

Network Access Manager の設定

この章では、Network Access Manager の設定の概要について、ならびにユーザ ポリシーおよび ネットワーク プロファイルの追加と設定の手順について説明します。

- Network Access Manager について (1 ~ ジ)
- Network Access Manager の展開 (4 ページ)
- DHCP 接続テストを無効 (6 ページ)
- Network Access Manager プロファイル (6 ~~- ジ)

Network Access Manager について

Network Access Managerは、ポリシーに従ってセキュアなレイヤ2ネットワークを提供するク ライアントソフトウェアです。最適なレイヤ2アクセスネットワークを検出して選択し、有 線ネットワークとワイヤレスネットワークの両方へのアクセスに対してデバイス認証を実行し ます。Network Access Managerは、セキュアなアクセスに必要なユーザおよびデバイスアイデ ンティティならびにネットワークアクセスプロトコルを管理します。管理者定義のポリシー に違反する接続をエンドユーザが確立しないように、インテリジェントに動作します。

Network Access Managerは、単一ホーム(一度に1つのネットワーク接続を許可する)になる よう設計されています。また、有線接続がワイヤレス接続によりも優先されます。そのため、 有線接続を使用してネットワークに接続した場合、ワイヤレスアダプタは IP アドレスを失い 無効になります。

有線またはワイヤレスネットワーク設定や特定の SSID がグループポリシーからプッシュされた場合、それらはNetwork Access Managerの適切な動作と競合する可能性があります。Network Access Managerがインストールされている場合、ワイヤレス設定のグループポリシーはサポートされません。



(注)

Network Access Manager は macOS または Linux には対応していません。

(注) Windows OS で ISE ポスチャを使用する場合は、Cisco Secure Client ISE ポスチャを開始する前 に Network Access Manager をインストールする必要があります。

Cisco Secure Client のNetwork Access Manager コンポーネントは、次の主要な機能に対応しています。

- キャプティブポータルの検出Network Access Manager によるキャプティブポータル検出要件(10ページ)を参照してください。キャプティブポータルの検出は、Windows 7 ではサポートされていません。
- Transport Layer Security (TLS) $\mathcal{T} \Box \vdash \Box \mathcal{V} \mathcal{V} \mathcal{V} \exists \mathcal{V} 1.2$
- ・有線(IEEE 802.3)およびワイヤレス(IEEE 802.11)ネットワークアダプタ。
- •Windows 7 以降でのモバイル ブロードバンド(3G) ネットワーク アダプタ(Microsoft モ バイル ブロードバンド API をサポートする WAN アダプタが必要です)。
- •Windows マシン クレデンシャルを使用した事前ログイン認証。
- Windows ログイン クレデンシャルを使用するシングル サインオン ユーザ認証。
- ・簡素化された IEEE 802.1X 設定。
- IEEE MACsec 有線暗号化および企業ポリシー制御。
- EAP 方式:
 - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS、およびLEAP(IEEE 802.3 有線のみ EAP-MD5、EAP-GTC、およびEAP-MSCHAPv2)。
- 内部 EAP 方式:
 - ・PEAP:EAP-GTC、EAP-MSCHAPv2、およびEAP-TLS。
 - EAP-TTLS: EAP-MD5 および EAP-MSCHAPv2 およびレガシー方式(PAP、CHAP、 MSCHAP、および MSCHAPv2)。
 - ・EAP-FAST:GTC、EAP-MSCHAPv2、およびEAP-TLS。
- ・暗号化モード:スタティックWEP(オープンまたは共有)、ダイナミックWEP、TKIP、 および AES。
- ・キー確立プロトコル: WPA、WPA2/802.11i。
- Cisco Secure Clientは、次の環境でスマートカードにより提供されるログイン情報に対応します。
 - Windows の Microsoft CAPI 1.0 および CAPI 2.0 (CNG)。
 - Windows ログインは ECDSA 証明書に対応していないため、Network Access Managerの シングル サインオン (SSO) は ECDSA クライアント証明書に対応していません。



(注) WPA3 Enhanced Open (OWE) および WPA3 Personal (SAE) のサ ポートが、Cisco Secure Client Release 5.0.02075 のネットワークア クセス マネージャに追加されました。

Suite B および FIPS

次の機能は、Windows 7 以降で FIPS 認定されています。例外を次に示します。

- ACS および ISE は Suite B には対応していませんが、OpenSSL 1.x 搭載の FreeRADIUS 2.x は対応しています。Microsoft NPS 2008 は Suite B に一部対応しています(NPS の証明書は RSA でなければなりません)。
- 802.1X/EAP は、Suite B の遷移プロファイルのみをサポートします(RFC 5430 の定義どおり)。
- MACsec は FIPS 準拠です。
- 楕円曲線 Diffie-Hellman (ECDH) キー交換はサポートされています。
- ・ECDSA クライアント証明書はサポートされています。
- OS ストアの ECDSA CA 証明書はサポートされています。
- ネットワーク プロファイルの(PEM エンコードされた) ECDSA CA 証明書はサポートされています。
- ・サーバの ECDSA 証明書チェーン検証はサポートされています。

シングルサインオンの「シングルユーザ」の適用

Microsoft Windows では複数のユーザーが同時にログインできますが、Cisco Secure Client Network Access Managerではシングルユーザーにネットワーク認証を制限します。Cisco Secure Client Network Access Managerは、ログインしているユーザーの数に関係なく、デスクトップまたは サーバー当たり1人のユーザーをアクティブにできます。シングルユーザログインの適用は、 いつでもシステムにログインできるユーザは1人のみで、管理者は現在ログインしているユー ザを強制的にログオフできないことを示しています。

Network Access Manager クライアントモジュールが Windows デスクトップにインストールされ ている場合、デフォルト動作はシングルユーザログインを適用することです。サーバにイン ストールされている場合、デフォルト動作はシングルユーザログインの適用を緩和すること です。いずれの場合も、デフォルトの動作を変更するようにレジストリを変更または追加でき ます。

制約事項

- Windows 管理者は、現在ログインしているユーザの強制ログオフが制限されています。
- 接続されたワークステーションへの RDP は同一ユーザにサポートされています。
- 同一ユーザと見なされるためには、クレデンシャルを同じフォーマットにする必要があります。たとえば、user/example は user@example.com と同じではありません。
- ・また、スマートカードユーザが同じPINを持っている場合、同一ユーザと見なされます。

シングル サインオンのシングル ユーザーの適用の設定

Windows ワークステーションまたはサーバで複数のユーザーを処理する方法を変更するには、 レジストリの EnforceSingleLogon の値を変更します。

Windows では、レジストリ キーは EnforceSingleLogon で、OverlayIcon レジストリ キーと同じ 場所にあります。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}

1つまたは複数のユーザーログインを設定するには、EnforceSingleLogonという名前のDWORD を追加し、1または0の値を指定します。

Windows の場合:

- •1は、シングルユーザーにログインを制限します。
- •0は、複数のユーザーにログインを許可します。

Network Access Manager の展開

Network Access Managerは Cisco Secure Client の一部として展開されます。Cisco Secure Client を Network Access Managerやその他のモジュールとともにインストールする方法については、 「AnyConnect 展開の概要」を参照してください。

ガイドライン

 Windowsのネットワークステータスタスクトレイアイコンの混同:Network Access Manager は、Windowsのネットワーク管理より優先します。したがって、Network Access Manager のインストール後、ネットワークに接続するためにネットワークステータスのアイコンを 使用できません。

推奨アクション:Windowsグループポリシーの[ネットワークアイコンを削除する (Remove the networking icon)]を設定することで、タスクトレイから Windows ネットワークアイコ ンを削除します。この設定は、トレイアイコンだけに影響します。ユーザは、コントロー ルパネルを使用してネイティブのワイヤレス ネットワークを確立できます。 Windows 7以降の非表示のネットワークおよびネットワークの選択: Network Access Manager は、Network Access Managerのネットワークスキャンリストで設定されたネットワークだ けに接続を試みます。

Windows 7 以降では、Network Access Managerは非表示 SSID をプローブします。最初の非 表示 SSID が見つかると、検索を中止します。複数の非表示ネットワークが設定されてい る場合、Network Access Managerは次のように SSID を選択します。

- 管理者が定義した最初の非表示社内ネットワーク
- 管理者が定義した非表示ネットワーク
- ユーザが定義した最初の非表示ネットワークNetwork Access Managerは一度に1つの 非ブロードキャストSSIDしかプローブできないため、サイトの非表示社内ネットワー クは1つのみにすることをお勧めします。
- ネットワークの接続性または長い接続時間の瞬時的な喪失: Network Access Managerをインストールする前に Windows でネットワークが定義済みである場合、Windows の接続マネージャがそのネットワークに接続を試みる場合があります。

推奨アクション:ネットワークが圏内にある場合、すべての Windows 定義ネットワーク に対して[自動的に接続する (Connect Automatically)]をオフにするか、Windows 定義ネッ トワークをすべて削除します。

- Network Access Manager モジュールは、このモジュールがクライアントシステムに初めて インストールされたときに、一部の既存の Windows 7 またはそれ以降のワイヤレス プロ ファイルをNetwork Access Manager プロファイル形式に変換するように設定できます。次の条件を満たすインフラストラクチャネットワークは変換が可能です。
 - •オープン
 - •静的 WEP
 - WPA/WPA2 Personal
 - •非 GPO ネイティブ Wi-Fi ユーザ ネットワーク プロファイルだけが変換されます。
 - プロファイルの変換中は、WLAN サービスがシステムで実行している必要があります。
 - ・変換は、Network Access Manager XML コンフィギュレーション ファイルがすでに存 在する場合(userConfiguration.xml) は実行されません。

ネットワークプロファイルの変換を有効にするには、PROFILE_CONVERSIONプロパティ の値を1に設定する MSI トランスフォームを作成し、それを MSI パッケージに適用しま す。またはコマンド ラインで PROFILE_CONVERSION プロパティを1に変更して、MSI パッケージをインストールします。たとえば、msiexec /i

