Fehlerbehebung bei Problemen mit kabelgebundenen Punkten in ISE 3.2 und Windows

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie eine grundlegende 802.1X-PEAP-Authentifizierung für die Identity Services Engine (ISE) 3.2 und die native Windows-Komponente konfiguriert wird.

Voraussetzungen

Anforderungen

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

- Protected Extensible Authentication Protocol (PEAP)
- PEAP 802.1x

Verwendete Komponenten

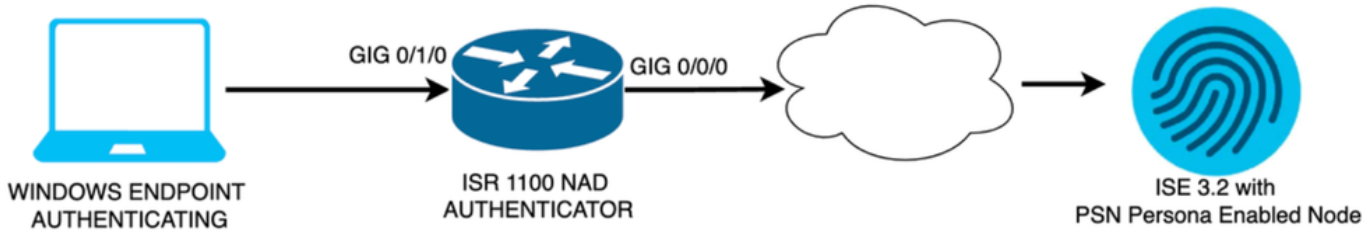
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Version der Cisco Identity Services Engine (ISE)
- Cisco C117 Cisco IOS® XE Software, Version 17.12.02
- Laptop mit Windows 10

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.

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm

Konfigurationen

Führen Sie die folgenden Schritte aus, um Folgendes zu konfigurieren:

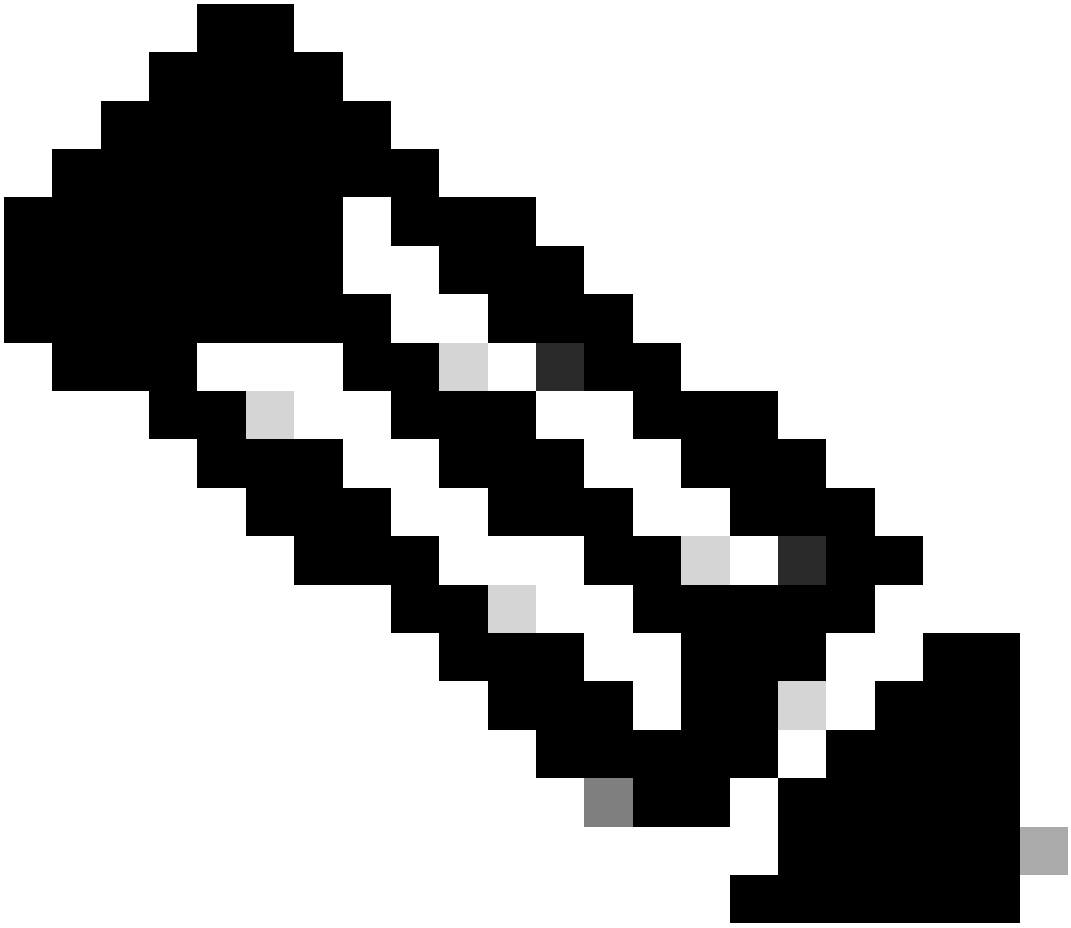
Schritt 1: Konfigurieren Sie den ISR 1100-Router.

Schritt 2: Identity Service Engine 3.2 konfigurieren

Schritt 3: Konfigurieren von Windows Native Supplicant

Schritt 1: Konfigurieren des ISR 1100 Routers

In diesem Abschnitt wird die grundlegende Konfiguration erläutert, die mindestens das NAD aufweisen muss, damit dot1x funktioniert.



