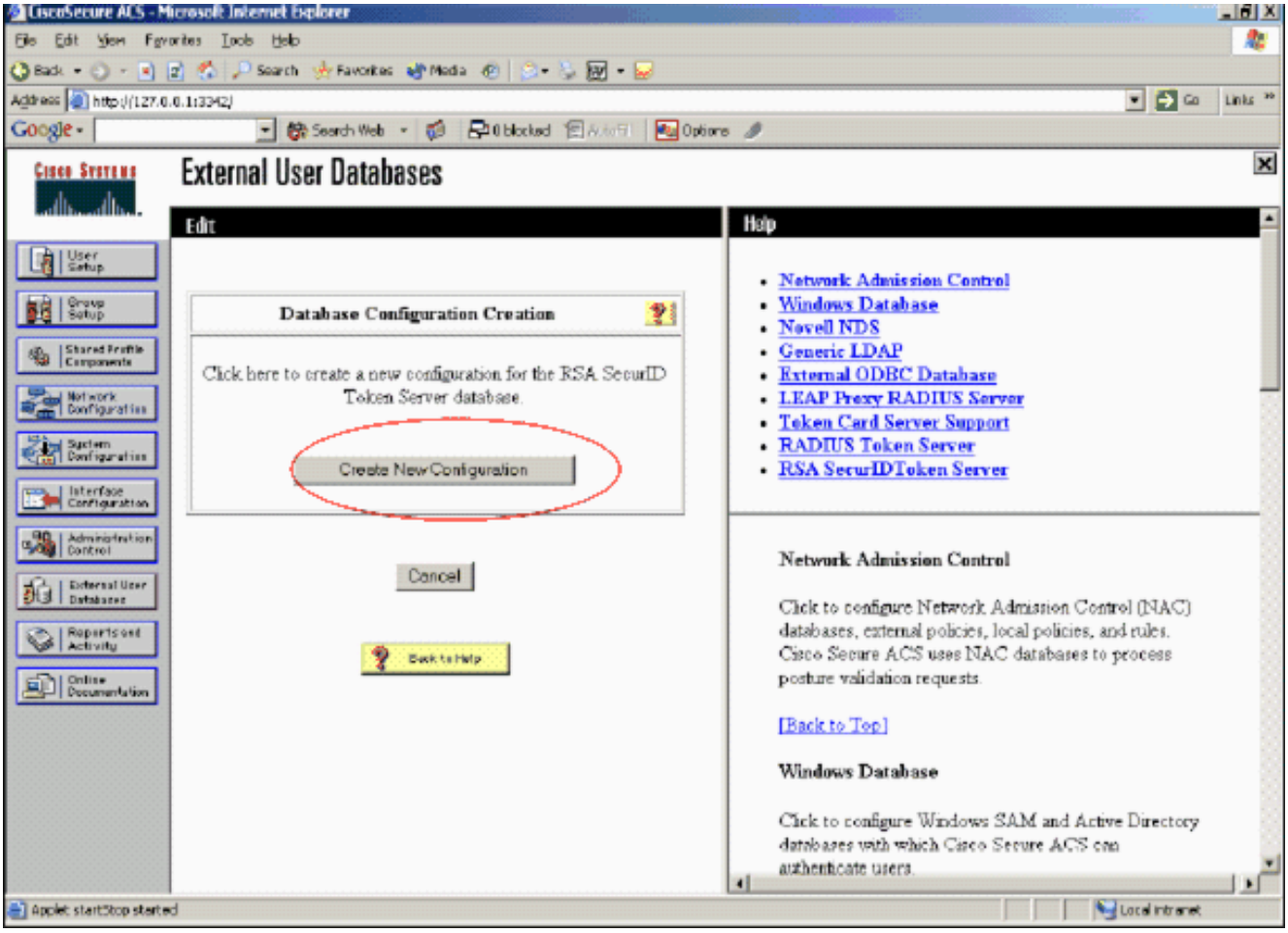
1. Cisco Secure ACS サーバと同じシステムに Windows 用の RSA Authentication Agent 5.6 以降をインストールします。
2. Authentication Agent のテスト認証機能を実行して接続を確認します。
3. RSA サーバ c:\Program Files\RSA **セキュリティ\ RSA 認証マネージャ\ prog ディレクトリ**から ACS サーバの c:\WINNT\system32 **ディレクトリ**に aceclnt.dll ファイルをコピーして下さい。
4. ナビゲーション バーで [External User Database] をクリックします。 次に、[External Database] ページで [Database Configuration] をクリックします。



