EAP-FAST-Authentifizierung mit Wireless LAN-Controllern und Identity Services Engine

Inhalt

Einführung

In diesem Dokument wird erläutert, wie der WLAN-Controller (WLC) für Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST)-Authentifizierung mithilfe eines externen RADIUS-Servers konfiguriert wird. In diesem Konfigurationsbeispiel wird die Identity Services Engine (ISE) als externer RADIUS-Server für die Authentifizierung des Wireless-Clients verwendet.

In diesem Dokument wird erläutert, wie Sie die ISE für die Bereitstellung der Wireless-Clients für die Bereitstellung von Anonymous and Authenticated In-Band (Automatic) Protected Access Credentials (PAC) konfigurieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco WLCs
- Grundkenntnisse des CAPWAP-Protokolls
- Kenntnisse zum Konfigurieren eines externen RADIUS-Servers, z. B. der Cisco ISE
- Funktionale Kenntnisse des allgemeinen EAP-Frameworks
- Grundkenntnisse zu Sicherheitsprotokollen, wie MS-CHAPv2 und EAP-GTC, und Kenntnisse zu digitalen Zertifikaten

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC der Serie 5520 mit Firmware-Version 8.8.111.0Cisco AP der Serie 4800AnyConnect NAMCisco Secure ISE Version 2.3.0.298Cisco Switch der Serie 3560-CX mit Version 15.2(4)E1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Das EAP-FAST-Protokoll ist ein öffentlich zugänglicher EAP-Typ nach IEEE 802.1X, den Cisco entwickelt hat, um Kunden zu unterstützen, die keine strenge Kennwortrichtlinie durchsetzen können und einen 802.1X-EAP-Typ bereitstellen möchten, für den keine digitalen Zertifikate erforderlich sind.

Das EAP-FAST-Protokoll ist eine Client-Server-Sicherheitsarchitektur, die EAP-Transaktionen mit einem Transport Level Security (TLS)-Tunnel verschlüsselt. Die Einrichtung von EAP-FAST-Tunneln basiert auf strengen Geheimnissen, die nur für Benutzer gelten. Diese sicheren Geheimnisse werden als PACs bezeichnet, die von der ISE mithilfe eines Master-Schlüssels generiert werden, der nur der ISE bekannt ist.

EAP-FAST findet in drei Phasen statt:

- **Phase Null (Automatische PAC-Bereitstellungsphase)** - EAP-FAST-Phase Null. Eine optionale

Phase ist ein tunnelsicheres Mittel, um einem EAP-FAST-Endbenutzer-Client eine PAC für den Benutzer bereitzustellen, der Netzwerkzugriff anfordert. **Die Bereitstellung einer PAC für den Endbenutzer-Client ist der einzige Zweck von Phase Null.Hinweis:** Phase Null ist optional, da PACs Clients auch manuell bereitgestellt werden können, anstatt Phase Null zu verwenden.Weitere Informationen finden Sie im Abschnitt PAC-Bereitstellungsmodi dieses Dokuments.

- **Phase 1**: In Phase 1 richten die ISE und der Endbenutzer-Client einen TLS-Tunnel auf der Grundlage der PAC-Anmeldeinformationen des Benutzers ein. Für diese Phase muss dem Endbenutzer-Client eine PAC für den Benutzer bereitgestellt werden, der versucht, auf das Netzwerk zuzugreifen, und die PAC basiert auf einem Master-Schlüssel, der noch nicht abgelaufen ist. In Phase 1 des EAP-FAST ist kein Netzwerkservice aktiviert.
- **Phase 2** - In Phase 2 werden die Anmeldeinformationen für die Benutzerauthentifizierung sicher mithilfe einer vom EAP-FAST im TLS-Tunnel unterstützten inneren EAP-Methode an den RADIUS weitergeleitet, der mithilfe der PAC zwischen dem Client und dem RADIUS-Server erstellt wurde. EAP-GTC, TLS und MS-CHAP werden als innere EAP-Methoden unterstützt. Für EAP-FAST werden keine anderen EAP-Typen unterstützt.

Weitere Informationen finden Sie unter Funktionsweise von EAP-FAST.

PAC

PACs sind sichere, gemeinsam genutzte Geheimnisse, die es der ISE und einem EAP-FAST-Endbenutzer-Client ermöglichen, sich gegenseitig zu authentifizieren und einen TLS-Tunnel für die Verwendung in Phase 2 von EAP-FAST einzurichten. Die ISE generiert PACs, indem sie den aktiven Master-Schlüssel und einen Benutzernamen verwendet.

PAC umfasst:

- **PAC-Key** - Gemeinsam genutzter geheimer Schlüssel, der an einen Client (und Client-Gerät) und eine Serveridentität gebunden ist.
- **PAC Opaque** (Opak **PAC**): Opakes Feld, das der Client zwischenspeichert und an den Server übergibt. Der Server stellt den PAC-Schlüssel und die Client-Identität für die gegenseitige Authentifizierung mit dem Client wieder her.
- **PAC-Info**: Enthält mindestens die Serveridentität, um dem Client das Zwischenspeichern verschiedener PACs zu ermöglichen. Optional enthält es weitere Informationen, wie z. B. die Ablaufzeit des PAC.

PAC-Bereitstellungsmodi

Wie bereits erwähnt, ist Phase Null eine optionale Phase.

EAP-FAST bietet zwei Optionen für die Bereitstellung eines Clients mit einer PAC:

- **Automatische PAC-Bereitstellung (EAP-FAST Phase 0 oder In-Band-PAC-Bereitstellung)**
- **Manuelle (Out-of-Band) PAC-Bereitstellung**

Die In-Band-/automatische PAC-Bereitstellung sendet eine neue PAC über eine gesicherte Netzwerkverbindung an einen Endbenutzer-Client. Die automatische PAC-Bereitstellung erfordert keine Eingriffe des Netzwerkbenutzers oder eines ISE-Administrators, vorausgesetzt, Sie konfigurieren die ISE und den Endbenutzer-Client, um die automatische Bereitstellung zu unterstützen.

Die neueste EAP-FAST-Version unterstützt zwei verschiedene In-Band-Konfigurationsoptionen für die PAC-Bereitstellung:

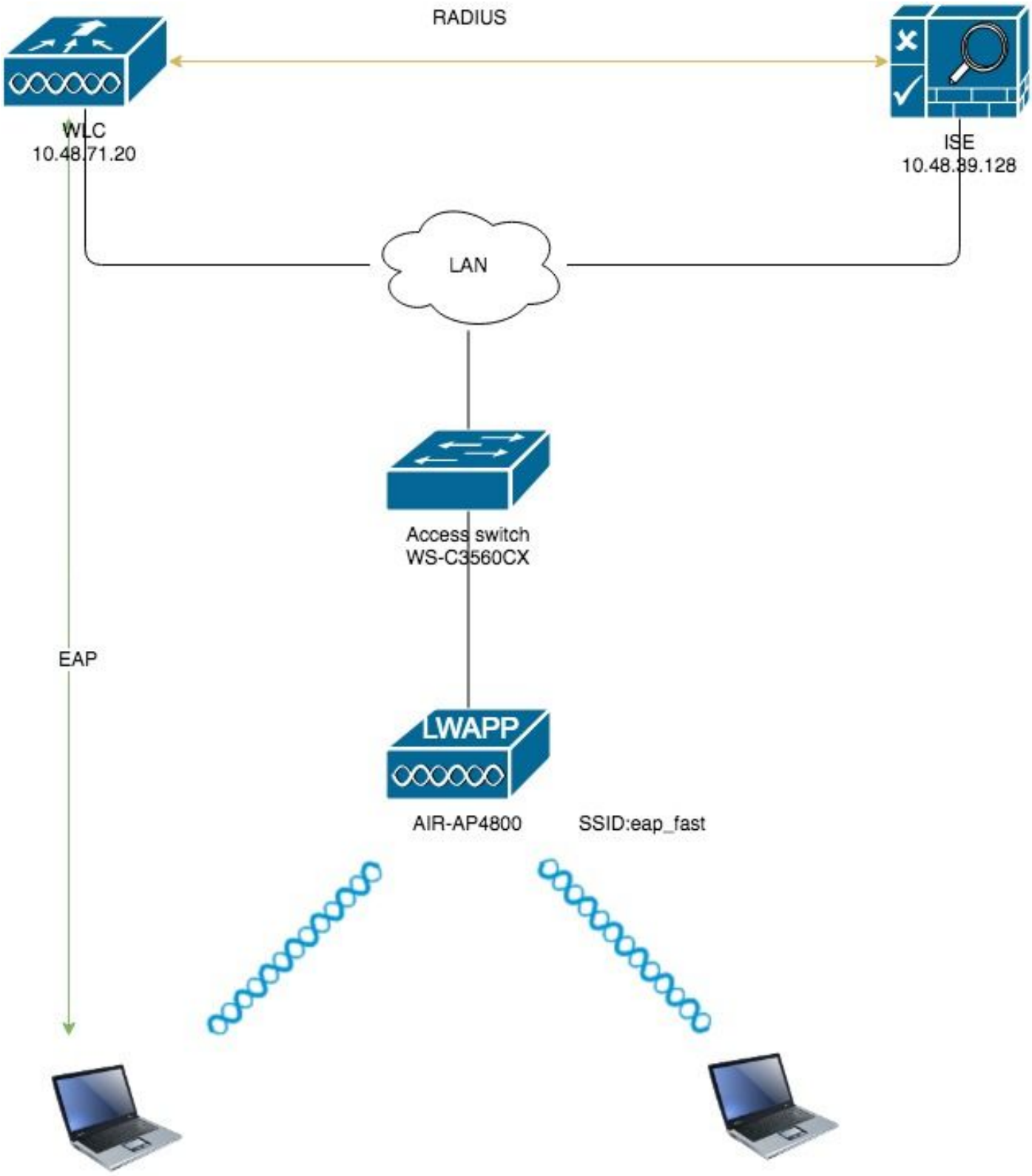
- **Anonyme In-Band-PAC-Bereitstellung**
- **Authentifizierte In-Band-PAC-Bereitstellung**

Hinweis: In diesem Dokument werden diese In-Band-PAC-Bereitstellungsmethoden und deren Konfiguration beschrieben.

Für die Out-of-Band-/manuelle PAC-Bereitstellung muss ein ISE-Administrator PAC-Dateien generieren, die dann an die entsprechenden Netzwerkbenutzer verteilt werden müssen. Benutzer müssen Endbenutzer-Clients mit ihren PAC-Dateien konfigurieren.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Konfigurieren des WLC für die EAP-FAST-Authentifizierung

Führen Sie die folgenden Schritte aus, um den WLC für die EAP-FAST-Authentifizierung zu konfigurieren:

1. Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server

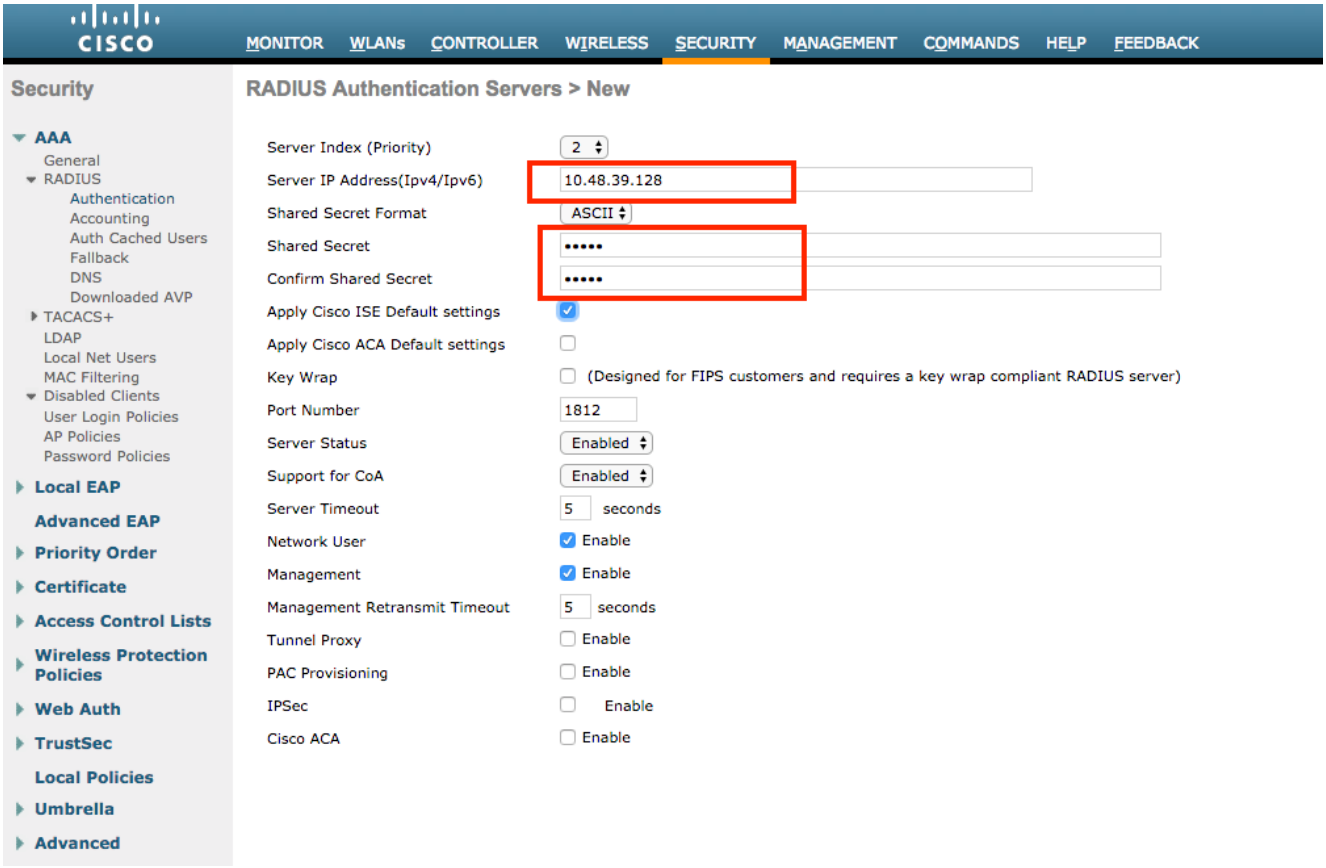
2. WLAN für die EAP-FAST-Authentifizierung konfigurieren

Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server

Der WLC muss konfiguriert werden, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten. Der externe RADIUS-Server validiert die Benutzeranmeldeinformationen anschließend mithilfe von EAP-FAST und ermöglicht den Zugriff auf die Wireless-Clients.

Gehen Sie wie folgt vor, um den WLC für einen externen RADIUS-Server zu konfigurieren:

1. Wählen Sie **Security** und **RADIUS Authentication (RADIUS-Authentifizierung)** in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen. Klicken Sie anschließend auf **Neu**, um einen RADIUS-Server zu definieren.
2. Definieren Sie die RADIUS-Serverparameter auf der Seite **RADIUS Authentication Servers > New** (RADIUS-**Authentifizierungsserver > Neu**). Zu diesen Parametern gehören:IP-Adresse des RADIUS-ServersGemeinsamer geheimer SchlüsselPort-NummerServerstatusIn diesem Dokument wird der ISE-Server mit der IP-Adresse 10.48.39.128 verwendet.



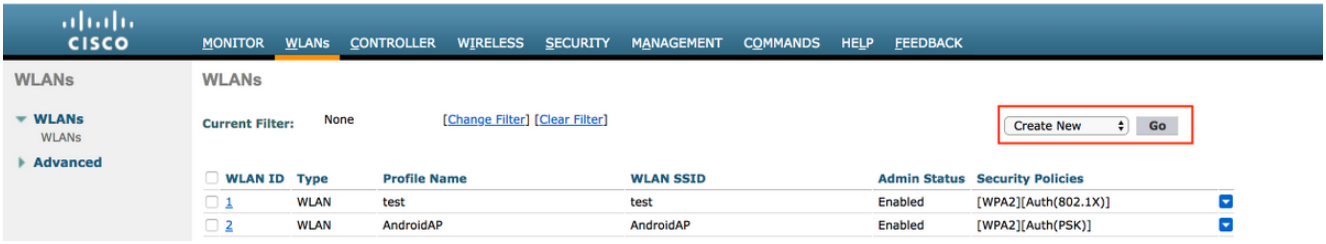
3. Klicken **Übernehmen**.

WLAN für die EAP-FAST-Authentifizierung konfigurieren

Konfigurieren Sie anschließend das WLAN, das die Clients zur Verbindung mit dem Wireless-Netzwerk für die EAP-FAST-Authentifizierung verwenden, und weisen Sie es einer dynamischen Schnittstelle zu. Der in diesem Beispiel konfigurierte WLAN-Name ist **schnell**. In diesem Beispiel wird dieses WLAN der Verwaltungsschnittstelle zugewiesen.

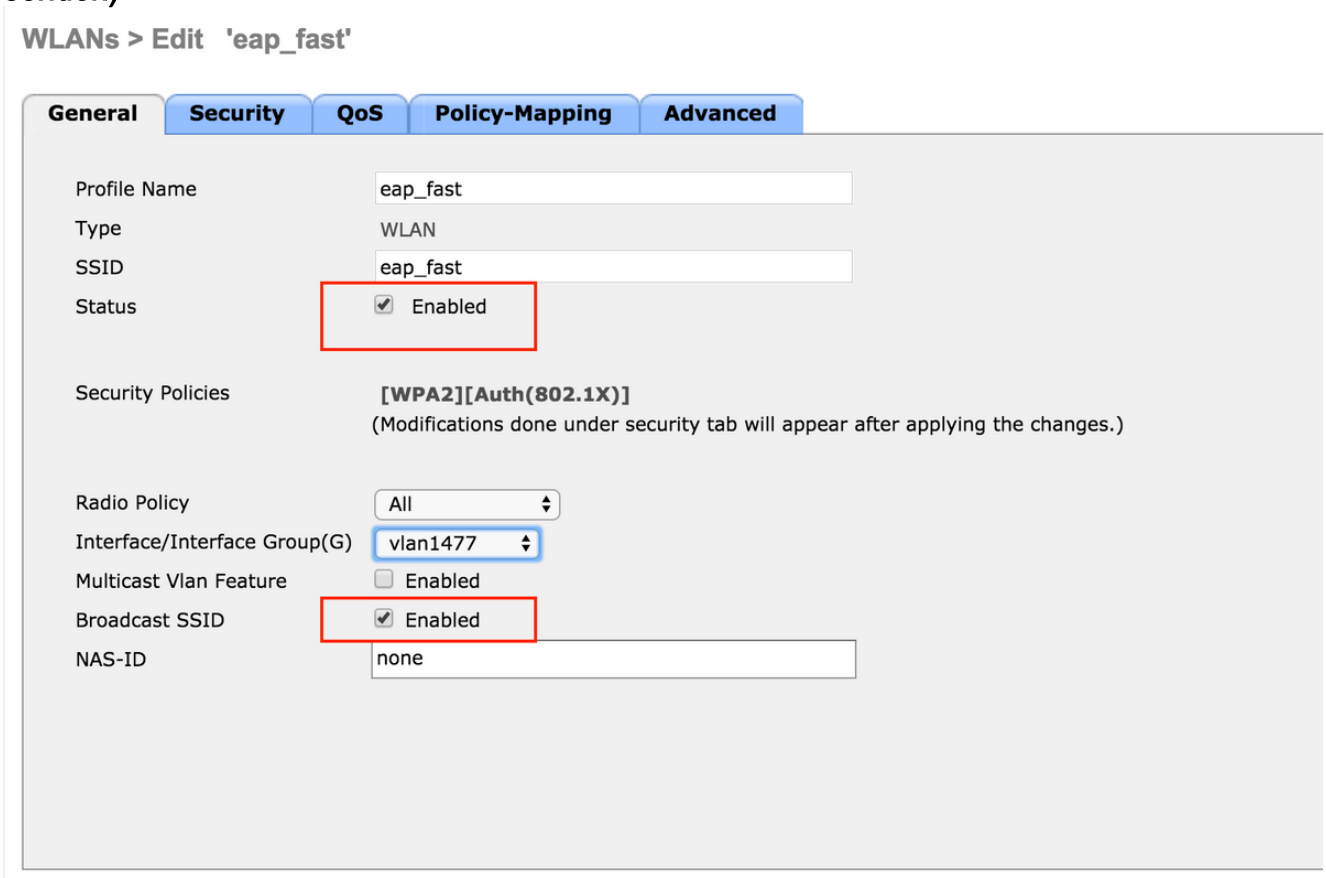
Gehen Sie wie folgt vor, um das **schnelle** WLAN und die zugehörigen Parameter zu konfigurieren:

1. Klicken Sie in der Benutzeroberfläche des Controllers auf **WLANs**, um die Seite WLANs anzuzeigen.Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu erstellen.



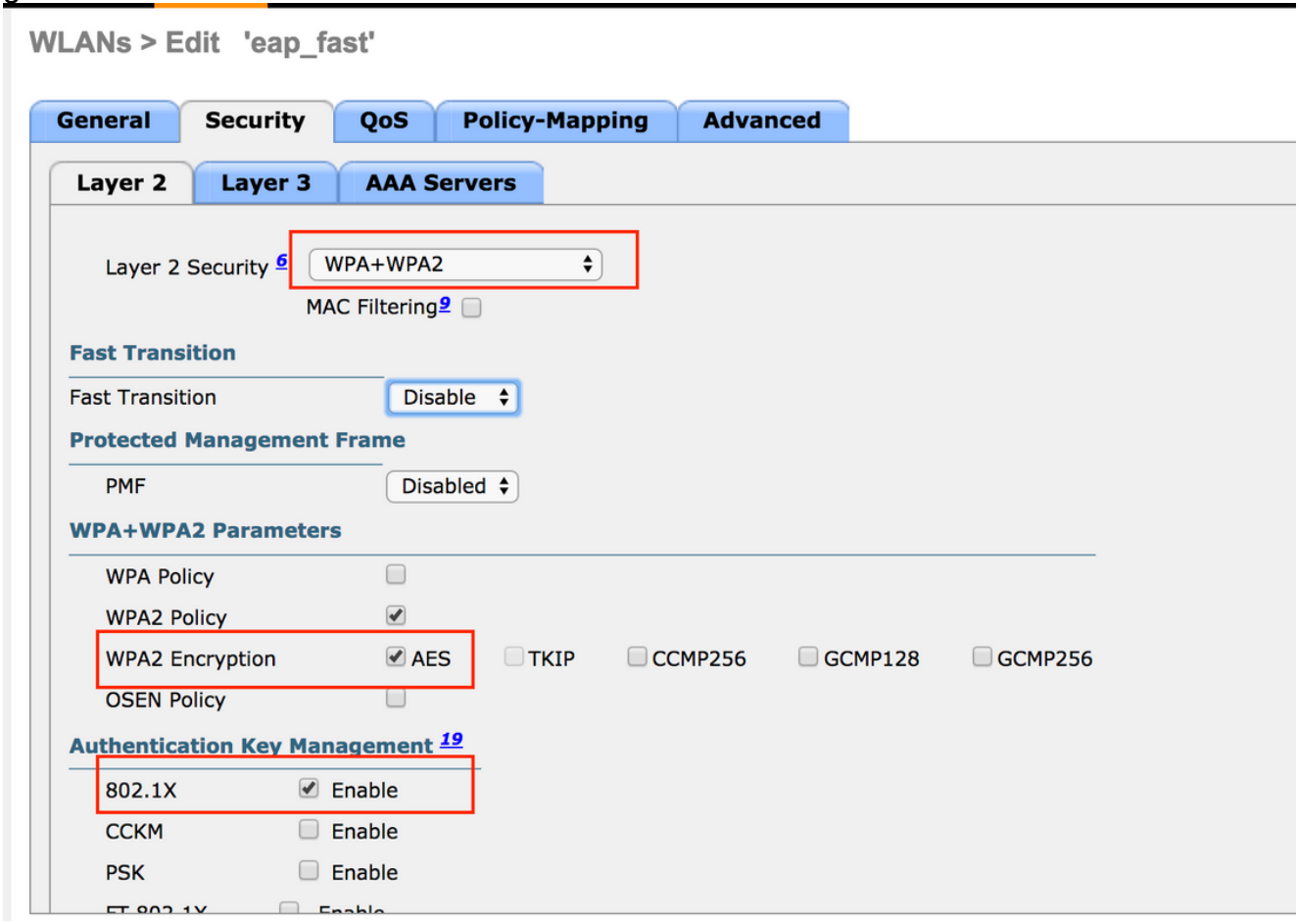
3. Konfigurieren Sie auf der Seite WLANs > New den Namen **eap_fast** WLAN-SSID, den Profilnamen und die WLAN-ID. Klicken Sie anschließend auf **Übernehmen**.

