Konfigurieren von Secure Client NAM für Dot1x mit Windows und ISE 3.2

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Konfigurieren
  - Netzwerkdiagramm
  - Konfigurationen
    - 1. Laden Sie Secure Client NAM (Network Access Manager) herunter, und installieren Sie es.
    - 2. Laden Sie den Secure Client NAM Profile Editor herunter, und installieren Sie ihn.
    - 3. Allgemeine Standardkonfigurationen
    - 4. Szenario 1: Konfigurieren der Secure Client NAM-Komponente für die PEAP-Benutzerauthentifizierung (MS-CHAPv2)
    - 5. Szenario 2: Konfigurieren der Secure Client NAM-Komponente für die gleichzeitige EAP-FAST-Benutzer- und Geräteauthentifizierung
    - 6. Szenario 3: Konfigurieren der Secure Client NAM-Komponente für die EAP TLS-Benutzerzertifikatauthentifizierung
    - 7. Konfigurieren von ISR 1100 und ISE zum Zulassen von Authentifizierungen basierend auf PEAP MSCHAPv2 aus Szenario 1
- Überprüfung
- Fehlerbehebung
  - Problem: Das NAM-Profil wird von Secure Client nicht verwendet.
  - Problem 2: Protokolle müssen zur weiteren Analyse gesammelt werden.
    - 1. Erweiterte NAM-Protokollierung aktivieren
    - 2. Reproduzieren Sie das Problem.
    - 3. Erfassen Sie das Secure Client DART-Paket.
- Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration des Secure Client Network Analysis Module (NAM) unter Windows beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis einer RADIUS-Komponente
- Punkt 1x
- PEAP
- PKI

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Windows 10 Pro Version 22H2, Build 19045.3930
- ISE 3.2
- Cisco C117 Cisco IOS® XE Software, Version 17.12.02
- Active Directory 2016

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird beschrieben, wie Secure Client NAM unter Windows konfiguriert wird. Es werden die Option "Pre-deploy" und der Profil-Editor für die dot1x-Authentifizierung verwendet. Außerdem werden einige Beispiele dafür gegeben, wie dies erreicht wird.

Im Netzwerk ist ein Supplicant eine Einheit an einem Ende eines Punkt-zu-Punkt-LAN-Segments, die durch einen Authentifikator authentifiziert werden soll, der mit dem anderen Ende dieser Verbindung verbunden ist. Der IEEE 802.1X-Standard verwendet den Begriff "Supplicant" für Hardware oder Software. In der Praxis ist eine Komponente eine Softwareanwendung, die auf einem Endbenutzercomputer installiert ist. Der Benutzer ruft die Komponente auf und sendet Anmeldeinformationen, um den Computer mit einem sicheren Netzwerk zu verbinden. Wenn die Authentifizierung erfolgreich ist, ermöglicht der Authentifizierer dem Computer in der Regel, eine Verbindung mit dem Netzwerk herzustellen.

Informationen zu Network Access Manager

Network Access Manager ist eine Client-Software, die ein sicheres Layer-2-Netzwerk im Einklang mit den entsprechenden Richtlinien bereitstellt. Es erkennt und wählt das optimale Layer-2-Zugriffsnetzwerk aus und führt eine Geräteauthentifizierung für den Zugriff auf kabelgebundene und Wireless-Netzwerke durch. Network Access Manager verwaltet die Identität von Benutzern und Geräten sowie die für den sicheren Zugriff erforderlichen Netzwerkzugriffsprotokolle. Die Lösung verhindert auf intelligente Weise, dass Endbenutzer Verbindungen herstellen, die gegen vom Administrator definierte Richtlinien verstoßen.

Der Network Access Manager ist Single-Homed-fähig und ermöglicht jeweils nur eine Netzwerkverbindung. Kabelgebundene Verbindungen haben zudem eine höhere Priorität als

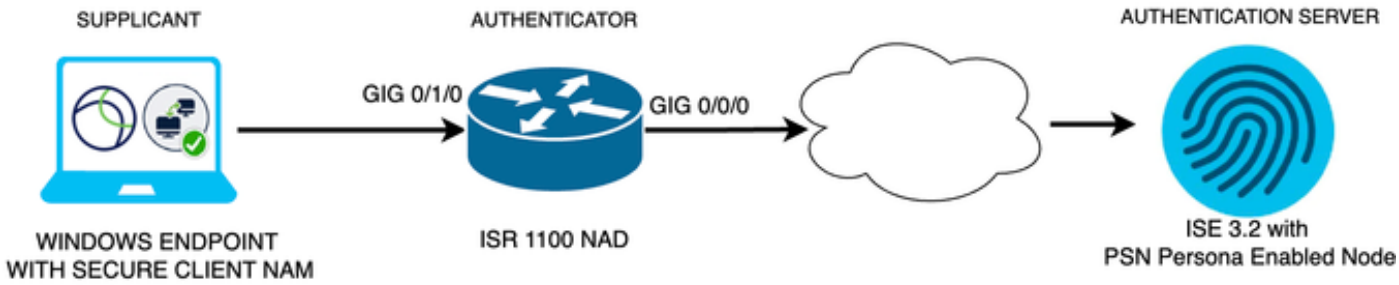
drahtlose Verbindungen. Wenn Sie also über eine Kabelverbindung mit dem Netzwerk verbunden sind, wird der Wireless-Adapter ohne IP-Adresse deaktiviert.

Konfigurieren

Netzwerkdiagramm

Es ist wichtig zu verstehen, dass für dot1x-Authentifizierungen drei Teile erforderlich sind: die Komponente, die dot1x ausführen kann, der Authentifizierer, der auch als NAS/NAD bezeichnet wird und als Proxy dient, der den dot1x-Datenverkehr innerhalb von RADIUS kapselt, und der Authentifizierungsserver.

In diesem Beispiel wird die Komponente auf unterschiedliche Weise installiert und konfiguriert. Später wird ein Szenario mit der Konfiguration des Netzwerkgeräts und dem Authentifizierungsserver angezeigt.



Netzwerkdiagramm

Konfigurationen

1. Herunterladen und Installieren von Secure Client NAM (Network Access Manager)

2. Laden Sie den Secure Client NAM-Profil-Editor herunter, und installieren Sie ihn.
3. Allgemeine Standardkonfigurationen
4. Szenario 1: Konfigurieren der Secure Client NAM-Komponente für die PEAP-Benutzerauthentifizierung (MS-CHAPv2)
5. Szenario 2: Konfigurieren der Secure Client NAM-Komponente für EAP-FAST gleichzeitig mit der Konfiguration der Benutzer- und Geräteauthentifizierung
6. Szenario 3, Teil 1: Konfigurieren der Secure Client NAM-Komponente für EAP-TLS
7. Szenario 3, Teil 2: Konfigurieren der NAD- und ISE-Demo

1. Laden Sie Secure Client NAM (Network Access Manager) herunter, und installieren Sie es.

Cisco Software-Download

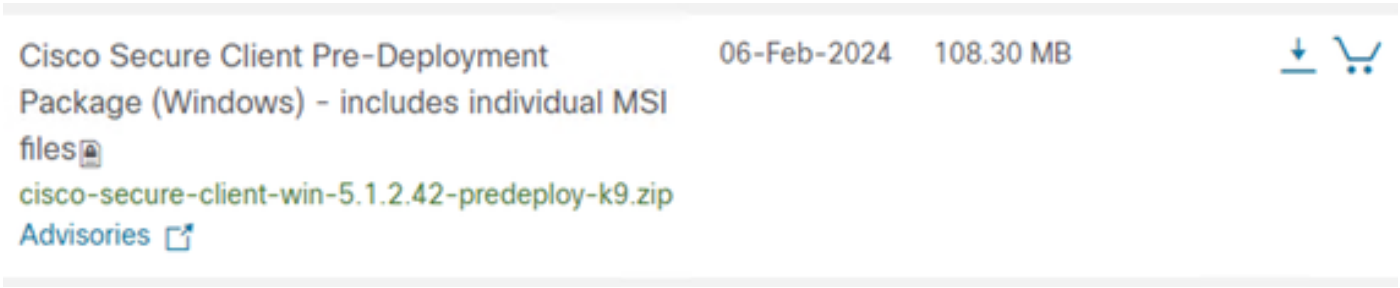
Geben Sie in der Suchleiste des Produktnamens "Secure Client 5" ein.

Downloads Startseite > Sicherheit > VPN- und Endpunkt-Sicherheits-Clients > Sicherer Client (einschließlich AnyConnect) > Sicherer Client 5 > AnyConnect VPN-Client-Software.

In diesem Konfigurationsbeispiel wird Version 5.1.2.42 verwendet.

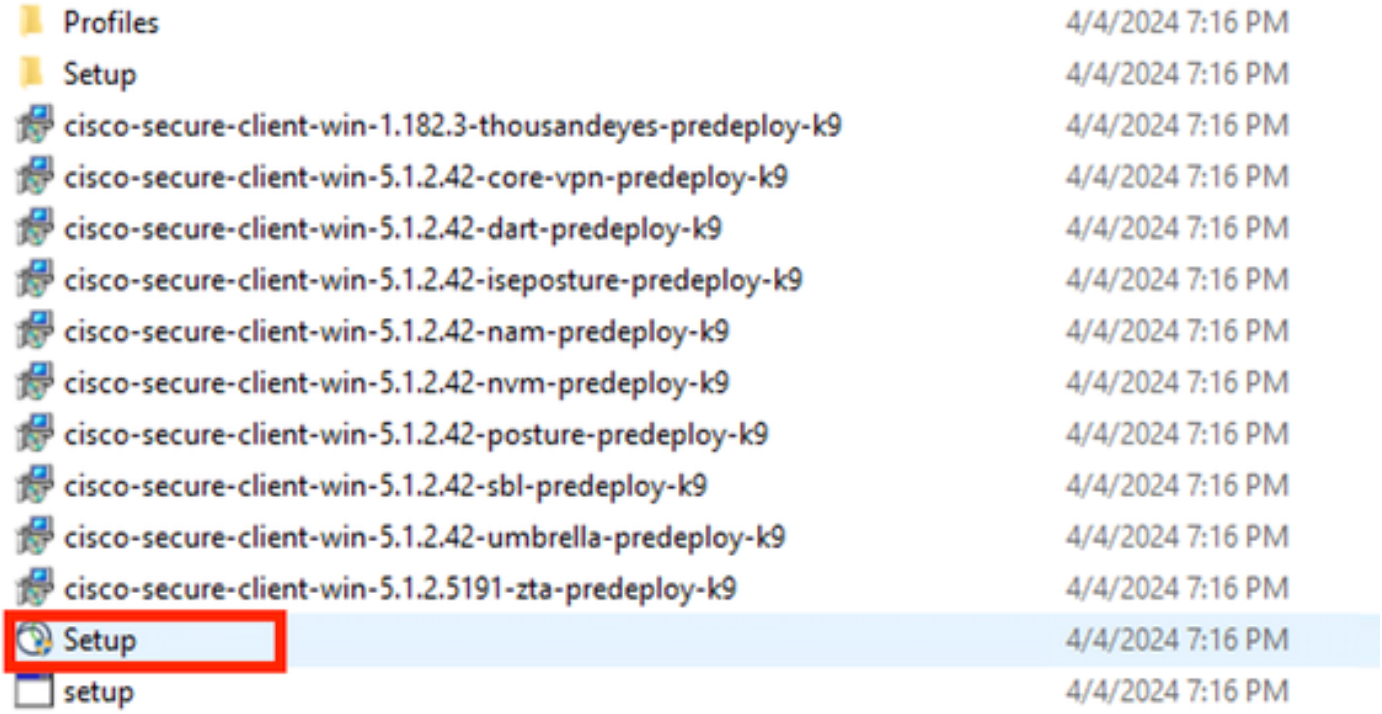
Es gibt mehrere Möglichkeiten, Secure Client auf Windows-Geräten bereitzustellen: über SCCM, die Identity Service Engine und das VPN-Headend. In diesem Artikel wird jedoch als Installationsmethode die Pre-Deploy-Methode verwendet.

Suchen Sie auf der Seite nach der Datei Cisco Secure Client Headend Deployment Package (Windows).



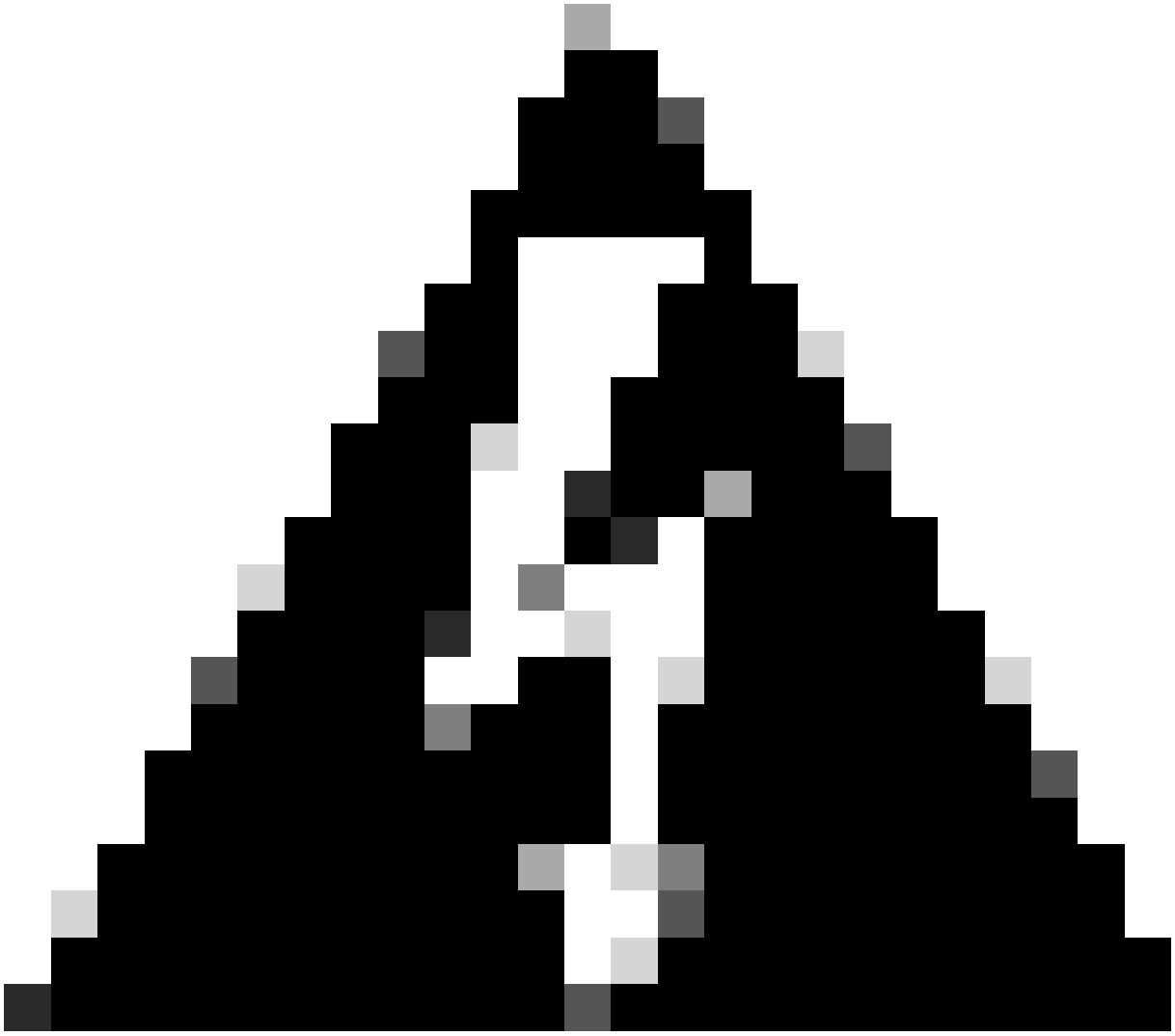
MSI-ZIP-Datei

Klicken Sie nach dem Herunterladen und Entpacken auf Setup.

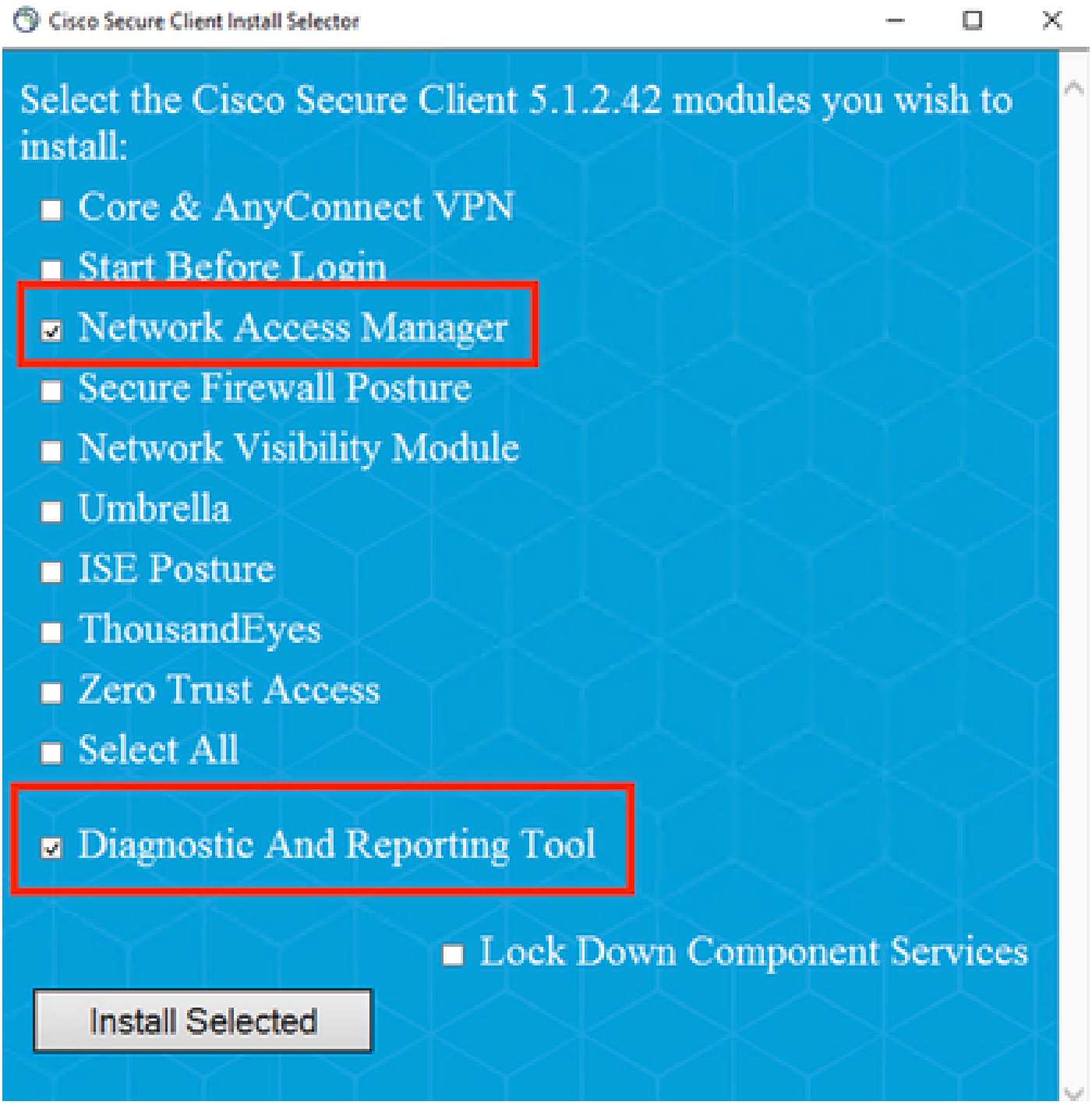


Sichere Client-Dateien

Installieren Sie die Module Network Access Manager und Diagnostics and Reporting Tool.



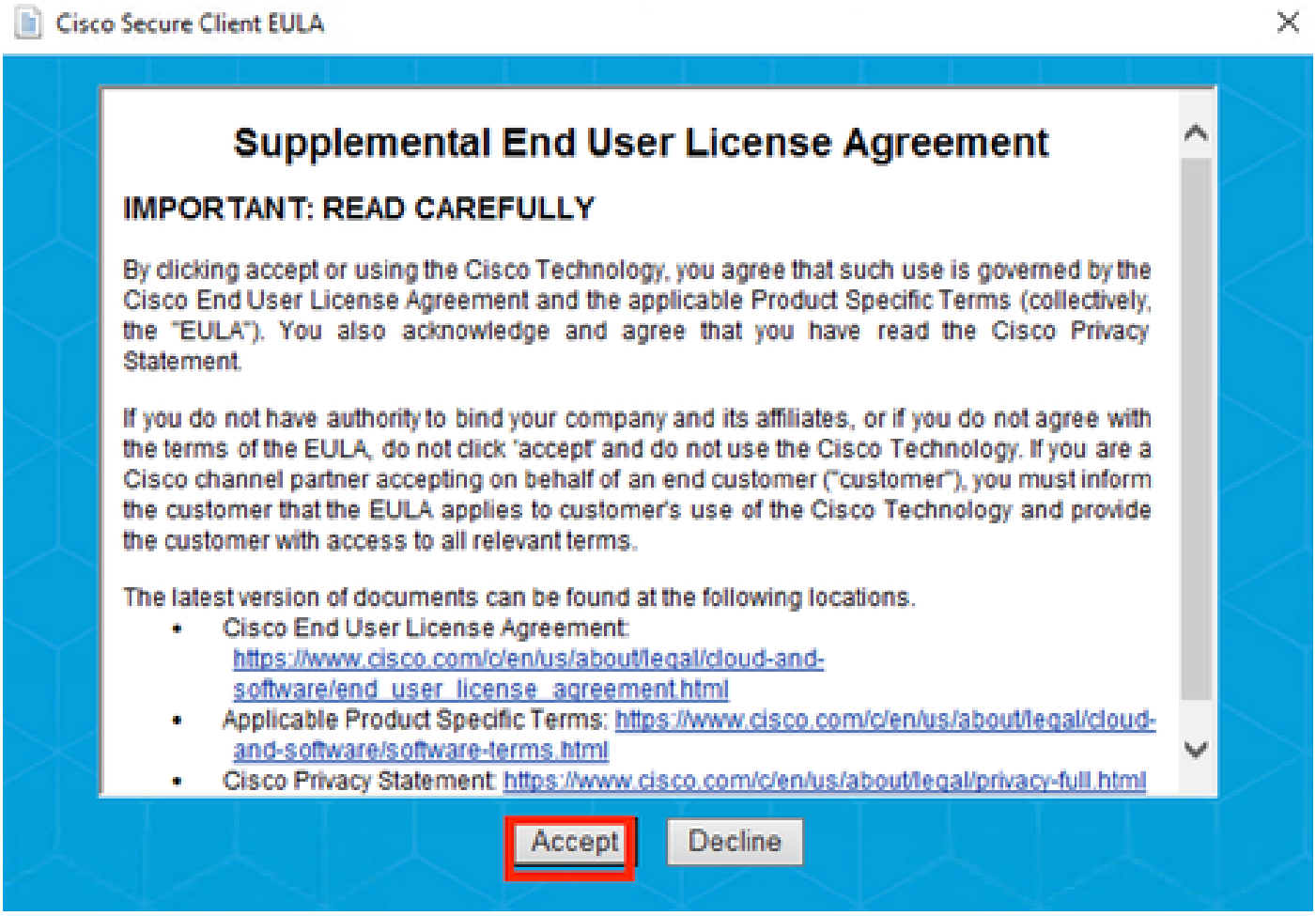
Warnung: Wenn Sie den Cisco Secure Client Wizard verwenden, wird das VPN-Modul automatisch installiert und in der GUI ausgeblendet. NAM funktioniert nicht, wenn das VPN-Modul nicht installiert ist. Wenn Sie einzelne MSI-Dateien oder eine andere Installationsmethode verwenden, stellen Sie sicher, dass Sie das VPN-Modul installieren.



Installationsauswahl

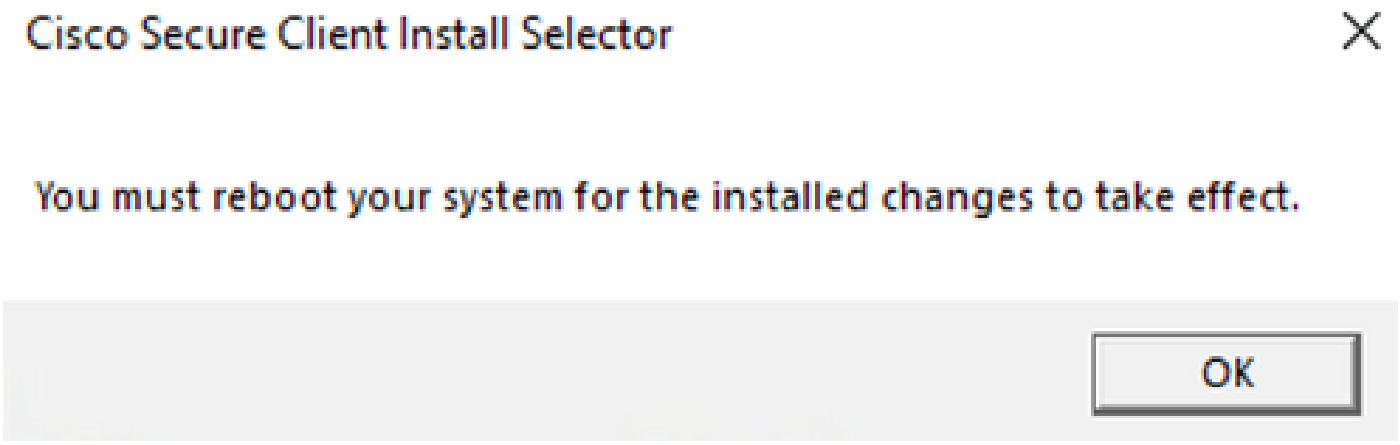
Klicken Sie auf Install Selected (Ausgewählte installieren).

Akzeptieren Sie die EULA.



EULA-Fenster

Nach der NAM-Installation ist ein Neustart erforderlich.



Fenster "Neustart erforderlich"

Nach der Installation kann es gefunden und von der Windows-Suchleiste geöffnet werden.

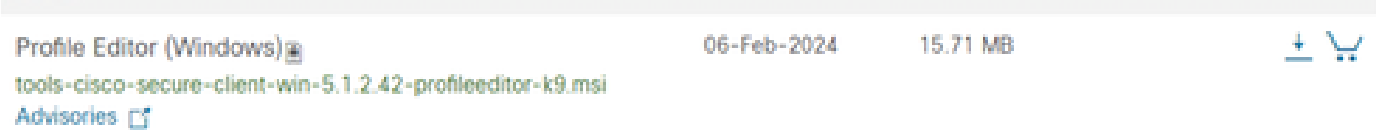
Secure Client-Programm

2. Laden Sie den Secure Client NAM Profile Editor herunter, und installieren Sie ihn.

Der Profil-Editor des Cisco Network Access Manager ist erforderlich, um die Dot1x-Voreinstellungen zu konfigurieren.

Die Option "Profil-Editor" befindet sich auf der Seite, auf der auch der sichere Client heruntergeladen wird.

In diesem Beispiel wird die Option mit Version 5.1.2.42 verwendet.



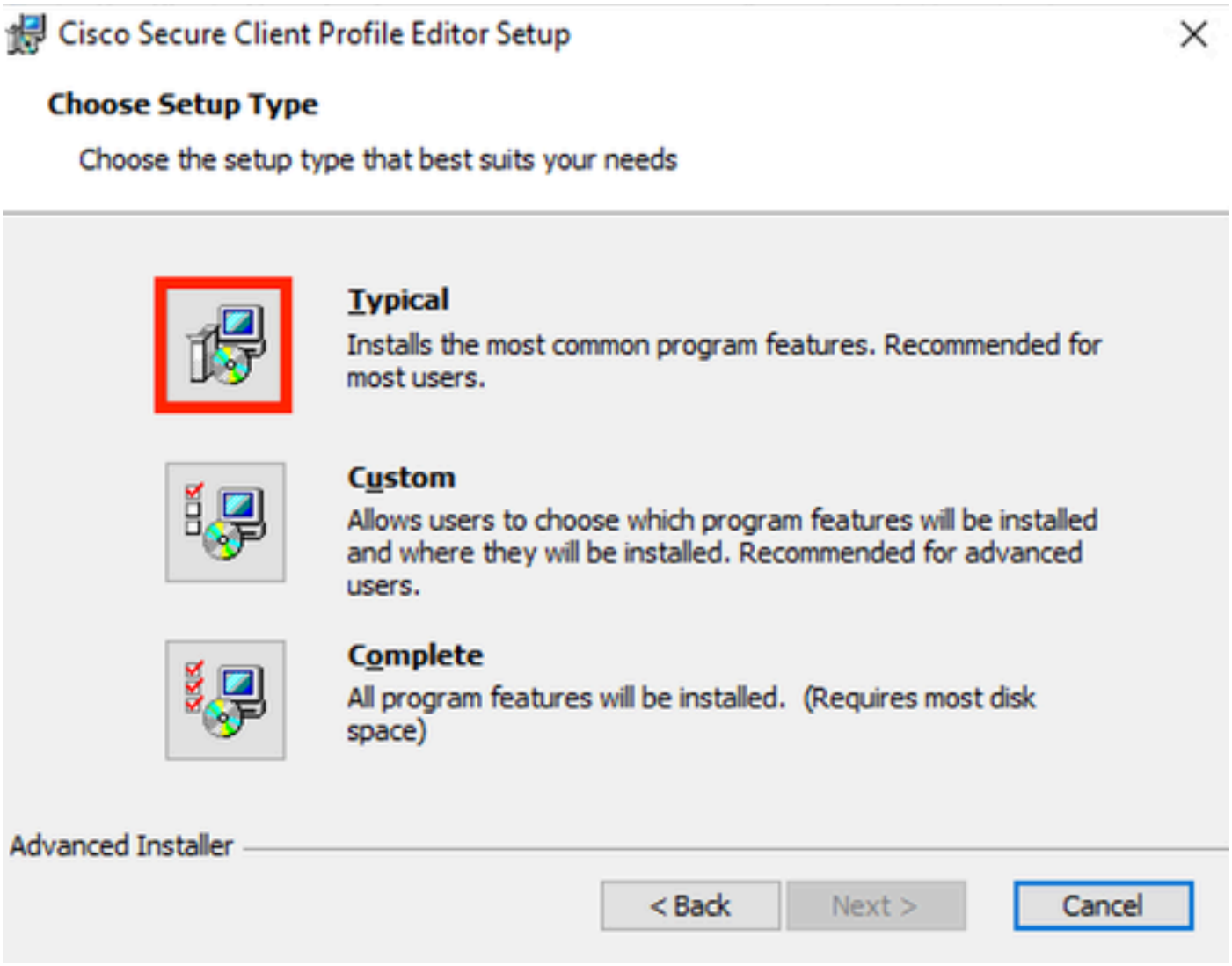
Profil-Editor

Fahren Sie nach dem Herunterladen mit der Installation fort.

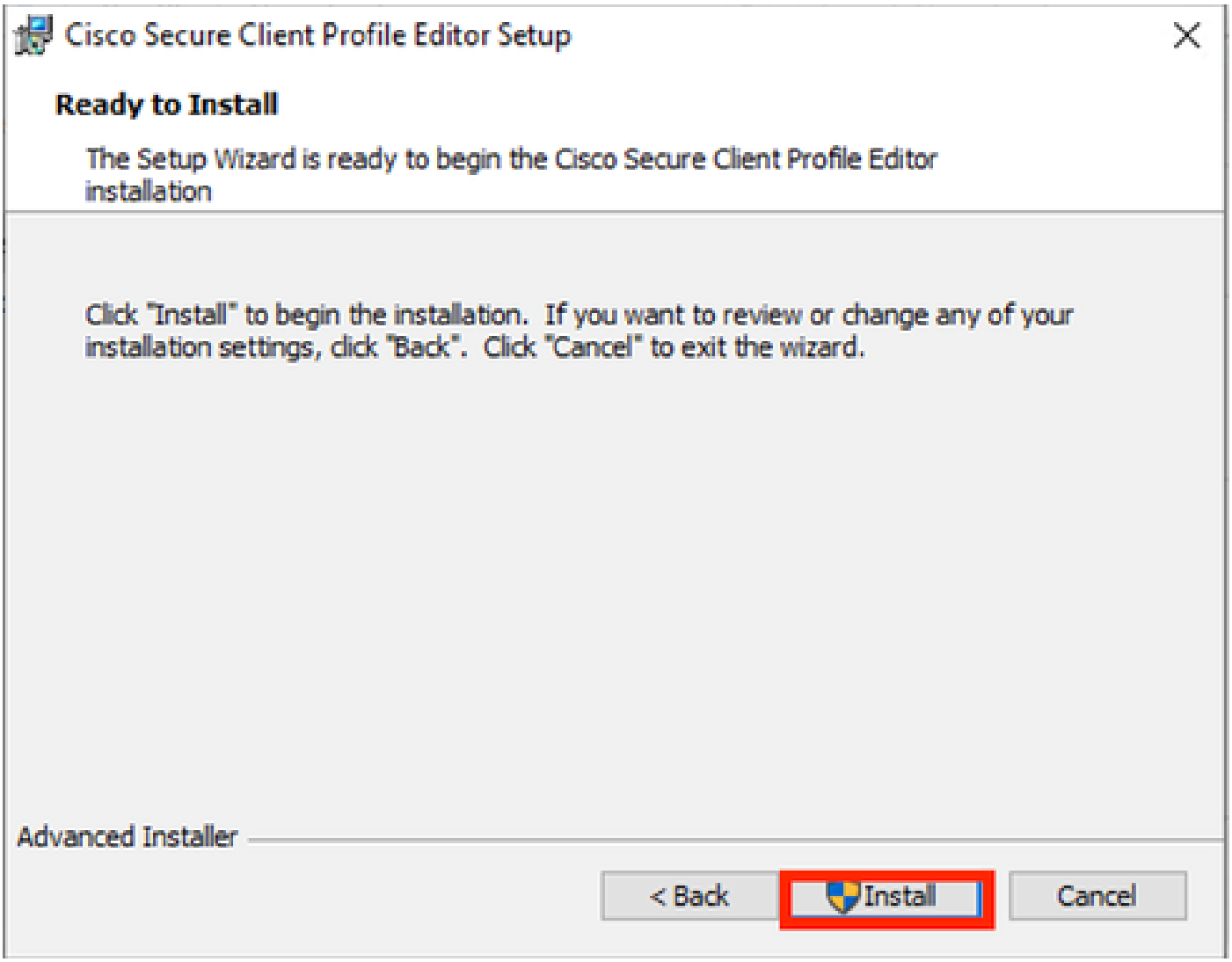
Führen Sie die msi-Datei aus.

Setup-Fenster des Profileditors

Verwenden Sie die Option Typisch.