Hinweis: Konfigurieren Sie bei ISE-Bereitstellungen mit mehreren Knoten die IP-Adresse des Knotens, auf dem die PSN-Rolle aktiviert ist. Diese Funktion kann aktiviert werden, wenn 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>
```

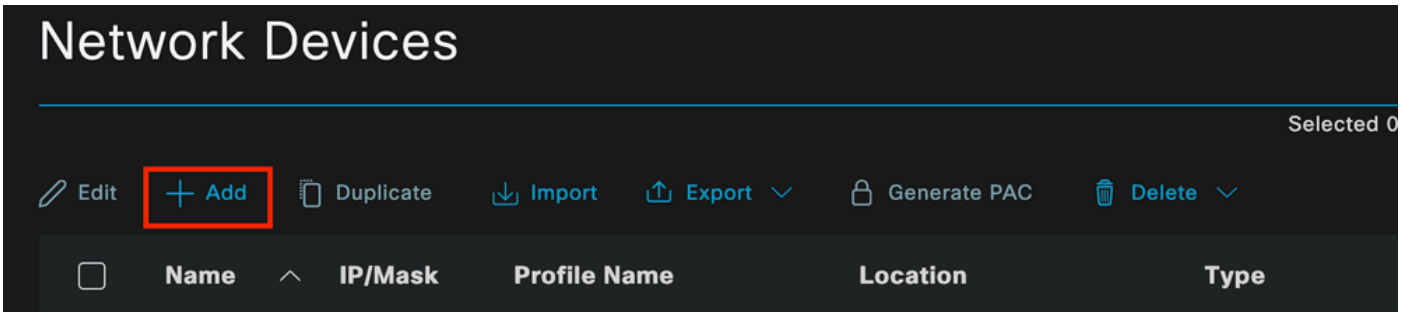
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication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

Schritt 2: Identity Service Engine 3.2 konfigurieren

2. a. Konfigurieren Sie das Netzwerkgerät, das für die Authentifizierung verwendet werden soll, und fügen Sie es hinzu.

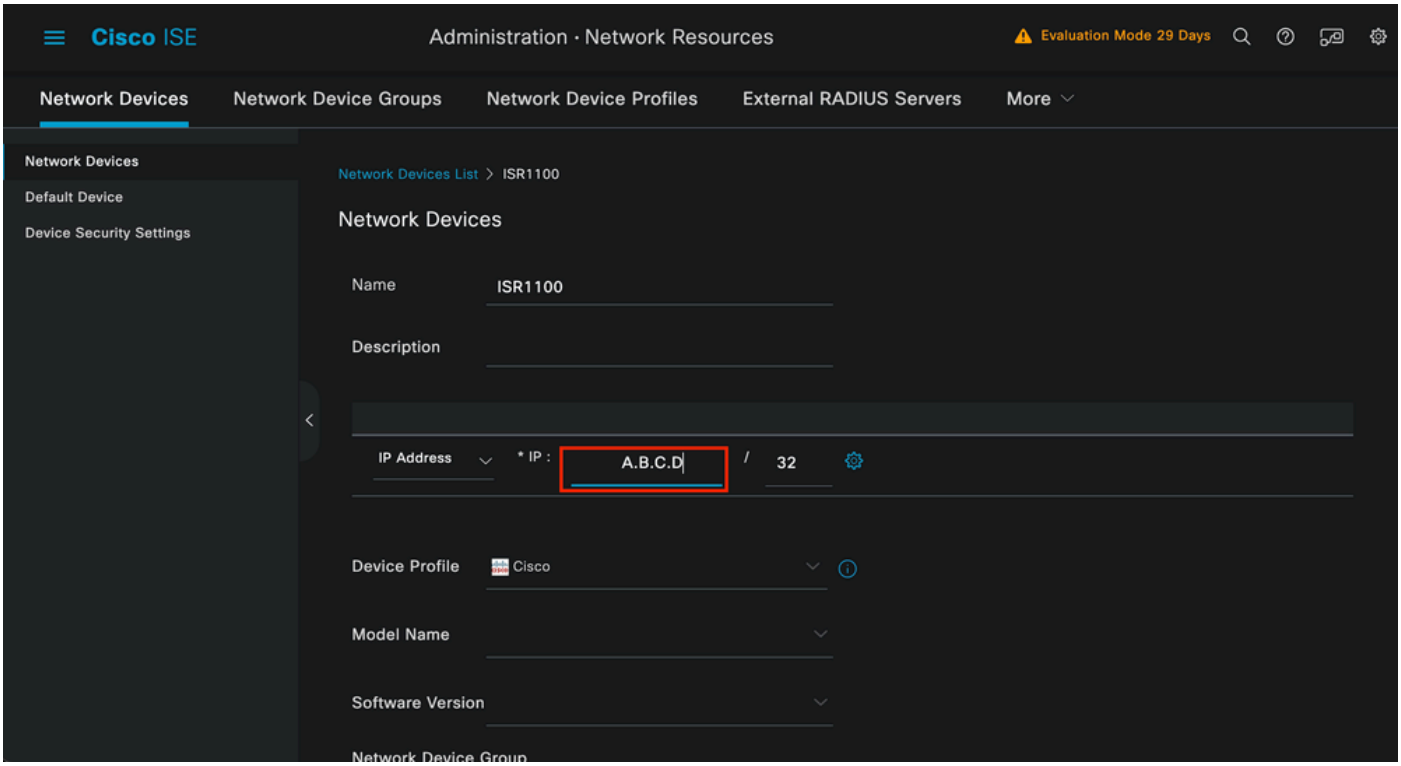
Fügen Sie den Abschnitt Netzwerkgerät zu ISE-Netzwerkgeräten hinzu.

Klicken Sie auf die Schaltfläche Hinzufügen, um zu starten.



ISE-Netzwerkgeräte

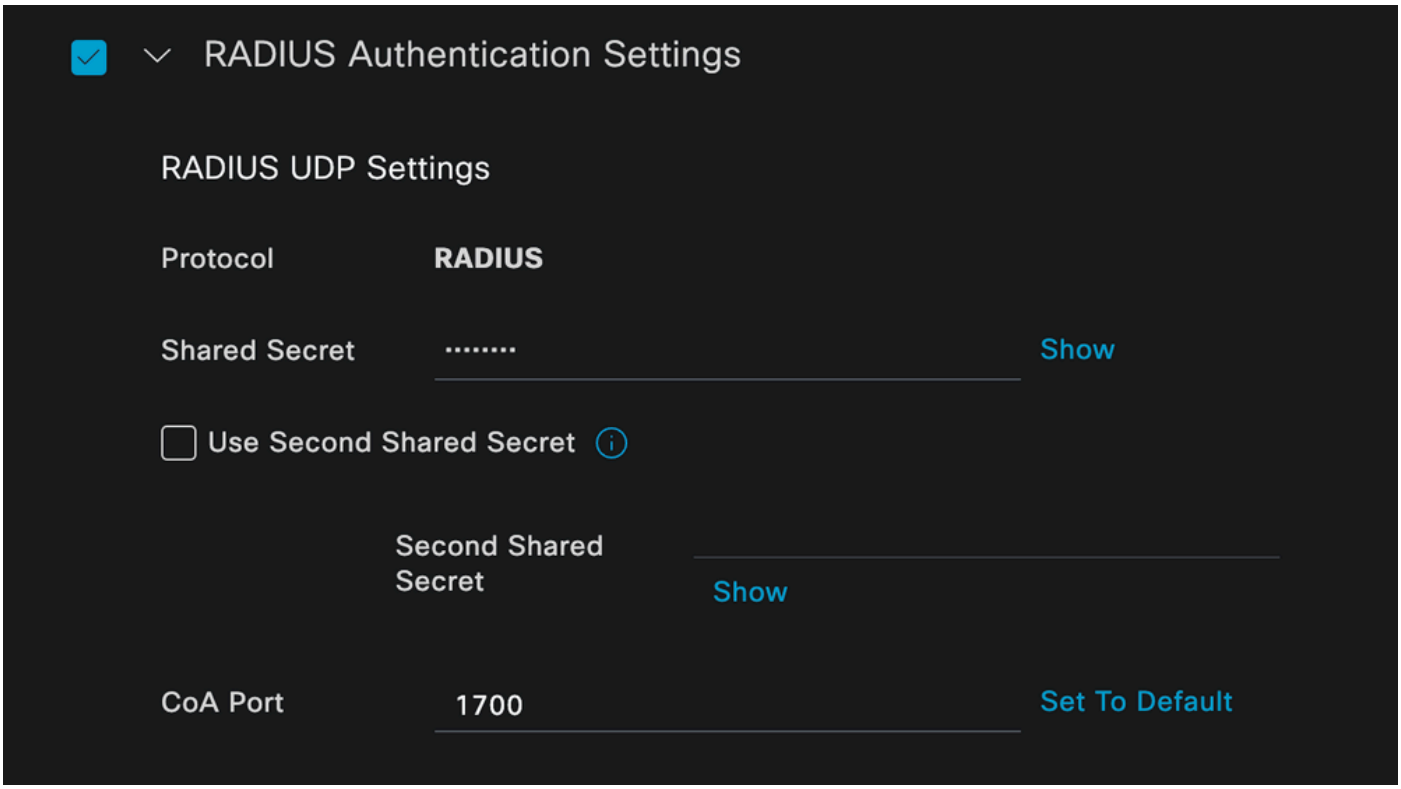
Geben Sie die Werte ein, weisen Sie dem von Ihnen erstellten NAD einen Namen zu, und fügen Sie außerdem die IP-Adresse hinzu, die das Netzwerkgerät für die Verbindung mit der ISE verwendet.



Seite zur Erstellung von Netzwerkgeräten

Scrollen Sie auf derselben Seite nach unten, um die Radius-Authentifizierungseinstellungen zu finden. Wie im nächsten Bild zu sehen.

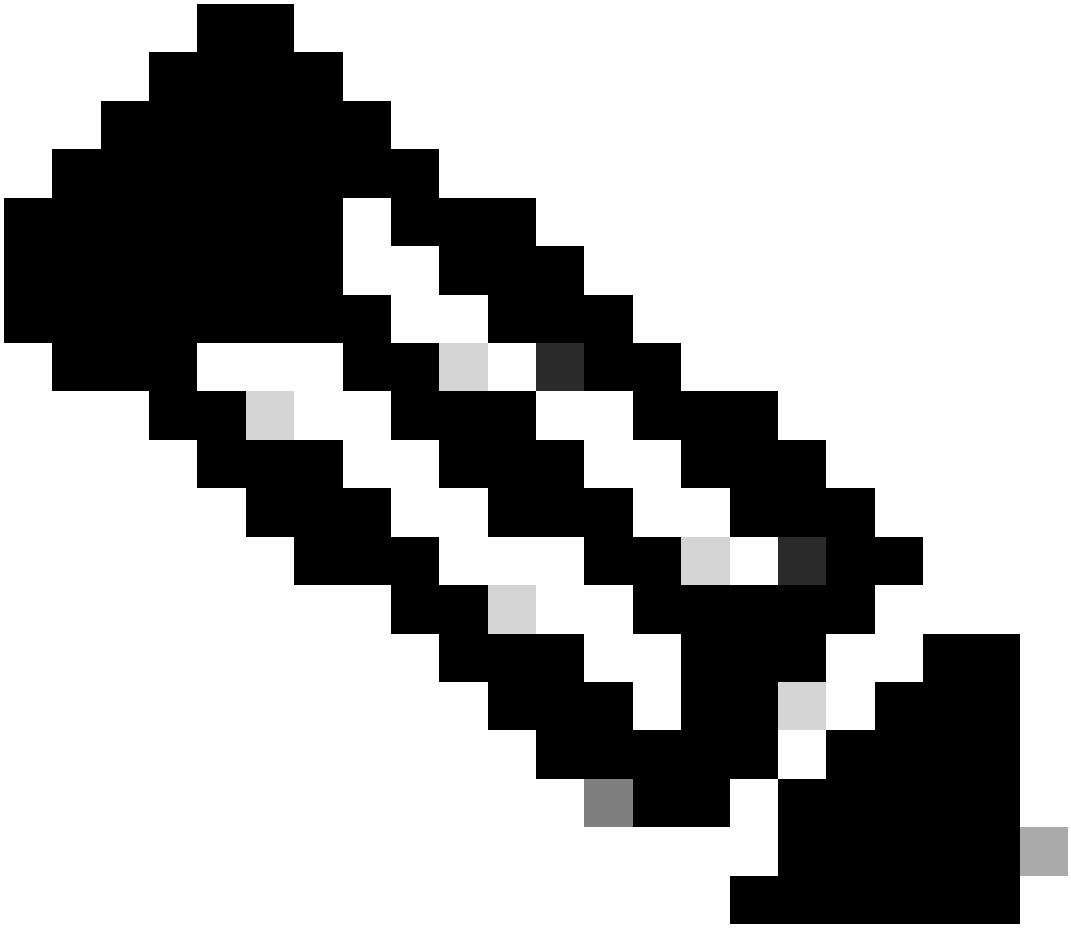
Fügen Sie den gemeinsamen geheimen Schlüssel hinzu, den Sie in Ihrer NAD-Konfiguration verwendet haben.



RADIUS-Konfiguration

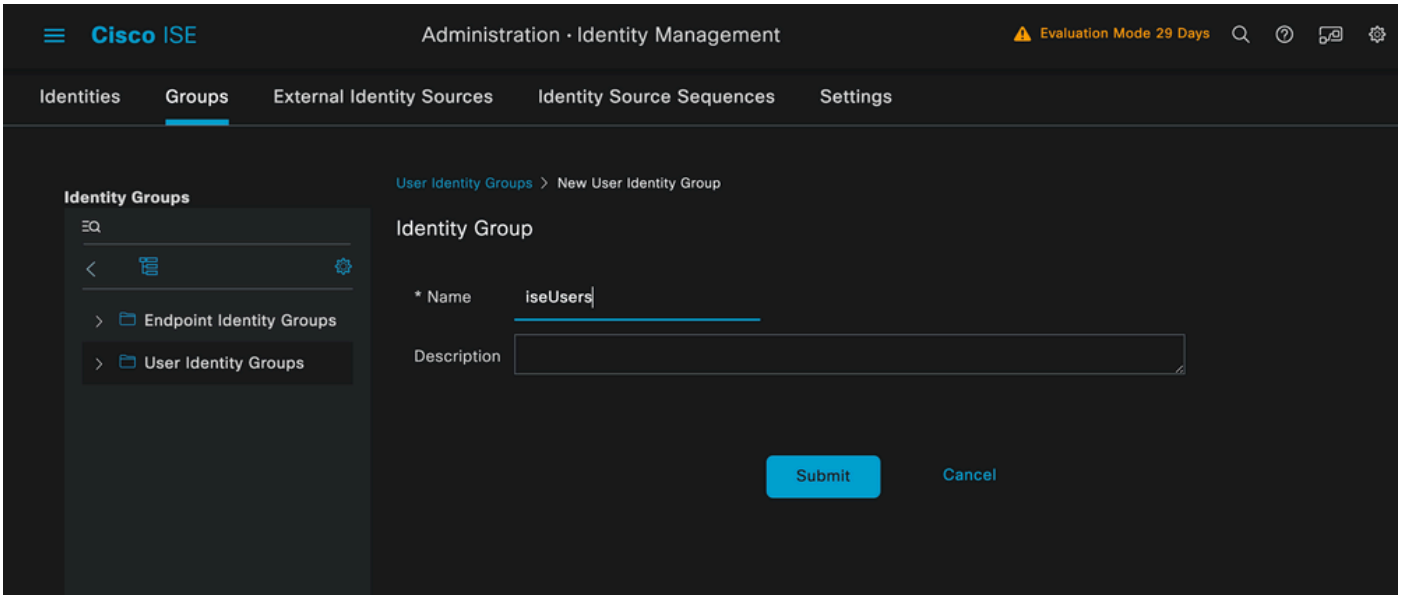
Speichern Sie die Änderungen.

2. b. Konfigurieren Sie die Identität, die zur Authentifizierung des Endpunkts verwendet wird.



> Hinweis: Um diesen Konfigurationsleitfaden beizubehalten, wird eine einfache lokale ISE-Authentifizierung verwendet.

Navigieren Sie zur Registerkarte Administration > Identity Management > Groups. Erstellen Sie die Gruppe und die Identität. Die für diese Demonstration erstellte Gruppe lautet iseUsers.

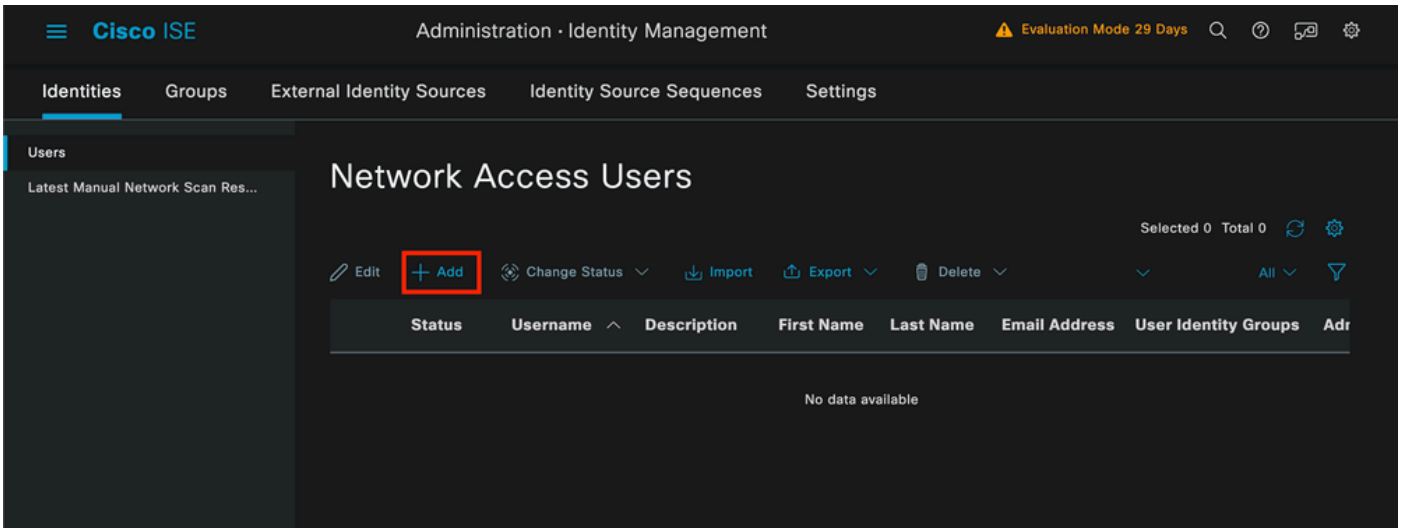


Identitätsgruppen-Erstellungsseite

Klicken Sie auf die Schaltfläche "Senden".

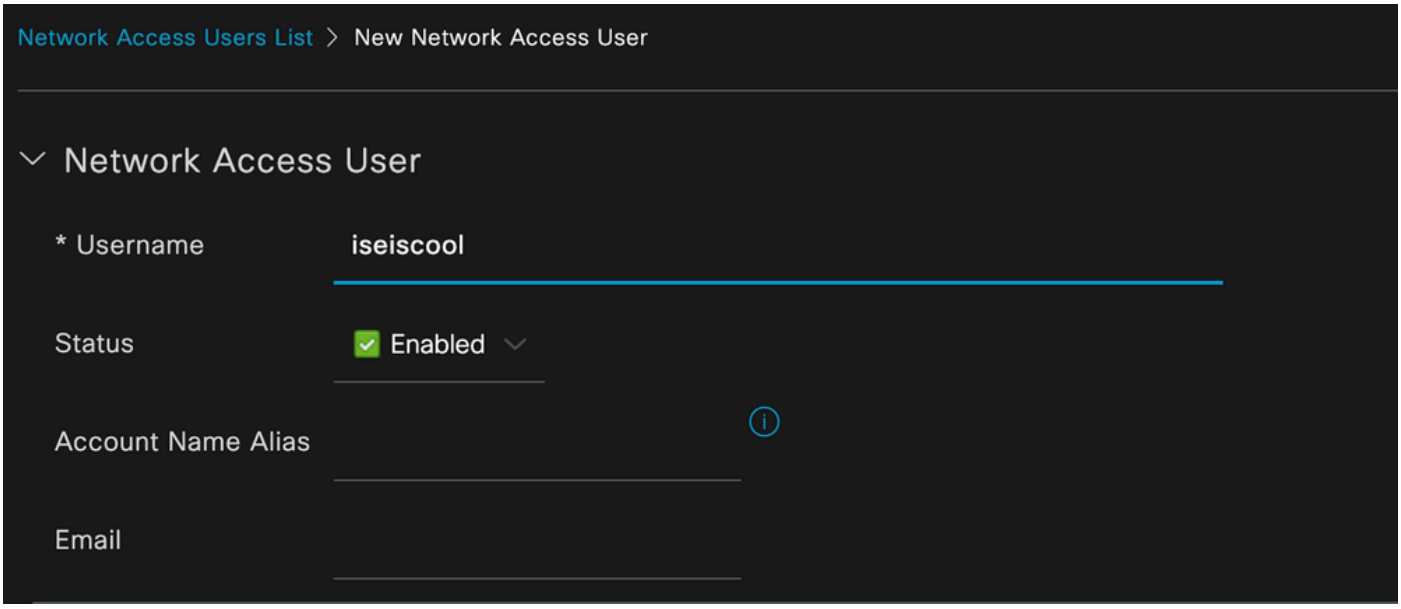
Navigieren Sie anschließend zur Registerkarte Administration > Identity Management > Identity.

Klicken Sie auf Hinzufügen.



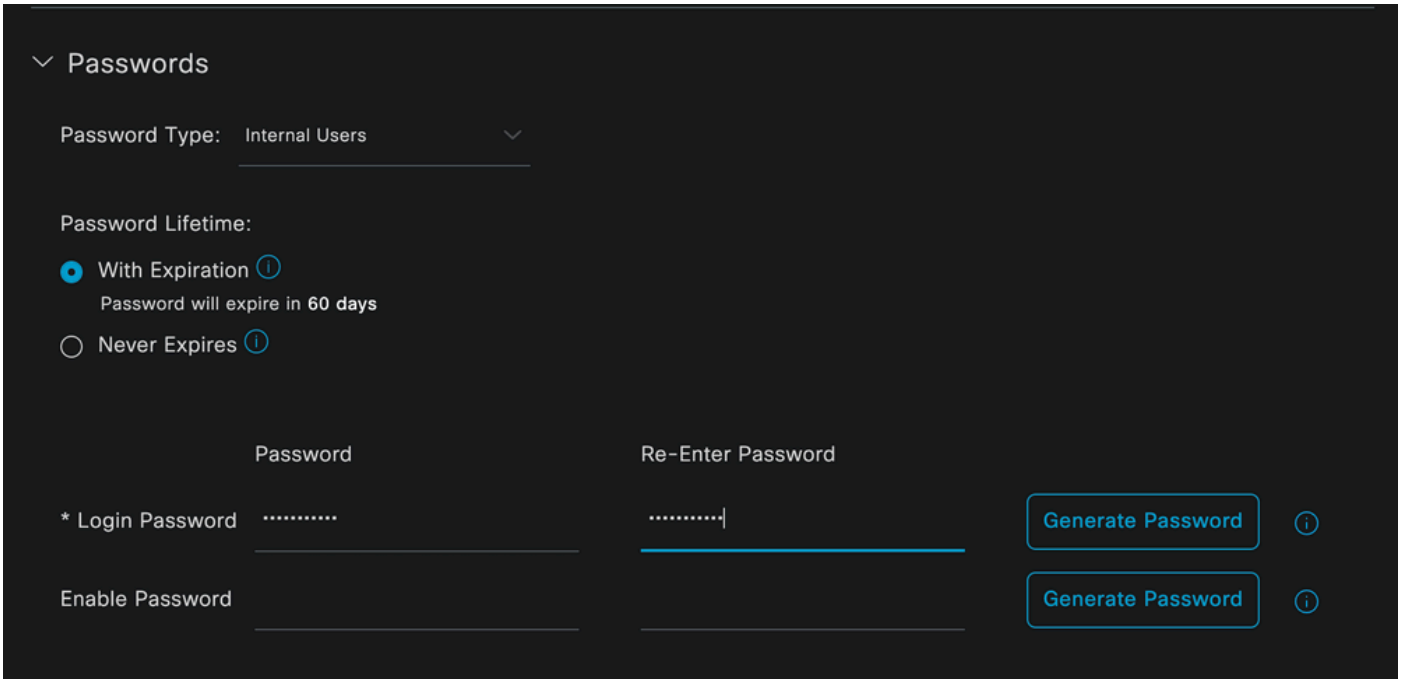
Seite "Benutzererstellung"

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



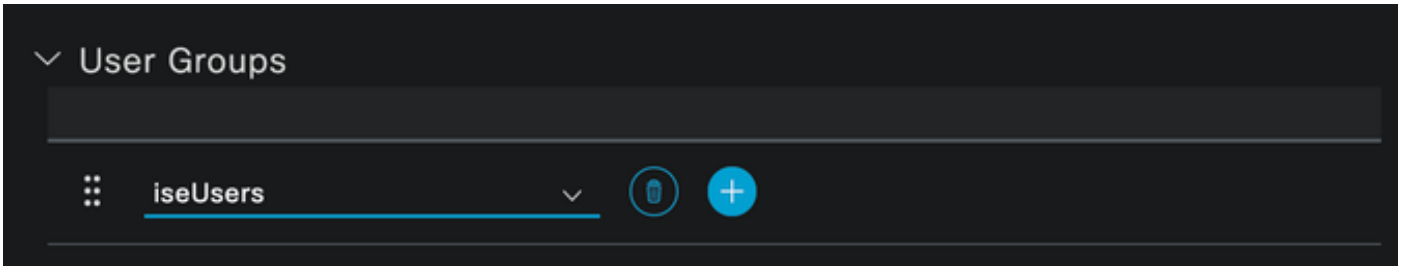
Dem Benutzernamen zugewiesener Name

Der nächste Schritt besteht darin, dem erstellten Benutzernamen ein Kennwort zuzuweisen. VainillaISE97 wird in dieser Demonstration verwendet.



Kennworterstellung

Weisen Sie den Benutzer der Gruppe iseUsers zu.



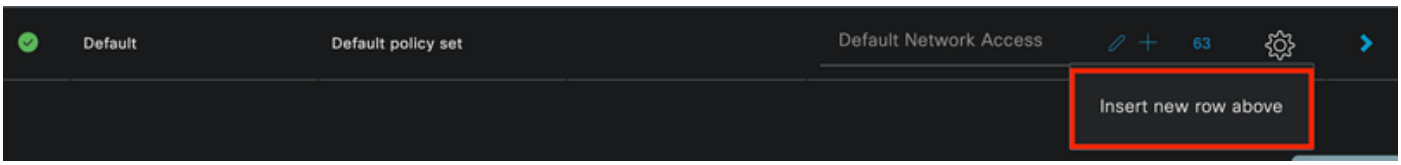
Zuweisung von Benutzergruppen

2. c. Konfigurieren des Richtliniensatzes

Navigieren Sie zu ISE Menu > Policy > Policy Sets.

