Identify-Based Networking Systems 設定ガイド

バージョン 1.0 2005 年 12 月

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Identity-Based Networking Systems の概要

概要

完全なネットワーク セキュリティの必要性が、これまでにないほど高まっています。しかし、それは十分に理解されておらず、悪意あるユーザによって情報が盗用、操作、および阻害されようとしています。さまざまなソリューションによって境界の防御がなされていますが、内部ネットワーク境界内には、情報の盗用と未許可のアクセスという最大の脅威が存続しています。

1 つの問題点として、企業ネットワークへの物理的および論理的アクセスが比較的容易であるという点が挙げられます。物理的および論理的アクセスの拡張により、モビリティのレベルが向上し、業務の運用効率および全体的な生産性が向上しました。しかし、このモビリティのレベルの向上と、セキュリティ ソリューションの制限により、ネットワークが外部にさらされるリスクも高まっています。

このマニュアルでは、ネットワーク管理者が ID ベースのネットワーク アクセス制御を確実に実装し、それをネットワーク エッジのユーザおよび個別のアクセス ポートにまで展開できる技術標準に基づいたフレームワークとシステムについて説明します。このシステムは、安全かつ信頼性があることで知られている強力な認証テクノロジーを使用して、ユーザまたはデバイス（あるいはその両方）を認識します。ユーザまたはデバイスの ID は、ネットワーク アクセス権の付与または拒否、ネットワーク パラメータの設定、およびその他のセキュリティ機能（状態の評価など）の操作を行うポリシーにマッピングすることによりさらに活用できます。

この設定ガイドでは、IEEE 802.1X を使用した ID ベース ネットワーキング システムの基本的な展開に重点を置いて説明します。シスコシステムズの Identity-Based Networking System がネットワークに提供するサービスと機能は、次のとおりです。

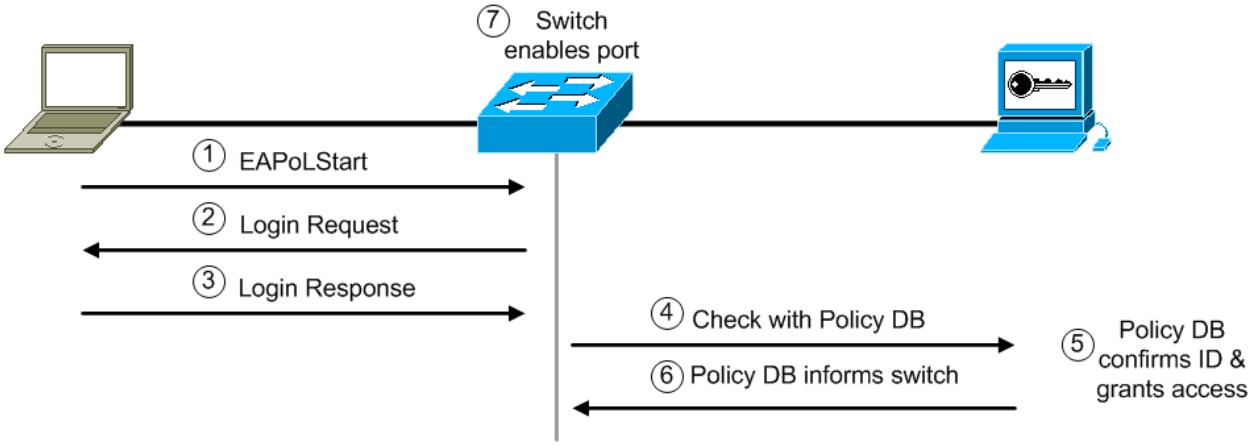
- ユーザまたはデバイス（あるいはその両方）の認証
- 管理者が設定した定義済みのポリシー セットへのネットワーク エンティティ ID のマッピング
- 設定済みの認証ポリシーに基づく、ポート レベルでのネットワーク アクセス権の付与または拒否
- アクセス権が付与された場合のリソース アクセスなど、その他のポリシーの実施

これらの機能は、シスコのエンドツーエンド システムが、Cisco Catalyst スイッチ製品ファミリ、ワイヤレス LAN アクセス ポイントおよびコントローラ、および CiscoSecure Access Control Server（ACS）とともに実装されたときに導入されます。システムの追加コンポーネントには、Windows XP、オプションの X.509 Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）認証アーキテクチャなど、IEEE 802.1X に適合したクライアント オペレーティング システムがあります。また、シスコのエンドツーエンド インフラストラクチャで展開する場合、Cisco IP Phone も、IEEE 802.1X に基づく ID ベース ネットワーキング システムと相互に運用可能です。

Cisco Catalyst スイッチは、IEEE 802.1X 標準に適合しているため、基本的なポートベースのネットワーク アクセス制御を実行できます。エンド デバイスで IEEE 802.1X に適合したクライアント ソフトウェアが設定されると、IEEE 802.1X 機能を実行する Cisco Catalyst スイッチは、バックエンドの CiscoSecure ACS サーバと連動して、要求元のユーザまたはシステムを認証します。

図 1-1 の高度なメッセージ交換は、ID ベースのシステム内でポートベースのアクセス制御がどのように機能するかを示しています。まず、ノート型パソコンなどのクライアントが IEEE 802.1X 対応のネットワークに接続し、LAN スイッチに開始メッセージを送信します。開始メッセージを受信すると、LAN スイッチはクライアントにログイン要求を送信し、クライアントはログイン応答を返します。スイッチは応答をポリシー データベースに転送し、ポリシー データベースはユーザを認証します。ユーザ ID が確認されると、ポリシー データベースはユーザのネットワーク アクセスを許可して、LAN スイッチに通知します。次に、LAN スイッチはクライアントに接続されたポートを有効化します。

図 1-1　　ポートベースのアクセス制御



ユーザまたはデバイスの証明書および参照情報は、CiscoSecure ACS によって処理されます。CiscoSecure ACS は、次のいずれかの方法で、ユーザまたはデバイスのポリシー プロファイル情報を参照できます。

- 統合されたユーザ データベースを内部的に使用
- Microsoft Active Directory、LDAP、Novell NDS、または Oracle データベースなどのデータベース ソースを外部的に使用

これにより、システムを既存のユーザ管理構造およびスキームに統合でき、展開全体が簡素化されます。

IEEE 802.1X の概要

IEEE 802.1X などのプロトコルの開発では、既存のプロトコルを使用してネットワーク デバイスおよびコンポーネントの通信を可能にすると同時に、ネットワーク管理者がネットワーク アクセス制御およびポリシーを柔軟に管理できるようにします。ネットワークに接続されたエンティティの ID を、対応する制御ポリシーに関連付けることで、これまでにない安全性と柔軟性が実現します。また、適切な設計と展開により、ネットワーク管理者は、セキュリティとネットワーク セグメントおよびリソースへのアクセス制御を向上させることができます。

IEEE 802.1X は、PPP（ポイントツーポイント プロトコル）または IEEE 802 メディアを使用して、メディアアクセス制御レイヤで Extensible Authentication Protocol（EAP）を伝送するためのカプセル化定義を提供するプロトコル標準です。IEEE 802.1X を使用すると、ポートベースのネットワーク アクセス制御をネットワーク デバイスに実装できます。IEEE 802.1X は、サプリカントとオーセンティケータの間で EAP メッセージを伝送します。次に、オーセンティケータは RADIUS プロトコルを介して EAP 情報を認証サーバに送信します。IEEE 802.1X は、ユーザまたはマシンの ID に基づいてネットワーク接続を許可または拒否する機能を提供するだけでなく、上位層プロトコルと連携して、ネットワーク ポリシーも実施します。

ここでは、IEEE 802.1X コンポーネントについて詳しく説明します。

IEEE 802.1X の主要なコンポーネント

サプリカント

サプリカントは、LAN およびスイッチ サービスへのアクセスを要求し、オーセンティケータ（スイッチ）からの要求に応答するデバイス（ワークステーション、ノート型パソコンなど）です。デバイスでは、Microsoft Windows XP オペレーティング システムで提供されるソフトウェアなど、IEEE 802.1X に適合したクライアント ソフトウェアが実行されている必要があります。

クライアントは、IEEE 802.1X 仕様では*サプリカント*です。

オーセンティケータ

オーセンティケータは、クライアントの認証ステータスに基づいて、ネットワークへの物理的なアクセスを制御するデバイス（Cisco Catalyst スイッチなど）です。通常、オーセンティケータは、クライアントと認証サーバ間の媒介（プロキシ）として機能します。オーセンティケータは、EAP を介してクライアントから ID 情報を要求し、RADIUS を介して認証サーバでその情報を確認したあと、認証サーバからの応答に基づいて、応答をクライアントに送信します。

スイッチが EAP over LAN（EAPOL）フレームを受信して、認証サーバに送信すると、イーサネット ヘッダーおよび EAP フレームは RADIUS 形式に再度カプセル化されます。EAP フレームは、カプセル化の間は変更または検査されません。認証サーバは、ネイティブのフレーム形式で EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、RADIUS ヘッダーが削除され、EAP フレームが残ります。このフレームは、IEEE 802.1X 形式にカプセル化されたあと、クライアントに送信されます。

認証サーバ

認証サーバは、クライアントの実際の認証を実行します。認証サーバは、クライアントの ID を確認し、クライアントが LAN およびスイッチ サービスへのアクセスを許可されたかどうかをスイッチに通知します。スイッチはプロキシとして機能するため、認証サーバはクライアントに対して透過的です。サポートされている認証サーバは、EAP 拡張機能を装備した RADIUS セキュリティ システムのみです。RADIUS は、RADIUS サーバと 1 つ以上の RADIUS クライアント間で安全な認証情報が交換されるクライアント / サーバ モデルを使用します。

EAP の方式

IEEE 802.1X は、複数の EAP 方式をサポートし、ID ベースのネットワーク アクセス制御を提供します。ここでは、4 つの EAP 方式を定義し、次の章でその設定方法について説明します。4 つの方式は、次のとおりです。

- EAP-Message Digest 5（MD5）
- EAP-Transport Level Security（EAP-TLS）
- Protected EAP（PEAP）
- EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）

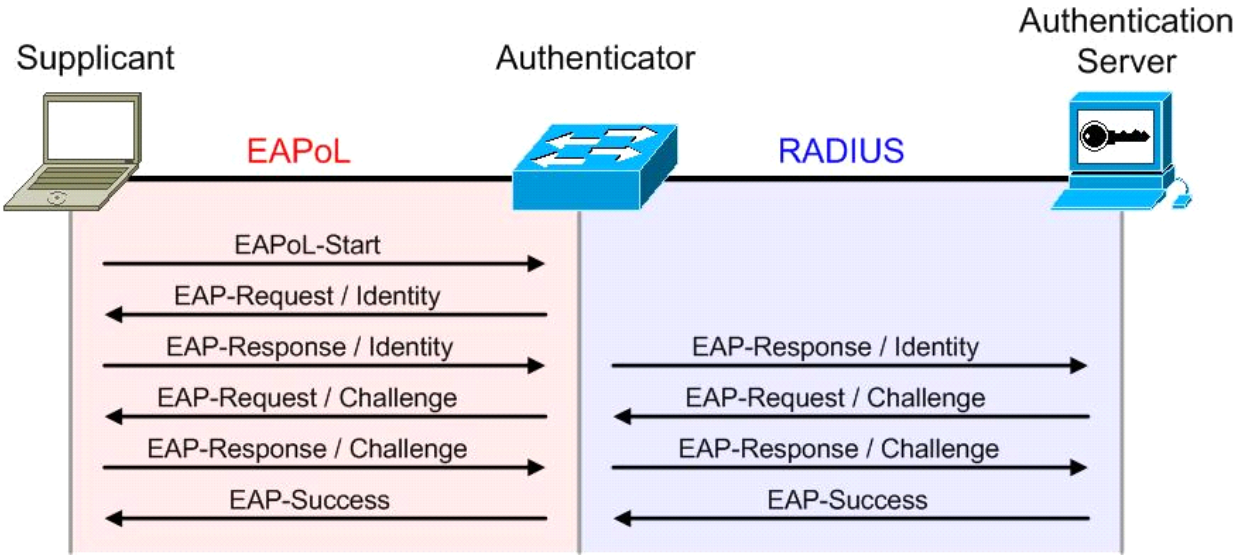
EAP-MD5

EAP-MD5 は、一般的な標準の EAP タイプで、RFC 1994（CHAP）および RFC 2284（EAP）に基づいています。ハッシュ アルゴリズムとして MD5 が指定されているため、EAP メッセージ内の MD5 チャレンジは、PPP CHAP プロトコルに似ています。MD5 のサポートは RFC 3748 に含まれているため、EAP の展開はすべて MD5 チャレンジ メカニズムをサポートする必要があります。

EAP-MD5 は、展開が最も簡単な EAP の 1 つですが、安全性が低く、他の EAP 方式に比べて、オフライン ディクショナリ攻撃などの影響を受けやすくなっています。

図 1-2 に、サプリカント、オーセンティケータ、および認証サーバ間の EAP-MD5 メッセージ交換を示します。まず、IEEE 802.1X サプリカントを実行するクライアントがネットワークに接続し、EAPoL-Start メッセージをオーセンティケータに送信します。オーセンティケータは EAP Identity 要求をサプリカントに送信し、サプリカントは EAP Identity 応答を返します。オーセンティケータは、RADIUS を介して認証サーバに応答を転送します。認証サーバは EAP-MD5 チャレンジをサプリカントに送信し、サプリカントは応答を返します。認証サーバはユーザ ID を確認し、ユーザのネットワーク アクセスを許可するようにオーセンティケータに指示します。次に、オーセンティケータはサプリカントに接続されたポートを有効化します。

図 1-2　　EAP-MD5 メッセージ交換



EAP-TLS

EAP-TLS は Microsoft Corporation によって開発された方式で、PPP の拡張機能として EAP を使用できるようにして、PPP および TLS 内で認証を実行し、整合性が保護された暗号スイート ネゴシエーションと鍵交換を提供します。EAP-TLS は RFC 2716 で定義され、X.509 PKI 証明書で認証された IEEE 802.1X ポートベースのアクセス制御を使用し、特に EAP-MD5 などのその他の EAP プロトコルの脆弱性に対処できるようになっています。ただし、これらの脆弱性に対処する場合、サーバだけでなくクライアントも相互認証のための証明書を必要とするため、展開が複雑になります。

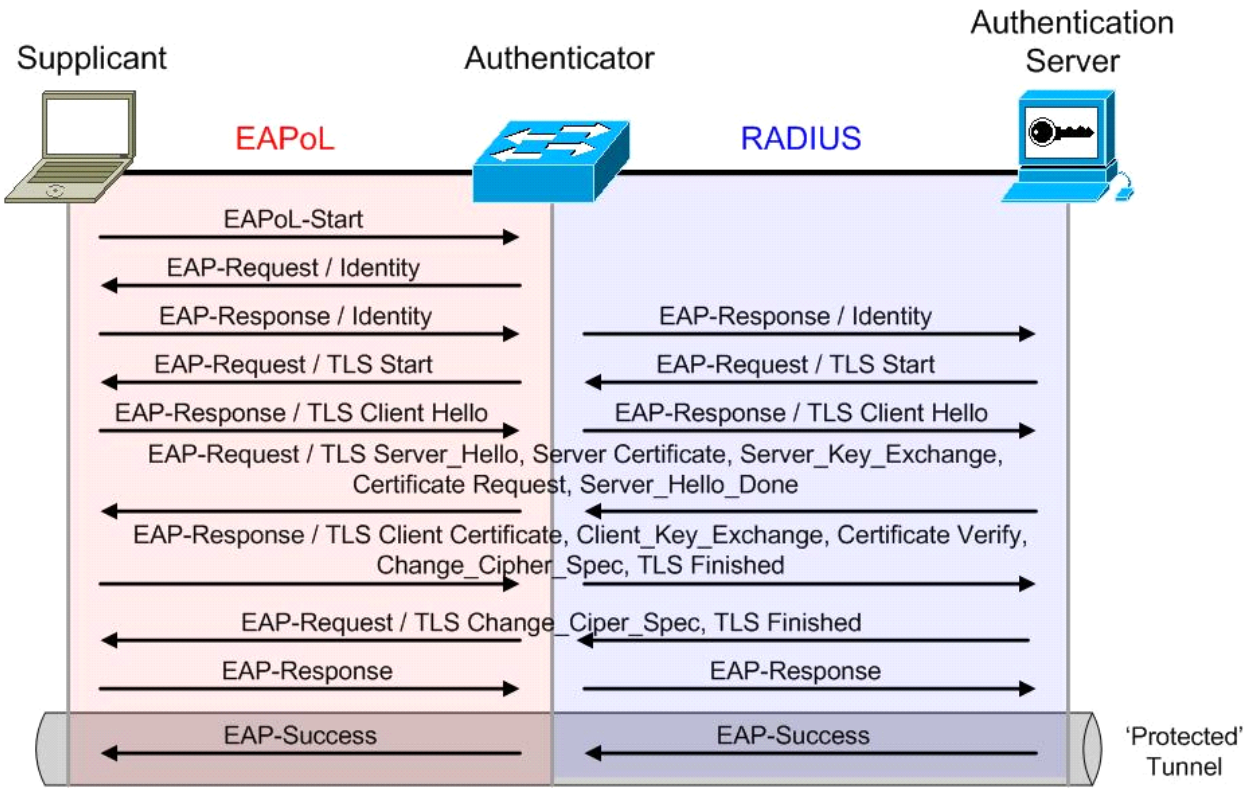
EAP-TLS の利点は、次のとおりです。

- パケット単位の機密性および整合性保護により、ユーザ ID を保護する機能
- 鍵交換のための標準化されたメカニズム
- フラグメンテーションおよび再アセンブリの組み込みのサポート
- 認識された成功 / 失敗の表示のサポート

IEEE 802.1X では、メッセージの EAP-TLS 交換により、サプリカントと認証サーバ間の相互認証、暗号化方式のネゴシエーション、および暗号鍵の決定が行われます。

図 1-3 に、サプリカント、オーセンティケータ、および認証サーバ間の EAP-TLS メッセージ交換を示します。まず、IEEE 802.1X サプリカントを実行するクライアントがネットワークに接続し、EAPoL-Start メッセージをオーセンティケータに送信します。オーセンティケータは EAP Identity 要求をサプリカントに送信し、サプリカントは EAP Identity 応答を返します。オーセンティケータは、RADIUS を介して認証サーバに応答を転送します。認証サーバは EAP-TLS Start メッセージをサプリカントに送信し、サプリカントは EAP-TLS Client Hello で応答します。認証サーバは X.509 PKI 証明書をサプリカントに送信し、サプリカントに証明書の送信を要求します。サプリカントは認証サーバの公開鍵を使用して証明書を確認し、証明書を更新された暗号スイートとともに認証サーバに送信します。認証サーバはサプリカントの証明書を確認して、ユーザの ID を認証し、暗号スイートを確認します。TLS トンネルが確立されると、認証サーバは、ユーザのネットワーク アクセスを許可するようにオーセンティケータに指示します。次に、オーセンティケータはサプリカントに接続されたポートを有効化します。

図 1-3　EAP-TLS メッセージ交換



PEAP（EAP-MSCHAPv2）

PEAP は、シスコシステムズ、Microsoft Corporation、および RSA Security Inc. によって開発されました。PEAP は、TLS を使用して暗号化され、整合性が保護された安全なチャネルを作成することで、セキュリティの問題に対処する EAP タイプです。実質的にすべての EAP タイプ（EAP-MSCHAPv2 など）との新しい EAP ネゴシエーションを行い、クライアントのネットワーク アクセス試行を認証します。TLS チャネルは、通常はオフライン ディクショナリ攻撃の影響を受けやすいパスワードベースの認証プロトコルを認証に使用し、ネットワーク アクセス試行に対する EAP ネゴシエーションおよび認証を保護します。また、PEAP 内で実行される EAP 方式には TLS 内の EAP メッセージがラップされ、鍵交換、セッション再開、フラグメンテーション、および再アセンブリのサポートが組み込まれます。さらに、PEAP により、証明書がなくても LAN クライアントを認証できるため、安全な有線 / 無線 LAN アーキテクチャの構築が容易になります。

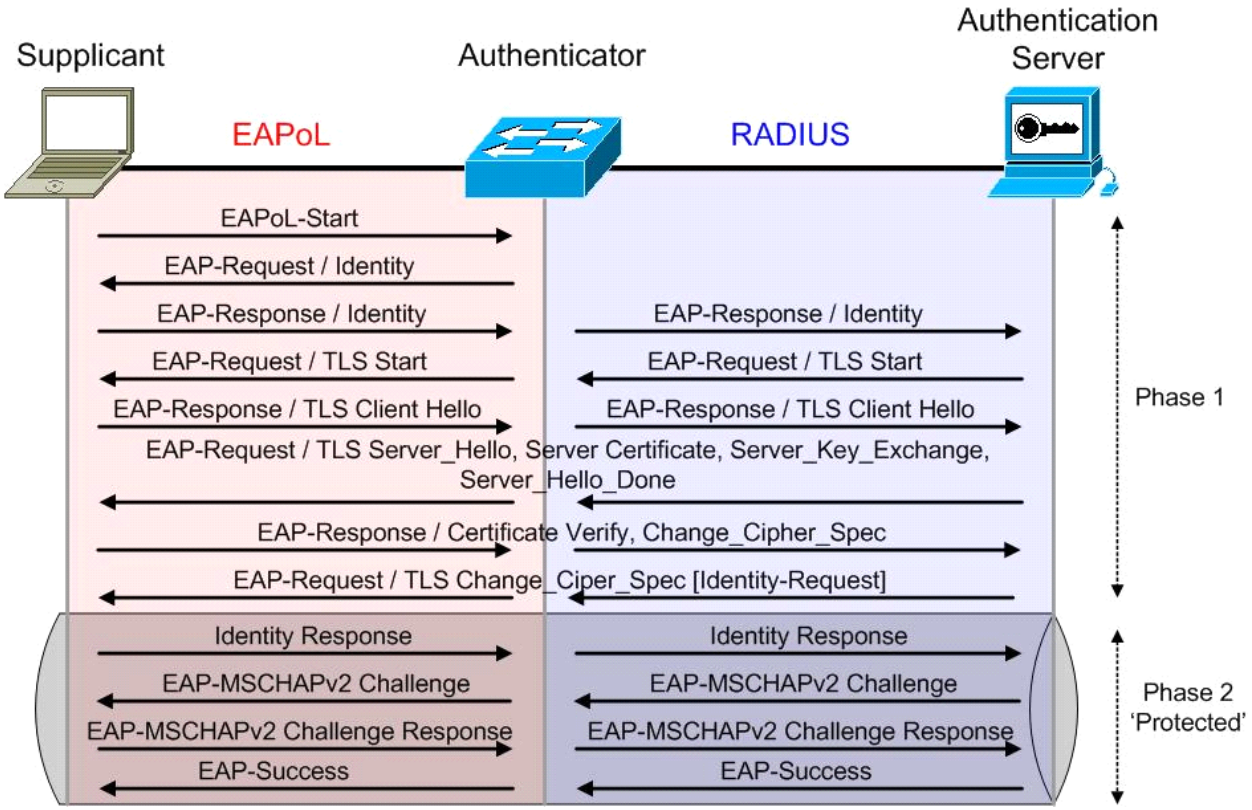
（注）　PEAP は、Windows XP Service Pack 1（SP1）、Windows XP Service Pack 2（SP2）、Windows Server 2003、および Windows 2000 Service Pack 4（SP4）でサポートされています。

MS-CHAPv2 は、MD4 および DES を使用して応答を暗号化する、パスワードベースのチャレンジ応答による相互認証プロトコルです。オーセンティケータはサプリカントにチャレンジを送信し、サプリカントは認証サーバにチャレンジを送信します。いずれかのチャレンジに対して正しく応答が返されなかった場合、接続が拒否されます。MS-CHAPv2 は、当初は Microsoft によって PPP 認証プロトコルとして設計され、ダイヤルアップおよび VPN 接続を保護していましたが、現在は EAP タイプとしても機能しています。MS-CHAPv2 は、以前のチャレンジ応答認証プロトコルよりも優れた保護機能を提供しますが、オフライン ディクショナリ攻撃に対しては依然として脆弱です。悪意あるユーザは、正常な MS-CHAPv2 交換をキャプチャして、正しいパスワードがわかるまでパスワードを推測する可能性があります。ただし、MS-CHAPv2 交換を PEAP と組み合わせて使用することで、TLS チャネルの強力なセキュリティによる保護が可能になります。

図 1-4 に、サプリカント、オーセンティケータ、および認証サーバ間の PEAP（MS-CHAPv2 を使用）のメッセージ交換を示します。まず、IEEE 802.1X サプリカントを実行するクライアントがネットワークに接続し、EAPoL-Start メッセージをオーセンティケータに送信します。オーセンティケータは EAP Identity 要求をサプリカントに送信し、サプリカントは EAP Identity 応答を返します。オーセンティケータは、RADIUS を介して認証サーバに応答を転送します。認証サーバは EAP-TLS Start メッセージをサプリカントに送信し、サプリカントは EAP-TLS Client Hello で応答します。認証サーバは、X.509 PKI 証明書をサプリカントに送信します。サプリカントは認証サーバの公開鍵を使用して証明書を確認し、更新された暗号スイートを送信します。認証サーバは、暗号スイートを受け入れます。TLS トンネルが確立されると、認証サーバは EAP-MSCHAPv2 チャレンジをサプリカントに送信し、サプリカントは応答を返します。

認証サーバはユーザ ID を確認し、ユーザのネットワーク アクセスを許可するようにオーセンティケータに指示します。次に、オーセンティケータはサプリカントに接続されたポートを有効化します。

図 1-4　PEAP（EAP-MSCHAPv2）のメッセージ交換



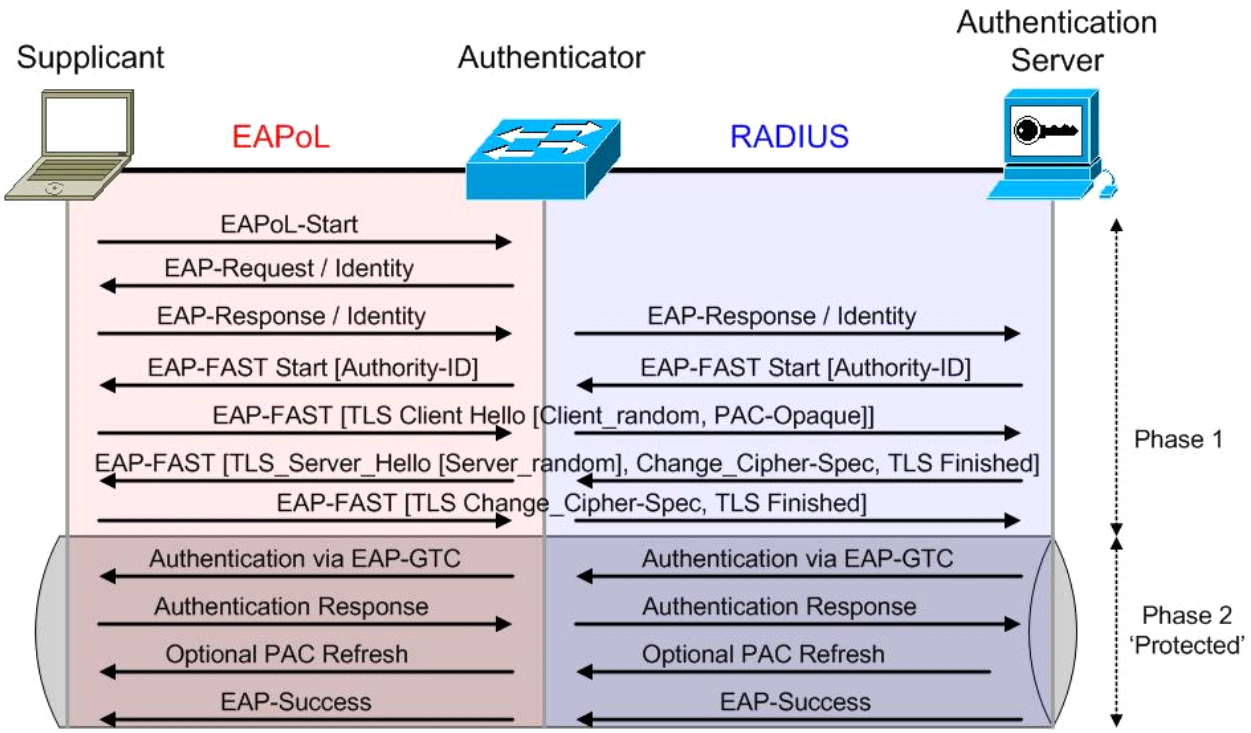
EAP-FAST

EAP-FAST はシスコシステムズによって開発され、2004 年 2 月にインターネット ドラフトとして IETF に提出されました。インターネット ドラフトは、2005 年 4 月に改訂され提出されました。EAP-FAST プロトコルは、TLS トンネル内で EAP トランザクションを暗号化するクライアント / サーバ セキュリティ アーキテクチャです。EAP-FAST は、この点では PEAP に似ていますが、EAP-FAST トンネルの確立はユーザに固有の強力な共有秘密鍵に基づいているという点が大きく異なります。この秘密は Protected Access Credential（PAC）と呼ばれ、自動（自動またはインバンド プロビジョニング）または手動（手動またはアウト オブ バンド プロビジョニング）でクライアント デバイスに配布されます。共有秘密に基づくハンドシェイクは、PKI インフラストラクチャに基づくハンドシェイクよりも本質的に高速であるため、EAP-FAST は、暗号化された EAP トランザクションを提供する 2 つのソリューションのうち、より高速のソリューションになります。

図 1-5 に、内部方式として EAP-GTC を使用するサプリカント、オーセンティケータ、および認証サーバ間の EAP-FAST メッセージ交換を示します。まず、IEEE 802.1X サプリカントを実行するクライアントがネットワークに接続し、EAPoL-Start メッセージをオーセンティケータに送信します。オーセンティケータは EAP Identity 要求をサプリカントに送信し、サプリカントは EAP Identity 応答を返します。オーセンティケータは、RADIUS を介して認証サーバに応答を転送します。認証サーバは、認証 ID を含む EAP-FAST Start メッセージをサプリカントに送信します。認証サーバが送信した認証 ID に基づいて、サプリカントは、サプリカントとサーバを相互に認証するために使用される一意の共有鍵である保存済みの Protected Access Credential（PAC）を選択します。サプリカントは、（PAC キーに基づいて）PAC opaque で認証サーバに応答を返します。認証サーバは、マスター キーを使用して PAC opaque を解読し、PAC キーを導き出します。この時点で、サプリカントとサーバの両方が同じ PAC キーを所有し、TLS トンネルを作成します。

認証サーバは EAP-GTC（Generic Token Card）要求をサプリカントに送信し、サプリカントは応答を返します。認証サーバはユーザ ID を確認し、ユーザのネットワーク アクセスを許可するようにオーセンティケータに指示します。次に、オーセンティケータはサプリカントに接続されたポートを有効化します。

図 1-5　EAP-FAST メッセージ交換



（注）　オプションとして、PAC が最初にクライアントに配布されるフェーズ 0 もあります。

シスコシステムズの製品およびソフトウェアのサポート

ここでは、基本的な ID ベース ネットワーキング システムをサポートするために必要なハードウェア プラットフォームと**最小限**必要なソフトウェア リリースについて説明します。

Cisco Catalyst シリーズ スイッチ

表 1-1　Cisco Catalyst シリーズ スイッチ

Cisco Catalyst 6500 Catalyst OS	6.2(2)
Cisco Catalyst 6500 IOS	12.1(12b)E
Cisco Catalyst 4500 Catalyst OS	6.2(1)
Cisco Catalyst 4500 IOS	12.1(12c)EW
Cisco Catalyst 4948 EMI/SMI	12.2(20)EWA
Cisco Catalyst 3750 EMI	12.1(11)AX

表 1-1　Cisco Catalyst シリーズ スイッチ（続き）

Cisco Catalyst 3750 SMI	12.1(11)AX
Cisco Catalyst 3560EMI	12.1(19)EA1
Cisco Catalyst 3560 SMI	12.1(19)EA1
Cisco Catalyst 3550 EMI	12.1(8)EA1
Cisco Catalyst 3550 SMI	12.1(8)EA1
Cisco Catalyst 2970	12.1(11)AX
Cisco Catalyst 2950 EI	12.1(6)EA2
Cisco Catalyst 2950 SI	12.1(9)EA1
Cisco Catalyst 2940	12.1(13)AY

（注）　表 1-1 は、ID ベース ネットワーキングを実現するために最小限必要なソフトウェアを示しています。ソフトウェア リリースの更新および遅延に関する最新情報は、Cisco Connection Online のソフトウェア センターを参照することを推奨します。

シスコシステムズのルータ

表 1-2　シスコシステムズのルータ

831、836、837	12.3(2)XA
871、876、877、878	12.3(8)YI
1701、1711、1712、1721、1751、1760	12.3(2)XA
1801、1802、1803、1811、1812	12.3(8)YI
1841、2800、3800 HWIC-4ESW および HWIC-9ESW	12.3(8)T4
2800、3800 NM-16ESW および NMD-36ESW	12.3(4)T
2800、3800 NME-16ES-1G、NME-X-23ES-1G、NME-XD-24ES-1S および NME-XD-48ES-2S	12.2(25)SEC

（注）　表 1-2 は、ID ベース ネットワーキングを実現するために最小限必要なソフトウェアを示しています。ソフトウェア リリースの更新および遅延に関する最新情報は、Cisco Connection Online のソフトウェア センターを参照することを推奨します。

シスコシステムズの無線 LAN アクセス ポイントおよびコントローラ

表 1-3　シスコシステムズの無線 LAN アクセス ポイントおよびコントローラ

1100、1200 Aironet 無線 LAN アクセス ポイント	12.2(4)JA
1100、1200 Aironet 無線 LAN アクセス ポイント（EAP-FAST サポート）	12.2(15)JA
851、857、871、876、877、878 ルータ	12.3(8)YI
1801、1802、1803、1811、1812 ルータ	12.3(8)YI
1841、2800、3800 ルータ用 HWIC-AP 無線 LAN カード	12.4(2)T
Cisco Catalyst 6500 シリーズ無線 LAN サービス モジュール	1.1
2000、4100、4400 無線 LAN コントローラ	2.2.127.9

（注）　表 1-3 は、ID ベース ネットワーキングを実現するために最小限必要なソフトウェアを示しています。ソフトウェア リリースの更新および遅延に関する最新情報は、Cisco Connection Online のソフトウェア センターを参照することを推奨します。

Cisco Secure Access Control Server

表 1-4　Cisco Secure Access Control Server

リリース 3.0	EAP-MD5 & EAP-TLS による IEEE 802.1X のサポート
リリース 3.1	無線クライアント用 PEAP（EAP-GTC）による IEEE 802.1X のサポート
リリース 3.2	Microsoft Windows クライアント用 PEAP（EAP-MSCHAPv2）による IEEE 802.1X のサポート EAP-TLS および PEAP（MS-CHAPv2）の IEEE 802.1X マシン認証サポート
リリース 3.2.3	EAP-FAST による IEEE 802.1X のサポート（マシン認証サポートを含む）

（注）　表 1-4 は、ID ベース ネットワーキングを実現するために最小限必要なソフトウェアを示しています。ソフトウェア リリースの更新および遅延に関する最新情報は、Cisco Connection Online のソフトウェア センターを参照することを推奨します。

CHAPTER 2

オーセンティケータ

「IEEE 802.1X の主要なコンポーネント」（p.1-3）で定義したように、オーセンティケータは、クライアントの認証ステータスに基づいてネットワークへの物理的なアクセスを制御します。オーセンティケータは、クライアントと認証サーバ間の媒介として機能し、クライアントから ID 情報を要求して、認証サーバでその情報を確認し、クライアントに応答を返します。オーセンティケータは、クライアントとは EAPOL を介して、認証サーバとは RADIUS を介して通信します。

この章では、オーセンティケータだけを取り上げます。これは、Cisco Catalyst スイッチまたは Cisco Aironet 無線 LAN アクセス ポイントの基本構成は、認証用に選択した EAP 方式に関係なく、IEEE 802.1X の展開では固有であるためです。EAP 方式はクライアントおよび認証サーバによって承認され、オーセンティケータは両者の間で情報の交換のみを行います。

（注） このマニュアルでは、無線 LAN コントローラは取り上げません。

Cisco IOS

Cisco IOS を実行する Cisco Catalyst スイッチには、IEEE 802.1X を有効にするための特定のコマンドが必要です。コマンドを追加で設定して、オプションの機能を有効にしたり、デフォルト パラメータを変更したりできます。必要なグローバル コマンドおよびインターフェイス コマンドについては、次の項で説明します。基本的な例を示し、最小限必要な設定を提示します。

