Konfigurieren von sicherem Zugriff für RA-VPNaaS mit Duo SSO und Statusüberprüfung mit der ISE

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der Statusüberprüfung für Remote-Access-VPN-Benutzer mit Identity Service Engine (ISE) und Secure Access mit Duo beschrieben.

Voraussetzungen

- Konfiguration der Benutzerbereitstellung bei sicherem Zugriff
- Duo SSO mit Authentifizierungsproxy oder Drittanbieter-IDP konfigurieren
- Verbindung der Cisco ISE mit Secure Access über den Tunnel

Anforderungen

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

- Identity Service Engine
- Sicherer Zugriff
- Cisco Secure Client
- Guide to Two-Factor Authentication - Duo Security
- ISE-Status
- Authentisierung, Ermächtigung und Buchhaltung

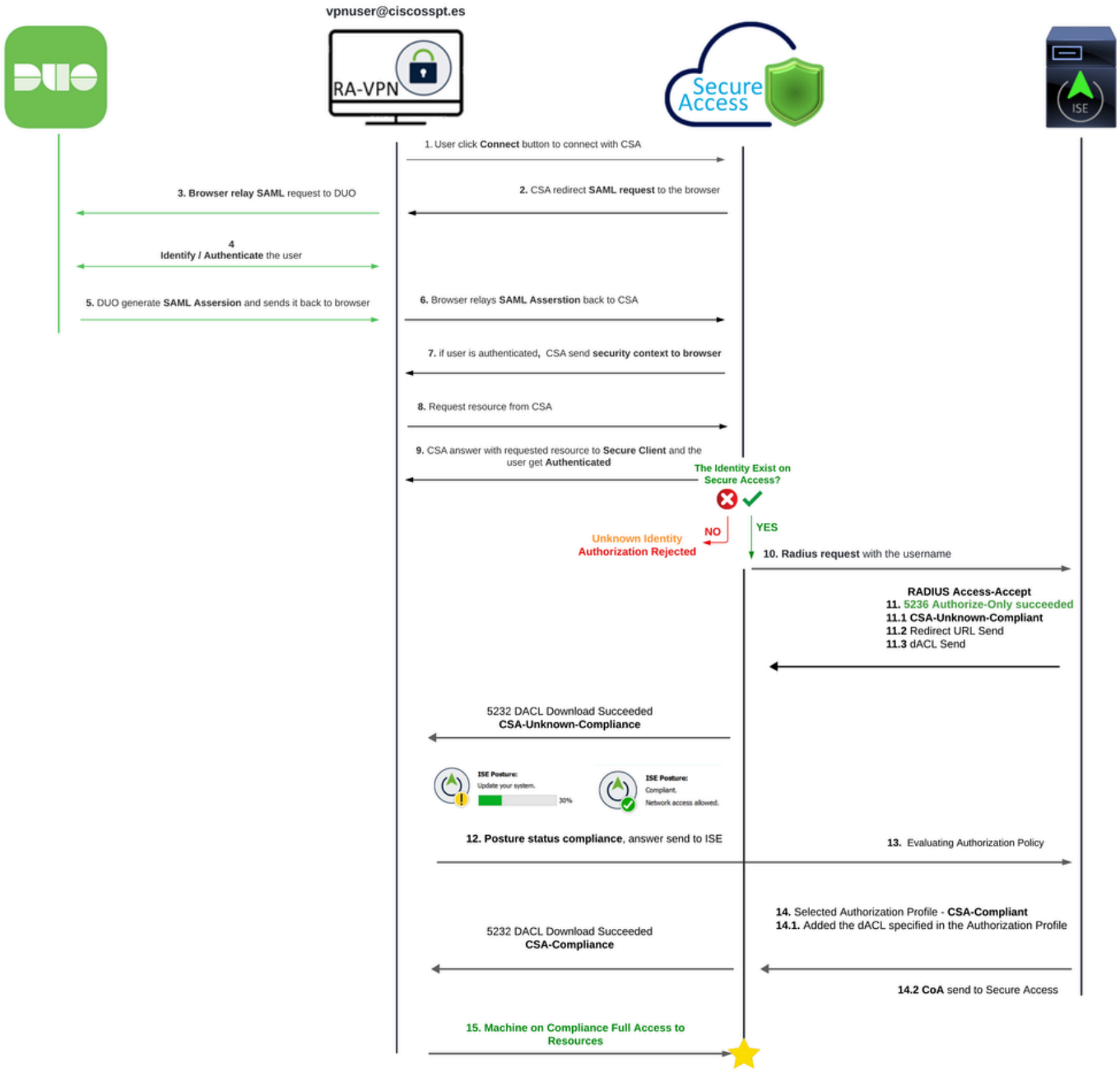
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Identity Service Engine (ISE) Version 3.3 Patch 1
- Sicherer Zugriff
- Cisco Secure Client - AnyConnect VPN Version 5.1.2.42

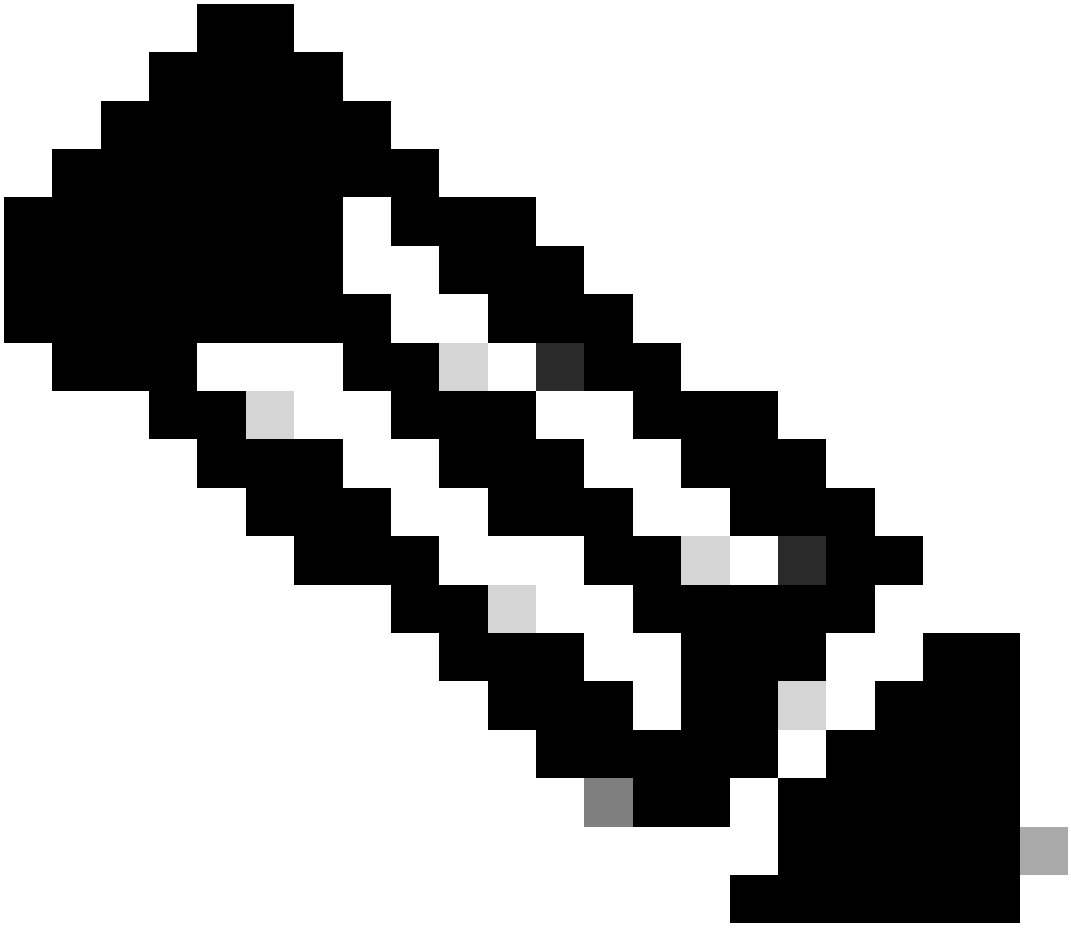
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen



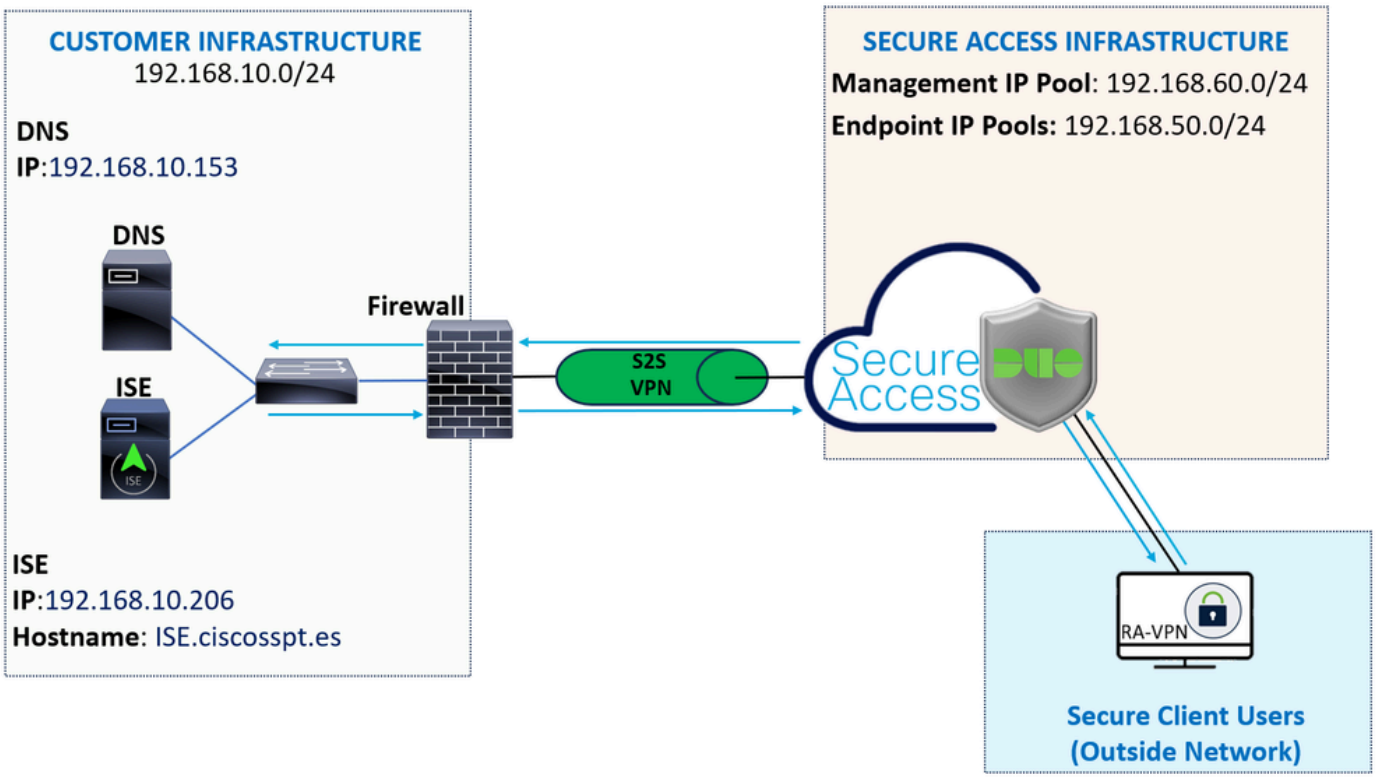
Die Integration von Duo SAML mit der Cisco Identity Services Engine (ISE) verbessert den Authentifizierungsprozess und erweitert die Cisco Secure Access-Lösungen um eine weitere Sicherheitsebene. Duo SAML bietet eine Single Sign-On (SSO)-Funktion, die den Benutzeranmeldeprozess vereinfacht und gleichzeitig hohe Sicherheitsstandards gewährleistet.

Nach der Authentifizierung über Duo SAML wird der Autorisierungsprozess von der Cisco ISE durchgeführt. Dies ermöglicht dynamische Entscheidungen bei der Zugriffskontrolle, die auf der Benutzeridentität und dem Gerätestatus basieren. Die ISE kann detaillierte Richtlinien durchsetzen, die festlegen, auf welche Ressourcen ein Benutzer zugreifen kann, wann und von welchen Geräten.

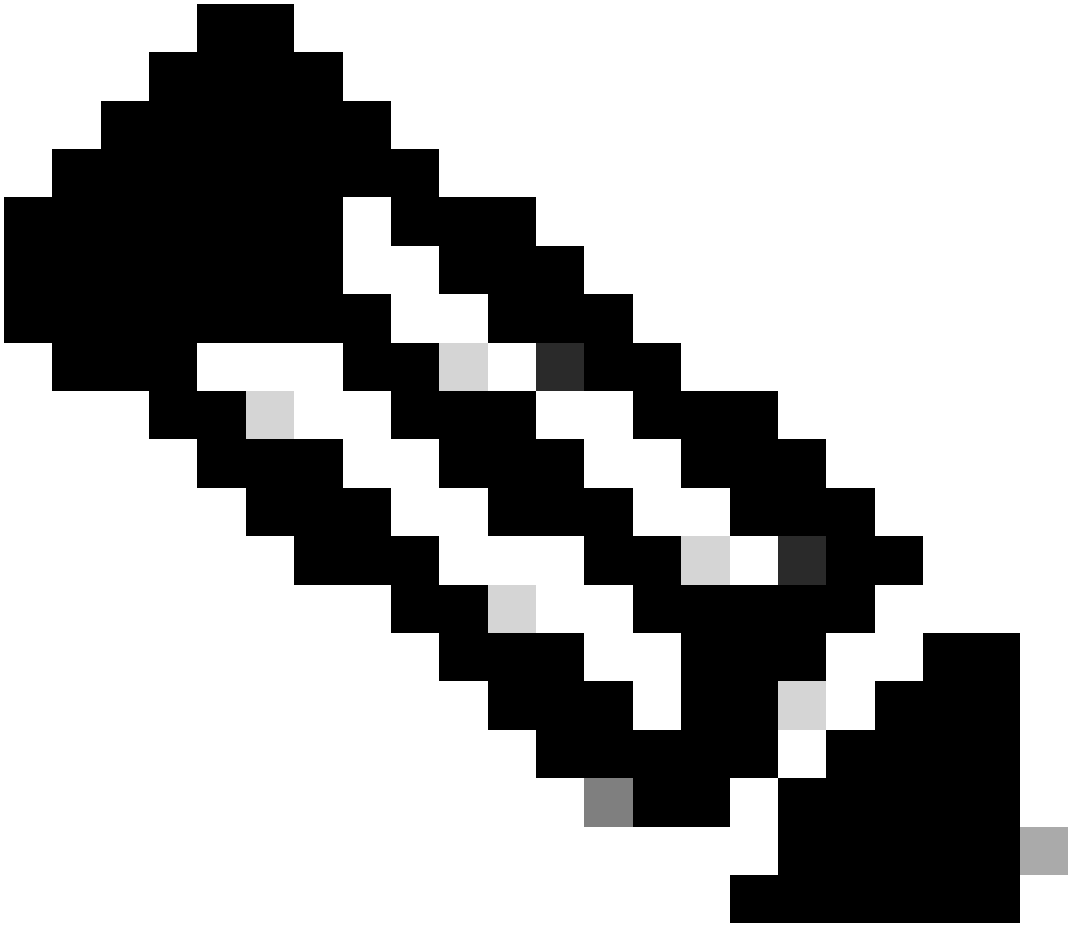


Hinweis: Um die RADIUS-Integration zu konfigurieren, müssen Sie sicherstellen, dass die Kommunikation zwischen beiden Plattformen stattfindet.

Netzwerkdiagramm



Konfigurieren



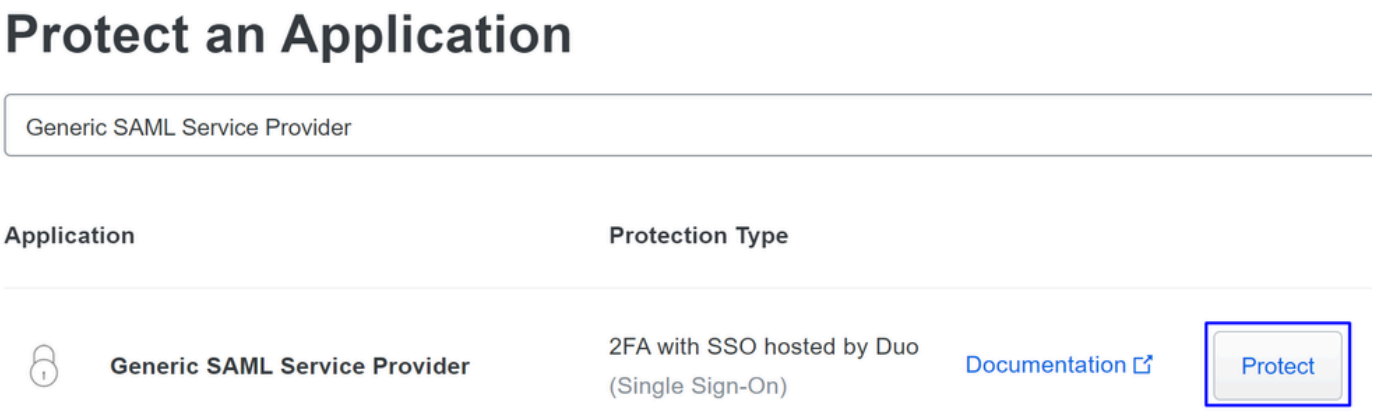
Hinweis: Bevor Sie mit der Konfiguration beginnen, müssen Sie die ersten Schritte mit Secure Access und ISE-Integration durchführen.

Duo Konfiguration

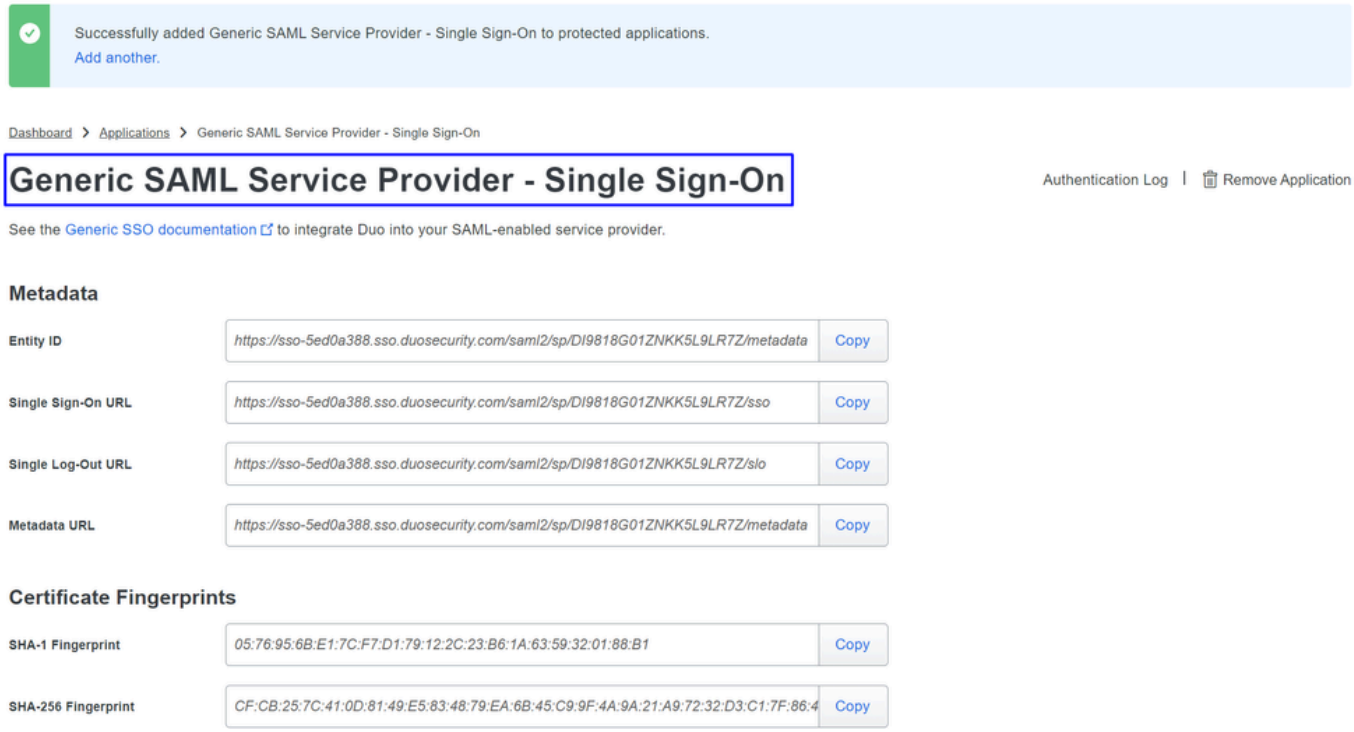
Um die RA-VPN-Anwendung zu konfigurieren, gehen Sie wie folgt vor:

Navigieren Sie zu Ihrem Duo Admin-Bereich.

- Navigieren Sie zu **Applications** > **Protect an Application**
  - Suchen nach **Generic SAML Service Provider**
  - Klicken Sie auf Protect



Die Anwendung muss auf dem Bildschirm angezeigt werden. Merken Sie sich den Anwendungsnamen für die VPN-Konfiguration.



In diesem Fall ist **Generic SAML Service Provider.**

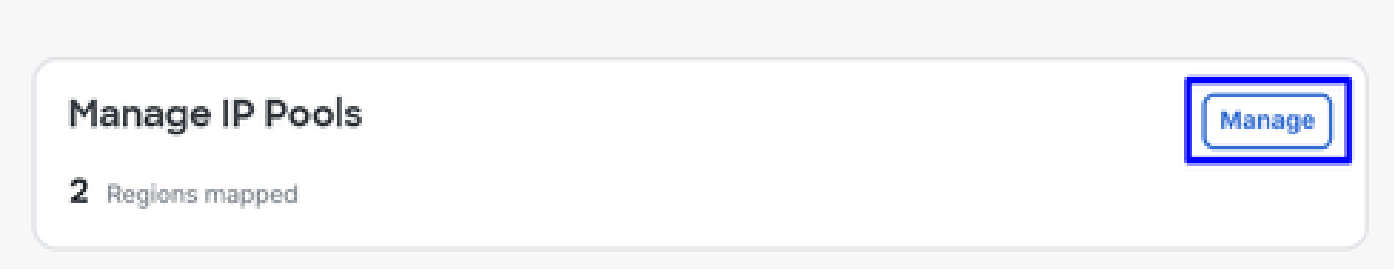
Konfiguration des sicheren Zugriffs

Konfigurieren der Radius-Gruppe auf den IP-Pools

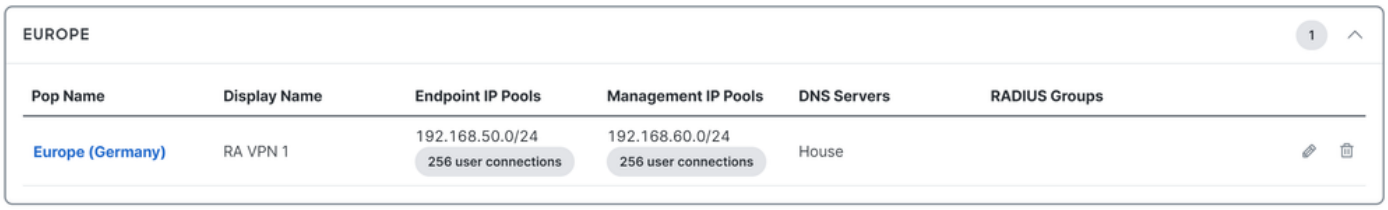
Um das VPN-Profil mit Radius zu konfigurieren, gehen Sie wie folgt vor:

Navigieren Sie zu Ihrem Dashboard für sicheren Zugriff.

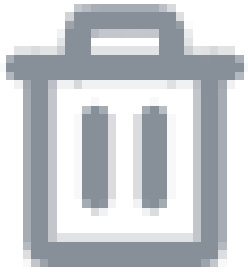
- Klicken Sie **Connect > Enduser Connectivity > Virtual Private Network**
- Klicken Sie unter der Pool-Konfiguration (**Manage IP Pools**) aufManage



- Wählen Sie den **IP Pool Region** und konfigurieren Sie den **Radius Server**

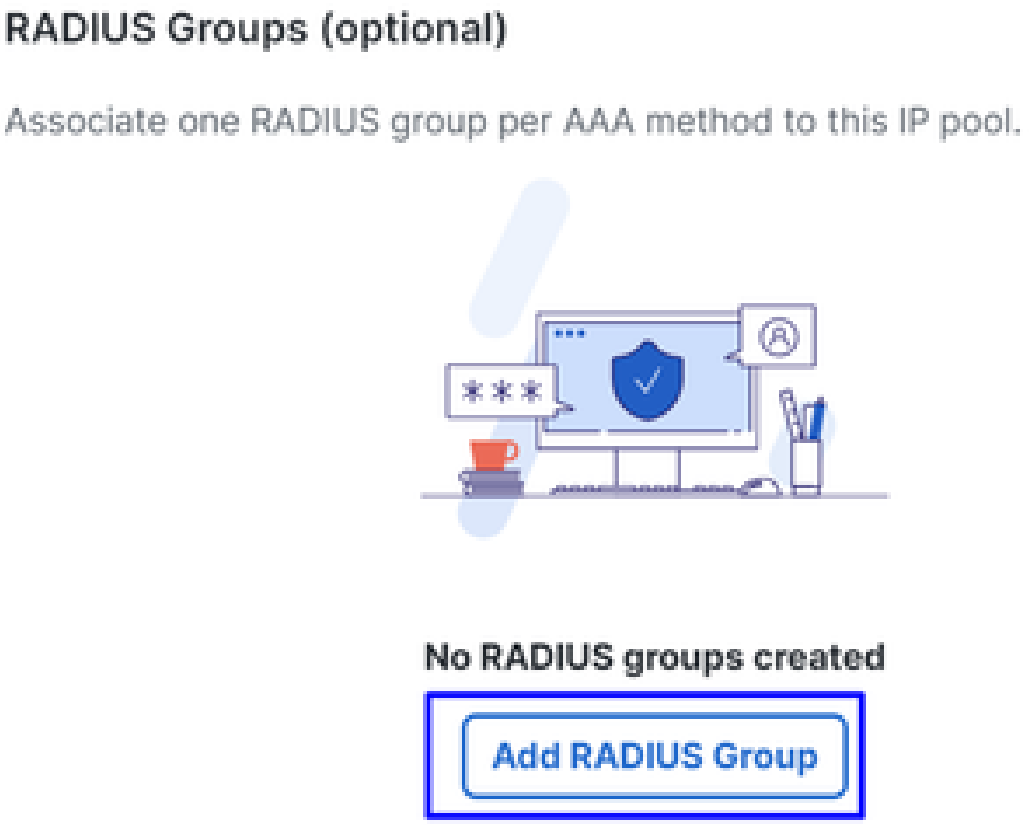


- Zum Bearbeiten auf den Bleistift klicken



- Wählen Sie nun im Dropdown-Menü "Konfiguration" des Abschnitts "IP-Pool" unter **Radius Group (Optional)**

- Klicken Sie auf Add RADIUS Group



← Edit RADIUS Group

Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

Group Name: Konfigurieren Sie einen Namen für Ihre ISE-Integration in Secure Access.

- **AAA method**

  - **Authentication**: Aktivieren Sie das Kontrollkästchen für, **Authentication** und wählen Sie den Port als Standard 1812 aus.

    - Falls Ihre Authentifizierung das Aktivieren des Kontrollkästchens erfordertMicrosoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)

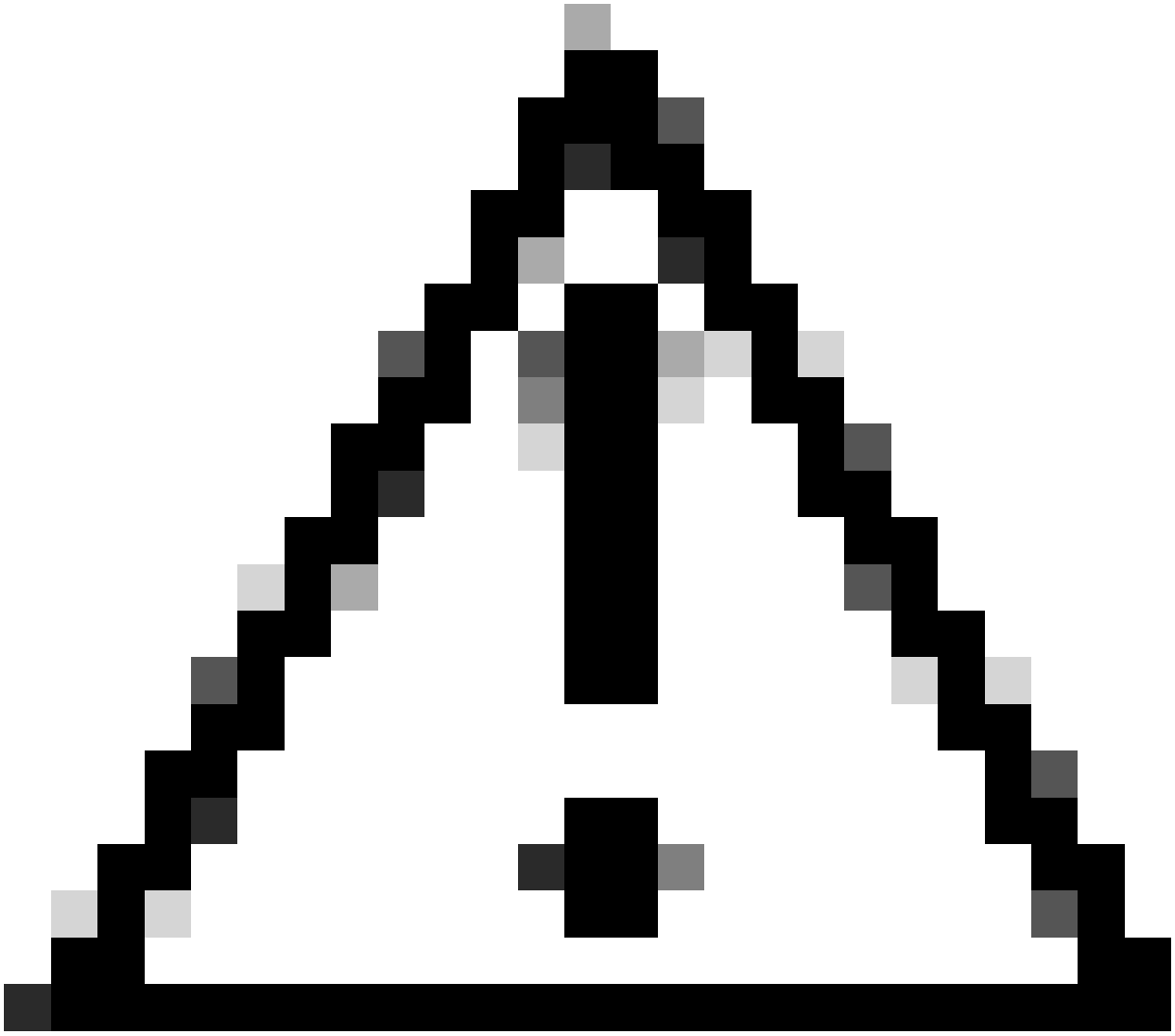
• **Authorization**: Markieren Sie das Kontrollkästchen für Authorization, und wählen Sie den Port als Standardport 1812 aus.

    - Aktivieren Sie das Kontrollkästchen, **Authorization mode Only Change of Authorization (CoA) mode** um den Status und Änderungen von der ISE zuzulassen.

• **Accounting**: Aktivieren Sie das Kontrollkästchen für die Autorisierung, und wählen Sie den Port als Standard 1813 aus.

    - Wählen Sie **Single or Simultaneous** (Im Einzel-Modus werden Buchhaltungsdaten nur an einen Server gesendet. Im Simultanmodus werden Accounting-Daten an alle Server in der Gruppe übertragen.)