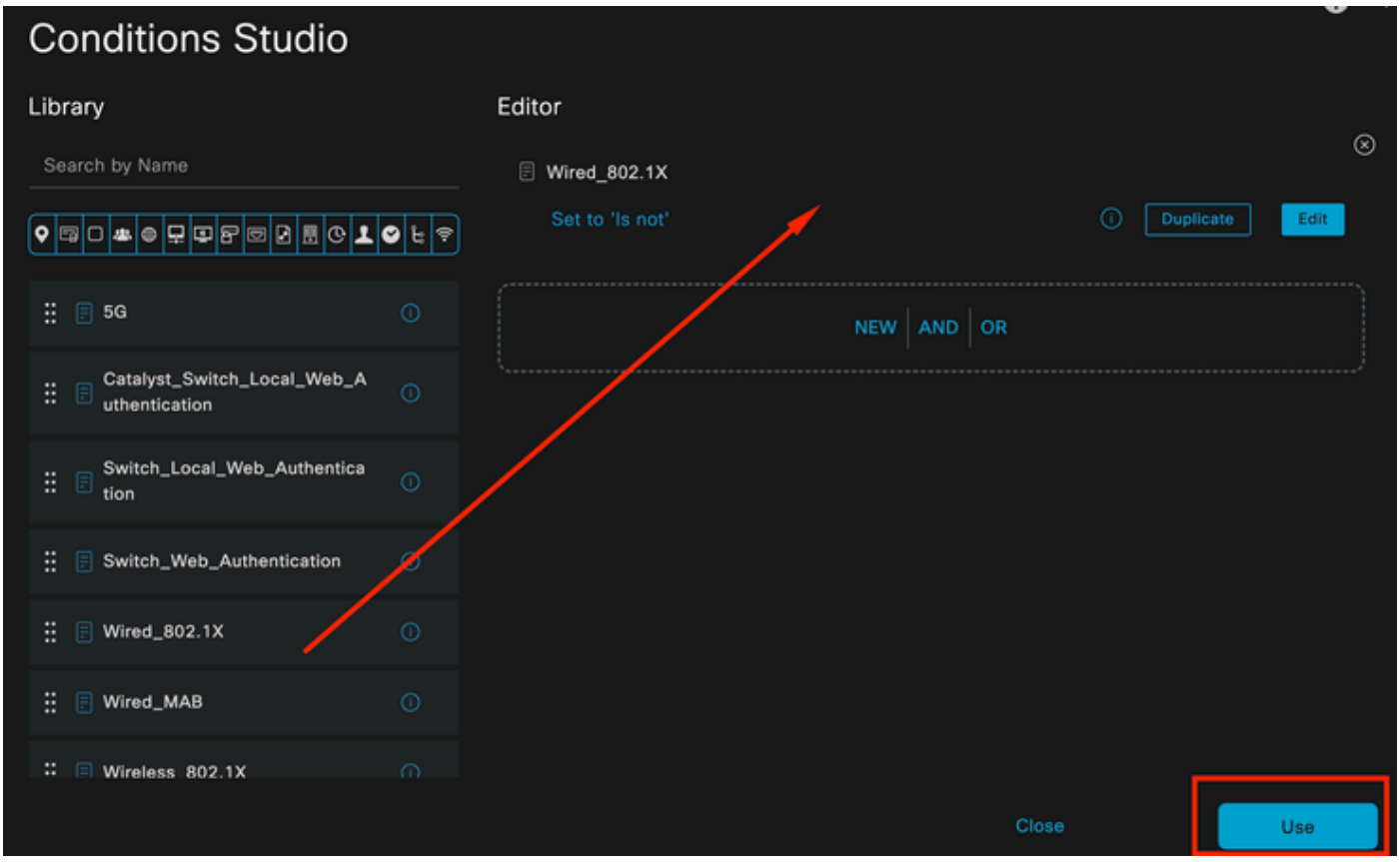
Der Standardrichtliniensatz kann verwendet werden. In diesem Beispiel wird jedoch ein Richtliniensatz erstellt, der als Wired bezeichnet wird. Die Klassifizierung und Differenzierung der Richtliniensätze erleichtert die Fehlerbehebung,

Wenn das Symbol "Hinzufügen" oder "Plus" nicht angezeigt wird, können Sie auf das Zahnrad-Symbol eines Richtliniensatzes klicken. Wählen Sie das Zahnrad-Symbol und dann Neue Zeile einfügen oben.



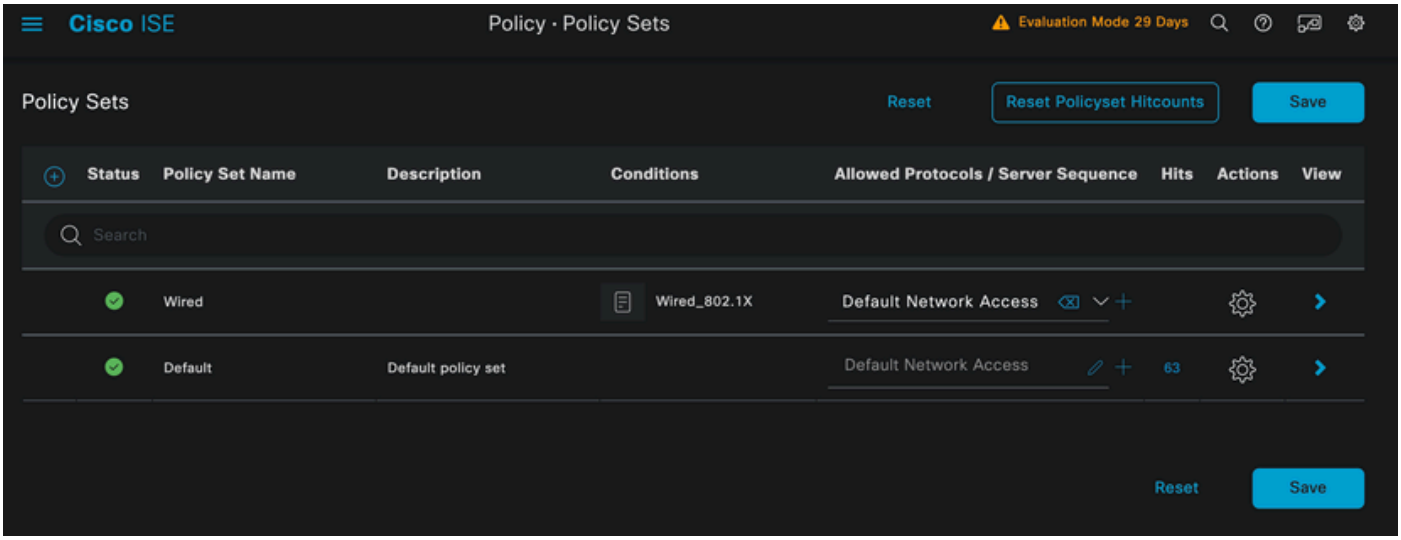
Richtlinienerstellung

Die in diesem Beispiel konfigurierte Bedingung ist Wired 8021x, eine Bedingung, die in neuen ISE-Bereitstellungen vorkonfiguriert ist. Ziehen Sie es, und klicken Sie dann auf Verwenden.



Condition Studio

Wählen Sie anschließend Default Network Access preconfigured allowed protocol service.

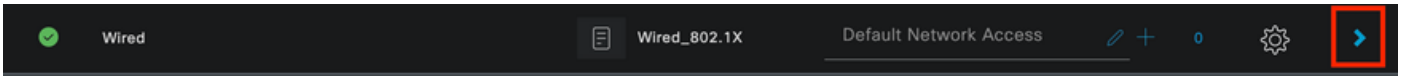


Richtlinienstatusansicht

Klicken Sie auf Speichern.

2. d. Konfigurieren Sie die Authentifizierungs- und Autorisierungsrichtlinien.

Klicken Sie auf den Pfeil rechts neben dem soeben erstellten Richtliniensatz.



Kabelgebundener Richtliniensatz

Erweiterung der Authentifizierungsrichtlinie

Klicken Sie auf das Symbol +.

Authentifizierungsrichtlinie hinzufügen

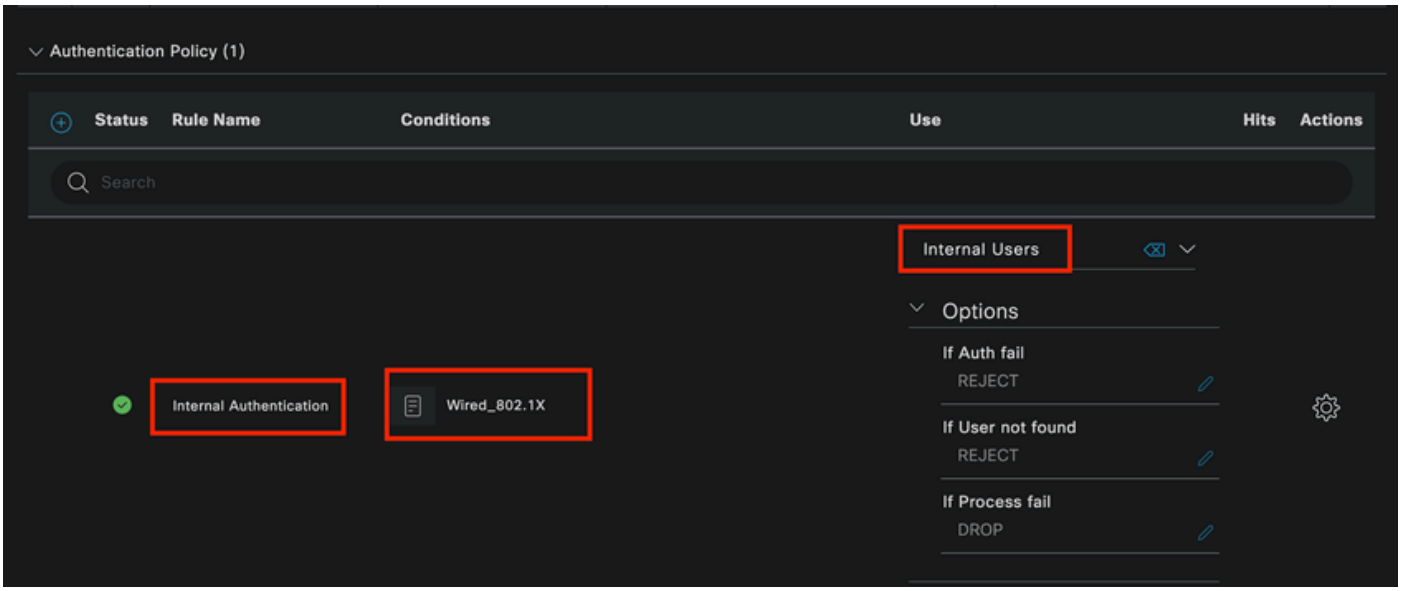
Weisen Sie der Authentifizierungsrichtlinie einen Namen zu. In diesem Beispiel wird die interne Authentifizierung verwendet.

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

Die vorkonfigurierte Bedingung Wired Dot1x ISE kann verwendet werden.

Wählen Sie abschließend in der Spalte Verwendung die Option Interne Benutzer aus der

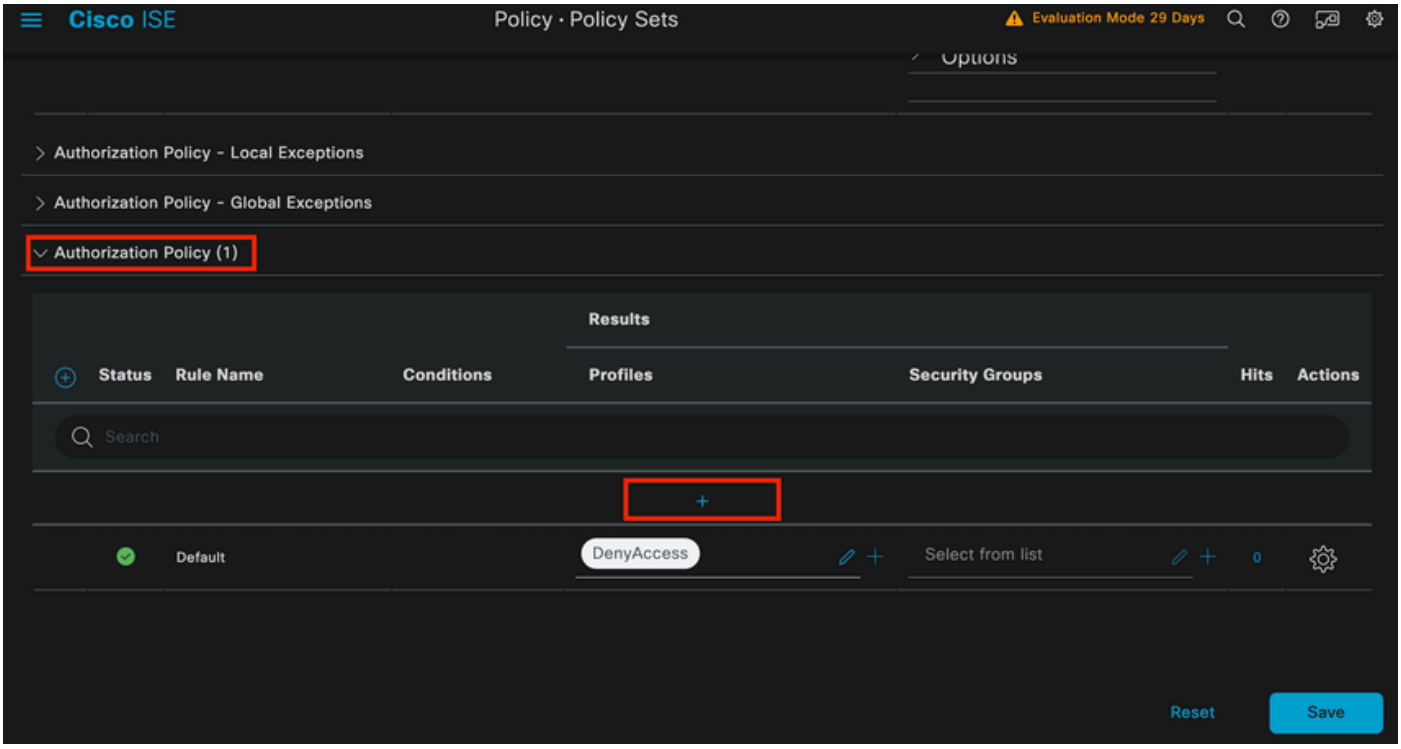
Dropdown-Liste aus.



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 soeben hinzugefügte Autorisierungsrichtlinie. In diesem Konfigurationsbeispiel wird der Name Internal ISE Users verwendet.

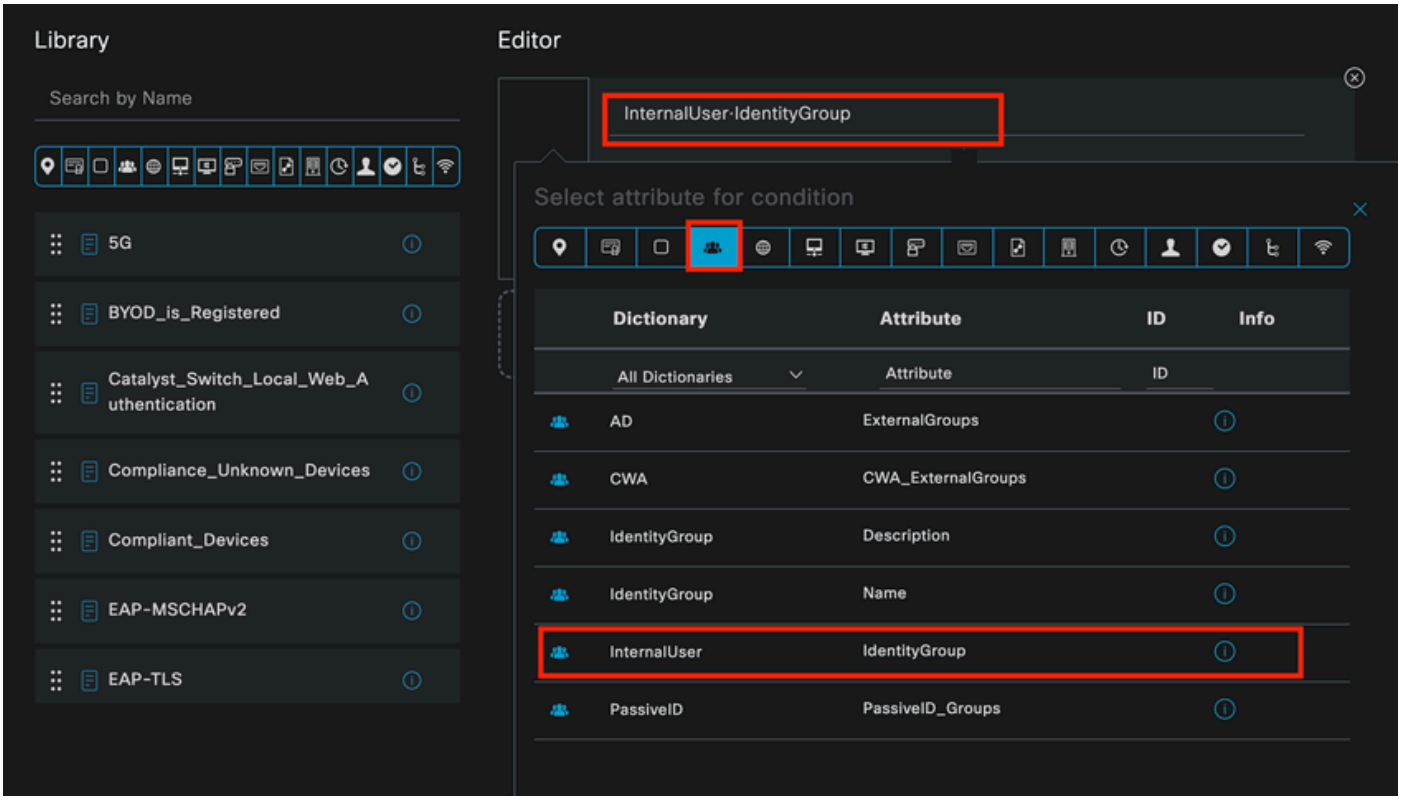
Um eine Bedingung für diese Autorisierungsrichtlinie zu erstellen, klicken Sie in der Spalte "Bedingungen" auf das Symbol +.

Der zuvor erstellte Benutzer ist Teil der IseUsers-Gruppe.

Klicken Sie im Editor auf den Click-Befehl, um ein Attribut hinzuzufügen.

Wählen Sie das Symbol für die Identitätsgruppe aus.

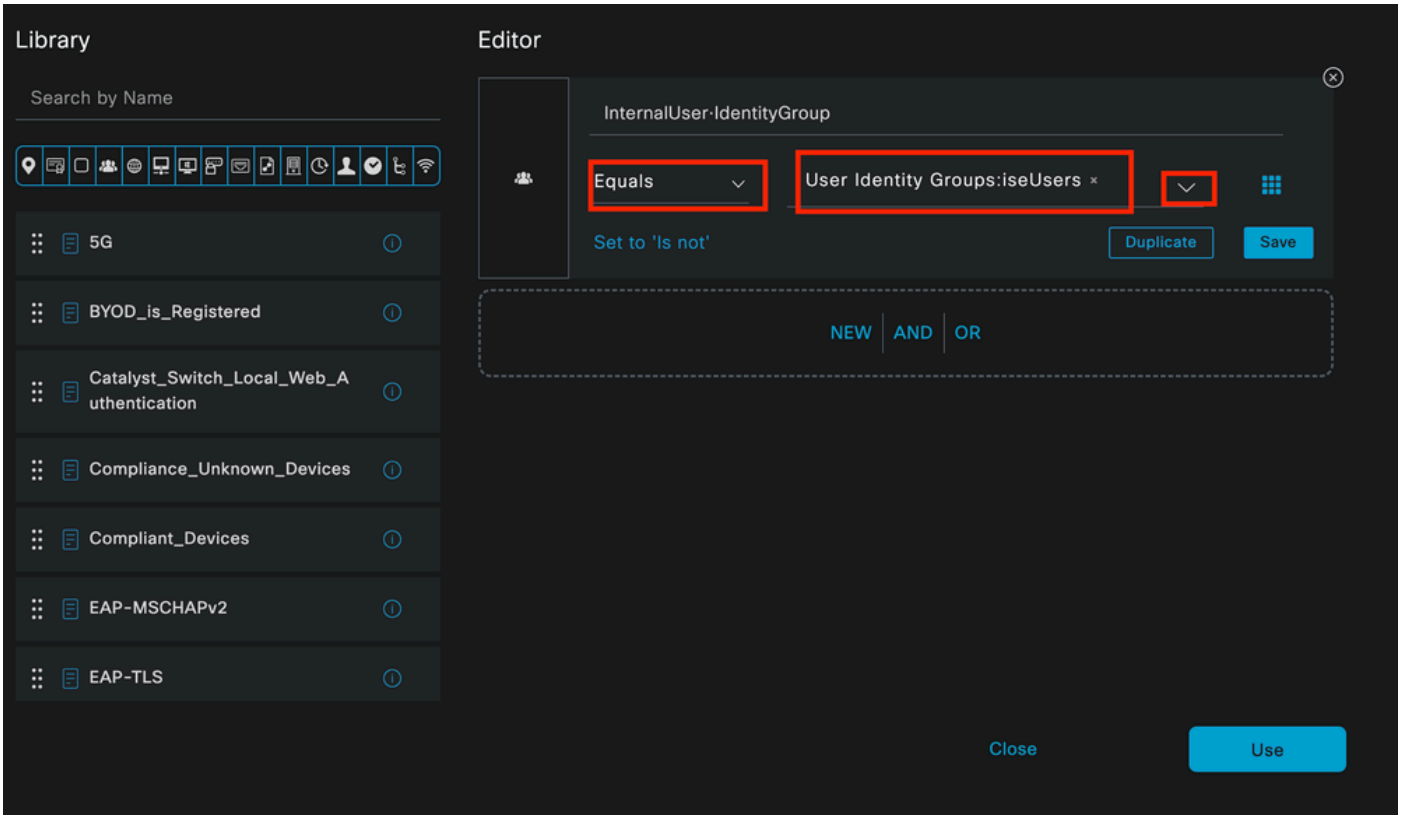
Wählen Sie aus dem Wörterbuch das InternalUser-Wörterbuch aus, das mit dem Identity Group-Attribut geliefert wird.



Condition Studio für Autorisierungsrichtlinien

Wählen Sie den Operator Gleich.

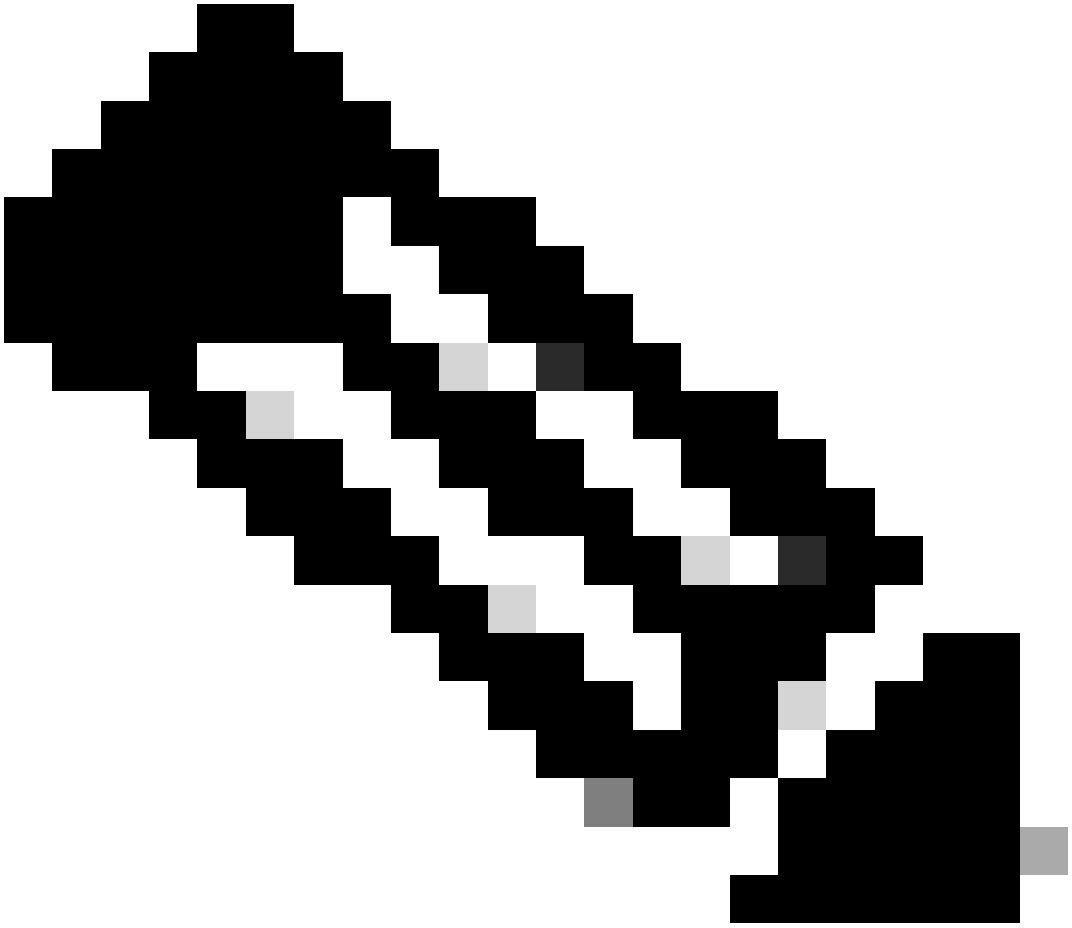
Wählen Sie in der Dropdown-Liste User Identity Groups (Benutzeridentitätsgruppen) die Gruppe IseUsers aus.



Bedingung für Autorisierungsrichtlinie abgeschlossen

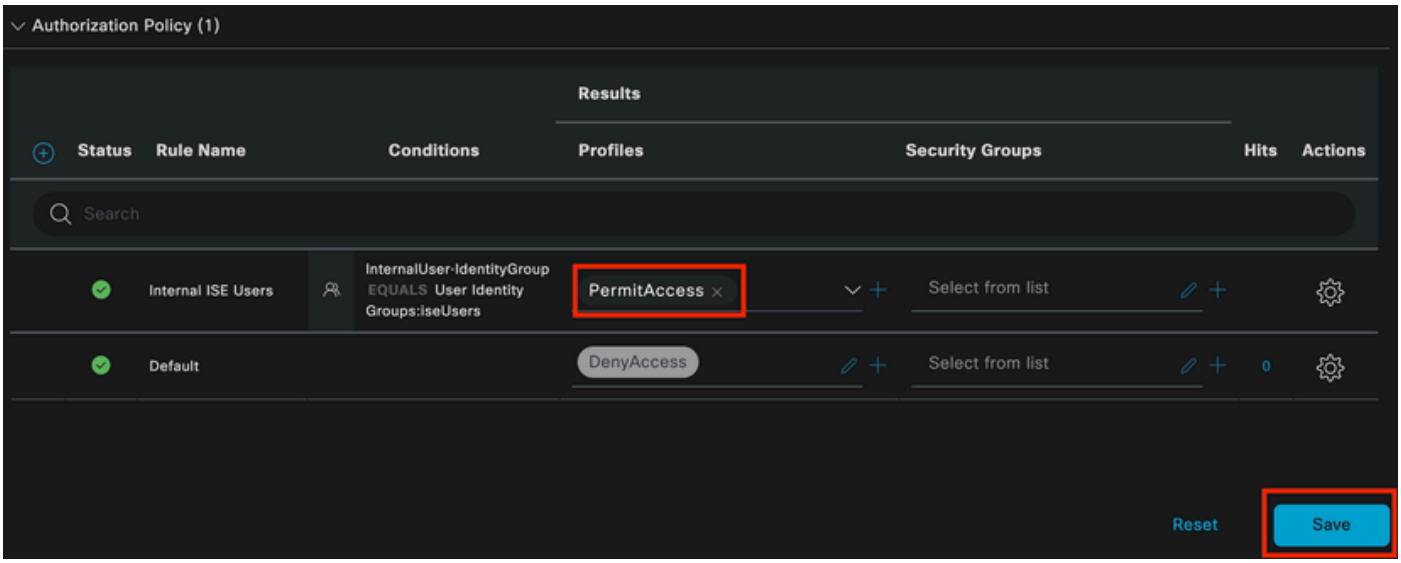