Cisco IOS の RADIUS 設定

Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために必要な RADIUS コマンドを示します。

表 2-1　Cisco IOS の RADIUS 設定コマンド

aaa new-model	AAA を有効化します。
aaa authentication dot1x [<list name> | **default**] **group radius**	IEEE 802.1X 認証方式リストを作成します。名前付きの方式リストを定義するか、キーワード default を使用してすべてのポートに適用します。その他の方式は設定オプションとして表示されますが、サポート対象は group radius のみです。
radius-server host [host name | **IP address**] auth-port [port] acct-port [port]	RADIUS サーバの IP アドレスを指定します。認証およびアカウンティング ポート番号をデフォルト値の 1645 と 1646 から変更します。
radius-server key [**string**]	RADIUS サーバで実行されるスイッチと RADIUS デーモンの間で使用される認証および暗号化キーを指定します。

Cisco IOS のグローバル IEEE 802.1X 設定

Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために必要なグローバル設定コマンドを示します。

表 2-2　Cisco IOS のグローバル IEEE 802.1X 設定コマンド

dot1x system-auth-control	スイッチで IEEE 802.1X 認証をグローバルに有効化します。

Cisco IOS のインターフェイス IEEE 802.1X 設定

Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために必要なインターフェイス設定コマンドを示します。

表 2-3　Cisco IOS のインターフェイス IEEE 802.1X 設定コマンド

switchport mode access / no switchport	IEEE 802.1X は、静的なレイヤ 2 アクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでのみ設定できます。IEEE 802.1X は、動的アクセス ポート、トランク ポート、または EtherChannel ではサポートされません。
dot1x port-control [force-authorized | force-unauthorized | **auto**]	ポートで IEEE 802.1X 認証を有効化します。デフォルトは force-authorized です。

Cisco IOS の IEEE 802.1X の動作確認

Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X の動作を確認するために使用する **show** コマンドを示します。

表 2-4　Cisco IOS のグローバル IEEE 802.1X Show コマンド

show dot1x	IEEE 802.1X の動作ステータスを表示します。
show dot1x [all | interface]	すべてのポートまたは特定のポートの IEEE 802.1X ステータスを表示します。
show dot1x statistics interface [interface]	特定のポートの IEEE 802.1X 統計を表示します。
show aaa servers	設定済みのすべての AAA サーバのステータスおよび運用情報を表示します。

Cisco IOS の基本的な設定例

基本的な設定例を示し、Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X を有効化するために最小限必要なコマンドを提示します。

```
aaa new-model
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
interface Gigabit 3/0/1
 switchport mode access
 dot1x port-control auto
!
radius-server host 10.1.1.5 auth-port 1812 acct-port 1813 key cisco
```

（注）　ユーザは、Cisco IOS 設定に AAA コマンドを追加すると、デバイス アクセスにも悪影響を与えることを理解する必要があります。たとえば、上記の設定例に示した AAA コマンドを追加すると、適切なアカウントをバックエンド サーバに追加するか、ローカル アカウントをデバイスに追加しないかぎり、Telnet アクセスが制限されます。

Cisco IOS の show dot1x interface の例

このコマンドの出力は、MAC アドレス 0006.5b88.06b1 のサプリカントが IEEE 802.1X 認証を正常に通過したことを示しています。また、インターフェイスに設定されている IEEE 802.1X パラメータも示しています。

```
Switch#show dot1x interface Gigabit 3/0/3
Supplicant MAC 0006.5b88.06b1
AuthSM State= AUTHENTICATED
BendSM State= IDLE
Posture = N/A
PortStatus= AUTHORIZED
MaxReq = 2
MaxAuthReq= 2
HostMode            = Single
PortContro= Auto
ControlDirection= Both
QuietPeriod= 60 Seconds
Re-authentication = Disabled
ReAuthPeriod= 3600 Seconds
ServerTimeout= 30 Seconds
SuppTimeout= 30 Seconds
TxPeriod= 30 Seconds
Guest-Vlan= 0
```

Cisco Catalyst OS

Cisco Catalyst OS を実行する Cisco Catalyst スイッチには、IEEE 802.1X を有効にするための特定のコマンドが必要です。追加でコマンドを設定して、オプションの機能を有効にしたり、デフォルト パラメータを変更したりできます。RADIUS、グローバル、およびポートの各コマンドについては、次の項で説明します。基本的な例を示し、最小限必要な設定を提示します。

Cisco Catalyst OS の RADIUS 設定

Cisco Catalyst OS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために必要な RADIUS コマンドを示します。

表 2-5　Cisco Catalyst OS の RADIUS 設定コマンド

set radius server [**IP address**] auth-port [port] acct-port [port] [primary]	RADIUS サーバの IP アドレスを指定します。認証およびアカウンティング ポートをデフォルト値の 1812 と 1813 から変更できます。プライマリ パラメータは、この特定の RADIUS サーバに優先的に接続するように設定できます。
set radius key [**key**]	RADIUS クライアントとサーバ間のすべてのトランザクションを認証するために使用するキーを指定します。

Cisco Catalyst OS のグローバル IEEE 802.1X 設定

Cisco Catalyst OS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために必要なグローバル設定コマンドを示します。

表 2-6　Cisco Catalyst OS のグローバル IEEE 802.1X 設定コマンド

set dot1x system-auth-control [enable | disable]	システムの dot1x を無効化 / 有効化します。

Cisco Catalyst OS のポート IEEE 802.1X 設定

Cisco Catalyst OS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために必要なポート設定コマンドを示します。

表 2-7　Cisco Catalyst OS のポート IEEE 802.1X 設定コマンド

set port dot1x [module/port] **port-control** [force-authorized | force-unauthorized | auto]	ポート制御タイプを指定します。デフォルトは force-authorized です。

Cisco Catalyst OS の IEEE 802.1X の動作確認

Cisco Catalyst OS を実行する Cisco Catalyst スイッチで IEEE 802.1X の動作を確認するために使用する **show** コマンドを示します。

表 2-8　Cisco Catalyst OS のグローバル IEEE 802.1X show コマンド

show radius	設定済みの RADIUS パラメータを表示します。
show dot1x	システムの IEEE 802.1X 機能を表示します。
show dot1x group [all | authenticated | group name]	IEEE 802.1X のユーザ グループ情報を表示します。
show dot1x user [all | user name]	IEEE 802.1X のユーザ情報を表示します。
show dot1x vlan [all | VLAN ID]	VLAN 内の IEEE 802.1X で認証されたユーザに関する情報を表示します。
show dot1x vlan-group [all | VLAN-group-name]	IEEE 802.1X VLAN のグループ情報を表示します。
show port dot1x [module/port]	特定のポート上のオーセンティケータが送受信する各種の Extensible Authentication Protocol（EAP）パケットについて、オーセンティケータの Port Access Entity（PAE）、バックエンド オーセンティケータ、および統計に関連する設定可能な値と現在の状態の値をすべて表示します。
show port dot1x statistics [module/port]	特定のポート上のオーセンティケータが送受信する各 EAP パケットの統計を表示します。
show port dot1x [module/port] **guest-vlan** [VLAN ID | none]	IEEE 802.1X ゲスト VLAN として機能するアクティブな VLAN を表示します。
show port dot1x auth-fail-vlan [VLAN ID | none]	IEEE 802.1X 認証に失敗したユーザの VLAN を持つポートに関する情報を表示します。

Cisco Catalyst OS の基本的な設定例

基本的な設定例を示し、Cisco Catalyst OS を実行する Cisco Catalyst スイッチで IEEE 802.1X を有効にするために最小限必要なコマンドを提示します。

```
set radius server 10.1.1.5 auth-port 1812 primary
set radius key cisco
!
set dot1x system-auth-control enable
!
set port dot1x 6/15 port-control auto
```

Cisco Catalyst OS の show port dot1x [mod/port] コマンドの例

このコマンドの出力は、ポート 6/15 に接続されたサプリカントが IEEE 802.1X 認証を正常に通過したことを示しています。また、ポートに設定されている IEEE 802.1X パラメータも示しています。

```
Switch> (enable) show port dot1x 6/15
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- -------------------
------------------------------------------------------------
 6/15 authenticated      idle       auto                authorized
```

```
Port  Port-Mode     Re-authentication   Shutdown-timeout   Control-Mode
                                                          admin   oper
-----
-------------------------------------------------------------------------------------------------
---------------------
 6/15 SingleAuth    disabled            disabled           Both    Both

Port  Posture-Token Critical Termination action Session-timeout
----- ------------- -------- ------------------
-------------------------------------------------------------------
 6/15 -             NO       NoReAuth          -
```

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイント

Cisco IOS を実行する Cisco Aironet 無線アクセス ポイントには、IEEE 802.1X を有効にするための特定のコマンドが必要です。追加でコマンドを設定して、オプションの機能を有効にしたり、デフォルト パラメータを変更したりできます。RADIUS、グローバル、およびインターフェイスの各コマンドについては、次の項で説明します。基本的な例を示し、最小限必要な設定を提示します。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントの RADIUS 設定

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントで IEEE 802.1X を設定するために必要な RADIUS コマンドを示します。

表 2-9　Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントの RADIUS 設定コマンド

aaa new-model	AAA を有効化します。
aaa authentication login [<list name> | default] **group radius**	認証方式リストを作成します。名前付きの方式リストを定義するか、キーワード default を使用してすべてのポートに適用します。
radius-server host [host name | IP address] **auth-port** [port] **acct-port** [port]	RADIUS サーバの IP アドレスを指定します。認証およびアカウンティング ポート番号をデフォルト値の 1645 と 1646 から変更します。
radius-server key [string]	RADIUS サーバで実行されるスイッチと RADIUS デーモンの間で使用される認証および暗号化キーを指定します。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントのグローバル設定

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントで IEEE 802.1X を設定するために必要なグローバル設定コマンドを示します。

表 2-10　Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントのグローバル IEEE 802.1X 設定コマンド

dot11 ssid [ssid-string]	SSID を作成し、新しい SSID の SSID 設定モードを開始します。SSID には、最大 32 文字の英数字を使用します。SSID は大文字と小文字を区別します。
authentication open eap [list name]	この SSID を開始するための認証タイプを設定します。オープン認証により、すべてのデバイスで認証を行い、アクセス ポイントとの通信を試行します。
authentication network-eap [list name]	（指定された SSID の）無線インターフェイスを設定して、ネットワーク EAP 認証をサポートします。ネットワーク EAP 認証では、ネットワークにアクセスする前に IEEE 802.1X クライアント認証が必要です。EAP をオープン認証に追加すると、802.11 オープン認証以外に IEEE 802.1X 認証が有効化されます。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントのインターフェイス設定

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントで IEEE 802.1X を設定するために必要なポート設定コマンドを示します。

表 2-11　Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントのインターフェイス設定コマンド

ssid [ssid string]	グローバルに設定された SSID を無線インターフェイスに割り当てます。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントの IEEE 802.1X の動作確認

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントで IEEE 802.1X の動作を確認するために使用する **show** コマンドを示します。

表 2-12　Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントの IEEE 802.1X show コマンド

show dot11 associations	無線アソシエーション テーブル、無線アソシエーション統計を表示するか、すべてのリピータ、すべてのクライアント、特定のクライアント、または基本サービス クライアントに関するアソシエーション情報を選択的に表示します。
show aaa servers	設定済みのすべての AAA サーバのステータスおよび運用情報を表示します。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントの基本的な設定例

基本的な設定例を示し、Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントで IEEE 802.1X を有効にするために最小限必要なコマンドを提示します。

```
aaa new-model
!
aaa authentication login eap_methods group radius
!
```

```
dot11 ssid cisco
   authentication open eap eap_methods
   authentication network-eap eap_methods
!
interface Dot11Radio0
ssid cisco
 !
ip radius source-interface BVI1
!
radius-server host 10.1.1.5 auth-port 1812 acct-port 1813
radius-server key cisco
```

（注）　名前付きの認証リストは、前項の Cisco IOS および Cisco Catalyst OS の例で使用したデフォルトの名前リスト オプションを使用して作成されるのではなく、コマンド **aaa authentication login** を使用して Cisco Aironet 無線 LAN アクセス ポイント設定で作成されます。これは、SSID 設定モードで使用される **authentication** [open | network-eap] コマンドには、リスト名が必要なためです。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントの show dot11 associations の例

このコマンドの出力は、MAC アドレス 0002.8ade.5af5 のサプリカントが EAP を介して IEEE 802.1X 認証を正常に通過したことを示しています。

```
ap#show dot11 associations

802.11 Client Stations on Dot11Radio0:
SSID [cisco] :

MAC Address    IP addressDeviceNameParentState
0002.8ade.5af5 12.1.1.52       350-client    sdelairselfEAP-Assoc
```

CHAPTER 3

EAP-MD5 の展開

この章では、サプリカントと認証サーバ間で EAP-MD5 を使用して、IEEE 802.1X ポートベースのアクセス制御を展開する方法について説明します。この展開例のサプリカントとして、Meetinghouse AEGIS クライアント バージョン 2.3.3.0 が使用されます。Cisco Secure ACS 4.0 は、認証サーバとして使用されます。Cisco Catalyst スイッチはオーセンティケータとして機能し、サプリカントと認証サーバ間に有線 LAN 接続を提供します。

認証サーバの設定

ここで示す手順は、EAP-MD5 認証用に Cisco Secure ACS 4.0 を設定する方法について説明しています。

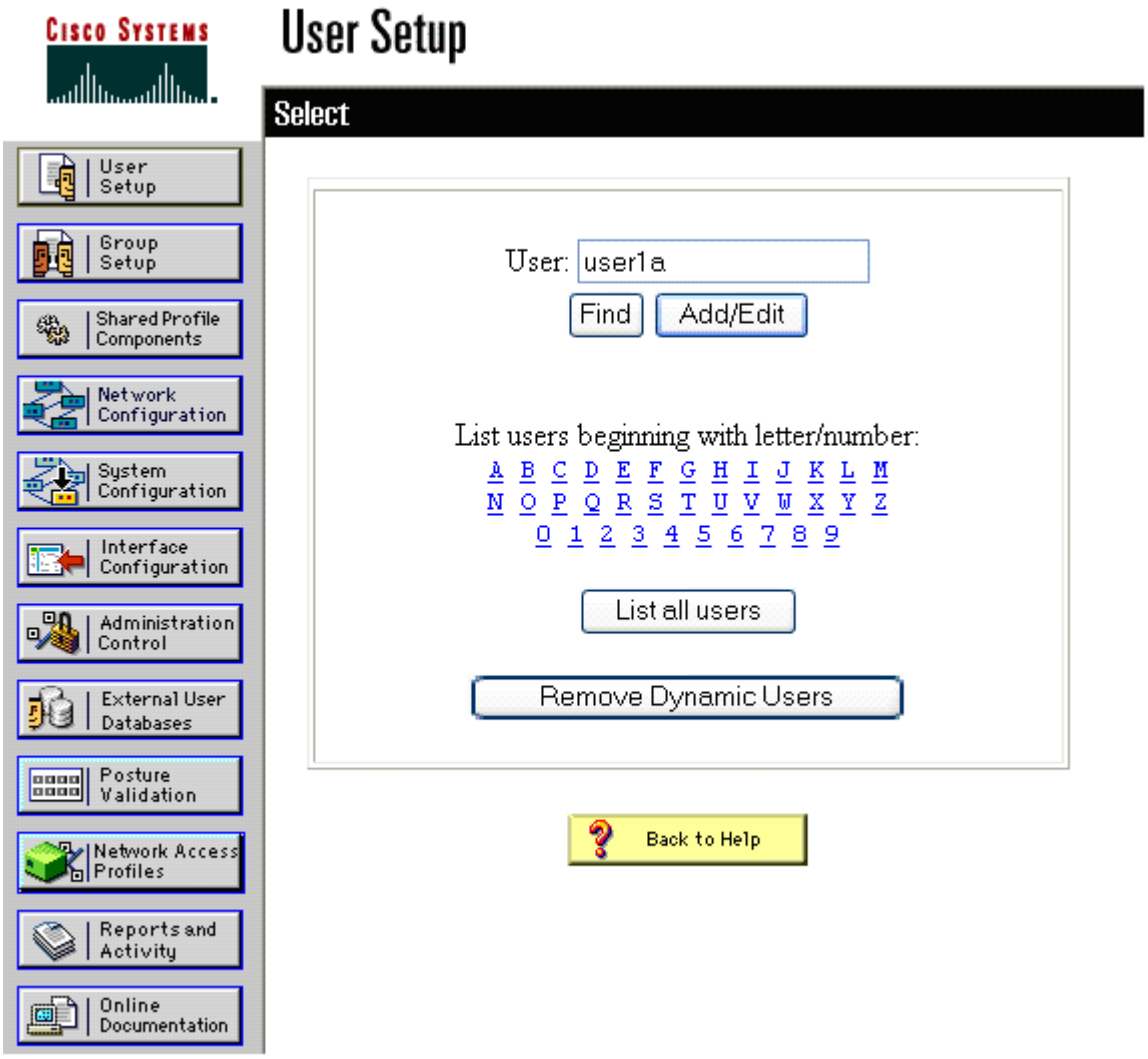
（注） ここでは、EAP-MD5 認証の設定に必要な手順についてのみ説明します。その他の機能の詳細については、『*Cisco Secure ACS Configuration Guide*』を参照してください。

ACS データベースでのユーザの作成

メイン メニューで **User Setup** をクリックします。User ボックスにユーザ名を入力し、**Add/Edit** ボタンをクリックします。

（注） EAP-MD5 は、Windows Active Directory などの外部ユーザ データベースを利用できない唯一の EAP 認証方式です。EAP-MD5 には、内部 ACS データベースが必要です。

図 3-1　ACS データベースでのユーザの作成

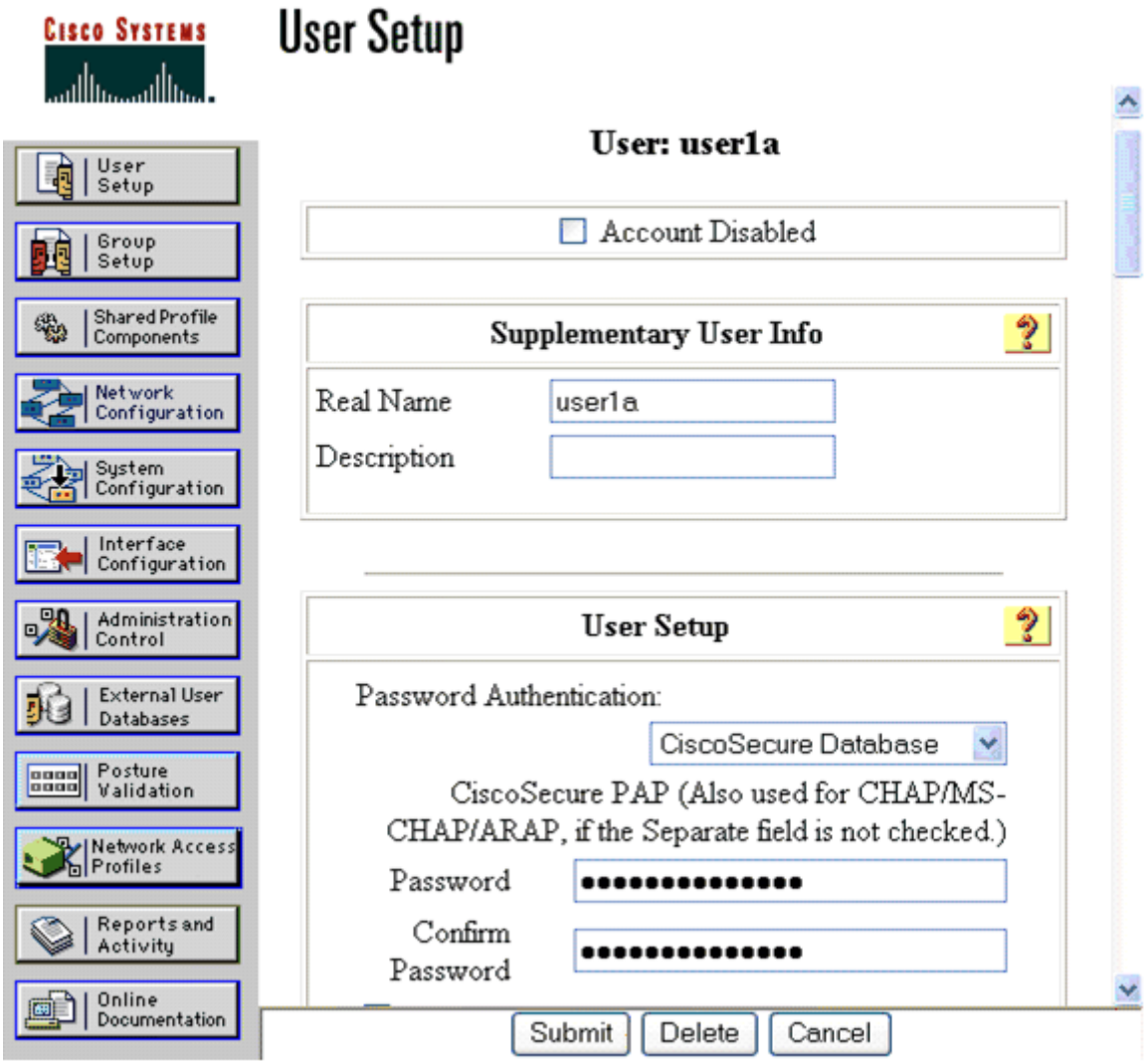


ACS データベースでのユーザの設定

User Setup セクションで、Password Authentication に CiscoSecure Database が選択されていることを確認します。次に、ユーザ パスワードを入力します。パスワードを再入力して確認します。**Submit** をクリックします。

（注）　EAP タイプとして MD5 で使用するパスワードを入力します。

図 3-2　ACS データベースでのユーザの設定

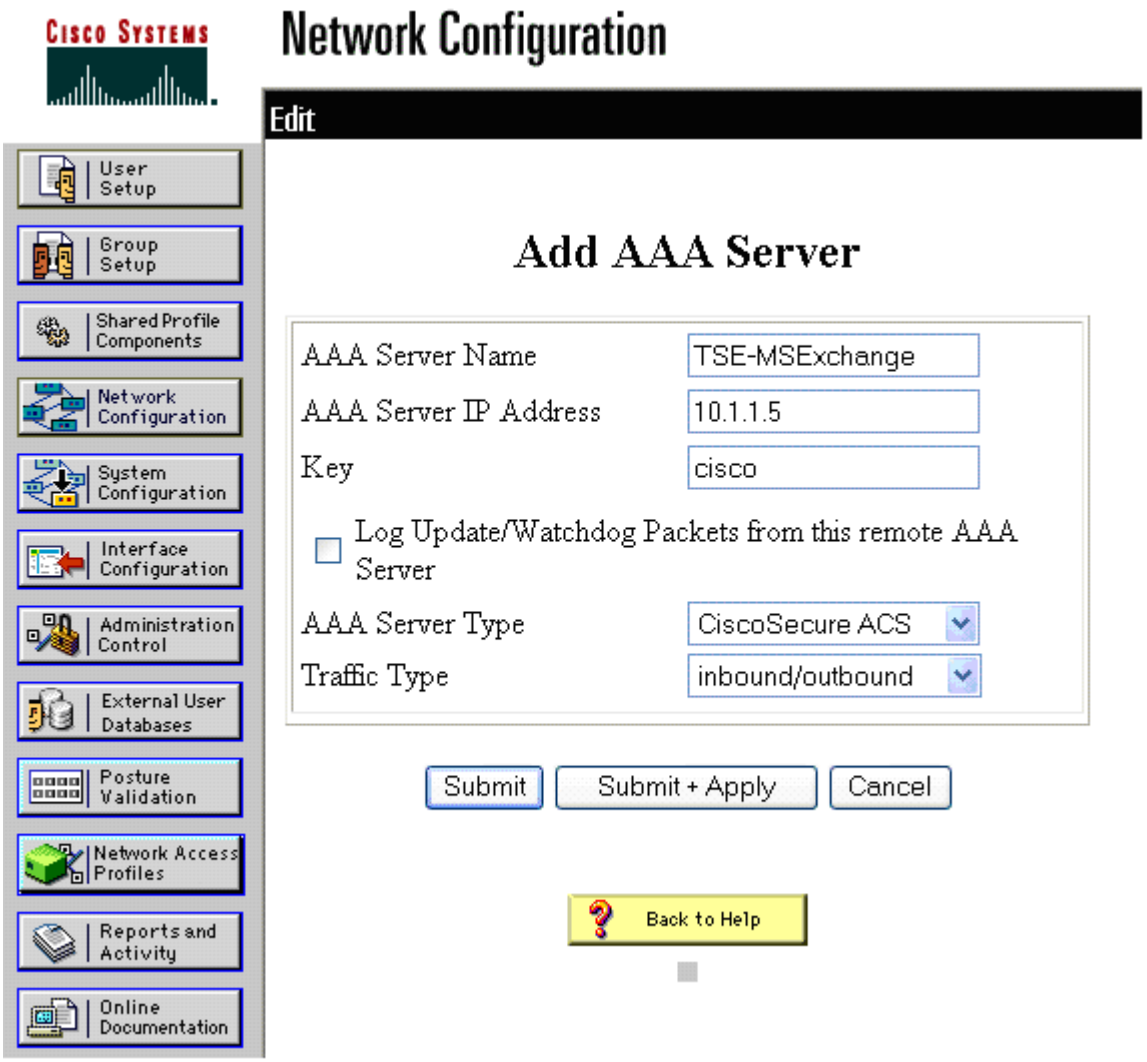


AAA サーバの設定

メイン メニューで **Network Configuration** をクリックします。AAA Server テーブルで、**Add Entry** をクリックします。Add AAA Server 画面で、AAA Server Name、AAA Server IP Address、および Key を入力します。AAA Server Type で、CiscoSecure ACS を選択します。Traffic Type で、デフォルト設定の inbound/outbound をそのまま使用します。**Submit + Apply** をクリックします。

（注）　デフォルトでは、ACS を実行するローカル マシンのホスト名と IP アドレスを含む AAA Server エントリが、AAA Server テーブルにすでに存在します。

図 3-3　AAA サーバの設定



AAA クライアントの設定

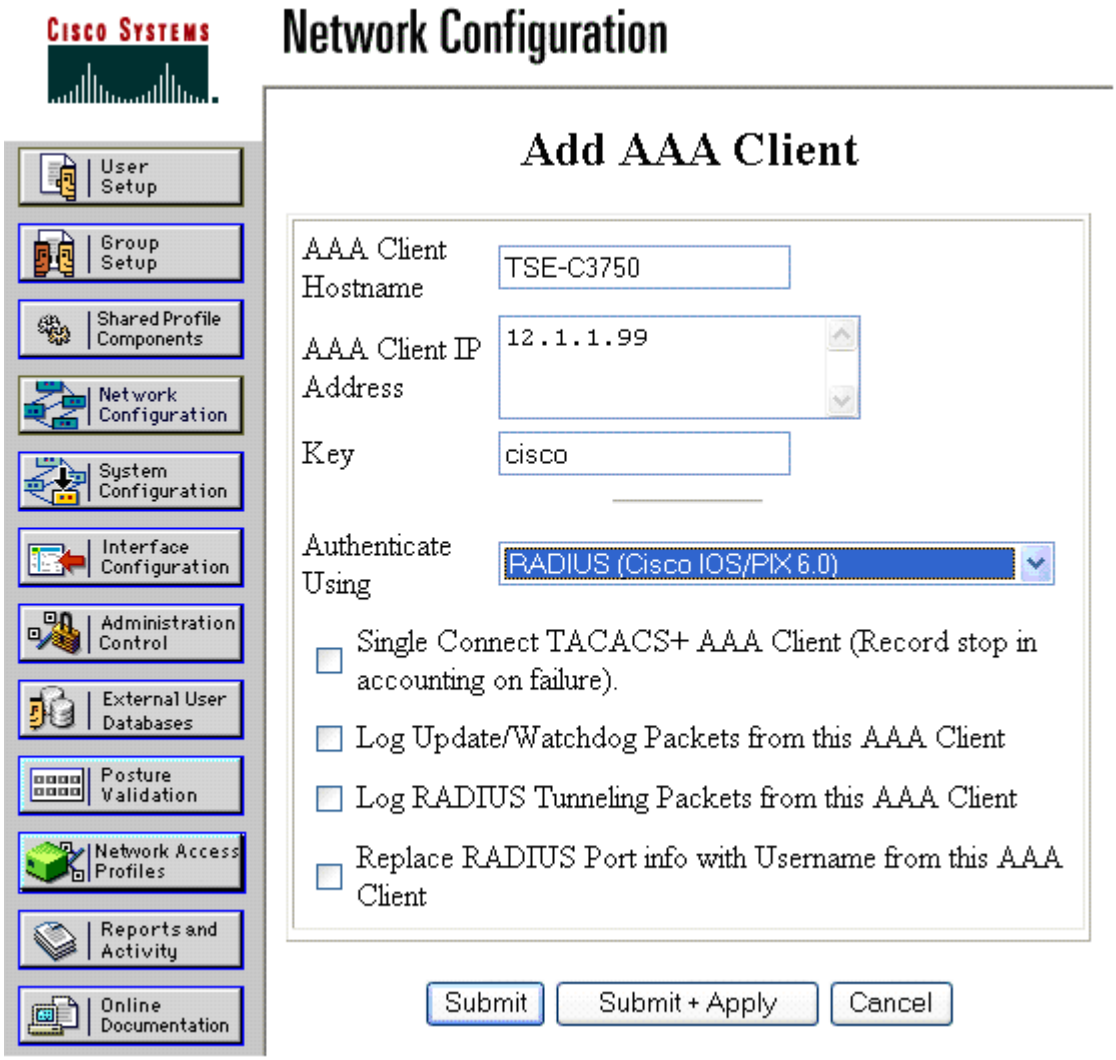
Network Configuration 画面から、AAA Clients テーブルの **Add Entry** をクリックして、オーセンティケータを追加します。Add AAA Client 画面で、AAA Client Host Name、AAA Client IP Address、および Key を入力します。Authenticate Using オプションで、RADIUS (Cisco IOS/PIX 6.0) を選択します。

（注）　RADIUS (Cisco IOS/PIX 6.0) オプションにより、Cisco IOS RADIUS Vendor-Specific Attribute（VSA）を使用できます。その他のセキュリティ制御プロトコル オプションは、RADIUS および TACACS+ に使用できます。

Submit + Apply をクリックします。

（注）　Key は、IOS または Catalyst OS オーセンティケータで設定されているキーと一致する必要があります。

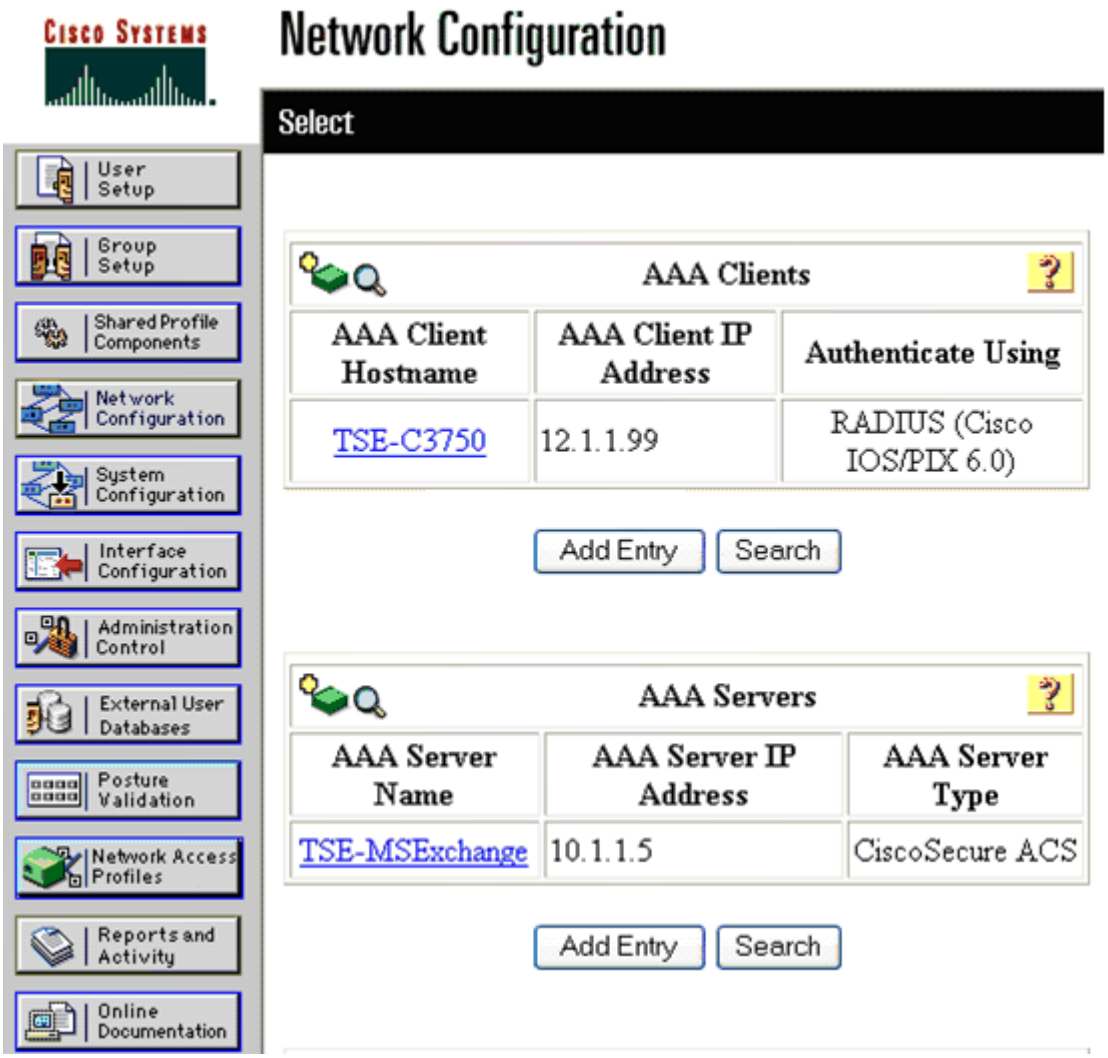
図 3-4　AAA クライアントの設定



ネットワーク設定の概要

AAA サーバおよび AAA クライアントを設定したあと、更新されたエントリのリストとともに Network Configuration メニューが表示されます。

図 3-5　ネットワーク設定の概要

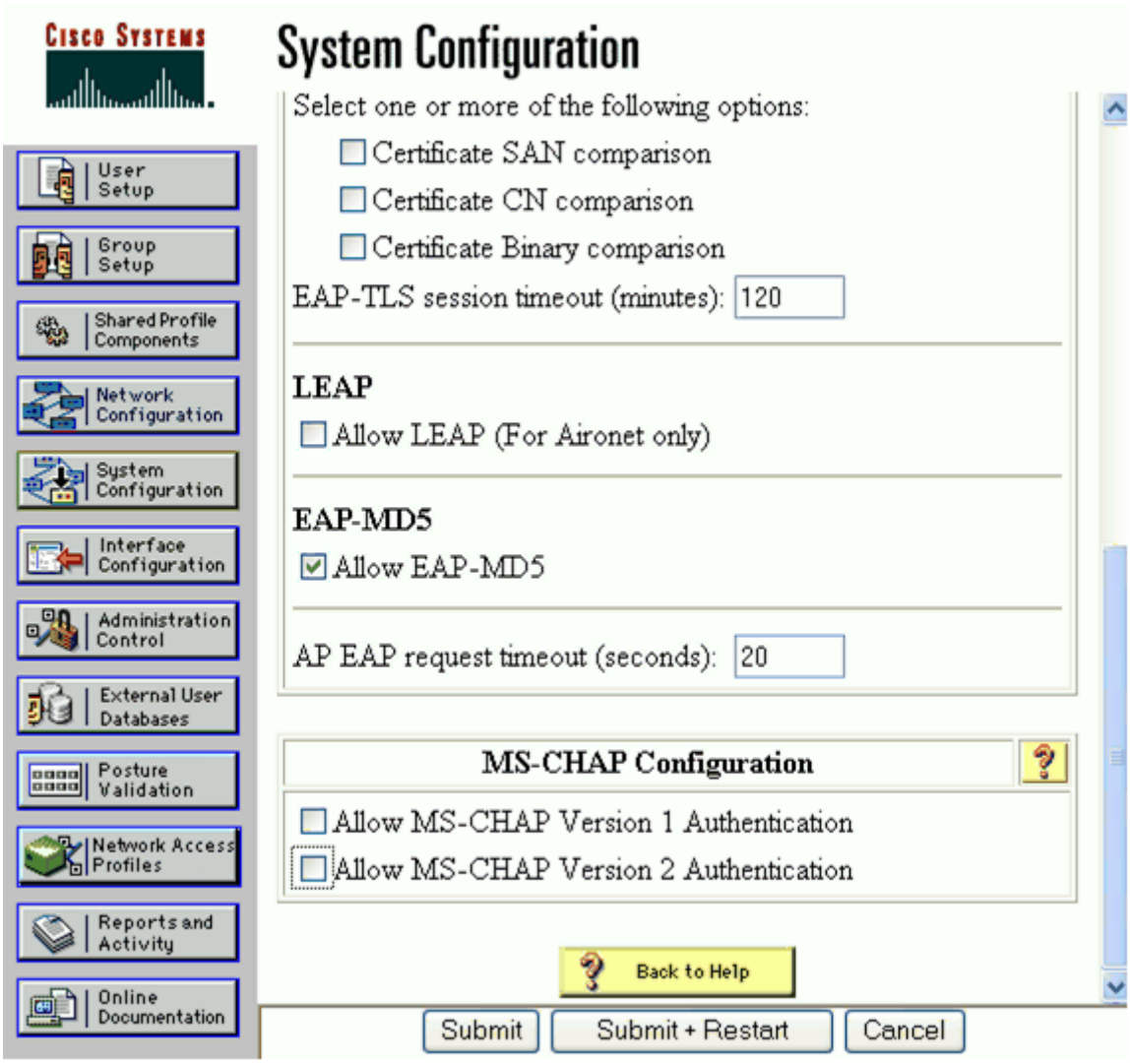


EAP-MD5 のグローバル認証設定

メイン メニューで **System Configuration** をクリックします。System Configuration メニューから、Global Authentication Setup を選択して、EAP 方式を設定します。EAP-MD5 セクションの Allow EAP-MD5 ボックスをオンにします。**Submit + Restart** をクリックします。

