Technical Overview

NAC フレームワーク コンフィギュレーション ガイド

目次

NAC コンフィギュレーション ガイド

概要

このガイドは、Network Admission Control（NAC; ネットワーク アドミッション コントロール）フレームワークで使用する各コンポーネントの設定をサポートすることを目的としています。本書では、NAC で使用する Cisco Secure Access Control Server（ACS）の設定方法、Microsoft Windows プラットフォームへの Cisco Trust Agent（CTA）のインストール方法、Network Access Device（NAD; ネットワーク アクセス デバイス）として機能する Cisco IOS および CatOS ソフトウェアベースのスイッチの設定方法を説明します。NAC の設計および実装に関わる追加の考慮事項および情報については、『ネットワーク アドミッション コントロールの実装』を参照してください。

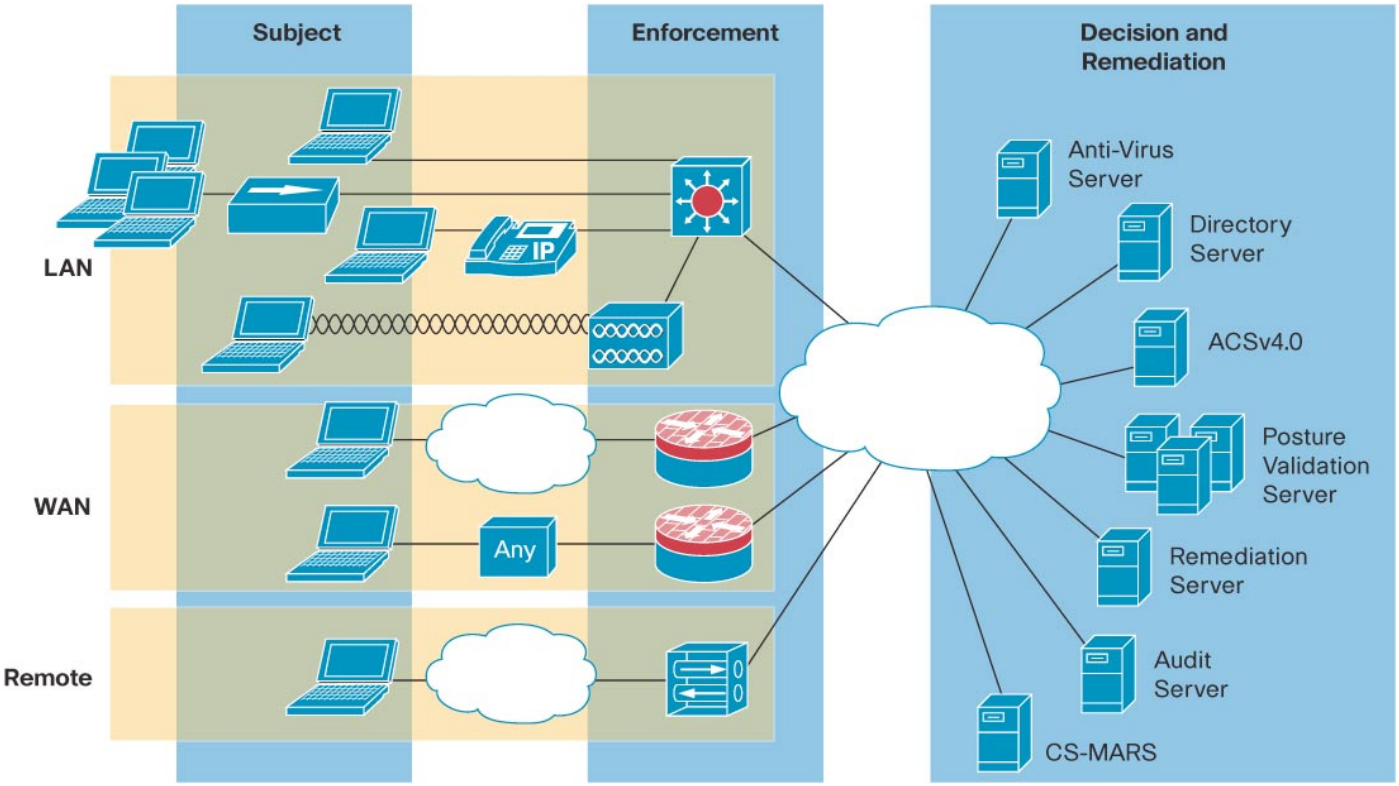
対象読者

本書は、Cisco NAC フレームワークの設定と実装を担当するセキュリティ エンジニア、ネットワーク エンジニア、エンジニアリング マネージャ、ネットワーク オペレータを対象としています。対象者が Microsoft Windows オペレーティング システムとクライアント マシン、および Cisco Secure ACS の設定と操作方法に精通していること、また Cisco IOS および CatOS デバイスの設定方法、Certificate Authority（CA; 認証局）とデジタル証明書が提供する信頼モデルを理解していることを前提として作成しています。

NAC のアーキテクチャと概要

NAC は、許可されていないエンドポイントや脆弱なエンドポイントからのネットワークへのアクセスを防止するために、ホストの状態（ポスチャ）のアセスメントを実施します。適合性の検証は、単一の ACS サーバで集中管理する許可ポリシーを通じて行うか、複数の NAC ポスチャ検証サーバに実施を委託します。一般的なエンドポイントはデスクトップ コンピュータ、ラップトップ、サーバですが、IP 電話、ネットワーク プリンタ、その他の専用ネットワーク接続デバイスもエンドポイントとして使用できます。

図 1. NAC フレームワーク実装シナリオ



Cisco NAC ポスチャ検証プロセスでは、次のような主要なコンポーネントが使用されます。

被験デバイス：

- **ホスト** — NAC を実施するネットワークにアクセスするマシン。
- **Posture Plugin（PP; ポスチャ プラグイン）** — ホストに常駐するシスコまたはサードパーティ製の DLL。同一のデバイスに常駐するポスチャ エージェントにホストのポスチャ クレデンシャルを提供します。
- **Posture Agent（PA; ポスチャ エージェント）** — ホスト上で 1 つまたは複数のポスチャ プラグインからポスチャ クレデンシャルを収集してネットワークと通信する、ホスト上の仲介役として機能するホスト エージェント ソフトウェア。シスコのポスチャ エージェント製品は、Cisco Trust Agent（CTA）です。
- **修復クライアント** — オペレーティング システムのパッチなど特定のクライアント ソフトウェアを更新するために修復サーバと連動する、修復管理ソリューションのコンポーネントの 1 つ。

NAC の実施：

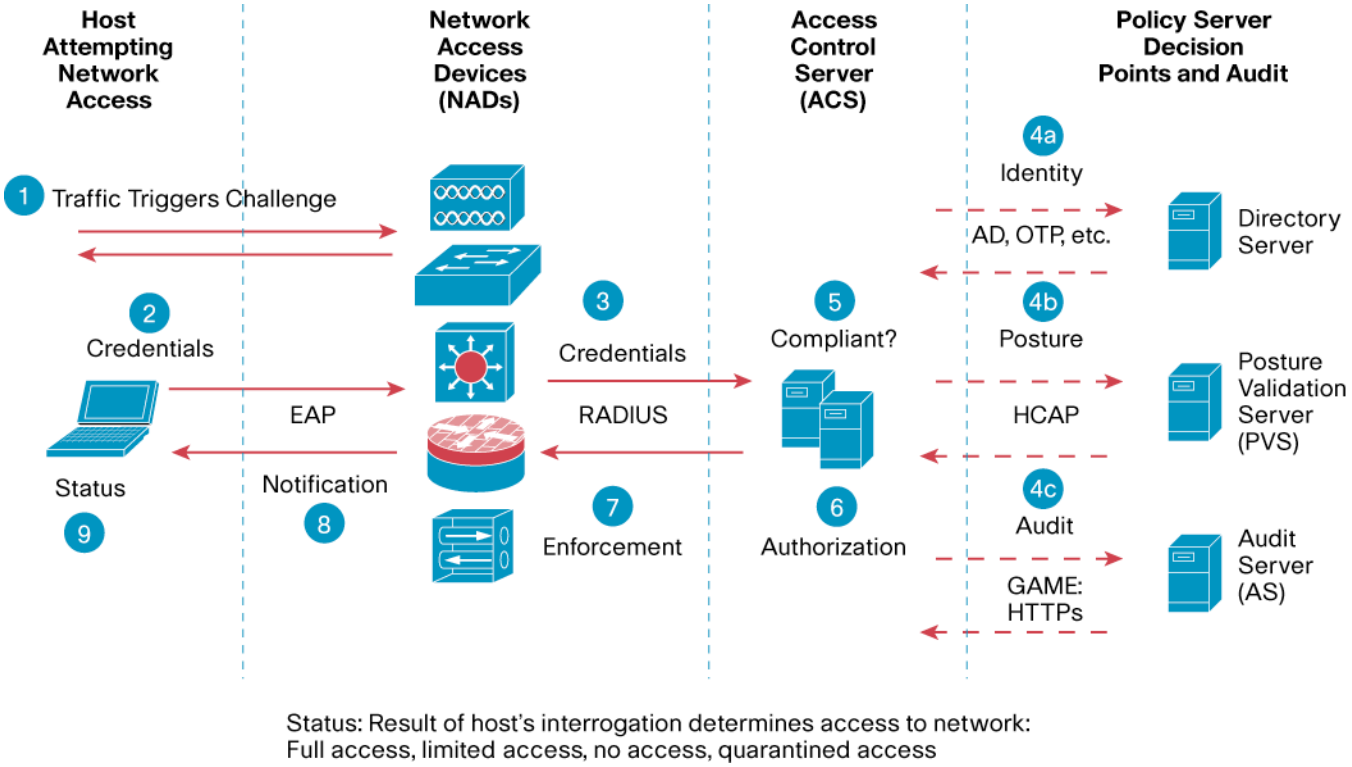
- **ネットワーク アクセス デバイス（NAD）**— NAC の実施ポイントとして機能するネットワーク デバイス。Cisco アクセス ルータ（800 - 7200）、VPN ゲートウェイ（VPN 3000 シリーズ）、Catalyst レイヤ 2 および レイヤ 3 スイッチ、ワイヤレス アクセス ポイントなどが含まれます。

決定と修復：

- **AAA（認証、許可、アカウンティング）サーバ** — 1 つまたは複数の認証や許可の決定を収集して単一のシステムの認証結果を決定し、NAD で NAC を実施するためにこの決定をネットワーク アクセス プロファイルにマッピングする、NAC の中心となるポリシー サーバ。Cisco Secure Access Control Server（ACS）は、NAC をサポートするシスコの AAA サーバ製品です。
- **ディレクトリ サーバ** — ユーザ、マシン、または両方の認証を行うための中央集中型のディレクトリ サーバ。ディレクトリ サービスには、Lightweight Directory Access Protocol （LDAP）、Microsoft Active Directory（AD）、Novell Directory Services （NDS）、One-time Token Password Servers （OTP） などがあります。
- **ポスチャ検証サーバ（PVS; Posture Validation Server）** — NAC におけるアプリケーション別のポリシー決定ポイントとして機能し、1 つまたは複数のポスチャ プラグインから収集したポスチャ クレデンシャルを一連のポリシー ルールと照合して認証を行う、1 つまたは複数のサードパーティ製のサーバ。アンチウイルス サーバ、セキュリティ アプリケーション サーバなどが PVS に該当します。
- **修復サーバ** — ポリシーに非適合のホストを適合させるために使用する管理ソリューション。専用のパッチ管理アプリケーションのほか、ソフトウェアを配布する Web サイトのような簡略なものも修復サーバに該当します。監査サーバ：ホストに対して Vulnerability Assessment（VA; 脆弱性アセスメント）を行い、ネットワーク アドミッションの前にホストの適合性のレベルやリスクを判定するサーバまたはソフトウェア

図 2 に、NAC アーキテクチャの主要なコンポーネントと、チャレンジ、許可、適合の強制を行う際の通信フローを示します。

図 2. NAC アーキテクチャの概要



NAC 許可プロセスは、次の手順で実施されます。各手順は、図 2 の数字に対応しています。

手順 1. NAC 対応のネットワーク アクセス デバイスが、ネットワーク リソースへの接続または使用を試みるホストを検出すると、ポスチャ検証が開始されます。

手順 2. NAD は、新しいエンドポイントを検出すると、AAA サーバ（ACS）とポスチャ エージェントとの間に通信パスを確立します。通信パスが確立されると、AAA サーバはエンドポイントに対して、1 つまたは複数のポスチャ プラグインのポスチャ クレデンシャルを要求します。

手順 3. ホストは、ホスト上の NAC の対応ソフトウェアコンポーネントが利用可能なポスチャ プラグインから収集したポスチャ クレデンシャルで要求に応答します。

手順 4. AAA サーバは、ローカルでポスチャ情報を検証するか、外部のポスチャ検証サーバに一部の決定を委託します。

手順 5. AAA サーバは、すべての代理サーバから各ポスチャ結果（ポスチャ トークン）を収集し、ホストの総合的な適合性（システム ポスチャ トークン）を決定します。

手順 6. タイマー、VLAN 割り当て、Downloadable ACL（Access Control List）といったの RADIUS アトリビュートで構成されるネットワーク アクセス プロファイルのネットワーク許可に、アイデンティティ（識別情報）の検証結果とシステム ポスチャ トークンがマッピングされます。

手順 7. これらの RADIUS アトリビュートが NAD に送信され、ホストで NAC が実施されます。

手順 8. 各プラグインにそれぞれのアプリケーションのポスチャとシステム全体のポスチャを通知するポスチャ ステータスが、ホストの CTA に送信されます。

手順 9. CTA の通知ダイアログを使用して、エンドユーザにメッセージを送信し、ネットワークにおける現在のホストの状態を通知できます（オプション）。

NAC アセスメント方式

NAC フレームワークでは、ホストとデバイスのポリシーへの適合性を検証するために、NAC L2 IP、NAC L3 IP、NAC L2 802.1X の 3 つのタイプのアセスメント方式を使用できます。NAC L2 IP と NAC L3 IP はともに、Extensible Authentication Protocol over UDP（EAPoUDP）をトランスポート メカニズムとして使用します。NAC L2 802.1X は、IEEE 802.1X をトランスポート メカニズムとして使用し、EAP-FAST（Flexible Authentication via Secure Tunneling）と呼ばれる新しい EAP 方式も使用します。図 2 に示したように、これらの方式の実施ポイントはネットワーク アクセス デバイスです。本書では、NAC L2 IP と NAC L2 802.1x の設定について説明します。NAC L3 IP の設定方法については、『ネットワーク アドミッション コントロールの実装』を参照してください。

NAC L2 IP

NAC L2 IP は、ホストのポスチャ アセスメントのトランスポートに EAP over UDP（EoU）を使用する点で NAC L3 IP と似ていますが、レイヤ 2 スイッチ ポートのレイヤ 3 に実装される点が NAC L3 IP と大きく異なります。

また NAC L2 IP には、Intercept ACL の概念がありません。NAC L2 IP では、NAD がホストから次のいずれかを受信したときにホストのポスチャ アセスメントが開始されます。

- DHCP 要求
- ARP 要求

NAD は、ホストから最初の DHCP または ARP 要求を受信すると、ホストに EoU 要求を送信してポスチャ検証プロセスを開始します。このプロセスは、クライアントからの DHCP 要求によって開始される場合、ARP 要求で開始されるときよりも早い時点で発生します。

NAC L2 802.lx

NAC L2 802.1x は、802.1x を活用してユーザおよびホストの認証情報を提供し、EAP-FAST プロトコルを使用してホストのポスチャ情報もトランスポートします。NAC L2 802.1x は、レイヤ 2 スイッチ ポート上で 802.1x を介してホストのアセスメントを開始します。

NAC L2 802.1x では、TLS トンネルでアイデンティティおよびポスチャ情報を転送するために、EAP-FAST for the EAP 方式をサポートするサプリカントが必要です。CTA に組み込まれたサプリカントは、EAP-FAST をサポートするほか、EAP-GTC、 EAP-MSCHAPv2、およびクライアント側認証のための EAP-TLS をサポートします。

次の表に、各方式の比較情報を示します。

表 1. NAC アセスメント方式の比較

アセスメント方式	長所	短所
統合レイヤ 2 アイデンティティおよびポスチャ	• NAC L2 802.1x でアイデンティティとポスチャを統合して検証 • L2 での実施 • Identity Based Networking Services（IBNS）に準拠	• NAC L2 IP および NAC L3 IP ではサポートされていない • 無線サポートのために、サプリカント ライセンスの購入が必要 • 監査を未サポート（将来的にサポート）
IEEE レガシー 802.1x およびポスチャ	• IBNS に準拠 • ポスチャを検証 • 監査をサポート	• 認証の順序のずれ（VLAN 割り当ての後にポスチャ検証） • 複数のクライアントまたは管理の複雑さ
IEEE レガシー 802.1x	IBNS に準拠	• ポスチャ検証なし • 監査を未サポート
ポスチャのみ（レイヤ 3）	• NAC L2 IP および NAC L3 IP • NAH 監査をサポート（L3-IP では将来的にサポート） • サプリカントはオプション	アイデンティティ検証なし

表 2. NAC アセスメント方式の機能とトレードオフ

機能	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
開始メカニズム	データ リンク アップ	DHCP または ARP	転送されたパケット
マシン アイデンティティ	✓	✓	
ユーザ アイデンティティ	✓		
ポスチャ	✓	✓	✓
VLAN 割り当て	✓		
URL リダイレクション		✓	✓
Downloadable ACL	6500 のみ（ポリシー ベース ACL）	✓	✓

機能	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
ポスチャ ステータス クエリー		✓	✓
802.1x ポスチャ変更	✓		

NAC リファレンス ネットワーク

次のネットワーク ダイアグラムは、IOS スイッチ設定関連セクションで参照してください。ホストである Client 1 は、ギガビット イーサネット 1/1 を通じて IOS スイッチに接続されています。このホストは、IOS スイッチの NAC L2 IP および NAC L2 802.1x セクション両方でクライアントとして動作します。本書では、Cisco Secure ACS、Microsoft Active Directory（AD）、アンチウイルス、修復、監査を含むすべてのサーバが VLAN 200 に配備されていることとします。

図 3. IOS スイッチ設定セクションで使用するリファレンス ネットワーク

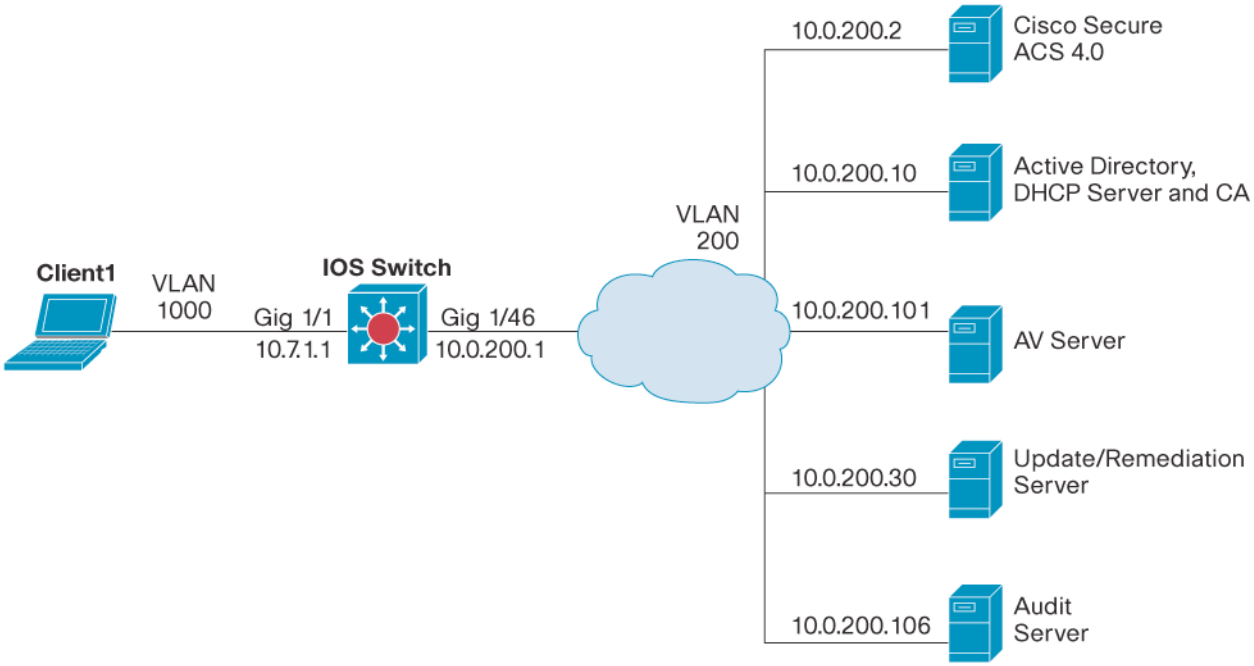
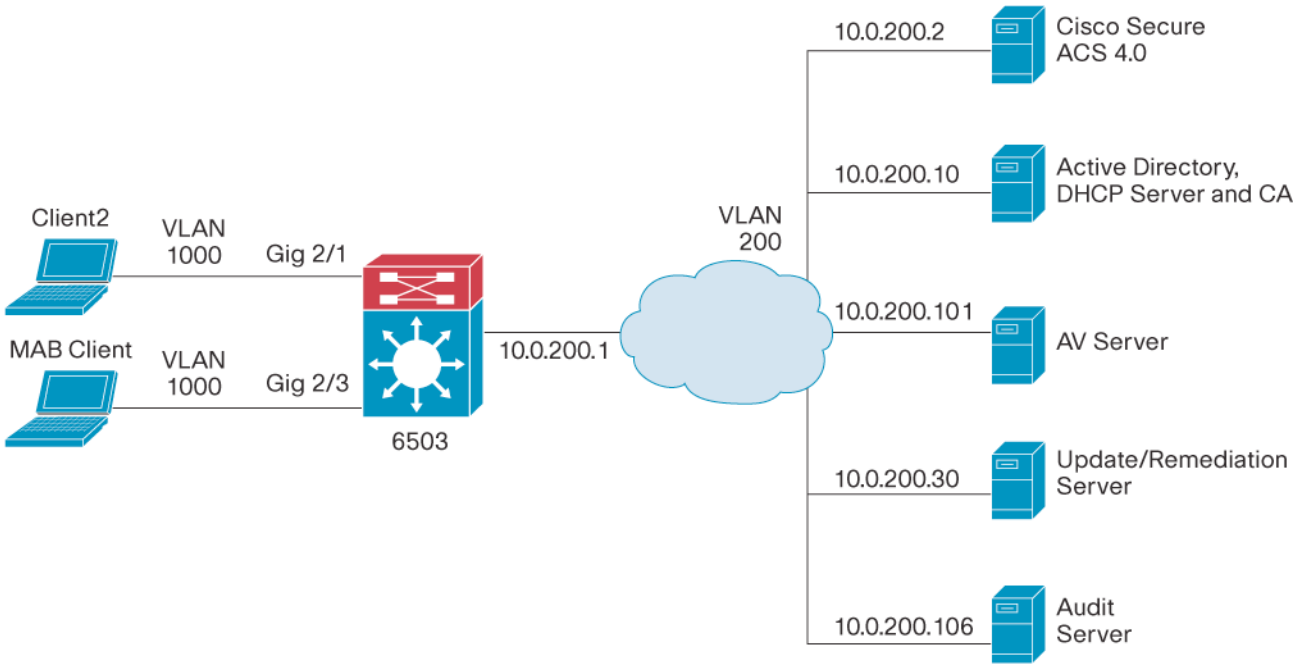


図 4 に示すリファレンス ネットワークは、CatOS スイッチ関連の設定セクションで参照してください。

Client 2 は、ポート 2/1 を通じて CatOS スイッチに接続されています。このホストは、CatOS スイッチの NAC L2 IP および NAC L2 802.1x セクション両方でクライアントとして動作します。3 つめのホストである MABClient は、ポート 2/3 を通じて CatOS スイッチに接続されています。このクライアントは、本書の MAC Authentication Bypass セクションでのみ使用します。本書では、Cisco Secure ACS、Microsoft AD、アンチウイルス、修復、監査を含むすべてのサーバが VLAN 200 に配備されていることとします。

図 4. CatOS スイッチ設定セクションで使用するリファレンス ネットワーク



NAC フレームワークでは、すべてのポリシー関連情報を Cisco Secure ACS に設定します。次のセクションでは、NAC のための基本的な Cisco Secure ACS 設定方法を説明します。特定のポリシーの追加の情報は、各アセスメント方式の設定セクションで説明します。

CISCO SECURE ACCESS CONTROL SERVER の一般的な設定

ここでは、Cisco Secure Access Control Server（ACS）がインストール済みで、NAC の設定を一切行っていないことを前提として、すべての NAC 実装シナリオで使用する Cisco Secure ACS 4.0 の基本的な設定方法を説明します。

注: NAC L2 IP および NAC L2 802.1X の実装には、Cisco ACS ソフトウェア v4.0 またはそれ以降のバージョンが必要です。このガイドでは、Cisco Secure ACS for Windows v4.0 を使用することを前提とし、ACS Solution Engine 固有の手順については説明しません。

ベンダ Attribute-Value Pair（AVP; アトリビュート値ペア）

NAC は、ユーザ アイデンティティまたはマシン アイデンティティ、およびその両方に加え、ホストのポスチャの適合性に基づいてネットワーク ホストを認証する機能も導入しました。ポスチャ適合性検証プロセスでは、ホストから送信されたクレデンシャルと、プロファイル ポリシーに定義された内容を比較します。要求されているクレデンシャルは、シスコまたは NAC パートナーのベンダが定義するアトリビュート値ペア（AVP）で作成されます。NAC アトリビュートは多くのベンダーやアプリケーションが提供しているため、Cisco Secure ACS にはデフォルトでシスコ以外の アトリビュートは含まれていません。したがって、NAC の適合性ポリシーで検証が必要な NAC Attribute Definition File（ADF; アトリビュート定義ファイル）は、ユーザが各ベンダからインポートする必要があります。

タスク 1：NAC パートナーの AVP のインポート

NAC アトリビュート定義ファイルをインポートするには、次の手順を実行します。ここでは、ユーザがすでにシスコ パートナーから ADF を取得し、ACS サーバにコピーしていることを前提としています。補足情報については、『Cisco Secure ACS 4.0 ユーザ ガイド』を参照してください。

手順 1. ACS サーバにコピーした ADF（.adf） ファイルの位置を確認します。

手順 2. この ADF ファイルを ACS ユーティリティの CSUtil.exe と同じディレクトリ（`<ACS Install Dir>\bin\`）、または CSUtil.exe. がアクセス可能なディレクトリに配置します。

手順 3. Cisco Secure ACS が稼動しているホストで MS DOS コマンド プロンプトを開き、CSUtil.exe. が配置されているディレクトリに変更します。

手順 4. 次のコマンドを使用して AVP を ACS に追加します。

```
CSUtil.exe -addAVP filename.adf
```

手順 5. 各 AVP の追加が正常に完了したら、次の ACS サービスの再起動が必要です。

- CSAdmin
- CSLog
- CSAuth

注: サービスには、**[スタート] > [プログラム] > [管理ツール] > [サービス]** を選択してアクセスできます。

ネットワーク設定

タスク 2：ネットワーク デバイス グループ（オプション）

ロケーションごと、またはサービスベースのフィルタリングに基づいて、ネットワーク アクセス デバイス（NAD）を Network Device Group（NDG; ネットワーク デバイス グループ）にグループ化する場合は、まず次の手順でネットワーク デバイス グループの使用をイネーブルにする必要があります。

手順 1. メインの ACS メニューから **Interface Configuration** を選択します。

手順 2. **Advanced Options** を選択し、ページ下部のボックスをクリックして **Network Device Groups** をイネーブルにします。この設定を行わないと、グループを割り当てられません。

手順 3. メインの ACS メニューから **Network Configuration** を選択し、**Add Entry** を選択します。**Network Device Group Name** と **Key** を入力します。

Network Device Group Name	Key
Switches	cisco123

タスク 3：AAA クライアントの設定

Network Configuration 画面で、**Network Device Group** の下のハイパーリンクを選択します。ネットワーク デバイス グループにまだ名前を割り当てていない場合は、*Not Assigned* と表示されます。このリンクをクリックすると **AAA Client** 画面が表示されます。

手順 1. **Add Entry** ボタンを選択して AAA クライアントを設定します。IP アドレスのワイルドカードを使用すると、すべての NAD を単一の AAA クライアントとして定義できます。

手順 2. Submit and Apply をクリックして変更を保存します。

（Not Assigned）AAA Clients				
AAA Client Hostname	**AAA Client IP Address**	**Key**	**Network Device Group**	**Authenticate Using**
Any	*.*.*.*	cisco123	（Not Assigned）	RADIUS（Cisco IOS/PIX 6.0）

注: ワイルドカードを使用した AAA クライアント定義は、認証のタイプに関わらず、他の AAA クライアント定義と同一にできません。

タスク 4：AAA サーバの設定

注: AAA サーバは、ホストのオペレーティング システムに割当てられたホスト名を使用して、ACS のインストール時に自動的に生成されます。

AAA サーバ情報は、ACS がインストールされているマシンのホスト名と IP アドレスを使用して生成されます。たとえば、次の手順 1 では、サーバ名 w2ks と IP アドレス 10.0.200.20 が予め設定されています。

手順 1. AAA Server Name のハイパーリンク w2ks を選択して、次に示すように AAA サーバの Key を設定します。

（Not Assigned）AAA Servers				
AAA Server Name	**AAA Server IP Address**	**AAA Server Type**	**Key**	**Network Device Group**
w2ks	10.0.200.20	Cisco Secure ACS	cisco123	（Not Assigned）

注: ACS サーバは、設定済みの Network Device Group にオプションで割り当てることができます。

インターフェイスの設定

RADIUS アトリビュートなど **Interface Configuration** セクションで設定する項目は、ACS 設定の他の部分で継承または使用できるように、この時点でイネーブルにしておく必要があります。

タスク 5：RADIUS アトリビュートの設定

メイン メニュー で Interface configuration ボタンを選択し、**RADIUS（IETF）** を選択して適切なアトリビュートを選択します。次に **RADIUS Cisco IOS/PIX6.0** を選択し、適切なアトリビュートを選択します。

手順 1. 必要な RADIUS アトリビュートを選択します。NAC に必要なのは以下に示すアトリビュートのみです。その他のすべてのアトリビュートは、以降の設定手順で時間を節約するために選択しないようにします。

RADIUS（IETF）	［027］Session-Timeout ［029］Termination-Action ［064］Tunnel-Type ［065］Tunnel-Medium-Type ［081］Tunnel-Private-Group-ID
RADIUS（Cisco IOS/PIX6.0）	［026/009/001］cisco-av-pair

注: アトリビュート 64、65、および 81 は、VLAN 割り当てにのみ必要です。

手順 2. **Interface Configuration > Advanced Options** を選択し、次のオプションをイネーブルにします。

Advanced Options：	Group-Level Shared Network Access Restrictions Group-Level Network Access Restrictions Group-Level Downloadable ACLs Network Access Filtering Distributed System Settings Cisco Secure ACS Database Replication Network Device Groups

注: ここで Group Downloadable ACLs ボックスを選択しないと、NAC L2 IP で Downloadable ACL を使用できません。

システム設定

メイン メニューから **System Configuration** を選択し、**ACS Certificate Setup** のリンク を選択して ACS Certificate Setup メニューを開きます。

タスク 6：ACS 証明書のセットアップ

Cisco Secure ACS は、クライアントにクレデンシャルを求めるチャレンジ要求の際にクライアントとの間に信頼を確立するために、デジタル証明書の設定が必要です。

注: 拡張性の高い NAC を実装するには、Production Public Key Infrastructure（PKI;公開キー インフラストラクチャ）と Production CA または Registration Authority（RA; 登録局）によって署名された証明書を使用することを強く推奨します。NAC 実装のこの部分の説明は大幅に省略されています。エンドポイント デバイス（CTA など）に ACS インフラストラクチャの身元を安全に証明するためには、内部、またはアウトソーシングした既存の PKI を使用する必要があります。認証局から証明書を取得する方法については、付録 4 を参照してください。

注: NAC 環境で NAC L2 802.1x を使用し、Microsoft Active Directory と統合する場合は、マシンおよびユーザ認証のために使用する認証メカニズムを検討する必要があります。

次に生成済みのデジタル証明書を使用して設定する例を示します。この例で証明書ファイルは、ACS サーバの `c:\files\certs\` に配置されています。

手順 1. **ACS Certificate Authority Setup** のリンクを選択します。CA 証明書のロケーションを指定し、**Submit** をクリックします。

ACS Certificate Authority Setup
Add new CA certificate to local certificate storage Certificate file: **C:\files\certs\ca.nac.cisco.com.cer**

手順 2. 新しい CA 証明書を追加したら、ACS を再起動します。**System Configuration > Service Control** を選択し、**Restart** をクリックします。

手順 3. 新しい CA 証明書をインストールしたら、Certificate Trust List（CTL; 証明書信頼リスト）に信頼できる機関として追加する必要があります。**ACS Certificate Setup** 画面のリンクから **Edit Certificate Trust List** を選択し、リストから該当の CA 名の隣のボックスをチェックし、**Submit** をクリックして変更を保存します。

Edit the Certificate Trust List（CTL）
ca

手順 4. CTL を変更したら、ACS の再起動が必要です。**System Configuration > Service Control** を選択して、**Restart** ボタンをクリックします。

手順 5. **Install Certificate** リンクを選択します。ACS 証明書のロケーションを指定し、**Submit** をクリックします。

Install New Certificate	
Read certificate from file	
Certificate file:	**C:\files\certs\ACS-1.nac.cisco.com.cer**
Private key file:	**C:\files\certs\ACS-1.PrivateKey.txt**
Private key password:	**cisco123**

手順 6. ACS 証明書をインストールしたら、ACS の再起動が必要です。メイン メニューから **System Configuration > Service Control** を選択して、**Restart** をクリックします。これで ACS 証明書インストール プロセスが完了です。

タスク 7：グローバル認証のセットアップ

Cisco Secure ACS は、認証および許可で使用するクレデンシャルをホストから Cisco Secure ACS に安全に転送するためにさまざまなプロトコルをサポートしています。したがって Cisco Secure ACS に対して、許可するプロトコルおよび各プロトコルのデフォルト設定を指定する必要があります。

注: 環境が限定されている場合およびセキュリティ上の特定の懸念がある場合を除き、すべてのプロトコルをグローバルにイネーブルにすることを推奨します。実際に使用するプロトコル オプションは、後で NAC のネットワーク アクセス プロファイルを作成するときに制限できますが、ここでイネーブルにしていないプロトコルは、ネットワーク アクセス プロファイルで使用できません。

手順 1. メイン メニューから **System Configuration** を選択し、**Global Authentication Setup** をクリックします。

手順 2. Network Access Profile の Authentication 設定で使用可能にするために、次のグローバル認証パラメータを選択します。

EAP Configuration	
PEAP	
Allow EAP-MSCHAPv2	
Allow EAP-GTC	
Allow Posture Validation	
Cisco client initial message:	**<empty>**
PEAP session timeout (minutes):	**120**
Enable Fast Reconnect:	**Yes**
EAP-FAST	
EAP-FAST Configuration（以下を参照）	
EAP-TLS	
Allow EAP-TLS	
Select one or more of the following options:	
Certificate SAN comparison	
Certificate CN comparison	
Certificate Binary comparison	
EAP-TLS Session Timout (minutes):	**120**

EAP Configuration

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds): **20**

MS-CHAP Configuration

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

手順 3. **Submit + Restart** をクリックして変更を保存します。

手順 4. **EAP-FAST Configuration** をクリックし、EAP-FAST 画面に入力します。

EAP-FAST Settings

EAP-FAST

Allow EAP-FAST

Active master key TTL: **1 month**

Retired master key TTL: **3 month**

Tunnel PAC TTL: **1 week**

Client Initial Message: <empty>

Authority ID Info: **cisco**

Allow anonymous in-band PAC provisioning

Allow authenticated in-band PAC provisioning

Accept client on authenticated provisioning

Require client certificate for provisioning

Allow Machine Authentication

Machine PAC TTL **1 week**

Allow Stateless Session Resume

Authorization PAC TTL **1 hour**

Allow inner methods

EAP-GTC

EAP-MSCHAPv2

EAP-TLS

Select one or more of the following EAP-TLS comparison methods:

Certificate SAN comparison

Certificate CN comparison

Certificate binary comparison

EAP-TLS session timeout (minutes): **120**

EAP-FAST master server

Actual EAP-FAST server status: **Master**

タスク 8：ロギングするアトリビュートの設定

注: ホストから送信されるシスコ以外の NAC アトリビュート値をロギングするには、まずアトリビュート定義ファイルを ACS にインポートし、ロギングをイネーブルにする必要があります。

手順 1. イネーブルにするログ ファイルとそのログ ファイルに記録するイベント アトビュートを設定します。メイン メニューから **System Configuration** オプションを選択し、**Logging** を選択します。

NAC で推奨するログ ファイルとロギングされるアトリビュートを示します。実際にロギングされるアトリビュートのリストは、環境に関連する NAC ベンダ アトリビュートによって、さらに多くなることがあります。

CSV Failed Attempts **Log to CSV Failed Attempts**	**CSV Passed Authentications** **Log to CSV Passed Auths**	**CSV RADIUS Accounting** **Log to RADIUS Accounting**
ロギングされるアトリビュート	ロギングされるアトリビュート	ロギングされるアトリビュート
Message-Type	Message-Type	User-Name
User-Name	User-Name	Group-Name
Caller-ID	Caller-ID	Calling-Station-Id A
Authen-Failure-Code	NAS-Port	Acct-Status-Type
NAS-Port	NAS-IP-Address	Acct-Session-Id
NAS-IP-Address	AAA Server	Acct-Session-Time
AAA Server	Filter Information	Acct-Input-Octets
Network Device Group	Network Device Group	Acct-Output-Octets
Access Device	Access Device	Acct-Input-Packets
PEAP/EAP-FAST-Clear-Name	PEAP/EAP-FAST-Clear-Name	Acct-Output-Packets
Logged Remotely	Logged Remotely	Framed-IP-Address
EAP Type	EAP Type	NAS-Port
EAP Type Name	EAP Type Name	NAS-IP-Address
Network Access Profile Name	Network Access Profile Name	Class
Shared RAC	Outbound Class	Termination-Action
Downloadable ACL	Shared RAC	Called-Station-Id
System-Posture-Assessment(Token)	Downloadable ACL	Acct-Delay-Time
Application-Posture-Assessment	System-Posture-Assessment	Acct-Authentic
Reason	Application-Posture-Assessment	Acct-Terminate-Cause
cisco-av-pair	Reason	Event-Timestamp
Cisco:PA:PA-Name	Cisco:PA:PA-Name	NAS-Port-Type
Cisco:PA:PA-Version	Cisco:PA:PA-Version	Port-Limit
Cisco:PA:OS-Type	Cisco:PA:OS-Type	NAS-Port-Id
Cisco:PA:OS-Version	Cisco:PA:OS-Version	AAA Server
Cisco:Host:ServicePacks	Cisco:Host:ServicePacks	ExtDB Info
Cisco:Host:Hotfixes	Cisco:Host:Hotfixes	Network Access Profile Name
Cisco:Host:Package	Cisco:Host:Package	cisco-av-pair
		Access Device
		Logged Remotely