4. Sobald Sie ein neues WLAN erstellt haben, wird die Seite **WLAN > Bearbeiten** für das neue WLAN angezeigt. Auf dieser Seite können Sie verschiedene Parameter für dieses WLAN definieren. Dies umfasst allgemeine Richtlinien, RADIUS-Server, Sicherheitsrichtlinien und 802.1x-Parameter.
5. Aktivieren Sie das Kontrollkästchen **Admin Status** unter **Allgemeine Richtlinien**, um das WLAN zu aktivieren. Wenn der Access Point die SSID in seinen Beacon-Frames übertragen soll, aktivieren Sie das Kontrollkästchen **Broadcast SSID (SSID senden)**.

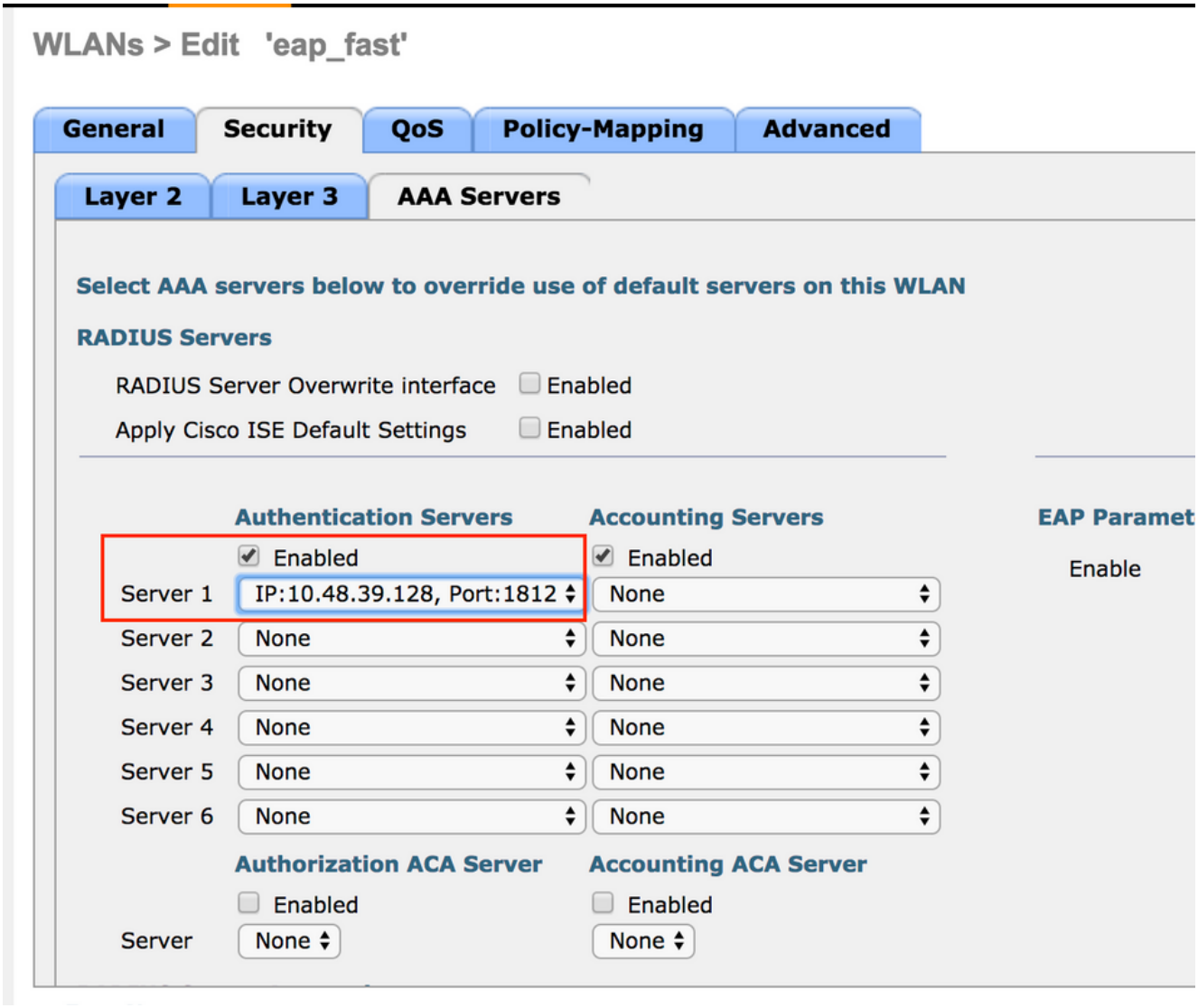


6. Unter **"WLAN -> Edit -> Security -> Layer 2"** Wählen Sie die WPA/WPA2-Parameter aus, und

wählen Sie dot1x für AKM aus.
In diesem Beispiel wird WPA2/AES + dot1x als Layer-2-Sicherheit für dieses WLAN verwendet. Die anderen Parameter können je nach Anforderung des WLAN-Netzwerks geändert werden.



7. Wählen Sie unter **"WLAN -> Edit -> Security -> AAA Servers"** im Dropdown-Menü unter RADIUS Servers den entsprechenden RADIUS-Server aus.



8. Klicken Sie auf **Übernehmen**.**Hinweis:** Dies ist die einzige EAP-Einstellung, die auf dem Controller für die EAP-Authentifizierung konfiguriert werden muss. Alle anderen EAP-FAST-spezifischen Konfigurationen müssen auf dem RADIUS-Server und den zu authentifizierenden Clients ausgeführt werden.

Konfigurieren des RADIUS-Servers für die EAP-FAST-Authentifizierung

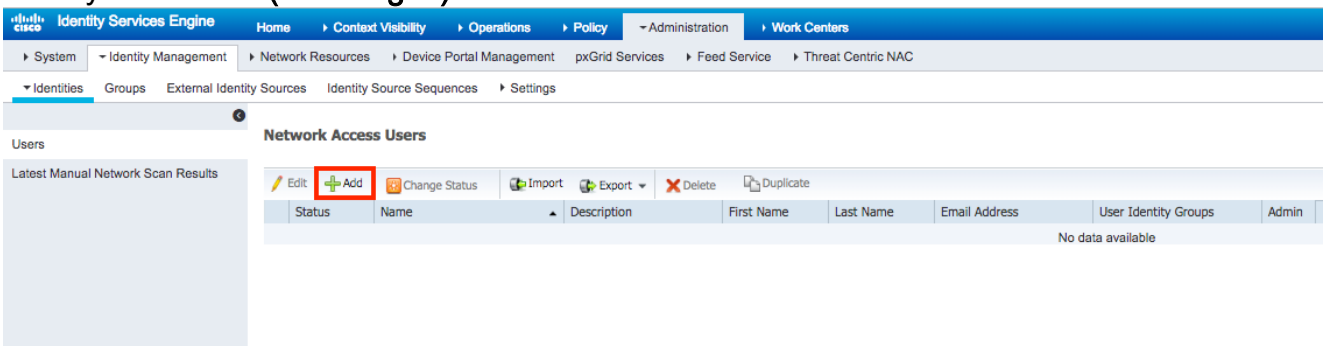
Führen Sie die folgenden Schritte aus, um den RADIUS-Server für die EAP-FAST-Authentifizierung zu konfigurieren:

1. Erstellen einer Benutzerdatenbank zum Authentifizieren von EAP-FAST-Clients
2. Hinzufügen des WLC als AAA-Client zum RADIUS-Server
3. Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit anonymer In-Band-PAC-Bereitstellung
4. Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit authentifizierter In-Band-PAC-Bereitstellung

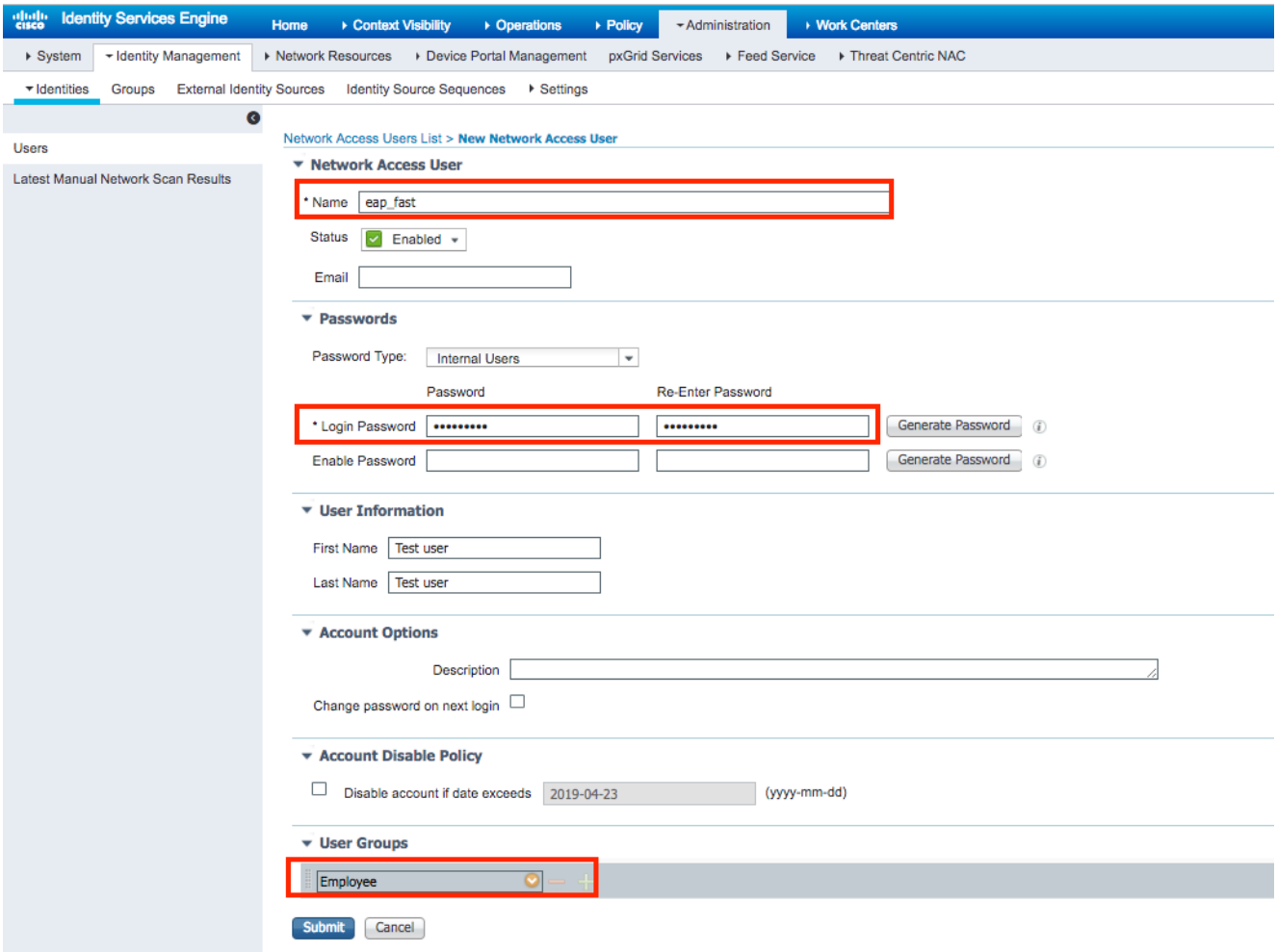
Erstellen einer Benutzerdatenbank zum Authentifizieren von EAP-FAST-Clients

In diesem Beispiel werden Benutzername und Kennwort des EAP-FAST-Clients als <*eap_fast*> bzw. <*EAP-fast1*> konfiguriert.