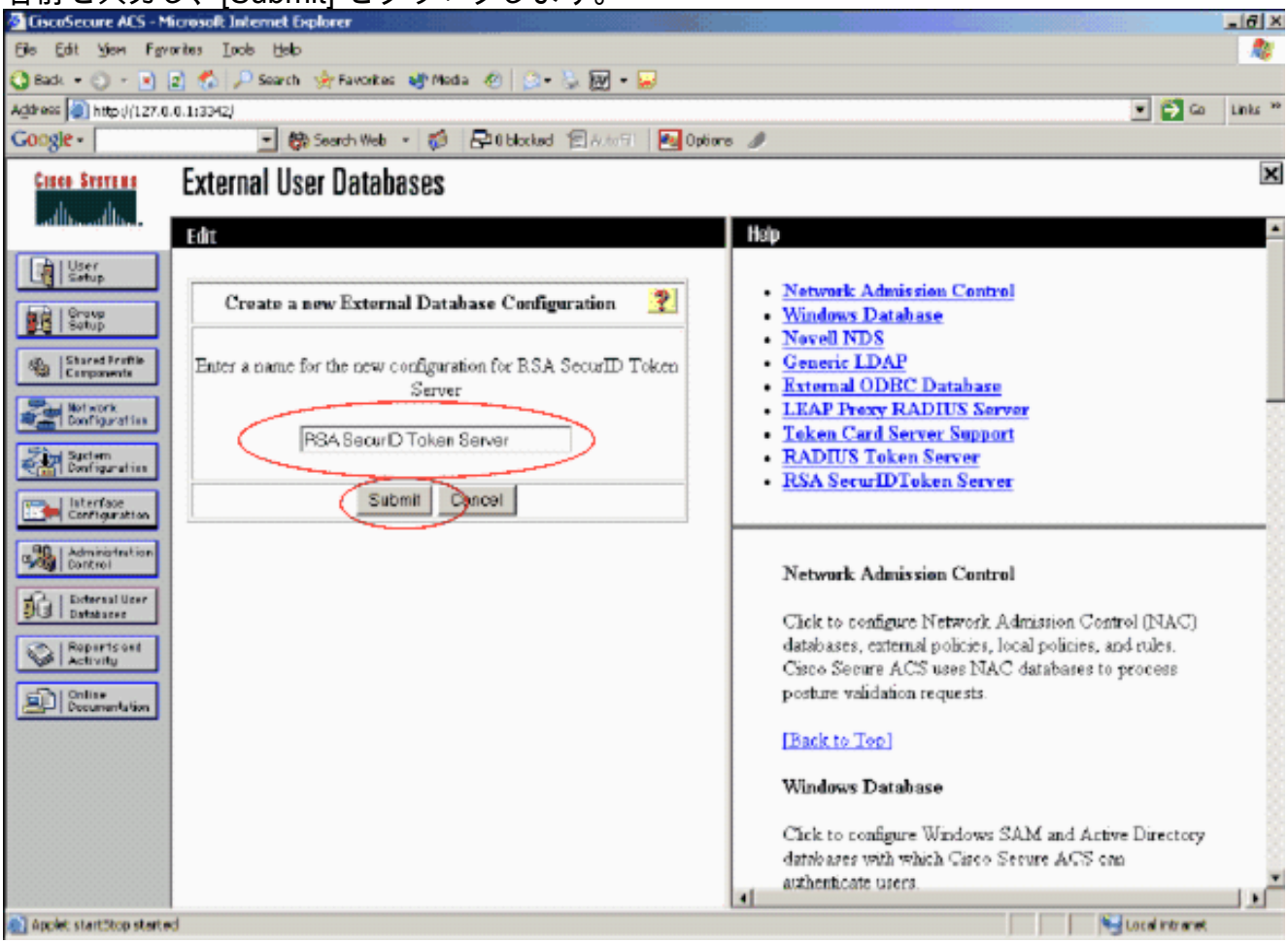
5. [External User Database Configuration] ページで、[RSA SecurID Token Server] をクリックします。