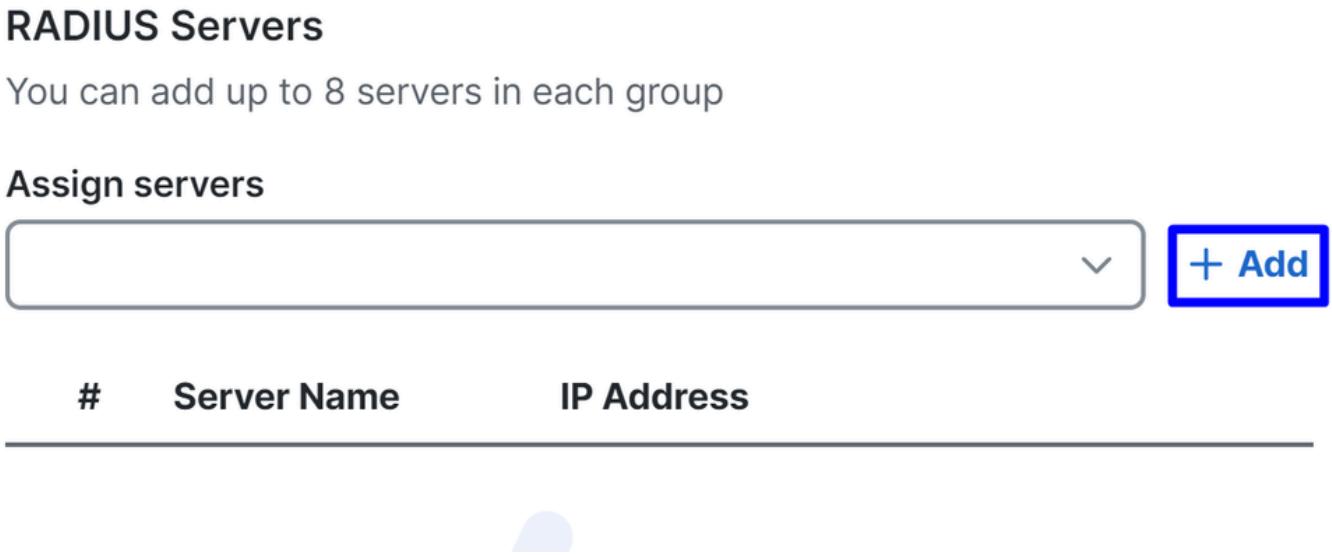
      • Aktivieren Sie das Kontrollkästchen für, **Accounting update** um die regelmäßige Generierung von RADIUS-Nachrichten für die Zwischenabrechnung und Aktualisierung zu aktivieren.



Achtung: Sowohl die Authentication als auch die **Authorization** Methoden müssen, wenn sie ausgewählt sind, denselben Port verwenden.

- Danach müssen Sie die (**RADIUS Servers** ISE) konfigurieren, die für die Authentifizierung über AAA verwendet wird. Siehe Abschnitt **RADIUS Servers**:

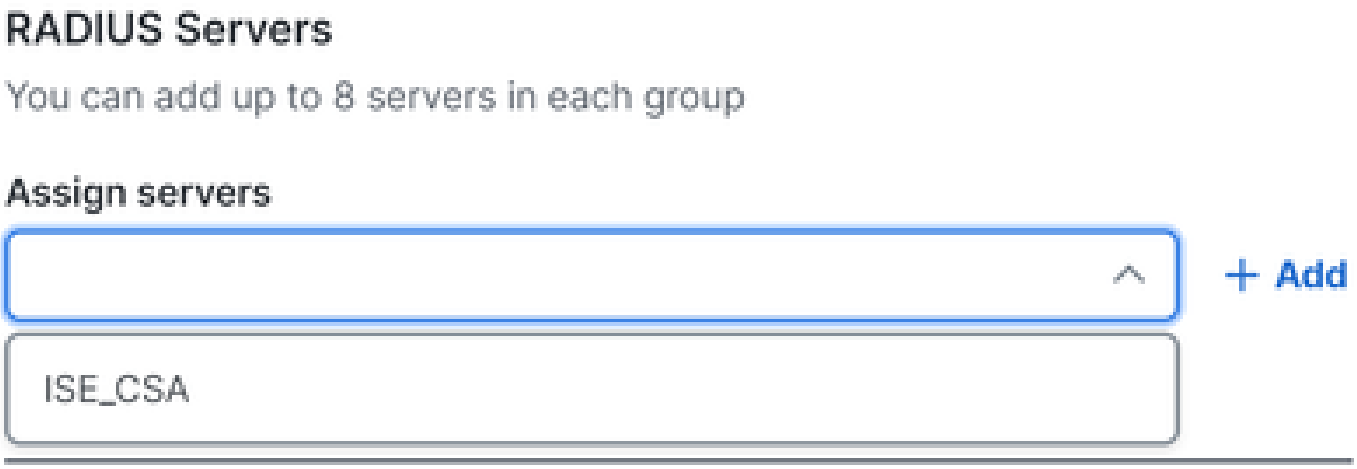
- Klicken Sie + Add



- Konfigurieren Sie dann die nächsten Optionen:

- Server Name: Konfigurieren Sie einen Namen, um Ihren ISE-Server zu identifizieren.
- **IP Address**: Konfigurieren Sie die IP-Adresse Ihres Cisco ISE-Geräts, die über sicheren Zugriff erreichbar ist.
- **Secret Key**: Konfigurieren des geheimen RADIUS-Schlüssels
- **Password**: Konfigurieren Sie Ihr Radius-Kennwort

- Klicken Sie unter der Assign Server Option auf Radius Server, weisen Sie Ihren Radius Server zu **Save** und wählen Sie Ihren ISE Server aus:



- Klicken Sie **Save** erneut, um die gesamte Konfiguration zu speichern.

← Edit RADIUS Group

Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1 hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA

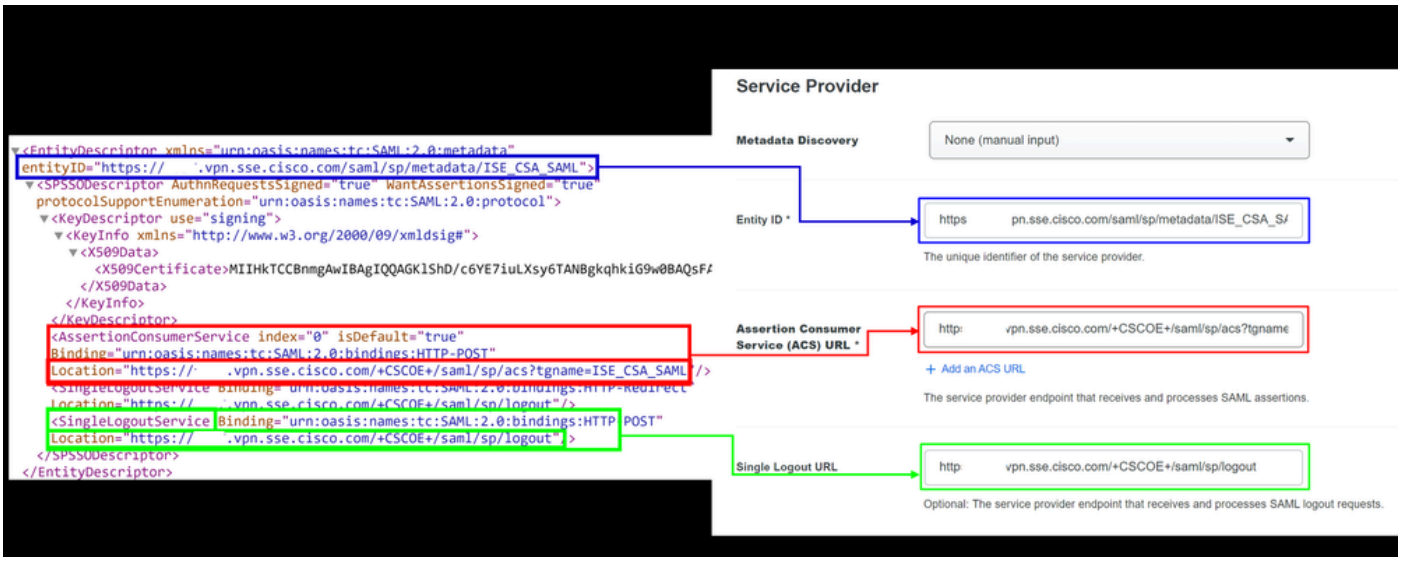
+ Add

#	Server Name	IP Address
1	ISE_CSA	192.168.10.206

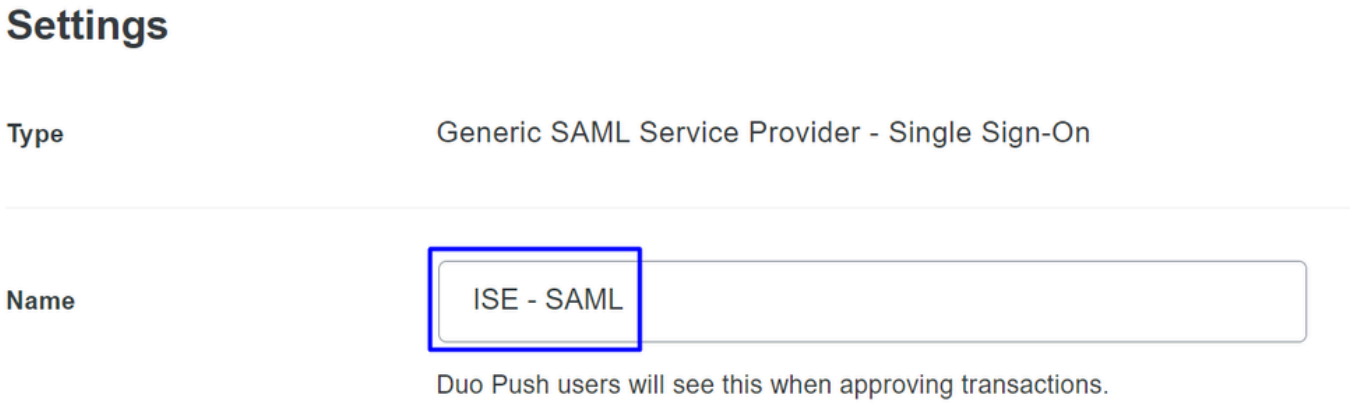
- **Protocols**: Auswahl **SAML**

- Klicken Sie auf Download Service Provider XML file

- Ersetzen Sie die Informationen in der Anwendung, die im Schritt "Duo Configuration" konfiguriert wurde.

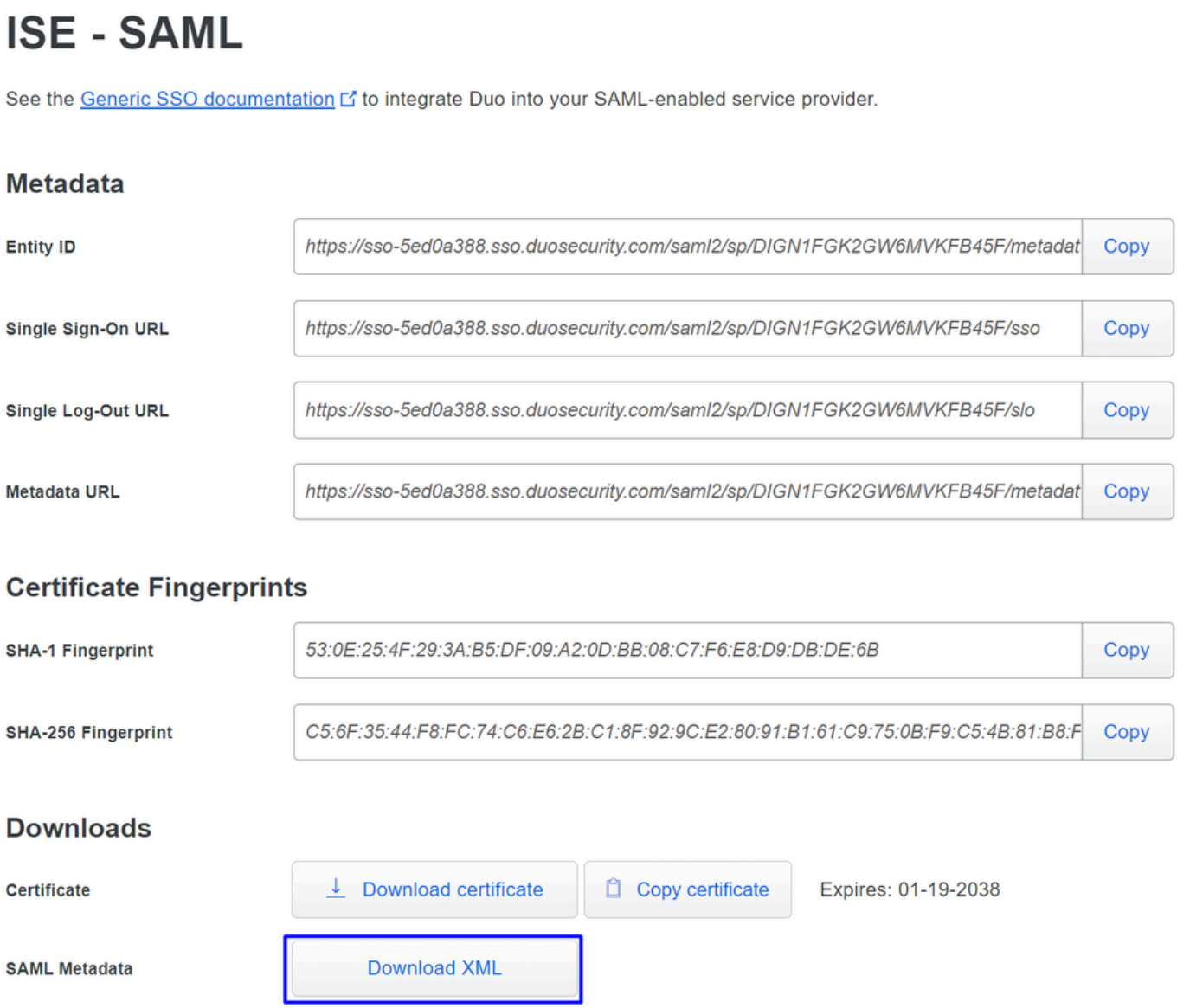


- Nachdem Sie diese Informationen konfiguriert haben, ändern Sie den Namen des Duo in einen Namen, der mit der von Ihnen vorgenommenen Integration zusammenhängt

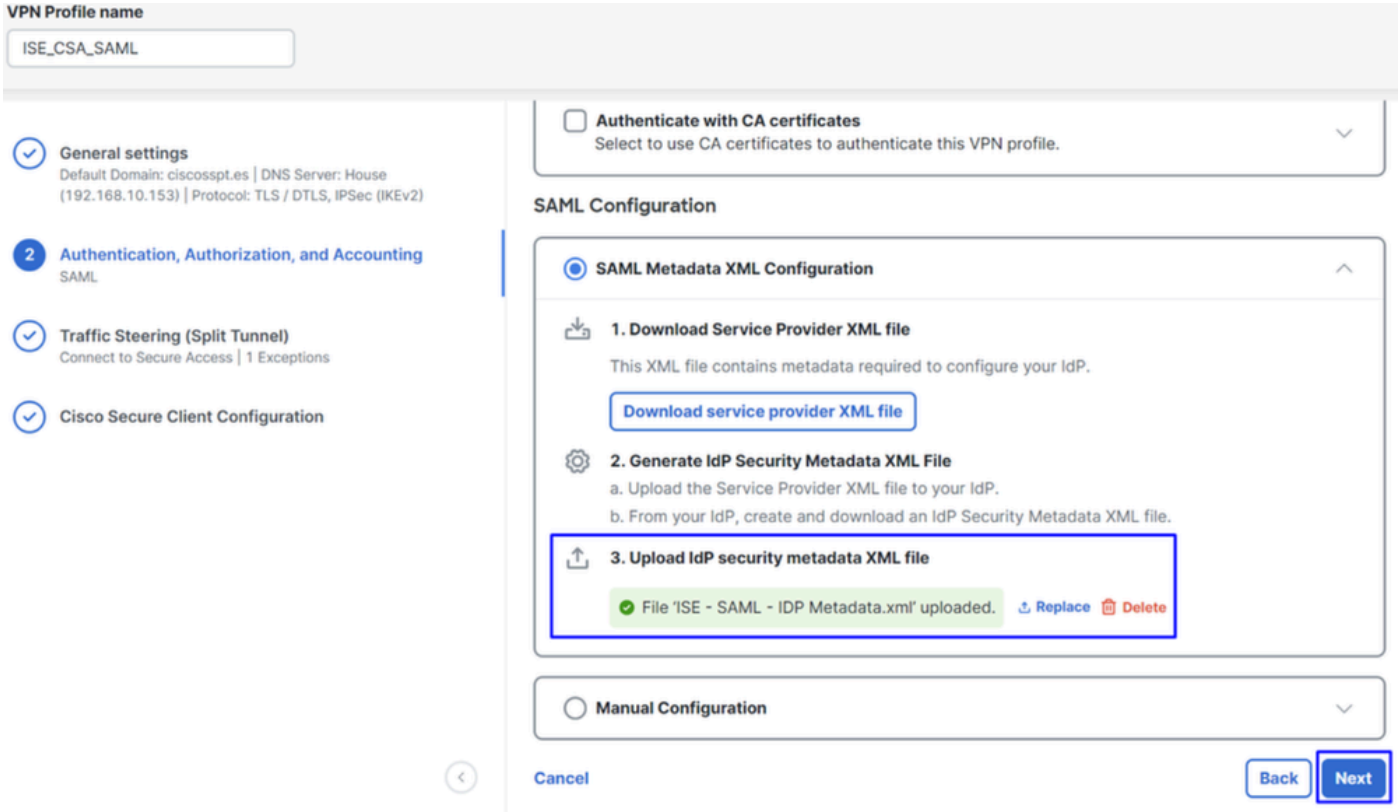


- Klicken Sie **Save** auf Ihre Anwendung auf Duo.

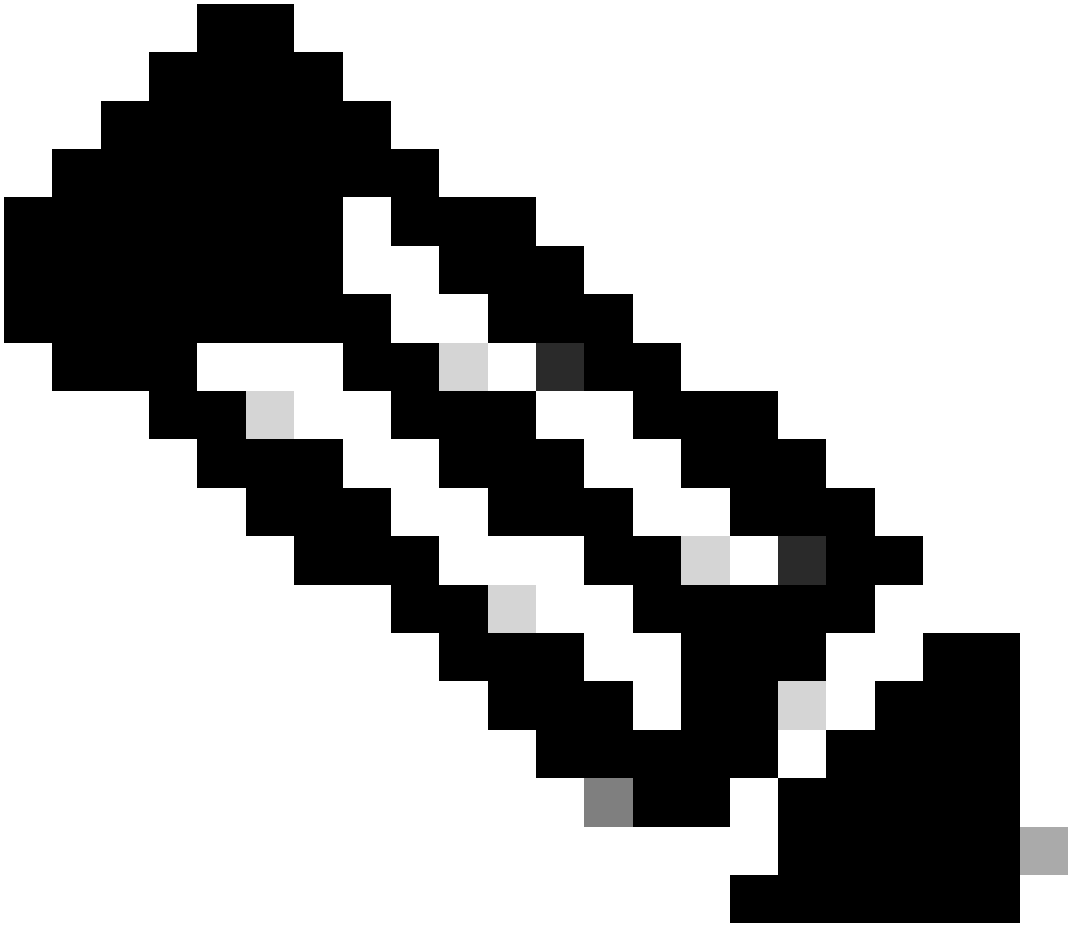
- Sobald Sie auf Speichern klicken, müssen Sie die **SAML Metadata** durch Klicken auf die Schaltfläche **Download XML**



- Laden Sie das **SAML Metadata** über Sicherer Zugriff unter der Option hoch **3. Upload IdP security metadata XML file** und klicken Sie auf **Next**

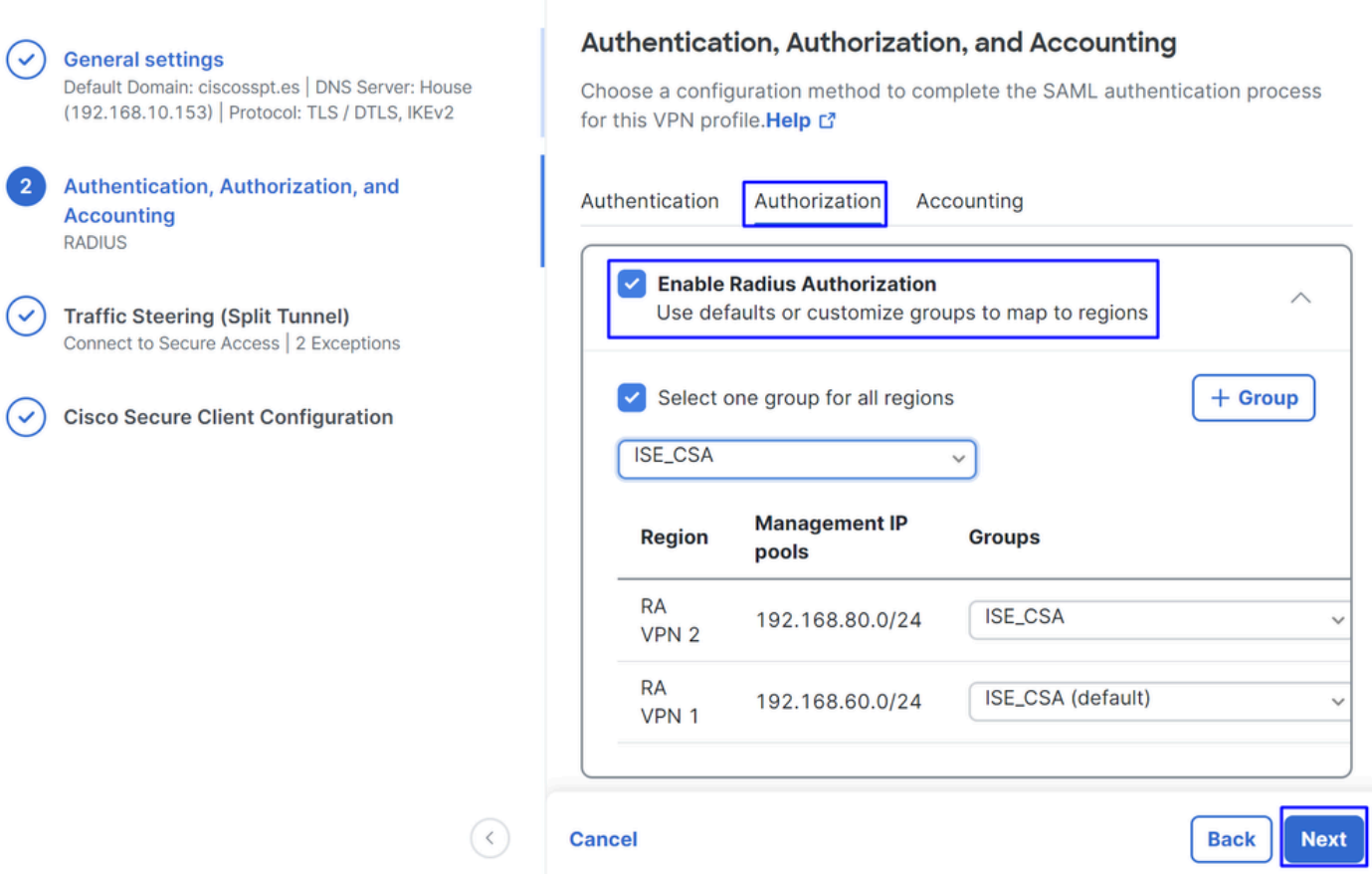


Setzen Sie die Autorisierung fort.



Hinweis: Nachdem Sie die Authentifizierung mit SAML konfiguriert haben, autorisieren Sie sie über die ISE. Das bedeutet, dass das von Secure Access gesendete RADIUS-Paket nur den Benutzernamen enthält. Das Kennwortfeld ist hier nicht vorhanden.

Autorisierung



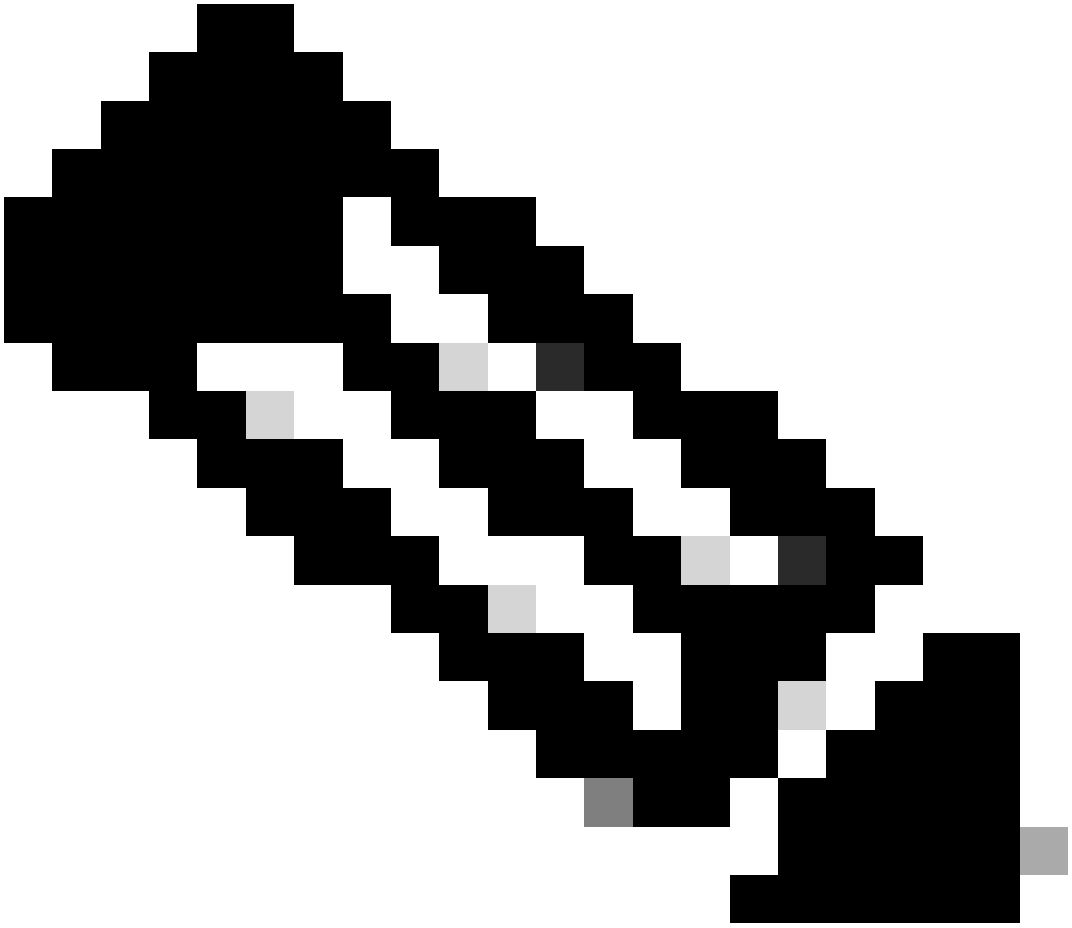
- **Authorization**

  - **Enable Radius Authorization**: Aktivieren Sie das Kontrollkästchen, um die Radius-Autorisierung zu aktivieren.

  - **Wählen Sie eine Gruppe für alle Regionen aus**: Aktivieren Sie das Kontrollkästchen, um einen spezifischen Radius-Server für alle Remote Access Virtual Private Network (RA-VPN)-Pools zu verwenden, oder definieren Sie ihn separat für jeden Pool.

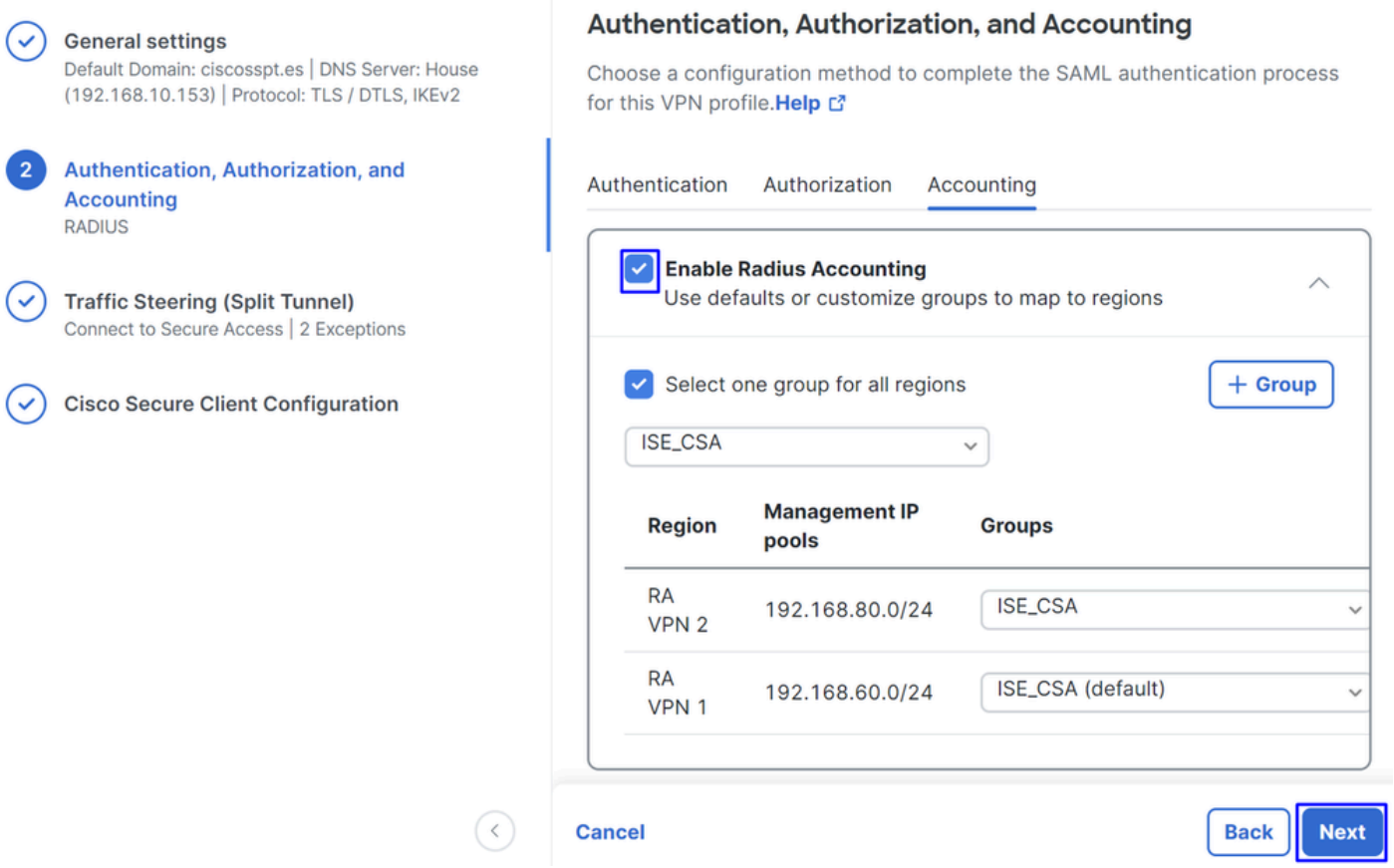
- Klicken Sie auf **Next**

Nachdem Sie alle **Authorization** Teile konfiguriert haben, fahren Sie bitte mit dem **Accounting**fort.