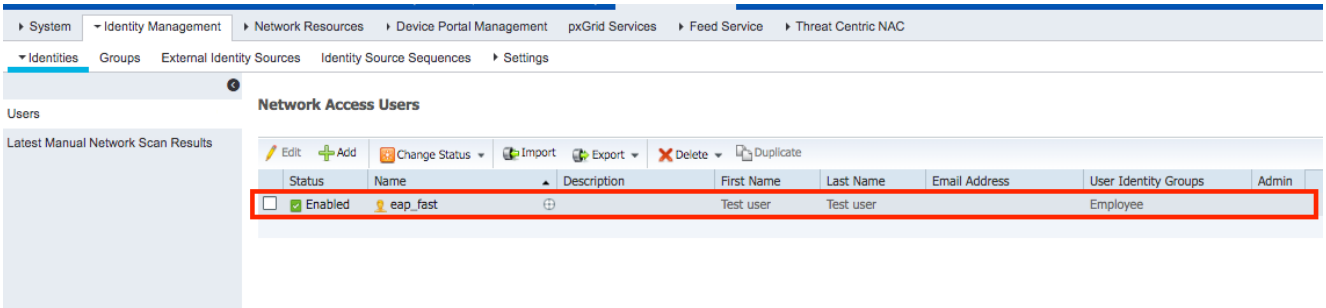
1. Navigieren Sie in der ISE Web-Admin-Benutzeroberfläche unter **"Administration -> Identity Management -> Users" (Verwaltung -> Identitätsverwaltung -> Benutzer),** und drücken Sie das Symbol **"Add" (Hinzufügen)**.



2. Füllen Sie die erforderlichen Formulare für den zu erstellenden Benutzer aus: **"Name"** und **"Anmeldekennwort"** und wählen Sie **"Benutzergruppe"** aus der Dropdown-Liste aus.[Optional können Sie weitere Informationen für das Benutzerkonto eingeben]
Drücken Sie **"Sumbit"**.



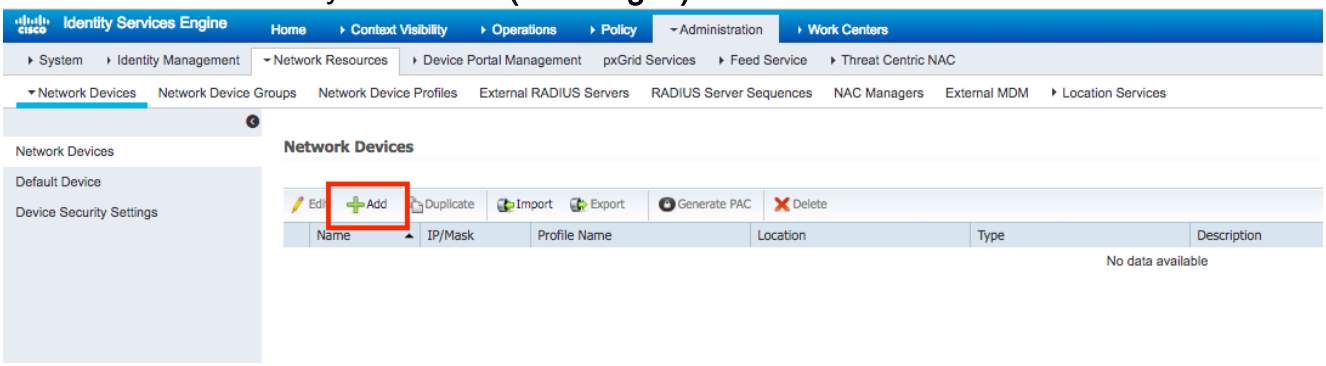
3. Der Benutzer wird erstellt.



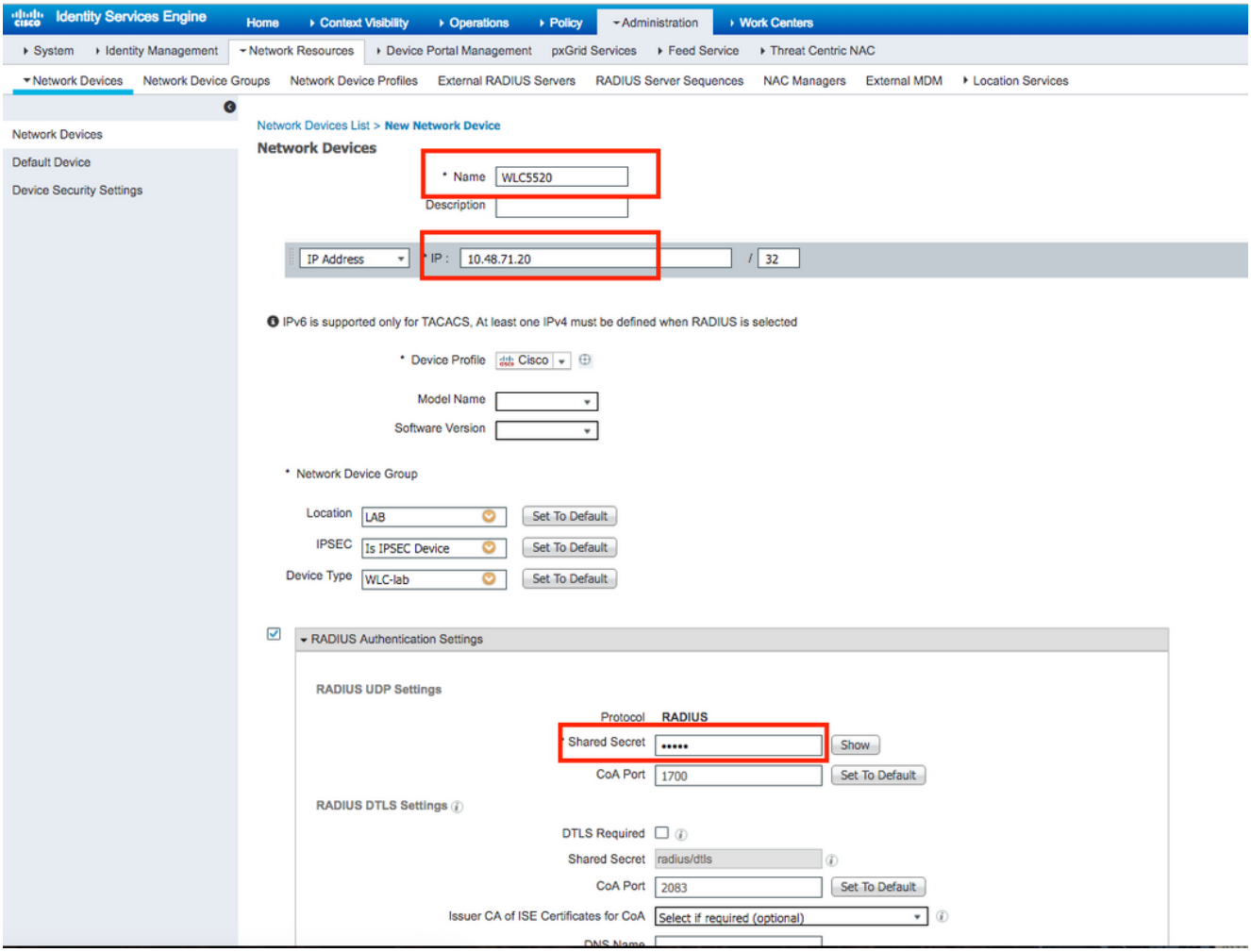
Hinzufügen des WLC als AAA-Client zum RADIUS-Server

Gehen Sie wie folgt vor, um den Controller als AAA-Client auf dem ACS-Server zu definieren:

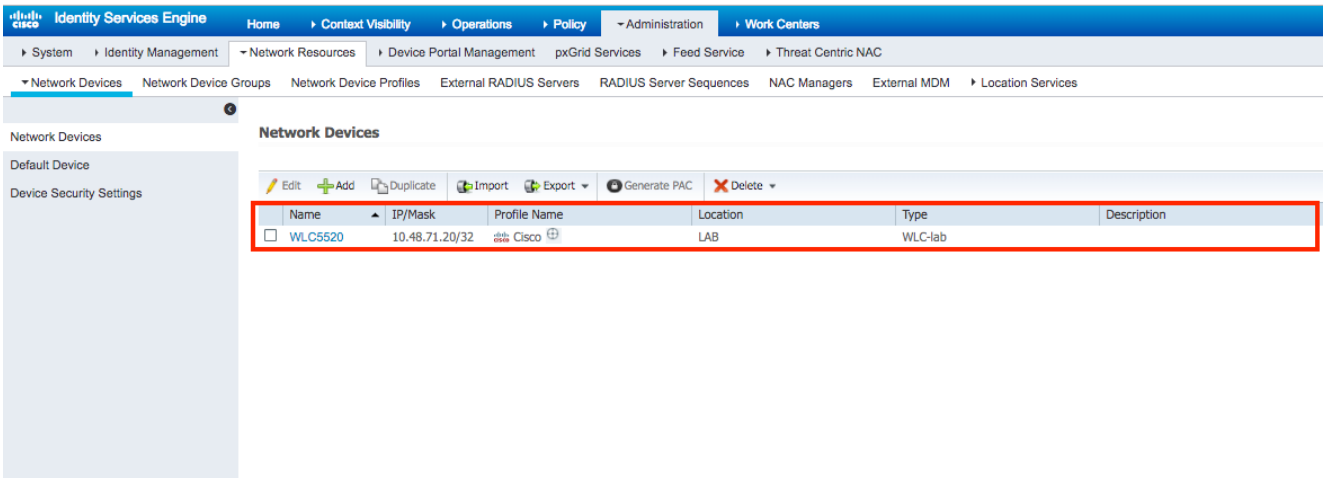
1. Navigieren Sie in der ISE Web-Admin-Benutzeroberfläche unter **"Administration -> Network Resources -> Network Devices" (Verwaltung -> Netzwerkressourcen -> Netzwerkgeräte),** und drücken Sie das Symbol **"Add" (Hinzufügen)**.



2. Füllen Sie die erforderlichen Formulare für das hinzuzufügende Gerät aus: "**Name**", "**IP**" und konfigurieren Sie das gleiche gemeinsam genutzte geheime Kennwort, wie im vorherigen Abschnitt für WLC konfiguriert wurde, im Formular "**Gemeinsamer geheimer Schlüssel**" [optional können Sie weitere Informationen für das Gerät wie Standort, Gruppe usw. eingeben].
Drücken Sie "**Sumbit**".