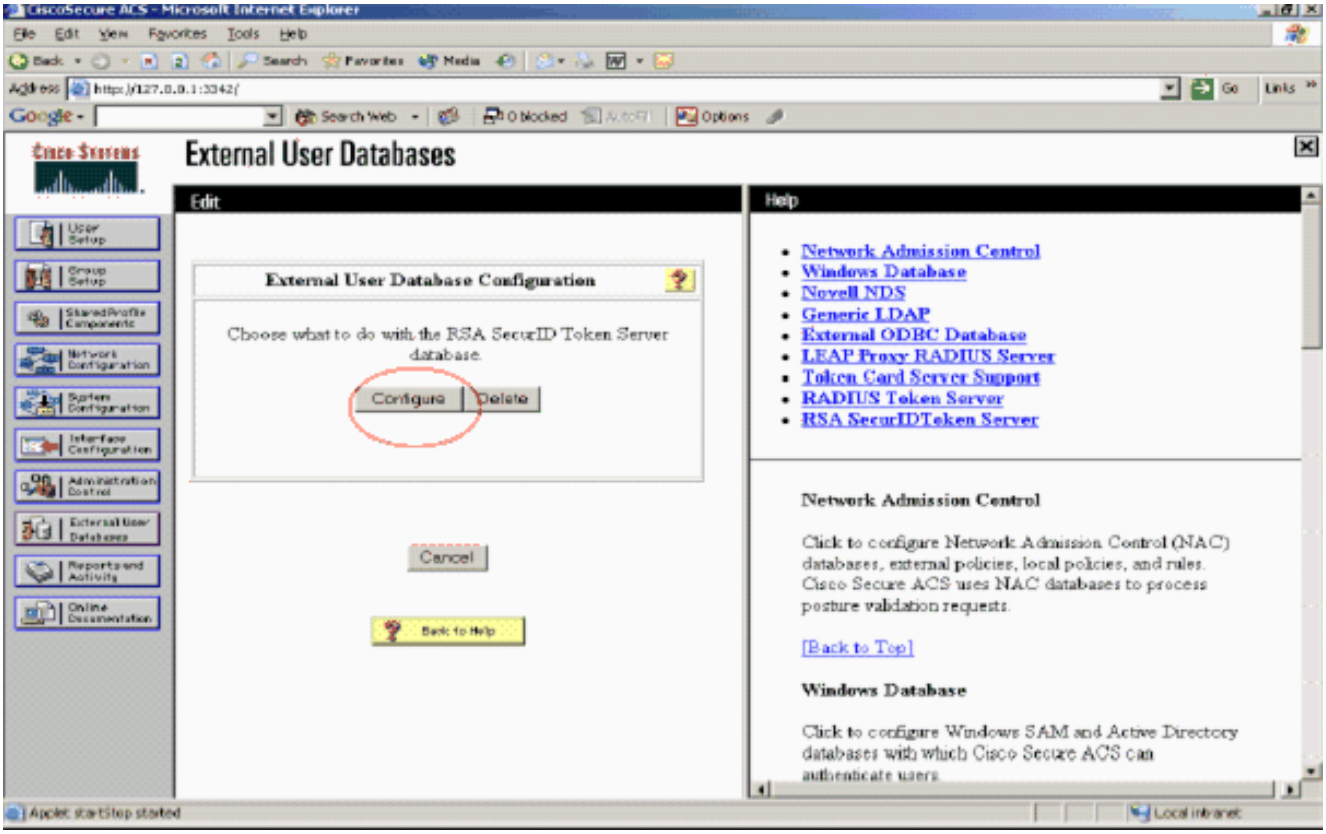
6. [Create New Configuration] をクリックします。



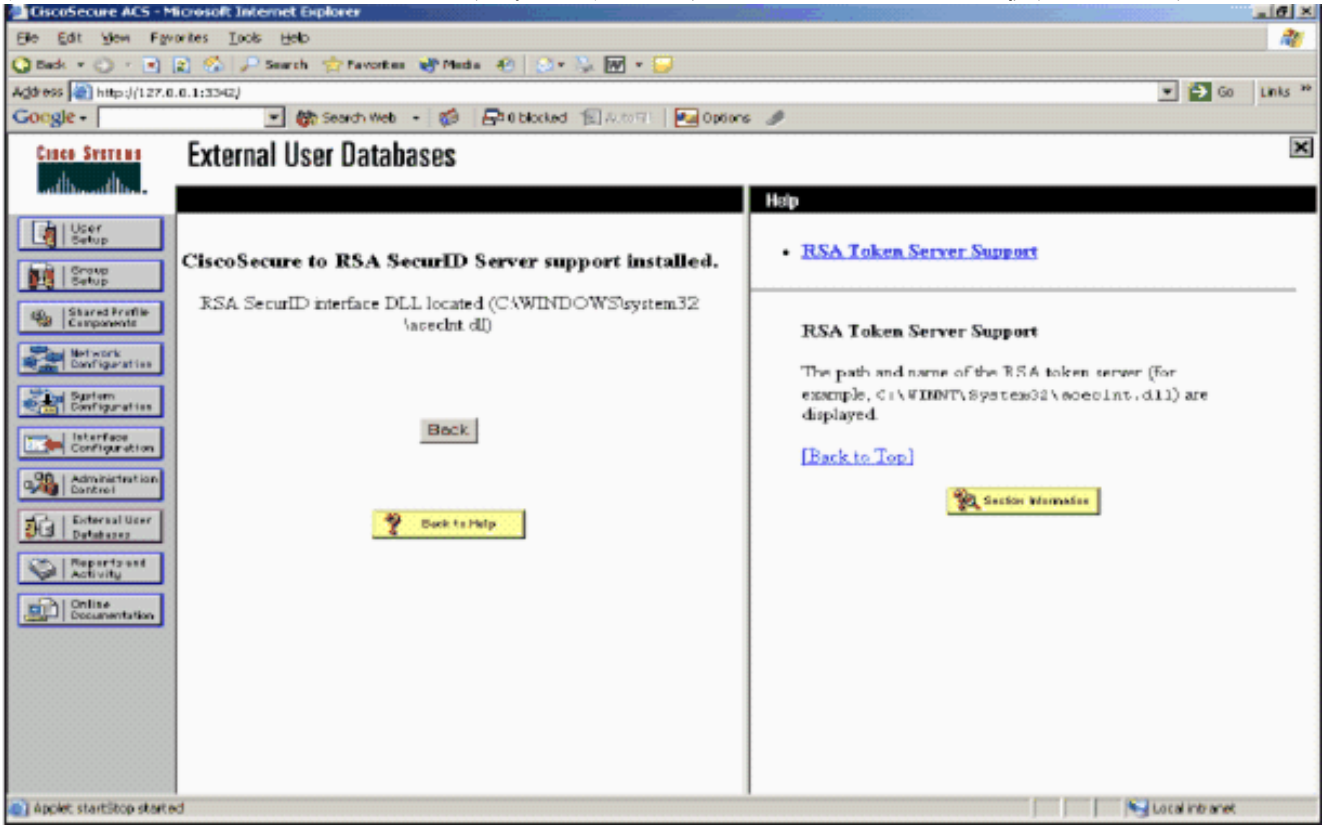
7. 名前を入力し、[Submit] をクリックします。



8. [Configure] をクリックします。



Cisco Secure ACS は、トークン サーバの名前およびオーセンティケータ DLL のパスを表示します。 この情報は、Cisco Secure ACS が RSA Authentication Agent に接続できることを確認します。 RSA SecurID 外部ユーザ データベースを Unknown User Policy に追加するか、特定のユーザ アカウントを割り当てて、このデータベースを認証に使用できます。

