ワイヤレスLANコントローラおよびIdentity Services Engineを使用したEAP-FAST認証

内容

概要

このドキュメントでは、外部 RADIUS サーバで使用する拡張認証プロトコル（EAP）Flexible Authentication via Secure Tunneling（FAST）認証のためにワイヤレス LAN コントローラ（WLC）を設定する方法について説明します。この設定例では、ワイヤレスクライアントを認証するために、外部RADIUSサーバとしてIdentity Services Engine(ISE)を使用します。

このドキュメントでは、ワイヤレスクライアントに対する匿名および認証済みのインバンド(Automatic)保護アクセスクレデンシャル(PAC)プロビジョニング用にISEを設定する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Lightweight アクセス ポイント（LAP）および Cisco WLC の設定に関する基礎知識
- CAPWAPプロトコルに関する基礎知識
- Cisco ISEなどの外部RADIUSサーバの設定方法に関する知識
- 一般的な EAP フレームワークに関する実践的な知識
- MS-CHAPv2 および EAP-GTC などのセキュリティ プロトコルに関する基本的な知識、デジタル証明書に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア リリース 8.8.111.0 が稼働する Cisco 5520 シリーズ WLCCisco 4800 シリーズ APAnyConnect NAM.Cisco Secure ISE バージョン 2.3.0.298Cisco 2950 シリーズ スイッチバージョン 15.2(4)E1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

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

背景説明

EAP-FASTプロトコルは、強力なパスワードポリシーを適用できない802.1X EAPの種類をデジタル証明書を必要としない802.1X EAPの導入をシスコがサポートするために開発した、一般アクセスのIEEE 802.1X EAPタイプです。

EAP-FAST プロトコルは、Transport Level Security（TLS）トンネルで EAP トランザクションを暗号化するクライアント サーバ型のセキュリティ アーキテクチャです。EAP-FAST トンネルは、ユーザに固有な強力なシークレットに基づいて確立されます。これらの強力な秘密はPACと呼ばれ、ISEのみが認識するマスターキーを使用してISEが生成します。

EAP-FAST は 3 つのフェーズで実行されます。

- **フェーズ 0（自動 PAC プロビジョニング フェーズ）：EAP-FAST フェーズ 0 は、オプション フェーズで、ネットワーク アクセスを要求するユーザのために EAP-FAST エンドユーザ クライアントに PAC を提供するトンネル セキュア方法です。エンドユーザ クライアントに PAC を提供することが、フェーズ 0 の唯一の目的です。注：フェーズ**ゼロはオプションです。これは、フェーズ0を使用する代わりに、PACを手動でクライアントにプロビジョニングできるためです。詳細については、このドキュメントの「PAC プロビジョニング モード」を参照してください。
- **フェーズ1**：フェーズ1では、ISEとエンドユーザクライアントが、ユーザのPACクレデンシ

ャルに基づいてTLSトンネルを確立します。このフェーズでは、ネットワーク アクセスの取得を試行するユーザ用の PAC がエンドユーザ クライアントに提供されていることと、期限の切れていないマスター キーに PAC が基づいていることが必要です。EAP-FAST のフェーズ 1 ではネットワーク サービスは有効になりません。
- **フェーズ 2：フェーズ 2 では、ユーザ認証クレデンシャルが、TLS 内で EAP-FAST によりサポートされる内部 EAP 方式を使用して、クライアントと RADIUS サーバ間の PAC を使用して作成された RADIUS に安全に渡されます。**内部 EAP 方式として EAP-GTC、TLS および MS-CHAP がサポートされています。その他の EAP タイプは EAP-FAST ではサポートされていません。

詳細は、『EAP-FAST の動作の仕組み』を参照してください。

PAC

PACは、ISEとEAP-FASTエンドユーザクライアントが相互に認証し、EAP-FASTフェーズ2で使用するTLSトンネルを確立できるようにする強力な共有秘密です。ISEは、アクティブなマスターキーとユーザ名を使用してPACを生成します。

PAC は、次のもので構成されています。

- **PAC-Key：クライアント (およびクライアント デバイス) とサーバの ID にバインドされている共有秘密情報。**
- **PAC Opaque：クライアントがキャッシュしてサーバに渡す暗号化されたフィールド。**サーバは、PAC-Key およびクライアント ID を復号化して、クライアントとの相互認証を行います。
- **PAC-Info：クライアントがさまざまな PAC をキャッシュできるように、少なくともサーバの ID が含まれています。**PAC の有効期限などの情報が含まれていることもあります。

PAC プロビジョニング モード

前述のように、フェーズ 0 はオプション フェーズです。

EAP-FAST は、PAC でクライアントをプロビジョニングする 2 つのオプションを提供します。

- **自動 PAC プロビジョニング (EAP-FAST フェーズ 0 またはインバンド PAC プロビジョニング)**
- **手動 (アウトオブバンド) PAC プロビジョニング**

インバンド/自動 PAC プロビジョニングは、セキュア ネットワーク接続を介して新規 PAC をエンドユーザ クライアントに送信します。自動PACプロビジョニングをサポートするようにISEとエンドユーザクライアントを設定する場合、ネットワークユーザまたはISE管理者の介入は必要ありません。

最新の EAP-FAST バージョンは、次に示す 2 種類のインバンド PAC プロビジョニング設定オプションをサポートします。

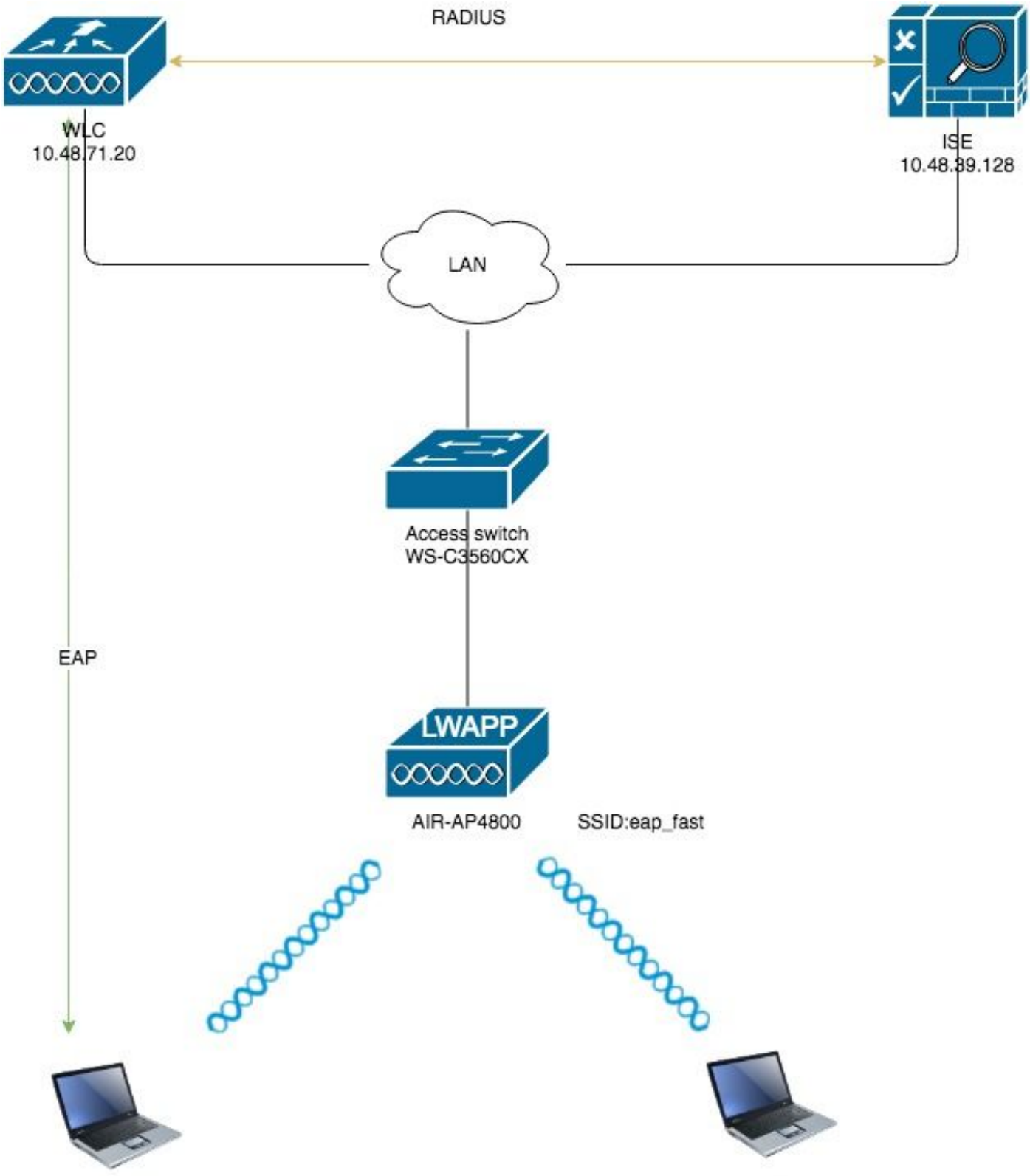
- **匿名インバンド PAC プロビジョニング**
- **認証付きインバンド PAC プロビジョニング**

注：このドキュメントでは、これらのインバンドPACプロビジョニング方法とその設定方法について説明します。

アウトオブバンド/手動PACプロビジョニングでは、ISE管理者がPACファイルを生成する必要があります。生成したファイルは、該当するネットワークユーザに配布する必要があります。ユーザは PAC ファイルでエンドユーザ クライアントを設定する必要があります。

設定

ネットワーク図



設定

EAP-FAST 認証用の WLC の設定

WLC の EAP-FAST 認証を設定するには、次の手順を実行します。

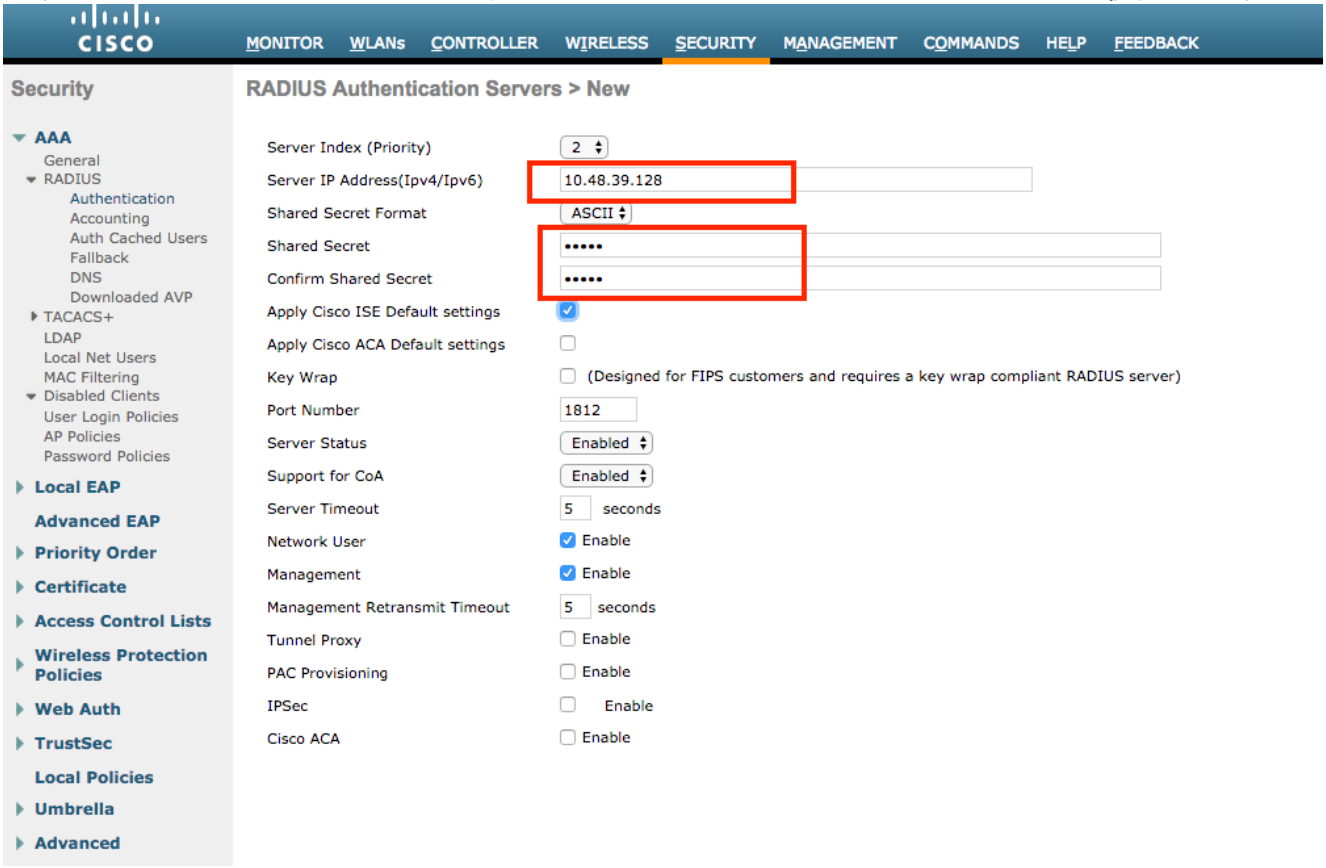
1. 外部 RADIUS サーバによる RADIUS 認証用の WLC の設定
2. EAP-FAST 認証用の WLAN を設定する