3. Gerät wird der Liste der ISE-Netzwerkzugriffsgeräte hinzugefügt. (NAD)

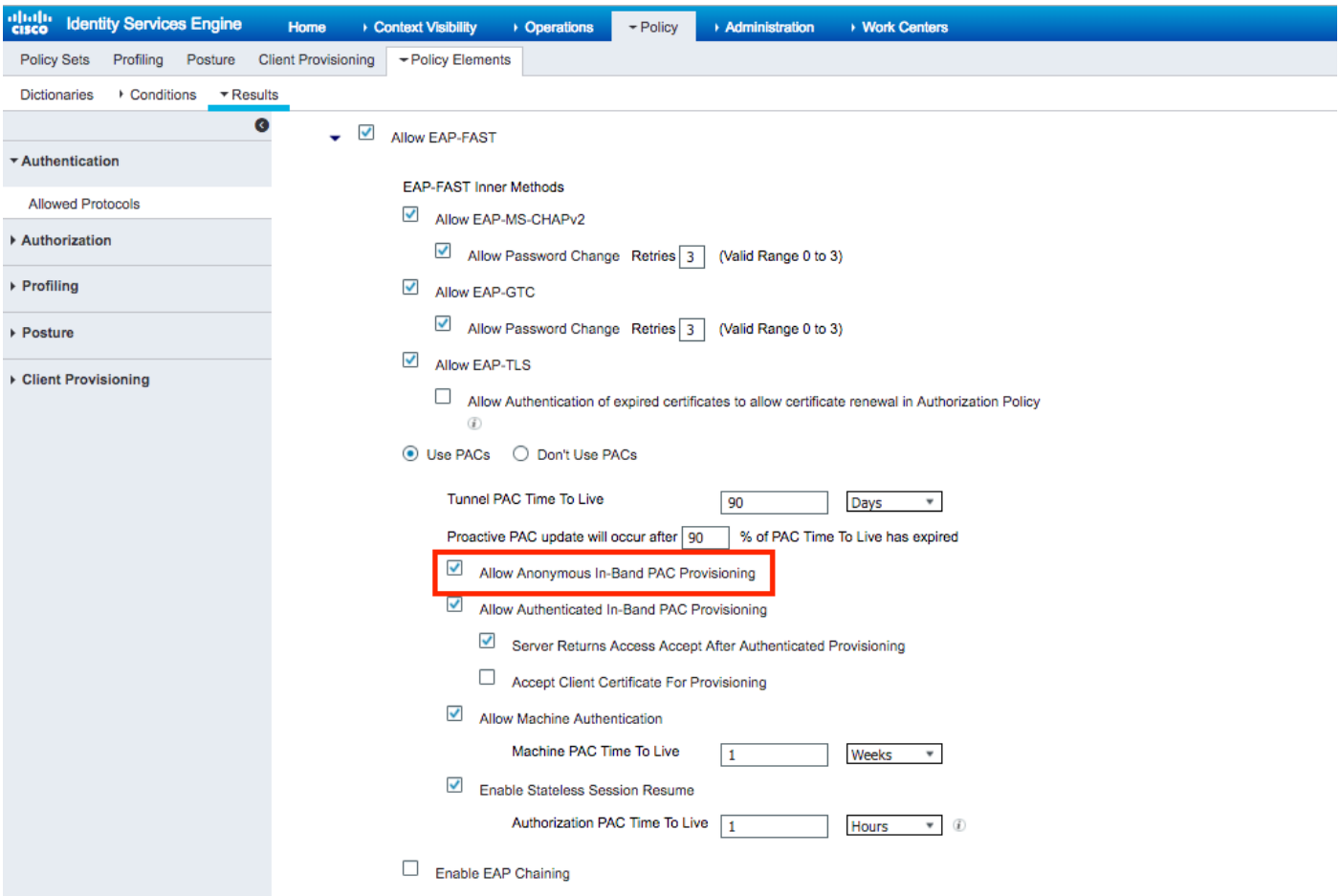


Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit anonymer In-Band-PAC-Bereitstellung

Im Allgemeinen sollte dieser Methodentyp verwendet werden, falls die Bereitstellung nicht über eine PKI-Infrastruktur verfügt.

Diese Methode wird in einem Authenticated Diffie-HellmanKey Agreement Protocol (ADHP)-Tunnel ausgeführt, bevor der Peer den ISE-Server authentifiziert.

Um diese Methode zu unterstützen, müssen wir "**Anonyme In-Band-PAC-Bereitstellung zulassen**" auf der ISE unter "**Authentifizierungs-zulässige Protokolle**" aktivieren:



Hinweis: Stellen Sie sicher, dass Sie die Kennworttypauthentifizierung zugelassen haben, wie z. B. EAP-MS-CHAPv2 für die innere EAP-FAST-Methode, da wir bei der anonymen In-Band-

Bereitstellung natürlich keine Zertifikate verwenden können.

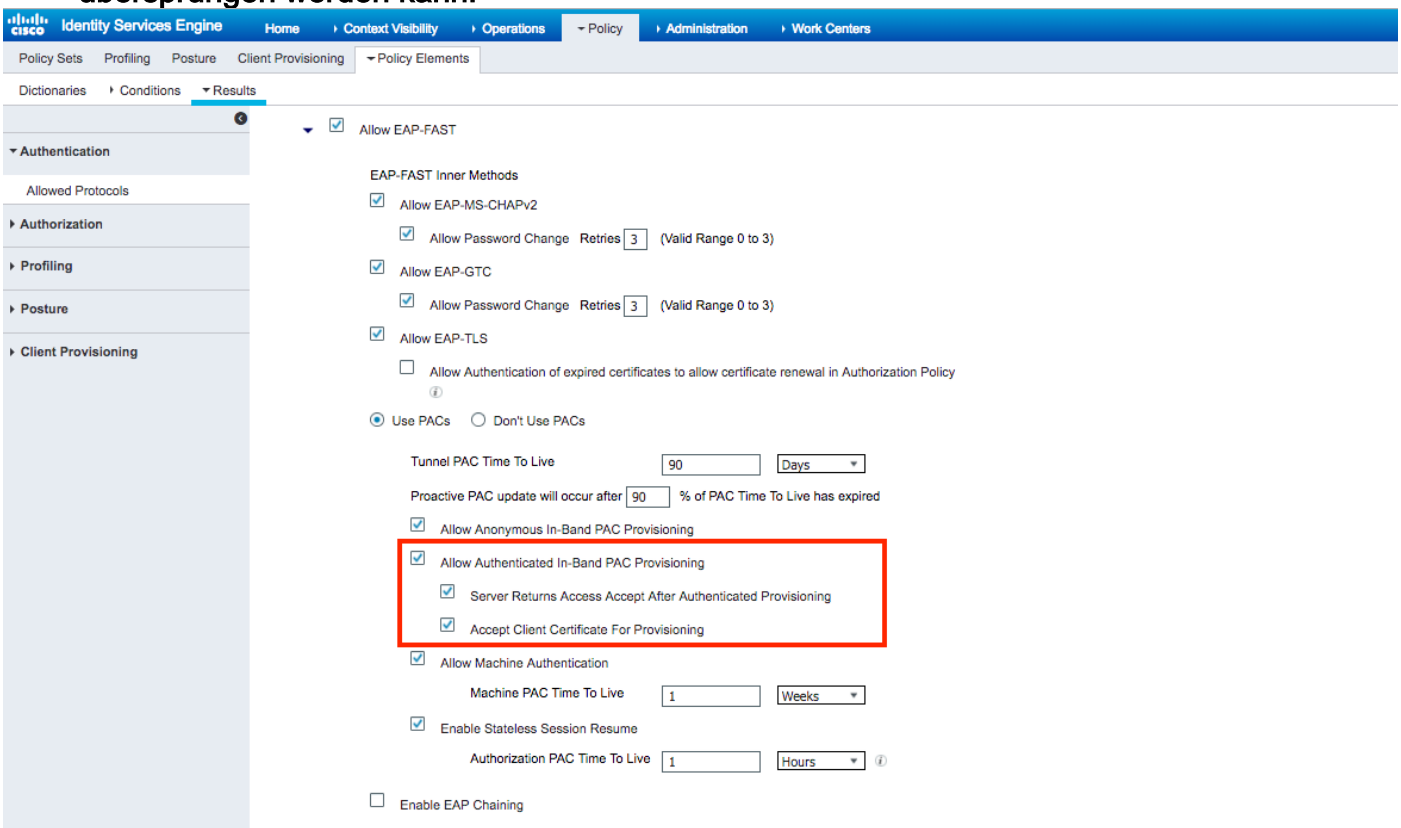
Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit authentifizierter In-Band-PAC-Bereitstellung

Dies ist die sicherste und empfohlene Option. Der TLS-Tunnel basiert auf dem Serverzertifikat, das vom Supplicant validiert wird, und das Client-Zertifikat wird durch die ISE validiert (Standard).

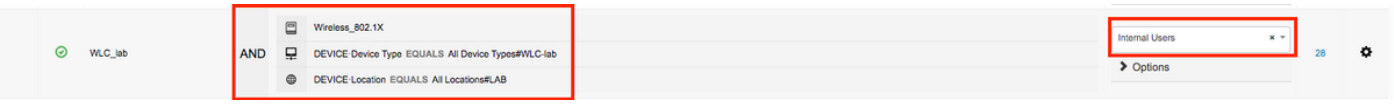
Für diese Option ist eine PKI-Infrastruktur für Client und Server erforderlich, die jedoch möglicherweise auf Serverseite beschränkt oder auf beiden Seiten übersprungen wird.

Für die ISE gibt es zwei zusätzliche Optionen für die authentifizierte In-Band-Bereitstellung:

1. **"Server Returns Access Accept After Authenticated Provisioning"** - Normalerweise sollte nach der PAC-Bereitstellung eine Access-Reject gesendet werden, die den Supplicant zur erneuten Authentifizierung mithilfe von PACs zwingt. Da die PAC-Bereitstellung jedoch im authentifizierten TLS-Tunnel erfolgt, können wir sofort mit Access-Accept reagieren, um die Authentifizierungszeit zu minimieren. (in diesem Fall sollten Sie sich vergewissern, dass Sie auf Client- und Serverseite vertrauenswürdige Zertifikate besitzen).
2. **"Accept Client Certificate For Provisioning" - Wenn Client-Geräte keine PKI-Infrastruktur bereitstellen und nur über ein vertrauenswürdiges Zertifikat für die ISE verfügen sollen, aktivieren Sie diese Option, mit der die Validierung von Client-Zertifikaten auf Serverseite übersprungen werden kann.**



Auf der ISE definieren wir auch einfache Authentifizierungsrichtlinien für Wireless-Benutzer. Im folgenden Beispiel werden Gerätetyp und Standort sowie Authentifizierungstyp als Verbindungsparameter verwendet. Der Authentifizierungsfluss, der dieser Bedingung entspricht, wird anhand der internen Benutzerdatenbank validiert.



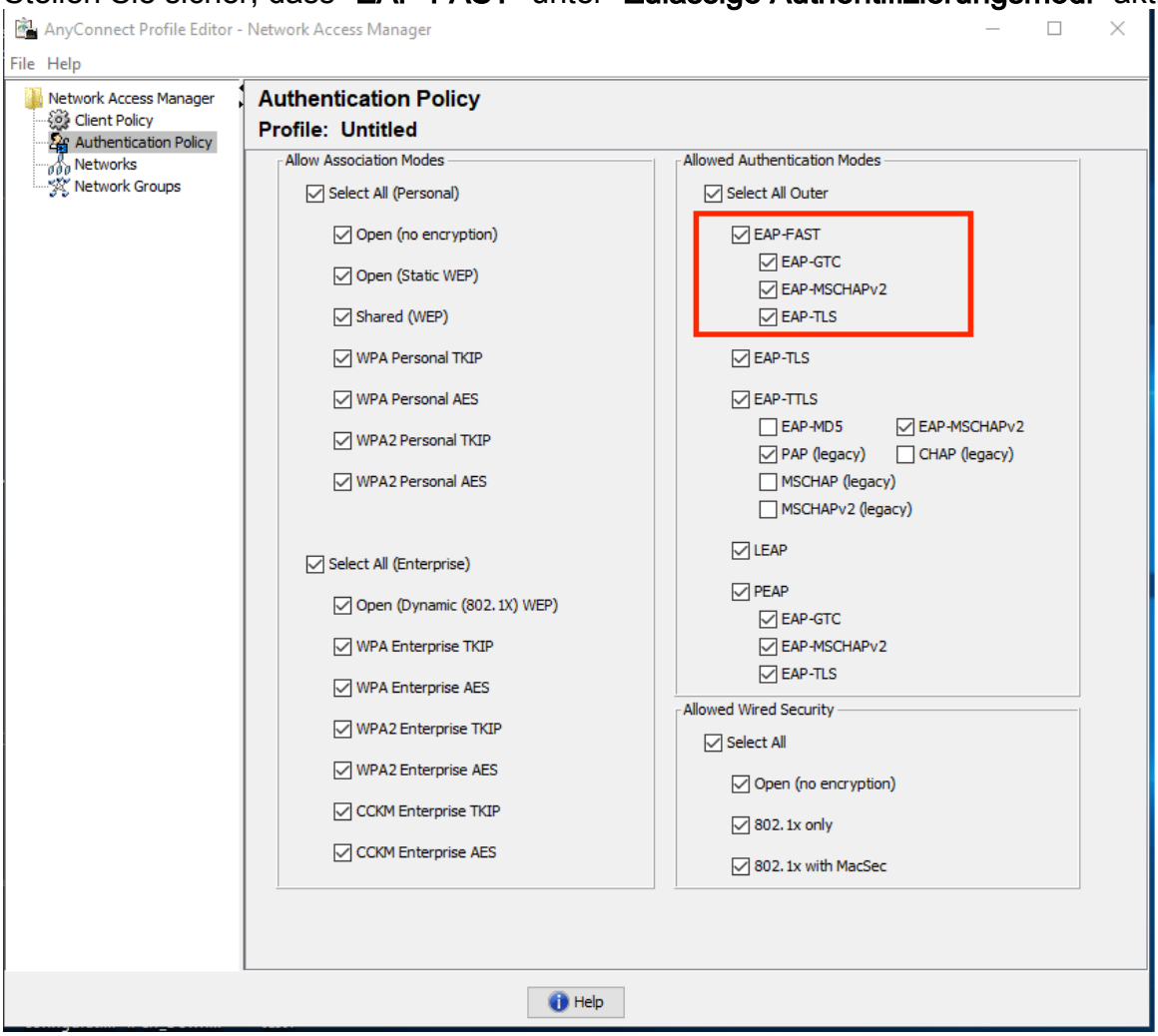
Überprüfen

In diesem Beispiel werden die Konfigurationseinstellungen für den Authenticated In-Band PAC Provisioning Flow und den Network Access Manager (NAM) zusammen mit den entsprechenden WLC-Debuggen angezeigt.