（注）　CiscoSecure ACS がインストールされている場合、EAP-MD5 はデフォルトで有効になっています。

図 3-6　EAP-MD5 のグローバル認証設定



クライアント設定

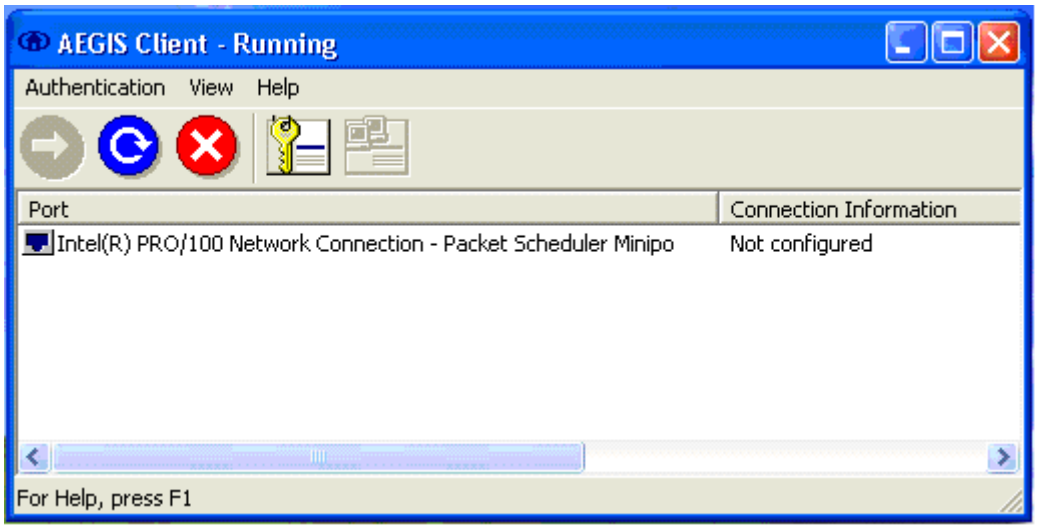
ここで示す手順は、EAP-MD5 認証用に Meetinghouse AEGIS クライアント バージョン 2.3.3.0 を設定する方法について説明しています。

（注）　Meetinghouse AEGIS クライアントは、Service Pack 2 を適用した Windows XP オペレーティング システムで実行されています。

Meetinghouse AEGIS クライアントのオープン

Meetinghouse AEGIS クライアントを開き、**Authentication** メニューをクリックして、Authentication Profile を選択します。

図 3-7　Meetinghouse AEGIS クライアント

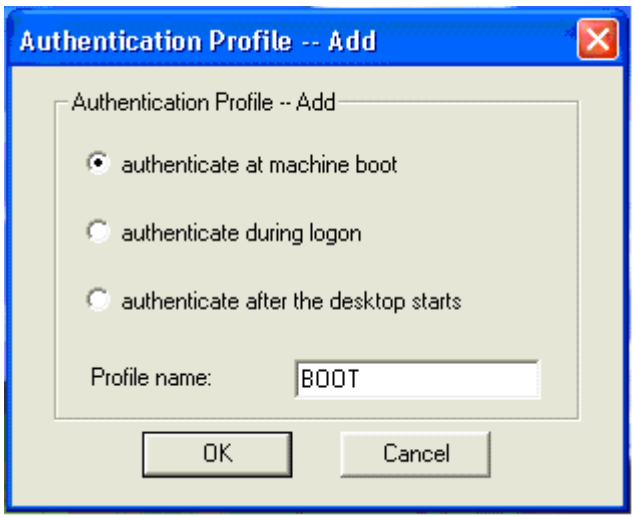


マシン認証プロファイルの作成

Authentication Profile メニューで、authenticate at machine boot オプションを選択し、プロファイル名を入力します。この例では、プロファイル名は BOOT です。このプロファイルでは、認証にユーザ証明書ではなくマシン証明書が使用されます。マシン認証を使用すると、ユーザがログオンする前にマシン プロセスを初期化できるため、バックエンド ディレクトリ システムへのログオンに必要な合計時間を短縮できます。

OK をクリックします。

図 3-8　マシン認証プロファイルの作成

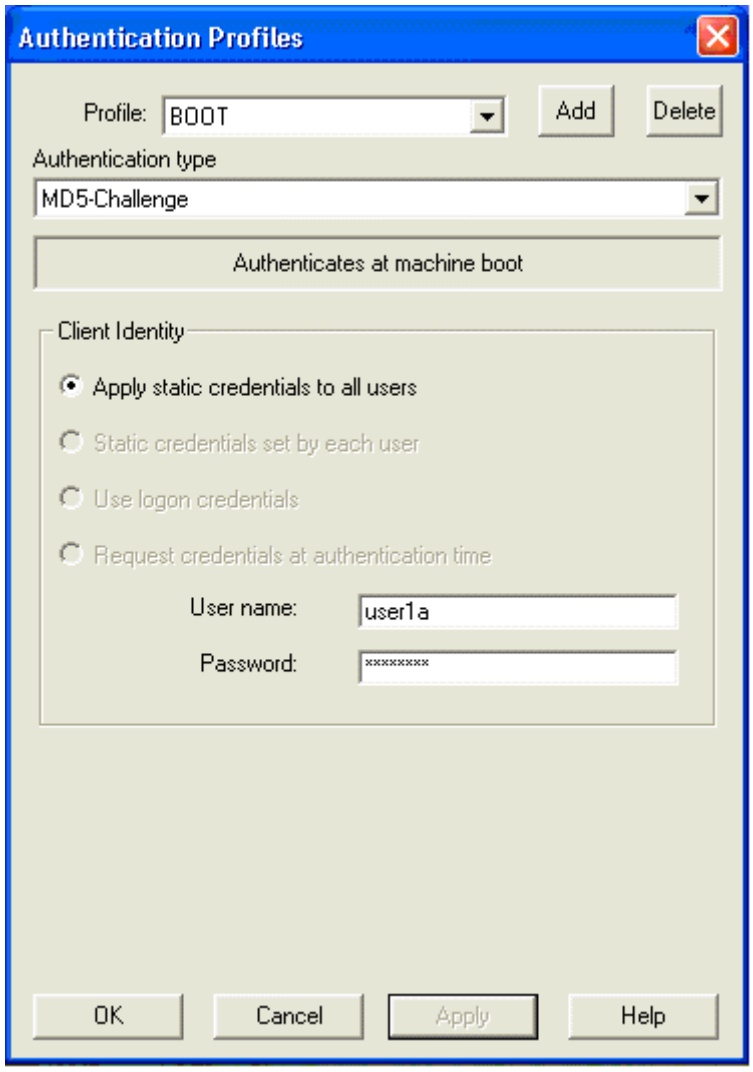


マシン認証プロファイルの設定

Authentication type に MD5-Challenge オプションを選択して、Client Identity 方式を設定します。この例では、Apply static credentials to all users オプションを使用します。これにより、管理者は、ユーザに関係なくマシンの静的証明書を設定できます。マシン認証はブート時に行われるため、認証用に Windows 証明書を収集する方法はありません。Static credentials set by each user、Request credentials at authentication time など、その他のオプションもありますが、これらはすべて、ユーザが個別に介入する必要があります。

OK をクリックします。

図 3-9　　マシン認証プロファイルの設定



ユーザ認証プロファイルの作成

Authentication Profile メニューで、authenticate during logon オプションを選択します。この例では、プロファイル名は LOGON です。**OK** をクリックします。

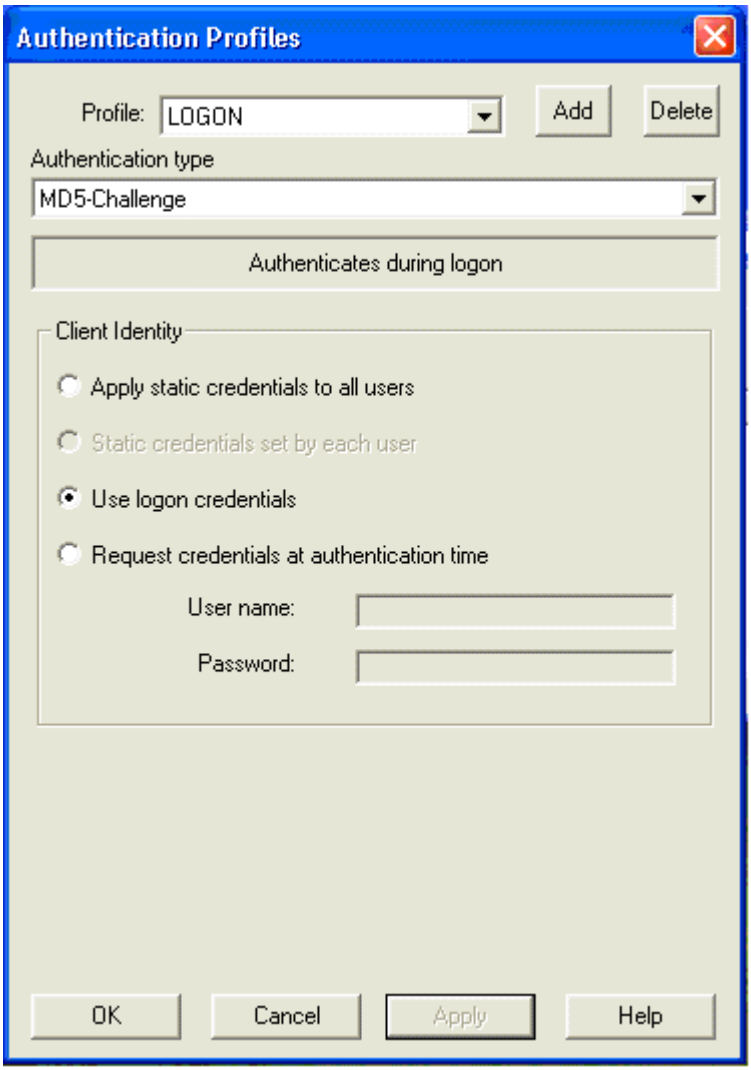
図 3-10　ユーザ認証プロファイルの作成

ユーザ認証プロファイルの設定

Authentication type に MD5-Challenge オプションを選択して、Client Identity 方式を設定します。この例では、Use logon credentials オプションが選択されています。これは、EAP-MD5 認証に Windows ユーザ名とパスワードが使用されることを意味します。その他のオプションもありますが、Use logon credentials オプションは Single Sign-On（SSO）方式を提供します。Apply static credentials to all users オプションでは、ネットワークへのアクセス時に特定のユーザを識別する方法が提供されません。Request credentials at authentication time オプションは、Use logon credentials オプションに似ていますが、ユーザの 2 番めのステップを作成します。

OK をクリックします。

図 3-11　ユーザ認証プロファイルの設定

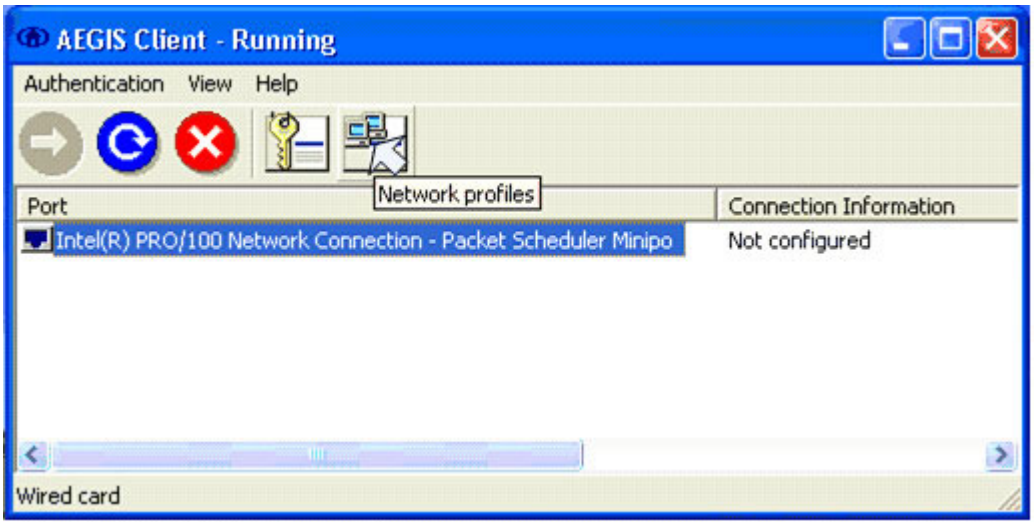


ネットワーク プロファイルの作成

最後の手順では、設定された認証プロファイルを参照するネットワーク プロファイルを作成します。これを行うには、表示されたリストから適切なネットワーク アダプタを選択して、**Network Profiles** アイコンをクリックします。

（注）　Meetinghouse AEGIS クライアントは、検出された任意のネットワーク アダプタにバインドされるため、ネットワーク プロファイルを適切なアダプタに適用する必要があります。

図 3-12　ネットワーク プロファイルの作成

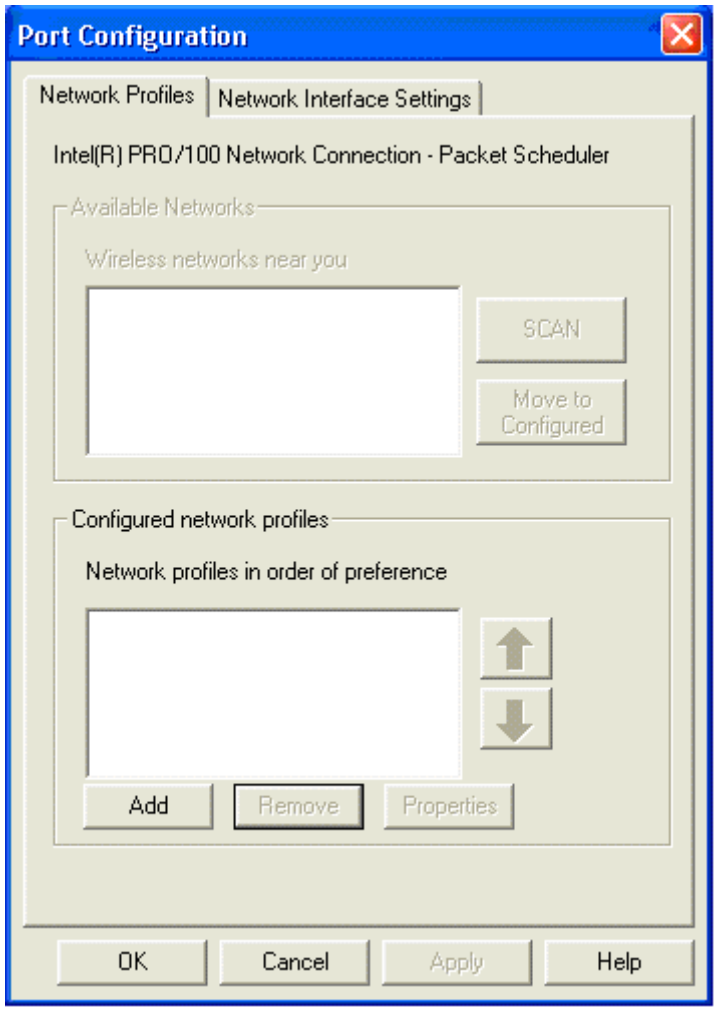


ポート設定の構成

選択したネットワーク アダプタのネットワーク プロファイルを作成するには、**Add** をクリックします。

（注）　Network Interface Settings タブは、認証タイムアウト、インターフェイス、DHCP オプションなど、プロトコル設定を構成するために使用されます。この例では、デフォルトのパラメータが使用されています。

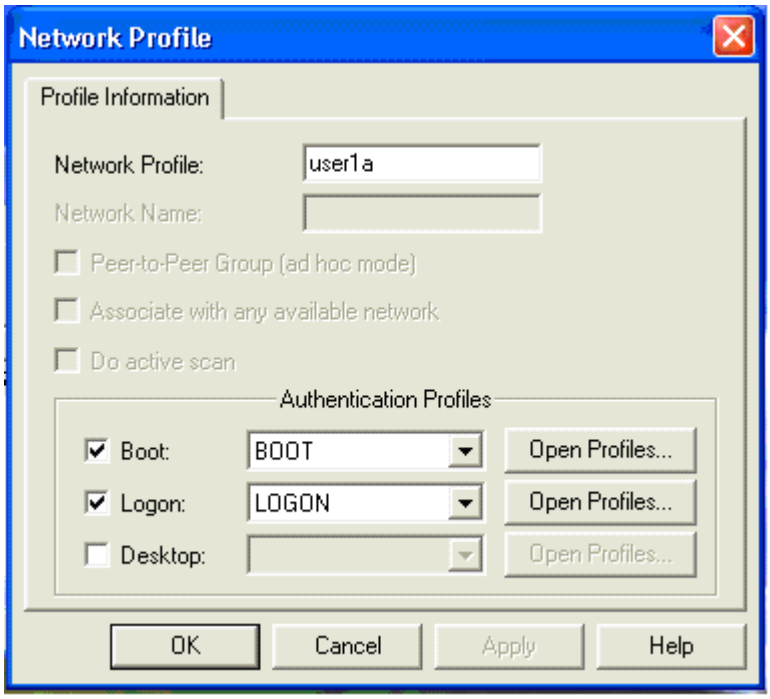
図 3-13　ポート設定の構成



ネットワーク プロファイルの設定

ネットワーク プロファイルの名前を入力します。Boot Authentication Profile のチェック ボックスをクリックして、ドロップダウン メニューから BOOT プロファイルを選択します。Logon Authentication Profile についてもこの手順を繰り返します。この場合は、ドロップダウン メニューから LOGON を選択します。**OK** をクリックします。

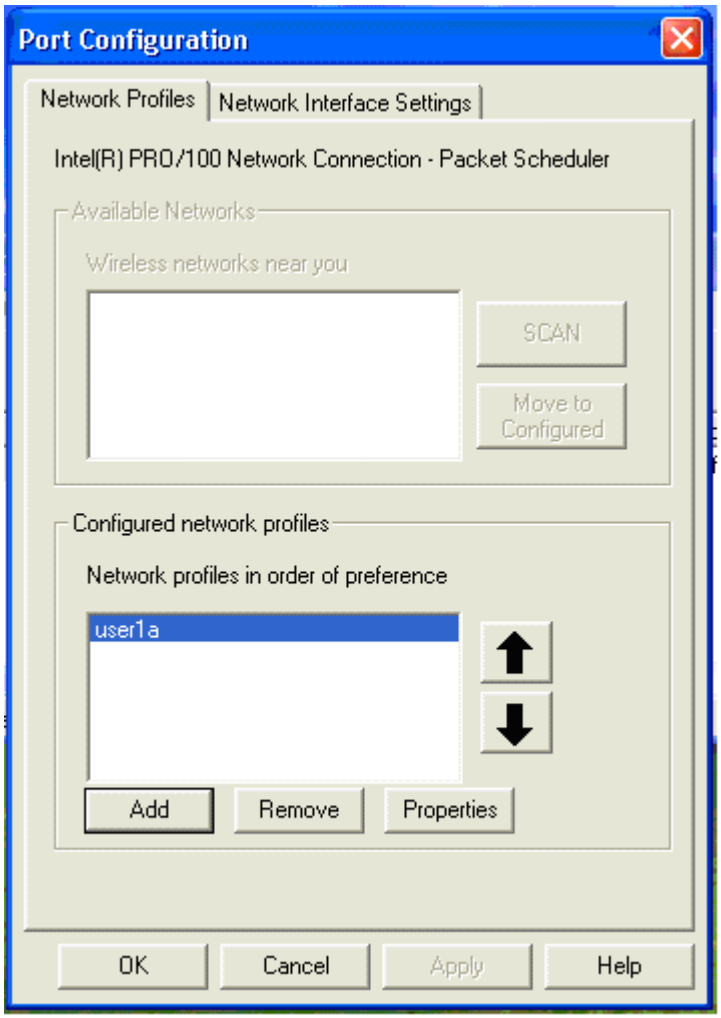
図 3-14　ネットワーク プロファイルの設定



ネットワーク プロファイルの適用

前述の手順で設定したネットワーク プロファイルが Configured Network Profiles ボックスに表示されます。**OK** をクリックして、プロファイルをネットワーク アダプタに適用します。

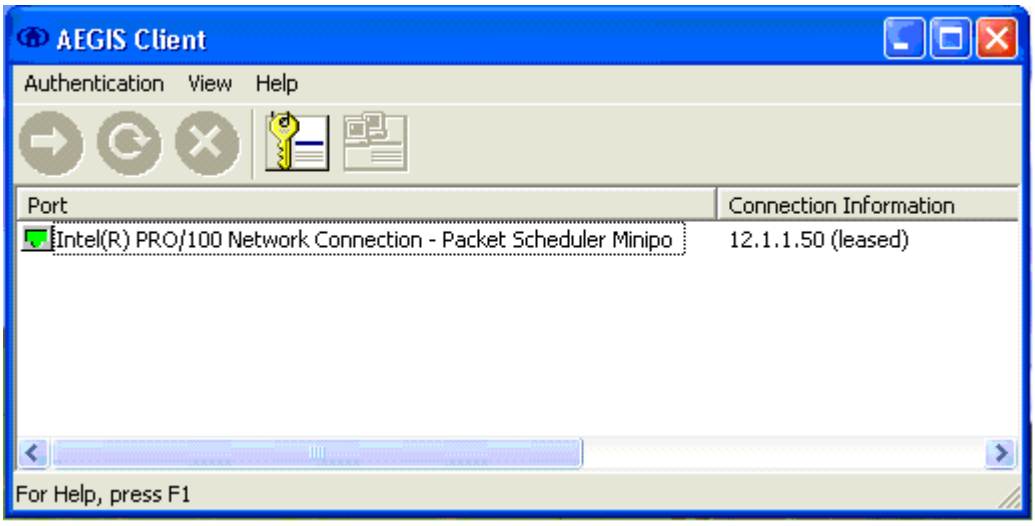
図 3-15　ネットワーク プロファイルの適用



クライアント認証の確認

ネットワーク プロファイルがネットワーク アダプタに適用されると、マシンおよびユーザ認証に対して IEEE 802.1X が正常に設定されます。クライアントが認証されると、DHCP を介して IP アドレスを受信し、ネットワーク アクセスが可能になります。

図 3-16　クライアント認証の確認



CHAPTER 4

EAP-TLS の展開

この章では、サプリカントと認証サーバ間で EAP-TLS を使用して、IEEE 802.1X ポートベースのアクセス制御を展開する方法について説明します。この展開例のサプリカントとして、Funk Odyssey クライアント バージョン 4.02.0.2000 が使用されます。Cisco Secure ACS 4.0 は、認証サーバとして使用されます。Cisco Catalyst スイッチはオーセンティケータとして機能し、サプリカントと認証サーバ間に有線 LAN 接続を提供します。

認証サーバの設定

ここで示す手順は、EAP-TLS 認証用に Cisco Secure ACS 4.0 を設定する方法について説明しています。

（注） ここでは、EAP-TLS 認証の設定に必要な手順についてのみ説明します。その他の機能の詳細については、『*Cisco Secure ACS Configuration Guide*』を参照してください。

不明なユーザ ポリシーの作成

メイン メニューで **External User Databases** をクリックします。External User Databases メニューで、Unknown User Policy を選択します。

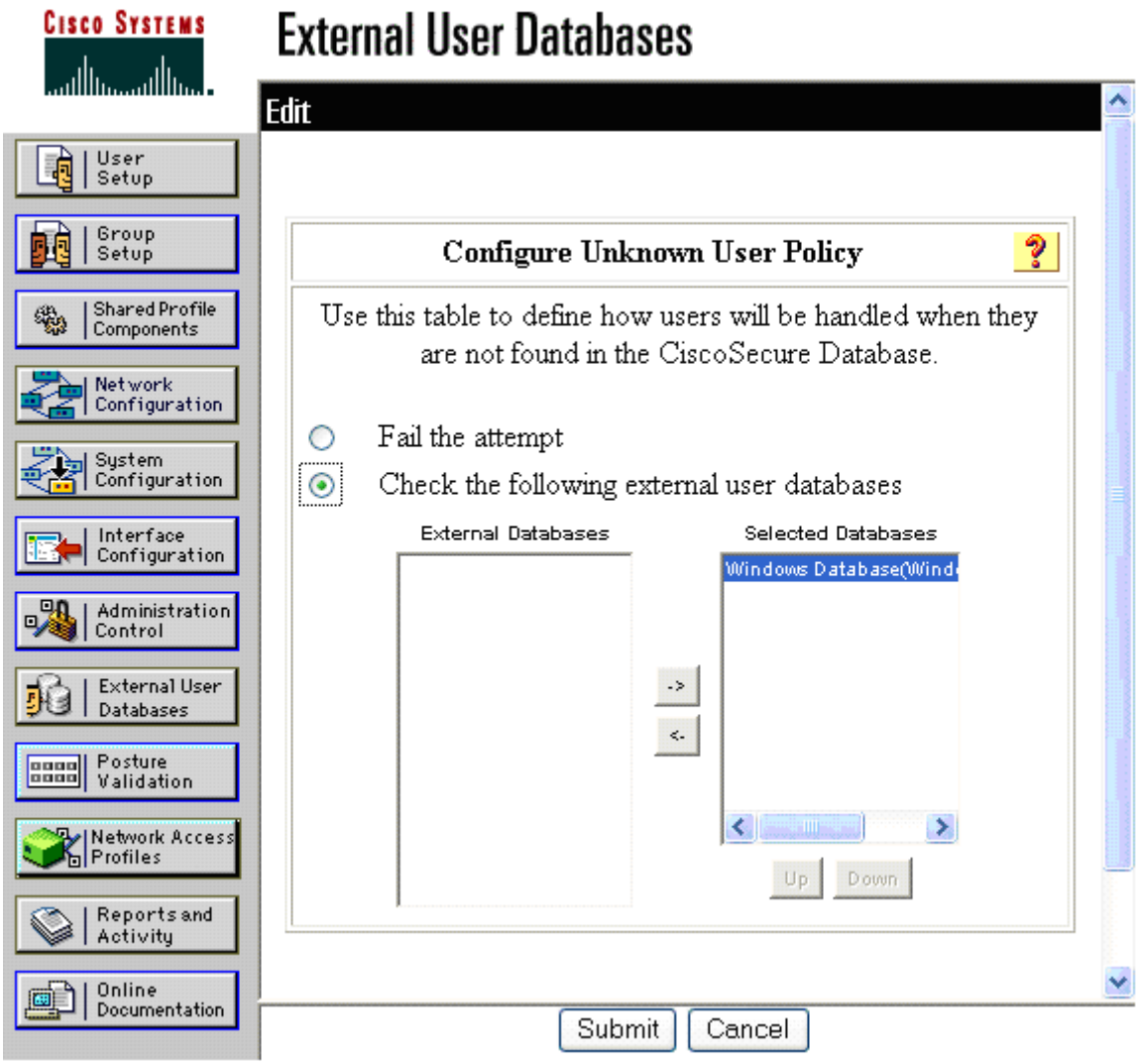
（注） EAP-TLS では、Windows Active Directory などの外部ユーザ データベースを使用する必要はありません。この EAP 方式では、内部 ACS データベースを使用できます。

図 4-1　不明なユーザ ポリシーの作成

不明なユーザ ポリシーの設定

Configure Unknown User Policy セクションで、Check the following external user databases オプション ボタンを選択します。Windows Database オプションを External Databases 列から Selected Databases 列に移動します。**Submit** をクリックします。

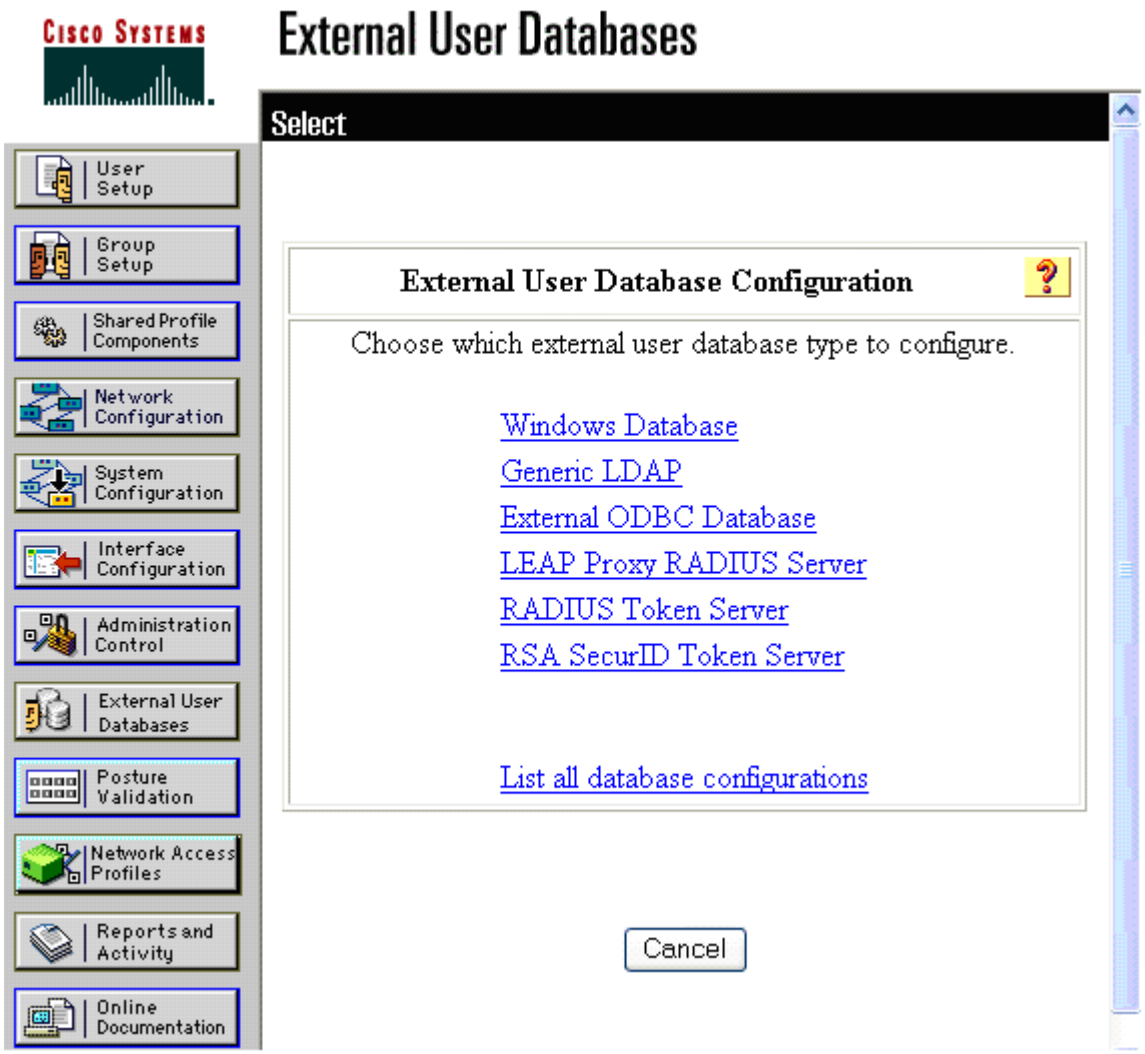
図 4-2　不明なユーザ ポリシーの設定



外部ユーザ データベースの選択

External User Databases メニューから Database Configuration オプションを選択します。External User Database Configuration セクションで、Windows Database オプションを選択します。