Hinweis: Wenn Sie diese Option nicht aktivieren, **Radio Authorization**kann die Statusüberprüfung nicht ausgeführt werden.

Buchhaltung



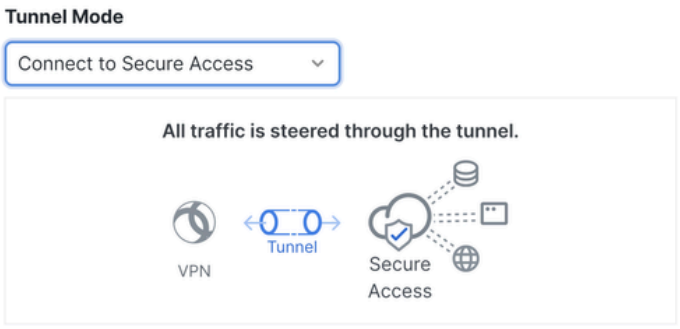
- **Accounting**
  - **Map Authorization groups to regions**: Wählen Sie die Regionen und wählen Sie Ihre **Radius Groups**

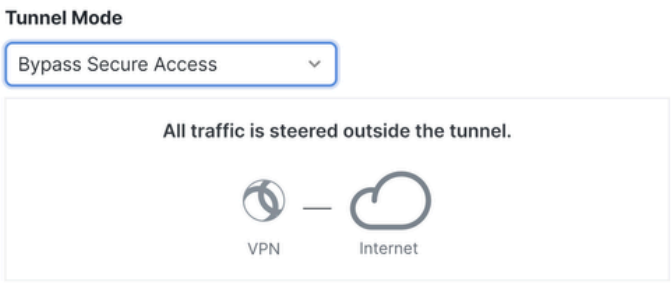
- Klicken Sie auf **Next**

After you have done configured the Authentication, Authorization and Accounting fahren Sie bitte fort mitTraffic Steering.

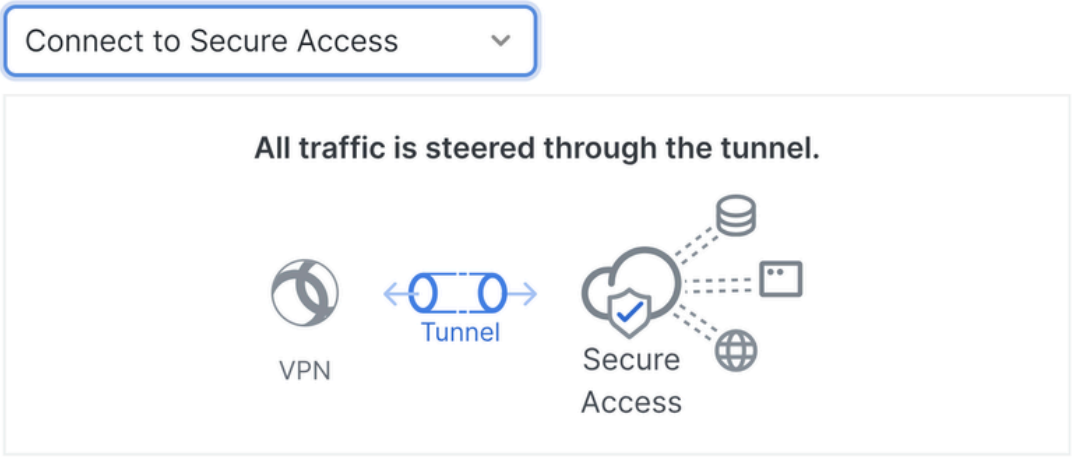
Verkehrssteuerung

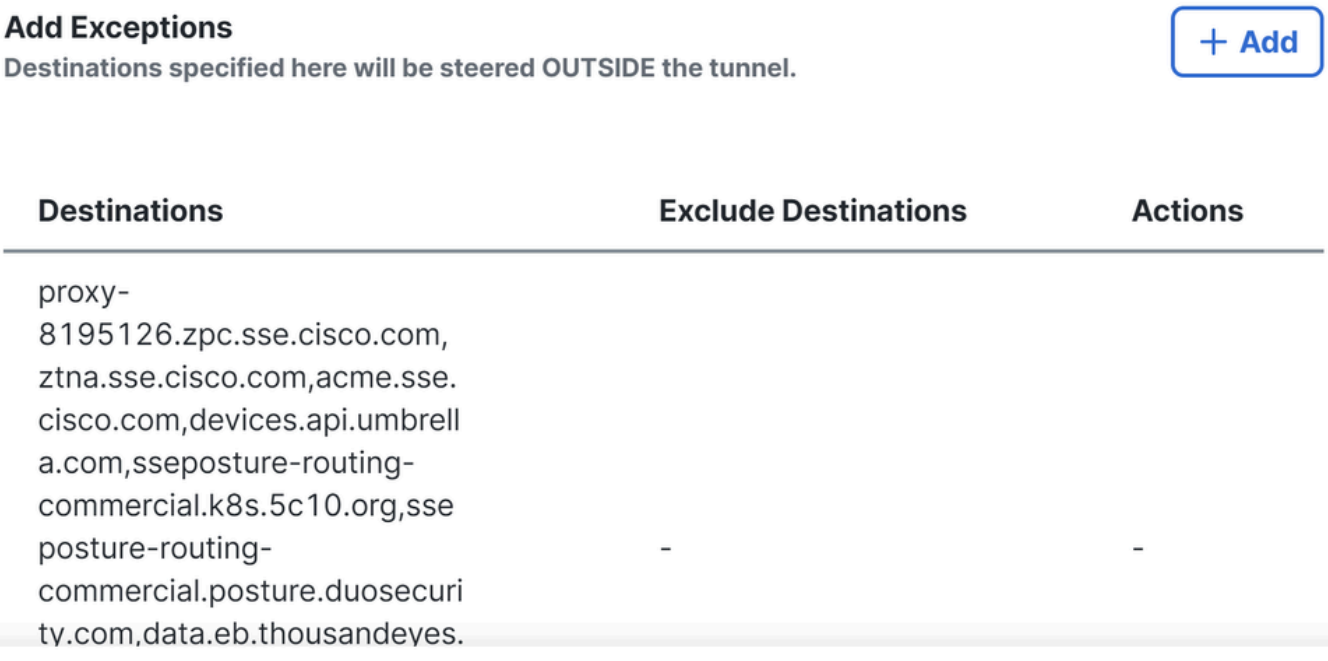
Unter "Traffic Steering" (Steuerung des Datenverkehrs) müssen Sie den Kommunikationstyp über Secure Access konfigurieren.





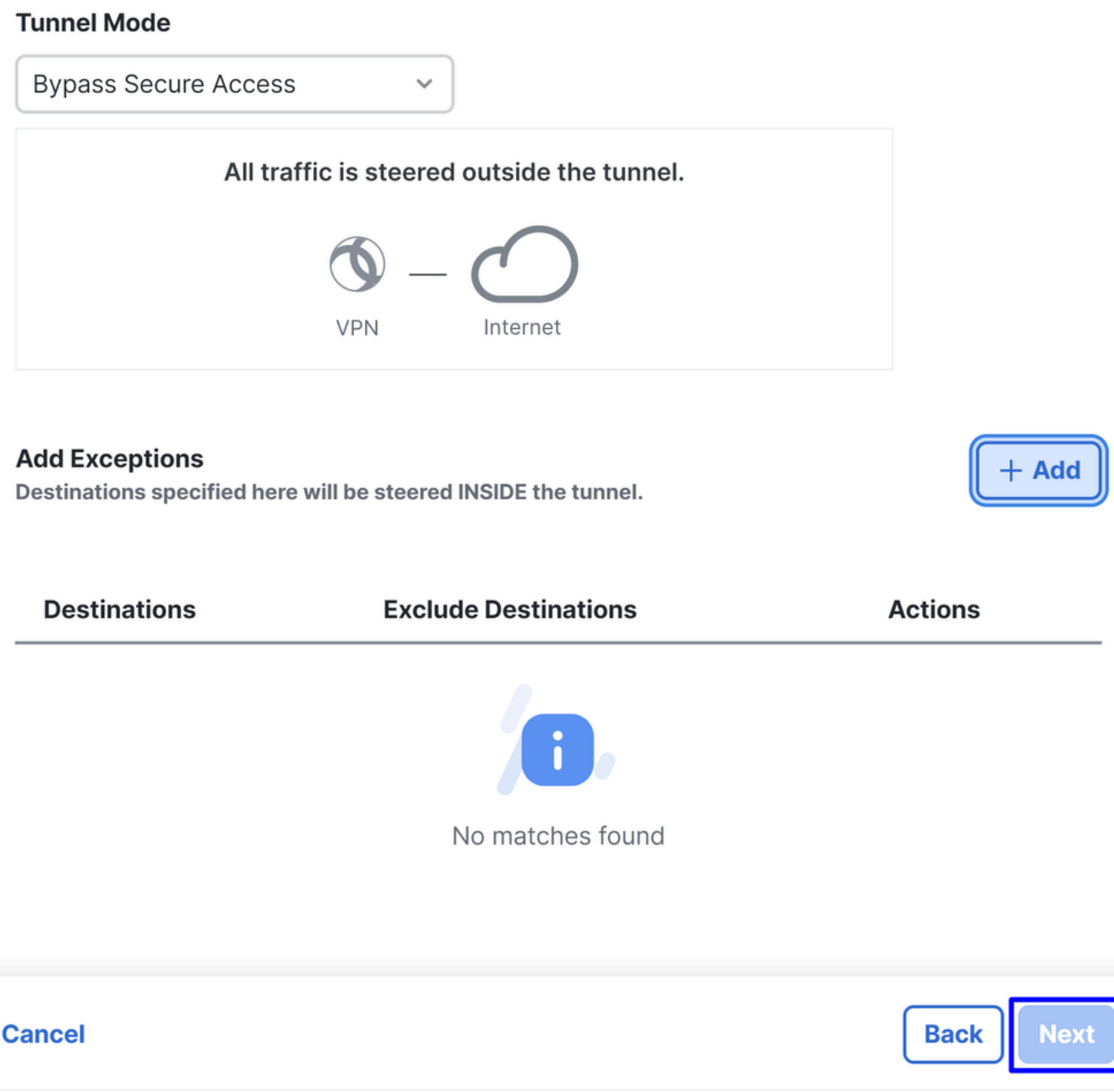
- Wenn Sie möchten, **Connect to Secure Access**werden alle Internet-Datenverkehrsrouten **Secure Access**

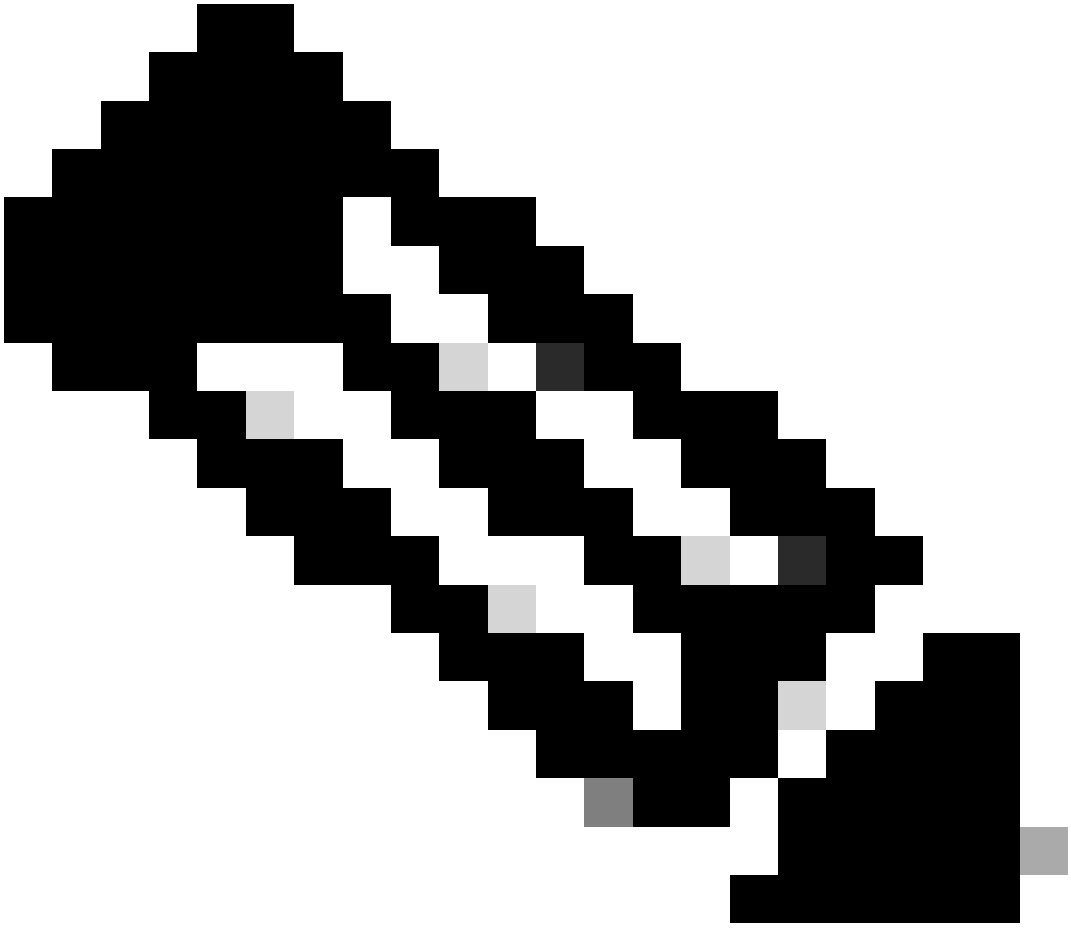




Wenn Sie Ausschlüsse für Internet-Domains oder IP-Adressen hinzufügen möchten, klicken Sie auf die **+ Add** Schaltfläche und dann auf **Next**.

- Wenn Sie sich entscheiden, **Bypass Secure Access**wird der gesamte Internet-Datenverkehr über Ihren Internet-Provider geleitet, nicht überSecure Access (kein Internet-Schutz)

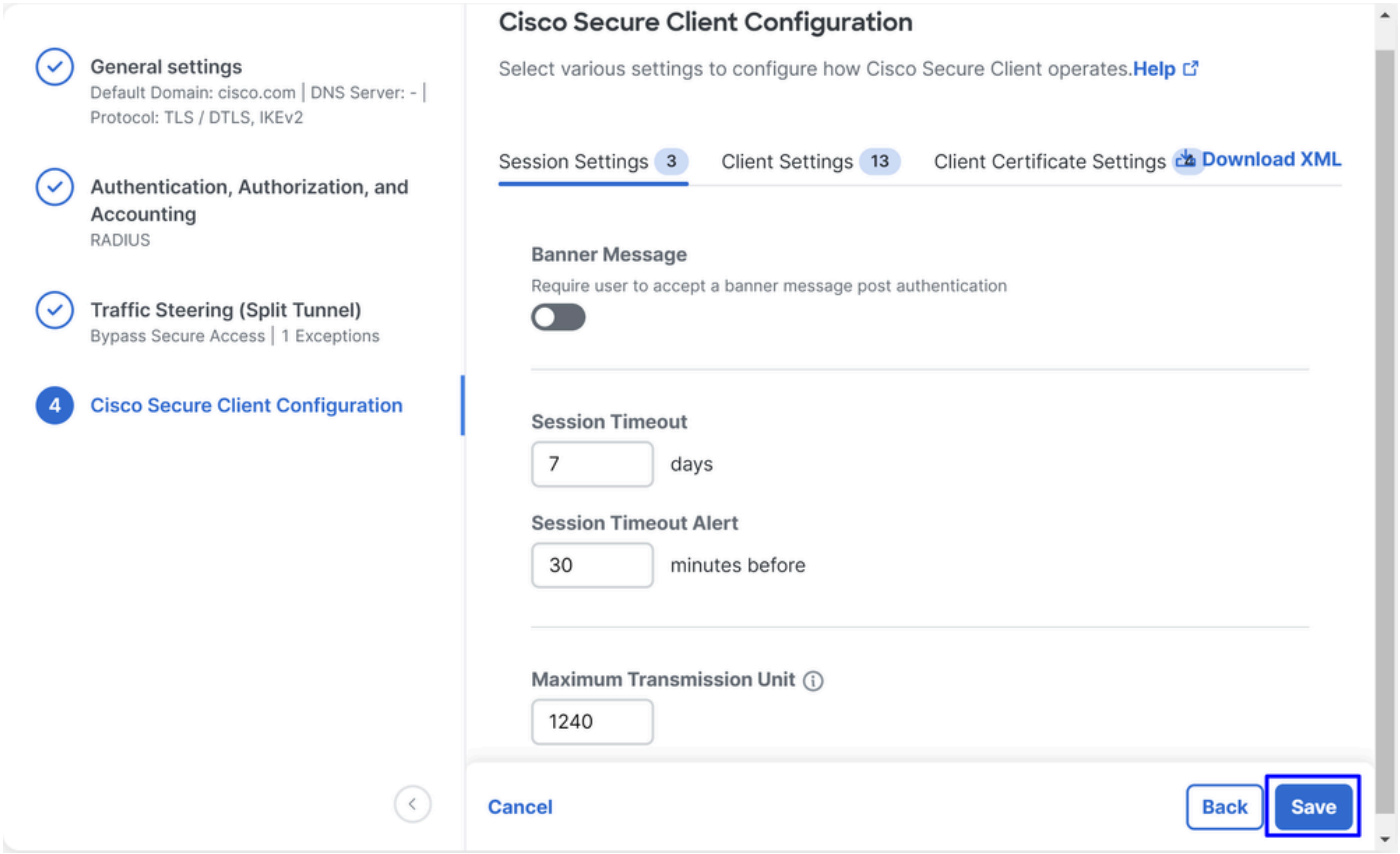




Hinweis: Fügen Sie **enroll.cisco.com** den ISE-Status hinzu, wenn Sie **Bypass Secure Access**auswählen.

In diesem Schritt wählen Sie alle privaten Netzwerkressourcen aus, auf die Sie über das VPN zugreifen möchten. Klicken Sie dazu auf **+ Add**, und klicken Sie dann auf, **Next** wenn Sie alle Ressourcen hinzugefügt haben.

Cisco Secure Client-Konfiguration



In diesem Schritt können Sie alles als Standard verwalten und auf klicken, **Save**aber wenn Sie Ihre Konfiguration weiter anpassen möchten, lesen Sie bitte das Cisco Secure Client Administratorhandbuch.

Name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL
ISE_CSA_SAML	ciscosspt.es TLS, IPSec (IKEv2)	SAML RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	vpn.sse.cisco.com/ISE_CSA_SAML

ISE-Konfigurationen

Konfiguration der Liste der Netzwerkgeräte

Um die Authentifizierung über die Cisco ISE zu konfigurieren, müssen Sie die zulässigen Geräte konfigurieren, die Abfragen an die Cisco ISE senden können:

- Navigieren Sie zu **Administration > Network Devices**
- Klicken Sie **+ Add**

Network Devices List > CSA

Network Devices

Name CSA

Description

IP Address * IP : 192.168.60.0 / 24

Device Profile Cisco

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret •••••••• Show

Use Second Shared Secret

Second Shared Secret Show

CoA Port 1700 Set To Default

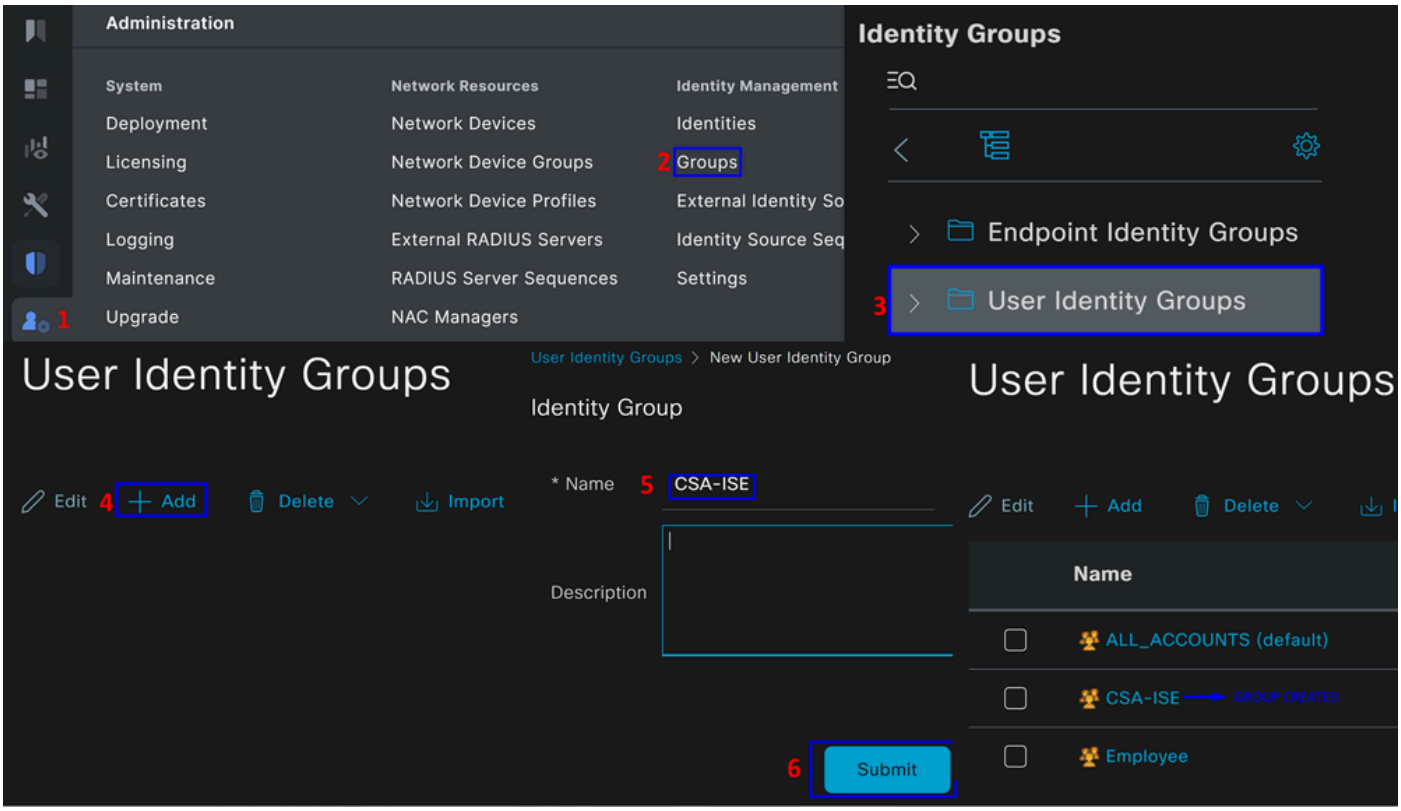
- **Name**: Verwenden Sie einen Namen zur Identifizierung von sicherem Zugriff.
- **IP Address**: Konfigurieren Sie die Management Interface des Schritts "IP Pool Region".
- **Device Profile**Cisco Produkte auswählen
    - **Radius Authentication Settings**
        - Shared Secret: Konfigurieren Sie den gleichen geheimen Schlüssel, der für den Schritt konfiguriert wurde, Secret Key (Geheimschlüssel).
            - **CoA Port**: Voreinstellung; 1700 wird auch für sicheren Zugriff verwendet

Nach diesem Klick **Save**, um zu überprüfen, ob die Integration ordnungsgemäß funktioniert, fahren Sie mit der Erstellung eines lokalen Benutzers für die Integrationsverifizierung fort.

Konfigurieren einer Gruppe

Gehen Sie wie folgt vor, um eine Gruppe zur Verwendung mit lokalen Benutzern zu konfigurieren:

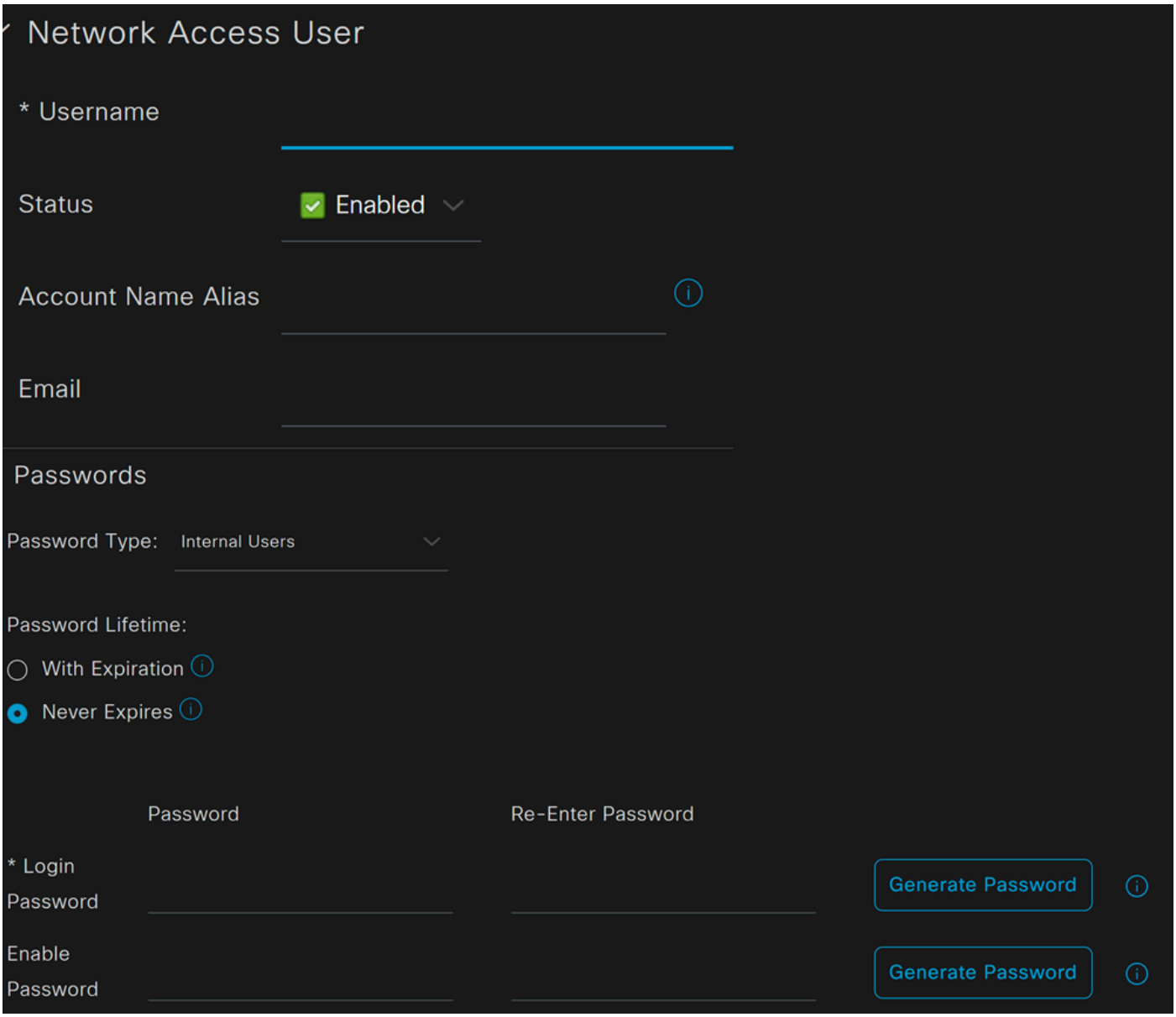
- Klicken Sie in **Administration > Groups**
- Klicken Sie auf **User Identity Groups**
- Klicken Sie auf + Add
- Erstellen Sie einen Namefür die Gruppe, und klicken Sie auf **Submit**

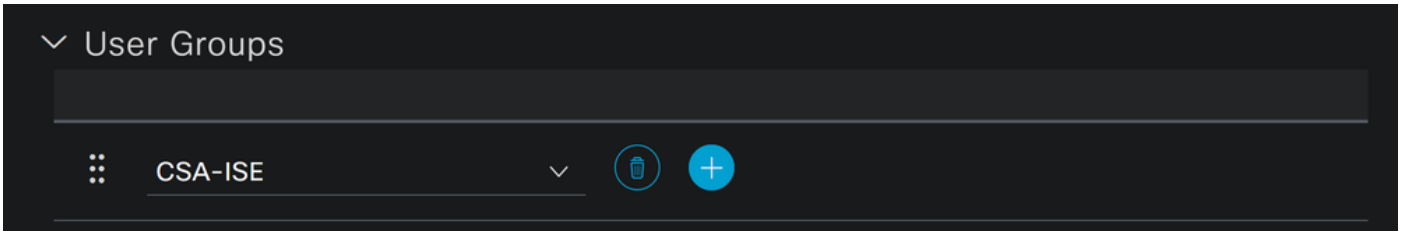


Lokalen Benutzer konfigurieren

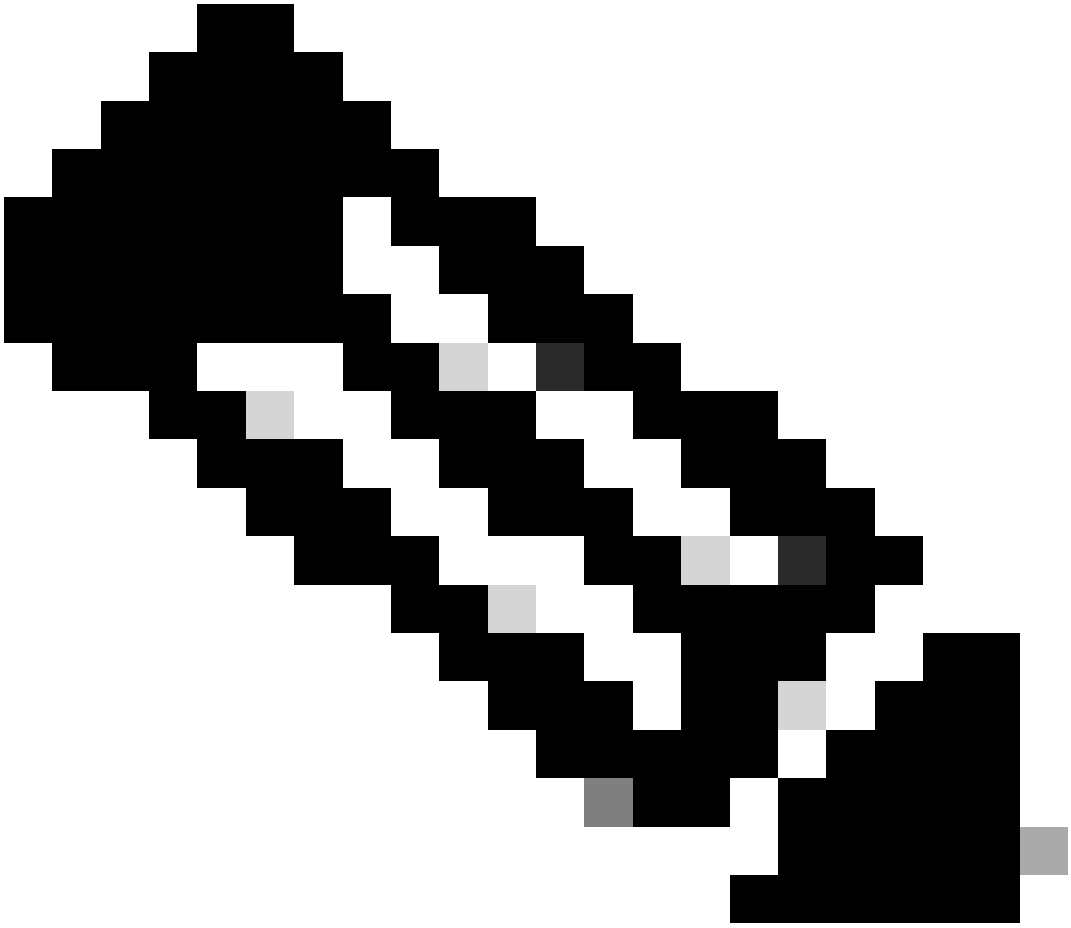
So konfigurieren Sie einen lokalen Benutzer, um Ihre Integration zu überprüfen:

- Navigieren Sie zu **Administration > Identities**
- Klicken Sie **Add +**





- **Username**: Konfigurieren Sie den Benutzernamen mit einer bekannten UPN-Bereitstellung in Secure Access; dies basiert auf dem Schritt Voraussetzungen
- **Status**:Aktiv
- **Password Lifetime**: Sie können es konfigurieren **With Expiration** oder Never Expires, je nach
- **Login Password**: Passwort für den Benutzer erstellen
- **User Groups**: Wählen Sie die Gruppe erstellt auf dem Schritt, Konfigurieren Sie eine Gruppe



Hinweis: Die auf UPN basierende Authentifizierung wird in den kommenden Versionen von Secure Access geändert.