アドミニストレーション コントロール

タスク 9：リモート アドミニストレータ アクセスの追加

Web ブラウザを介してリモートから ACS を管理するには、メイン メニューから **Administration Control** ボタンを選択して、この機能をイネーブルにする必要があります。1 つまたは複数のアカウントを追加すると、HTTP を介して ACS にログインすることができます。

手順 1. **Add Administrator** ボタンを選択し、Administration Control セクションに次の情報を追加します。

Administrator Name：	Administrator
Password：	cisco123
Administrator Privilege：	Grant All

Shared Profile Component（共有プロファイル コンポーネント）

共有プロファイル コンポーネントは、ACS 内でのフィルタリングや RADIUS 内でのネットワーク認証のために、さまざまなネットワーク アクセス プロファイルで再利用可能な設定です。共有プロファイル コンポーネントは、ネットワーク アクセス プロファイルを設定する前に定義しておく必要があります。

注: ネットワーク アクセス プロファイルは Cisco Secure ACS 4.0 の新機能です。認証、ポスチャ検証および許可コンポーネントを個別に作成し、使用するアクセス方式や NAD の IP アドレスに応じて、マッピングすることができます。

タスク 10：Downloadable ACL の設定

最初に設定する共有コンポーネントは Downloadable ACL です。レイヤ 3 または レイヤ 4（L3/L4）の Access Control Entry（ACE; アクセス コントロール エントリ）がルータまたは VPN コンセントレータにダイナミックにダウンロードされ、このリストを使ってホストからネットワークへのアクセスが許可されます。これらの ACL は、デフォルトのインターフェイス ACL よりも優先されます。

次に ACL の例を示します。組織で実際に使用する ACL の定義は、適用する前に VoIP、セキュリティ ポリシーなど使用するアプリケーションやサービスに基づいて入念に調査、検証する必要があります。

手順 1. 次に示す ACL を設定します。メイン メニューから **Shared Profile Components** を選択し、**Downloadable IP ACLs** を選択します。**Add** ボタンをクリックして新しい ポスチャ ACL を作成します。ネットワークで使用する各 ACL 定義（例：healthy_acl）に対して新しい ACE（アクセス コントロール エントリ）を追加します。このポスチャ ACL に適切なすべての ACE を入力したら、**Submit** をクリックしてこの ACL の ACE を保存します。最後にもう一度 **Submit** をクリックしてこのポスチャ ACL を保存します。

手順 2. ポリシーで使用する 2 つめのポスチャ ACL （quarantine_acl）を作成します。この例は、リファレンス ネットワーク アーキテクチャの IP アドレスを使用して設定しています。

Name	NAF	ACL Definition
healthy_acl	(All-AAA-Client)	permit ip any any
quarantine_acl	(All-AAA-Client)	remark Allow DHCP permit udp any eq bootpc any eq bootps remark Allow EAPoUDP permit udp any any eq 21862 remark Allow DNS permit udp any any eq 53 remark Allow HTTP to UpdateServer permit tcp any host 10.0.200.30 eq www remark allow client access to qualys permit ip any host 10.0.200.106

注: Downloadable IP ACL オプションが表示されない場合は、RADIUS Attributes セクションで Downloadable ACLs をイネーブルにする必要があります。

タスク 11：RADIUS Authorization Component（RAC; RADIUS 許可コンポーネント）

RADIUS 許可コンポーネントは、ネットワーク許可中にネットワーク アクセス デバイスに適用される RADIUS アトリビュートのセットです。

手順 1. RAC を設定します。メイン メニューから **Shared Profile Components** を選択して **RADIUS Authorization Components** を選択し、新しい各 RAC に対して **Add** ボタンをクリックします。各 RAC には、Cisco IOS/PIX 6.0、IETF、Ascend など 1 つまたは複数のベンダの RADIUS アトリビュートを追加できます。

注: NAC で使用する Session-Timeout 値は、ACS のパフォーマンスに大きな影響を及ぼす可能性があります。したがって、ネットワークの規模や ACS トランザクションのキャパシティに応じて調整することを強く推奨します。

手順 2. NAC L2 IP 用に次の RAC エントリ、割り当てるアトリビュート、値を作成します。

注: 次に示す RAC は、NAC L2 IP 用と NAC L2 802.1x 用に分かれています。RAC は、異なるタイプの NAC サービスや異なるロケーション別にも設定することができます。

RAC Name	Vendor	Assigned Attributes	Value
L2_IP_Healthy_RAC	Cisco	cisco-av-pair (1)	status-query-timeout=300
	Cisco	cisco-av-pair (1)	sec:pg=Healthy_hosts
	IETF	Termination-Action (29)	RADIUS-Request (1)
	IETF	Session-Timeout (27)	36000
L2_IP_Transition_RAC	IETF	Session-Timeout (27)	60
	IETF	Termination-Action (29)	RADIUS-Request (1)
L2_IP_Quarantine_RAC	Cisco	cisco-av-pair (1)	status-query-timeout=300
	Cisco	cisco-av-pair (1)	url-redirect-acl=quarantine_url_redir_acl
	Cisco	cisco-av-pair (1)	sec:pg=Quarantine_hosts

RAC Name	Vendor	Assigned Attributes	Value
	IETF	Session-Timeout (27)	36000
	IETF	Termination-Action (29)	RADIUS-Request (1)

注: RADIUS アトリビュートの詳細情報については、付録 2 を参照してください。

注: url-redirect-acl アトリビュートで指定する ACL は、スイッチ上に設定しておく必要があります。このアトリビュートでは大文字と小文字が区別され、名前が厳密にマッチする必要があります（この例の ACL 名：**quarantine_url_redir_acl**）。ACL 名がマッチしなければ、この ACL はスイッチ上で機能しません。

注: url-redirect 文字列用の シスコ AVP は RAC に入力可能ですが、この URL 値は **NAP > posture validation > Specific Rule > System Posture Token Configuration > URL Redirect** フィールドを使用して入力することを推奨します。

手順 3. NAC L2 802.1x 用の次の RAC エントリ、割り当てるアトリビュート、値を作成します。

RAC Name	Vendor	Assigned Attributes	Value
L2_1x_Healthy_RAC	IETF	Session-Timeout (27)	3600
	IETF	Termination-Action (29)	RADIUS-Request (1)
	IETF	Tunnel-Type (64)	[T1] VLAN (13)
	IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
	IETF	Tunnel-Private-Group-ID (81)	[T1] healthy
L2_1x_Transition_RAC	IETF	Session-Timeout (27)	30
	IETF	Termination-Action (29)	RADIUS-Request (1)
L2_1x_Quarantine_RAC	IETF	Session-Timeout (27)	3600
	IETF	Termination-Action (29)	RADIUS-Request (1)
	IETF	Tunnel-Type (64)	[T1] VLAN (13)
	IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
	IETF	Tunnel-Private-Group-ID (81)	[T1] quarantine

参考のために、NAC の RADIUS-Accept 応答で ACS から送信される可能性があるすべてのアトリビュートを表 3 に示します。

表 3. RADIUS アトリビュート

NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP	#	アトリビュート名	説明
✓			1	User-Name	アクセス要求の EAP アイデンティティ応答からコピーされる。
	✓	✓	8	Framed-IP-Address	ホストの IP アドレス。
	✓	✓	26	Vendor-Specific Cisco（9、1） CiscoSecure-Defined-ACL	ACL 名。 ACS により自動的に送信される。
✓			26	Vendor-Specific Cisco（9、1） sec:pg	ポリシーベースの ACL 割り当て。Catalyst 6000 のみに適用。 sec:pg = <group-name>
	✓	✓	26	Vendor-Specific Cisco（9、1） url-redirect	リダイレクション URL。 url-redirect=<URL>
	✓	✓	26	Vendor-Specific Cisco（9、1） url-redirect-acl	リダイレクト URL のために名前付きの ACL を適用。ACL は NAD のローカルへの定義が必要。IOS スイッチでのみ使用可能。 url-redirect-acl=<ACL-Name>
✓	✓	✓	26	Vendor-Specific、Cisco（9、1）、posture-token	ポスチャ トークン/ステート名。 ACS により自動的に送信される。
	✓	✓	26	Vendor-Specific Cisco（9、1） status-query-timeout	ステータス クエリー タイマーを設定。
	✓	✓	26	Vendor-Specific Cisco（9、1） host-session-id	監査に使用されるセッション識別子。 ACS により自動的に送信される。
	✓	✓	26	Vendor-Specific Microsoft = 311	ステータス クエリーのキー：MS-MPPE-Recv-Key ACS により自動的に送信される。
✓	✓	✓	27	Session-Timeout	再検証タイマーを設定（秒）。
✓	✓	✓	29	Termination-Action	セッション タイムアウトのアクション。 （0）デフォルト：セッションの終了 （1）Radius 要求：再認証
✓			64	Tunnel-Type	13 = VLAN
✓			65	Tunnel-Medium-Type	6 = 802
✓	✓	✓	79	EAP Message	Access Request および Access Challenge の EAP 要求/応答パケット。 • Access Accept では EAP Success • Access Reject では EAP Failure
?	?	?	80	Message Authenticator	パケットの完全性を保証するための HMAC-MD5。
✓			81	Tunnel-Private-Group-ID	VLAN 名。

グループとユーザのセットアップ

タスク 12：グループのセットアップ

ここでは認証にローカルのユーザ名とグループを使用する例を示します。この方法により、Cisco Secure ACS と Microsoft Active Directory との統合前にユーザ認証を行うことができます。ユーザおよびグループ認証のために ACS と Microsoft AD を統合する方法は、本書の別のセクションで説明します。

Group and User Setup			
Group Number	**Group Name**	**Local ACS Users**	**Password**
1: Group 1	Employees	Administrator	cisco
1: Group 1	Employees	employee1	cisco
2: Group 2	Contractors	contractor1	cisco
3: Group 3	Guest	guest1	cisco
4: Group 4	Utilities	Utilities1	cisco

手順 1. メイン ACS メニューから **Group Setup** をクリックします。

手順 2. **Rename** をクリックします。最初の 3 つのデフォルト グループ名は自由に変更できます。この設定例では、メイン メニューから Group Setup を選択し、上記の表に示す名前に変更します。Application Specific Device（ASD; アプリケーション固有デバイス）に使用するもう 1 つのグループも名前を変更します。

タスク 13：ユーザ セットアップ

手順 1. メイン ACS メニューから **User Setup** をクリックします。**User** ダイアログ ボックスで最初のユーザ名に上記の表のように **employee1** を入力し、**Add/Edit** ボタンをクリックします。

手順 2. **User Setup** 下の **User: employee1（New User）** 画面で、ユーザのパスワードとして **cisco** を入力します。**Group to which the user is assigned** ドロップダウン ボックスで、このユーザを **Employees** グループに割り当てます。下までスクロールして **Submit** をクリックします。

手順 3. 残りの各ユーザ（**contractor1、guest1、utilities**）に対して同じ手順を繰り返します。

注: 各 RADIUS アトリビュートは、ネットワーク アクセス プロファイルのセクションで設定、適用されるため、各グループに対して設定する必要はありません。

ポスチャ検証

ポスチャ検証は、NAC 設定の中心となる要素です。ポスチャ検証のセクションでは、ホストのポスチャの適合性を検証するルールを作成します。この適合性の結果として、ネットワークへのアクセスを許可または拒否するトークンが NAD に送信されます。このトークンには、Healthy、Checkup、Transition、Quarantine、Infected および Unknown があります。

Cisco Secure ACS は、次の方法でポスチャ検証を実行できます。

- Cisco Secure ACS のローカルで検証する
- HCAP プロトコルを介し、1 つまたは複数のポスチャ検証サーバ（PVS）を使用して外部で検証する
- GAME プロトコルを介し、NAC Agentless Host（NAH; NAC エージェントレス ホスト）をサポートする監査サーバを使用して検証する

注: ローカルおよび外部でのポスチャ検証は同時に実行できます。ただし、ローカルおよび外部で同一の NAC クレデンシャル タイプ（ベンダ/アプリケーションの組み合わせ）を同時に検証することはできません。たとえば、Trend Micro の情報をローカルの ACS および外部の Trend Policy Server で同時に検証することはできません。

ポスチャ検証ポリシーは、ACS のメイン メニューの **Posture Validation** で設定します。これらのポリシーは、後で選択してネットワーク アクセス プロファイルに適用します。ポリシーは個別に定義するので、組み合わせたり再利用したりして、多くのロケーションの複数のネットワーク サービスに対して異なるアクセスを提供することができます。

タスク 14：内部ポスチャ検証のセットアップ

ポスチャ検証ポリシーはルールで構成されます。これらのルールは一連の条件から作成します。クライアントから受信するクレデンシャルが各条件に一致すると、ポリシー アセスメント結果が得られます。

手順 1. リファレンス ネットワークのポリシー要件を ACS のローカルに作成するには、次の表に従って NAC ポスチャ検証ポリシーを定義します。これらのポリシーを作成するには、メイン メニューから **Posture Validation** を選択し、**Internal Posture Validation Setup** を選択します。

手順 2. **Add Policy** を選択して新しいポリシーを作成します。

手順 3. 新しいポスチャ検証ポリシーの名前および説明（任意）を入力し、**Submit** をクリックします。

手順 4. この新しいポリシーを構成するポスチャ検証ルールを入力します。特定のポスチャ アセスメント結果を得るために必要な条件をこのポリシーに設定します。このルールを作成するには、**Add Rule** をクリックします。

手順 5. **Add Condition Set** をクリックし、ポスチャ検証ルールの条件を定義する画面を開きます。

手順 6. 次の表を参考に、必要な条件の定義に適した Attribute、Operator、Value を追加し、**Submit** をクリックします。たとえば、クライアントの CTA のバージョンを検証する条件を設定するには、**Attribute** メニューから *Cisco:PA:PA-Version* クレデンシャルを選択し、Operator を >= に変更し、Value フィールドに 2.0.0.30 と入力して **Enter** をクリックします。複数のクレデンシャルを同時に検証する必要がある場合は、ルールに条件を追加します。

注: 単一のルールとして複数の条件を検証するには、**Submit** を選択したあと、*Match 'OR' inside Condition and'AND' between Condition Sets* オプションを選択してもう一度 **Submit** をクリックします。

手順 7. **Done** をクリックして最初の **Posture Validation Rules** 画面に戻ります。

手順 8. ルールに必要なすべての変更を行ったら、ページ下部の **Apply and Restart** をクリックします。

Policy Name	#	Condition	Posture Assessment	Notification String
CTA	1	Cisco:PA:PA-Version >= 2.0.0.30 AND Cisco:PA:Machine-Posture-State >= 1	Cisco:PA:Healthy	
	2	Default	Cisco:PA:Quarantine	
Windows	1	(Cisco:PA:OS-Type contains Windows XP AND Cisco:Host:ServicePacks contains 2) OR (Cisco:PA:OS-Type contains Windows 2000 AND Cisco:Host:ServicePacks contains 4)	Cisco:Host:Healthy	
	2	Default	Cisco:Host:Quarantine	
CSA	1	Cisco:HIP:CSAOperationalState = 1 AND Cisco:HIP:CSAVersion >= 4.5.0.0	Cisco:HIP:Healthy	
	2	Default	Cisco:HIP:Quarantine	

注: ルールの定義時にすべてのルールに通知文字列（notification string）を指定できます。通知文字列に入力があると、CTA はクライアント デバイス上でデフォルトの Web ブラウザの起動を試みます。たとえば、ルールのポスチャ アセスメントの通知文字列に http://x.x.x.x/quarantine.html と入力すると、自動的にブラウザを起動して検疫アセスメントを行うことができます。

Network Access Profile（ネットワーク アクセス プロファイル）

ネットワーク アクセス プロファイルの設定方法は、各アクセス方式（NAC L2 IP、NAC L2 802.1x、NAC エージェントレス ホスト（NAH））のセクションで説明します。

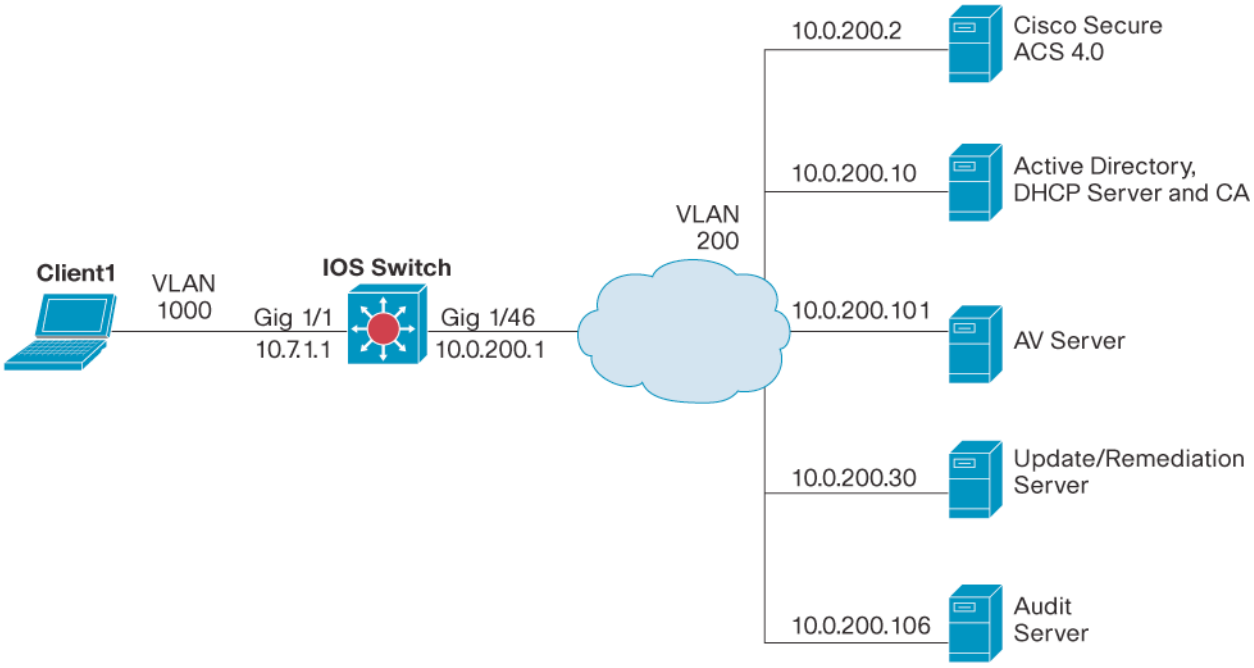
IOS スイッチの NAC L2 IP 設定

このセクションでは、IOS スイッチ上で NAC L2 IP の基本機能をイネーブルにする各種コンポーネントの設定方法を説明します。次の順序で操作を行います。

1. ネットワーク接続性のテスト（NAD と ACS サーバ間）
2. IOS スイッチへの NAC L2 IP の設定
3. クライアントへの Cisco Trust Agent のインストールと設定
4. Cisco Secure ACS 4.0 への NAC L2 IP の設定
5. NAC L2 IP 機能のテスト
6. NAC L2 IP のための監査（Qualys、NAD、ACS）サポートの設定
7. 監査設定のテスト
8. NAC L2 IP のエージェントレス ホスト サポートの設定
9. NAC L2 IP のエージェントレス ホスト サポートのテスト

図 5 は、このセクションで説明する NAC L2 IP 設定情報で参照してください。

図 5. IOS スイッチ参照図



ネットワーク接続性のテスト

スイッチ コンソールおよびその他の必要なサーバ（DHCP、DNS、修復、Antivirus（AV; アンチウイルス）など）から ACS サーバに ping できることを確認します。

IOS スイッチへの NAC L2 IP の設定

タスク 1：AAA の設定

Cisco NAC で使用する Cisco ISO スイッチで NAC L2 IP のために AAA をイネーブルにするには、以下の手順を実行します。

手順 1. **aaa new-model** グローバル設定コマンドを使用して、スイッチ サービス上で AAA をイネーブルにします。

```
IOS-Switch(config)#aaa new-model
```

手順 2. **aaa authentication eou default group radius** コマンドを使用して、スイッチが EAPoUDP の認証に RADIUS を使用するように設定します。

```
IOS-Switch(config)#aaa authentication eou default group radius
```

手順 3. **aaa authorization network default group radius** コマンドを使用して、スイッチがすべてのネットワーク関連サービス要求に対して許可を実行するように設定します。

```
IOS-Switch(config)#aaa authorization network default group radius
```

手順 4. **aaa accounting network default start-stop group radius** コマンドを使用して、EAPoUDP 認証のために AAA アカウンティングをイネーブルにします。

```
IOS-Switch(config)#aaa accounting network default start-stop group radius
```

タスク 2：RADIUS サーバの設定

Cisco IOS 上に RADIUS サーバを設定するために必要な最小限の手順を説明します。

手順 5. **radius-server host** コマンドを使用して、RADIUS サーバのホスト名または IP アドレス（およびオプションで認証およびアカウンティング ポート）を設定します。認証用のデフォルトの RADIUS ポート番号は 1645 です。アカウンティング用のデフォルトの RADIUS ポート番号は 1646 です。

```
IOS-Switch(config)#radius-server host 10.0.200.20
```

手順 6. **radius-server key** コマンドを使用して、RADIUS サーバの暗号化キーを指定します。このキーは、Cisco Secure ACS Server でこの NAD に対して設定されたキーと一致する必要があります。一致しなければ、NAD および Cisco Secure ACS はポスチャ検証情報を交換できません。「ACS の一般的な設定」のセクションの「タスク 3： AAA クライアントの設定」を参照してください。

```
IOS-Switch(config)#radius-server key cisco123
```

手順 7. **radius-server attribute 8 include-in-access-req** コマンドを使用して、スイッチが Access-Request および Accounting-Request パケットで Framed-IP-Address RADIUS アトリビュート（Attribute[8]）を送信するように設定します。

```
IOS-Switch(config)#radius-server attribute 8 include-in-access-req
```

手順 8. **radius-server vsa send authentication** コマンドを使用して、NAD がベンダ固有アトリビュートを認識、使用するように設定します。

```
IOS-Switch(config)#radius-server vsa send authentication
```

手順 9. **ip radius source-interface** コマンドを使用して、すべての発信 RADIUS パケットの NAD インターフェイスを指定します。

```
IOS-Switch(config)#ip radius source-interface Vlan200
```

注: 手順 9 はオプションですが、NAD と Cisco Secure ACS との間に複数のパスがある場合には、指定することを推奨します。ソース インターフェイスを指定することにより、Cisco Secure ACS は、RADIUS メッセージの送信元の NAD を認識できるようになります。この NAD を示す Cisco Secure ACS AAA クライアント レコードにこれと同じ IP アドレスを設定する必要があります。

タスク 3：IP デバイス トラッキング と DHCP スヌーピングのイネーブル

IP デバイス トラッキングをイネーブルにしている場合、スイッチはホストを検出すると、ホストの IP と MAC アドレス、スイッチがホストを検出したインターフェイスなどの情報を含むエントリを IP デバイス トラッキング テーブルに追加します。ホストが検出されると、ホストのステートは ACTIVE に設定されます。

手順 1. スイッチ上で IP デバイス トラッキングをイネーブルにします。オプションでプローブ カウントとプローブの間隔を設定できます。

```
IOS-Switch(config)#ip device tracking
```

手順 2. NAC ポスチャ検証の開始に使用する DHCP スヌーピングを設定します（オプション）。

```
IOS-Switch(config)#ip dhcp snooping
```

手順 3. クライアント VLAN で DHCP スヌーピングをイネーブルにします。

```
IOS-Switch(config)#ip dhcp snooping vlan 1000
```

手順 4. DHCP スヌーピングが DHCP サーバ上のポートを信頼するように設定します。この例では、このポートはギガビット イーサネット 1/46 です。

```
IOS-Switch(config-if)#ip dhcp snooping trust
```

タスク 4：インターフェイス ACL の設定

ここでは、NAD に インターフェイス ACL を設定するために必要な手順を説明します。

着信クライアント トラフィックに適用するデフォルト ACL を作成します。この ACL は、以降のセクションでクライアントの着信スイッチ ポートに適用されます。この ACL はスイッチ ポートのデフォルト セキュリティ ポリシーです。ACS からダウンロードされる ACL はすべて、インターフェイス ACL に優先して適用されます。

手順 1. インターフェイス ACL を設定します。

```
IOS-Switch(config)#ip access-list extended interface_acl
IOS-Switch(config-ext-nacl)#permit udp any any eq 21862
IOS-Switch(config-ext-nacl)#remark Allow DHCP
IOS-Switch(config-ext-nacl)#permit udp any eq bootpc any eq bootps
IOS-Switch(config-ext-nacl)#remark Allow DNS
IOS-Switch(config-ext-nacl)#permit udp any any eq domain
IOS-Switch(config-ext-nacl)#remark Allow HTTP access to update server
IOS-Switch(config-ext-nacl)#permit tcp any host 10.0.200.30 eq www
IOS-Switch(config-ext-nacl)#remark Allow ICMP for test purposes
IOS-Switch(config-ext-nacl)#permit icmp any any
IOS-Switch(config-ext-nacl)#remark Implicit Deny
IOS-Switch(config-ext-nacl)#deny ip any any
```

タスク 5：Cisco NAC のグローバル ポリシーの設定

ここでは、Cisco IOS スイッチに Cisco NAC グローバル ポリシーを設定するために必要な手順を説明します。

手順 1. EAPoUDP ポスチャ プロセスをイネーブルにする IP アドミッション ルールを作成します。

```
IOS-Switch(config)#ip admission name NAC-L2-IP eapoudp
```

タスク 6：Cisco NAC インターフェイスの設定

ここでは、Cisco IOS スイッチに Cisco NAC インターフェイスを設定するために必要な手順を説明します。

手順 1. 作成した インターフェイス ACL をクライアント スイッチポートの着信トラフィックに適用します。

```
IOS-Switch(config-if)#ip access-group interface_acl in
```

注: NAC は VLAN には設定できません。物理スイッチポートにのみ設定できます。

手順 2. **ip admission** コマンドを使用して、作成済みのアドミッション コントロール ルールをクライアント側の Cisco NAC インターフェイスに適用します。タスク 5 の手順 1 で指定したルール名を使用します。

```
IOS-Switch(config-if)#ip admission NAC-L2-IP
```

注: スイッチ インターフェイスが **ip admission name** コマンドを受け付けない場合は、インターフェイスで **switchport mode access** がイネーブルにされていることを確認します。

タスク 7：EAPoUDP タイマーの設定

手順 1. **eou timeout hold-period** コマンドを使用して、EAPoUDP 保留期間タイマーを設定します。このタイマーには、クレデンシャル検証の失敗（Accept-Reject）または EAPoUDP アソシエーションの失敗の後に、新しいアソシエーションを再試行するまでの待機時間（秒）を指定します。デフォルト値は 180 秒です。

```
IOS-Switch(config)#eou timeout hold-period 180
```

手順 2. **eou timeout status-query** コマンドを使用して、EAPoUDP ステータス クエリー タイマーを設定します。クライアントのクレデンシャル検証とセキュリティ ポスチャ セッションの確立に成功した後、NAD はクライアントにステータス クエリーを送信します。NAD は、クライアントから正常に応答を受信しない場合、指定された時間（秒）待機してから新しいステータス クエリー メッセージを送信します。このタイマーは、ステータス クエリー コマンドの実行が成功し、NAD が応答を受信するたびにリセットされます。デフォルト値は 300 秒です。

```
IOS-Switch(config)#eou timeout status-query 300
```

手順 3. **eou timeout revalidation** コマンドを使用して、EAPoUDP 再検証期間タイマーを設定します。クレデンシャル認証とセキュリティ ポスチャ セッションの確立に成功した後、NAD は指定された時間（秒）待機してからクライアントの再検証を開始し、Cisco NAC クライアント アドミッション ポリシーに変更が発生していないかどうかを確認します。デフォルト値は 36000 秒（10 時間）です。

```
IOS-Switch(config)#eou timeout revalidation 36000
```

注: ステータス クエリーおよび再検証タイムアウトは、Cisco Secure ACS で設定してポスチャ トークンのために NAD に送信することができます。この場合、Cisco Secure ACS のタイマーは、このセクションで説明したスイッチのグローバル EAPoUDP タイマーに優先して適用されます。

タスク 8：EAPoUDP ロギングのイネーブル

ここでは、NAD 上で EAPoUDP ロギングをイネーブルにする方法を説明します。

手順 1. **eou logging** コマンドを使用して EAPoUDP ロギングをイネーブルにします。

```
IOS-Switch(config)#eou logging
```

タスク 9：スイッチ上での HTTP サーバのイネーブル

ここでは、NAD 上で HTTP サーバをイネーブルにする方法を説明します。

手順 1. **ip http server グローバル**設定コマンドを使用して HTTP サーバをイネーブルにします。

```
IOS-Switch(config)#ip http server
```

Cisco Trust Agent（CTA）のインストールと設定

CTA は、クライアントのポスチャ検証を実行するために必要なコンポーネントです。CTA のインストール、設定、管理の詳細情報については、『Cisco Trust Agent アドミニストレータ ガイド 2.0』（http://www.cisco.com/jp/service/manual_j/index_sec_ta.shtml）を参照してください。

Cisco Trust Agent は、次に説明するいずれかの ctasetup.exe ファイルを使用してインストールします。

注: CTA ファイルおよびインストールに関する詳細情報については、『Cisco Trust Agent アドミニストレータ ガイド 2.0』を参照してください。

Cisco Trust Agent Windows .exe のバージョン

CTA for Windows は、CTA の実装およびパッケージングのために複数のオプションを提供します。管理者は、スクリプティング インターフェイス、サプリカントまたはその両方を noisy または silent インストールで展開することができます。

次の表に Windows で使用可能なパッケージを示します。

Windows

CTA.exe ファイル	説明
ctasetup-win-[version].exe	このパッケージのインストールは、noisy です。エンド ユーザは、ライセンス契約への同意、インストール先フォルダの選択、その他の一般的なインストール オプションの選択を求められます。このパッケージは、CTA スクリプティング インターフェイスのみをインストールします。このパッケージではサプリカントはインストールされません。
ctasetup-supplicant-win-[version].exe	このパッケージのインストールは、interactive です。エンド ユーザは、ライセンス契約への同意、インストール先フォルダの選択、その他の一般的なインストール オプションの選択を求められます。このパッケージは、CTA スクリプティング インターフェイスおよびサプリカント両方をインストールできます。エンド ユーザは、インストールする CTA 機能の選択も求められます。
CtaAdminEx-win-[version].exe	このパッケージでは、エンド ユーザ用のサイレント インストール パッケージを作成します。管理者は、このパッケージから ctasilent-win-[version].exe ファイルを抽出します。管理者は、エンド ユーザに代わってライセンス契約に同意し、エンド ユーザにオプションの選択を要求しない完全なサイレント インストールとして ctasilent-win-[version].exe ファイルを展開します。このパッケージではサプリカントはインストールされません。
CtaAdminEx-supplicant-win-[version].exe	このパッケージでは、エンド ユーザ用のサイレント インストール パッケージを作成します。管理者は、このパッケージから ctasilent-supplicant-win-[version].exe ファイルを抽出します。管理者は、エンド ユーザに代わってライセンス契約に同意し、エンド ユーザにオプションの選択を要求しない完全なサイレント インストールとして ctasilent-supplicant-win-[version].exe ファイルを展開します。このパッケージでは、サプリカントがインストールされます。

注: IEEE 802.1x セキュリティ プロトコルによって保護されているネットワークに接続、アクセスするクライアントには、サプリカントが必要です。エンドユーザは、クライアント-サーバ認証が成功した後にのみ、802.1x 対応のアクセス デバイス（イーサネット スイッチ）上のポート アクセス コントロールによってネットワークへの接続を許可されます。

タスク 1：CTA 用のクライアント証明書のインストール

正しく認証を実行するために、Cisco Secure ACS にインストールした証明書を CTA にもインストールする必要があります。クライアント上の CTA には、2 つの方法で証明書を追加できます。ここでは、CTA のインストール前に証明書を追加する方法を説明します。証明書は、CTA のインストール後にルート ストアに追加することもできます（この手順は、後のセクションで説明します）。

手順 1. client1 に *certs* という名前のフォルダを作成し、CTA.exe ファイルと同じディレクトリに配置します。

手順 2. クライアントを ACS で認証するときに CTA が使用する CA 証明書を *certs* フォルダに配置します。

注: CTA は、**certs** サブディレクトリに配置されているすべてのパブリック証明書をインポートします。このフォルダは、cta.exe ファイルと同じディレクトリに配置する必要があります。

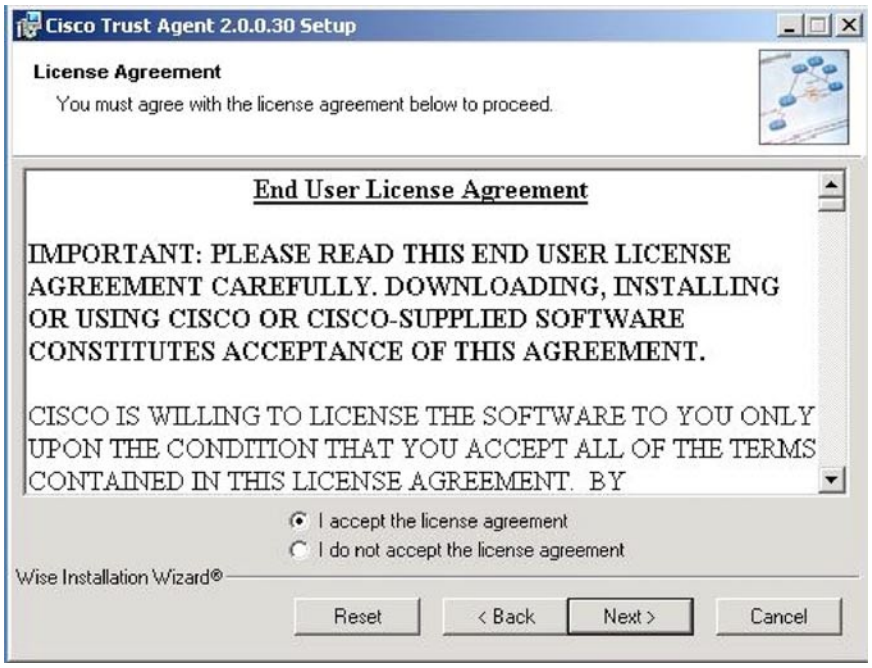
タスク 2：CTA 2.0 のインストール

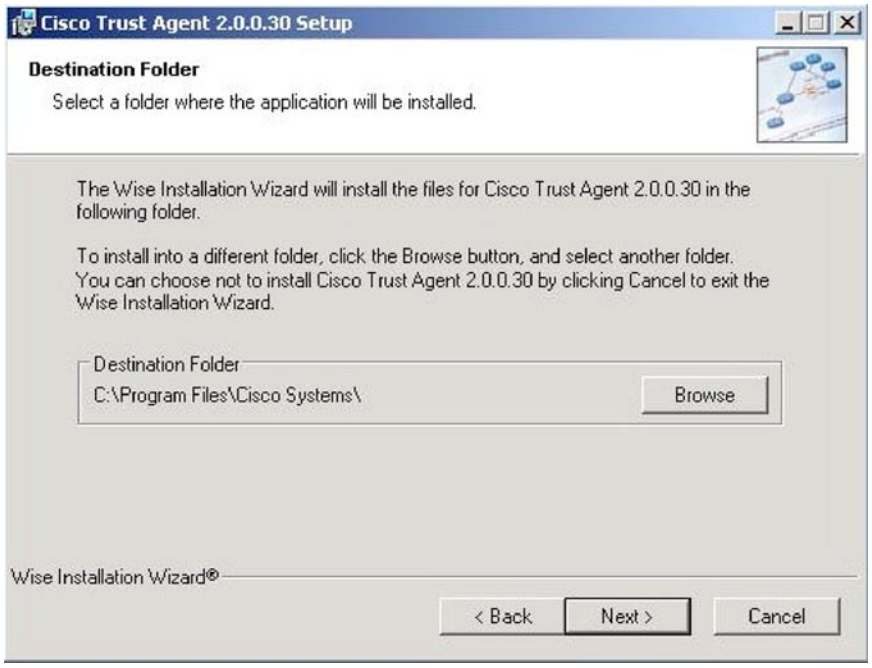
手順 1. CTA セットアップ ファイルをクライアントにダウンロードまたはコピーします。クライアント上で CTA.exe ファイルが配置されているフォルダを開き、使用する ctasetup ファイルをダブルクリックします（この例では **ctasetup-win-[version].exe** を使用）。

Cisco Trust Agent の **Installation Wizard** が表示されます。

手順 2. **Next** をクリックします。

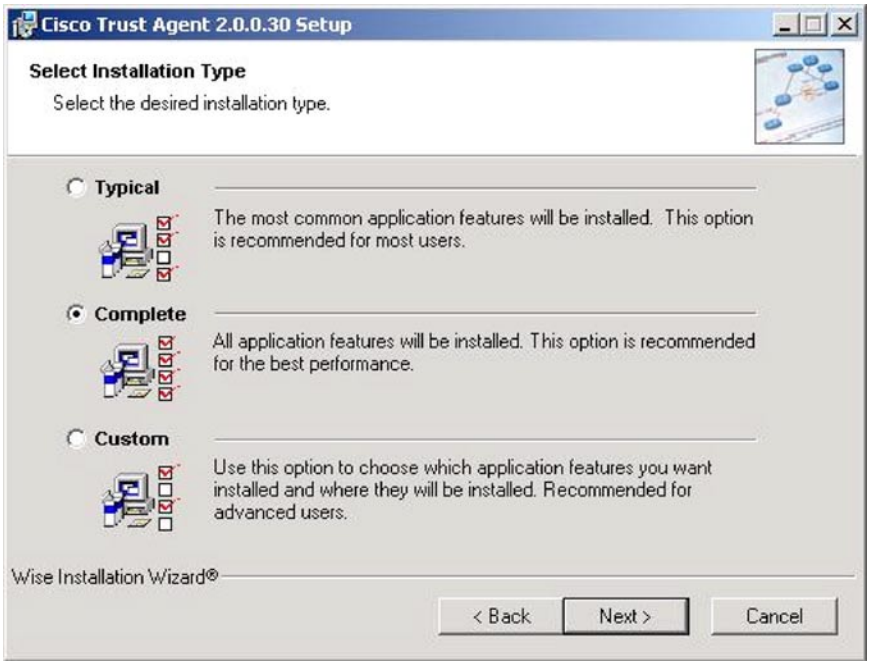
手順 3. **Next** をクリックして License Agreement（ライセンス契約）を受諾します。Destination Folder ウィンドウが表示されます。