外部 RADIUS サーバによる RADIUS 認証用の WLC の設定

ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります。そうすると、外部 RADIUS サーバは、EAP-FAST を使用してユーザのクレデンシャルを検証し、ワイヤレス クライアントにアクセス権を付与します。

外部 RADIUS サーバ用に WLC を設定するには、次の手順を実行します。

1. コントローラの GUI から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サーバを定義します。
2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義します。次のパラメータがあります。RADIUS サーバの IP アドレス共有秘密ポート番号サーバ ステータスこのドキュメントでは、IPアドレスが10.48.39.128のISEサーバを使用します。



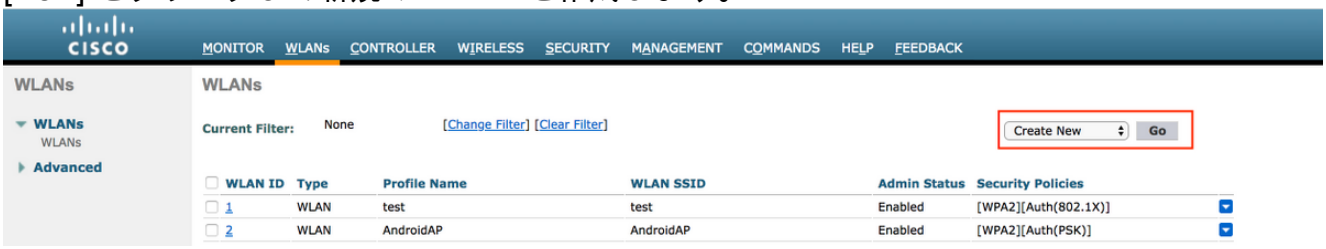
3. クリック **Apply**.

EAP-FAST 認証用の WLAN を設定する

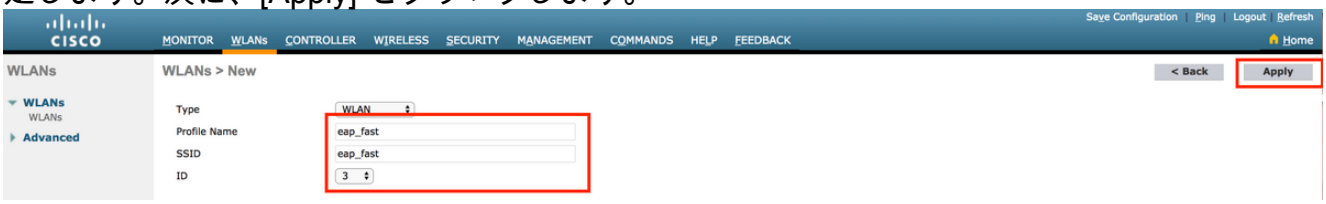
次に、EAP-FAST 認証のためにワイヤレス ネットワークに接続するときにクライアントが使用する WLAN を設定し、ダイナミック インターフェイスに割り当てます。この例で設定される WLAN 名は eap fast です。この例では、この WLAN を管理インターフェイスに割り当てます。

eap fast WLAN およびその関連パラメータを設定するには、次の手順を実行します。

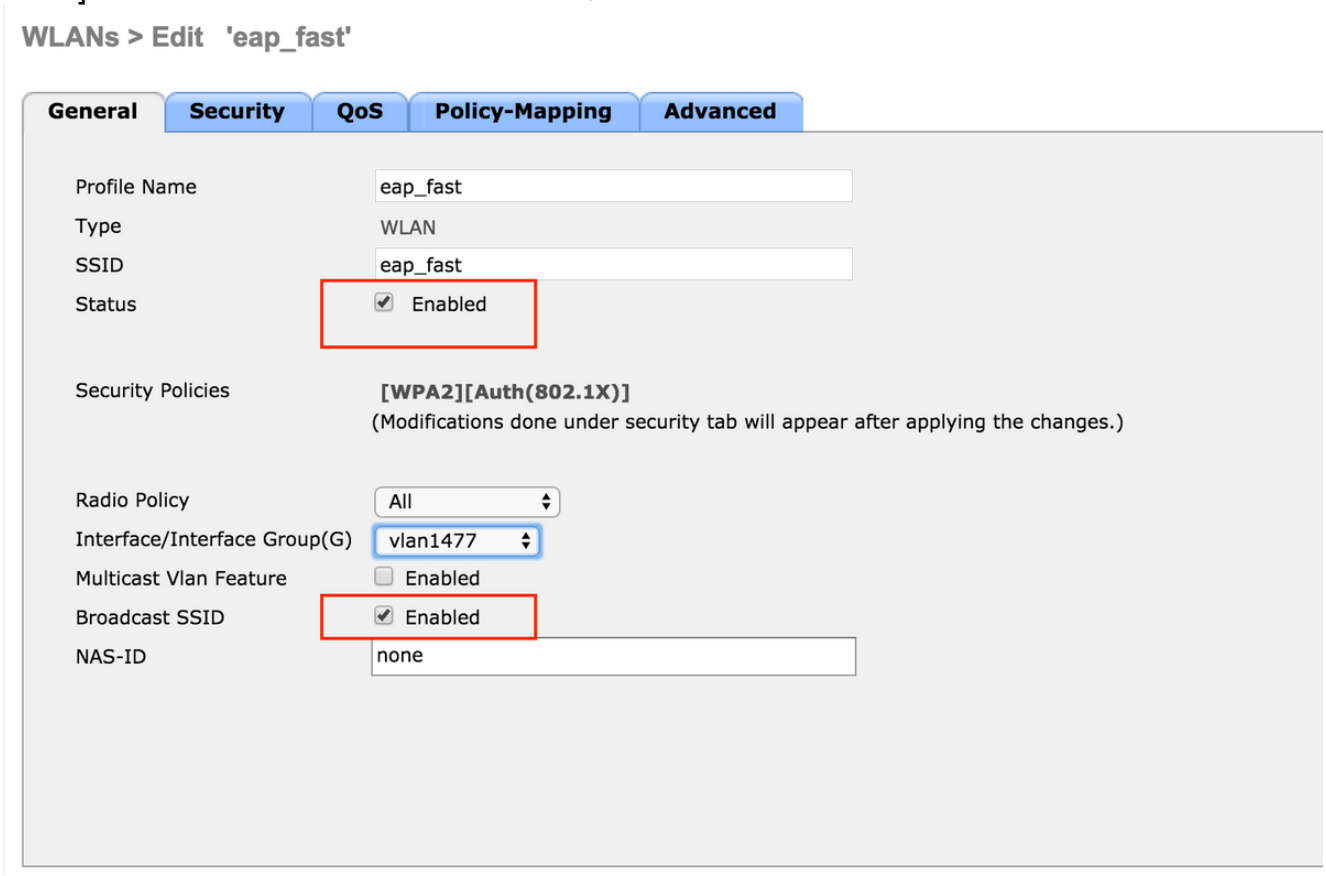
1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このページには、コントローラに存在する WLAN の一覧が表示されます。
2. [New] をクリックして新規の WLAN を作成します。



3. [WLANs] > [New]ページで**eap_fast WLAN SSID**名、プロファイル名、およびWLAN IDを設定します。次に、[Apply] をクリックします。

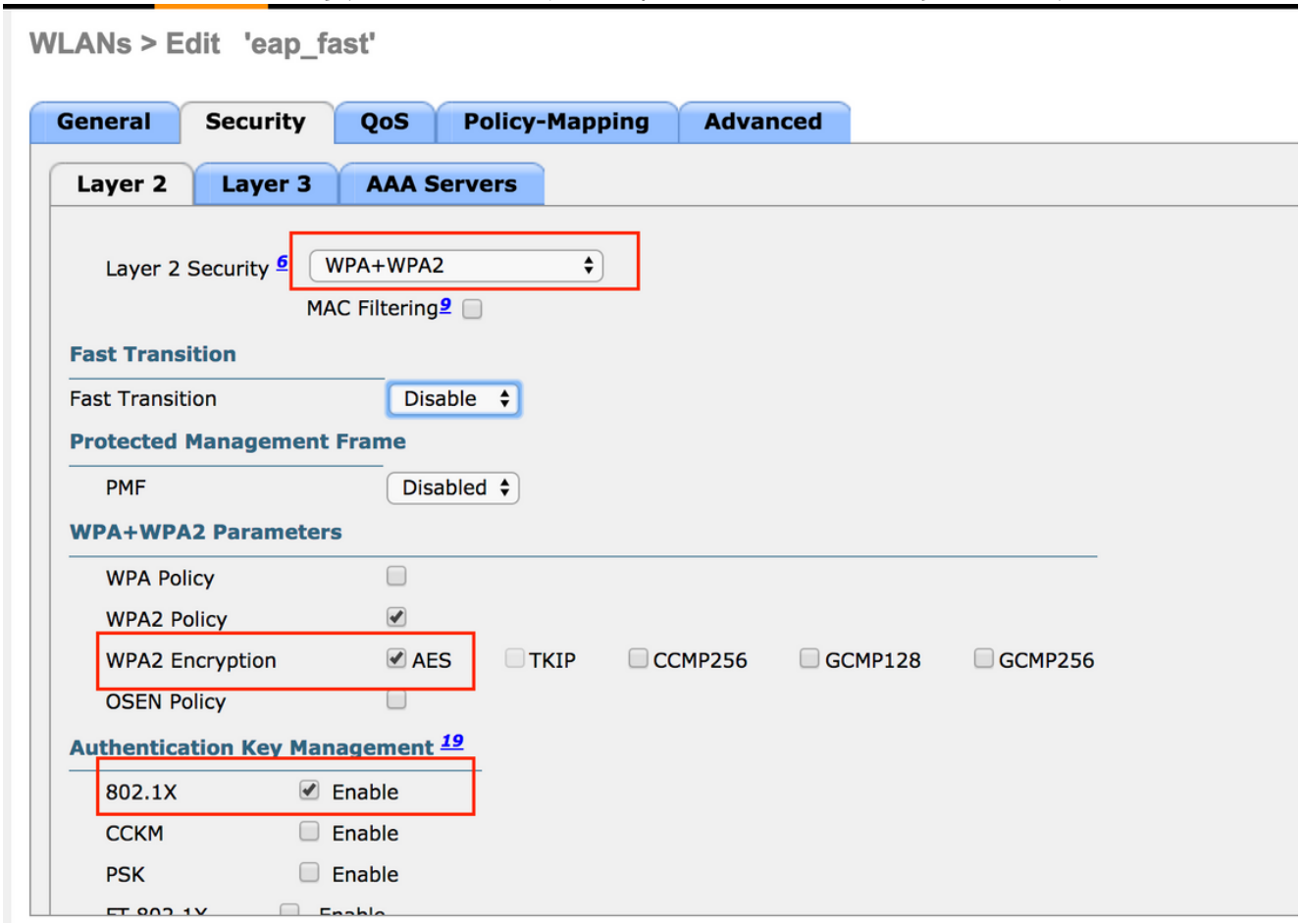


4. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されます。このページでは、その WLAN に固有のさまざまなパラメータを定義できます。このページには、[General Policies]、[RADIUS Servers]、[Security Policies]、[802.1x] パラメータがあります。
5. WLANを有効にする**には、[General Policies]**タブの**[Admin Status]**チェックボックスをオンにします。AP にビーコン フレームで SSID をブロードキャストさせる場合は、[Broadcast SSID] にチェックボックスをオンにします。