$cisco-secure-client-win-<\!version\!\!>\!nam-predeploy-k9.msi\ PROFILE_CONVERSION=1_{\circ}$

ISEポスチャが開始する前にNetwork Access Managerをインストールする必要があります。
 ISE ポスチャは、Network Access Manager プラグインを使用して、ネットワーク変更ベントおよび 802.1x WiFi を検出します。

DHCP 接続テストを無効

ネットワークがダイナミック IP アドレスを使用するように設定されている場合は、Windows OS サービスは DHCP を使用して接続を確立しようとします。ただし、オペレーティングシス テム プロセスがNetwork Access Managerに DHCP トランザクションが完了したことを通知する までに最大で2分かかる場合があります。OS の DHCP トランザクションに加えて、Network Access Managerが DHCP トランザクションをトリガーすることによって、OS 経由の接続が確 立するまでの時間を短縮し、ネットワーク接続を確認します。

接続テストでNAMによるDHCPトランザクションの使用を無効にする場合は、次のレジスト リキーをDWORDとして追加し、指定された値を設定します。

- 64 ビット Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco Secure Client Network Access Manager\DisableDHCP を1に設定
- 32 ビット Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client Network Access Manager\DisableDHCP を1に設定



Network Access Manager の DHCP 接続テストを無効にすると、多くの場合、接続時間が長くなるため、有効にしておくことを強くお勧めします。

Network Access Manager プロファイル

Network Access Manager プロファイルは、Network Access Manager プロファイル エディタで設 定されます。このエディタは ASDM でスタンドアロン Windows アプリケーションとして使用 できます。

クライアント ポリシー ウィンドウ

[クライアントポリシー (Client Policy)]ウィンドウでは、クライアントポリシー オプション を設定できます。この項では次のトピックについて説明します。

接続の設定

ユーザログインの前または後にネットワーク接続しようとするかどうかを定義できます。

- •[デフォルト接続タイムアウト(Default Connection Timeout)]: ユーザ作成ネットワークの 接続タイムアウトとして使用する秒数。デフォルト値は40秒です。
- 「ユーザ ログインの前(Before User Logon)]: ユーザがログインする前にネットワークに 接続します。サポートされているユーザ ログインの種類として、ユーザ アカウント (Kerberos)認証、ユーザ GPO のロード、GPO ベースのログイン スクリプト実行があり

ます。[ユーザログインの前(Before User Logon)]を選択した場合、[ユーザがログインで きるまでに待機する時間(Time to Wait Before Allowing a User to Logon)]も設定できます。

 「ユーザがログインできるまでに待機する時間(Time to Wait Before Allowing a User to Logon)]: Network Access Managerが完全にネットワーク接続するのに待機する最大(最 悪のケース)秒数を指定します。この時間内にネットワーク接続が確立できない場合、 Windows ログインプロセスはユーザログインにより継続されます。デフォルトは5秒で す。



- (注) ワイヤレス接続を管理するようNetwork Access Managerが設定されている場合、[ユーザがログインできるまでに待機する時間(Time to Wait Before Allowing a User to Logon)]を30秒以上に設定する必要があります。ワイヤレス接続の確立にさらに時間が必要になる可能性があるためです。DHCP経由でIPアドレスを取得するために必要な時間も考慮する必要があります。2つ以上のネットワークプロファイルが設定されている場合、2回以上の接続試行に対応するように値を大きくする必要があります。
 - •[ユーザ ログイン後(After User Logon)]: Windows へのユーザ ログイン後にネットワークに接続します。

メディア

Network Access Manager クライアントにより制御されるメディアの種類を指定します。

• [Wi-Fi(ワイヤレス)メディアの管理(Manage Wi-Fi (wireless) Media)]: Wi-Fi メディア の管理、また任意で WPA/WPA2 ハンドシェイクの検証ができるようになります。

IEEE 802.11i ワイヤレス ネットワーキング標準では、サプリカント(この場合はNetwork Access Manager)がアクセス ポイントの RSN IE(堅牢でセキュアなネットワーク情報交 換)を検証する必要があることを規定しています。IE は、キー導出時に IEEE 801.X プロ トコル パケットの EAPOL キー データに送信され、ビーコン/プローブ応答フレームにあ るアクセス ポイントの RSN IE に一致する必要があります。

 [WPA/WPA2ハンドシェイクの検証の有効化(Enable validation of WPA/WPA2 handshake)]:
 WPA/WPA2ハンドシェイクを検証します。オフの場合、この任意の検証手順はスキップ されます。



- (注) 一部のアダプタでは、アクセスポイントの RSN IE を常に提供するわけではないため、認証試行に失敗し、クライアントが接続されません。
 - ランダム化されたMACアドレスを有効にする:(Windows 10以降のみ)ランダム化をサポートするハードウェアまたはドライバーのランダム化を有効にします。有効にすると、

ー意の各ワイヤレスネットワーク SSID が新しいランダム化されたアドレスを利用し、そ のプライベートアドレスをネットワークに使用します。必要に応じて、ランダム化された アドレスを 24 時間ごとに変更することもできます。接続を忘れて再接続すると、新しい MAC アドレスが割り当てられます。MAC アドレスのランダム化の有効化 (19ページ) を参照してください。

- 「デフォルトのアソシエーションタイムアウト(秒) (Default Association Timeout (sec))]:
 WPA/WPA2 ハンドシェイクを有効にした場合は、デフォルトのアソシエーションタイム アウトを指定する必要があります。
- [有線(IEEE 802.3)メディアの管理(Manage Wired (IEEE 802.3) Media)]: 有線接続の管理を有効にします。
- [モバイルブロードバンドメディアの管理(Manage Mobile Broadband Media)]: Windows
 モバイルブロードバンドアダプタの管理を有効にします。この機能は、デフォルトでは
 無効になっています。

- (注) この機能はベータ版に入っています。Cisco TAC は、ベータ版に は対応していません。
 - [データローミングの有効化(Enable Data Roaming)]: データローミングを許可するかどうかを指定します。

エンドユーザ制御

ユーザに対して次の制御を設定できます。

- [クライアントの無効化(Disable Client)]:ユーザーは、Cisco Secure Client UI を使用して、Network Access Managerによる有線メディアおよびワイヤレスメディアの管理を無効および有効にできます。
- [ユーザグループの表示(Display User Groups)]:管理者定義のグループに対応しない場合でも、ユーザが作成したグループ(CSSC 5.x から作成)を表示して、接続できるようにします。
- ・[接続時に実行するスクリプトまたはアプリケーションの指定(Specify a script or application to run when connected)]:ユーザは、ネットワーク接続時に実行するスクリプトまたはア プリケーションを指定できます。



- (注) スクリプト設定は1つのユーザ設定ネットワークに固有であり、 ユーザはローカルファイル(.exe、.bat、または.cmd)を指定し て、そのネットワークが接続状態になったときに実行できます。 競合を避けるために、スクリプト機能では、ユーザはユーザ定義 のネットワークについてのみスクリプトまたはアプリケーション を設定でき、管理者定義のネットワークについては設定できませ ん。スクリプト機能では、スクリプトの実行に関して管理者ネッ トワークをユーザが変更できません。このため、ユーザは管理者 ネットワークのインターフェイスを使用できません。また、ユー ザが実行中のスクリプトを設定できないようにする場合、この機 能はNetwork Access Manager GUI に表示されません。
 - •[自動接続(Auto-connect)]: ユーザが選択しなくても自動的にネットワークに接続しま す。デフォルトは自動接続です。
 - マシン接続タイプの選択:ユーザー定義ネットワークを追加するときに、エンドユーザー に対して[ログオン前に接続を許可(Allow Connection Before Logon)]の選択を有効にし ます。エンドユーザーの選択によって、ユーザーがログインする前にネットワークが接続 できるかどうかが決まります。次に、個人、共有WEP、またはオープンセキュリティを 選択できます。

[デフォルトで有効にする(Enable by Default)]: ユーザー定義ネットワークを追加すると きに、エンドユーザーに対して[ログオン前の接続を許可(Allow Connection Before Logon)] を自動的に許可します。



(注) AnyConnectを以前のバージョンから4.9.01095以降にアップグレードする場合、新しい機能で更新された xmlを取得するために、適切なプロファイルエディタで configuration.xml ファイルを開き、ファイルを保存する必要があります。

管理ステータス

- [サービスオペレーション (Service Operation)]: このサービスをオフにすると、このプロ ファイルを使用しているクライアントはレイヤ2接続を確立するために接続できません。
- [FIPS モード(FIPS Mode)]: FIPS モードを有効にすると、Network Access Managerは政府の要件を満たす方法で暗号化操作を行います。

連邦情報処理標準(FIPS 140-2 Level 1)は、暗号化モジュールのセキュリティ要件を指定 する米国政府標準規格です。FIPS は、ソフトウェアとハードウェアのタイプに応じて、 MACsec または Wi-Fi 用のNetwork Access Managerでサポートされています。 表 1: Network Access Managerによる FIPS サポート

メディア/オペレーティ ング システム	Windows 7 以降
MACsec で有線	Intel HW MACsec 対応 NIC の場合、 またはハードウェア以外の MACsec を使用している場合に FIPS に準拠 しています。
Wi-Fi	FIPS に準拠していません。

 [Captive Portal Detection (キャプティブポータルの検出)]:キャプティブポータルを検出 するときにデフォルトのWebブラウザの自動起動を有効または無効にするかを選択でき ます。追加情報については、「キャプティブポータルについて」を参照してください。 キャプティブポータルの検出を有効にすると、ユーザーはログイン情報を入力するか、 ポータルページを確認するように求められ、起動されたブラウザでのネットワークアクセ スが許可されます。デフォルトのWebブラウザが起動すると、ネットワークUIタイルに 「アクションが必要です。インターネットがありません。ブラウザを開いて接続してくだ さい。(Action needed, no internet. Open browser and connect.)」と表示されます。このUI タイルは、認証時に「キャプティブポータルが検出されました(Captive Portal Detected)」 および「接続済み(Connected)」に変わります。キャプティブポータル検出の設定が存在 しない場合、Network Access Manager はオプションを無効に設定します。