手順 4. デフォルトの Destination Folder をそのまま受入れ、**Next** をクリックします。

手順 5. Select Installation Type ダイアログ ボックスが表示されます。



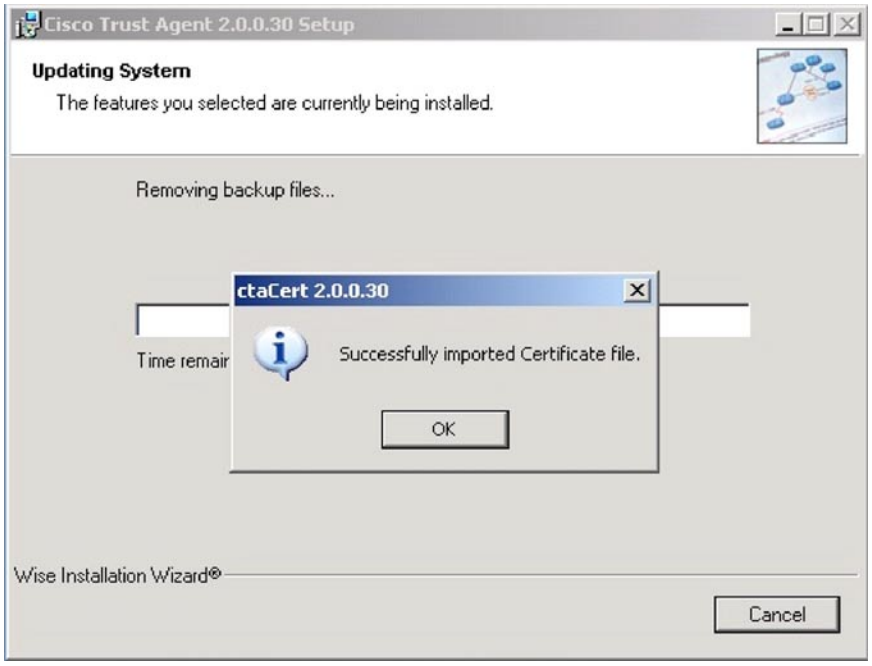
手順 6. **Complete** ラジオ ボタンをクリックします。

手順 7. 使用する機能を選択し、**Next** をクリックします。

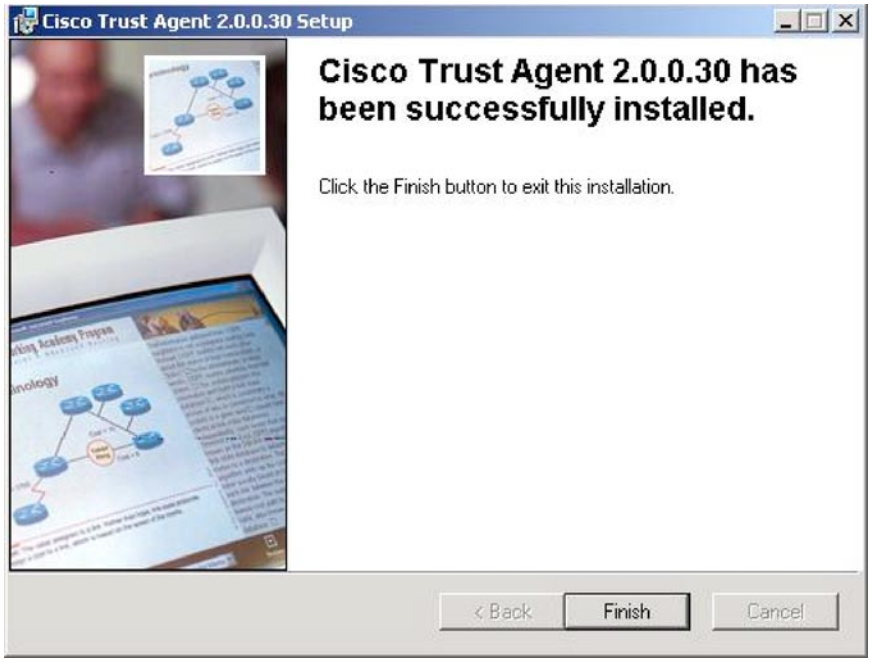
手順 8. **Next** をクリックします。

手順 9. 選択したディレクトリにアプリケーションがインストールされます。

手順 10. インストール中に証明書のインポートが成功すると、次のメッセージが表示されます。**OK** をクリックします。



手順 11. インストールが完了すると、**Installation Completed** ウィンドウが表示されます。



手順 12. Finish をクリックしてこのウインドウを閉じます。

タスク 3：（オプション）CTA へのルート証明書の手動でのインストール

タスク 1 の手順 1 で CTA のフォルダに *certs* フォルダをコピーしなかった場合は、Cisco Trust Agent を使用する前にルート証明書をインストールする必要があります。

証明書を手動でインストールするには、次の手順を実行します。

手順 1. ネットワーク クライアントに証明書をコピーします。

手順 2. ネットワーク クライアントでコマンド プロンプトを開きます。

手順 3. Cisco Trust Agent がインストールされているディレクトリに変更します。デフォルトのロケーションは、次のディレクトリです。

```
C:\Program Files\Cisco Systems\CiscoTrustAgent\
```

手順 4. 次のコマンドを入力します。

```
ctaCert.exe /add "cert_path_&_cert_name" /store "Root"
```

（cert_path_&cert_name は証明書への完全なパスと完全なファイル名です）

証明書がネットワーク クライアントの信頼される証明書ストアに追加されます。

NAC L2 IP のネットワーク アクセス プロファイルの設定

ここでは、NAC L2 IP をサポートするネットワーク アクセス プロファイル（認証、ポスチャ検証、許可）の設定方法を説明します。Cisco Secure ACS 4.0 では、次の 2 つの方法でネットワーク アクセス プロファイルを設定できます。

- 空のプロファイルを追加し、必要なすべての情報を設定する。
- テンプレート プロファイルを使用し、このテンプレートに含まれている基本情報をベースにネットワーク アクセス プロファイルをカスタマイズする。

Cisco Secure ACS 4.0 には予め 7 つのネットワーク アクセス プロファイル テンプレートが定義されています。

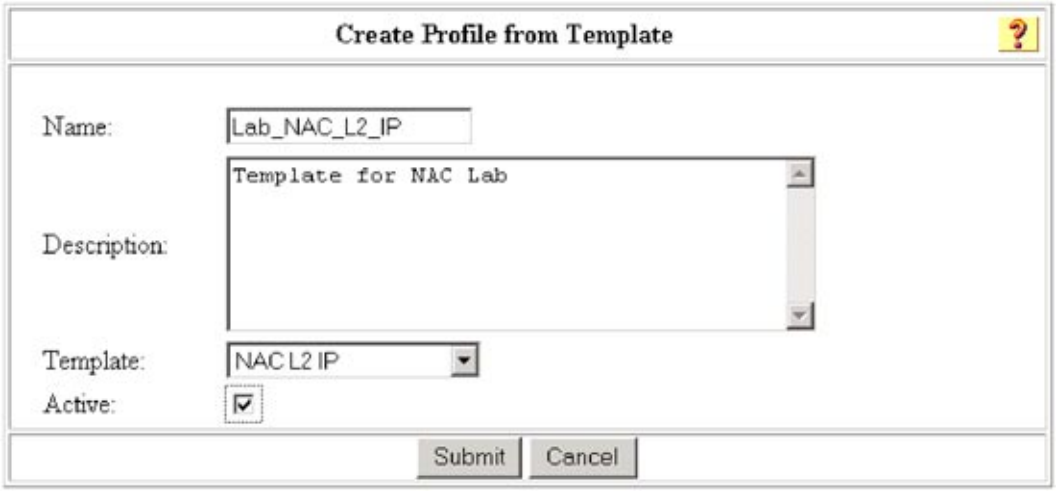
- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- Microsoft IEEE 802.1x
- Wireless（NAC L2 802.1x）
- Authentication Bypass（802.1x fallback）
- Agentless Host

ここでは、NAC L2 IP ネットワーク アクセス プロファイル テンプレートを使用して基本プロファイルを作成し、必要な変更を加えてこのテンプレートをカスタマイズします。

タスク 1：テンプレートからの NAC L2 IP プロファイルの作成

手順 1. **Network Access Profiles** メイン メニューで **Add Template Profile** を選択します。

手順 2. Template ドロップ ダウン ボックスで NAC L2 IP を選択し、NAC L2 IP のテンプレートを作成します。次の図に示すような名前を付けます。**Active** をチェックしてこのプロファイルをイネーブルにします。



手順 3. **Submit** をクリックします。

タスク 2：認証の設定

手順 1. タスク 1 で作成した新しいネットワーク アクセス プロファイルの **Authentication** のリンクを選択します。

手順 2. この基本テンプレートの一部として、**Allow Posture Validation** がすでに選択されています。

手順 3. **Submit** をクリックします。

タスク 3：ポスチャ検証の設定

参考として、ポスチャ検証の設定を以下に示します。

手順 1. 作成したプロファイルの Network Access Profiles 画面から **Posture Validation** のリンクを選択します。

手順 2. Posture Validation Rules 画面で **Add Rule** を選択します。

手順 3. 新しいポスチャ検証のルールとして次の情報を追加します。

<table>
<tr><th colspan="2">Name: Lab_NAC_L2_IP</th></tr>
<tr><td>Required Condition Types</td><td>Cisco:PA
Cisco:Host</td></tr>
<tr><td>Posture Validation Policies</td><td>CTA
Windows</td></tr>
<tr><td>Assessment Result Configuration</td><td>
<table>
<tr><th>Result</th><th>Message</th><th>URL Redirect</th></tr>
<tr><td>Healthy</td><td>NAC-L2-IP: Healthy</td><td></td></tr>
<tr><td>Checkup</td><td>NAC-L2-IP: Checkup</td><td></td></tr>
<tr><td>Transition</td><td>NAC-L2-IP: Transition</td><td></td></tr>
<tr><td>Quarantine</td><td>NAC-L2-IP: You have been Quarantined. Please click on the link below and follow the procedures to update your system: http://update.nac.cisco.com/quarantine.html</td><td>http://update.nac.cisco.com/quarantine.html</td></tr>
<tr><td>Infected</td><td>NAC-L2-IP: Infected</td><td>http://update.nac.cisco.com/quarantine.html</td></tr>
<tr><td>Unknown</td><td>NAC-L2-IP: Unknown</td><td>http://update.nac.cisco.com/quarantine.html</td></tr>
</table>
</td></tr>
<tr><th colspan="2">Audit Selection</th></tr>
<tr><td>Audit Server</td><td>None</td></tr>
</table>

手順 4. **Submit** をクリックします。

手順 5. 左側のラジオボタンを選択し、**Up/Down** ボタンを使用して Lab_NAC_L2_IP ルールをリストの最上部に移動します。

Posture Validation for Lab_NAC_L2_IP		
Rule Name	**Condition**	**Action**
	Required Credential Types	**Associate With**
• Lab_NAC_L2_IP	Cisco:PA Cisco:Host	Windows、CTA (Internal)
• NAC-SAMPLE-POSTURE-RULE	Cisco:PA	NAC-SAMPLE-CTA-POLICY、(Internal)

Add Rule | Up | Down

The Up/Down buttons submit and save the sort order to the database

Determine Posture Validation for NAH:

No Audit Server was selected

Select

Done

手順 6. **Done** をクリックします。

手順 7. Network Access Profiles 画面で **Apply and Restart** をクリックします。

タスク 4：許可

手順 1. テンプレートから **Authorization** のリンクをクリックします。

手順 2. 許可をイネーブルにします。

User Group	Assessment Result	Deny Access	Shared RAC	Downlodable ACL
Any	Healthy	No	L2_IP_Healthy_RAC	healthy_ACL
Any	Checkup	No	L2_IP_Healthy_RAC	healthy_ACL
Any	Transition	No	L2_IP_Quarantine_RAC	quarantine_ACL
Any	Quarantine	No	L2_IP_Quarantine_RAC	quarantine_ACL
Any	Infected	No	L2_IP_Quarantine_RAC	quarantine_ACL
Any	Unknown	No	L2_IP_Quarantine_RAC	quarantine_ACL
If a condition is not defined or there is no matched condition:		No	L2_IP_Quarantine_RAC	quarantine_ACL
Include RADIUS attributes from user's group:				No
Include RADIUS attributes from user record:				No

手順 3. **Submit** をクリックします。

タスク 5：NAC L2 IP 設定のテスト

ここでは、NAC L2 IP が正しく設定されていること、Cisco Secure ACS から正しいポスチャ トークンを受信すること、Cisco Secure ACS からダウンロードされた正しい ACL が NAD に適用されていることを確認する方法を説明します。

注: このタスクでは URL リダイレクションは行いません。別のタスクで行います。

クライアントが Healthy とみなされ、Healthy のロールに配置されるには、必要なクレデンシャル情報を NAD に返し、この情報が NAD から Cisco Secure ACS に送信される必要があります。Network Access Profile のセクションで作成した各クレデンシャルのポスチャ検証の要件を満たしているクライアントには *Healthy* アプリケーション ポスチャ トークンが渡されます。このクレデンシャルには、**Cisco Trust Agent**、エージェント バージョン **2.0.0.30** 以上、OS-Type contains **Windows XP** が含まれます。

注: クライアントは、Cisco Secure ACS が具体的に要求しているクレデンシャルのみを Cisco Secure ACS に渡すことに注意してください。

手順 1. まず **no shut** コマンドを入力し、クライアントが接続しているスイッチポート（ギガビット イーサネット 1/1） をもう一度イネーブルにします。

手順 2. NAD のコンソールに次の出力が表示されます。

```
04:01:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigEthernet1/1, changed state to up
1d19h: %EOU-6-SESSION: IP=10.7.1.2| HOST=DETECTED| Interface=GigabitEthernet1/1
1d19h: %EOU-6-SESSION: IP=10.7.1.3| HOST=DETECTED| Interface=GigabitEthernet1/1
1d19h: %EOU-6-CTA: IP=10.7.1.3| CiscoTrustAgent=DETECTED
1d19h: %EOU-6-POLICY: IP=10.7.1.3| HOSTNAME=
1d19h: %EOU-6-POSTURE: IP=10.7.1.3| HOST=AUTHORIZED| Interface=GigabitEthernet11
1d19h: %EOU-6-AUTHTYPE: IP=10.7.1.3| AuthType=EAP
1d19h: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
1d19h: %EOU-6-POLICY: IP=10.7.1.3| HOSTNAME=
1d19h: %EOU-6-POSTURE: IP=10.7.1.3| HOST=AUTHORIZED| Interface=GigabitEthernet11
1d19h: %EOU-6-AUTHTYPE: IP=10.7.1.3| AuthType=EAP
1d19h: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
```

手順 3. Cisco Trust Agent が検出されたこと、クライアントに割り当てられたポスチャ トークンが *Healthy* であること、ACS で作成した Downloadable Healthy_ACL が NAD に適用されていることを出力で確認します。

手順 4. **show eou all** コマンドを入力し、クライアントの現在のステータスを確認します。

```
NAC4948#show eou all
  ------------------------------------------------------------------------
  Address        Interface            AuthType   Posture-Token Age(min)
  ------------------------------------------------------------------------
  10.7.1.2     GigEthernet1/1         EAP       Healthy        12
```

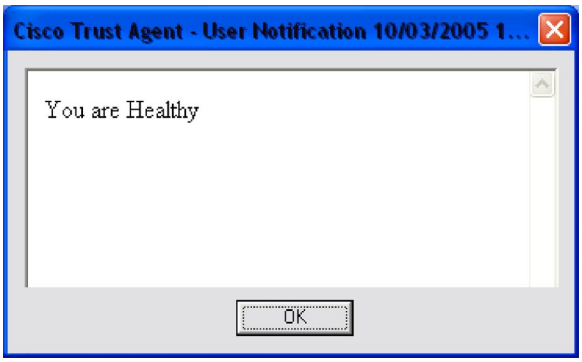
手順 5. Healthy_ACL がスイッチポートにダウンロードされ適用されていることを確認します。

```
NAC4948#show ip access-lists
Extended IP access interface_acl
    10 permit udp any any eq 21862
    20 permit udp any host 10.0.200.10 eq domain
    30 permit udp any eq bootpc any eq bootps
    40 permit icmp any any
Extended IP access list xACSACLx-IP-Healthy_ACL-433866ab
    10 permit ip any any
```

手順 6. Downloadable ACL がスイッチポートに適用されていることを確認します。クライアントの IP アドレスが Healthy ACL のソースの *any* とリプレースされていることが確認できます。

```
NAC4948#show ip access-list interface GigE 1/1
IP Admission access control entires (Inbound)
     permit ip host 10.7.1.2 any
```

手順 7. クライアント上で CTA ポップアップ メッセージが表示されます。



手順 8. ACS 上で適切なレポートを使用してクライアント情報を確認します。たとえば、クライアントと ACS 間に正しく通信が確立されたことを確認する場合は、**Passed Authentications** レポートを使用します。

タスク 6：NAC L2 IP のトラブルシューティング

ここでは、トラブルシューティングに役立つ重要なサマリー情報を提供します。クライアントに *Healthy* トークンではなく *Quarantine* トークンが与えられていることを前提として、このトラブルシューティングの方法について説明します。

手順 1. クライアントを強制的に Quarantine ロールに配置します。まず、クライアントが検証に失敗するポスチャ検証ルールを ACS に設定します。そのために、Healthy ポスチャ ステータスを与えるために必要な CTA の最小バージョンを変更します。現在は CTA バージョン 2.0.0.30 が稼動しているため、クライアントは次のルールに適合しません。

Policy Name	#	Condition	Posture Assessment	Notification String
CTA	1	Cisco:PA:PA-Name contains Cisco Trust Agent Cisco:PA:PA-Version >= 3.0.0.0	Cisco:PA:Healthy	
	2	Default	Cisco:PA:Quarantine	

手順 2. **clear eou all** コマンドを入力し、検証プロセスをリスタートします。

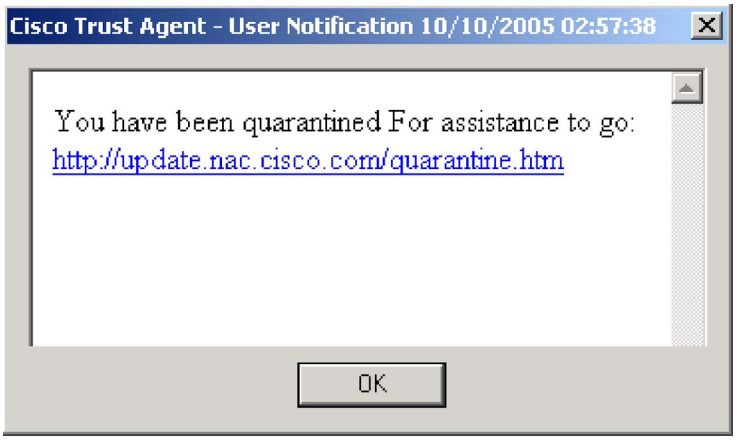
```
NAC4948#clear eou all

04:53:29: %EOU-6-SESSION: IP=10.7.1.2| HOST=REMOVED| Interface=GigEthernet1/1

04:53:34: %EOU-6-SESSION: IP=10.7.1.2| HOST=DETECTED| Interface=GigEthernet1/1

04:53:34: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=DETECTED

04:53:34: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-Quarantine-43408f9d

04:53:34: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Quarantine

04:53:34: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=DMA-WXP01:dma

04:53:34: %EOU-6-POSTURE: IP=10.7.1.2| HOST=AUTHORIZED| Interface=GigEthernet1/1

04:53:34: %EOU-6-AUTHTYPE: IP=10.7.1.2| AuthType=EAP
```

手順 3. クライアントに Quarantine トークンが割り当てられ、NAD に Quarantine ACL がダウンロードされたことを確認します。

```
NAC4948#show eou all

  ------------------------------------------------------------------------

  Address        Interface            AuthType   Posture-Token Age(min)

  ------------------------------------------------------------------------

  10.7.1.2     GigEthernet1/1        EAP       Quarantine     2

  NAC4948#show access-lists

  Extended IP access list interface_acl

     10 permit udp any any eq 21862

     20 permit udp any host 10.0.200.10 eq domain

     30 permit udp any eq bootpc any eq bootps

     40 permit icmp any any
```

```
Extended IP access list quarantine_url_redir_acl
    10 deny tcp any host 10.0.200.30 eq www
    30 permit tcp any any eq www
Extended IP access list xACSACLx-IP-Quarantine-43408f9d
    10 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
    20 permit udp any any eq 21862
    30 permit udp any any eq domain
    40 permit ip any 10.0.200.0 0.0.0.255

NAC4948#show access-lists dynamic interface GigE 1/1
IP Admission access control entires (Inbound)
     permit udp host 10.7.1.2 eq bootpc host 255.255.255.255 eq bootps
     permit udp host 10.7.1.2 any eq 21862
     permit ip host 10.7.1.2 10.0.200.0 0.0.0.255
```

手順 4. クライアント上で CTA によって次のようなポップアップ メッセージが表示されます。



手順 5. ACS レポートを確認し、クライアントが検疫された理由に関する情報を収集します。

URL リダイレクション

ここでは、URL リダイレクションを使用して、セキュリティ ポリシーへの適合に必要な更新やソフトウェアの修復のためのアクセスをホストに提供する方法を説明します。

URL ACL 情報は、基本的な ACS 設定セクションの検疫用 RADIUS 許可コンポーネント設定で定義済みです。

参照：タスク 11：RADIUS 許可コンポーネント（RAC）（url-redirect-acl=quarantine_url_redir_acl）。アップデート サーバの URL は、タスク 3：ポスチャ検証の設定の際に、Network Access Profile 設定の Posture Validation セクションで定義済みです。

タスク 1：スイッチへの URL リダイレクションの設定

URL リダイレクト用の ACL は、スイッチに設定する必要があります。ACS で定義された ACL 名は、スイッチに設定された ACL 名とマッチする必要があります。

手順 1. スイッチに URL リダイレクト用 ACL を設定します。

```
IOS-Switch(config)#ip access-list extended quarantine_url_redir_acl
deny tcp any host 10.0.200.30 eq www
permit tcp any any eq www
```

手順 2. クライアントを Quarantine のロールに強制的に配置して URL リダイレクションをテストします。

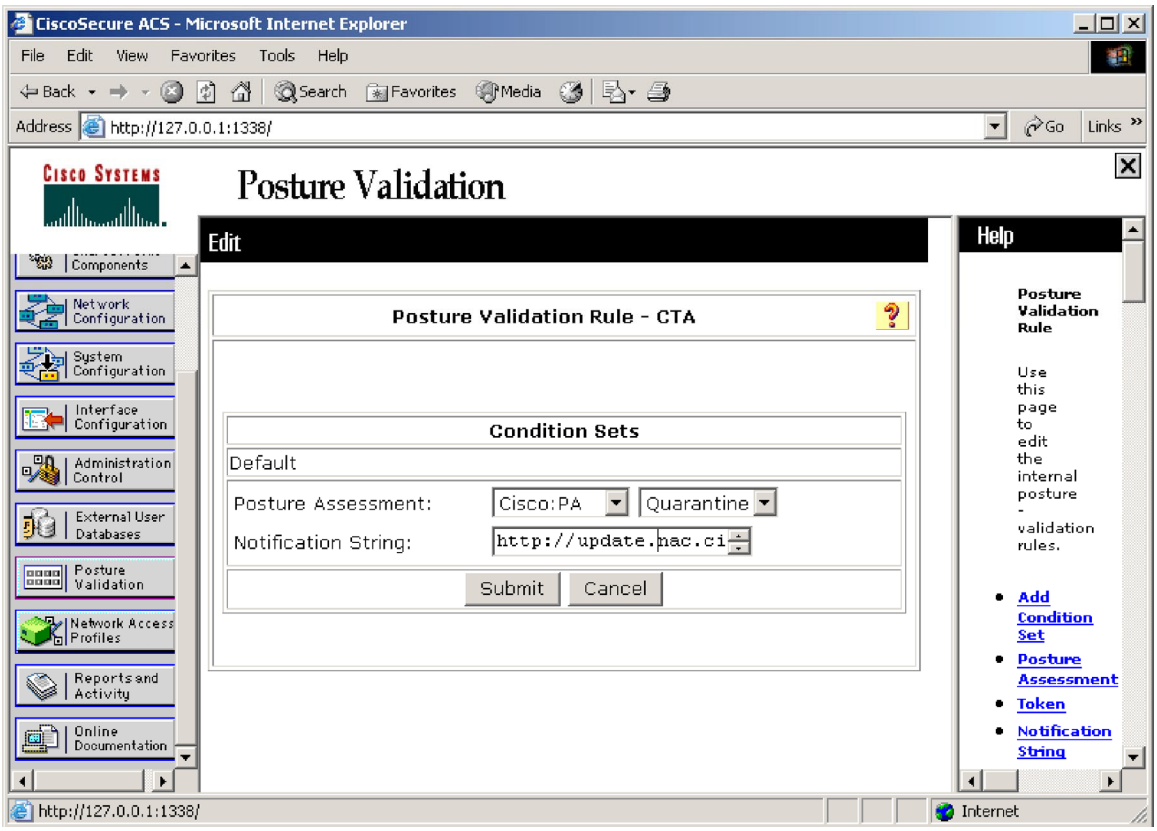
注: URL リダイレクト用 ACL は、アップデート サーバへのトラフィックはリダイレクトせず、他のすべての宛先へのトラフィックをリダイレクトします。

ブラウザの自動起動

CTA 2.0 は、ACS で事前定義された URL を受信すると、クライアント マシン上でデフォルトの Web ブラウザを自動的に開くことができます。この URL は、各ポスチャ検証ルールを定義するときに通知文字列（notification string）フィールドに設定できます。通知文字列に入力があると、CTA はクライアント デバイス上でデフォルトの Web ブラウザを起動し、この URL の表示を試みます。たとえば、検疫ルールのポスチャ アセスメントの通知文字列に http://x.x.x.x/quarantine.html と入力すると、自動的にブラウザを起動して検疫アセスメントを行うことができます。

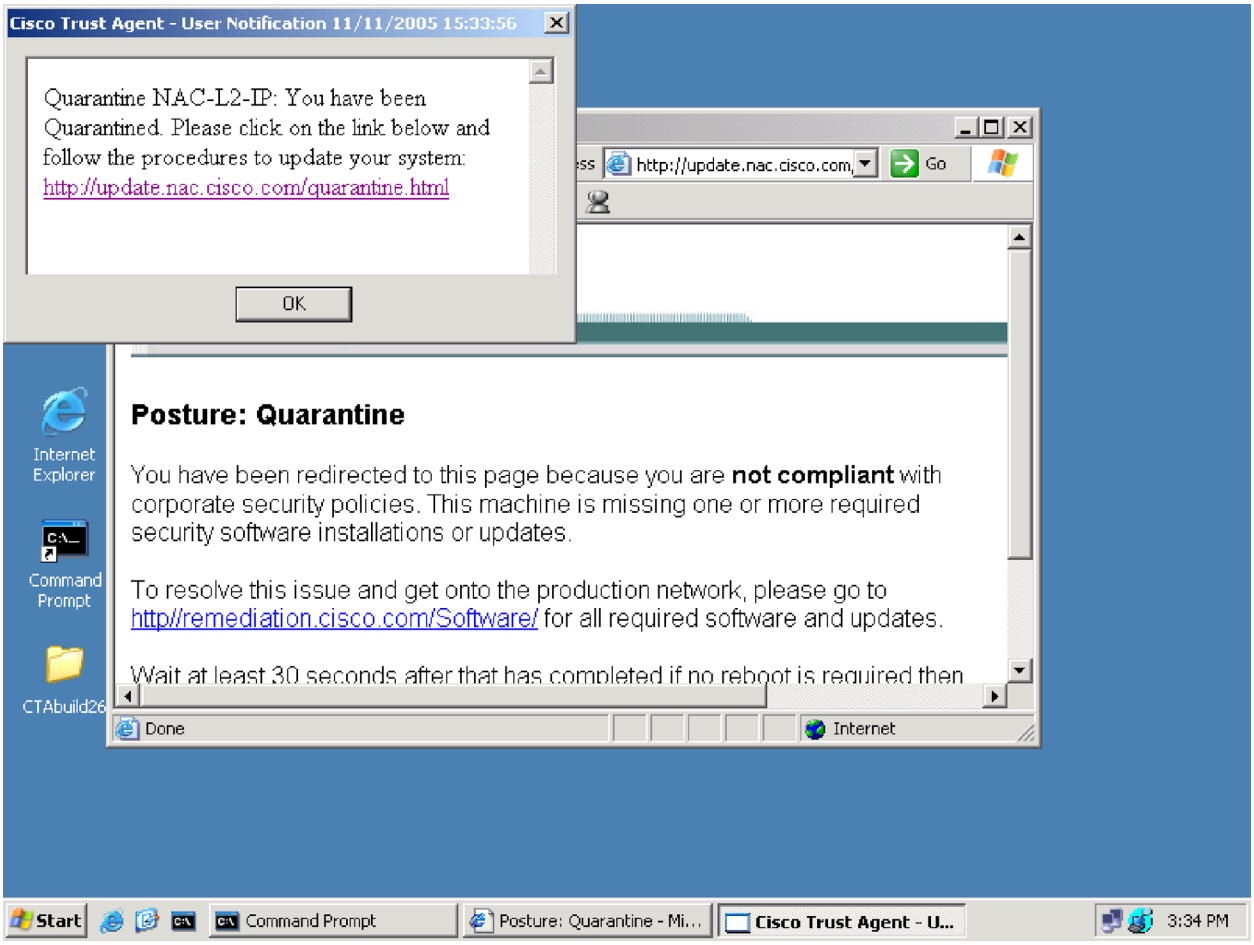
タスク 1：通知文字列への URL の入力

手順 1. Notification String フィールドに、クライアントのブラウザで開く URL を入力します。このページを開くには、ACS メニューから **Posture Validation** を選択し、**Internal Posture Validation Setup** のリンクをクリックして、使用するポスチャ検証ルールを選択します。この例で使用しているのは、CTA ポスチャ検証ルールのデフォルトの検疫設定です。たとえば、クライアントに CTA バージョン 3.0.0.0 またはそれ以降がインストールされていない場合、クライアントは検証に失敗し、Quarantine ロールに配置されます。この検疫が発生すると、CTA は通知文字列として修復のための URL http://update.nac.cisco.com/quarantine.html を受信し、クライアントをこのサイトに接続します。



タスク 2：クライアント上でのブラウザの自動起動の確認

手順 1. クライアントをスイッチ ポートに接続します。このクライアントは、 CTA バージョン 3.0.0.0 が稼動していないため、Quarantine ロールに配置されます。クライアントのデフォルト ブラウザが起動し、通知文字列に指定された URL への接続を試みることを確認します。



NAC Agentless Host（エージェントレス ホスト）

NAC では、プリンタ、スキャナ、サポートされていないオペレーティング システムを使用するホストなど、ポスチャ エージェントを持たないため認証を実行できないホストに、次のような複数の方法でネットワークへのアクセスを許可できます。

- スイッチに定義する静的な例外
  - MAC
  - IP
- Cisco Secure ACS
  - NAP Advanced Filtering
  - Network Access Restriction（NAR；ネットワーク アクセス制限）
- 監査サーバ

タスク 1：IOS への NAH のための静的な例外の設定

IOS に静的な例外を設定し、IP または MAC アドレスに基づいてホストにアクセスを許可することができます。

ここでは、静的な例外を設定する方法を説明します。

手順 1. IP アドレスに基づいてホストにアクセスを許可するために、identity profile configuration の下に許可ステートメントを作成します。

```
#exception based method, DEVICE-TYPE (CDP IP PHONE), MAC or IP
identity profile eapoudp
! static NAC bypass by IP address
 device authorize ip-address 10.7.1.x policy NAH_Profile
! static NAC bypass by MAC address
 device authorize mac-address 000c2986cfbf policy NAH_Profile
```

手順 2. MAC アドレスに基づいてホストにアクセスを許可するために、identity profile configuration の下に許可ステートメントを作成します。この例では、クライアントの MAC アドレスである 000c.2999.fa96 を使用しています。

注: これは MAC アドレスのみを指定する例です。

```
 ! statically permit this MAC to bypass NAC instead of ACS
 device authorize mac-address 000c.2999.fa96
```

手順 3. エージェントレス ホストに URL リダイレクションを許可するプロファイルも設定できます。エージェントレス ホストのためのアイデンティティ プロファイルと、アップデート サーバへのアクセスを許可するリダイレクト URL を作成します。

```
! Statically permit access to NAHs
ip access-list extended NAH_ACL
  permit ip any any

identity policy NAH_Profile
 access-group NAH_ACL
 ! Optional URL redirection
 redirect url http://update.nac.cisco.com/quarantine.htm match
quarantine_url_redir_acl
```

手順 4. EoU テーブルをクリアし、静的に許可されたクライアントの再認証を行います。

```
clear eou all
```

手順 5. クライアントが NAD によって静的に許可された後、EoU テーブルを表示して ACS による許可と静的な許可の違いを確認します。

```
IOS-Switch(config)#show eou all

------------------------------------------------------------------------

Address        Interface            AuthType   Posture-Token Age(min)

------------------------------------------------------------------------

10.7.1.2       GigEthernet1/1        STATIC     -----        12
```

手順 6. ここでは NAD に静的な例外を作成する例を説明しました。次のセクションでは、Cisco Secure ACS に集中管理型の静的な例外を作成する方法を説明します。Cisco Secure ACS の例外を機能させるには、**no device authorize ip-address** および **no device authorize mac-address コマンド**を入力して、上記の手順で作成した NAD の 静的な NAH 許可をディセーブルにする必要があります。

タスク 2：Cisco Secure ACS での NAH の集中管理

このセクションでは、NAC エージェントレス ホスト（NAH）用の ACS 例外をシミュレートするために、エージェント EoU プロセスを停止します。クライアント上の CTA は後で使用するのでアンインストールしません。その後に Cisco Secure ACS に例外を設定します。

注: この方法は、監査サーバ/GAME を使用せずに、MAC アドレスに基づいた集中管理型の例外を設定するときに使用します。

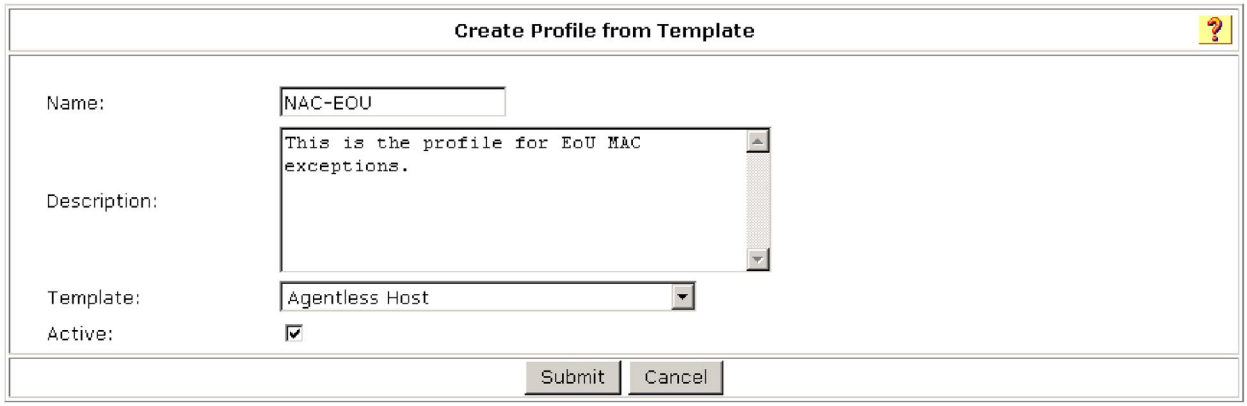
注: このタスクを開始する前に、上記のタスク 1 で実施した NAD のすべての設定を削除してください。

手順 1. Client#1 でコンピュータのデスクトップ アイコンを右クリックし、**[管理]** を選択します。

手順 2. **[コンピュータの管理]** ウィンドウから **[サービスとアプリケーション]** を選択し、次に **[サービス]** を選択します。**Cisco Trust Agent EOU Daemon** という名前のサービスを選択し、そのエントリを右クリックして **[停止]** を選択します。

手順 3. クライアントのインターフェイスの MAC アドレスを記録します。この情報を確認するには、コマンド ウィンドウで **ipconfig /all** コマンドを入力します。

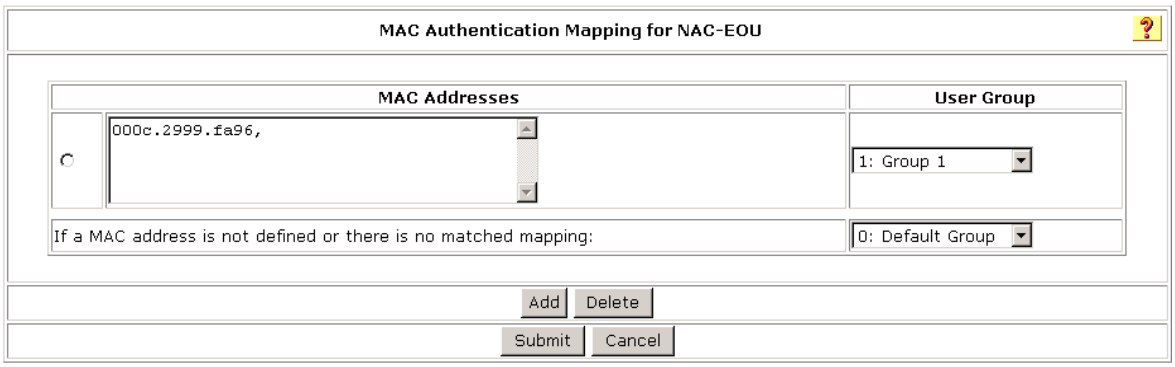
手順 4. ACS の管理コンソールで **Network Access Profiles** を選択し、**Add Template Profile** をクリックします。次に示す値を入力します（MAC アドレスは正しいアドレスを使用してください）。



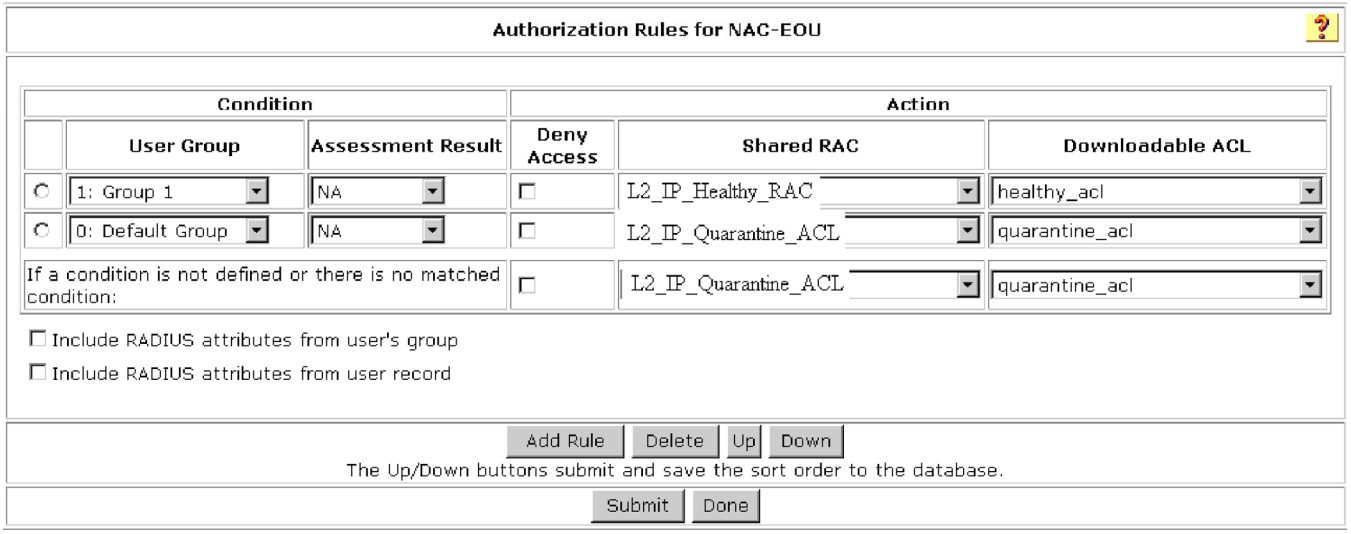
手順 5. Network Access Profile NAC-EOU で **Authentication** リンクをクリックします。**Authentication Profiles** のリストで **Allow MAC-Authentication-Bypass** を選択し、**Submit** をクリックします。

手順 6. もう一度 Network Access Profile NAC-EOU で **Authentication** リンクをクリックし、**MAC Authentication Bypass Configuration** リンクを選択します。