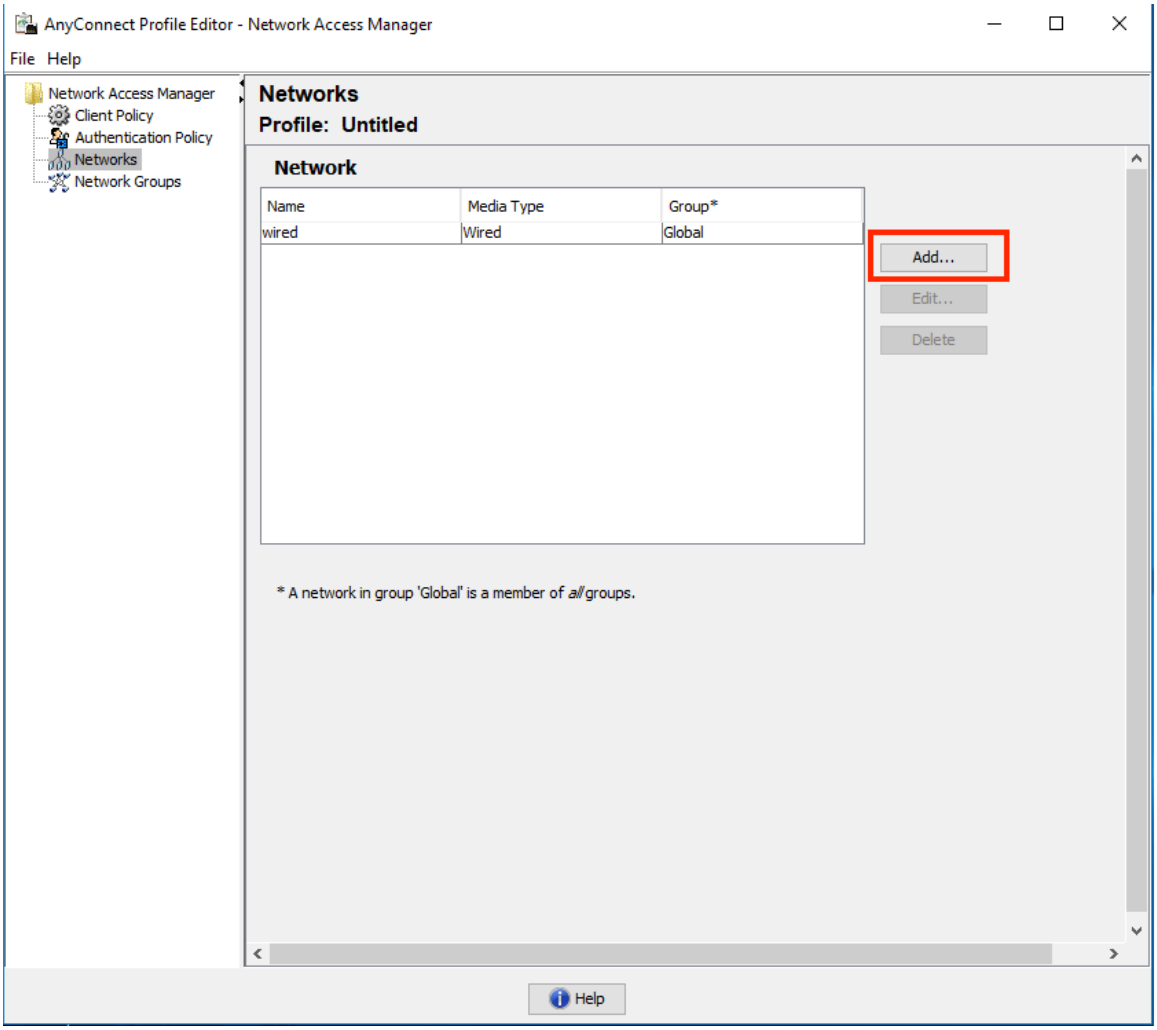
NAM-Profilkonfiguration

Die folgenden Schritte müssen ausgeführt werden, um das AnyConnect NAM-Profil für die Authentifizierung von Benutzersitzungen mit der ISE mithilfe von EAP-FAST zu konfigurieren:

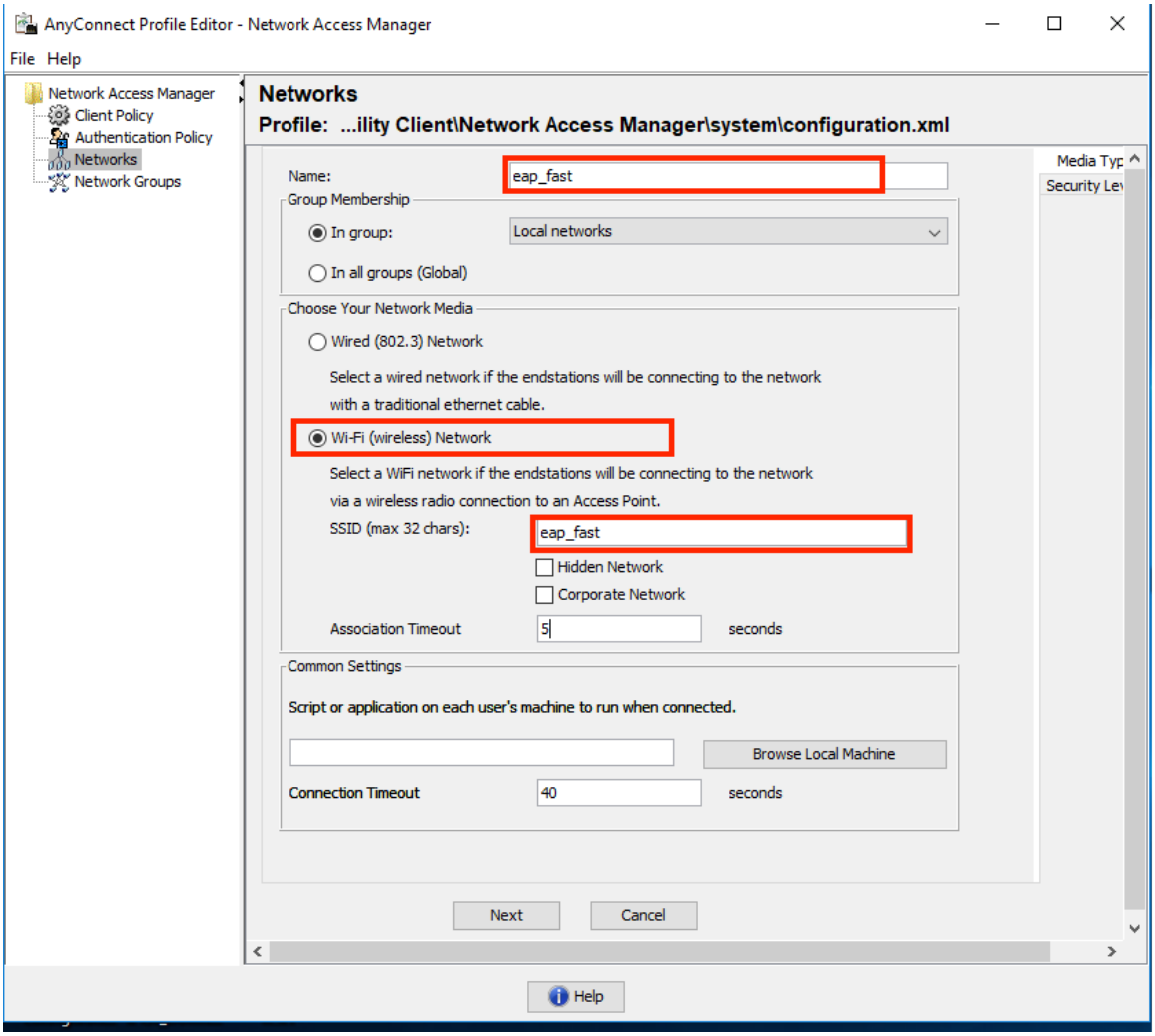
1. Öffnen Sie den Network Access Manager Profile Editor, und laden Sie die aktuelle Konfigurationsdatei.
2. Stellen Sie sicher, dass "**EAP-FAST**" unter **"Zulässige Authentifizierungsmodi"** aktiviert ist.



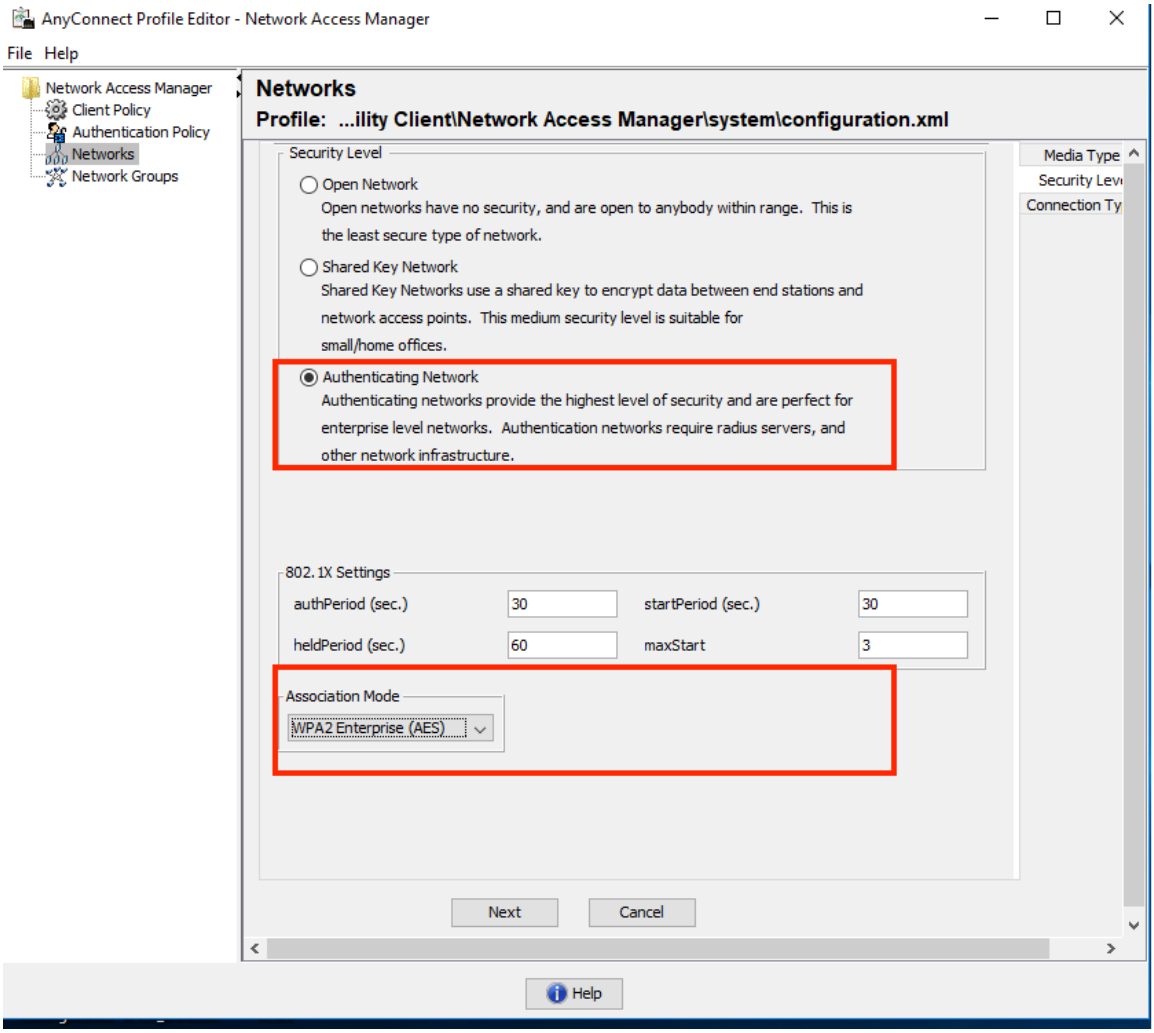
3. Neues Netzwerkprofil "**hinzufügen**":