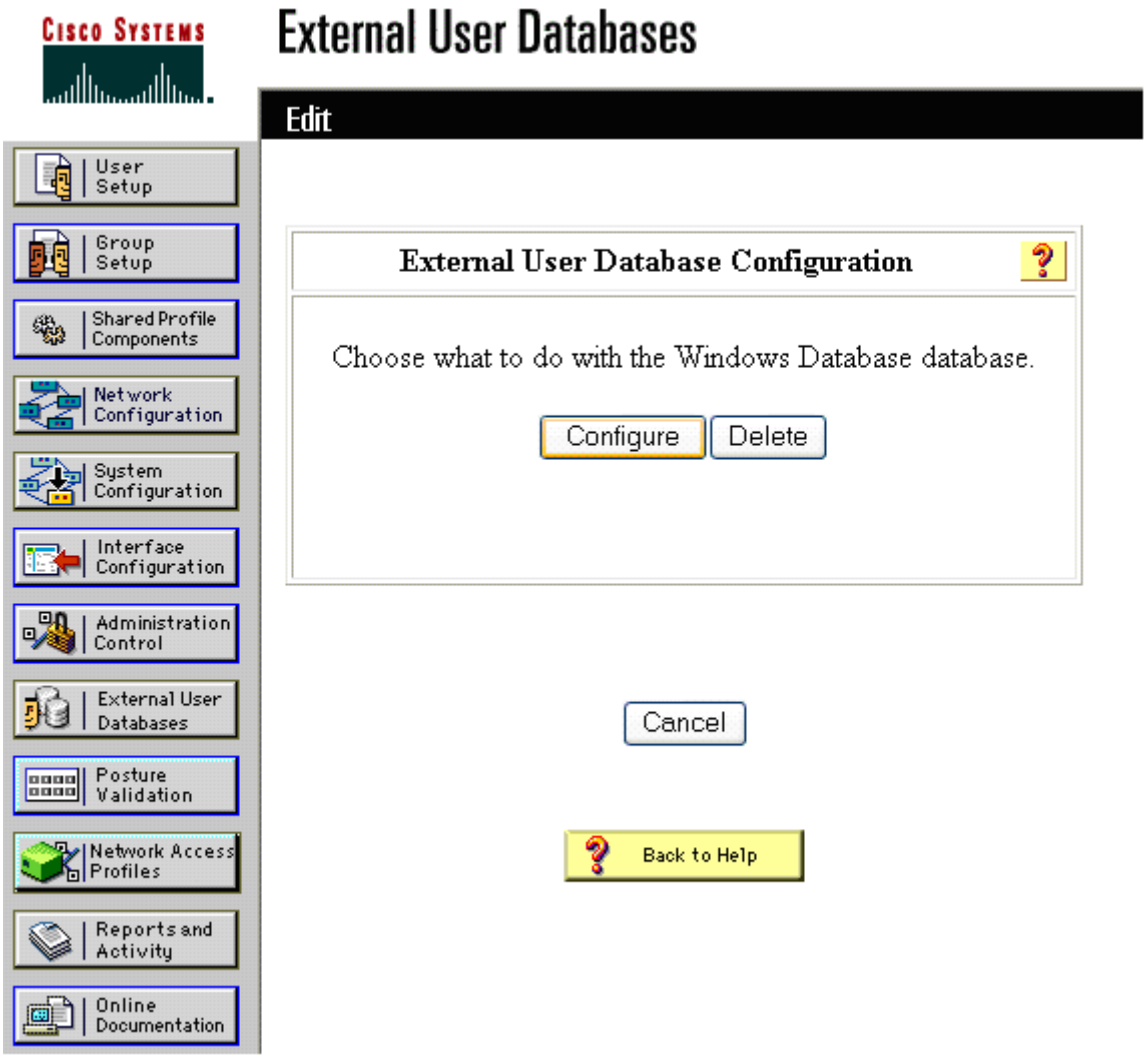
図 4-3　外部ユーザ データベースの選択



Windows データベースの設定の選択

External User Database Configuration セクションで、**Configure** ボタンをクリックします。

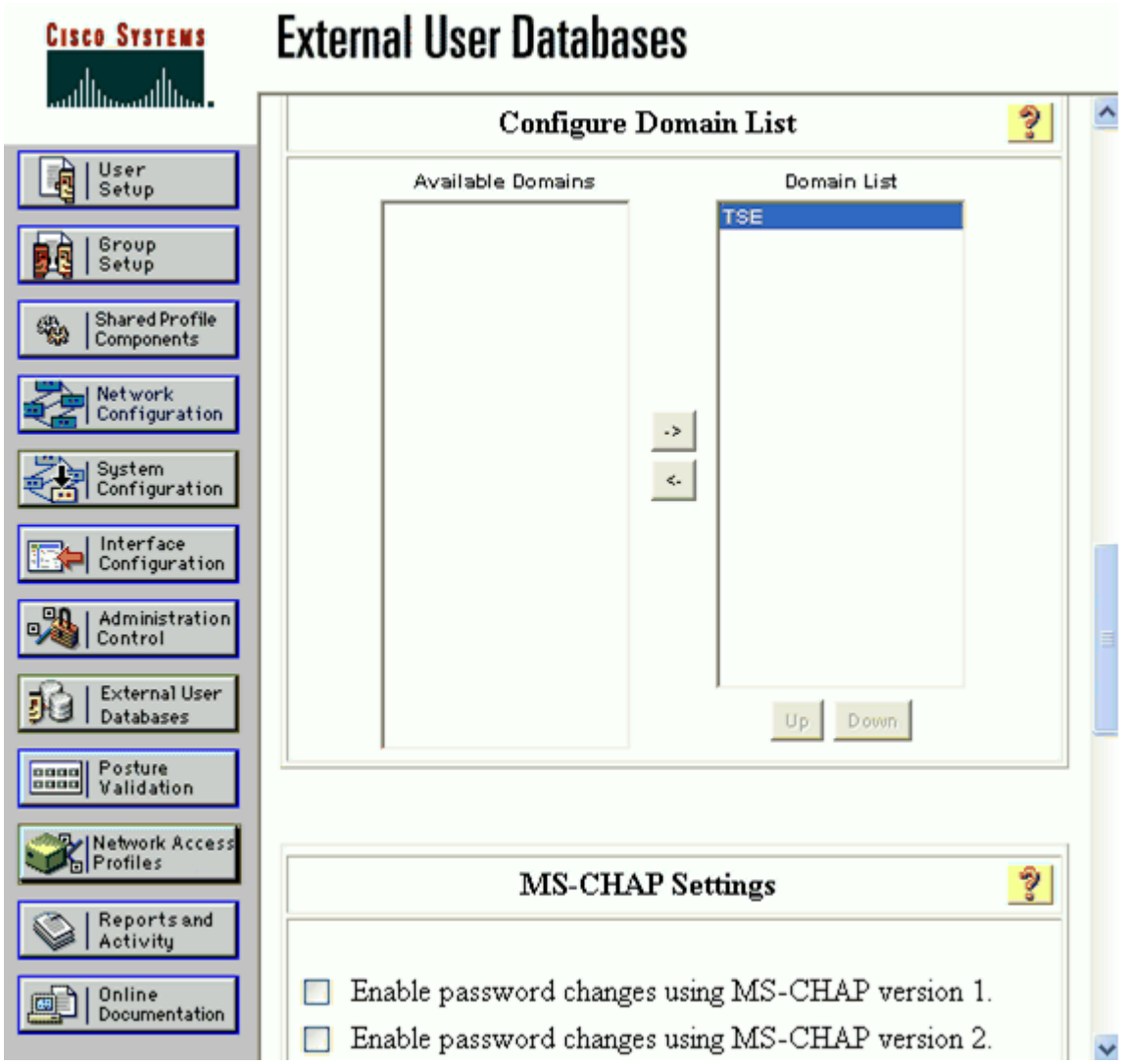
図 4-4　Windows データベースの設定の選択



Windows データベースの設定

Windows User Database Configuration メニューの Configure Domain List セクションにスクロールします。適切なドメイン名を選択して、Available Domains 列から Domain List 列に移動します。

図 4-5　Windows データベースの設定



次に、Machine Authentication セクションにスクロールして、Enable EAP-TLS Machine Authentication ボックスをオンにします。**Submit** をクリックします。

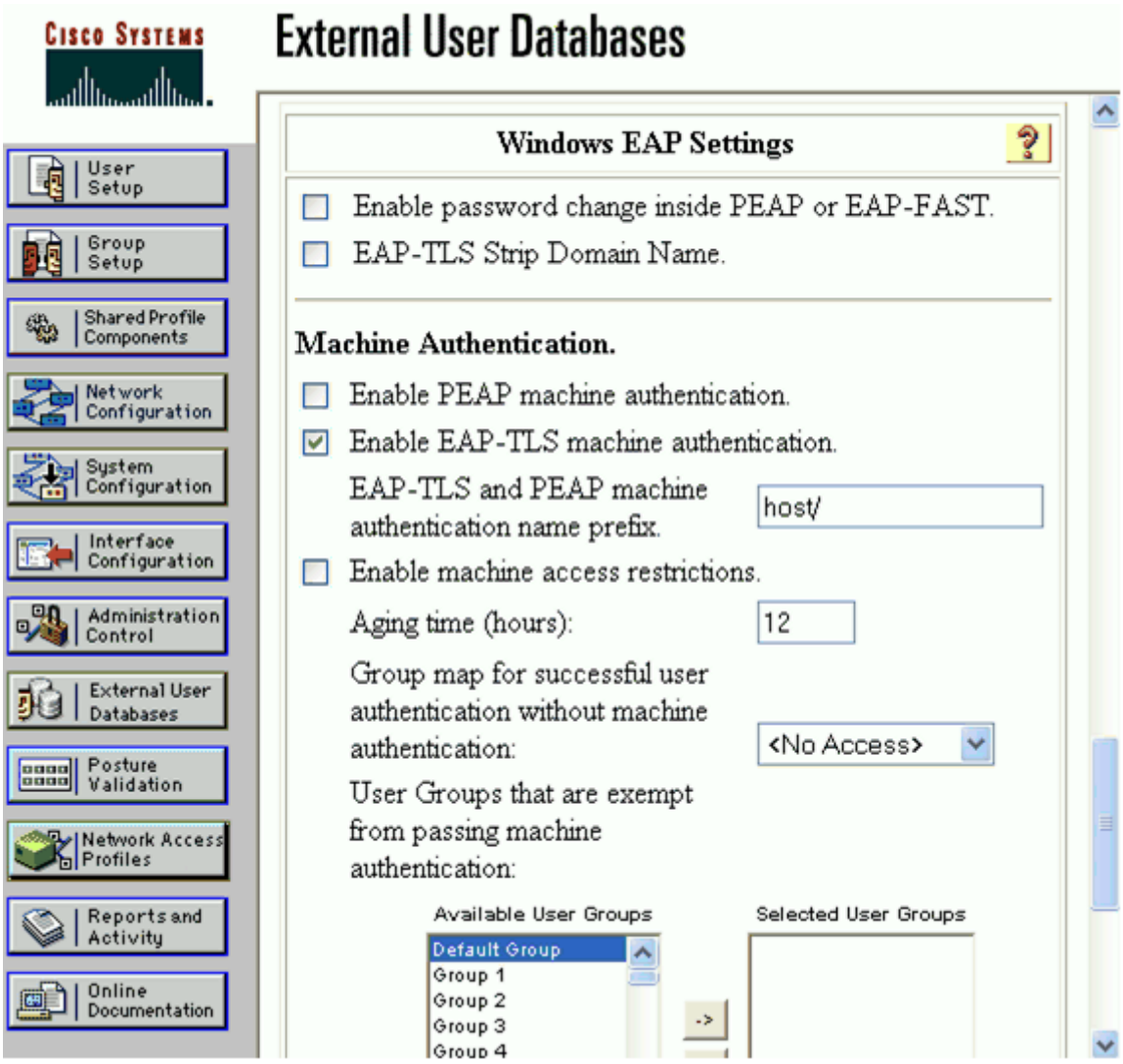
（注） EAP-TLS によるマシン証明書を使用して、マシン認証を有効にするには、Enable EAP-TLS machine authentication ボックスをオンにします。次の項では、マシン アカウント プロファイルを使用するようにサプリカントを設定するため、この例ではこのオプションを設定します。

このほかにも、複数のマシン認証オプションを設定できます。

- EAP-TLS Strip Domain Name：Cisco Secure ACS で、エンドユーザ証明書の Subject Alternative Name（SAN）フィールドから導き出されたユーザ名からドメイン名を削除するには、このチェックボックスをオンにします。
- EAP-TLS and PEAP machine authentication name prefix：管理者が Cisco Secure ACS で、PEAP（EAP-MSCHAPv2）または EAP-TLS で認証されているマシン名の先頭に文字列 host/ の代わりに別の文字列を使用する場合は、このボックスに文字列を入力します。

- Enable machine access restrictions：ユーザ認証の条件としてマシン認証を使用する場合は、このボックスをオンにします。マシン認証に失敗したコンピュータを使用してネットワークにアクセスする Microsoft PEAP および EAP-TLS ユーザは、通常は認証されますが、グループ マッピング リストで定義された認証のみを受信します。
- Group map for successful user authentication without machine authentication：マシン アクセス制限機能が有効になっている場合、このリストは、認証を通過し、マシン認証に失敗したコンピュータを使用する EAP-TLS または Microsoft PEAP ユーザに認証が適用される場合のユーザ グループを指定します。

図 4-6　EAP-TLS マシン認証の有効化



AAA サーバの設定

「AAA サーバの設定」(p.3-3) を参照してください。すべての EAP 方式で同じ手順が使用されます。

AAA クライアントの設定

「AAA クライアントの設定」（p.3-4）を参照してください。すべての EAP 方式で同じ手順が使用されます。

ネットワーク設定の確認

「ネットワーク設定の概要」（p.3-5）を参照してください。すべての EAP 方式で同じ手順が使用されます。

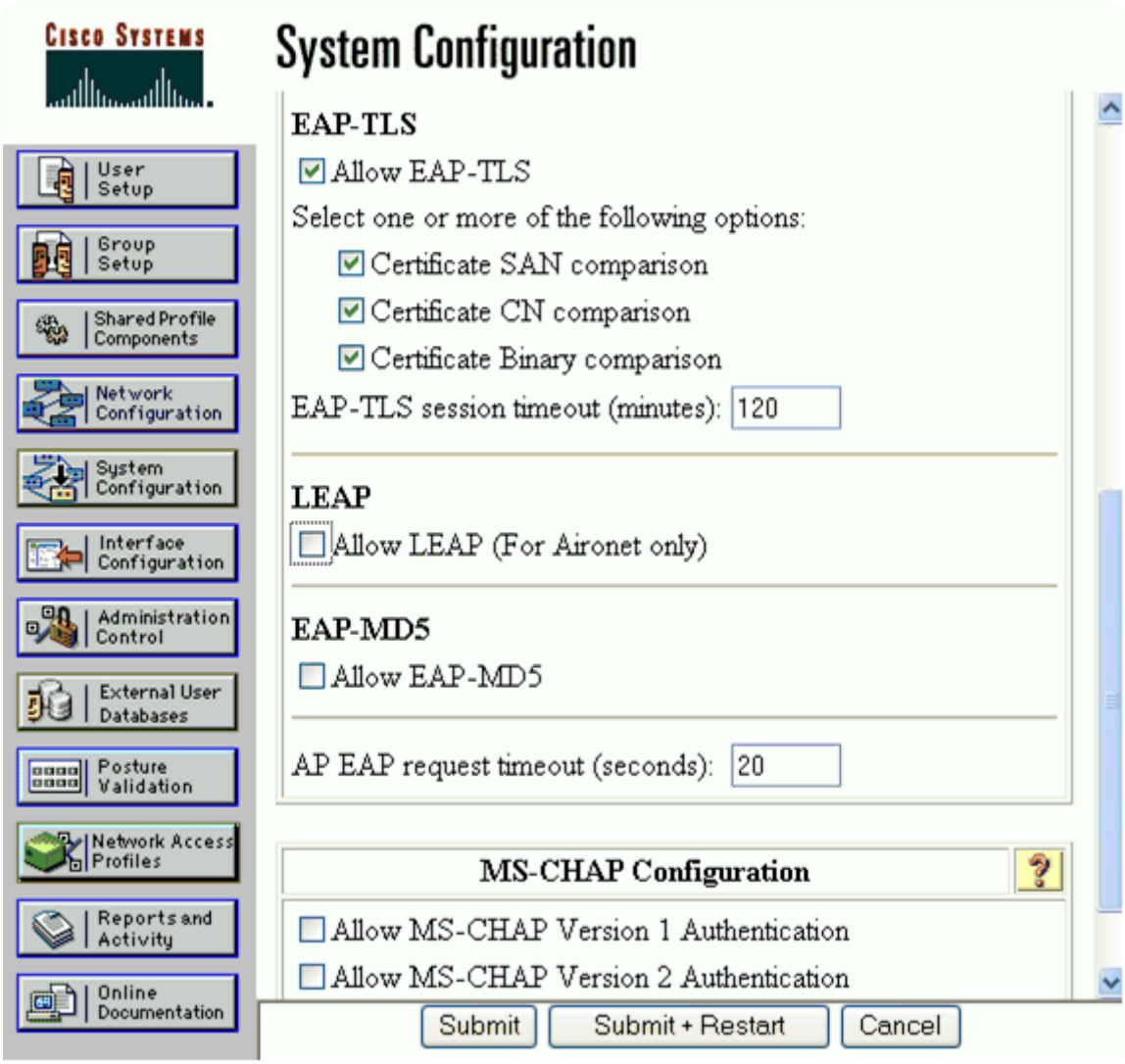
EAP-TLS のグローバル認証設定

メイン メニューで **System Configuration** をクリックします。System Configuration メニューで、Global Authentication Setup を選択して、EAP 方式を設定します。Allow EAP-TLS ボックス、および EAP-TLS セクションの 3 つの証明書比較オプションをすべてオンにします。**Submit + Restart** をクリックします。

（注） 証明書を CiscoSecure ACS にインストールする方法については、付録 C「CiscoSecure ACS での X.509v3 PKI 証明書のインストール」を参照してください。

（注） Certificate Comparison オプションは、ACS がエンドユーザ クライアントからの EAP Identity 応答に対してユーザ ID を確認する方法を指定します。ユーザ ID の確認は、エンドユーザ クライアントが提示した証明書の情報に対して行われます。この比較は、ACS とエンドユーザ クライアント間に EAP-TLS トンネルが確立されたあとに行われます。Certificate Comparison オプションには、エンドユーザ証明書の Subject Alternative Name フィールド、エンドユーザ証明書の Common Name フィールド、およびエンドユーザ証明書と Active Directory に格納されているエンドユーザ証明書とのバイナリ比較が含まれます。複数のオプションを選択した場合、ACS は表示されている順序で比較を実行し、最初に比較が成功した時点で停止します。

図 4-7　EAP-TLS のグローバル認証設定



クライアント設定

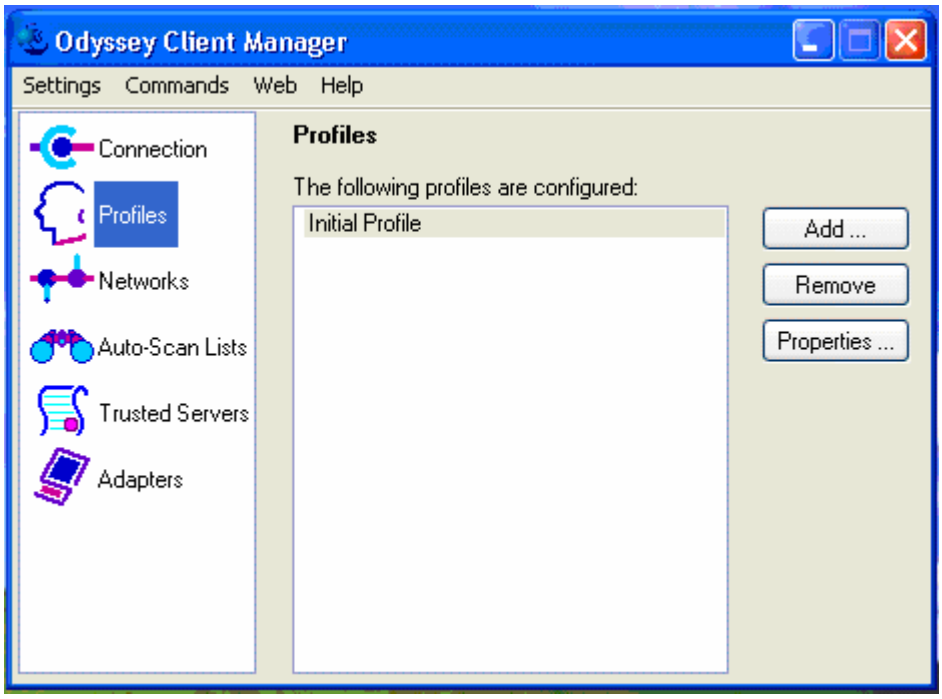
ここで示す手順は、EAP-TLS 認証用に Funk Odyssey クライアント バージョン 4.02.0.2000 を設定する方法について説明しています。

（注）　Funk Odyssey クライアントは、Service Pack 2 を適用した Windows XP オペレーティング システムで実行されています。

Funk Odyssey クライアントのオープン

Funk Odyssey クライアントを開き、**Authentication** メニューをクリックして、Authentication Profile を選択します。

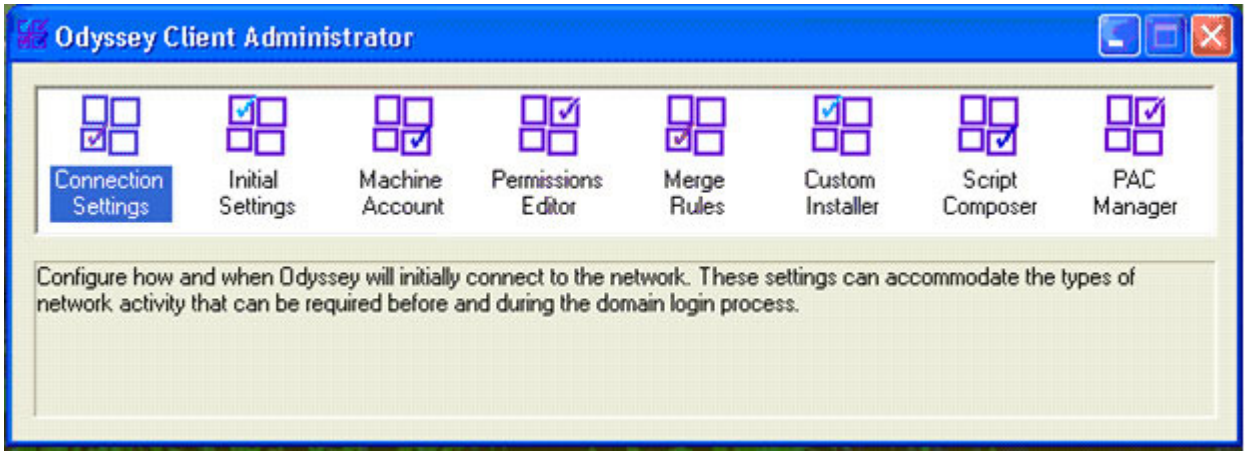
図 4-8　Funk Odyssey クライアント



Connection Settings の Machine Account パラメータの設定

マシン認証を設定するには、まず Connection Settings の Machine Account パラメータを設定する必要があります。Odyssey Client Manager メニューで、Settings、Odyssey Client Administrator の順に選択します。Odyssey Client Administrator メニューで、Connection Settings を選択します。

図 4-9　Odyssey Client Administrator メニューの Connection Settings の選択

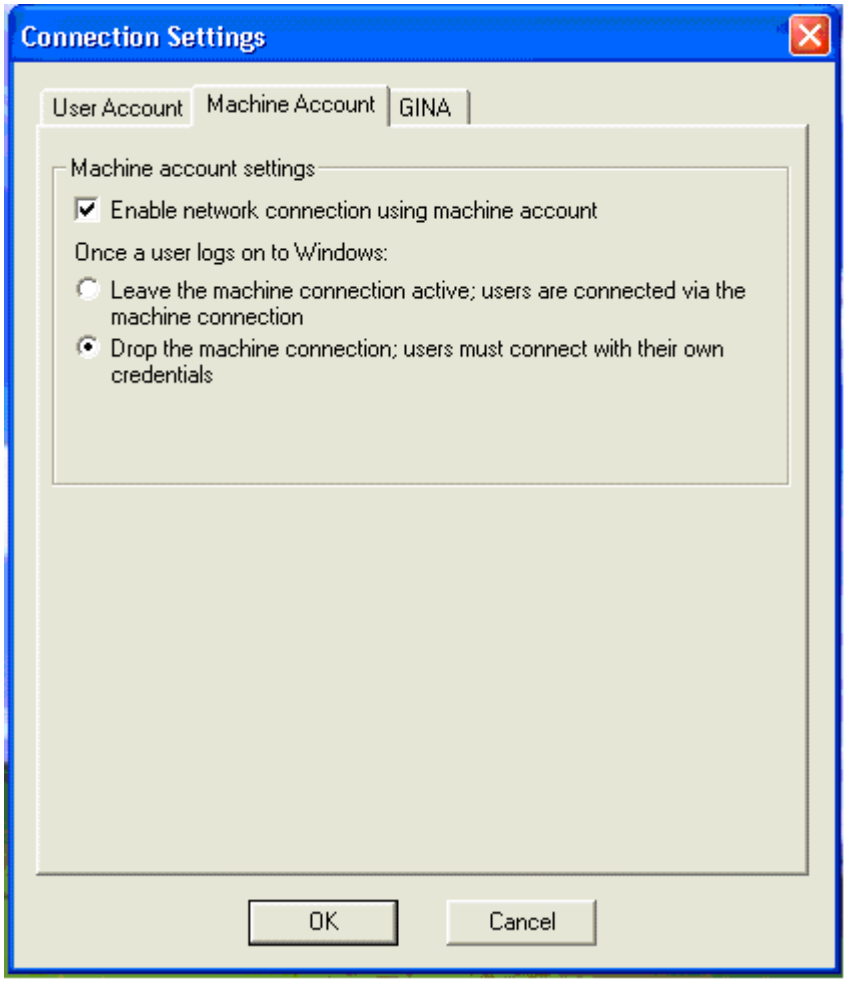


Connection Settings ウィンドウで、Machine Account タブを選択します。Machine account settings セクションで、Enable network connection using machine account ボックスをオンにします。次に、Drop the machine connection; users must connect with their own credentials オプション ボタンを選択します。**OK** をクリックします。

（注）　Drop the machine connection; users must connect with their own credentials オプションは、ユーザがシステムにログオンした際、マシン プロファイルではなくユーザ プロファイルを参照するようにクライアントに指示するため、管理者は個別のマシンだけでなく、個別のユーザも確認できます。

Connection Settings では、User Account と GINA の 2 つのオプション タブも設定できます。User Account タブは、ユーザ証明書に依存するネットワーク認証のタイミングを設定するために使用されます。GINA タブは、Odyssey GINA モジュールを設定するために使用されます。Odyssey GINA モジュールを使用すると、Windows XP または 2000 のユーザが、Windows ログオンの前に Windows ログオン証明書を使用してネットワークに接続できます（これは、ユーザがネットワーク接続を必要とする起動プロセスを使用する場合に便利です）。

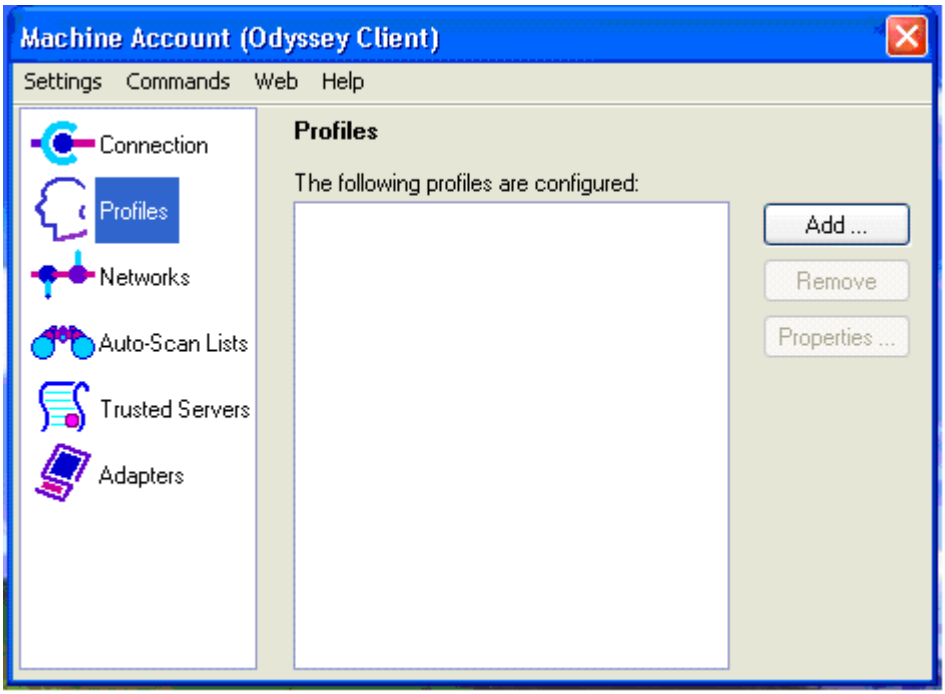
図 4-10　Connection Settings の Machine Account パラメータの設定



マシン プロファイルの作成

Odyssey Client Administrator メニューで、Machine Account を選択します。Machine Account (Odyssey Client) ウィンドウが表示されます。このウィンドウは、ユーザ プロファイルの作成に使用される Odyssey Client Manager ウィンドウに似ています。メニューの Profiles オプションを選択して、**Add** をクリックします。

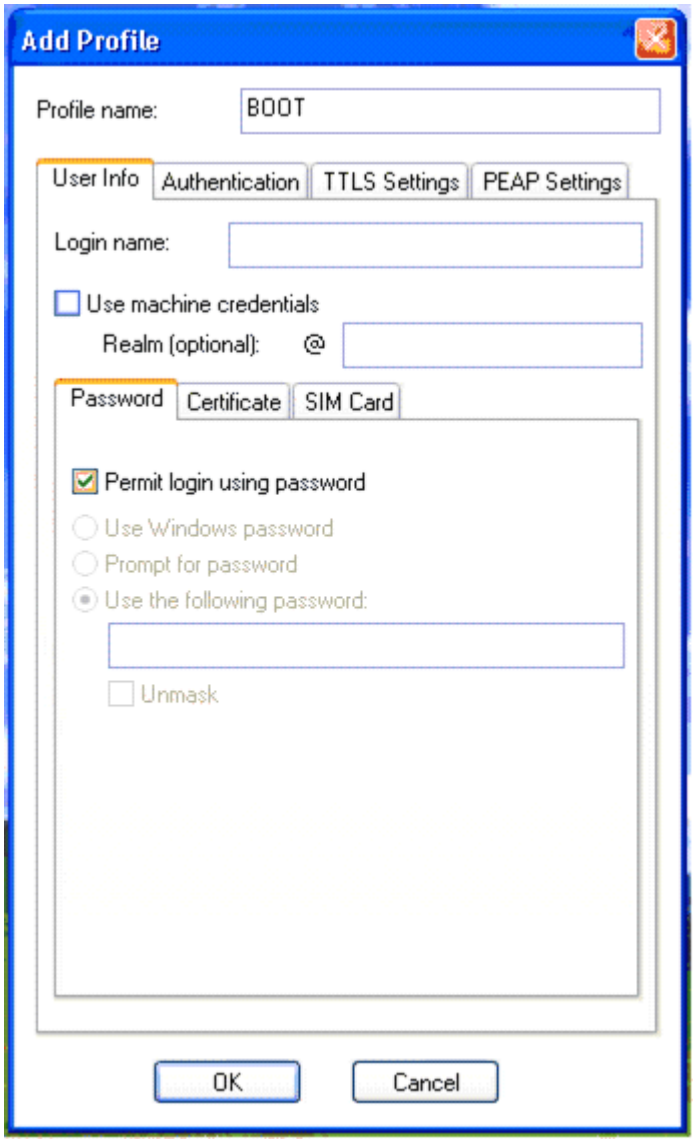
図 4-11　マシン プロファイルの作成



マシン プロファイルの認証情報の設定

Add Profile 画面で、プロファイルの名前を入力します。この例では、プロファイル名は BOOT です。User Info タブで、Use machine credentials ボックスをオンにします。User Info タブの下部にある Password タブで、デフォルト値をオンのままにしておきます。

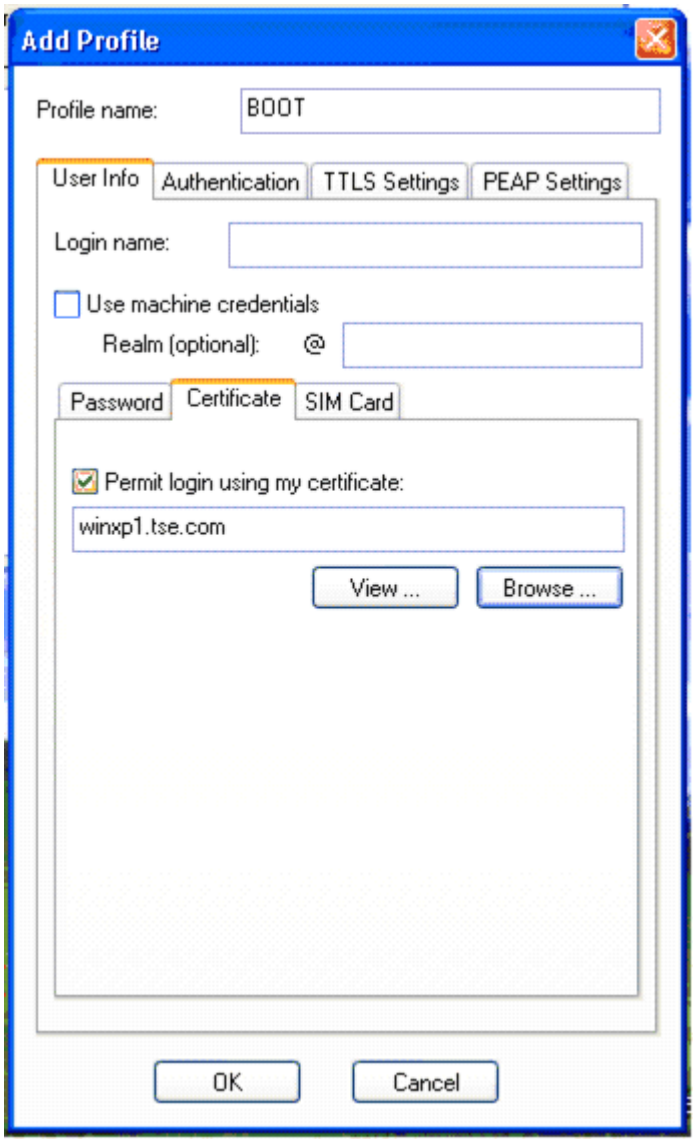
図 4-12　マシン プロファイルのパスワード情報の設定



次に、User Info タブの下部にある **Certificate** タブをクリックします。Permit login using my certificate ボックスをオンにします。次に、**Browse** タブをクリックして、マシンの適切な証明書を選択します。

（注）　証明書をクライアント　マシンにインストールする方法については、付録 B「クライアントでの X.509v3 PKI 証明書のインストール」を参照してください。

図 4-13　マシン プロファイルの証明書情報の設定



マシン プロファイルの認証方式の設定

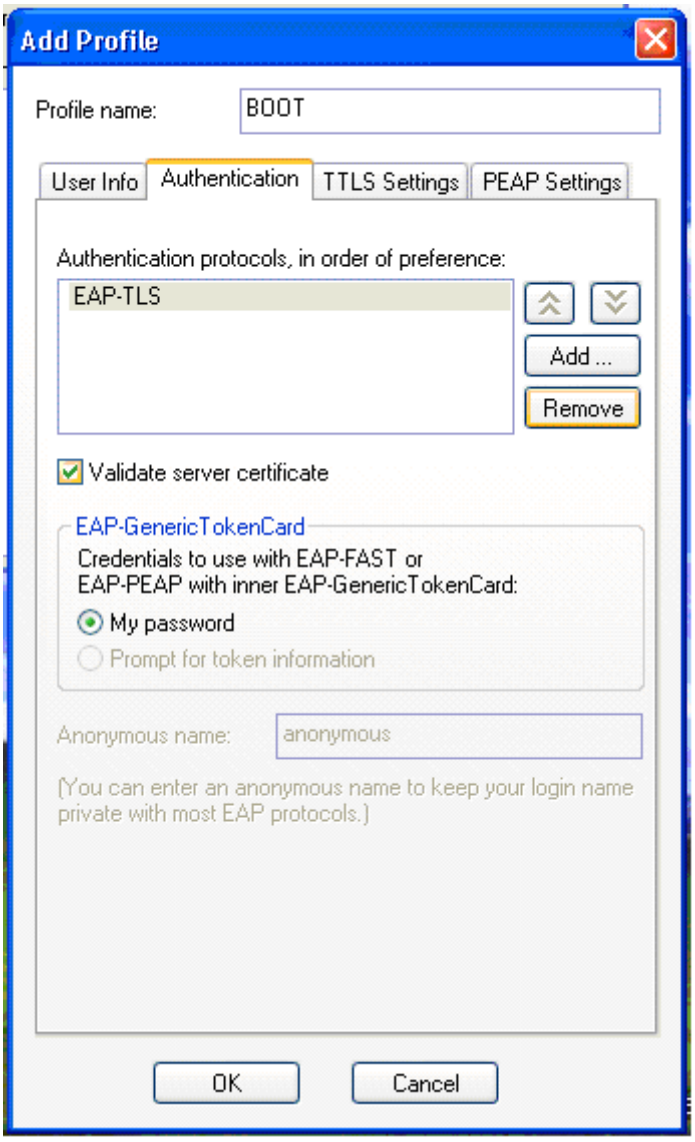
Authentication タブで、Authentication Protocols ボックスの隣にある **Add** をクリックします。EAP-TLS を選択して、**OK** をクリックします。次に、（認証プロトコルとしてデフォルトで表示されている）EAP-TTLS を選択して、**Remove** をクリックします。Validate server certificate ボックスをオンにします。

（注）　相互認証を有効にするには、Validate server certificate ボックスをオンにします（デフォルト）。この機能は、EAP-TTLS、PEAP、EAP-TLS などの特定のプロトコルで提供され、ユーザは、サーバがユーザ証明書に基づいてユーザ ID を確認するときに、認証サーバの ID を証明書に基づいて確認できます。User Profile セクションで同じオプションがオンになっています。

OK をクリックして、プロファイルを保存します。

（注）　EAP-GenericTokenCard セクションでオンになっているデフォルトのパラメータは無視してください。この情報は、PEAP および EAP-FAST のみに適用されます。