Klicken Sie auf Verwenden.

Wählen Sie abschließend das Ergebnisautorisierungsprofil aus, das den Authentifizierungsteil dieser Identitätsgruppe empfängt.



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

Die ISE ist mit dem Profil Zugriffsberechtigung vorkonfiguriert. Wählen Sie es aus.



Autorisierungsrichtlinie abgeschlossen

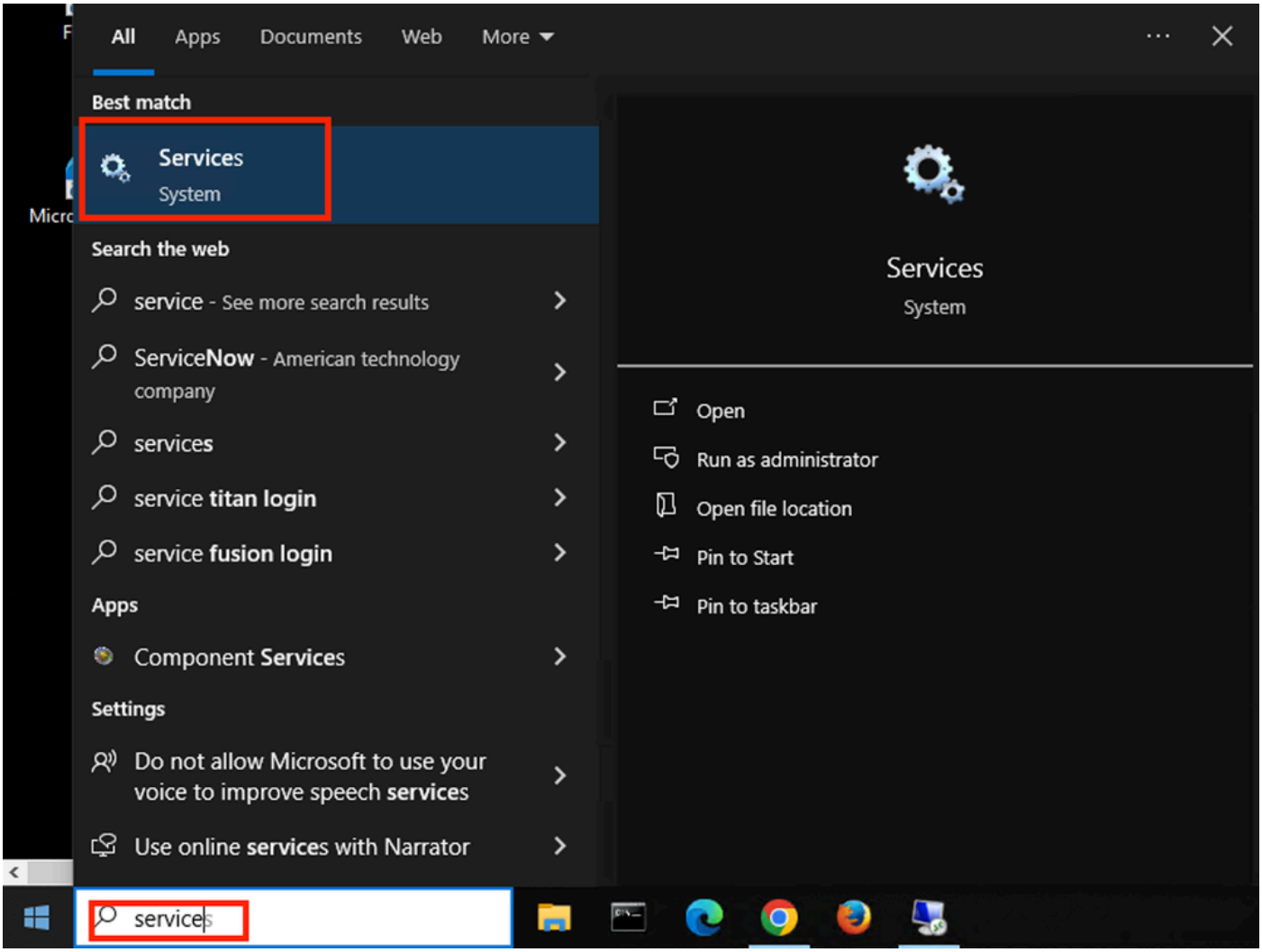
Klicken Sie auf Speichern.

Die Konfiguration für die ISE ist abgeschlossen.

Schritt 3: Konfiguration der nativen Windows-Komponente

3. a. Aktivieren Sie Wired dot1x unter Windows.

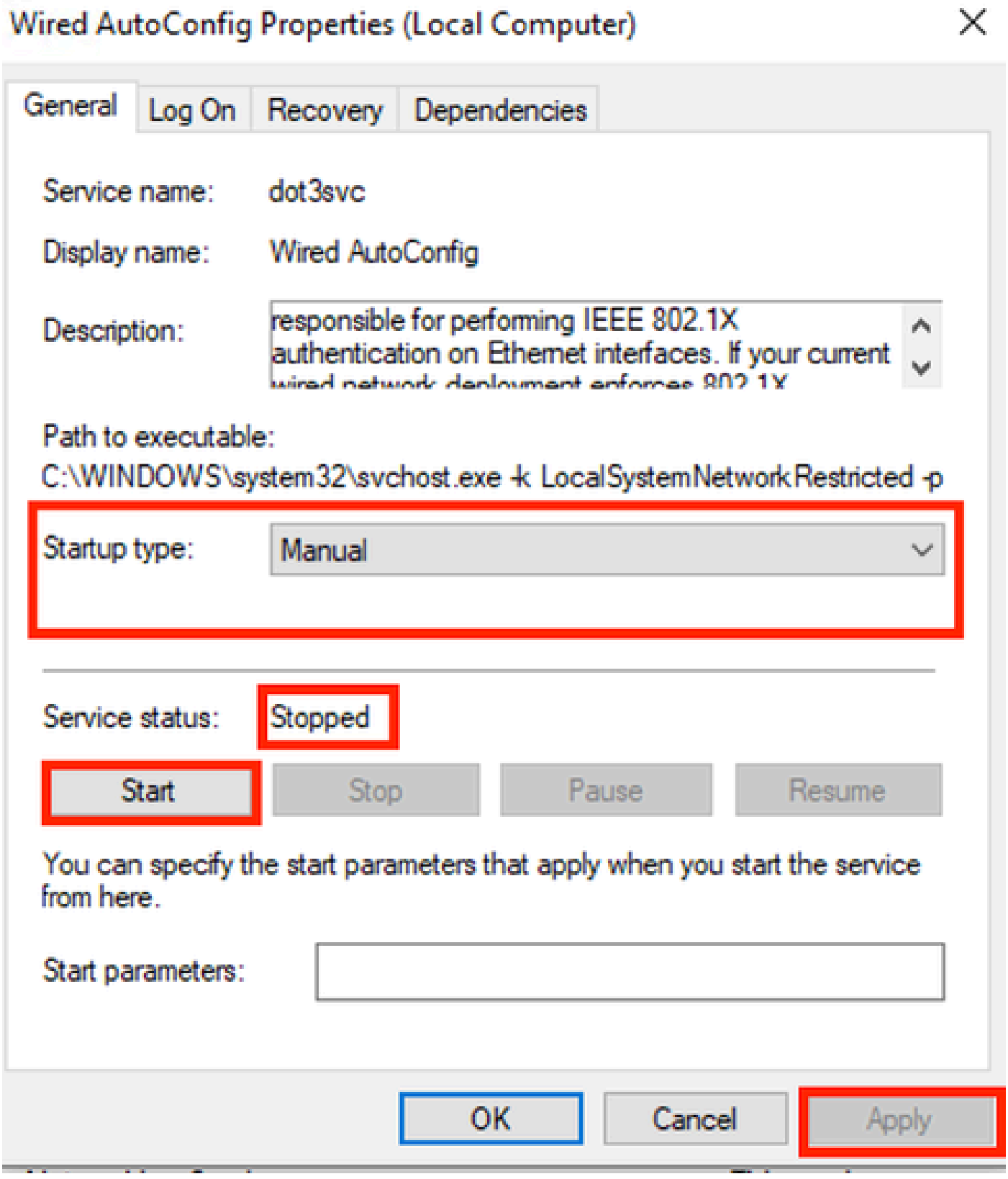
Öffnen Sie in der Windows-Suchleiste Dienste.



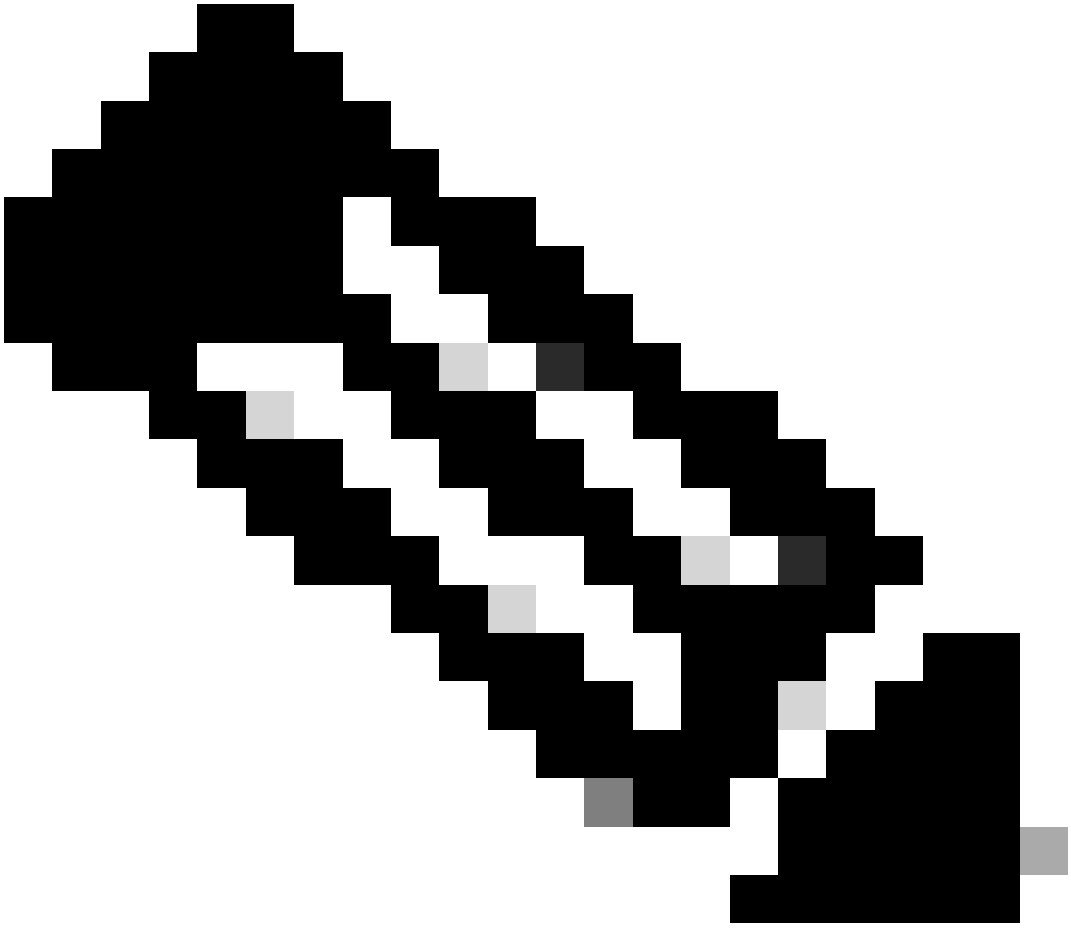
Windows-Suchleiste

Suchen Sie unten in der Liste Dienste den Eintrag Kabelgebundene Autokonfiguration.

Klicken Sie mit der rechten Maustaste auf Wired AutoConfig, und wählen Sie Eigenschaften aus.



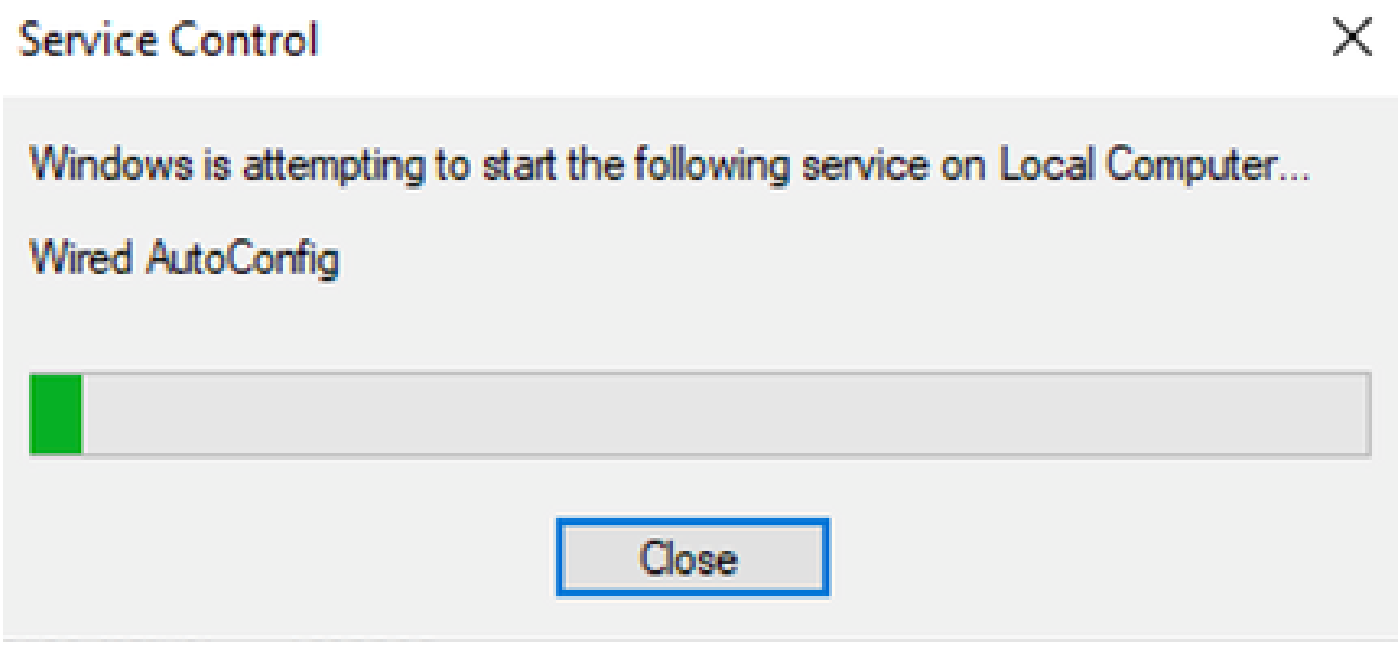
Eigenschaftenfenster



Hinweis: Der Wired AutoConfig (DOT3SVC)-Service ist für die Durchführung der IEEE 802.1X-Authentifizierung an Ethernet-Schnittstellen verantwortlich.

Der Starttyp Manuell ist ausgewählt.

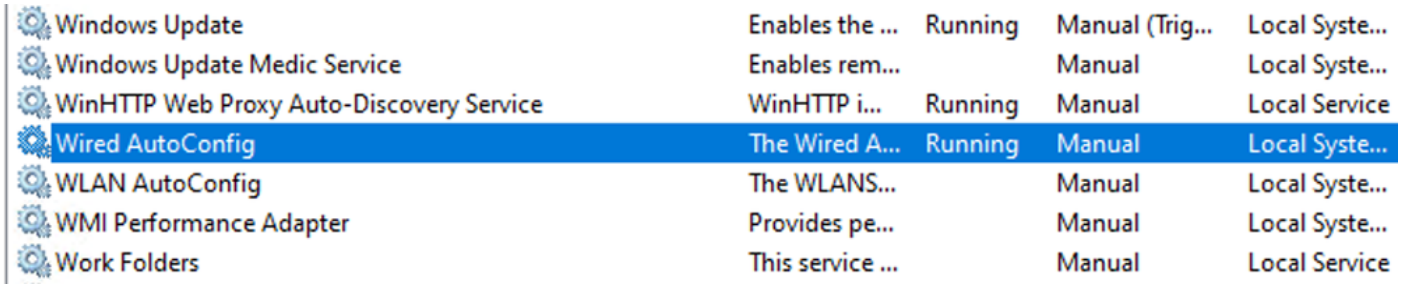
Da der Dienststatus Gestoppt ist. Klicken Sie auf Start.



Servicesteuerung

Klicken Sie anschließend auf OK.

Der Dienst wird danach ausgeführt.



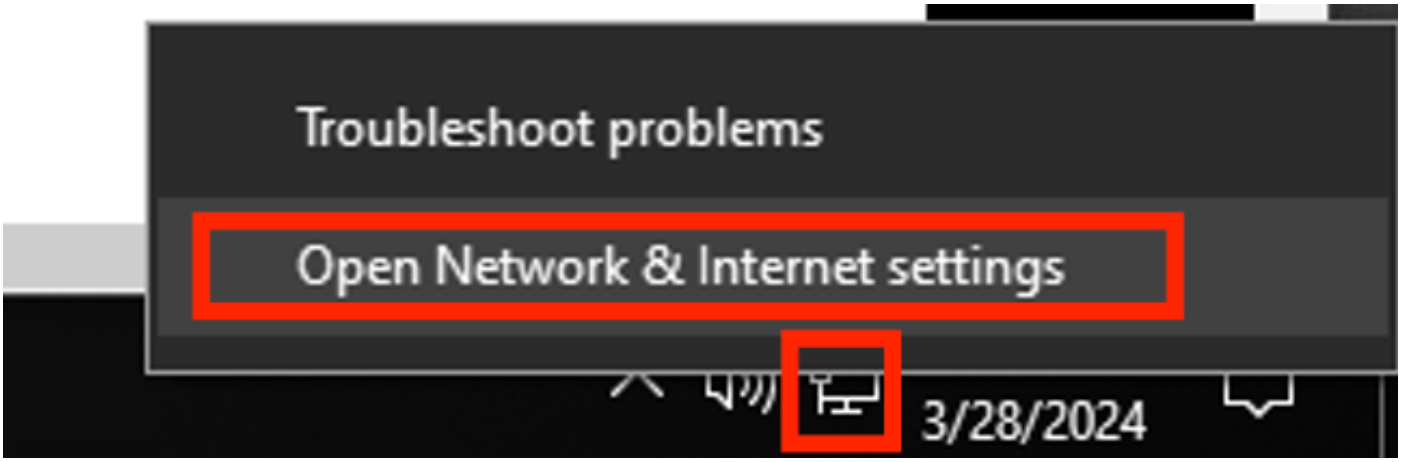
Kabelgebundener AutoConfig-Service

3. b. Konfigurieren Sie die Windows-Laptop-Schnittstelle, die mit dem NAD Authenticator (ISR 1100) verbunden ist.

Suchen Sie in der Taskleiste nach der rechten Ecke, und verwenden Sie dann das Computersymbol.

Doppelklicken Sie auf das Computersymbol.

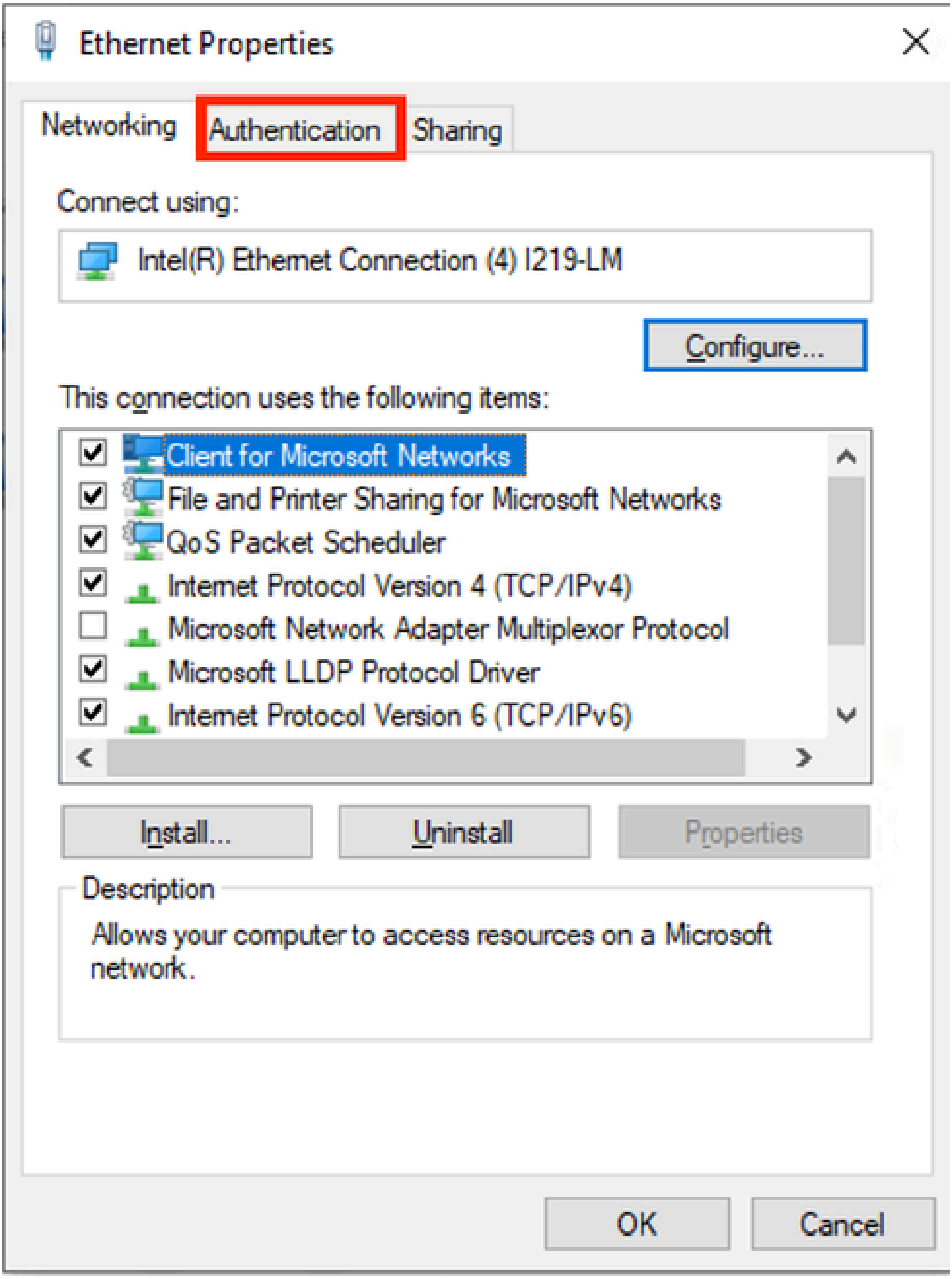
Wählen Sie Netzwerk- und Interneteinstellungen öffnen aus.



Windows-Taskleiste

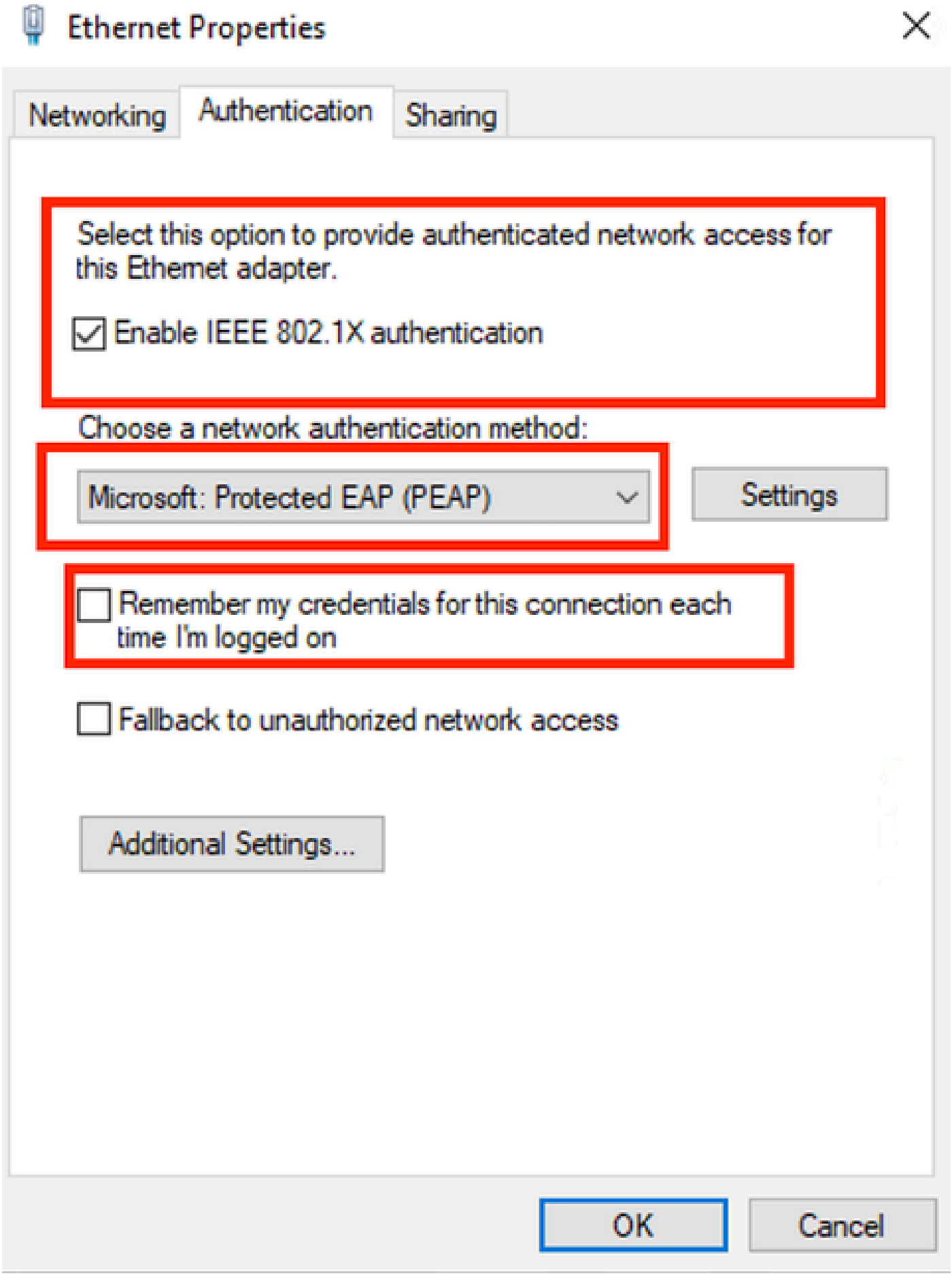
Wenn das Fenster Netzwerkverbindungen geöffnet wird, klicken Sie mit der rechten Maustaste auf die Ethernet-Schnittstelle, die mit dem ISR Gig 0/1/0 verbunden ist. Klicke auf die Option Eigenschaften.

Klicken Sie auf die Registerkarte Authentifizierung.



Ethernet-Schnittstelleneigenschaften

Aktivieren Sie das Kontrollkästchen IEEE 802.1X-Authentifizierung aktivieren.

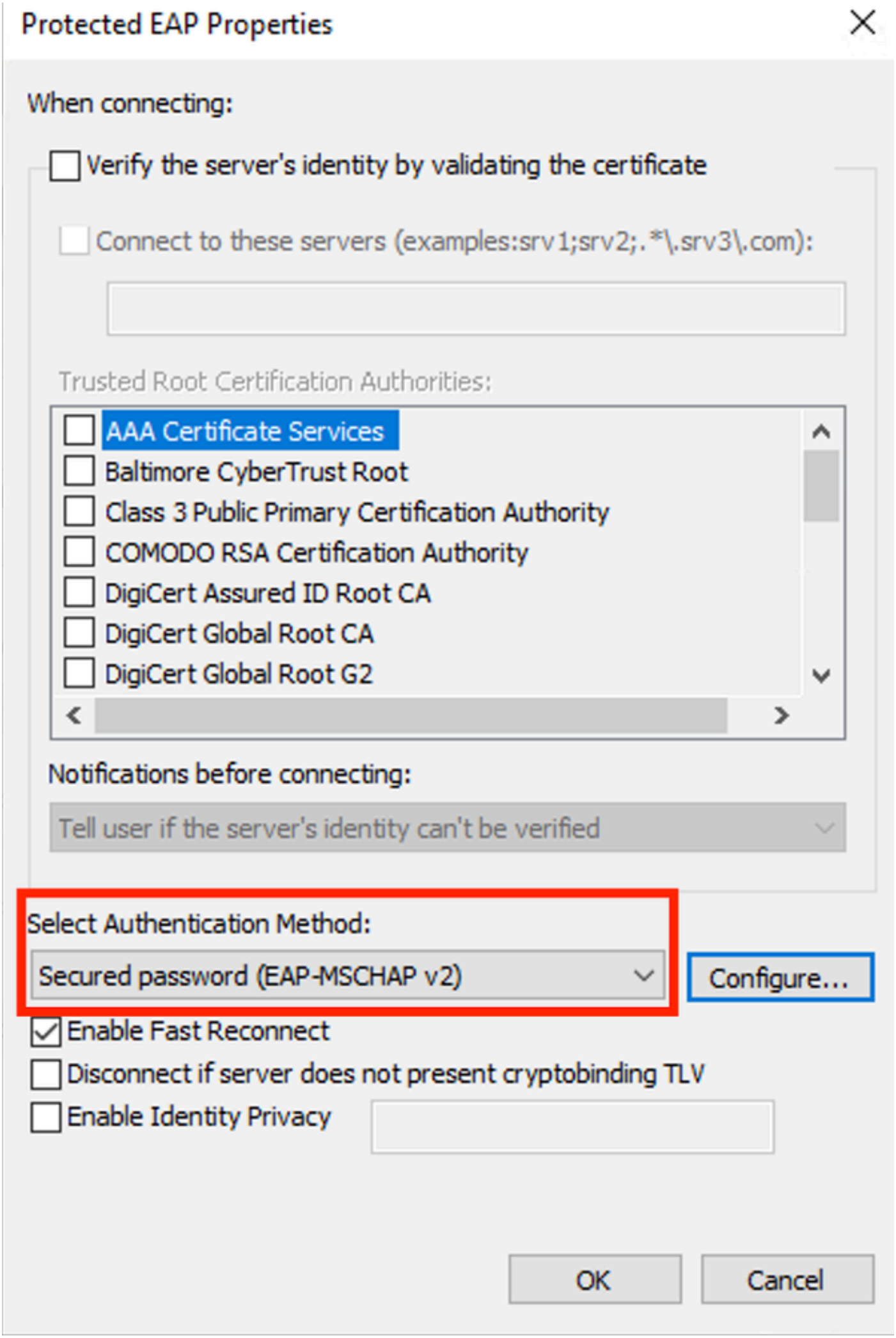


Authentifizierungs-Ethernet-Eigenschaften

Wählen Sie Protected EAP (PEAP) aus.

Deaktivieren Sie die Option Anmeldedaten für diese Verbindung speichern, wenn ich angemeldet bin.

Klicken Sie auf Einstellungen.



PEAP-Eigenschaften

zeigt detaillierte Informationen zu den dot1x-Sitzungen an, die auf dem angegebenen Port ausgeführt werden.

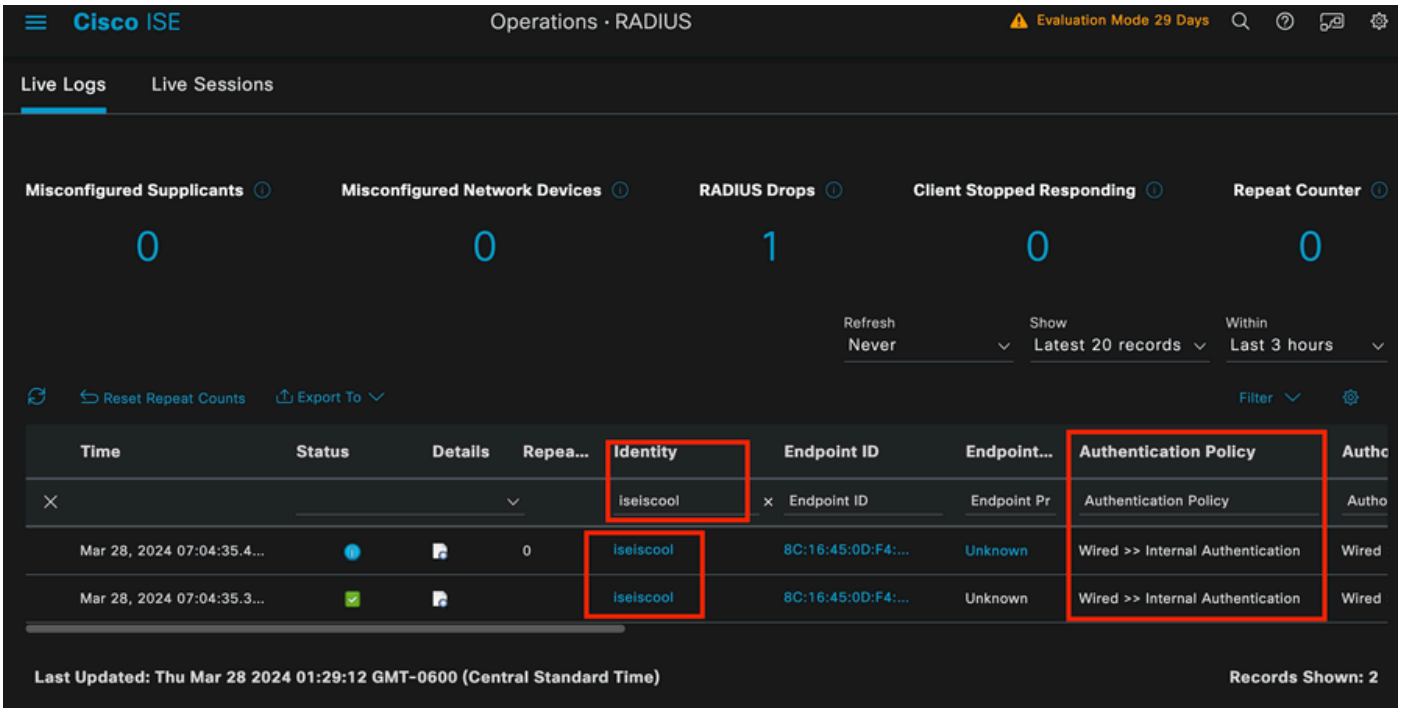
```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details