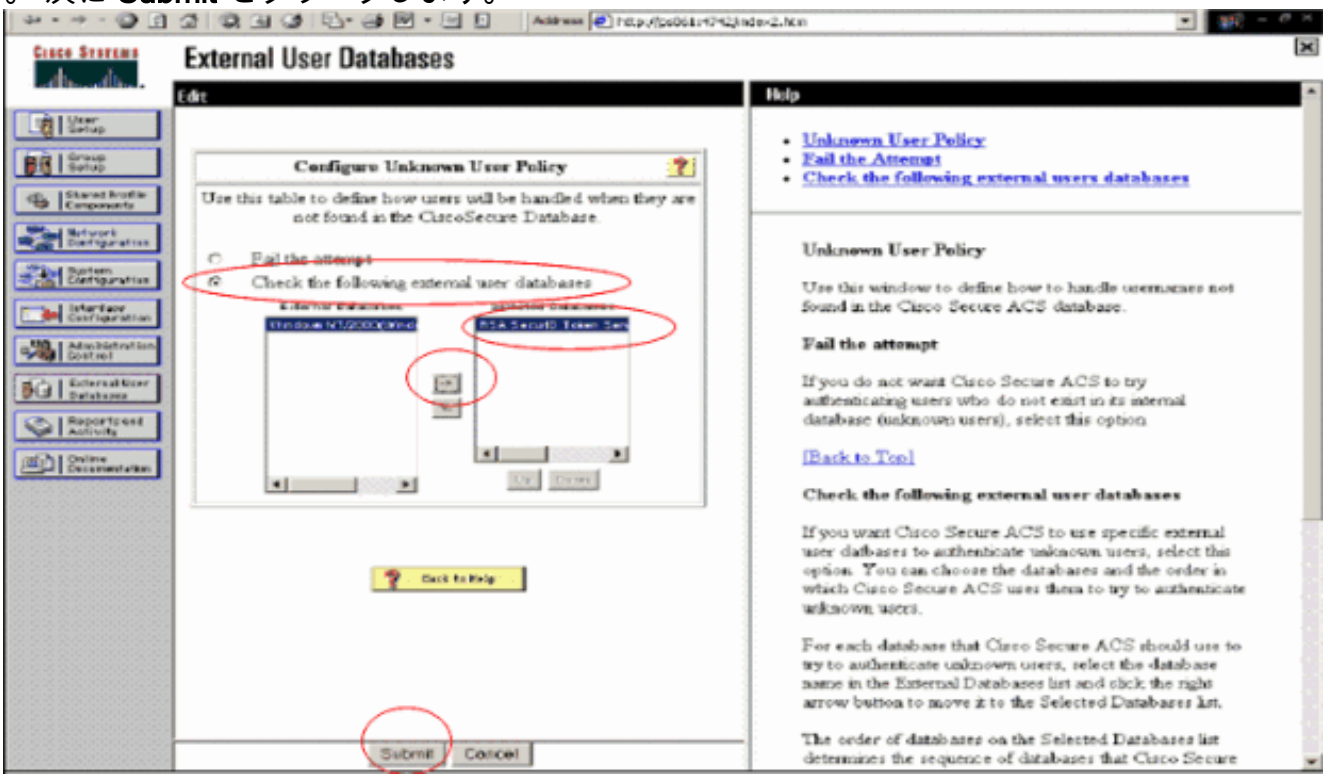


Unknown User Policy に対する RSA SecurID 認証の追加/設定

次の手順を実行します。

1. ACS のナビゲーション バーで、[External User Database] > [Unknown User Policy] をクリックします。

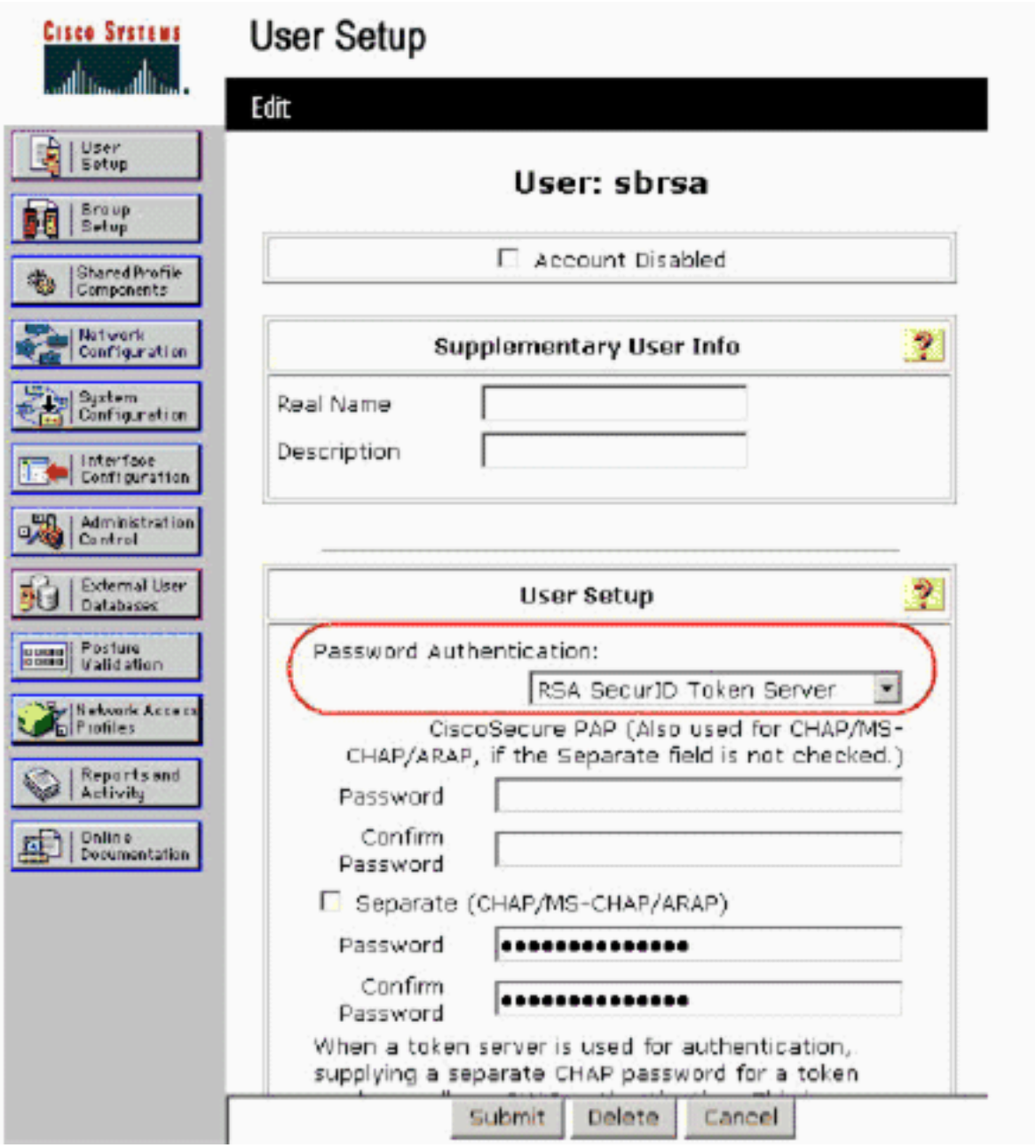
2. [Unknown User Policy] ページで、[Check the following external user databases を選択し、[RSA SecurID Token Server] を強調表示にし、[Selected Databases] ボックスに移動します。 次に **Submit** をクリックします。