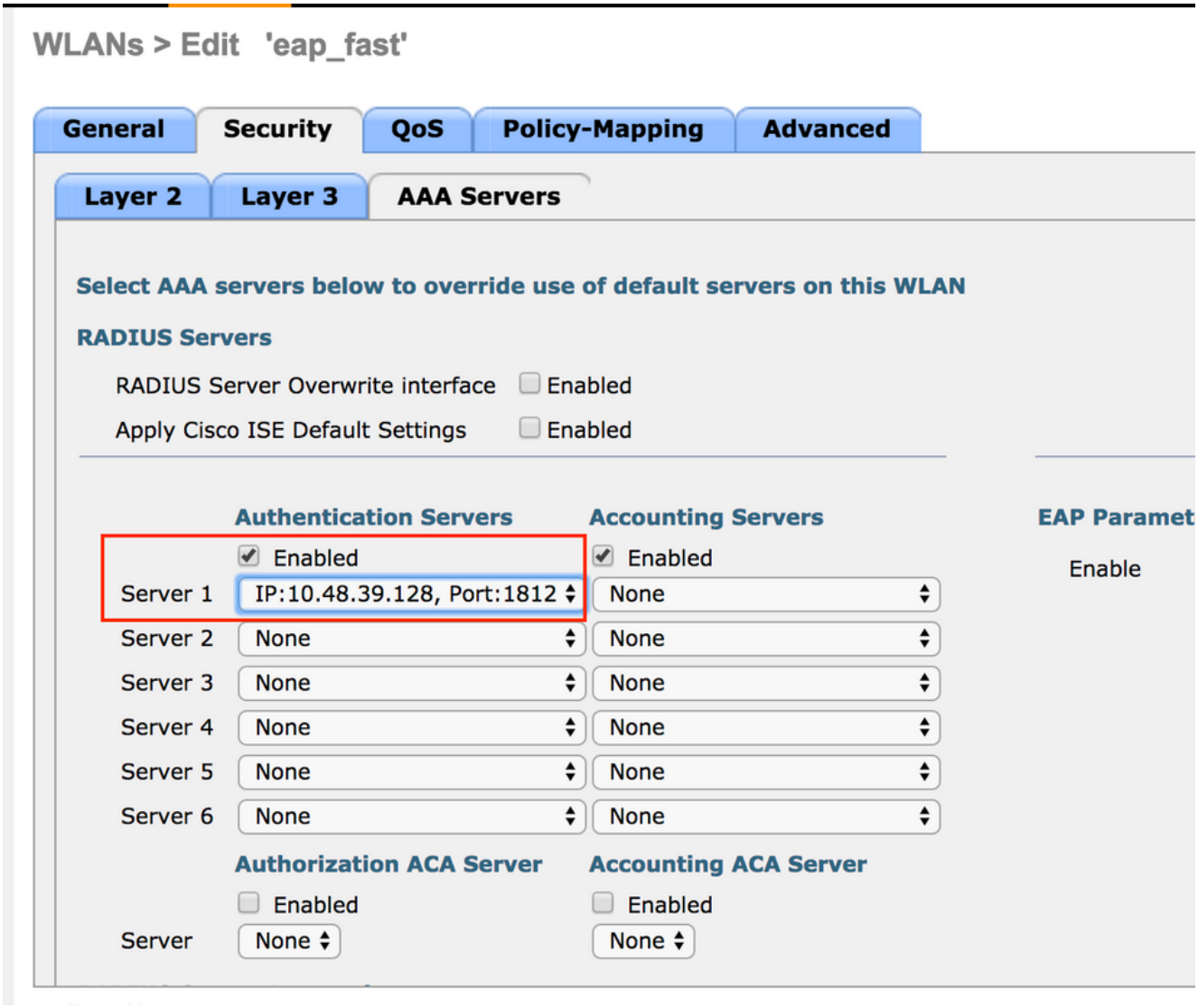


6. 通常の"**[WLAN] -> [Edit] -> [Security] -> [Layer 2]** タブで[WPA/WPA2 parameters]を選択し、AKMに[dot1x]を選択します。
この例では、このWLANのレイヤ2セキュリティとしてWPA2/AES + dot1xを使用します。

WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます。



7. [WLAN] -> [Edit] -> [Security] -> [AAA Servers] タブで、[RADIUS Servers]のプルダウンメニューから適切なRADIUSサーバを選択します。



8. [Apply] をクリックします。**注：**これは、EAP認証用にコントローラで設定する必要がある唯一のEAP設定です。EAP-FAST に固有なその他すべての設定は、RADIUS サーバおよび認証が必要なクライアントで行う必要があります。

EAP-FAST 認証のための RADIUS サーバの設定

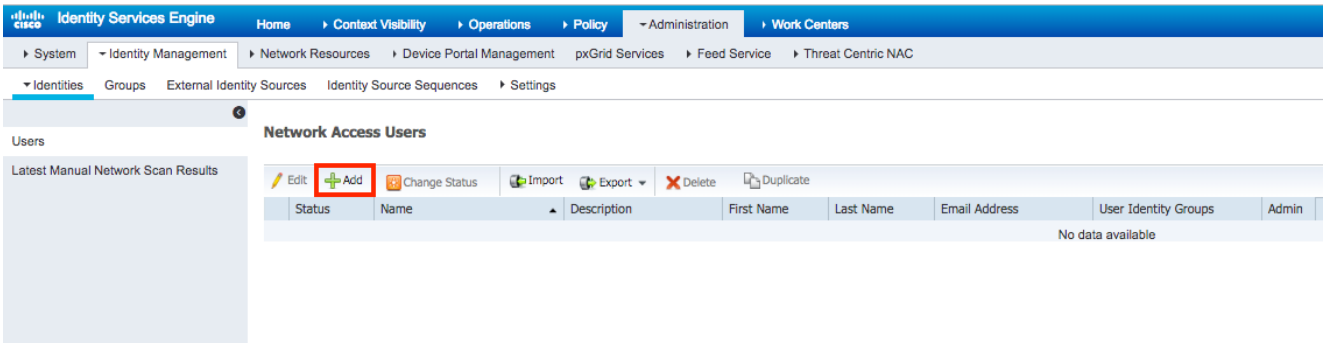
RADIUS サーバの EAP-FAST 認証を設定するには、次の手順を実行します。

1. EAP-FAST クライアント認証用のユーザ データベースの作成
2. AAA クライアントとしての WLC の RADIUS サーバへの追加
3. 匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定
4. RADIUS サーバの EAP-FAST 認証に認証付きインバンド PAC プロビジョニングを設定する