手順 7. 例外の対象となるクライアント MAC を設定します。Windows のフォーマットどおりの ***XX-XX-XX-XX-XX-XX*** ではなく、**xxxx.xxxx.xxxx** のフォーマットで入力してください。**Group 1** は許可されるエージェントレス ホストに、**Default Group** は許可されないデバイスに使用されます。



手順 8. NAC-EOU Network Access Profile で **Authorization** リンクをクリックし、ポリシーを次に示すように設定します。



手順 9. **Apply and Restart** を選択し、EoU Agentless アクセス プロファイルをイネーブルにします。

手順 10. NAD で EoU clientless をイネーブルにします。

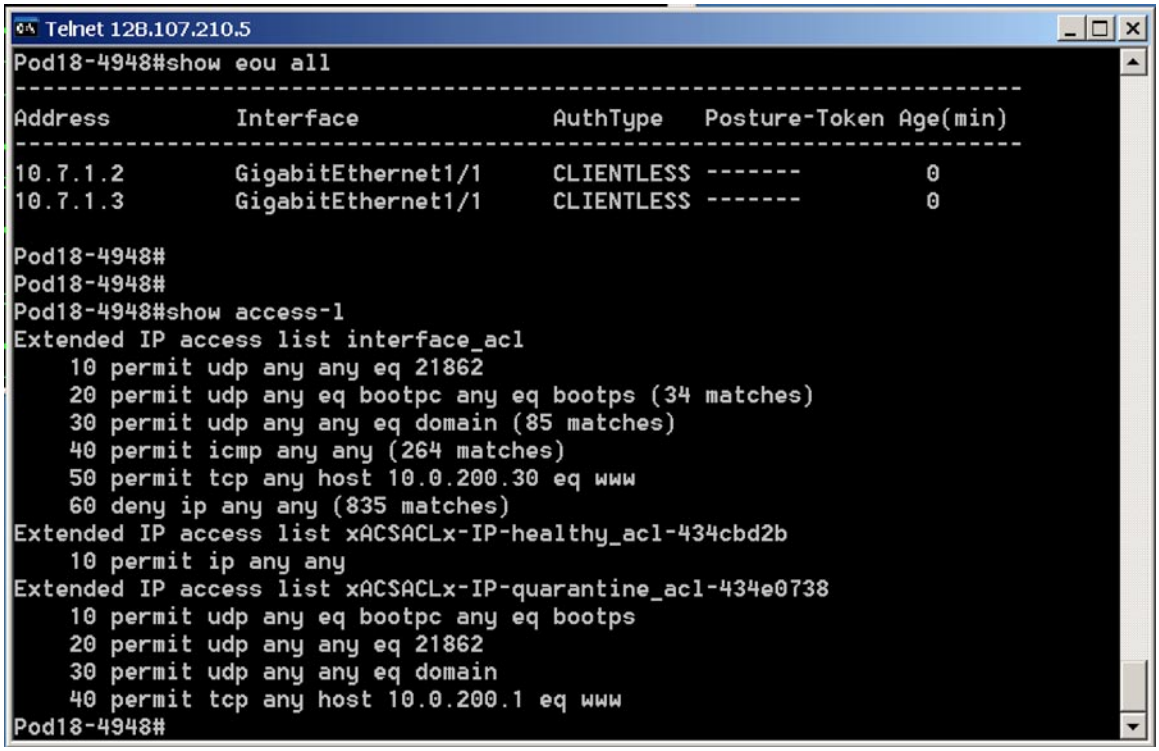
```
IOS-Switch(config)#eou allow clientless
```

手順 11. 必要な場合、**debug eou all** コマンドをイネーブルにしてこれらの手順で発生するプロセスのデバッグ情報を表示します。

手順 12. クライアントレス デバイスの処理プロセスを高速化するために、**clear eou all** および **clear ip device tracking all** コマンドを入力します。

手順 13. Client #1 で、コマンド プロンプトから **ipconfig/renew** を入力し、インターフェイス アドレスを更新します。クライアントレス デバイス処理が開始されます。

手順 14. 再び NAD で **show eou all** コマンドを実行し、クライアントレス デバイス処理の結果を確認します。表と適用されたアクセス コントロール リストのサンプルの出力が表示されます。



手順 15. Reports and Activities の下の Passed Authentications Active ログを確認します。

	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Downloadable ACL
5	00:45:28	Authen OK	000d.880f.ffd4	Default Group	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	L2_IP_Healthy_RAC	healthy_acl
5	00:45:28	Authen OK	000c.2999.fa96	Group 1	000c.2999.fa96	000c.2999.fa96	10.0.200.1	NAC-EOU	L2_IP_Quarantine_RAC	quarantine_acl

タスク 3：監査サーバでの NAH のダイナミックな管理

ここでは、使用する Cisco Secure ACS と外部監視サーバの設定方法を説明します。

注: タスク 2 の設定では、例外の処理に MAC Authentication Bypass Configuration オプションを使用しました。この例外は、管理者の管理対象外の非応答ホストに対しても使用できます。

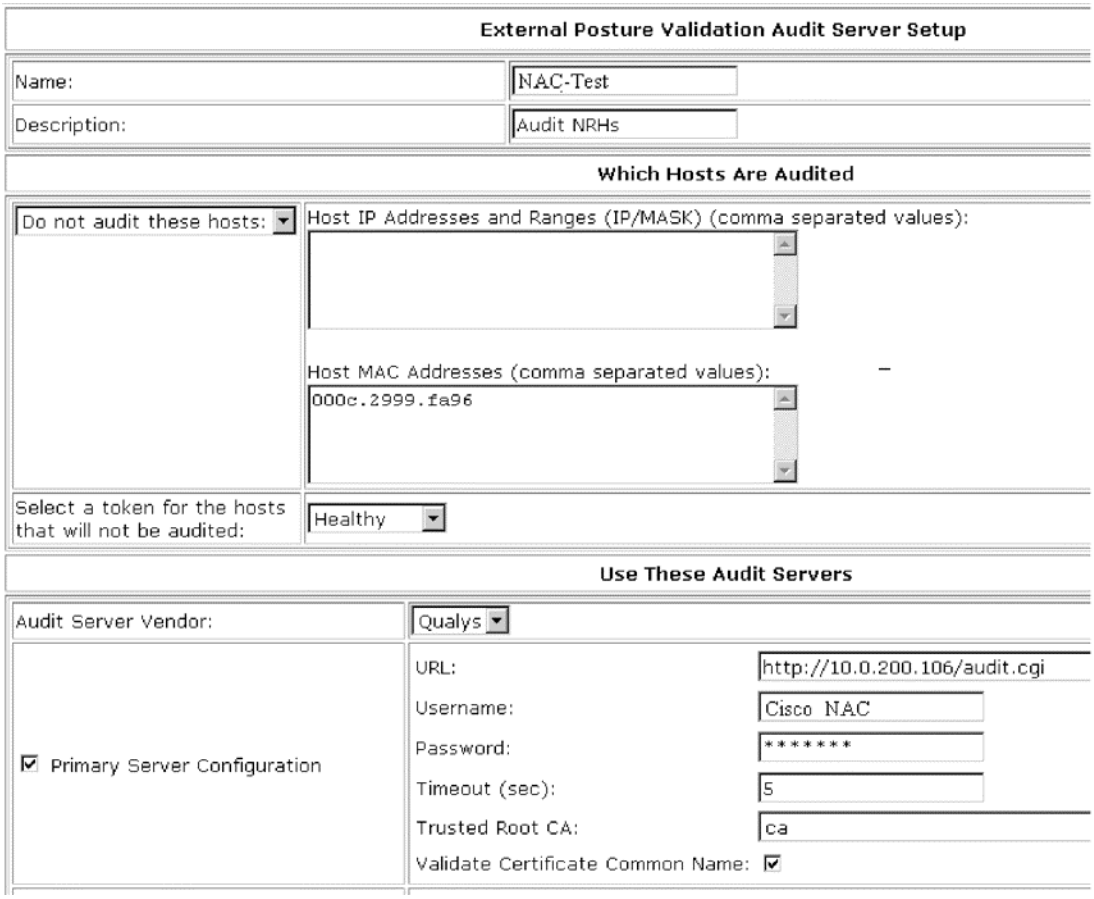
注: このタスクの情報をテストするために、タスク 2 で行った NAD へのすべての設定を削除してください。

手順 1. すでに説明した手順で、CSUtil を使用して監査サーバ用の適切なアトリビュート定義ファイルを ACS にインポートする必要があります。

```
[attr#0]
vendor-id=
vendor-name=
application-id=
application-name=
attribute-id=attribute-name=
attribute-profile=
attribute-type=
```

手順 2. アトリビュート ファイルをインポートしたら、監査サーバを外部ポスチャ検証サーバとして設定します。ACS スタートアップ画面から **Posture Validation** タブを選択します。**External Posture Validation Audit Setup** を選択し、**Add Server** をクリックします。**Audit Server Vendor**: の下に監査サーバ ベンダ リストが表示されない場合は、手順 1 が正常に完了しているかどうか確認してください。

手順 3. 次に示すようにテンプレートに情報を入力します。MAC アドレスには有効なアドレスを入力してください。

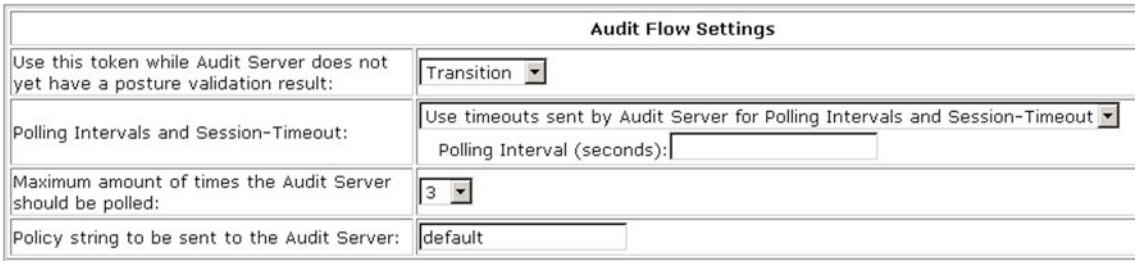


ここでは、Client#1（**000c.2999.fa96**）の MAC アドレスを使用した監査の例外の例を示しています。同様に IP アドレスを使用した監査の例外もサポートされています。

既知の（許可された）ホスト（000c.2999.fa96）には Healthy トークンが与えられます。

許可されていないホストは、このサーバによって監査が行われます。

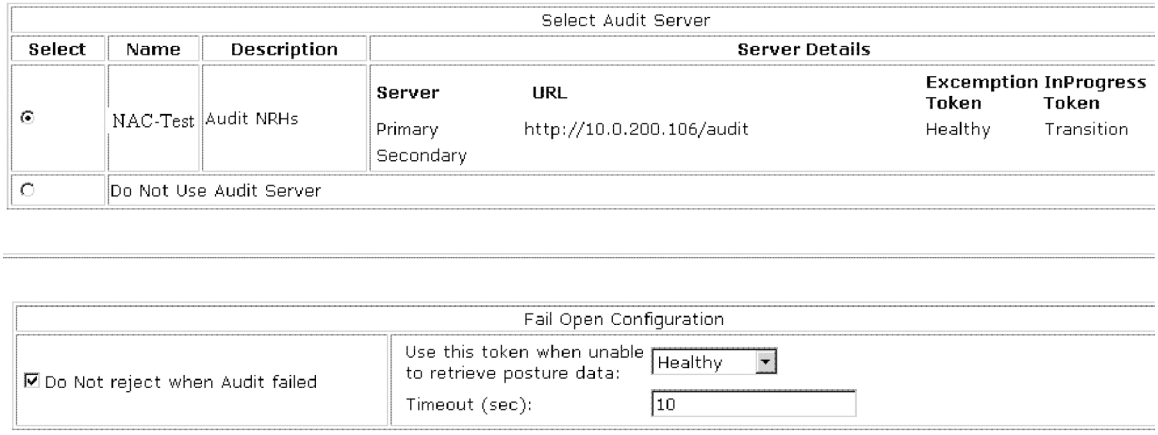
引き続き次に示す例のように設定を行います。



通常 Transition ステートは、NRH の検出後、監査ベンダのサーバから結果を受信するまでの間の中間ステートとして使用されます。Transition RAC（または中間トークンと関連する RAC）は、監査ベンダ サーバとホスト間にアクセスを提供する必要があります。アクセスが許可されなければ、スキャンは行われないため監査は失敗します。

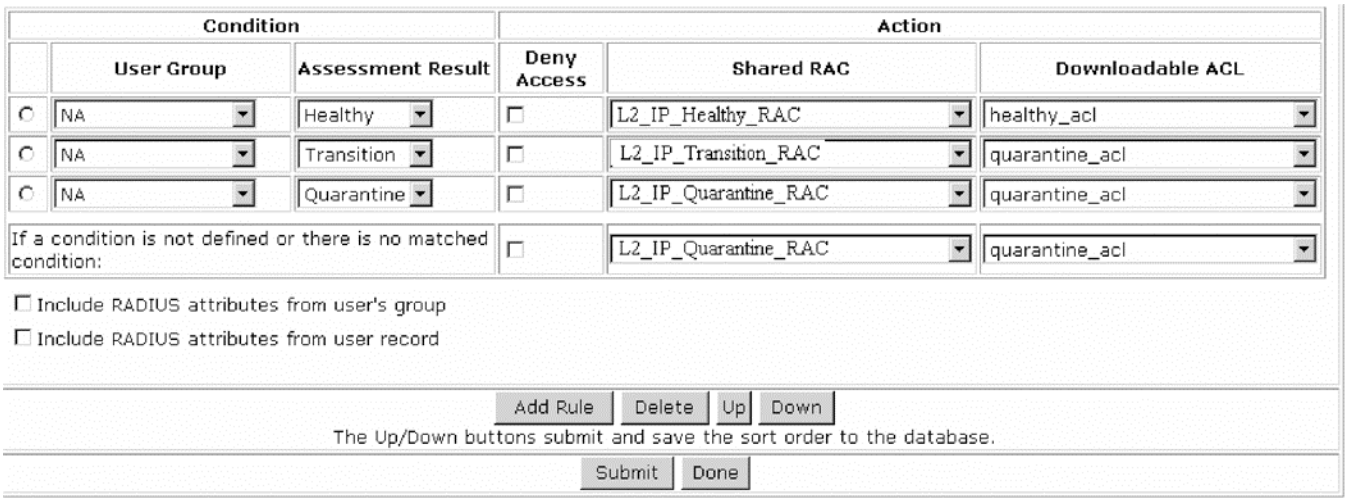
この例では、Transition トークンを使用します。また、ACS から監査サーバにスキャン結果を問い合わせる回数を決定します。

手順 4. **Network Access Profile**、**Posture Validation**、**Select Audit** の順に選択し、既存の NAC-EOU を修正します。前の手順で入力した監査サーバ設定が表示されます。この設定をアクティブにします。



ここでは、**Do Not reject when Audit failed** を選択しています。このコマンドの目的は監査サーバにアクセス不可能な場合にフェール オープンにすることです。このケースでは、Healthy ポスチャと、タイムアウト（10 秒）を選択しています。つまり、検出された後 10 秒以内にスキャンに成功しなかったすべての NRH には自動的に Healthy トークンが与えられます。

手順 5. 監査の設定の最後の手順は、ベンダ サーバから返される結果に基づいてホストに適用するトークンの定義です。次の値を入力します。



手順 6. 監査の開始プロセスを高速化するために、NAD 設定に次の内容を追加します。

```
IOS-Switch(config)#eou max-retry 2

IOS-Switch(config)#eou timeout retransmit 5 [Verify]
```

前の NAH の例と同様に、**clear ip device tracking all** コマンドを実行すると、スイッチによる NRH 処理を高速化できます。

eou allow clientless がまだイネーブルであること、および CTA EOU Daemon が起動していないことを確認します。

参考のためにサンプル レポートと eou 出力を示します。

```
Pod18-4948#clear ip device tracking all
Pod18-4948#show eou
18:21:39: %EOU-6-SESSION: IP=10.7.1.2| HOST=DETECTED| Interface=GigabitEthernet1
/1
18:21:39: %EOU-6-SESSION: IP=10.7.1.3| HOST=DETECTED| Interface=GigabitEthernet1
/1
18:21:39: %EOU-6-SESSION: IP=10.7.1.2| HOST=REMOVED| Interface=GigabitEthernet1/
1
18:21:39: %EOU-6-SESSION: IP=10.7.1.3| HOST=REMOVED| Interface=GigabitEthernet1/
1all
18:21:44: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
18:21:44: %EOU-6-CTA: IP=10.7.1.3| CiscoTrustAgent=NOT DETECTED
18:21:44: %EOU-6-POLICY: IP=10.7.1.3| ACLNAME=#ACSACL#-IP-healthy_acl-434cbd2b
18:21:44: %EOU-6-POLICY: IP=10.7.1.3| TOKEN=Healthy
18:21:44: %EOU-6-POLICY: IP=10.7.1.3| HOSTNAME=Unknown User
18:21:44: %EOU-6-POSTURE: IP=10.7.1.3| HOST=AUTHORIZED| Interface=GigabitEtherne
t1/1
18:21:44: %EOU-6-AUTHTYPE: IP=10.7.1.3| AuthType=CLIENTLESS
18:21:44: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-quarantine_acl-434e2aa
9
18:21:44: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Transition
18:21:44: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=Unknown User
18:21:44: %EOU-6-POSTURE: IP=10.7.1.2| HOST=AUTHORIZED| Interface=GigabitEtherne
t1/1
18:21:44: %EOU-6-AUTHTYPE: IP=10.7.1.2| AuthType=CLIENTLESS
-------------------------------------------------------------------------
Address         Interface              AuthType   Posture-Token Age(min)
-------------------------------------------------------------------------
10.7.1.2        GigabitEthernet1/1     CLIENTLESS Transition      0
10.7.1.3        GigabitEthernet1/1     CLIENTLESS Healthy         0

Pod18-4948#
18:21:59: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-quarantine_acl-434e2aa
9
18:21:59: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Transition
18:21:59: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=Unknown User
18:21:59: %EOU-6-POSTURE: IP=10.7.1.2| HOST=AUTHORIZED| Interface=GigabitEtherne
t1/1
18:21:59: %EOU-6-AUTHTYPE: IP=10.7.1.2| AuthType=CLIENTLESS
Pod18-4948#
18:22:04: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
18:22:04: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-healthy_acl-434cbd2b
18:22:04: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Healthy
18:22:04: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=Unknown User
```

手順 7. **show eou all** 出力で次のことを確認します。

- Client#1 は即座に例外が許可されました（したがって Healthy ステートが与えられました）。
- 2 つめの例のクライアント（10.7.1.2）は、スキャニング結果待ちのため Transition ステートに置かれました。その後、次に示すようにこのクライアントにも Healthy ステートが与えられました。

```
--------------------------------------------------------------------------------
Address         Interface              AuthType   Posture-Token Age(min)
--------------------------------------------------------------------------------
10.7.1.2        GigabitEthernet1/1     CLIENTLESS Healthy         0
10.7.1.3        GigabitEthernet1/1     CLIENTLESS Healthy         0
```

手順 8. ACS Passed Authentications ログを表示し、ステートの変更を確認します。

Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Downloadable ACL	System-Posture-Assessment
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000c.2999.fa96	..	000c.2999.fa96	000c.2999.fa96	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000c.2999.fa96	..	000c.2999.fa96	000c.2999.fa96	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy

このケースでは、2 例目のクライアントの MAC アドレスは 000d.880f.ffd4 です。

NAC L2 802.1X

次のセクションでは、IOS を実行するスイッチおよび CatOS を実行するスイッチの NAC L2 802.1x 設定について説明します。

IOS スイッチの NAC L2 802.1x の設定

このセクションでは、NAC L2 802.1x の基本機能をイネーブルにする各種コンポーネントを設定します。次の手順で操作を行います。

手順 1. IOS スイッチへの NAC L2 802.1x の設定

手順 2. Cisco Secure ACS への NAC L2 802.1x の設定

手順 3. CTA のインストール（NAC L2 802.1x サプリカントを含む）

手順 4. NAC L2 802.1x のテスト

手順 5. エージェントレス ホスト処理のための NAC L2 802.1x の設定（MAC-Auth-Bypass）

手順 6. MAC-Auth-Bypass のテスト

手順 7. ゲスト アクセス処理のための NAC L2 802.1x の設定

手順 8. ゲスト アクセスの NAC L2 802.1x のテスト

注: NAC L2 IP セクションでインストールした CTA のバージョンには、NAC L2 802.1x サプリカントが含まれていませんでした。したがってこのセクションでは、NAC L2 802.1x をサポートするためにサプリカントを含む CTA をインストールします。

NAC L2 802.1x 実装方式の概要

802.1x NAC の設定について説明する前に、802.1x の実装方式に NAC L2 802.1x と従来の IEEE 802.1x の 2 つがあることを理解する必要があります。

1 つめの NAC L2 802.1x では、NAC 対応の 802.1x サプリカントを使用して 802.1x アクセス コントロール カンバセーション内でアイデンティティおよびポスチャ クレデンシャルの検証を行います。

2 つめの方式では、まず NAC 非対応の 802.1 x サプリカントを使用してポートにアクセスしようとするエンドポイントのアイデンティティ クレデンシャルを検証し、エンドポイントが IP アドレスを取得し NAC L2 IP 問合せを開始した後に NAC L2 IP を使用してポスチャ クレデンシャルを検証します。

2 つのオプションの大きな違いは、クライアントからサーバへの通信でアイデンティティとポスチャを組み合わせるために使用する EAP 方式です。NAC 対応 802.1x は、TLS トンネルでユーザおよびマシンのクレデンシャルを転送するように修正されているため、EAP 方式として EAP-FAST を使用する必要があります。CTA のサプリカントは、EAP-GTC、 EAP-MSCHAPv2、およびクライアント側認証のための EAP-TLS をサポートします。

次のセクションでは、CTA 2.0 に含まれる NAC 対応サプリカントを使用して、1 つめの方式である NAC L2 802.1x を設定する方法を説明します。802.1x と NAC L2 IP を使用する 2 つめの方式の設定を希望する場合は、付録に掲載している詳細な設定情報を参照してください。

NAC L2 802.1x のクレデンシャルの概要

NAC L2 802.1x の理解を深めるために、まずクライアントからネットワークに送信可能な 2 つのクレデンシャルについて説明します。Microsoft Windows 環境では、2 つのアイデンティティ クレデンシャル セットをネットワークに提示できます。

1 つめのクレデンシャル セットは、コンピュータのユーザの前にマシンを認証するマシン認証の概念に基づいています。Microsoft は、起動時にコンピュータのアイデンティティおよびクレデンシャルを使用してクライアントのシステムを認証できるようにするマシン認証機能を提供しています。したがって、クライアントはドメイン グループ ポリシー オブジェクト（GPO）モデルの更新および参加に必要なセキュアなチャネルを確立することができます。

マシン認証により、コンピュータは、起動時にデバイス ドライバをロードした直後に 802.1x を使用してネットワークに対して自身の認証を実施することができます。この後コンピュータは、Windows ドメイン コントローラと通信してマシン グループ ポリシーを取得できます。マシン認証は、802.1x の使用によりドメイン GPO が機能しなくなる問題を解消するために導入されました。

802.1x で使用される 2 つめのタイプのクレデンシャルは、ユーザ認証です。ユーザは Graphic Identification and Authentication （GINA）（ログイン画面）が表示されたあと、コンピュータまたは Windows ドメインにログインします。ログインに使用したユーザ名とパスワードは、802.1x 認証のアイデンティティ クレデンシャルとして使用できます。

NAC L2 802.1x 環境では、CTA サプリカントは EAP-FAST を使用してマシンおよびユーザ認証を実行します。EAP-FAST は Protected Access Credential （PAC）を使用してクライアントと RADIUS サーバを相互に認証します。PAC は、クライアントと

サーバの相互認証に使用される一意の共有クレデンシャルで、特定のクライアントのユーザ名およびサーバ機関 ID と関連付けられています。PAC により、Public Key Infrastructure（PKI）およびデジタル証明書を使用する必要性が排除されました。EAP-FAST の詳細情報については、以下の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/wr/airo1k/eapfast/chapter01/eapfast.shtml

EAP-FAST は、3 つの基本フェーズで構成されます。

- フェーズ 0（オプション）：PAC が最初にクライアントに配布されます。
- フェーズ 1： PAC を使用してセキュアなトンネルが確立されます。
- フェーズ 2：確立されたトンネルでクライアントが認証されます。

EAP-FAST 仕様では、PAC のプロビジョニング方法に、アウトオブバンド プロビジョニングおよびインバンド プロビジョニングの 2 つがあります。NAC L2 802.1x に対応する CTA サプリカントを使用する場合は、インバウンド プロビジョニングでのみ PAC をプロビジョニングできます。CTA サプリカントは、ACS サーバによってインバウンド プロビジョニングを許可されている場合で、クライアント側の認証がマシンに割当てられた証明書（マシン証明書）を使用して成功したマシン認証、または成功したユーザ認証の場合にのみ、ホストに PAC をプロビジョニングします。NAC L2 802.1x 対応の CTA サプリカントは、アウトオブバンド プロビジョニングをサポートしません。

ここでは、設定を簡略化するためにユーザ認証のみを設定します。認証は ACS のローカルのユーザ名およびパスワード データベースで行います。

IOS スイッチへの NAC L2 802.1x の設定

注: 前のセクションでのテストのために NAC L2 IP を設定している場合は、NAC L2 802.1x 設定を開始する前に、スイッチポートの NAC L2 IP 設定をクリアしてください。

手順 1. スイッチポートの NAC L2 IP 設定をクリアします。次のコマンドを実行します。

```
IOS-Switch(config)#int gig 1/1
IOS-Switch(config-if)#no switchport acces vlan 1000
IOS-Switch(config-if)#no ip admission NAC-L2-IP
IOS-Switch(config-if)#no ip access-group interface_acl in
```

手順 2. ギガビットイーサネット 1/1 にスイッチポート コマンドを追加します。

```
IOS-Switch(config-if)#switchport
IOS-Switch(config-if)#switchport mode access
```

これで NAC L2 802.1x 設定を開始する準備が整いました。

タスク 1：NAC L2 802.1x の VLAN 設定

NAC L2 802.1x は、VLAN 割り当てを通じてポリシーを適用します。したがって、スイッチには適切な VLAN を設定する必要があります。スイッチへの 802.1x 設定例として、次の VLAN および VLAN インターフェイスを使用します。

VLAN 名	VLAN	4948 サブネット
employees	10	10.7.10.*
contractors	20	10.7.20.*
utilities	30	10.7.30.*
guests	40	10.7.40.*

VLAN 名	VLAN	4948 サブネット
healthy	50	10.7.50.*
checkup	60	10.7.60.*
transition	70	10.7.70.*
quarantine	80	10.7.80.*
infected	90	10.7.90.*
unknown	100	10.7.100.*
voice	110	10.7.110.*
servers	200	10.0.200.*
nads	255	10.0.255.*

```
interface Vlan10
 description Corporate VLAN
 ip address 10.7.10.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan20
 description Contractors VLAN
 ip address 10.7.20.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan30
 description Utilities VLAN
 ip address 10.7.30.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan40
 description Guests VLAN
 ip address 10.7.40.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan50
 description Healthy VLAN
 ip address 10.7.50.1 255.255.255.0
 ip helper-address 10.0.200.10
!
```

```
interface Vlan60
 description Checkup VLAN
 ip address 10.7.60.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan70
 description Transition VLAN
 ip address 10.7.70.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan80
 description Quarantine VLAN
 ip address 10.7.80.1 255.255.255.0
 ip access-group Interface_ACL in
 ip helper-address 10.0.200.10
!
interface Vlan90
 description Infected VLAN
 ip address 10.7.90.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan100
 description Unknown VLAN
 ip address 10.7.100.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan110
 description Voice VLAN
 ip address 10.7.110.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan200
 description Servers VLAN
 ip address 10.0.200.1 255.255.255.0
```

```
 ip helper-address 10.0.200.10
!
interface Vlan255
 description Unknown VLAN
 ip address 10.0.255.7 255.255.255.0
 ip helper-address 10.0.200.10
```

タスク 2：NAC L2 802.1x のための NAD への AAA 設定

ここでは、NAD で NAC L2 802.1x のために AAA をイネーブルにする手順を説明します。

注: 前のセクションの NAC L2 IP 設定で AAA をイネーブルにしている場合は、手順 1 は省略してください。

タスク 2 は、NAC L2 802.1x を使用する IOS スイッチ上で AAA をイネーブルにするために必要な最小限の手順です。

手順 1. **aaa new-model** グローバル設定コマンドを使用して、スイッチ サービス上で AAA をイネーブルにします。

手順 2. **aaa authentication dot1x default group radius** グローバル設定コマンドを使用して、スイッチが 802.1x 認証に RADIUS を使用するように設定します。

```
IOS-Switch(config)#aaa authentication dot1x default group radius
```

注: 前の NAC L2 IP 設定のセクションで AAA をイネーブルにしている場合は、手順 1 および 手順 3 は省略してください。

手順 3. **aaa authorization network default group radius** グローバル設定コマンドを使用して、スイッチがすべてのネットワーク関連サービス要求に対して許可を実行するように設定します。

手順 4. **aaa accounting dot1x default start-stop group radius** グローバル設定コマンドを使用して、802.1x アカウンティングのための AAA アカウンティングをイネーブルにします。

```
IOS-Switch(config)#aaa accounting dot1x default start-stop group radius
```

手順 5. **ip radius source-interface** グローバル設定コマンドを使用して、すべての発信 RADIUS パケットの NAD インターフェイスを設定します。

タスク 3：スイッチでの 802.1x のイネーブル

手順 6. **dot1x system-auth-control** グローバル設定コマンドを使用して、802.1x をイネーブルにします。

```
IOS-Switch(config)#dot1x system-auth-control
```

タスク 4：インターフェイスへの 802.1x の設定

手順 7. **dot1x port-control auto** コマンドを使用して、ギガビット イーサネット 1/1 上の 802.1x ポート コントロール を auto に設定します。

```
IOS-Switch(config-if)#dot1x port-control auto
```

手順 8. **dot1x timeout reauth-period server** コマンドを使用して、ACS のタイマー セットで使用する 802.1x 再認証タイマーを設定します。

```
IOS-Switch(config-if)#dot1x timeout reauth-period server
```

手順 9. **dot1x reauthentication** コマンドを使用して、インターフェイスの 802.1x 再認証をイネーブルにします。

```
IOS-Switch(config-if)#dot1x reauthentication
```

NAC L2 802.1x 用のネットワーク アクセス プロファイルの設定

ここでは、NAC L2 802.1x をサポートするネットワーク アクセス プロファイル（認証、ポスチャ検証、許可）の設定方法を説明します。Cisco Secure ACS 4.0 では、次の 2 つの方法でネットワーク アクセス プロファイルを設定できます。

- 空のプロファイルを追加し、必要なすべての情報を設定する。
- テンプレート プロファイルを使用し、このテンプレートに含まれている基本情報をベースにネットワーク アクセス プロファイルをカスタマイズする。

Cisco Secure ACS 4.0 には予め 7 つのネットワーク アクセス プロファイル テンプレートが定義されています。

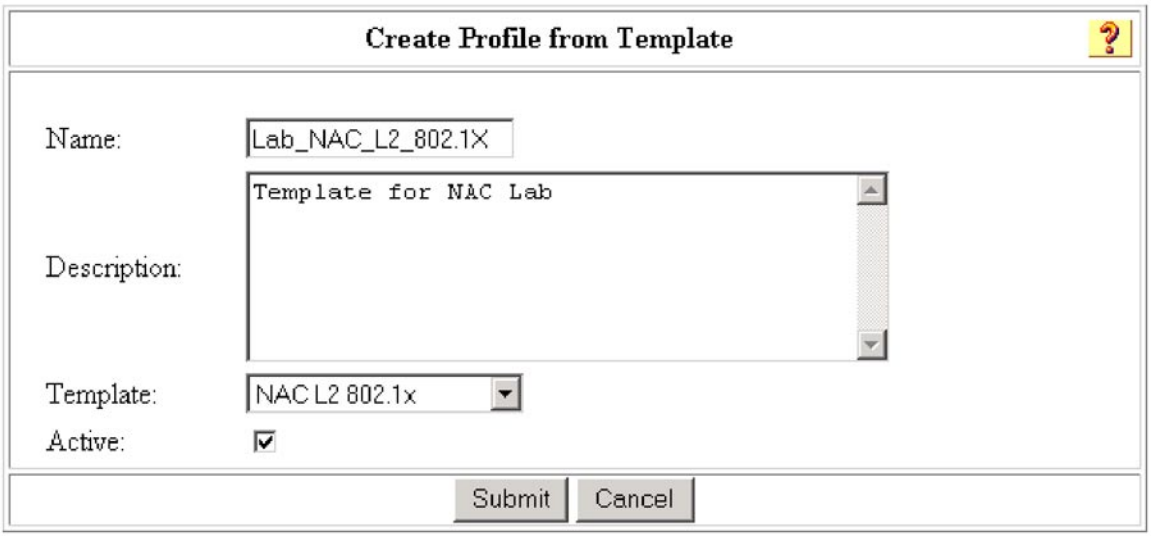
- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- Microsoft IEEE 802.1x
- Wireless（NAC L2 802.1x）
- Authentication Bypass（802.1x fallback）
- Agentless Host

ここでは、NAC L2 802.1x ネットワーク アクセス プロファイル テンプレートを使用して基本プロファイルを作成し、必要な変更を加えてこのテンプレートをカスタマイズします。

タスク 1：テンプレートからの NAC L2 802.1x プロファイルの作成

手順 1. メイン メニューから **Network Access Profiles** を選択し、**Add Template Profile** を選択します。

手順 2. Template ドロップ ダウン メニューで NAC L2 802.1x を選択し、NAC L2 802.1x のテンプレートを作成します。次の図に示すような名前を付けます。**Active** をチェックしてこのプロファイルをイネーブルにします。



手順 3. **Submit** をクリックします。

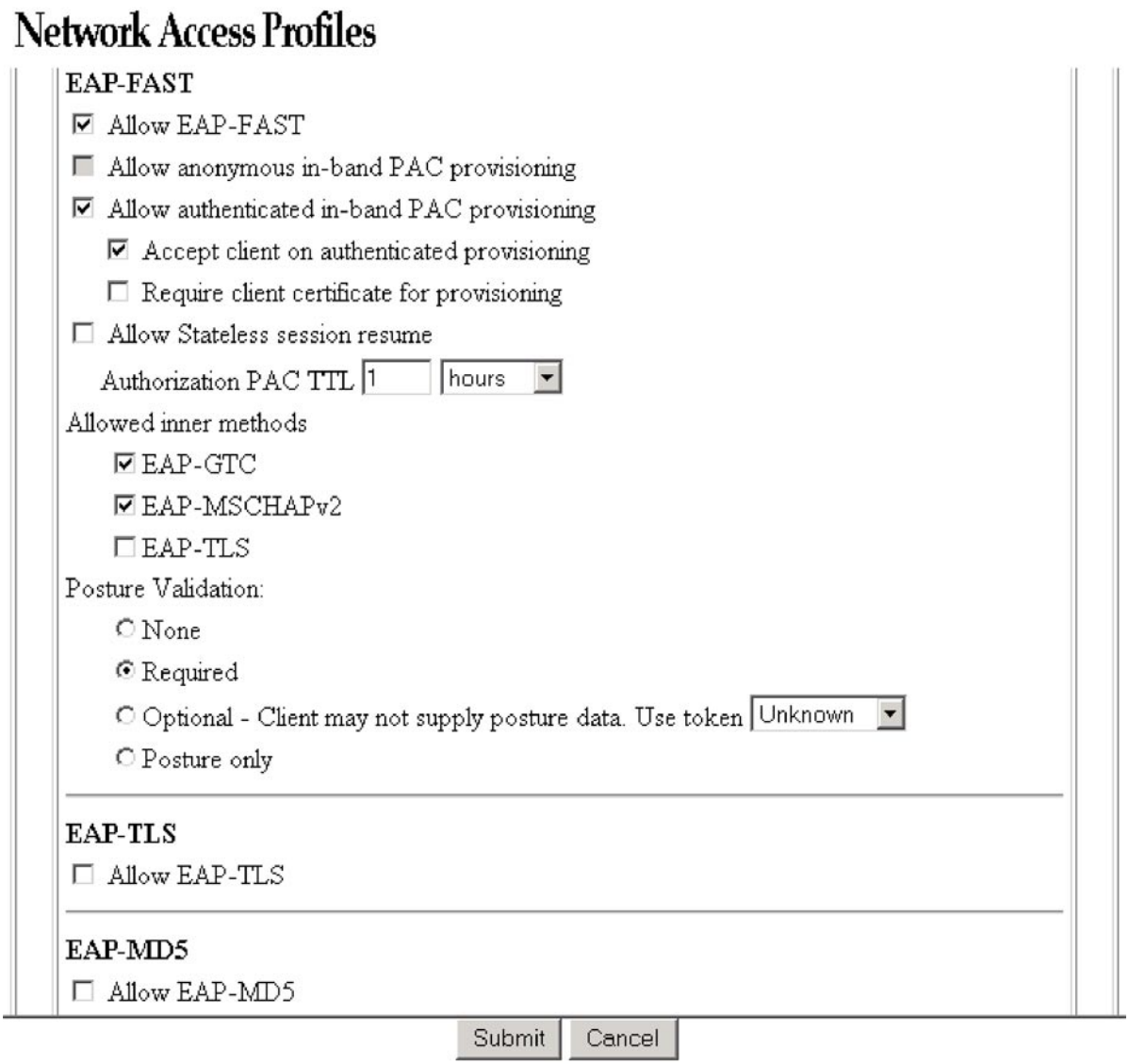
注: Cisco Secure ACS 4.0 テンプレートの一部として、サンプルの RADIUS 許可コンポーネントが作成されます。この設定においては、無視して構いません。

タスク 2：認証

手順 1. Network Access Profiles 画面で、新しいプロファイルの Authentication のリンクを選択します。

○	Lab_NAC_L2_802.1X	Authentication Posture Validation Authorization	Template for NAC Lab	YES

手順 2. この基本テンプレートの一部として、EAP-FAST 設定の一部がすでに選択されています。



手順 3. **Submit** をクリックします。

注: EAP-GTC をイネーブルにして CTA サプリカントを使用する場合、サプリカントがシングル サインオンを使用するように設定している場合でも、常にユーザのクレデンシャルが要求されます。ユーザ クレデンシャルが要求されないようにするには、EAP-GTC 方式のチェックを外します。

タスク 3：ポスチャ検証

参考として、ポスチャ検証の設定を次に示します。

手順 1. Network Access Profiles 画面から、作成したプロファイルの **Posture Validation** のリンクを選択します。

手順 2. テンプレートに次のポスチャ ポリシーを追加します。

Name: L2-Posture	
Required Condition Types	Cisco:PA Cisco:Host
Posture Validation Policies	CTA Windows
Assessment Result Configuration	

Result	Message	URL Redirect
Healthy	NAC L2 802.1x Healthy	
Checkup	Please update your software to prevent being quarantined by the network.	
Transition	Computer under audit…	
Quarantine	NAC L2 802.1x Quarantined	
Infected	Infected	
Unknown		