Network Access Manager によるキャプティブポータル検出要件

- Network Access Manager の構成可能なエンドユーザコントロール内では、キャプティブポータルの修復はオプションではありません。
- ・キャプティブポータルの検出は、Windows7ではサポートされていません。
- ・競合の可能性を回避するために、Network Access Manager のキャプティブポータル検出を 有効にすると、Windowsネットワーク位置認識サービスのキャプティブポータル検出が無 効になります。このWindows サービスは、Network Access Manager が無効に設定された か、アンインストールされた場合にのみ復元されます。
- Network Access Manager は 10 秒ごとに接続をプローブし、Web 認証の完了を検出すると、 インターネット接続を提供します。ユーザーがいつログアウトするかは監視しません。

認証ポリシーウィンドウ

[認証ポリシー(Authentication Policy)] ウィンドウでは、すべてのネットワーク接続に適用さ れる、アソシエーションおよび認証ネットワークフィルタを作成できます。アソシエーション モードまたは認証モードのいずれもオンにしない場合、認証 Wi-Fi ネットワークに接続できま せん。モードのサブセットを選択すると、それらのタイプのネットワークにのみ接続できま す。目的のアソシエーションモードまたは認証モードをそれぞれ選択するか、[すべて選択 (Select All)]を選択します。

内部方式も特定の認証プロトコルのみに制限される可能性があります。内部方式は、[許可された認証モード(Allowed Authentication Modes)]ペインの外部方式(トンネリング)下にイン デントされて表示されます。

認証プロトコル選択のメカニズムは、現在のクライアント認証データベースと統合されていま す。セキュアなワイヤレス LAN 展開では、ユーザが新しい認証システムを作成する必要はあ りません。

内部トンネリングに使用できる EAP 方式は、内部方式のクレデンシャル タイプと外部トンネ リング方式に基づいています。次のリストで、外部トンネル方式はそれぞれ、各クレデンシャ ルタイプに対応した内部方式の種類を一覧表示しています。

- PEAP
 - •パスワードクレデンシャル: EAP-MSCHAPv2 または EAP-GTC
 - ・トークンクレデンシャル: EAP-GTC
 - ・証明書クレデンシャル: EAP-TLS
- EAP-FAST
 - パスワード クレデンシャル: EAP-MSCHAPv2 または EAP-GTC
 - ・トークンクレデンシャル: EAP-GTC
 - ・証明書クレデンシャル: EAP-TLS
- EAP-TTLS
 - ・パスワードクレデンシャル: EAP-MSCHAPv2、EAP-MD5、PAP(L)、CHAP(L)、MSCHAP(L)、MSCHAP-v2(レガシー)。
 - トークンクレデンシャル: PAP(レガシー)。チャレンジ/レスポンス方式はトークンベースの認証には適していないため、Network Access Managerでサポートされるデフォルトトークンオプションは PAPです。
 - •証明書クレデンシャル:該当なし。

[ネットワーク(Networks)] ウィンドウ

[ネットワーク(Networks)]ウィンドウでは、企業ユーザの事前定義ネットワークを設定できます。すべてのグループで使用できるネットワークを設定するか、または特定のネットワークで使用するグループを作成できます。[ネットワーク(Networks)]ウィンドウには、既存のウィンドウにペインを追加できるウィザードが表示され、[次へ(Next)]をクリックしてより多くの設定オプションに進むことができます。

グループとは、基本的に、設定された接続(ネットワーク)の集合です。設定された各接続 は、グループに属するか、すべてのグループのメンバーである必要があります。



(注) 下位互換性を確保するため、Cisco Secure Services Client で展開された管理者作成のネットワークは、SSID をブロードキャストしない非表示ネットワークとして扱われます。ユーザネットワークは、SSID をブロードキャストするネットワークとして扱われます。

新しいグループを作成できるのは管理者だけです。設定にグループが定義されていない場合、 プロファイルエディタによって自動生成グループが作成されます。自動生成グループには、管 理者定義のグループに割り当てられていないネットワークが含まれます。クライアントは、ア クティブグループに定義されている接続を使用してネットワーク接続の確立を試みます。[ネッ トワークグループ(Network Groups)]ウィンドウの[ネットワークの作成(Create Networks)] オプションの設定に応じて、エンドユーザは、ユーザネットワークをアクティブグループに 追加するか、アクティブグループからユーザネットワークを削除できます。

定義されているネットワークは、リストの先頭にあるすべてのグループで使用できます。グ ローバルネットワーク内にどのネットワークがあるかを制御できるため、ユーザ定義のネット ワークが存在する場合も、エンドユーザが接続できる企業ネットワークを指定できます。エン ドユーザは管理者が設定したネットワークを変更したり、削除したりできません。



(注) エンドユーザは、globalNetworks セクションのネットワークを除き、グループにネットワーク を追加できます。これらのネットワークはすべてのグループ内に存在し、プロファイルエディ タを使用してしか作成できないためです。

企業ネットワークの一般的なエンドユーザは、このクライアントを使用するためにグループの 知識は必要ありません。アクティブグループは設定内の最初のグループですが、グループが1 つしか使用できない場合、アクティブグループは認識されず、表示されません。一方で、複数 のグループが存在する場合、UIにはアクティブグループが選択されたことを示すグループの リストが表示されます。ユーザはアクティブグループから選択でき、設定はリブート後も保持 されます。[ネットワークグループ(Network Groups)]ウィンドウの[ネットワークの作成 (Create Networks)]オプションの設定に応じて、エンドユーザは、グループを使用せずに自 分のネットワークを追加または削除できます。



(注) グループ選択はリブート後も持続して、ネットワークは修復されます(そのためには、トレイ アイコンを右クリックしながら[ネットワーク修復(Network Repair)]を選択します)。Network Access Managerが修復されるか、またはリスタートされると、以前のアクティブなグループが 使用されます。

ネットワーク、メディアタイプページ

[ネットワーク(Networks)]ウィンドウの[メディアタイプ(Media Type)]ページにより、有 線ネットワークまたはワイヤレスネットワークを作成または編集できます。設定は、選択内容 によって異なります。

最初のダイアログには、次のセクションが含まれています。

- [名前(Name)]: このネットワーク用に表示される名前を入力します。
- [グループメンバーシップ(Group Membership)]: このプロファイルが使用できるように するネットワーク グループ(複数の場合もあり)を選択します。
- 「ネットワークメディア (Network Media)]: [有線(Wired)]または[Wi-Fi (ワイヤレス) (Wi-Fi (wireless))]を選択します。[Wi-Fi]を選択すると、次のパラメータも設定できます。
 - [SSID]: ワイヤレス ネットワークの SSID (サービス セット識別子) を入力します。
 - 「非表示ネットワーク(Hidden Network)]: SSIDをブロードキャストしない場合でも、 ネットワークへの接続を許可します。
 - 「社内ネットワーク(Corporate Network)]: [社内(Corporate)]として設定されたネットワークが近接にある場合、まずそのネットワークに強制的に接続します。社内ネットワークが非ブロードキャスト(非表示)SSIDを使用し、非表示として設定されている場合、Network Access Managerは非表示 SSID をアクティブにプローブし、企業SSID が範囲内にあれば接続を確立します。
 - [アソシエーションタイムアウト(Association Timeout)]: Network Access Managerが、 使用できるネットワークを再評価するまでに特定のワイヤレスネットワークとのアソ シエーションを待機する時間を入力します。デフォルトのアソシエーションタイムア ウトは5秒です。
- 共通設定
 - [スクリプトまたはアプリケーション (Script or application)]: ローカルシステムで実行するファイルのパスとファイル名を入力するか、フォルダを参照してファイルを選択します。次のルールは、スクリプトおよびアプリケーションに適用されます。
 - Start Before Login モードではスクリプトを実行できません。
 - •.exe、.bat、または.cmd 拡張子のファイルが受け入れられます。
 - ユーザは、管理者が作成したネットワークで定義されたスクリプトまたはアプリケーションは変更できません。
 - プロファイルエディタを使用してパスおよびスクリプトまたはアプリケーションのファイル名のみを指定できます。スクリプトまたはアプリケーションがユーザのマシンに存在しない場合、エラーメッセージが表示されます。ユーザは、スクリプトまたはアプリケーションがマシンにないこと、およびシステム管理者に問い合わせる必要があると通知されます。

- アプリケーションがユーザのパスに存在する場合を除いて、実行するアプリケーションのフルパスを指定する必要があります。アプリケーションがユーザのパスに存在する場合は、アプリケーション名またはスクリプト名だけを指定できます。
- •[接続タイムアウト (Connection Timeout)]: Network Access Managerが、(接続 モードが自動の場合)別のネットワークに接続しようとするか、または別のアダ プタを使用するまでにネットワーク接続の確立を待機する秒数を入力します。



認証を完了するまでに 60 秒近くかかるスマートカード認証シス テムもあります。スマートカードを使用している場合、特に、ス マートカードが接続に成功するまでにいくつかネットワークに接 続しなければならない場合に、[接続タイムアウト (Connection Timeout)]値を増やす必要があります。



(注) 特定のスマートカードミドルウェアで見つかった問題を軽減する ために、Cisco Secure Client Network Access Manager はテストデー タに対して署名操作を実行し、その署名を検証することで、ス マートカード PIN を検証します。このテスト署名はスマートカー ドにある証明書ごとに行われ、証明書の数によってはスマート カード認証が大幅に遅延する場合があります。テスト署名操作を 無効にする場合は、HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/ Cisco Secure Client Network Access Manager でレジストリエントリ に DisableSmartcardPinVerifyBySigning を追加して DWORD を1 に設定できます。このキーを有効にする変更を加える場合は、正 しく動作するように、すべてのスマートカードおよび関連する ハードウェアでその変更を完全にテストしてください。