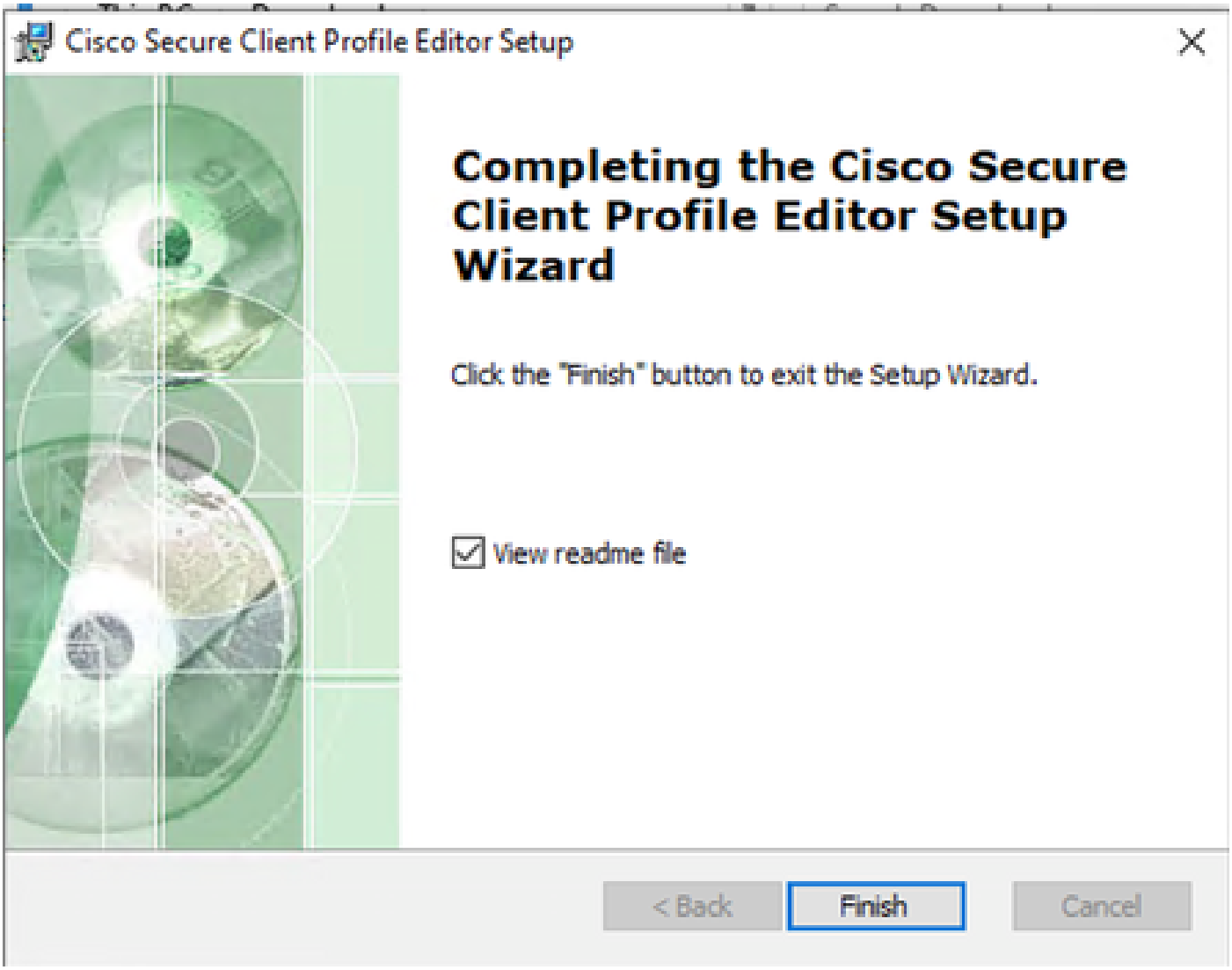


Profil-Editor einrichten



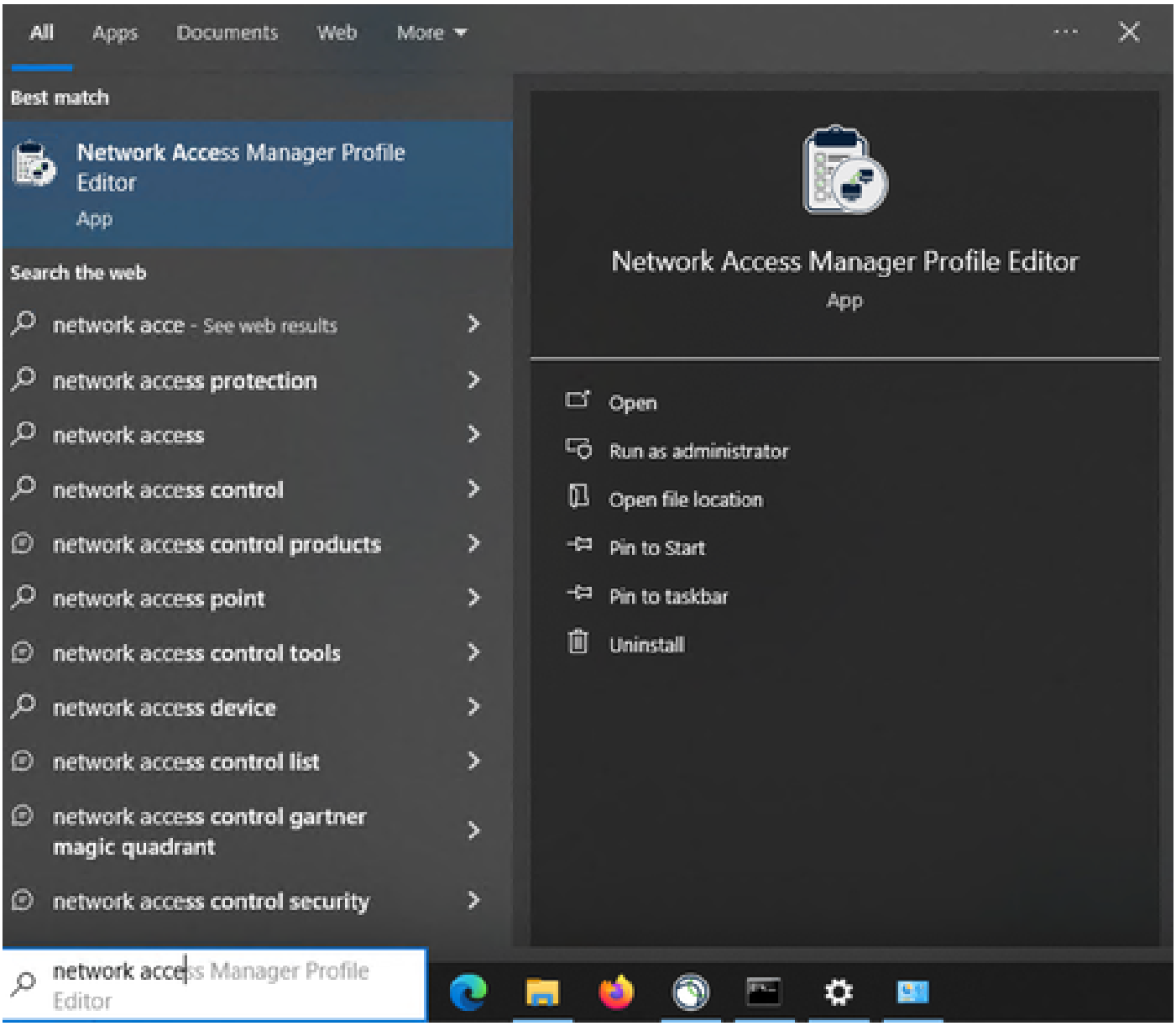
Installationsfenster

Klicken Sie auf Beenden.



Ende der Profil-Editor-Einrichtung

Öffnen Sie nach der Installation den Network Access Manager Profile Editor in der Suchleiste.



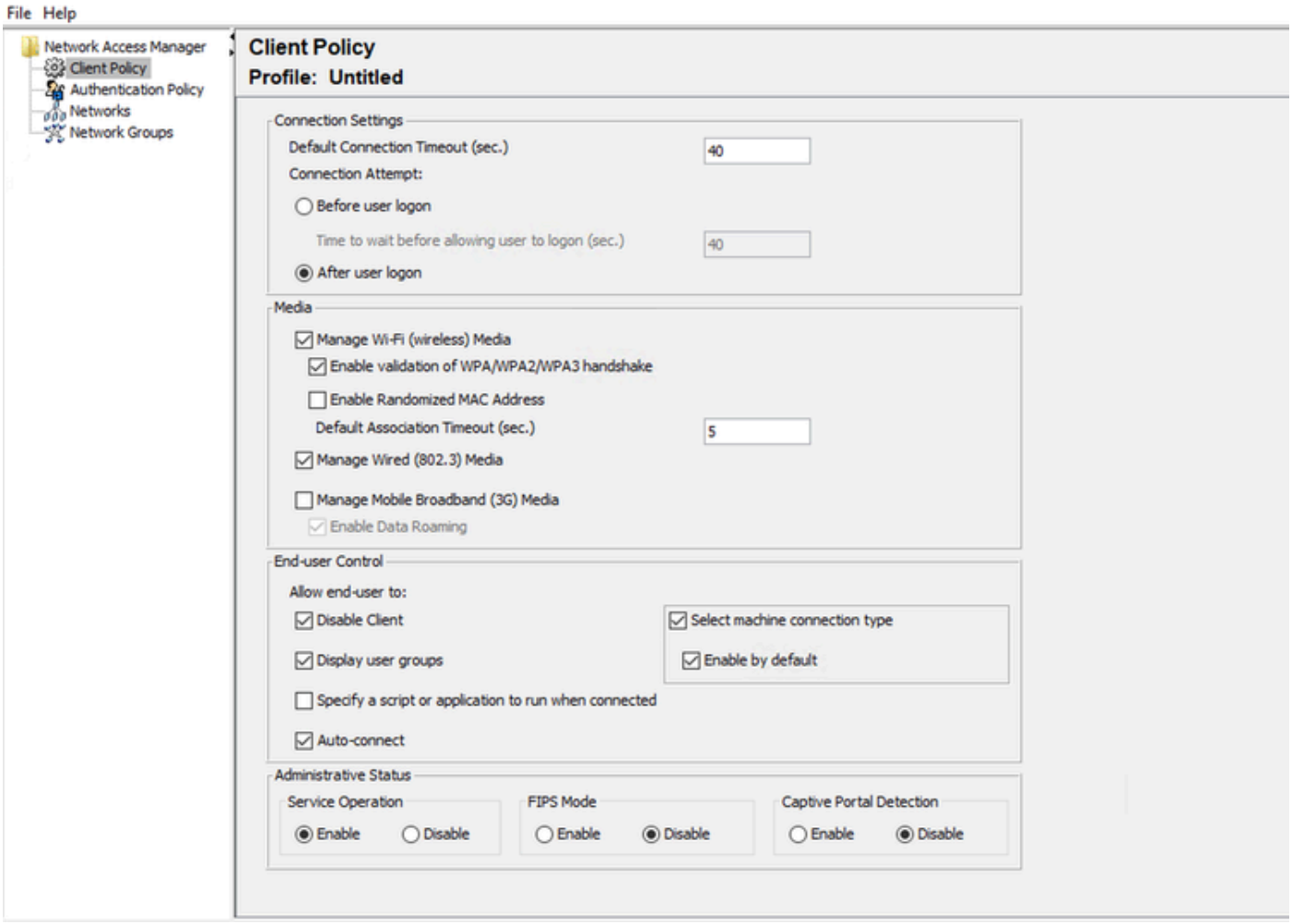
Profil-Editor für NAM in der Suchleiste

Die Installation von Network Access Manager und Profile Editor ist abgeschlossen.

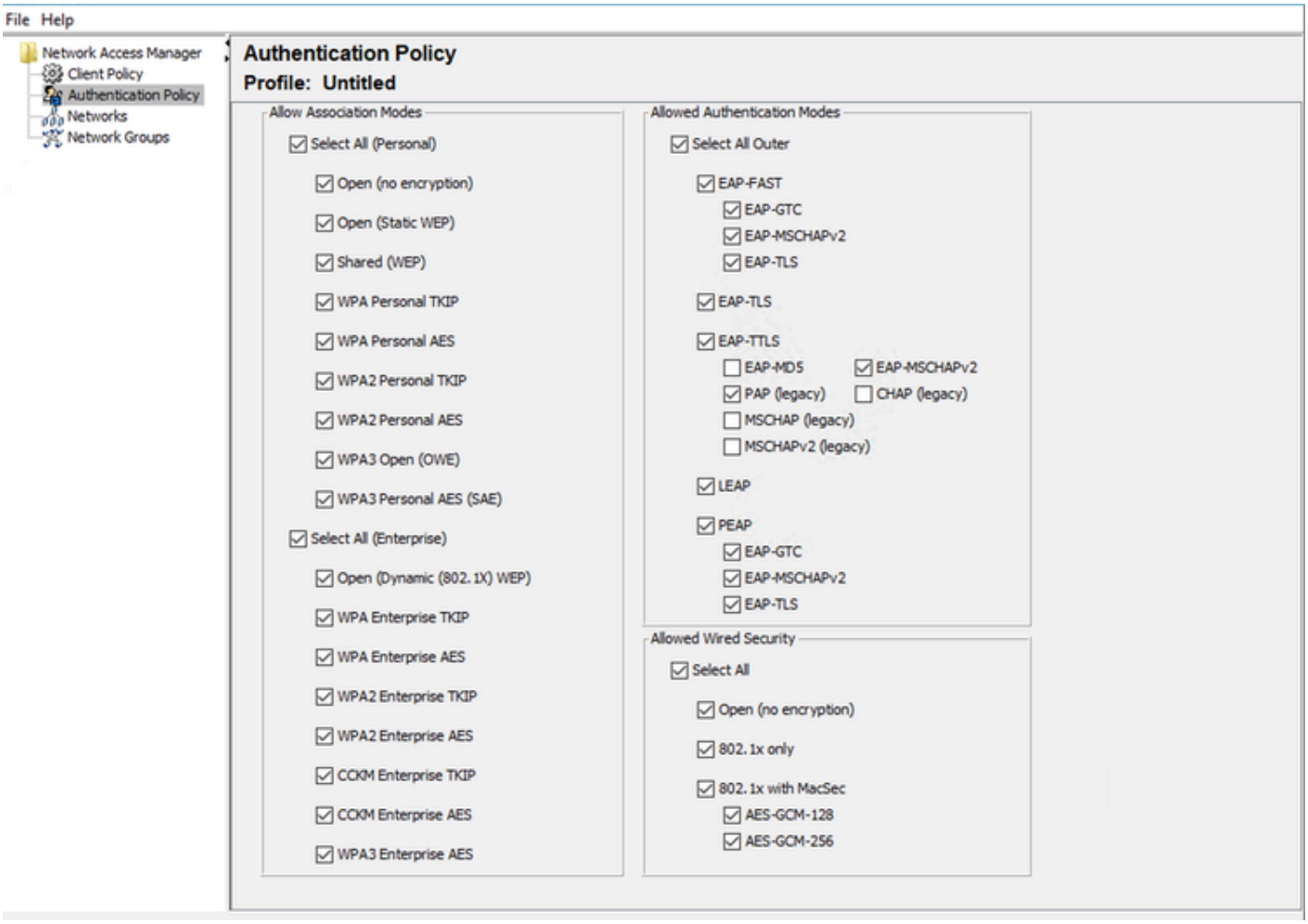
3. Allgemeine Standardkonfigurationen

Alle in diesem Artikel vorgestellten Szenarien enthalten Konfigurationen für:

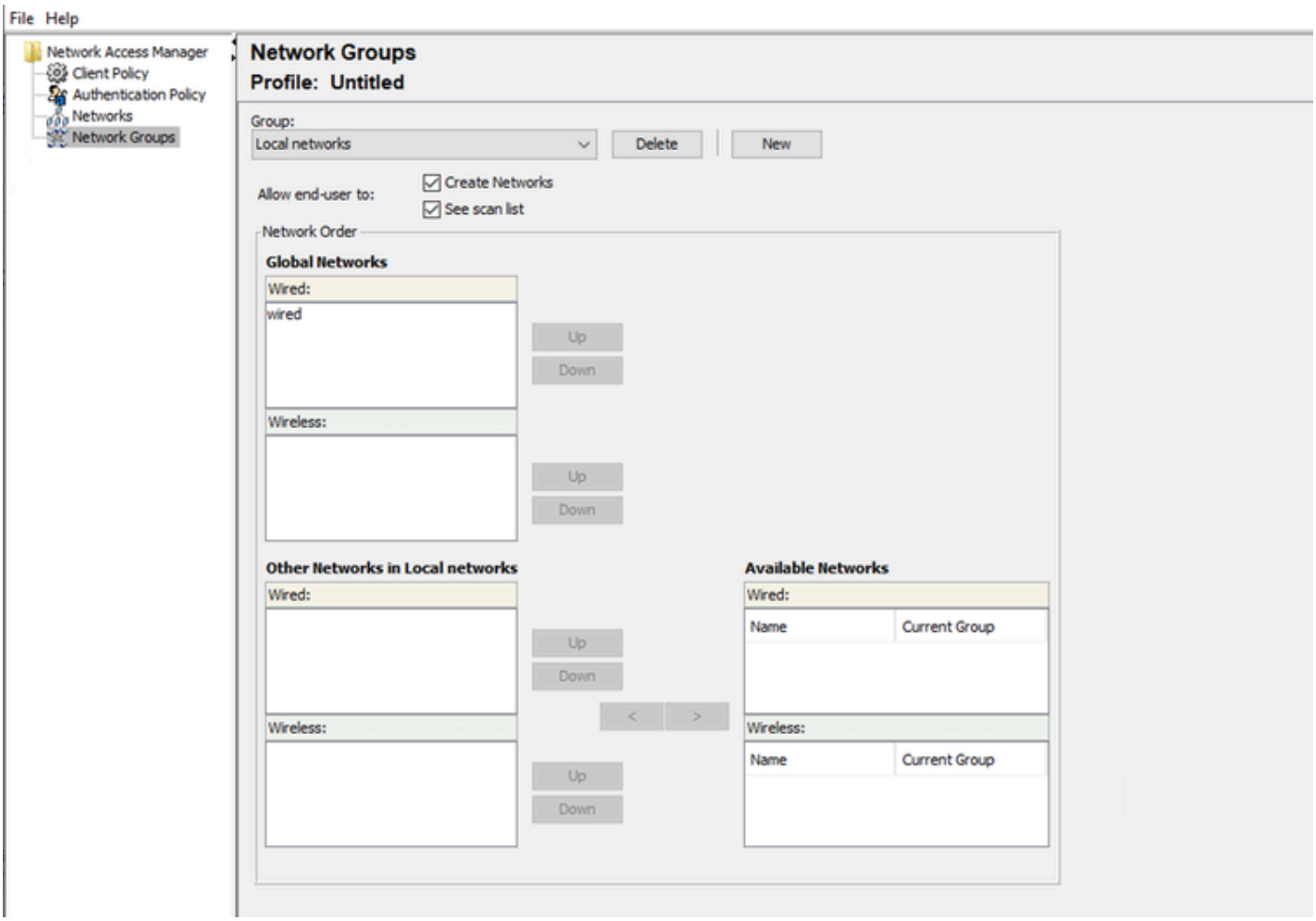
- Client-Richtlinie
- Authentifizierungsrichtlinie
- Netzwerkgruppen



NAM Profile Editor-Clientrichtlinie



Authentifizierungsrichtlinie des NAM-Profil-Editors



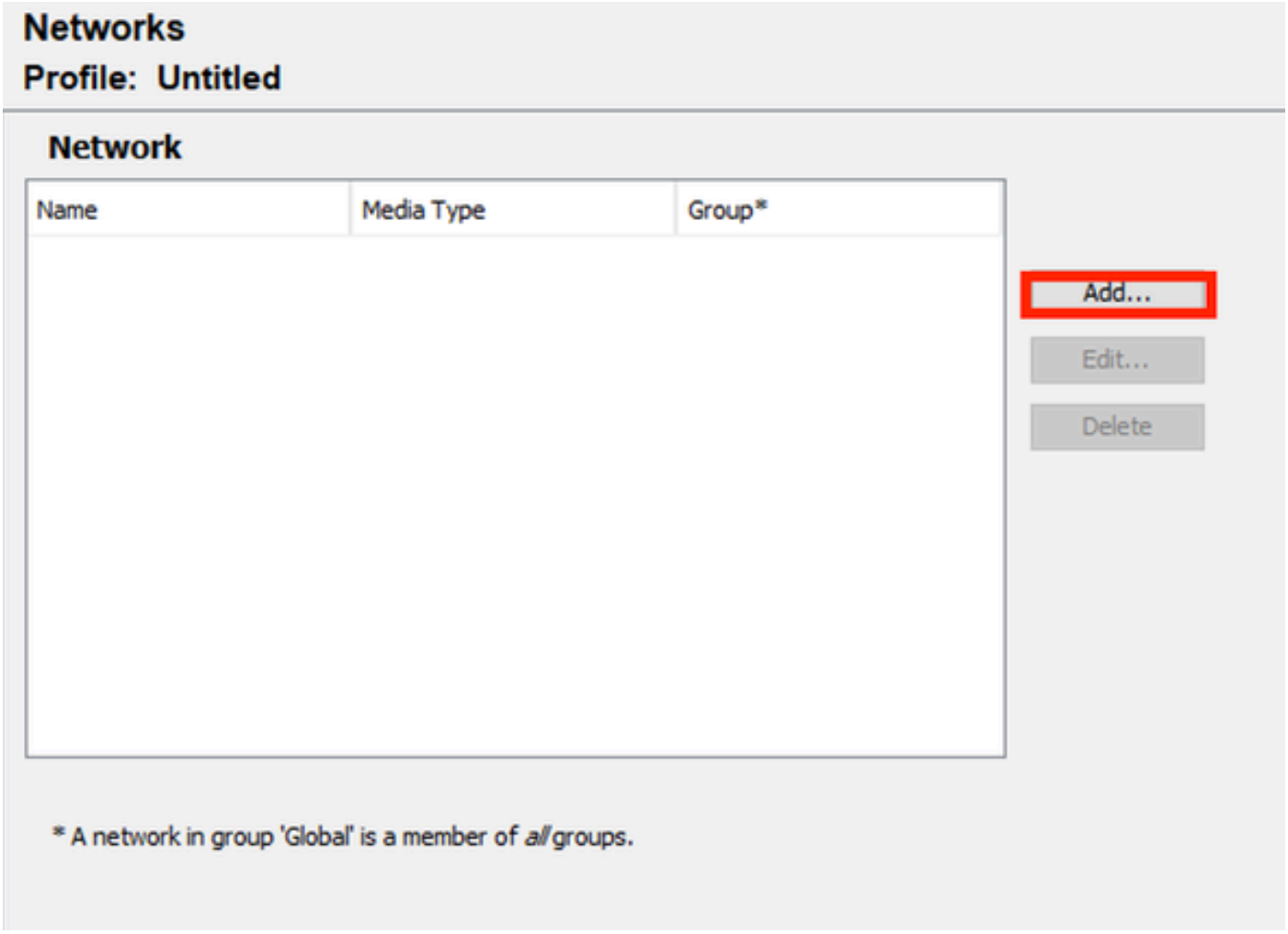
Registerkarte "Netzwerkgruppen"

4. Szenario 1: Konfigurieren der Secure Client NAM-Komponente für die PEAP-Benutzerauthentifizierung (MS-CHAPv2)

Navigieren Sie zum Abschnitt Netzwerke.

Das standardmäßige Netzwerkprofil kann gelöscht werden.

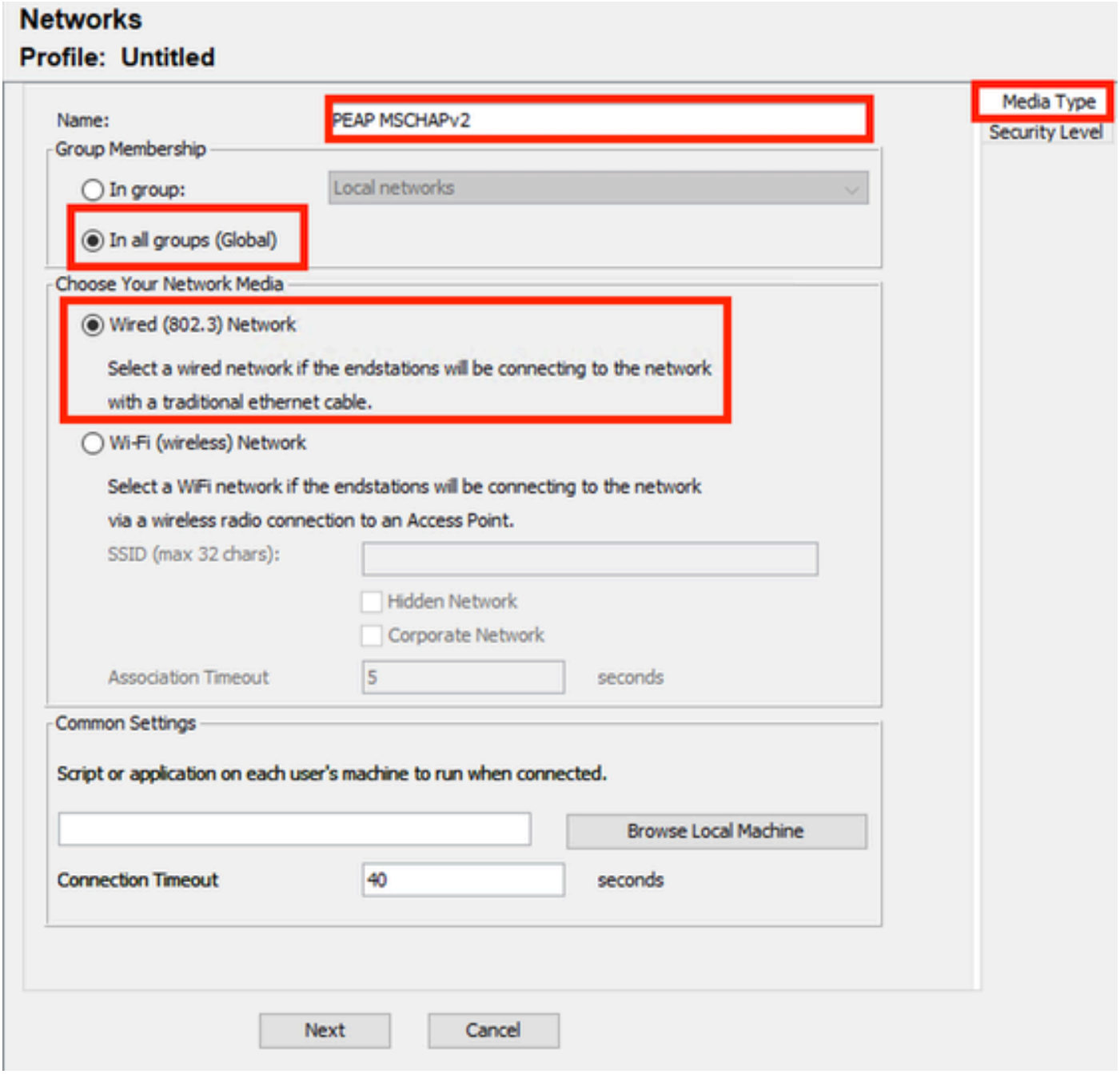
Klicken Sie auf Hinzufügen.



Erstellung von Netzwerkprofilen

Nennen Sie das Netzwerkprofil.

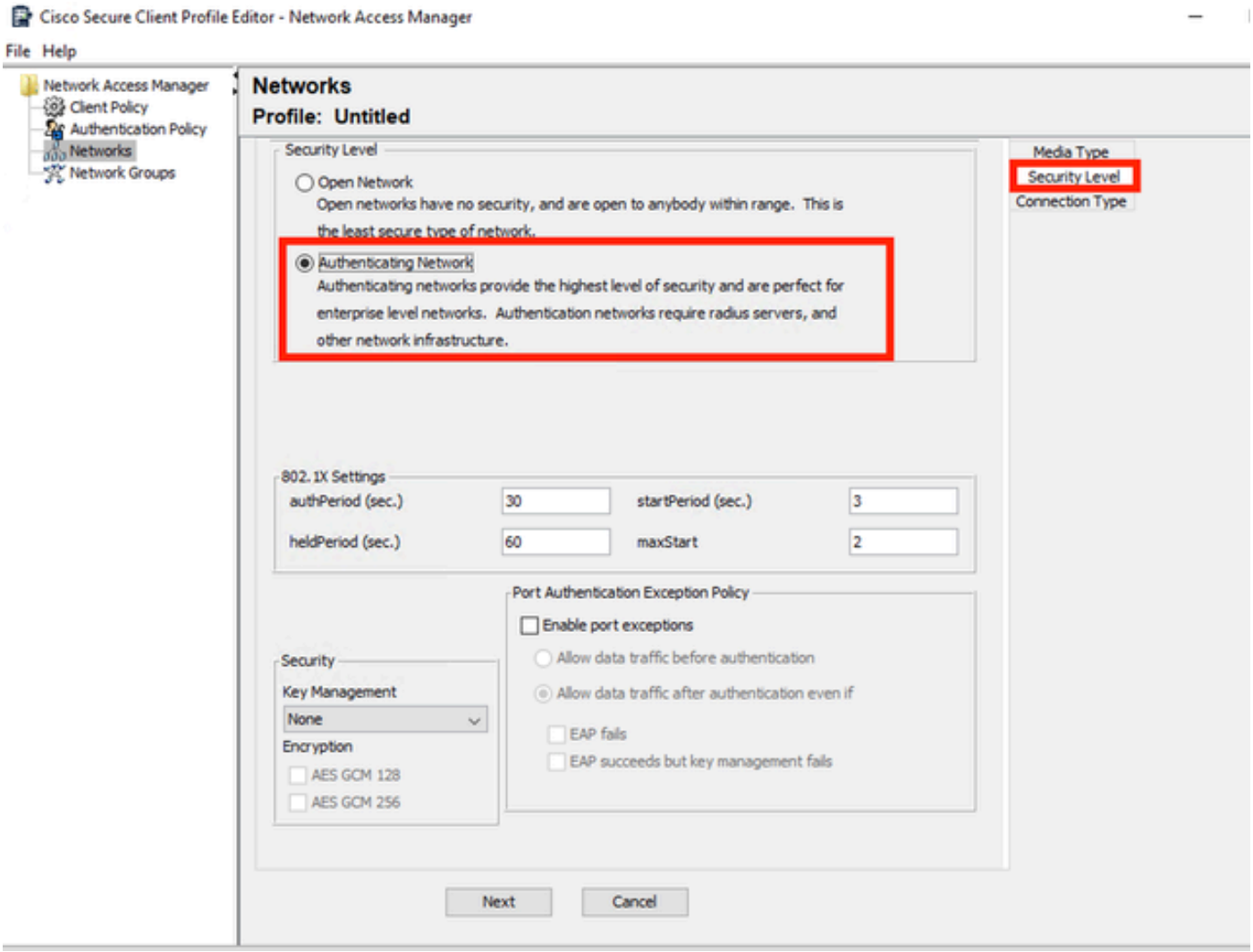
Wählen Sie Global als Gruppenmitgliedschaft aus. Wählen Sie Kabelgebundene Netzwerkmedien aus.



Abschnitt "Netzwerkprofil Medientyp"

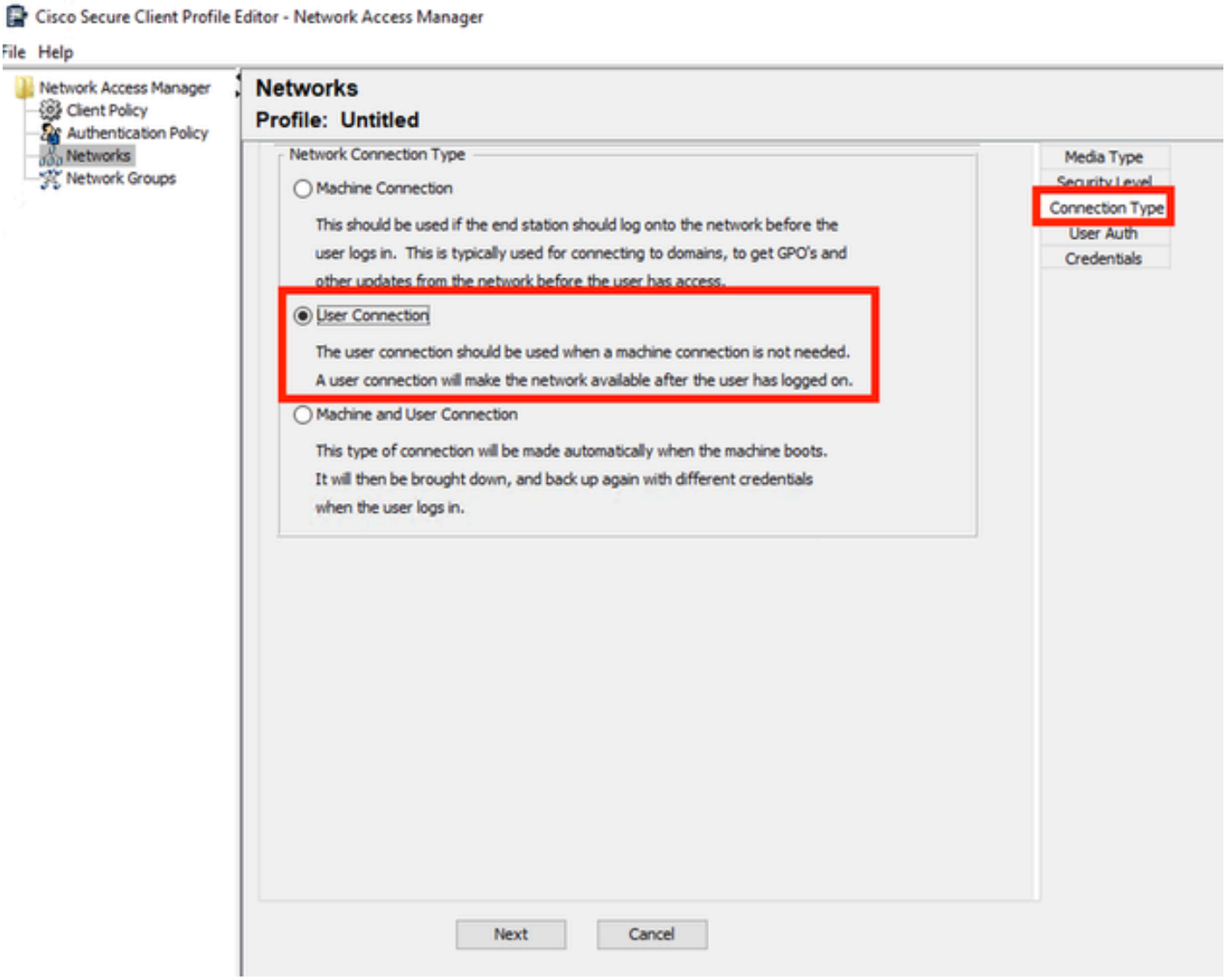
Klicken Sie auf Next (Weiter).

Wählen Sie Authenticating Network aus, und verwenden Sie die Standardeinstellung für die restlichen Optionen im Abschnitt Security Level (Sicherheitsstufe).



Netzwerkprofil - Sicherheitsstufe

Klicken Sie auf Weiter, um mit dem Abschnitt Verbindungstyp fortzufahren.