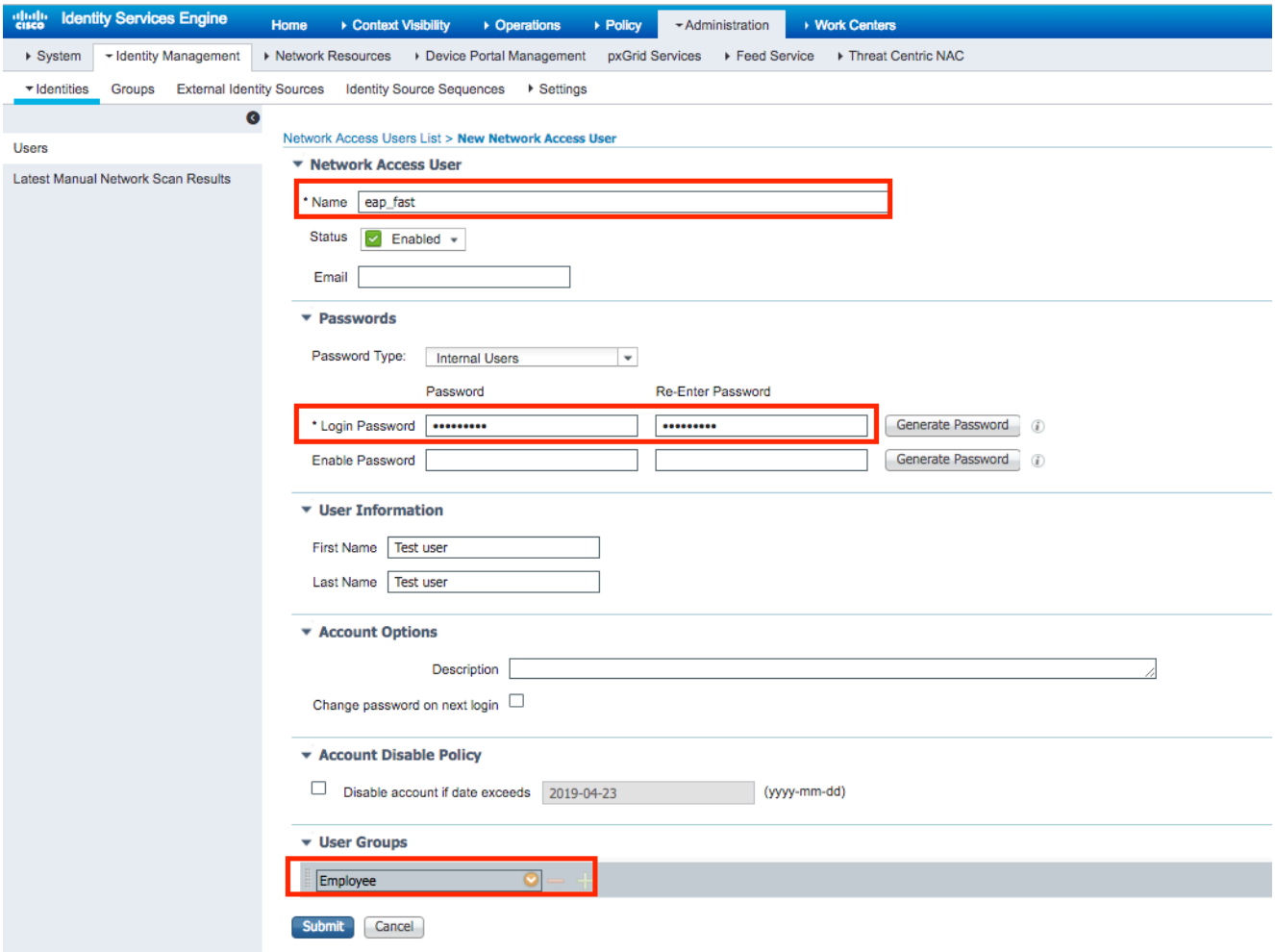
EAP-FAST クライアント認証用のユーザ データベースの作成

この例では、EAP-FASTクライアントのユーザ名とパスワードをそれぞれ<*eap_fast*>および<*EAP-fast1*>として設定します。

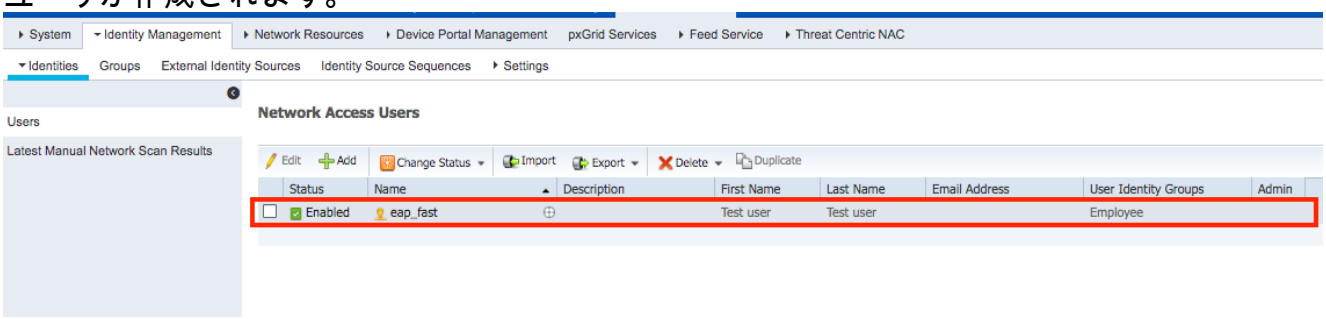
1. ISE Web管理UIで、**[Administration] -> [Identity Management] -> [Users]の下に移動し、[Add]アイコンを押**します。



2. 作成するユーザーに必要なフォーム(「Name」および「Login password」を入力し、ドロップダウン・リストから「User group」を選択します。[オプションで、ユーザーアカウントの他の情報を入力できます]
「Sumbit」を押します



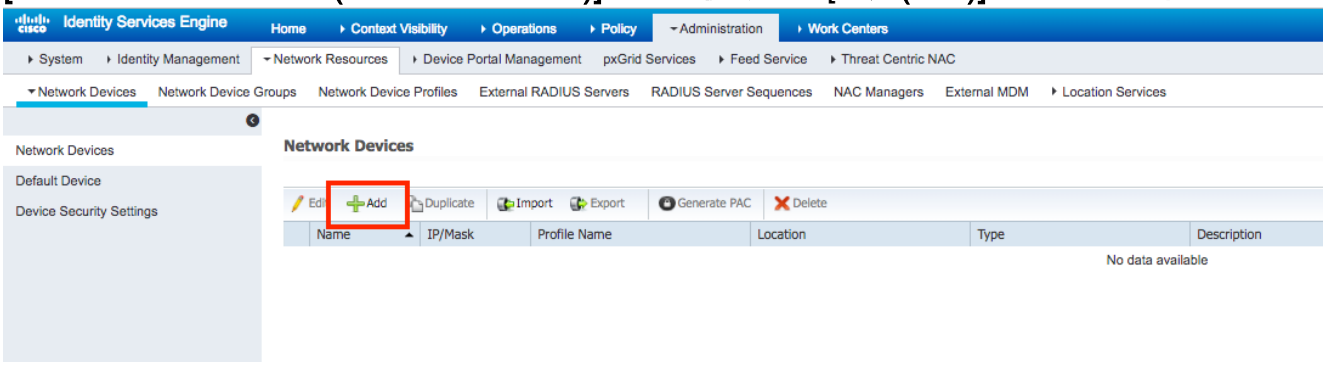
3. ユーザが作成されます。



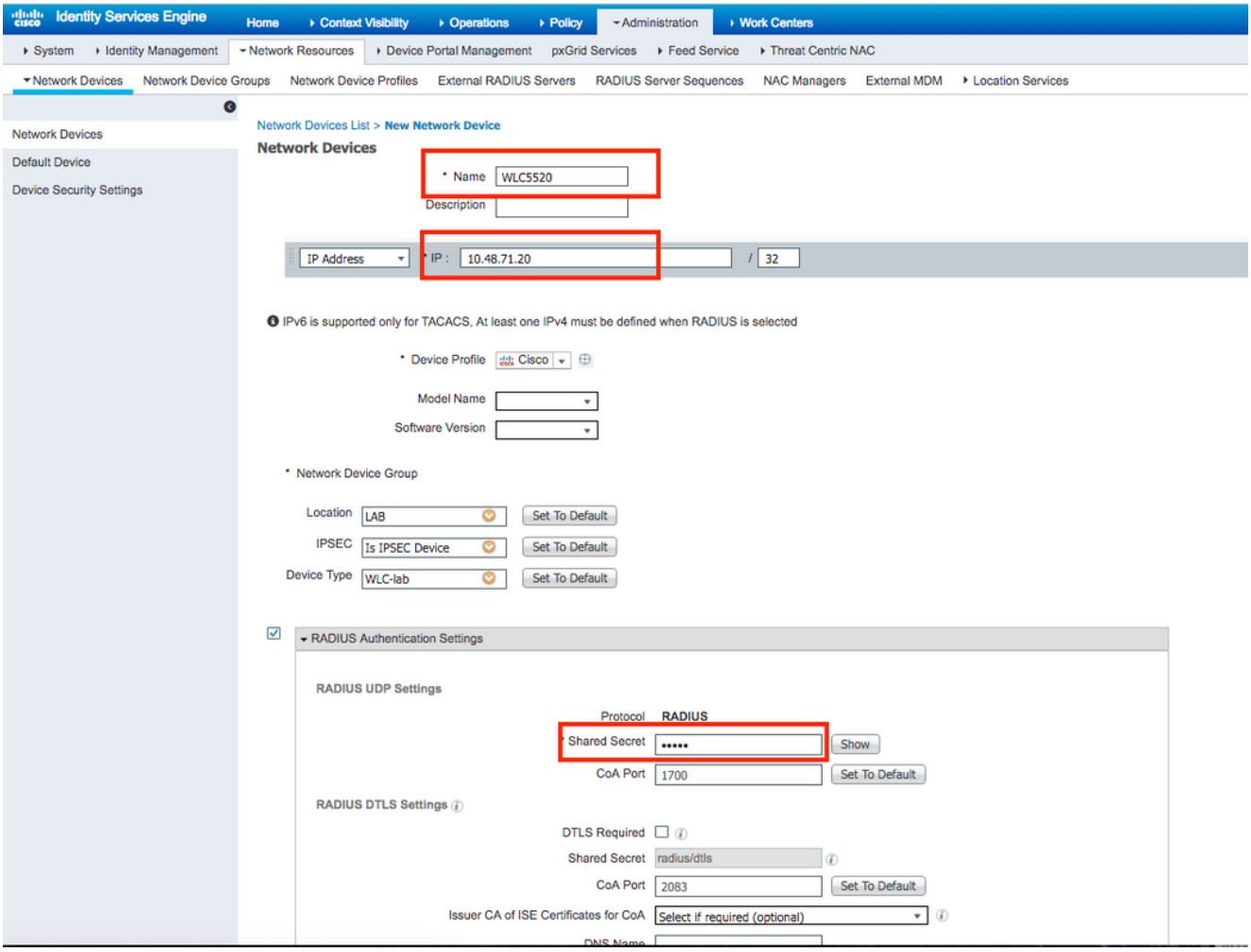
AAA クライアントとしての WLC の RADIUS サーバへの追加

ACS サーバでコントローラを AAA クライアントとして定義するには、次の手順を実行します。

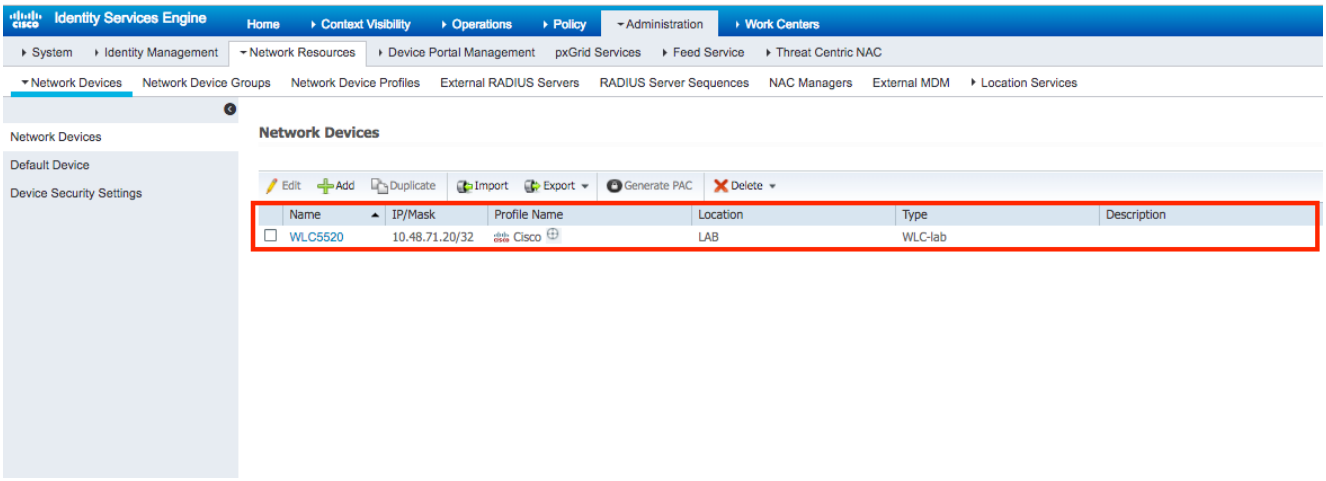
1. ISE Web管理UIで、[管理(Administration)] -> [ネットワークリソース(Network Resources)] -> [ネットワークデバイス(Network Devices)]の下に移動し、[追加(Add)]アイコンを押します。



2. 追加するデバイスに必要なフォーム(「Name」、「IP」)に入力し、前のセクションでWLCで設定した共有秘密パスワードと同じ共有秘密パスワードを設定します。[オプションで、場所、グループなどの情報を入力できます。
「Sumbit」を押します



3. デバイスがISEネットワークアクセスデバイスリストに追加されます。(NAD)