ネットワーク、セキュリティレベルページ

[ネットワーク (Networks)]ウィザードの[セキュリティ レベル (Security Level)]ページで、 [オープンネットワーク (Open Network)]、[認証ネットワーク (Authentication Network)]、ま たは (ワイヤレスネットワーク メディアにのみ表示される)[共有キーネットワーク (Shared Key Network)]を選択します。これらのネットワークタイプの設定フローはそれぞれ異なって おり、次の項で説明します。

- ・認証ネットワークの設定:企業を安全に保つために推奨されます。
- オープンネットワークの設定:推奨されません。ただし、キャプティブポータル環境を 介したゲストアクセスの提供に使用できます。Network Access Managerは、キャプティブ ポータルの状態にあるときはブラウザの自動起動をサポートしません。

 ・共有キーネットワークの設定:小規模オフィスまたはホームオフィスなどの無線ネット ワークに推奨されます。

さらに、オープン、共有、または認証ネットワーク内では、次のことができます。MAC アド レスのランダム化の有効化 (19ページ)

認証ネットワークの設定

[セキュリティレベル (Security Level)] セクションで [認証ネットワーク (Authenticating Network)]を選択した場合、次に説明するペインが追加で表示されます。これらのペインの設定を完了したら、[次へ (Next)] ボタンをクリックするか、[接続タイプ (Connection Type)] タブを選択して [ネットワーク接続タイプ (Network Connection Type)] ダイアログを開きます。

802.1X 設定ペイン

ネットワーク設定に応じて IEEE 802.1X 設定を調整します。



- (注) Cisco Secure Client ISE ポスチャがNetwork Access Managerとともにインストールされた場合、 ISE ポスチャはNetwork Access Manager プラグインを使用してネットワーク変更イベントと 802.1X WiFi を検出します。
 - [authPeriod(sec)]:認証が開始された場合、認証メッセージの間隔がこの設定を超えるとサ プリカントはタイムアウトします。認証を再度開始するには、サプリカントでオーセン ティケータが必要です。
 - [heldPeriod (sec)]:認証が失敗した場合、サプリカントはこの設定で定義された時間だけ待 機し、この時間を超えると別の認証が試行されます。
 - [startPeriod (sec)]: EAPOL-Start メッセージに対する応答をオーセンティケータから受信しない場合に、EAPOL-Start メッセージを再送信する間隔(秒)です。
 - [maxStart]:サプリカントが、オーセンティケータが存在しないと見なす前に、IEEE 801.X プロトコルパケット、EAPOL Key データ、または EAPoL-Start を送信することで、サプ リカントがオーセンティケータの認証を開始する回数です。これが発生した場合は、サプ リカントはデータトラフィックを許可します。

 \mathcal{O}

ヒント 単一の認証有線接続がオープンおよび認証ネットワークの両方と動作するように設定できます。これは、[startPeriod]および[maxStart]を注意深く設定して、認証開始試行に費やす合計時間がネットワーク接続タイマーよりも小さくなるようにします([startPeriod]x[maxStart]<ネットワーク接続タイマー)。</p>

このシナリオでは、ネットワーク接続タイマーを([startPeriod] x [maxStart])秒だけ大きくして、DHCPアドレスを取得してネットワーク接続を完了するために十分な時間をクライアントに与えることに注意してください。

逆に、認証が成功した後にのみデータトラフィックを許可するには、認証の開始に費やした総時間がネットワーク接続タイマーより長くなるような [startPeriod] および [maxStart] になるようにします([startPeriod] x [maxStart] > ネットワーク接続タイマー)。

セキュリティペイン

有線ネットワークの場合にのみ表示されます。

- [セキュリティ (Security)]ペインで、次のパラメータの値を選択します。
 - •[キー管理(Key Management)]: MACsec 対応有線ネットワークで使用するキー管理プロトコルを決定します。
 - [なし(None)]: キー管理プロトコルを使用しません。また、有線暗号化を実行しま せん。
 - [MKA]:サプリカントは、MACsecキー承諾プロトコルポリシーと暗号キーをネゴシ エートしようとします。MACsecはMACレイヤセキュリティで、有線ネットワーク でMACレイヤ暗号化を行います。MACsecプロトコルは、暗号化を使用してMAC レベルフレームを保護する手段であり、MACsecKeyAgreement(MKA)エンティティ に依存して暗号キーをネゴシエートおよび配布します。
 - •[暗号化(Encryption)]
 - •[なし(None)]: データトラフィックの整合性チェックは行われますが、暗号化はさ れません。
 - [MACsec: AES-GCM-128]: このオプションは、キー管理に MKA を選択した場合のみ 使用できます。AES-GCM-128 を使用して、データトラフィックが暗号化されます。
 - [MACsec: AES GCM 256]: このオプションは、エンタープライズエッジ(eEdge)統合を備えた特定の IOS バージョンでサポートされており、キー管理に MKA を選択した場合にのみ使用できます。スイッチ側の設定が一致する必要があります。MACsec 256 暗号化規格を有効にすることによって、MACsec Key Agreement (MKA)を使用した802.1AE 暗号化は、MACsec 対応デバイスとホストデバイス間の暗号化用にダウンリンク ポートでサポートされています。

詳細については、「Identity-Based Networking Services: MAC Security」を参照してください。

ポート認証例外ポリシーペイン

このペインは、有線ネットワークでのみ表示されます。

[ポート認証例外ポリシー(Port Authentication Exception Policy)]ペインでは、認証プロセス中のIEEE 802.1X サプリカントの動作を変更できます。ポート例外が有効でない場合、サプリカントはその既存の動作を続け、設定が完全に成功した場合のみ(または、この項で前述したように、オーセンティケータからの応答がない状態でmaxStarts数の認証が開始された後に)ポートを開きます。次のいずれかのオプションを選択します。

- [認証前にデータ トラフィックを許可 (Allow data traffic before authentication)]:認証試行 の前にデータ トラフィックが許可されます。
- [次の場合でも認証後にデータトラフィックを許可(Allow data traffic after authentication even if)]:次の場合でもデータトラフィックが許可されます。
 - •[EAP 失敗(EAP Fails)]:選択すると、EAP が失敗した場合でも、サプリカントは認 証を試行します。認証に失敗した場合、サプリカントは認証に失敗したにもかかわら ず、データトラフィックを許可します。
 - •[EAP は成功したがキー管理に失敗(EAP succeeds but key management fails)]: 選択す ると、EAPは成功してキー管理が失敗した場合、サプリカントはキーサーバとのキー のネゴシエートを試行しますが、何らかの理由によりキーネゴシエーションに失敗し た場合でもデータトラフィックを許可します。この設定は、キー管理が設定されてい る場合のみ有効です。キー管理がなしに設定されている場合、このチェックボックス は淡色表示されます。

C)

制約事項 MACsec には、ACS バージョン 5.1 以降および MACsec 対応スイッチが必要です。ACS または スイッチの設定については、『Catalyst 3750-X and 3560-X Switch Software Configuration Guide』 [英語] を参照してください。

アソシエーション モード

このペインは、ワイヤレスネットワークの場合にのみ表示されます。

アソシエーション モードを選択します。

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA2 Enterprise (TKIP)
- WPA2 Enterprise (AES)
- CCKM(TKIP): (Cisco CB21AG ワイヤレス NIC が必要)
- CCKM(AES): (Cisco CB21AG ワイヤレス NIC が必要)

オープン ネットワークの設定

オープンネットワークは、認証や暗号化を使用しません。オープン(非セキュア)ネットワー クを作成するには、次の手順を実行します。

- ステップ1 [セキュリティレベル (Security Level)] ページで [オープン ネットワーク (Open Network)]を選択しま す。この選択肢では、最もセキュリティレベルの低いネットワークが提供されます。これは、ゲストアク セス ワイヤレス ネットワークに推奨されています。
- **ステップ2** [次へ (Next)] をクリックします。
- ステップ3 接続タイプを決定します。

Wi-Fi (ワイヤレス) 設定ペインで、[WPA3 オープン (WPA3 Open)] (OWE とも呼ばれる) チェックボッ クスを選択できます。

共有キー ネットワークの設定

Wi-Fiネットワークは、エンドポイントとネットワークアクセスポイント間のデータを暗号化 する際に使用される暗号キーを導出するために、共有キーを使用することがあります。WPA または WPA2 Personal、WPA3 Personal を備えた共有キーを使用すると、小規模オフィスや自 宅オフィスに適した Medium レベルのセキュリティクラスが実現します。



(注) 共有キーによるセキュリティは、企業ワイヤレスネットワークには推奨しません。

セキュリティレベルを共有キーネットワークにする場合は、次の手順を実行します。

- ステップ1 [共有キーネットワーク(Shared Key Network)] を選択します。
- ステップ2 [セキュリティレベル (Security Level)]ウィンドウで [次へ (Next)]をクリックします。
- **ステップ3** [ユーザ接続(User Connection)] または [マシン接続(Machine Connection)] を指定します。
- ステップ4 [次へ (Next)]をクリックします。
- ステップ5 [共有キータイプ (Shared Key Type)]: 共有キーのタイプを決定する共有キーアソシエーションモードを 指定します。次の選択肢があります。
 - [WEP]: スタティック WEP 暗号化とのレガシー IEEE 802.11 オープン システム アソシエーション。
 - [Shared]: スタティック WEP 暗号化とのレガシー IEEE 802.11 共有キー アソシエーション。
 - [WPA/WPA2 Personal]: パスフレーズ事前共有キー(PSK)から暗号キーを導出する Wi-Fi セキュリ ティプロトコル。
 - WPA3 Personal (SAE とも呼ばれます)

- ステップ6 レガシー IEEE 802.11 WEP または共有キーを選択した場合は、40 ビット、64 ビット、104 ビット、または 128 ビットを選択します。40 または 64 ビットの WEP キーは、5 個の ASCII 文字または 10 桁の 16 進数で ある必要があります。104 または 128 ビットの WEP キーは、13 個の ASCII 文字または 26 桁の 16 進数で ある必要があります。
- ステップ7 WPA または WPA2 Personal を選択した場合は、(TKIP/AES)を使用する暗号化のタイプを選択し、共有 キーを入力します。入力するキーは、8 ~ 63 個の ASCII 文字またはちょうど 64 桁の 16 進数である必要が あります。共有キーが ASCII 文字で構成されている場合は、[ASCII]を選択します。共有キーに 64 桁の 16 進数が含まれている場合は、[16進数(Hexadecimal)]を選択します。
- ステップ8 [完了 (Done)] をクリックします。[OK] をクリックします。