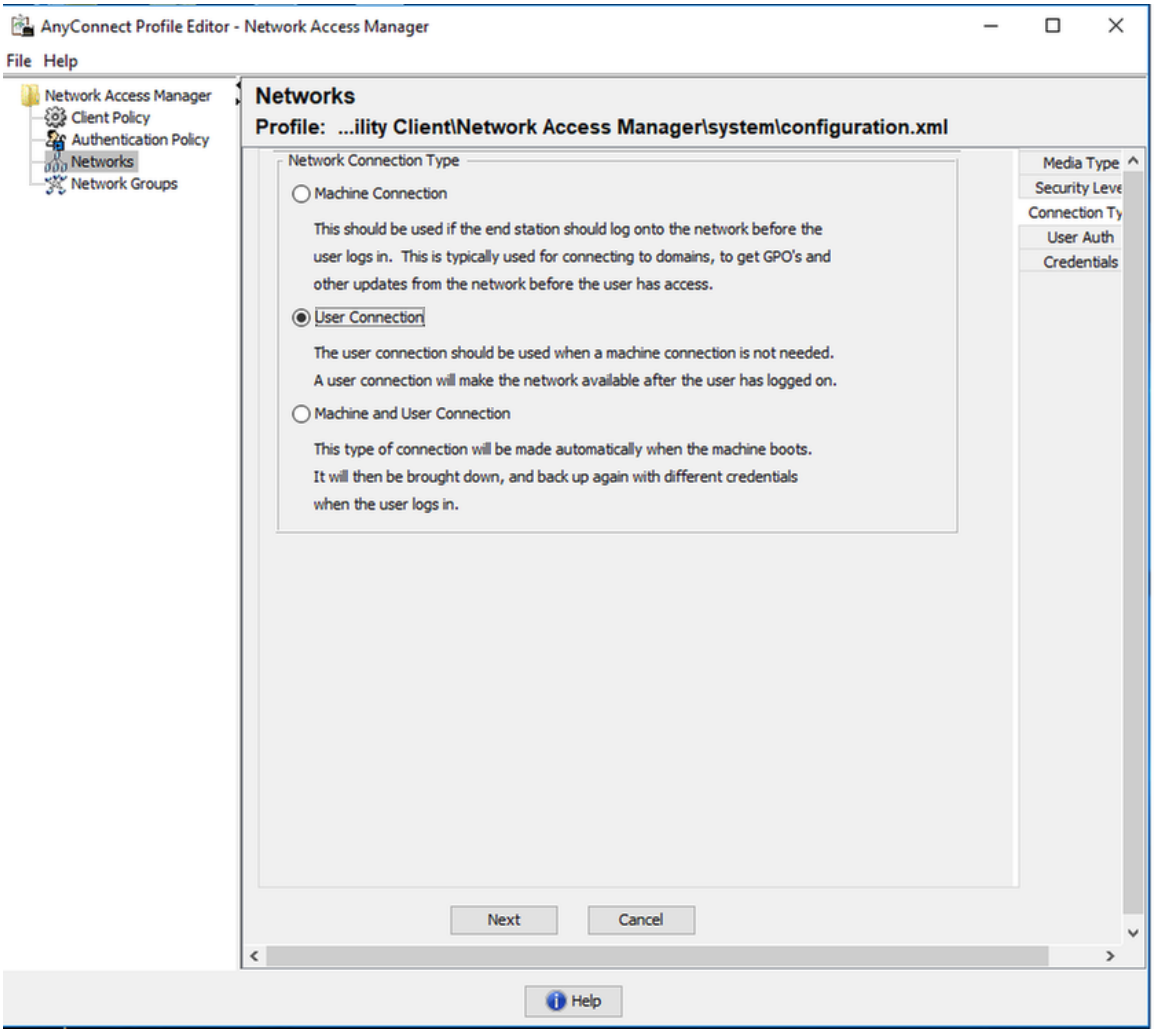
4. Im Konfigurationsabschnitt **"Medientyp"** definieren Sie das Profil "**Name**", das Wireless-Netzwerk als Ihren Mediennetzwerktyp und geben den SSID-Namen an.



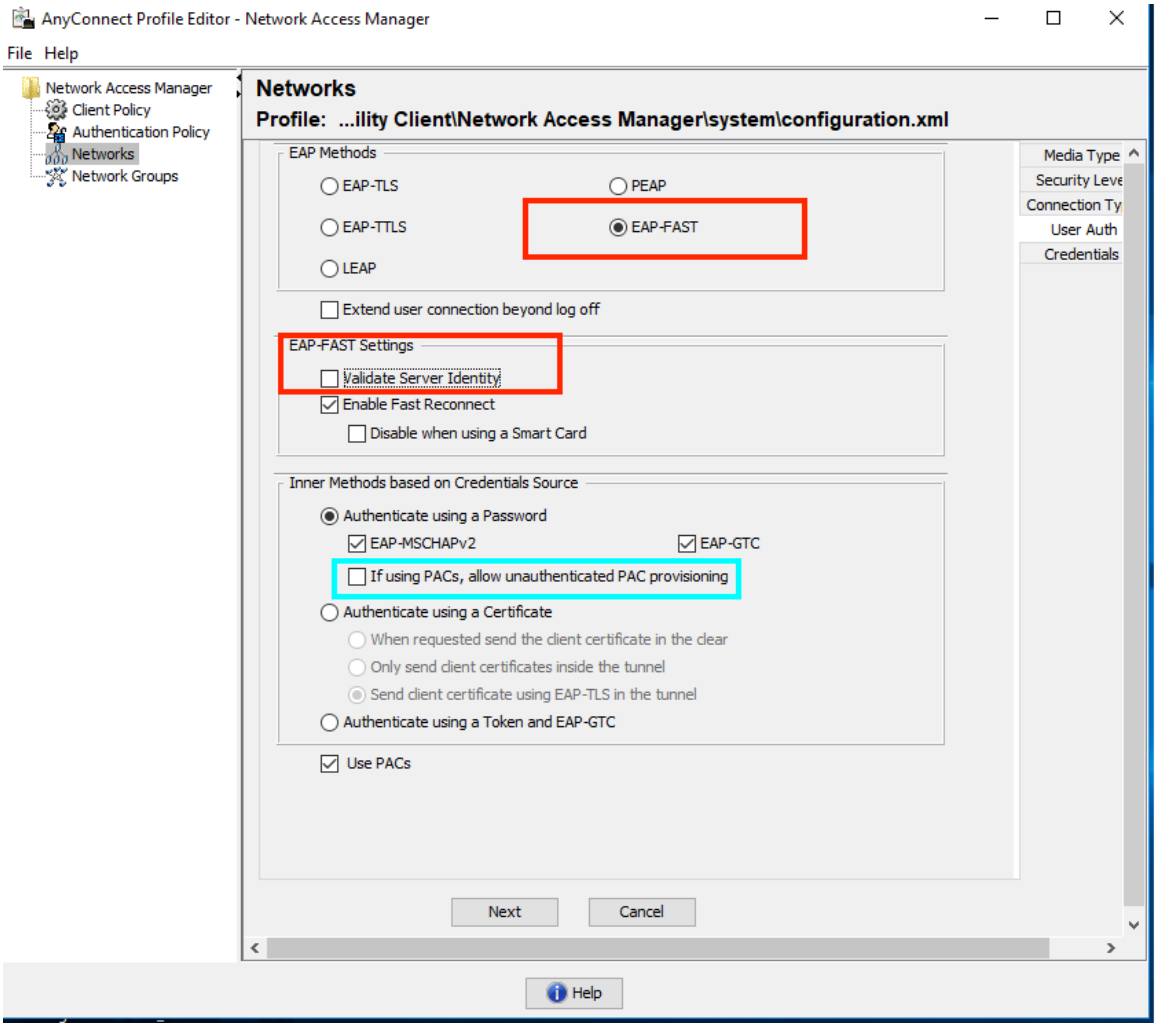
5. Wählen Sie auf der Registerkarte "**Sicherheitsstufe**" die Option "Authenticating Network" (Netzwerk authentifizieren) aus, und geben Sie den Zuordnungsmodus als WPA2 Enterprise (AES) an.



6. In diesem Beispiel wird die Benutzertypauthentifizierung verwendet. Wählen Sie daher unter der nächsten Registerkarte "**Verbindungstyp**" die Option "**Benutzerverbindung".**

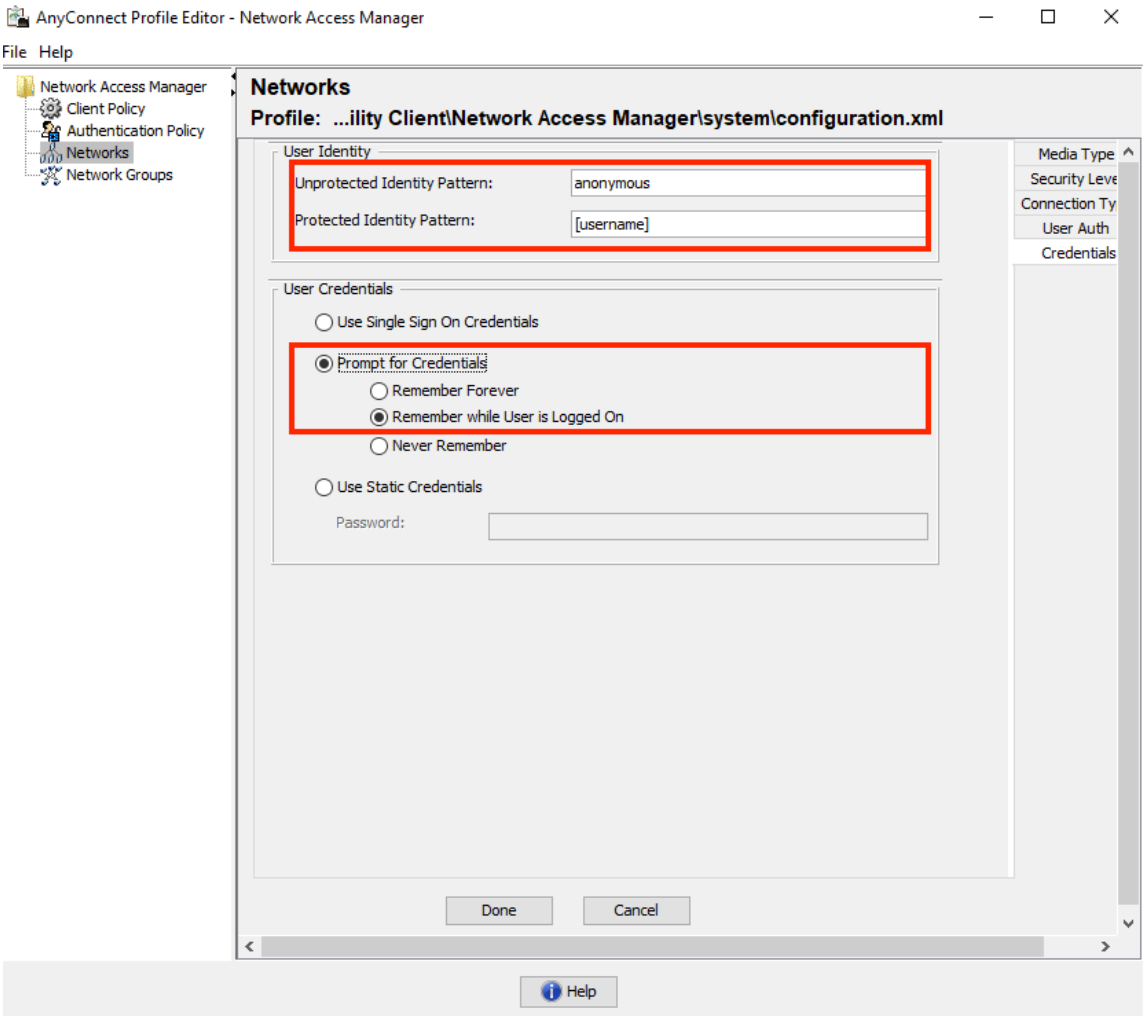


7. Geben Sie auf der Registerkarte "**User Auth**" (Benutzerauthentifizierung) EAP-FAST als zulässige Authentifizierungsmethode an, und deaktivieren Sie die Validierung von Serverzertifikaten, da in diesem Beispiel keine vertrauenswürdigen Zertifikate verwendet werden.