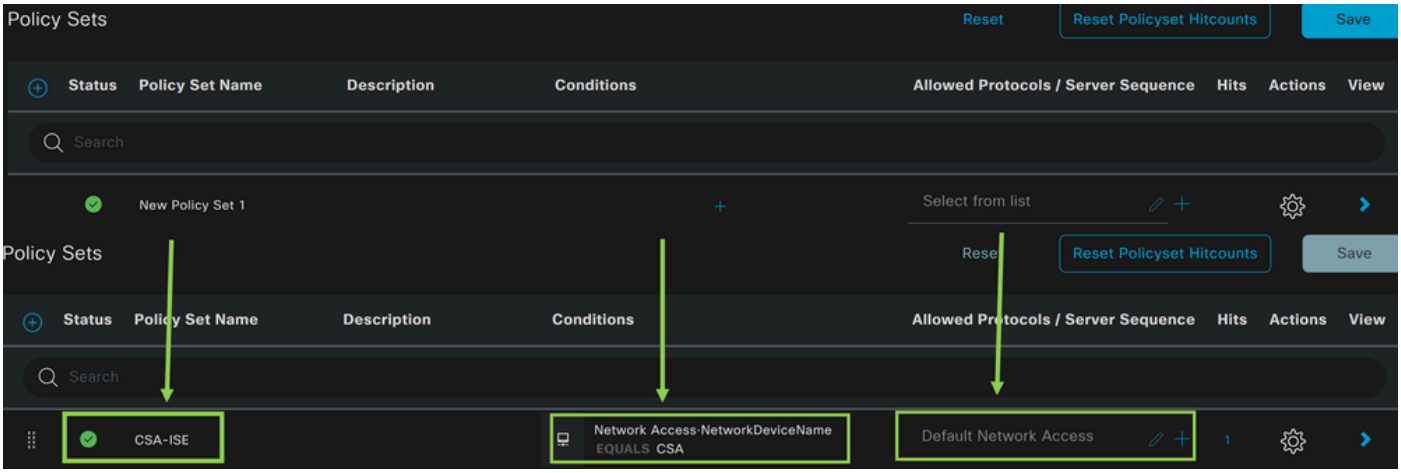
Anschließend können Sie **Save** die Konfiguration vornehmen und mit dem Schritt fortfahren **Configure Policy Set**.

Policy Set konfigurieren

Konfigurieren Sie unter dem Richtliniensatz die Aktion, die die ISE während der Authentifizierung und Autorisierung ausführt. Dieses Szenario veranschaulicht den Anwendungsfall für die Konfiguration einer einfachen Richtlinie, die den Benutzerzugriff ermöglicht. Zunächst überprüft die ISE den Ursprung der RADIUS-Authentifizierungen und überprüft, ob die Identitäten in der ISE-Benutzerdatenbank vorhanden sind, um den Zugriff zu ermöglichen.

Um diese Richtlinie zu konfigurieren, navigieren Sie zu Ihrem Cisco ISE Dashboard:

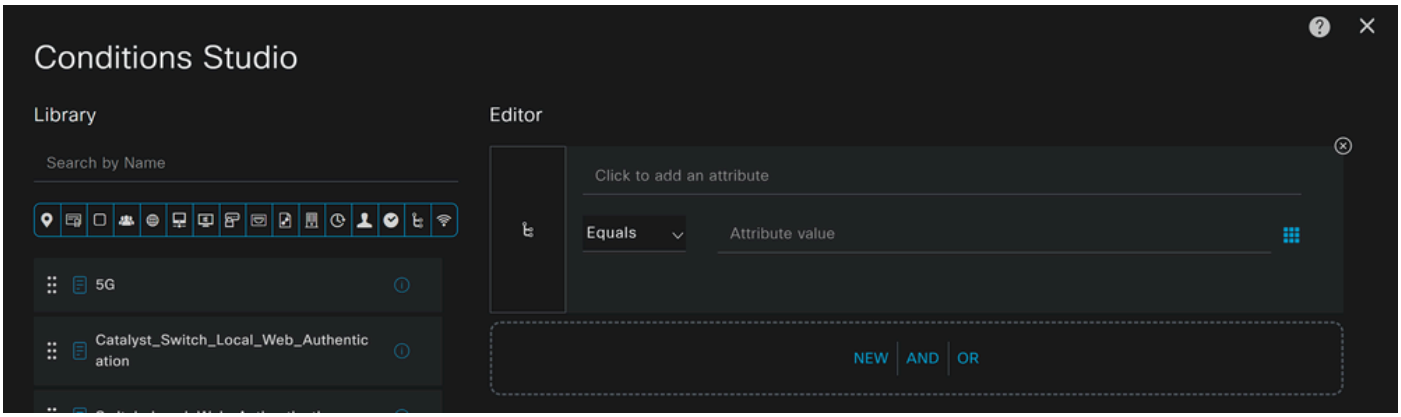
- Klicken Sie Policy > Policy Sets
- Klicken Sie auf, + um einen neuen Richtliniensatz hinzuzufügen



Erstellen Sie in diesem Fall einen neuen Richtliniensatz, anstatt ihn unter dem Standardsatz zu verwenden. Konfigurieren Sie anschließend die Authentifizierung und Autorisierung auf der Grundlage dieses Richtlinienpakets. Die konfigurierte Richtlinie ermöglicht den Zugriff auf das Netzwerkgerät, das im Schritt Configure Network Devices List (Liste der Netzwerkgeräte konfigurieren) definiert wurde, um zu überprüfen, ob diese Authentifizierungen von stammen, und um dann in die Richtlinie als zu gelangenCSA Network Device List. **Conditions**. Und schließlich die zulässigen Protokolle, wie **Default Network Access**.

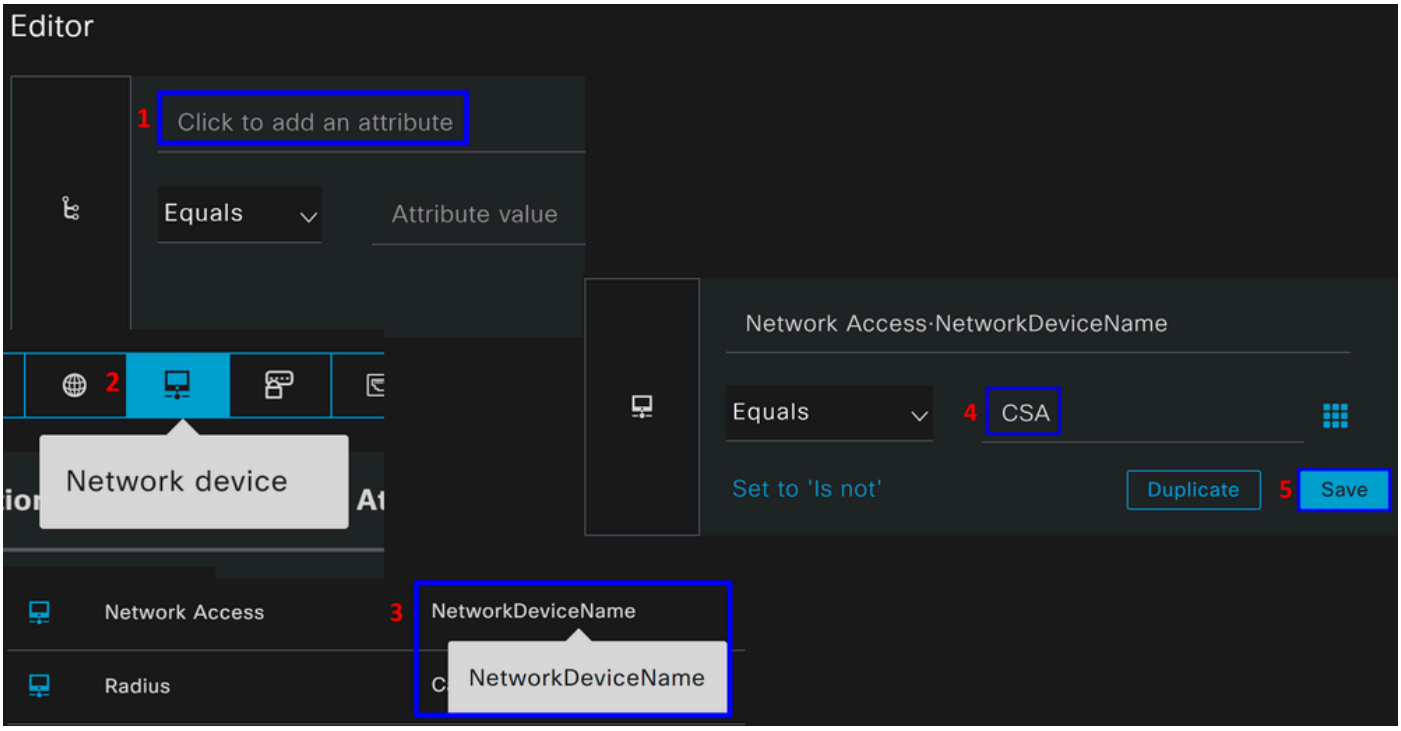
So erstellen Sie **condition** das , das mit dem Richtliniensatz übereinstimmt:

- Klicken Sie +
- Zu **Condition Studio**den verfügbaren Informationen gehören:



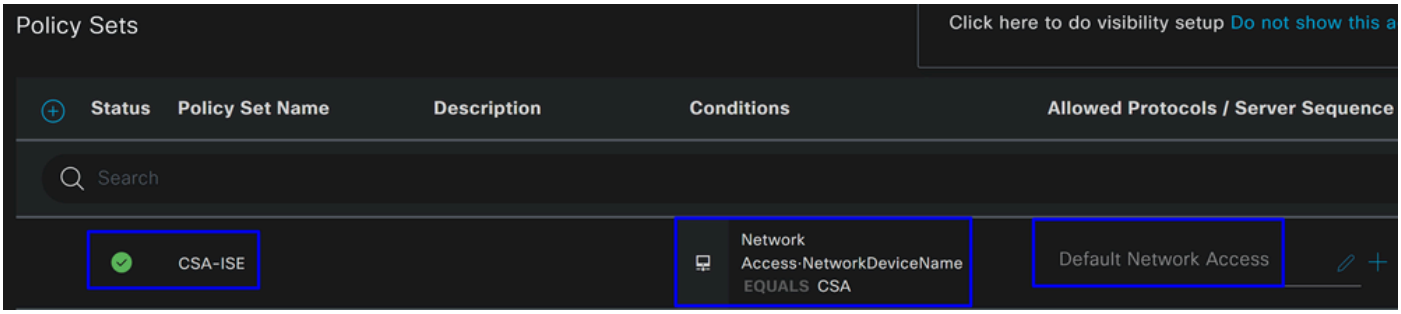
- Klicken Sie zum Erstellen der Bedingungen auf Click to add an attribute
- Klicken Sie auf die **Network Device** Schaltfläche
- Klicken Sie unter den Optionen dahinter auf **Network Access - Network Device Name** Option

- Schreiben Sie unter der Option Equals den Namen des **Network Device** unter dem Schritt Configure Network Devices List
- Klicken Sie auf **Save**

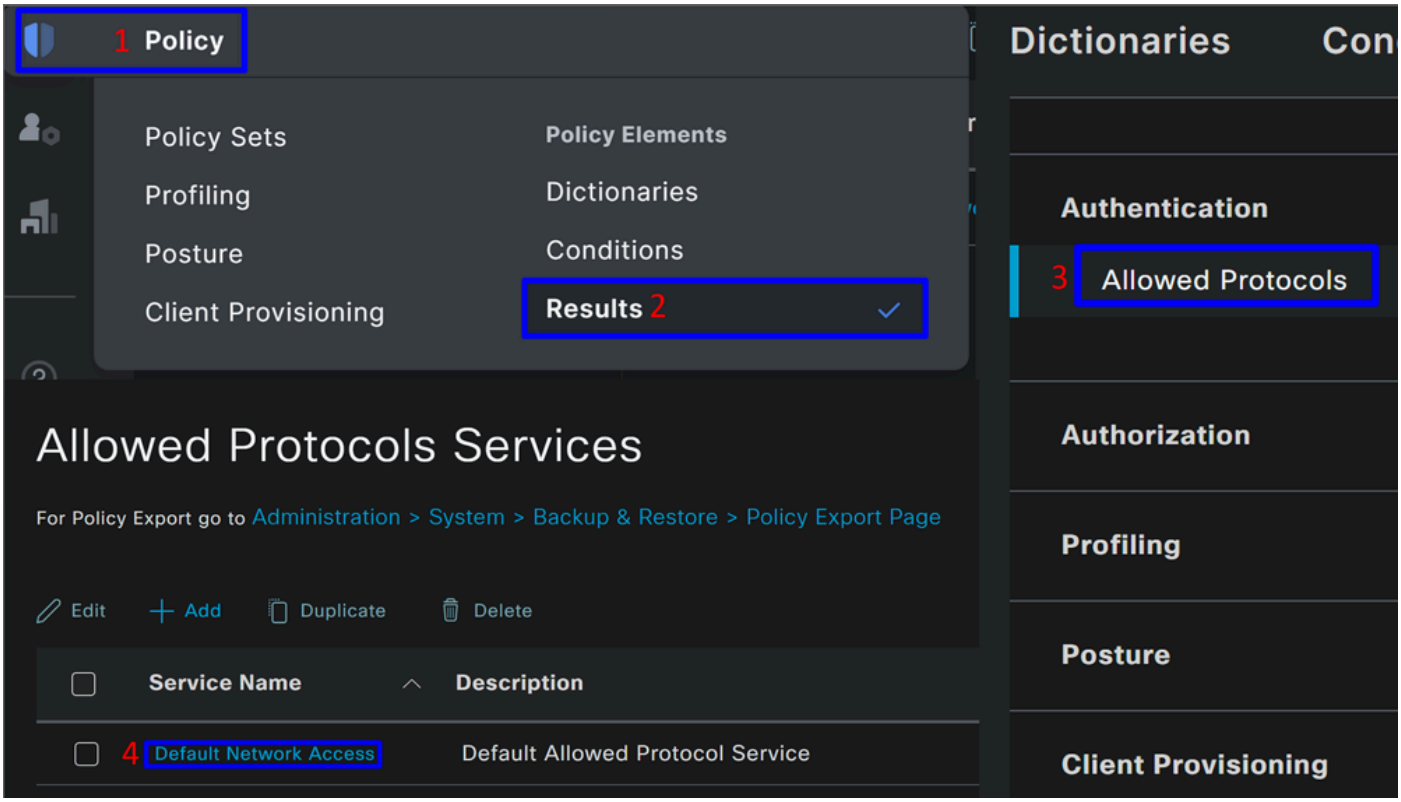


Diese Richtlinie genehmigt nur die Anforderung der Quelle, CSAdas **Authentication** und die **Authorization** Einrichtung unter dem Richtliniensatz fortzusetzen, **CSA-ISE**und überprüft außerdem die zulässigen Protokolle auf der Grundlage der **Default Network Access** für die zulässigen Protokolle.

Das Ergebnis der definierten Richtlinie muss sein:



- Um zu überprüfen, ob **Default Network Access Protocols** zulässig ist, fahren Sie mit den folgenden Anweisungen fort:
  - Klicken SiePolicy > Results
    - Klicken Sie **Allowed Protocols**
    - Klicken Sie **Default Network Access**

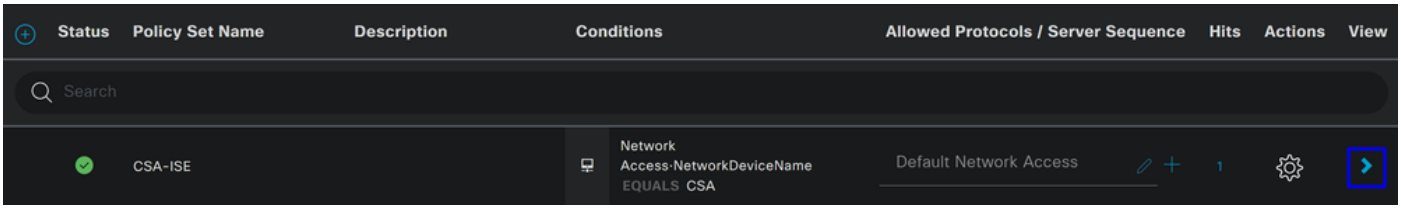


- Anschließend werden alle Protokolle angezeigt, die auf **Default Network Access**

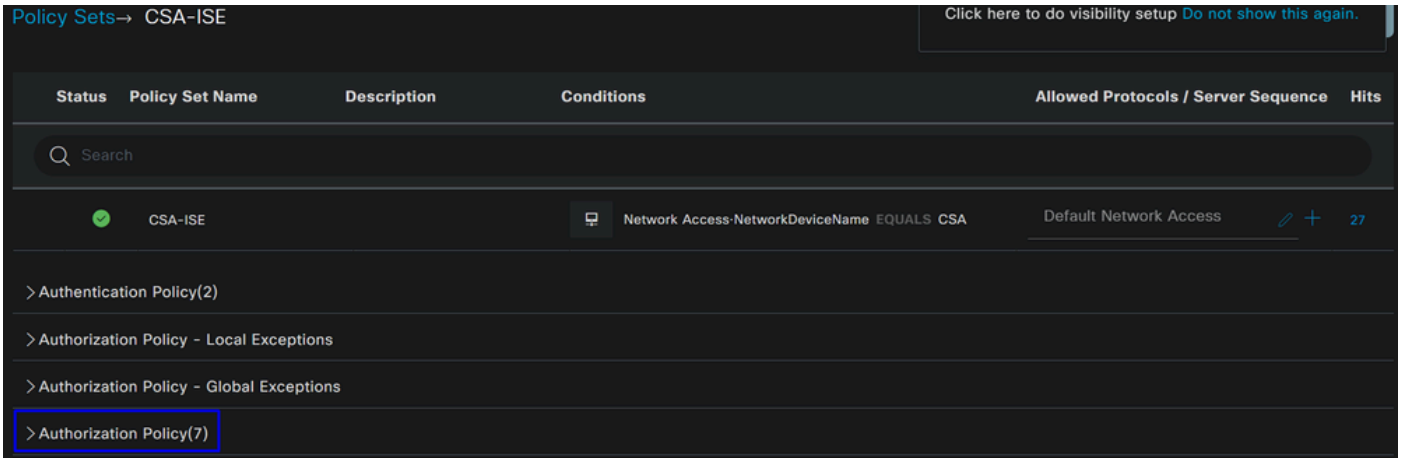
Autorisierung für Policy Set konfigurieren

Gehen Sie wie folgt vor, um die **Authorization** Richtlinie unter **Policy Set** zu erstellen:

- Klicken Sie >



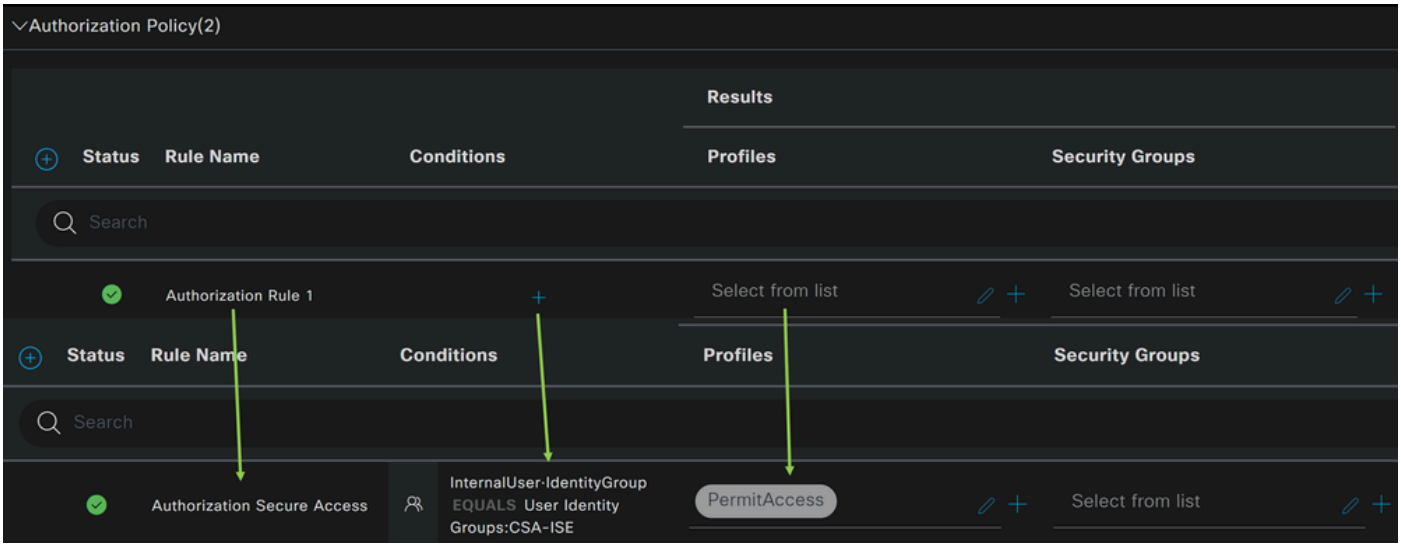
- Danach werden die **Authorization** Richtlinien angezeigt:



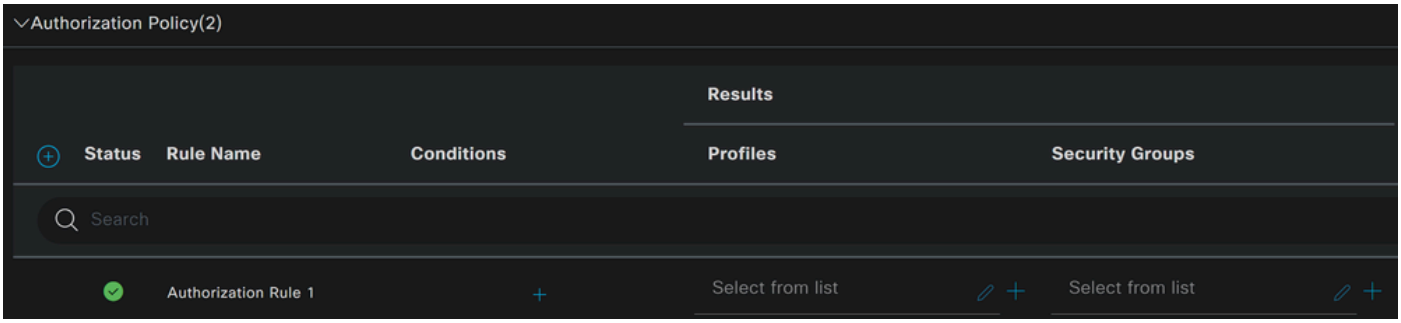
Die Richtlinie ist die gleiche, die Sie im Schritt Configure Policy Set definiert haben.

Autorisierungsrichtlinie

Sie haben viele Möglichkeiten, die Autorisierungsrichtlinie zu konfigurieren. In diesem Fall autorisieren Sie nur die Benutzer in der Gruppe, die im Schritt Konfigurieren einer Gruppe definiert ist.Im nächsten Beispiel wird die Autorisierungsrichtlinie konfiguriert:

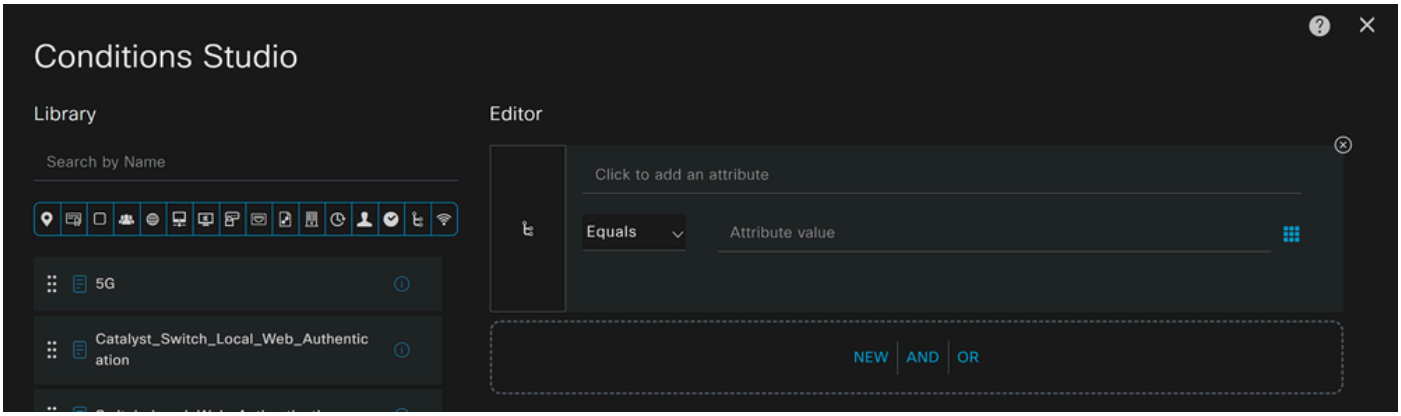


- Klicken Sie **Authorization Policy**
- Klicken Sie auf, + um die Autorisierungsrichtlinie wie folgt zu definieren:

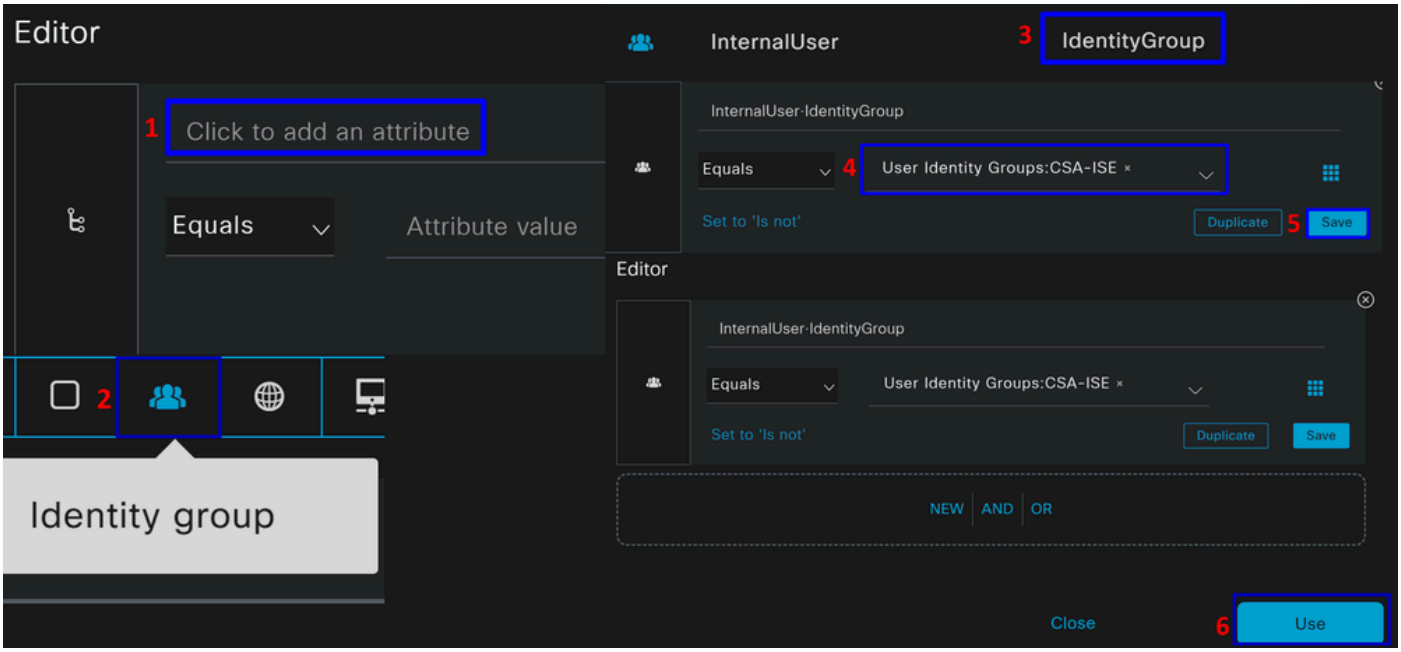


- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles

- Wenn Sie einen Namen **Name** konfigurieren, um die Autorisierungsrichtlinie leicht zu identifizieren
- Um das zu konfigurieren, **Condition**klicken Sie auf die Schaltfläche +
- Unter **Condition Studio**finden Sie die Informationen:

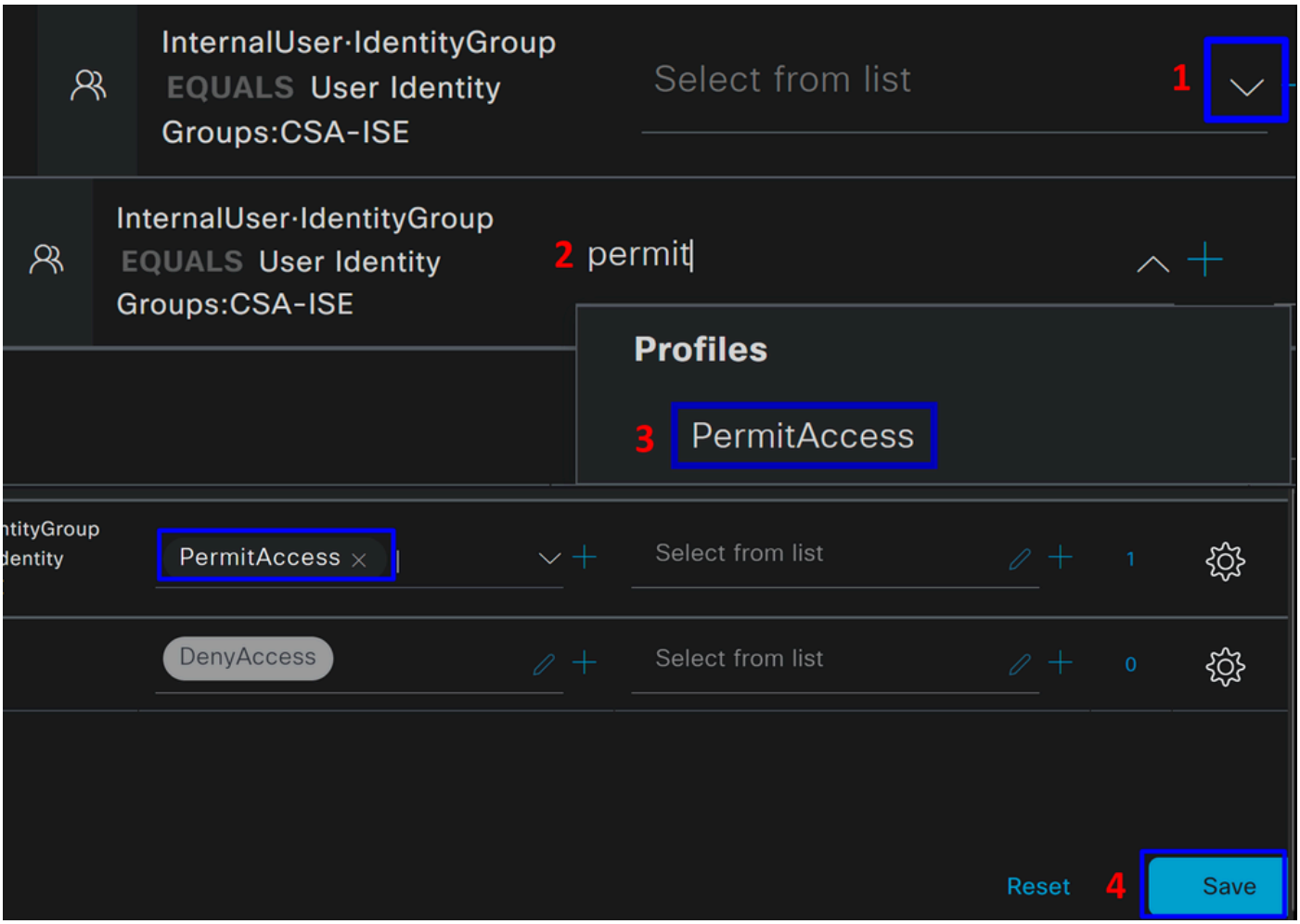


- Klicken Sie zum Erstellen der Bedingungen auf Click to add an attribute
- Klicken Sie auf die **Identity Group** Schaltfläche
- Klicken Sie unter den Optionen dahinter auf **Interner Benutzer - IdentityGroup** Option
- Verwenden Sie unter der **Equals** Option das Dropdown-Menü, um nach der für die Authentifizierung **Group** genehmigten im Schritt Konfigurieren einer Gruppe zu suchen.
- Klicken Sie auf **Save**
- Klicken Sie auf **Use**



Anschließend müssen Sie die **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- Klicken Sie unter **Authorization Policy**auf die Dropdown-Schaltfläche **Profiles**
- Nach Genehmigung suchen
- Auswählen **PermitAccess**
- Klicken Sie auf Save

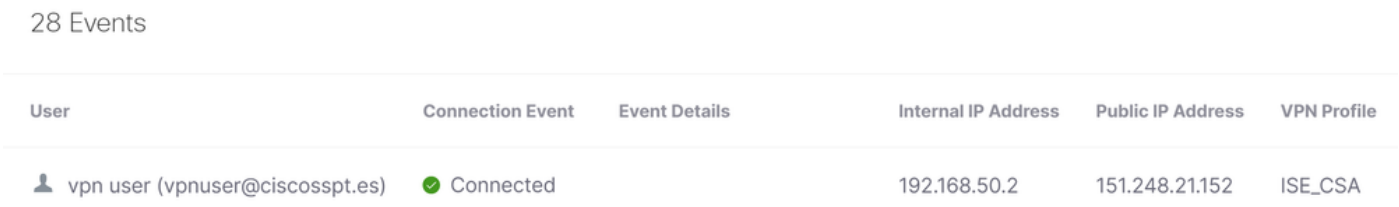


Anschließend haben Sie Ihre **Authorization** Richtlinie definiert. Authentifizieren Sie sich, um zu überprüfen, ob der Benutzer problemlos eine Verbindung herstellt und ob Sie die Protokolle auf Secure Access und ISE sehen können.