MAC アドレスのランダム化の有効化

Windows 10 以降でのみ、サポートするハードウェアまたはドライバーの MAC アドレスのラン ダム化を有効にすることができます。Windows は、プローブ要求またはネットワークへの接続 にランダムアドレスを使用します。ネットワークごとのアドレスは、クライアントが特定の ネットワークに接続するときに常に同じアドレスを使用するように計算されます。接続を忘れ て再接続すると、新しい MAC アドレスが割り当てられます。

- クライアントポリシーで許可されている場合は、ネットワーク、セキュリティレベルページ (14ページ)の[MACアドレスのランダム化を有効にする (Enable MAC Address Randomization)]チェックボックスをオンにします。有効にすると、各ワイヤレスネット ワークはランダムな MAC アドレスを使用します。この MAC アドレスは、ネットワーク がユーザー設定から削除されない限り保持されます。
- どのセキュリティレベルでも、手順1と2が完了していれば、[毎日ランダムMACアドレスを変更する(Change Random MAC Address Daily)]をチェックできます。このオプションにより、各ワイヤレスネットワークはランダムな MAC アドレスを利用でき、24時間保持されます。24時間が経過すると、新しい接続時にランダム MAC アドレスが新たに生成されます。

ネットワーク、ネットワーク接続タイプペイン

ここでは、Network Access Manager プロファイル エディタの [セキュリティ レベル (Security Level)]に続く、[ネットワーク (Networks)]ウィンドウの[ネットワーク接続タイプ (network connection type)]ペインについて説明します。次のいずれかの接続タイプを選択します。

 [マシン接続(Machine Connection)]: Windows Active Directory に保存されているデバイス 名が認証に使用されます。マシン接続は通常、接続時にユーザクレデンシャルが必要ない 場合に使用します。ユーザがログオフし、ユーザクレデンシャルが使用できない場合で も、エンドステーションがネットワークにログインする必要がある場合にこのオプション を選択します。このオプションは通常、ユーザがアクセスする前に、ドメインに接続し、 ネットワークから GPO および他のアップデートを取得する場合に使用します。



 (注) 既知のネットワークが使用できない場合、Cisco Secure Client Start Before Login (SBL) は失敗します。SBLモードで許可されるネッ トワーク プロファイルには、非 802-1X 認証モードを採用するす べてのメディア タイプ (オープン WEP、WPA/WPA2 パーソナ ル、および静的キー (WEP) ネットワークなど)が含まれます。 Network Access Managerを [ユーザがログインする前 (Before User Logon)]に、およびマシン接続認証用に設定している場合、 Network Access Managerはユーザにネットワーク情報を要求し、 VPN SBL は正常に行われます。

• [ユーザ接続(User Connection)]: ユーザクレデンシャルを認証に使用します。

[クライアントポリシー(Client Policy)]ペインで[ユーザがログインする前(Before User Logon)]が選択されている場合、Windowsスタート画面でユーザがログインクレデンシャルを入力した後、Network Access Managerはユーザのクレデンシャルを収集します。Windows がユーザのWindows セッションを開始している間に、ネットワーク接続が確立されます。

[クライアントポリシー(Client Policy)] ペインで [ユーザがログインした後(After User Logon)] が選択されている場合、ユーザが Windows にログインしてから、接続が開始されます。

ユーザがログオフすると、現在のユーザのネットワーク接続は終了します。マシンネット ワーク プロファイルが使用可能な場合、NAM はマシン ネットワークに再接続します。

 [マシンおよびユーザ接続(Machine and User Connection)]:[セキュリティレベル(Security Level)]ペインで選択したように、[認証ネットワーク(Authenticating Network)]を設定 している場合にのみ指定できます。マシン ID とユーザ クレデンシャルの両方を使用しま すが、マシン部分はユーザがデバイスにログインしていない場合のみ有効です。2つの部 分の設定は同じですが、マシン接続の認証タイプとクレデンシャルは、ユーザ接続の認証 タイプとクレデンシャルと異なる場合があります。

マシン接続を使用していてユーザがログインしていないとき、およびユーザ接続を使用していてユーザがログインしているときにネットワークに PC を常時接続するには、このオプションを選択します。

EAP-FAST が (次のペインで) EAP 方式として設定されている場合、EAP チェーンがサ ポートされています。つまり、Network Access Managerによって、マシンおよびユーザが 既知のエンティティであり、企業によって管理されていることが検証されます。

このネットワーク接続タイプを選択すると、[ネットワーク(Networks)]ダイアログに追加のタブが表示されます。これらのタブでは、選択されたネットワーク接続タイプのEAP 方式とクレデンシャルを設定できます。

ネットワーク、ユーザまたはマシンの認証ページ

ネットワーク接続タイプを選択した後、それらの接続タイプの認証方式を選択します。認証方 式を選択した後、選択した方式に対応するように表示が更新され、追加情報を提供するように 要求されます。



(注) MACsec を有効にした場合は、PEAP、EAP-TLS、または EAP-FAST などの MSK キー派生をサ ポートする EAP 方式を必ず選択します。また、MACsec が有効でない場合にも、Network Access Managerを使用すると、MACsec を考慮して MTU が 1500 から 1468 に削減されます。

EAP の概要

EAP は、認証プロトコルを伝送するトランスポート プロトコルから認証プロトコルをデカッ プリングするための要件を示した IETF RFC です。このデカップリングによって、トランスポー トプロトコル (IEEE 802.1X、UDP、または RADIUS など)は、認証プロトコルを変更せずに EAP プロトコルを伝送できます。

基本的な EAP プロトコルは、次の4つのパケット タイプから構成されます。

- EAP要求:オーセンティケータは、要求パケットをサプリカントに送信します。各要求にはtypeフィールドがあり、要求されている内容を示します。これには、使用するサプリカントアイデンティティや EAP タイプなどが含まれます。シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。
- EAP応答:サプリカントは応答パケットをオーセンティケータに送信し、シーケンス番号 を使用して元の EAP 要求と照合します。EAP 応答のタイプは、通常 EAP 要求と一致しま すが、応答が負(NAK)の場合は除きます。
- EAP 成功:オーセンティケータは認証に成功した場合にサプリカントに成功パケットを送信します。
- EAP 失敗:オーセンティケータは、認証が失敗した場合、サプリカントに失敗パケットを 送信します。

EAP が IEEE 802.11X システムで使用中の場合、アクセス ポイントは EAP パススルー モード で動作します。このモードでは、アクセスポイントはコード、識別子、および長さのフィール ドを確認して、サプリカントから受信した EAP パケットを AAA サーバーに転送します。AAA サーバーオーセンティケータから受信したパケットは、サプリカントに転送されます。

EAP-GTC

EAP-GTCは、単純なユーザ名とパスワード認証に基づくEAP認証方式です。チャレンジ/レス ポンス方式を使用せずに、ユーザ名とパスワードの両方がクリアテキストで渡されます。この 方式は、トンネリング EAP 方式の内部で使用(次のトンネリング EAP 方式を参照)、または ワンタイム パスワード(OTP)を使用する場合に推奨されます。 EAP-GTCは、相互認証を提供しません。クライアントのみ認証するため、不正なサーバがユー ザのクレデンシャルを取得するおそれがあります。相互認証が必要な場合、EAP-GTC はトン ネリング EAP 方式の内部で使用され、サーバ認証を提供します。

EAP-GTCによりキー関連情報は提供されないため、MACsecではこの方式は使用できません。 さらなるトラフィック暗号化のためにキー関連情報が必要な場合、EAP-GTCはトンネリング EAP 方式の内部で使用され、キー関連情報(および必要に応じて内部および外部の EAP 方式 の暗号化バインド)を提供します。

パスワード ソースオプションには、次の2つがあります。

- [パスワードを使った認証(Authenticate using a Password)]: 十分に保護された有線環境にのみ適しています。
- •[トークンを使った認証(Authenticate using a Token)]:トークンコードまたは OTP のラ イフタイムが短い(通常約10秒)ため、より高いセキュリティを備えています。



 (注) Network Access Manager、オーセンティケータ、または EAP-GTC プロトコルのいずれもパスワードとトークンコード間を区別でき ません。これらのオプションは、Network Access Manager内のクレ デンシャルのライフタイムにのみ影響を与えます。パスワード は、ログアウトまでかそれ以降も記憶できますが、トークンコー ドは記憶できません(認証ごとにユーザがトークンコードの入力 を求められるため)。
 パスワードが認証に使用される場合、ハッシュ化パスワードを使 用するデータベースに対しての認証でこのプロトコルを使用でき ます。これは、パスワードがオーセンティケータにクリアテキス トで渡されるためです。この方式は、データベースがリークして

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) は、TLSプロトコル (RFC 2246) に基づく IEEE 802.1X EAP 認証アルゴリズムです。TLS は、X.509 デジタル証明書に基づく相互認証を使用します。 EAP-TLS メッセージ交換は、相互認証、暗号スイート ネゴシエーション、キー交換、クライ アントと認証サーバ間の検証、およびトラフィック暗号化に使用できるキー関連情報を提供し ます。

次のリストに、EAP-TLSクライアント証明書が有線およびワイヤレス接続に強固な認証を提供 できる主な理由を示します。

- •通常、ユーザが介入することなく認証が自動で実行される。
- ユーザパスワードへの依存がない。
- デジタル証明書が強固な認証保護を提供する。

いる可能性がある場合に推奨されます。

- メッセージ交換が公開キー暗号化により保護される。
- •証明書がディクショナリ攻撃の被害を受けにくい。
- 認証プロセスにより、データ暗号化および署名のための相互決定されたキーが生成される。