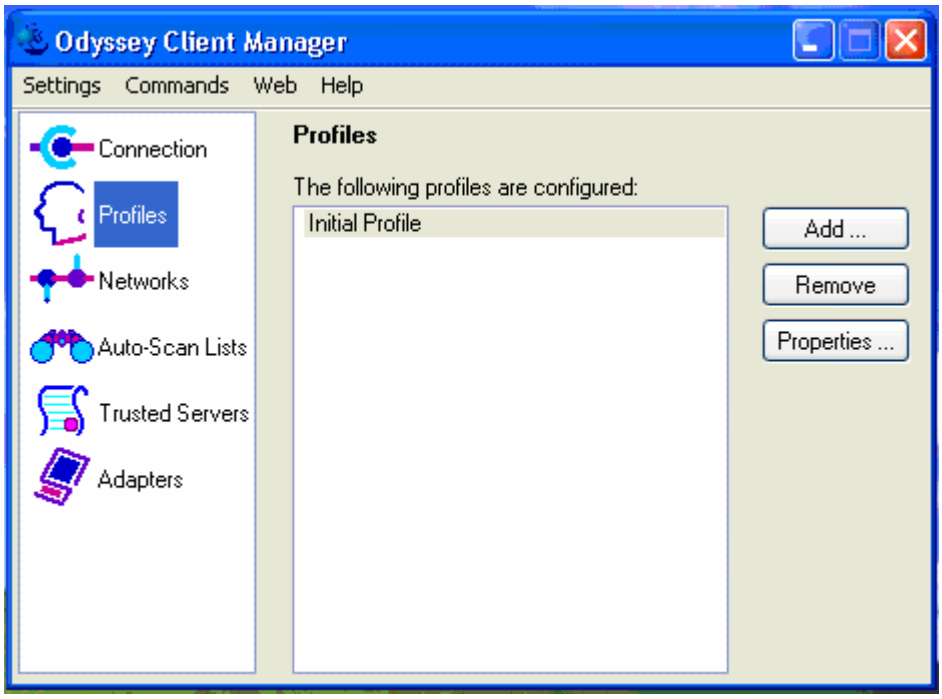
図 4-14　　マシン プロファイルの認証方式の設定



ユーザ プロファイルの作成

Funk Odyssey Client Manager で、左側のメニューの Profiles オプションを選択し、**Add** を選択して新しいユーザ プロファイルを作成します。

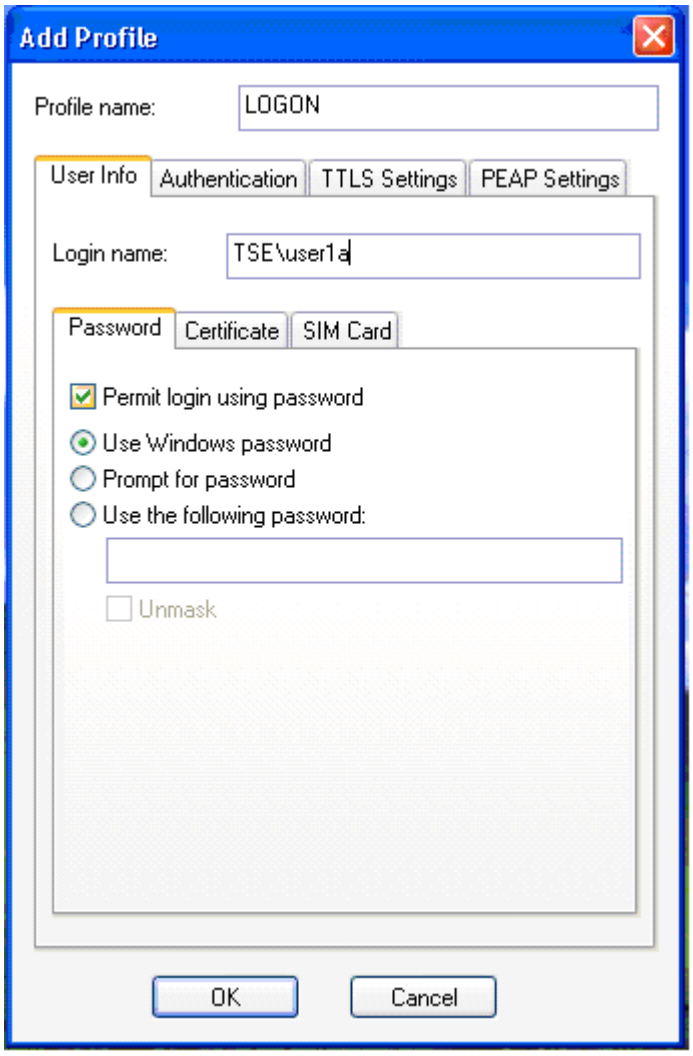
図 4-15　ユーザ プロファイルの作成



ユーザ プロファイルの認証情報の設定

Add Profile 画面で、プロファイルの名前を入力します。この例では、プロファイル名は LOGON です。User Info タブで、現在マシンにログインしているユーザの名前とドメインが Login name に自動的に読み込まれます。User Info タブの下部にある Password タブで、デフォルト値の Permit login using password および Use Windows password をオンのままにしておきます。

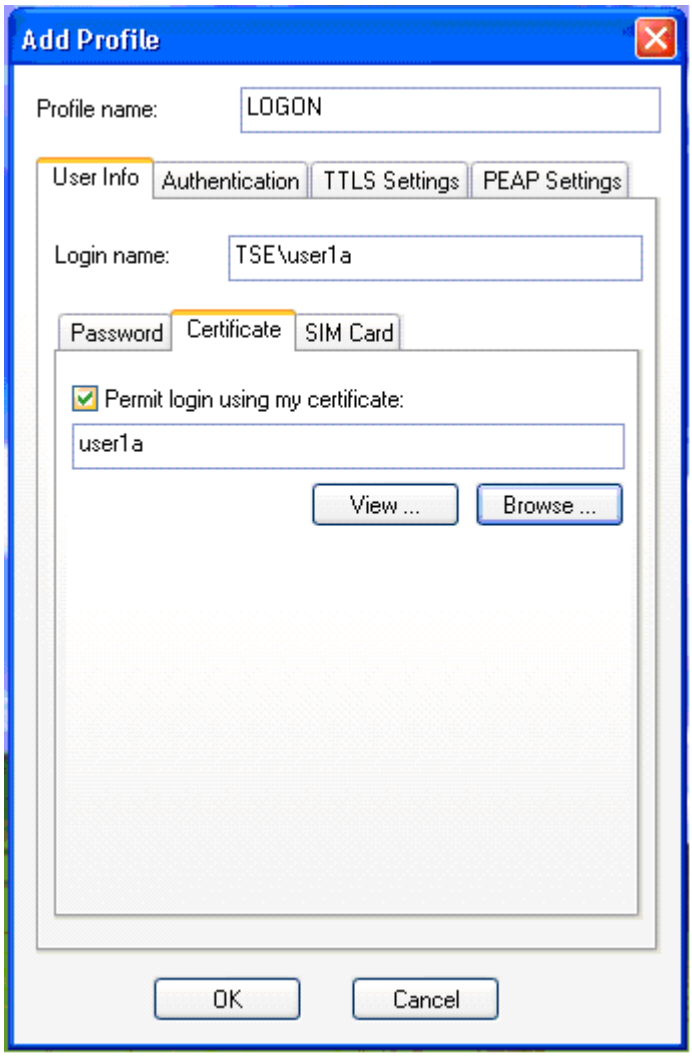
図 4-16　ユーザ プロファイルのパスワード情報の設定



次に、User Info タブの下部にある **Certificate** タブをクリックします。Permit login using my certificate ボックスをオンにします。次に、**Browse** タブをクリックして、現在のユーザの適切な証明書を選択します。

（注）　証明書をクライアント　マシンにインストールする方法については、付録 B「クライアントでの X.509v3 PKI 証明書のインストール」を参照してください。

図 4-17　ユーザ プロファイルの証明書情報の設定

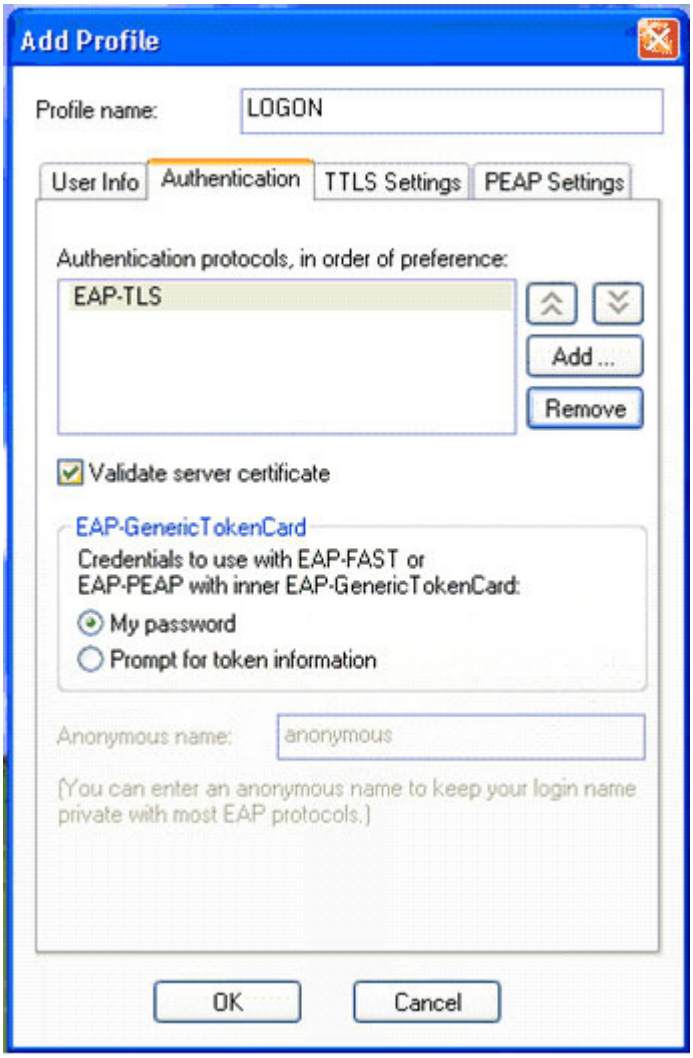


ユーザ プロファイルの認証方式の設定

Authentication タブで、Authentication Protocols ボックスの隣にある **Add** をクリックします。EAP-TLS を選択して、**OK** をクリックします。次に、（認証プロトコルとしてデフォルトで表示されている）EAP-TTLS を選択して、**Remove** をクリックします。Validate server certificate ボックスをオンにします。**OK** をクリックして、プロファイルを保存します。

（注）　EAP-GenericTokenCard セクションでオンになっているデフォルトのパラメータは無視してください。この情報は、PEAP および EAP-FAST のみに適用されます。

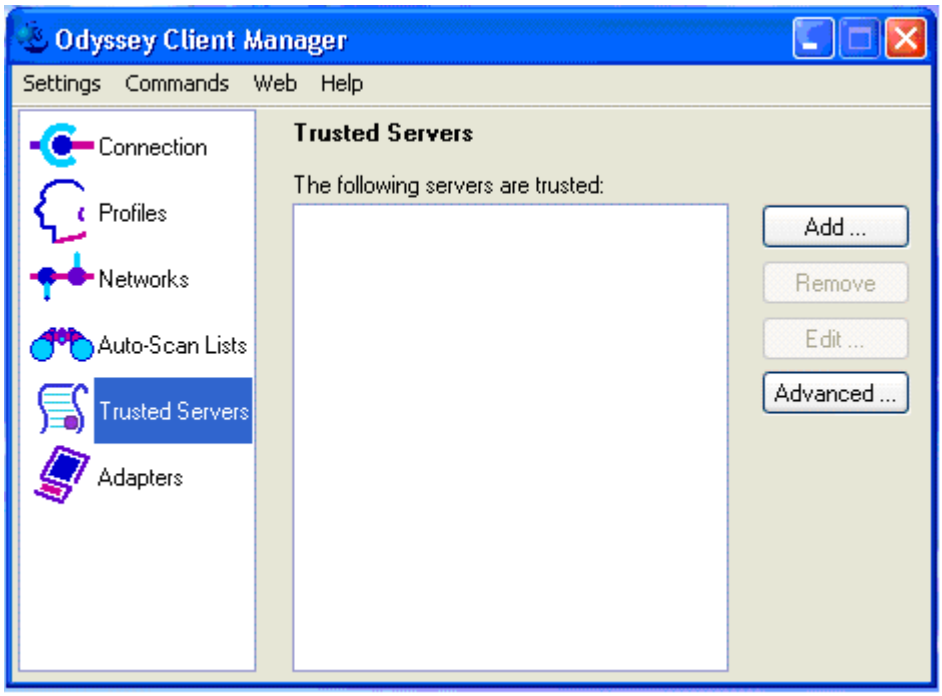
図 4-18　ユーザ プロファイルの認証方式の設定



信頼されたサーバの追加

Funk Odyssey Client Manager で、左側のメニューの Trusted Servers オプションを選択し、**Add** をクリックして新規の信頼されたサーバ エントリを作成します。

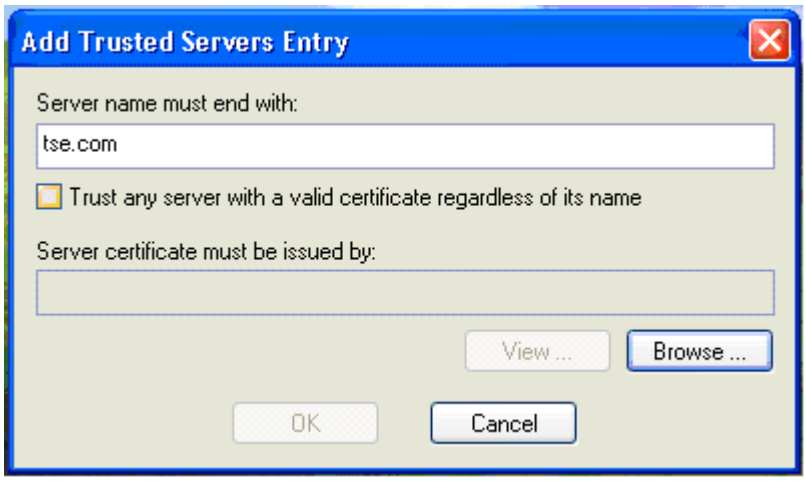
図 4-19　信頼されたサーバの追加



信頼されたサーバ エントリの設定

Server name must end with テキスト ボックスにドメイン名を追加します。この例では、tse.com ドメインが使用されています。

図 4-20　信頼されたサーバ エントリの設定

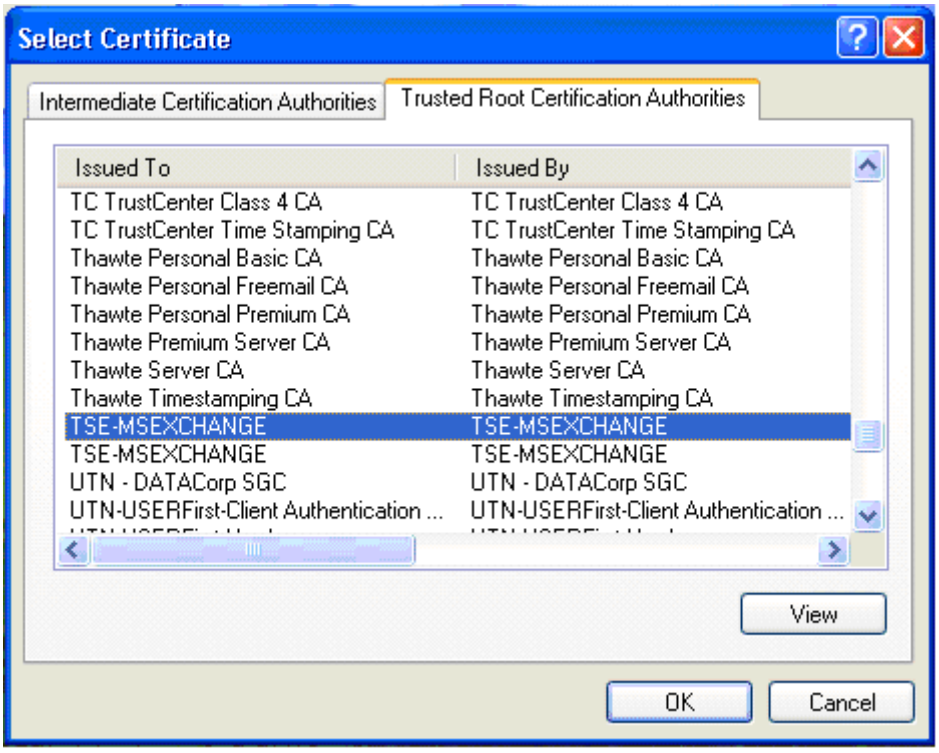


（注）　Trust any server with a valid certificate regardless of its name ボックスをオンにして、信頼されたサーバのドメイン名を入力することもできます。これにより、指定された署名付き証明書を持つすべてのサーバを信頼できます。

信頼されたルート認証局の選択

Add Trusted Servers Entry ウィンドウの **Browse** をクリックして、Server certificate must be issued by オプションの値を選択します。Select Certificate ウィンドウの **Trusted Root Certification Authorities** タブをクリックします。証明書を発行した認証局を選択します。**OK** をクリックします。

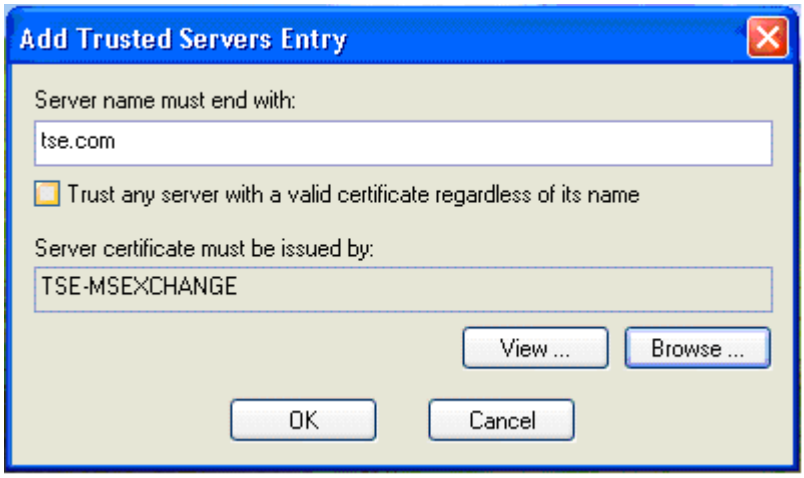
図 4-21　信頼されたルート認証局の選択



信頼されたサーバ エントリの保存

Add Trusted Servers Entry ウィンドウで **OK** をクリックして、信頼されたサーバ エントリの設定を保存します。

図 4-22　信頼されたサーバ エントリの保存

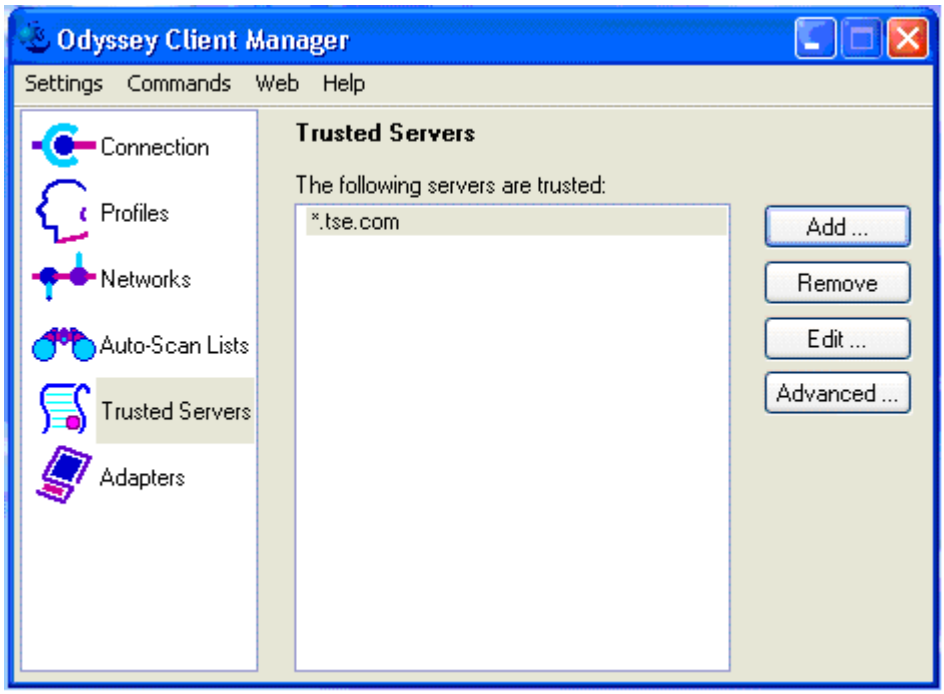


信頼されたサーバの確認

信頼されたサーバが設定されると、Trusted Servers リストにエントリが表示されます。

（注）　信頼されたサーバを最初に追加すると、管理ドメイン内のユーザは、ネットワークへのアクセス時に信頼性を有効にする必要がありません。

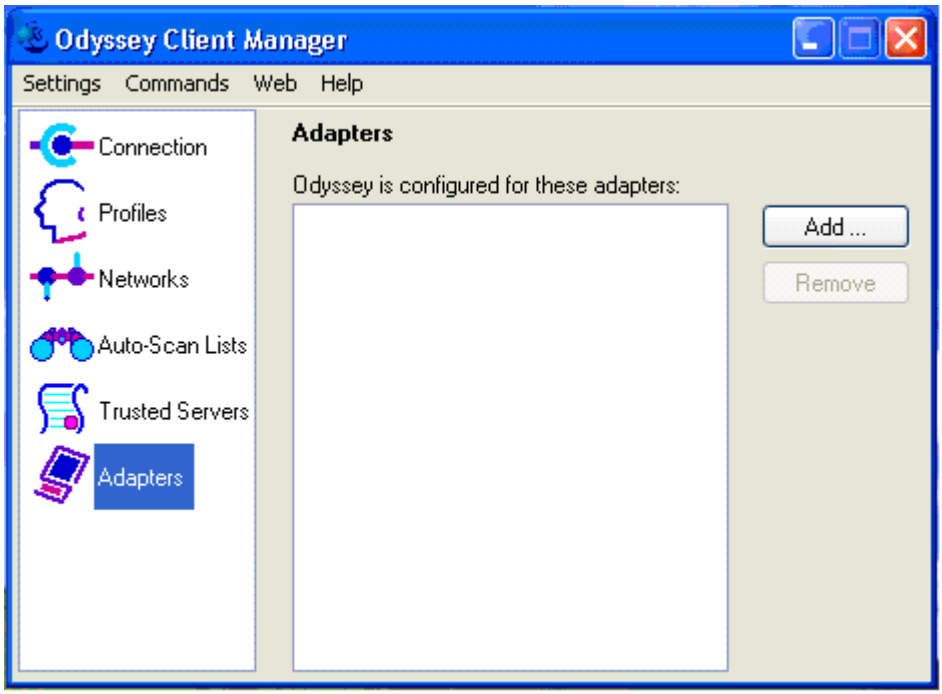
図 4-23　信頼されたサーバの確認



ユーザ プロファイルへのアダプタの適用

Funk Odyssey Client Manager メイン メニューで、Adapters オプションを選択します。**Add** をクリックします。

図 4-24　　ユーザ プロファイルへのアダプタの適用



ユーザ プロファイルへのアダプタの追加

この例では、有線接続が使用されます。適切なアダプタを選択するには、**Wired 802.1X** タブをクリックし、適切なイーサネット アダプタを選択します。**OK** をクリックします。

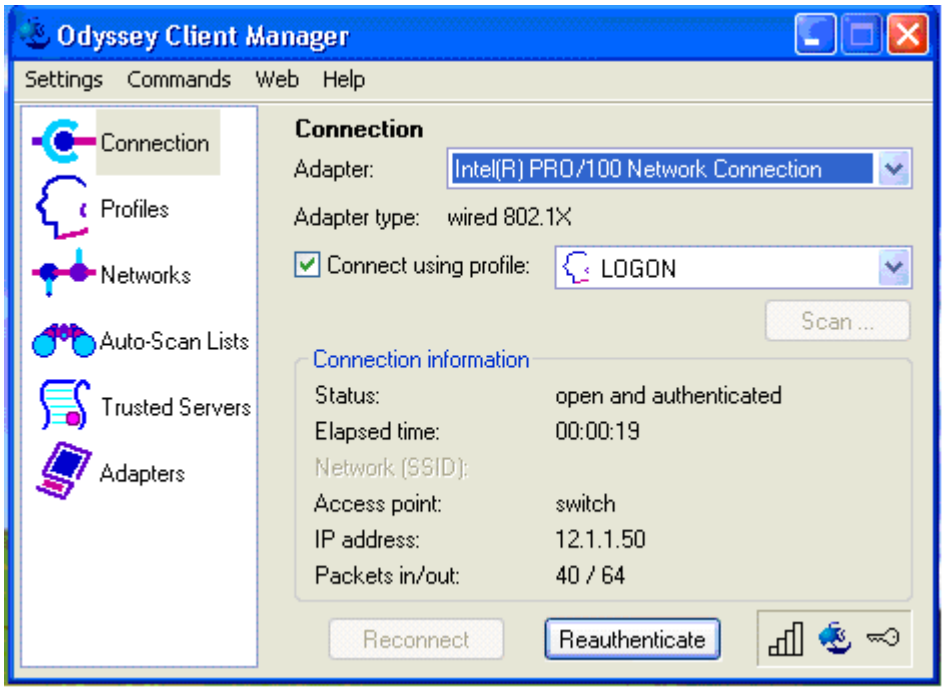
図 4-25　ユーザ プロファイルへのアダプタの追加

ユーザ プロファイルのネットワーク接続の確認

Funk Odyssey Client Manager メイン メニューで、Connection オプションを選択します。Adapter ドロップダウン メニューから、適切なアダプタが選択されていることを確認します。Connect using profile ボックスをオンにして、前述の手順で作成した LOGON プロファイルをドロップダウン メニューから選択します。

クライアントが EAP-TLS を介して IEEE 802.1X 認証を通過すると、Connection information セクションに表示されるステータスが open and authenticated に変わります。

図 4-26　ユーザ プロファイルのネットワーク接続の確認



CHAPTER 5

PEAP（EAP-MSCHAPv2）の展開

この章では、サプリカントと認証サーバ間で PEAP（EAP-MSCHAPv2）を使用して、IEEE 802.1X ポートベースのアクセス制御を展開する方法について説明します。この展開例のサプリカントとして、ネイティブの Microsoft Windows XP クライアントを使用します。Cisco Secure ACS 4.0 は、認証サーバとして使用されます。Cisco Catalyst スイッチはオーセンティケータとして機能し、サプリカントと認証サーバ間に有線 LAN 接続を提供します。

認証サーバの設定

ここで示す手順は、PEAP（EAP-MSCHAPv2）認証用に Cisco Secure ACS 4.0 を設定する方法について説明しています。

（注） ここでは、PEAP（EAP-MSCHAPv2）認証の設定に必要な手順についてのみ説明します。その他の機能の詳細については、『*Cisco Secure ACS Configuration Guide*』を参照してください。

外部ユーザ データベースの作成

「不明なユーザ ポリシーの作成」（p.4-1）を参照してください。手順は PEAP（EAP-MSCHAPv2）の場合も同じです。

（注） PEAP では、Windows Active Directory などの外部ユーザ データベースを使用する必要はありません。この EAP 方式では、内部 ACS データベースを使用できます。

外部ユーザ データベースの設定

「不明なユーザ ポリシーの設定」（p.4-2）を参照してください。手順は PEAP（EAP-MSCHAPv2）の場合も同じです。

外部ユーザ データベースの選択

「外部ユーザ データベースの選択」（p.4-3）を参照してください。手順は PEAP（EAP-MSCHAPv2）の場合も同じです。

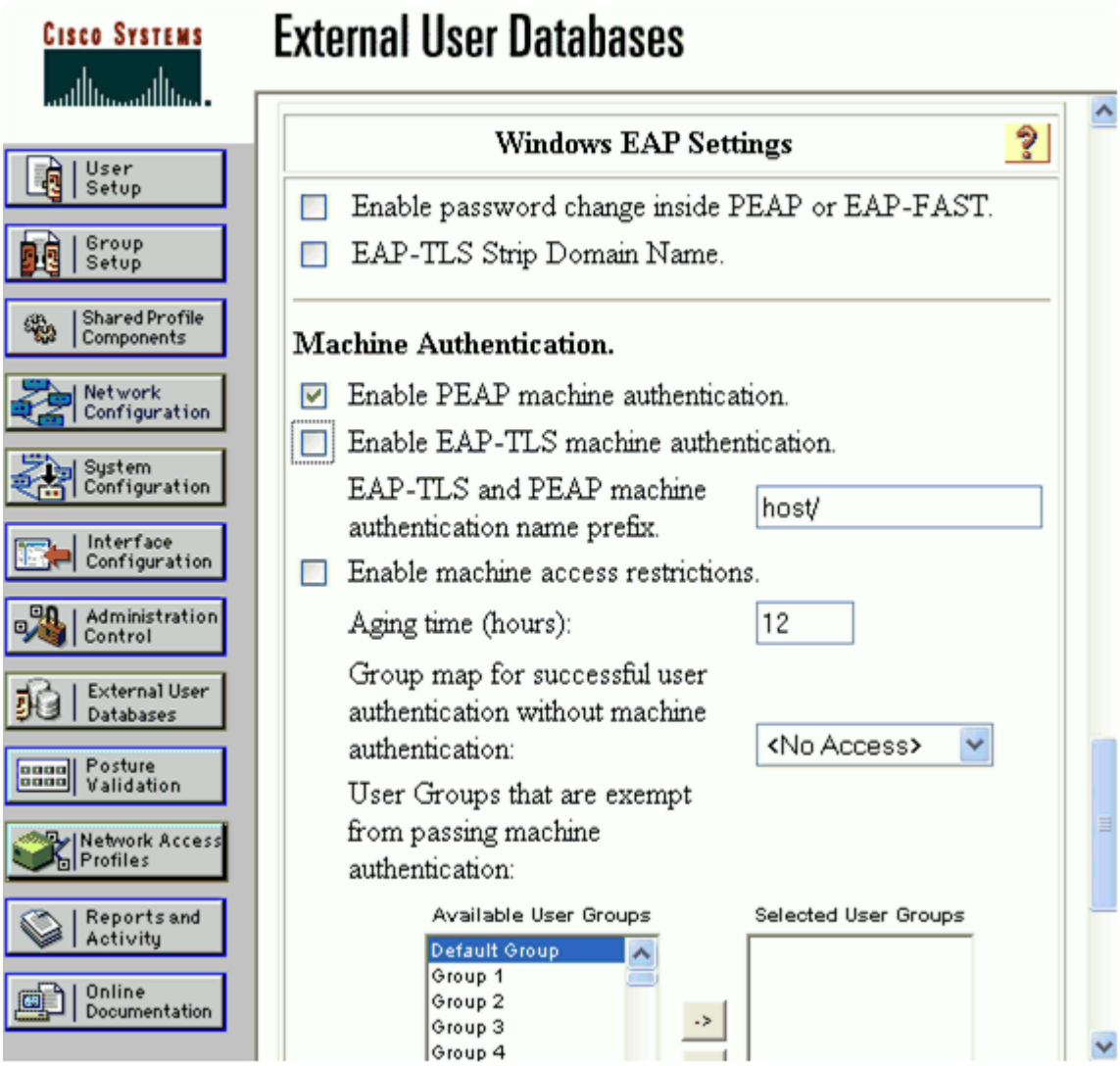
Windows データベースの設定の選択

「Windows データベースの設定の選択」(p.4-4) を参照してください。手順は PEAP（EAP-MSCHAPv2）の場合も同じです。

Windows データベースの設定

「Windows データベースの設定」(p.4-5) を参照してください。最初の手順は、PEAP（EAP-MSCHAPv2）の場合も同じです。最後の手順で、Machine Authentication セクションにスクロールして、Enable PEAP Machine Authentication ボックスをオンにします。**Submit** をクリックします。

図 5-1　PEAP マシン認証の有効化



AAA サーバの設定

「AAA サーバの設定」(p.3-3) を参照してください。すべての EAP 方式で同じ手順が使用されます。

AAA クライアントの設定

「AAA クライアントの設定」（p.3-4）を参照してください。すべての EAP 方式で同じ手順が使用されます。

ネットワーク設定の確認

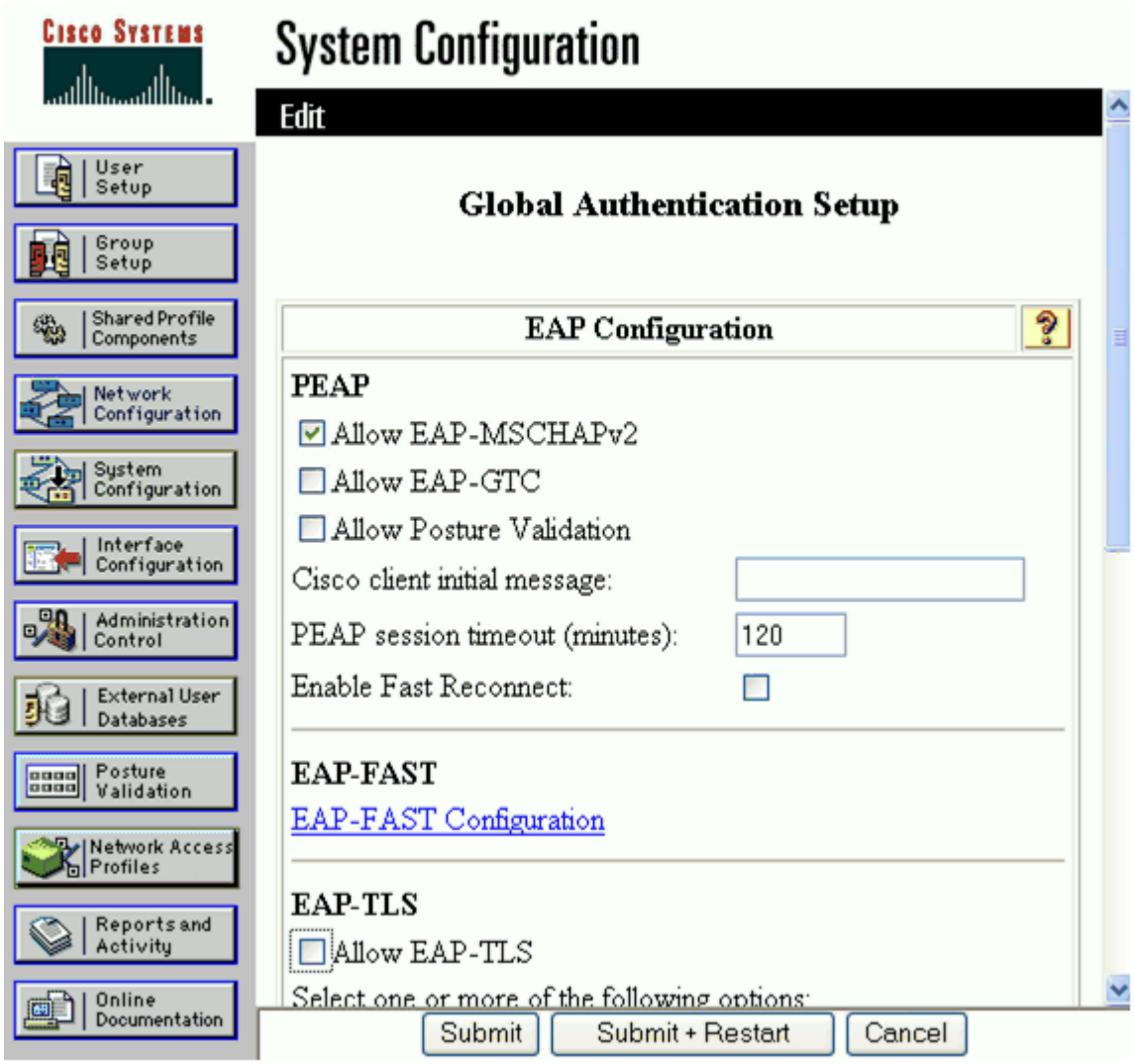
「ネットワーク設定の概要」（p.3-5）を参照してください。すべての EAP 方式で同じ手順が使用されます。

グローバル認証設定

メイン メニューで **System Configuration** をクリックします。System Configuration メニューから、Global Authentication Setup を選択して、EAP 方式を設定します。PEAP セクションの Allow EAP-MSCHAPv2 ボックスをオンにします。**Submit + Restart** をクリックします。

（注） PEAP 内部方式でオンになっているのは、Allow EAP-MSCHAPv2 ボックスのみです。これは、ネイティブの Windows XP SP2 IEEE 802.1X サプリカントの場合、この例で使用される唯一の方式であるためです。

図 5-2　PEAP のグローバル認証設定



クライアント設定

ここで示す手順は、PEAP（EAP-MSCHAPv2）認証用にネイティブの Microsoft Windows XP クライアントを設定する方法について説明しています。