            Interface:  GigabitEthernet0/1/0

               IIF-ID:  0x08767C0D

          MAC Address:  8c16.450d.f42b

         IPv6 Address:  Unknown

         IPv4 Address:  Unknown

            User-Name:  iseiscool <--------- The username configured for Windows Native Supplicant

               Status:  Authorized <--------- An indication that this session was authorized by the PSN

               Domain:  DATA

       Oper host mode:  multi-auth

     Oper control dir:  both

      Session timeout:  N/A

    Common Session ID:  22781F0A0000000C83E28461

      Acct Session ID:  0x00000003

               Handle:  0xc6000002

       Current Policy:  POLICY_Gi0/1/0




Local Policies:

        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

      Security Policy:  Should Secure



Server Policies:




Method status list:

       Method           State

        dot1x           Authc Success <--------- An indication that dot1x is used for this authenticati
```

```
Router#
```

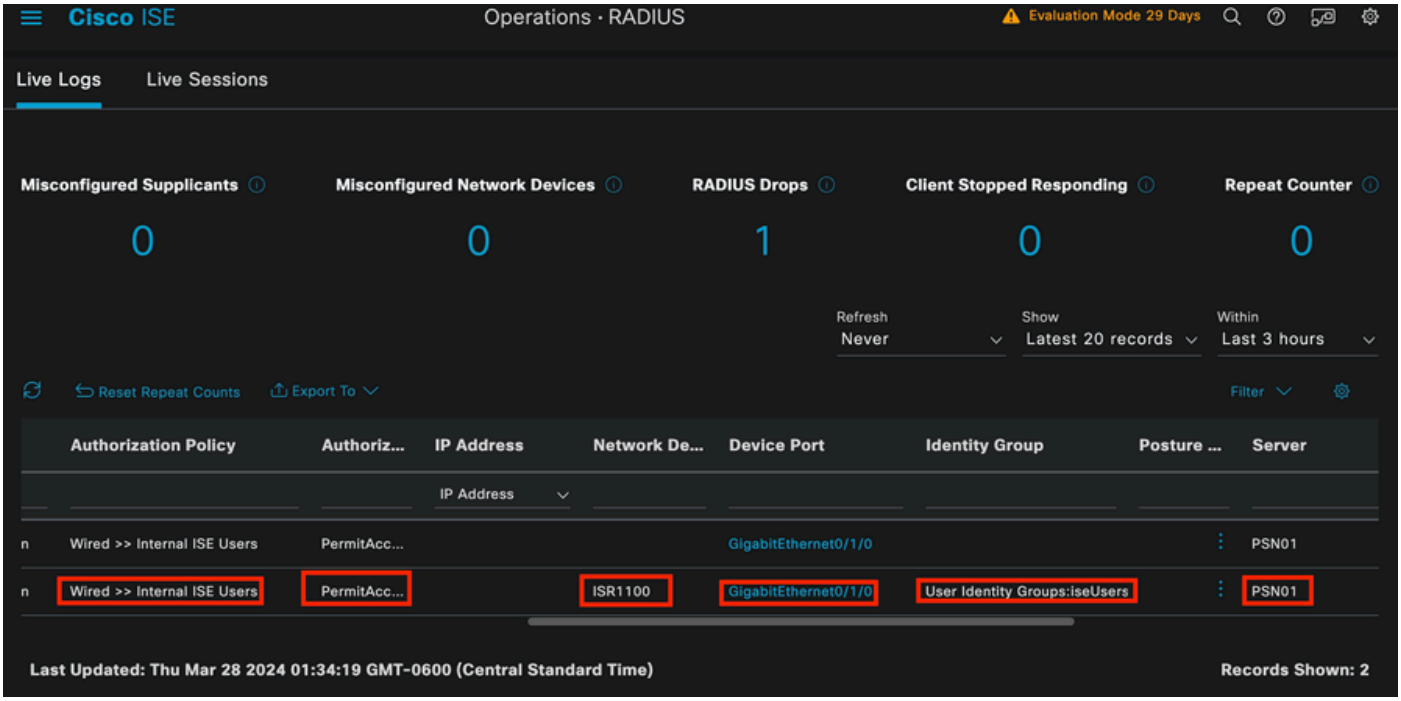
ISE-Protokolle

Navigieren Sie zur Registerkarte Operations > Radius > Live logs (Vorgänge > Radius > Live-Protokolle).

Filtern Sie nach der Identität des Benutzernamens. In diesem Beispiel wird der Benutzername iseiscool verwendet.



ISE-Livelogs



ISE-Livelogs

Beachten Sie, dass Live-Protokolle in dieser Schnellansicht wichtige Informationen bereitstellen:

- Zeitstempel der Authentifizierung.
- Verwendete Identität
- MAC-Adresse des Endpunkts
- Policy Set und Authentifizierungsrichtlinie, die getroffen wurde.
- Betroffene Richtlinien und Autorisierungsrichtlinien
- Ergebnis des Autorisierungsprofils
- Das Netzwerkgerät, das die Radius-Anforderung an die ISE sendet.
- Die Schnittstelle, mit der der Endpunkt verbunden ist.
- Die Identitätsgruppe des authentifizierten Benutzers.
- Der Policy Server Node (PSN), der die Authentifizierung behandelt hat.

Fehlerbehebung

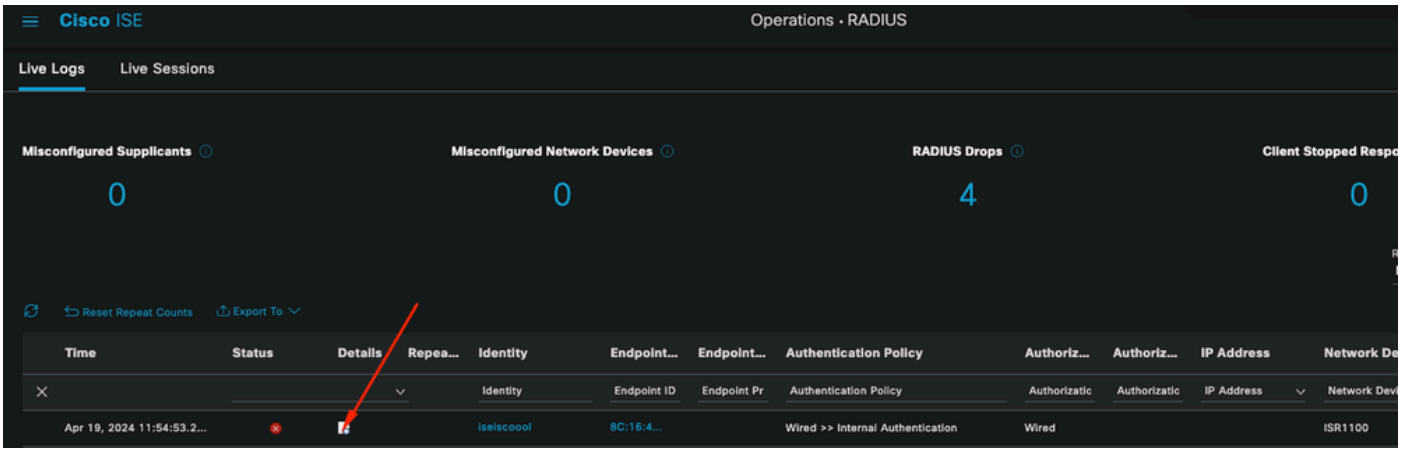
1 - Lesen der ISE-Live-Protokolldetails

Navigieren Sie zur Registerkarte Operations > Radius > Live logs (Operationen > Radius > Live-Protokolle), filtern Sie nach Auth status: Failed OR (Auth-Status: Fehlgeschlagen ODER nach dem Benutzernamen ODER der MAC-Adresse ODER dem verwendeten Netzwerkzugriffsgerät).

Rufen Sie Operations > Radius > Live logs > Desired authentication > Live log details auf.

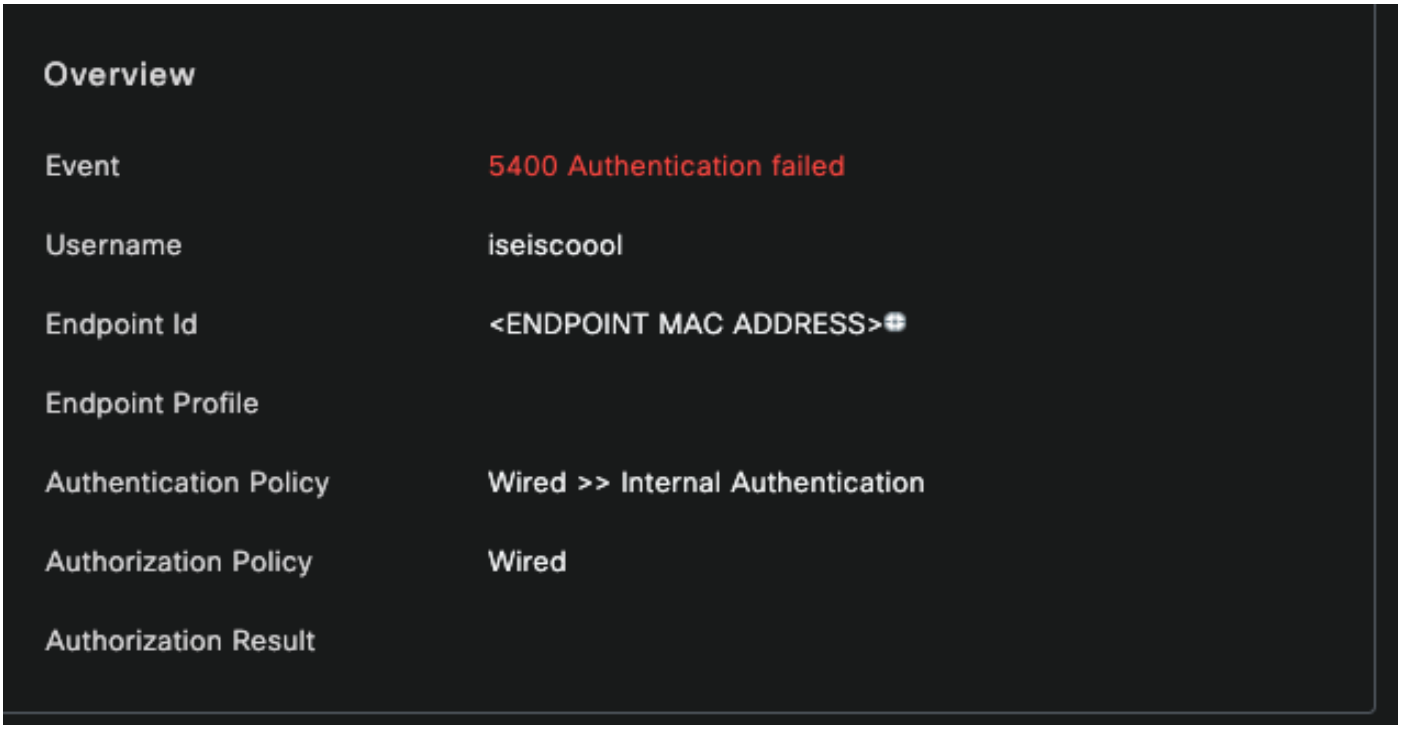
Klicken Sie auf der gleichen Seite nach dem Filtern der Authentifizierung auf das Symbol Suchen.

Erstes Szenario: Der Benutzer gibt seinen Benutzernamen mit einem Tippfehler ein.



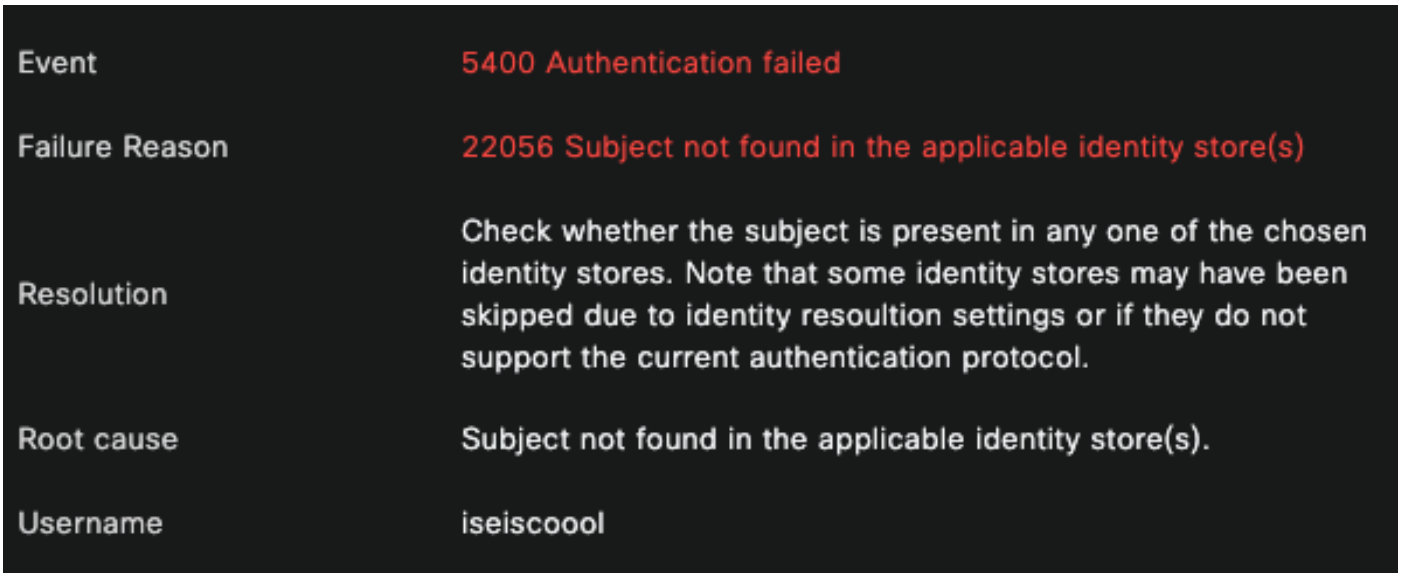
Details zum Live-Protokoll öffnen

Sobald die Details des Live-Protokolls geöffnet sind, können Sie sehen, dass die Authentifizierung fehlgeschlagen ist. Außerdem wird der verwendete Benutzername aufgelistet.



Übersichtsabschnitt

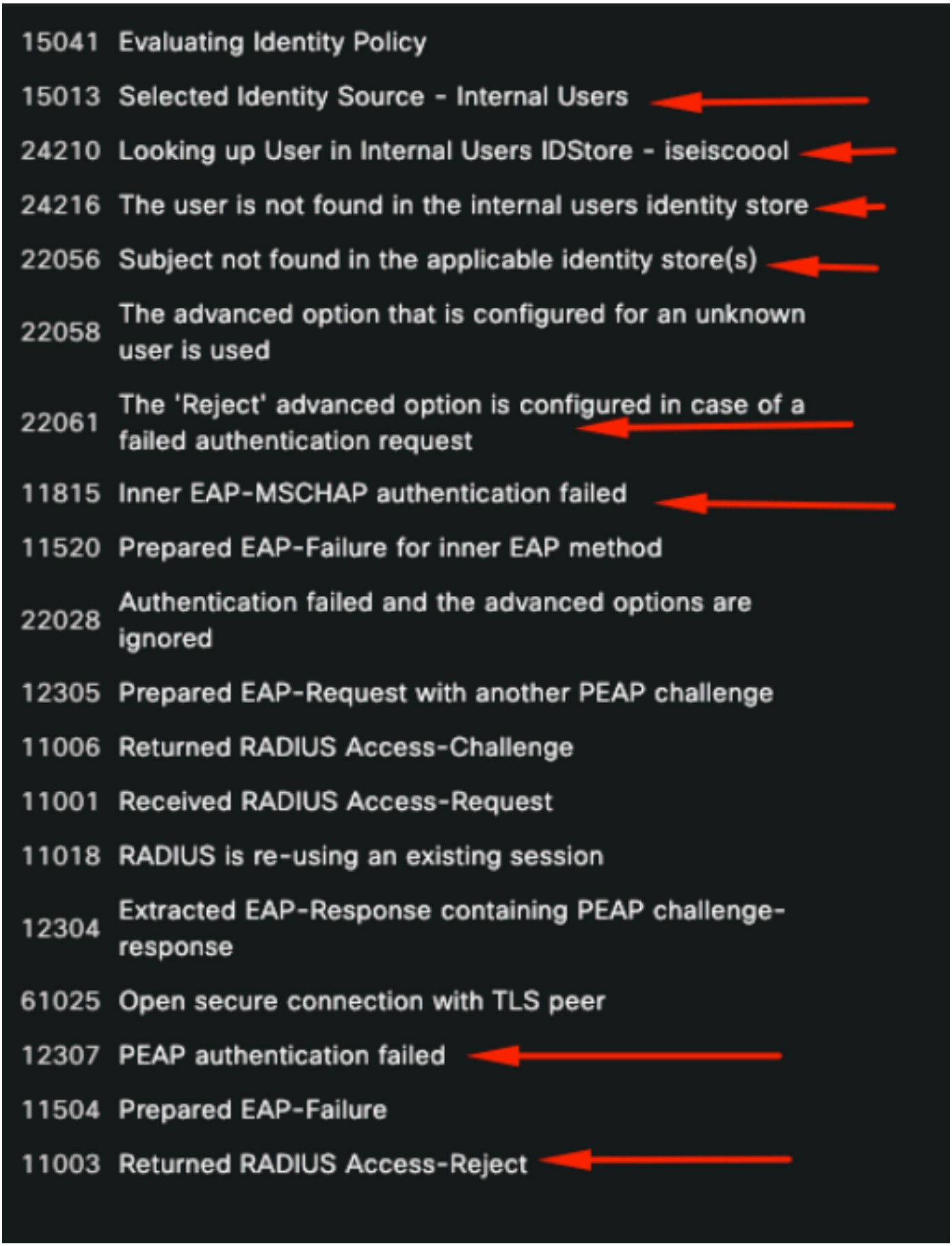
Im gleichen Live-Protokolldetail im Abschnitt "Authentifizierungsdetails" finden Sie dann die Fehlerursache, die Ursache und die Behebung des Fehlers.



Authentifizierungsdetails

In diesem Szenario schlägt die Authentifizierung fehl, weil der Benutzername einen Tippfehler aufweist. Dieselbe Fehlermeldung würde jedoch angezeigt, wenn der Benutzer nicht in der ISE erstellt wird oder wenn die ISE nicht überprüfen kann, ob der Benutzer in anderen Identitätsspeichern, z. B. LDAP oder AD, vorhanden ist.

Abschnitt Schritte



Abschnitt "Live Log Details"

Im Abschnitt mit den Schritten wird der Prozess ausführlich beschrieben, den ISE während des

RADIUS-Gesprächs ausgeführt hat.

Hier finden Sie Informationen wie:

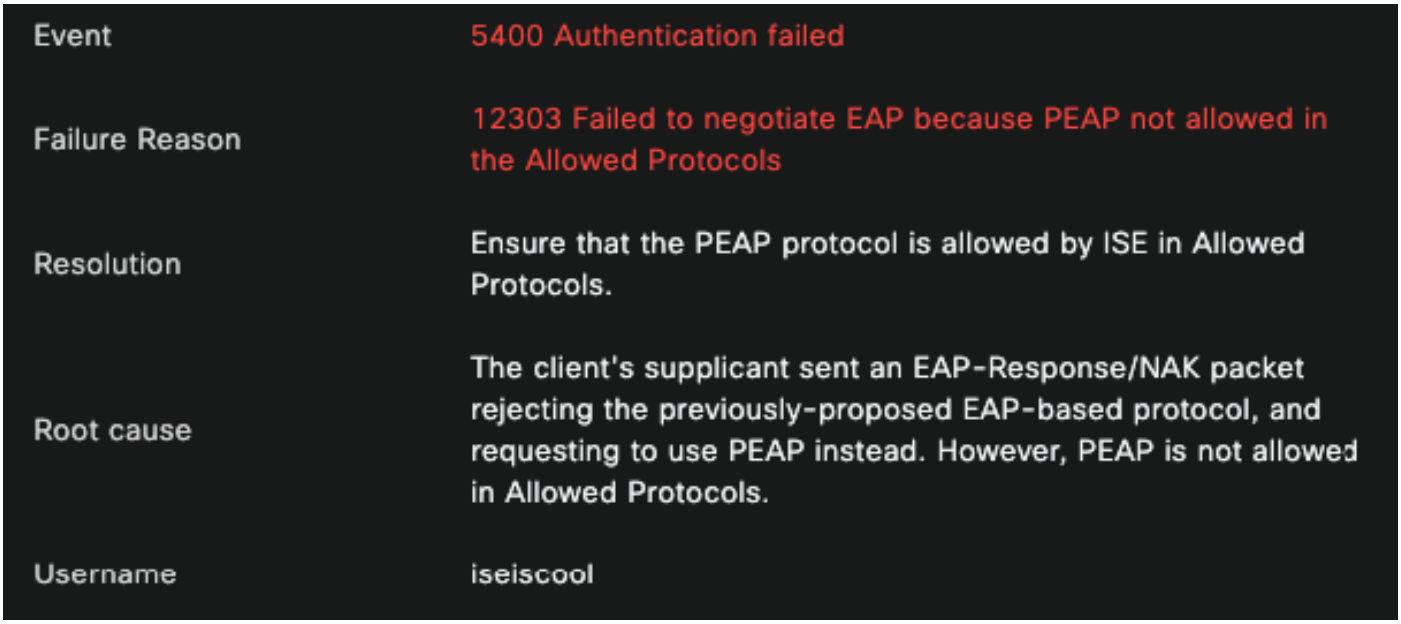
- Wie das Gespräch begann.
- SSL-Handshake-Prozess.
- Die ausgehandelte EAP-Methode.
- EAP-Methodenprozess.

In diesem Beispiel ist zu sehen, dass die ISE gerade die internen Identitäten für diese Authentifizierung eingecheckt hat. Der Benutzer wurde nicht gefunden, und aus diesem Grund sendete die ISE als Antwort eine Access-Reject-Nachricht.

Zweites Szenario: Der ISE-Administrator hat PEAP für die Protokolle Policy Set Allowed (Richtliniensatz zulässig) deaktiviert.

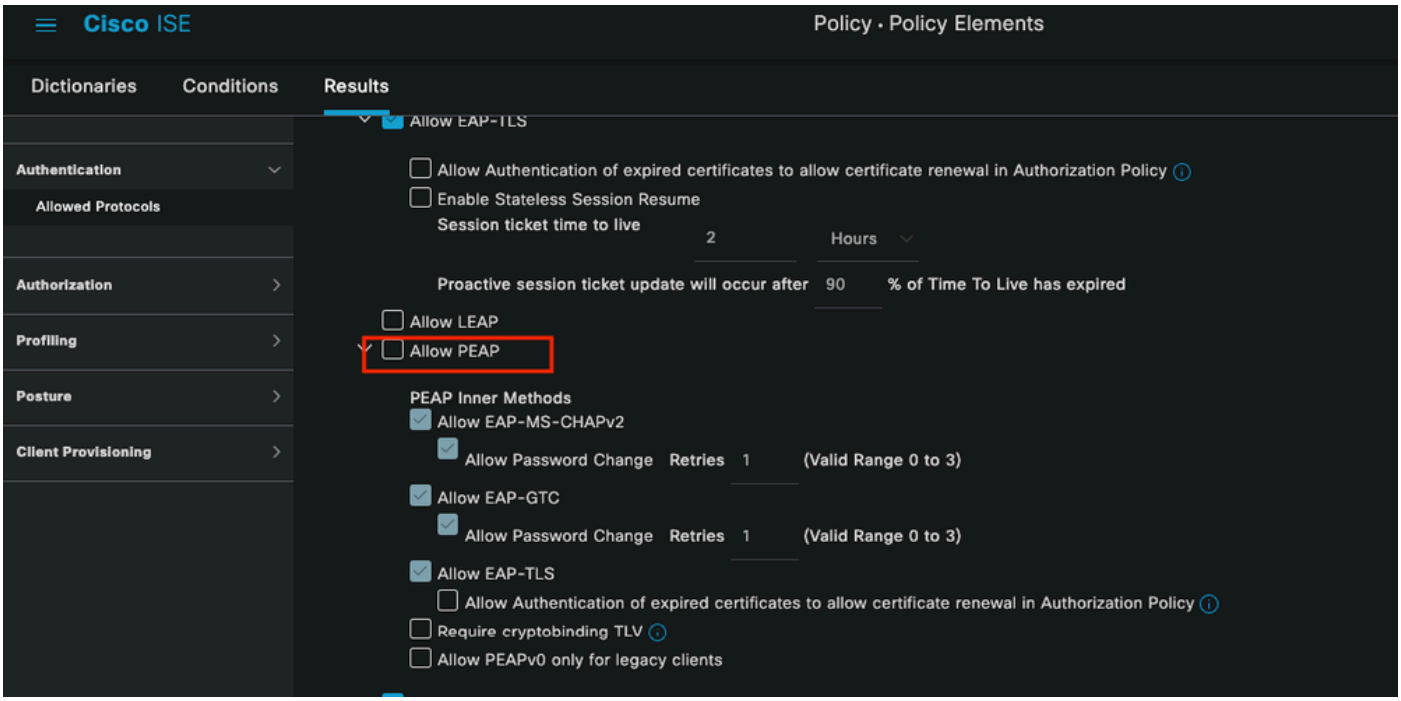
2 - PEAP deaktiviert

Sobald die Details des Live-Protokolls aus der fehlgeschlagenen Sitzung geöffnet werden, wird die Fehlermeldung "PEAP is not allowed in the Allowed Protocols" (PEAP ist in den zulässigen Protokollen nicht zulässig) angezeigt.



Live-Log-Detailbericht

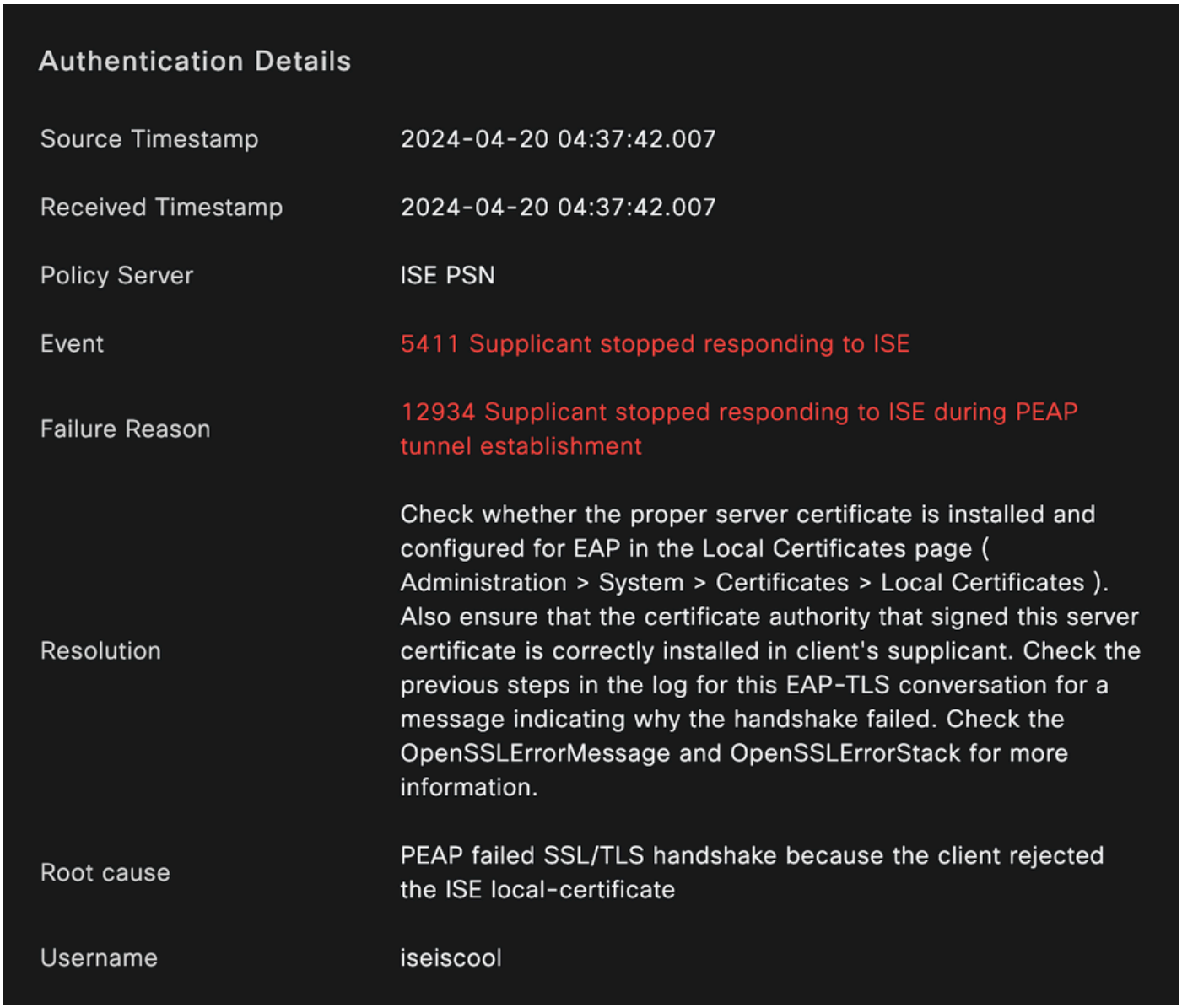
Dieser Fehler ist leicht zu beheben. Die Lösung besteht darin, zu Policy > Policy Elements > Authentication > Allowed Protocols zu navigieren. Überprüfen Sie, ob die Option PEAP zulassen deaktiviert ist.



Abschnitt "Zulässige Protokolle"

Drittes Szenario: Die Authentifizierung schlägt fehl, da der Endpunkt dem ISE-Zertifikat nicht vertraut.