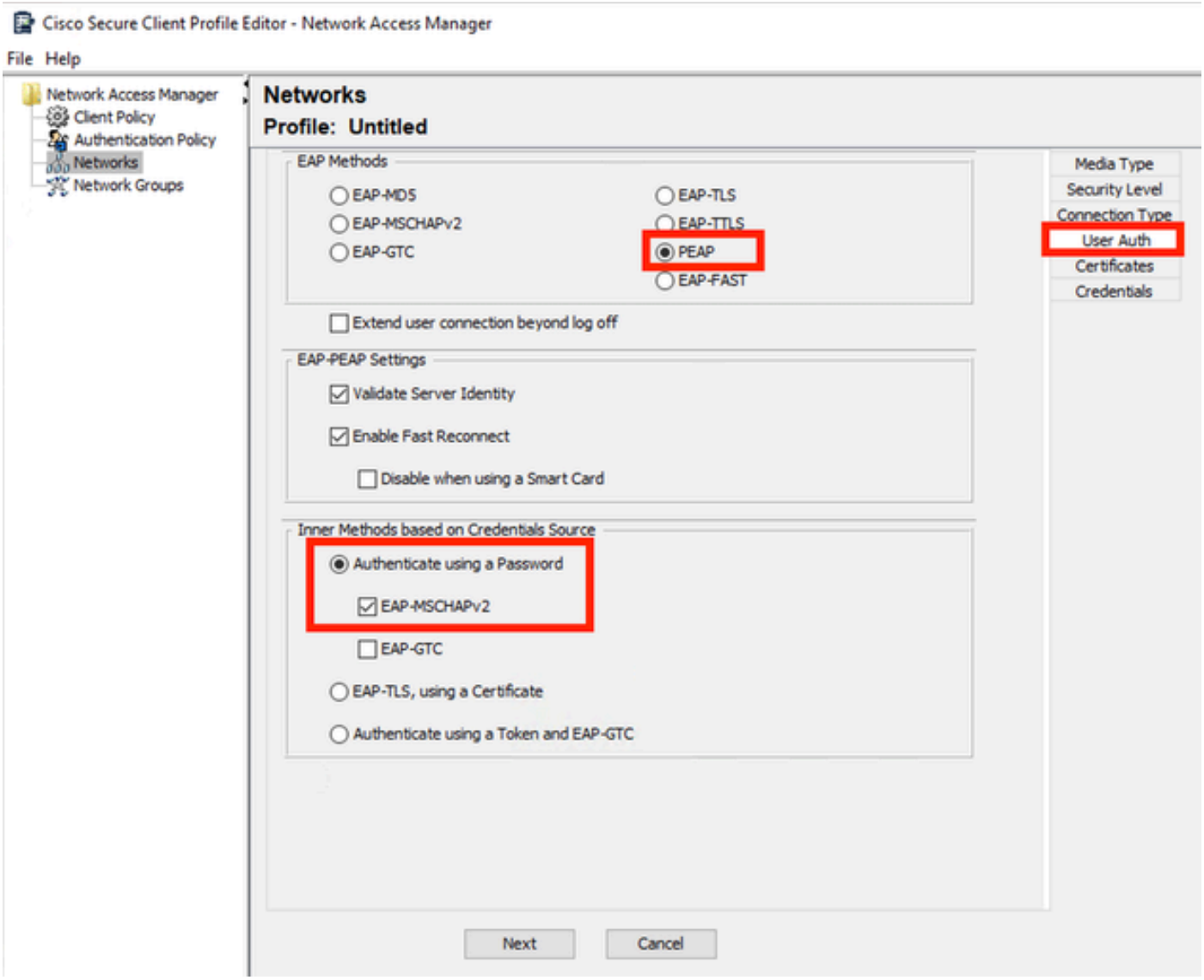


Verbindungstyp des Netzwerkprofils

Wählen Sie den Verbindungstyp Benutzerverbindung aus.

Klicken Sie auf Weiter, um mit dem jetzt verfügbaren Abschnitt Benutzerauthentifizierung fortzufahren.

Wählen Sie PEAP als allgemeine EAP-Methode aus.



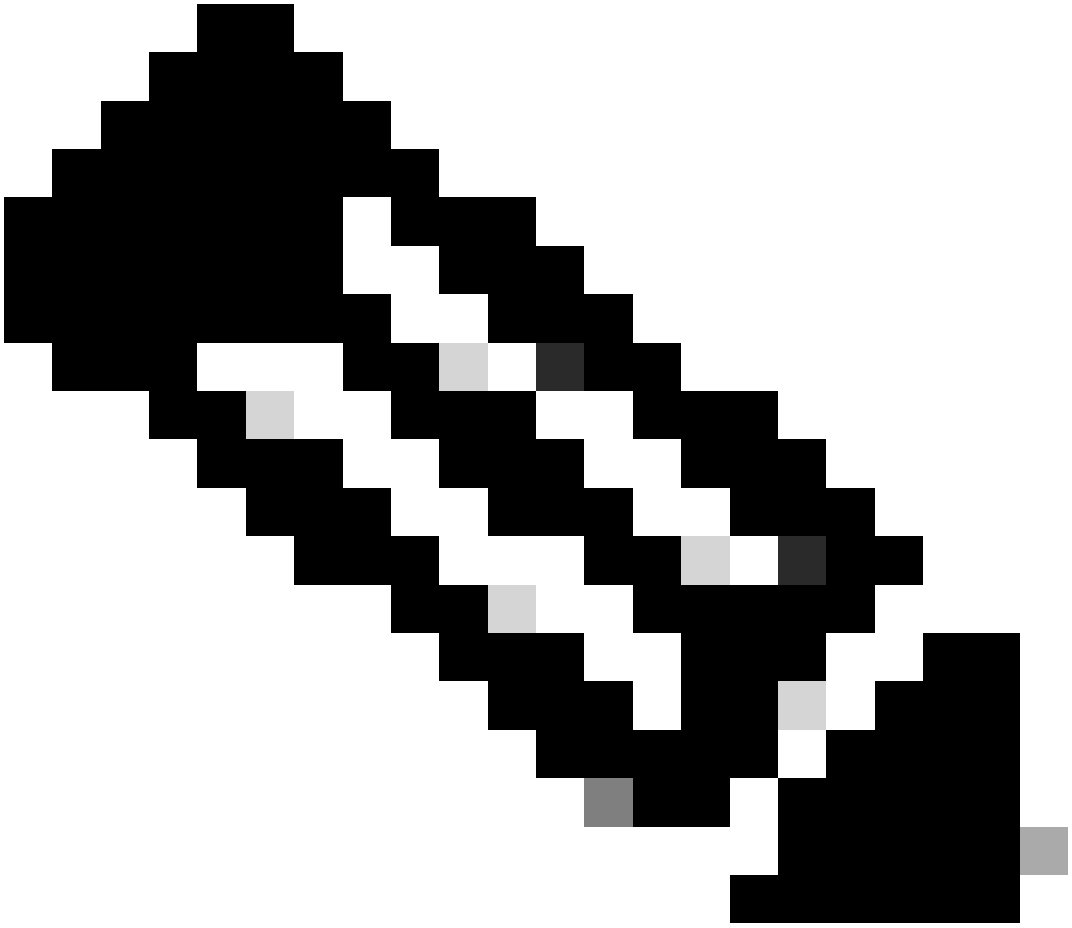
Netzwerkprofil-Benutzerauthentifizierung

Ändern Sie nicht die Standardwerte in den EAP-PEAP-Einstellungen.

Fahren Sie mit dem Abschnitt Interne Methoden auf Basis der Anmeldeinformationsquelle fort.

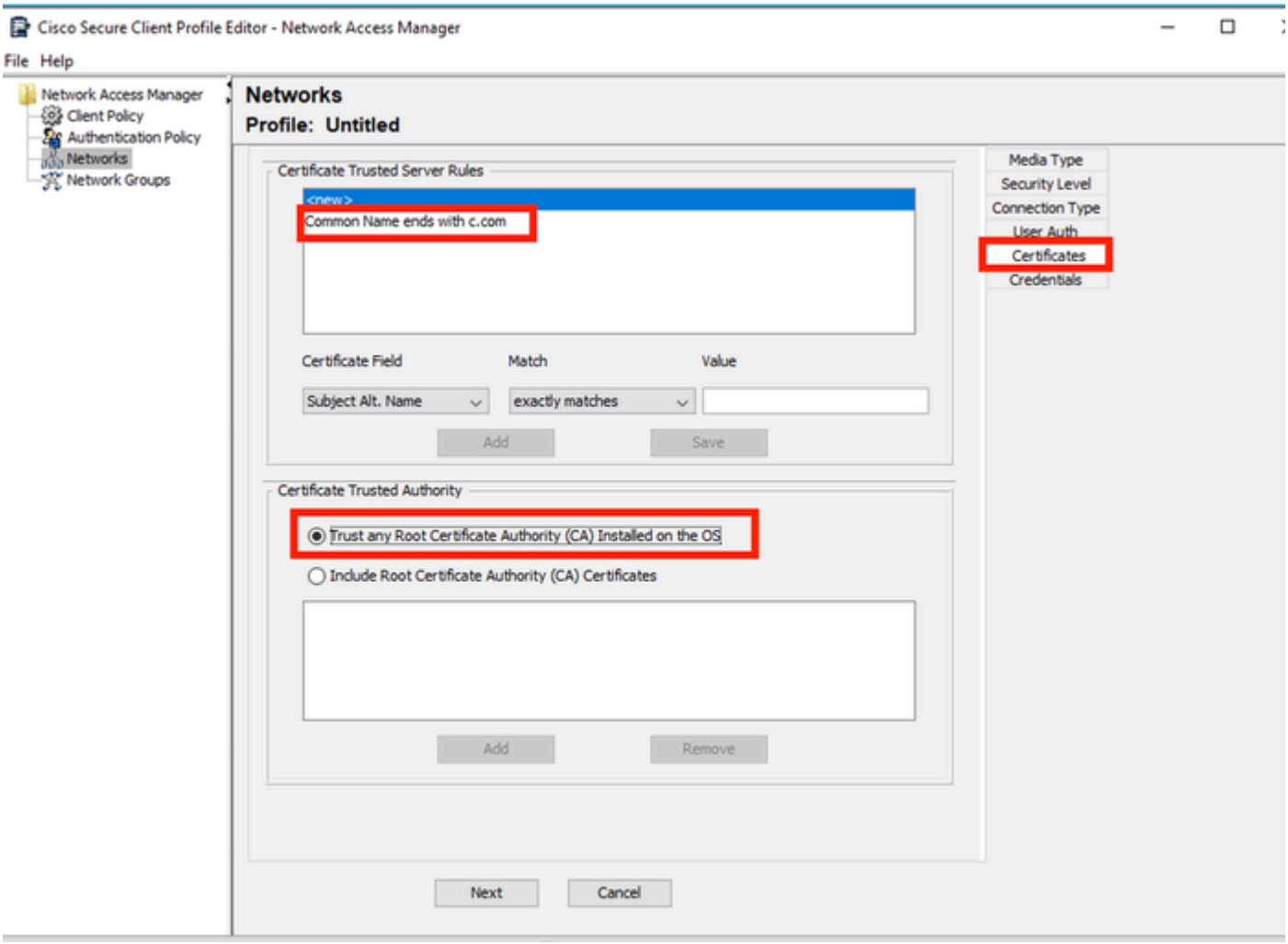
Wählen Sie unter den verschiedenen internen Methoden für EAP-PEAP die Option Authenticate using a Password (Mit Kennwort authentifizieren) und dann EAP-MSCHAPv2 aus.

Klicken Sie auf Weiter, um mit dem Abschnitt Zertifikat fortzufahren.



Hinweis: Der Zertifikatabschnitt wird angezeigt, da die Option Serveridentität in den EAP-PEAP-Einstellungen validieren ausgewählt ist. Bei EAP PEAP erfolgt die Kapselung mithilfe des Serverzertifikats.

Im Abschnitt Zertifikate wird in Regeln für vertrauenswürdige Server für Zertifikate die Regel Common Name end mit c.com verwendet. Dieser Konfigurationsabschnitt bezieht sich auf das Zertifikat, das der Server während des EAP-PEAP-Datenflusses verwendet. Wenn Identity Service Engine (ISE) in Ihrer Umgebung verwendet wird, können Sie den allgemeinen Namen des Policy Server Node EAP-Zertifikats verwenden.

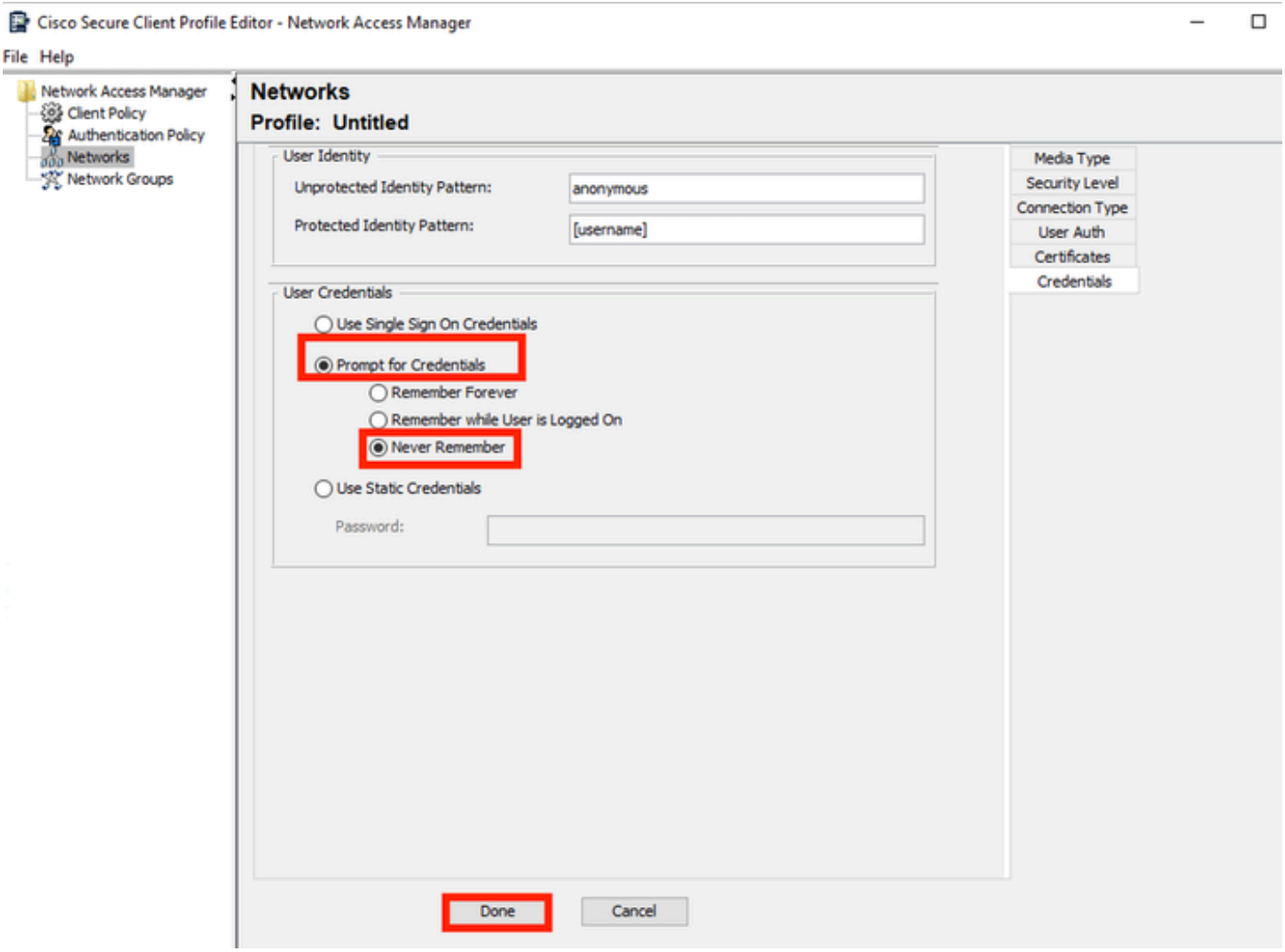


Abschnitt "Netzwerkprofil-Zertifikat"

In der vertrauenswürdigen Zertifizierungsstelle für Zertifikate können zwei Optionen ausgewählt werden. In diesem Szenario wird anstelle des Hinzufügens eines spezifischen Zertifizierungsstellenzertifikats, das das RADIUS-EAP-Zertifikat signiert hat, die Option Auf dem Betriebssystem installierte Stammzertifizierungsstelle vertrauen verwendet.

Mit dieser Option vertraut das Windows-Gerät allen EAP-Zertifikaten, die von einem Zertifikat signiert wurden, das unter Benutzerzertifikate verwalten - Aktueller Benutzer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate enthalten ist.

Klicken Sie auf Next (Weiter).



Abschnitt "Netzwerkprofil-Anmeldedaten"

Im Abschnitt Anmeldedaten wird nur der Abschnitt Benutzeranmeldedaten geändert.

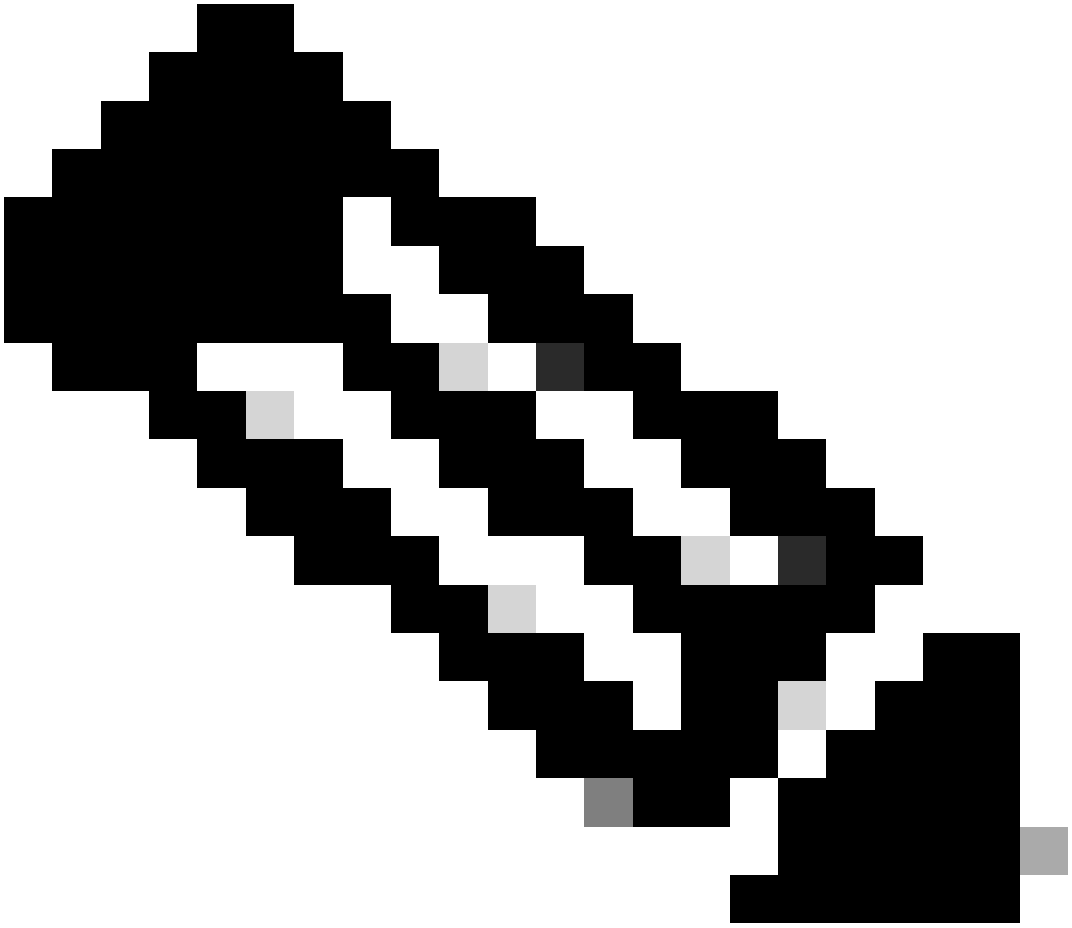
Die Option Prompt for Credentials > Never Remember ist aktiviert. Bei jeder Authentifizierung muss der Benutzer, der die Authentifizierung vornimmt, seine Anmeldeinformationen eingeben.

Klicken Sie auf Done (Fertig).

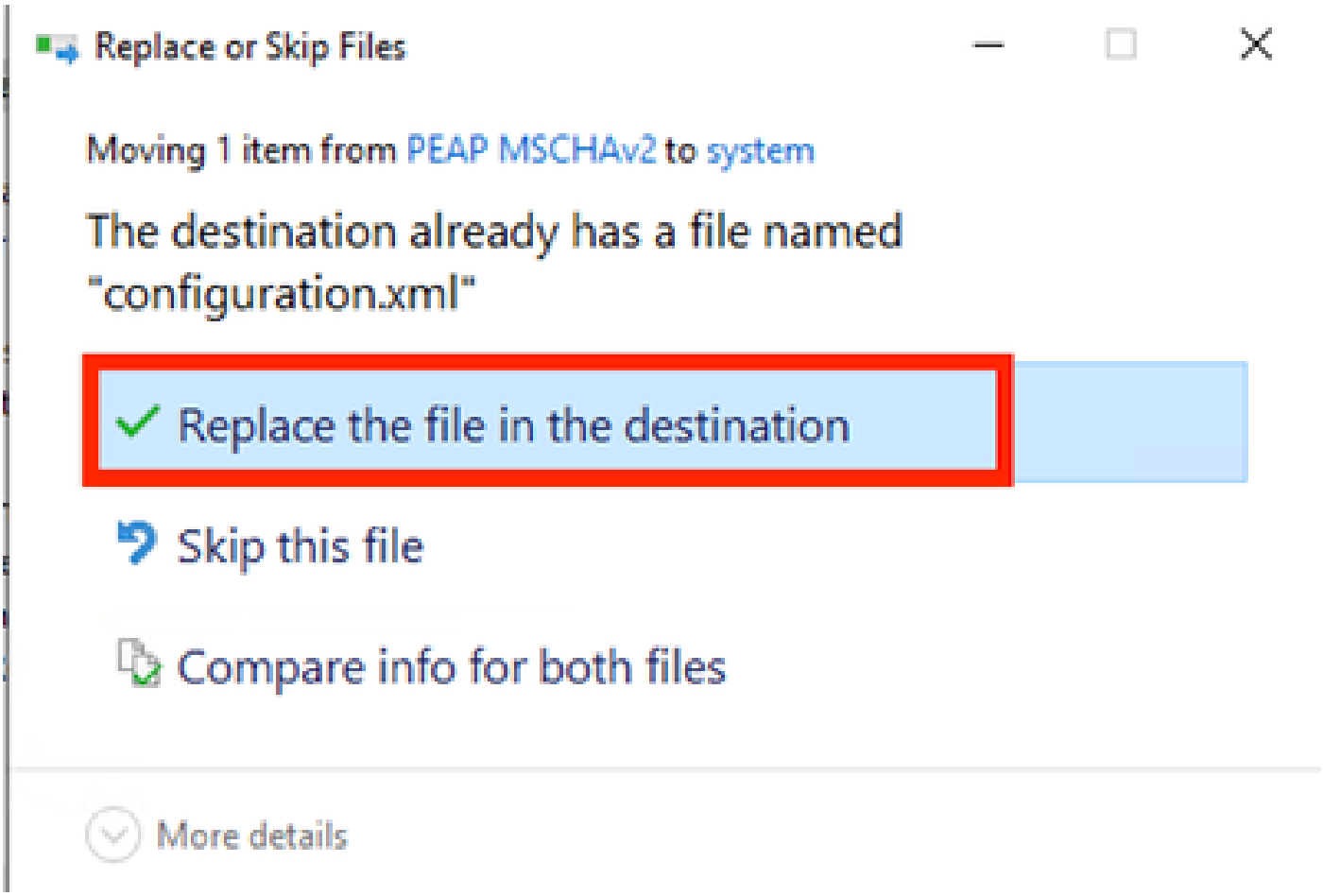
Speichern Sie das Profil des Secure Client Network Access Manager als configuration.xml mit der Option Datei > Speichern unter.

Um Secure Client Network Access Manager zur Verwendung des gerade erstellten Profils zu veranlassen, ersetzen Sie die Datei configuration.xml im nächsten Verzeichnis durch das neue:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



Hinweis: Die Datei muss den Namen configuration.xml haben, sonst funktioniert sie nicht.

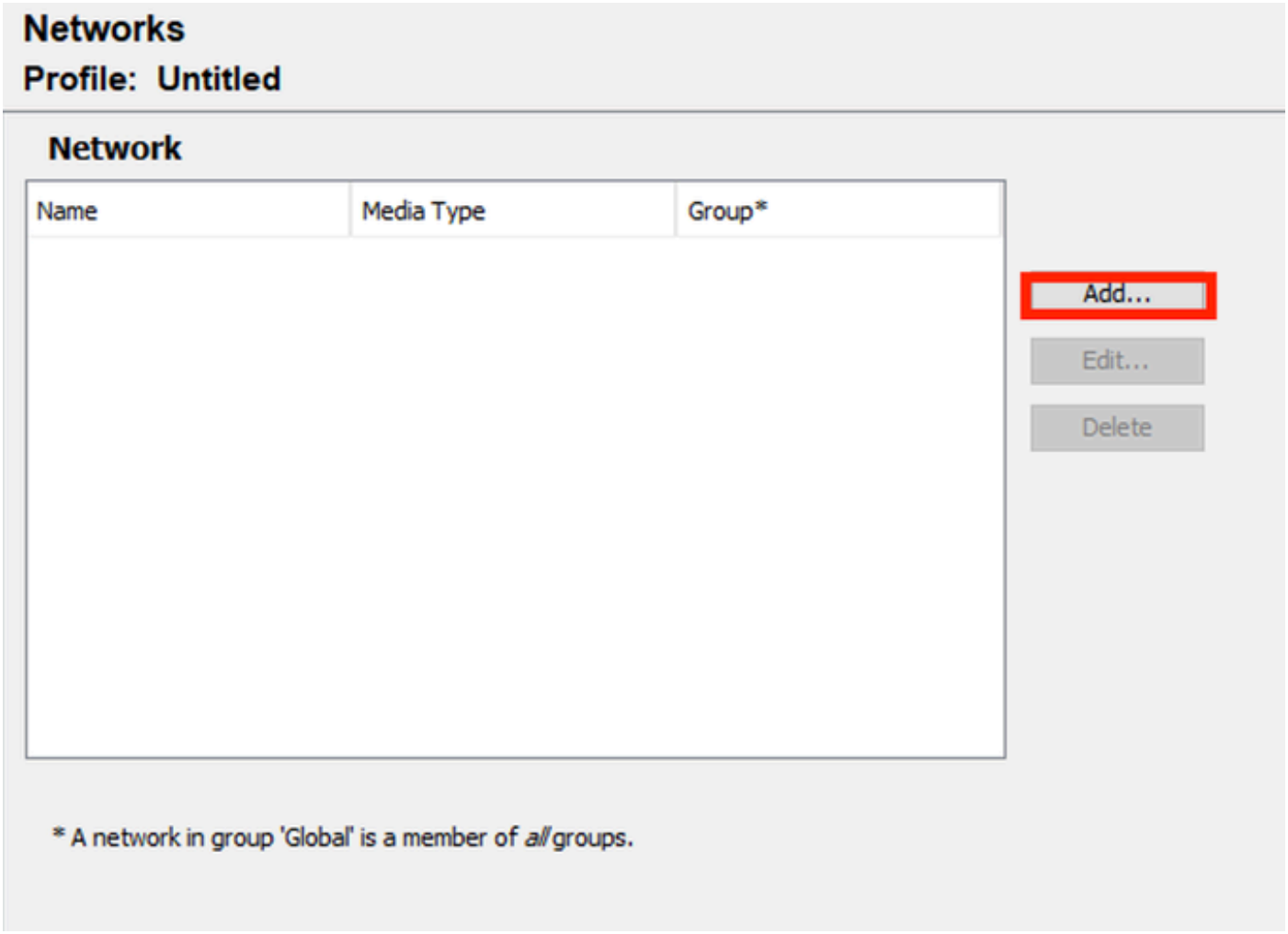


Dateiabschnitt ersetzen

5. Szenario 2: Konfigurieren der Secure Client NAM-Komponente für die gleichzeitige EAP-FAST-Benutzer- und Geräteauthentifizierung

Öffnen Sie den NAM Profile Editor, und navigieren Sie zum Abschnitt Netzwerke.

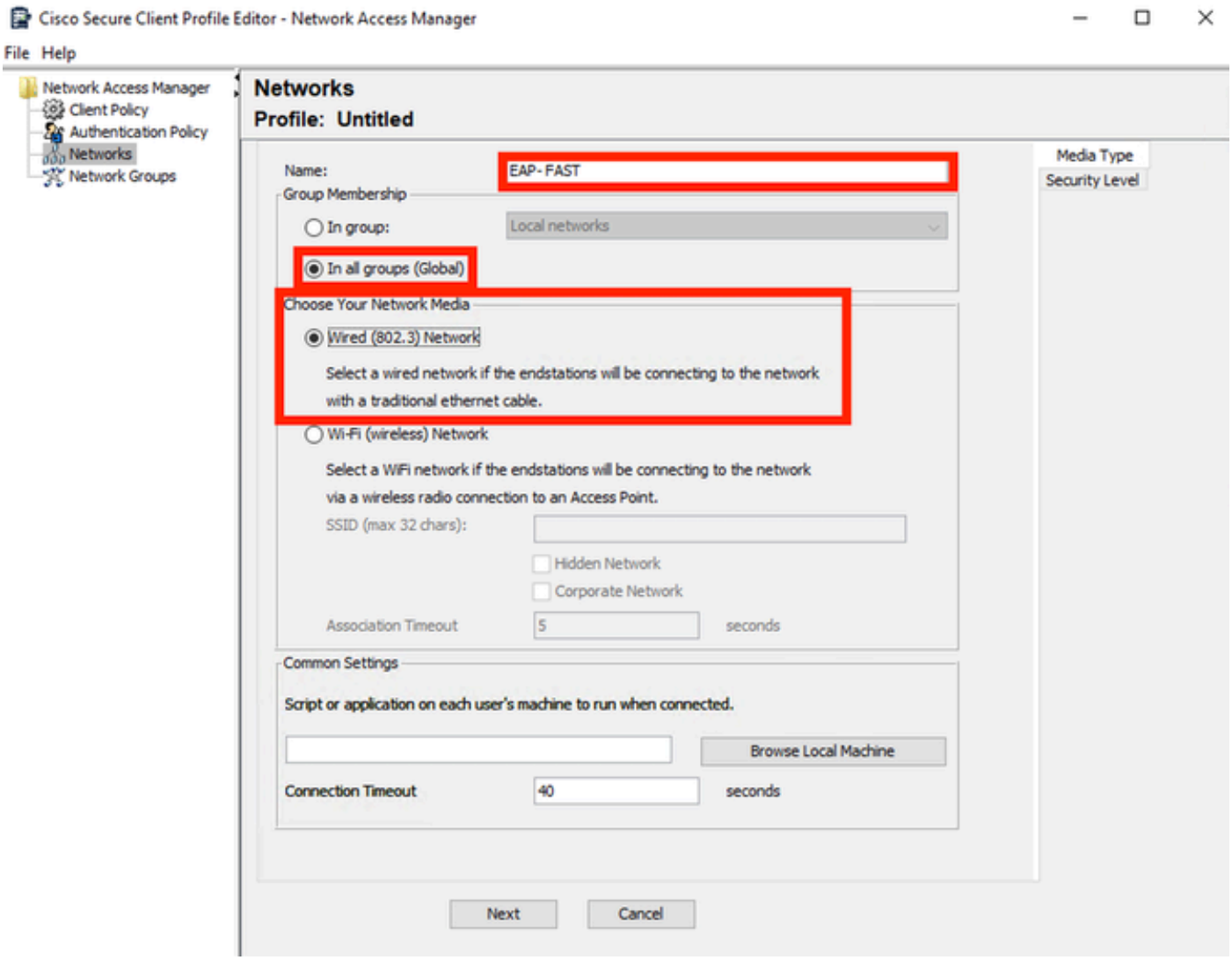
Klicken Sie auf Hinzufügen.



NAM Profile Editor - Registerkarte "Netzwerk"

Geben Sie einen Namen in das Netzwerkprofil ein.

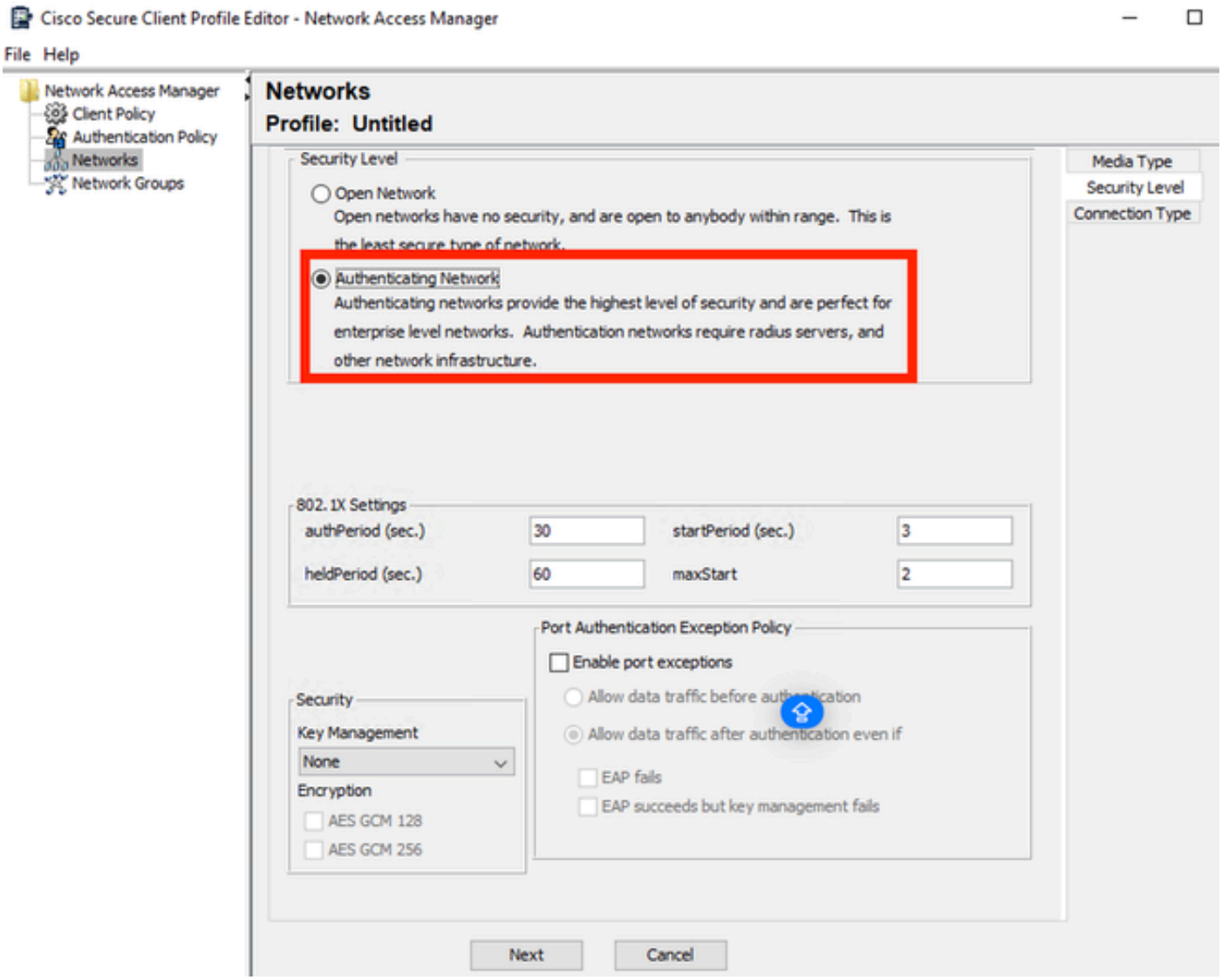
Wählen Sie Global als Gruppenmitgliedschaft aus. Wählen Sie WiredNetwork Media.