（注）　ネイティブ クライアントは、Service Pack 2 を適用した Windows XP オペレーティング システムで実行されています。

ローカル エリア接続の IEEE 802.1X の有効化

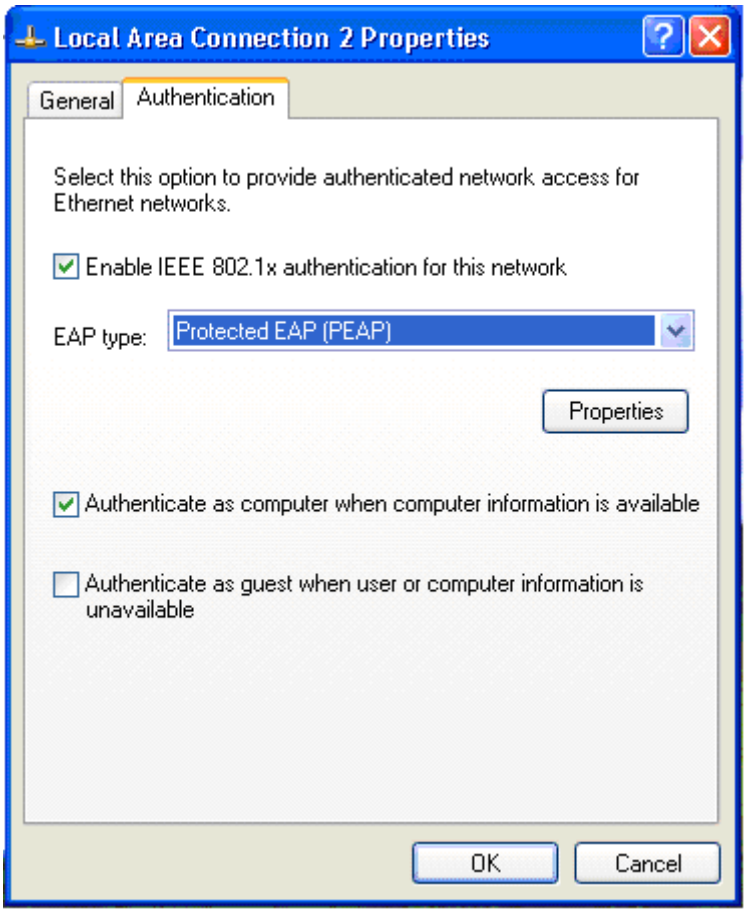
IEEE 802.1X パラメータを設定するには、**Start**、**Control Panel** の順にクリックし、Network and Internet Connections を選択します。次に、Network Connections を選択して、適切な Local Area Connection Properties メニューを開きます。

Local Area Connection Properties ウィンドウで、Authentication タブを選択します。Enable IEEE 802.1X authentication for this network ボックスをオンにします。EAP タイプのドロップダウン メニューから、Protected EAP (PEAP) を選択します。マシン認証を有効にしたあと、Active Directory ログイン期間全体を短縮するには、Authenticate as computer when computer information is available をオンにします。

（注）　企業の Active Directory ドメインへのログイン時間が短縮され、セキュリティ リスクも発生しないため、Authenticate as computer when computer information is available を使用することを推奨します。この機能がサプリカントと ACS の両方で有効になっている場合、ログイン画面が表示される前にマシン認証がすでに行われているため、企業の Active Directory ドメインへのログインに必要な時間が短縮されます。この機能がサプリカントで有効になっていて、ACS では有効になって**いない**場合、認証は失敗し、サプリカントのリブート時にポートは「保留」状態になります。サプリカントは、タイマーが期限切れになるまで待機し、ユーザ証明書で再認証を試行する必要があるため、ログイン時間が長くなる可能性があります。

（注）　現在、Authenticate as guest when user or computer information is unavailable チェックボックスの使用は推奨されていません。

図 5-3　　ローカル エリア接続の IEEE 802.1X 認証の有効化



PEAP プロパティの設定

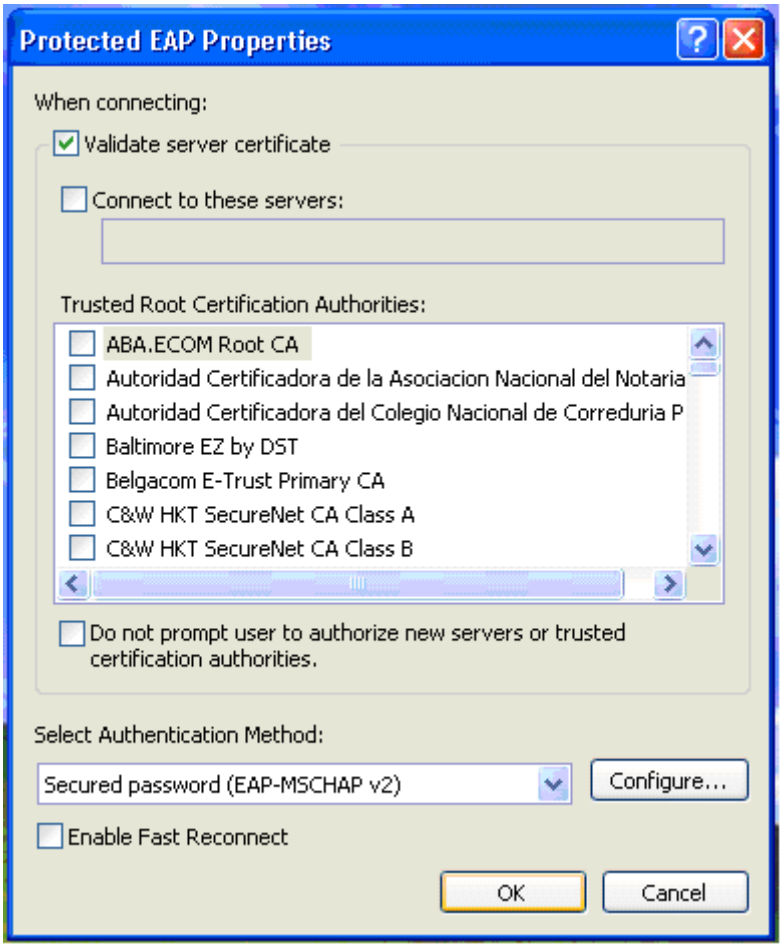
Protected EAP Properties メニューで、When connecting セクションの Validate server certificate ボックスをオンにします。この例では、Connect these servers ボックスをオンにしたり、Trusted Root Certification Authorities セクションのボックスをオンにする必要はありません。証明書はデスクトップ / ノート型 PC にすでにインストールされているため、認証局は Trusted Root Certification Authorities リストにすでに追加されています。

（注）　PEAP では、ユーザまたはコンピュータ（あるいはその両方）の証明書は不要ですが、認証サーバのみが、クライアントも信頼する必要がある有効な商用認証局からの証明書を必要とします。

Do not prompt user to authorize new servers or trusted certification authorities パラメータをオンにすると、ユーザがドメインの外部からネットワークにアクセスし、新規サーバまたは認証局を確認する必要があるときに、メッセージ画面を表示しないようにできます。

Enable Fast Reconnect パラメータを有効にすると、PEAP で TLS セッションを迅速に再開して、再認証を試行できます。PEAP Part 2 が成功した場合、RADIUS サーバは PEAP Part 1 で作成された TLS セッションをキャッシュできるため、PEAP Part 1 または PEAP Part 2 を再実行しなくてもセッションを再開できます。このオプションは、デフォルトで無効になっています。クライアントで有効にすると、このオプションを認証サーバでも設定する必要があります。無線 LAN 展開の場合、Enable Fast Reconnect のみを使用することを推奨します。

図 5-4　PEAP プロパティの設定



EAP-MSCHAPv2 プロパティの設定

Protected EAP Properties メニューで、Select Authentication Method セクションのドロップダウン メニューから Secured Password (EAP-MSCHAPv2) オプションを選択します。**Configure...** ボタンをクリックします。Automatically use my Windows logon name and password (and domain if any) ボックスがオンになっていることを確認します（ボックスはデフォルトでオンになっています）。**OK** をクリックします。

Protected EAP Properties ウィンドウで **OK** をクリックし、Local Area Connection ウィンドウで **OK** をクリックして、設定を保存します。

図 5-5　EAP-MSCHAPv2 プロパティの設定

CHAPTER 6

EAP-FAST の展開

この章では、サプリカントと認証サーバ間で EAP-FAST を使用して、IEEE 802.1X ポートベースのアクセス制御を展開する方法について説明します。この展開例のサプリカントとして、Cisco Aironet 無線 LAN クライアントを使用します。Cisco Secure ACS 4.0 は、認証サーバとして使用されます。Cisco Aironet 無線 LAN アクセス ポイントはオーセンティケータとして機能し、サプリカントと認証サーバ間に無線 LAN 接続を提供します。

認証サーバの設定

ここで示す手順は、EAP-FAST 認証用に Cisco Secure ACS 4.0 を設定する方法について説明しています。

（注） ここでは、EAP-FAST 認証の設定に必要な手順についてのみ説明します。その他の機能の詳細については、『*Cisco Secure ACS Configuration Guide*』を参照してください。

外部ユーザ データベースの作成

「不明なユーザ ポリシーの作成」（p.4-1）を参照してください。手順は EAP-FAST の場合も同じです。

（注） EAP-FAST では、Windows Active Directory などの外部ユーザ データベースを使用する必要はありません。この EAP 方式では、内部 ACS データベースを使用できます。

外部ユーザ データベースの設定

「不明なユーザ ポリシーの設定」（p.4-2）を参照してください。手順は EAP-FAST の場合も同じです。

外部ユーザ データベースの選択

「外部ユーザ データベースの選択」（p.4-3）を参照してください。手順は EAP-FAST の場合も同じです。

Windows データベースの設定の選択

「Windows データベースの設定の選択」（p.4-4）を参照してください。手順は EAP-FAST の場合も同じです。

Windows データベースの設定

「Windows データベースの設定」（p.4-5）を参照してください。最初の手順は、EAP-FAST の場合も同じです。Submit をクリックします。

AAA サーバの設定

「AAA サーバの設定」(p.3-3)を参照してください。すべての EAP 方式で同じ手順が使用されます。

AAA クライアントの設定

「AAA クライアントの設定」（p.3-4）を参照してください。すべての EAP 方式で同じ手順が使用されます。

ネットワーク設定の確認

「ネットワーク設定の概要」（p.3-5）を参照してください。すべての EAP 方式で同じ手順が使用されます。

グローバル認証設定

メイン メニューで **System Configuration** をクリックします。System Configuration メニューから、Global Authentication Setup を選択して、EAP 方式を設定します。EAP-FAST セクションにスクロールして、**EAP-FAST Configuration** をクリックします。

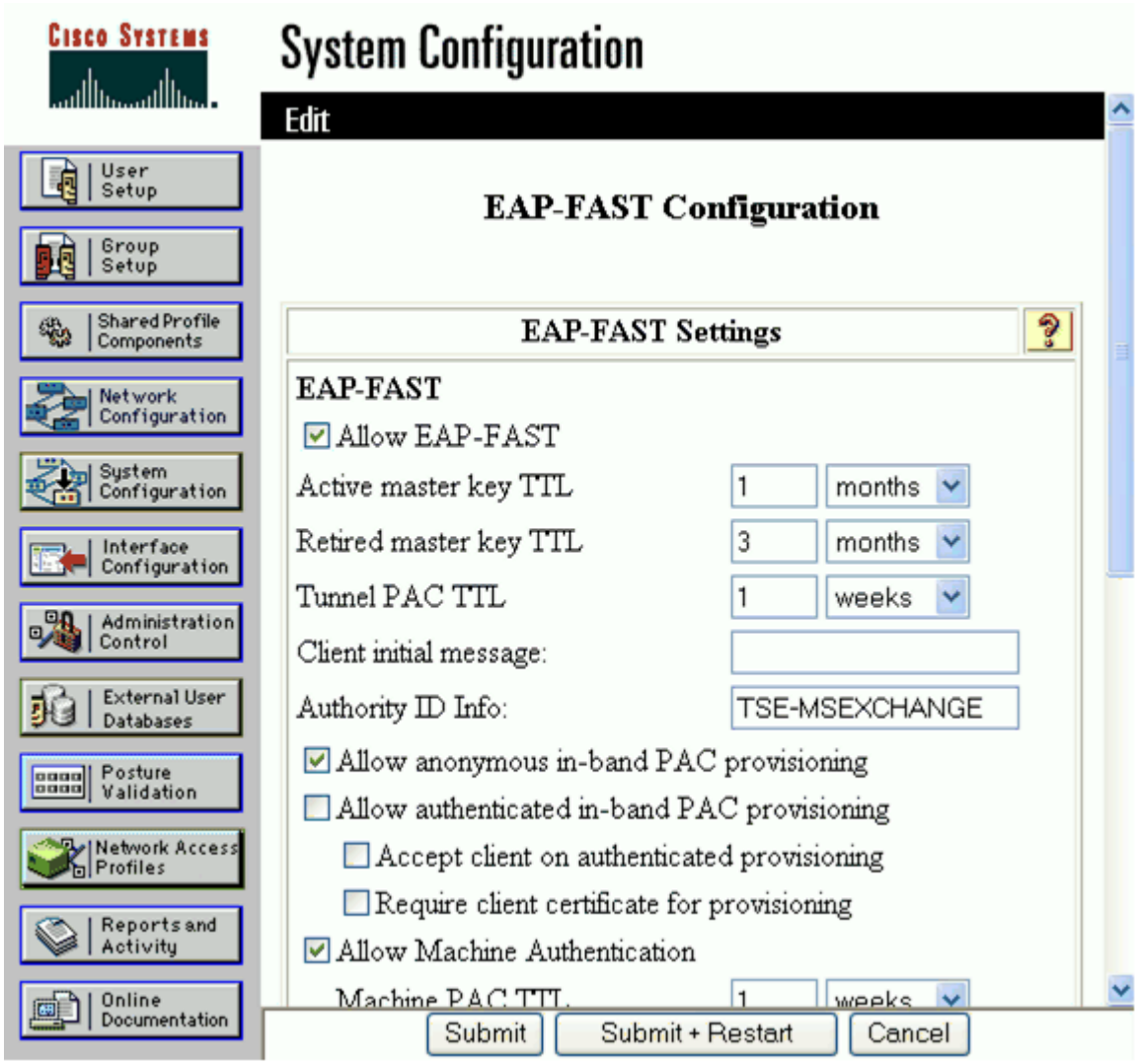
Allow EAP-FAST ボックスをオンにします。Active Master Key TTL、Retired Master Key TTL、および Tunnel PAC TTL は、デフォルト値のままにしておきます。Authority ID info テキスト ボックスに、ACS サーバの DNS ホスト名を入力します。

（注） Authority ID info は、認証される ACS サーバを決定するためにエンドユーザが使用できる、この ACS サーバのテキスト ID です。

Allow anonymous in-band PAC provisioning ボックスをオンにします。

（注） 匿名インバンド PAC プロビジョニングを有効にすると、クライアントに新しい PAC を提供する場合に、ACS がエンドユーザ クライアントとの安全な接続を確立できるようになります。このオプションにより、エンドユーザ クライアントと ACS の間で匿名 TLS ハンドシェイクが有効になります。

図 6-1　EAP-FAST のグローバル認証設定



Allow Machine Authentication ボックスをオンにして、Machine PAC TTL の設定をデフォルト値のままにしておきます。Allow Stateless Session Resume ボックスをオンにして、Authorization PAC TTL の設定をデフォルト値のままにしておきます。

（注）　通常は、Allow Stateless Session Resume ボックスをオンにしておく必要があります。これにより、ACS は EAP-FAST クライアントの許可済み PAC をプロビジョニングして、常に EAP-FAST のフェーズ 2 を実行できます。

Allowed Inner Methods で、1 つ以上のオプションをオンにして、EAP-FAST トンネル内で使用される EAP 方式を決定します。

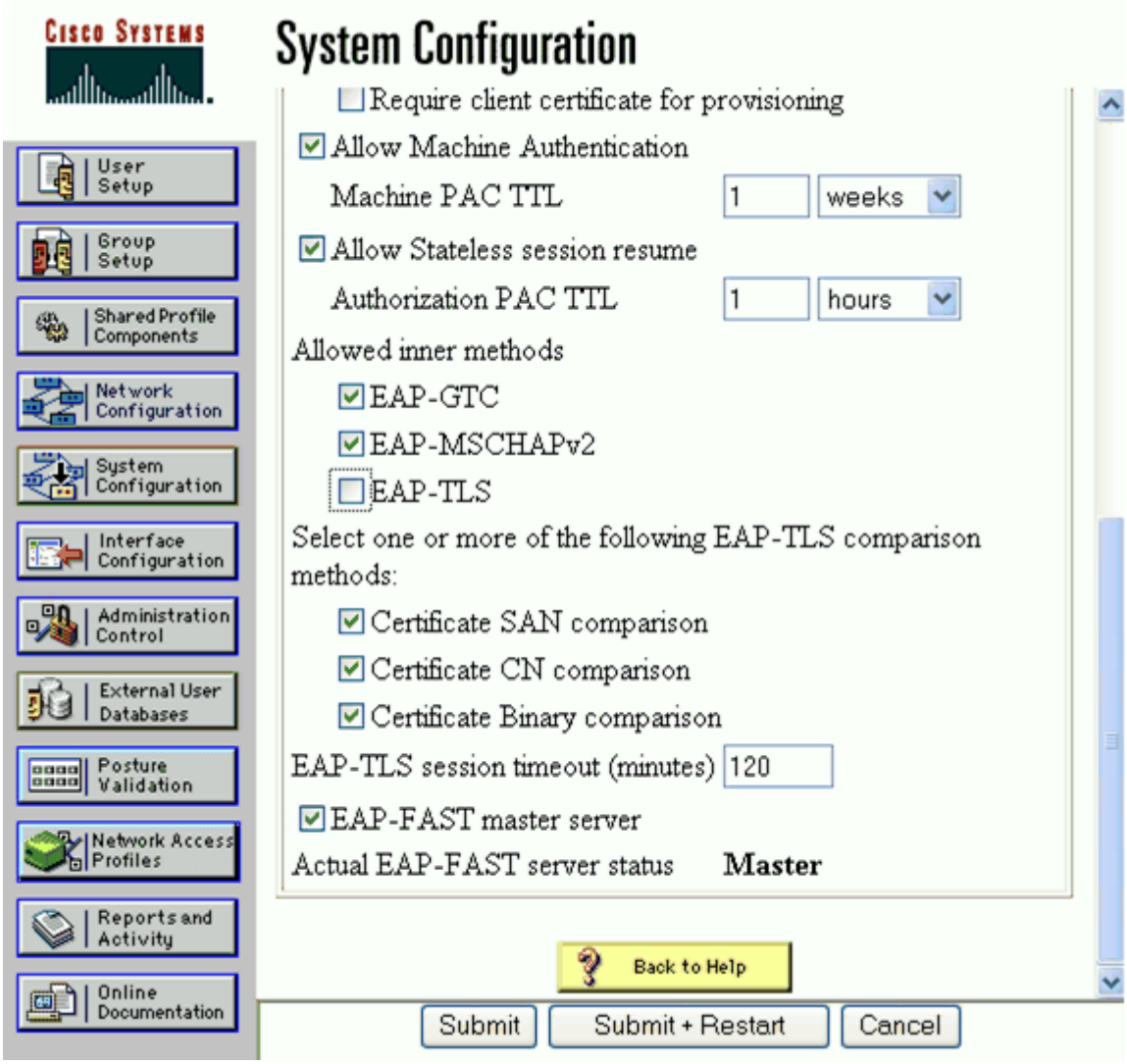
（注）　この例では Allow anonymous in-band PAC provisioning が使用されているため、EAP-MSCHAP を選択する必要があります。これは、EAP-FAST のフェーズ 0 で使用される唯一の内部方式であるためです。EAP-GTC も、EAP-FAST フェーズ 2 で使用されるためオンにする必要があります。

Select one or more of the following EAP-TLS comparison methods で、1 つ以上のオプションを選択します。EAP-FAST master server ボックスをオンにします。

（注）　EAP-FAST master server チェック ボックスをオンにすると、ACS が独自のマスター キーを作成して独自の EAP-FAST 設定を使用するかどうか、または複製された別の（スレーブまたは複製）ACS から受信した EAP-FAST 設定、マスター キー、および許可 ID を使用するかどうかが決まります。

Submit + Restart をクリックします。

図 6-2　EAP-FAST マシン認証の有効化と許可された内部方式の選択



クライアント設定

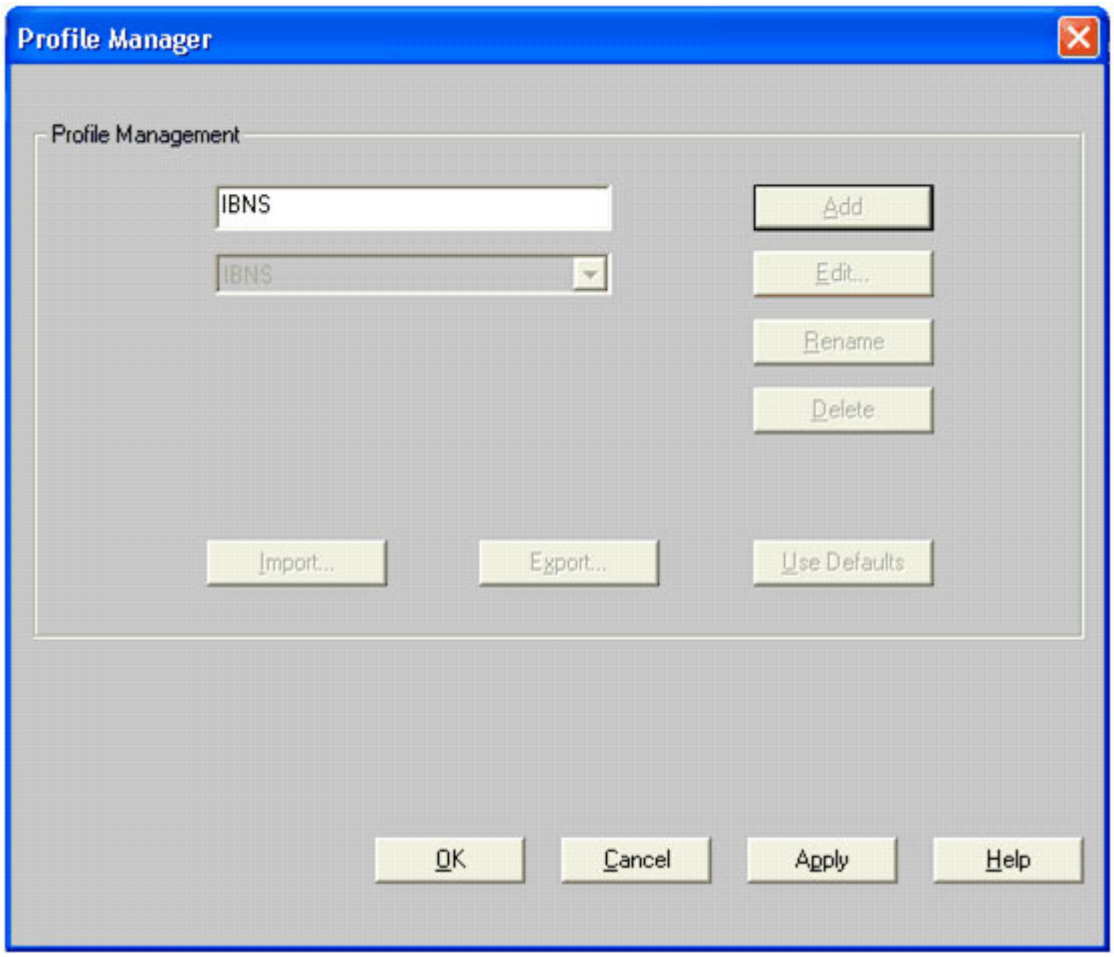
ここで示す手順は、EAP-FAST 認証用に Cisco Aironet 無線 LAN クライアントを設定する方法について説明しています。

（注）　Cisco Aironet 無線 LAN クライアントは、Service Pack 2 を適用した Windows XP オペレーティング システムで実行されています。

EAP-FAST のプロファイルの作成

Cisco Aironet 無線 LAN クライアント ユーティリティを開き、メイン メニューから Profile Manager を選択します。**Add** ボタンをクリックして、新しいプロファイルの名前を入力します。この例で使用するプロファイル名は IBNS です。**Apply** をクリックして、プロファイルを保存します。

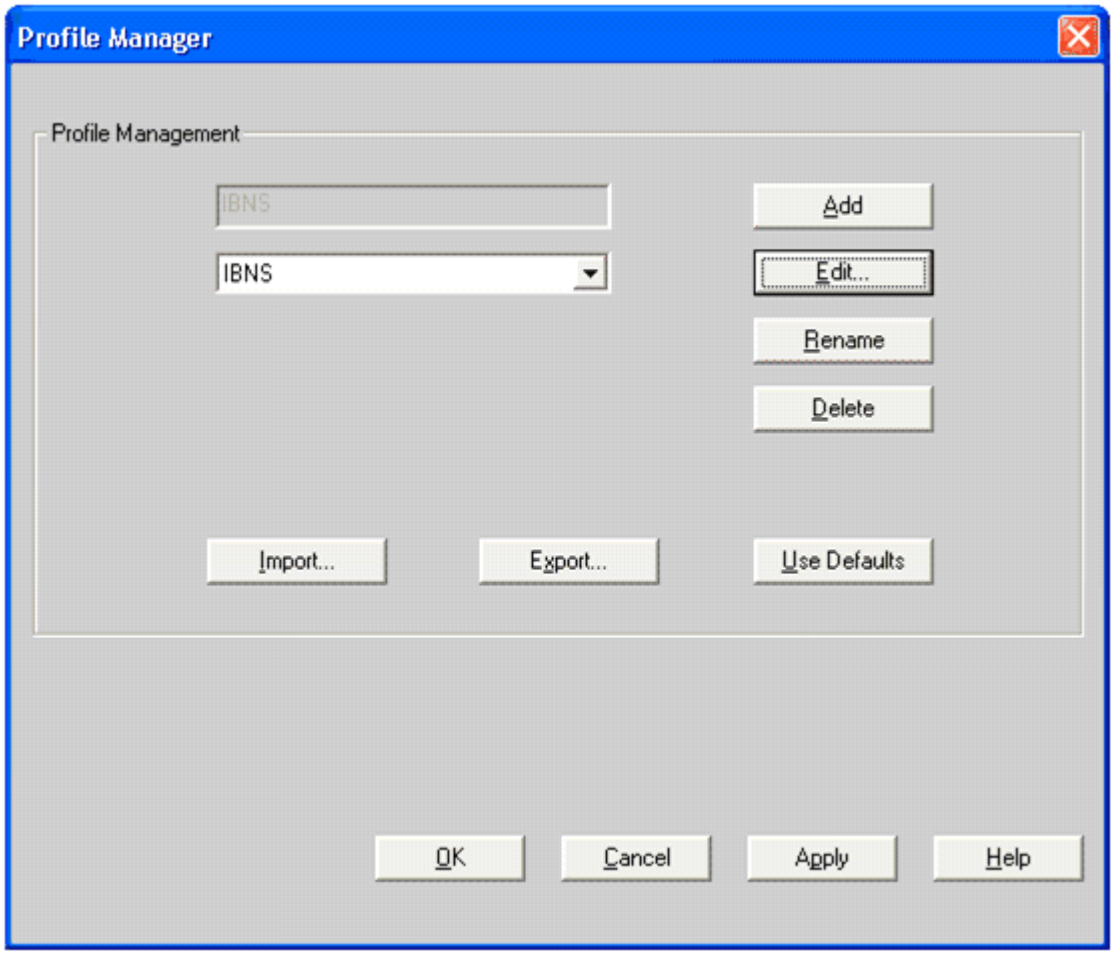
図 6-3　EAP-FAST のプロファイルの作成



プロファイル設定の編集

Profile Manager ウィンドウで、設定するプロファイルをドロップダウン ボックスから選択します。この例では、IBNS プロファイルを選択します。**Edit** をクリックして、プロファイル パラメータを設定します。

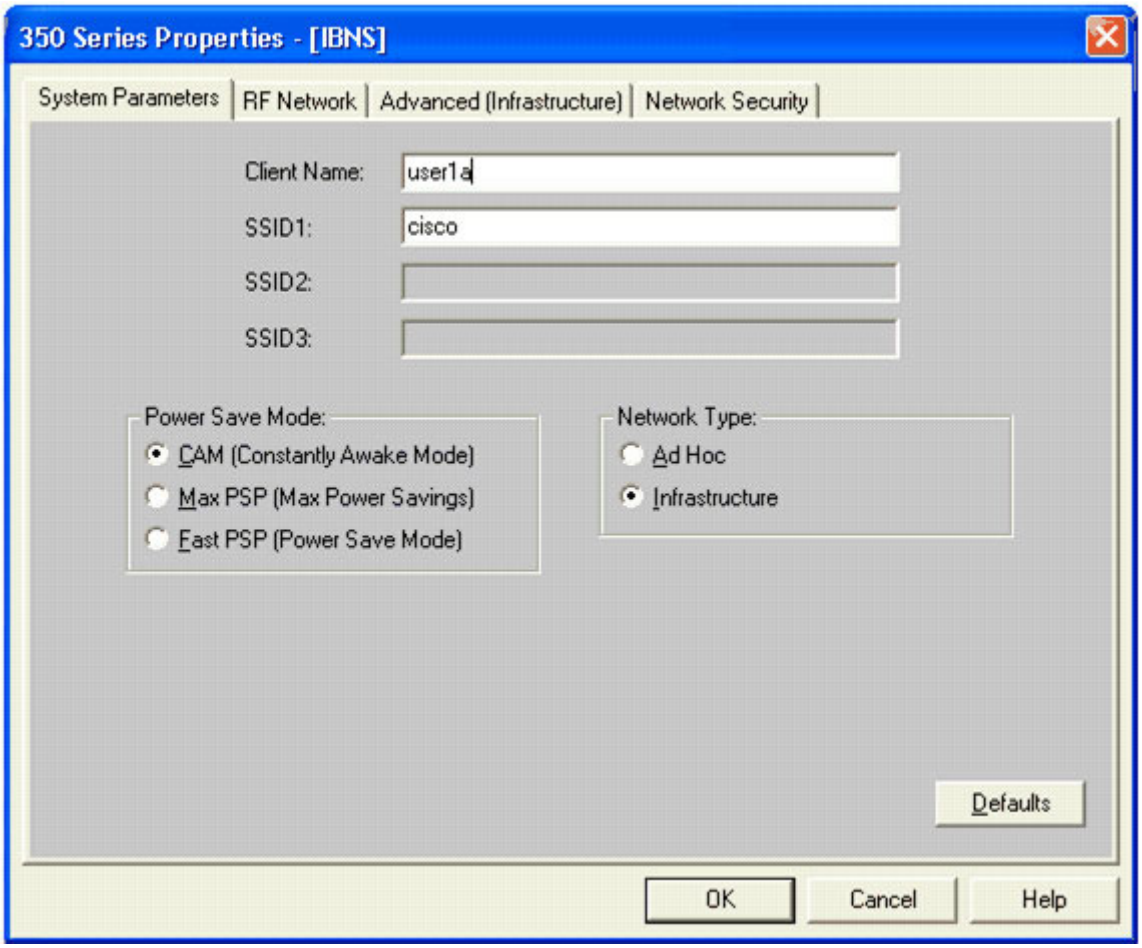
図 6-4　プロファイル設定の編集



プロファイルのシステム パラメータの設定

System Parameters ウィンドウで、プロファイルのクライアント名と SSID を入力します。この例では、Client Name に user1a、SSID に cisco を使用します。Power Save Mode および Network Type パラメータには、デフォルトのオプションを使用します。

図 6-5　プロファイルのシステム パラメータの設定



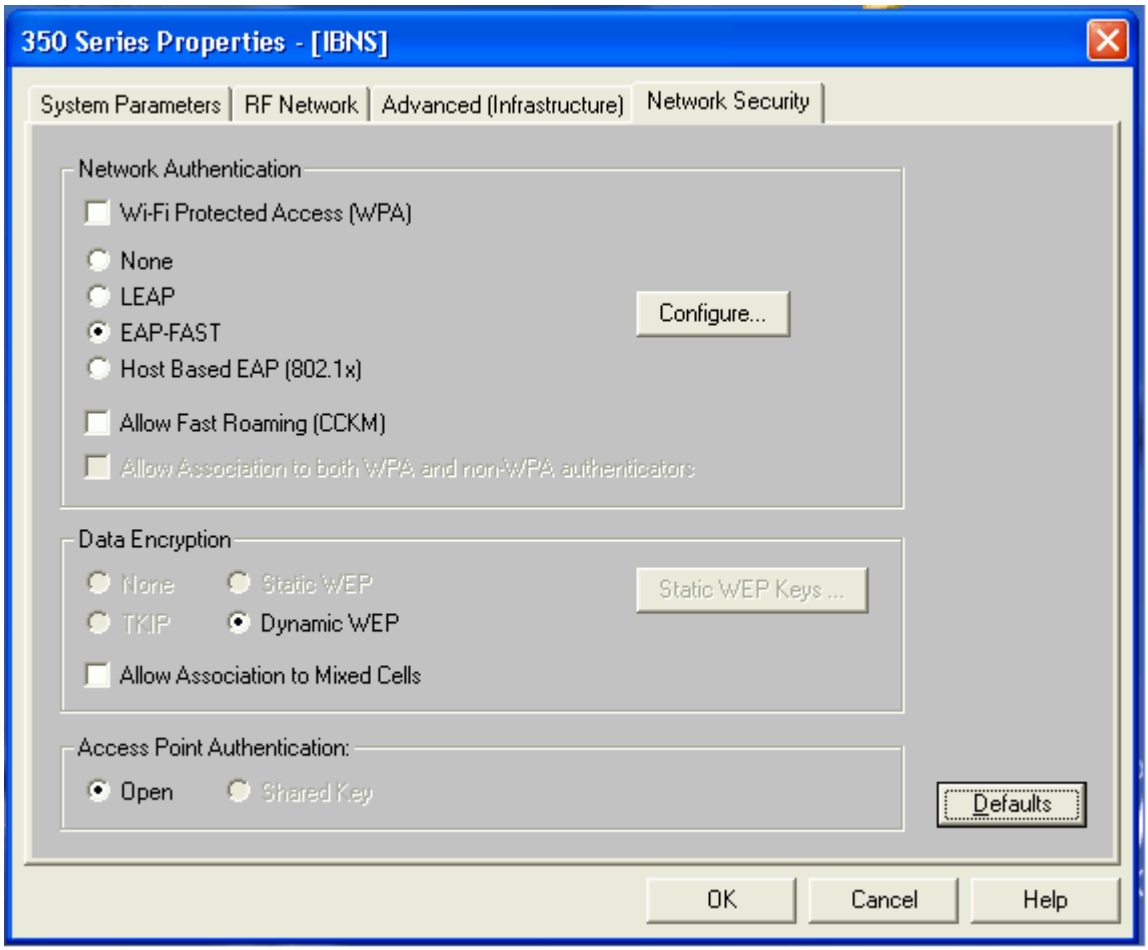
プロファイルのネットワーク セキュリティの設定

Network Authentication セクションの Network Security ウィンドウで、EAP-FAST オプション ボタンを選択します。

Data Encryption セクションで、Dynamic WEP のデフォルトの設定をそのまま使用します。これは、EAP 認証プロセスで WEP キーが動的に生成されることを意味します。

Access Point Authentication セクションで、デフォルト設定の Open をそのまま使用します。

図 6-6　プロファイルのネットワーク セキュリティの設定



プロファイルの EAP-FAST 設定の構成

Network Security ウィンドウの Network Authentication セクションで **Configure** ボタンをクリックして、プロファイルの EAP-FAST 設定を選択します。User Name and Password Settings セクションに表示されている、デフォルト設定の Use Temporary User Name and Password および Use Windows Logon User Name and Password を使用します。これはデフォルトのオプションであり、EAP-FAST ユーザ名およびパスワードとして、Windows ユーザ名とパスワードが使用されます。Logon Options には、次のデフォルト設定を使用します。

- Include Windows Logon Domain with User Name：複数のドメインを持つ環境で必要です。
- No Network Connection Unless User is Logged In：ユーザがログオフしたあと、クライアント アダプタを強制的に切断して、別のユーザが同じ証明書を使用して無線ネットワークにアクセスできないようにします。
- Authentication Timeout Value (seconds) ：EAP-FAST 認証の試行が失敗とみなされ、エラー メッセージが表示されるまでの時間を秒単位で指定します。