EAP-TLSには、次の2つのオプションが含まれています。

- [サーバ証明書の確認(Validate Server Certificate)]: サーバ証明書の検証を有効にします。
- 「高速再接続を有効にする(Enable Fast Reconnect)]: TLS セッション再開を有効にします。これにより、TLS セッションデータがクライアントとサーバの両方で保持されている限り、短縮化した TLS ハンドシェイクを使用することによってはるかに高速な再認証ができます。

(注) [スマートカードを使用するときは無効にする (Disable When Using a Smart Card)]オプションは、マシン接続認証では使用できません。

EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) は、EAP-TLS 機能を拡張する2フェーズの プロトコルです。フェーズ1では、完全なTLS セッションを実行して、フェーズ2で使用す るセッション キーを導出し、サーバとクライアント間で属性を安全にトンネリングします。 フェーズ2中では、トンネリングされた属性を使用して、多数のさまざまなメカニズムを使用 する追加認証を実行できます。

Network Access Managerは、EAP-TTLS 認証中に使用する内部および外部方式の暗号化バインド をサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要がありま す。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャック できる中間者攻撃の特殊クラスからの保護を提供します。

フェーズ2で使用できる認証メカニズムには、次のプロトコルが含まれます。

 PAP (パスワード認証プロトコル):ピアが2ウェイハンドシェイクを使用してそのアイ デンティティを証明する単純な方式を提供します。ID/パスワードペアは、認証が認めら れるか失敗するまで、ピアからオーセンティケータに繰り返し送信されます。相互認証が 必要な場合は、EAP-TTLSを設定して、フェーズ1でサーバの証明書を検証する必要があ ります。

パスワードがオーセンティケータに渡されるため、ハッシュ化パスワードを使用するデー タベースに対しての認証でこのプロトコルを使用できます。データベースがリークしてい る可能性がある場合は、この方式をお勧めします。



- (注) EAP-TTLS PAP は、トークンおよび OTP ベースの認証で使用でき ます。
 - CHAP(チャレンジハンドシェイク認証プロトコル):3 ウェイハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLSを設定して、フェーズ1でサーバの証明書を検証する必要があります。このチャレンジ/レスポンス方式を使用する場合、オーセンティケータのデータベースにクリアテキストパスワードを保存する必要があります。
 - MS-CHAP (Microsoft CHAP): 3 ウェイ ハンドシェイクを使用してピアのアイデンティ ティを検証します。相互認証が必要な場合は、EAP-TTLSを設定して、フェーズ1でサー バの証明書を検証する必要があります。パスワードのNT-hashに基づいてこのチャレンジ/ レスポンス方式を使用する場合は、オーセンティケータのデータベースにクリアテキスト パスワード、または最低でもパスワードのNT-hashのいずれかを保存しておく必要があり ます。
 - MS-CHAPv2:応答パケット内にピアチャレンジおよび成功パケット内にオーセンティケー タ応答を含めることによって、ピア間の相互認証を提供します。サーバの前に、クライア ントが認証されます。(ディクショナリ攻撃を防ぐために)サーバをクライアントの前に 認証する必要がある場合、EAP-TTLSを設定してフェーズ1でサーバの証明書を検証する 必要があります。パスワードのNT-hashに基づいてこのチャレンジ/レスポンス方式を使用 する場合は、オーセンティケータのデータベースにクリアテキストパスワード、または 最低でもパスワードのNT-hash のいずれかを保存しておく必要があります。

EAP-TTLS の設定

- EAP: 次の EAP 方法の使用を許可します。
 - EAP-MD5(EAP Message Digest 5): 3 ウェイ ハンドシェイクを使用してピアのアイ デンティティを検証します(CHAPと類似)。このチャレンジ/レスポンス方式を使用 する場合、オーセンティケータのデータベースにクリア テキストパスワードを保存 する必要があります。
 - EAP-MSCHAPv2:3 ウェイハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。(ディクショナリ攻撃の防止のためなどで)サーバをクライアントの前に認証する必要がある場合、EAP-TTLSを設定してフェーズ1でサーバの証明書を検証する必要があります。パスワードのNT-hashに基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードのNT-hashのいずれかを保存しておく必要があります。
- EAP-TTLS 設定
 - [サーバーIDの検証(Validate Server Identity)]:サーバー証明書の検証を有効にします。



- (注) これを有効にする場合は、RADIUS サーバーにインストールされ たサーバー証明書にサーバー認証の拡張キーの使用状況(EKU) が含まれていることを確認します。RADIUS サーバーでは、認証 時にクライアントにその設定済みの証明書を送信するとき、ネッ トワークアクセスおよび認証のためにこのサーバ認証設定が必要 です。
 - •[高速再接続を有効にする(Enable Fast Reconnect)]: 内部認証が省略されるかどう か、またはオーセンティケータによって制御されているかどうかに関係なく、外部 TLS セッション再開のみを有効にします。

- (注) [スマートカードを使用するときは無効にする (Disable When Using a Smart Card)]は、マシン接続認証では使用できません。
 - [内部方式(Inner Methods)]: TLSトンネルが作成された後で内部方式の使用を指定します。Wi-Fiメディアタイプにのみ使用できます。

PEAP オプション

Protected EAP (PEAP) は、トンネリング TLS ベースの EAP 方式です。PEAP は、内部認証方 式の暗号化に対するクライアント認証の前に、サーバ認証にTLSを使用します。内部認証は、 信頼される暗号保護されたトンネル内部で実行され、証明書、トークン、およびパスワードを 含む、さまざまな内部認証方式をサポートします。Network Access Managerは、PEAP 認証中に 使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な 場合は、EAP-FASTを使用する必要があります。暗号化バインドは、クレデンシャルを知らな くても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供 します。

PEAP は、次のサービスを提供することによって EAP 方式を保護します。

- EAP パケットに対する TLS トンネル作成
- メッセージ認証
- •メッセージの暗号化
- •クライアントに対するサーバの認証

次の認証方式を使用できます。

- •パスワードを使った認証
 - EAP-MSCHAPv2:3ウェイハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。(ディクショナリ攻撃の防止のためなどで)サーバをクライアントの前に認証する必要がある場合、PEAPを設

定してサーバの証明書を検証する必要があります。パスワードのNT-hashに基づいて チャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキストパスワード、または最低でもパスワードのNT-hashのいずれかを保存してお く必要があります。

- EAP-GTC(EAP Generic Token Card): ユーザ名とパスワードを伝送するために EAP エンベロープを定義します。相互認証が必要な場合は、PEAP を設定してサーバの証 明書を検証する必要があります。パスワードがクリアテキストでオーセンティケータ に渡されるため、ハッシュ化パスワードを使用するデータベースに対しての認証でこ のプロトコルを使用できます。この方式は、データベースがリークしている可能性が ある場合に推奨されます。
- ・証明書を使った EAP-TLS
 - EAP-TLS:ユーザ証明書を伝送するために EAP エンベロープを定義します。中間者 攻撃(有効なユーザの接続のハイジャック)を避けるため、同じオーセンティケータ に対する認証用に PEAP(EAP-TLS)および EAP-TLS プロファイルを混在させないこ とをお勧めします。その設定に応じて、オーセンティケータを設定する必要がありま す(プレーンおよびトンネリングされた EAP-TLSの両方を有効にしない)。

PEAPの設定

- PEAP-EAP 設定
 - [サーバーIDの検証(Validate Server Identity)]: サーバー証明書の検証を有効にしま す。



- (注) これを有効にする場合は、RADIUS サーバーにインストールされ たサーバー証明書にサーバー認証の拡張キーの使用状況(EKU) が含まれていることを確認します。RADIUS サーバーでは、認証 時にクライアントにその設定済みの証明書を送信するとき、ネッ トワークアクセスおよび認証のためにこのサーバ認証設定が必要 です。
 - •[高速再接続を有効にする(Enable Fast Reconnect)]:外部TLSセッション再開のみを 有効にします。オーセンティケータは、内部認証を省略するかどうかを制御します。
 - [スマートカードを使用するときは無効にする(Disable When Using a Smart Card)]:
 スマートカードを使用して認証する場合に高速再接続を使用しません。スマートカードは、ユーザ接続にのみ適用されます。
 - [トークンおよび EAP-GTC を使用して認証する(Authenticate using a token and EAP-GTC)]: マシン認証には使用できません。
 - ・クレデンシャル ソースに基づく内部方式

- [パスワードを使用した認証(Authenticate using a password)]: [EAP-MSCHAPv2]または [EAP-GTC]。
- [証明書を使用した認証(Authenticate using a certificate)]: EAP-TLS に対応。
- •[トークンおよび EAP-GTC を使用して認証する(Authenticate using a token and EAP-GTC)]: マシン認証には使用できません。

(注) ユーザログインの前に、スマートカードのサポートは Windows では使用できません。

EAP-FAST 設定

EAP-FASTは、IEEE 802.1X認証タイプで、柔軟性があり、展開や管理も容易です。EAP-FAST は、さまざまなユーザーおよびパスワードデータベースタイプ、サーバ主導のパスワードの 失効と変更、およびデジタル証明書(任意)をサポートします。

EAP-FASTは、証明書を使用せず、ディクショナリ攻撃からの保護を提供する IEEE 802.1X EAP タイプを展開するお客様向けに開発されました。

マシン接続とユーザー接続の両方が設定されている場合、EAP チェーンがサポートされていま す。これは、Network Access Managerが、マシンおよびユーザーが既知のエンティティであり、 企業によって管理されていること検証することを意味し、社内ネットワークに接続している ユーザー所有資産を制御するのに便利です。EAP チェーンの詳細については、RFC 3748 を参 照してください。

EAP-FAST は、TLS メッセージを EAP 内にカプセル化します。また、次の 3 つのプロトコル フェーズから構成されます。

- Authenticated Diffie-Hellman Protocol (ADHP) を使用して Protected Access Credential (PAC) と呼ばれる共有秘密クレデンシャルを持つクライアントをプロビジョニングするプロビ ジョニング フェーズ。
- 2. トンネルの確立に PAC を使用するトンネル確立フェーズ。
- 3. 認証サーバでユーザーのクレデンシャル(トークン、ユーザー名/パスワード、またはデジ タル証明書)を認証する認証フェーズ。