Bereich Medientyp

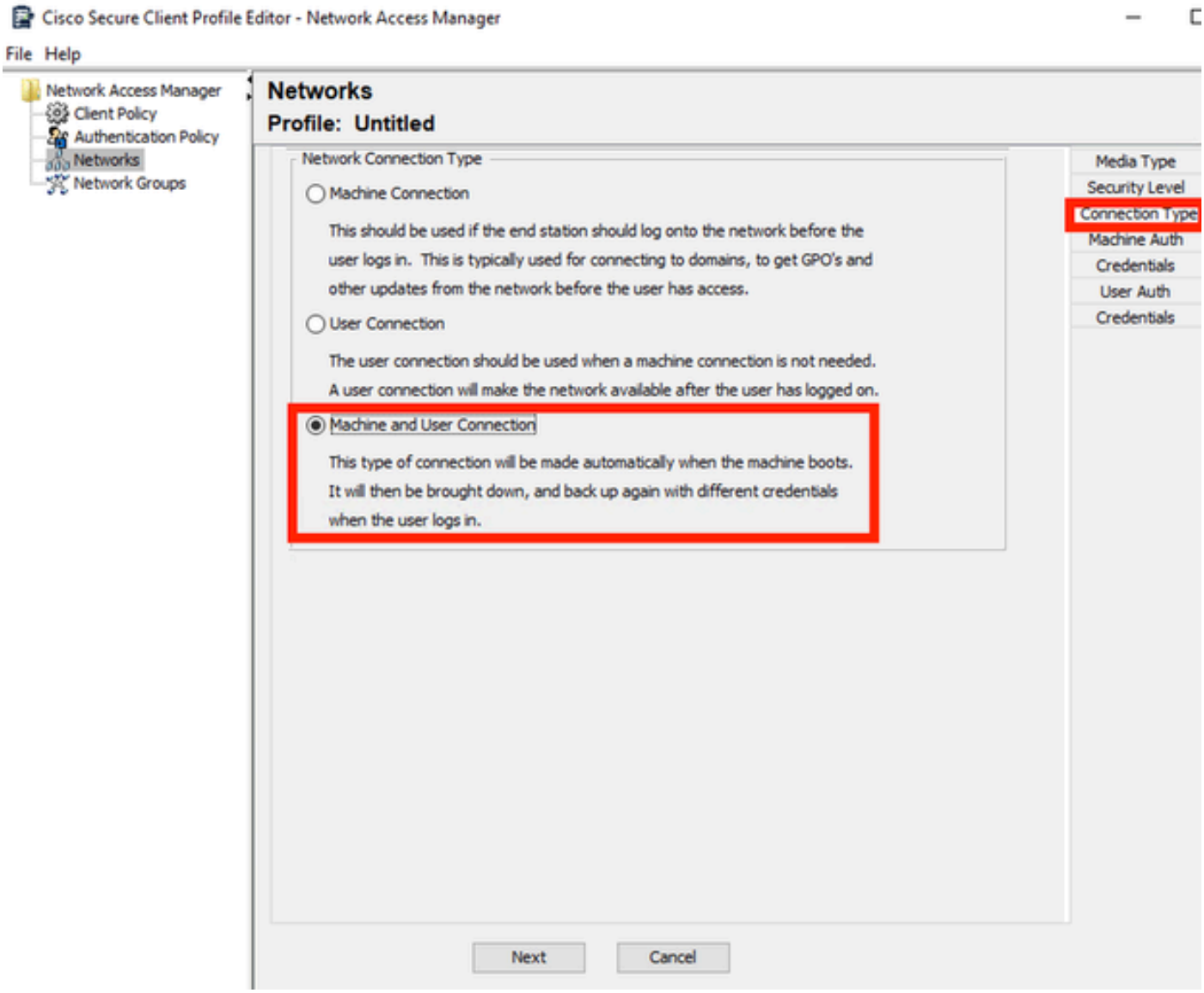
Klicken Sie auf Next (Weiter).

Wählen Sie Authenticating Network aus, und ändern Sie die Standardwerte für die restlichen Optionen in diesem Abschnitt nicht.



Abschnitt "Sicherheitsebenenprofil-Editor"

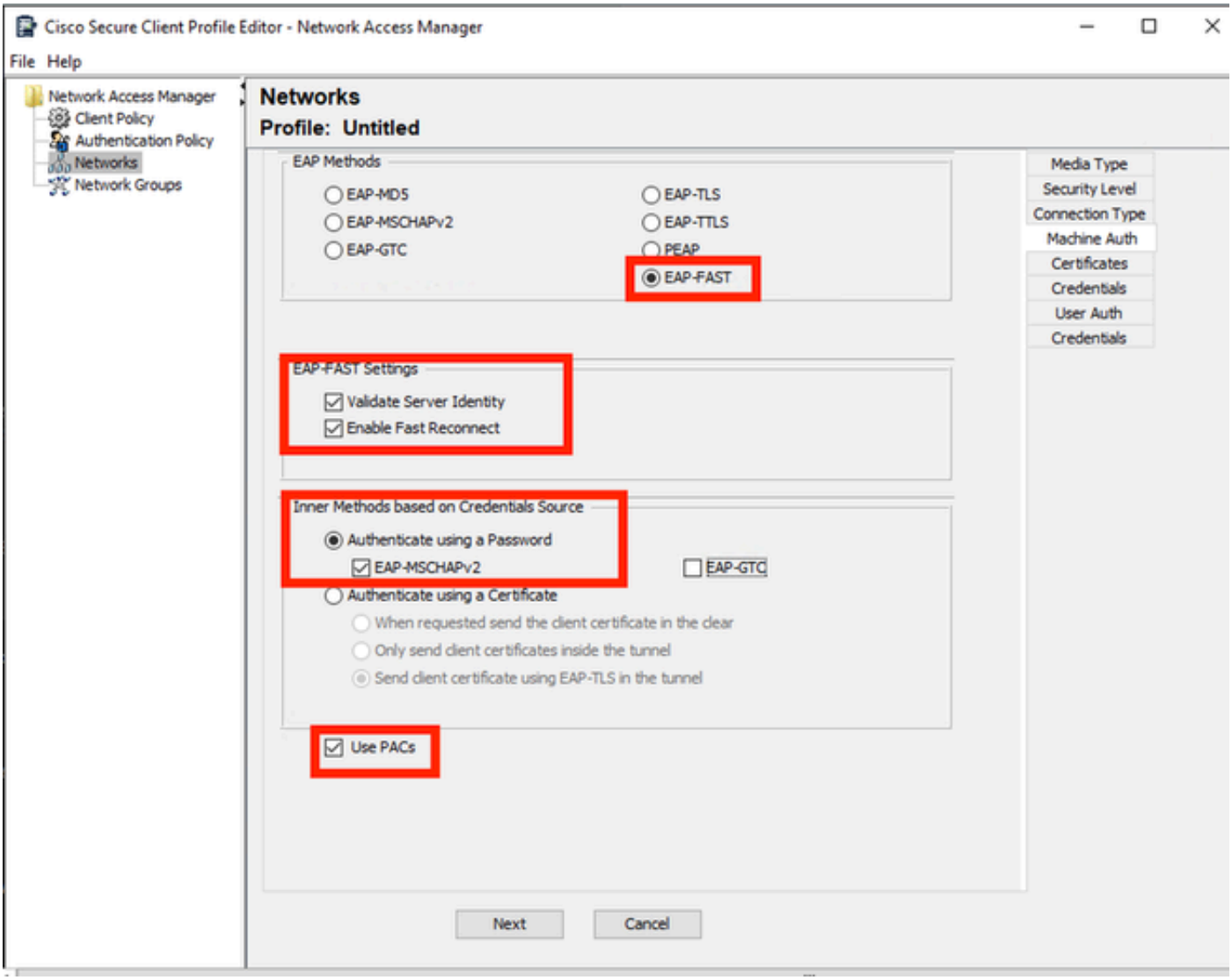
Klicken Sie auf Weiter, um mit dem Abschnitt Verbindungstyp fortzufahren.



Abschnitt "Verbindungstyp"

Konfigurieren Sie die Benutzer- und Computerauthentifizierung gleichzeitig, indem Sie die dritte Option auswählen.

Klicken Sie auf Next (Weiter).

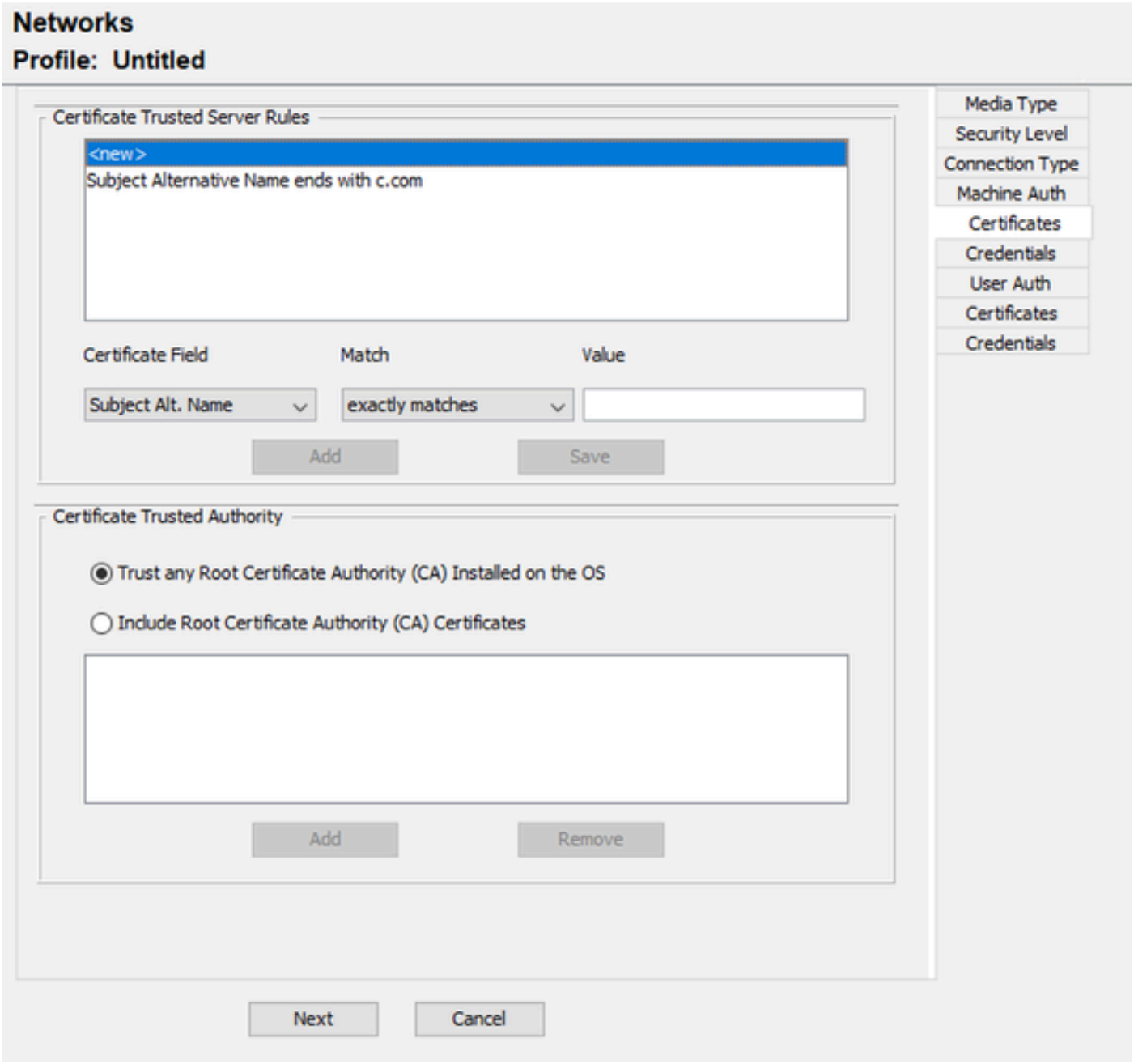


Bereich "Computerauthentifizierung"

Wählen Sie im Abschnitt Computerauthentifizierung EAP-FAST als EAP-Methode aus. Ändern Sie nicht die Standardwerte der EAP FAST-Einstellungen. Wählen Sie für den Abschnitt Innere Methoden auf Basis der Anmeldeinformationsquelle die Option Authentifizieren mit einem Kennwort und EAP-MSCHAPv2 als Methode aus. Wählen Sie dann die Option PACs verwenden.

Klicken Sie auf Next (Weiter).

Im Abschnitt Zertifikate endet in Regeln für vertrauenswürdige Server für Zertifikate der allgemeine Regelname mit c.com. Dieser Abschnitt bezieht sich auf das Zertifikat, das der Server während des EAP-PEAP-Flusses verwendet. Wenn die Identity Service Engine (ISE) in Ihrer Umgebung verwendet wird, kann der allgemeine Name des Policy Server Node EAP-Zertifikats verwendet werden.

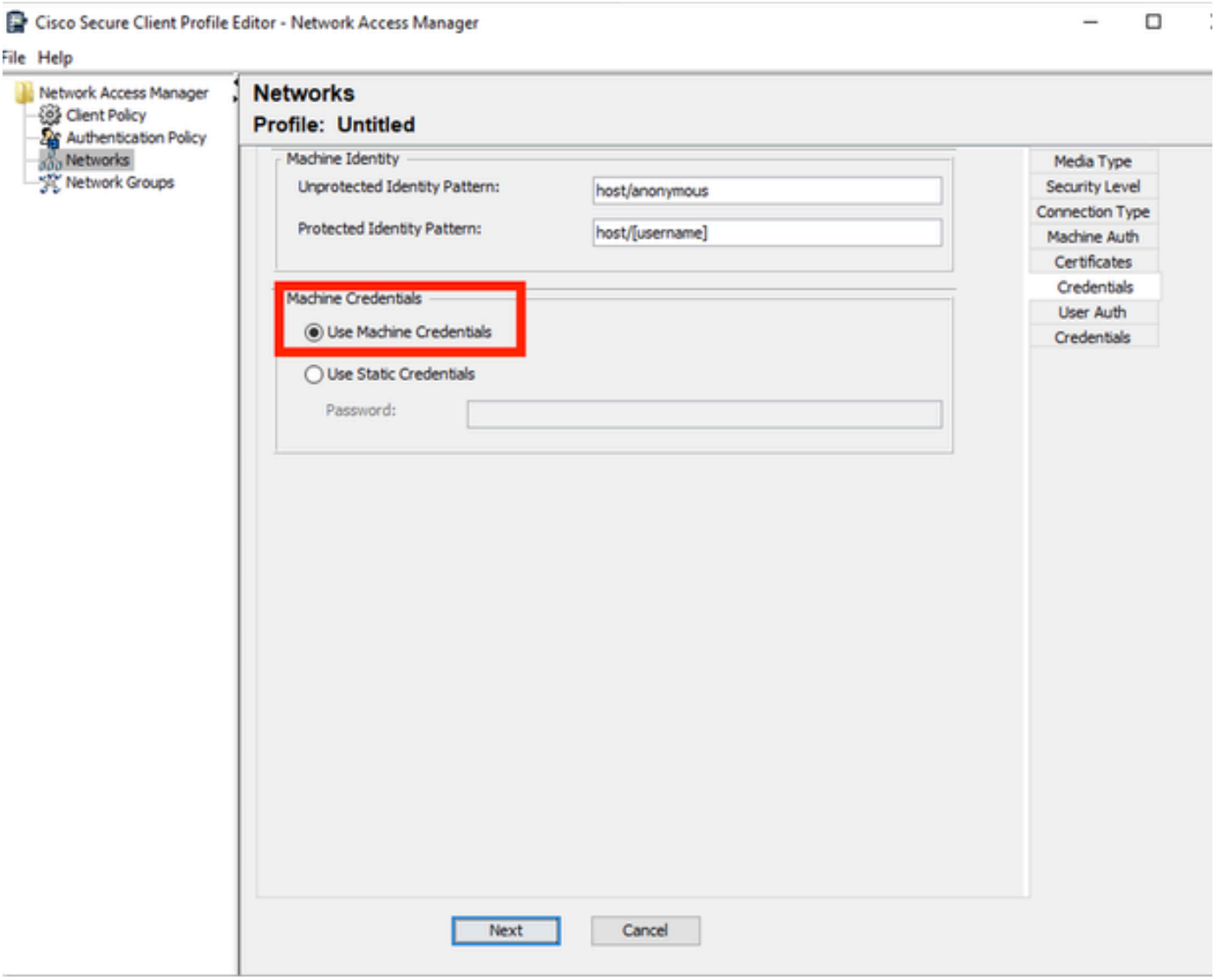


Abschnitt "Zertifikatvertrauensstellung des Computer-Authentifizierungsservers"

In der vertrauenswürdigen Zertifizierungsstelle für Zertifikate können zwei Optionen ausgewählt werden. Verwenden Sie in diesem Szenario anstelle eines spezifischen Zertifizierungsstellenzertifikats, das das RADIUS-EAP-Zertifikat signiert hat, die Option Auf dem Betriebssystem installierte Stammzertifizierungsstelle vertrauen.

Mit dieser Option vertraut Windows jedem EAP-Zertifikat, das von einem Zertifikat signiert wird, das im Programm Benutzerzertifikate verwalten enthalten ist (Aktueller Benutzer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate).

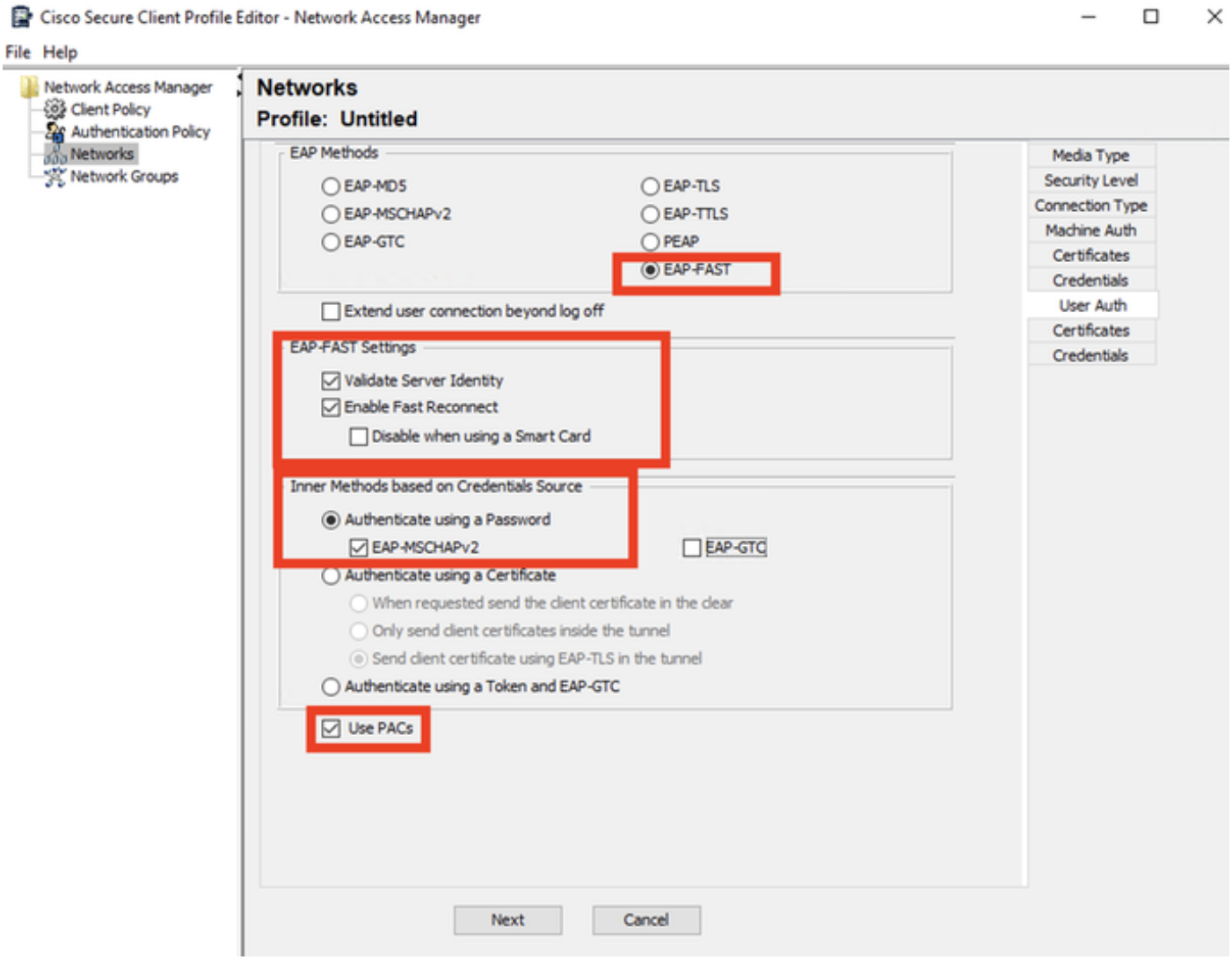
Klicken Sie auf Next (Weiter).



Abschnitt "Anmeldeinformationen für die Authentifizierung der Maschine"

Wählen Sie im Abschnitt Computeranmeldeinformationen die Option Computeranmeldeinformationen verwenden aus.

Klicken Sie auf Next (Weiter).



Abschnitt "Benutzerauthentifizierung"

Wählen Sie als Benutzerauthentifizierung EAP-FAST als EAP-Methode aus.

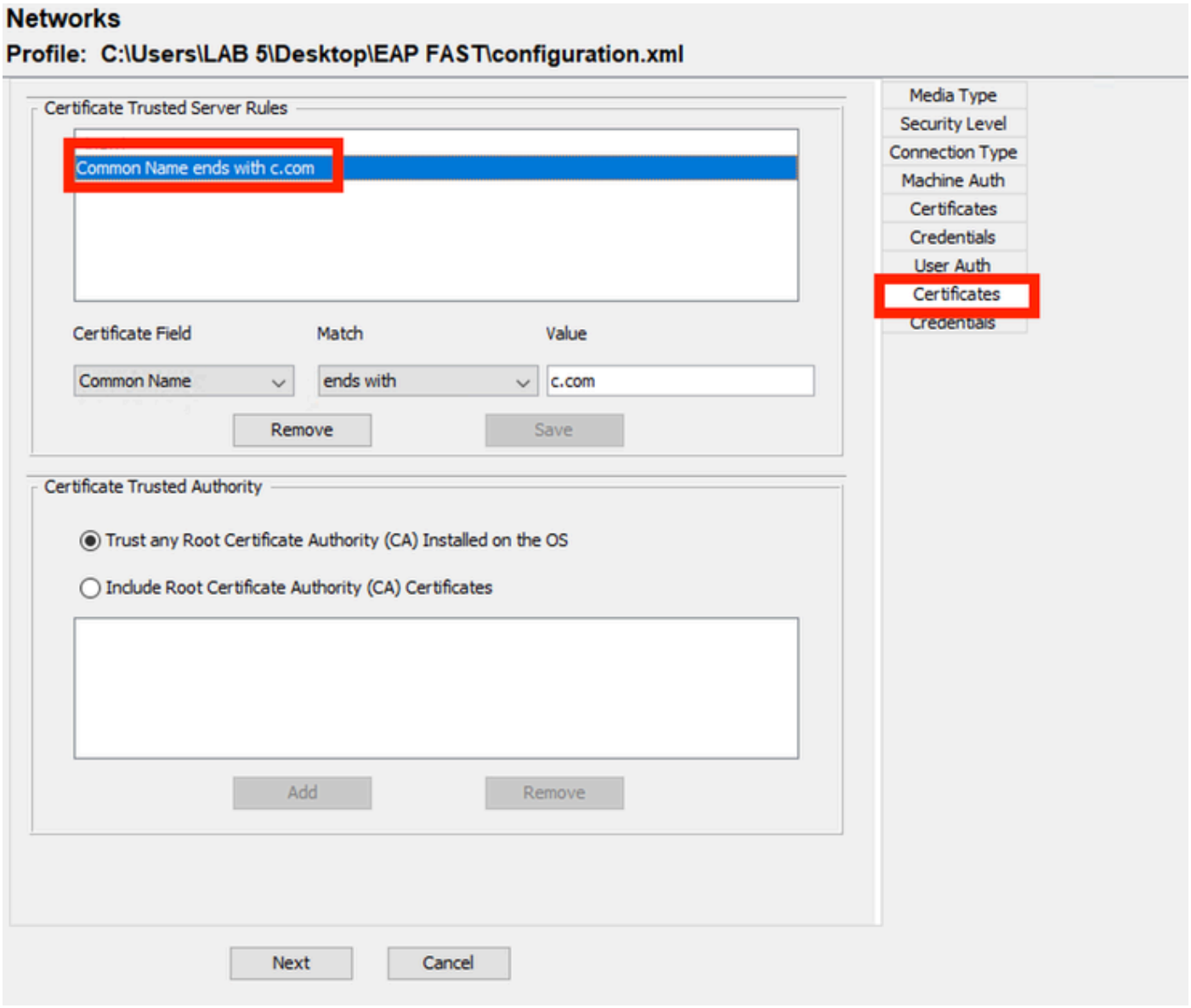
Ändern Sie nicht die Standardwerte im Abschnitt EAP-FAST-Einstellungen.

Wählen Sie für den Quellabschnitt "Interne Methode auf Basis von Anmeldeinformationen" die Option Authentifizieren mit einem Kennwort und EAP-MSCHAPv2 als Methode aus.

Wählen Sie PACs verwenden aus.

Klicken Sie auf Next (Weiter).

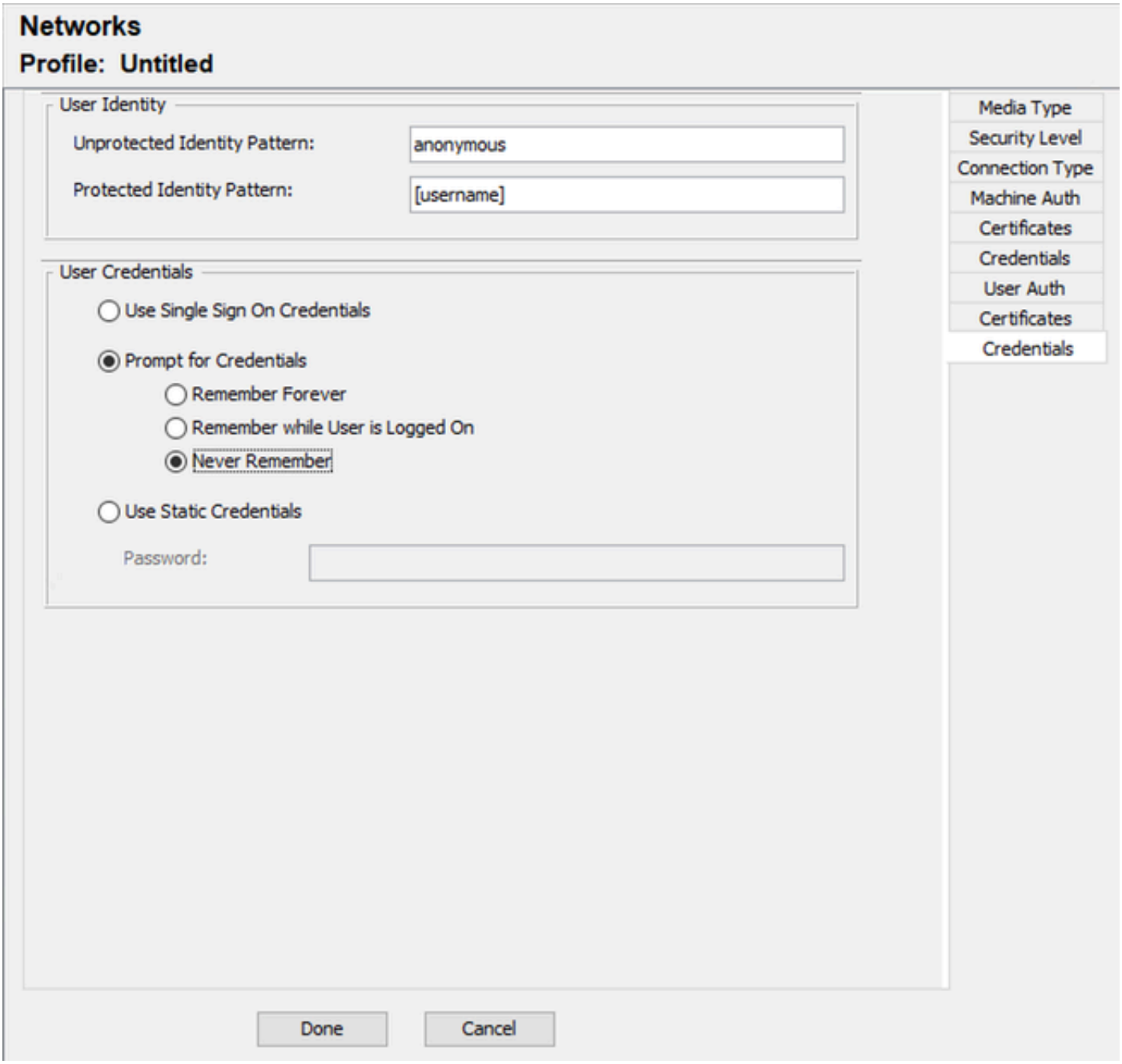
Im Abschnitt Zertifikate unter Regeln für vertrauenswürdige Zertifikatserver ist die Regel Common Name endet mit c.com. Diese Konfigurationen gelten für das Zertifikat, das der Server während des EAP-PEAP-Flows verwendet. Wenn ISE in Ihrer Umgebung verwendet wird, kann der allgemeine Name des Policy Server Node EAP-Zertifikats verwendet werden.



Zertifikatvertrauenswürdigkeitsabschnitt des Benutzerauthentifizierungsservers

In der vertrauenswürdigen Zertifizierungsstelle für Zertifikate können zwei Optionen ausgewählt werden. In diesem Szenario wird anstelle des Hinzufügens eines spezifischen Zertifizierungsstellenzertifikats, das das RADIUS-EAP-Zertifikat signiert hat, die Option Auf dem Betriebssystem installierte Stammzertifizierungsstelle vertrauen verwendet.

Klicken Sie auf Next (Weiter).



Anmeldeinformationen für Benutzerauthentifizierung

Im Abschnitt "Anmeldedaten" wird nur der Abschnitt "Benutzeranmeldedaten" geändert.

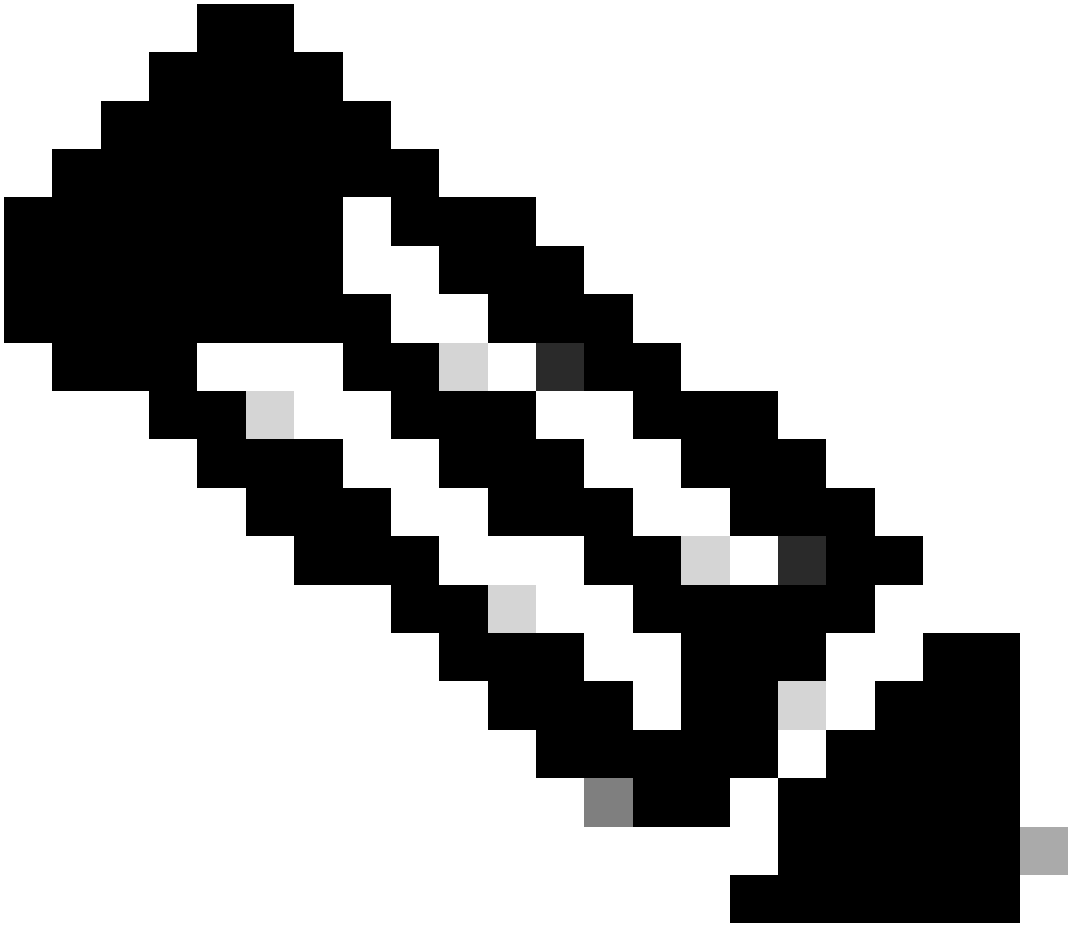
Die Option Prompt for Credentials > Never Remember ist aktiviert. Bei jeder Authentifizierung muss der authentifizierende Benutzer also seine Anmeldeinformationen eingeben.

Klicken Sie auf die Schaltfläche Fertig.

Wählen Sie Datei > Speichern unter aus, und speichern Sie das Profil des Secure Client Network Access Manager unter configuration.xml.

Wenn Sie möchten, dass der Secure Client Network Access Manager das soeben erstellte Profil verwendet, ersetzen Sie die Datei configuration.xml im nächsten Verzeichnis durch das neue:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



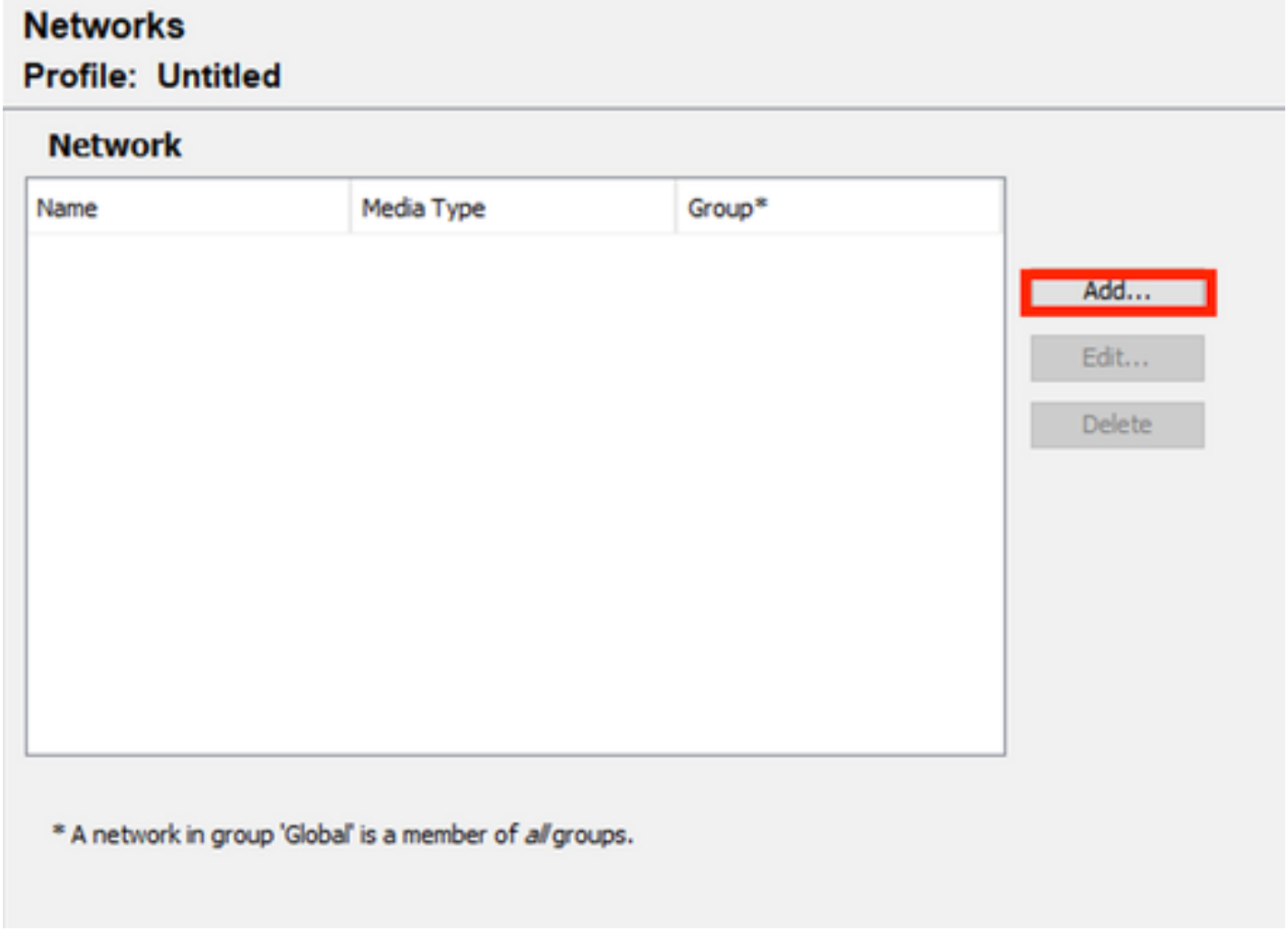
Hinweis: Die Datei muss den Namen configuration.xml haben, sonst funktioniert sie nicht.