Audit Selection	
Audit Server	None

手順 3. **Submit** をクリックします。

タスク 4：許可

手順 1. テンプレートから **Authorization** のリンクをクリックします。

手順 2. 許可をイネーブルにします。

User Group	Assessment Result	Deny Access	Shared RAC	Downlodable ACL
Employees	Healthy	No	L2_1x_Healthy_RAC	
Contractors	Healthy	No	L2_1x_Healthy_RAC	
Any	Healthy	No	L2_1x_Healthy_RAC	
Guests	Any	No	L2_1x_Quarantine_RAC	
Utilities	Any	No	L2_1x_Quarantine_RAC	
If a condition is not defined or there is no matched condition:			L2_1x_Quarantine_RAC	
Include RADIUS attributes from user's group:				No
Include RADIUS attributes from user record:				No

手順 3. **Submit** をクリックします。

CTA のインストール

ここでは、CTA と NAC L2 802.1 x サプリカントをインストールする方法を説明します。

タスク 1：CTA 用のクライアント証明書のインストール

正しく認証を実行するために、Cisco Secure ACS にインストールした証明書を CTA にもインストールする必要があります。クライアント上の CTA には、2 つの方法で証明書を追加できます。ここでは、CTA のインストール前に証明書を追加する方法を説明します。証明書は、CTA のインストール後にルート ストアに追加することもできます。2 つめの方法は、このセクションの最後に説明します。

手順 1. client1 に *certs* という名前のフォルダを作成し、CTA.exe ファイルと同じディレクトリに配置します。

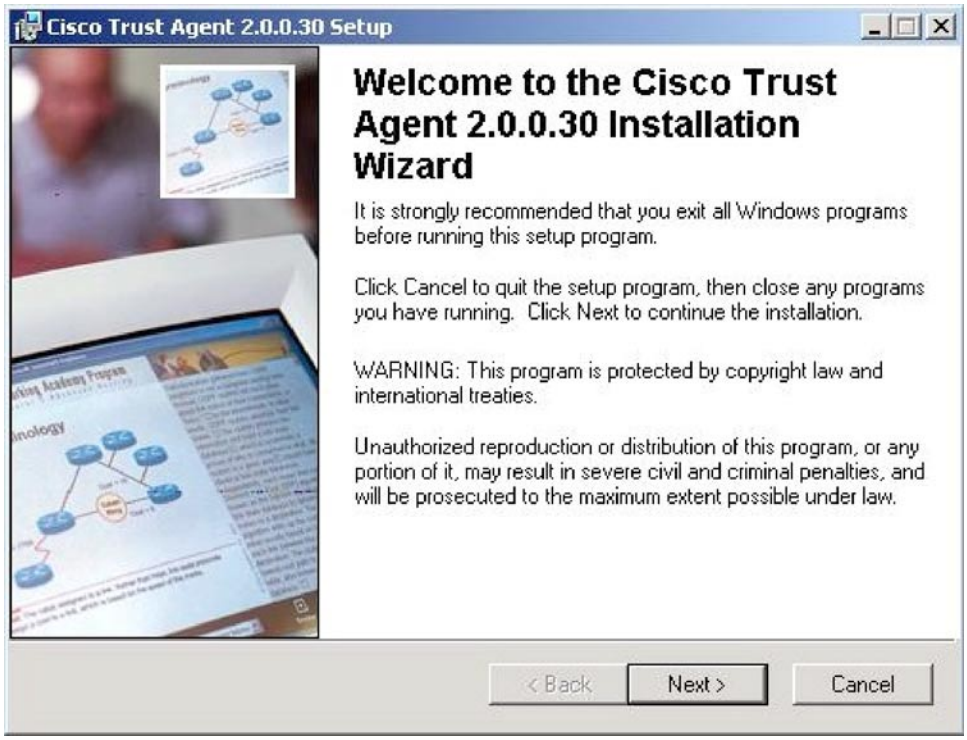
手順 2. クライアントを ACS で認証するときに CTA が使用する CA 証明書を **certs** フォルダに配置します。

注: CTA は、certs サブディレクトリに配置されているすべてのパブリック証明書をインポートします。このフォルダは、cta.exe ファイルと同じディレクトリに配置する必要があります。

タスク 2：CTA 2.0 のインストール

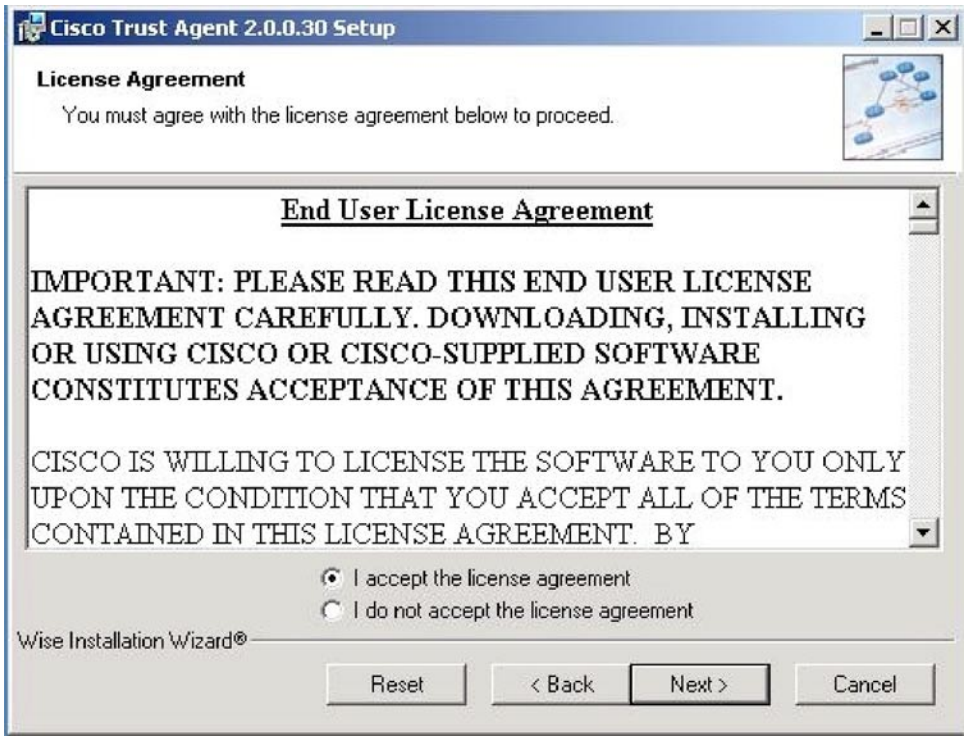
手順 1. CTA サプリカント セットアップ ファイルをクライアントにダウンロードします。クライアント上で CTA.exe ファイルが配置されているフォルダを開き、使用する ctasetup ファイルをダブルクリックします（この例では **ctasetup-supplicant-win-[version].exe** を使用）。

Cisco Trust Agent の **Installation Wizard** が表示されます。

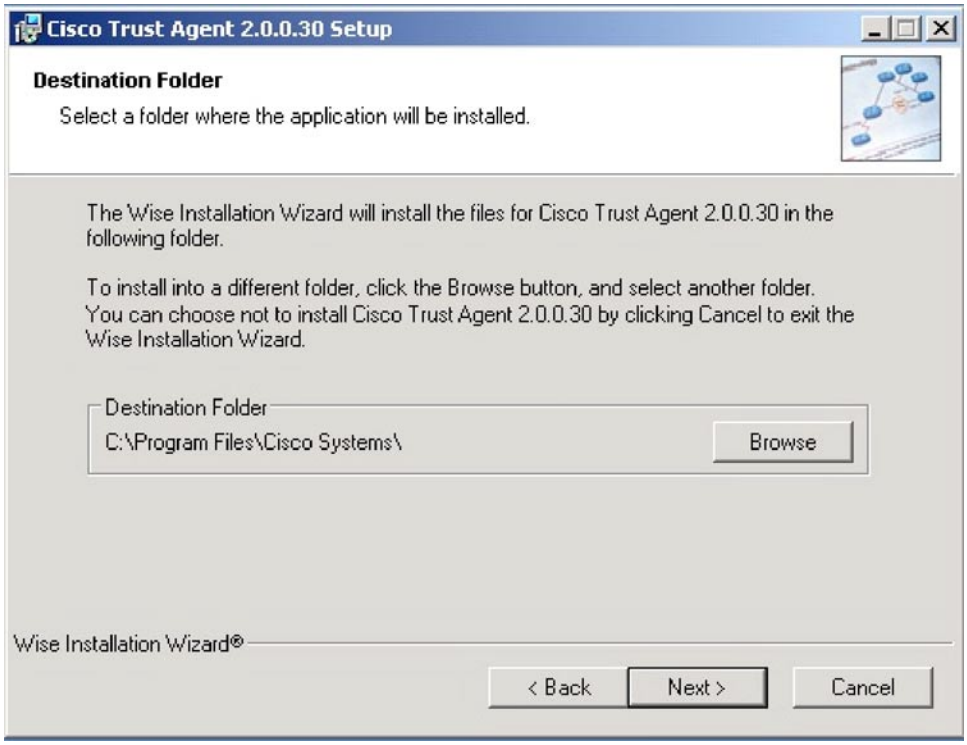


手順 2. **Next** をクリックします。

手順 3. **Next** をクリックして License Agreement（ライセンス契約）を受諾します。**Destination Folder** ウィンドウが表示されます。



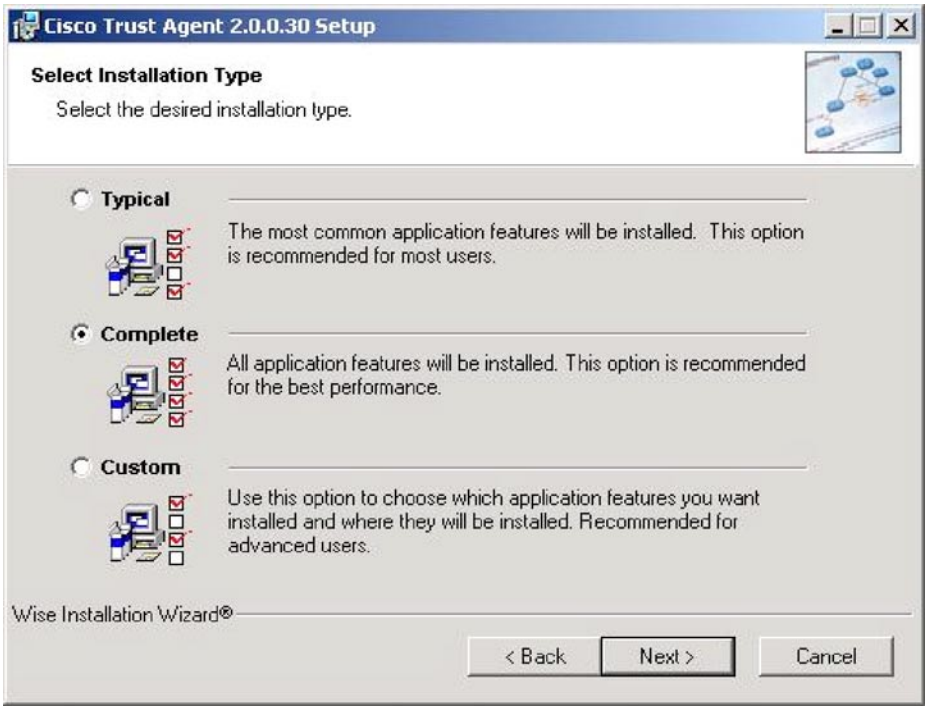
手順 4. デフォルトの Destination Folder をそのまま受入れ、**Next** をクリックします。



手順 5. **Select Installation Type** ダイアログ ボックスが表示されます。

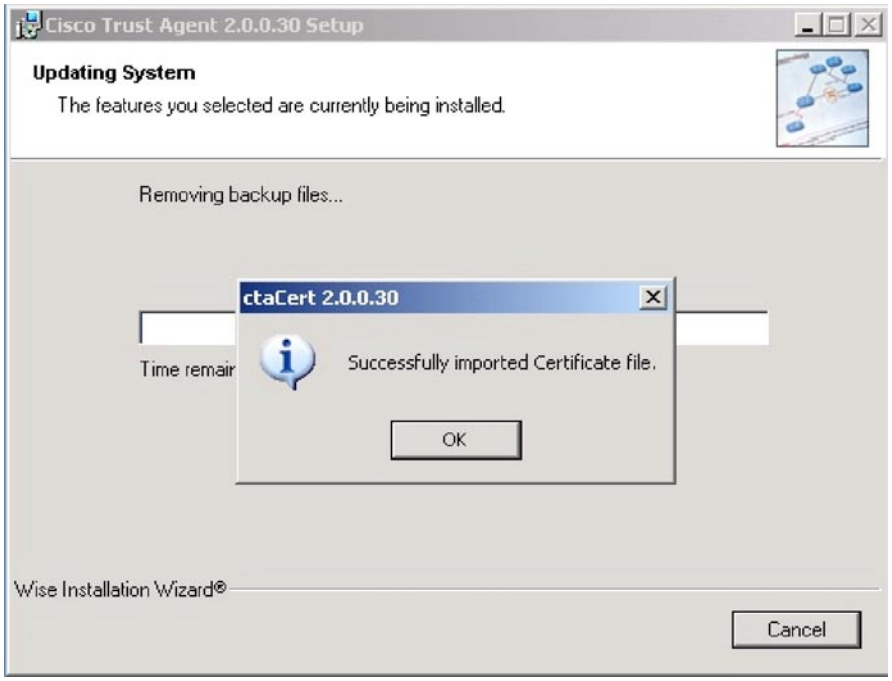
手順 6. **Complete** ラジオ ボタンをクリックします。

手順 7. **Next** をクリックします。

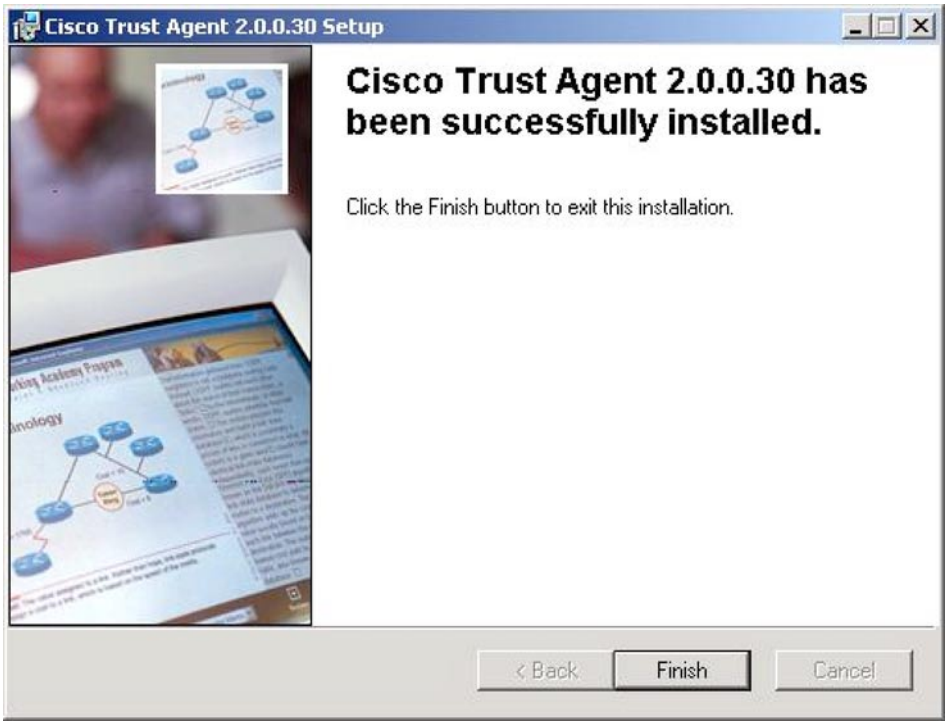


手順 8. 選択したディレクトリにアプリケーションがインストールされます。

手順 9. インストール中に証明書のインポートが成功すると、次のメッセージが表示されます。**OK** をクリックします。

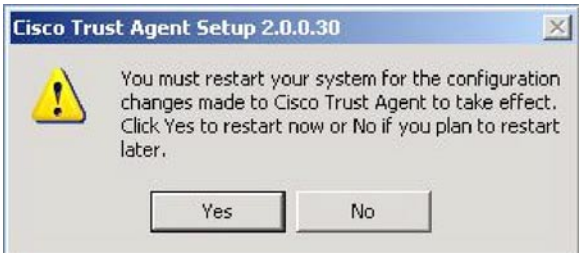


手順 10. インストールが完了すると、**Installation Completed** ウィンドウが表示されます。



手順 11. Finish をクリックしてアプリケーションのインストールを終了します。

手順 12. システムの再起動が必要です。必要なときに、再起動を求めるメッセージが表示されます。



タスク 3：（オプション）CTA へのルート証明書の手動でのインストール

タスク 1 の手順 1 で CTA のフォルダに *certs* フォルダをコピーしなかった場合は、Cisco Trust Agent を使用する前にルート証明書をインストールする必要があります。

証明書を手動でインストールするには、次の手順を実行します。

手順 1. ネットワーク クライアントに証明書をコピーします。

手順 2. ネットワーク クライアントでコマンド プロンプトを開きます。

手順 3. Cisco Trust Agent がインストールされているディレクトリに変更します。デフォルトのロケーションは、次のディレクトリです。

```
C:\Program Files\Cisco Systems\CiscoTrustAgent\
```

手順 4. 次のコマンドを入力します。

```
ctaCert.exe /add "cert_path_&_cert_name" /store "Root"
```

（cert_path_&cert_name は証明書への完全なパスと完全なファイル名です）

証明書がネットワーク クライアントの信頼される証明書ストアに追加されます。

CTA の設定

サプリカントへの設定の変更はありません。サプリカントは、常にマシン認証を試みるようにデフォルトで設定されています。サプリカントはマシン認証のための適切なクレデンシャルを持たないため、Cisco Secure ACS は、ネットワーク アクセス デバイスからの最初の RADIUS 要求に対して、RADIUS Access-Reject 応答を発行します。このとき、スイッチ上の 802.1x ステート マシンによりポートが保留ステートに移行されるため、スイッチがクライアントからの EAPOL-Starts を受け付けられなくなることに注意してください。スイッチの保留ステート中にサプリカントが EAPOL-Starts を送信すると、エンドユーザのログイン体験が通常よりも遅くなる可能性があります。サプリカントは、スイッチが 802.1x ステート マシンを接続ステートに移行して、サプリカントからの EAPOL-Starts を受け付けるようになるまで待機してから、正常な 802.1x 交換を開始し、ユーザ ログインを完了する必要があります。

NAC L2 802.1x 機能の確認

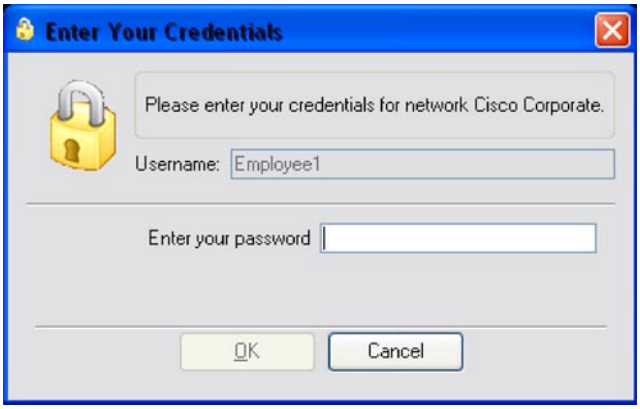
ここでは、NAC L2 802.1x が正しく設定されていること、Cisco Secure ACS から正しいポスチャ トークンを受信すること、Cisco Secure ACS からの正しい VLAN 割り当てが NAD に適用されることを確認する方法を説明します。

クライアントが Healthy とみなされ、Healthy のロールに配置されるには、必要なクレデンシャル情報を NAD に返し、この情報が NAD から Cisco Secure ACS に送信される必要があります。Network Access Profile のセクションで作成した各クレデンシャルのポスチャ検証の要件を満たしているクライアントには Healthy アプリケーション ポスチャ トークンが渡されます。このクレデンシャルには、**Cisco Trust Agent**、エージェント バージョン **>=2.0.0.30**、OS-Type contains **Windows XP** が含まれます。

注: クライアントは、Cisco Secure ACS が具体的に要求しているクレデンシャルのみを Cisco Secure ACS に渡すことに注意してください。

手順 1. no shut コマンドを入力し、クライアントが接続しているスイッチポートをもう一度イネーブルにします。

手順 2. クライアント上に、サプリカントからの次のようなクレデンシャル要求が表示されます。



手順 3. **show dot1x all** コマンドを発行してクライアントのステータスを確認します。

```
NAC4948#sh dot1x all

Dot1x Info for interface GigabitEthernet 1/1

---------------------------------------------------

Supplicant MAC 000d.80cd.cda6

   AuthSM State     = AUTHENTICATED

   BendSM State     = IDLE

   Posture          = Healthy

   ReAuthPeriod     = 3600 Seconds (From Authentication Server)

   ReAuthAction     = Terminate

   TimeToNextReauth  = 3570 Seconds

PortStatus       = AUTHORIZED

MaxReq           = 2

MaxAuthReq       = 2

HostMode         = Single

PortControl      = Auto

ControlDirection  = Both

QuietPeriod      = 60 Seconds

Re-authentication = Enabled

ReAuthPeriod     = From Authentication Server

ServerTimeout    = 30 Seconds
```

```
SuppTimeout      = 30 Seconds
TxPeriod         = 30 Seconds
Guest-Vlan       = 0
```

手順 4. クライアントのスイッチポートが適切な VLAN に配置されたことを確認します。

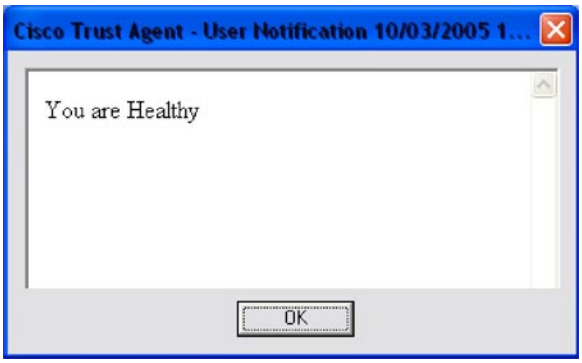
```
NAC4948#sh vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                         active    Ge1/5, Ge1/6, Ge1/7, Ge1/8
                                               Ge1/9, Ge1/10, Ge1/13, Ge1/15
                                               Ge1/16, Ge1/17, Ge1/18, Ge1/19
                                               Ge1/20, Ge1/21, Ge1/22, Ge1/23
                                               Ge1/24, Gi1/2
10   employees                       active    Ge1/3
20   contractors                     active
30   utilities                       active
40   guests                          active
50   healthy                         active    Ge1/1
60   checkup                         active
70   transition                      active
80   quarantine                      active
90   infected                        active
100  unknown                         active    Ge1/4, Ge1/11, Ge1/14
110  voice                           active
200  servers                         active    Ge1/12
255  nads                            active
```

手順 5. クライアントのスイッチ ポートが VLAN 50（Healthy）に配置されたことが確認できます。次のインターフェイス コマンドを実行すると、インターフェイスのスイッチ ポート情報も確認できます。

```
NAC4948#sh int GigE 1/1 switchport
Name: Ge1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
```

```
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 50 (healthy)
…
```

手順 6. クライアント上で CTA により次のようなポップアップ メッセージが表示されます。



手順 7. ACS 上で適切なレポートを使用してクライアント情報を確認します。ここでは、クライアントと ACS 間に正しく通信が確立されているので、Passed Authentications レポートを使用します。

次に、クライアントが *Healthy* トークンではなく *Quarantine* トークンを与えられた場合のトラブルシューティング方法について説明します。

まず、クライアントを強制的に Quarantine ロールに配置します。そのために、クライアントが検証に失敗するポスチャ検証ルールを ACS に設定します。

手順 8. Healthy ポスチャ ステータスを得るために必要な CTA の最小バージョンを変更します。

```
Cisco:PA:PA-Name contains Cisco Trust Agent
Cisco:PA:PA-Version >= 3.0.0.0
```

現在は CTA バージョン 2.0.0.30 が稼動しているため、クライアントは次のルールに適合しません。

手順 9. 次のデバックをイネーブルにします。

```
debug dot1x events
```

手順 10. `dot1x initialize interface x/x` コマンドを入力し、認証プロセスをリスタートします。

```
00:55:00: dot1x-ev:auth_initialize_enter:000d.60cd.cda6: Current ID=0
00:55:00: dot1x-ev:dot1x_update_port_direction: Updating oper direction for Ge1/1
 (admin=Both, current oper=Both)
00:55:00: dot1x-ev:dot1x_update_port_direction: New oper direction for Ge1/1 is Both
00:55:00: dot1x-ev:dot1x_port_cleanup_author: cleanup author on interface
GigabitEthernet1/1
00:55:00: dot1x-ev:dot1x_update_port_status: Called with host_mode=0 state
```

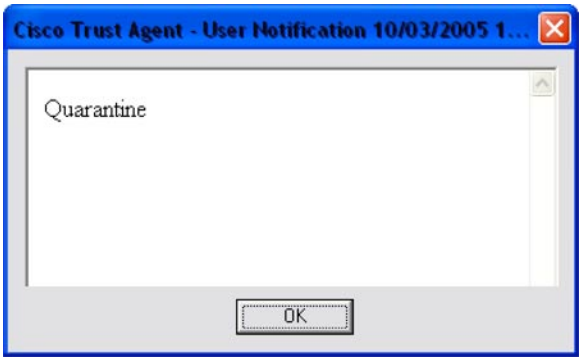
```
UNAUTHORIZED
00:55:00: dot1x-ev:dot1x_update_port_status: using mac 000d.60cd.cda6 to send port to
unauthorized on vlan 80
00:55:00: dot1x-ev:Found a supplicant block for mac 000d.60cd.cda6 1E113F0
00:55:00: dot1x-ev:dot1x_port_unauthorized: Host-mode=0 radius/guest vlan=80 on
GigabitEthernet1/1
```

手順 11. クライアントが VLAN 80（検疫 VLAN）に配置されていることを確認します。

```
NAC4948#sh dot1x int
NAC4948#sh dot1x interface GigE 1/1
Supplicant MAC 000d.80cd.cda6
   AuthSM State     = AUTHENTICATED
   BendSM State     = IDLE
   Posture          = Quarantine
   ReAuthPeriod     = 3600 Seconds (From Authentication Server)
   ReAuthAction     = Reauthenticate
   TimeToNextReauth  = 3482 Seconds
PortStatus       = AUTHORIZED
MaxReq          = 2
MaxAuthReq       = 2
HostMode         = Single
PortControl      = Auto
ControlDirection  = Both
QuietPeriod      = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod     = From Authentication Server
ServerTimeout    = 30 Seconds
SuppTimeout      = 30 Seconds
TxPeriod         = 30 Seconds
Guest-Vlan       = 0
```

このサンプル出力では、正しいユーザ名とパスワードが入力されたため、クライアントは正常に認証されましたが、クレデンシャル チェックの 1 つに失敗したため、Quarantine ロールに配置されました。

手順 12. クライアント上で CTA により次のようなポップアップ メッセージが表示されます。



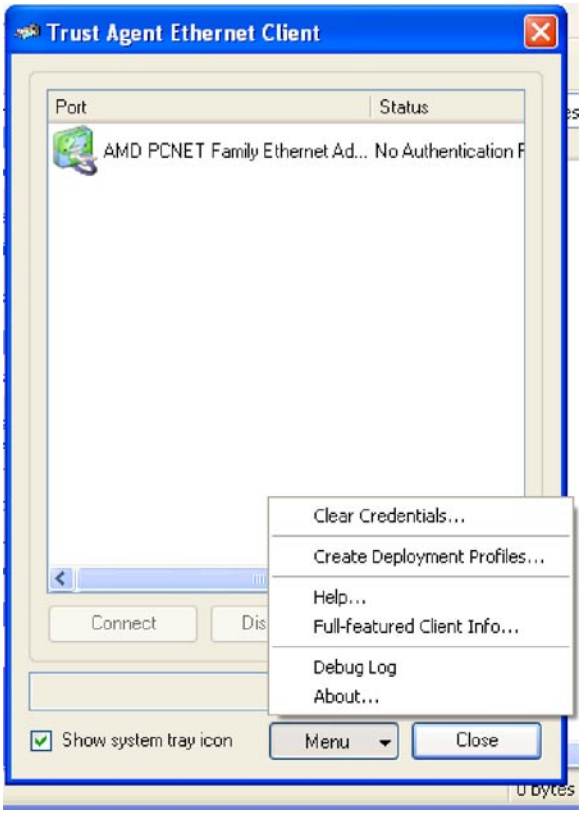
手順 13. ACS レポートを表示し、クライアントが検疫された理由を収集します。

レポート情報を確認することにより、どこで問題が発生したかを把握し、トラブルシューティング プロセスを開始することができます。

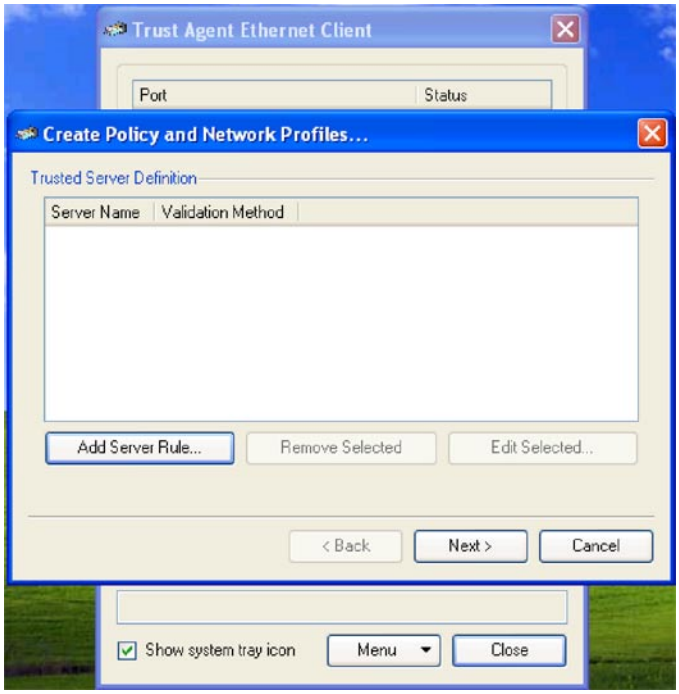
サプリカントのシングル サインオンの設定

CTA サプリカントの設定

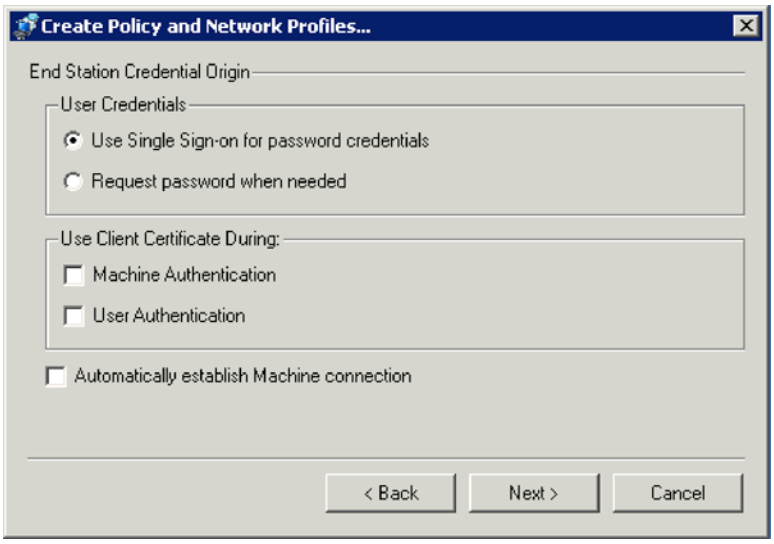
CTA サプリカントと NAC L2 802.1x を設定する場合、ほとんどのポリシーはサーバで定義されます。クライアントにもいくつかの利用可能なオプションがあります。これらのオプションは、XML ファイルを使用して設定します。これらの XML ファイルを作成するには、まず管理用ワークステーションに CTA サプリカントをインストールします。このワークステーション上で、**Trust Agent Ethernet Client Open** メニュー オプションにアクセスします。CTA サプリカント GUI のメニュー ボタンの下に **Create Deployment Profiles** オプションが表示されます。



このオプションを選択すると、Deployment Profile を作成するためのウィザードが表示されます。このウィザードの最初の画面は Trusted Server Definition ダイアログです。



このダイアログでは、信頼する ACS サーバを定義できます。検証方法として 証明書または PAC を指定できます。ACS サーバがクライアントに送信したクレデンシャルが EAP-FAST のフェーズ 1 で検証され、SSL トンネルが確立されます。

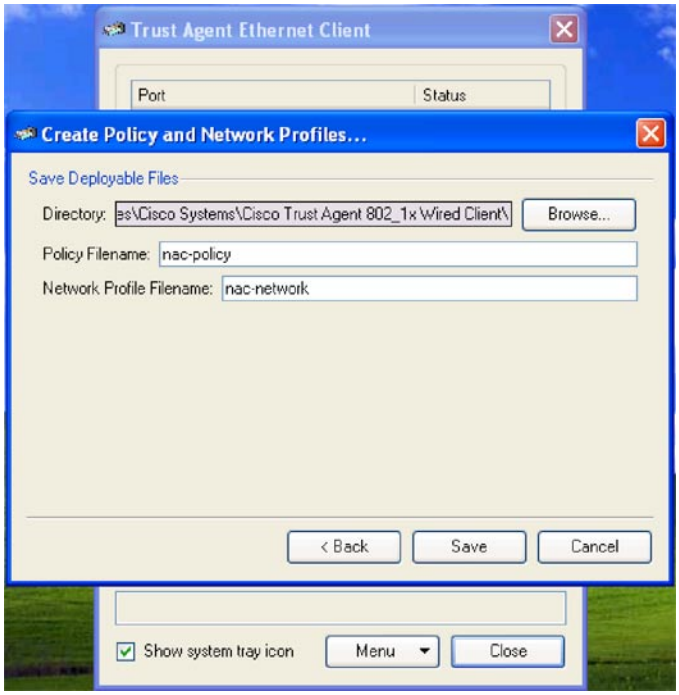


このダイアログは 3 つのセクションに分かれています。最初のセクションでは、ユーザ クレデンシャルの取得方法をサプリカントに指示します。シングル サインオン ラジオボタンを選択すると、クライアントはユーザ ログインのユーザ名とパスワードの使用を試みることができます。もう一方のボタンを選択すると、クライアントはパスワード クレデンシャルをユーザに要求できます。

このダイアログの 2 つめのセクションでは、ホスト上で証明書の使用が可能なときに、サプリカントがどの目的で証明書を使用するかを決定します。証明書は、ユーザまたはマシンの認証に使用できます。このダイアログは、すでにホストに証明書がプロビジョニングされていることを前提としています。

3 つめの **Automatically establish Machine Authentication** セクションは、デフォルトでイネーブルにされていますが、ここではチェックを外し、ディセーブルにします。

エンド ステーションのクレデンシャルのオリジンの定義が完了したら、Deployment Profile を定義する 2 つの XML ファイルを保存するためのダイアログが表示されます。ユーザは、ネットワーク プロファイル ファイルとポリシー ファイルの作成先を選択できます。



管理者は、エンドユーザのステーションへの通常のファイル移動方法を使用できます（Microsoft SMS など）。

- CTA Client インストール ファイルをエンドユーザのマシンにエクスポートします。
- エンドユーザのマシンでこのインストール ファイルを実行します。ここではマシンを再起動しません。
- ポリシーおよびプロファイル設定ファイルを、インストーラが作成した次のフォルダにエクスポートします。
- **重要：**既存のクライアントを更新する場合は、新たに展開する設定ファイルと既存のファイルを置き換える必要があります。指定された各フォルダには、1 つの xml ファイルしか保存できません。これらのファイルを <install directory>\profiles\policies および <install directory>\profiles\networks フォルダに移動してください。

注: デフォルトの<install directory> は、Program Files\Cisco Trust Agent Ethernet Client\ policy configuration file: <install directory>\profiles\policies network configuration file: <install directory>\profiles\networks です。

エンドユーザのマシンを再起動します。エンドユーザの CTA クライアントが自動的に起動し、展開された設定ファイルを使用します。

サプリカントを使用しないホストの考慮事項

NAC L2 802.1x ネットワークに接続するすべてのホストにサプリカントがインストールされるわけではありません。このタイプのホストのためにいくつかの Identity Based Networking Services（IBNS）機能が開発されています。これらは IBNS 機能であって NAC のために開発されたものではありませんが、NAC 対応ネットワークでのエージェントレス ホストの処理に重要な役割を果たします。これらの IBNS 機能により、802.1x サプリカントが稼動しないホストにゲスト アクセス用の VLAN を割り当てること、MAC アドレスに基づいてホストを認証することが可能になります。

802.1x 非対応ホスト用のゲスト VLAN

ゲスト VLAN により、802.1x 非対応ホストは 802.1x 認証を使用するネットワークにアクセスすることが可能になります。802.1x 認証をサポートするためのシステムのアップグレード中にゲスト VLAN を使用できます。

1 つの VLAN を 802.1x ゲスト VLAN として設定すると、すべての 802.1x 非対応ホストはこの VLAN に配置されます。ゲスト VLAN としては、プライベート VLAN および RSPAN VLAN を除き、任意の VLAN を設定できます。ポートがすでにゲスト VLAN 上に（で）転送を行っているときに、そのホストのネットワーク インターフェイス上で 802.1 x サポートをイネーブルにすると、このポートはただちにゲスト VLAN から外され、オーセンティケータが認証の発生を待機します。

ポート上での 802.1x 認証をイネーブルにすると、802.1x プロトコルが開始されます。ホストが一定の時間内にオーセンティケータから送信されたパケットに応答できない場合、オーセンティケータはこのポートをゲスト VLAN に配置します。

ゲスト VLAN は、シングル認証モードおよびマルチホスト モードの両方でサポートされています。

Windows XP ホスト上でのゲスト VLAN に対する 802.1x 認証設定の注意事項

ここでは、Windows XP ホスト上でのゲスト VLAN に対する 802.1x 認証設定の際の注意事項を説明します。

- ゲスト VLAN がイネーブルにされているポートは、単一方向ポートとして設定できません。逆に言えば、単一方向ポートにはゲスト VLAN を設定できません。
- ホストがオーセンティケータに応答できなかった場合、ポートは 180 秒間接続ステートに置かれます。この時間が経過すると、ホストにログイン/パスワード ウィンドウは表示されません。ユーザは、ネットワーク インターフェイス ケーブルを取り外し、再度接続する必要があります。
- 不正なログインまたはパスワードで応答するホストは認証に失敗します。認証が失敗したホストは、ゲスト VLAN に配置されません。ホストが最初に認証に失敗すると、Quiet-Period タイマーが始動し、このタイマーに設定された期間はアクティビティが一切発生しません。Quiet-Period タイマーが失効すると、ホストにログイン/パスワード ウィンドウが表示されます。ホストが 2 回目の認証に失敗すると、Quiet-Period タイマーが再度始動し、このタイマーに設定された期間はアクティビティは一切発生しません。その後ホストに 3 回目のログイン/パスワード ウィンドウが表示されます。ホストが 3 回目の認証に失敗すると、ポートは接続および未許可ステートに置かれます。ユーザは、ネットワーク インターフェイス ケーブルを外して再度接続する必要があります。

ホストは、Authenticator Port Access Entity からのユーザ名およびパスワード認証要求に応答しない場合、ゲスト VLAN に配置されます。