Um eine Verbindung zum VPN herzustellen, können Sie das auf Secure Access erstellte Profil verwenden und sich über Secure Client mit dem ISE-Profil verbinden.

- **Wie wird das Protokoll in Secure Access angezeigt, wenn die Authentifizierung genehmigt wird?**
  - Navigieren zum Dashboard für sicheren Zugriff

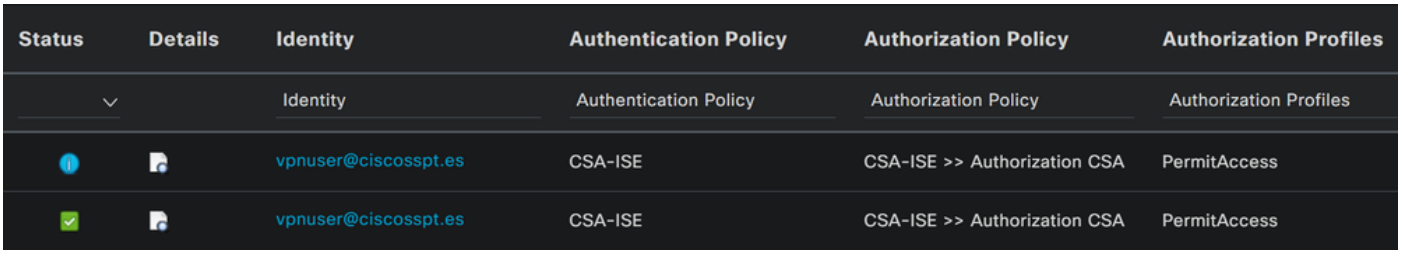
- Klicken Sie **Monitor > Remote Access Log**



- **Wie wird das Protokoll in der ISE angezeigt, wenn die Authentifizierung genehmigt wird?**

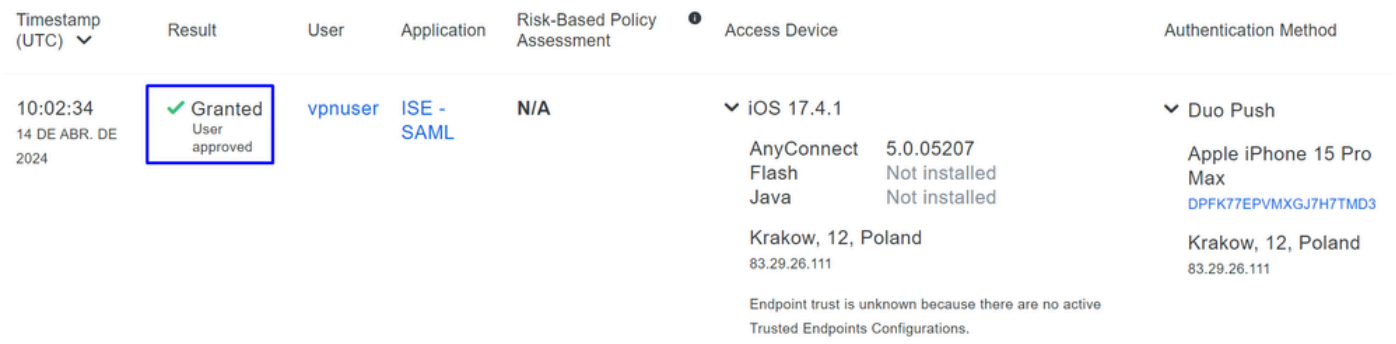
  - Navigieren Sie zum **Cisco ISE Dashboard**

    - Klicken Sie **Operations > Live Logs**



Wie wird das Protokoll in Duo angezeigt, wenn die Authentifizierung genehmigt wird?

- Navigieren Sie zum Duo Admin-Bereich.
- Klicken Sie **Reports > Authentication Log**



Konfigurieren von lokalen Radius- oder Active Directory-Benutzern

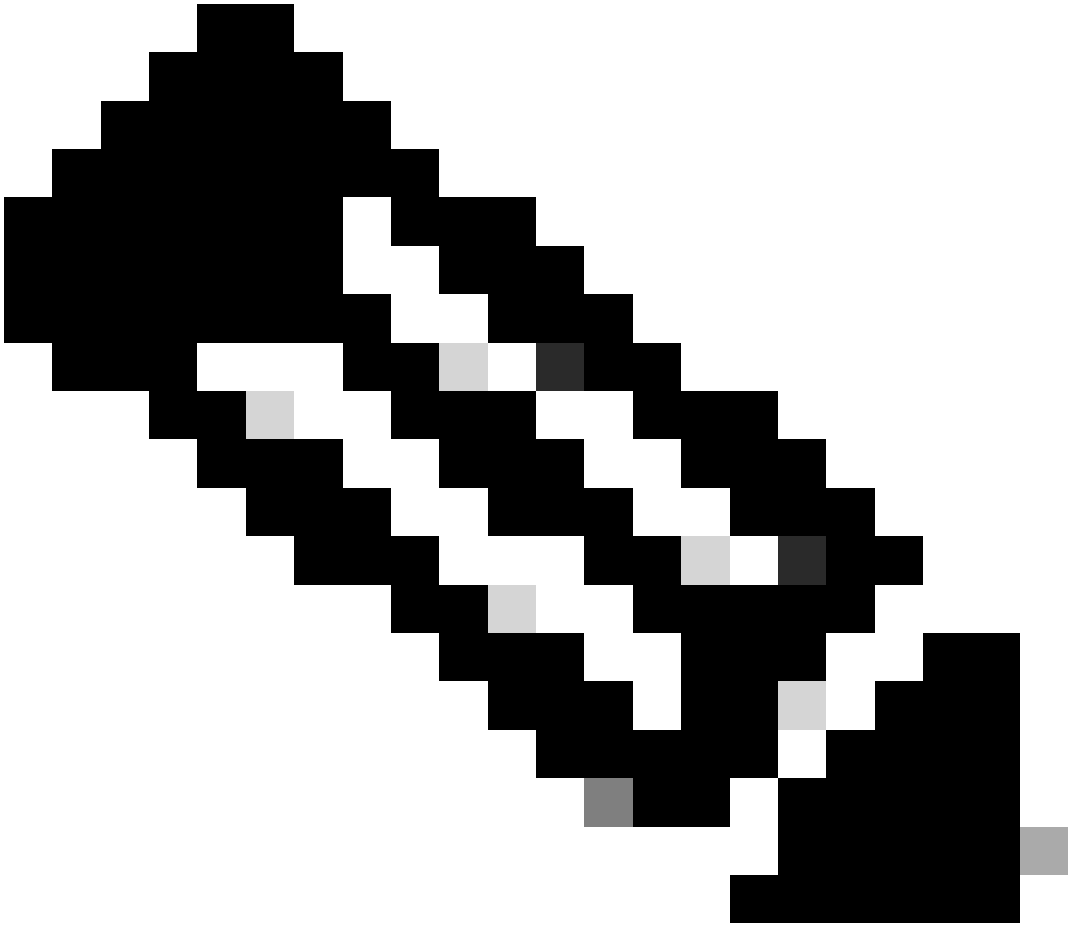
Konfigurieren des ISE-Status

Erstellen Sie in diesem Szenario die Konfiguration, um die Endpunkt-Compliance zu überprüfen, bevor Sie den Zugriff auf interne Ressourcen gewähren oder verweigern.

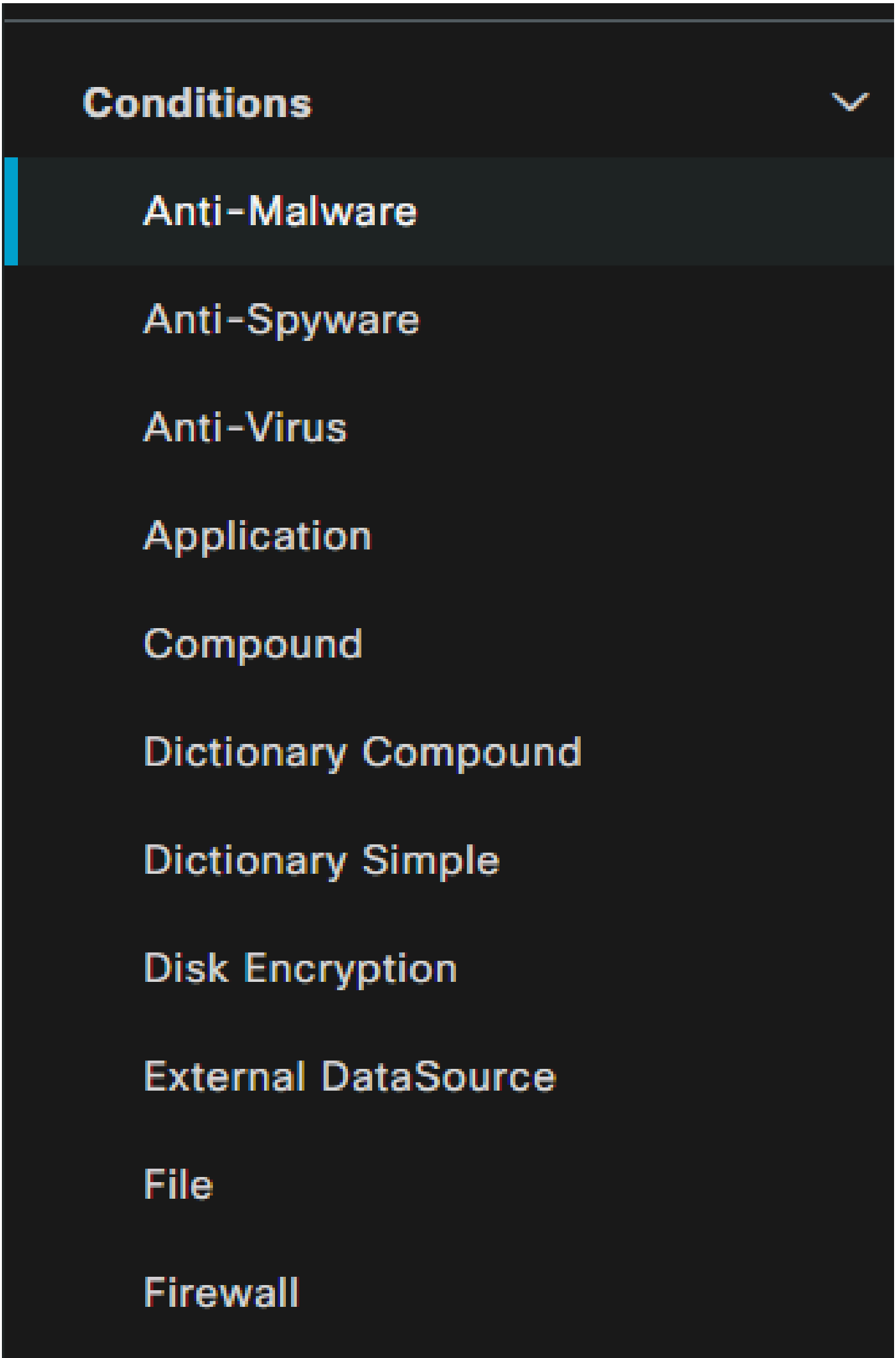
Gehen Sie wie folgt vor, um die Konfiguration vorzunehmen:

Statusbedingungen konfigurieren

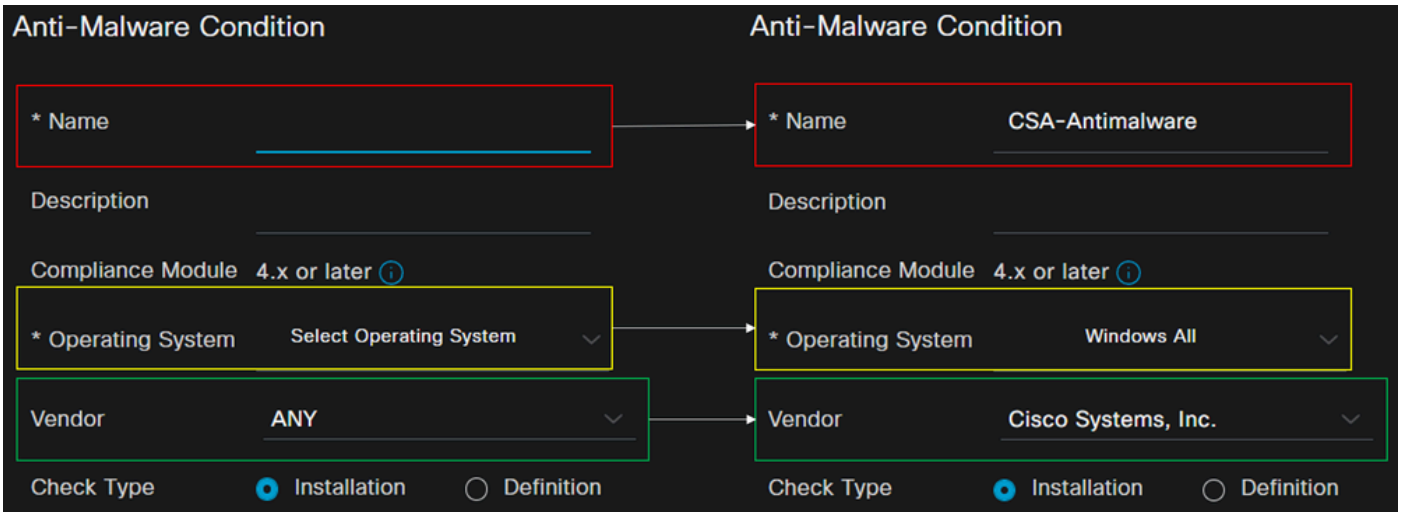
- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Policy Elements > Conditions**
- Klicken Sie **Anti-Malware**



Hinweis: Hier finden Sie viele Optionen, um den Status Ihrer Geräte zu überprüfen und die richtige Bewertung auf Grundlage Ihrer internen Richtlinien vorzunehmen.

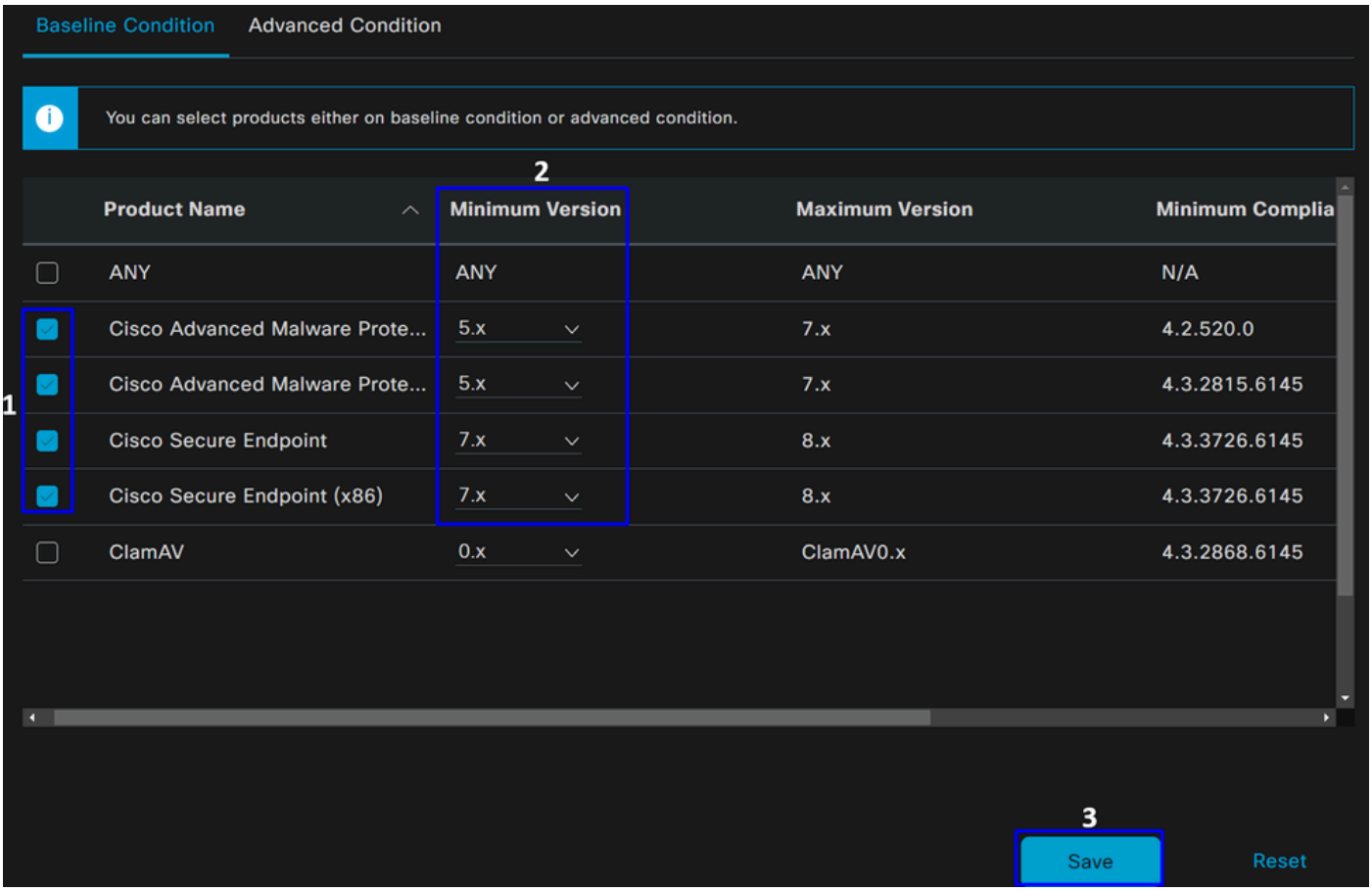

Conditions
Anti-Malware
Anti-Spyware
Anti-Virus
Application
Compound
Dictionary Compound
Dictionary Simple
Disk Encryption
External DataSource
File
Firewall

Anti-Malware Condition dass die Antivirus-Installation auf dem System erkannt wird. Sie können bei Bedarf auch die Version des Betriebssystems auswählen.



- **Name**: Verwenden Sie einen Namen, um den Anti-Malware-Zustand zu erkennen.
- **Operating System**: Wählen Sie das operative System, das Sie unter der Bedingung setzen möchten
- **Vendor**: Wählen Sie einen Anbieter oder eine BELIEBIGE
- **Check Type**: Sie können überprüfen, ob der Agent installiert ist, oder die Definitionsversion für diese Option angeben.

- Für **Products for Selected Vendor**konfigurieren Sie, was Sie über den Malwareschutz auf dem Gerät überprüfen möchten.

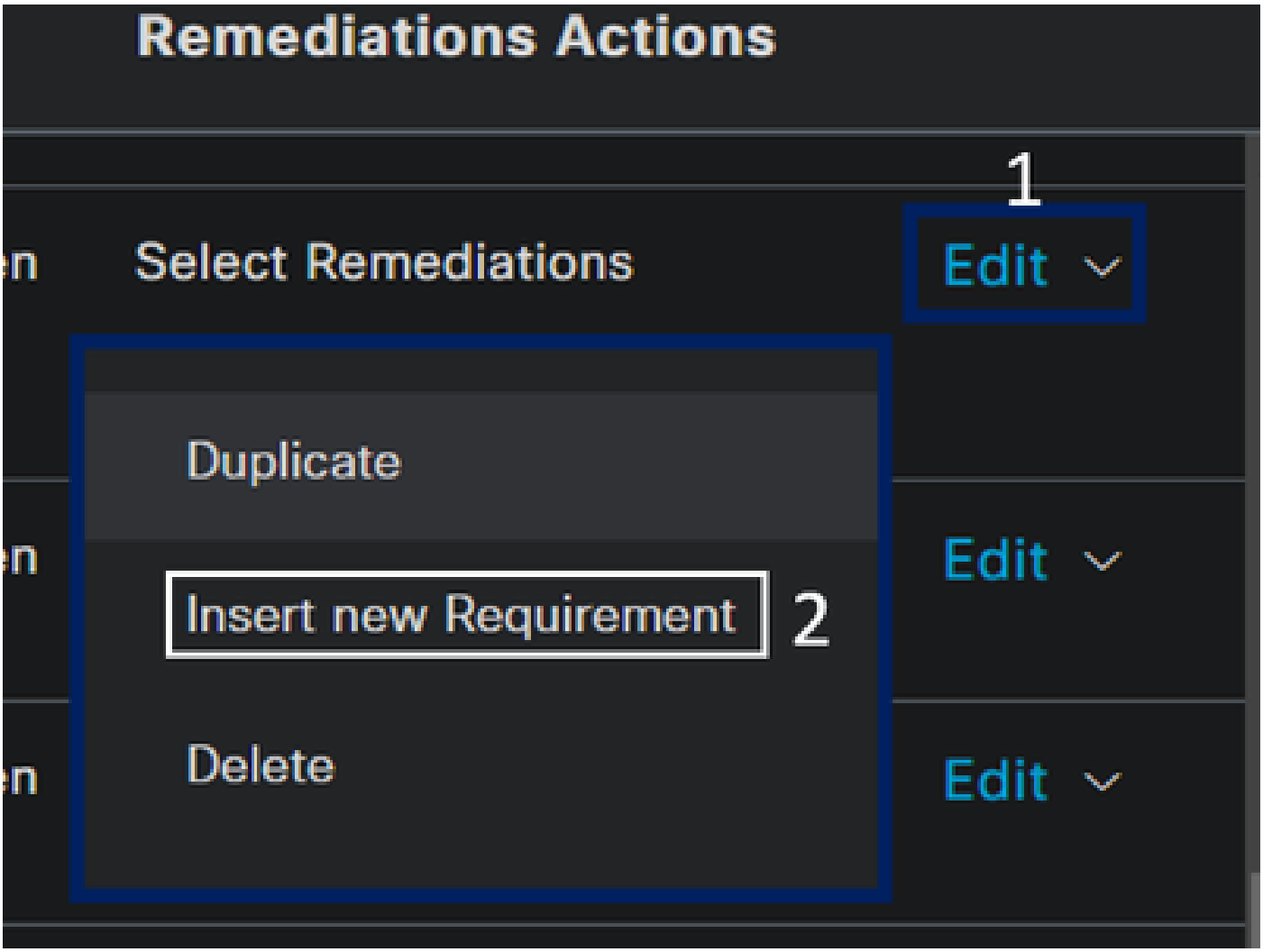


- Aktivieren Sie das Kontrollkästchen für die Bedingungen, die Sie evaluieren möchten.
- Konfigurieren Sie die zu überprüfende Mindestversion.
- Klicken Sie auf Speichern, um mit dem nächsten Schritt fortzufahren

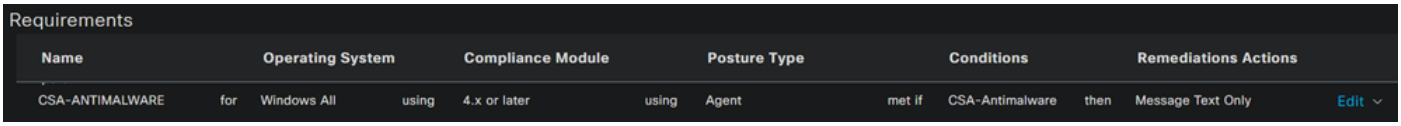
Sobald Sie es konfigurieren, können Sie mit dem Schritt fortfahren, **Configure Posture Requirements**.

Statusanforderungen konfigurieren

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Policy Elements > Requeriments**
- Klicken Sie auf eine **Edit** der Anforderungen, und klicken Sie auf **Insert new Requirement**



- Konfigurieren Sie unter den neuen Anforderungen die folgenden Parameter:



- **Name**: Konfigurieren Sie einen Namen, um die Anti-Malware-Anforderung zu erkennen.

- **Operating System**: Wählen Sie das Betriebssystem, das Sie unter der Bedingung Schritt, Betriebssystem

- **Compliance Module**: Sie müssen sicherstellen, dass Sie das gleiche Compliance-Modul, das Sie unter der Bedingung Schritt, Anti-Malware-Bedingung haben

- **Posture Type**: Agent auswählen

- **Conditions**: Wählen Sie die Bedingung(en), die Sie im Schritt "Statusbedingungen konfigurieren" erstellt haben.

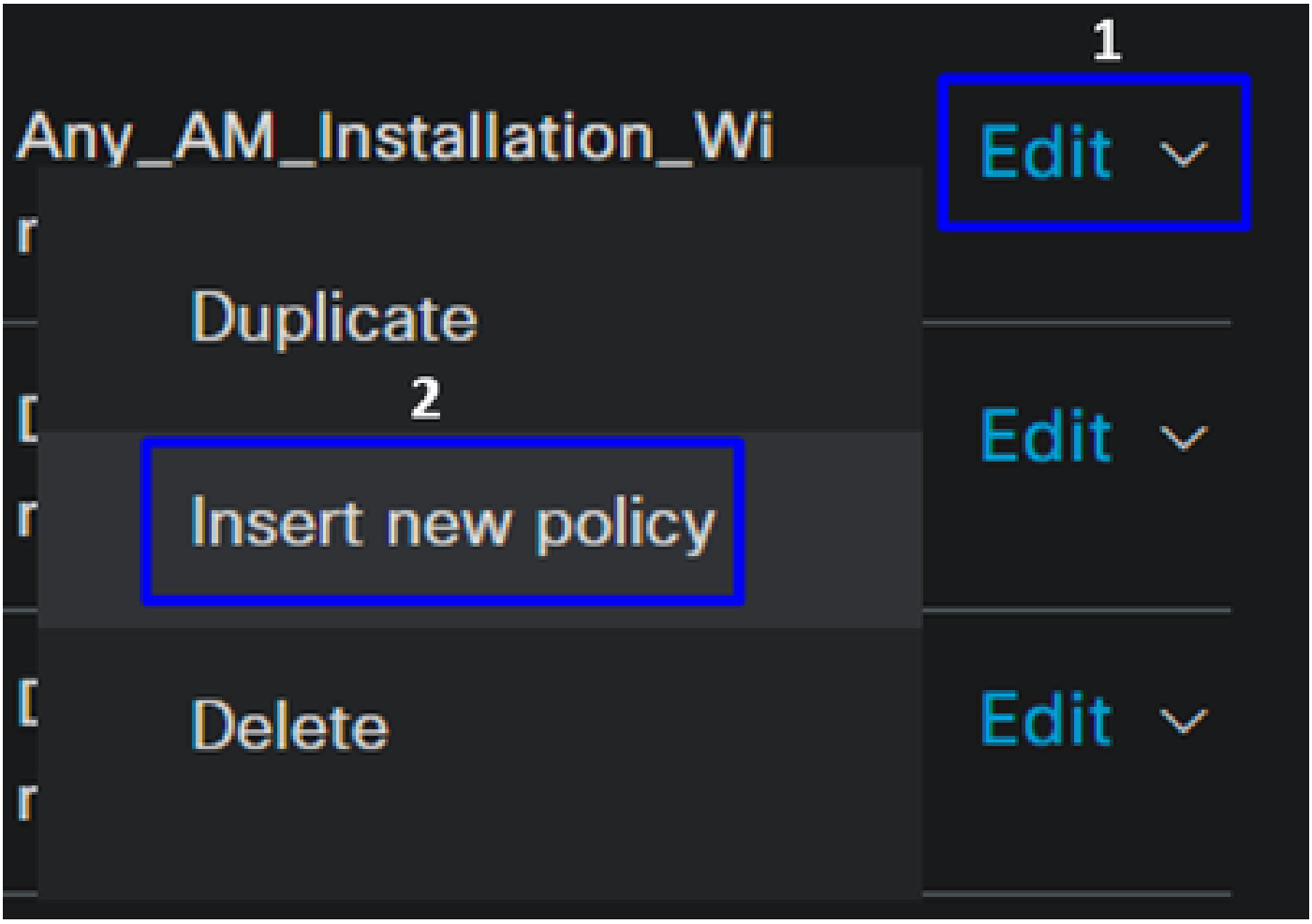
- **Remediations Actions**: Wählen Sie **Message Text Only** für dieses Beispiel aus, oder verwenden Sie eine andere Wiederherstellungsaktion.

- Klicken Sie auf **Save**

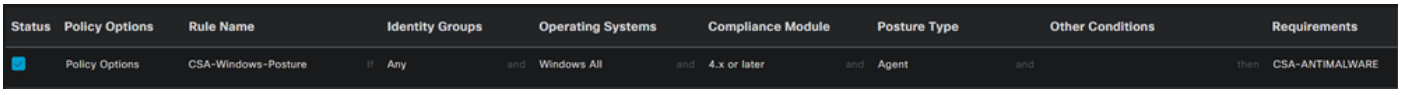
Nach der Konfiguration können Sie mit dem Schritt fortfahren, **Configure Posture Policy**

Statusrichtlinie konfigurieren

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Posture Policy**
- Klicken Sie auf eine **Edit** der Richtlinien, und klicken Sie auf **Insert new Policy**



- Konfigurieren Sie unter der neuen Richtlinie die folgenden Parameter:



- **Status**: Aktivieren Sie das Kontrollkästchen zum Aktivieren der Richtlinie.
- **Rule Name**: Konfigurieren Sie einen Namen zur Erkennung der konfigurierten Richtlinie.