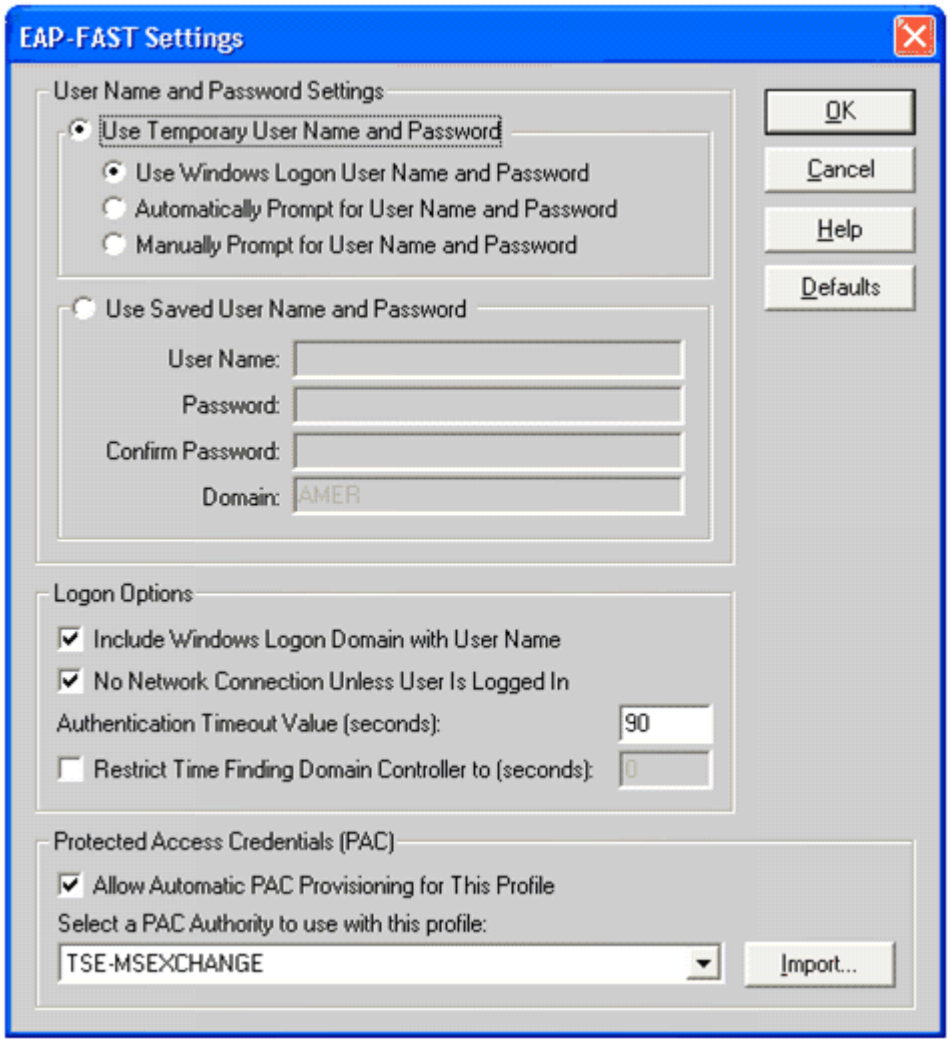
Protected Access Credentials セクションで、デフォルト値の Allow Automatic PAC Provisioning for This Profile ボックスを使用します。これにより、必要に応じて PAC が自動的に取得されます（たとえば、PAC が期限切れになった場合、クライアント アダプタが別のサーバにアクセスした場合、EAP-FAST ユーザ名が以前にプロビジョニングされた PAC と一致しない場合など）。

（注）　Select a PAC Authority to use with the profile の値は、ユーザがネットワークへのログインを試行するまで空白のままです。最初にログインが成功したあと、自動 PAC プロビジョニング プロセスを介して PAC Authority 値が読み込まれます。

EAP-Settings ウィンドウで **OK** をクリックして、設定を保存します。

Profile Properties ウィンドウで **OK** をクリックして、前述の手順で設定した System Parameters および Network Security オプションを保存します。

図 6-7　　プロファイルの EAP-FAST 設定の構成



APPENDIX A

オプションの Cisco IOS および Cisco Catalyst OS の設定コマンド

この付録では、IEEE 802.1X の設定に使用できるオプションの Cisco IOS および Cisco Catalyst OS のコマンドを示します。

Cisco IOS

Cisco IOS を実行する Cisco Catalyst スイッチでは、特定のコマンドを使用して IEEE 802.1X を有効にする必要がありますが、追加コマンドの設定により、オプションの機能を有効にしたり、デフォルト パラメータを変更したりできます。この追加の RADIUS、グローバル、およびインターフェイスの各コマンドについては、次の項で説明します。

Cisco IOS の RADIUS 設定

Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために使用されるオプションの RADIUS 設定コマンドを示します。

表 A-1　Cisco IOS のオプションの RADIUS 設定コマンド

aaa authorization network [<list name> | default] **group radius**	（オプション）ユーザ単位の ACL または VLAN 環境など、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 認証のスイッチを設定します。
ip radius source-interface [interface]	（オプション）RADIUS パケットのソース アドレスのインターフェイスを指定します。
radius-server vsa send [authentication | accounting]	（オプション）スイッチが RADIUS IETF 属性 26 で定義された VSA を認識および使用できるように設定します。認証またはアカウンティング オプションの指定により、認識されたベンダー固有の属性セットを認証またはアカウンティングのみに制限します。

Cisco IOS のグローバル IEEE 802.1X 設定

Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために使用されるオプションのグローバル コンフィギュレーション コマンドを示します。

表 A-2　Cisco IOS のオプションのグローバル コンフィギュレーション コマンド

dot1x guest-vlan supplicant	（オプション）IEEE 802.1X 対応のサプリカントが Guest VLAN を開始できるように設定します。

Cisco IOS のインターフェイス IEEE 802.1X 設定

Cisco IOS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために使用されるオプションのインターフェイス コンフィギュレーション コマンドを示します。

表 A-3　Cisco IOS のオプションのインターフェイス コンフィギュレーション コマンド

dot1x control-direction [in | both]	（オプション）ポート制御を単方向または双方向制御に変更します。デフォルトは双方向モードです。
dot1x default	（オプション）設定可能な IEEE 802.1X パラメータをデフォルト値にリセットします。
dot1x guest-vlan [VLAN ID]	（オプション）アクティブな VLAN を IEEE 802.1X guest VLAN として指定します。
dot1x host-mode	（オプション）IEEE 802.1X で許可されたポートで、1 つまたは複数のホスト（クライアント）を許可します。デフォルトはシングル ホスト モードです。
dot1x max-reauth-req [count]	（オプション）スイッチが再起動する前に ID 要求を再送信する回数を設定します。デフォルトは 2（30 秒ごとに 1 回）です。
dot1x max-req [count]	（オプション）スイッチが再起動する前に EAPoL データ フレームを再送信する回数を設定します。デフォルトは 2 回（30 秒ごとに 1 回）です。
dot1x reauthentication	（オプション）クライアントの定期的な再認証を有効にします。デフォルトは無効です。
dot1x timeout [reauth-period | quiet-period | tx-period] [seconds]	（オプション）reauth-period、quiet-period、server-timeout、supp-timeout、tx-period などの項目のタイマーを設定します。reauth-period のデフォルトは 3600 秒です。quiet-period のデフォルトは 60 秒です。server-timeout のデフォルトは 30 秒です。supp-timeout のデフォルトは 30 秒です。tx-period のデフォルトは 5 秒です。

Cisco Catalyst OS

Cisco Catalyst OS を実行する Cisco Catalyst スイッチでは、特定のコマンドを使用して IEEE 802.1X を有効にする必要がありますが、追加コマンドの設定により、オプションの機能を有効にしたり、デフォルト パラメータを変更したりできます。この追加の RADIUS、グローバル、およびインターフェイスの各コマンドについては、次の項で説明します。

Cisco Catalyst OS のグローバル IEEE 802.1X 設定

Cisco Catalyst OS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために使用されるオプションのグローバル コンフィギュレーション コマンドを示します。

表 A-4　Cisco Catalyst OS のオプションのグローバル コンフィギュレーション コマンド

set dot1x max-req [count]	(オプション) 認証セッションをタイムアウトする前に、ステート マシンが EAP-Request フレームをサプリカントに再送信する最大回数を指定します。デフォルトは 2 です。
set dot1x max-reauth-req	(オプション) サプリカントへの最大再試行回数を設定します。
set dot1x quiet-period [seconds]	(オプション) 認証を試行する間のアイドル時間を指定します。デフォルトは 60 秒です。
set dot1x radius-accounting [enable | disable]	(オプション) IEEE 802.1X RADIUS アカウンティングおよびトラッキングを指定します。デフォルトは無効です。
set dot1x radius-keepalive [enable | disable]	(オプション) IEEE 802.1X RADIUS キープアライブ状態を指定します。デフォルトは有効です。
set dot1x radius-vlan-assignment [enable | disable]	(オプション) IEEE 802.1X RADIUS VLAN 割り当てを指定します。デフォルトは無効です。
set dot1x re-authperiod [seconds]	(オプション) 再認証の再送信時間の時間定数を指定します。デフォルトは 3600 秒です。
set dot1x server-timeout [seconds]	(オプション) バックエンド オーセンティケータが認証サーバにパケットを再送信する時間定数を指定します。デフォルトは 30 秒です。
set dot1x shutdown-timeout [seconds]	(オプション) セキュリティ違反後にポートがシャットダウンされる時間を指定します。デフォルトは 300 秒です。
set dot1x supp-timeout [seconds]	(オプション) EAP-Request パケットの再送信の時間定数を指定します。デフォルトは 30 秒です。
set dot1x tx-period [seconds]	(オプション) EAP-Request/Identity フレームの再送信の時間を指定します。デフォルトは 30 秒です。
set dot1x vlan-group [VLAN group] [VLAN ID]	(オプション) VLAN グループ名を指定します。

Cisco Catalyst OS のポート IEEE 802.1X 設定

Cisco Catalyst OS を実行する Cisco Catalyst スイッチで IEEE 802.1X を設定するために使用されるオプションのポート コンフィギュレーション コマンドを示します。

表 A-5　Cisco Catalyst OS のオプションのポート コンフィギュレーション コマンド

set port dot1x [module/port] **auth-fail-vlan** [VLAN | none]	（オプション）IEEE 802.1X 認証に失敗したエンド ホストへの制限されたアクセスを提供する VLAN を設定します。デフォルトは none です。
set port dot1x [module/port] **critical**	（オプション）ポートをクリティカルに設定します。
set port dot1x [module/port] **guest-vlan** [VLAN | none]	（オプション）アクティブな VLAN を IEEE 802.1X guest VLAN として指定します。デフォルトは none です。
set port dot1x [module/port] **initialize**	（オプション）ポートで IEEE 802.1X を初期化します。このコマンドにより、新規の認証用に現在のステート マシンがクリアされます。
set port dot1x [module/port] **multiple-authentication** [enable | disable]	（オプション）複数のホストがポートへのアクセス権を取得できるように、複数の認証を指定します。デフォルトは無効です。
set port dot1x [module/port] **multiple-host** [enable | disable]	（オプション）複数ユーザのアクセスを指定します。デフォルトは無効です。
set port dot1x [module/port] **port-control-direction** [both | in]	（オプション）ポートのトラフィック制御方向を指定します。デフォルトは両方です。
set port dot1x [module/port] **re-authenticate** [enable | disable]	（オプション）ポートに接続されたエンティティの再認証を相互に開始します。デフォルトは無効です。
set port dot1x [module/port] **re-authentication** [enable | disable]	（オプション）再認証期間内にポートに接続されたエンティティの再認証を自動的に開始します。デフォルトは無効です。
set port dot1x [module/port] **shutdown-timeout** [enable | disable]	（オプション）セキュリティ違反後のポートのシャットダウン タイムアウト期間を指定します。デフォルトは無効です。
set port dot1x [module/port]**test-eapol-capable**	（オプション）eapol 機能をテストします。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイント

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントでは、特定のコマンドを使用して IEEE 802.1X を有効にする必要がありますが、追加コマンドの設定により、オプションの機能を有効にしたり、デフォルト パラメータを変更したりできます。この追加の RADIUS、グローバル、およびインターフェイスの各コマンドについては、次の項で説明します。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントの RADIUS 設定

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントで IEEE 802.1X を設定するために使用されるオプションの RADIUS コンフィギュレーション コマンドを示します。

表 A-6　Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントのオプションの RADIUS コンフィギュレーション コマンド

aaa authorization network [<list name> | default] **group radius**	(オプション) ユーザ単位の ACL または VLAN 環境など、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 認証のスイッチを設定します。
ip radius source-interface [interface]	(オプション) RADIUS パケットのソース アドレスのインターフェイスを指定します。
radius-server vsa send [authentication | accounting]	(オプション) スイッチが RADIUS IETF 属性 26 で定義された VSA を認識および使用できるように設定します。認証またはアカウンティング オプションの指定により、認識されたベンダー固有の属性セットを認証またはアカウンティングのみに制限します。

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントのインターフェイス設定

Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントで IEEE 802.1X を設定するために使用されるオプションのインターフェイス コンフィギュレーション コマンドを示します。

表 A-7　Cisco IOS を実行する Cisco Aironet 無線 LAN アクセス ポイントのオプションのインターフェイス設定コマンド

dot1x client-timeout [seconds]	(オプション) 認証が失敗する前に、認証を試行するクライアントからの応答をアクセス ポイントが待機する秒数を入力します。
dot1x reauth-period [seconds | server]	(オプション) 認証されたクライアントを強制的に再認証する前に、アクセス ポイントが待機する間隔を秒数で入力します。 認証サーバで指定された再認証期間を使用するようにアクセス ポイントを設定するための **server** キーワードを入力します。このオプションを使用する場合、認証サーバの RADIUS 属性 27 を Session-Timeout に設定します。この属性は、セッションまたはプロンプトの終了前にクライアントにサービスが提供される最大秒数を設定します。クライアント デバイスが EAP 認証を実行する際、サーバはこの属性をアクセス ポイントに送信します。

APPENDIX **B**

クライアントでの X.509v3 PKI 証明書のインストール

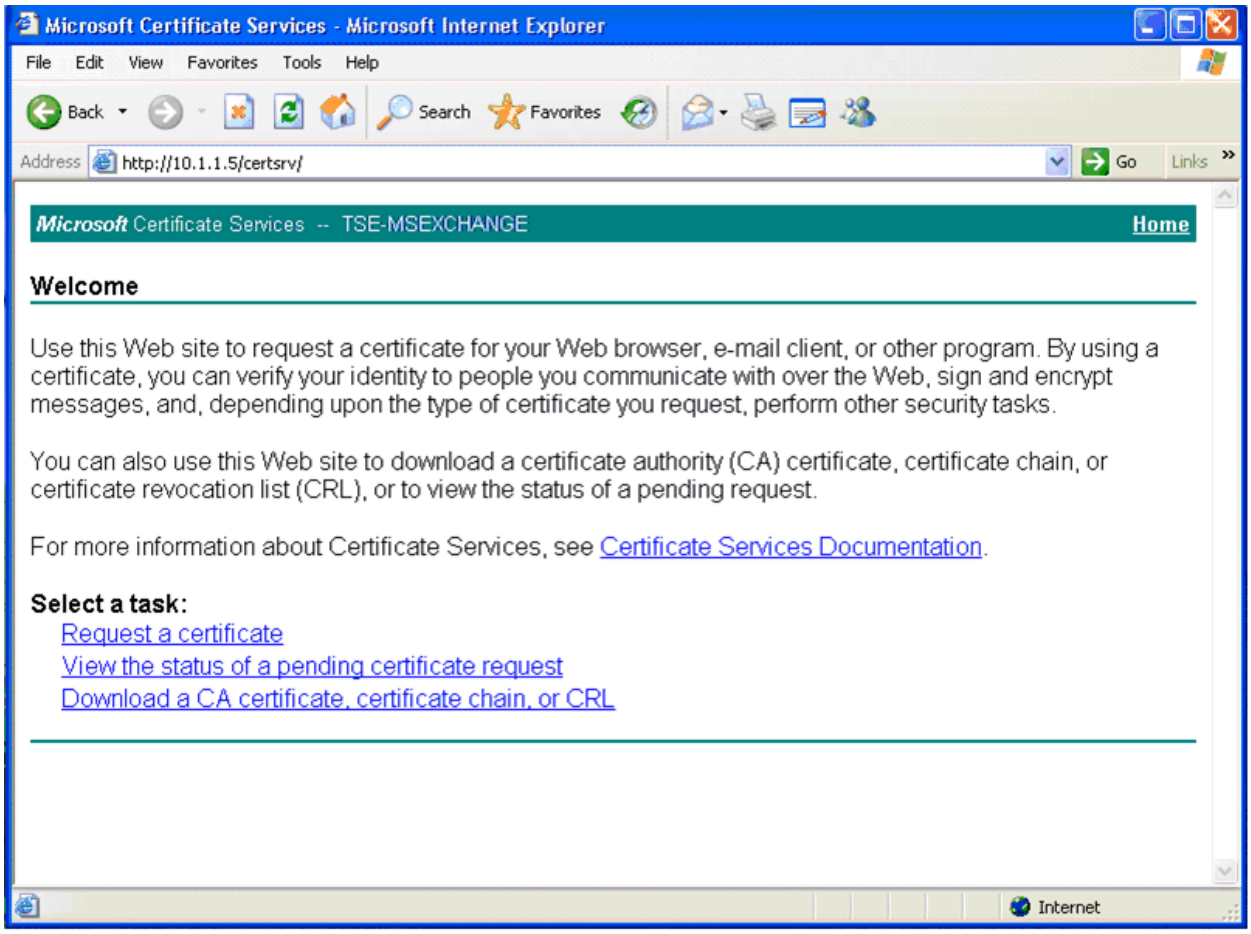
この付録では、デスクトップ / ノート型 PC で X.509 PKI 証明書をインストールするプロセスについて説明します。EAP-TLS と IEEE 802.1X（PEAP または EAP-FAST）を認証方式として使用する場合、証明書が必要になります。

EAP 方式の展開に関する項で説明したように、この付録で使用されるデスクトップ / ノート型 PC では、Microsoft Windows XP with Service Pack 2 が実行されています。

認証局へのアクセス

Web ブラウザを開き、認証局のアドレス http://< 認証局のアドレスまたはホスト名 >/certsrv/ を入力します。プロンプトが表示されたらログインします。Welcome 画面で、タスク リストの Request a Certificate リンクを選択します。

図 B-1　認証局へのアクセス

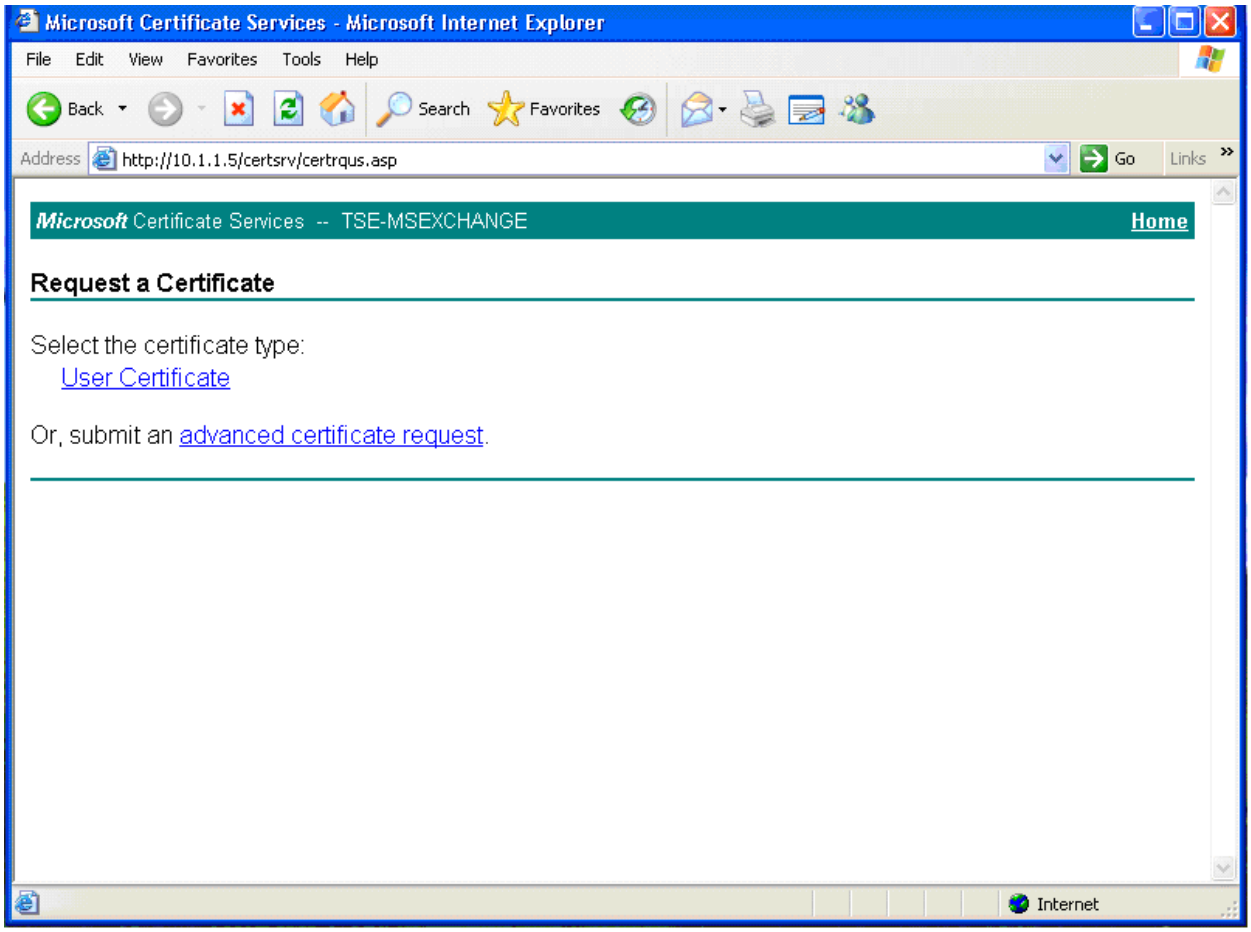


証明書の要求

Request a Certificate 画面で、証明書タイプの User Certificate オプションを選択します。

（注）　プロンプトが表示されたら **Yes** をクリックして、証明書の要求元のサーバを信頼します。

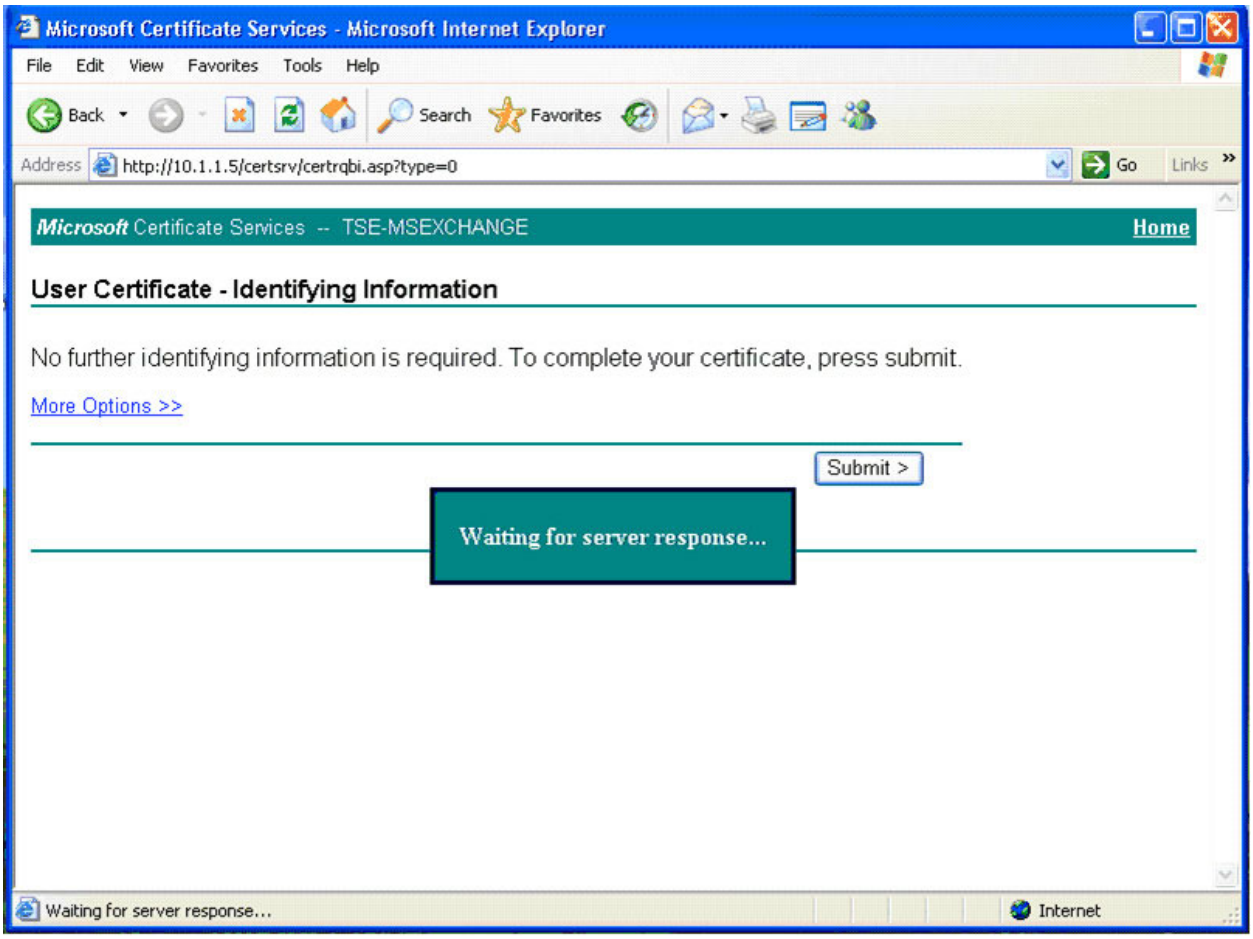
図 B-2　証明書の要求



証明書要求の完了

User Certificate - Identifying Information 画面で、Submit を選択して要求を完了します。要求が完了するまで Waiting for server response というステータス メッセージが表示されます。

図 B-3　証明書要求の完了

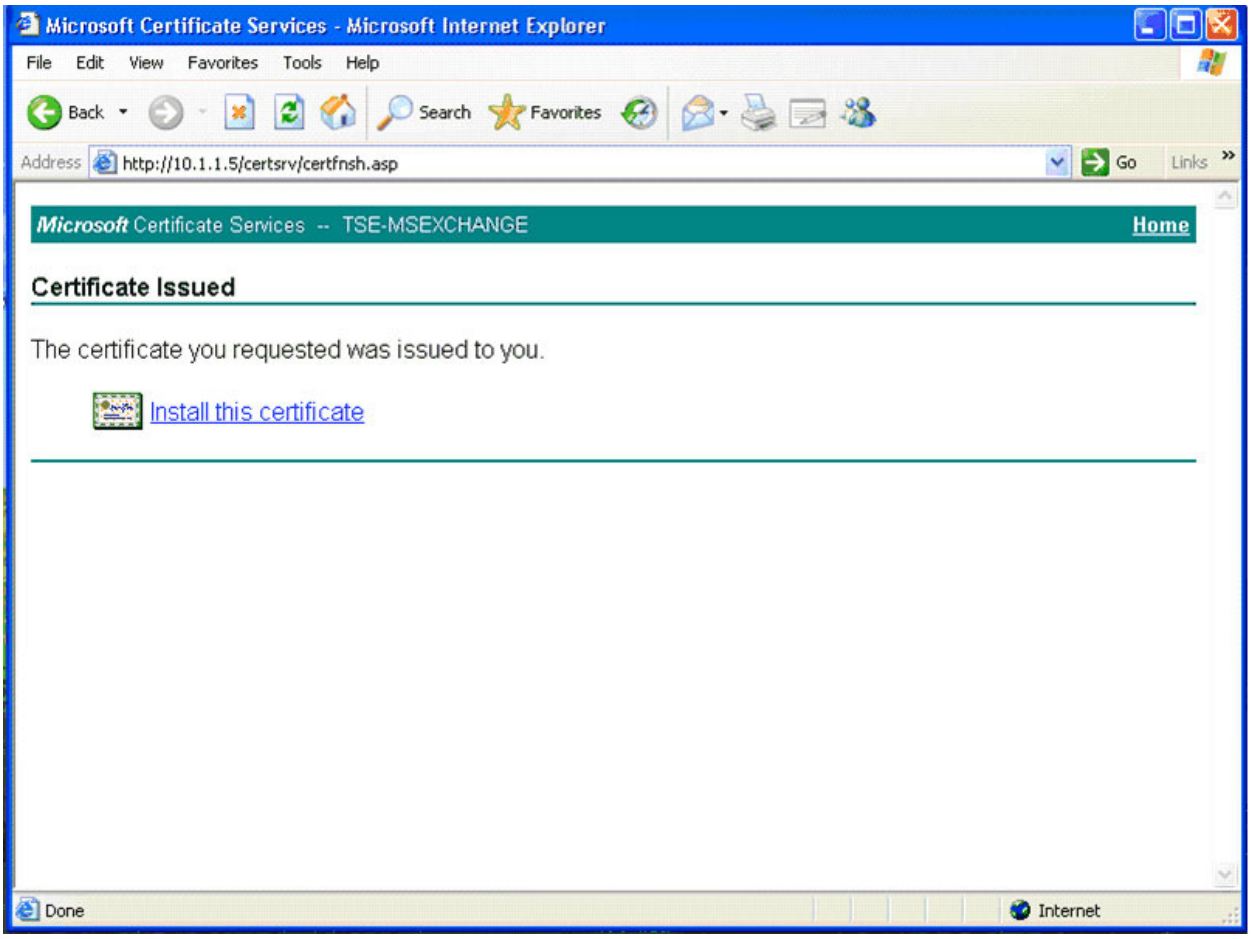


証明書のインストール

証明書が発行されたあと、Install this certificate オプションを選択して、デスクトップ / ノート型 PC に証明書をインストールします。

（注）　プロンプトが表示されたら **Yes** をクリックして、証明書の要求元のサーバを信頼します。

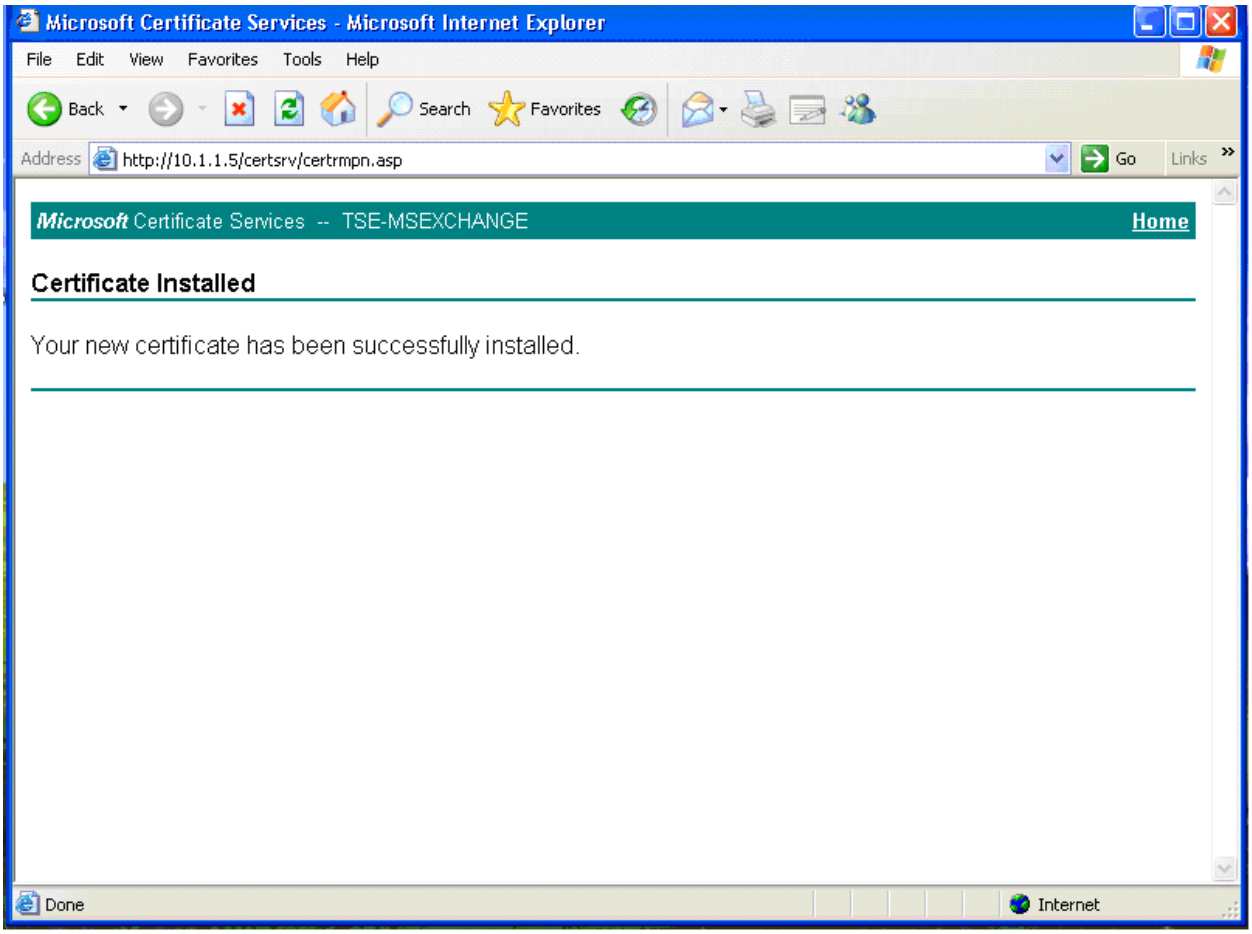
図 B-4　　証明書のインストール



証明書インストールの完了

証明書が正常にインストールされると、Certificate Installed 画面が表示されます。

図 B-5　証明書インストールの完了



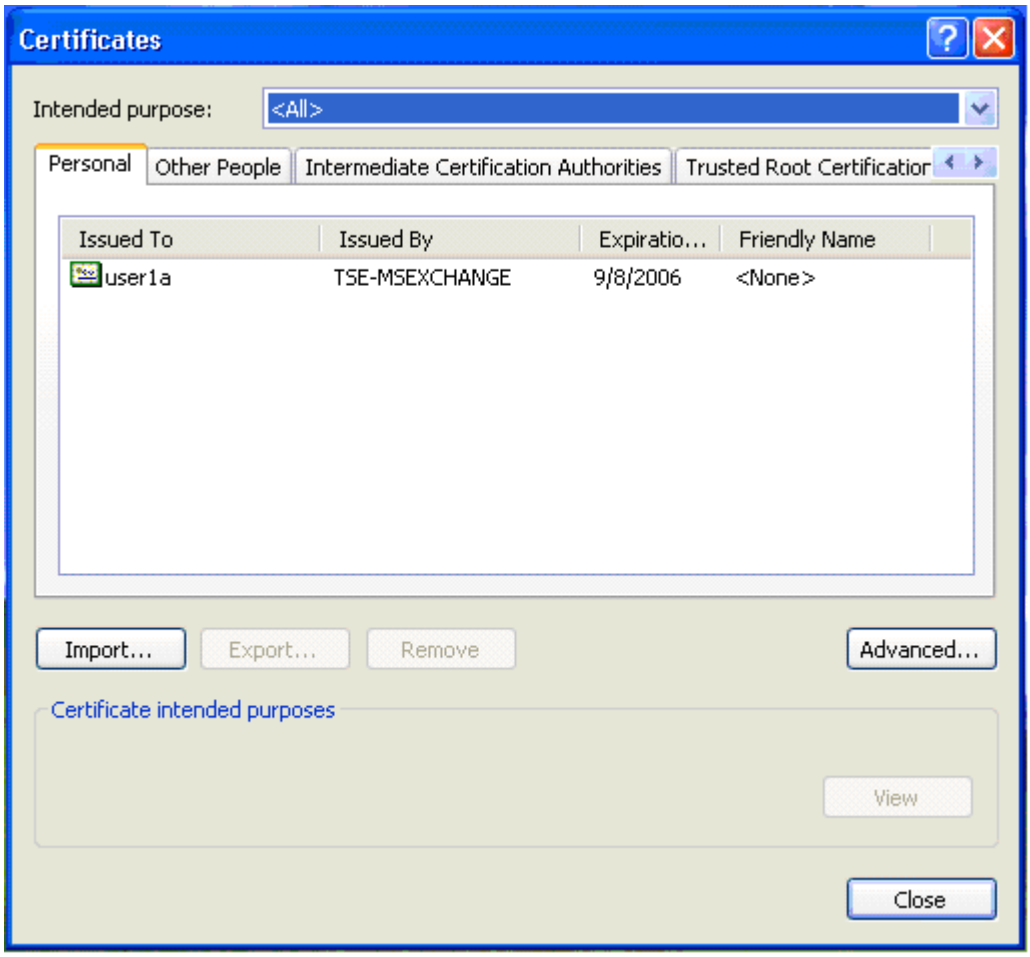
証明書インストールの確認

証明書インストールを確認するには、Web ブラウザのメニューから Tools、Internet Options の順に選択して、Content タブを選択します。