---

6. Szenario 3: Konfigurieren der Secure Client NAM-Komponente für die EAP TLS-Benutzerzertifikatauthentifizierung

Öffnen Sie den NAM Profile Editor, und navigieren Sie zum Abschnitt Netzwerke.

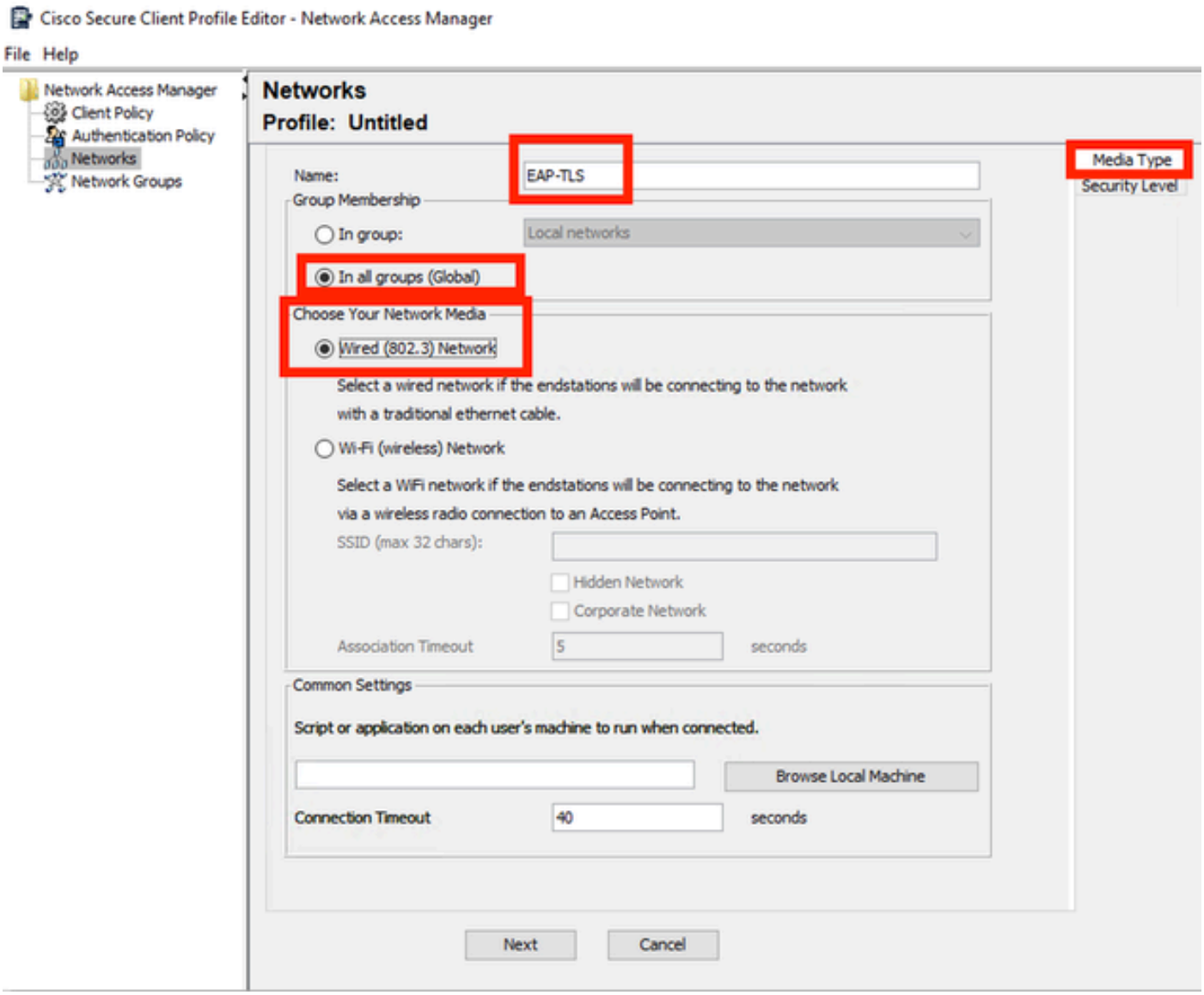
Klicken Sie auf Hinzufügen.



Bereich Netzwerkerstellung

Nennen Sie das Netzwerkprofil. In diesem Fall wird das Profil mit dem für dieses Szenario verwendeten EAP-Protokoll benannt.

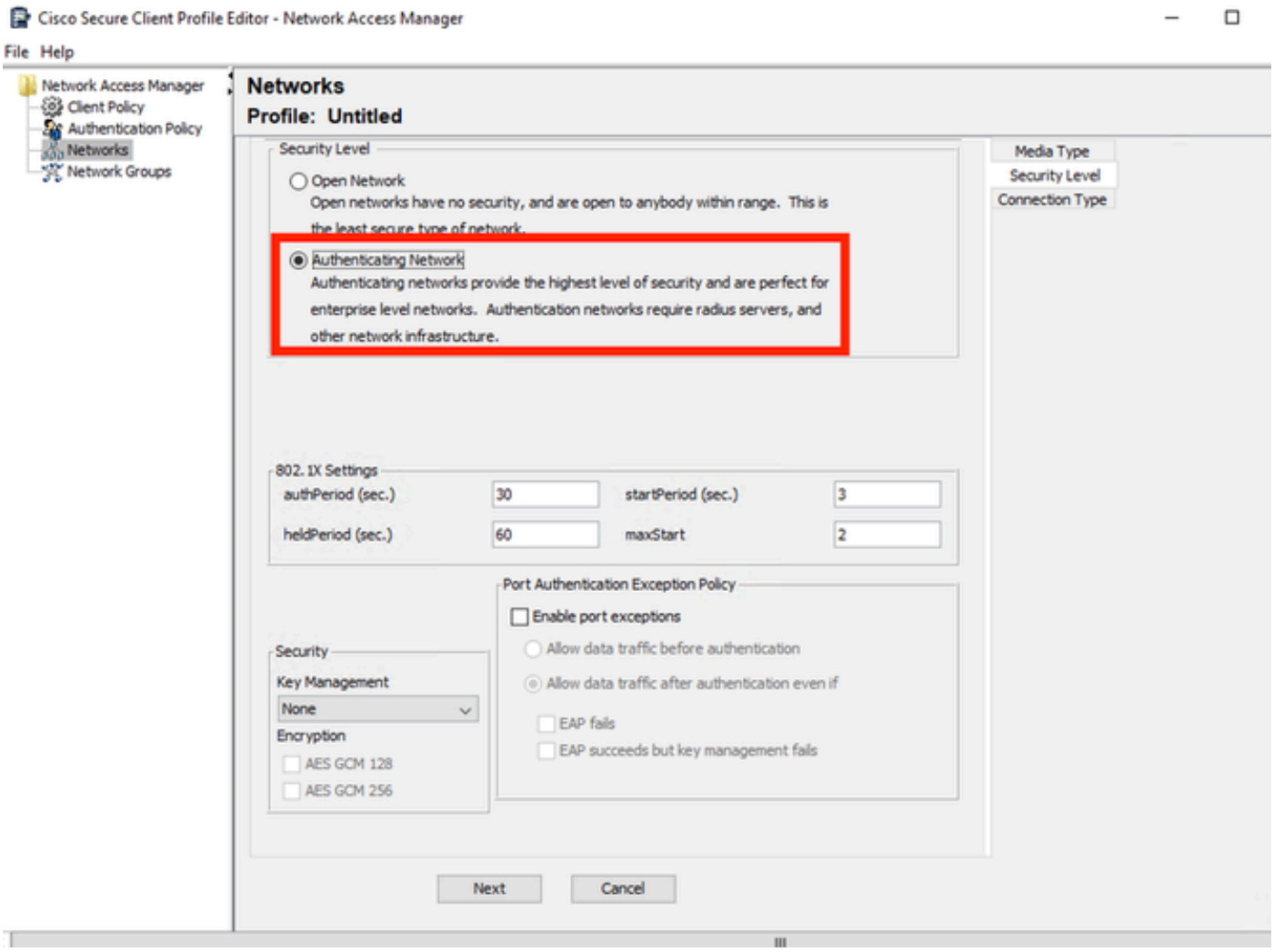
Wählen Sie Global als Gruppenmitgliedschaft aus. und kabelgebundene Netzwerkmedien.



Bereich Medientyp

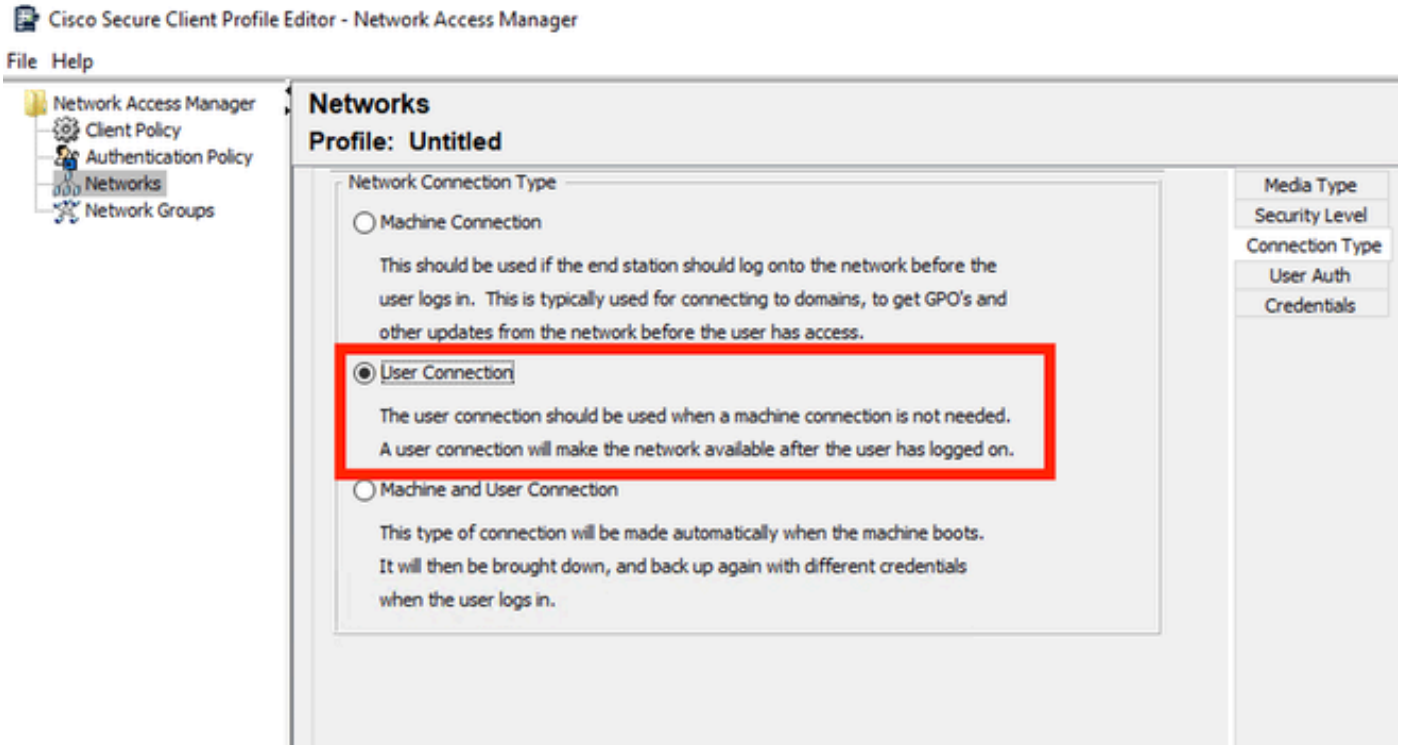
Klicken Sie auf Next (Weiter).

Wählen Sie Authentifizierendes Netzwerk aus, und ändern Sie die Standardwerte für die übrigen Optionen im Abschnitt Sicherheitsstufe nicht.



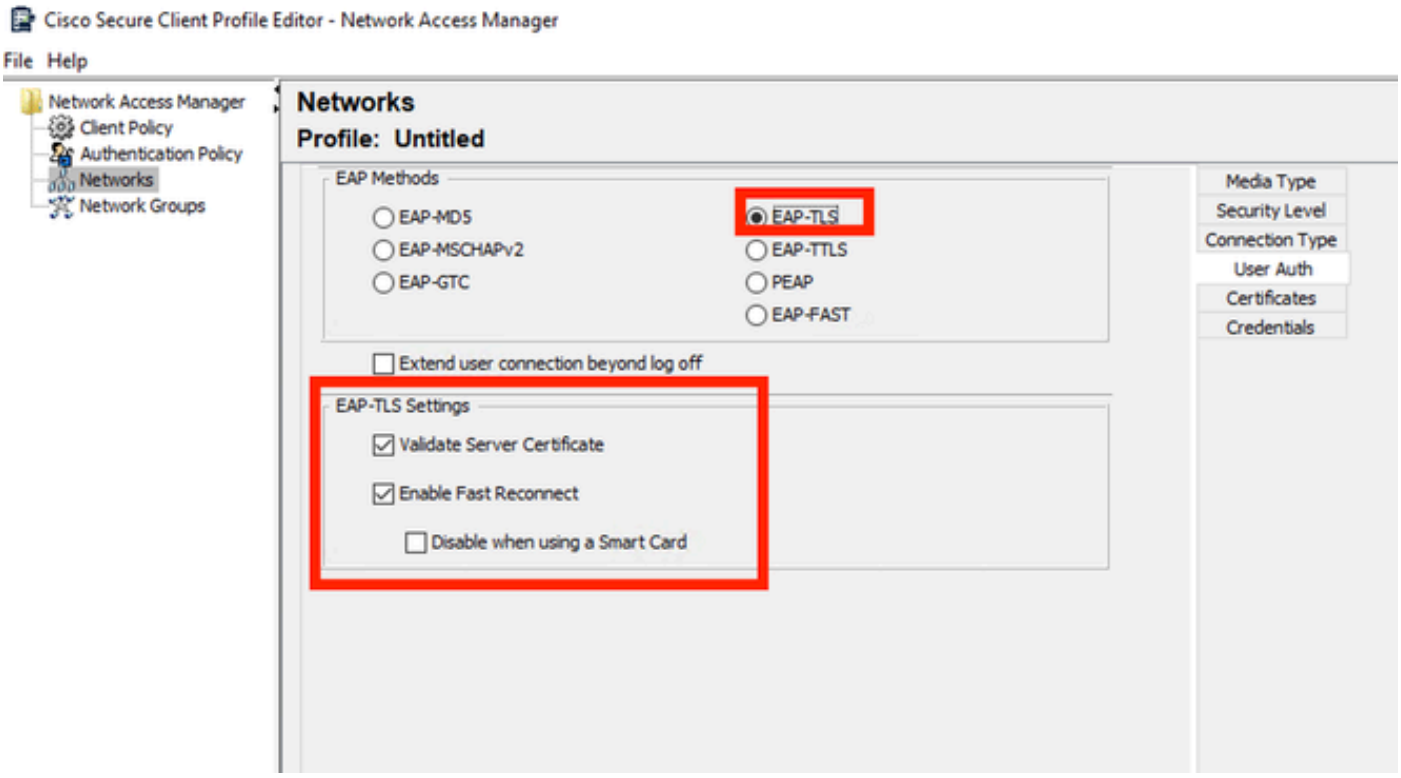
Sicherheitsstufe

Dieses Szenario bezieht sich auf die Benutzerauthentifizierung mit einem Zertifikat. Aus diesem Grund wird die Option User Connection verwendet.



Verbindungstyp

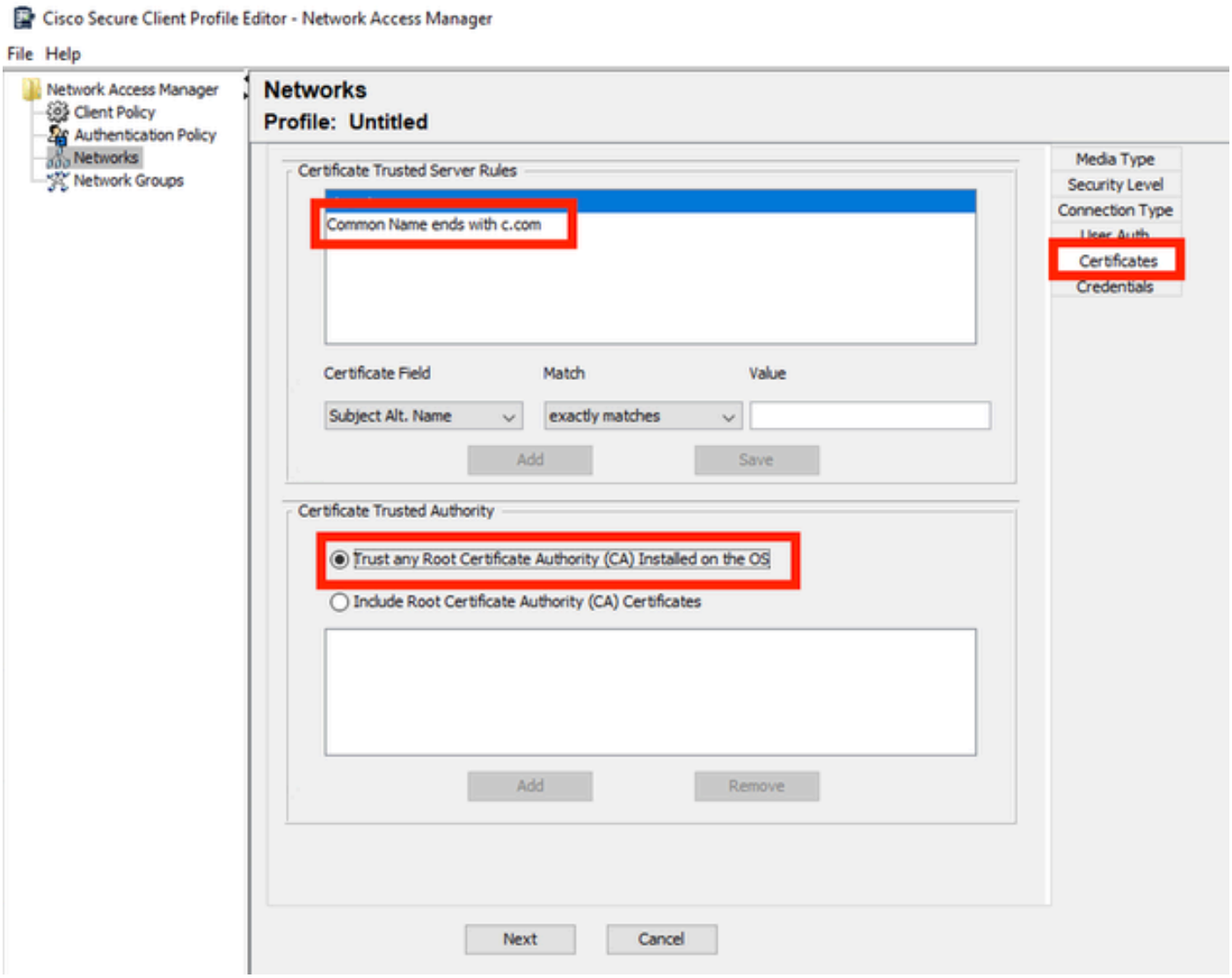
Konfigurieren Sie EAP-TLS als EAP-Methode. Ändern Sie nicht die Standardwerte im Abschnitt EAP-TLS-Einstellungen.



Bereich "Benutzerauthentifizierung"

Erstellen Sie für den Abschnitt "Zertifikate" eine Regel, die mit dem AAA-EAP-TLS-Zertifikat übereinstimmt. Wenn Sie die ISE verwenden, finden Sie diese Regel im Abschnitt Administration > System > Certificates (Verwaltung > System > Zertifikate).

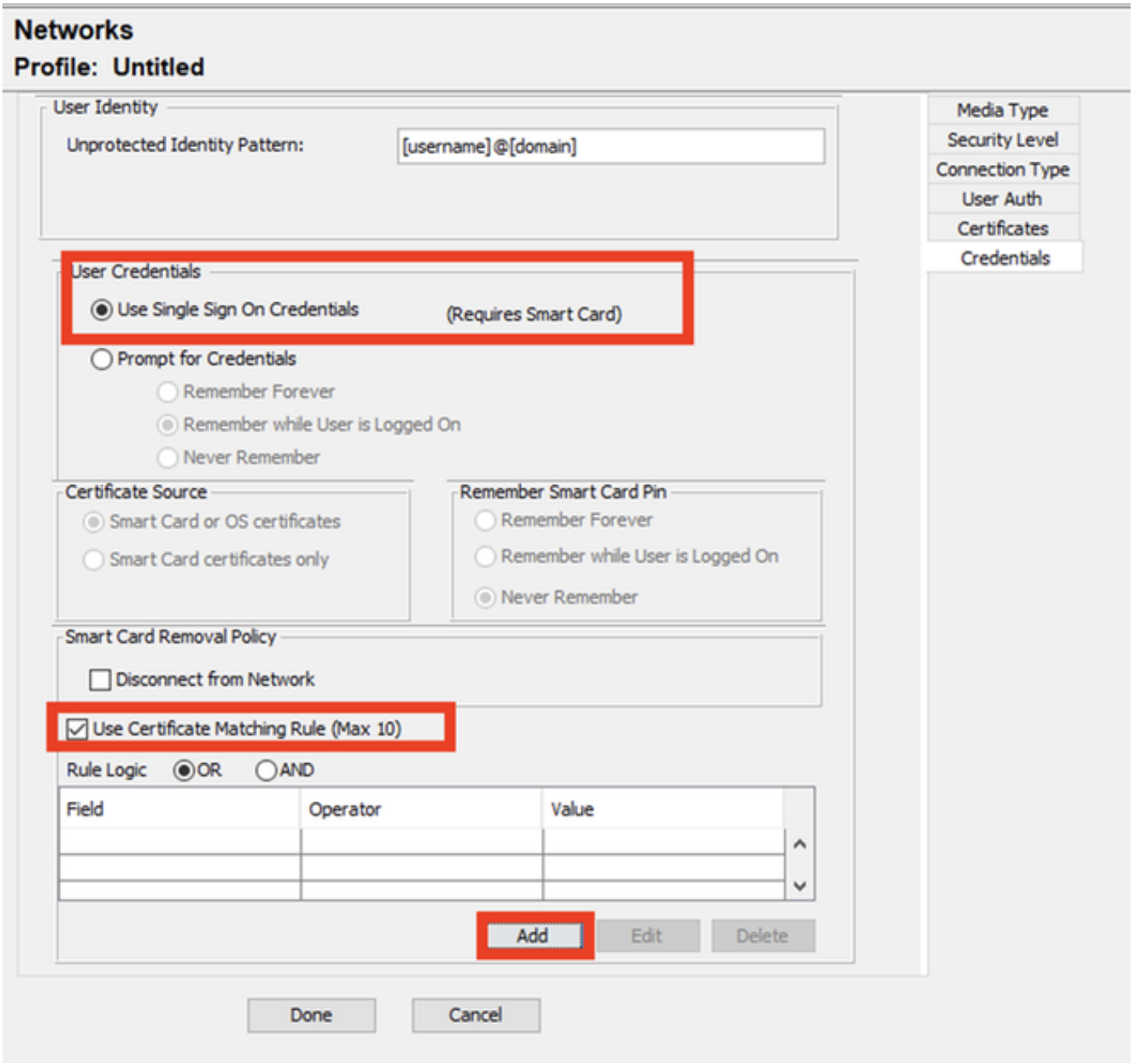
Wählen Sie im Abschnitt Certificate Trusted Authority (Vertrauenswürdige Zertifizierungsstelle für Zertifikate) die Option Trust any Root Certificate Authority (Zertifizierungsstelle für Stammzertifikate) aus, die auf dem Betriebssystem installiert ist.



Zertifikatvertrauenseinstellungen des Benutzerauthentifizierungsservers

Klicken Sie auf Next (Weiter).

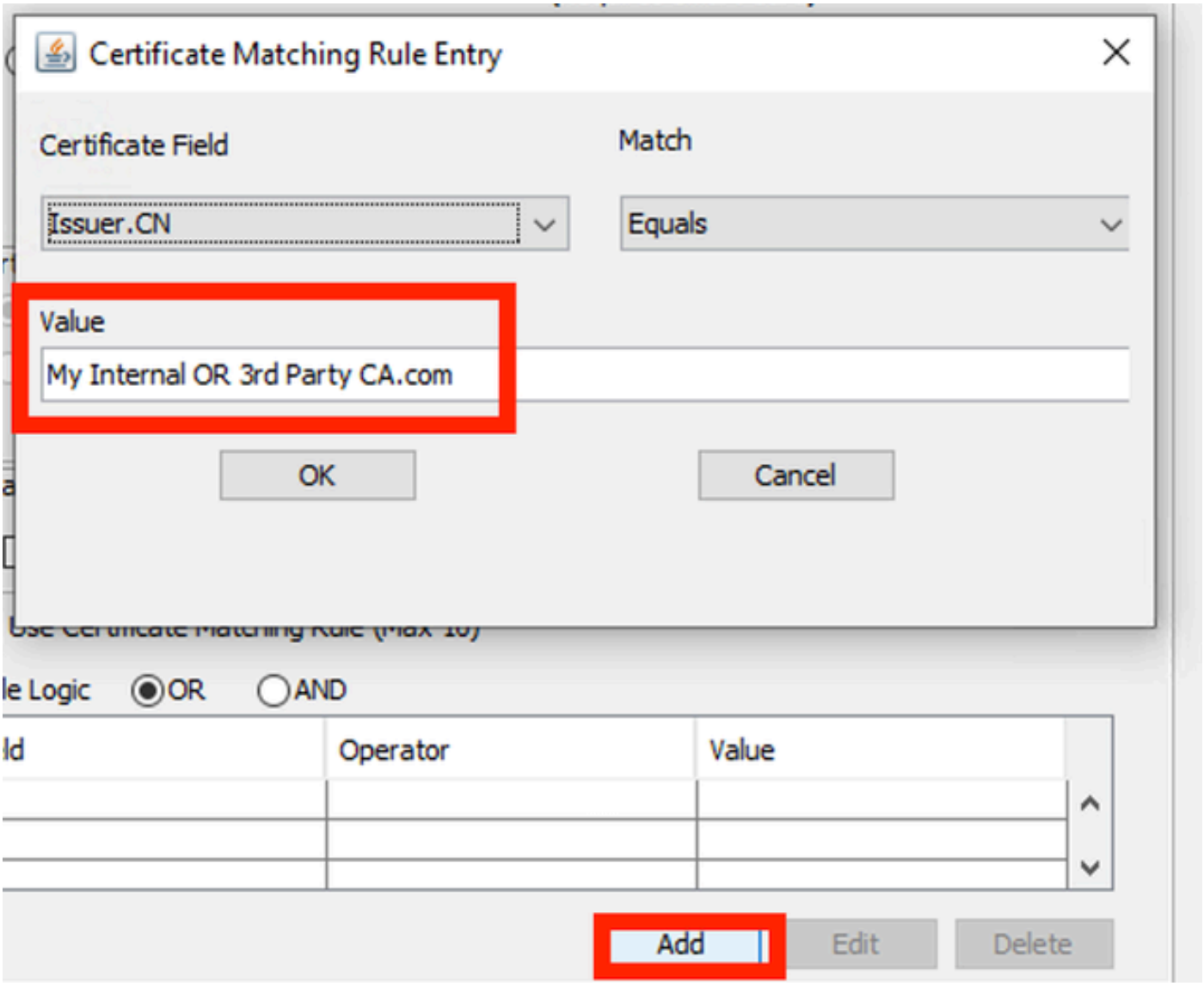
Ändern Sie im Abschnitt User Credentials (Benutzeranmeldeinformationen) nicht die Standardwerte im ersten Teil.



Abschnitt "Benutzer-Authentifizierungsdaten"

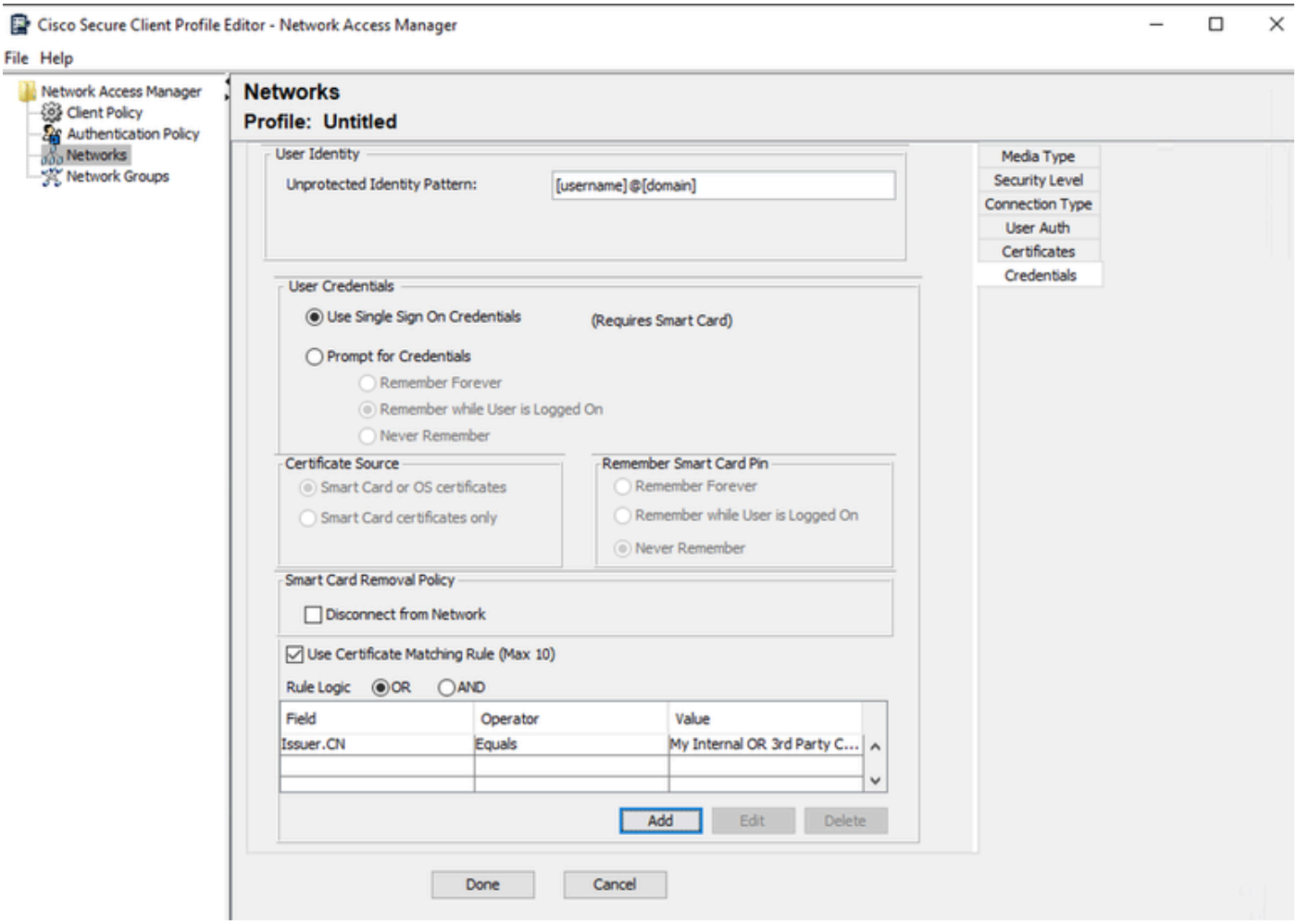
Es ist wichtig, eine Regel zu konfigurieren, die mit dem Identitätszertifikat übereinstimmt, das der Benutzer während des EAP-TLS-Prozesses sendet. Klicken Sie dazu auf das Kontrollkästchen neben Regel für die Zertifikatzuordnung verwenden (max. 10).

Klicken Sie auf Hinzufügen.



Fenster "Certificate Matching Rule"

Ersetzen Sie die Zeichenfolge My Internal OR 3rd Party CA.com durch die CN des Benutzerzertifikats.



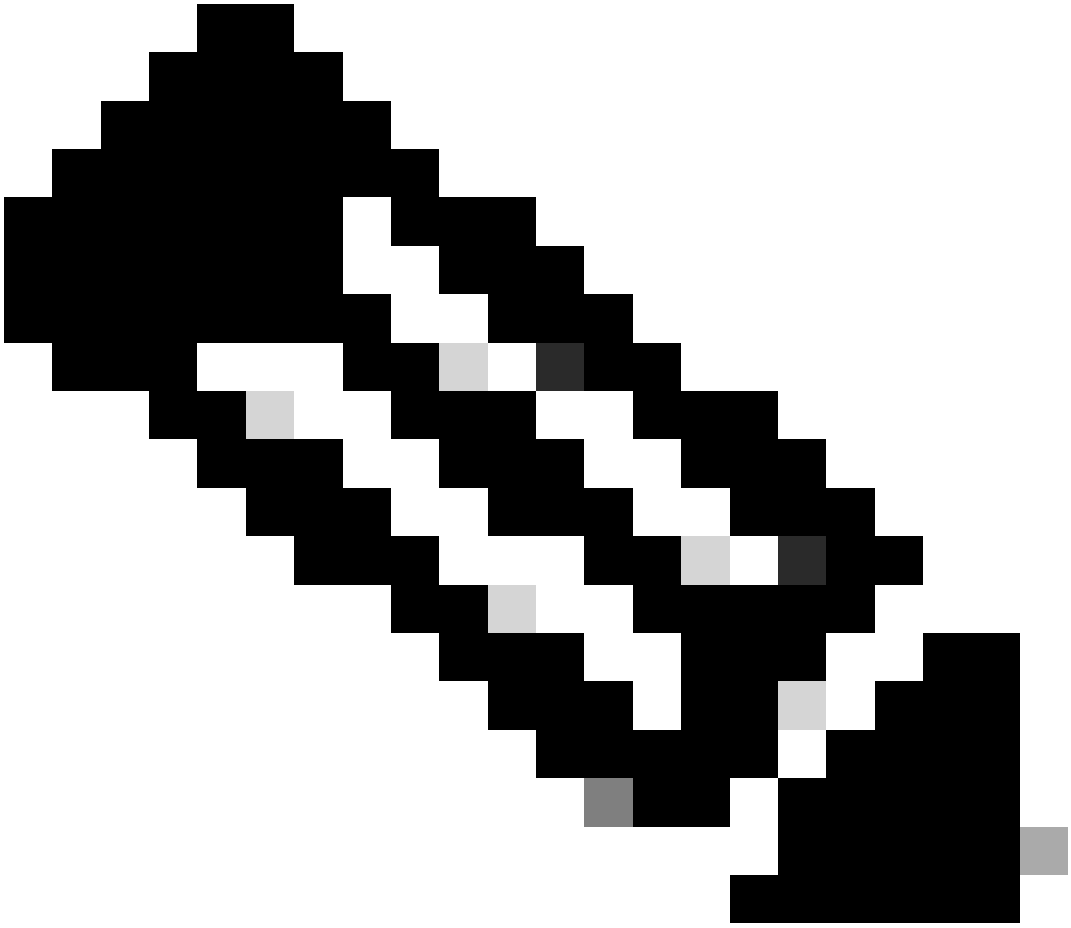
Abschnitt "Anmeldeinformationen für Benutzerauthentifizierungszertifikat"

Klicken Sie auf Fertig, um die Konfiguration abzuschließen.