Hinweis: Stellen Sie in der realen Produktionsumgebung sicher, dass Sie auf der ISE installiertes Zertifikat installiert haben, und lassen Sie die Option zur Validierung von Serverzertifikaten in den NAM-Einstellungen aktiviert.
Hinweis: Option "Bei Verwendung von PACs muss die nicht authentifizierte PAC-Bereitstellung zugelassen werden" nur bei anonymer In-Band-PAC-Bereitstellung ausgewählt werden.

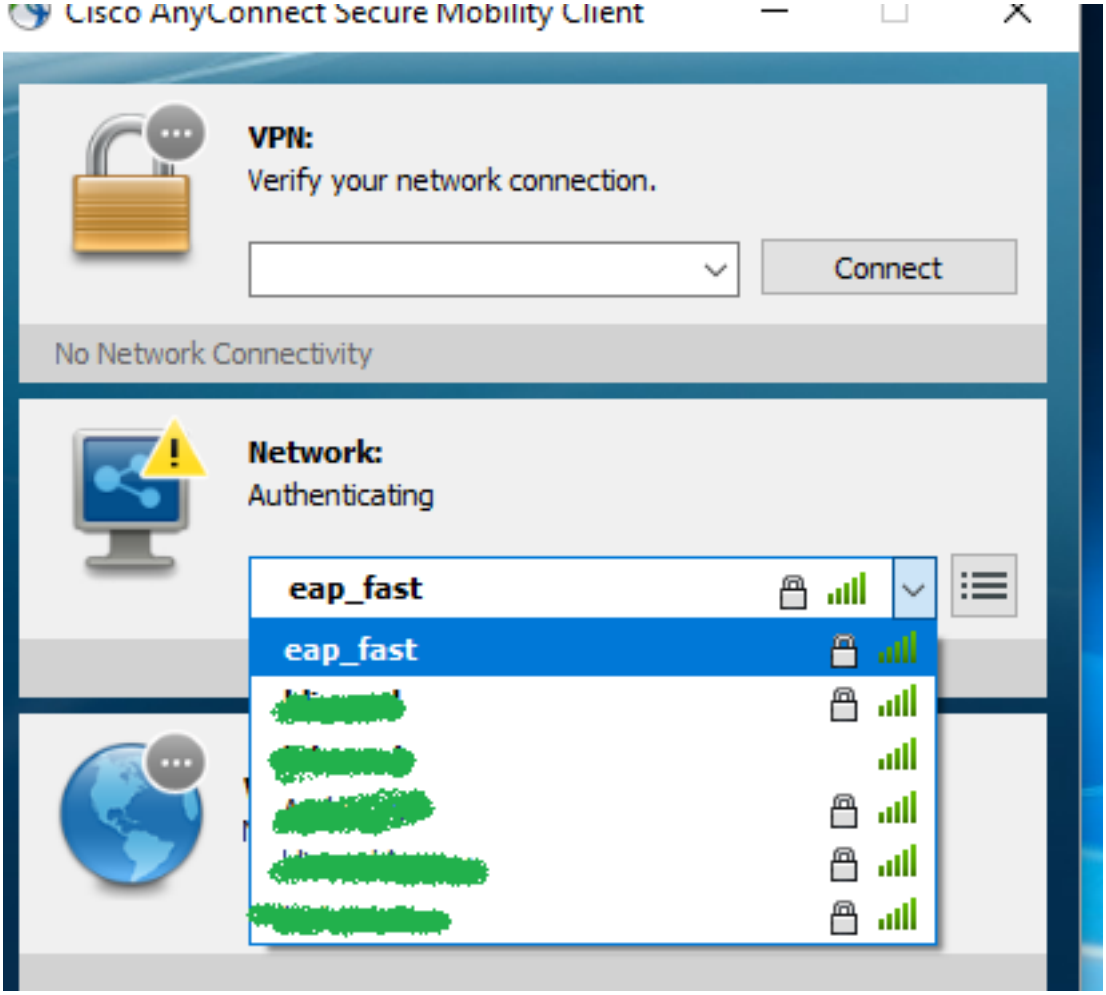
8. Definieren Sie Benutzeranmeldeinformationen, entweder als SSO für den Fall, dass Sie dieselben Anmeldeinformationen wie für die Anmeldung verwenden möchten, oder wählen Sie "Aufforderung zur Eingabe von Anmeldeinformationen" aus, falls der Benutzer bei der Verbindung mit dem Netzwerk um Anmeldeinformationen gebeten werden soll, oder definieren Sie statische Anmeldeinformationen für diesen Zugriffstyp. In diesem Beispiel wird der Benutzer beim Verbindungsversuch mit dem Netzwerk zur Eingabe von Anmeldeinformationen aufgefordert.



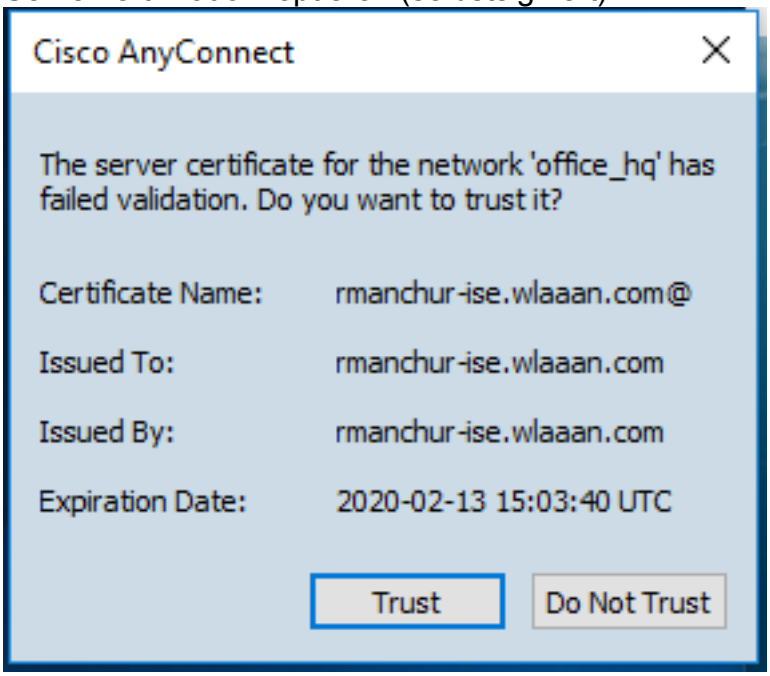
9. Speichern Sie das konfigurierte Profil im entsprechenden NAM-Ordner.

Testen Sie die Verbindung zum SSID mithilfe der EAP-FAST-Authentifizierung.

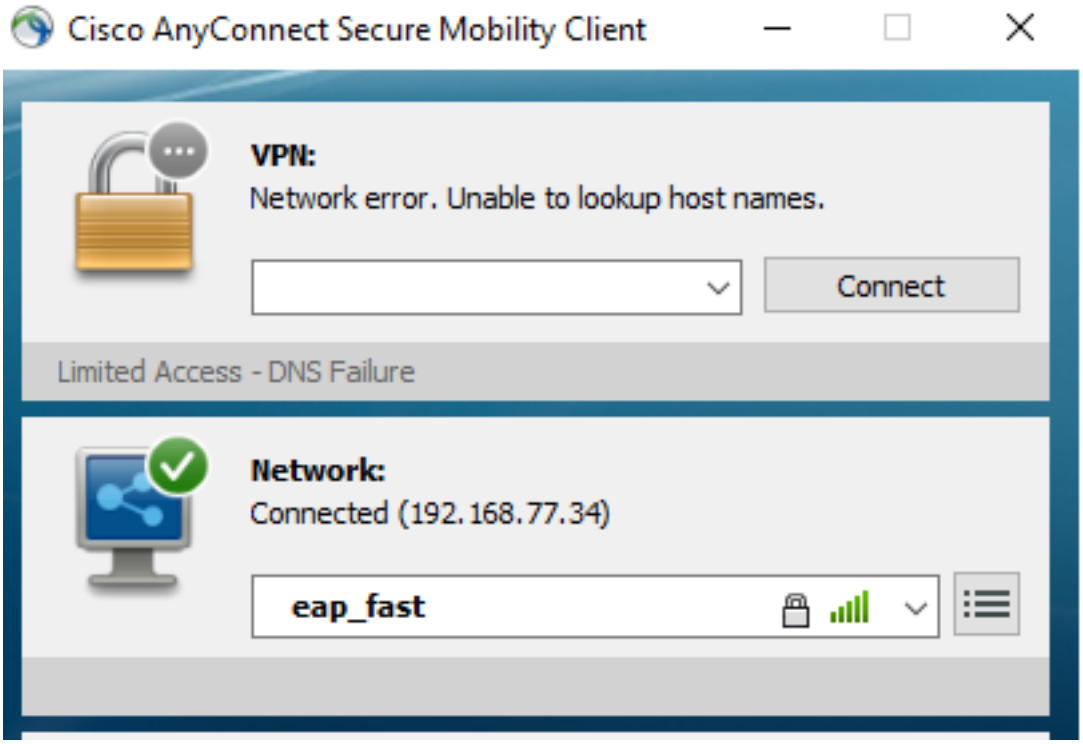
1. Wählen Sie das entsprechende Profil aus der AnyConnect-Netzwerkliste aus



2. Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung ein.
3. Serverzertifikat akzeptieren (selbstsigniert)



4. Fertig



ISE-Authentifizierungsprotokolle

ISE-Authentifizierungsprotokolle, die den EAP-FAST- und PAC-Bereitstellungs-Flow anzeigen, sind unter "**Operations -> RADIUS -> Live Logs**" (**Vorgänge -> RADIUS -> Live Logs**) zu sehen und können mithilfe des Symbols "**Zoom**" detaillierter dargestellt werden:

1. Der Client hat mit der Authentifizierung begonnen, und die ISE schlug EAP-TLS als Authentifizierungsmethode vor. Der Client lehnte jedoch EAP-FAST ab und schlug dies vor. Dabei handelte es sich um die vereinbarte Methode für Client und ISE.

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. Der TLS-Handshake wurde zwischen Client und Server gestartet, um eine geschützte Umgebung für den PAC-Austausch bereitzustellen, und wurde erfolgreich abgeschlossen.

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. Die interne Authentifizierung wurde gestartet, und die Benutzeranmeldeinformationen wurden mithilfe von MS-CHAPv2 erfolgreich von der ISE validiert (Authentifizierung auf Basis von Benutzernamen/Kennwort).