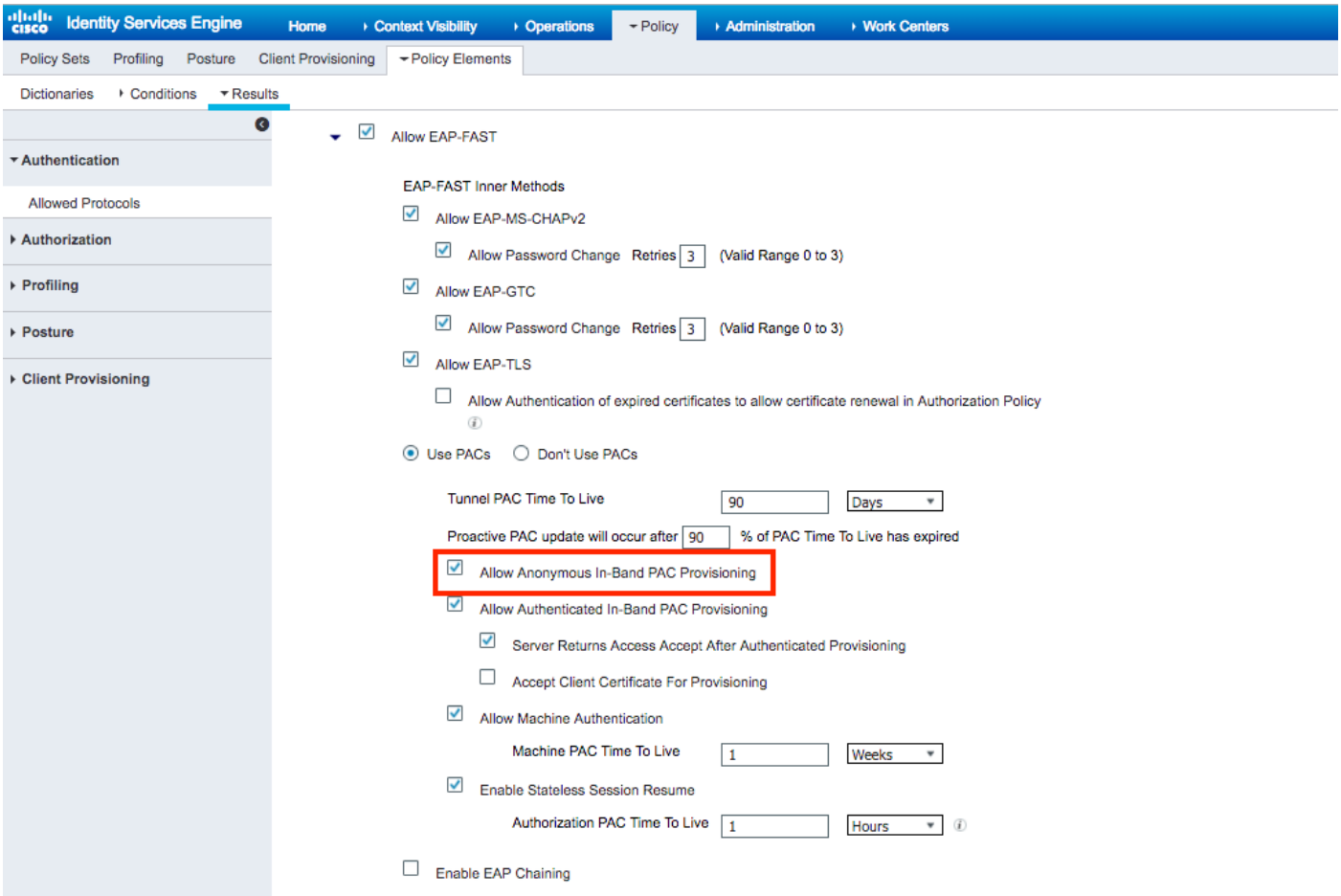


匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定

一般的には、このタイプの方法を使用して、導入にPKIインフラストラクチャがない場合を想定します。

この方式は、ピアがISEサーバを認証する前に、Authenticated Diffie-HellmanKey Agreement Protocol(ADHP)トンネル内で動作します。

この方法をサポートするには、[Authentication Allowed Protocols] でISEの[Allow Anonymous In-band PAC Provisioning]を有効にする必要があります。



注：EAP-FAST内部方式に対してEAP-MS-CHAPv2などのパスワードタイプの認証を許可していることを確認してください。これは、明らかに匿名インバンドプロビジョニングでは証明書を使

用できないためです。

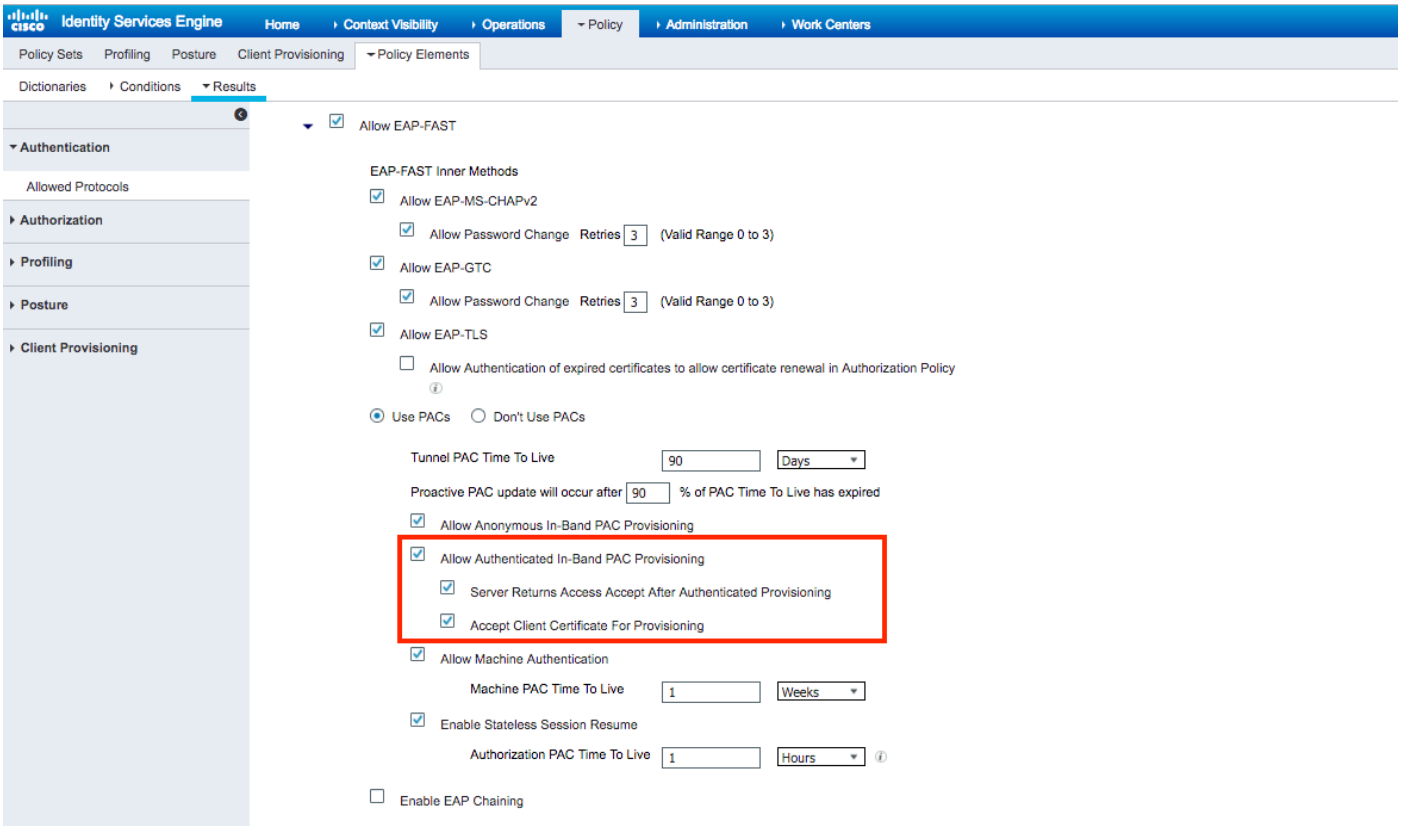
RADIUS サーバの EAP-FAST 認証に認証付きインバンド PAC プロビジョニングを設定する

これは最もセキュアで推奨されるオプションです。TLSトンネルは、サプリカントによって検証されるサーバ証明書に基づいて構築され、クライアント証明書はISE（デフォルト）によって検証されます。

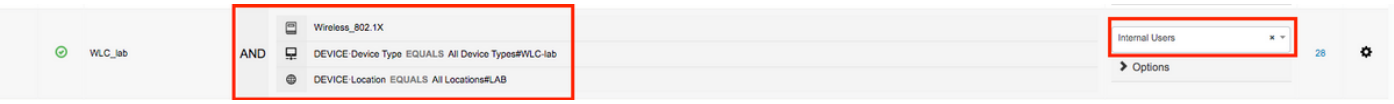
このオプションでは、クライアントとサーバのPKIインフラストラクチャが必要ですが、サーバ側だけに限定されるか、両側でスキップされる場合があります。

ISEでは、認証済みインバンドプロビジョニングに2つの追加オプションがあります。

1. 「**Server Returns Access Accept After Authenticated Provisioning**」:通常、PACプロビジョニング後に、PACを使用してサプリカントを再認証するようにAccess-Rejectを送信する必要があります。ただし、PACプロビジョニングは認証されたTLSトンネルで実行されるため、認証時間を最小限に抑えるために、Access-Acceptで即座に応答できます。（このような場合は、クライアント側とサーバ側に信頼できる証明書があることを確認してください）。
2. **「プロビジョニング用クライアント証明書の受け入れ」：クライアントデバイスにPKIインフラストラクチャを提供せず、ISE上に信頼できる証明書のみを持つ場合は、そのオプションを有効にします。これにより、サーバ側のクライアント証明書の検証をスキップできます。**



ISEでは、無線ユーザに対する単純な認証ポリシーセットも定義します。次の例では、接続パラメータのデバイスタイプと場所と認証タイプとして、その条件に一致する認証フローが内部ユーザデータベースに対して検証されます。



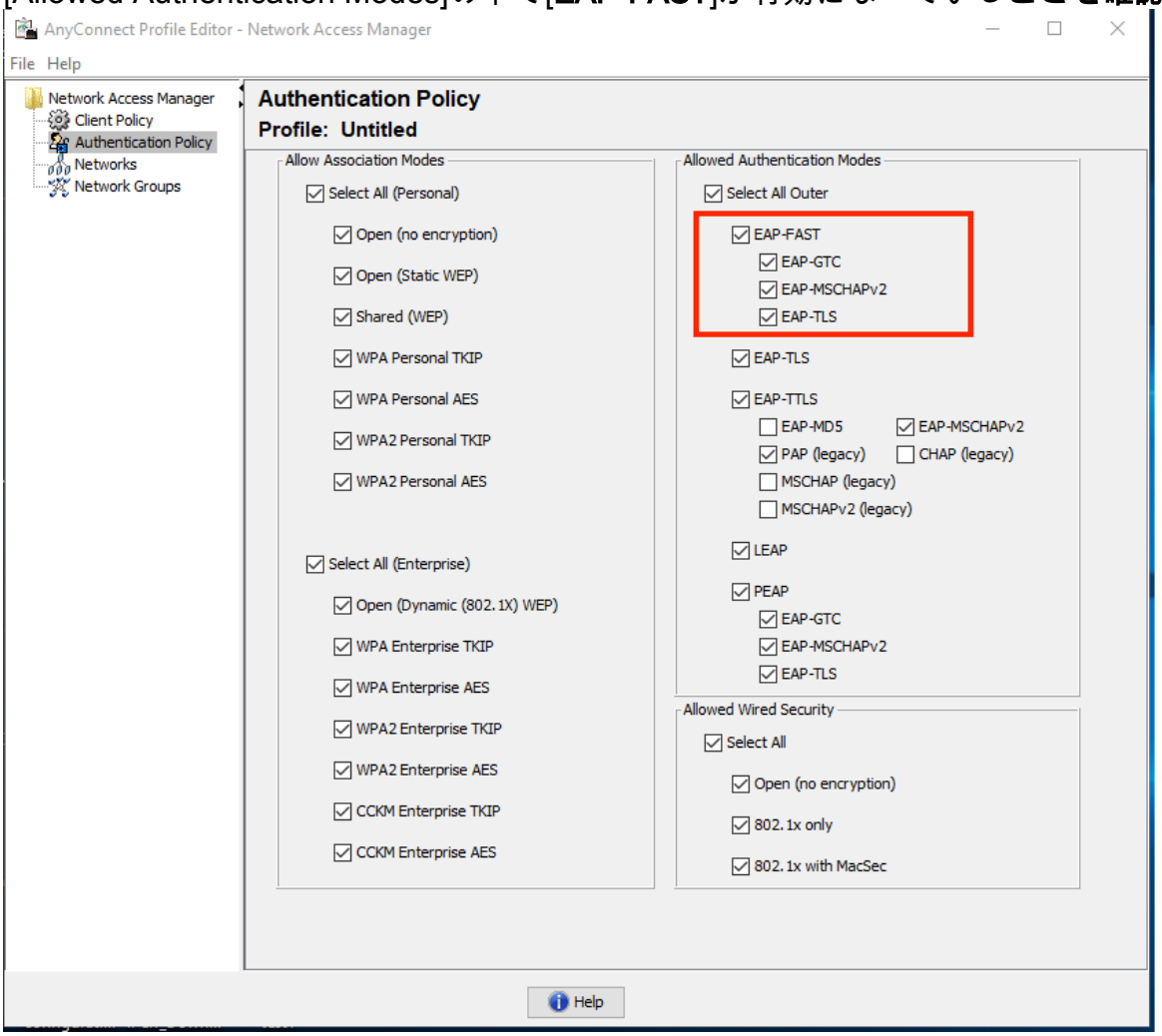
確認

この例では、それぞれのWLCデバッグとともに、認証済みインバンドPACプロビジョニングフローとNetwork Access Manager(NAM)の設定値を示します。