Wählen Sie Datei > Speichern unter, um das Profil des Secure Client Network Access Manager als configuration.xml zu speichern.

Wenn Sie möchten, dass der Secure Client Network Access Manager das soeben erstellte Profil verwendet, ersetzen Sie die Datei configuration.xml im nächsten Verzeichnis durch das neue:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



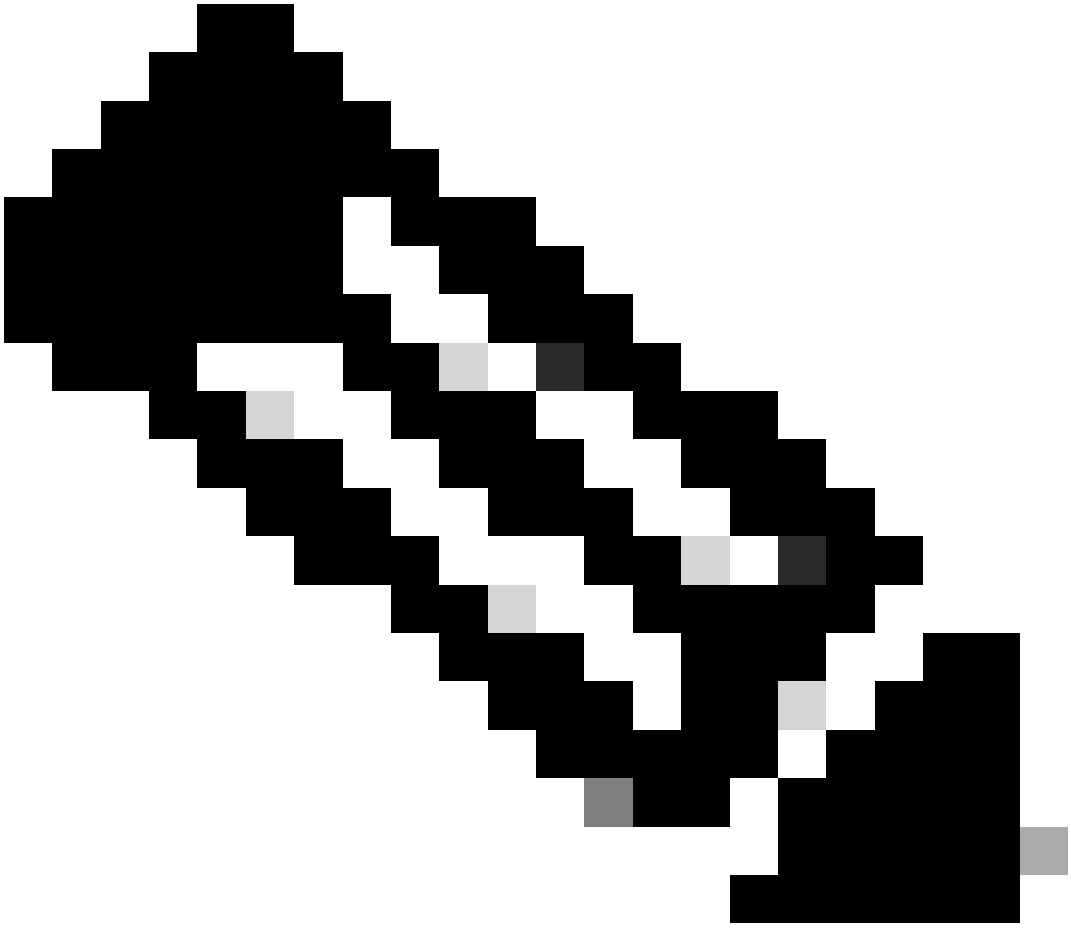
Hinweis: Die Datei muss den Namen configuration.xml haben, sonst funktioniert sie nicht.

---

7. Konfigurieren von ISR 1100 und ISE zum Zulassen von Authentifizierungen basierend auf PEAP MSCHAPv2 aus Szenario 1

Konfigurieren Sie den ISR 1100 Router.

In diesem Abschnitt wird die grundlegende Konfiguration beschrieben, die für das NAD erforderlich ist, damit dot1x funktioniert.



Hinweis: Zeigen Sie bei ISE-Bereitstellungen mit mehreren Knoten auf einen beliebigen Knoten, auf dem die Rolle "Policy Server Node" aktiviert ist. Sie können dies überprüfen, indem Sie auf der Registerkarte Administration > System > Deployment zu ISE navigieren.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
```

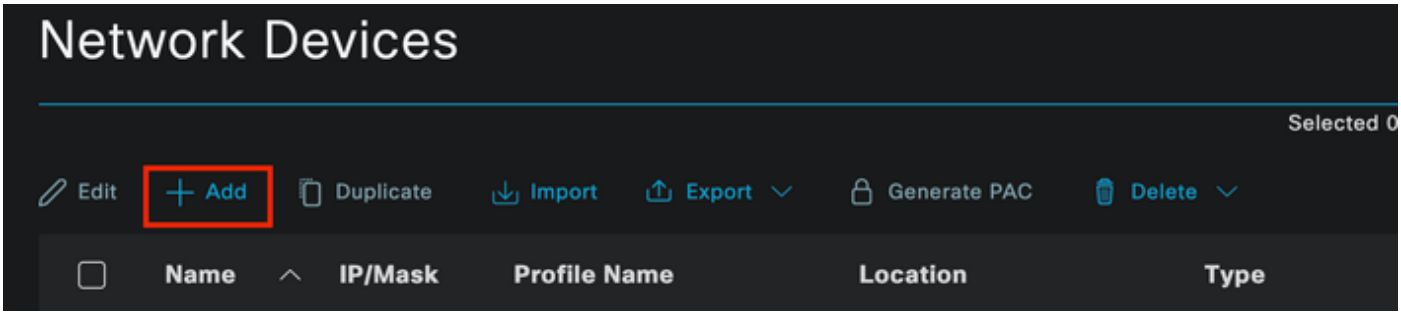
```
 key <Your shared secret>
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

Identity Service Engine 3.2 konfigurieren

Konfigurieren des Netzwerkgeräts

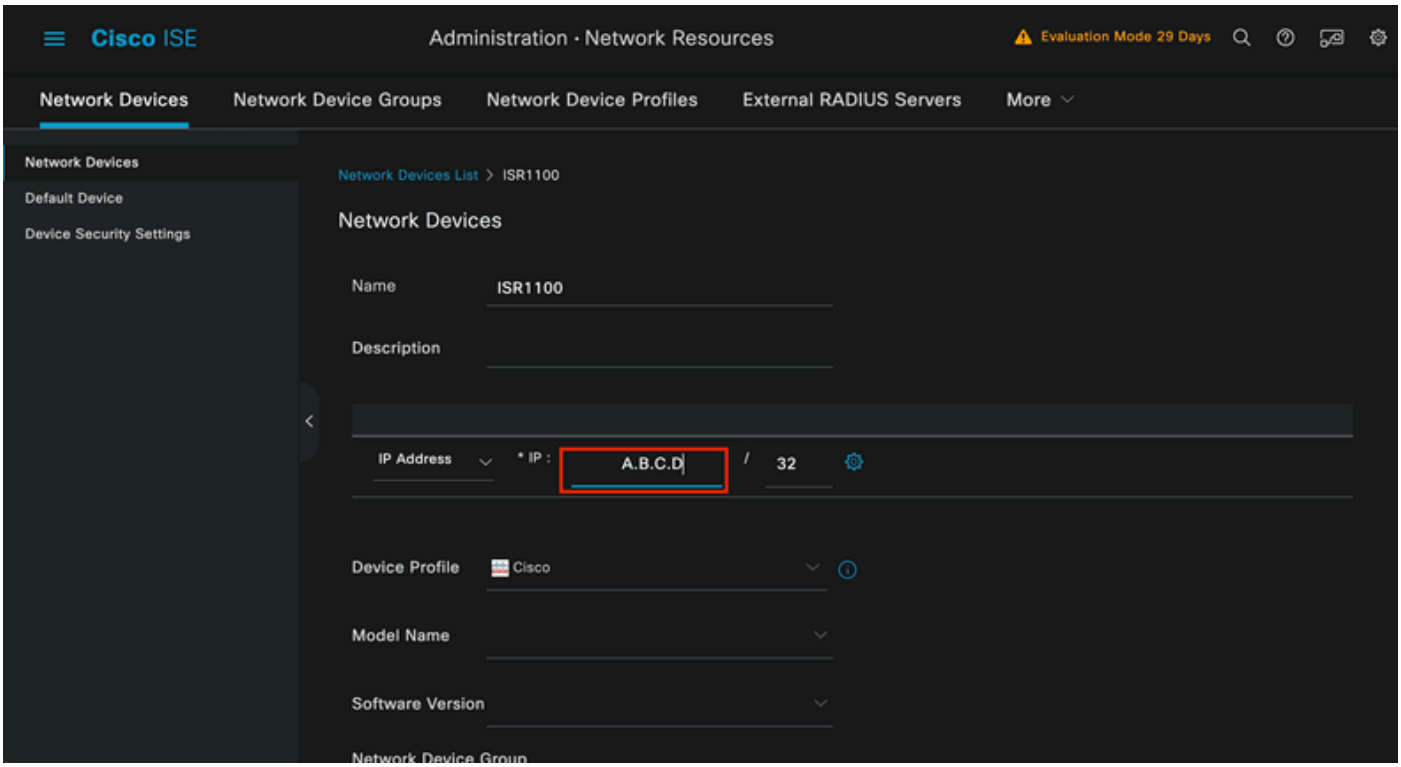
Fügen Sie ISR NAD zu ISE Administration > Network Resources > Network Devices hinzu.

Klicken Sie auf Hinzufügen.



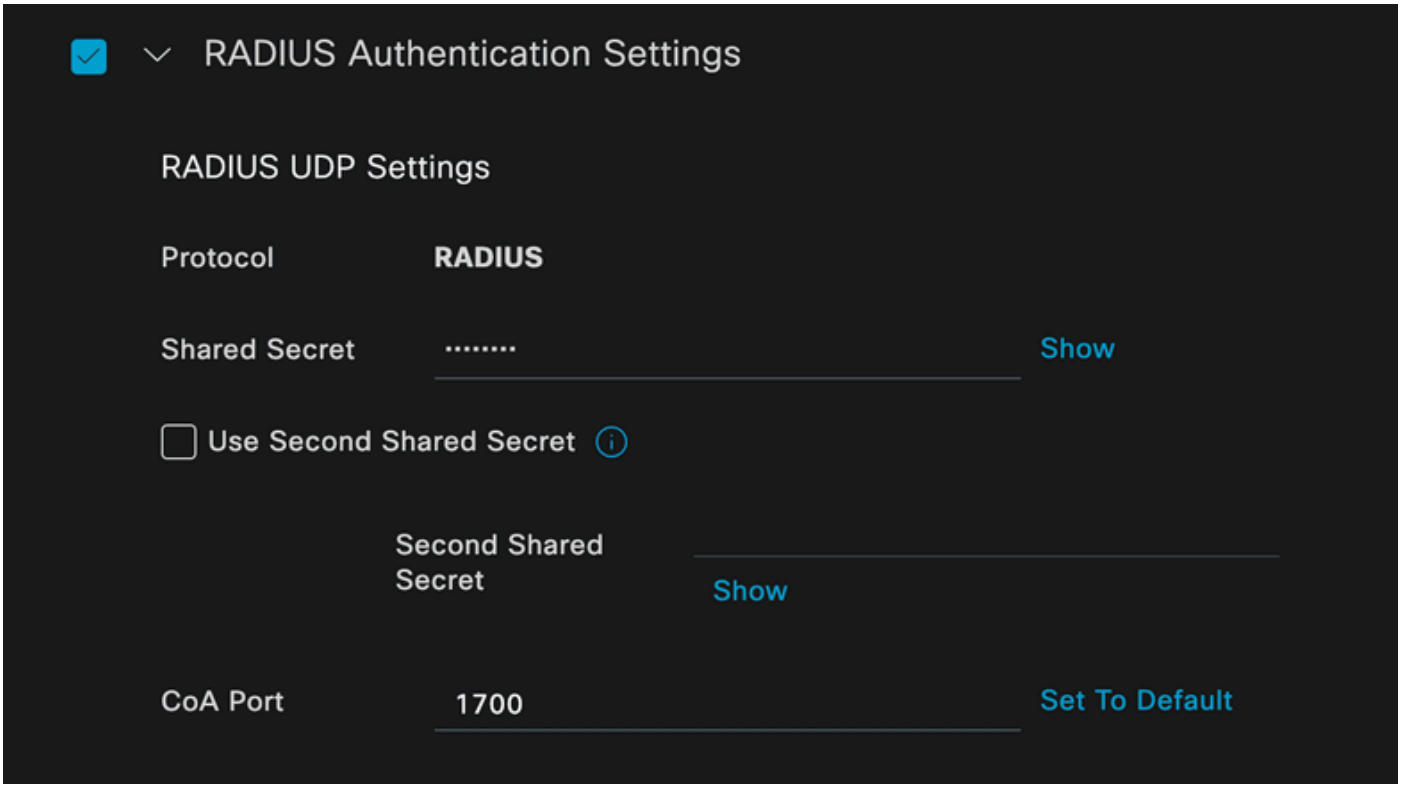
Abschnitt "Netzwerkgerät"

Weisen Sie dem von Ihnen erstellten NAD einen Namen zu. Fügen Sie die IP des Netzwerkgeräts hinzu.



Erstellung von Netzwerkgeräten

Fügen Sie am unteren Rand der Seite den gleichen gemeinsamen geheimen Schlüssel hinzu, den Sie in der Konfiguration des Netzwerkgeräts verwendet haben.



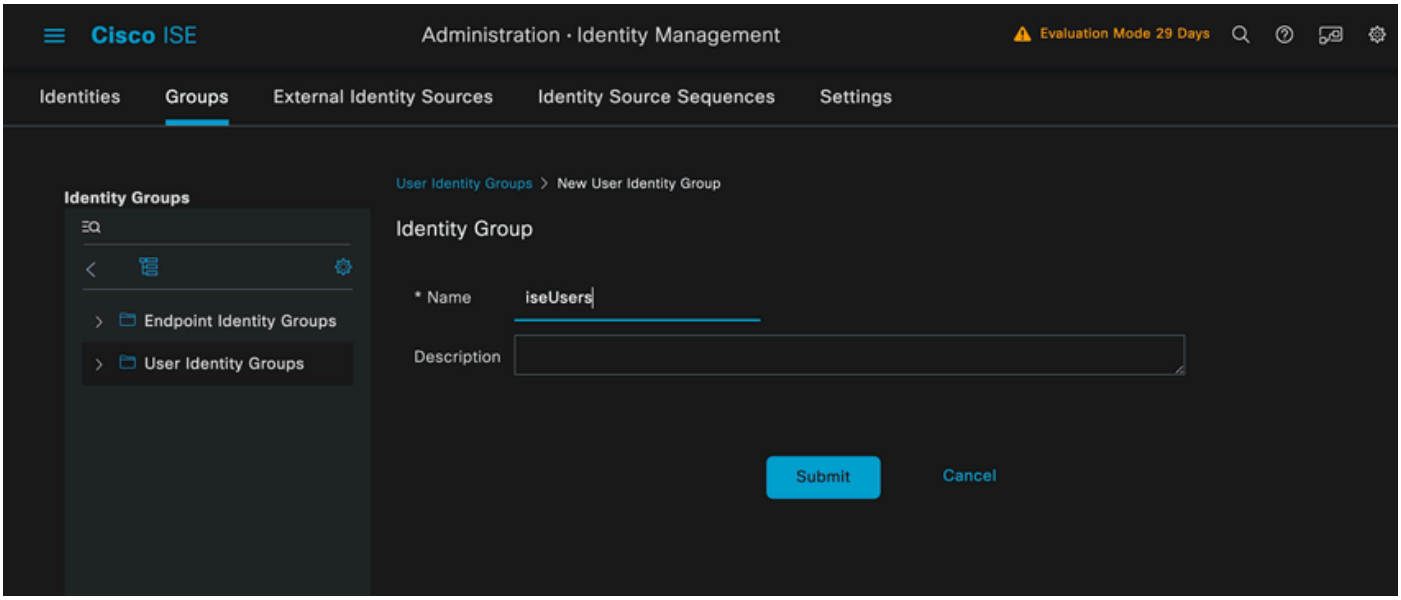
RADIUS-Einstellungen für Netzwerkgeräte

Speichern Sie die Änderungen.

Konfigurieren Sie die Identität für die Authentifizierung des Endpunkts.

Die lokale ISE-Authentifizierung wird verwendet. Die externe ISE-Authentifizierung wird in diesem Artikel nicht erläutert.

Navigieren Sie zur Registerkarte Administration > Identity Management > Groups (Verwaltung > Identitätsverwaltung > Gruppen), und erstellen Sie die Gruppe, der der Benutzer angehört. Die für diese Demonstration erstellte Identitätsgruppe lautet iseUsers.

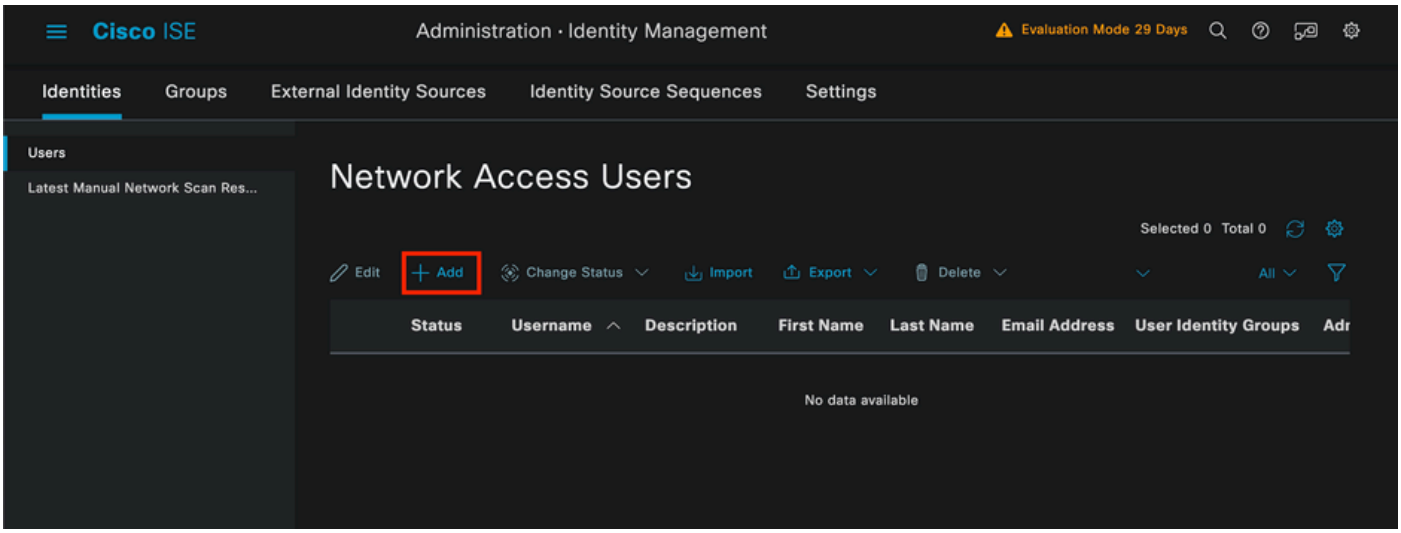


Erstellung von Identitätsgruppen

Klicken Sie auf Senden.

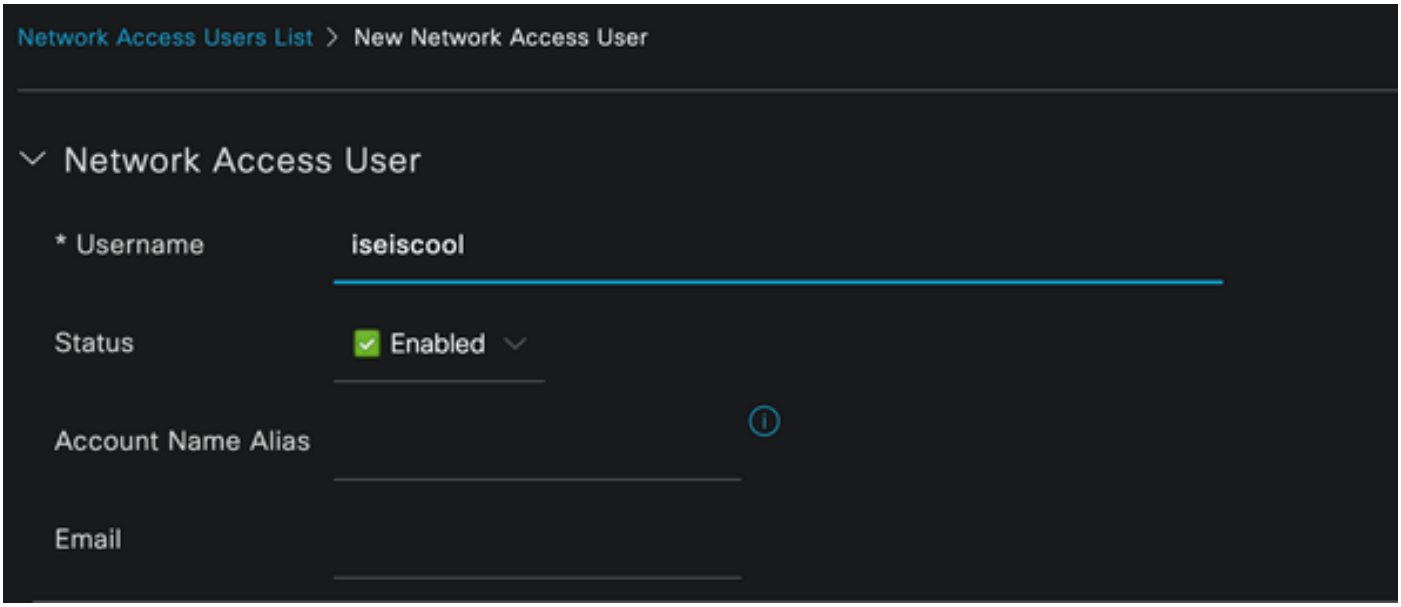
Navigieren Sie zu Administration > Identity Management > Identity Tab.

Klicken Sie auf Hinzufügen.



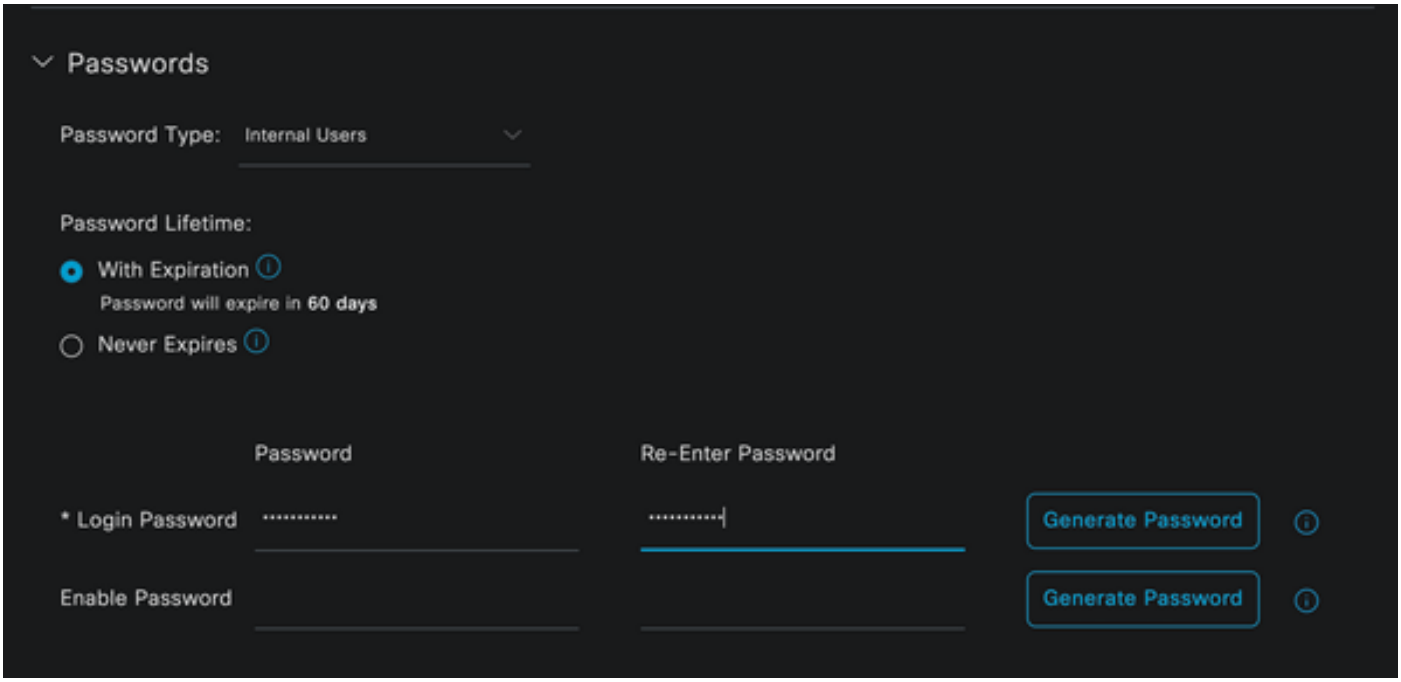
Abschnitt "Netzwerkzugriffsbenutzer"

Als Teil der Pflichtfelder beginnen Sie mit dem Namen des Benutzers. Der Benutzername iseiscool wird in diesem Beispiel verwendet.



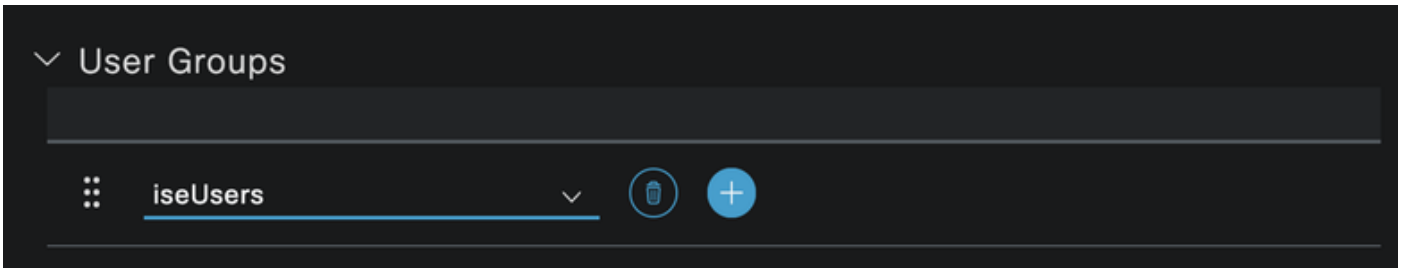
Erstellung von Netzwerkzugriffsbenutzern

Weisen Sie dem Benutzer ein Kennwort zu. VainillaISE97 wird verwendet.



Abschnitt "Benutzerkennwort erstellen"

Weisen Sie den Benutzer der Gruppe iseUsers zu.

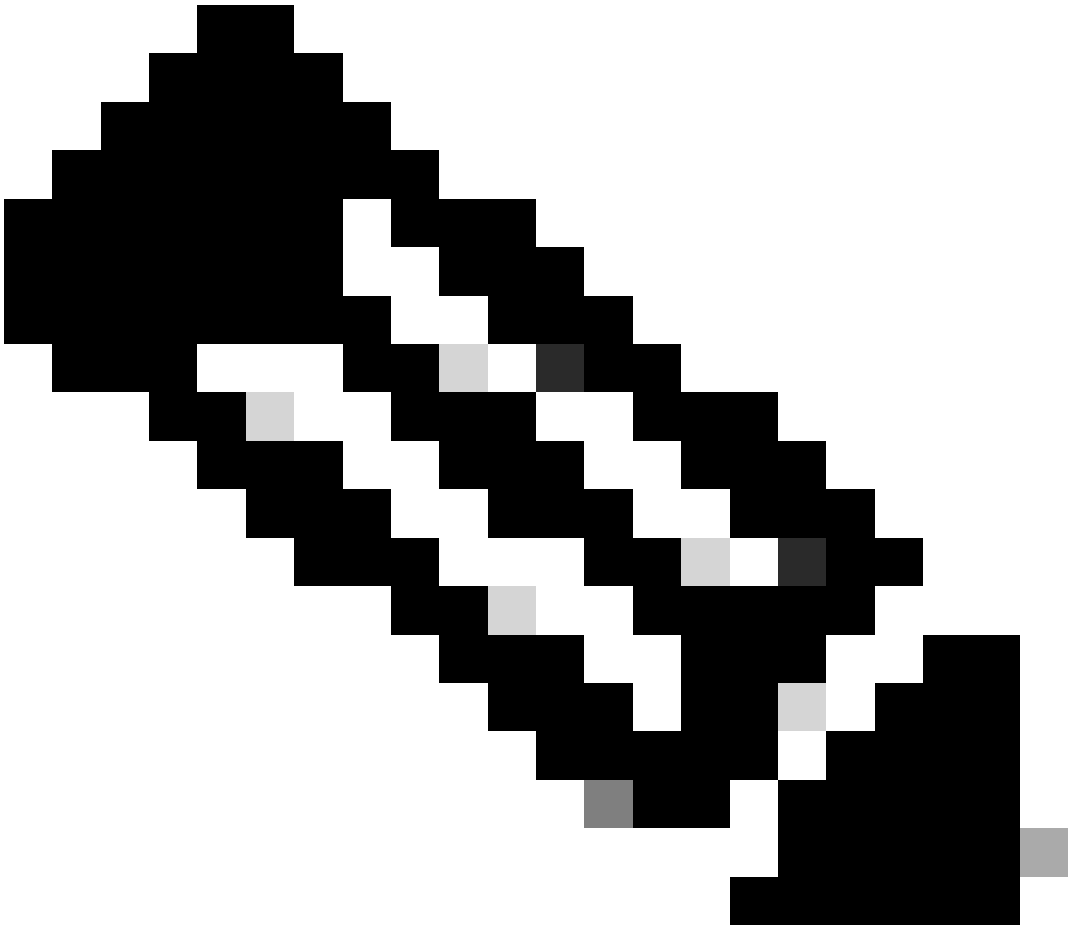


Benutzergruppenzuweisung

Konfigurieren Sie den Policy Set.

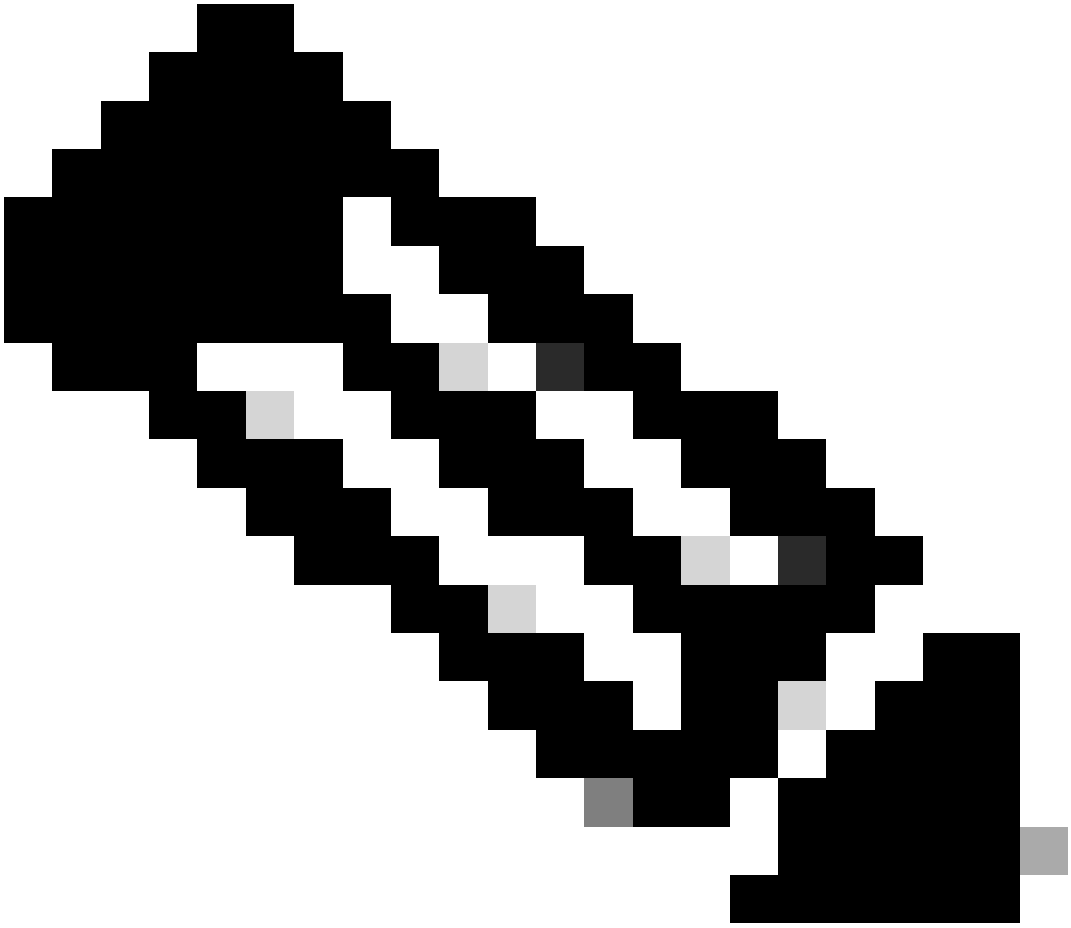
Navigieren Sie zu ISE Menu > Policy > Policy Sets.

Der standardmäßige Policy Set kann verwendet werden. Für dieses Beispiel wird jedoch eine mit dem Namen Wired erstellt.