Navigieren Sie zu den Details des Live-Protokolls. Suchen Sie den Datensatz für die fehlgeschlagene Authentifizierung, und überprüfen Sie die Live-Protokolldetails.

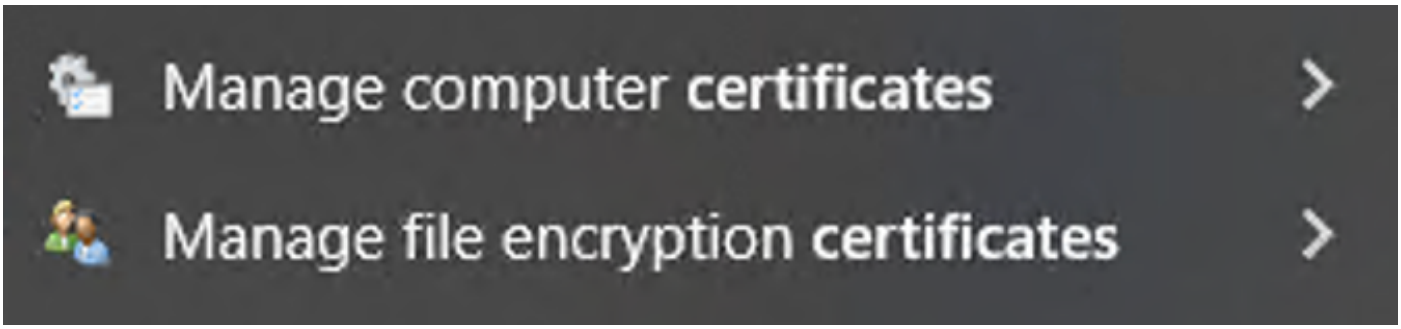


Live-Protokolldetails

Der Endpunkt lehnt das für die Einrichtung des PEAP-Tunnels verwendete Zertifikat ab.

Um dieses Problem zu beheben, überprüfen Sie am Windows-Endpunkt, an dem das Problem aufgetreten ist, ob die Zertifizierungsstellenkette, die das ISE-Zertifikat signiert hat, im Abschnitt Benutzerzertifikate verwalten > Vertrauenswürdige Stammzertifizierungsstellen ODER Computerzertifikate verwalten > Vertrauenswürdige Stammzertifizierungsstellen aufgeführt ist.

Sie können auf diesen Konfigurationsabschnitt auf Ihrem Windows-Gerät zugreifen, indem Sie sie in der Windows-Suchleiste durchsuchen.

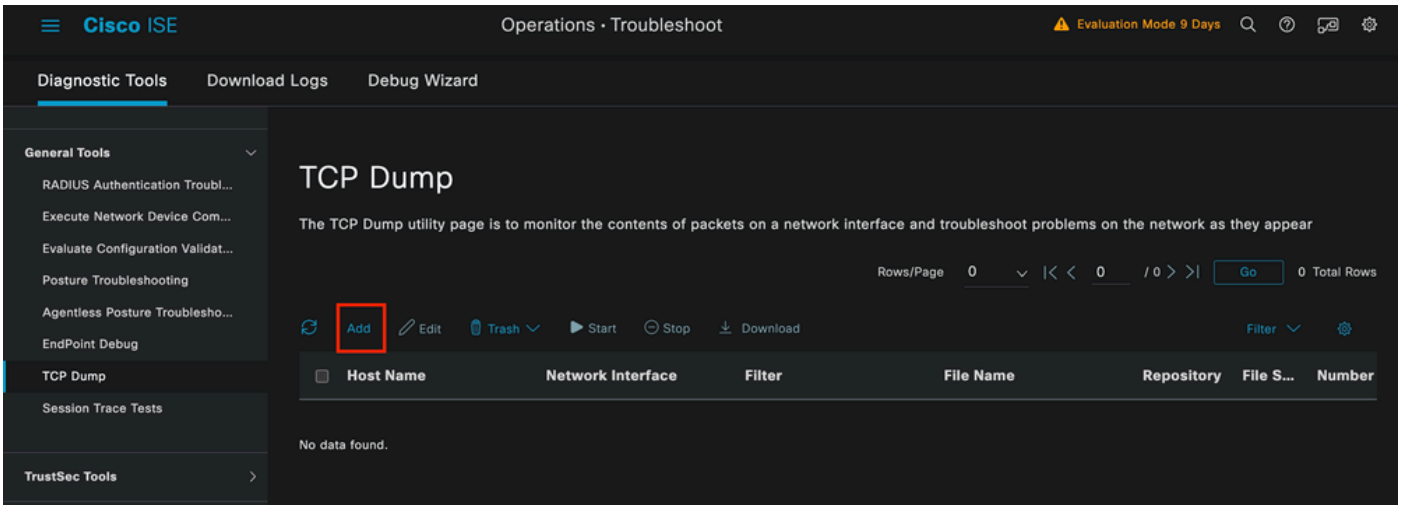


Ergebnisse der Windows-Suchleiste

3 - ISE TCP-Dump-Tool (Paketerfassung)

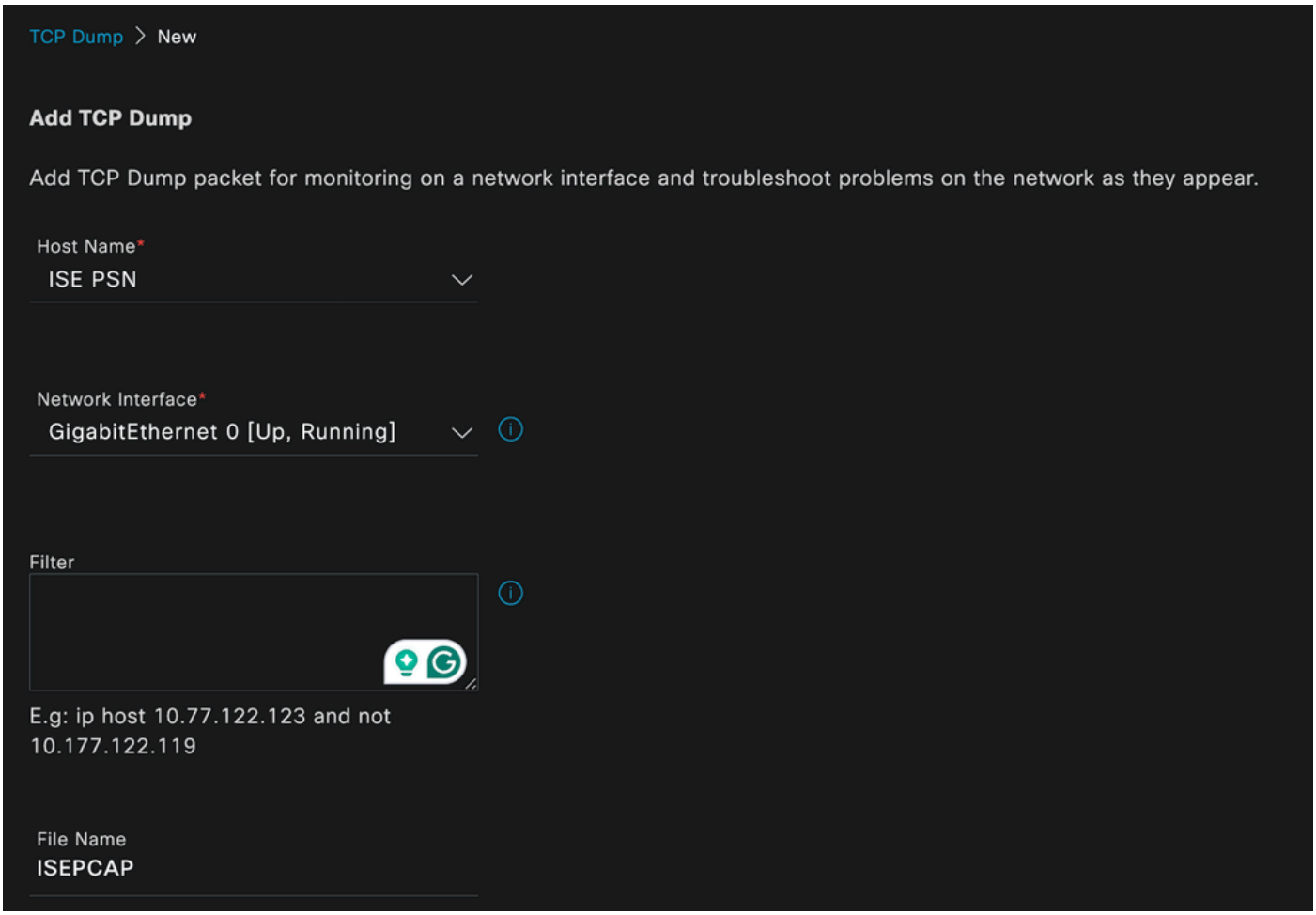
Bei der Fehlerbehebung ist eine Paketerfassungsanalyse unerlässlich. Direkt von der ISE können Paketerfassungen auf allen Knoten und jeder Schnittstelle der Knoten übernommen werden.

Um auf dieses Tool zuzugreifen, navigieren Sie zu Operations > Diagnostic Tools > General Tools > TCP Dump.

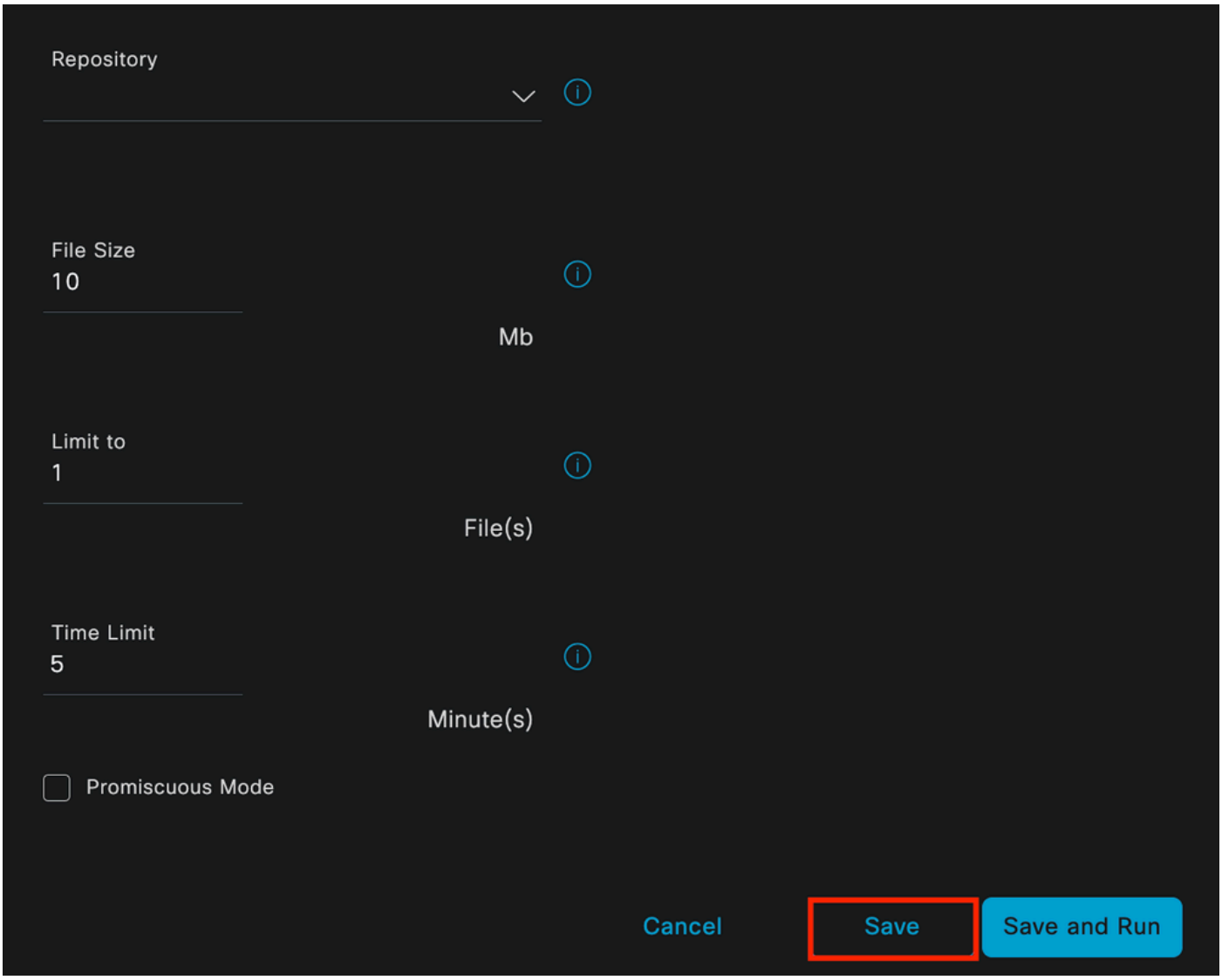


TCP-Dump-Abschnitt

Klicken Sie auf die Schaltfläche Hinzufügen, um die Konfiguration eines pcap-Systems zu starten.



Erstellen eines TCP-Dumps

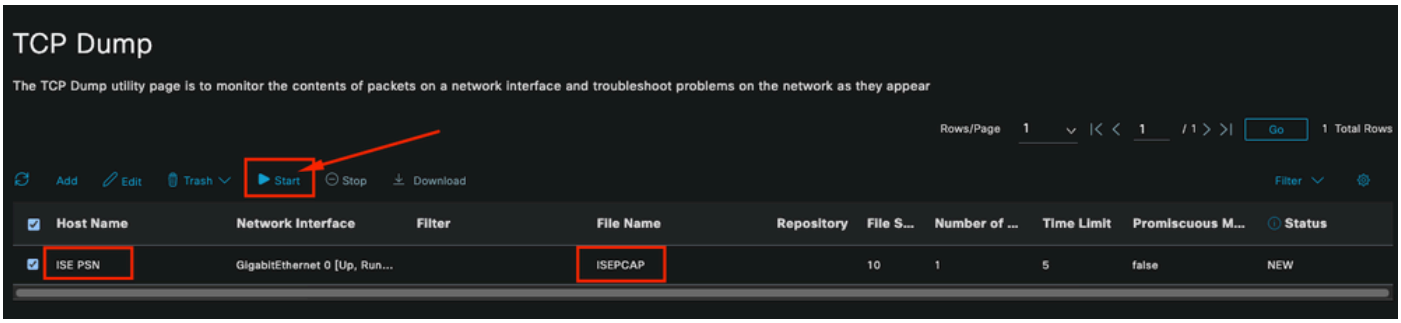


TCP-Dump-Abschnitt

Um eine pcap in der ISE zu erstellen, müssen Sie folgende Daten eingeben:

- Wählen Sie den Knoten aus, an dem Sie pcap verwenden möchten.
- Wählen Sie die ISE-Knotenschnittstelle aus, die für pcap verwendet wird.
- Falls Sie bestimmten Datenverkehr erfassen müssen, verwenden Sie die Filter. Die ISE bietet Ihnen einige Beispiele.
- Nennen Sie die pcap. In diesem Szenario haben wir ISEPCAP verwendet.
- Wählen Sie das Repository aus. Wenn kein Repository ausgewählt ist, wird die Erfassung auf der lokalen ISE-Festplatte gespeichert und kann über die GUI heruntergeladen werden.
- Falls erforderlich, ändern Sie zusätzlich die Größe der pcap-Datei.
- Wenn nötig, mehr als eine Datei verwenden, sodass, wenn die pcap-Datei die Dateigröße überschreitet, eine neue Datei anschließend erstellt wird.
- Verlängern Sie ggf. die Zeit für die Erfassung des Datenverkehrs für die pcap-Lösung.

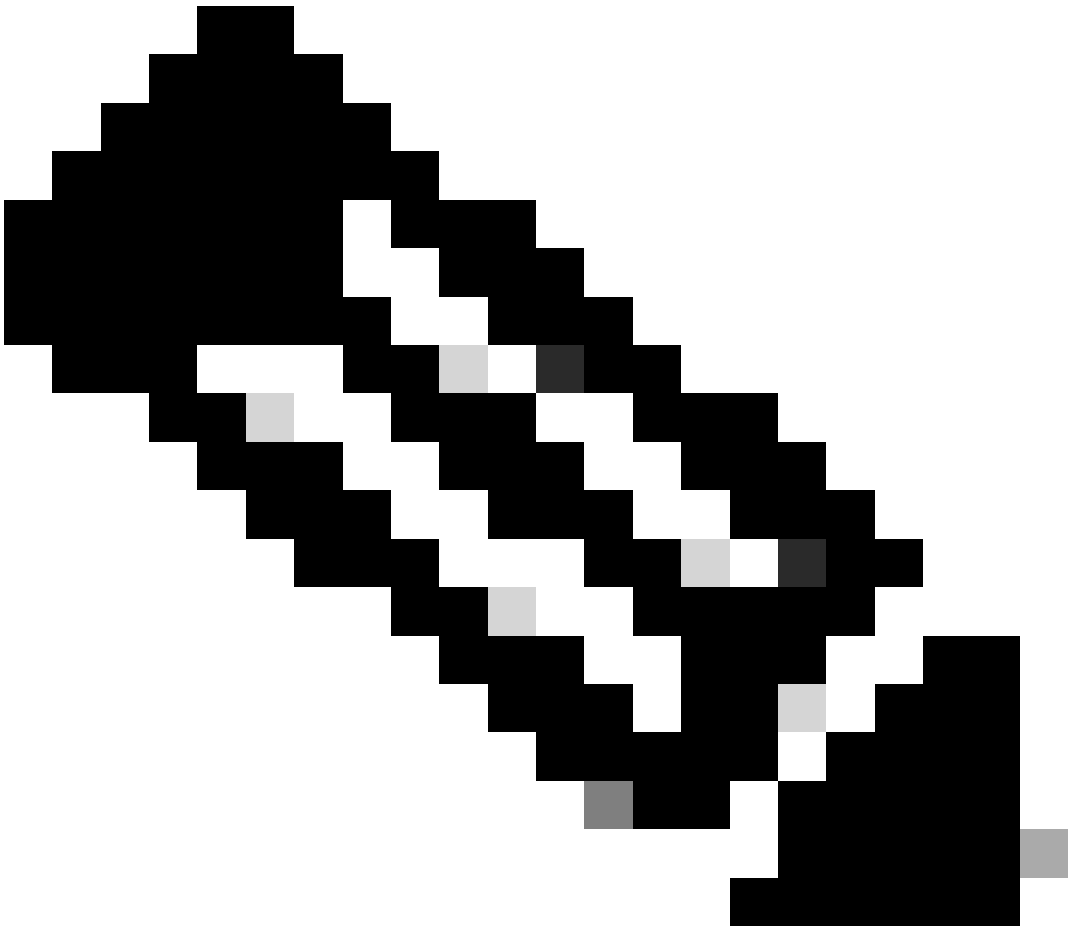
Klicken Sie abschließend auf die Schaltfläche Speichern.



TCP-Dump-Abschnitt

Wählen Sie dann, wenn Sie bereit sind, die pcap, und klicken Sie auf die Start-Taste.

Sobald Sie auf Start klicken, wird die Spalte Status in den Status RUNNING geändert.



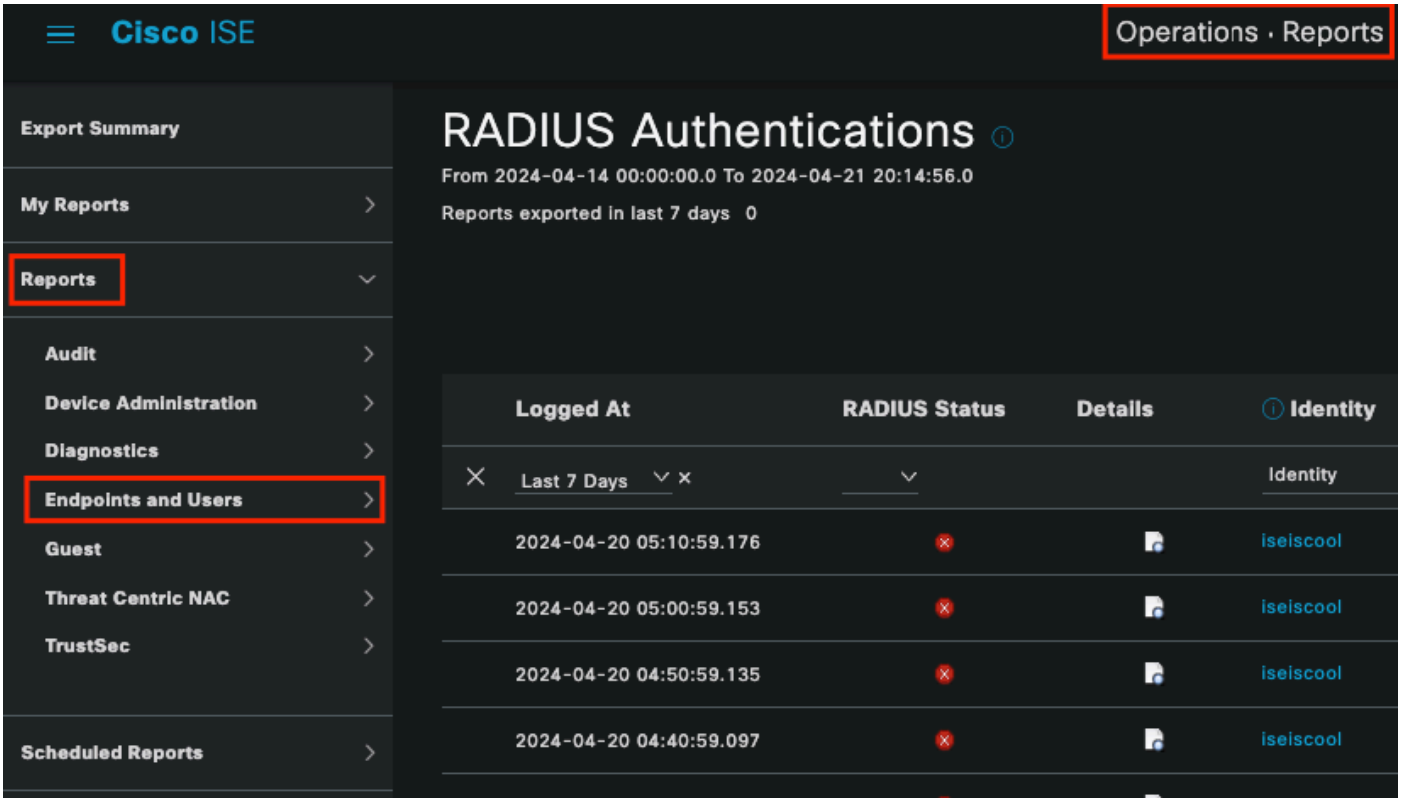
Hinweis: Während PCAP im AUSGEFÜHRTEN Zustand ist, replizieren Sie das Fehlerszenario oder das Verhalten, das Sie erfassen müssen. Nach Abschluss des Gesprächs werden die Details des RADIUS-Gesprächs im PCAP angezeigt.

Sobald die benötigten Daten erfasst wurden, während PCAP ausgeführt wird, beenden Sie die Erfassung von pcap. Wählen Sie es erneut aus, und klicken Sie auf Beenden.

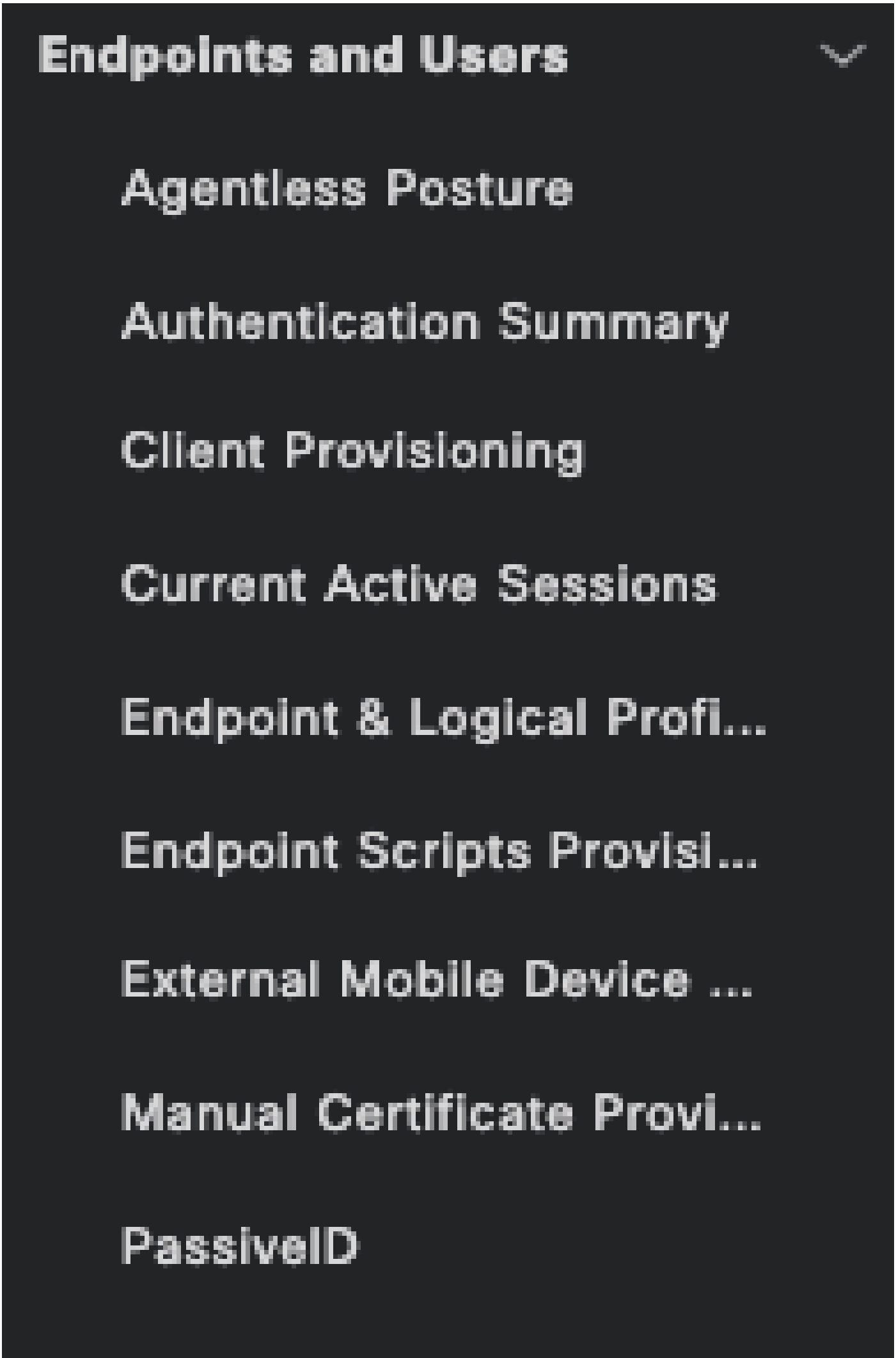
3 - 1 ISE-Berichte

Falls eine tiefere Analyse erforderlich ist, bietet die ISE nützliche Berichte, um vergangene Ereignisse zu untersuchen.

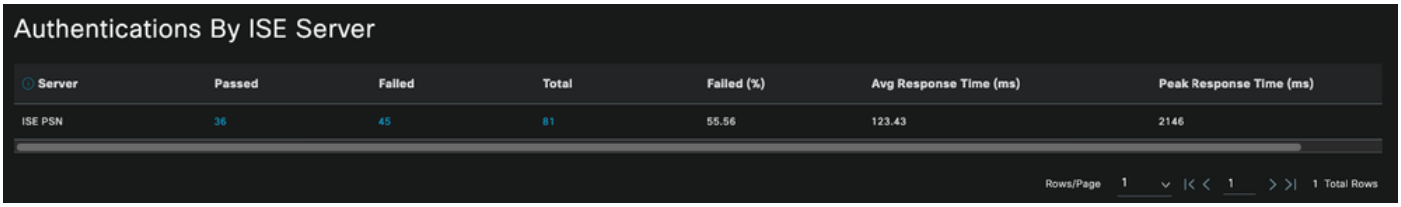
Um sie zu finden, navigieren Sie zu Operations > Reports > Reports > Endpoints and Users



ISE-Berichtsabschnitt


Endpoints and Users
Agentless Posture
Authentication Summary
Client Provisioning
Current Active Sessions
Endpoint & Logical Profi...
Endpoint Scripts Provisi...
External Mobile Device ...
Manual Certificate Provi...
PassiveID

: Bei der in diesem Dokument beschriebenen Bereitstellung wurde nur ein PSN verwendet. Bei größeren Bereitstellungen können Sie anhand dieser Daten jedoch feststellen, ob ein Lastenausgleich erforderlich ist.



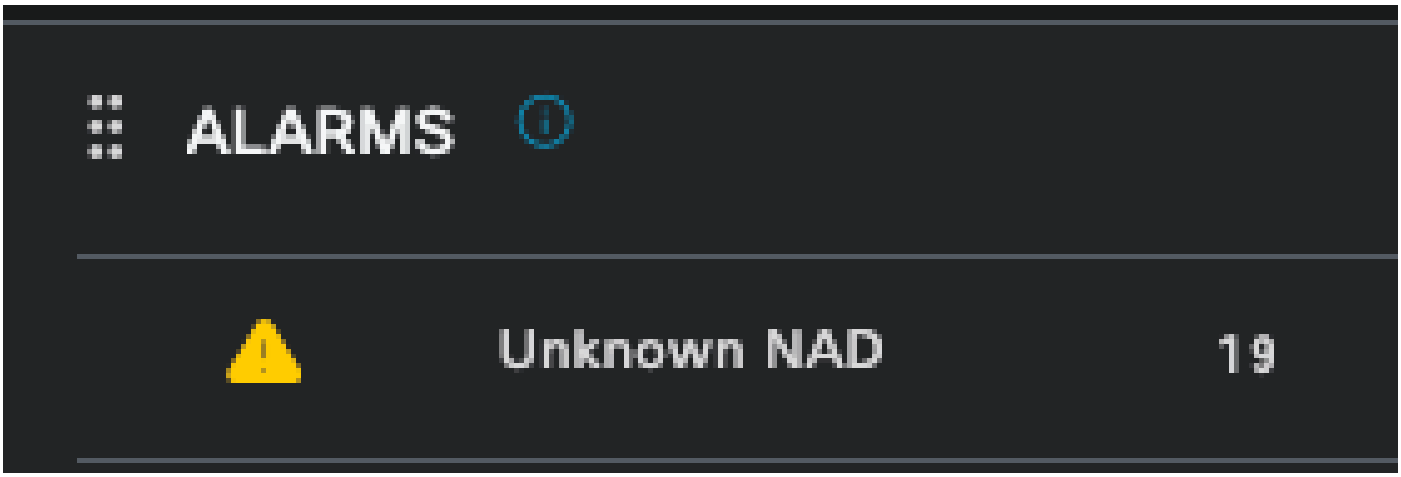
Authentifizierungen durch ISE-Server

4 - ISE-Alarme

Im Abschnitt "Alarme" des ISE-Dashboards werden die Bereitstellungsprobleme angezeigt.

Nachfolgend sind einige ISE-Alarme aufgeführt, die bei der Fehlerbehebung hilfreich sind.

Unknown NAD (Unbekanntes NAD) - Dieser Alarm wird angezeigt, wenn ein Netzwerkgerät einen Endpunkt authentifiziert und sich an die ISE wendet. Die ISE vertraut dem System jedoch nicht, und die RADIUS-Verbindung wird getrennt. Die häufigsten Gründe sind, dass das Netzwerkgerät nicht erstellt wurde oder die vom Netzwerkgerät verwendete IP nicht mit der ISE-registrierten IP-Adresse übereinstimmt.

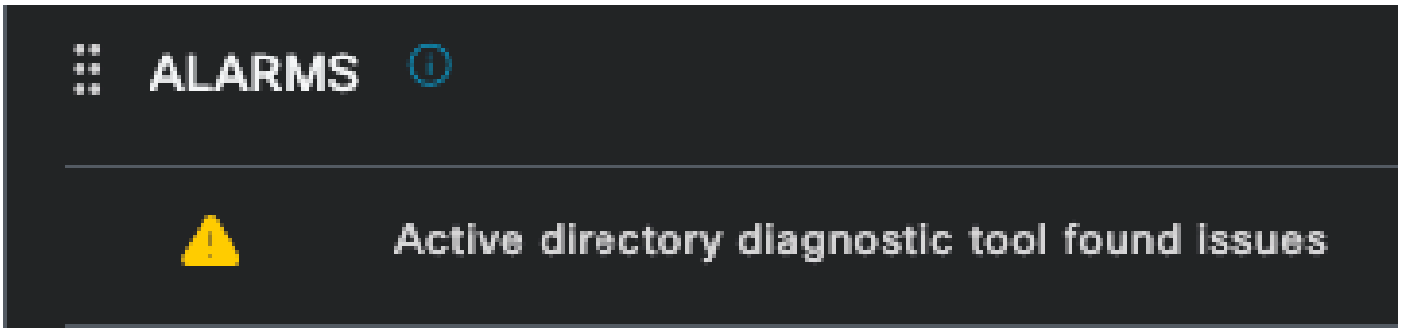


Unbekanntes NAD

Supplicant Stopped Responding (Antwort für angehaltene Supplicants) - Dieser Alarm tritt auf, wenn ein Problem mit der Kommunikation der Supplicants vorliegt. Die meiste Zeit ist er auf eine fehlerhafte Konfiguration in der Supplicant zurückzuführen, die auf der Endpunktseite überprüft und untersucht werden muss.

Supplicant reagiert nicht mehr