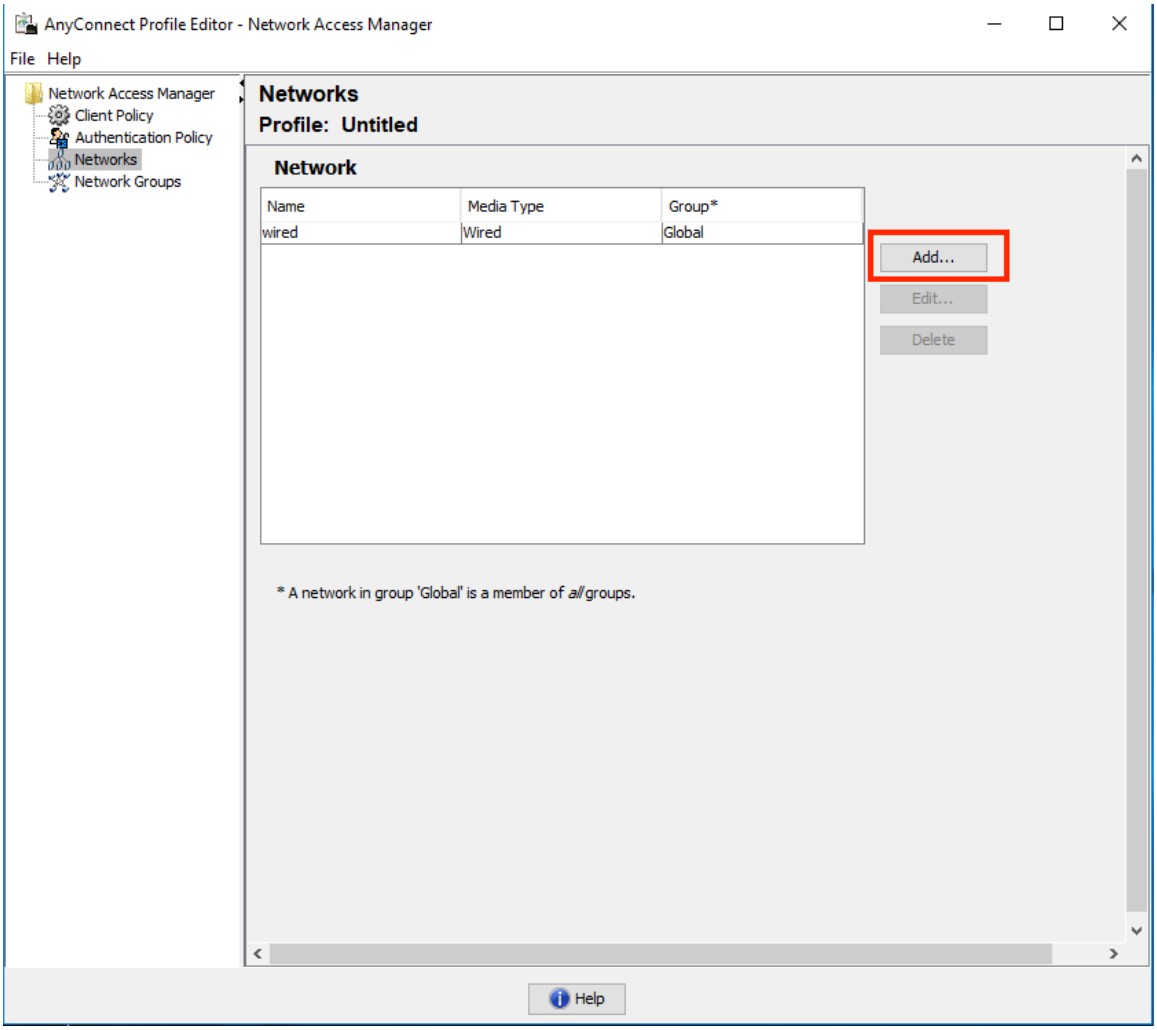
NAMプロファイルの設定

EAP-FASTを使用してISEに対してユーザセッションを認証するようにAnyconnect NAMプロファイルを設定するには、次の手順を実行する必要があります。

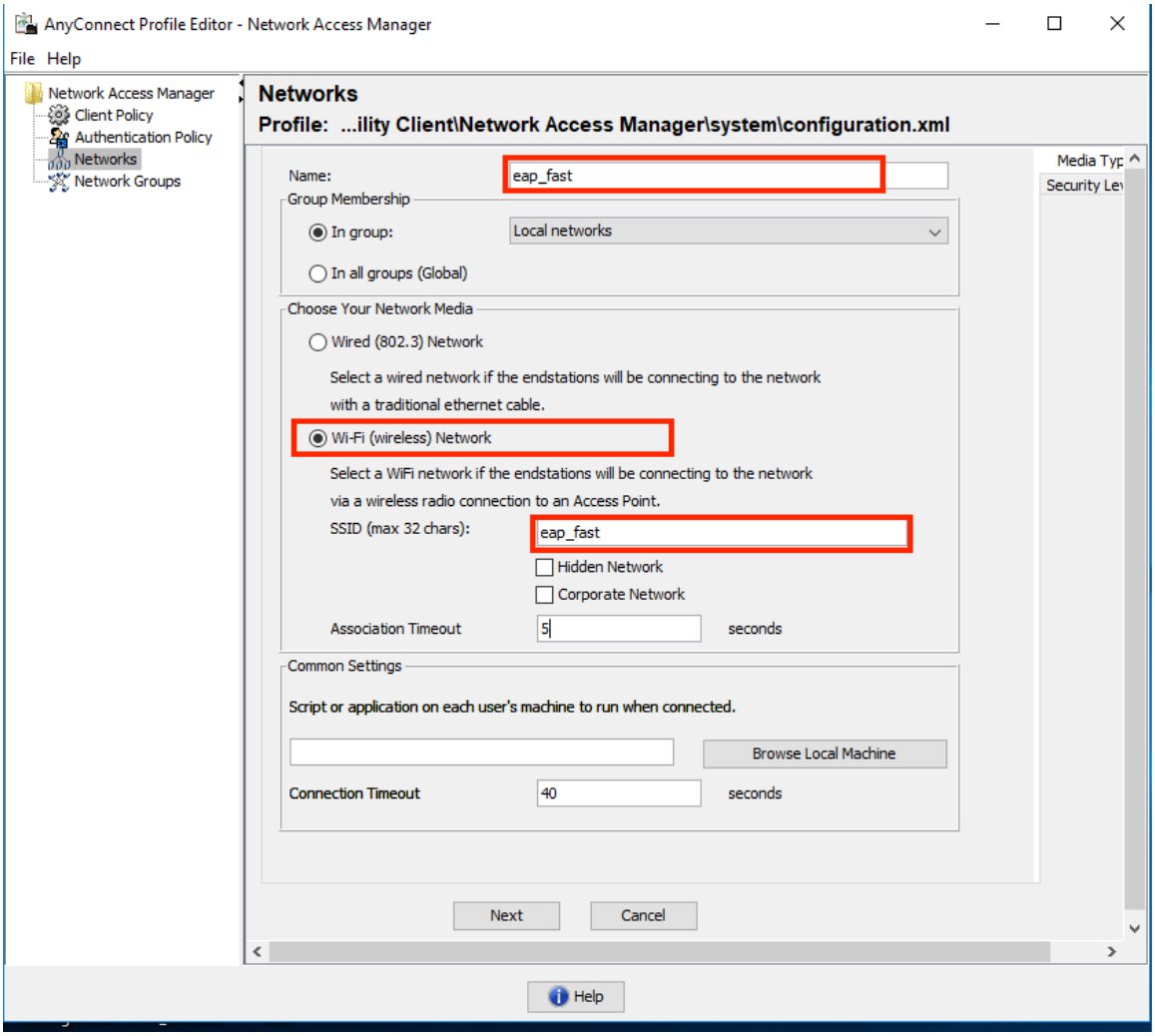
1. Network Access Manager Profile Editorを開き、現在の設定ファイルをロードします。
2. [Allowed Authentication Modes]の下で**[EAP-FAST]が有効になっていることを確認します。**