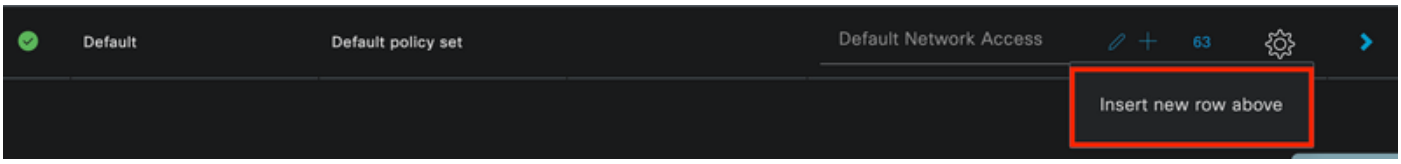


Hinweis: Die Klassifizierung und Differenzierung der Richtliniensätze hilft bei der Fehlerbehebung,

---

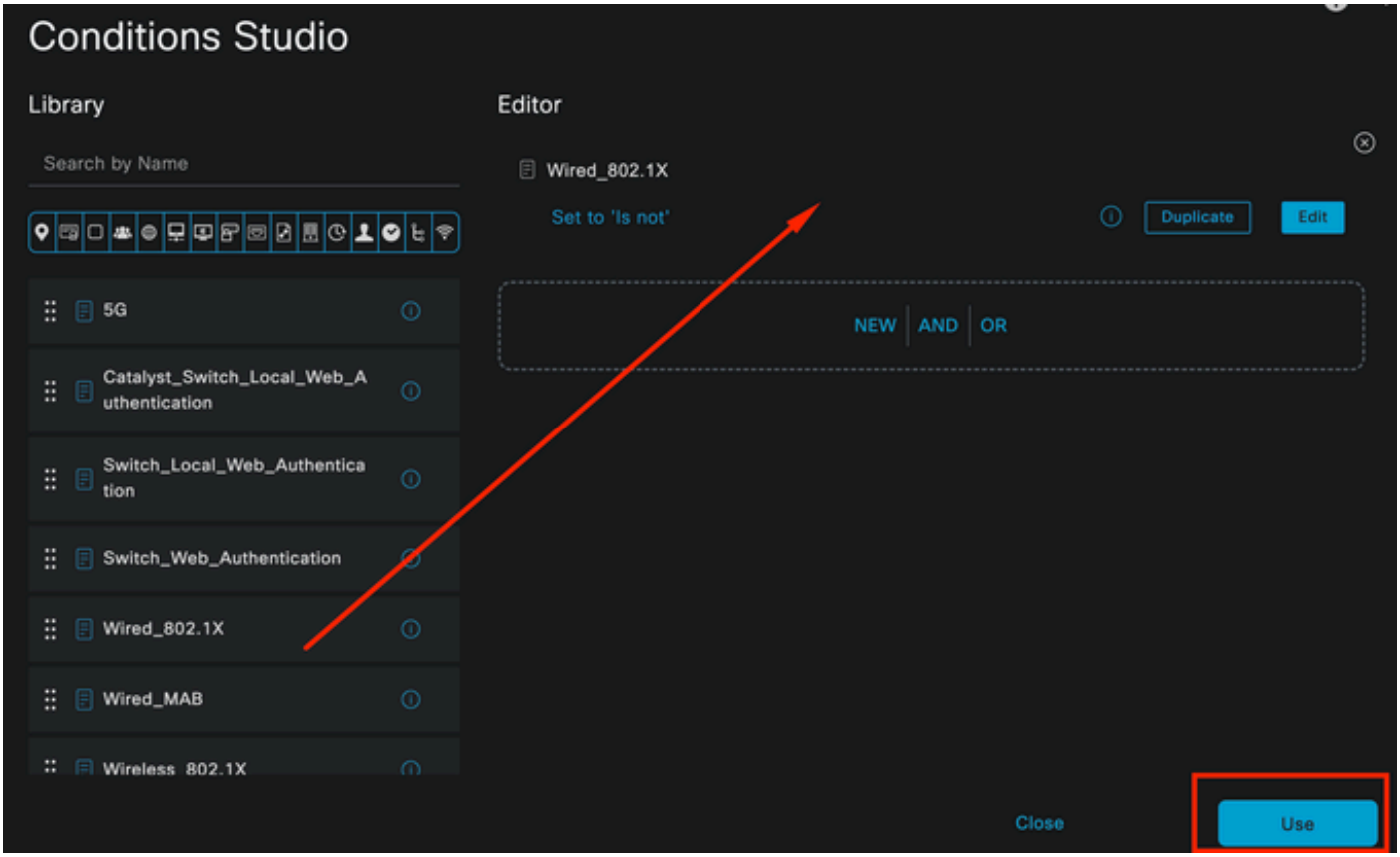


Hinweis: Wenn das Symbol zum Hinzufügen oder Hinzufügen nicht angezeigt wird, kann auf das Zahnrad-Symbol eines Policy Sets geklickt werden, und dann Neue Zeile einfügen auswählen.



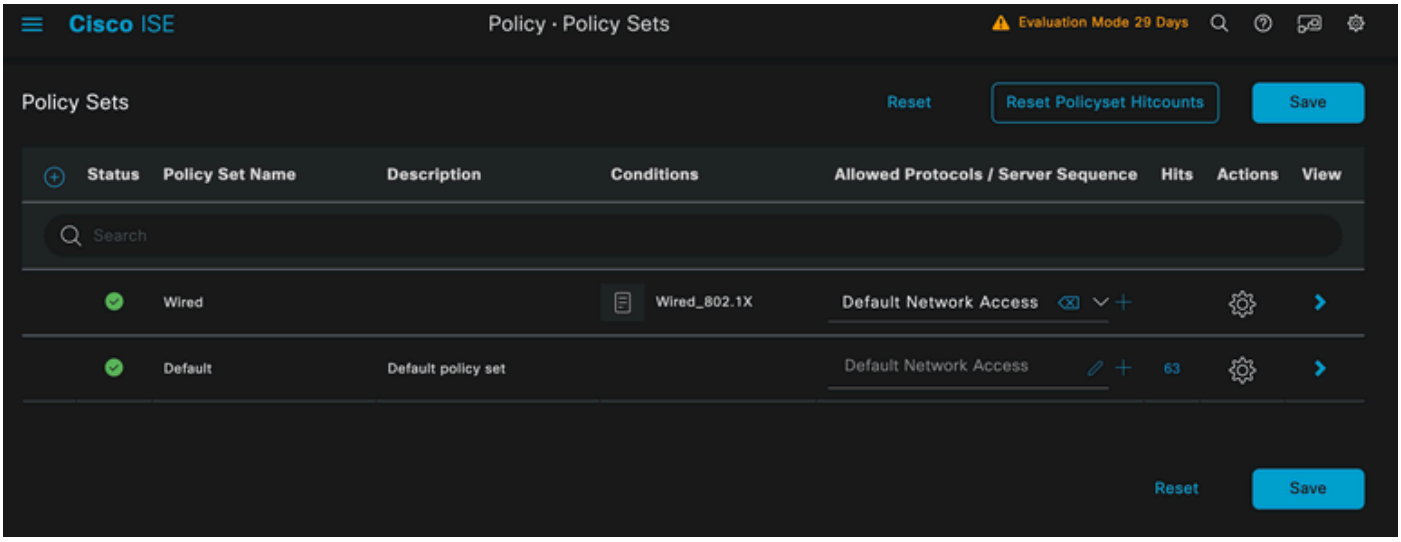
Optionen für Zahnradsymbole

Die verwendete Bedingung lautet Wired 8021x. Ziehen Sie es, und klicken Sie dann auf Verwenden.



Bedingung für Authentifizierungsrichtlinie Studio

Wählen Sie im Abschnitt Zugelassene Protokolle die Option Standard-Netzwerkzugriff aus.

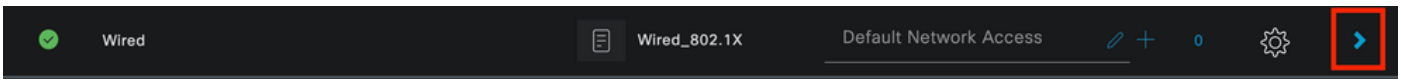


Policy Sets - Allgemeine Ansicht

Klicken Sie auf Speichern.

2. Buchstabe d Konfigurieren der Authentifizierungs- und Autorisierungsrichtlinien

Klicken Sie auf das Symbol >.



Kabelgebundener Richtliniensatz

Erweitern Sie den Abschnitt Authentifizierungsrichtlinie.

Klicken Sie auf das Symbol +.

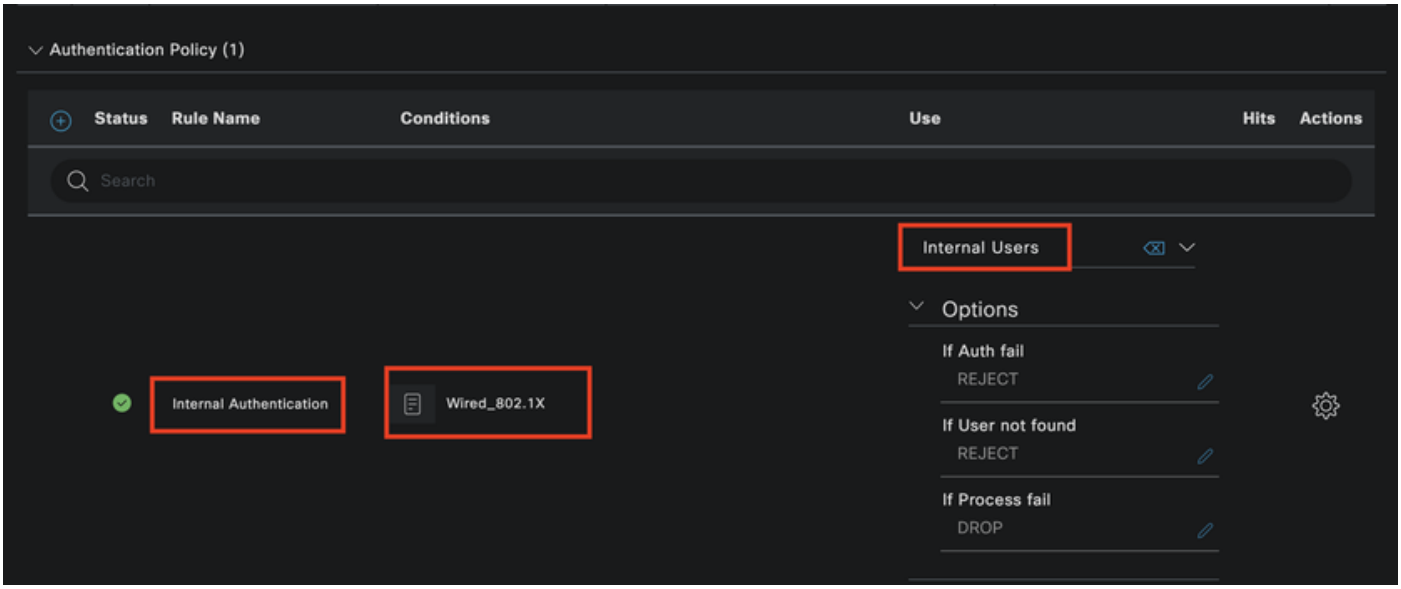
Authentifizierungsrichtlinie

Weisen Sie der Authentifizierungsrichtlinie einen Namen zu. In diesem Beispiel wird die interne Authentifizierung verwendet.

Klicken Sie in der Spalte "Bedingungen" für diese neue Authentifizierungsrichtlinie auf das Symbol +.

Die vorkonfigurierte Bedingung Wired Dot1x wird verwendet.

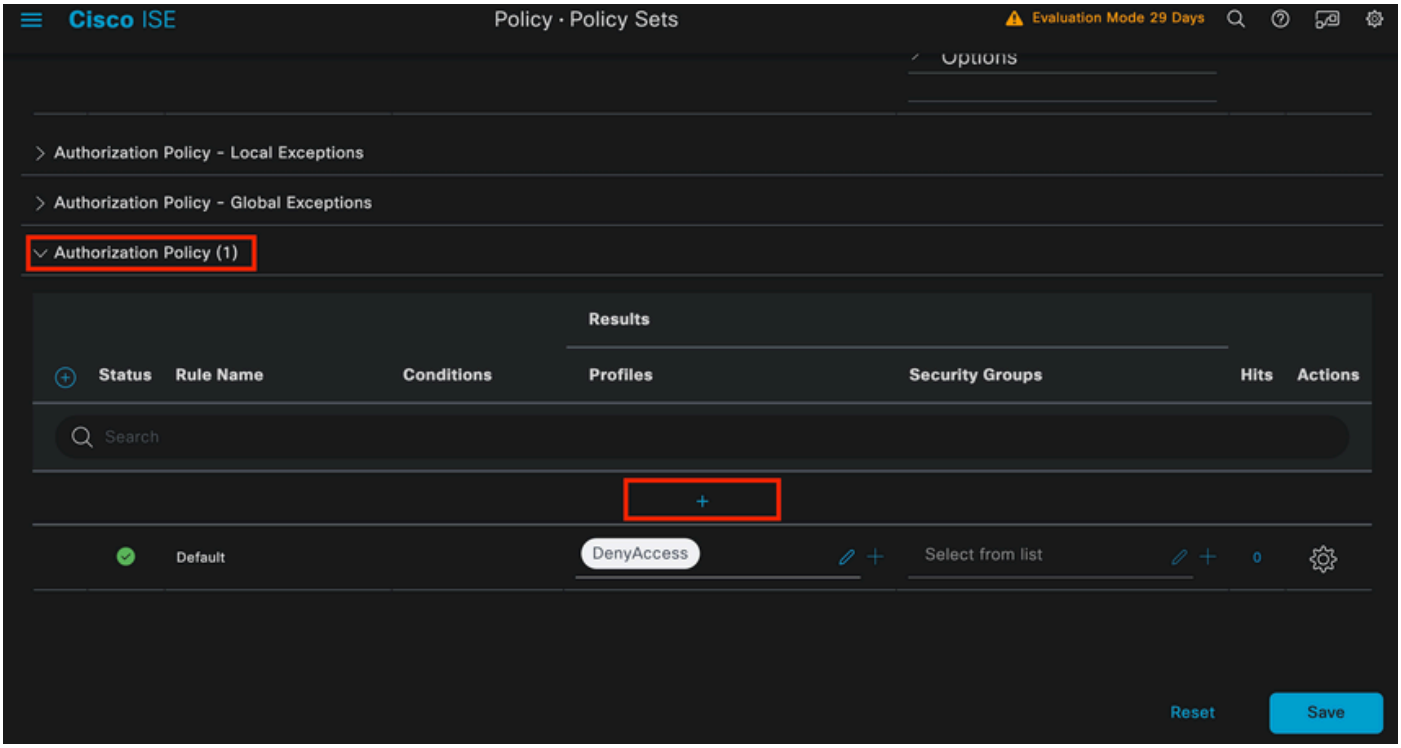
Wählen Sie abschließend in der Spalte Verwenden die Option Interne Benutzer aus.



Authentifizierungsrichtlinie

Autorisierungsrichtlinie.

Der Abschnitt Autorisierungsrichtlinie befindet sich unten auf der Seite. Erweitern Sie das Fenster, und klicken Sie auf das Symbol +.



Autorisierungsrichtlinie

Nennen Sie die kürzlich erstellte Autorisierungsrichtlinie. In diesem Konfigurationsbeispiel wird der Name Internal ISE Users verwendet.

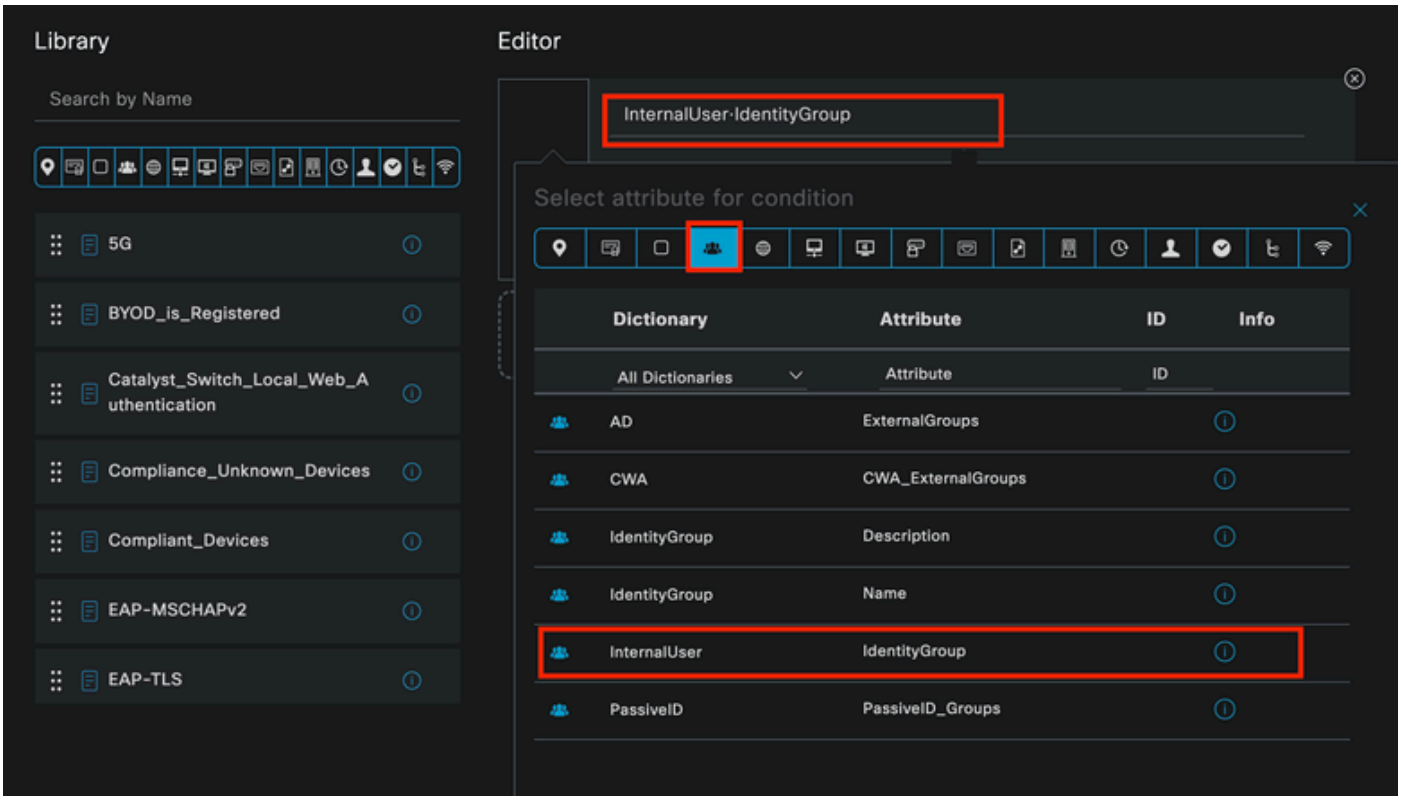
Um eine Bedingung für diese Autorisierungsrichtlinie zu erstellen, klicken Sie auf das +-Symbol in der Spalte Bedingungen.

Die Gruppe IseUsers wird verwendet.

Klicken Sie auf den Abschnitt Attribute.

Wählen Sie das Symbol IdentityGroup aus.

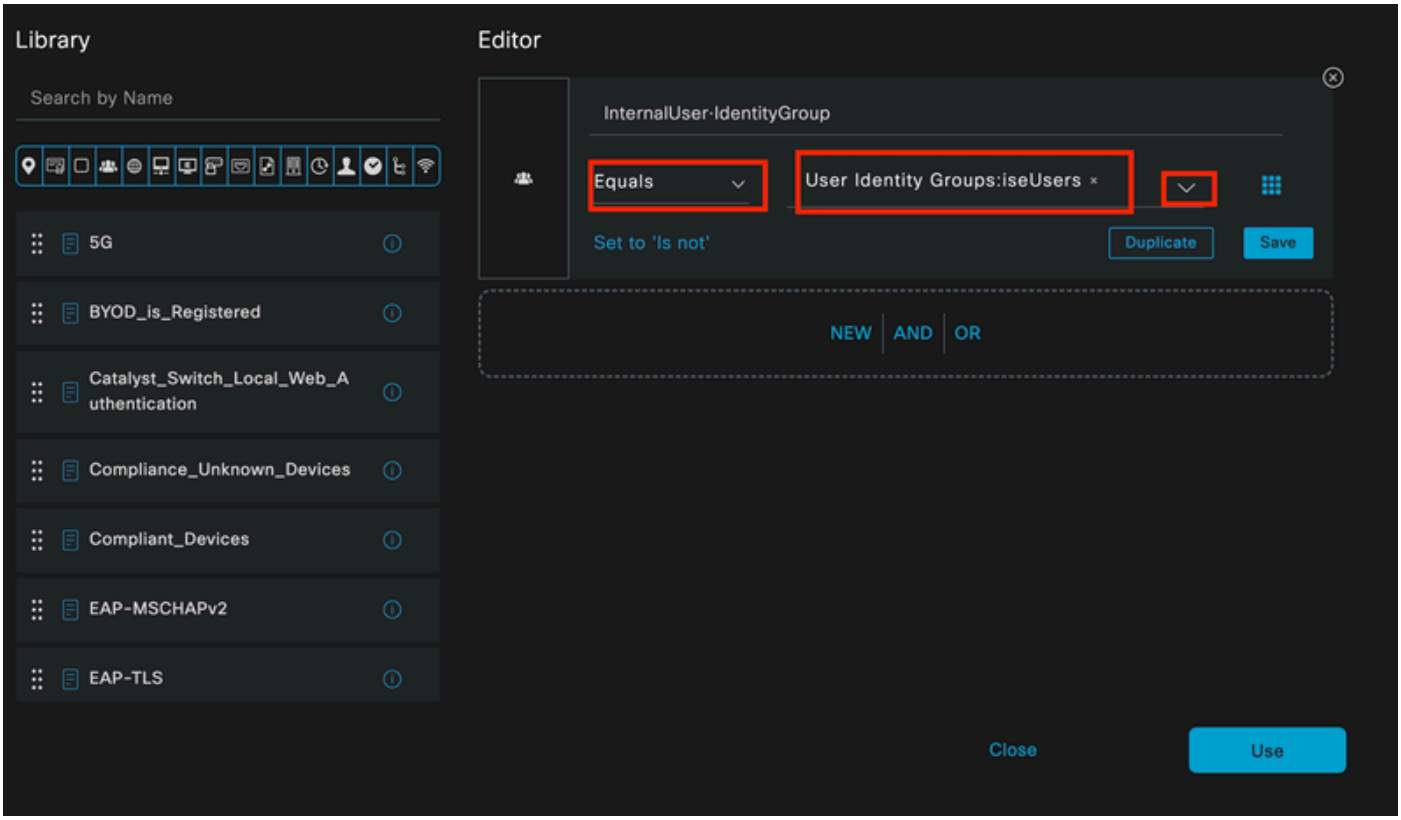
Wählen Sie aus dem Wörterbuch das InternalUser-Wörterbuch aus, das mit dem IdentityGroup-Attribut geliefert wird.



Bedingungserstellung

Wählen Sie den Operator Gleich.

Wählen Sie unter Benutzeridentitätsgruppen die Gruppe IseUsers aus.

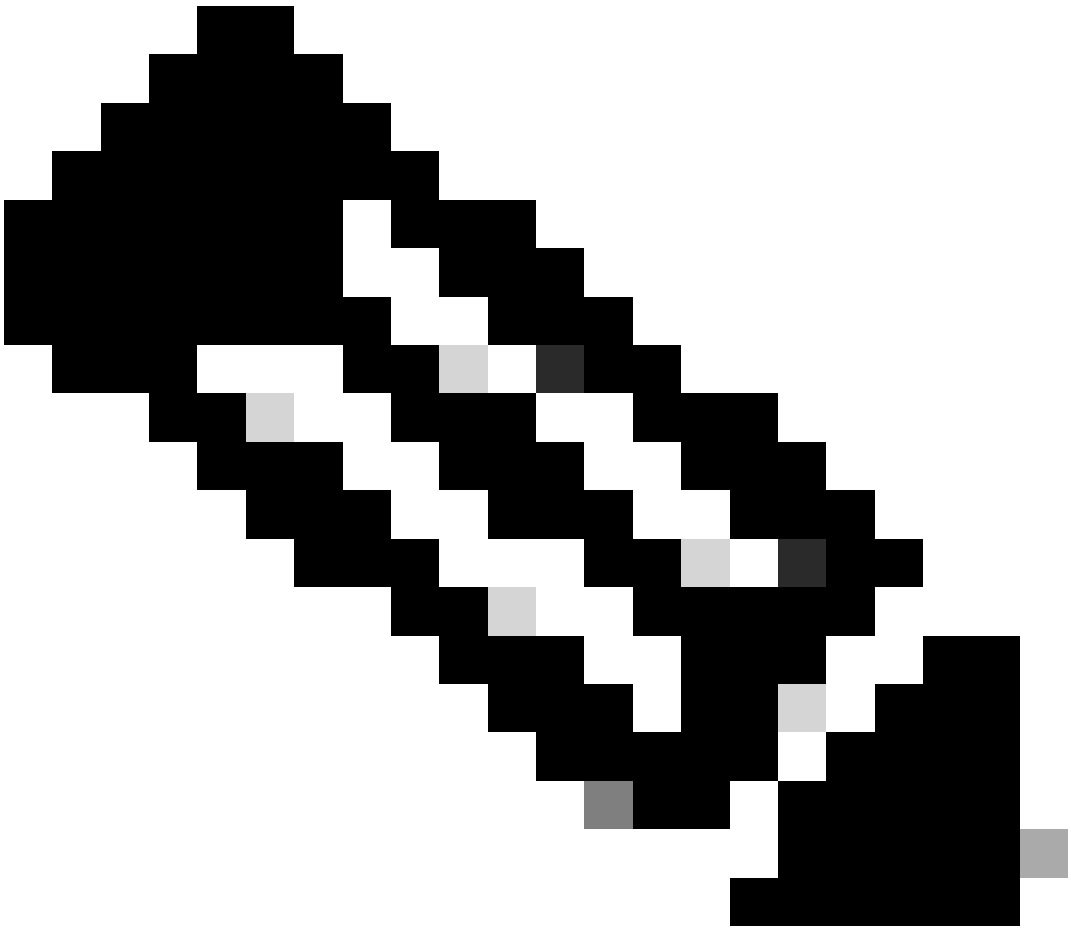


Bedingungserstellung

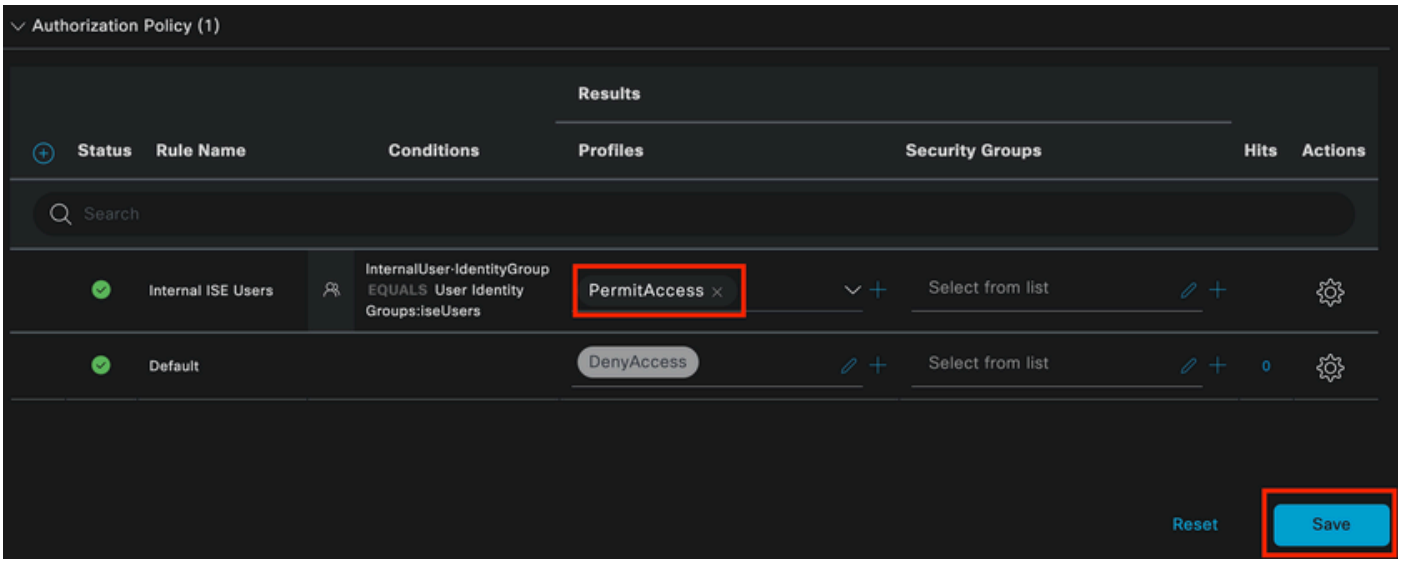
Klicken Sie auf Verwenden.

Fügen Sie das Autorisierungsprofil für Ergebnisse hinzu.

Das vorkonfigurierte Profil Zugriffsberechtigung wird verwendet.



Hinweis: Beachten Sie, dass die Authentifizierungen, die an die ISE gesendet werden und diesen Wired Dot1x-Richtliniensatz treffen, der nicht Teil der Benutzeridentitätsgruppe ISEUsers ist, die Standard-Autorisierungsrichtlinie treffen, die das Ergebnis DenyAccess hat.



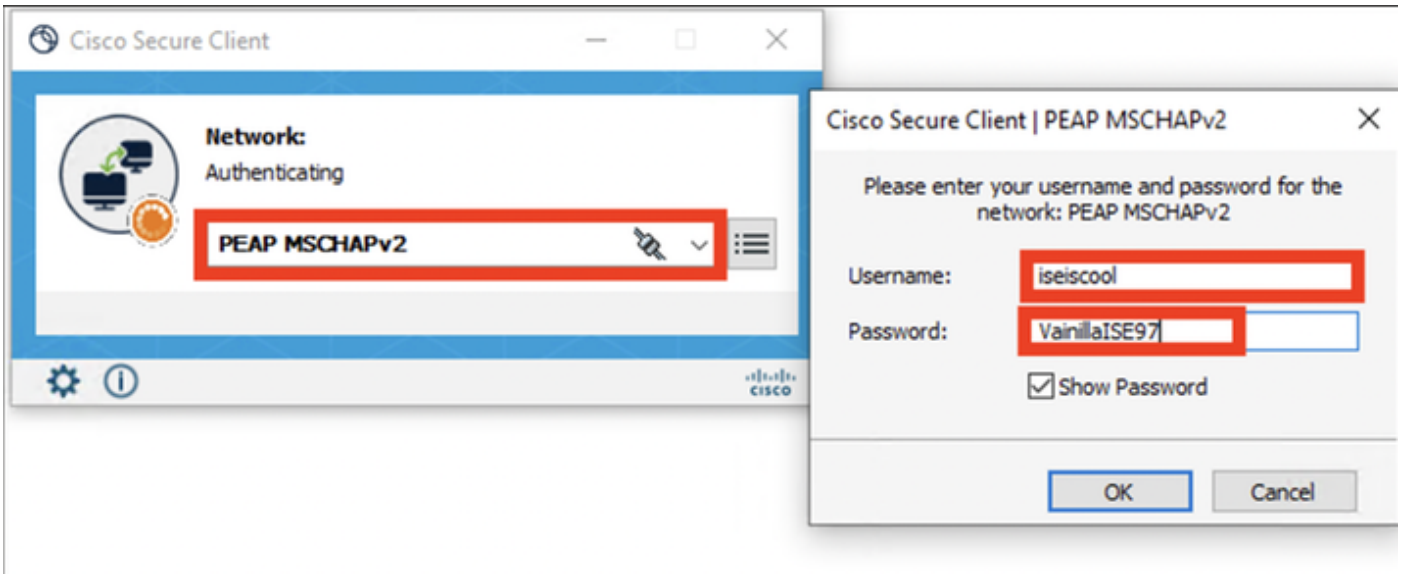
Autorisierungsrichtlinie

Klicken Sie auf Speichern.

Überprüfung

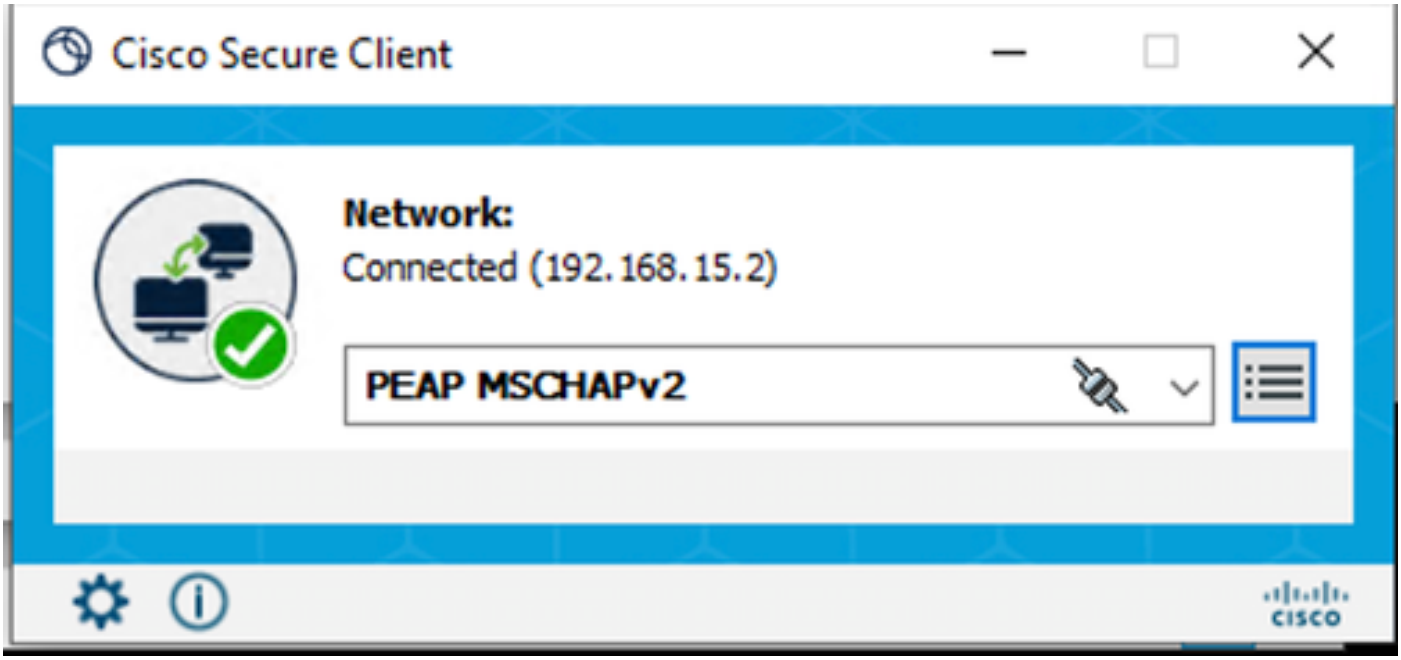
Nach Abschluss der Konfiguration fragt Secure Client die Anmeldeinformationen ab und legt die Verwendung des PEAP MSCHAPv2-Profils fest.

Die zuvor erstellten Anmeldeinformationen werden eingegeben.



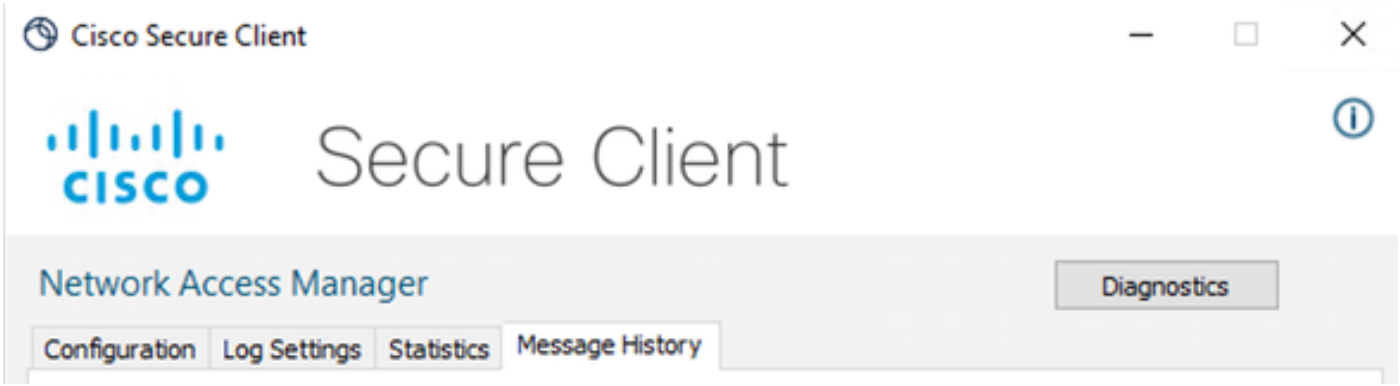
NAM des sicheren Clients

Wenn sich das Endgerät korrekt authentifiziert, NAM zeigt an, dass eine Verbindung besteht.