Das Active Directory-Diagnosetool hat Probleme gefunden - Wenn Active Directory zur Überprüfung der Benutzeridentität verwendet wird, wenn Probleme mit dem Kommunikationsprozess auftreten oder die Verbindung unterbrochen ist, wird dieser Alarm angezeigt. Dann würden Sie erkennen, warum die Authentifizierungen, dass die Identität auf dem AD existiert, fehlschlagen.



AD-Diagnose fehlgeschlagen

COA (Change of Authorization, Autorisierungsänderung) fehlgeschlagen - Mehrere Flows in der ISE verwenden CoA. Dieser Alarm informiert Sie, wenn während der CoA-Port-Kommunikation mit einem Netzwerkgerät Probleme aufgetreten sind.

COA fehlgeschlagen

5 - ISE-Debugkonfiguration und Protokollsammlung

Um mit den Authentifizierungsprozessdetails fortzufahren, müssen Sie die nächsten Komponenten in DEBUG für MAB- und Dot1x-Probleme aktivieren:

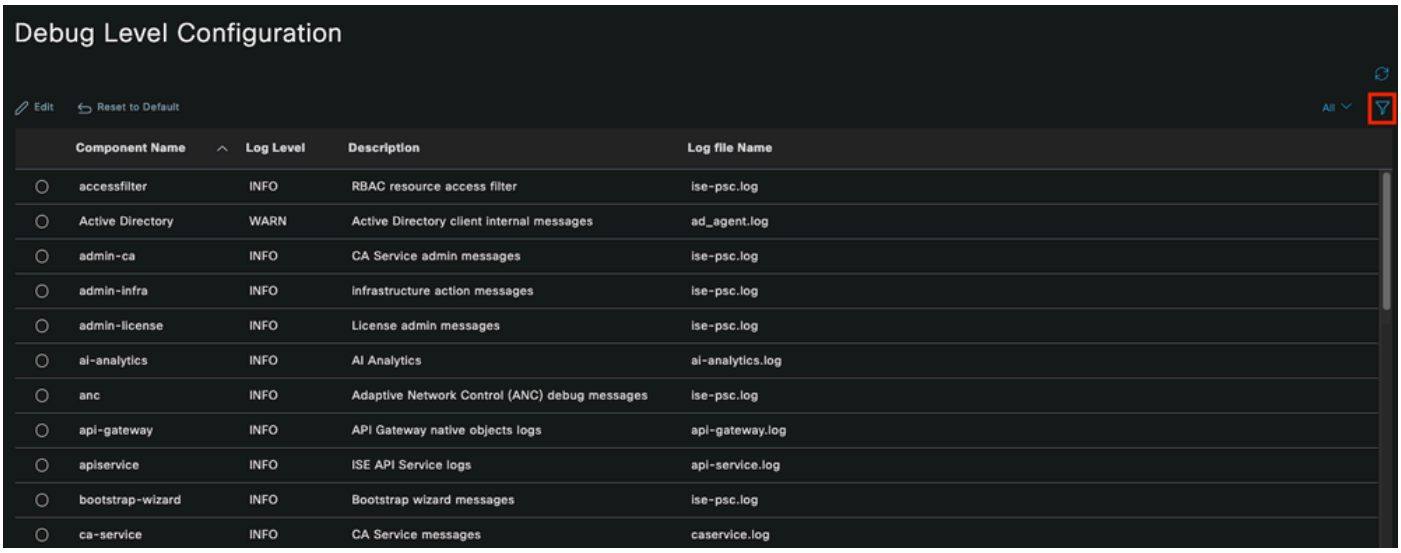
Problem: dot1x/mab

Attribute, die auf die Debugstufe festgelegt werden sollen.

- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

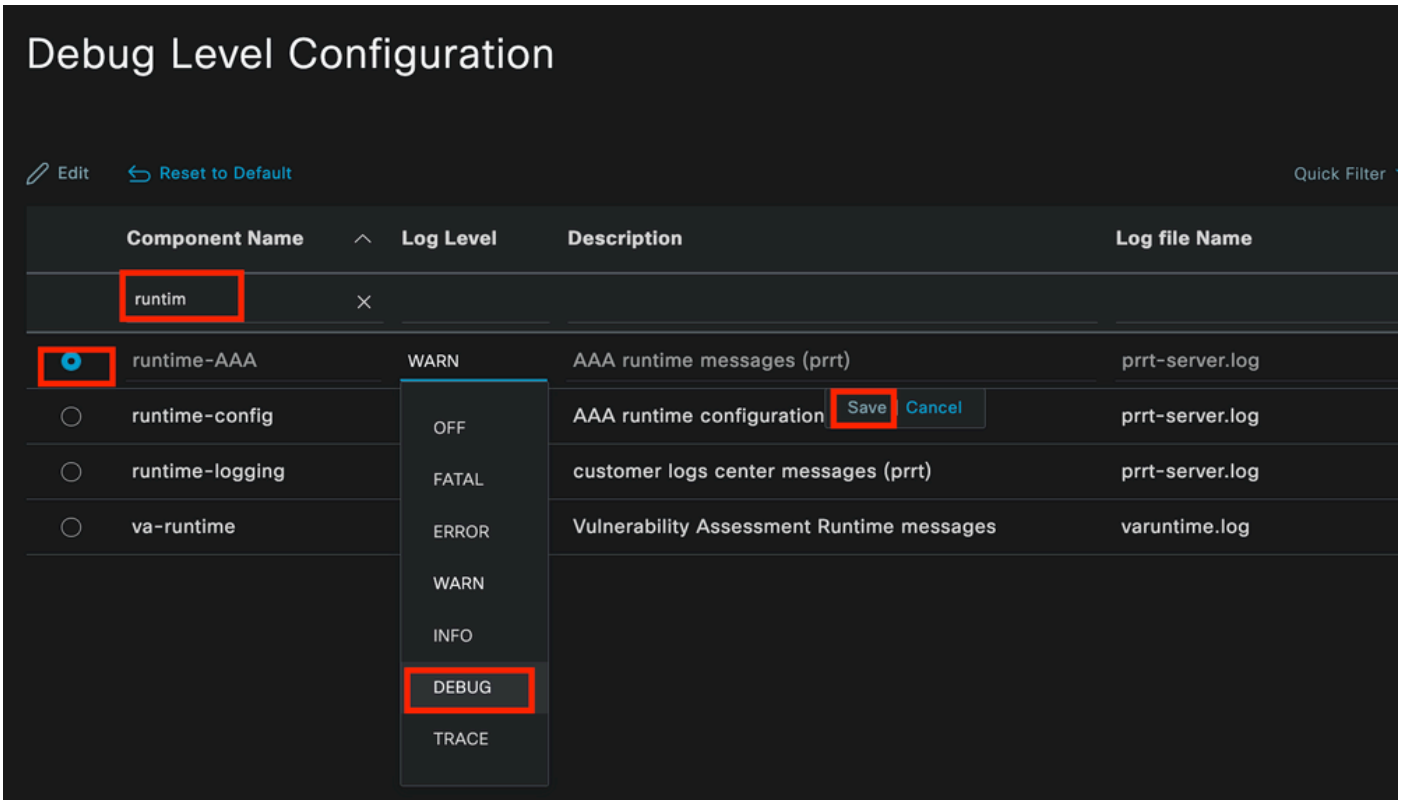
Damit die Komponenten die DEBUG-Ebene erreichen, muss zuerst ermittelt werden, welches das PSN ist, das die fehlgeschlagene oder zu untersuchende Authentifizierung erhält. Sie können diese Informationen aus den Live-Protokollen abrufen. Danach müssen Sie zum ISE-Menü gehen > Troubleshoot > Debug Wizard > Debug Log Configuration > Select the PSN > Click the Edit Button.

Das nächste Menü wird angezeigt. Klicken Sie auf das Filtersymbol:



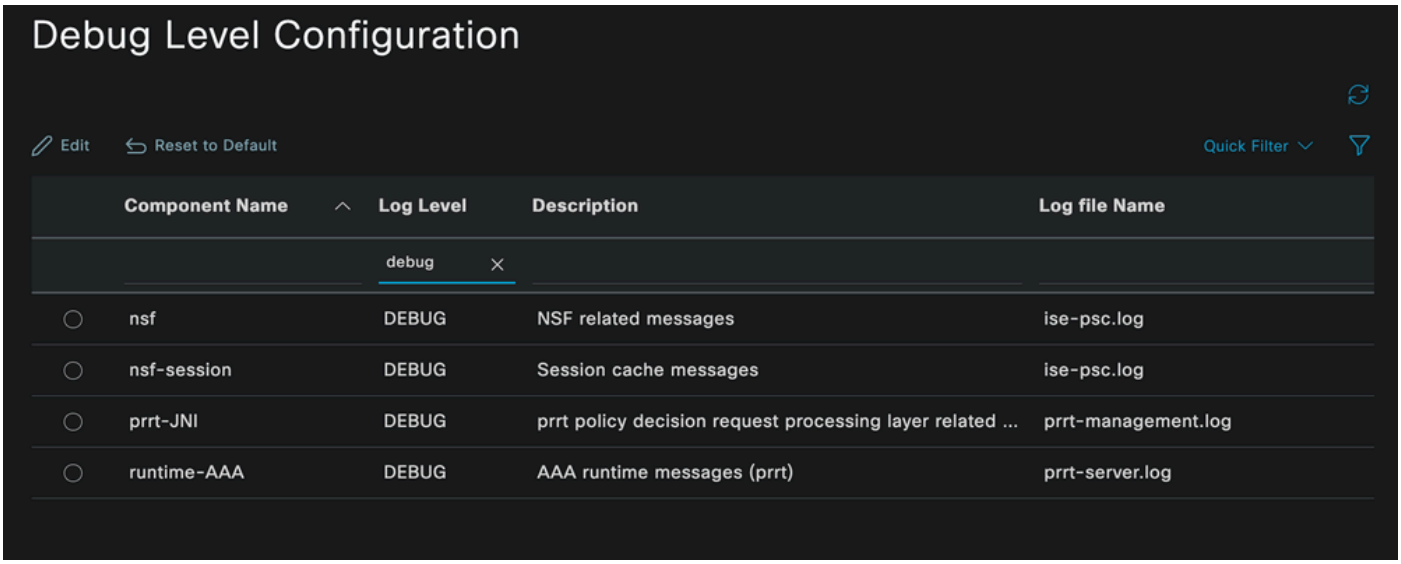
Konfiguration des Debugprotokolls

Suchen Sie in der Spalte Komponentenname nach den zuvor aufgeführten Attributen. Wählen Sie die einzelnen Protokollstufen aus, und ändern Sie sie in DEBUG. Speichern Sie die Änderungen.



Einrichtung der Laufzeit-AAA-Komponente

Wenn Sie alle Komponenten fertig konfiguriert haben, filtern Sie sie mit DEBUG, damit Sie sehen können, ob alle Komponenten korrekt konfiguriert wurden.

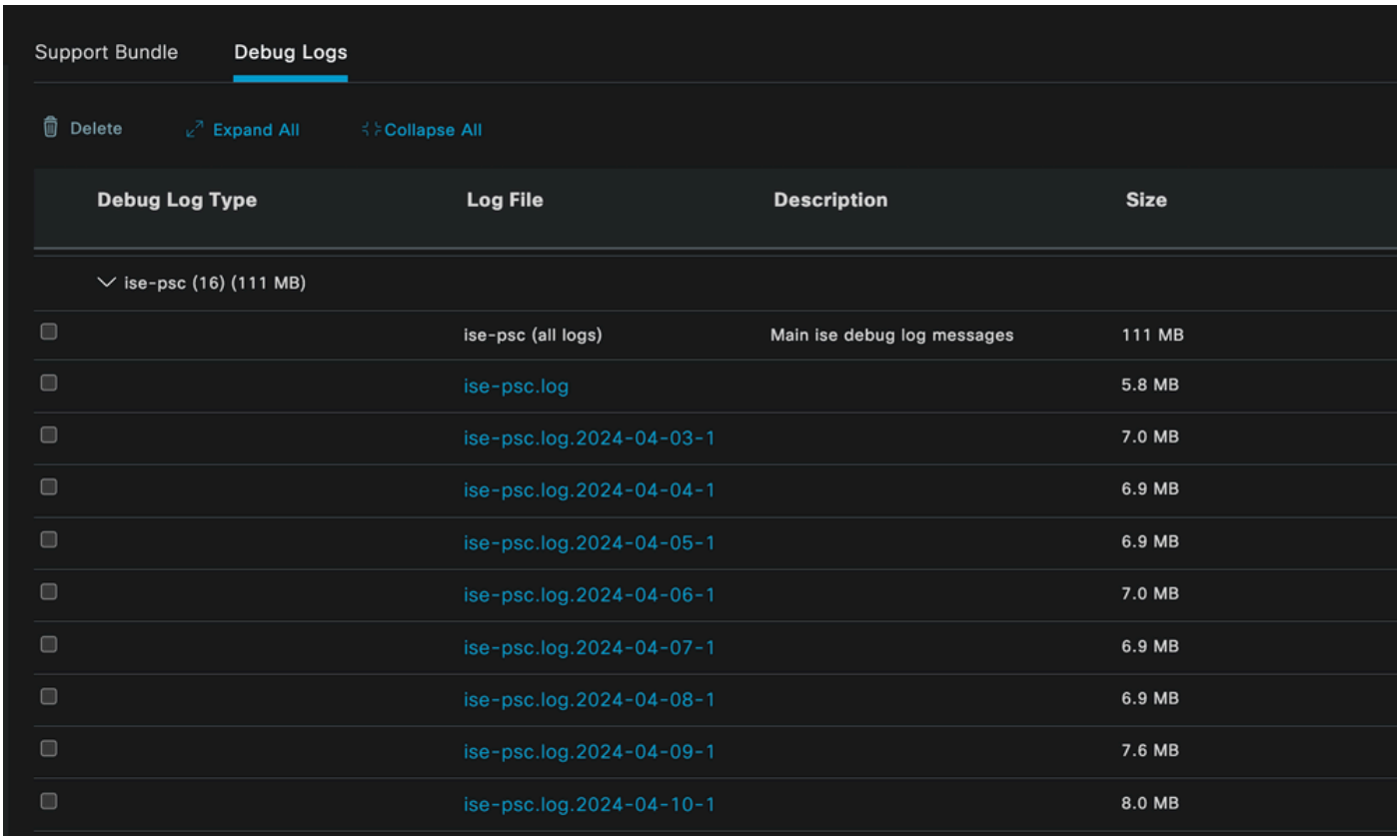


Konfiguration des Debugprotokolls

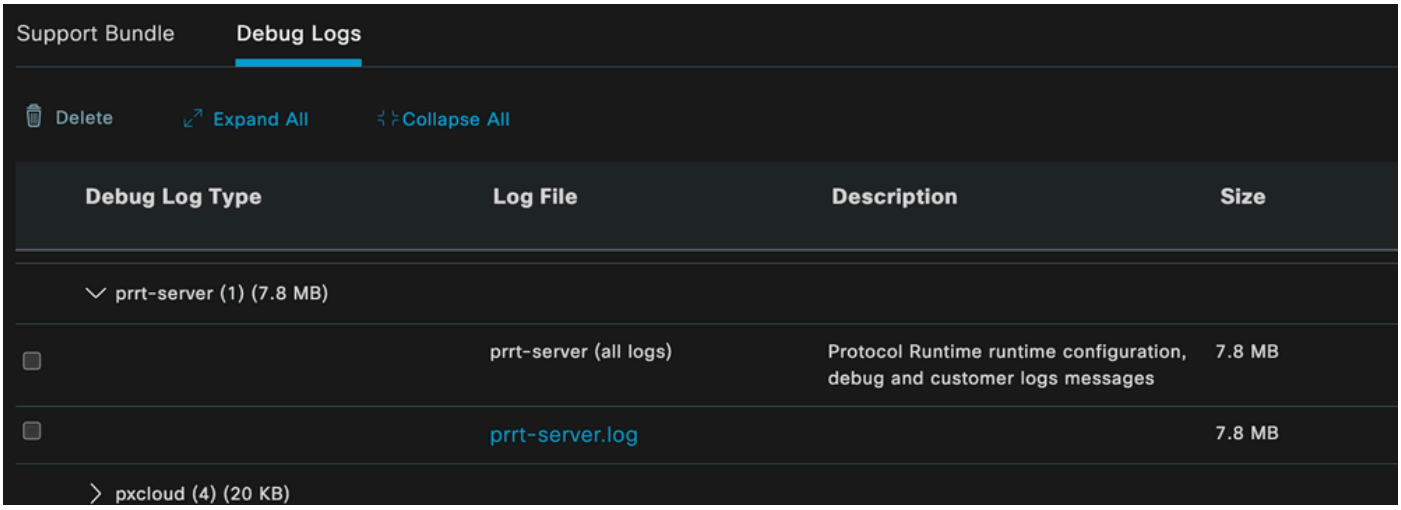
Falls die Protokolle sofort analysiert werden müssen, können Sie sie herunterladen, indem Sie zum Pfad ISE-Menü > Operationen > Fehlerbehebung > Download-Protokolle > Appliance-Knotenliste > PSN navigieren und DEBUGS > Debug-Protokolle aktivieren.

In diesem Fall müssen Sie für dot1x- und mab-Probleme die Dateien prrt-server.log und ise-psc.log herunterladen. Das Protokoll, das Sie herunterladen müssen, ist das Protokoll mit dem Datum Ihres letzten Tests.

Klicken Sie einfach auf die Protokolldatei in diesem Bild und laden Sie sie herunter (in blauer Schrift dargestellt).



Debug-Protokolle vom PSN-Knoten

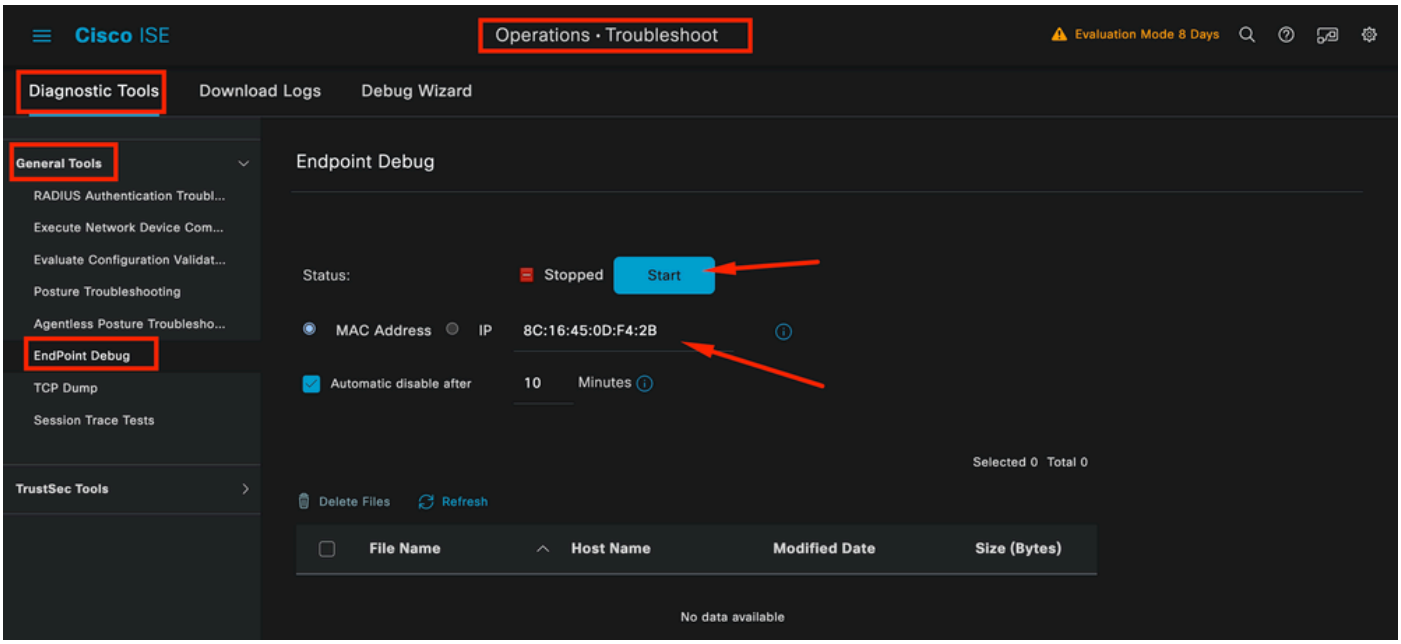


Abschnitt Debug-Protokolle

6 - ISE per Endpoint-Fehlerbehebung

Es gibt auch eine andere Option zum Abrufen von DEBUG-Protokollen, die auf Endpunkt-Debug-Protokollen basierend auf MAC-Adresse oder IP-Adresse basieren. Sie können das Endpoint Debug-ISE-Tool verwenden.

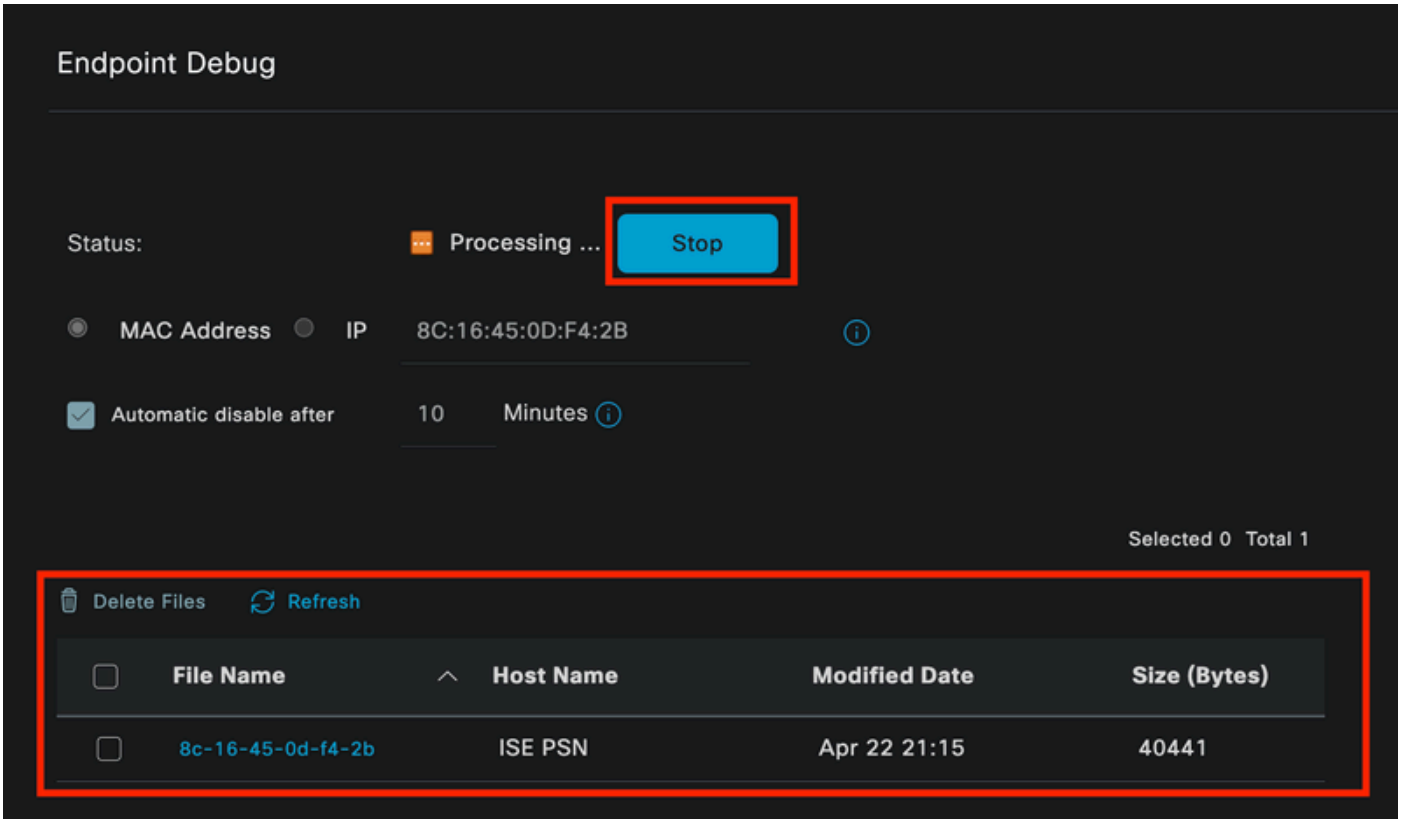
Navigieren Sie zu ISE Menu > Operations > Troubleshoot > Diagnostic Tools > General Tools > Endpoint Debug.



Endpunktdebuggen

Geben Sie dann die gewünschten Endpunktinformationen ein, um mit der Protokollerfassung zu beginnen. Klicken Sie auf Start.

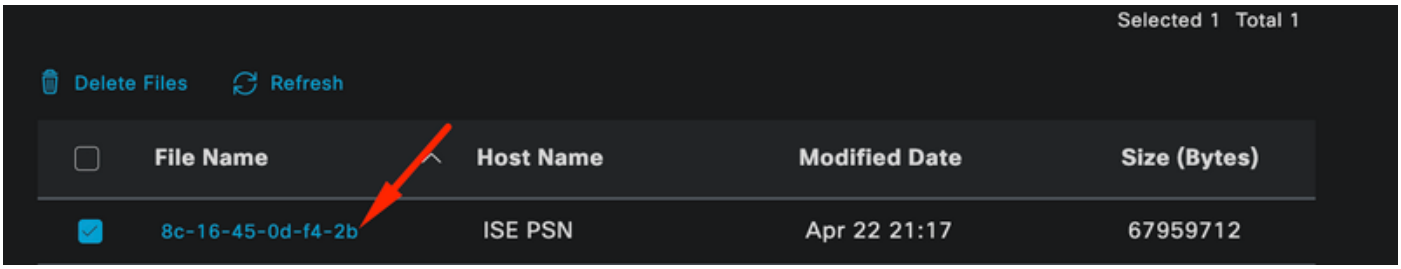
Klicken Sie dann in der Warnmeldung auf Weiter.



Endpunktdebuggen

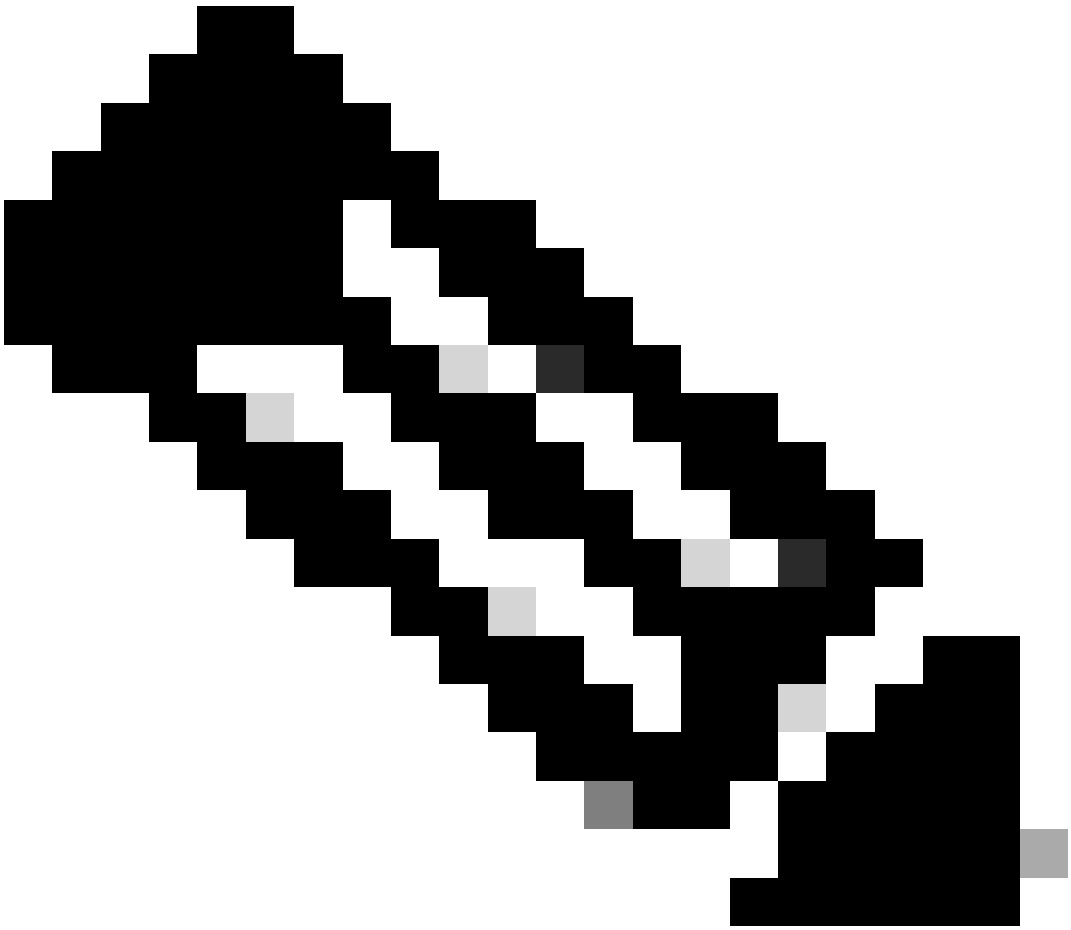
Wenn die Informationen erfasst wurden, klicken Sie auf Beenden.

Klicken Sie in diesem Bild auf den blau dargestellten Dateinamen.



Endpunktdebuggen

Sie müssen die Authentifizierungsprotokolle mit DEBUG-Protokollen anzeigen können, ohne sie direkt aus der Konfiguration des Debug-Protokolls aktivieren zu müssen.

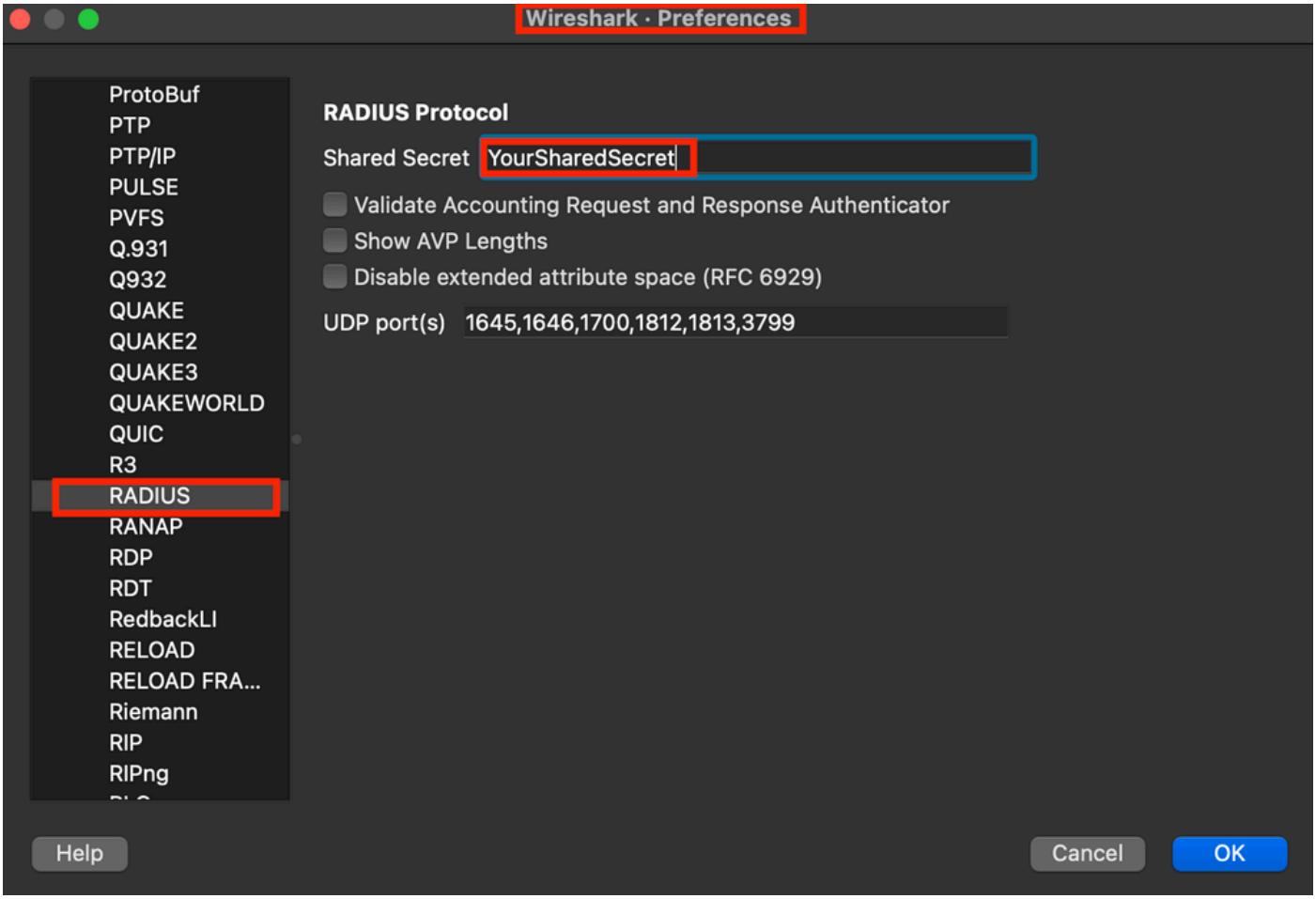


Hinweis: Da in der Endpoint Debug-Ausgabe einige Dinge fehlen könnten, würden Sie eine vollständigere Protokolldatei erhalten, die mit der Debug Log-Konfiguration erstellt und alle erforderlichen Protokolle aus jeder beliebigen Datei heruntergeladen würde, die Sie benötigen. Wie im vorherigen Abschnitt zur ISE-Debugkonfiguration und -Protokollsammlung erläutert.

---

7 - Entschlüsseln von RADIUS-Paketen

Radius-Pakete werden mit Ausnahme des Felds für das Benutzerkennwort nicht verschlüsselt. Sie müssen jedoch das gesendete Kennwort überprüfen. Sie können das vom Benutzer gesendete Paket anzeigen, indem Sie zu Wireshark > Preferences > Protocols > RADIUS navigieren und dann den von der ISE und dem Netzwerkgerät verwendeten gemeinsamen RADIUS-Schlüssel hinzufügen. Danach werden die RADIUS-Pakete entschlüsselt angezeigt.



Wireshark Radius-Optionen

8 - Befehle zur Fehlerbehebung bei Netzwerkgeräten

Der nächste Befehl dient zur Behebung von Problemen mit dem ISR 1100 oder kabelgebundenen NAD-Gerät.

8 - 1 Um festzustellen, ob der AAA-Server oder die ISE vom Netzwerkgerät aus erreichbar ist, verwenden Sie show aaaa servers.