特定のユーザ アカウントに対する RSA SecurID 認証の追加/設定

次の手順を実行します。

1. メイン ACS Admin GUI から [User Setup] をクリックします。 ユーザ名を入力し、[Add] をクリックします（または、変更する既存のユーザを選択）。
2. [User Setup] > [Password Authentication] の下で、[RSA SecurID Token Server] を選択します。 次に **Submit** をクリックします。

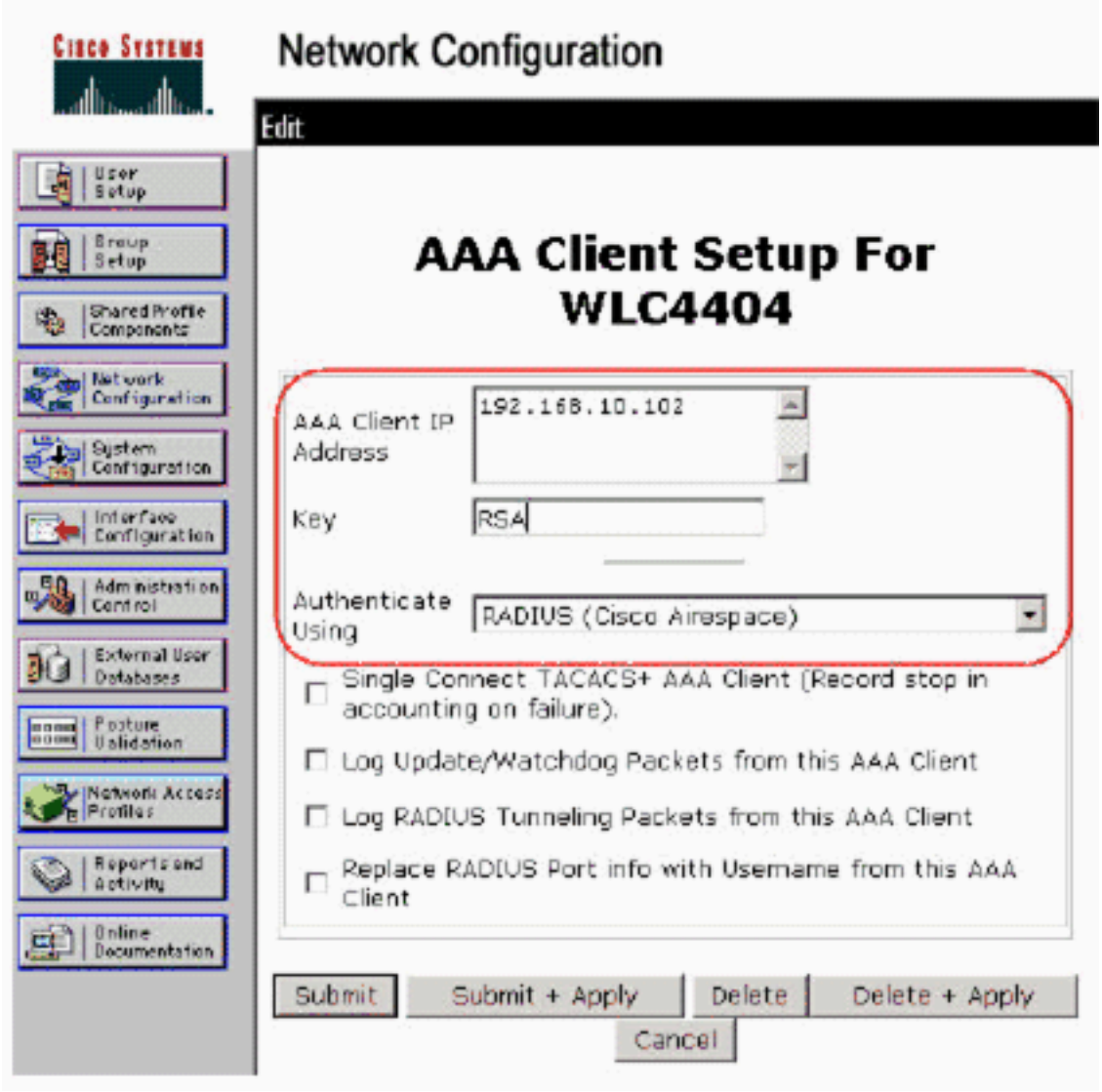


Cisco ACS での RADIUS クライアントの追加