タスク 1：インターフェイスの ゲスト VLAN サポートのイネーブル

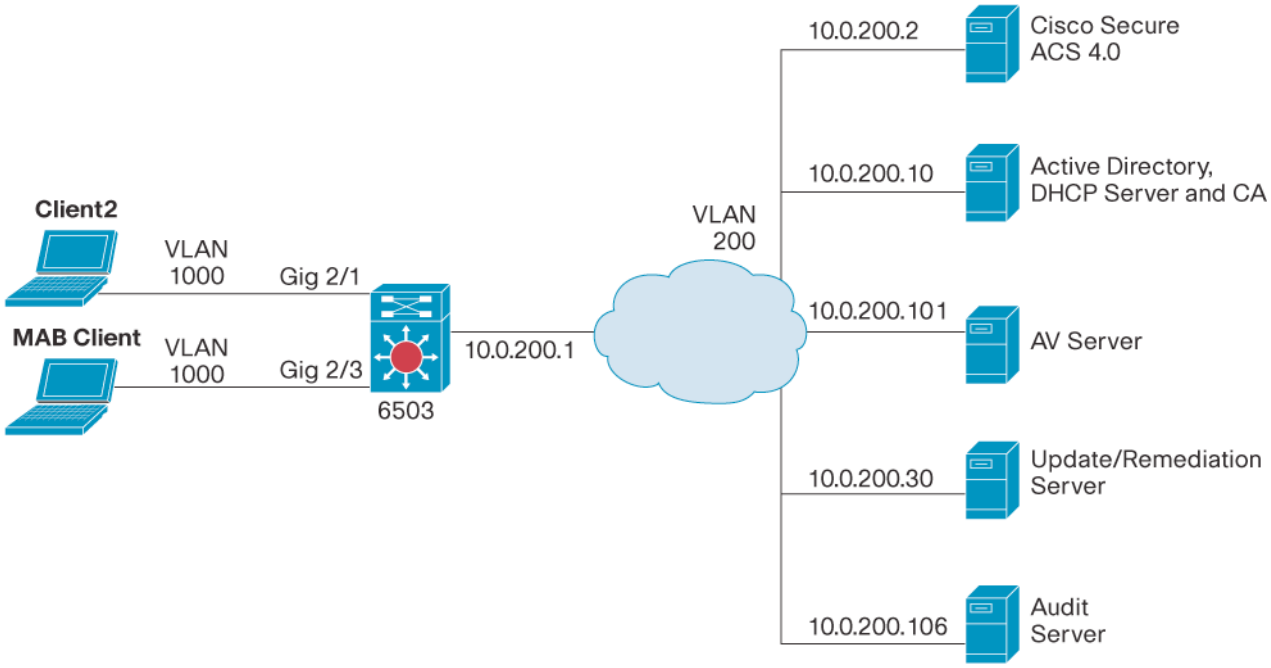
```
IOS-Switch(config)# interface gigabitethernet1/1

IOS-Switch(config-if)# dot1x guest-vlan 40
```

サプリカント サービスが停止したこと、またはサプリカントがアンインストールされたことを確認します。Windows の Wireless Zero Config サービスが停止したことを確認します。その後、サプリカントレス デバイスがゲスト VLAN に配置されたことを確認します。

CatOS スイッチへの NAC L2 IP の設定

ここでは、CatOS スイッチへの NAC L2 IP および NAC L2 802.1x の設定方法を説明します。このセクションでは、図 6 を参照してください。

図 6. CatOS のリファレンス ネットワーク



タスク 1：NAC L2 IP の設定

手順 1. スイッチで RADIUS をイネーブルにします。

```
Console> (enable) set radius server 10.0.200.20 primary
Console> (enable) set radius key cisco123
```

手順 2. スイッチで NAC L2 IP のために EAPoUDP をイネーブルにします。

```
Console> (enable) set eou enable
```

手順 3. ポスチャ検証を必要とする L2IP ポートのために EAPoUDP をイネーブルにします。

```
Console> (enable) set port eou 2/1 auto
```

手順 4. 以前に設定されたすべてのセキュリティ ACL を削除します。

```
Console> (enable) clear security acl all
```

手順 5. このポリシー ベース ACL をイネーブルにします。この ACL が参照されます。

```
Console> (enable)!Permit ARP
Console> (enable) set security acl ip nac permit arp
Console> (enable) set security acl ip nac permit arp-inspection any any
```

```
Console> (enable)!Permit DHCP Snooping
Console> (enable) set security acl ip nac permit dhcp-snooping
Console> (enable)!Permit DNS
Console> (enable) set security acl ip nac permit udp any any eq 53
Console> (enable)!Create an entry that allows access for healthy hosts access and that
Console> (enable) matches the healthy policy group name defined in ACS.
Console> (enable) set security acl ip nac permit ip group Healthy_hosts any
Console> (enable)!Create an entry that allows limited access for quarantine hosts
access and that matches the quarantine policy group name defined in ACS.
Console> (enable) set security acl ip nac permit ip group Quarantine_hosts 10.0.200.0
0.0.0.255
Console> (enable) set security acl ip nac permit ip 10.0.200.0 0.0.0.255 group
Quarantine_hosts
   !Permit quarantine hosts the ability to communicate with the default gateway
Console> (enable) set security acl ip nac permit ip group Quarantine_hosts host 10.9.1.1
Console> (enable)!Allow the default gateway to communicate with quarantine hosts
Console> (enable) set security acl ip nac permit ip host 10.9.1.1 group
Quarantine_hosts
Console> (enable)!Allow EOU
Console> (enable) set security acl ip nac permit eapoudp
Console> (enable)!Allow DHCP
Console> (enable) set security acl ip nac permit udp any eq 67 any
Console> (enable) set security acl ip nac permit udp any eq 68 any
```

手順 6. このセキュリティ ACL をコミットし、適切な VLAN に適用します。

```
Console> (enable) commit security acl all
```

手順 7. この セキュリティ ACL をデフォルト L2 IP VLAN （1000） にマッピングします。

```
Console> (enable) set security acl map nac 1000
```

注: **show security acl info all** コマンドを入力し、設定したセキュリティ ACL を確認します。

手順 8. NAC L2 IP 機能を確認します。

```
Console> (enable) show policy group all


-------------------------------------------------
Group Name          = Healthy
Group Id            = 1
No.of IP Addresses    = 1
Is Changed flag      = 0
Src Type            = ACL CLI
    List of Hosts in group.
    ----------------------
    Interface     = 2/1
    IpAddress     = 10.7.50.5
    Src type      = NAC
```

タスク 2：NAC L2 802.1x の設定

前のセクションの NAC L2 IP の手順で RADIUS をイネーブルにし、802.1x 用の VLAN を設定しているので、簡単な手順で CatOS に NAC L2 802.1x を設定できます。

手順 1. 802.1x 認証をグローバルにイネーブルにします。

```
Console> (enable) set dot1x system-auth-control enable
```

手順 2. dot1x クライアント の ポート 2/1 の 802.1x コントロールをイネーブルにします。

```
Console> (enable) set port dot1x 2/1 port-control auto
```

手順 3. このポートで再認証をイネーブルにします。

```
Console> (enable) set port dot1x 2/1 reauthentication
```

手順 4. NAC L2 802.1x 機能を確認します。

```
Console> (enable) show port dot1x 2/1
Console> (enable) show port 2/1
```

Catalyst 6500 のゲスト VLAN 設定例

ポート 2/1 を 802.1x のゲスト VLAN 40 に追加する例を示します。

```
Console> (enable) set port dot1x 2/1 guest-vlan 40
Port 2/1is Multiple-authentication enabled, guest-vlan can not be enabled
6506-CatOS> (enable) set port dot1x 2/1 multiple-authentication disable
```

```
Port 2/1Multiple-authentication option disabled
6506-CatOS> (enable) set port dot1x 2/1guest-vlan 40
Port 2/1Guest Vlan is set to 40
6506-CatOS> (enable) show port dot1x guest-vlan
Guest-Vlan    Status   Mod/Ports
------------- -------- ------------------
40             active        2/1
none          none     2/2,3/2-48,8/1-8
```

Catalyst 6500 での MAC Authentication Bypass の設定

MAC Authentication Bypass は、ポート単位で設定する IBNS 機能です。スイッチは、スイッチに接続しているホストの MAC アドレスを使って Cisco Secure ACS サーバに RADIUS 要求を送信します。この MAC アドレスが ACS の内部データベースで見つかった場合、ACS サーバは Access-Accept で応答を返し、ホストはネットワークへのアクセスを許可されます。この MAC 認証は 802.1x の後に発生するので、EAP 認証を完了できないすべてのデバイスのアクセスを拒否するデフォルトの 802.1x セキュリティ ポリシーをバイパスします。MAC Authentication Bypass は、ホストに NAH アクセスを許可できる有効な機能です。また MAC アドレスの Organizationally Unique Identifier（OUI; 組織固有識別子）を使用して MAC アドレスをワイルドカード検索することにより、同じ OUI 範囲内のアドレスを持つデバイスにネットワークへのアクセスを許可することができます。ネットワークへのアクセスを許可する必要があっても 802.1x 対応サプリカントを持たないプリンタやターミナルなどのデバイスにとって便利な機能です。MAC Authentication Bypass はダイナミックな機能なので、ネットワーク内のすべてのポートに設定することができ、プリンタが接続されるポートに明示的に設定する必要はありません。

注: MAC Authentication Bypass は、現時点で Catalyst 6500 でのみサポートされています。

タスク 1：Catalyst 6500 の設定

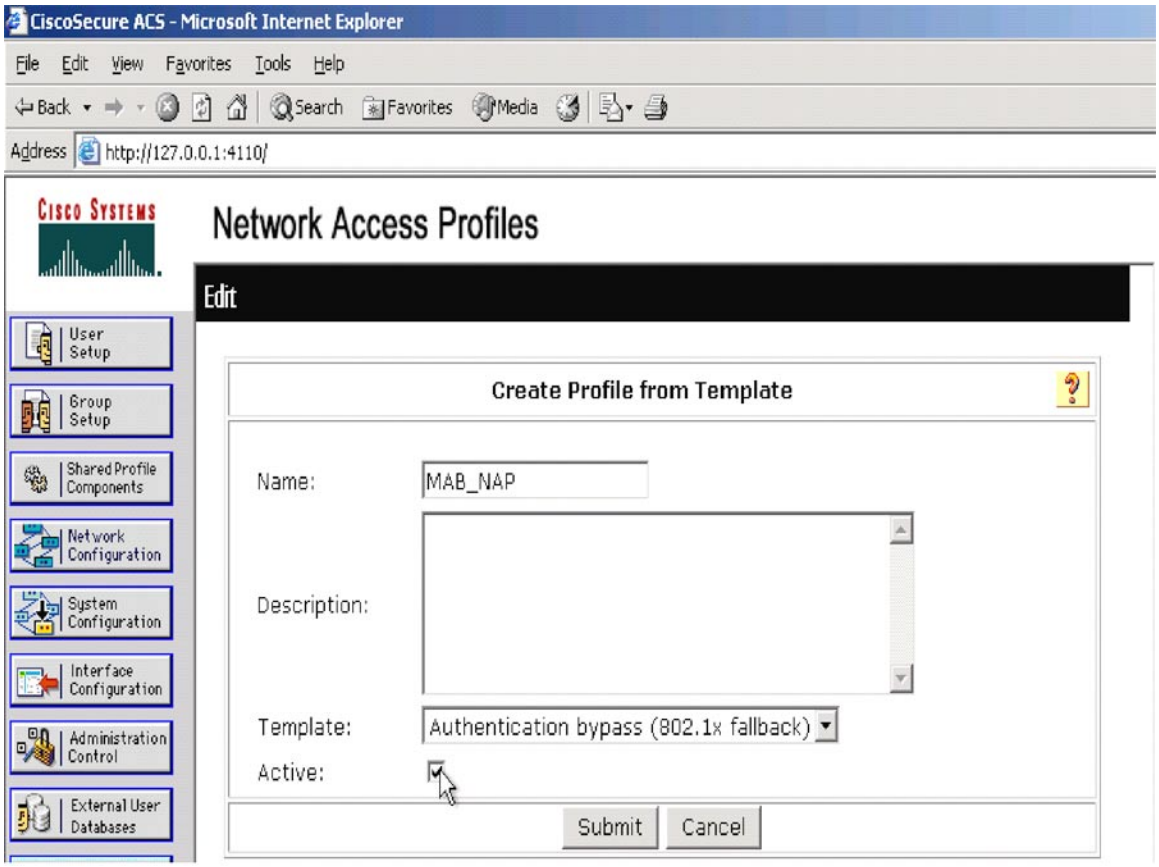
Catalyst 6500 では、いくつかのコマンドを使って MAC Authentication Bypass を設定します。ここでは、Catalyst 6500 の 802.1x 認証に必要な RADIUS 設定が実施済みであることを前提としています。この機能は、次に示すようにグローバルにイネーブルにした後に、ポートに対して適用する必要があります。

```
6506-CatOS   > (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.

6506-CatOS   > (enable) set port mac-auth-bypass 2/3 enable
Mac-Auth-Bypass successfully enabled on 2/3.
```

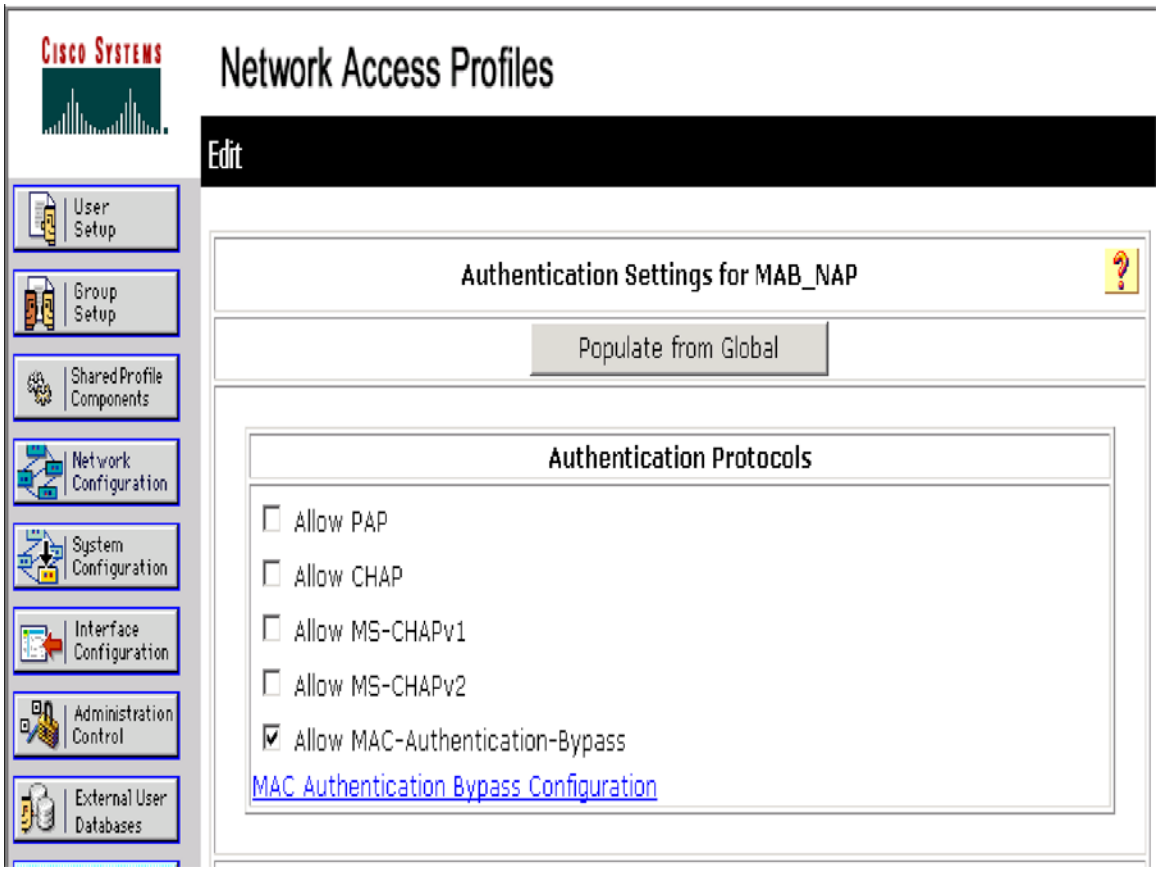
タスク 2：Cisco Secure ACS への MAC Authentication Bypass の設定

MAC Authentication Bypass （MAB） を行うために、Cisco Secure ACS にはホストの正確な MAC アドレスまたは MAC アドレスのワイルドカード マッチと一致する設定が必要です。ワイルドカード マッチは、VMware イメージの MAC アドレスの OUI 部の認証に使用されます。

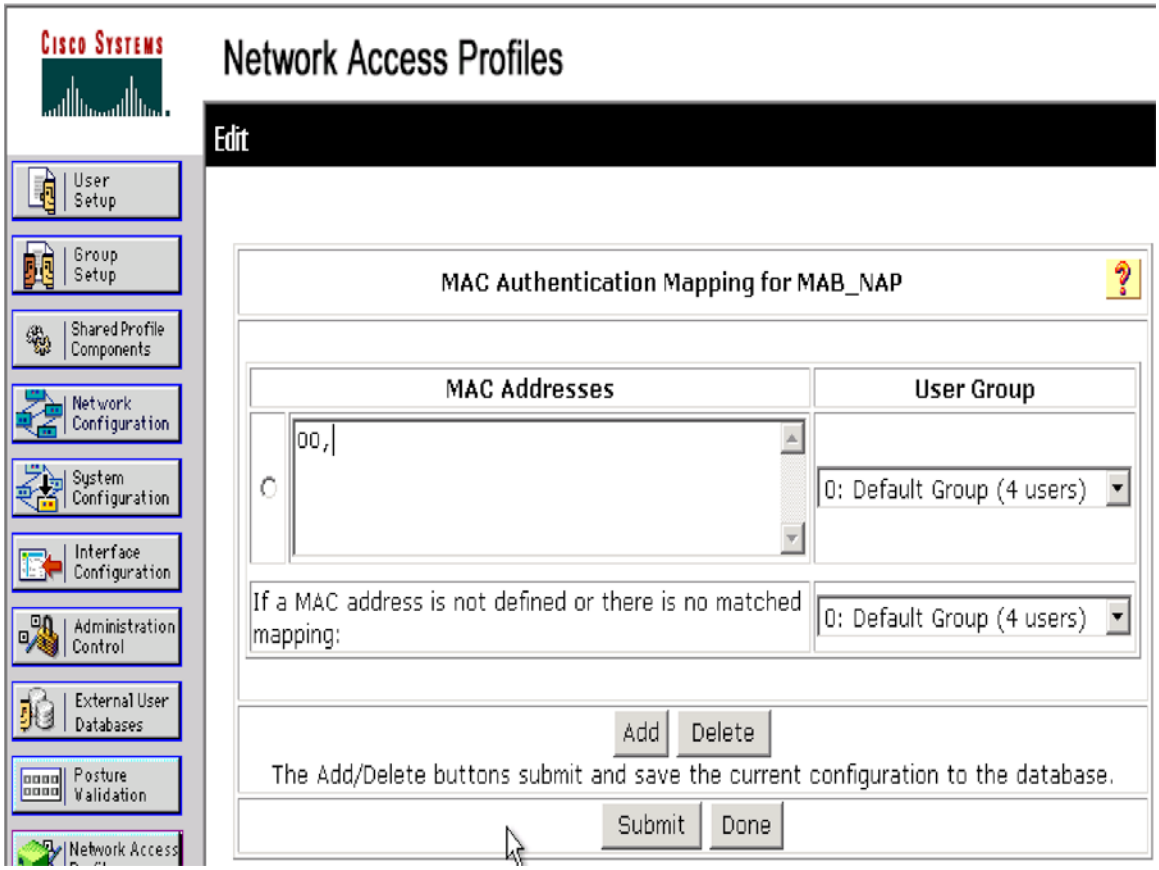
手順 1. Catalyst 6500 からの MAB 要求を処理するネットワーク アクセス プロファイルを作成します。NAP > Add Template Profile > Authentication Bypass (802.1x fallback) を選択し、次の NAP を作成します。



手順 2. Network Access Profile > MAB_NAP > Authentication Settings を選択し、MAC Authentication Bypass をイネーブルにします。



手順 3. Network Access Profile > MAB_NAP > MAC_Authentication_Bypass_Configuration の下の Add ボタンを選択し、MAC List を作成します。



手順 4. MAC Address テキスト ボックスにクライアントのインターフェイス MAC アドレスの先頭の文字列を入力します。ここに *00,* と入力した場合、このカンマ（,）は、ACS に対して、入力された文字列まで一致する MAC アドレス マッチをワイルドカード検索するように指示します。たとえば、*00-95,* と入力した場合、*5* まで一致する MAC アドレス マッチがワイルドカード検索されます。MAC アドレスをユーザ グループにマッピングすることもできます（この例では Default Group）。

タスク 3：モニタリング

この設定を適用した後、次に示すように show コマンドで この機能をモニタリングします。

手順 1. このポートの MAC 認証が実行されます。

```
6506-CatOS   > (enable) sho port mac-auth-bypass 2/3
Port  Mac-Auth-Bypass State MAC Address      Auth-State       Vlan
----- -------------------- ----------------- -----------------  -----
 2/3  Enabled             00-00-00-00-00-00 waiting          10

Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 2/3  reauthenticate    3600          NO      -
```

手順 2. ポートの認証が成功します。

```
6506-CatOS   > (enable) sho port mac-auth-bypass 2/3
Port  Mac-Auth-Bypass State MAC Address      Auth-State       Vlan
----- -------------------- ----------------- -----------------  -----
 2/3  Enabled             00-0a-95-dc-32-4a authenticated     50

Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 2/3  reauthenticate    1000          NO      -
```

手順 3. **show vlan** コマンドの出力を確認して、VLAN 割り当てを検証します。VLAN 50 は、グループの IETF RADIUS アトリビュートが示すように、*healthy* にマッチします。

```
6506-CatOS   > (enable) sho vlan 50
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
50   healthy                          active    68     2/3,2/47
                                                       15/1
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
50   enet  100050     1500  -      -      -      -    -        0      0
VLAN MISTP-Inst DynCreated  RSPAN
---- ---------- ---------- --------
50   -          static     disabled
```

手順 4. 「Reports and Activity/Passed Authentications」の下に、MAC 認証の成功を示す次の ACS ログ メッセージと一致するメッセージが表示されます。

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port
07/14/2005	21:43:10	Authen OK	00-0a-95-dc-32-4a	..	00-0a-95-dc-32-4a	201

MICROSOFT ACTIVE DIRECTORY の統合

Cisco Secure ACS は、認証の決定を Windows、LDAP、ODBC データベース、RADIUS トークン サーバ、RSA SecurID トークン サーバ などの外部サーバに委任できます。認証サーバのリストには、優先順位を付けることができます。Cisco Secure ACS はマッチが見つかるまでリストの順に各サーバで認証を試みますが、すべてのサーバを試みてもマッチが見つからなければ認証は失敗します。Cisco Secure ACS が外部のサーバを使用して認証を実行するように設定するには、**External User Databases** の下で各タイプのサーバを設定する必要があります。

注: ACS サーバを AD ドメインに追加します。

Microsoft Active Directory

注: Microsoft Active Directory で認証を実行するには、ACS サーバをドメインのメンバーにする必要があります。

Cisco Secure ACS の外部ユーザ データベースの設定は、3 つのセクションに分かれています。

1. Unknown User Policy
2. Database Group Mappings
3. Database Configuration

まず、外部データベースの使用をイネーブルにし、データベースのタイプを指定する必要があります。ACS **External User Database > Unknown User Policy** を選択し、次の図に示すように Windows Database を選択します。

Unknown User Policy

Fail the attempt

Check the following external user databases

Selected Databases:

Windows Database (Windows Database)

注: 認証に使用する複数のデータベースを指定する場合、Cisco Secure ACS は、信頼できる応答を受信するまで、指定された順番で各ディレクトリ サーバに問合せます。応答時間とユーザ体験を向上させるためには、信頼できる応答を返す確立が高いディレクトリ サーバをリストの上位に配置する必要があります。

Microsoft Active Directory によって認証されたユーザの許可方法を Cisco Secure ACS に通知するために、次のように Active Directory グループを ACS の各ネットワーク グループにマッピングする必要があります。このマッピングを行うには、**External User Database > Database Group Mappings > Windows Database > *Domain*** を選択します。リファレンス ネットワークのドメイン名は **NAC** です。

Database Group Mappings

Windows Database

Domain Configurations: NAC

NT groups “Users, *” matches Cisco Secure group “Employees”

NT groups “Contractors, *” matches Cisco Secure group “*Contractors*“

NT groups “Guests, *” matches Cisco Secure group “*Guests*“

外部データベース設定の最後の手順は、ACS が受信した要求を認証するために使用するデータベースの順番の指定です。**External User Database > Database Configuration > Windows Database > Configure** を選択し、ユーザおよびマシン認証のために nac.cisco.com Active Directory ドメインを使用するように設定します。

Dialin Permission

Verify that *Grant dialin permission to user* setting has been enabled from within the Windows User Manager for users configured for Windows User Database authentication.

Unknown User Policy

Use the next sequential External Database in the Selected Databases list in case of an “External DB user invalid or bad password” error.

Configure Domain List

Domain List:

NAC

\LOCAL

MS-CHAP Settings

Enable password changes using MS-CHAP version 1.

Enable password changes using MS-CHAP version 2.

Windows EAP Settings

Enable password change inside PEAP or EAP-FAST.

EAP-TLS Strip Domain Name.

Machine Authentication

Enable PEAP machine authentication.

Enable EAP-TLS machine authentication.

EAP-TLS and PEAP machine authentication name prefix: host/

Enable machine access restrictions.

Aging time (hours): 12

Group map for successful user authentication without machine authentication: <No Access>

ユーザおよびマシン認証の設定

ここでは、次のようなホスト認証を実施するための Cisco Secure ACS およびスイッチの設定方法を説明します。

- ユーザ認証
- マシン認証
- ユーザおよびマシン認証

ユーザおよびマシン認証の概要

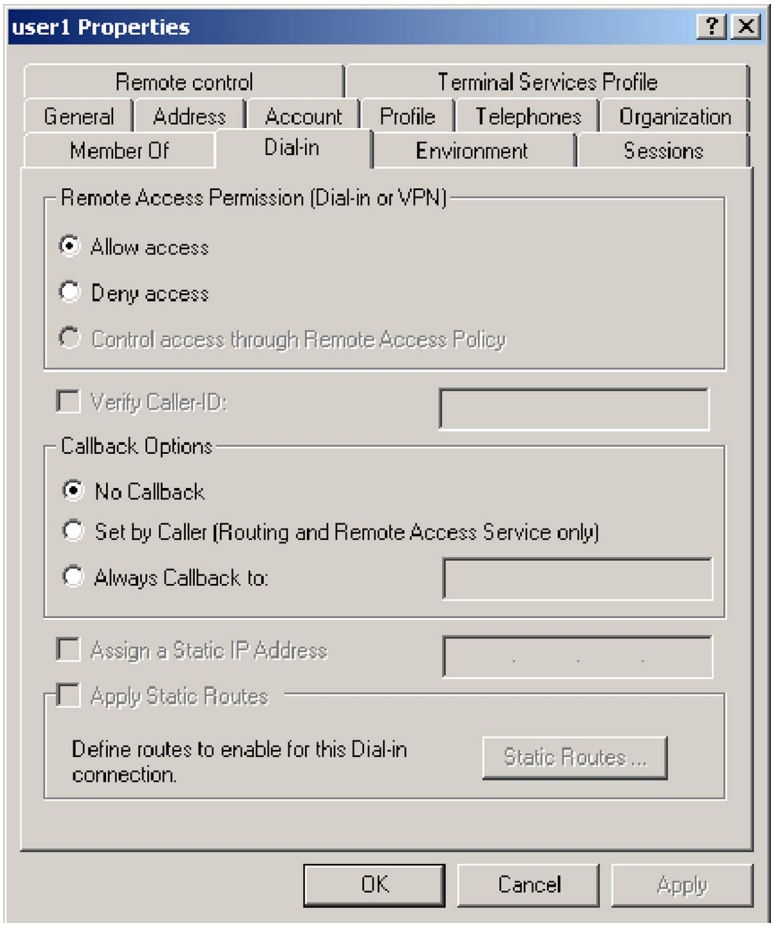
NAC-L2-802.1x のマシン ポスチャ ステートの考え方では、マシンおよびユーザ認証中に複数の 802.1x 認証が発生する可能性があります。802.1x トランザクションで最も一般的なマシンおよびユーザ認証のシナリオは次のとおりです。

- マシンが起動する。
- サプリカントがポスチャとともにマシン認証を実行する（最初の 802.1x 交換）。
- マシン上のすべてのサービスが完了し、マシンのステートが起動から稼動に変更されたため、CTA がポスチャ ステータスの変更を開始する。
- サプリカントがポスチャとともにマシン認証を実行する（2 回目の 802.1x 交換）。
- ユーザがログインする。
- サプリカントがポスチャとともにユーザ認証を実行する（3 回目の 802.1x 交換）。
- ログインが完了し、マシンのステートが稼動からログインに変更されたため、CTA がポスチャ ステータスの変更を開始する。
- サプリカントがポスチャとともにユーザ認証を実行する（4 回目の 802.1x 交換）。

タスク 1：Cisco Secure ACS と AD との通信の設定

手順 1. NAP > Lab_NAC_L2_802.1X > Authentication > Credential Validation Databases > Selected Databases を選択し、チェックされているデータベースのリストに Windows Database を追加します。

手順 2. ここでは、Cisco Secure ACS が Microsoft Active Directory とユーザおよびマシン認証情報を正しく交換できるように、ユーザ認証を行う場合にはユーザ プロパティの Dial-In の設定で、マシン認証を行う場合にはマシンのプロパティの Dial-In の設定で *Allow Access* をイネーブルにします。*Active Directory Users and Computers Management Tool* でこの設定をイネーブルにする図を示します。



AD の統合をテストするために次の手順を実行します。

手順 3. クライアント デスクトップ上の Cisco Trust Agent サプリカント GUI の **Menu** ボタンで **Clear Credentials** をクリックします。

手順 4. ユーザ名 NAC\User1 とパスワード cisco123 を使用してログインし、Active Directory を使用したユーザ認証をテストします。

NAC のトラブルシューティング

NAC は複雑なソリューションですが、このソリューションの各コンポーネントからはさまざまな情報が入手できます。これらのコンポーネントは、問題の特定に役立つコマンド、レポート、ロギング出力を提供します。ここでは、アドミッション コントロール プロセスの対象となるクライアント（ホスト）から、AAA およびポリシー サーバまで、各コンポーネントが提供する情報について説明します。

Cisco Trust Agent と CTA サプリカントのロギング

CTA は、通常のセットアップ ルーチンでエージェントとともにインストールされるロギング デーモンを提供します。インストール プロセスが完了した後、このロギング機能はデフォルトでディセーブルにされます。CTA ロギング機能は、さまざまな方法でイネーブルにできます。CTA のインストール完了後にロギングをイネーブルにする場合には、ctasetup 実行ファイルと同じディレクトリに正しく設定された *ctalogd.ini* ファイルを配置しておきます。デフォルトでは、インストール時に ctalogd.tmp という名前のファイルが適切なフォルダにコピーされるように設定されています。このファイルを .ini タイプのファイルに名前を変更すると、ロギング サービスが Windows で再起動し、ロギングがイネーブルにされます。ロギング サービスは、コマンドラインからも起動できます。

サンプルの ctalogd.ini ファイルとその説明を示します。

```
;
;このファイルには、Cisco Trust Agent のロギング設定が含まれています。
;これらの設定を使用するには、ファイル名を "ctalogd.ini" に変更します。
;

;
; 0 = ロギングのディセーブル
; 1 = ロギングのイネーブル
;

 [main]
EnableLog=1

;
; このセクションでは、Cisco Trust エージェントの
; 各種コンポーネントのロギングの詳細レベルを設定できます。
;
; 0 = ディセーブル
; 1 = 重大なイベントのみロギング
; 2 = 重大および警告イベントのみロギング
; 3 = 重大、警告、およびインフォメーショナル イベントをロギング
```

```
;

 [LogLevel]
PADaemon=3
NetTrans=3
PAPlugin=3
CTAMsg=3
CTAD=3
PEAP=3
EAPTLV=3
EAPSQ=3
PPMgr=3
PSDaemon=3
HostPP=3
CTASI=3
ScriptPlugin=3
CTASC=3
CTAVSTLV=3
CTASTATE=3
```

ctalogd.ini の各エントリは、CTA の一部をなす特定のデーモンを参照します。インストールに含まれるこのサンプル ファイルは、.ini ファイル タイプのファイルに名前が変更された場合、各デーモンのロギング レベルを High に設定します。通常はこれでトラブルシューティングを行うために十分な情報が得られます。各デーモンのロギング レベルを 15 に設定すると、完全なパケット ダンプがイネーブルにされます。CTA ロギングは、次のシンタックスを使用してコマンド プロンプトからもイネーブルにできます。

```
ctalogd { start| stop | restart | enable [-t] | disable | clear }
```

ctalogd がログファイルを書き込む場所も変更できます。詳細情報については、『Cisco Trust Agent アドミニストレータ ガイド』（http://www.cisco.com/jp/service/manual_j/index_sec_ta.shtml）を参照してください。

この例は、ロギングレベルを High に設定して各デーモンが記録した、成功した EoU セッションの一部です。理解しやすいように、メッセージの大半は省略しています。タブで区切られたフィールドは、シーケンス番号、時間、日付、重要度、デーモン ID、メッセージを示しています。

```
103    13:49:32.095    07/08/2005    Sev=Info/4    NetTrans/0x6310000E
EAPoUDP Session 4 created for NAD 172.31.211.1, total session count: 2

109    13:49:32.305    07/08/2005    Sev=Info/5    PEAP/0x6340000D
Server certificate (/O=Cisco Systems, Inc./CN=Server) has been validated by local CA
certificate    (/O=Cisco Systems, Inc./CN=Stress).
```

```
110   13:49:32.335  07/08/2005   Sev=Info/5   PEAP/0x6340000F
Server certificate matches following DN checking rule: CN*"Server", ISSUER-CN="Stress"

  111   13:49:32.365   07/08/2005   Sev=Info/4   PEAP/0x63400003
  PEAP handshake success

  112   13:49:32.405   07/08/2005   Sev=Info/6   EAPTLV/0x63500002
  EAP Identity:  PCTOO:NAC User

  120   13:49:32.836   07/08/2005   Sev=Info/4   PEAP/0x63400008
  PEAP received a message of: EAP Success

  121   13:49:32.866   07/08/2005   Sev=Info/5   EAPTLV/0x63500004
  Done with EAP-TLV processing

  125   13:49:33.036   07/08/2005   Sev=Info/5   PEAP/0x6340000C
  PEAP processing finished

  126   13:49:33.046   07/08/2005   Sev=Info/4   PAPlugin/0x63200001
  Application Posture Result = Healthy

  127   13:49:33.086   07/08/2005   Sev=Info/4   PAPlugin/0x63200002
  System Posture Result = Healthy

  129   13:49:33.177   07/08/2005   Sev=Warning/2 PAPlugin/0xA3200010
  CTAPP receives UserMsg Notification: Content = healthyL2IP
```

この例は、EoU セッションが作成され、CTA が ACS からサーバ証明書を受信し、この証明書が信頼できるものと検証され、証明書フィルタ ルールにマッチしたことを示しています。また、メッセージの PEAP ハンドシェークが成功した後に、クライアントのポスチャを検証する登録済みの証明書が ACS に送信され、結果が CTA に返されたことが分かります。

CTA ロギング設定ファイルの設定は、次のコマンドを使用して DOS プロンプトから変更できます。

```
clogcli { enable | disable | clear | loglevel [1-3, 15] }
```

clogcli コマンドを使用して Command Line Interface（CLI; コマンド ライン インターフェイス）からもロギングを開始できます。詳細情報については、『Cisco Trust Agent アドミニストレータ ガイド』を参照してください。

クライアント上の CTA のステータスは、**ctastat** コマンドを使用して即座に取得できます。出力のサンプルを以下に示します。この出力は、CTA が起動後のポスチャ検証回数、現在のシステム ポスチャ トークン、最新のステータス クエリーの結果、登録されているすべてのポスチャ エージェントを示しています。

```
> ctastat.exe
CTA Statistics Reporting Tool
```

```
  Cisco Trust Agent Statistics
  Current Time: Mon Jul 18 08:10:59 2005

  Session Information
     Session Number (Hex): 01000000
        System Posture Token Value: Healthy
           Received on: Mon Jul 18 07:50:30 2005
           Total Postures Received: 1
        Last SQ Response was "No Status Change"
        Plugin Vendor/Application: 9/1
           Application Posture Token Value: Healthy
              Received: Mon Jul 18 07:50:30 2005
           Posture Request last received: Mon Jul 18 07:50:30 2005
              Length of last response to Posture Req: 28
              Sent: Mon Jul 18 07:50:30 2005
        Plugin Vendor/Application: 9/2
           Posture Request last received: Mon Jul 18 07:50:30 2005
              Length of last response to Posture Req: 167
              Sent: Mon Jul 18 07:50:30 2005
```

NAD のロギング、show コマンド、セッション コントロール、デバッグ

NAC のネットワーク アクセス デバイスとして機能する Cisco IOS デバイスおよび CatOS デバイスは、通常のコンソールを通じて情報を提供するとともに、syslog 機能と一部の RADIUS アカウンティング機能を提供します。提供される情報と方式は、NAC の実装方法（L2/L3-IP を使用するか L2-802.1x を使用するか）によって異なります。

次のコマンドは、EoU 関連のイベントのロギング レベルをインフォメーショナルのみに変更します。その結果、NAD コンソールおよび/または管理ステーションに詳細な大量のデータがレポートされます。CiscoWorks Security and Information Management System（SIM）または Cisco Secure Monitoring Analysis and Response System（CS-MARS）から完全な情報を得るには、これらのデータが必要となります。

```
eou logging

  *Jul 18 04:12:16.878 MDT: %EOU-6-SESSION: IP=172.31.211.2|
HOST=DETECTED|   Interface=GigabitEthernet1/9
  *Jul 18 04:12:16.882 MDT: %EOU-6-CTA: IP=172.31.211.2| CiscoTrustAgent=DETECTED
  *Jul 18 04:12:22.446 MDT: %EOU-6-POLICY: IP=172.31.211.2| ACLNAME=#ACSACL#-IP-healthy-42c46e7c
  *Jul 18 04:12:22.446 MDT: %EOU-6-POLICY: IP=172.31.211.2| TOKEN=Healthy
  *Jul 18 04:12:22.446 MDT: %EOU-6-POLICY: IP=172.31.211.2| HOSTNAME=PCTOO:Jane Dough
```

```
  *Jul 18 04:12:22.446 MDT: %EOU-6-POSTURE: IP=172.31.211.2|
HOST=AUTHORIZED|   Interface=GigabitEthernet1/9
  *Jul 18 04:12:22.450 MDT: %EOU-6-AUTHTYPE: IP=172.31.211.2| AuthType=EAP
```

このコマンドは、NAD が ACS にレポートするときに、ステーション ID を MAC アドレスから IP アドレスに変更します。MAC アドレスはホップごとに変更されるので、クライアントが NAD からシングル ホップ以上離れている場合に便利です。

```
  eou allow ip station-id
```

L2-802.1x NAC 実装では、L2/L3-IP 設定のようなロギング機能が利用できません。その代わりに NAD に組み込まれている 802.1x アカウンティング機能を使用します。次のコマンドを実行して 802.1x アカウンティングをイネーブルにします。

```
  aaa accounting dot1x default group radius
```