他のトンネリング EAP 方式とは異なり、EAP-FAST は内部および外部方式間に暗号化バイン ドを提供して、攻撃者が有効なユーザーの接続をハイジャックする特殊な中間者攻撃を防止し ます。

EAP-FAST の設定

- EAP-FAST 設定
 - [サーバーIDの検証(Validate Server Identity)]:サーバー証明書の検証を有効にします。これを有効にすると、管理ユーティリティに2つの追加のダイアログが導入され

EAP-FAST の設定

て、Network Access Manager プロファイル エディタのタスク リストに [証明書 (Certificate)] ペインがさらに追加されます。



「高速再接続を有効にする(Enable Fast Reconnect)]:セッション再開を有効にします。EAP-FASTで認証セッションを再開する2つのメカニズムには、内部認証を再開するユーザ認可PACと、短縮化した外部TLSハンドシェイクができるTLSセッション再開があります。この[高速再接続を有効にする(Enable Fast Reconnect)]パラメータは、両方のメカニズムを有効または無効にします。オーセンティケータがいずれを使用するかを決定します。



(注) マシン PAC は、短縮化した TLS ハンドシェイクを提供し、内部
 認証を省きます。この制御は、PACパラメータを有効/無効にする
 ことによって処理します。

- (注) [スマートカードを使用するときは無効にする (Disable When Using a Smart Card)]オプションは、ユーザ接続認証にのみ使用できま す。
 - [クレデンシャルソースに基づく内部方式(Inner methods based on Credentials Source)]:パ スワードまたは証明書を使用する認証ができます。
 - 「パスワードを使用した認証(Authenticate using a password)]: [EAP-MSCHAPv2]または[EAP-GTC]。EAP-MSCHAPv2は、相互認証を提供しますが、サーバーを認証する前にクライアントを認証します。サーバーを最初に認証する相互認証を使用する場合は、EAP-FASTを認証付きプロビジョニングのみに設定して、サーバーの証明書を検証します。パスワードのNT-hashに基づいてこのチャレンジ/レスポンス方式を使用して、EAP-MSCHAPv2を使用する場合は、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードのNT-hashのいずれかを保存しておく必要があります。パスワードはEAP-GTC内でクリアテキストでオーセンティケータに渡されるため、データベースに対する認証でこのプロトコルを使用できます。
 - [証明書を使用した認証(Authenticate using a certificate)]: 証明書を使用する認証に対しての基準を、要求された場合にクライアント証明書を暗号化しないで送信、トンネ

ル内でのみクライアント証明書を送信、またはトンネル内で EAP-TLS を使用してク ライアント証明書を送信から決定します。

- ・トークンおよび EAP-GTC を使用して認証します。
- [PAC を使用する(Use PACs)]: EAP-FAST 認証での PAC の使用を指定できます。PAC は、ネットワーク認証を最適化するためにクライアントに配布されるクレデンシャルです。



(注) EAP-FASTでは大半の認証サーバーが PACを使用するため、通常 は PAC オプションを使用します。このオプションを削除する前 に、認証サーバーが EAP-FAST で PAC を使用しないことを確認 します。使用する場合は、クライアントの認証試行が失敗しま す。

LEAP 設定

LEAP (Lightweight EAP) はワイヤレス ネットワークに対応しています。拡張認証プロトコル (EAP) フレームワークに基づき、WEPよりセキュアなプロトコルを作成するためシスコによ り開発されました。

(注) 強力なパスワードおよび定期的に失効するパスワードを使用しない限り、LEAP はディクショ ナリ攻撃を受ける場合があります。認証方式がディクショナリ攻撃の被害を受けにくい EAP-FAST、PEAP、または EAP-TLS を使用することをお勧めします。

ユーザ認証にのみ使用できる LEAP 設定:

・ログオフを越えたユーザ接続の延長:ユーザがログオフしても接続は開いたままです。同じユーザが再度ネットワークにログインしても、接続はアクティブのままです。

詳細については、「Dictionary Attack on Cisco LEAP Vulnerability」を参照してください。

ネットワーク クレデンシャルの定義

[ネットワーク (Networks)]>[クレデンシャル (Credentials)] ペインで、ユーザー クレデン シャルまたはマシンクレデンシャルのいずれを使用するか指定し、信頼サーバ検証ルールを設 定します。

ユーザクレデンシャルの設定

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデ ンティティが異なる場合があります(マシン認証の次にユーザ認証が行われるなど)。たとえ ば、ピアでは最初に nouser@cisco.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエー トされると、そのピアは johndoe@cisco.com のアイデンティティを要求する場合があります。 そのため、ユーザーのアイデンティティにより保護が提供される場合でも、カンバセーション がローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

ユーザ接続で、プレースホルダ[username]および[domain]を使用する場合、次の条件が当ては まります。

- 認証にクライアント証明書を使用する場合:さまざまなX509証明書プロパティから[ユーザー名(username)]および[ドメイン(domain)]のプレースホルダ値を取得します。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@example.com(ユーザ名=userA、ドメイン=example.com)、マシン認証のアイデンティティが hostA.example.com(ユーザ名=hostA、ドメイン=example.com)の場合、次のプロパティが解析されます。
- ・ユーザー証明書ベースの認証の場合:
 - SubjectAlternativeName: UPN = userA@example.com
 - Subject = .../CN=userA@example.com/...
 - Subject = userA@eample.com
 - Subject = .../CN=userA/DC=example/DC=com/...
 - Subject = userA (no domain)
- •マシン証明書ベースの認証の場合:
 - SubjectAlternativeName: DNS = hostA.example.com
 - Subject = .../DC=hostA.example.com/...
 - Subject = .../CN=hostA.example.com/...
 - Subject = hostA.example.com
- クレデンシャルのソースがエンドユーザの場合:ユーザが入力する情報からプレースホル ダ値を取得します。
- クレデンシャルがオペレーティングシステムから取得される場合:ログイン情報からプレースホルダ値を取得します。
- ・クレデンシャルが静的である場合:プレースホルダを使用しません。

[クレデンシャル (Credentials)]ペインでは、目的のクレデンシャルを関連付けられたネット ワークの認証で使用するために指定できます。

- **ステップ1**[保護されたアイデンティティパターン(Protected Identity Pattern)]でユーザアイデンティティを定義しま す。Network Access Managerでは、次のアイデンティティプレースホルダのパターンがサポートされます。
 - [username]: ユーザー名を指定します。ユーザが username@domain または domain\username を入力した 場合、ドメインの部分は削除されます。

- [raw]: ユーザーの入力のとおりにユーザー名を指定します。
- [domain]: ユーザデバイスのドメインを指定します。
- **ステップ2** 一般的な、保護されていないアイデンティティ パターンを指定します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイ デンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の 対象になります。

- anonymous@[domain]:値がクリアテキストで送信されるときに、ユーザアイデンティティを隠すために、トンネリングされた方式内でよく使用されます。実際のユーザアイデンティティは、保護されたアイデンティティとして、内部方式で提供されます。
- [username]@[domain]: トンネリングされていない方式の場合。
 - (注) 保護されていないアイデンティティ情報はクリアテキストで送信されます。最初のクリア テキストアイデンティティ要求または応答が改ざんされた場合は、TLS セッションが確立 されるとサーバがアイデンティティを検証できないことを検出することがあります。たと えば、ユーザ ID が無効であるか、または EAP サーバが処理する領域内にない場合があり ます。
- **ステップ3**保護されるアイデンティティパターンを指定します。

ユーザー ID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングを有効にするために必要な情報のみを指定する場合があります。

- [username]@[domain]
- ユーザのアイデンティティとして使用する実際の文字列(プレースホルダなし)

ステップ4 次のユーザクレデンシャル情報をさらに提供します。

- 「シングル サインオン クレデンシャルを使用(Use Single Sign On Credentials)]: クレデンシャルをオペレーティング システムのログイン情報から取得します。ログイン クレデンシャルが失敗すると、Network Access Managerは一時的に(次のログインまで)切り替わり、ユーザに GUI でクレデンシャルの入力を求めます。
 - (注) Network Access Manager および SSO で、Windows ログイン クレデンシャルを自動的に使用 することはできません。Network Access Managerで SSO を使用するには、ログオン クレデ ンシャルを代行受信する必要があります。したがって、インストールまたはログオフの後 に再起動を求められます。
- [スタティッククレデンシャルを使用(Use Static Credentials)]: ユーザクレデンシャルをこのプロファ イルエディタが提供するネットワーク プロファイルから取得します。スタティック クレデンシャル が失敗すると、Network Access Managerは、新しい設定がロードされるまでクレデンシャルを再度使用 しません。
 - (注) アンパサンドはこのフィールドで無効な文字です。

- [クレデンシャルのプロンプト(Prompt for Credentials)]: クレデンシャルを次に指定されたとおりに Cisco Secure Client GUI を使用してエンドユーザーから取得します。
 - 「永久に記憶(Remember Forever)]: クレデンシャルは永久に記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。クレデンシャルはファイルに保存され、ローカルマシンパスワードを使用して暗号化されます。
 - 「ユーザのログイン中記憶(Remember while User is Logged On)]: クレデンシャルはユーザがログ オフするまで記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャル の入力を再度求められます。
 - [記憶しない(Never Remember)]: クレデンシャルは一切記憶されません。Network Access Manager は、認証のためにクレデンシャル情報が必要なたびに、ユーザに入力を求めます。

ステップ5 証明書が要求されたときに、認証のためにいずれの証明書ソースを使用するかを決定します。

- [スマートカードまたは OS 証明書(Smart Card or OS certificates)]: Network Access Managerは、OS の 証明書ストアまたはスマートカードで検出される証明書を使用します。
- •[スマートカード証明書のみ(Smart Card certificates only)]: Network Access Managerは、スマートカードで検出される証明書のみを使用します。
- ステップ6 [スマートカード PIN を記憶(Remember Smart Card Pin)] パラメータでは、Network Access Managerがス マートカードから証明書を取得するために使用した PIN を記憶する期間を決定します。使用できるオプ ションについては、ステップ2を参照してください。
 - (注) PIN は、証明書自体よりも長く保存されることは決してありません。