```
Router>show aaa servers

RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname
     State: current UP, duration 2876s, previous duration 0s
     Dead: total time 0s, count 0

     Platform State from SMD: current UP, duration 2876s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
```

```
Platform State from WNCD (1) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (2) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (3) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (4) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (5) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (6) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (7) : current UP, duration 3015s, previous duration 0s
Platform State from WNCD (8) : current UP, duration 3015s, previous duration 0s

WNCD Platform Dead: total time 0s, count 0UP

Quarantined: No

Authen: request 11, timeouts 0, failover 0, retransmission 0

        Response: accept 1, reject 0, challenge 10
        Response: unexpected 0, server error 0, incorrect 0, time 33ms
        Transaction: success 11, failure 0
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        Dot1x transactions:

        Response: total responses: 11, avg response time: 33ms
        Transaction: timeouts 0, failover 0
        Transaction: total 1, success 1, failure 0

        MAC auth transactions:
        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0

        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        MAC author transactions:

        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3
        Request: start 1, interim 0, stop 0
        Response: start 1, interim 0, stop 0

        Response: unexpected 0, server error 0, incorrect 0, time 27ms
        Transaction: success 2, failure 1
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0

Elapsed time since counters last cleared: 47m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

```
     Consecutive Response Failures: total 0
             SMD Platform : max 0, current 0 total 0
             WNCD Platform: max 0, current 0 total 0
             IOSD Platform : max 0, current 0 total 0

     Consecutive Timeouts: total 3
             SMD Platform : max 0, current 0 total 0
             WNCD Platform: max 0, current 0 total 0
             IOSD Platform : max 3, current 0 total 3

     Requests per minute past 24 hours:
             high - 0 hours, 47 minutes ago: 4
             low  - 0 hours, 45 minutes ago: 0
             average: 0

Router>
```

8-2 Um den Portstatus, Details, die auf die Sitzung angewendeten ACLs, die Authentifizierungsmethode und weitere hilfreiche Informationen anzuzeigen, verwenden Sie den Befehl show authentication sessions interface <Schnittstelle, an der der Laptop angeschlossen ist> Details.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A0000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0


Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Server Policies:


Method status list:
Method State
dot1x Authc Success

Router#
```

8-3 Führen Sie den Befehl show running-config aaa aus, um zu überprüfen, ob alle erforderlichen Befehle für aaa in der globalen Konfiguration vorhanden sind.

```
Router#sh run aaa
!
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 Cisc0123
!
!
radius server COHVSRADISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRADISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#
```

8-4 Ein weiterer nützlicher Befehl ist test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy.

```
Router#test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy
User was successfully authenticated.

Router#
```

9 - Für Netzwerkgeräte relevante Fehlerbehebungen

- debug dot1x all - Zeigt alle dot1x EAP-Meldungen an
- debug aaa authentication - Zeigt Debugging-Authentifizierungsinformationen von AAA-Anwendungen an.
- debug aaa Authorization: Zeigt Debugging-Informationen für die AAA-Autorisierung an.
- debug radius authentication - Bietet detaillierte Informationen zu Aktivitäten auf Protokollebene, nur für die Authentifizierung
- debug radius - Stellt detaillierte Informationen zu Aktivitäten auf Protokollebene bereit

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.