NAD show コマンド

さまざまな show コマンドが NAC セッションのステートをレポートします。**show eou all** コマンドは、認証タイプ、クライアントに割り当てられている現在のポスチャ トークン、NAC セッションの存続時間などの情報を含む、NAD 上の現在の NAC セッションに関する簡易なテーブルを表示します。

```
  show eou { all | posture token | authentication }


  ---------------------------------------------------------------------------
  Address        Interface            AuthType   Posture-Token Age(min)
  ---------------------------------------------------------------------------
  172.31.211.2    GigabitEthernet1/9    EAP       Healthy        15
```

特定の NAC クライアントおよびそのセッションに関する詳細情報は、**show eou ip** または **show eou mac** コマンドを実行することによって確認できます。これらのコマンドを実行すると、上記の show eou コマンドの情報に加え、時間の値、（設定されている場合）URL ダウンロードに関する情報、適用されている Downloadable ACL インスタンスが表示されます。

```
  show eou { ip x.x.x.x | mac h.h.h.h }


  Address           : 172.31.211.2
  MAC Address        : 0004.5aa8.2bde
  Interface         : GigabitEthernet1/9
  AuthType          : EAP
  Audit Session ID   : 00000031007C75E400000002AC1FD302
  PostureToken       : Healthy
  Age(min)          : 15
  URL Redirect       : NO URL REDIRECT
  URL Redirect ACL   : NO URL REDIRECT ACL
  ACL Name          : #ACSACL#-IP-healthy-42c46e7c
  User Name         : PCTOO:Jane Dough
```

```
  Revalidation Period : 3600 Seconds
  Status Query Period : 300 Seconds
  Current State       : AUTHENTICATED
```

ip device tracing コマンドは、IOS プラットフォーム スイッチが認識している IP エンド ステーションの存在を表示します。

```
  show ip device tracking { all | interface | ip | mac }


  IP Device Tracking = Enabled
  ------------------------------------------------------------
    IP Address    MAC Address      Interface        STATE
  ------------------------------------------------------------
  172.31.211.2    0004.5aa8.2bde GigabitEthernet1/9    ACTIVE
```

802.1x 環境で **show dot1x** コマンドを実行すると、ポートのステート、現在のポスチャ トークン、タイマー設定を示すインターフェイスごとの情報のテーブルが表示されます。

```
  show dot1x { all | interface | statistics interface }


  Supplicant MAC 000f.20ca.665c
    AuthSM State     = AUTHENTICATED
    BendSM State     = IDLE
    Posture          = Healthy
    ReAuthPeriod     = 3600 Seconds (From Authentication Server)
    ReAuthAction     = Reauthenticate
    TimeToNextReauth  = 3590 Seconds
  PortStatus          = AUTHORIZED
  MaxReq              = 2
  MaxAuthReq          = 2
  HostMode            = Single
  PortControl         = Auto
  QuietPeriod         = 60 Seconds
  Re-authentication    = Enabled
  ReAuthPeriod        = From Authentication Server
  ServerTimeout       = 30 Seconds
  SuppTimeout         = 30 Seconds
  TxPeriod            = 30 Seconds
  Guest-Vlan          = 216
```

```
AuthFail-Vlan        = 0
AuthFail-Max-Attempts = 3
```

IOS NAD clear コマンド

NAC EoU セッションは、次に説明するコマンドを使用して、セッションごと、インターフェイスごと、または NAD 全体で 1 度にリセットまたは再検証を行うことができます。

clear コマンドは、該当の NAC セッションを完全にリセットし、これらのセッションに関するすべての情報を削除します。IP エンド ステーションが再び NAC に参加するには、再度検出される必要があります。**clear** コマンドは、*all* オプションを使用すると NAD 全体に適用できます。また、EAP などの特定の認証タイプ、特定のインターフェイス、単一の IP または MAC アドレス、ポスチャ トークンに適用することもできます。

```
clear eou { all | authentication | interface | ip | mac | posturetoken }
```

initialize コマンドは、該当のセッションに関連するすべての NAC ステート情報をクリアします。これらのセッションの存在は削除されません。このコマンドを実行すると、NAD は該当のクライアントとの NAC 通信を開始します。

```
eou initialize revalidate { all | authentication | interface | ip | mac | posturetoken }
```

revalidate コマンドを実行すると、NAD はセッションをクリアせずに NAC クライアントの再検証を開始します。クライアントは、再検証中、**revalidate** コマンドが入力される前と同じネットワーク アクセスを維持します。

```
eou revalidate { all | authentication | interface | ip | mac | posturetoken }
```

802.1x が設定された NAC セッションは、次のコマンドを使用してリセットまたは再認証することができます。**initialize** コマンドを実行すると、インターフェイス上の 802.1x ステート マシンはリセットされ、クライアントとサプリカントの 802.1x 認証プロセスが開始されます。

```
dot1x initialize interface
```

re-auth コマンドを実行すると、インターフェイスを簡単に再認証できます。802.1x ステート マシンはリセットされません。クライアントが現在 VLAN に割り当てられている場合、再認証が完了するまでその割り当ては継続されます。

```
dot1x re-auth interface
```

NAD debag コマンド

IOS debug コマンドは、NAC セッションが失敗している正確な場所に関する情報を提供します。これらのコマンドは、各プロトコルの詳細なトレース、または特定のプロトコルから受信したパケットのみの情報を表示します。

```
debug eou { all | events | packets }


debug dot1x { all | errors | events | packets | state-machine }


debug radius { authentication | brief | e-log }
```

CatOS NAD show コマンド

```
show eou config

show eou ip-address x.x.x.x

show eou all

show dhcp-snooping bindings

show policy group <name>

show dot1x user [ <username> | all ]

show dot1x group <group name>
```

トラブルシューティングのフロー

NAC に関連する問題は、主に 3 つの異なるカテゴリーに分類することができます。

- **試行なし**—Cisco Secure ACS に対して認証が試行されない問題
- **試行失敗**—Cisco Secure ACS が RADIUS 認証の試行を受信したが、正常に処理できずに誤ったまたは予期しないポスチャ認証の結果が返される問題

トラブルシューティングとログおよびレポートの解析

NAC 実装のトラブルシューティングの最初の手順は、NAD のチェックです。NAD は、クライアントとネットワークの間に配置されているため、解決策のヒントを即座に提供します。L2-802.1x 実装で NAD がサプリカントを検出している場合や、L2-IP 実装で検出された CTA のメッセージを受信した場合は、ACS レポートで問題のタイプを確認することができます。

試行なしの問題

試行なしの問題の特徴は、Cisco Secure ACS の Failed Attempts レポートまたは Passed Authentications レポートにレポート エントリが存在しないことです。通常これらの問題は、NAC ソリューションに何らかの通信の問題があることを意味します。L2/L3-IP の場合は、NAC の対象となるクライアント上のファイアウォール、クライアントとネットワーク アクセス デバイス間に配置されているファイアウォール、または NAD 上のアクセス コントロール リストにブロックされている EAP-over-UDP ポートが原因である可能性があります。これらの NAC 実装は IP を介して通信するため、DHCP サーバへのクライアントのアクセスをブロックする ACL が原因の場合もあります。インターフェイス アクセス リストは、すべての NAC 方式を利用するクライアントに対して、次の推奨する最小限のアクセス レベル制限を行う必要があります。

```
permit udp any eq bootpc any eq bootps

permit udp any any eq 21862
```

NAC L2 802.1x 実装の場合は、スイッチポートの設定ミスやインストールが正常に完了しなかったサプリカントが原因の可能性があります。どちらの実装とも RADIUS と ACS の正常な通信に依存するので、NAD からの正しい RADIUS ソース アドレスが ACS に設定されているかどうかも関係します。IOS または CatOS の show コマンドを実行することにより、NAD が問題のインターフェイスまたはスイッチ ポート上でホストを検出したか、CTA または CTA サプリカントが NAD に正常に応答しているかどうかを把握することができます。

Windows Service Pack 2 がホストにインストールされている場合、CTA のための例外を設定せずに Windows ファイアウォールがイネーブルにされていると、試行なしの問題が発生します。この問題を解決するには、Windows の [コントロール パネル] で **[セキュリティ センター]** を選択し、このウィンドウ下部の **[Windows ファイアウォール]** をクリックします。**[例外]** タブを選択し、**[プログラムの追加]** を選択します。CTA 実行ファイルを選択して **[OK]** をクリックします。

試行失敗の問題

試行失敗は、ACS の Failed Attempts レポートのエントリに記録されます。通常これらの問題は、誤って設定されているポリシー、プロファイル、またはルールに認証要求がマッチすることによって発生します。また、クライアントのポスチャ エージェントから返されるクレデンシャルが不足していることも原因となります。

このレポートは、ACS サーバの IP アドレス、NAD の IP アドレス、クライアントの IP または MAC アドレス、クライアントのアイデンティティなどを示す多くのフィールドで構成されます。また、Authen-Failure-Code および Author-Failure-Code の問題のトラブルシューティングに必要な多くの情報を提供する 2 つのフィールドも含まれています。Reason アトリビュートは、役立つ情報を提供することもあるので、このアトリビュートもこのレポートに含む必要があります。次の表に、現在文書化されている Authen-Failure-Codes（AFC） のリスト、AFC 発生の理由、その問題を解決するために推奨するアクションを示します。

Authen-Failure-Code	原因	推奨するアクション
Authentication protocol is not allowed for this profile.	認証要求がネットワーク アクセス プロファイルとマッチしましたが、プロトコルがプロファイルで許可されていませんでした。	ネットワーク アクセス プロファイルの設定と NAP の認証設定を確認します。
EAP-FAST anonymous in-band provisioning is not permitted.		
Error communicating with the audit server or invalid response.	監査サーバとの通信に問題があります。	監査サーバが稼動していること、および正しくフォーマットされた応答を返していることを確認します。
Too many audit round trips.	ラウンドトリップが多すぎます。	監査サーバが正常に稼動していることを確認します。または監査サーバのタイムアウト時間を増やします。監査ポリシーで許可されているラウンドトリップを増やすこともできます。
MAC auth bypass is not allowed.	要求がプロファイルとマッチしましたが、MAC auth bypass が未許可でした。	
Access denied due to unmatched profile.	アクセス要求がイネーブルにされているプロファイル リストのプロファイルとマッチしませんでした。	
MAC auth bypass group is disabled.		MAC auth bypass グループをイネーブルにします。
Access rejected due to authorization policy.	マッチした許可ルールがアクセス拒否に設定されていたため、アクセスが拒否されました。	選択した Network Access Profile の許可セクションのグループ設定とマッチしないために発生した可能性があります。
Posture Validation failed due to unmatched profile.	どのアクセス プロファイルともマッチしませんでした。要求はポスチャ検証が設定されていないグローバル設定にフォールバックされました。	該当のプロファイルの Network Access Profile 設定を確認します。
User's credentials reside in an external DB that is not configured for this profile.	ACS ユーザ データベースにユーザ情報が存在しませんでした。	ACS にユーザを追加するか、NAF の認証セクションで外部データベースを設定します。
MAC auth bypass group is disabled.		

Authen-Failure-Code	原因	推奨するアクション
External User Not Found.	設定された外部データベースにユーザ名が存在しませんでした。	外部ユーザ データベースにユーザ情報を追加するか、このユーザに適切な外部データベースを設定します。
Posture Validation Failure (general).		
Users in this group are disabled.	ディセーブルにされたユーザ グループです。	グループ設定を変更します。
External DB not operational.	設定された外部ユーザ データベースに接続できません。	
External DB password invalid	-	-
Auth type not supported by External DB	-	-
External DB user unknown	設定された外部ユーザ データベースにユーザが存在しません。	外部ユーザ データベースにユーザを追加します。
External DB EAP authentication failed	-	-
External DB not configured	-	-
EAP type not configured	-	-
EAP-TLS or PEAP authentication failed during SSL handshake	-	-
EAP-FAST user was provisioned with new PAC	-	-
EAP-FAST user PAC is invalid	-	-
EAP-FAST in-band provisioning is not permitted	-	-
Posture Validation Failure (general)	-	-
External DB user access denied (Machine Access Restriction)	-	-
Posture Validation settings contain unknown attribute(s)	-	ポスチャ検証設定を確認し、未知のアトリビュートを削除します。
EAP-FAST anonymous in-band provisioning is not permitted	-	-
Error communicating with the audit server or invalid response		外部監査サーバの通信設定を確認します。
MAC auth bypass is not allowed	-	-
Posture Validation Failure on Internal Policy	-	-
Posture Validation Failure on External Policy	外部ポリシー サーバから応答を受信しませんでした。	-

認証通過の問題

認証通過（Passed Autheticationsの問題は、Cisco Secure ACS の Passed Authentications レポートのエントリに記録されます。これらの問題は、ポスチャ認証の結果が予期しないもの、または正しくないものであることです。これらは特別な問題ではなく、ACS の設定方法のエラー、またはクライアント上のポスチャ エージェントから送信されたアトリビュート内のデータの解釈ミスが原因の可能性があります。

正しく設定された Passed Authentications レポートには、Failure Codes 以外、Failed Attempts レポートと同様の情報が表示されます。さらに Passed Authentications レポートは、EAP タイプ、その認証の試みのために選択されたプロファイルのネットワーク アクセス プロファイル名、ネットワーク アクセス プロファイルのポスチャ検証のセクションで設定した NAC ポリシーにより返されたアプリケーション ポスチャ トークン、結果として得られたシステム ポスチャ トークン、その理由も提供します。Passed Authentications レポートの Reason フィールドには、選択されたポスチャ検証ルール、システム ポスチャ トークンを返されたポリシー、ポリシー内のマッチしたルールが表示されます。Passed Authentications レポートにアトリビュート情報が含まれている場合、選択されたポリシー内でマッチしたルールとこれらの値を照合し、特定のトークンが選択された理由を把握できます。アプリケーション ポスチャ トークン フィールドには、外部ポリシー検証サーバから得られた結果も表示されます。

Cisco Secure ACS のこのバージョンでは、各ポリシー、プロファイル、ルールの順序付けが非常に重要です。Cisco Secure ACS は、ベストマッチではなく、ファーストマッチ手法を使ってマッチングを実行します。このロジックを使用するため、ACS がポリシー、プロファイル、ルールをチェックする順番への考慮が必要です。通常は、最も複雑なポリシー、プロファイル、ルールを順序リストの最初に配置します。これにより、複雑な認証要求が単純なネットワーク アクセス プロファイルによってマッチングされ、誤って認証される事態を防止することができます。

付録

付録 1：参考ドキュメント

- ソリューションに関するドキュメント
  - Implementing NAC: Phase One Configuration and Deployment（英語）
  - ネットワーク アドミッション コントロール テクニカル FAQ
  - ネットワーク アドミッション コントロール導入ガイド
- NAC コンポーネントに関するドキュメント
  - Cisco Trust Agent (CTA) アドミニストレータ ガイド 2.0
  - Cisco Secure Access Control Server (ACS) ユーザ ガイド Windows 版 version 4.0
    - http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/sec/acs/acsugw/index.shtml
  - Cisco VPN 3000 コンセントレータ（英語）
    - NAC Administration and Configuration, v4.7.1
- プロトコルに関するドキュメント
  - EAP Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-FAST, Internet Draft, April 2005
  - RFC 2246: SSL
  - RFC 2616: HTTP
  - RFC 2617: HTTP digest authentication
  - RFC 2865: Remote Authentication Dial In User Service (RADIUS)
  - Internet Assigned Numbers Authority (IANA), Protocol Numbers and Assignment Services
  - RFC 2279: UTF-8, a transformation format of ISO 10646, January 1998.

付録 2：NAC アトリビュートのリファレンス

Attribute Namespace

すべての NAC アトリビュートは、ベンダおよびアプリケーション タイプに基づいたネームスペースで指定します。各ベンダおよびアプリケーションのタイプは、EAP 交換では番号で表されますが、通常は次のフォーマットで参照されます。

```
Vendor-ID: Application-Type: Attribute
```

Vendor ID は、グローバルに一意のベンダ識別子を含む 32 ビットのフィールドです。上位オクテットは 0、下位 3 オクテットは International Assigned Numbers Authority により定義されているベンダの SMI ネットワーク管理プライベート エンタプライズ コードがネットワーク バイト順に格納されます。シスコシステムズの Vendor ID は 9 です。

Application Type は、グローバルに一意のポスチャ アプリケーション タイプを表す 16 ビットのフィールドです。現在 Application Type は次のように定義されています。

ベンダ	Application Type	Application Type 名	説明
*	1	PA	ポスチャ エージェント
*	2	Host	ホスト情報
*	3	AV	アンチウイルス
*	4	FW	ファイアウォール
*	5	HIPS	ホスト侵入保護サービス
*	6	Audit	監査

32768 - 65535 — ローカルでの使用のために予約済み（グローバルに一意の必要がないカスタム プラグインまたはスクリプトを単一の組織内で記述するお客様が使用できます。）

アトリビュートのデータ型

データ型	演算子	説明
OctetArray	=、!=	可変長の任意のデータ。
Integer32	=、<、>、!=、>=、<=	ネットワーク バイト順の 32 ビットの符号付きの値。
Unsigned32	=、<、>、!=、>=、<=	ネットワーク バイト順の 32 ビットの符号なし値。
String	=、!=、>、<、>=、<=、contains、does not contain、start with、end with、regular-expression	OctetArray データ型から派生したデータ型。ISO/IEC IS 10646-1 文字セットを使用して UTF-8 変換フォーマット（UTF-8）で表される人間に解読可能な文字列。 **注 1：**7 ビット US-ASCII でエンコードされた情報は、UTF-8 文字セットも US-ASCII 文字セットも同一です。 **注 2：**UTF-8 は、1 つの文字/コード ポイントを表現するために複数バイトが必要となることがあるため、UTF8String のオクテット長はエンコードされた文字数とは異なることがあります。
IPv4Address	ワイルドカードとマスク	OctetArray データ型から派生したデータ型。IPv4Address には、最も重要なオクテットを先頭に 4 オクテットを含む必要があります。例："10.11.12.13" IPv4Address = 0A 0B 0C 0D
IPv6Address	ワイルドカードとマスク	OctetArray データ型から派生したデータ型。IPv6Address には、最も重要なオクテットを先頭に 16 オクテットを含む必要があります。 例：*0A0A:0B0B:0C0C:0D0D:0E0E:0F0F:1010:1111* IPv6Address = 0A 0A 0B 0B 0C 0C 0D 0D 0E 0E 0F 0F 10 10 11 11
Time	=、<、>、!=、>=、<=	Unsigned32 データ型から派生したデータ型。Coordinated Universal Time（UTC; 協定世界時） 1970 年 1 月 1 日からの秒数を表します。

データ型	演算子	説明
Version	=、<、>、!=、>=、<=	OctetArray データ型から派生したデータ型。8 オクテットは 4 つの 2 オクテット セットに分割されます。最も重要な 2 オクテットにはメジャー バージョン、次の 2 オクテットにはマイナー バージョン、最後の 2 つの 2 オクテットにはベンダが定義する 2 つのオクテット値を指定します。通常、3 つめのオクテットはレビジョン番号、最後のオクテットはビルド番号です。 例："3.5.1.350" の値：00 03 00 05 00 01 01 5E **注：**使用されないすべてのフィールドは 0 に設定する必要があります。

アトリビュートのリファレンス

Application-Posture-Token （APT） AVP は、Request-Response によって特定のベンダおよびアプリケーション タイプから送信されるポスチャ AVP の検証結果を表します。この AVP は Posture Notification 用の AVP で、NAC ソリューションの Client API Posture Notification 要求、EAP-TLV Posture-Notification 要求、および HCAP Posture Validation 応答の各インターフェイス間で送信できます。

System-Posture-Token（SPT） AVP は、Request-Response によって 1 つまたは複数のベンダおよびアプリケーション タイプから送信されるポスチャ AVP の総合的な検証結果を表します。この AVP は Posture Notification AVP で、NAC ソリューションの Client API Posture Notification 要求、EAP-TLV Posture-Notification 要求、および HCAP Posture Validation 応答の各インターフェイス間で送信できます。

ベンダ（番号）	アプリケーション タイプ（番号）	アトリビュート名	アトリビュート番号	型	値またはフォーマット
*（任意）	*（任意）	Application-Posture-Token	1	Unsigned32	0 = Healthy 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown
*（任意）	*（任意）	System-Posture-Token	2	Unsigned32	0 = HealthySystem 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown
Cisco（9）	PA	PA-Name	3	String	ポスチャ エージェント名。 シスコの場合は Cisco Trust Agent。
Cisco（9）	PA	PA-Version	4	Version	フォーマット = major.minor.revision.build
Cisco（9）	PA	OS-Type	5	String	ホストのオペレーティング システム名。 Windows Server 2003 Datacenter Edition Windows Server 2003 Enterprise Edition Windows Server 2003 Web Edition Windows Server 2003 Standard Edition Windows XP Home Edition Windows XP Professional

ベンダ（番号）	アプリケーション タイプ（番号）	アトリビュート名	アトリビュート番号	型	値またはフォーマット
					Windows 2000 Datacenter Server Windows 2000 Advanced Server Windows 2000 Server Windows NT Workstation 4.0 Windows NT Server 4.0 Enterprise Edition Windows NT Server 4.0 Windows NT 4.0 Windows NT 3.51 Windows 95 Windows 95 OSR2 Windows 98 Windows 98 SE Windows Me
Cisco（9）	PA	OS-Version	6	Version	ホストのオペレーティング システムのバージョン。 フォーマット：major.minor.revision.build
Cisco（9）	PA	User-Notification	7	String	値には 1 つ以上の文字を含みます。 例：*Your anti virus signature file is out-of-date. Please update your signature file from* http://www.in-companyxyz..remediation-server.com.
Cisco（9）	PA	OS-Kernel	8	String	例：Linux 2.4.20-8 i386
Cisco（9）	PA	Kernel Version	9	Version	ホストのオペレーティング システムのバージョン。 フォーマット：major.minor.revision.build
Cisco（9）	PA	Action	10		URL
Cisco（9）	OS	Machine-Posture-State	11		このアトリビュートは、マシンの稼動状況を示します。 1 － 起動中 2 － 稼動中 3 － ログイン中
Cisco（9）	OS	ServicePacks	6	String	例：ServicePack 4
Cisco（9）	OS	HotFixes	7	String	例：|KB12345|Q21345|
Cisco（9）	OS	HostFQDN	8	String	例：xp1.nac.cisco.com
Cisco（9）	OS	Package	100	Extended Query Protocol	-
*（任意）	AV	Software-Name	3	String	ソフトウェア製品名。
*（任意）	AV	Software-ID	4	Unsigned32	ソフトウェア製品の数値識別子。
*（任意）	AV	Version	5	Version	ソフトウェアのバージョン。
*（任意）	AV	Scan-Engine-Version	6	Version	AV スキャン エンジンのバージョン。

ベンダ（番号）	アプリケーション タイプ（番号）	アトリビュート名	アトリビュート番号	型	値またはフォーマット
*（任意）	AV	DAT-Version	7	Version	値には AV シグニチャ ファイルのバージョンを含みます。例：559.0.0.0, 4.5.2.0
*（任意）	AV	DAT-Date	8	Time	AV シグニチャ ファイルのリリース時刻。
*（任意）	AV	Protection-Enabled	9	Unsigned32	0 = ディセーブル 1 = イネーブル
*（任意）	AV	Action	10	String	フォーマットとコンテンツはベンダによって異なります。 サポートされている最長文字列は 255 文字です。
Cisco（9）	HIP	CSAVersion	5	Version	CSA のバージョン。
Cisco（9）	HIP	CSAOperationalState	9	Unsigned32	0 = ディセーブル 1 = イネーブル
Cisco（9）	HIP	TimeSinceLastSuccessfulPoll	11	Unsigned32	-
Cisco（9）	HIP	CSAMCName	32768	String	-
Cisco（9）	HIP	CSAStatus	32769	String	値は "|" によって区切られます。 global_testmode_on rootkit_detected ipforwarding_on
Cisco（9）	HIP	DaysSinceLastSuccessfulPoll	32770	Unsigned32	例：3

付録 3：NAC の RADIUS アトリビュート

次の表に、シスコのベンダ固有アトリビュート（VSA）を含む、NAC に関連するすべての RADIUS アトリビュートを示します。

NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP	番号	アトリビュート名	説明
✓			1	User-Name	アクセス要求の EAP アイデンティティ応答からコピーされる。
	✓	✓	8	Framed-IP-Address	ホストの IP アドレス。
	✓	✓	26	Vendor-Specific Cisco（9、1） CiscoSecure-Defined-ACL	ACL 名。 ACS により自動的に送信される。
✓			26	Vendor-Specific Cisco（9、1） sec:pg	ポリシーベースの ACL 割り当て。Catalyst 6000 のみに適用。 sec:pg = <group-name>
	✓	✓	26	Vendor-Specific、Cisco（9、1）、url-redirect	リダイレクション URL。 url-redirect=<URL>
	✓	✓	26	Vendor-Specific Cisco（9、1） url-redirect-acl	リダイレクト URL のために名前付きの ACL を適用。ACL は NAD のローカルへの定義が必要。IOS スイッチでのみ使用可能。 url-redirect-acl=<ACL-Name>
✓	✓	✓	26	Vendor-Specific	ポスチャ トークン/ステート名。

NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP	番号	アトリビュート名	説明
				Cisco（9、1） posture-token	ACS により自動的に送信される。
	✓	✓	26	Vendor-Specific Cisco（9、1） status-query-timeout	ステータス クエリー タイマーを設定。
	✓	✓	26	Vendor-Specific Cisco（9、1） host-session-id	監査に使用されるセッション識別子。 ACS により自動的に送信される。
?	✓	✓	26	Vendor-Specific Microsoft = 311	ステータス クエリーのキー：MS-MPPE-Recv-Key ACS により自動的に送信される。
✓	✓	✓	27	Session-Timeout	再検証タイマーを設定（秒）。
✓	✓	✓	29	Termination-Action	セッション タイムアウトのアクション。 （0）デフォルト：セッションの終了 （1）Radius 要求：再認証
✓			64	Tunnel-Type	13 = VLAN
✓			65	Tunnel-Medium-Type	6 = 802
✓	✓	✓	79	EAP Message	Access Request および Access Challenge の EAP 要求/応答パケット。 • Access Accept では EAP Success • Access Reject では EAP Failure
?	?	?	80	Message Authenticator	パケットの完全性を保証するための HMAC-MD5。
✓			81	Tunnel-Private-Group-ID	VLAN 名。

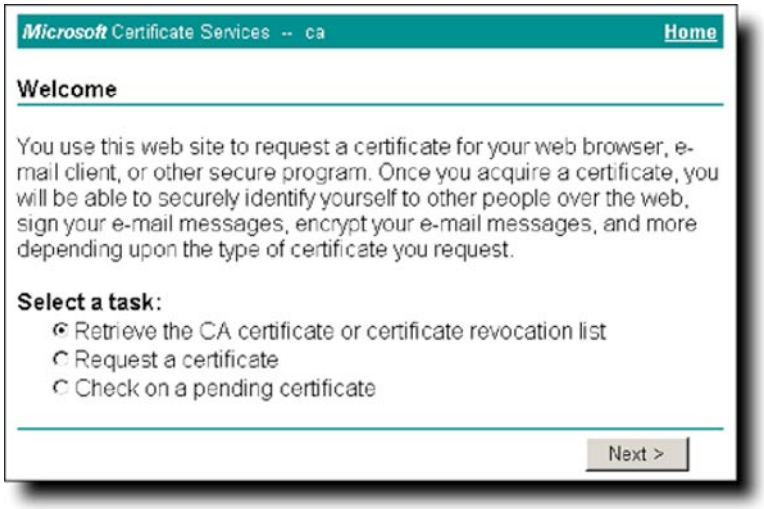
付録 4：Windows 2000 Server を使用した ACS デジタル証明書の登録

公開キー インフラストラクチャ（PKI）では、証明書のスケーラブルな展開のために認証局（CA）が必要です。Microsoft Windows 2000 Server と Windows 2003 Server は、この目的のためにオプションで認証局コンポーネントを提供します。ここでは、Microsoft Windows 2000 Server の認証局を使用して CA 証明書の取得およびデジタル証明書の要求を行う方法を説明します。

認証局のパブリック証明書の取得

手順 1. Web ブラウザ インスタンスを開き、URL http://ca.company.com/certsrv/ を入力してローカルの Microsoft Windows 2000 Server Certificate Authority に接続します。CA 証明書を取得するために、有効なユーザ名とパスワードの入力を求められる場合があります。

手順 2. 許可されたら、右の図のダイアログが表示されます。**Retrieve the CA certificate** を選択し、**Next** をクリックします。



手順 3. コンピュータへの直接の **Install this CA certification path** オプションと、ファイルとしてダウンロードするオプションがあります。CA 証明書を保存し、後ですべての ACS およびクライアントに配布できるように、**CA 証明書をダウンロードする**オプションを選択することを推奨します。

注: DER エンコードまたは Base64 エンコードを使用できます。両フォーマットともサポートされています。

手順 4. 証明書は、Windows オペレーティングシステムを実行している任意のホストコンピュータにインストールできます。証明書を右クリックし、**Install Certificate** を選択します。証明書は、**Trusted Root Certification Authorities** ストアに保存します。

Cisco Secure ACS のデジタル証明書の要求

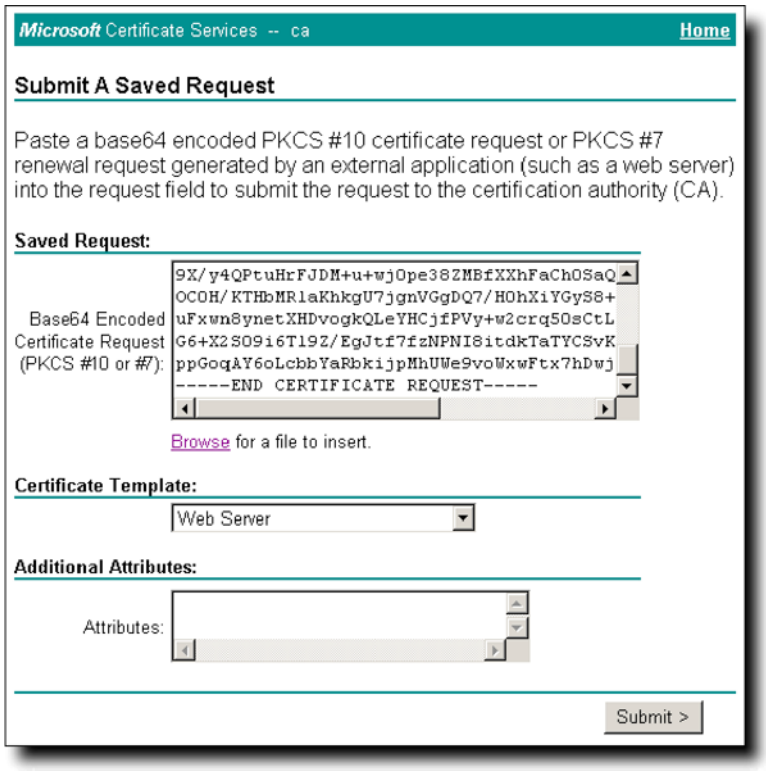
手順 5. Cisco Secure ACS の NAC の設定中に、**System Configuration > ACS Certificate Setup > Generate Certificate Signing Request** 画面で Certificate Signing Request（CSR; 証明書署名要求）を作成する必要があります。CSR は、認証局がプライベート キーでデジタル署名するエンコードされたテキスト ブロックです。

手順 6. 新しい Web ブラウザ インスタンスを開き、URL http://ca.company.com/certsrv/ を入力してローカルの Microsoft Windows 2000 Server Certificate Authority に接続します。新しい証明書を要求するために、有効なユーザ名とパスワードの入力を求められることがあります。

手順 7. **Request a certificate** を選択し **Next** をクリックします。

手順 8. ACS の証明書は Web サーバと同じなので、**Advanced Request** を選択し、**Next** をクリックします。

Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file オプションを選択し、**Next** をクリックします。



手順 9. ACS から CSR のすべての部分を**選択**し、**コピー（CTRL + C キー）**してフォームに**貼り付ける（CTRL + P キー）**か、**Browse** を選択して保存された CSR を検索し、アップロードします。

手順 10. Certificate Template として **Web Server** を選択し、CA による署名のためにオプションのアトリビュートを追加します。

手順 11. **Submit** をクリックして証明書要求を完了します。CA の設定方法に応じて、要求が自動的に許可されるか、または CA 管理者が要求を承認するまで待機します。

手順 12. 要求が自動的に許可される場合、**Download CA certificate** と DER または Base64 エンコードを選択して新しい ACS 証明書を取得できます。これが CA により署名され ACS のパブリック キーが含まれる ACS のデジタル証明書となります。

手順 13. 要求の承認が必要な場合、CA 管理者から承認されるまで待機します。承認されたら http://ca.company.com/certsrv/ を開いて CA に戻り、**Check on a pending certificate** を選択して証明書をダウンロードします。

付録 5：802.1x および NAC L2 IP の設定

802.1x と NAC L2 IP の概要

NAC には、既存の 802.1x サプリカントを使用してホストのアイデンティティ クレデンシャルを検証し、次に NAC L2 IP を使用してホストのポスチャ クレデンシャルを検証する実装オプションがあります。次のいずれかの理由がある場合に、この階層型のアプローチが必要となります。

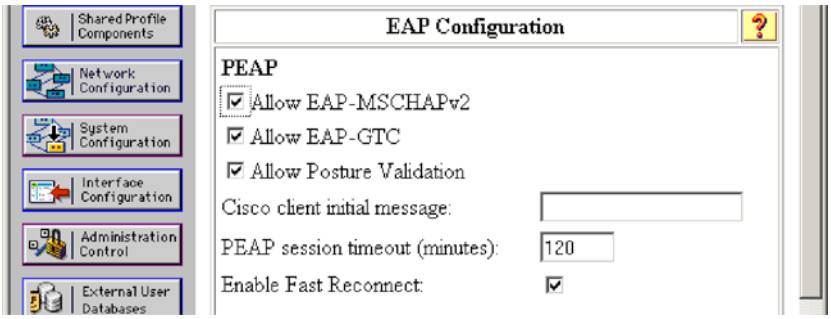
1. ホストに NAC 非対応の 802.1x サプリカントがインストール済みで、IBNS ソリューション上に NAC が実装されている。
2. ネットワーク管理者がアイデンティティおよびポスチャ クレデンシャルの検証を行うだけでなく、NAC L2 IP のみでサポートされている NAH 監査機能を利用する必要がある。

タスク 1：Cisco Secure ACS の設定

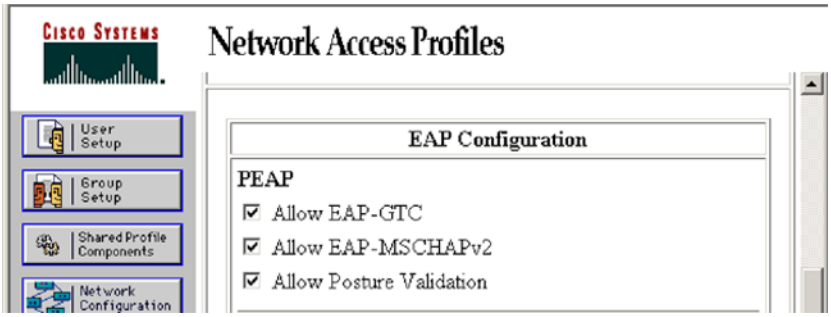
CiscoSecure ACS サーバが 802.1x サプリカントを使用してアイデンティティ クレデンシャルを認証し、CTA を使用してポスチャ クレデンシャルを認証できるようにするには、以下の手順を実行します。

前のセクションで行った ACS 設定をベースにするので、簡単な設定で Microsoft 802.1x サプリカントをサポートできます。

手順 1. System Configuration > Global Authentication Setup にナビゲートし、Network Access Profiles の Authentication 設定で EAP-MSCHAPv2 方式を使用できるように、EAP-MSCHAPv2 が選択されていることを確認します。これらの設定は、すべてのマシン認証に有効です。マシン認証の認証方式は、Microsoft 802.1x サプリカントのマシンおよびユーザ認証の方式と同一である必要があるため、ドメイン クレデンシャル（SID 定義）でマシン認証を実行するときはこの方式を選択する必要があります。Meetinghouse などのサードパーティ製の 802.1x サプリカントを使用する場合は、ネットワーク アクセス プロファイルで使用できるように EAP-GTC オプションを選択します。これらの設定を次の図に示します。

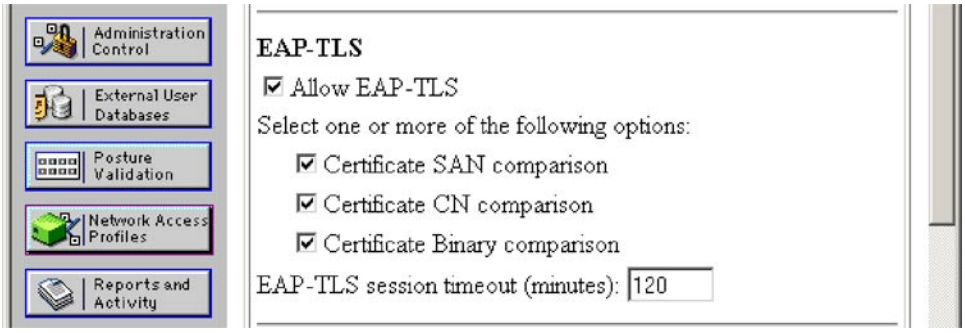


手順 2. Network Access Profiles にナビゲートし、NAC L2 IP ネットワーク アクセス プロファイルの Authentication リンクを選択します。NAC L2 IP の認証設定で、EAP Configuration の PEAP セクションまでスクロールし、EAP-MSCHAPv2 セクションが選択されていることを確認します。Microsoft 802.1x サプリカントに関連するのは EAP-MSCHAPv2 のみです。サードパーティ製のサプリカントを使用する場合は、EAP-GTC ボックスも選択します。



注: 認証に EAP-TLS を使用する場合は、System Configuration >Global Authentication Settings > EAP-TLS で正しい EAP-TLS 設定を選択する必要があります。EAP-TLS をイネーブルにし、適切な証明書比較オプションを選択し、EAP-TLS セッション タイムアウトを指定します。すでに説明したように、これらの設定はすべてのマシン認証に有効です。マシン認証の認証方式は、Microsoft 802.1x サプリカントのマシンおよびユーザ認証の方式と同一である必要があるため、証明書でマシン認証を実行するときはこの方式を選択する必要があります。グローバルの EAP-TLS 設定を次の図に示します。比較の際に最大限の柔軟性を提供するために、通常は利用可能なすべての証明書比較オプションを選択します。

Network Access Profiles にナビゲートし、NAC L2 IP ネットワーク アクセス プロファイルの Authentication リンクを選択します。NAC L2 IP の認証設定で、EAP-TLS セクションまでスクロールし、EAP-TLS が選択されていることを確認します。



注: マシンおよびユーザ認証に EAP-TLS を使用する場合は、マシンおよびユーザ認証設定のガイドラインを提供するドキュメント（http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a008009256b.shtml）を参照してください。

タスク 2：NAD インターフェイスへの 802.1x と NAC L2 IP の設定

802.1x と NAC L2 IP は、簡単な手順でスイッチに設定できます。

手順 1. 各オペレーティング システムのインターフェイスで 802.1x をイネーブルにし、IP アドミッション ポリシーを割り当てます。

IOS：

```
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
 ip access-group 101 in
 dot1x port-control auto
 spanning-tree portfast
```

```
ip admission NAC L2 IP
```