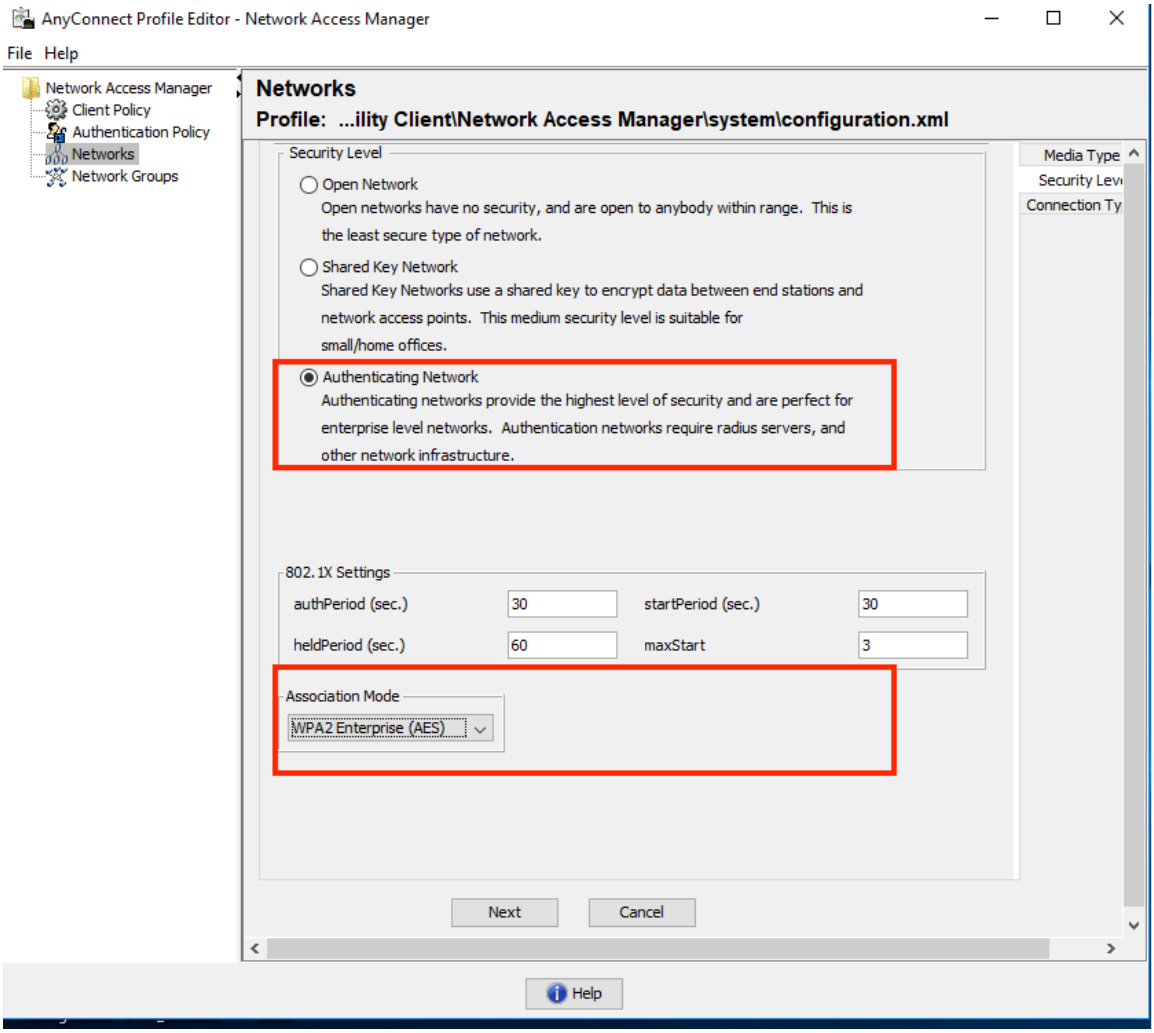
3. 新しいネットワークプロファイルを「追加」します。



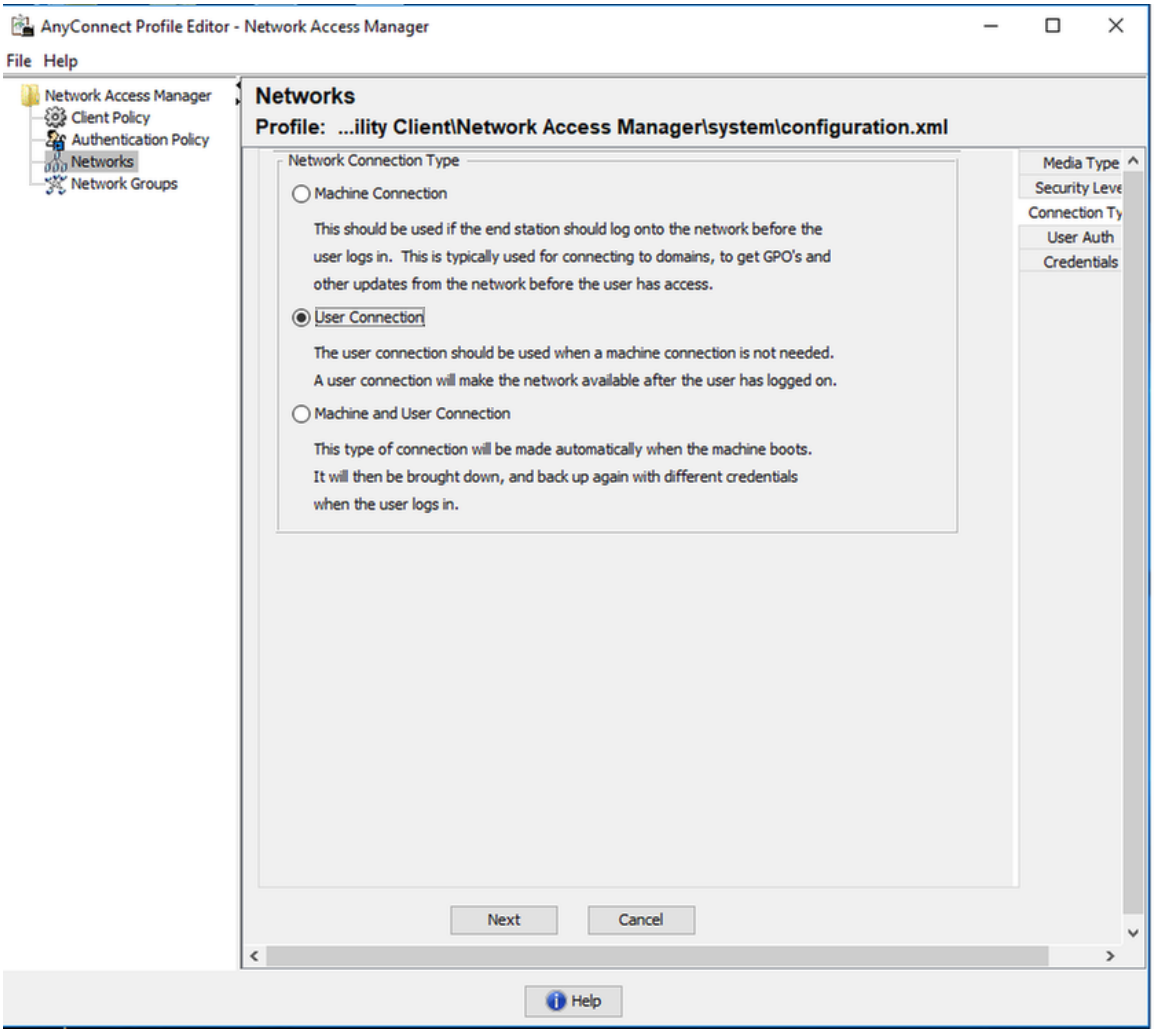
4. [Media type] 設定セクションで、プロファイル「**Name**」を定義し、メディアネットワークタイプとしてwirelessを定義し、SSID名を指定します。



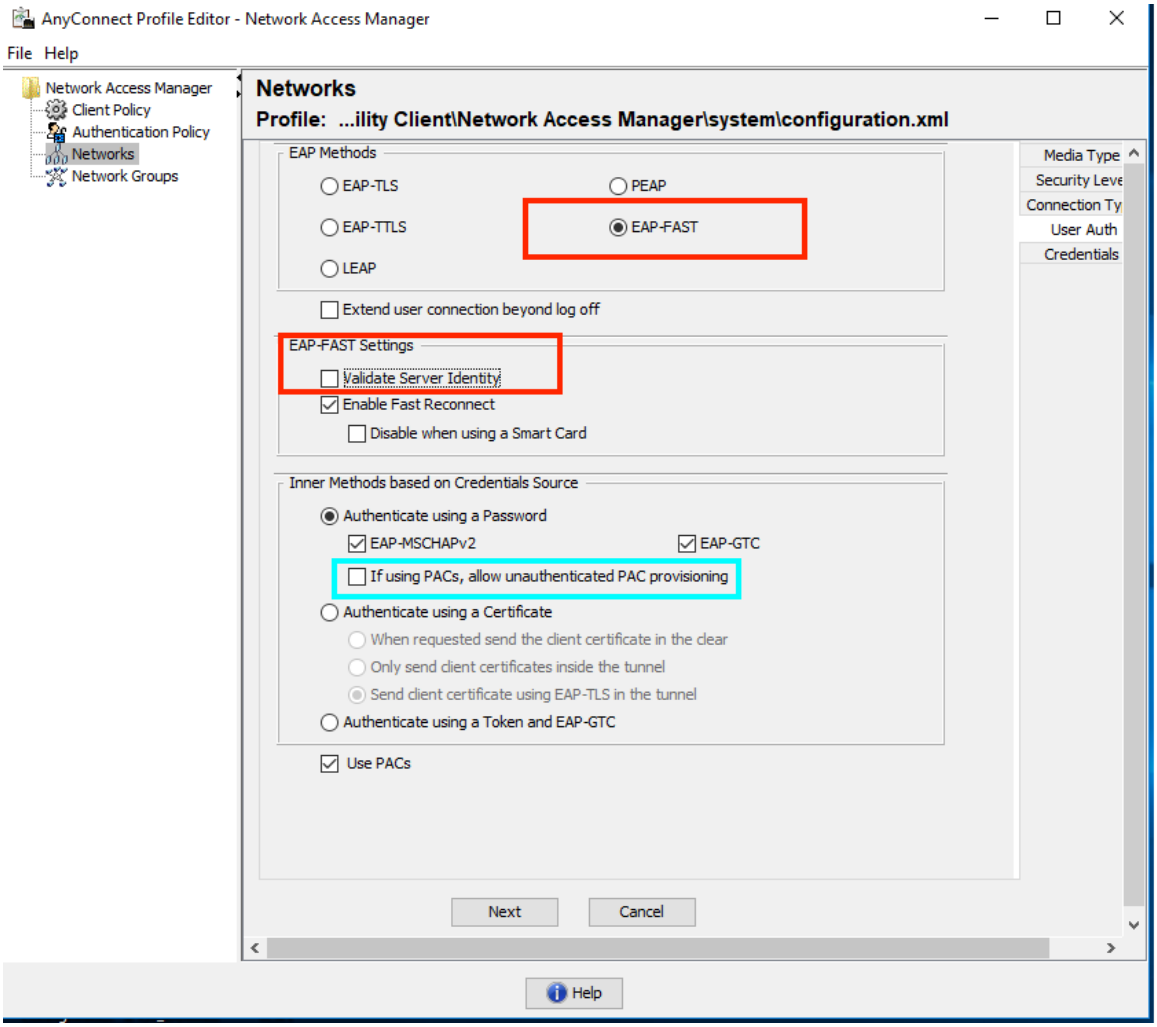
5. [Security Level] 設定タブで[Authenticating Network]を選択し、アソシエーションモードを[WPA2 Enterprise (AES)]に指定します



6. この例では、ユーザーの種類の認証を使用しています。次のタブの[Connection type]で[User Connection]を選択します。

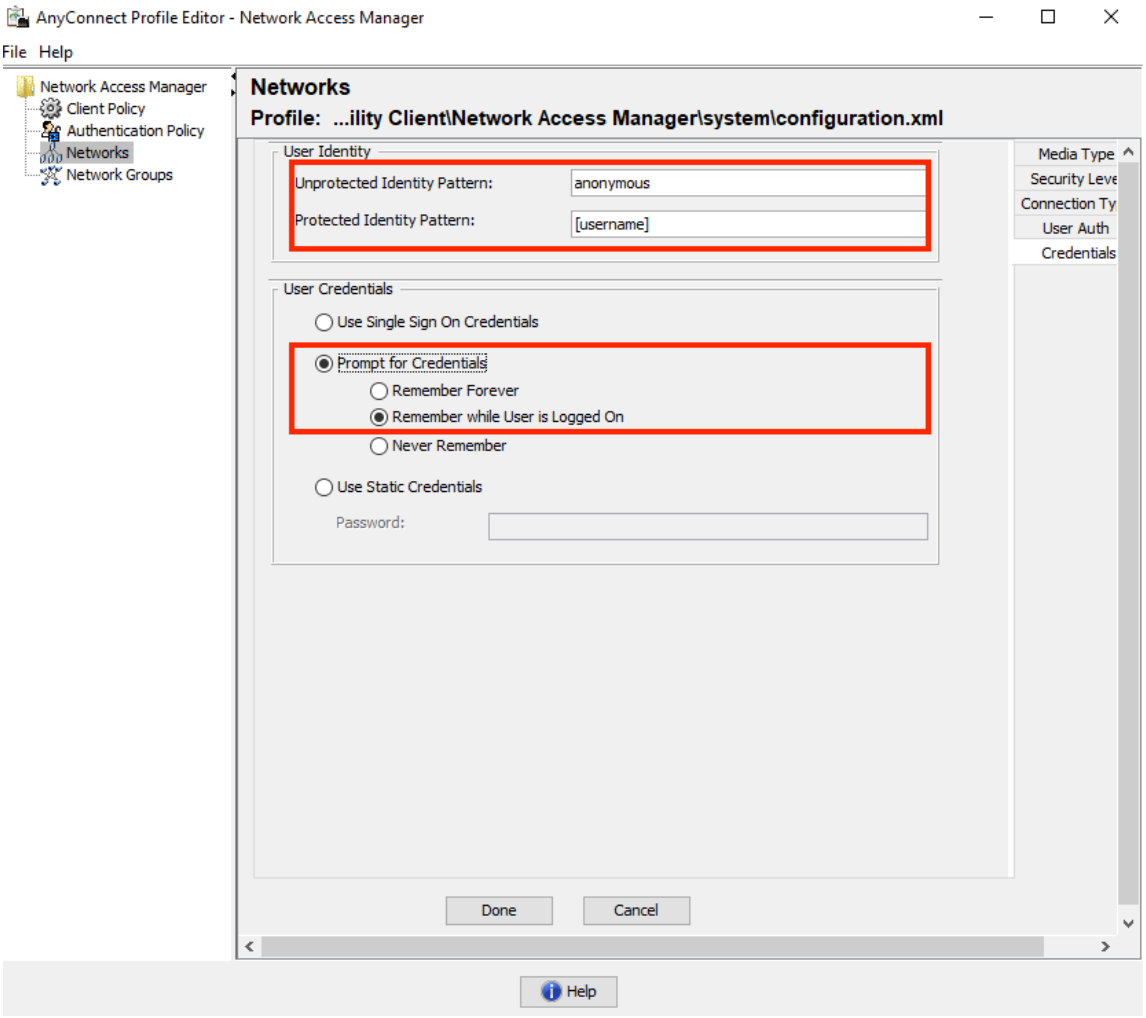


7. この例では信頼できる証明書を使用していないため、[User Auth] タブで、許可される認証方式としてEAP-FASTを指定し、サーバ証明書の検証を無効にします。