- **Identity Groups**: Wählen Sie die zu bewertenden Identitäten aus.
- **Operating Systems**: Wählen Sie das Betriebssystem basierend auf der Bedingung und den zuvor konfigurierten Anforderungen aus.
- **Compliance Module**: Wählen Sie das Compliance-Modul basierend auf der Bedingung und den zuvor konfigurierten Anforderungen aus.
- Posture Type: Agent auswählen
- **Requeriments**: Wählen Sie die auf dem Schritt konfigurierten Anforderungen, Configure Posture Requirements
- Klicken Sie auf **Save**

Konfiguration der Client-Bereitstellung

Um den Benutzern das ISE-Modul bereitzustellen, konfigurieren Sie die Client-Bereitstellung so, dass die Computer mit dem ISE-Statusmodul ausgestattet werden. Auf diese Weise können Sie den Systemstatus überprüfen, sobald der Agent installiert wurde. Um mit diesem Prozess fortzufahren, gehen Sie wie folgt vor:

Navigieren Sie zu Ihrem ISE Dashboard.

- Klicken Sie **Work Center > Client Provisioning**
- Auswählen **Resources**

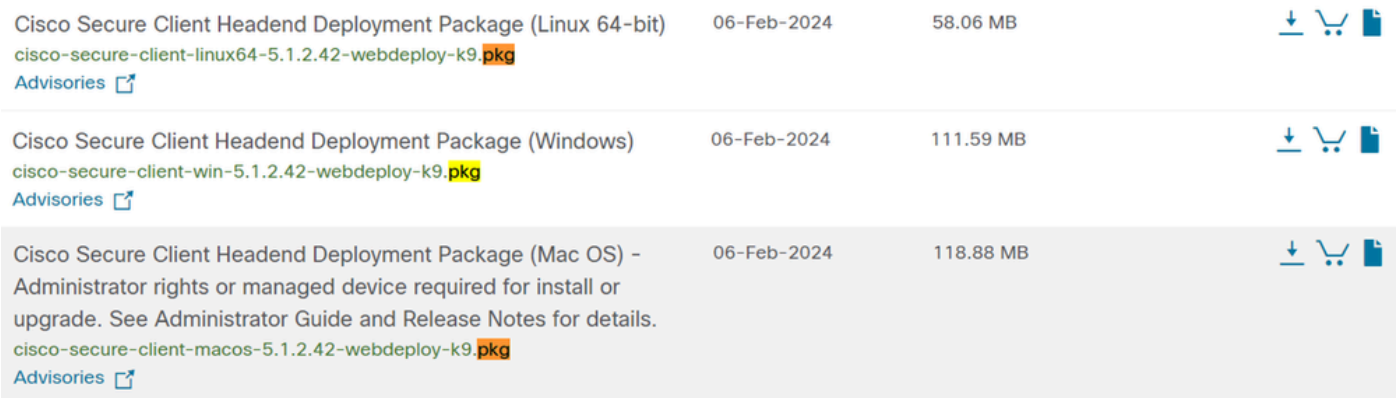
Bei der Clientbereitstellung müssen drei Dinge konfiguriert werden:

Zu konfigurierende Ressourcen	Beschreibung
1. **Agent Resources**	Secure Client-Webbereitstellungspaket.
2. **Compliance Module**	Cisco ISE Compliance-Modul
3. **Agent Profile**	Steuerung des Bereitstellungsprofils
3. **Agent Configuration**	Legen Sie fest, welche Module bereitgestellt werden sollen, indem Sie das Bereitstellungsportal mithilfe des Agentenprofils und der Agentenressourcen

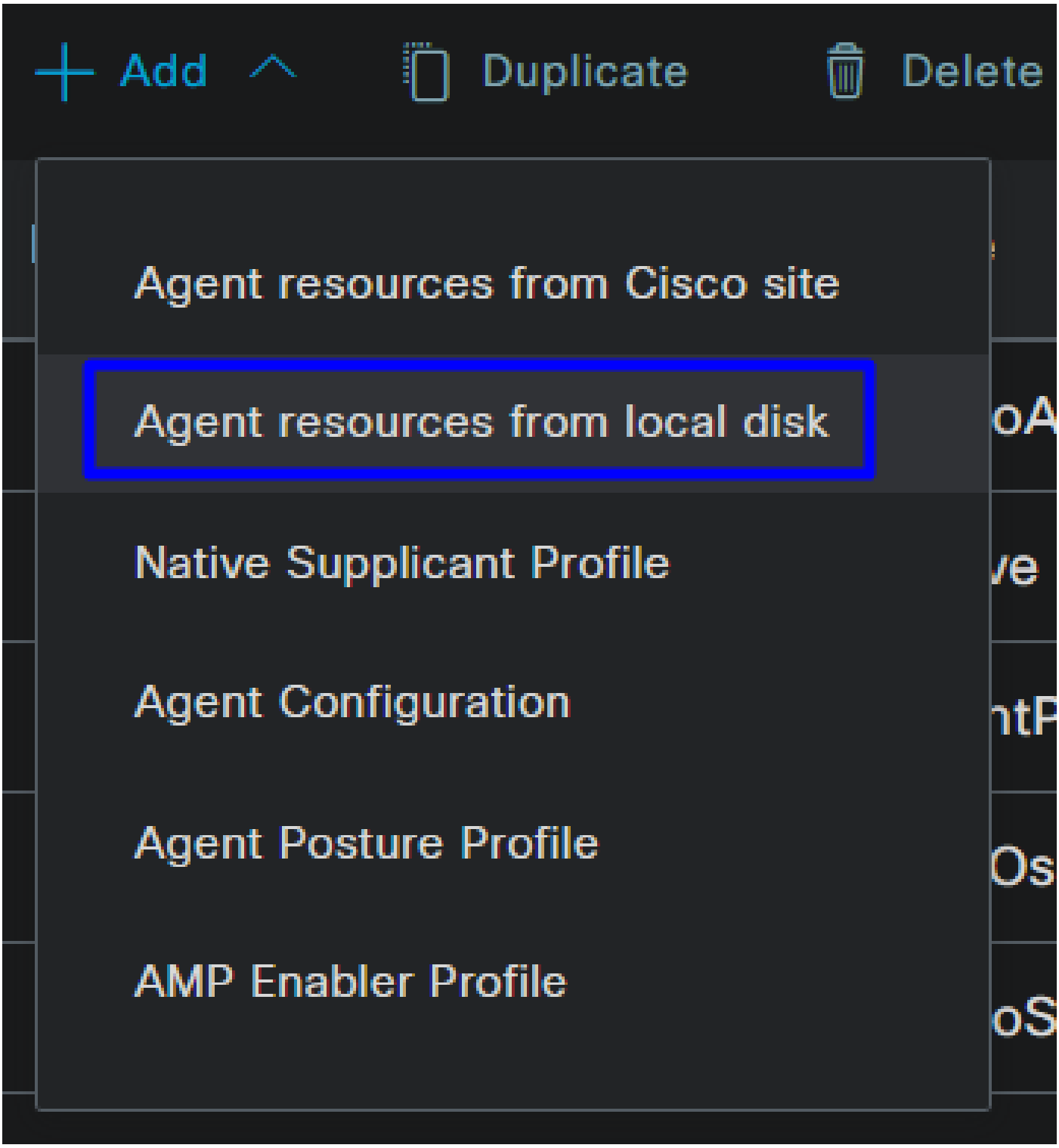
	einrichten.

Step 1 Agentenressourcen herunterladen und hochladen

- Um eine neue Agentenressource hinzuzufügen, navigieren Sie zum Cisco Download-Portal, und laden Sie das Web-Bereitstellungspaket herunter. Die Web-Bereitstellungsdatei muss das Format .pkg aufweisen.

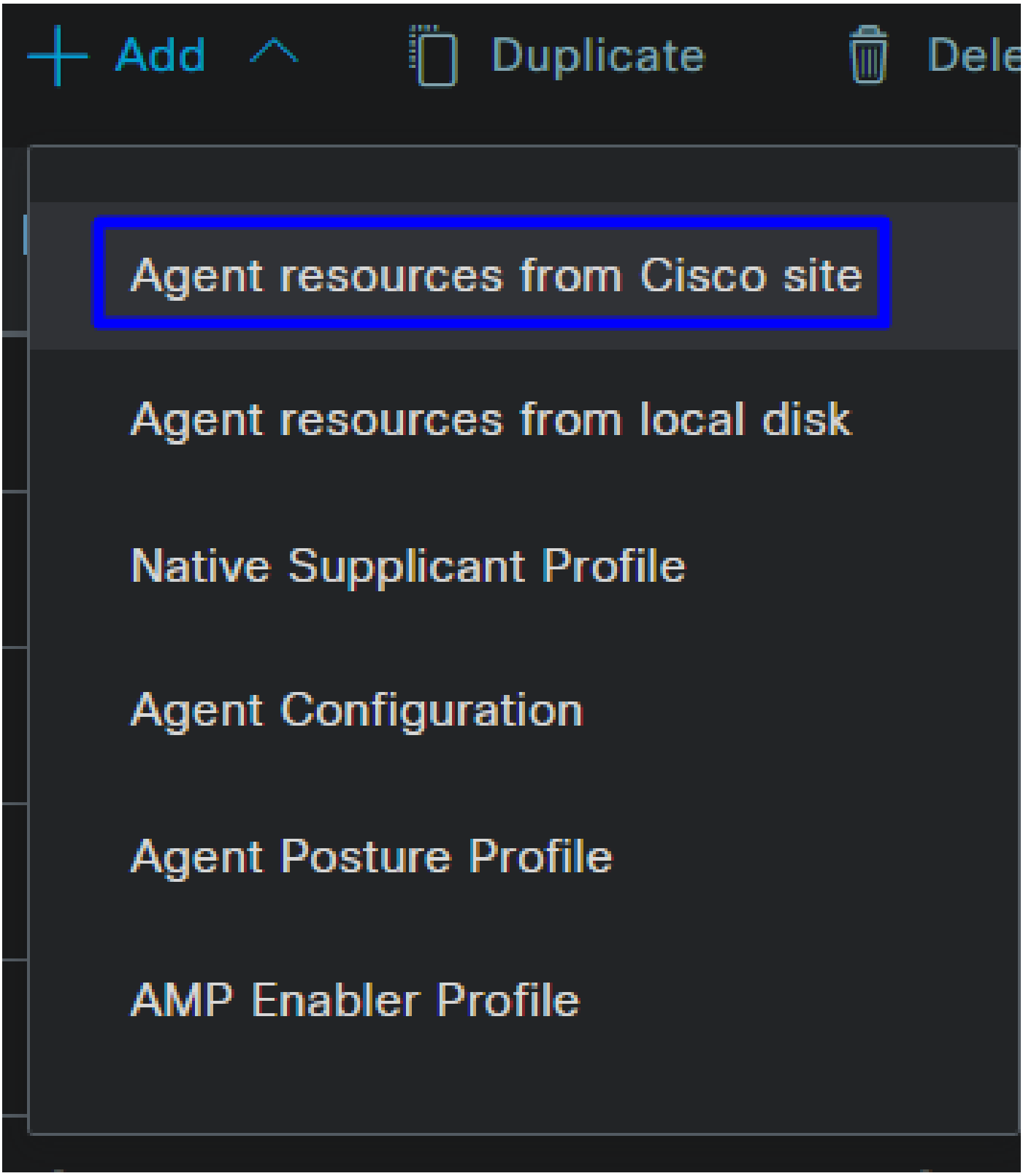


- Klicken Sie auf + Add > Agent resources from local disk und laden Sie die Pakete hoch.

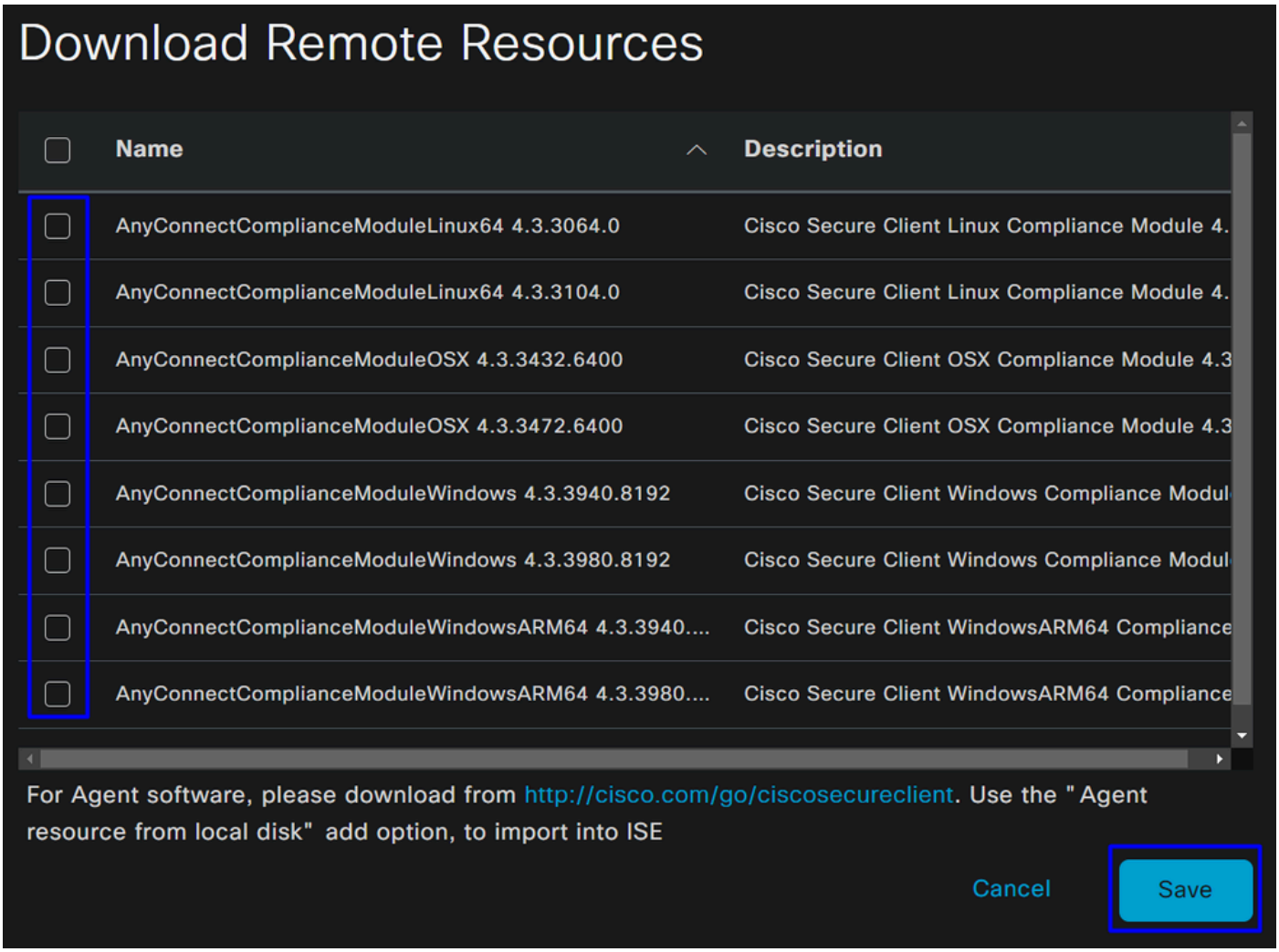


Step 2 Compliance-Modul herunterladen

- Klicken Sie + Add > Agent resources from Cisco Site

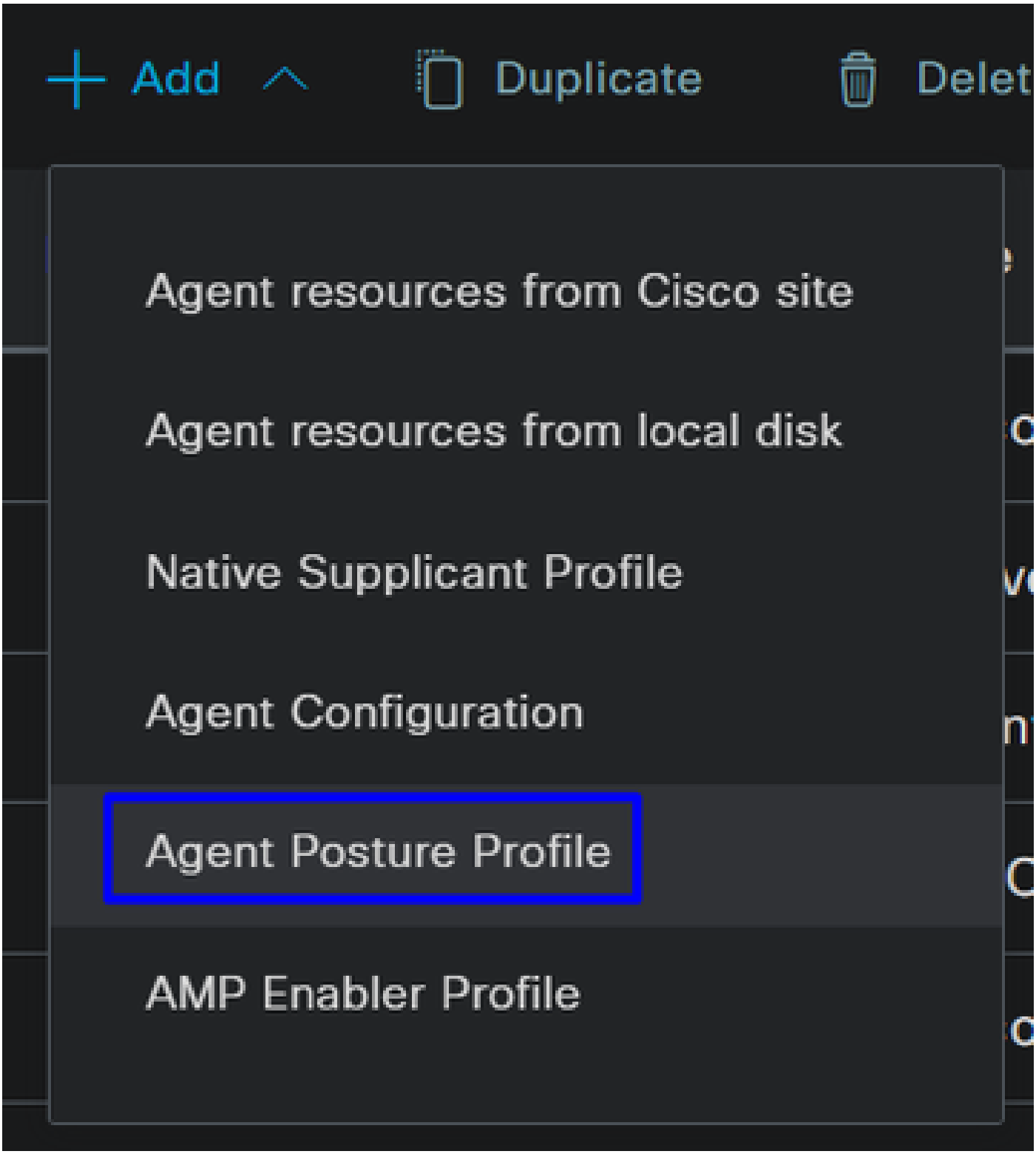


- Aktivieren Sie das Kontrollkästchen für jedes erforderliche Compliance-Modul, und klicken Sie auf **Save**

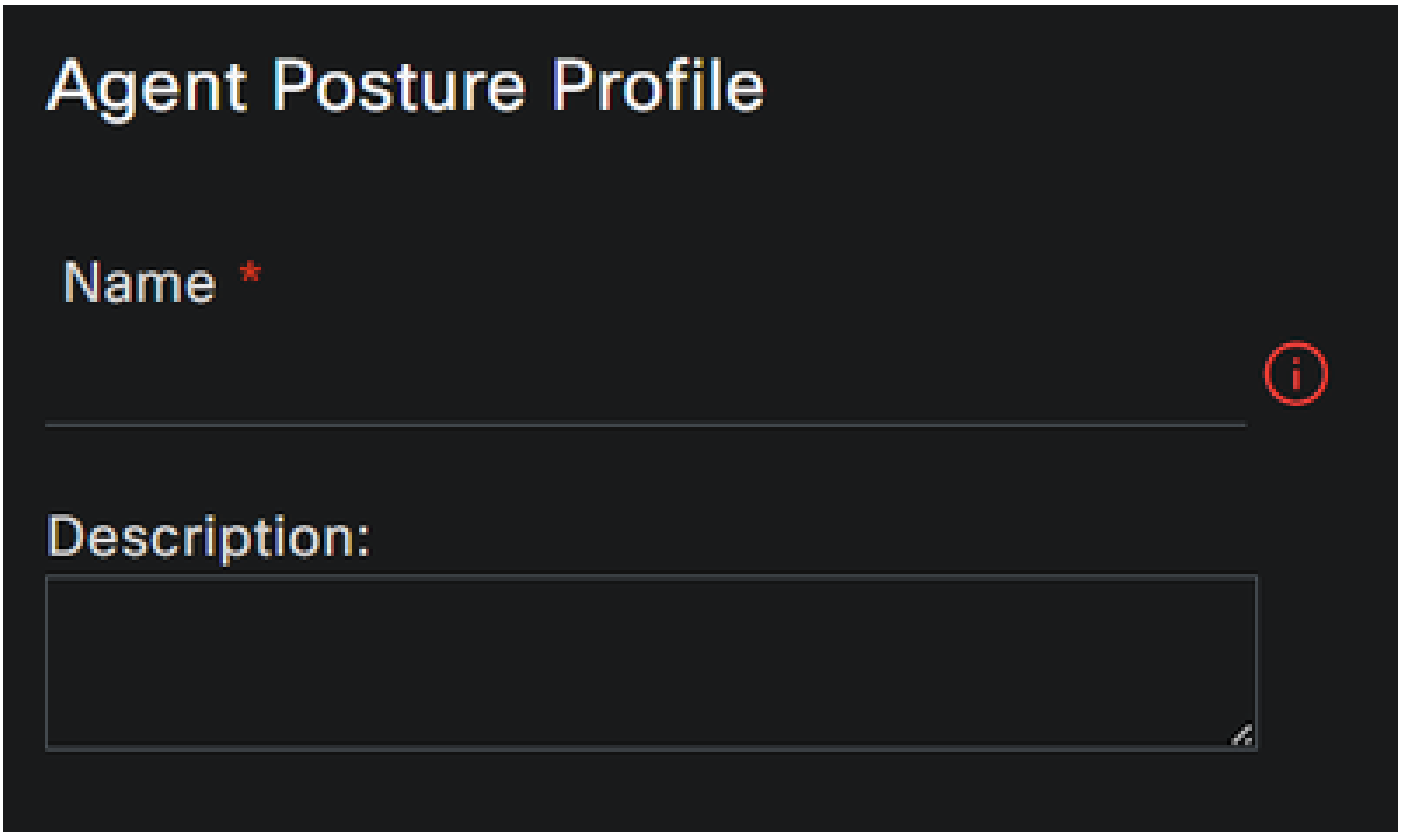


Step 3Konfigurieren des Agentenprofils

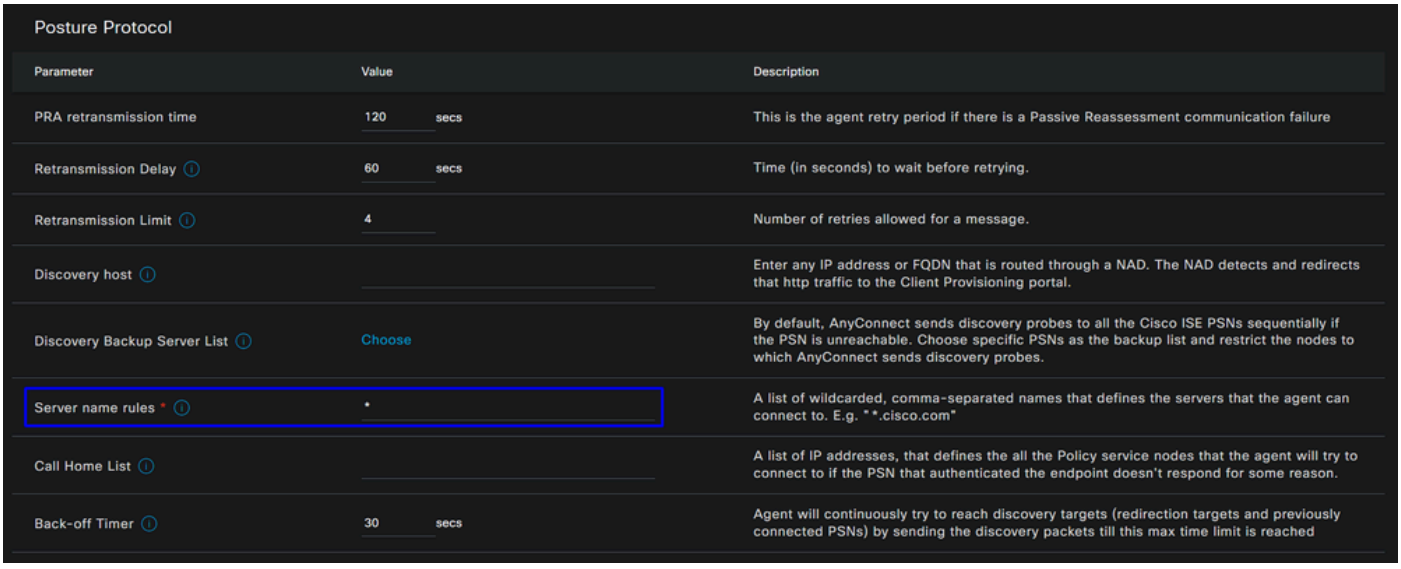
- Klicken Sie + Add > Agent Posture Profile



- Erstellen Sie einen **Name** für **Posture Profile**

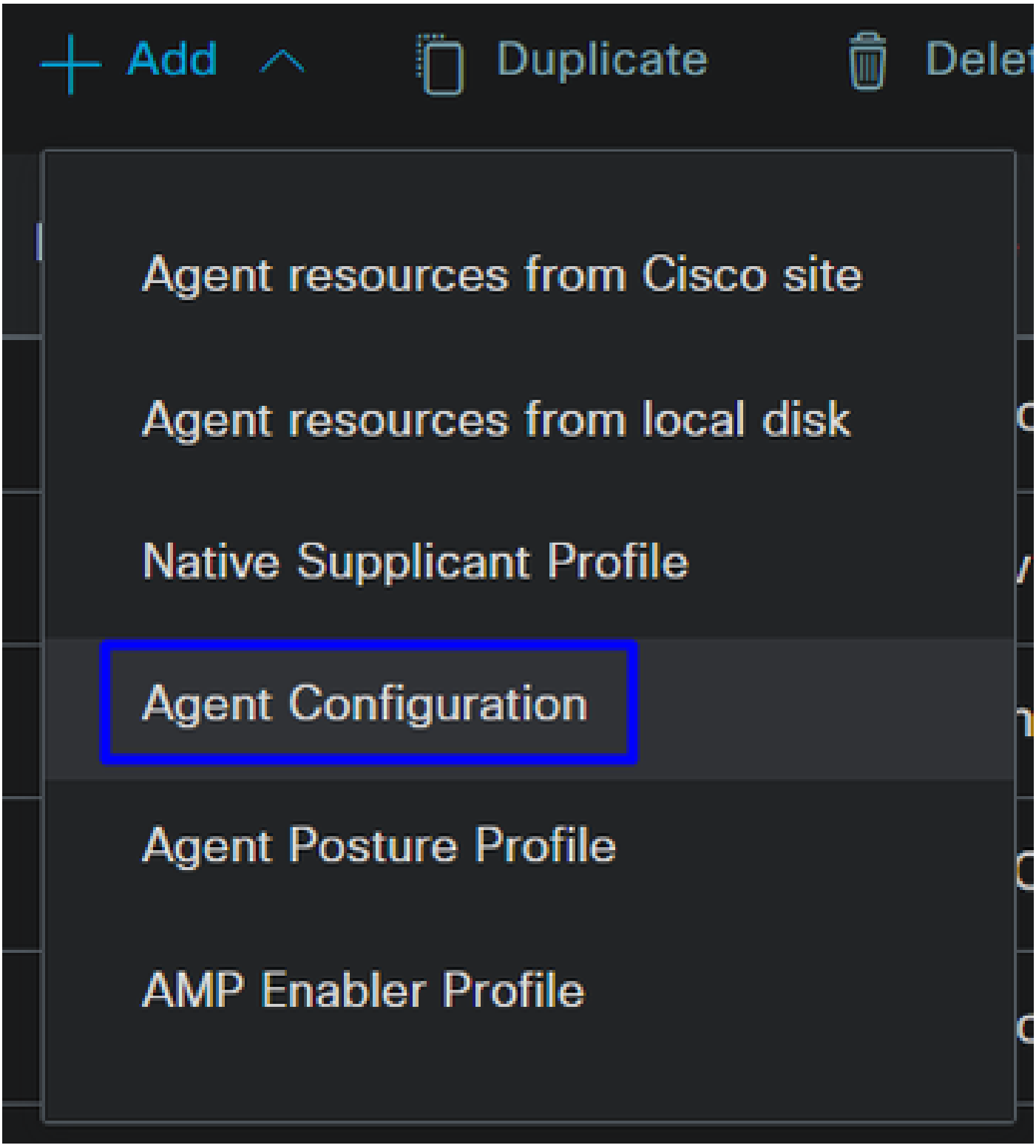


- Legen Sie unter "Servernamen" ein ***** und klicken Sie **Save** danach auf

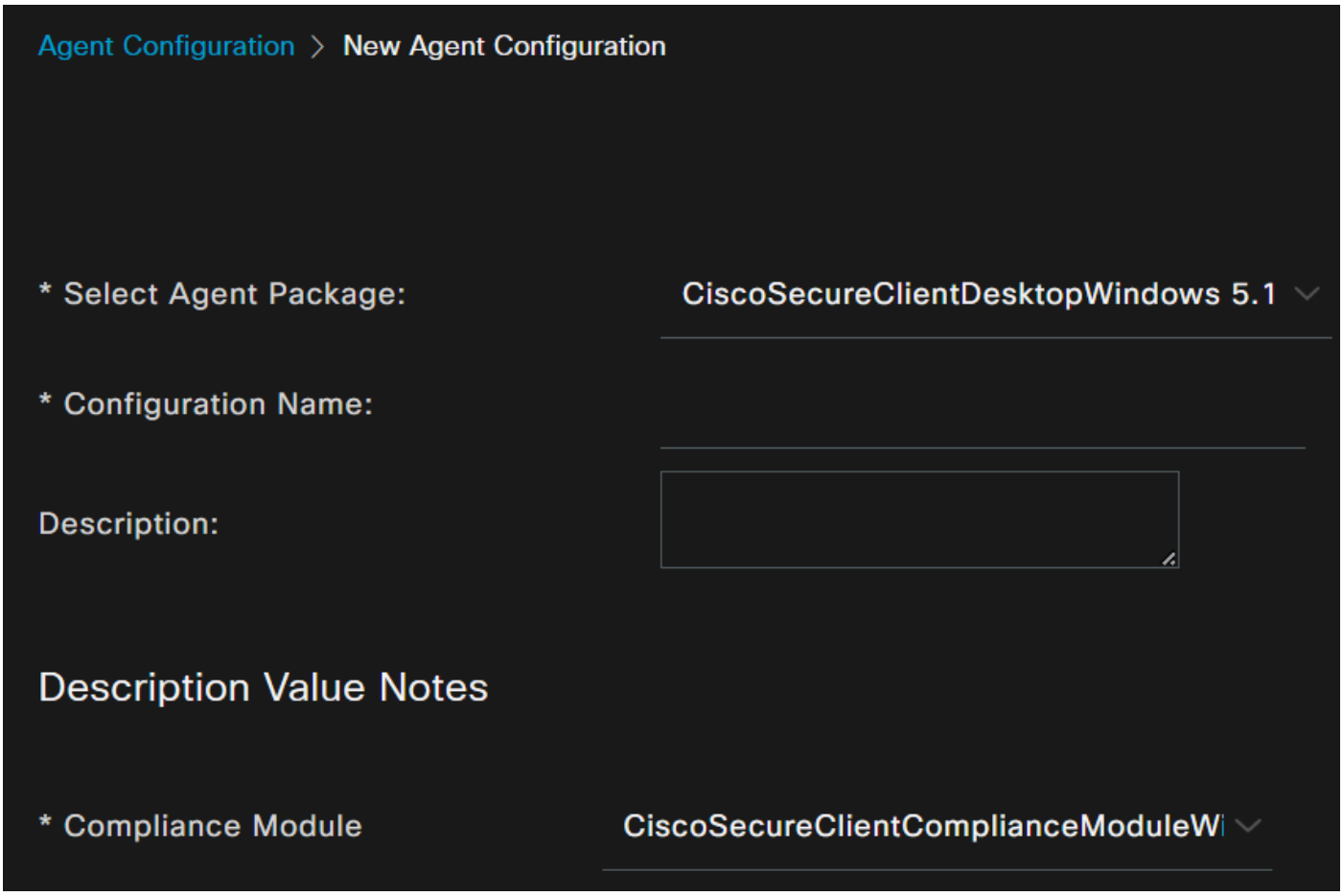


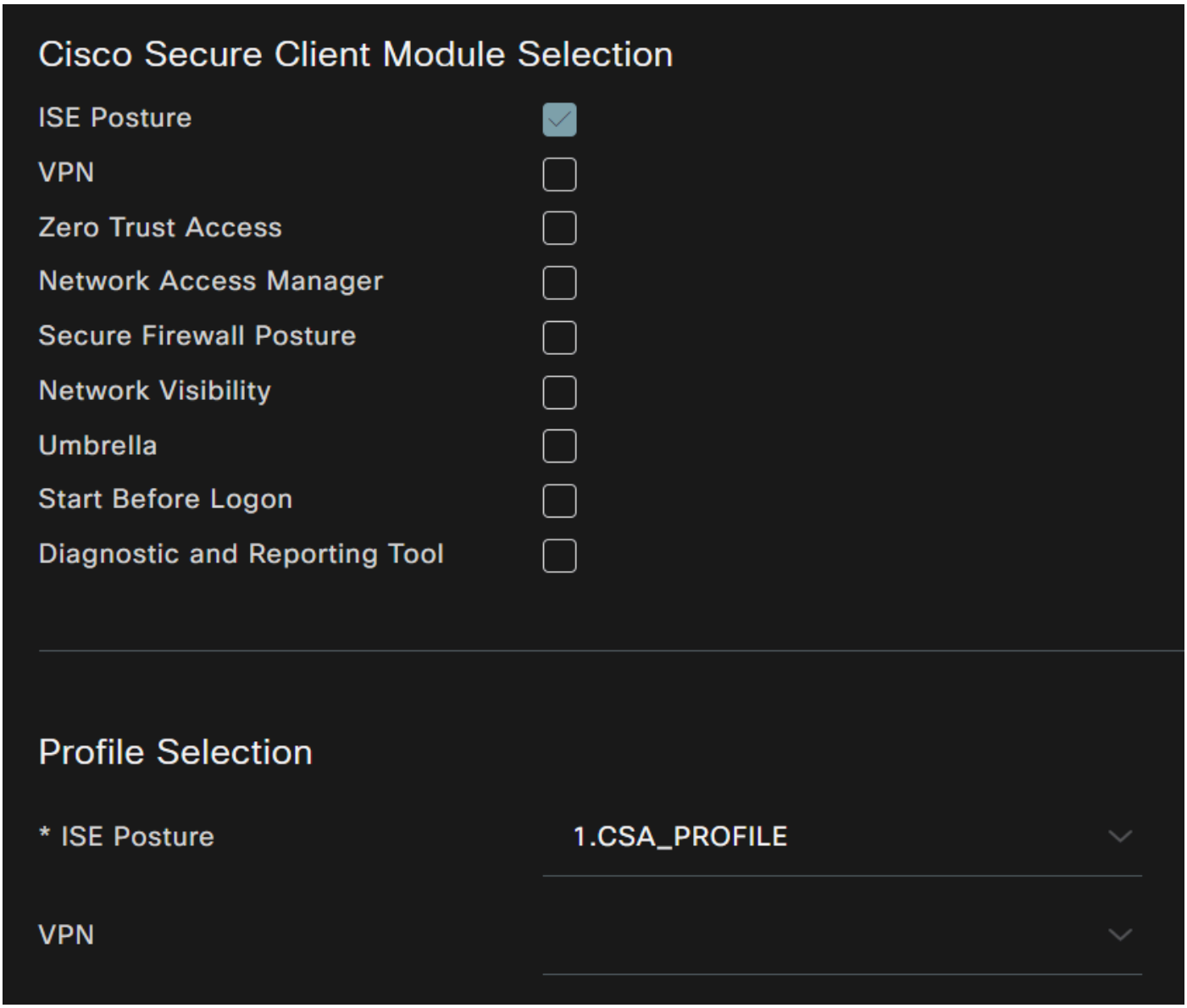
Step 4 Konfigurieren der Agentenkonfiguration