別名 Cryptographic Service Provider (CSP) および Key Storage Provider (KSP) というスマート カードのチップとドライバによっては、他より接続に時間がかかるスマート カードもありま す。接続タイムアウトを長くすると、ネットワークにスマートカードベースの認証を実行する のに十分な時間を与えることができます。

マシンクレデンシャルの設定

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデ ンティティが異なる場合があります(マシン認証の次にユーザ認証が行われるなど)。たとえ ば、ピアでは最初に nouser@example.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシ エートされると、そのピアは johndoe@example.com のアイデンティティを要求する場合があり ます。そのため、ユーザーのアイデンティティにより保護が提供される場合でも、カンバセー ションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

マシン接続の場合に、[ユーザー名(username)]および[ドメイン(domain)]プレースホルダ が使用されたときは、常に次の条件が適用されます。

 認証にクライアント証明書を使用する場合:さまざまなX509証明書プロパティから[ユー ザー名(username)]および[ドメイン(domain)]のプレースホルダ値を取得します。プ ロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデ ンティティが userA@cisco.com(ユーザー名 =userA、ドメイン =cisco.com)、マシン認証 のアイデンティティが hostA.cisco.com(ユーザー名 =hostA、ドメイン =cisco.com)の場 合、次のプロパティが解析されます。

- ・ユーザー証明書ベースの認証の場合:
 - SubjectAlternativeName: UPN = userA@example.com
 - Subject = .../CN=userA@example.com/...
 - Subject = userA@example.com
 - Subject = .../CN=userA/DC=example.com/...
 - Subject = userA (no domain)
- ・マシン証明書ベースの認証の場合:
 - SubjectAlternativeName: DNS = hostA.example.com
 - Subject = .../DC=hostA.example.com/...
 - Subject = .../CN=hostA.example.com/...
 - Subject = hostA.example.com
- クライアント証明書が認証に使用されない場合:クレデンシャルをオペレーティングシス テムから取得し、[ユーザー名(username)]プレースホルダは割り当てられたマシン名を 表します。
- [クレデンシャル (Credentials)]パネルでは、目的のマシン クレデンシャルを指定できます。
- ステップ1 [保護されているアイデンティティパターン (Protected Identity Pattern)]でマシンアイデンティティを定義 します。Network Access Managerでは、次のアイデンティティプレースホルダのパターンがサポートされま す。
 - [username]: ユーザー名を指定します。ユーザーが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
 - [raw]: ユーザーの入力のとおりにユーザー名を指定します。
 - •[domain]: ユーザーの PC のドメインを指定します。
- ステップ2 典型的な保護されていないマシン アイデンティティのパターンを定義します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイ デンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の 対象になります。

- host/anonymous@[domain]
- マシンのアイデンティティとして送信する実際の文字列(プレースホルダなし)

ステップ3保護されているマシンアイデンティティのパターンを定義します。

ユーザー ID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正し い領域へのルーティングを有効にするために必要な情報のみを指定する場合があります。典型的な保護さ れているマシン アイデンティティのパターンは次のとおりです。

- host/[username]@[domain]
- ・マシンのアイデンティティとして使用する実際の文字列(プレースホルダなし)
- ステップ4 次のマシン クレデンシャル情報をさらに提供します。
 - [マシン クレデンシャルを使用(Use Machine Credentials)]: クレデンシャルをオペレーティング シス テムから取得します。
 - [スタティック クレデンシャルを使用(Use Static Credentials)]:展開ファイルに送信する実際のスタ ティックパスワードを指定します。スタティッククレデンシャルは、証明書ベースの認証には適用さ れません。

適切な証明書を選択するための Network Access Manager の設定

クライアント認証時に2つの証明書が存在する場合、Network Access Managerは証明書の属性 に基づいて最適な証明書を自動的に選択します。優先する証明書の条件は顧客によって異なる ため、次に示す証明書の選択を定義するフィールドを設定し、また証明書選択をオーバーライ ドするルールを指定する必要があります。

複数の証明書が同一ルールに一致するか、ルールに一致する証明書がない場合は、ACEエンジンが、証明書の優先順位を指定するアルゴリズムを実行し、特定の基準(秘密キーがあるかどうか、マシンストアからの証明書であるかどうかなど)に基づいて証明書を選択します。複数の証明書の優先順位が同一の場合、ACEエンジンはその優先順位で最初に検出した証明書を選択します。

- ステップ1 Cisco Secure Client プロファイルエディタから [ネットワーク (Networks)] タブを選択します。
- ステップ2 編集するネットワークを選択します。
- ステップ3 [マシンクレデンシャル (Machine Credentials)] タブを選択します。
- ステップ4 ページ下部で [証明書一致ルールを使用する (Use Certificate Matching Rule)]を選択します。
- ステップ5 [証明書フィールド(Certificate Field)] ドロップダウンメニューから、検索条件として使用するフィール ドを選択します。
- ステップ6 [一致(Match)] ドロップダウン メニューから、検索にフィールドの完全一致([等しい(Equals)]) また は部分一致([含む(Includes)]) を含めるかどうかを指定します。
- ステップ7 [値(Value)]フィールドに、証明書の検索条件を入力します。

信頼サーバ検証ルールの設定

[サーバ ID の検証(Validate Server Identity)]オプションが [EAP] 方式に設定されている場合、 [証明書(Certificate)]パネルが有効になって証明書サーバまたは認証局に対する検証ルールを 設定できます。検証の結果によって、証明書サーバまたは認証局が信頼されるかどうかが決定 されます。

証明書サーバの検証ルールを定義するには、次の手順を実行します。

- **ステップ1** オプション設定が[証明書フィールド(Certificate Field)]および[一致(Match)]カラムに表示されたとき に、ドロップダウン矢印をクリックし、目的の設定を選択します。
- ステップ2 [値 (Value)] フィールドに、値を入力します。
- ステップ3 ルールの下で [追加 (Add)] をクリックします。
- **ステップ4** [証明書信頼済み認証局(Certificate Trusted Authority)] ペインで、次のいずれかのオプションを選択します。
 - [OS にインストールされたすべてのルート認証局(CA)を信頼(Trust any Root Certificate Authority (CA) Installed on the OS)]:選択すると、ローカルマシンまたは証明書ストアのみがサーバの証明書チェーン検証の対象になります。
 - •[ルート認証局(CA)証明書を含める(Include Root Certificate Authority (CA) Certificates)]。
 - (注) [ルート認証局(CA)証明書を含める(Include Root Certificate Authority (CA) Certificates)]
 を選択した場合は、[追加(Add)]をクリックしてCA証明書を設定にインポートする必要があります。使用している証明書がWindows 証明書ストアからエクスポートされる場合は、[Base 64 encoded X.509 (.cer)]オプションを使用します。

ネットワーク グループ ウィンドウ

[ネットワーク グループ(Network Groups)] ウィンドウで、ネットワーク接続を特定のグルー プに割り当てます。接続をグループに分類することにより、次の複数の利点がもたらされま す。

- ・接続の確立試行時のユーザエクスペリエンスの向上。複数の非表示ネットワークが設定された場合、接続が正常に確立するまで、クライアントは非表示ネットワークのリストを定義された順序で順を追って調べます。このような場合に、接続を確立するために必要な時間を大幅に短縮するためにグループが使用されます。
- ・設定された接続の管理の簡略化。企業内で複数の役割を持つ(または同じ領域に頻繁にア クセスする)ユーザがグループ内のネットワークを調整して選択可能なネットワークのリ ストを管理しやすくする場合に、管理者ネットワークをユーザネットワークから分離でき ます。

配布パッケージの一部として定義されたネットワークはロックされています。これは、ユーザ が設定を編集することや、ネットワーク プロファイルを削除することを防止するためです。

ネットワークをグローバルとして定義できます。グローバルとして定義すると、ネットワーク は[グローバルネットワーク(Global Networks)]セクションに表示されます。このセクショ ンは、有線とワイヤレスネットワークタイプの間で分割されます。このタイプのネットワー クに対しては、ソート順序の編集のみを実行できます。

すべての非グローバルネットワークは、グループ内に存在する必要があります。1つのグルー プがデフォルトで作成されています。すべてのネットワークがグローバルの場合にそのグルー プを削除できます。

- ステップ1 ドロップダウン リストからグループを選択します。
- ステップ2 [ネットワークの作成 (Create networks)]を選択して、エンドユーザがこのグループ内にネットワークを 作成できるようにします。これをオフにした場合、展開されたときにNetwork Access Managerはこのグルー プからユーザ作成ネットワークをすべて削除します。これにより、ユーザがネットワーク設定を別のグルー プに再入力する必要が生じることがあります。
- ステップ3 [スキャンリストの表示 (See scan list)]を選択して、Cisco Secure Client GUI を使用してグループがアクティ ブグループとして選択されたときに、エンドユーザーがスキャンリストを表示できるようにします。また は、このチェックボックスをオフにして、ユーザによるスキャンリストの表示を制限します。たとえば、 ユーザが近くのデバイスに誤って接続することを防ぐ必要がある場合に、スキャンリストへのアクセスを 制限します。
 - (注) これらの設定は、グループごとに適用されます。
- ステップ4 右矢印および左矢印を使用して、[グループ(Group)]ドロップダウン リストから選択したグループに対してネットワークを挿入または削除します。ネットワークが現在のグループから移動された場合は、デフォルトグループに配置されます。デフォルトグループを編集する場合、デフォルトグループからネットワークを移動できません([>]ボタンを使用)。
 - (注) 指定のネットワーク内で、各ネットワークの表示名は一意である必要があります。このため、 1つのグループには同じ表示名を持つ2つ以上のネットワークを含められません。
- **ステップ5** 上矢印および下矢印を使用してグループ内のネットワークの優先順位を変更します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。