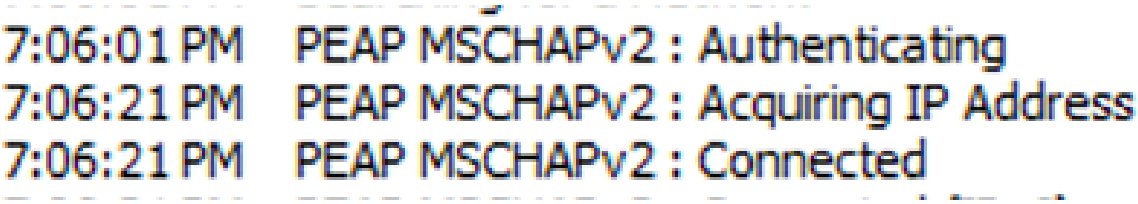


NAM des sicheren Clients

Wenn Sie auf das Informationssymbol klicken und zum Abschnitt Nachrichtenverlauf navigieren, werden die Details zu jedem Schritt angezeigt, den NAM durchgeführt hat.



Nachrichten des sicheren Clients



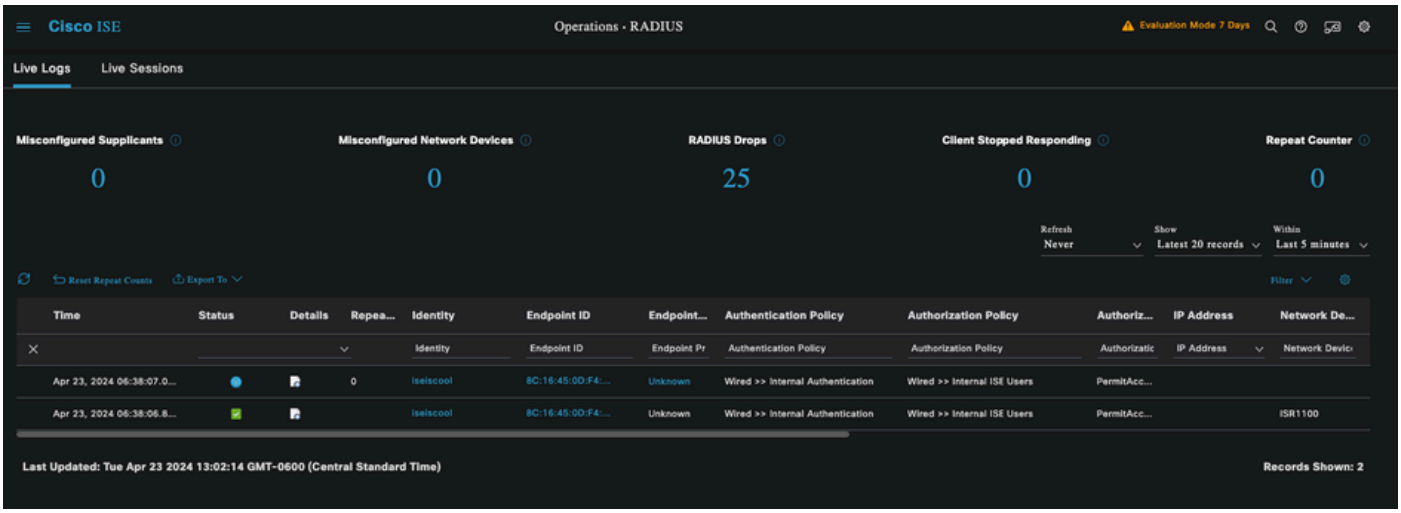
Nachrichten des sicheren Clients

Navigieren Sie von der ISE zu Operations > Radius LiveLogs, um die Details der Authentifizierung anzuzeigen. Wie im nächsten Bild zu sehen ist, wird der benutzte Benutzername angezeigt.

Weitere Details wie:

- Zeitstempel.
- MAC-Adresse.
- Verwendeter Policy Set.
- Authentifizierungsrichtlinie.

- Autorisierungsrichtlinie.
- Sonstige sachdienliche Informationen.



ISE RADIUS-Live-Protokolle

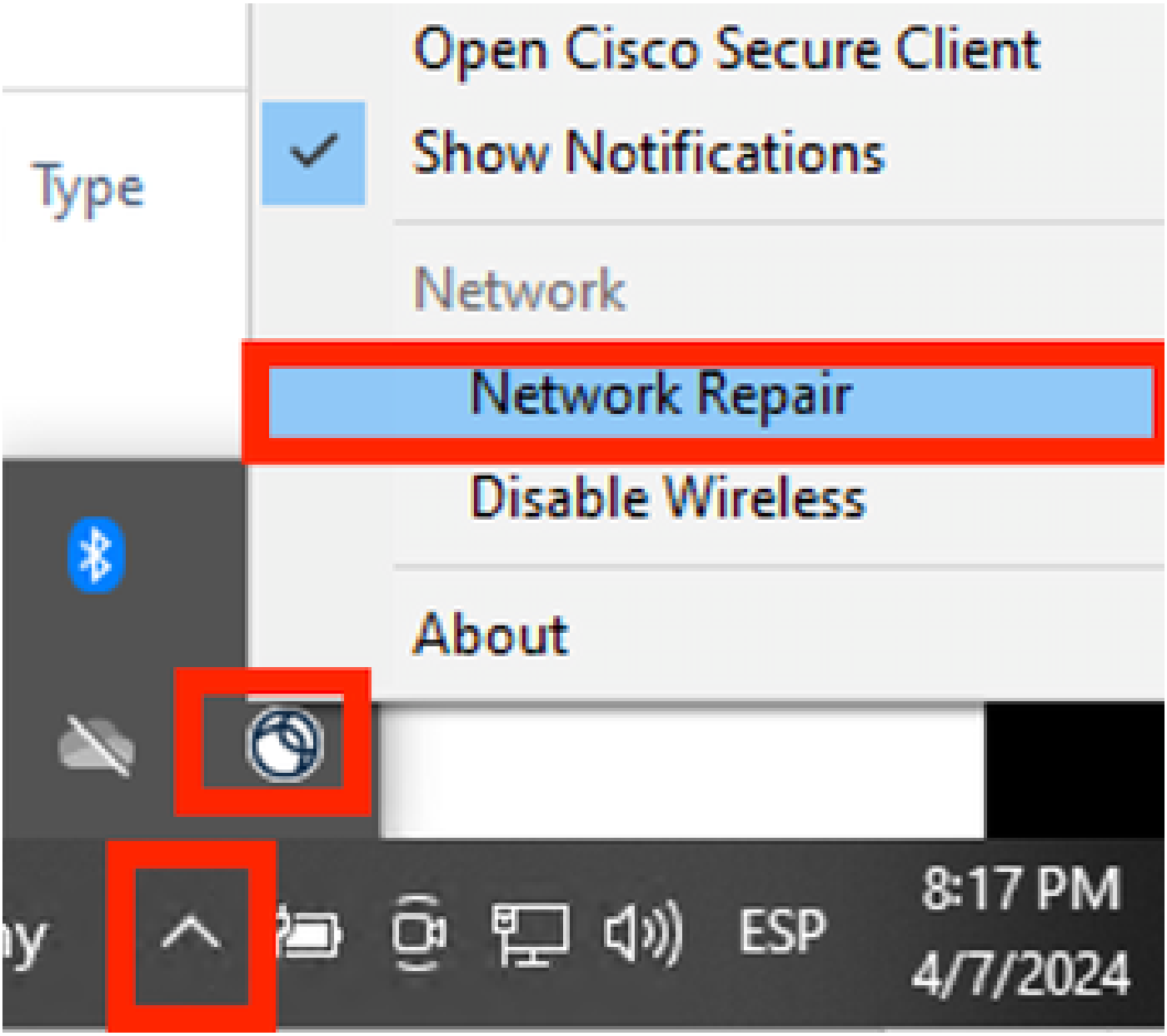
Da Sie sehen, dass die richtigen Richtlinien angewendet werden und das Ergebnis ein erfolgreicher Authentifizierungsstatus ist, wird der Schluss gezogen, dass die Konfiguration korrekt ist.

Fehlerbehebung

Problem: Das NAM-Profil wird von Secure Client nicht verwendet.

Wenn das neue Profil, das im Profil-Editor erstellt wurde, nicht von NAM verwendet wird, verwenden Sie die Option Network Repair für Secure Client.

Sie finden diese Option, indem Sie zur Windows-Leiste navigieren > auf das Zirkumflex-Symbol klicken > mit der rechten Maustaste auf das Symbol für sicheren Client klicken > auf Netzwerkreparatur klicken.



Bereich Netzwerkreparatur

Problem 2: Protokolle müssen zur weiteren Analyse gesammelt werden.

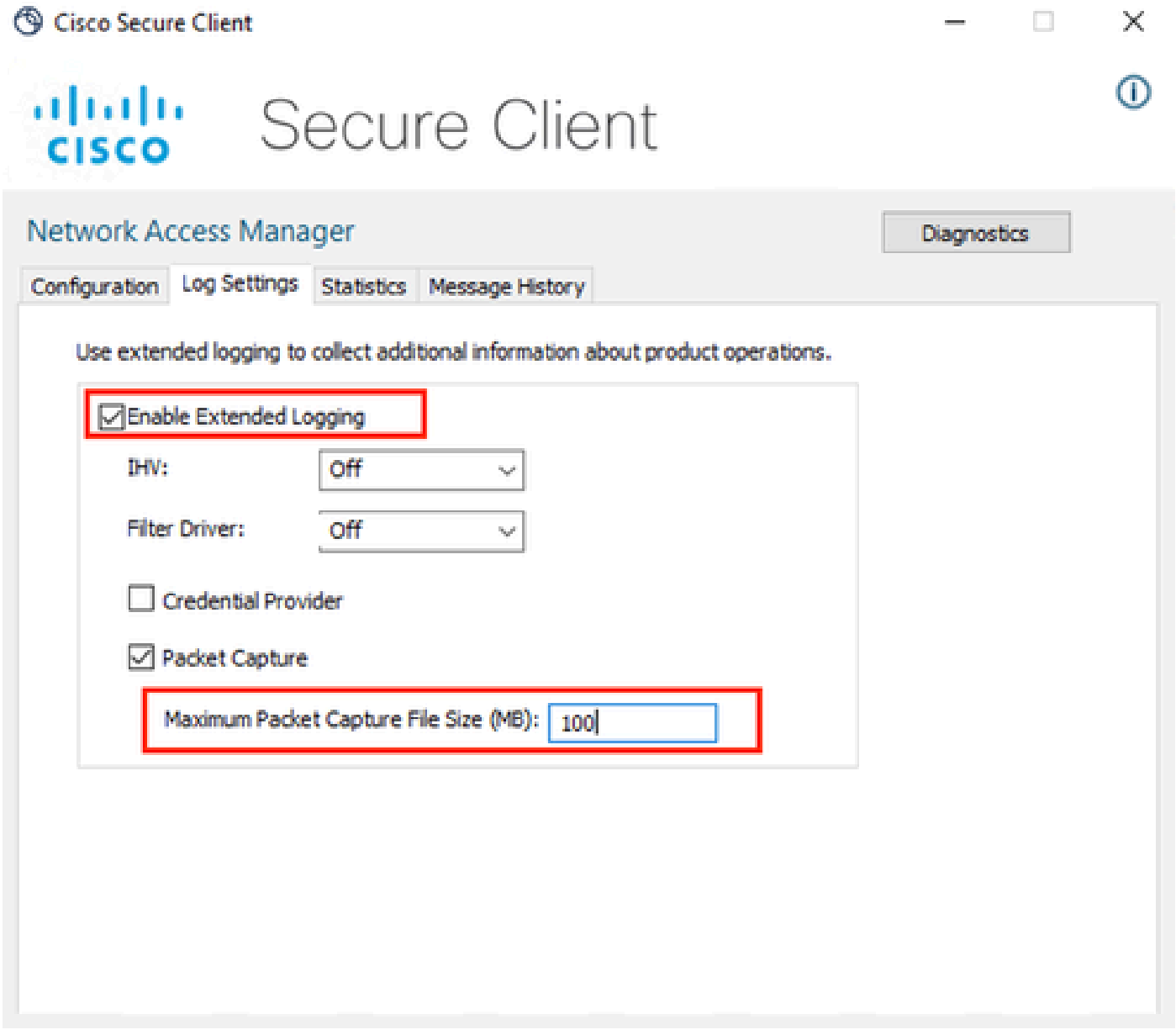
1. Erweiterte NAM-Protokollierung aktivieren

Öffnen Sie NAM, und klicken Sie auf das Zahnrad-Symbol.

NAM-Schnittstelle

Navigieren Sie zur Registerkarte Protokolleinstellungen. Aktivieren Sie das Kontrollkästchen "Erweiterte Protokollierung aktivieren".

Legen Sie die Größe der Paketerfassungsdatei auf 100 MB fest.



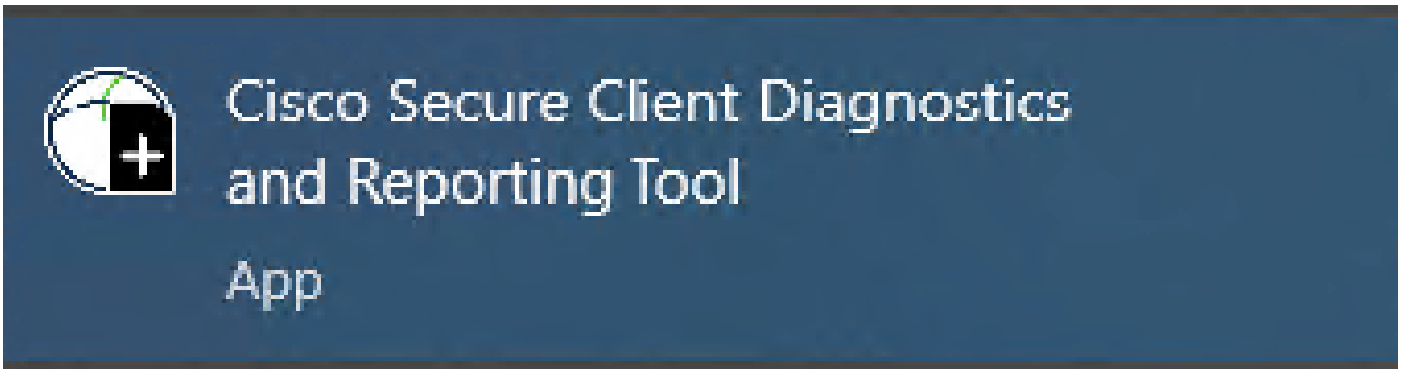
NAM-Protokolleinstellungen des sicheren Clients

2. Reproduzieren Sie das Problem.

Wenn die erweiterte Protokollierung aktiviert ist, reproduzieren Sie das Problem mehrmals, um sicherzustellen, dass die Protokolle erstellt und der Datenverkehr erfasst wird.

3. Erfassen Sie das Secure Client DART-Paket.

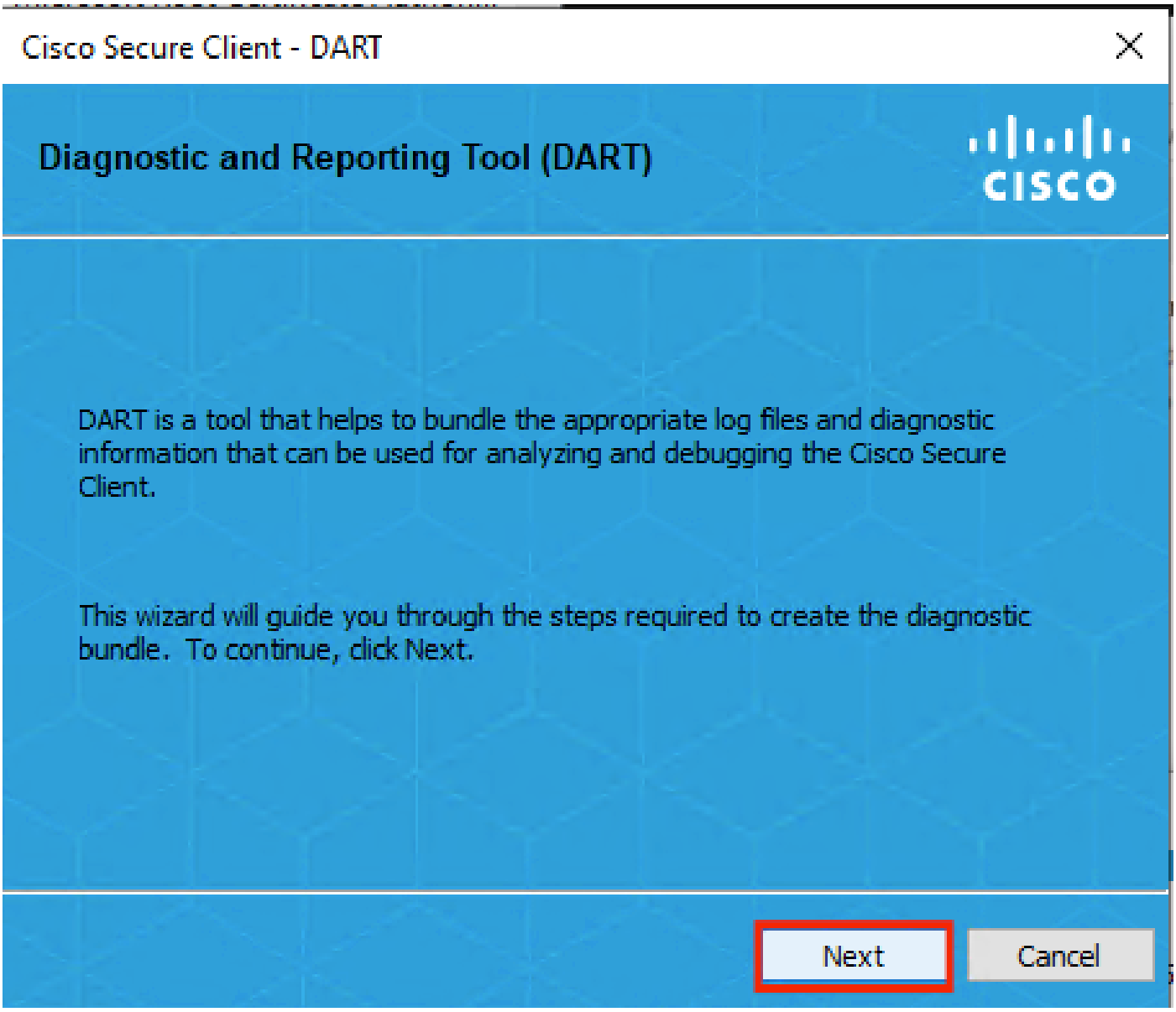
Navigieren Sie in Windows zur Suchleiste, und geben Sie Cisco Secure Client Diagnostics and Reporting Tool ein.



DART-Modul

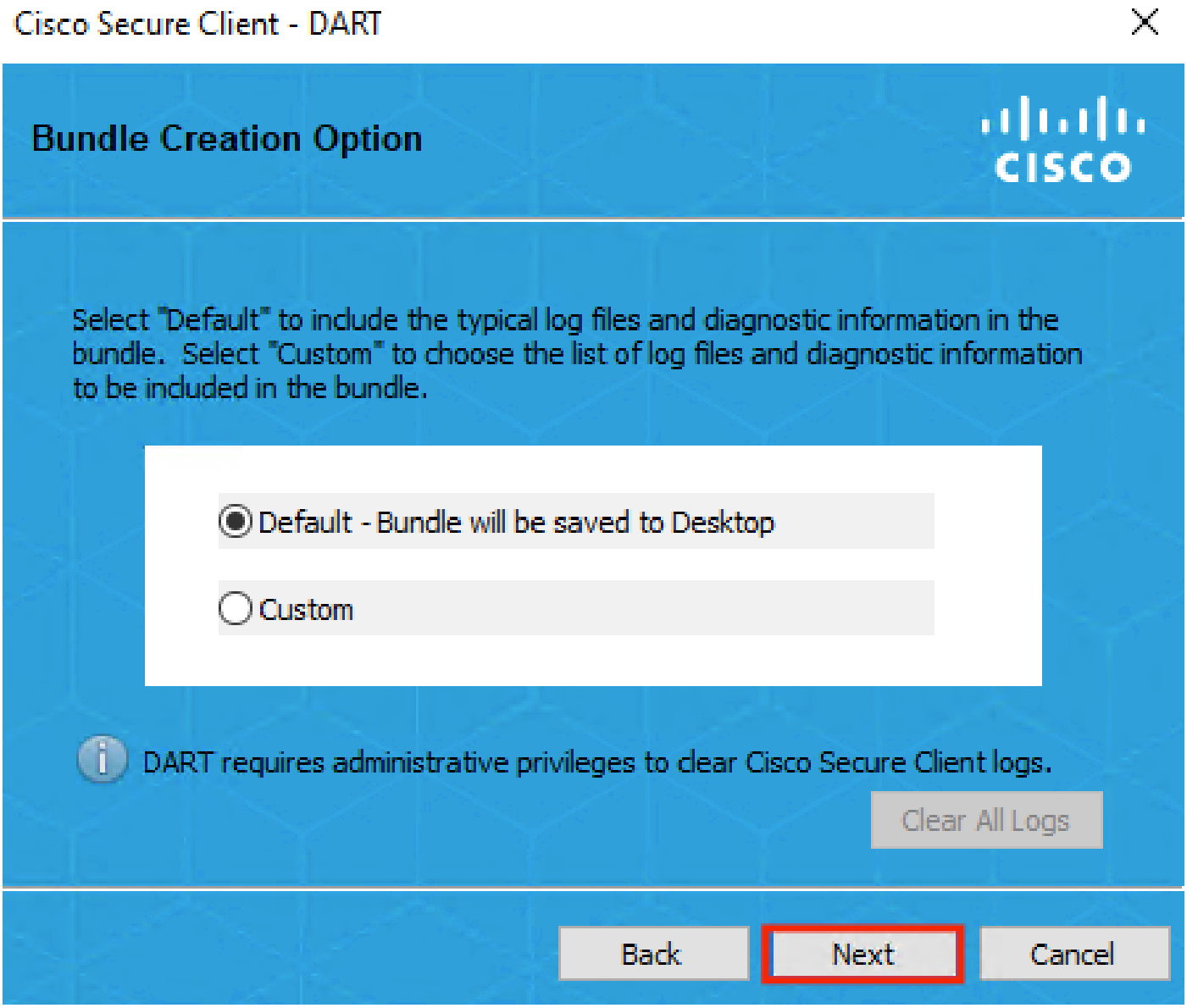
Während des Installationsvorgangs haben Sie auch dieses Modul installiert. Dieses Tool hilft bei der Fehlerbehebung, indem es Protokolle und relevante dot1x-Sitzungsinformationen sammelt.

Klicken Sie im ersten Fenster auf Weiter.



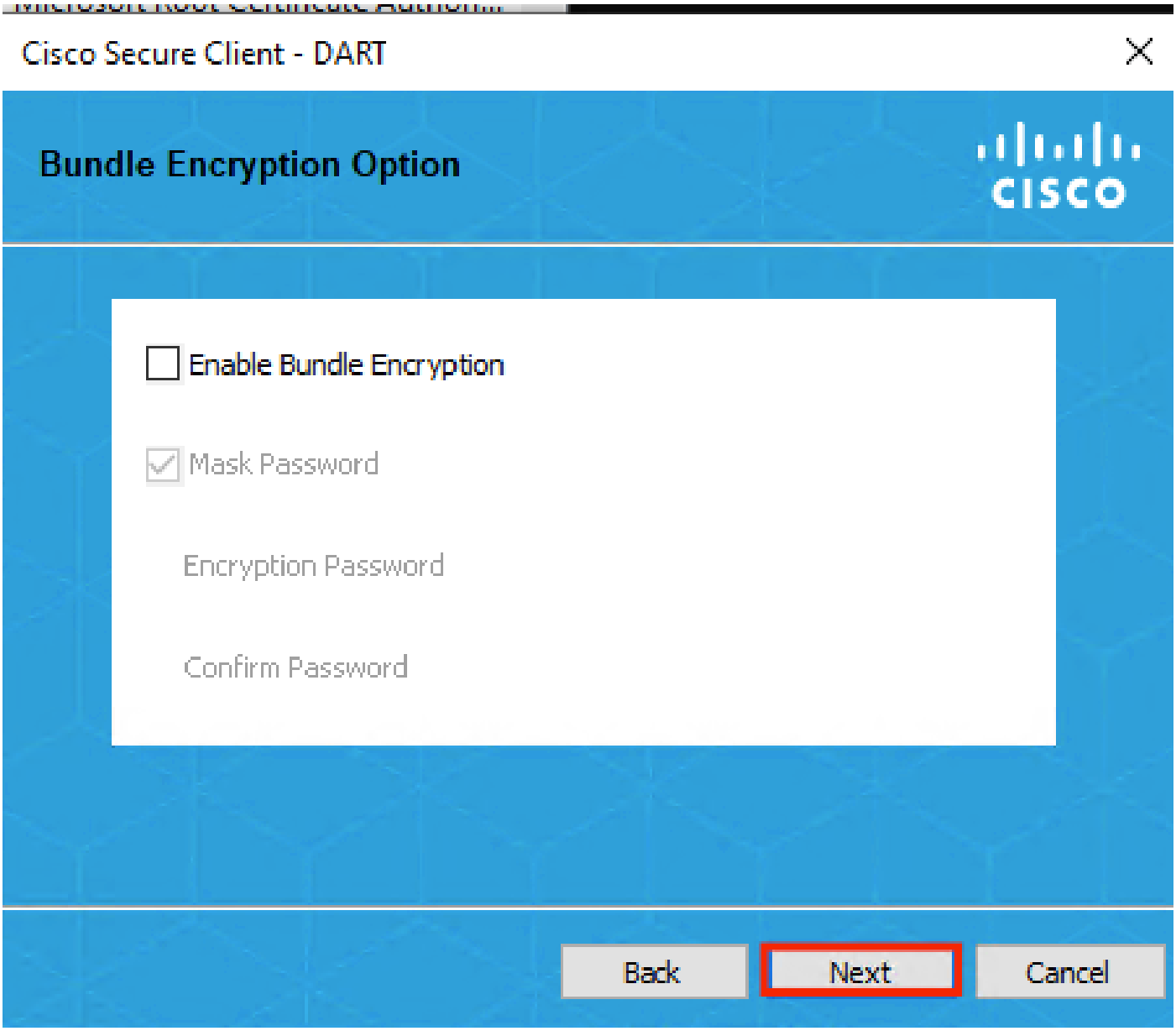
DART-Modul

Klicken Sie erneut auf Weiter, um das Protokollpaket auf dem Desktop zu speichern.



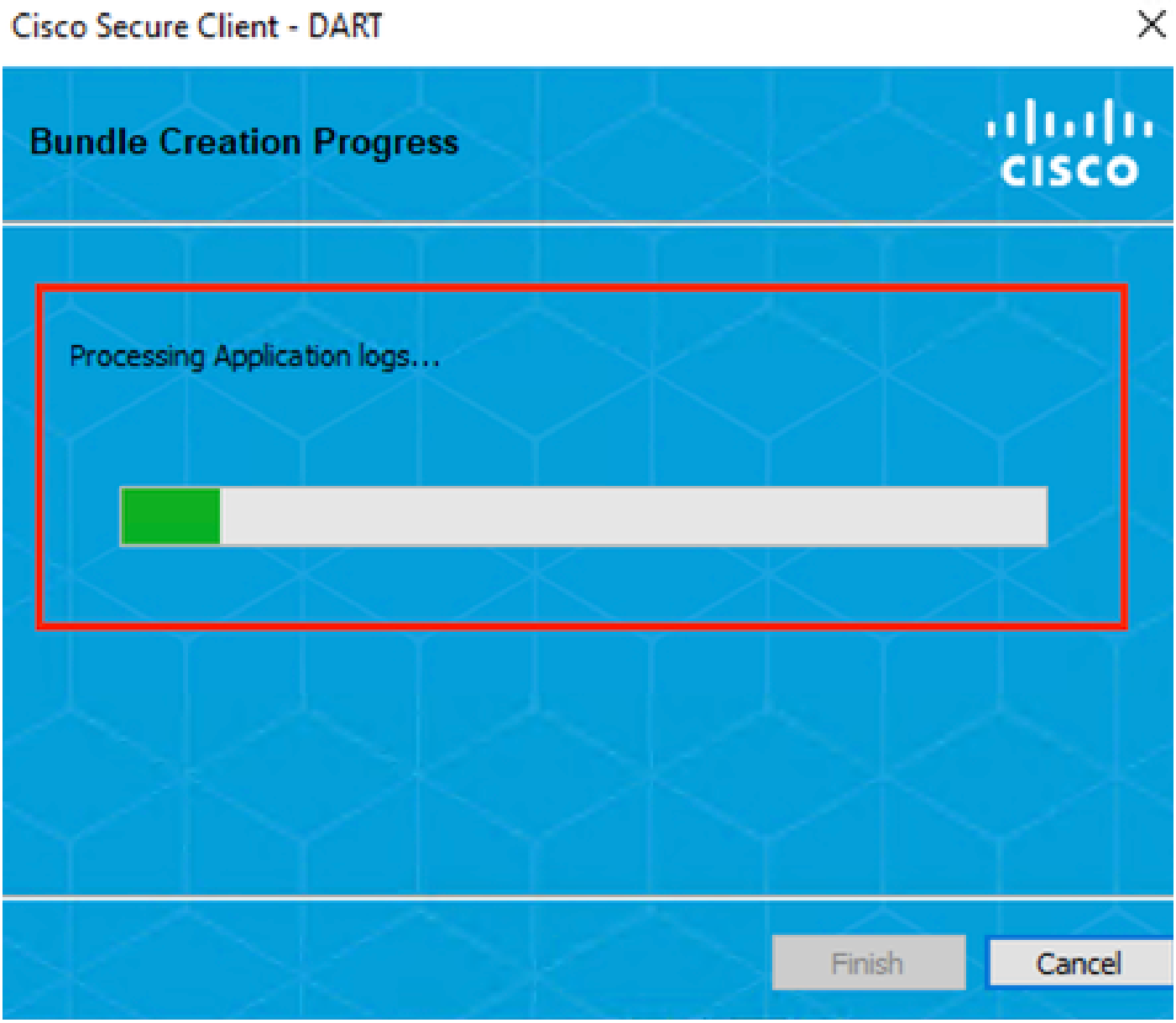
DART-Modul

Aktivieren Sie ggf. das Kontrollkästchen Paketverschlüsselung aktivieren.



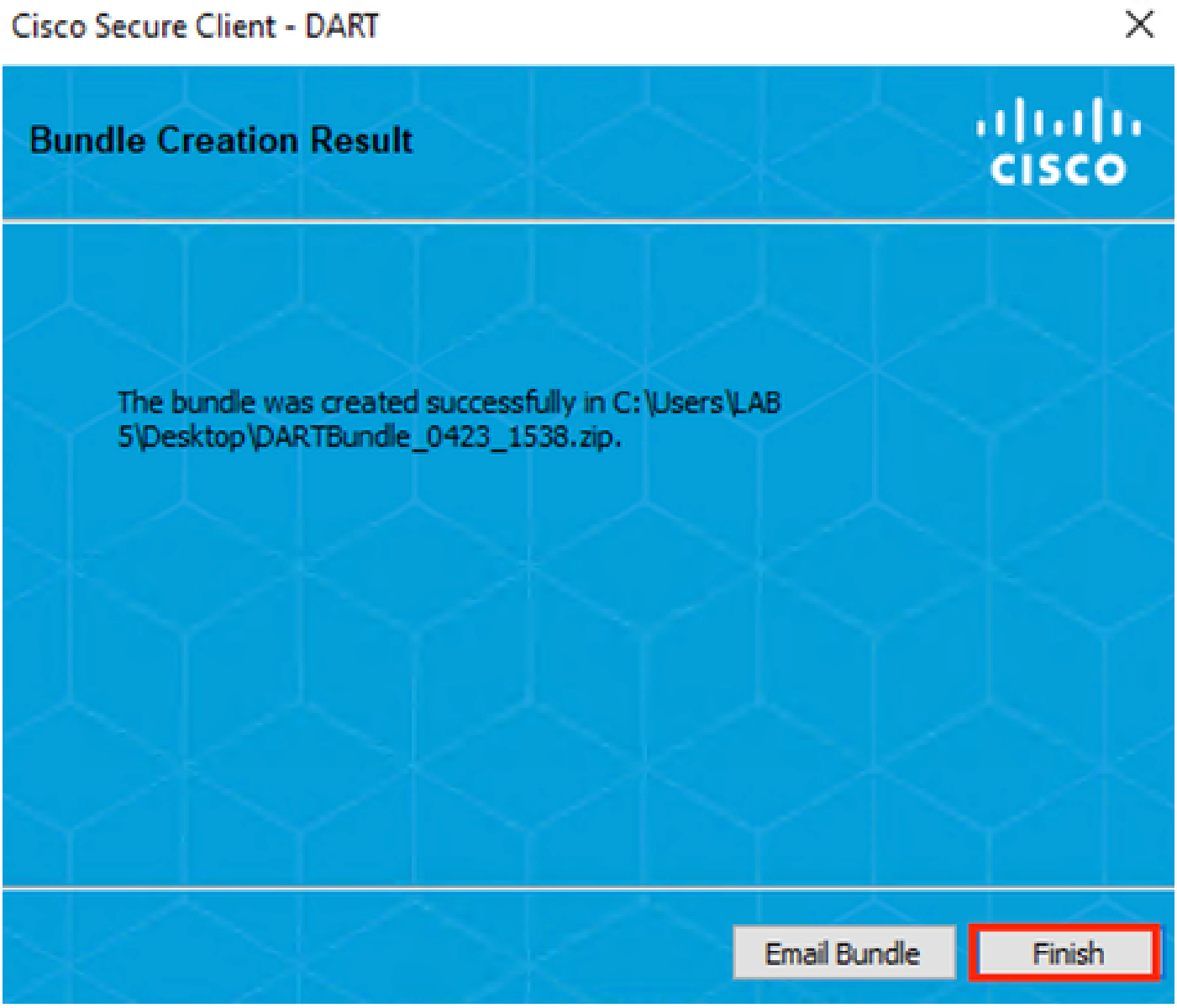
DART-Modul

DART-Protokollsammlung wird gestartet.



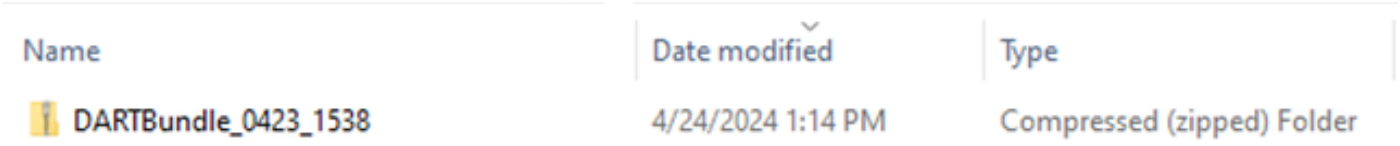
DART-Protokollsammlung

Es kann 10 Minuten oder länger dauern, bis der Prozess abgeschlossen ist.



Ergebnis der DART-Paketerstellung

Die DART-Ergebnisdatei befindet sich im Desktop-Verzeichnis.



DART-Ergebnisdatei

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.