図 B-6　　証明書インストールの確認

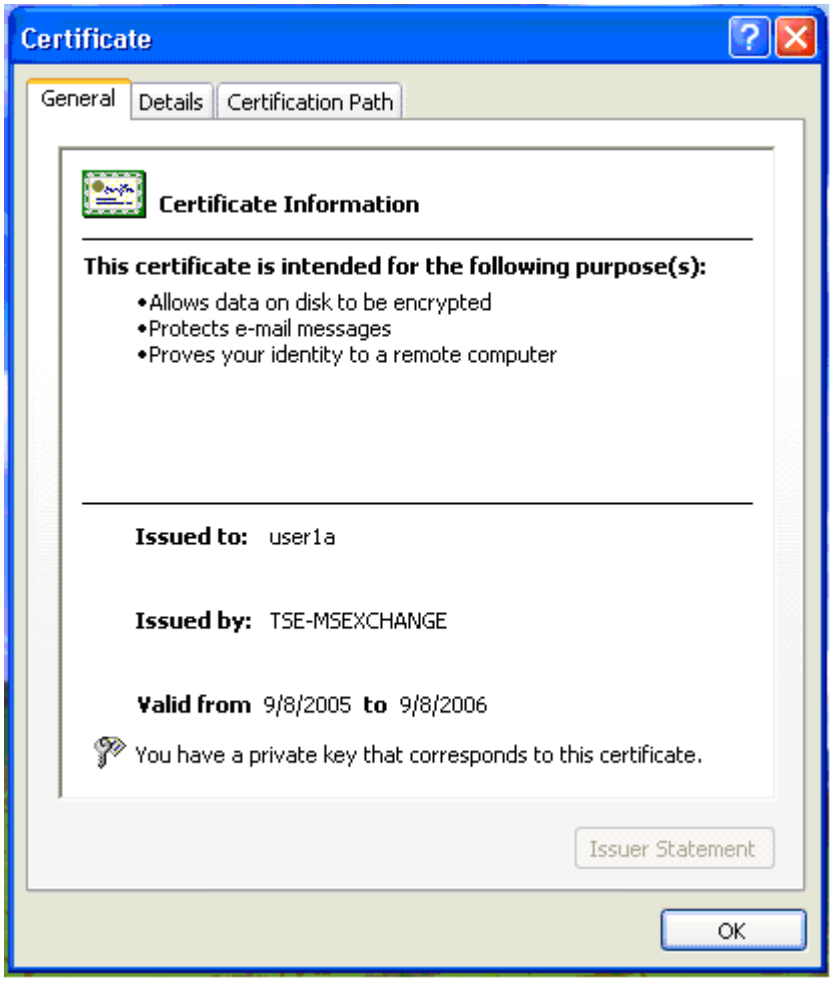
Certificates セクションで、Certificates ボタンを選択します。デスクトップ / ノート型 PC で発行およびインストールされている証明書を示す画面が表示されます。

図 B-7　インストールされた証明書リストの表示



詳細を表示するには、証明書を選択して **View** ボタンをクリックします。

図 B-8　証明書の詳細の表示



証明書インストールの確認

APPENDIX C

CiscoSecure ACS での X.509v3 PKI 証明書のインストール

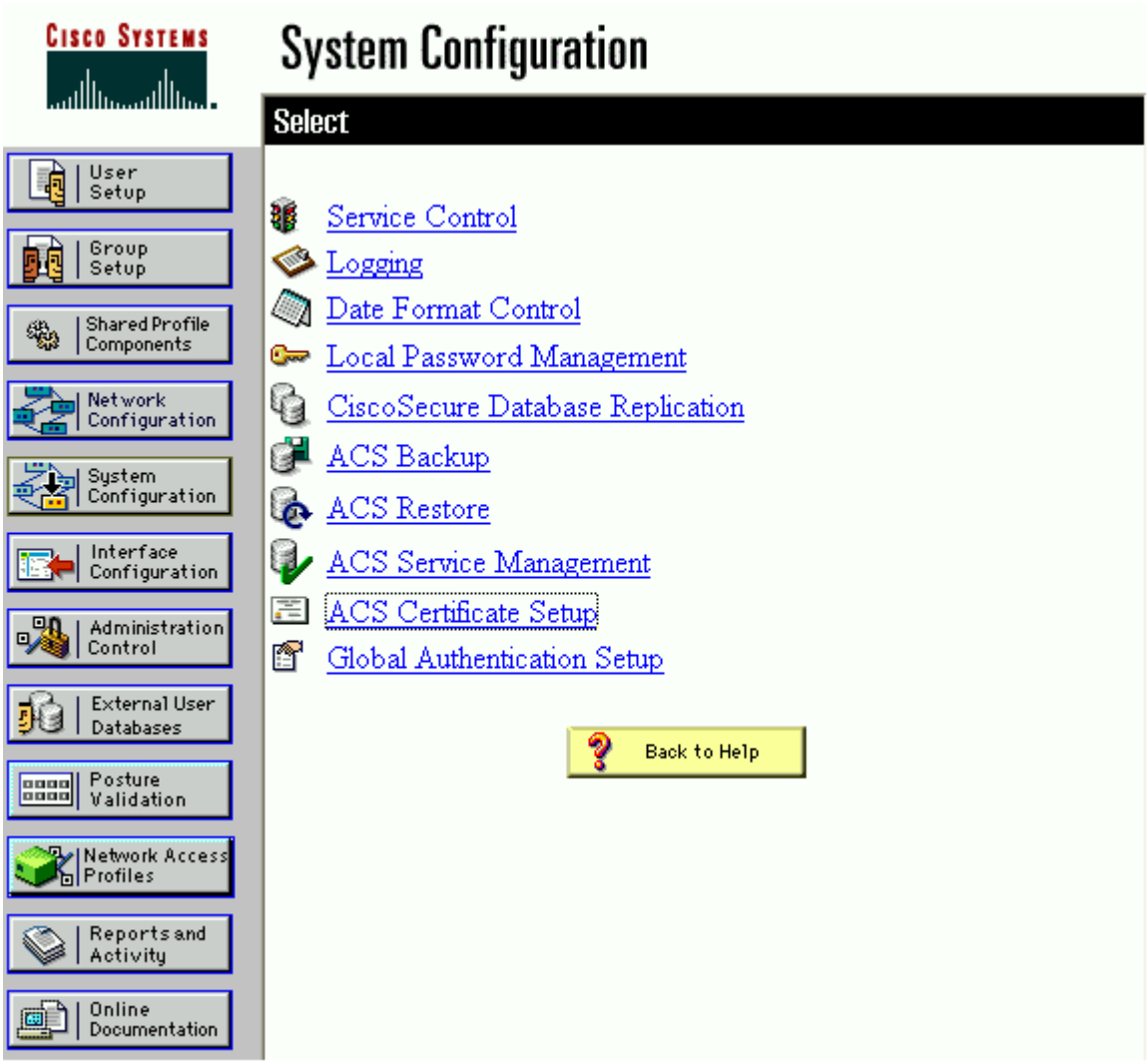
この付録では、CiscoSecure ACS で X.509 PKI 証明書をインストールするプロセスについて説明します。EAP-TLS または PEAP と IEEE 802.1X を認証方式として使用する場合、証明書が必要になります。

CiscoSecure ACS は、Windows Server 2003 Enterprise Edition で実行されています。

ACS 証明書設定の選択

メイン メニューで System Configuration を選択します。System Configuration メニューから、ACS Certificate Setup を選択します。

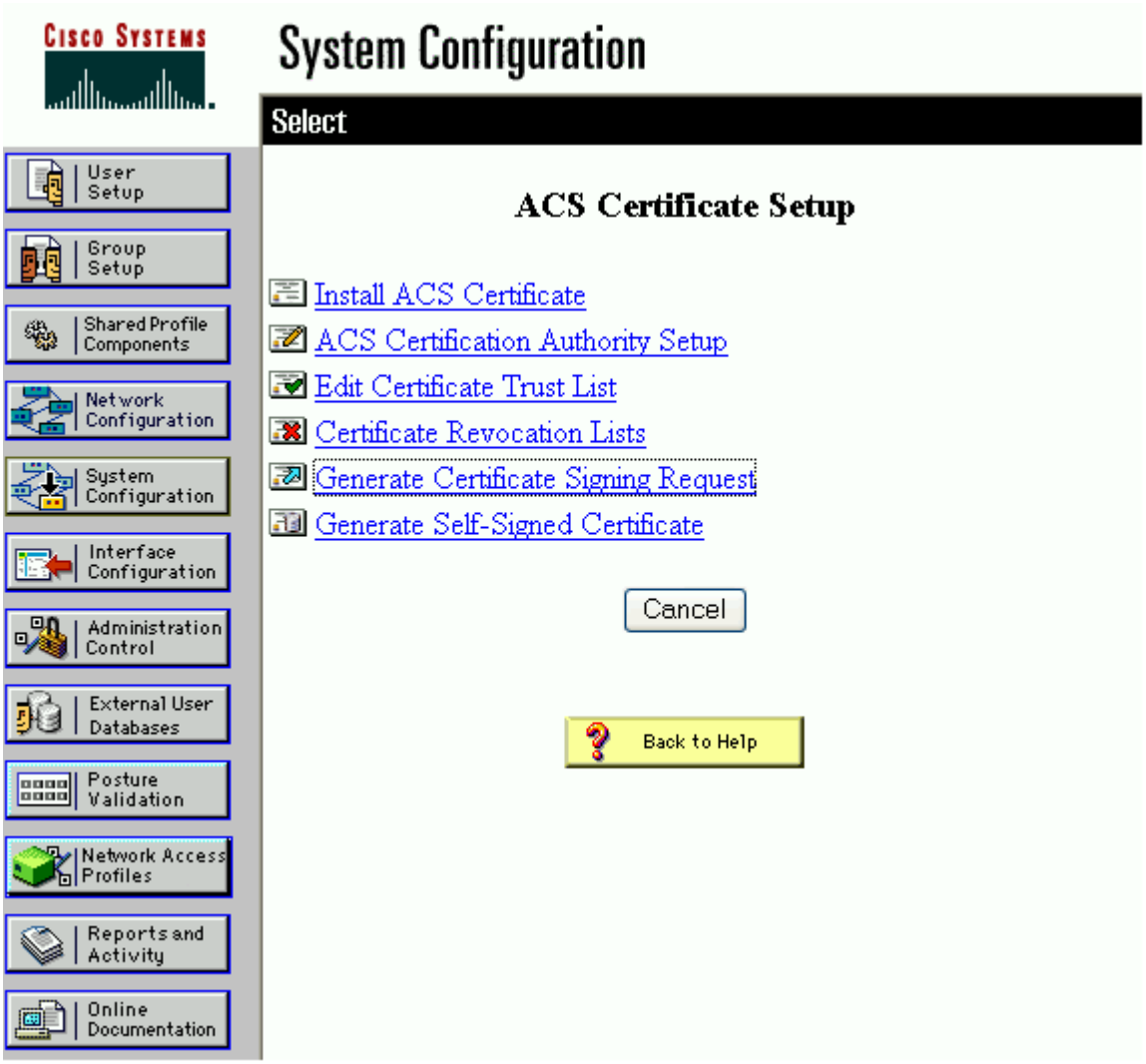
図 C-1　ACS 証明書設定の選択



Certificate Signing Request の生成の選択

ACS Certificate Setup メニューから、Generate Certificate Signing Request を選択します。

図 C-2　Certificate Signing Request の生成の選択



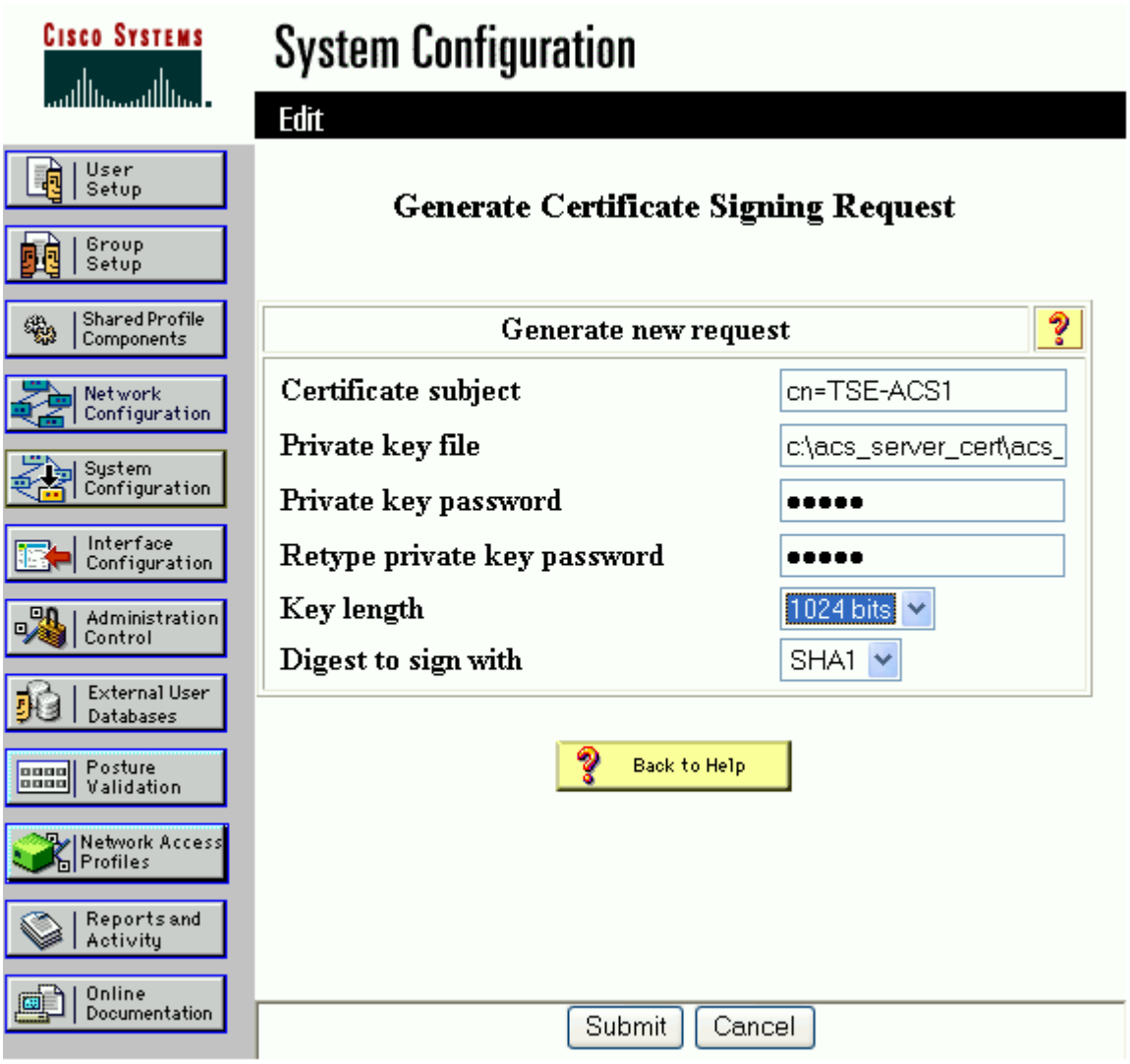
Certificate Signing Request の発行

Certificate Subject ボックスに共通名の値を入力します。共通名は、証明書の一部の値で、Certificate Subject 値として ACS で必要になります。Private key file ボックスに完全なディレクトリ パスとファイル名を入力します。この例では、Private key file の値として C:\acs_server_cert\acs_server_cert.pvk が入力されています。

（注）　管理者は、プライベート キー ファイルを格納するディレクトリを選択または作成する必要があります。

Private key password ボックスにパスワードを入力します。Retype private key password ボックスに同じパスワードを再入力します。適切な Key length と Digest to sign with の値を選択します。この例では、Microsoft CA を使用しているため、キー長には 1024、ダイジェストには SHA1 が使用されています。**Submit** をクリックします。

図 C-3　Certificate Signing Request の発行



Certificate Signing Request のコピー

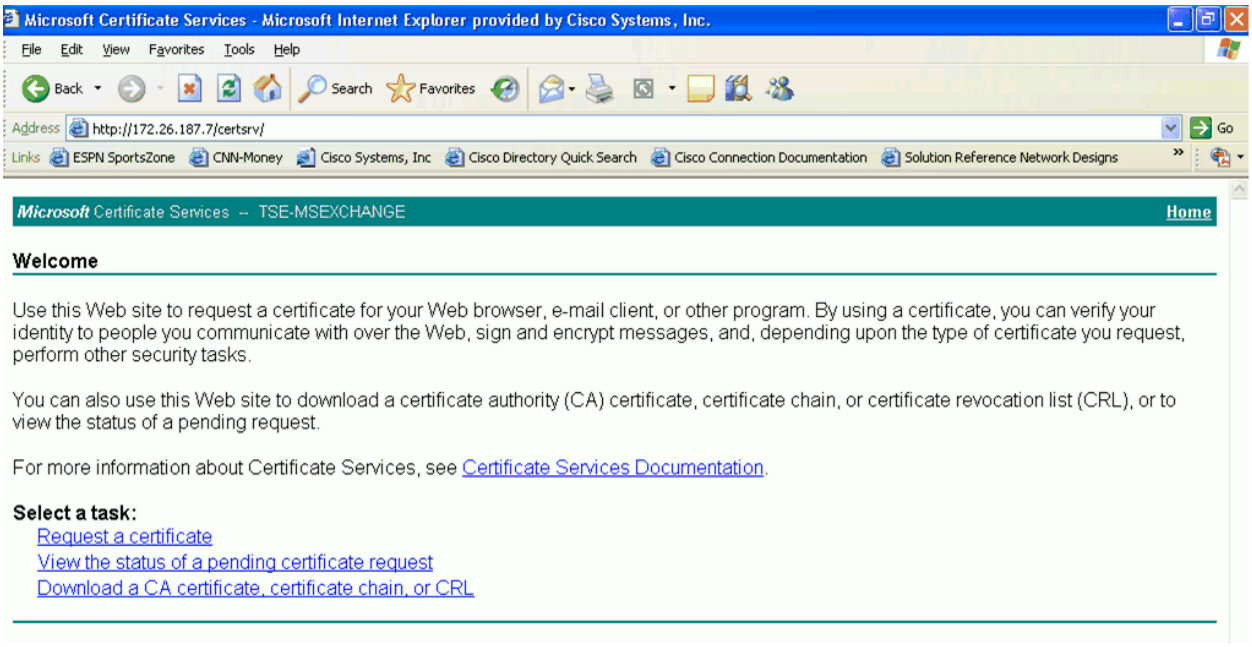
右側のフレームで Certificate Signing Request をコピーします。この情報は、ACS 証明書の要求に使用されます。

図 C-4　Certificate Signing Request のコピー

認証局へのアクセス

Web ブラウザを開き、認証局のアドレス http://< 認証局のアドレスまたはホスト名 >/certsrv/ を入力します。プロンプトが表示されたらログインします。Welcome 画面で、タスク リストの Request a Certificate リンクを選択します。

図 C-5　認証局へのアクセス

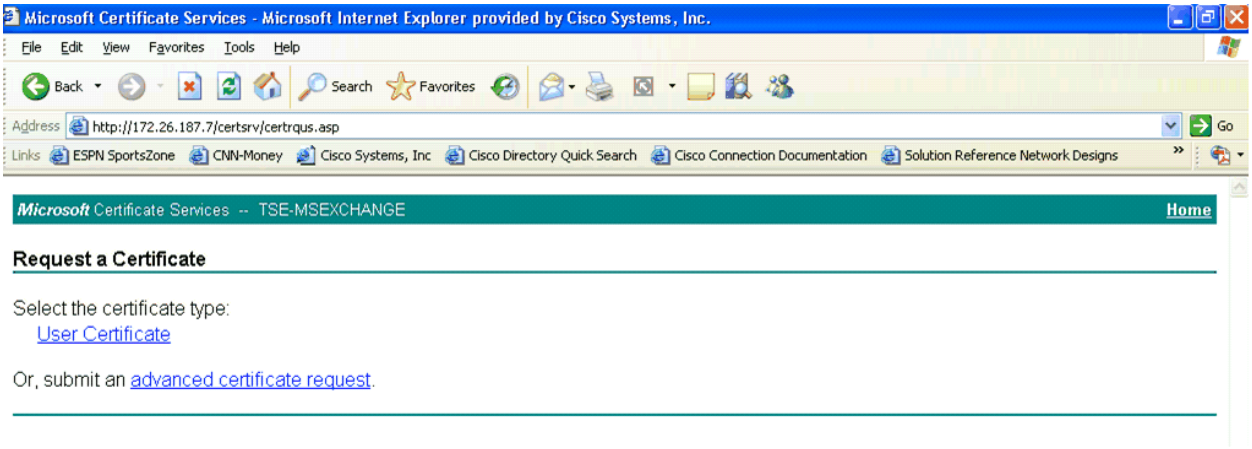


高度な証明書の要求

Request a Certificate 画面で、advanced certificate request オプションを選択します。

（注）　プロンプトが表示されたら **Yes** をクリックして、証明書の要求元のサーバを信頼します。

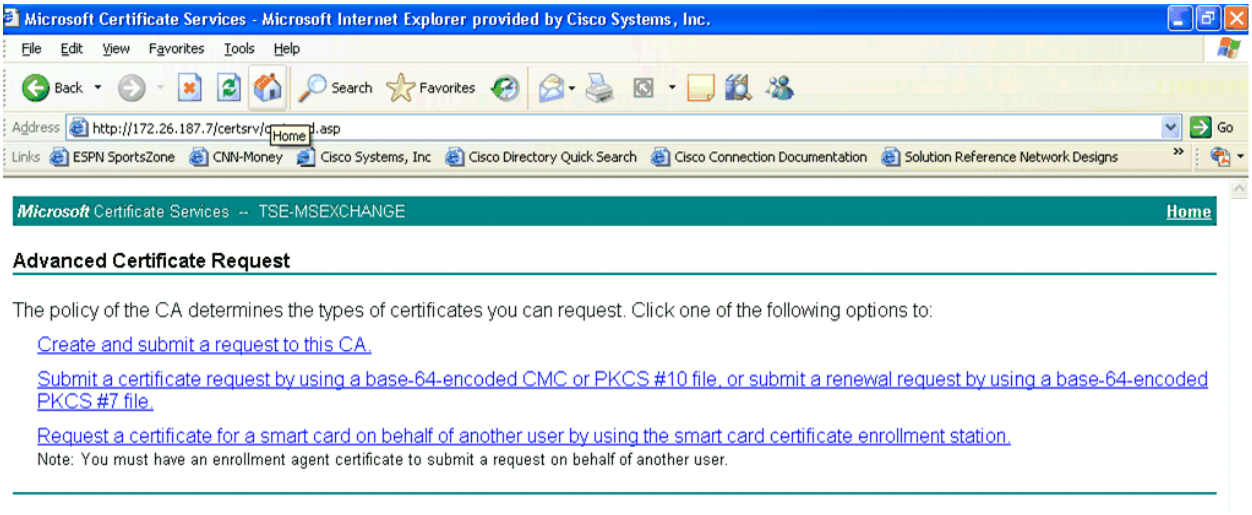
図 C-6　高度な証明書の要求



証明書要求の発行

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file をクリックします。

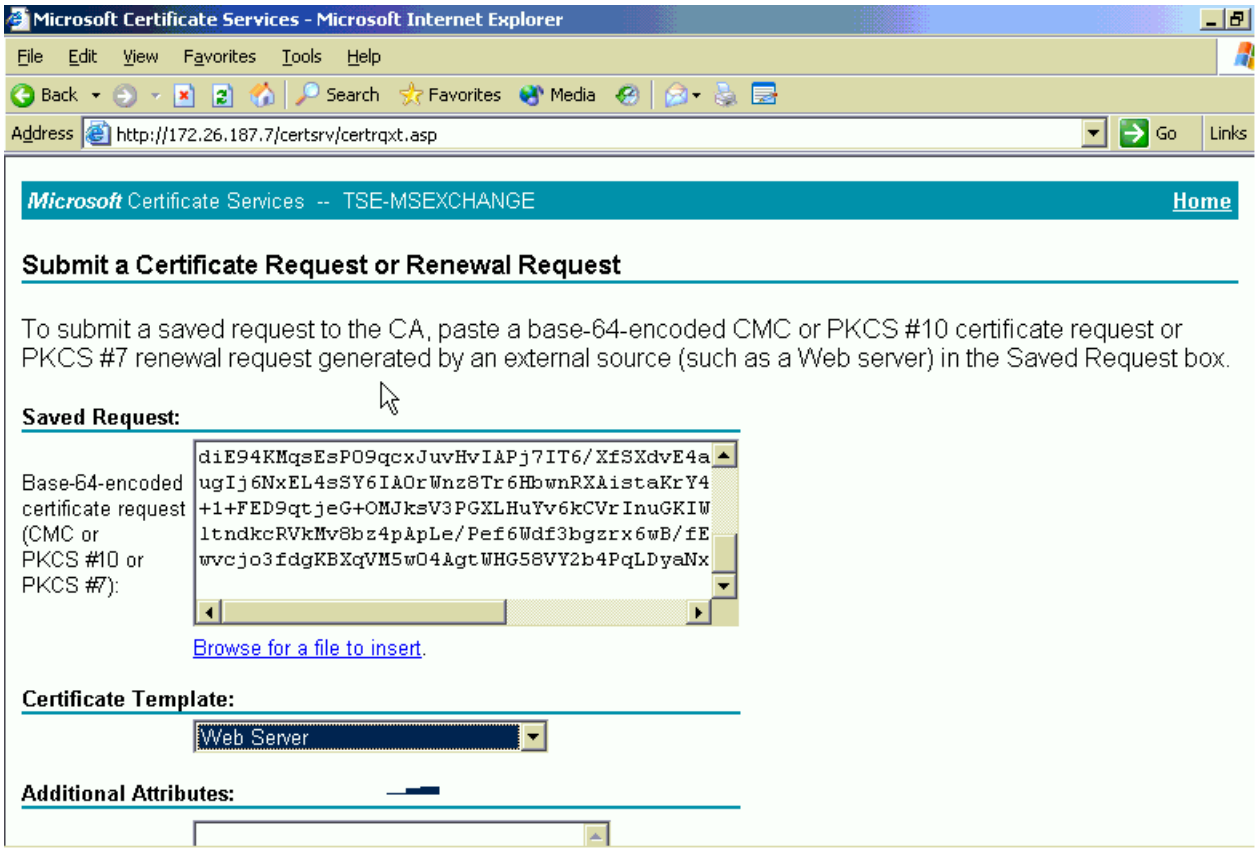
図 C-7　　証明書要求の発行



証明書要求の完了

Submit a Certificate Request or Renewal Request で、Certificate Signing Request を Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7) ボックスに貼り付けます。Certificate Template で Web Server を選択します。**Submit** をクリックします。

図 C-8　証明書要求の完了

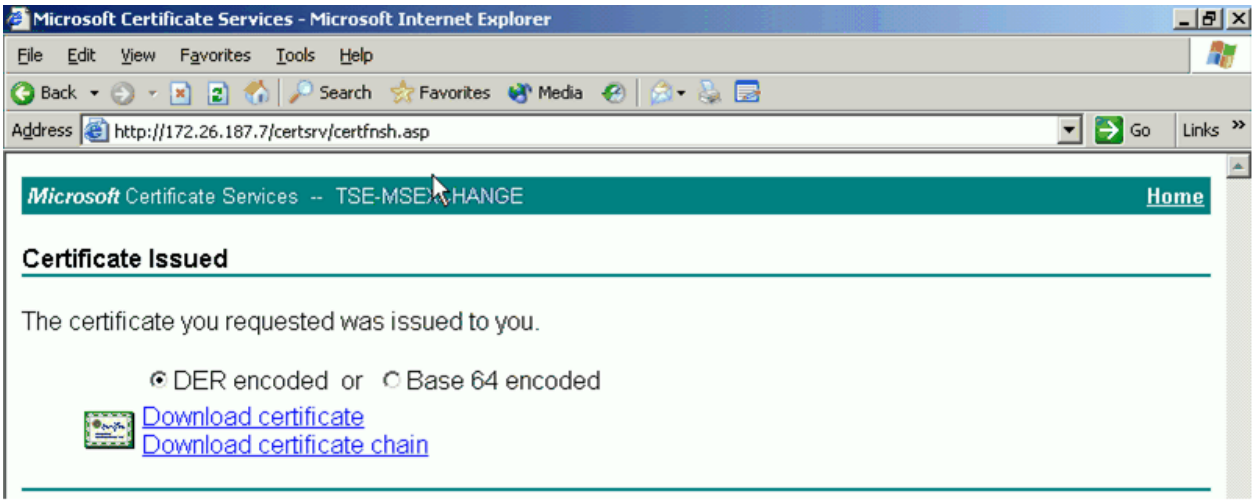


ACS への証明書のダウンロード

Download certificate をクリックして、証明書を ACS に保存します。**Download certificate chain** をクリックして、証明書チェーンを ACS に保存することもできます。

（注）　証明書は、「Certificate Signing Request の発行」（p.C-3）で作成したプライベート キー ファイルと同じディレクトリに保存してください。

図 C-9　発行された証明書のダウンロード

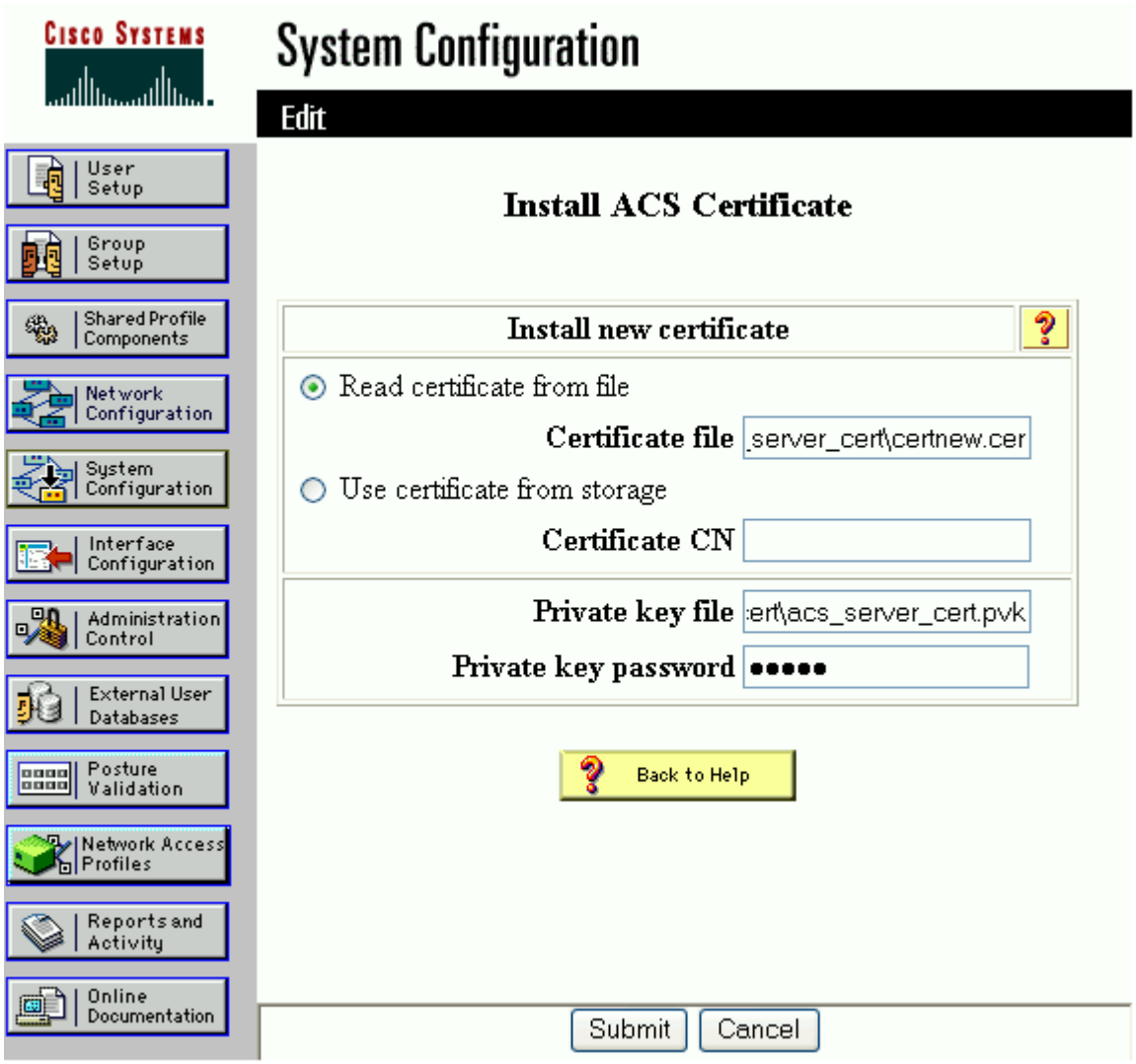


ACS への証明書のインストール

ACS メイン メニューから **System Configuration** をクリックします。System Configuration メニューから ACS Certificate Setup を選択します。ACS Certificate Setup メニューから Install ACS Certificate を選択します。

Read certificate from file オプション ボタンを選択して、Certificate file ボックスに証明書の完全なパスとファイル名を入力します。前述の手順で証明書ファイルが ACS にすでに保存されているため、この例ではこのオプションが選択されています。**Submit** をクリックします。

図 C-10　ACS への証明書のインストール



ACS 証明書インストールの確認

証明書のインストールが完了すると、Installed Certificate Information が表示されます。設定の変更を適用するには、ACS メイン メニューから System Configuration を選択します。次に、System Configuration メニューから Service Control を選択します。**Restart** をクリックして、設定の変更を適用します。

図 C-11　ACS 証明書インストールの確認

APPENDIX D

参考資料

この付録では、このマニュアルの作成に使用した参考資料のリストを示します。

シスコ製品マニュアル

- 『*Cisco Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEC*』
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sec/3750scg/index.htm
- 『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)SG*』
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_25s/conf/index.htm
- 『*Catalyst 4000 Series Software Configuration Guide, 8.3 GLX and 8.4 GLX*』
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/8_3/configur/index.htm
- 『*Catalyst 6500 シリーズ スイッチ ソフトウェア コンフィギュレーション ガイド Release 8.4*』
  http://www.cisco.com/jp/service/manual_j/sw/cat60/65scg/
- 『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.3(7)JA*』
  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/b1237ja/i1237sc/index.htm
- 『*Cisco Aironet 1200 シリーズEAP-FAST 導入ガイド*』
  http://www.cisco.com/jp/service/manual_j/wr/airo1k/eapfast/title/eapfttl.shtml
- 『*Cisco Secure ACS ユーザ ガイド Windows 版 Version 4.0*』
  http://www.cisco.com/jp/service/manual_j/sec/acs/acsugw/

パートナー製品マニュアル

- 『*Meetinghouse AEGIS Enterprise Client*』
  http://store.mtghouse.com/newWeb/cgi-bin/products_aegis_enterprise.asp
- 『*Funk Odyssey Client User and Administration Guide, 4.0*』
  http://www.funk.com/Docs/odyc40man.pdf
- 『*Microsoft - Define 802.1X Authentication for Wireless Networks on Client Computers*』
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/fe1d12a1650a-4006-b389-e1f4ea68b991.mspx

業界標準

- 『*RFC 1994 - PPP Challenge Handshake Authentication Protocol (CHAP)*』
  http://www.faqs.org/rfcs/rfc1994.html
- 『*RFC 2716 - PPP EAP TLS Authentication Protocol*』
  http://www.faqs.org/rfcs/rfc2716.html
- 『*RFC 2759 - Microsoft PPP CHAP Extensions, Version 2*』
  http://www.faqs.org/rfcs/rfc2759.html
- 『*DRAFT Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control (Revision)*』
  http://standards.ieee.org/reading/ieee/std/lanman/restricted/802.1X-2004.pdf
- 『*RFC 2865 - Remote Authentication Dial In User Service (RADIUS)*』
  http://www.faqs.org/rfcs/rfc2865.html
- 『*RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』
  http://www.faqs.org/rfcs/rfc3580.html
- 『*RFC 3748 - Extensible Authentication Protocol (EAP)*』
  http://www.faqs.org/rfcs/rfc3748.html
- 『*Protected EAP Protocol (PEAP) Version 2*』
  http://www.faqs.org/ftp/pub/internet-drafts/draft-josefsson-pppext-eap-tls-eap-10.txt
- 『*EAP Flexible Authentication via Secure Tunneling (EAP-FAST)*』
  http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-02.txt