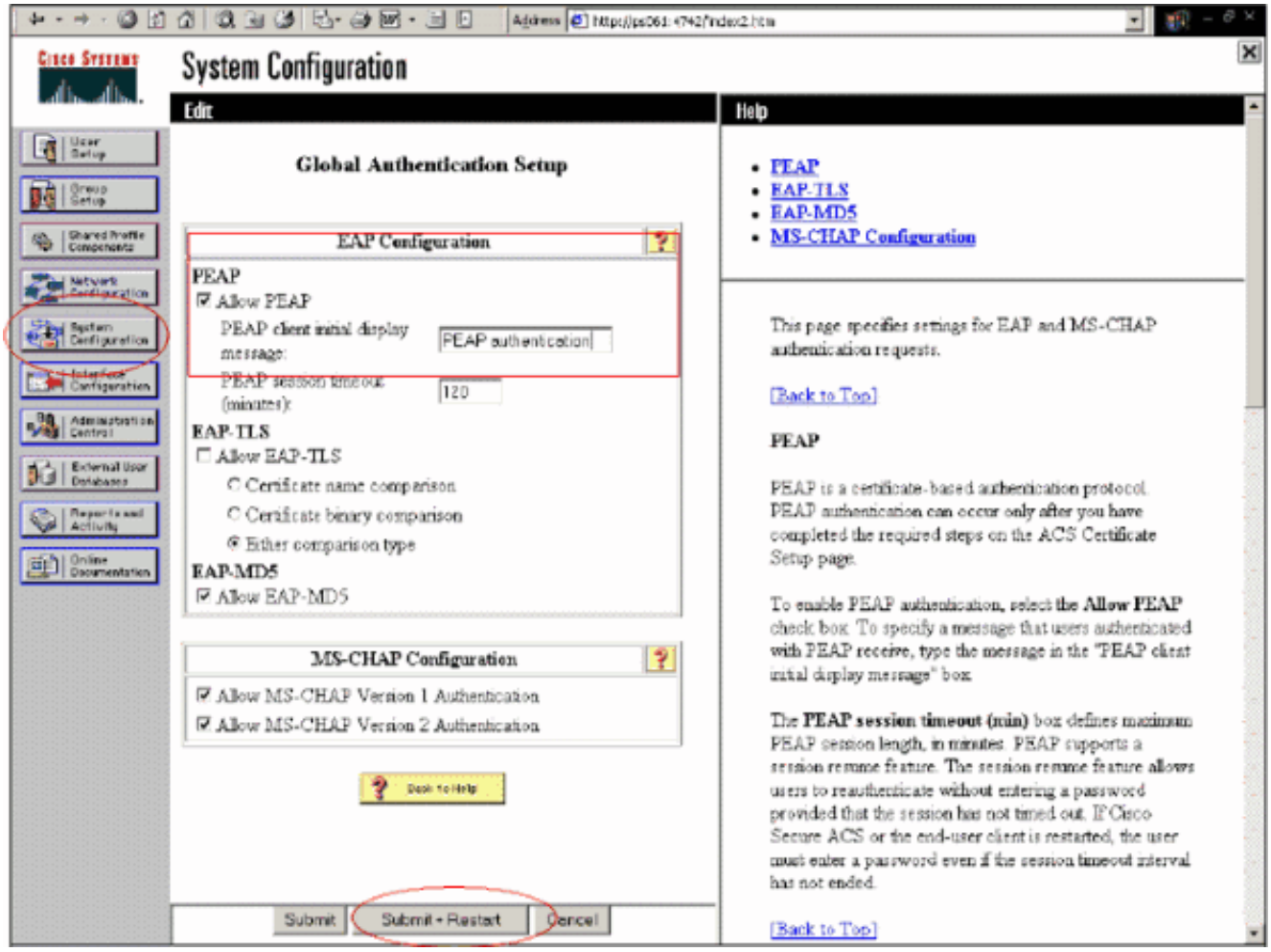
Cisco ACS サーバ インストールでは、ACS に PEAP クライアントの認証を転送するために、NAS として動作する WLC の IP アドレスが必要になります。

次の手順を実行します。

1. [Network Configuration] の下で、使用する WLC の AAA クライアントを追加または編集します。 AAA のクライアントと ACS の間で使用される「共有秘密」鍵を入力します（WLC に共通）。 この AAA クライアントに対して [Authenticate Using] > [RADIUS (Cisco Airespace)] を選択します。 次に [Submit + Apply] をクリックします。