- Klicken Sie + Add > Agent Configuration



- Konfigurieren Sie anschließend die folgenden Parameter:

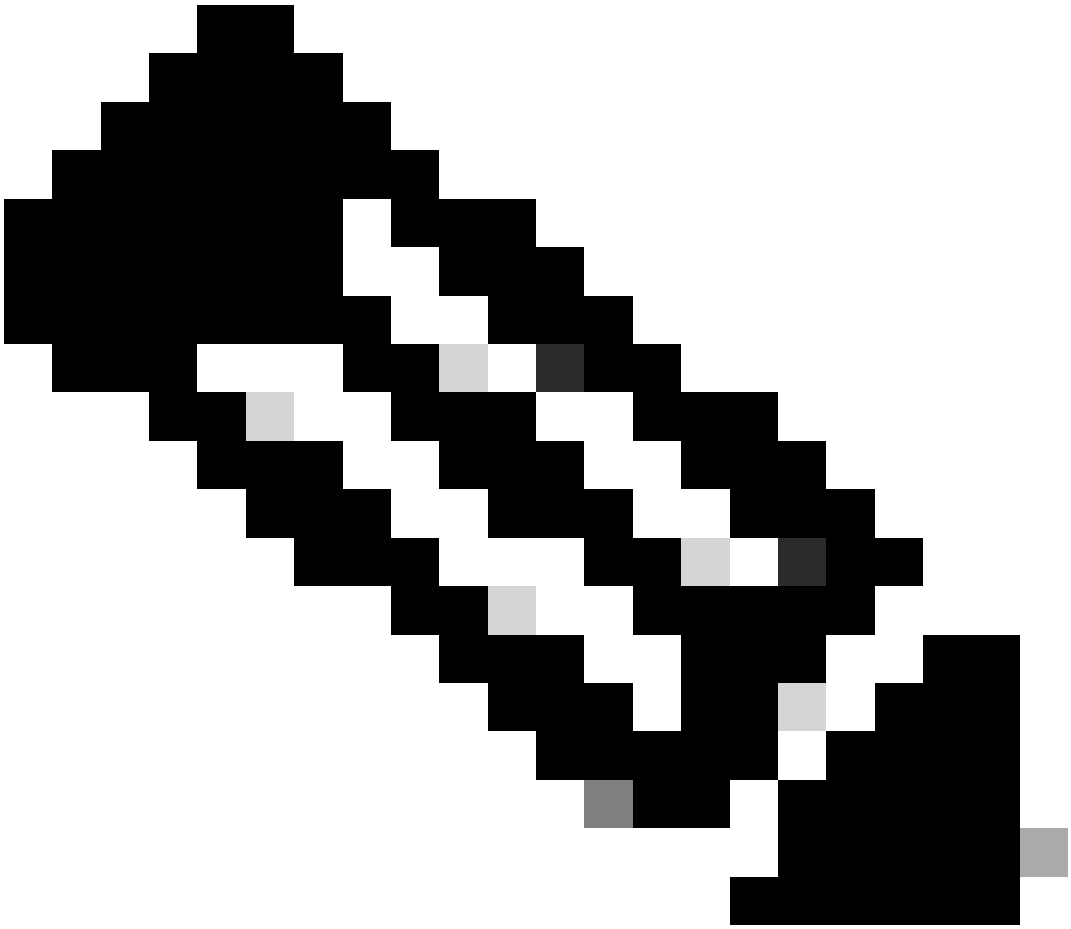

Agent Configuration
New Agent Configuration
* Select Agent Package:
CiscoSecureClientDesktopWindows 5.1
* Configuration Name:
Description:
Description Value Notes
* Compliance Module
CiscoSecureClientComplianceModuleW



- Select Agent Package : Wählen Sie das hochgeladene Paket für die Step1 Download and Upload Agent-Ressourcen aus.
- **Configuration Name**: Wählen Sie einen Namen, um die **Agent Configuration**
- **Compliance Module**: Wählen Sie das Compliance-Modul aus, das Sie auf der Seite Schritt 2 Compliance-Modul herunterladen heruntergeladen haben.
- Cisco Secure Client Module Selection
  - **ISE Posture**: Kontrollkästchen markieren
- **Profile Selection**

- **ISE Posture**: Wählen Sie das ISE-Profil aus, das unter Schritt 3 Konfigurieren des Agent-Profils konfiguriert wurde.

- Klicken Sie auf **Save**

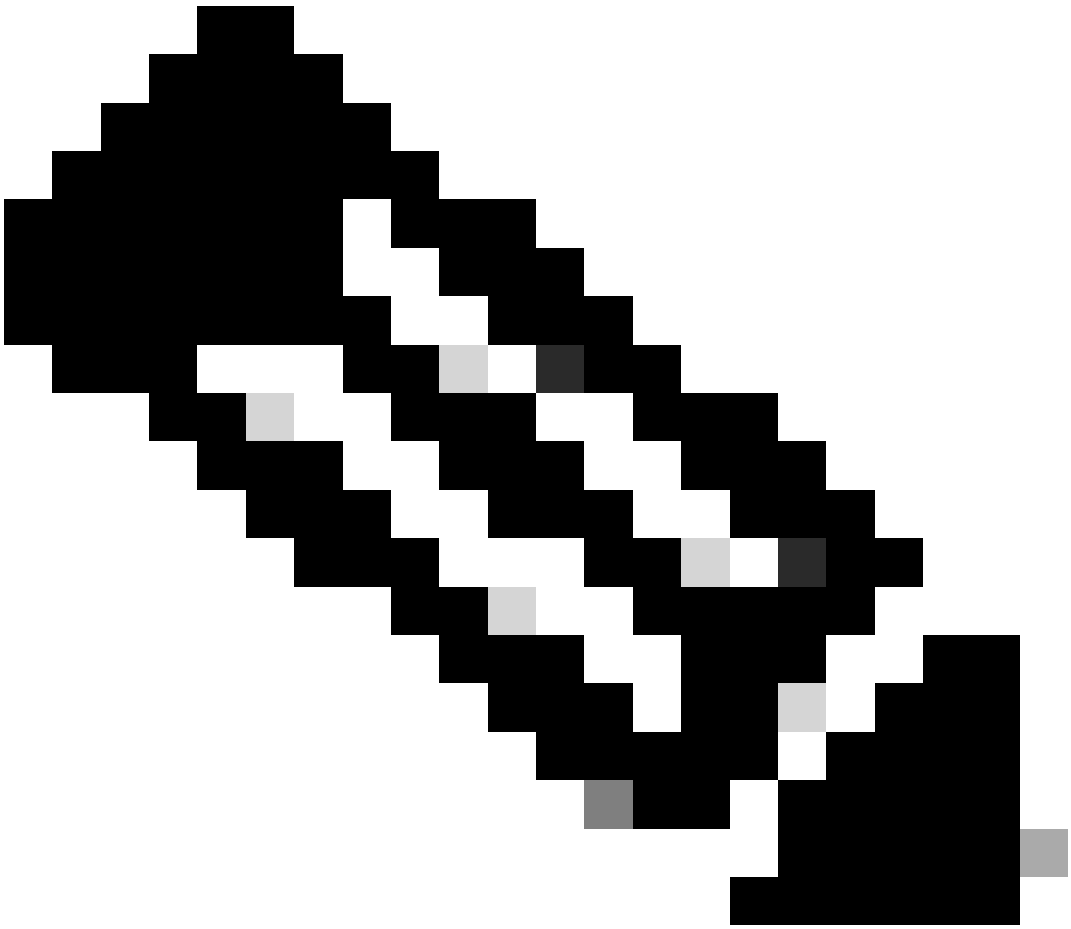


Hinweis: Es wird empfohlen, dass jedes Betriebssystem (Windows, Mac OS oder Linux) über eine unabhängige Client-Konfiguration verfügt.

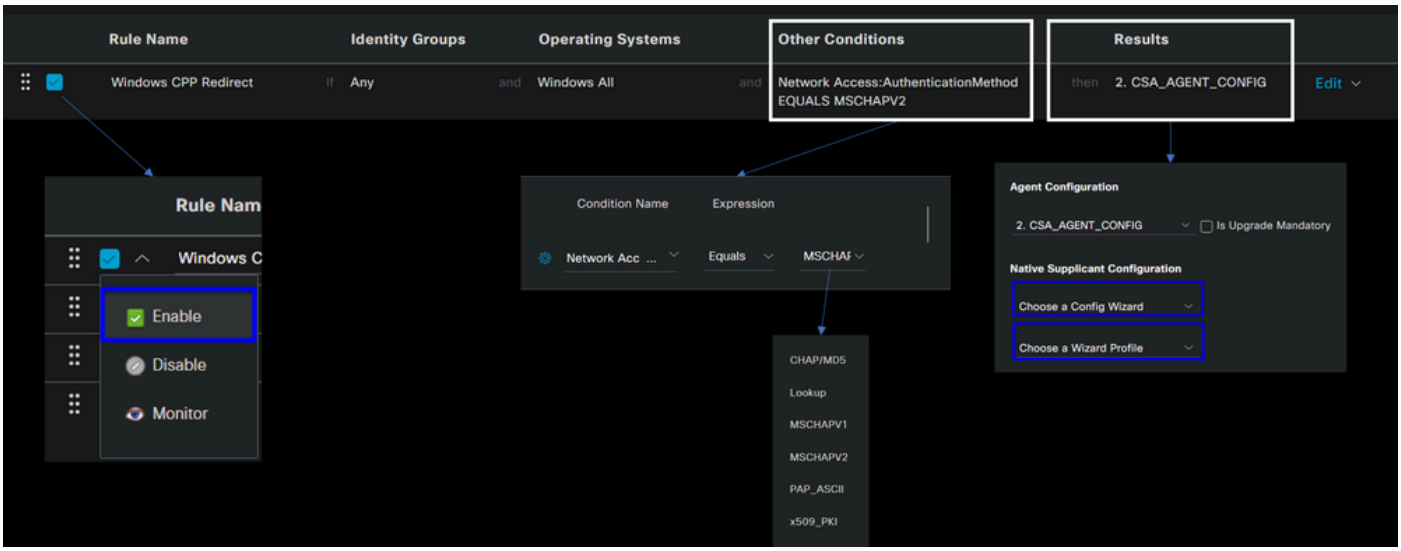
Client-Bereitstellungsrichtlinie konfigurieren

Um die Bereitstellung des ISE-Status und der im letzten Schritt konfigurierten Module zu ermöglichen, müssen Sie eine Richtlinie für die Bereitstellung konfigurieren.

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie **Work Center > Client Provisioning**



Hinweis: Es wird empfohlen, dass für jedes Betriebssystem (Windows, Mac OS oder Linux) eine Client-Konfigurationsrichtlinie gilt.



- **Rule Name**: Konfigurieren Sie den Namen der Richtlinie auf Basis des Gerätetyps und der Identitätsgruppenauswahl, um jede Richtlinie leicht identifizieren zu können.
- **Identity Groups**: Wählen Sie die Identitäten aus, die Sie in der Richtlinie bewerten möchten.
- **Operating Systems**: Wählen Sie das Betriebssystem basierend auf dem Agentenpaket aus, das auf dem Schritt ausgewählt wurde. Wählen Sie Agentenpaket aus.
- **Other Condition**: Wählen Sie **Network Access** basierend auf der **Authentication Method**EQUALS zu der im Schritt konfigurierten Methode, Add RADIUS Group (RADIUS-Gruppe hinzufügen) aus, oder lassen Sie das Feld leer.
- **Result**: Wählen Sie die unter Schritt 4 Konfigurieren der Agentenkonfiguration konfigurierte Agentenkonfiguration aus.
  - **Native Supplicant Configuration**: Wählen Sie Config Wizard und Wizard Profile
- Markieren Sie die Richtlinie als aktiviert, wenn sie nicht im Kontrollkästchen als aktiviert aufgeführt ist.

Erstellen der Autorisierungsprofile

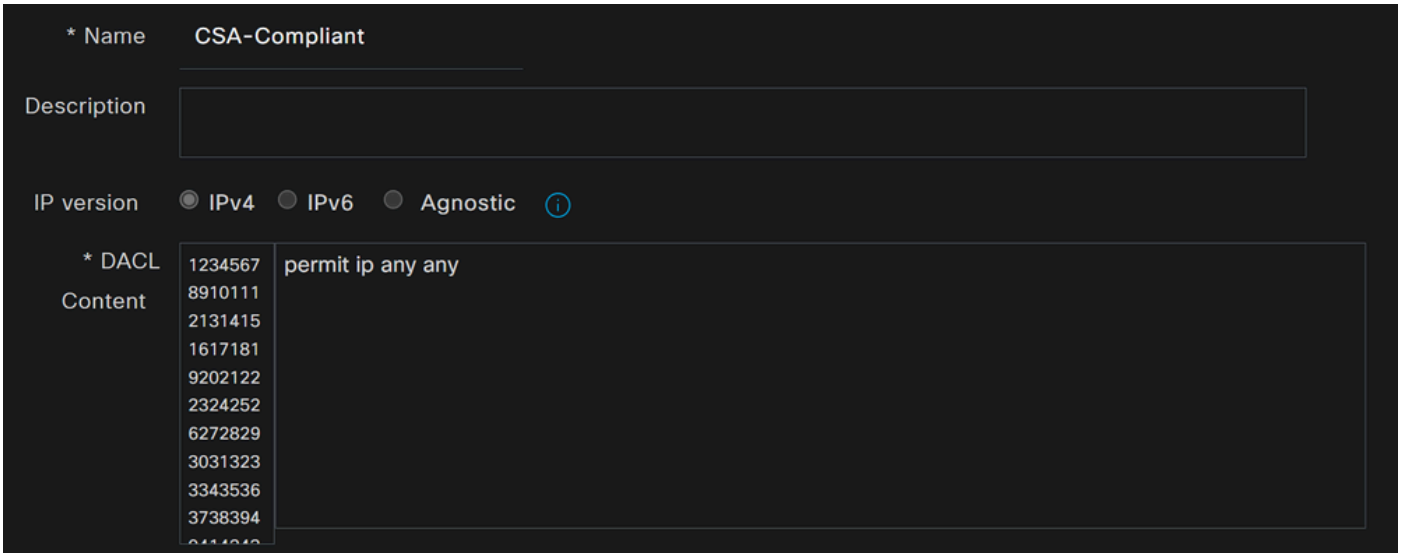
Das Autorisierungsprofil schränkt den Zugriff auf die Ressourcen je nach dem Benutzerstatus nach dem Authentifizierungsprozess ein. Die Autorisierung muss überprüft werden, um anhand des Status zu bestimmen, auf welche Ressourcen der Benutzer zugreifen kann.

Autorisierungsprofil	Beschreibung
Konformität	Benutzerkonform - Agent installiert - Status verifiziert
Unbekannte	Benutzer nicht bekannt - Umleitung zur Installation des Agenten - Zur

Compliance	Überprüfung ausstehende Statusüberprüfung
Zugriff verweigern	Benutzer nicht konform - Zugriff verweigern

Um die DACL zu konfigurieren, navigieren Sie zum ISE Dashboard:

- Klicken Sie **Work Centers > Policy Elements > Downloadable ACLs**
- Klicken Sie **+Add**
- Erstellen Sie **Compliant DACL**



- **Name**: Fügen Sie einen Namen hinzu, der auf die DACL-konforme
- **IP version**: Auswahl **IPv4**
- DACL Content: Erstellen Sie eine herunterladbare Zugriffskontrollliste (DACL), die Zugriff auf alle Ressourcen des Netzwerks bietet.

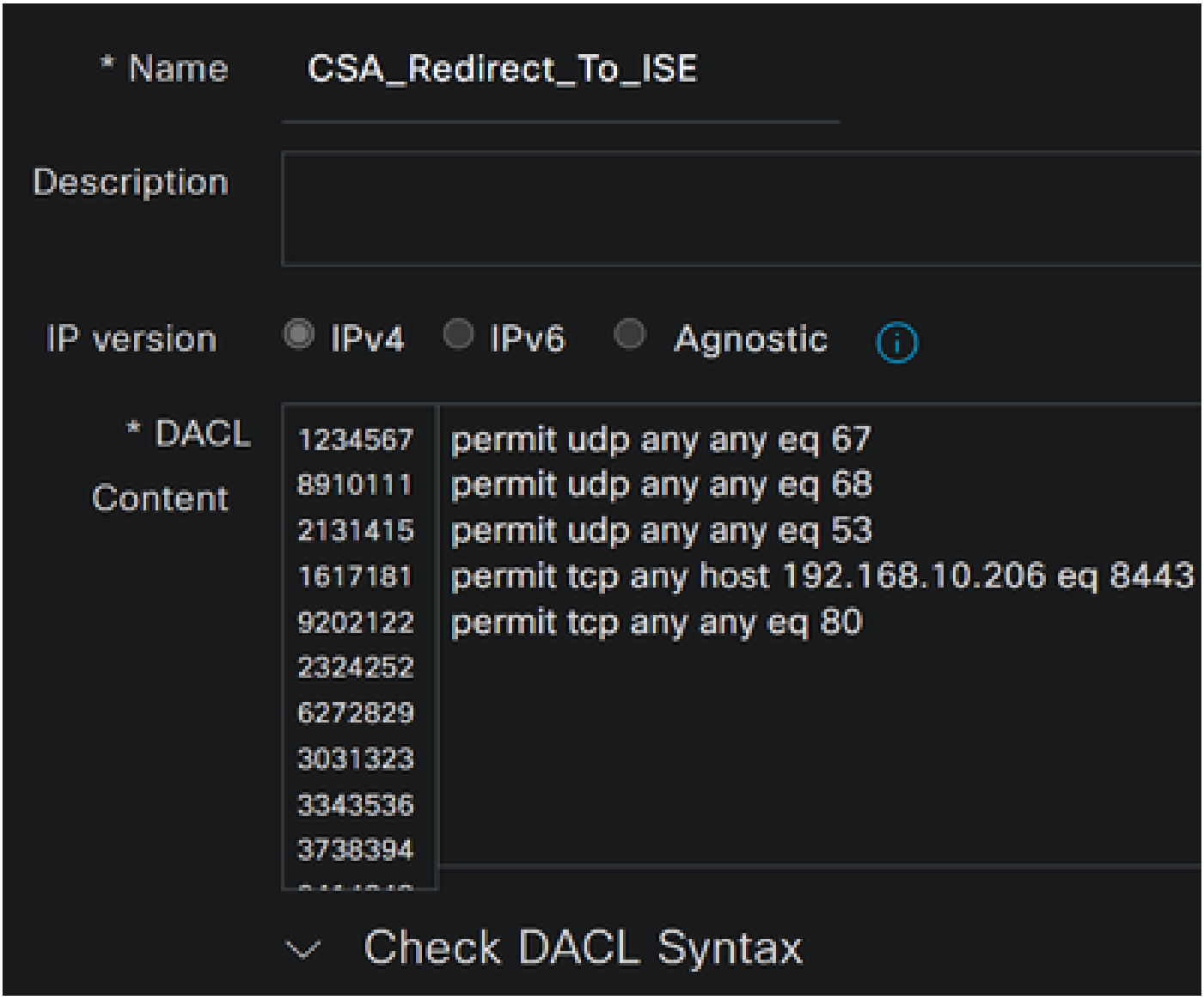
<#root>

```
permit ip any any
```

Klicken Sie auf, **Save** und erstellen Sie die unbekannte Compliance-DACL.

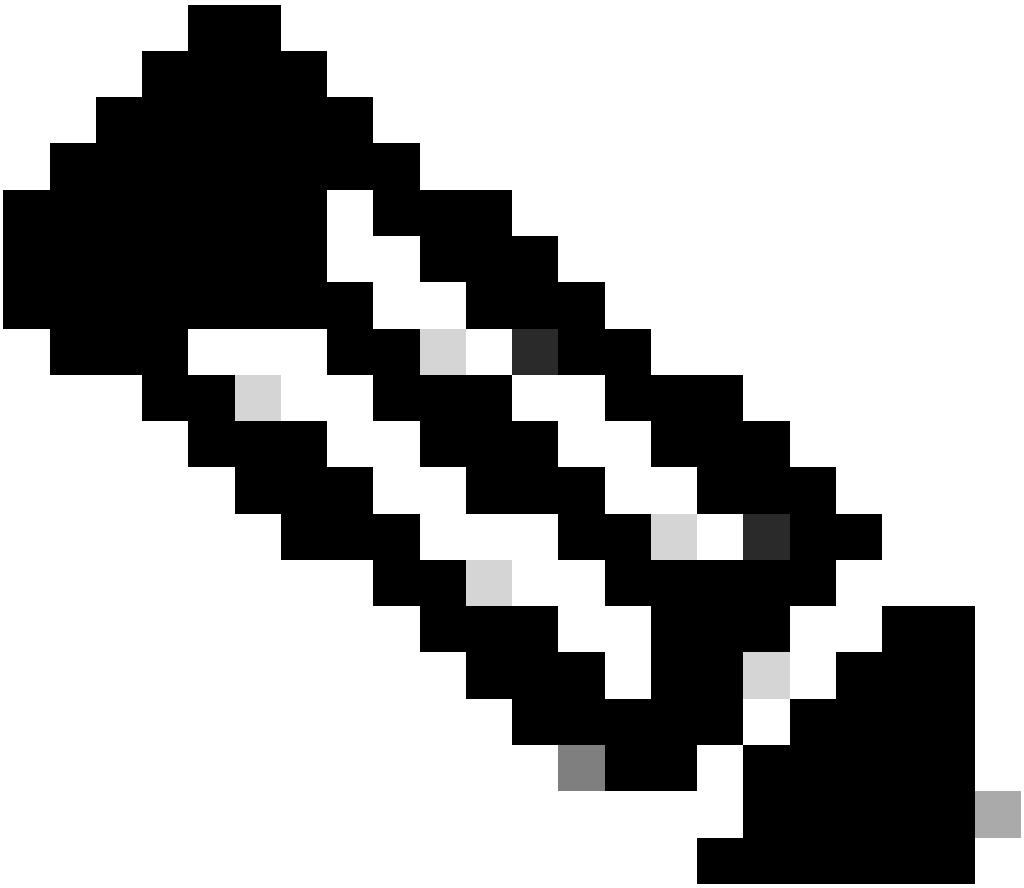
- Klicken Sie **Work Centers > Policy Elements > Downloadable ACLs**

- Klicken Sie **+Add**
- Erstellen Sie **Unknown Compliant DACL**



- **Name**: Fügen Sie einen Namen hinzu, der auf die DACL-Unknown-Compliant verweist.
- **IP version**: Auswahl **IPv4**
- **DACL Content**: Erstellen einer DACL mit eingeschränktem Zugriff auf Netzwerk, DHCP, DNS, HTTP und das Bereitstellungsportal über Port 8443

```
permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80
permit tcp any host 192.168.10.206 eq 8443
```

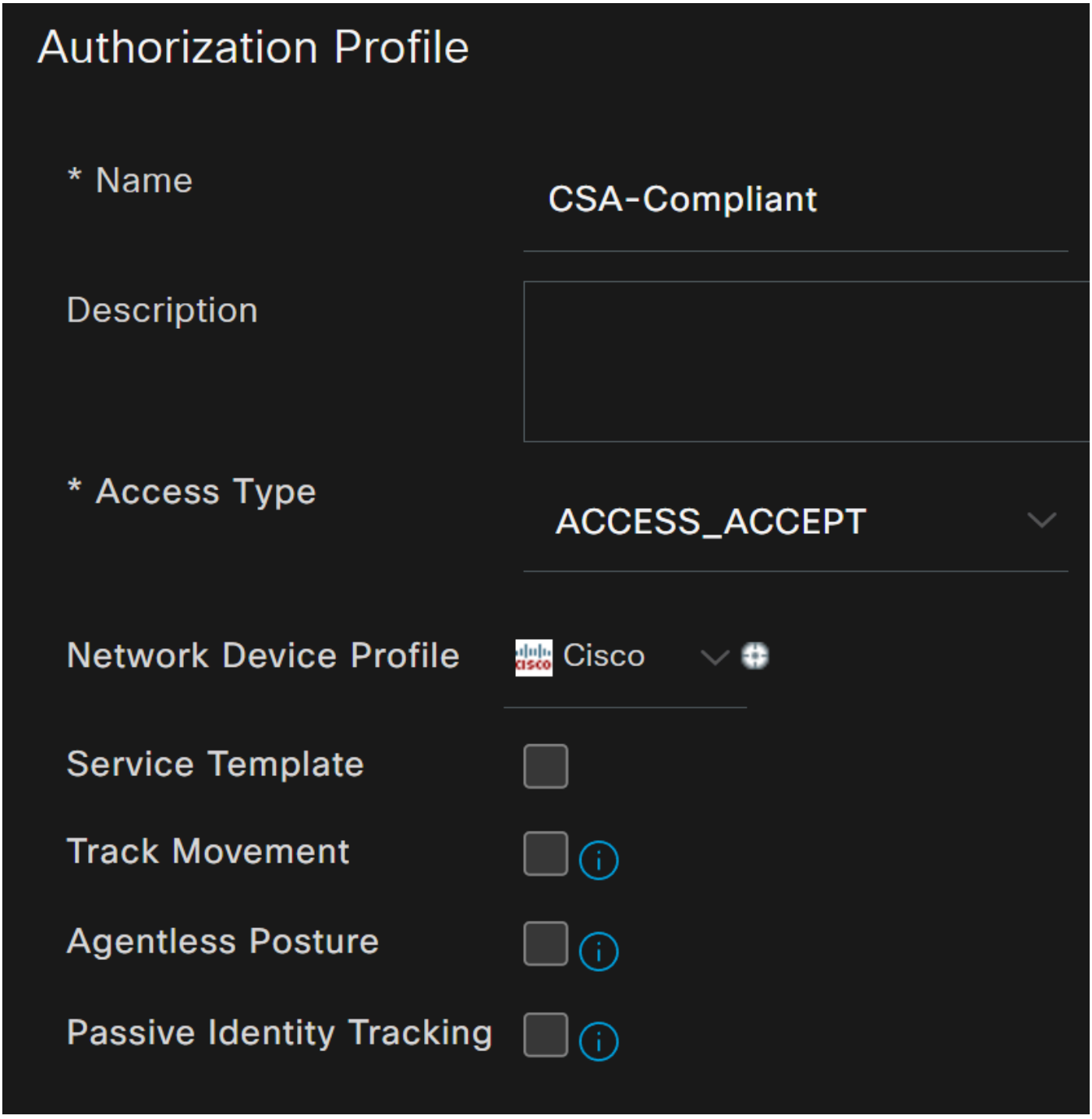


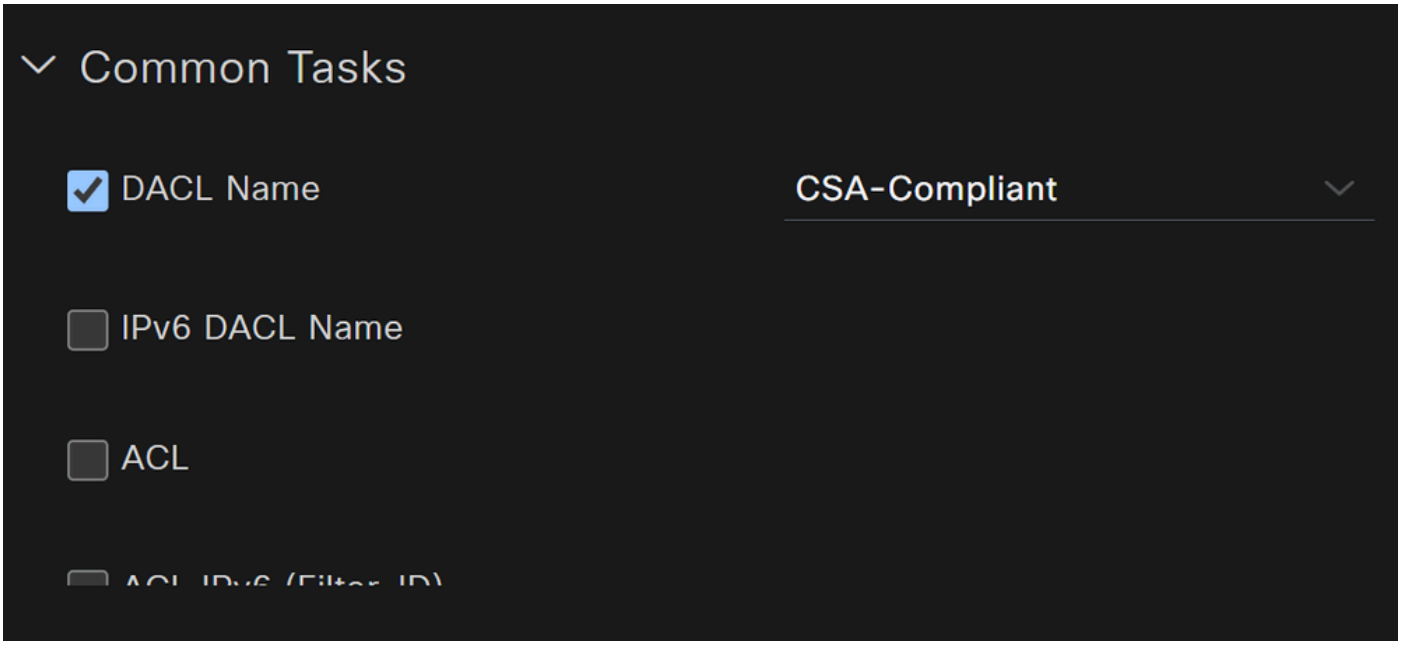
Hinweis: In diesem Szenario entspricht die IP-Adresse 192.168.10.206 dem Cisco Identity Services Engine (ISE)-Server, und Port 8443 ist für das Bereitstellungsportal festgelegt. Dies bedeutet, dass TCP-Datenverkehr an die IP-Adresse 192.168.10.206 über Port 8443 zugelassen wird, wodurch der Zugriff auf das Bereitstellungsportal erleichtert wird.