CatOS を搭載する Catalyst 6500 での 802.1x と NAC L2 IP の設定

```
set port dot1x 2/3 port-control auto
set port eou 2/3 auto
set spantree portfast 2/3 enable
```

ポート上に 802.1x と NAC L2 IP が設定されたことを確認できます。

付録 6：Policy-Based ACL（PBACL；ポリシーベース ACL）の設定

NAC 2 のダイナミックな許可ポリシーは、ダイナミックな VLAN 割り当てによって実行されます。修復サービスへのアクセスのみに制限する検疫の VLAN Access Control List（VACL；VLAN ACL）など他の追加の許可は、スイッチ上に予め設定しておく必要があります。この一般的なサポートモデルの例外の 1 つが Catalyst 6500 でサポートされているポリシーベース ACL の使用です。

ポリシーベース ACL は、インフラストラクチャ内のユーザ グループを表すポリシーベースの定義が ACE にダイナミックに作成される ACL です。これらのグループ定義は、6500 がポートの新しい IP アドレスを学習するときに 6500 TCAM の ACL 実装に拡張されます。6500 は、新しい IP アドレスを学習すると、このポートに適用するグループ ポリシーを検索し、ACE のグループ定義を新しい IP アドレスに置き換えて TCAM に ACE を作成します。これらのグループ定義は、静的な定義（CLI ポートベースの割り当て）、または RADIUS 割り当てを通じて作成されるダイナミックな定義となります。

NAC L2 802.1x では、通常、ACS によって割り当てられたポスチャ ポリシーをベースに、ポートがダイナミックにグループに割り当てられます。PBACL は NAC L2 802.1x のみの機能ではなく、アクセス コントロール ポリシーをダイナミックに実装する手段として NAC L2 IP でもサポートされています。

ここでは、NAC L2 802.1x ポスチャ アセスメントが発生した後に、ACS から返される Healthy または Quarantine ポスチャ トークンをベースに、PBACL の機能を使用して ACE を作成する方法を説明します。前のセクションで作成したトポロジと NAC ポリシーを使用します。

グループ 割り当ては、受信した sec:pg（シスコの VSA）によって決定されます。sec:pg 定義は、このドキュメントの前半の RADIUS 許可コンポーネント（RAC）のセクションで、NAC L2 IP の各ポスチャ トークンに対して作成しました。Catalyst 6500 の場合は、これらと同じ RAC を NAC L2 802.1x で使用できます。スイッチ インフラストラクチャ全体が Catalyst 6500 のみで構成されていない場合は、6500 から送信されて適切な sec:pg 値を返す RADIUS 要求をネットワーク アクセス フィルタによって区別できます。実際には、スイッチは理解していない RADIUS アトリビュートを無視してドロップするので、ネットワーク アクセス フィルタは必要ないと考えられます。

このことを念頭に置いて、すべての 802.1x 要求に対応する次の RAC を作成しました。Catalyst 6500 の PBACL を活用するために NAC L2 802.1x が使用できる RAC 設定の例を示します。

RAC 名	Assigned Attribute	値
L2_1x_Healthy_RAC		
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Healthy_hosts

RAC 名	Assigned Attribute	値
L2_1x_Checkup_RAC		
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Checkup_hosts
L2_1x_Transition_RAC		
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Transition_hosts
L2_1x_Quarantine_RAC		
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Quarantine_hosts
L2_1x_Infected_RAC	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Infected_hosts
L2_1x_Unknown_RAC	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Unknown_hosts

これらの RAC を使用する Catalyst 6500 の PBACL には、sec:pg の値と関連するグループ名の設定が必要です。このガイドでは、説明を簡略化するために、Catalyst 6500 の PBACL 設定で healthy_hosts および quarantine_hosts の値のみを使用します。

次に示す PBACL である nac_pbacl の設定は、healthy_hosts にネットワークへの無制限のアクセスを許可し、quarantine_hosts には 修復サーバが配置されているサブネット 10.0.200.0/24 へのアクセスのみを許可します。

注: これらの設定は、他のすべての NAC L2 802.1x 設定（RADIUS および 802.1x 設定）が設定済みで機能していることを前提としています。

これらの VLAN は、Catalyst 6503 上ですでに設定され名前が付けられています。次に CatOS で VLAN を作成し名前を付ける例を示します。

```
#assign vlan 50 and 80 to be the healthy and quarantine vlans
set vlan 50 name healthy type ethernet mtu 1500 said 100050 state active
set vlan 80 name quarantine type ethernet mtu 1500 said 100080 state active
```

以前に定義されたすべての ACE を削除します。

```
clear security acl all
```

次の PBACL を作成します。

```
#nac_pbacl
# allow the pbacl to inspect arp and dhcp for address information
set security acl ip nac_pbacl permit arp
set security acl ip nac_pbacl permit arp-inspection any any
set security acl ip nac_pbacl permit dhcp-snooping

# allow all vlans to access dns
set security acl ip nac_pbacl permit udp any any eq 53

# allow healthy hosts access to the network
set security acl ip nac_pbacl permit ip group healthy_hosts any

# allow quarantined hosts to access to the remediation servers and allow the
# remediation servers to communicate back to the quarantined hosts
set security acl ip nac_pbacl permit ip group quarantine_hosts 10.0.200.0 0.0.0.255
set security acl ip nac_pbacl permit ip 10.0.200.0 0.0.0.255 group quarantine_hosts

# allow quarantined hosts to communicate back and forth with the vlan's router
set security acl ip nac_pbacl permit ip group quarantine_hosts host 10.9.80.1
set security acl ip nac_pbacl permit ip host 10.9.80.1 group quarantine_hosts

# commit the security acl
commit security acl all

# map the pbacl to the healthy and quarantine vlans with statistics enabled
set security acl map nac_pbacl 50,80 statistics enable
```

この例では、NAC L2 802.1x の healthy ポスチャを受信したホストと、その後の Catalyst 6500 TCAM の内容を確認できる **show** コマンドを紹介します。また、NAC L2 802.1x の quarantine ポスチャを受信したホストと、その後の 6500 TCAM の内容を確認できるコマンドも紹介します。

まずこの例では、ユーザ名が cisco のポート 2/2 のユーザが認証され、healthy ポスチャを受信し、healthy_hosts のグループに割り当てられて VLAN 50 に割り当てられています。DHCP に割り当てられた 10.9.50.100 がスヌープされ、グループ テーブルに追加されています。

```
cat6500-nac (enable) show dot1x group all

Group Manager Info
-----------------------------------------------------------------
Info of Group healthy_hosts
User Count  = 1
-----------------------------------------------------------------
Username                      Mod/Port   UserIP          VLAN
--------                      --------   ------          ----
cisco                         2/2       10.9.50.100     50
-----------------------------------------------------------------
Info of Group quarantine_hosts
User Count  = 0
```

次の **show** コマンドでは、ポート 2/2 のスヌープされた IP アドレス 10.9.50.100 が PBACL に追加され、キーワード *"healthy_hosts"* が IP アドレスに正しく置き換えられて Catalyst 6500 TCAM に挿入されたことを確認できます。

```
cat6500-nac (enable) show security acl tcam interface 50

Input
IP
0. redirect arp (matches 4)
1. bridge udp any any fragment (matches 0)
2. redirect udp any any (matches 0)
3. bridge udp any any 53 (matches 17)
4. bridge ip host 10.9.50.100 any (matches 46)
               ^^^^^^^^^^^^ - snooped IP address substituted for
                  group “healthy_hosts”
5. deny ip any any (matches 26)

Output
IP
0. redirect (L3) arp (matches 0)
1. bridge udp any any fragment (matches 0)
2. redirect (L3) udp any any (matches 0)
3. bridge udp any any 53 (matches 0)
```

```
  4. bridge ip host 10.9.50.100 any (matches 0)
                ^^^^^^^^^^^^ - snooped IP address substituted for
                   group "healthy_hosts"
  5. deny ip any any (matches 0)
```

次の例では、ユーザ名が cisco の 2/2 のユーザが認証され、quarantine ポスチャを受信し、quarantine_hosts のグループに割り当てられて VLAN 80 に割り当てられています。DHCP に割り当てられた 10.9.80.100 がスヌープされ、グループ テーブルに追加されています。

```
  cat6500-nac (enable) show dot1x group all


  Group Manager Info
  ------------------------------------------------------------------
  Info of Group healthy_hosts
  User Count  = 0
  ------------------------------------------------------------------
  ------------------------------------------------------------------
  Info of Group quarantine_hosts
  User Count  = 1
  ------------------------------------------------------------------
  Username                      Mod/Port   UserIP          VLAN
  --------                      --------   ------          ----
  cisco                         2/1       10.9.80.100     80
```

次の **show** コマンドでは、ポート 2/2 のスヌープされた IP アドレス 10.9.80.100 が PBACL に追加され、キーワード "quarantine_hosts" が IP アドレスに正しく置き換えられて Catalyst 6500 TCAM に挿入されたことを確認できます。

```
  cat6500-nac (enable) sho security acl tcam interface 80

  Input
  IP
  0. redirect arp (matches 0)
  1. bridge udp any any fragment (matches 0)
  2. redirect udp any any (matches 0)
  3. bridge udp any any 53 (matches 0)
  4. bridge ip host 10.9.80.100 10.0.200.0 0.0.0.255 (matches 0)
                ^^^^^^^^^^^^ - snooped IP address substituted for
                   group "quarantine_hosts"
```

```
5. bridge ip 10.0.200.0 0.0.0.255 host 10.9.80.100 (matches 0)
6. bridge ip host 10.9.80.100 host 10.9.80.1 (matches 0)
7. bridge ip host 10.9.80.1 host 10.9.80.100 (matches 0)
8. deny ip any any (matches 4)

Output
IP
0. redirect (L3) arp (matches 0)
1. bridge udp any any fragment (matches 0)
2. redirect (L3) udp any any (matches 0)
3. bridge udp any any 53 (matches 0)
4. bridge ip host 10.9.80.100 10.0.200.0 0.0.0.255 (matches 0)
                  ^^^^^^^^^^^^ - snooped IP address substituted for
                  group "quarantine_hosts"
5. bridge ip 10.0.200.0 0.0.0.255 host 10.9.80.100 (matches 0)
6. bridge ip host 10.9.80.100 host 10.9.80.1 (matches 0)
7. bridge ip host 10.9.80.1 host 10.9.80.100 (matches 0)
8. deny ip any any (matches 0)
```

付録 7：Microsoft サプリカントの設定

ここでは、Microsoft 802.1x サプリカントの設定方法を簡潔に説明します。この機能に関するドキュメントは、オンラインで数多く公開されています。

http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc

http://www.microsoft.com/technet/community/columns/cableguy/cg1202.mspx

Windows XP または Windows 2000 クライアントの 802.1x 認証を設定するには、次の手順を実行します。

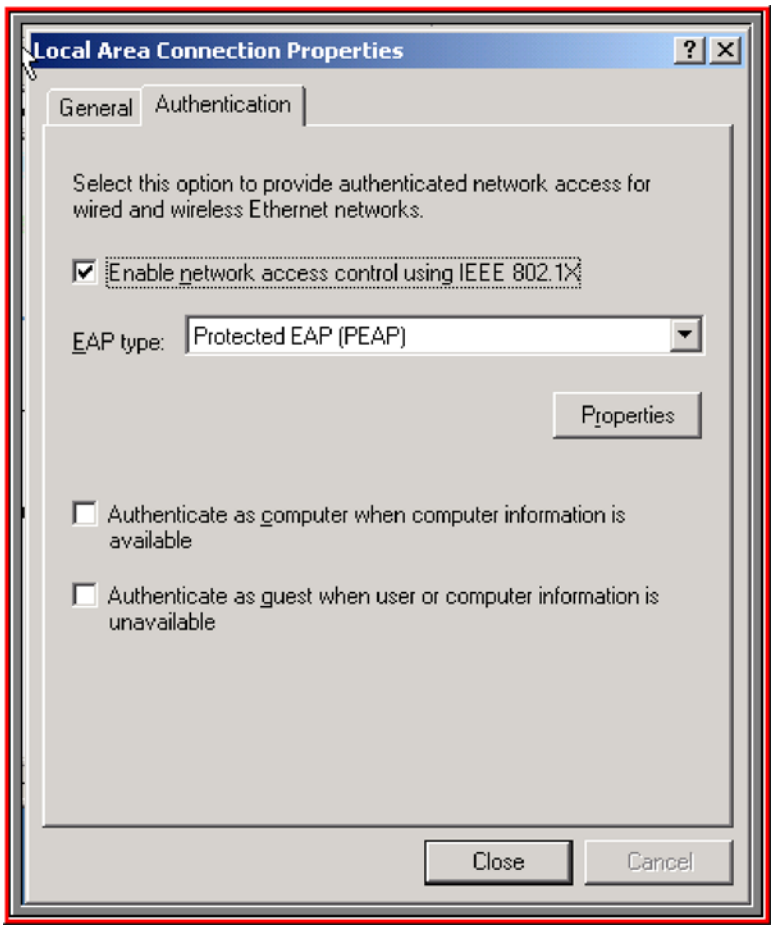
手順 1. エンドユーザのマシンで、**[ネットワーク接続]** を開きます（**[スタート] > [設定] > [ネットワーク接続]**）。

手順 2. 該当の接続を右クリックし、**[プロパティ]** を選択します。

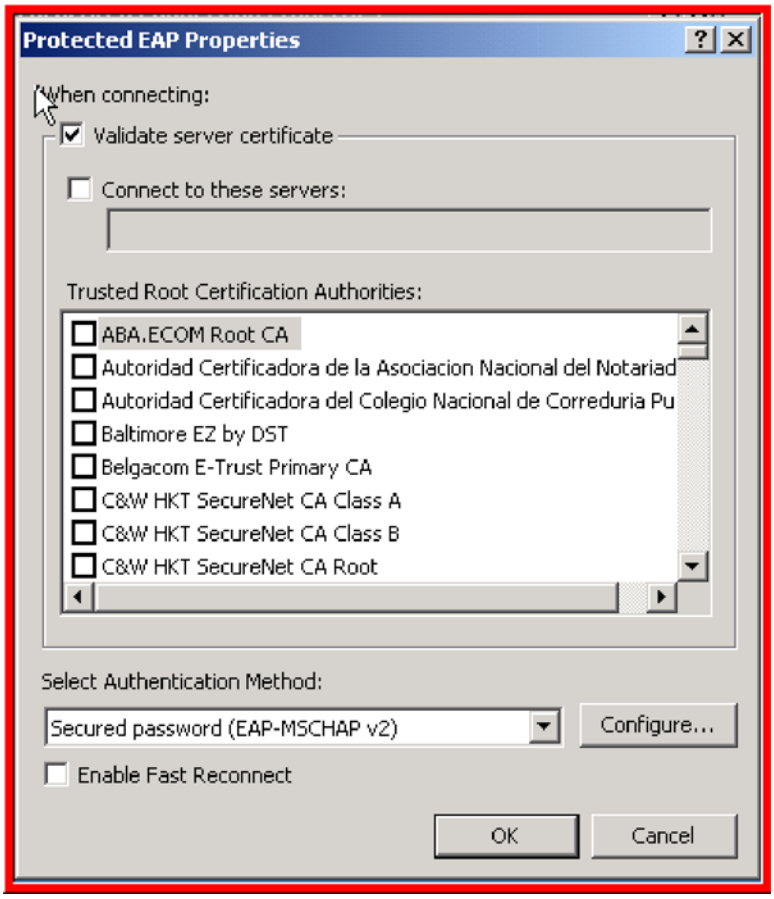
手順 3. [全般] タブで、[*接続時に通知領域にインジケータを表示する*] オプションが選択されていることを確認します。

手順 4. [認証] タブで、[*このネットワークで IEEE802.1x を有効にする*] チェック ボックスをチェックします。[EAP の種類] として **[保護された EAP（PEAP）]** を選択します。

手順 5. [EAP の種類] のドロップダウン ボックスの下の **[プロパティ]** を選択します。下のウィンドウを参照してください。



手順 6. [*サーバの証明書を有効化する*] ボックスがデフォルトで選択されています。この設定のままだと、サプリカントはサーバの証明書が失効していないこと、正しい署名を持つこと、信頼されたルート証明機関を持つことを確認します。このオプションを選択している場合、コンピュータが自動的に接続するサーバ、および信頼されたルート証明機関の指定が必要となります。ここでは設定を簡略化するために、[サーバの証明書を有効化する] ボックスのチェックを外します。下にこのウィンドウを示します。



手順 7. [セキュリティで保護されたパスワード (EAP-MSCHAP v2)] の隣の **[構成]** ボタンを選択すると、認証に Windows のログオン名とパスワード（ドメインがある場合はドメイン）を使用するかどうか指定することができます。このオプションを選択して [OK] をクリックします。つまり、ネットワーク アクセスの認証と Active Directory ドメインの認証を個別に行えます。

手順 8. ここでも設定を簡略化するために、標準の AD を使用します。下にデフォルトの設定を示すウィンドウを示します。

手順 9. ここまでの設定が完了すると、802.1x 認証を行うことができます。

ユーザ情報またはコンピュータ情報が使用できない場合でも、コンピュータがネットワークへの認証を試みるように指定するには、**[ユーザーまたはコンピュータ情報が利用できないときは、ゲストとして認証する]** ボックスを選択します。このチェックボックスは、デフォルトでチェックされています。Microsoft Active Directory の代替メカニズムとしてこのオプションを設定すると、AD ドメインが利用できない場合に、認証されたゲスト アカウントがコンピュータにログインできます。コンピュータは、ヌルのユーザ名とパスワードでネットワークへのログインを試みます。ACS 環境では、スイッチがサプリカントからこれらの EAPOL フレームに応答する方法を考慮して、この機能をディセーブルにすることを推奨します。この機能がデフォルトどおりにイネーブルにされていると、サプリカントにプラグインされているスイッチ ポートは、正しいユーザ クレデンシャルが適用されるまで認証ステートに置かれます。サプリカントでこの機能をディセーブルにすると、スイッチポートは予期どおりに接続ステートに置かれます。

ユーザがログオンしていない場合でも、コンピュータがネットワークへの認証を試みるように指定するには、**[コンピュータ情報が利用できるときは、コンピュータとして認証する]** チェックボックスを選択します。サプリカントでこの機能をイネーブルにしても、Cisco Secure ACS でイネーブルにしていないと、認証は失敗し、サプリカントの再起動時にポートは保留ステートに置かれるため、ログインにかかる時間が長くなってしまいます（サプリカントは、タイマーが失効してからユーザ クレデンシャルを使用して再認証を試行します）。

マシン認証はドメインへのログインより先に実行されるため、この機能を使用することによって企業の AD ドメインへのログイン時間を短縮できます。マシン認証は、サプリカントの起動時または再起動時に、ログイン画面が表示される前に発生します。その後ユーザがマシンにログインすると、ドメインにログインするためのクレデンシャルに即座にアクセスされ、ユーザのクレデンシャルに基づいて 802.1x の再認証が行われます。対照的に、この機能がディセーブルになっていると、（ACS でマシン認証が事前に設定されていない場合）クライアントは標準のユーザ認証を行います。この場合、ユーザのクレデンシャルが認証される前に、ドメインへのログインはタイムアウトになるため、ドメインへのログイン時間が長くなります。したがって、企業 AD ドメインへのログイン時間を短縮するマシン認証を実行することを推奨します。また、ゲストとしてネットワークに認証するオプションは使用しないことを推奨します（このオプションはデフォルトでイネーブルにされています）。

付録 8：略語と用語

略語	説明
ACE	Access Control Entry（アクセス コントロール エントリ）
ACK	Acknowledgement（受信応答）
ACL	Access Control List（アクセス コントロール リスト）
ACS	Access Control Server
AD	Active Directory（Microsoft）
AID	Authority Identity（機関 ID）
AP	Access Point（アクセス ポイント）
API	Application Programming Interface（アプリケーション プログラミング インターフェイス）
ARP	Address Resolution Protocol
AV	Anti Virus（アンチウイルス）
CAM	Clean Access Manager（CCA）
CAS	Clean Access Server（CCA）
CCA	Cisco Clean Access
CDP	Cisco Discovery Protocol
CHAP	Challenge Handshake Authentication Protocol
CSA	Cisco Security Agent
CTA	Cisco Trust Agent
CTASI	CTA Scripting Interface
DB	Database（データベース）
DC	Domain Controller（ドメイン コントローラ）（Microsoft）
DFS	Distributed File System（分散ファイル システム）
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name（認定者名）
DNS	Domain Name Service（ドメイン ネーム サービス）
DoS	Denial of Service（サービス拒絶）
DOT1X	IEEE 802.1x
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAPoRADIUS	EAP over RADIUS
EAPoUDP	EAP over UDP
EOU	EAP Over UDP
FAST	Flexible Authentication Secure Tunnel
GAME	Generic Authorization Message Exchange
GINA	Graphical Identification and Authentication（Microsoft）
GPO	Group Policy Object（グループ ポリシー オブジェクト）（Microsoft）
GTC	Generic Token Card

略語	説明
HA	High Availability（ハイ アベイラビリティ）
HAL	Hardware Abstraction Layer（ハードウェア抽象化レイヤ）
HCAP	Host Credential Authentication Protocol
HIPS	Host Intrusion Prevention System（ホスト侵入防止システム）
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secured
IAS	Internet Access Server（Microsoft）
IBNS	Identity Based Networking Services
IDS	Intrusion Detection System（侵入検知システム）
IID	Initiator Identity
IOS	Internetworking Operating System
IP	Internet Protocol（インターネット プロトコル）
L2	Layer 2（レイヤ 2）
L2TP	Layer 2 Tunneling Protocol（レイヤ 2 トンネリング プロトコル）
L3	Layer 3（レイヤ 3）
LAN	Local Area Network（ローカル エリア ネットワーク）
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control（メディア アクセス制御）
MITM	Man In The Middle（中間者）
MS	Microsoft（マイクロソフト）
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MVAP	Multi VLAN Access Ports
NAC	Network Admission Control（ネットワーク アドミッション コントロール）
NAD	Network Access Device（ネットワーク アクセス デバイス）
NAF	Network Access Filter（ネットワーク アクセス フィルタ）
NAH	NAC Agentless Host（NAC エージェントレス ホスト）
NAK	Negative Acknowledgement（否定応答）
NAR	Network Access Restriction（ネットワーク アクセス制限）
NAT	Network Address Translation（ネットワーク アドレス変換）
NDIS	
NDS	Netware Directory Services（Novell）
NRH	Non Responding Host（非応答ホスト）
NTLM	
ODBC	Open Database Connect
OOB	Out Of Band（アウトオブバンド）
OS	Operating System（オペレーティング システム）

略語	説明
OTP	One Time Password（ワンタイム パスワード）
PA	Posture Attribute（ポスチャ アトリビュート）
PAC	Provisioned Access Credential
PACL	Port ACL（ポート ACL）
PAE	Port Access Entity（ポート アクセス エンティティ）
PBACL	Policy Based ACL（ポリシーベース ACL）
PEAP	Protected EAP
PKI	Public Key Infrastructure（公開キー インフラストラクチャ）
PPTP	
PVLAN	Private VLAN（プライベート VLAN）
QoS	Quality of Service
RAC	RADIUS Attribute Component
RPC	Remote Procedure Call（リモート プロシージャ コール）
SAML	Security Assertion Markup Language
SIMS	Security Information Management System（セキュリティ情報管理システム）
SLB	Server Load Balancing（サーバ負荷バランシング）
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SQ	Status Query（ステータス クエリー）
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TLS	Tunnel Layer Security
TLV	Type Length Value
UDP	Universal Datagram Protocol
URL	Universal Resource Locator
VACL	VLAN ACL
VLAN	Virtual Local Area Network（仮想 LAN）
VoIP	Voice over IP
VPN	Virtual Private Network（バーチャル プライベート ネットワーク）
VSA	Vendor Specific Attribute（ベンダー固有アトリビュート）
VVID	Voice VLAN Identifier
WAN	Wide Area Network（ワイド エリア ネットワーク）
WEP	Wireless Encrypted Protection
WLAN	Wireless LAN（無線 LAN）
WoL	Wake on LAN

用語	定義
802.1x、dot1x	IEEE 802.1x。レイヤ 2 のネットワーク認証方式を定めた標準。無線ネットワーキング用の 802.11a/b/g と混同しないようにしてください。
AAA	Authentication, Authorization, and Accounting（認証、認可、アカウンティング）。通常は、ダイアルアップ、無線、VPN、802.1x などのユーザのネットワーク アクセスを認証する機能です。中央の AAA サーバは、1 つまたは複数の認証サーバによる認証決定をもとにシステムの単一の結果を判定します。NAD でポリシーを適用するために、AAA サーバはこの決定をネットワーク アクセス プロファイルにマッピングします。
Access-Accept	ユーザが認証されたことをアクセス サーバに通知する RADIUS サーバからの応答パケット。このパケットには、ユーザに割当てられた AAA 機能を定義するユーザ プロファイルが含まれます。
Access-Challenge	認証の前にユーザに追加情報の提供を要求する RADIUS サーバからの応答パケット。
Access-Reject	ユーザが認証されなかったことをアクセス サーバに通知する RADIUS サーバからの応答パケット。
Access-Request	ユーザの認証を要求するアクセス サーバが RADIUS サーバに送信する要求パケット。
Accounting	ネットワーク管理サブシステムの Accounting（アカウンティング）は、リソース利用状況に関するネットワーク データを収集する機能です。
ACE	Access Control Entry（アクセス コントロール エントリ）。ACL エントリには、タイプ、エントリが参照するユーザまたはグループの修飾子、一連のアクセス権が指定されます。一部のエントリ タイプのグループまたはユーザの修飾子は未定義です。
ACL	Access Control List（アクセス コントロール リスト）
ACS	Access Control Server または Cisco Secure Access Control Server
APT	Application Posture Token（アプリケーション ポスチャ トークン）。ベンダのアプリケーションの適合性チェックの結果で、そのコンポーネントの健全性を示します。ポスチャ検証のすべての APT がプライマリ PVS によって統合され、System Posture Token（SPT; システム ポスチャ トークン）が作成されます。
APT、Application Posture Token（アプリケーション ポスチャ トークン）	特定のベンダのアプリケーションのポスチャ検証の結果。
Audit Server（監査サーバ）	ホスト 上の PA を使用せずにポスチャのクレデンシャルを判定できるサーバ。このサーバは、ホストのポスチャ クレデンシャルを判定するとともに、ポスチャ検証サーバとしても機能できる必要があります。
Authentication（認証）	ネットワーク管理セキュリティでは、人物またはプロセスのアイデンティティを検証することです。
Authorization（許可）	各サービスのワンタイム認証または許可、ユーザごとのアカウント リストとプロファイル、ユーザ グループ、IP、IPX、ARA および Telnet をサポートするリモート アクセス コントロール手法。
AVP	Attribute-value pair（アトリビュート値ペア）
CSA、Cisco Security Agent	Cisco Security Agent は、サーバおよびデスクトップ コンピューティング システムを脅威から保護します。ホストへの侵入防止、分散型ファイアウォール、悪質なモバイル コードからの保護、オペレーティング システムの完全性の保証、単一のエージェント パッケージへの監査ログなどを融合してさまざまなセキュリティ機能を提供します。総合的なセキュリティ戦略の一角をなす Cisco Security Agent は、ネットワーク アドミッション コントロールと SAFE ブループリントを強化し、エンドポイントにまで保護機能を拡張します。
CSM	Cisco Security Manager
CS-MARS	Cisco Secure Monitoring, Analysis and Response System（CS-MARS）は、攻撃への対応、監視、被害の拡散防止のためのハイ パフォーマンスでスケーラブルなアプライアンス ファミリです。ネットワーク インテリジェンス、コンテキストの相関分析、ベクトル分析、異常検出、ホットスポット識別、および被害の拡散防止の自動化機能が統合された CS-MARS により、ネットワークおよびセキュリティ デバイスをより効果的に使用することができます。

用語	定義
CTA	Cisco Trust Agent。シスコの PA 製品です。PA ポスチャ プラグインが含まれます。
CTA、Cisco Trust Agent	CTA はシスコのポスチャ エージェント製品で、有線のみをサポートするサプリカントが組み込まれています。
CTASI	CTA Scripting Interface
DAI	Dynamic ARP Inspection
DHCP Snooping（DHCP スヌーピング）	DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリング、および DHCP スヌーピング バインディング データベース（または DHCP スヌーピング バインディング テーブル）の構築および維持により、ネットワーク セキュリティを提供する DHCP セキュリティ機能です。 DHCP スヌーピングは、信頼できないホストと DHCP サーバ間でファイアウォールのような機能を果たします。DHCP スヌーピングを使用して、エンドユーザに接続する信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続する信頼できるインターフェイスとを区別することができます。 DHCP スヌーピングにより、クライアント IP アドレス、MAC アドレス、ポート、VLAN 番号、リースおよびバインディング タイプを格納する DHCP バインディング テーブルが作成されます。この機能は、スイッチ上の特定の VLAN 上でイネーブルにできます。スイッチは、レイヤ 2 VLAN ドメイン内ですべての DHCP メッセージ ブリッジングを代行受信します。
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）は、TLS ベースの RFC 3748 に準拠する EAP 方式です。 EAP-FAST は、対称鍵アルゴリズムを使用して認証プロセスのトンネル化を実現します。トンネルの確立には、AAA サーバを通じて、EAP-FAST により動的なプロビジョニングおよび管理が可能な Protected Access Credential（PAC）を使用します。
EAP-FAST	EAP Flexible Authentication by Secure Tunneling
EAP-GTC	EAP Generic Token Card
EAPOL	EAP over LAN
EAP-TLS	EAP Transport Layer Security
Endpoint（エンドポイント）	ネットワーク リソースへの接続や使用を試みる任意のマシン。
EoU、EAPoUDP	Extensible Authentication Protocol over User Datagram Protocol
GAME	Generic Authorization Message Exchange
GINA	Graphical Identification and Authentication（Microsoft）
HCAP	Host Credential Authorization Protocol
Host（ホスト）	エンドポイント デバイスの別名。
Host（ホスト）	ネットワーク リソースへの接続や使用を試みる任意のマシン。
IID、Initiator Identity	マシン認証における IID は、ホストの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）（例：jdoe-pc.cisco.com）です。ユーザ認証における IID は、ユーザ名（例：jdoe）です。
MAB	MAC Authentication Bypass（MAC-Auth-Bypass）
Machine Authentication（マシン認証）	マシン認証は、アイデンティティとして、Active Directory に登録されている実際のコンピュータ名を使用して行われます。クレデンシャルは、使用される EAP のタイプに応じて、パスワードベースまたは PKI 証明書ベースのクレデンシャルを使用できます。
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2

用語	定義
NAC	Network Admission Control（ネットワーク アドミッション コントロール）。NAC は、ネットワーク インフラストラクチャを活用して、ネットワーク コンピューティング リソースにアクセスしようとするすべてのデバイスにセキュリティ ポリシーへの適合を強制することにより、ウイルスやワームがもたらす損害を抑制する、シスコシステムズが主導する業界イニシアチブです。NAC は、ネットワーク自体によるセキュリティの脅威の自動的な特定、防止、適応を実現するためにネットワーク インテリジェンスを強化する、シスコの自己防衛型ネットワーク構想の一角をなします。
NAC L2 802.1x	Cisco CatOS および IOS スイッチで 802.1x プロトコルを使用するシスコの NAC 実装です。
NAC L2 IP	Cisco スイッチがレイヤ 2 で EAPoUDP を介して行う NAC。
NAC L3 IP	Cisco ルータが レイヤ 3 で EAP over UDP を介して行う NAC。
NAD	Network Access Device（ネットワーク アクセス デバイス）。ネットワーク アクセス デバイスは、エンドポイント デバイスに許可されたネットワーク アクセス権を与えるポリシーを適用するポイントです。
NAD、Network Access Device（ネットワーク アクセス デバイス）	ネットワーク アクセス デバイスは、ホストに許可されたネットワーク アクセス権を与えるポリシーを適用するポイントです。
NAF、Network Access Filter（ネットワーク アクセス フィルタ）	NAF は、1 つまたは複数のネットワーク エレメント（IP アドレス、AAA クライアント（ネットワーク デバイス）、ネットワーク デバイス グループ（NDG））の組み合わせで構成される名前付きのグループです。NAF により、AAA クライアントをベースに Downloadable ACL またはネットワーク アクセス制限を指定し、これを通じてユーザにネットワークへのアクセスを許可することができます。各 AAA クライアントを明示的にリストする必要はありません。
NAH	NAC Agentless Host（NAC エージェントレス ホスト）
NAH、NAC Agentless Host（NAC エージェントレス ホスト）	ポスチャ検証を実施するための 802.1x サプリカントまたは CTA がインストールされていないホスト。
NDG、Network Device Group（ネットワーク デバイス グループ）	単一の論理的なグループとして機能するネットワーク デバイスの集合。
NRH	Nonresponsive Host（非応答ホスト）
PA	Posture Agent（ポスチャ エージェント）。1 つまたは複数のポスチャ プラグインからポスチャ クレデンシャルを収集してネットワークと通信する、エンドポイント上の単一のコンタクト ポイントとして機能するアプリケーション。シスコのポスチャ エージェントは、Cisco Trust Agent（CTA）です。
PA、Posture Agent（ポスチャ エージェント）	1 つまたは複数のポスチャ プラグインからポスチャ クレデンシャルを収集してネットワークに安全にそれらの情報を通知する、ホスト上の単一のコンタクト ポイントとして機能するアプリケーション。
PAC	Protected Access Credential
PDP、Policy Decision Point（ポリシー決定ポイント）	ポリシー管理および条件フィルター機能を提供します。
PEAP	Protected EAP
PEAP-GTC	
PEP、Policy Enforcement Point（ポリシー適用ポイント）	ACS がポリシー適用ポイントとして機能し、ポリシーを管理します。
Plugin（プラグイン）、Posture Plugin（ポスチャ プラグイン）	同一のエンドポイント上のポスチャ エージェントに、エンドポイントのポスチャ認証およびネットワーク認証のために必要な、ホストのポスチャ クレデンシャルを提供するサードパーティ製 DLL。
Posture（ポスチャ）	現在のホストのステータスと設定。アンチウイルスのレベル、ホットフィックス、OS タイプなどが含まれます。
Posture Agent（ポスチャ エージェント）	1 つまたは複数のポスチャ プラグインからポスチャ クレデンシャルを収集してネットワークと通信するエンドポイント上の単一のコンタクト ポイントとして機能するアプリケーション。シスコのポスチャ エージェントは、Cisco Trust Agent（CTA）です。

用語	定義
Posture Credentials（ポスチャ クレデンシャル）	エンドポイント デバイスの特定の時期のハードウェアおよびソフトウェア（OS およびアプリケーション）情報を示すステート情報。
Posture Credentials（ポスチャ クレデンシャル）	ネットワーク エンドポイントの特定の時期のハードウェアおよびソフトウェア（OS およびアプリケーション）情報を示すステート情報。
Posture Plugin（ポスチャ プラグイン）	エンドポイントのポスチャ検証およびネットワーク認証のために同一のエンドポイント上のポスチャ エージェントにホストのポスチャ クレデンシャルを提供するサードパーティ製 DLL。
Posture Validation（ポスチャ検証）	1 つまたは複数のポスチャ検証サーバとその適合ポリシーを使用して行う、エンドポイント デバイスのポスチャ クレデンシャルの認証。
Posture Validation（ポスチャ検証）	1 つまたは複数のポスチャ検証サーバとその適合ポリシーを使用した、ネットワーク エンドポイントのポスチャ クレデンシャルの認証。
Posture Validation Server（ポスチャ検証サーバ）	ポスチャ認証サーバは、NAC においてアプリケーション別のポリシー決定ポイントとして機能し、一連のポリシー ルールと照合してポスチャ クレデンシャルを検証します。
PP	Posture Plugin（ポスチャ プラグイン）
PV	Posture Validation（ポスチャ検証）。ユーザのマシン（ホスト）の一般的な状態と健全性を示す一連のアトリビュートを検証します。
PV	Posture Validation（ポスチャ検証）。ユーザのマシン（ホスト）の一般的な状態と健全性を示す一連のアトリビュートを検証します。
PVS、Policy Server（ポリシー サーバ）、Vendor Policy Server（ベンダ ポリシー サーバ）、Posture Validation Server（ポスチャ検証サーバ）、External Posture Validation Server（外部ポスチャ検証サーバ）	ポスチャ検証に使用されるシスコまたはサードパーティ製のサーバ。ポスチャ検証サーバは、NAC におけるアプリケーション別のポリシー決定ポイントとして機能し、一連のポリシー ルールと照合してポスチャ クレデンシャルを検証します。
PVS、Posture Validation Server（ポスチャ検証サーバ）、Policy Server（ポリシーサーバ）、Vendor Policy Server（ベンダ ポリシー サーバ）、External Posture Validation Server（外部ポスチャ検証サーバ）	ポスチャ検証に使用されるシスコまたはサードパーティ製のサーバ。ポスチャ検証サーバは、NAC におけるアプリケーション別のポリシー決定ポイントとして機能し、一連のポリシー ルールと照合してポスチャ クレデンシャルを検証します。
RAC	RADIUS Attribute Component
RADIUS	Remote Authentication Dial-In User Service。ネットワーク アクセスの AAA の一元化を可能にする、幅広く利用されているプロトコルです。
SCM	Switchport Configuration Manager
SDM	Security Device Manager（セキュリティ デバイス マネージャ）
SPT	System Posture Token（システム ポスチャ トークン）。1 つまたは複数のアプリケーション ポスチャ トークンを収集して決定されたエンドポイント デバイスの単一のポスチャ検証結果です。エンドポイントのポスチャ検証から得られた最終的なポスチャ ステートとなります。
SPT、System Posture Token（システム ポスチャ トークン）	1 つまたは複数のアプリケーション ポスチャ トークンを収集して決定されたホストの単一のポスチャ検証結果です。
Token: Check-up	ホストはポリシーの適合範囲内ですが、更新を入手可能です。このステートは、ホストを Healthy State にプロアクティブに修復するために使用されます。
Token: Healthy	ホストはポリシーに適合しています。ホストからネットワークへのアクセスは制限されません。

用語	定義
Token: Infected	ホストは他のホストにとってアクティブな脅威です。このホストのネットワーク アクセスは厳格に制限するか、完全に拒否する必要があります。
Token: Quarantine	ホストはポリシーに適合していません。このホストのネットワーク アクセスは検疫ネットワークのみに制限されて修復が行われます。このホストはアクティブな脅威ではありませんが、既知の攻撃やウイルス感染に脆弱です。
Token: Transition	ホストのポスチャ検証が行われています。ホストにはポスチャ検証が完了するまで暫定的なアクセスが提供されます。すべてのサービスが稼動していない可能性があるホスト ブート プロセス中または検証結果が判明していないときに使用されるステートです。
Token: Unknown	ホストのポスチャを特定できません。正確なポスチャを特定できるまで、ホストの検疫、認証、または修復を行います。
User Authentication（ユーザ認証）	ログイン時に 802.1x を使用してユーザ情報を確認する手法。ユーザ認証は、ユーザの Active Directory（ドメイン）のクレデンシャル、またはクライアント側の証明書で提供されるクレデンシャルを通じて実行できます。
VSA、Vendor Specific Attribute	大半のベンダが VSA を使用して付加価値機能をサポートします。

シスコシステムズ株式会社

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
http://www.cisco.com/jp/

お問い合わせ先 (シスコ コンタクトセンター)
http://www.cisco.com/jp/service/contactcenter/

お問合せ先

06.07