2. RSA Keon 認証局など既知の信頼できる認証局からサーバ証明書を適用し、インストールします。このプロセスの詳細については、Cisco ACS に付属しているドキュメントを参照してください。 RSA Certificate Manager を使用して、追加のヘルプのために RSA Keon Aironet 実装ガイドを参照できます。 続行する前に、次の作業を正常に完了する必要があります。
   注: 自己署名証明書も使用できます。 これらの使用方法については Cisco Secure ACS のドキュメントを参照してください。
3. [System Configuration] > [Global Authentication Setup] の下で、[Allow PEAP authentication] のチェックボックスをオンにします。



802.1x 用 Cisco ワイヤレス LAN コントローラ コンフィギュレーションの設定

次の手順を実行します。

1. Cisco Secure ACS サーバに接続できるように設定するために、コントローラを設定するには、WLC のコマンドライン インターフェイスに接続します。
2. 認証用に RADIUS サーバを設定するために WLC から **config radius auth ip-address** コマンドを入力します。**注:** RSA Authentication Manager の RADIUS サーバによってテストする場合は、RSA Authentication Manager の RADIUS サーバの IP アドレスを入力します。 Cisco ACS サーバでテストする場合は、Cisco Secure ACS サーバの IP アドレスを入力します。
3. 認証用の UDP のポートを指定するには WLC から **config radius auth port** コマンドを入力します。 ポート 1645 または 1812 は、RSA Authentication Manager および Cisco ACS サーバの両方で、デフォルトでアクティブです。
4. WLC 上に共有秘密を設定するには WLC から **config radius auth secret** コマンドを入力します。 これは、この RADIUS クライアント用に RADIUS サーバに作成された共有秘密に一致する必要があります。
5. 認証をイネーブルにするために WLC から **config radius auth enable** コマンドを入力します。 望ましい場合は、**config radius auth disable** コマンドを入力して認証をディセーブルにします。 認証はデフォルトでディセーブルになっていることに注意してください。
6. WLC で、必要な WLAN に適切なレイヤ 2 セキュリティ オプションを選択します。
7. RADIUS 設定が正しく設定されていることを確認するには、**show radius auth statistics** コマンドおよび **show radius summary** コマンドを使用します。**注:** EAP 要求タイムアウトのデフォルト タイマーは小さく、変更する必要がある場合があります。 これは、**config advanced eap request-timeout <seconds>** コマンドを使用して実行できます。 要件に基づいて ID 要求

のタイムアウトを調整するために役立つ場合もあります。 これは、**config advanced eap identity-request-timeout <seconds>** コマンドを使用して実行できます。

802.11 ワイヤレス クライアントの設定

ワイヤレス ハードウェアおよびクライアントのサプリカントを設定する方法の詳細な説明は、さまざまな Cisco のドキュメントを参照してください。

既知の問題

次に、RSA の SecureID 認証で既知の問題の一部を示します。

- RSA のソフトウェア トークン。 XP2 でこの認証方式を使用するときは、新しい Pin モードと Tokencode の次のモードはサポートされません。 （ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip の結果修正）
- ACS の実装が古いか、上記のパッチがない場合、クライアントはユーザが「Enabled; New PIN Mode」から「Enabled」に遷移するまで認証できません。 ユーザにワイヤレス以外の認証を行わせるか、「テスト認証」RSA アプリケーションを使用することによって、これを実現できます。
- 4 文字または英数字の PIN が拒否されます。 新しい Pin のモードのユーザが PIN ポリシーに違反すると、認証プロセスが失敗し、ユーザには理由も経緯もわかりません。 通常ユーザがポリシーに違反すると、PIN が拒否されたことを示すメッセージが送信され、PIN のポリシーの内容をユーザに再表示しながら、再入力が促されます（PIN のポリシーが 5 ~ 7 桁の場合にユーザが 4 桁を入力など）。

関連情報

- ACS と Active Directory グループのマッピングに基づく WLC を使用したダイナミック VLAN 割り当ての設定例
- WLC を使用したワイヤレス LAN 上のクライアント VPN の設定例
- ワイヤレス LAN コントローラでの認証の設定例
- ワイヤレス LAN コントローラおよび外部 RADIUS サーバを使用する EAP-FAST 認証の設定例
- SDM による固定 ISR のワイヤレス認証種別の設定例
- 固定 ISR のワイヤレス認証種別の設定例
- Cisco 保護拡張認証プロトコル
- RADIUS サーバとの EAP 認証
- テクニカルサポートとドキュメント - Cisco Systems