注：実際の実稼働環境では、信頼できる証明書がISEにインストールされていることを確認し、NAM設定でサーバ証明書の検証オプションを有効にしておいてください。
注：オプション「PACを使用している場合、非認証PACプロビジョニングを許可する」は、匿名インバンドPACプロビジョニングの場合にのみ選択する必要があります。

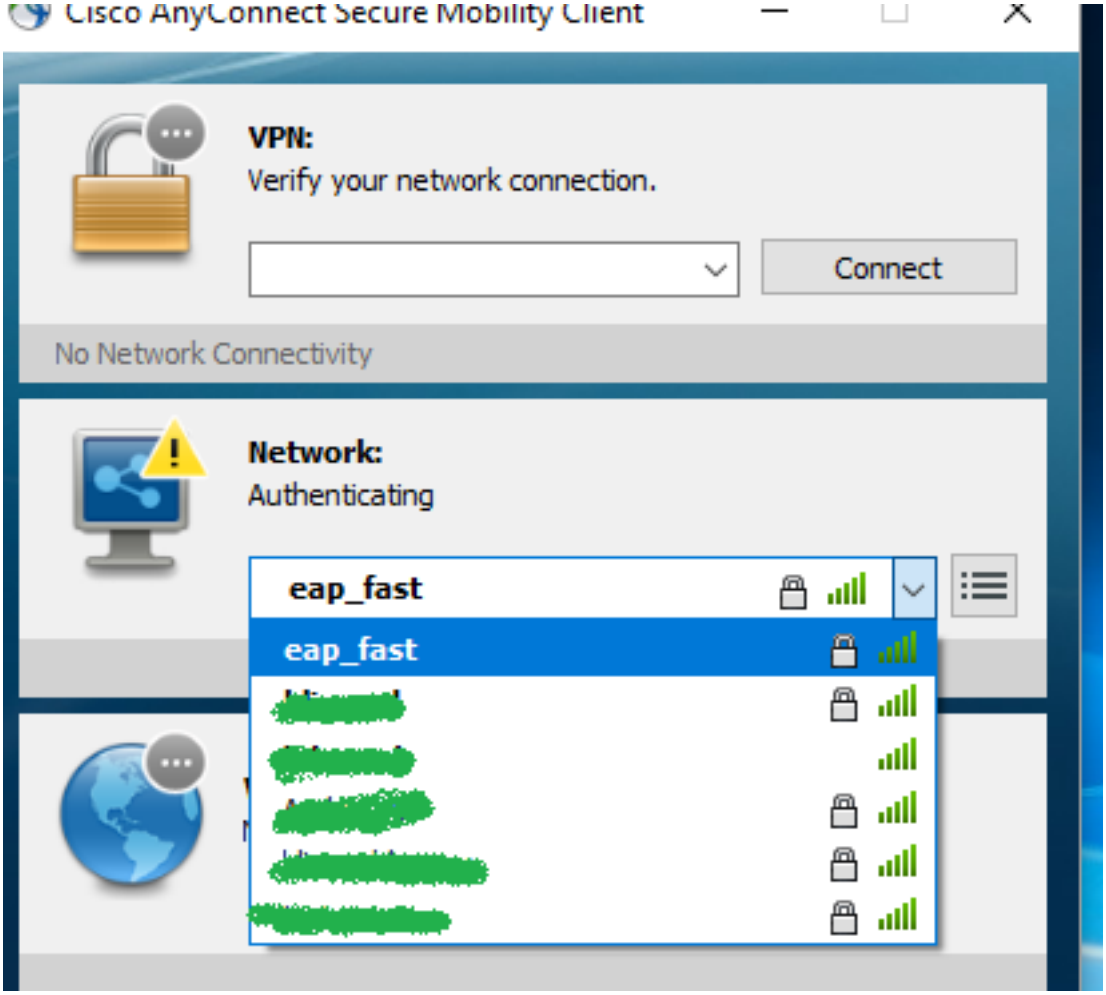
8. ユーザのクレデンシャルをSSOとして定義します。ログイン時と同じクレデンシャルを使用する場合は、[クレデンシャルの入力を求める]を選択し、ネットワークへの接続中にクレデンシャルを求める場合は[クレデンシャルの入力]を選択します。この例では、ユーザに対して、ネットワークへの接続の試行時にクレデンシャルを要求します。



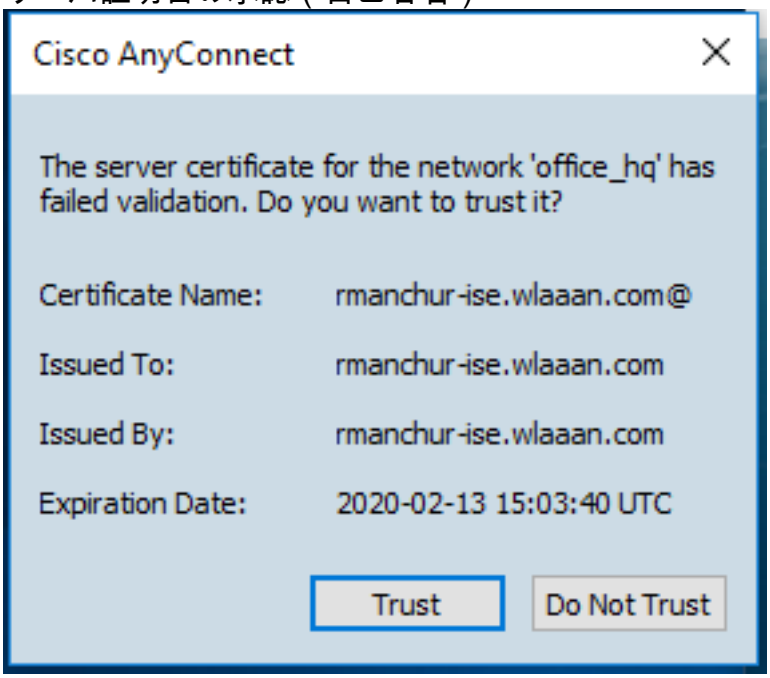
9. 設定されたプロファイルを各NAMフォルダに保存します。

EAP-FAST認証を使用して、SSIDへの接続をテストします。

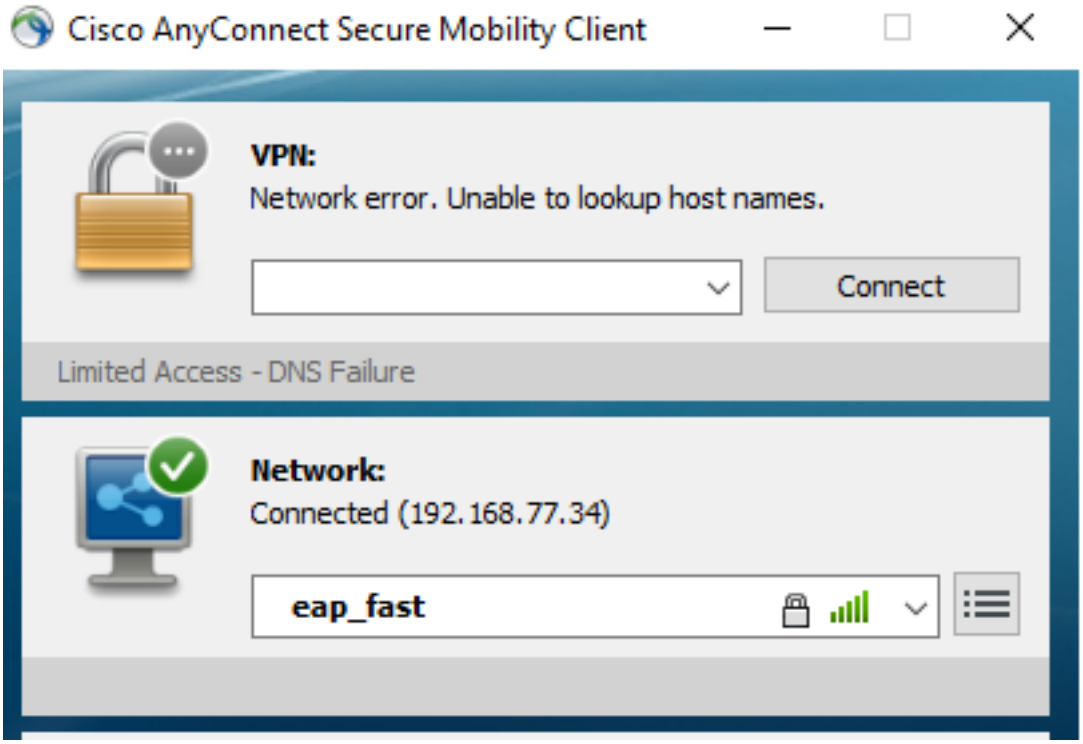
1. Anyconnectネットワークリストからそれぞれのプロファイルを選択します



2. 認証に必要なユーザ名とパスワードを入力します
3. サーバ証明書の承認（自己署名）



4. Done



ISE認証ログ

EAP-FASTおよびPACプロビジョニングフローを示すISE認証ログは、[Operations] -> [RADIUS] -> [Live Logs] の下に表示され、[Zoom] アイコンを使用して詳細を確認できます。

1. クライアントが認証を開始し、ISEが認証方式としてEAP-TLSを提案していましたが、クライアントが拒否し、代わりにEAP-FASTを提案しました。これは、クライアントとISEの両方が合意した方式でした。

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12101	Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100	Prepared EAP-Request proposing EAP-FAST with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12102	Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

2. クライアントとサーバの間でPAC交換のために提供された保護環境へのTLSハンドシェイクが開始され、正常に完了しました。

12800 Extracted first TLS record; TLS handshake started

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12807 Prepared TLS Certificate message

12808 Prepared TLS ServerKeyExchange message

12810 Prepared TLS ServerDone message

12811 Extracted TLS Certificate message containing client certificate

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request (⏰ Step latency=13317 ms)

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12812 Extracted TLS ClientKeyExchange message

12813 Extracted TLS CertificateVerify message

12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message

12802 Prepared TLS Finished message

12816 TLS handshake succeeded

3. 内部認証が開始され、ユーザクレデンシャルがMS-CHAPv2を使用してISEによって正常に検証されました（ユーザ名/パスワードベースの認証）