Jetzt verfügen Sie über die erforderliche DACL zum Erstellen der Autorisierungsprofile.

Rufen Sie zum Konfigurieren der Autorisierungsprofile das ISE Dashboard auf:

- Klicken Sie **Work Centers > Policy Elements > Authorization Profiles**
  - Klicken Sie **+Add**
  - Erstellen Sie **Compliant Authorization Profile**





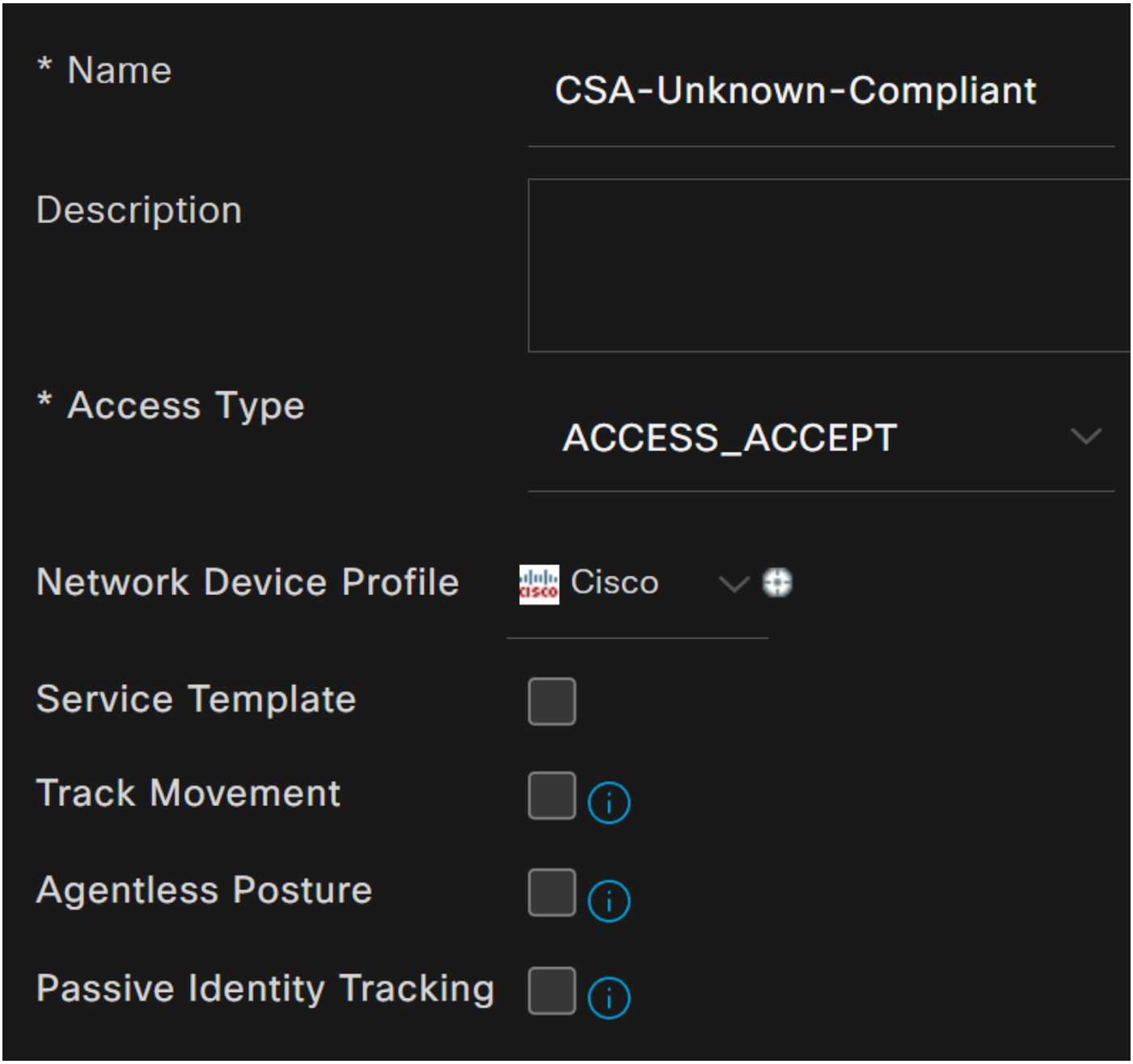
- **Name**: Erstellen Sie einen Namen, der auf das kompatible Autorisierungsprofil verweist.
- Access Type: Auswahl **ACCESS_ACCEPT**

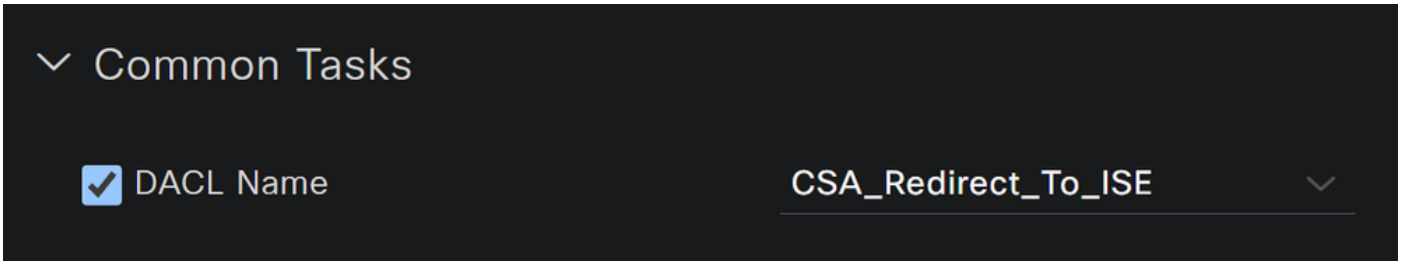
- **Common Tasks**
  - **DACL NAME**: Wählen Sie die auf dem Schritt "Compliant DACL" konfigurierte DACL aus.

Klicken **Save** und erstellen Sie Unknown Authorization Profile

- Klicken Sie **Work Centers > Policy Elements > Authorization Profiles**
- Klicken Sie **+Add**

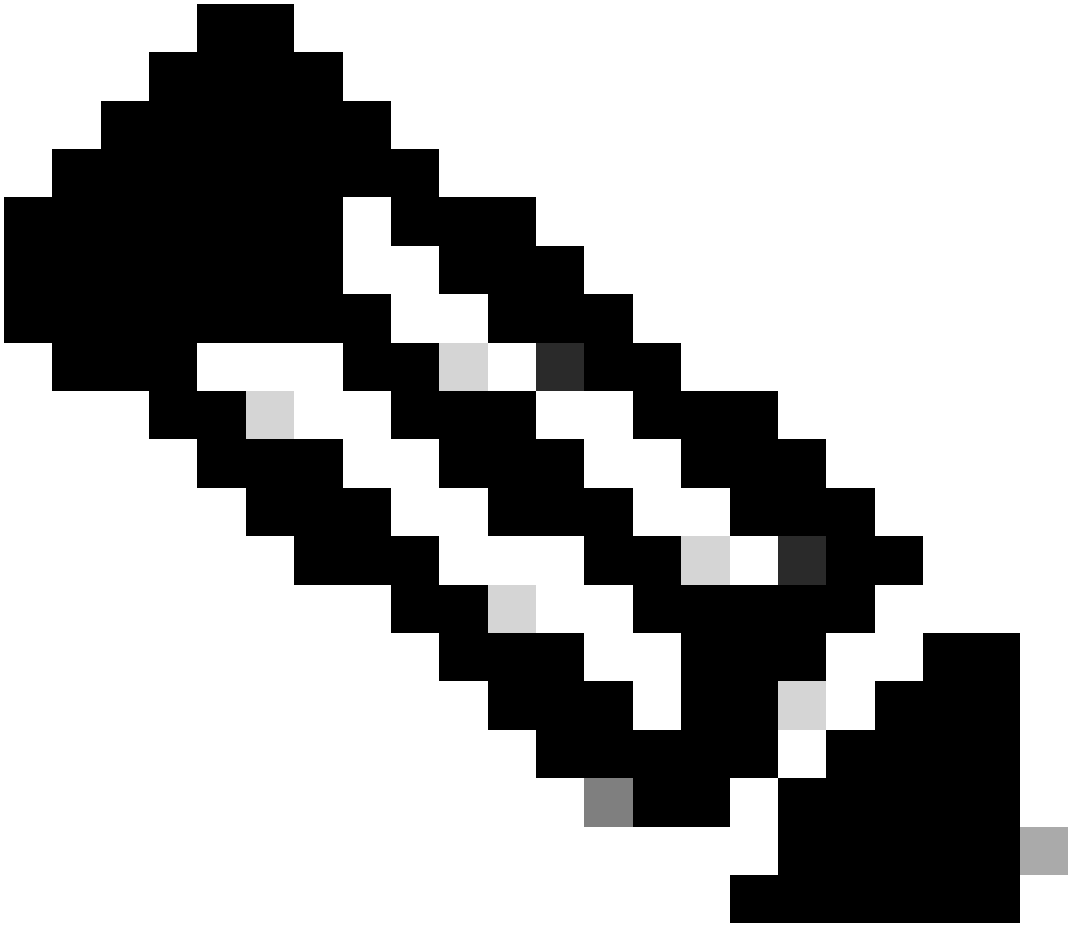
- Erstellen Sie **Uknown Compliant Authorization Profile**





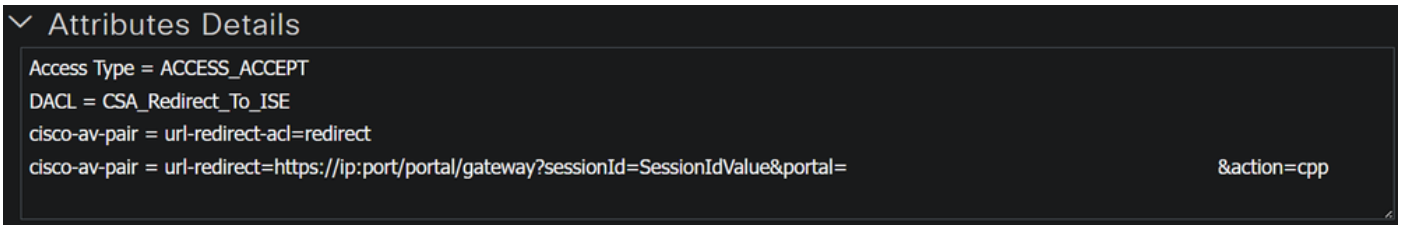
- **Name**: Erstellen Sie einen Namen, der auf das unbekannte, kompatible Autorisierungsprofil verweist.
- Access Type: Auswahl **ACCESS_ACCEPT**

- **Common Tasks**
    - **DACL NAME**: Wählen Sie die auf dem Schritt Unknown Compliant DACL konfigurierte DACL aus.
        - **Web Redirection (CWA,MDM,NSP,CPP)**
            - Auswählen **Client Provisioning (Posture)**
                - **ACL**: Muss redirect
                - **Value**: Wählen Sie das Standard-Bereitstellungsportal aus, oder wählen Sie es aus, wenn Sie ein anderes Portal definiert haben.



Hinweis: Der Name der Umleitungs-ACL für sicheren Zugriff für alle Bereitstellungen lautet **redirect**.

Nachdem Sie alle diese Werte definiert haben, müssen Sie etwas Ähnliches unter Attributes Details haben.



Klicken Sie hier, **Save** um die Konfiguration zu beenden und mit dem nächsten Schritt fortzufahren.

Festlegen von Statusrichtlinien

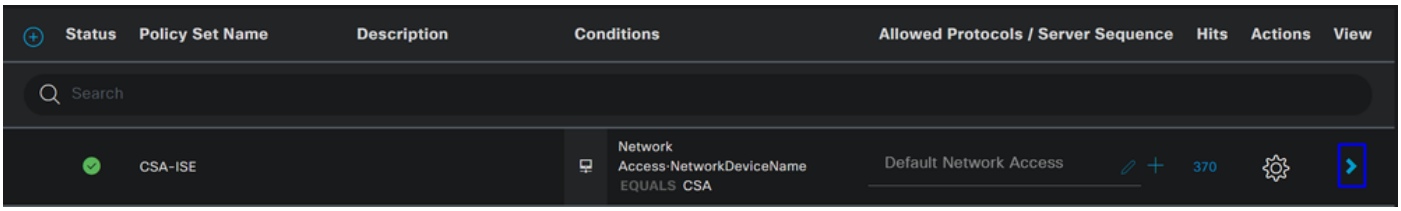
Die drei Richtlinien, die Sie erstellen, basieren auf den Autorisierungsprofilen, die Sie konfiguriert haben. **DenyAccess**Sie müssen also keine weitere Richtlinie erstellen.

Richtliniensatz - Autorisierung	**Autorisierungsprofil**
Konformität	Autorisierungsprofil - konform
Unbekannte Compliance	Autorisierungsprofil - Unbekannt
Nicht konform	Zugriff verweigern

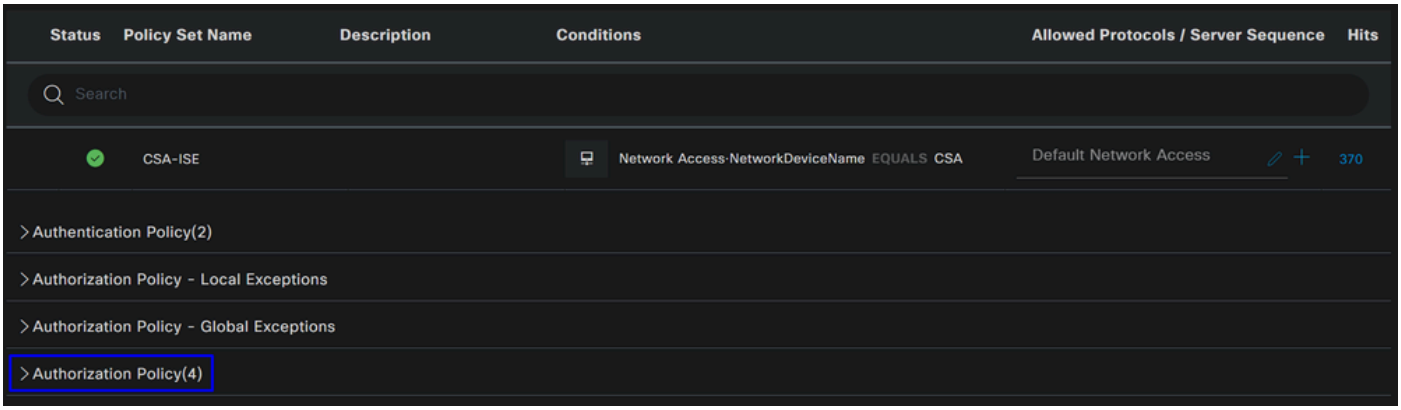
Rufen Sie Ihr ISE Dashboard auf.

- Klicken Sie **Work Center > Policy Sets**

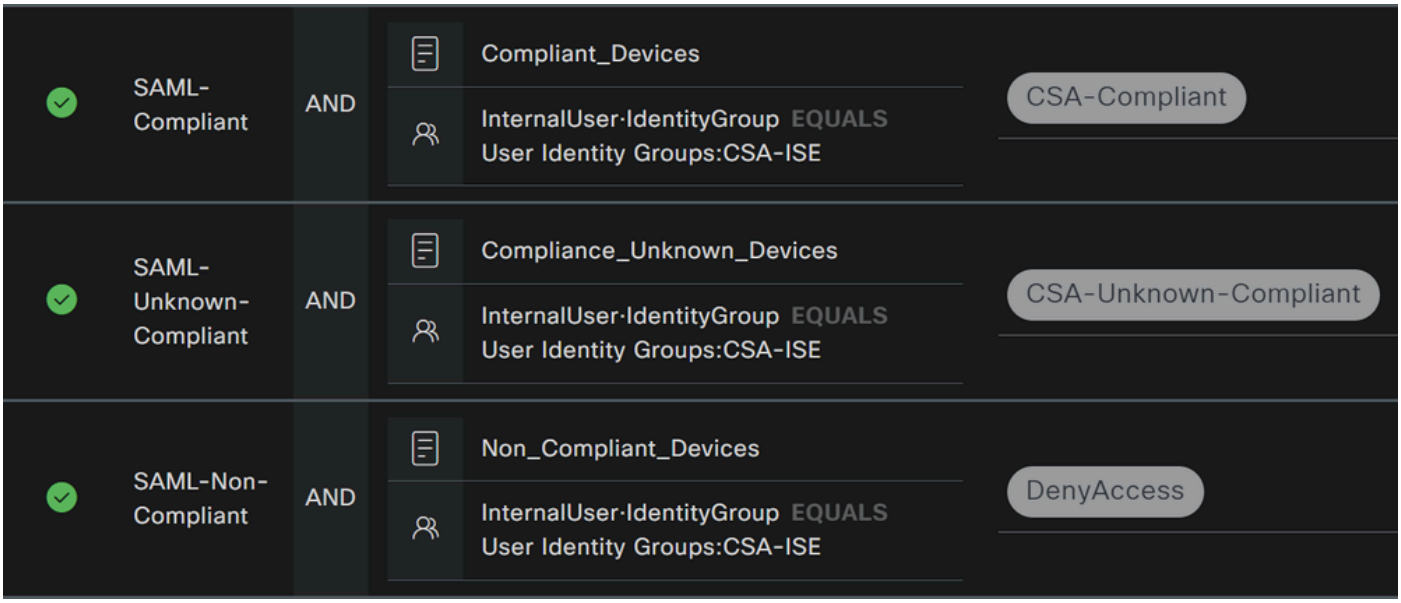
- Klicken Sie auf > die Schaltfläche, um auf die von Ihnen erstellte Richtlinie zuzugreifen.



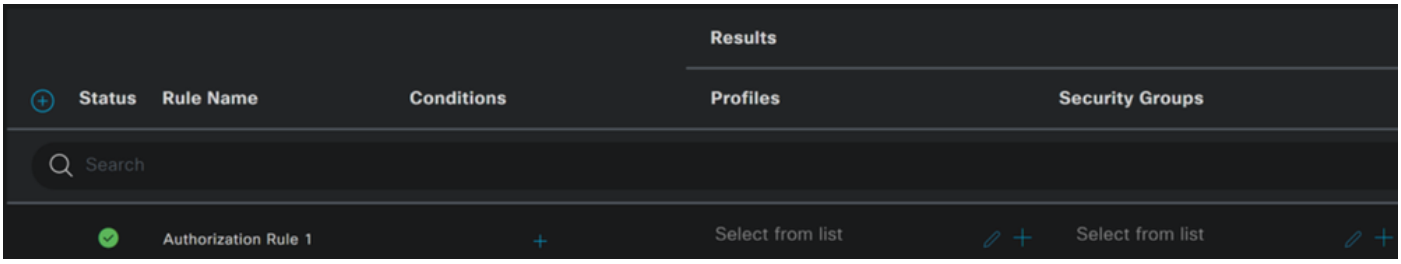
- Klicken Sie auf Authorization Policy



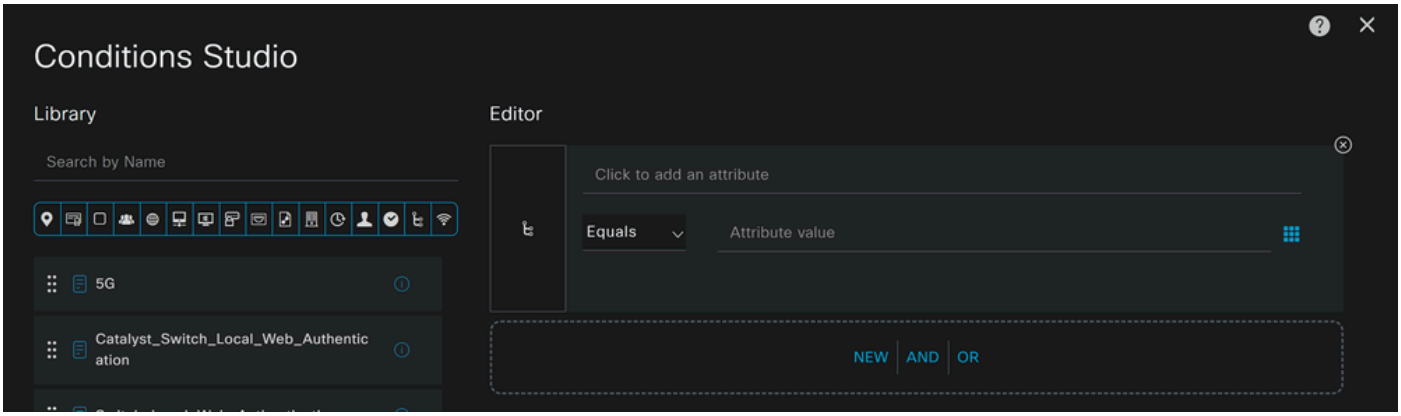
- Erstellen Sie die nächsten drei Richtlinien in der folgenden Reihenfolge:



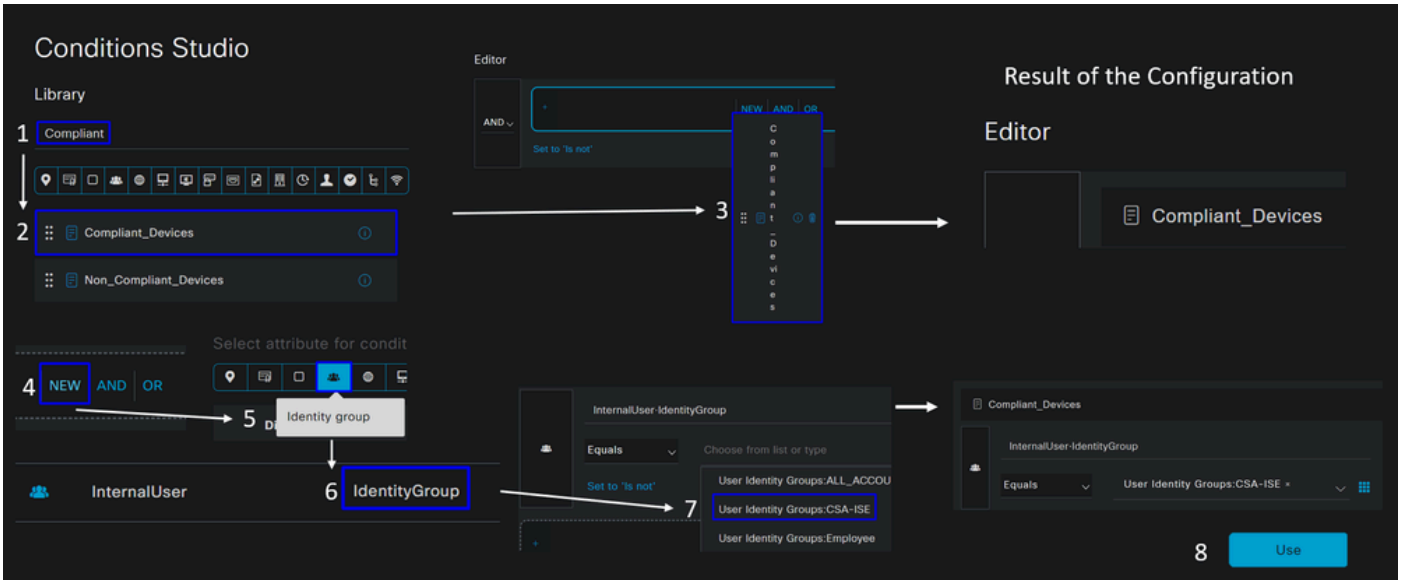
- Klicken Sie auf, + um die **CSA-Compliance** Richtlinie zu definieren:



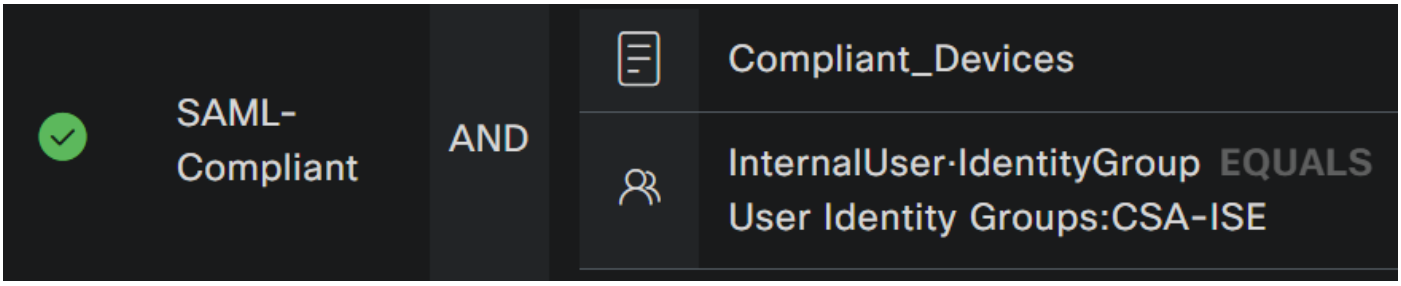
- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles
- Wenn Sie einen Namen **Name** konfigurieren auf **CSA-Compliance**
- Um das zu konfigurieren, **Condition**klicken Sie auf die Schaltfläche +
- Unter **Condition Studio**finden Sie die Informationen:



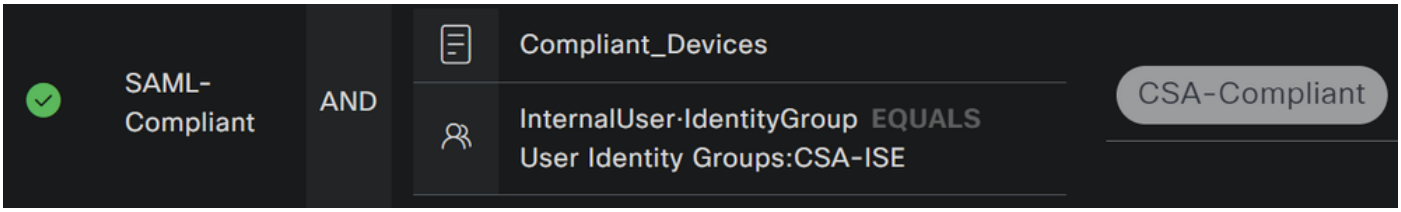
- Um die Bedingung zu erstellen, suchen Sie nach **compliant**
- Sie müssen Folgendes anzeigen: Compliant_Devices
- Drag & Drop unter dem **Editor**
- Klicken Sie unter Editor in **New**
- Klicken Sie auf das **Identity Group** Symbol
- Auswählen **Internal User Identity Group**
- Wählen **Equals**Sie unter die **User Identity Group** passende aus.
- Klicken Sie auf **Use**



- Als Ergebnis haben Sie das nächste Bild

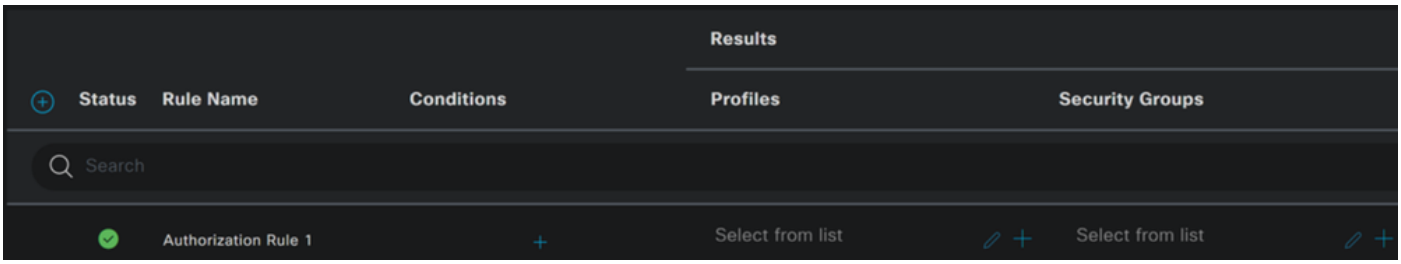


- Wählen Sie unter **Profile** Klicken Sie unter der Dropdown-Schaltfläche das auf dem Schritt konfigurierte Autorisierungsprofil für die Beschwerde aus: Compliant Authorization Profile



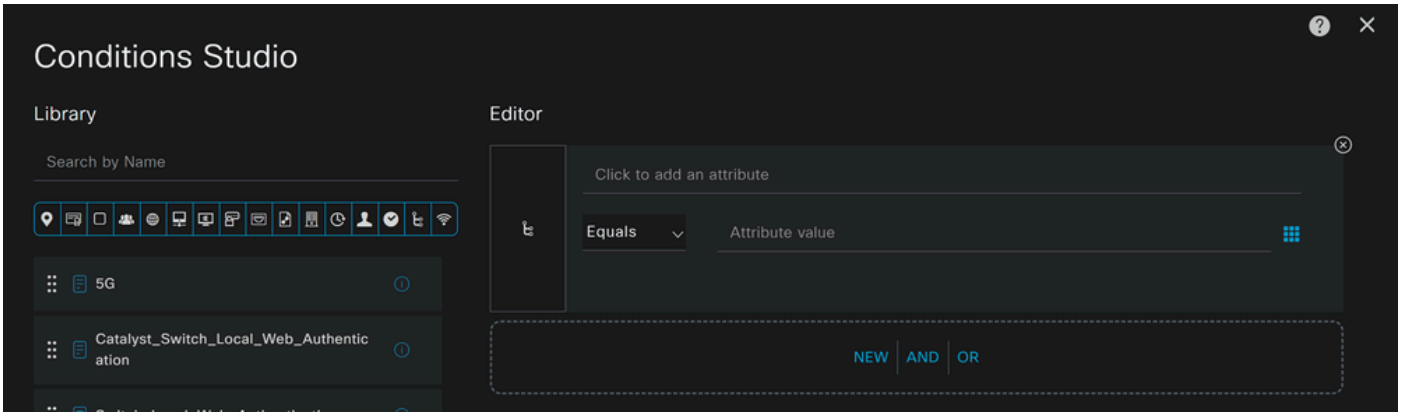
Jetzt haben Sie die konfiguriert **Compliance Policy Set**.

- Klicken Sie auf, + um die **CSA-Unknown-Compliance** Richtlinie zu definieren:

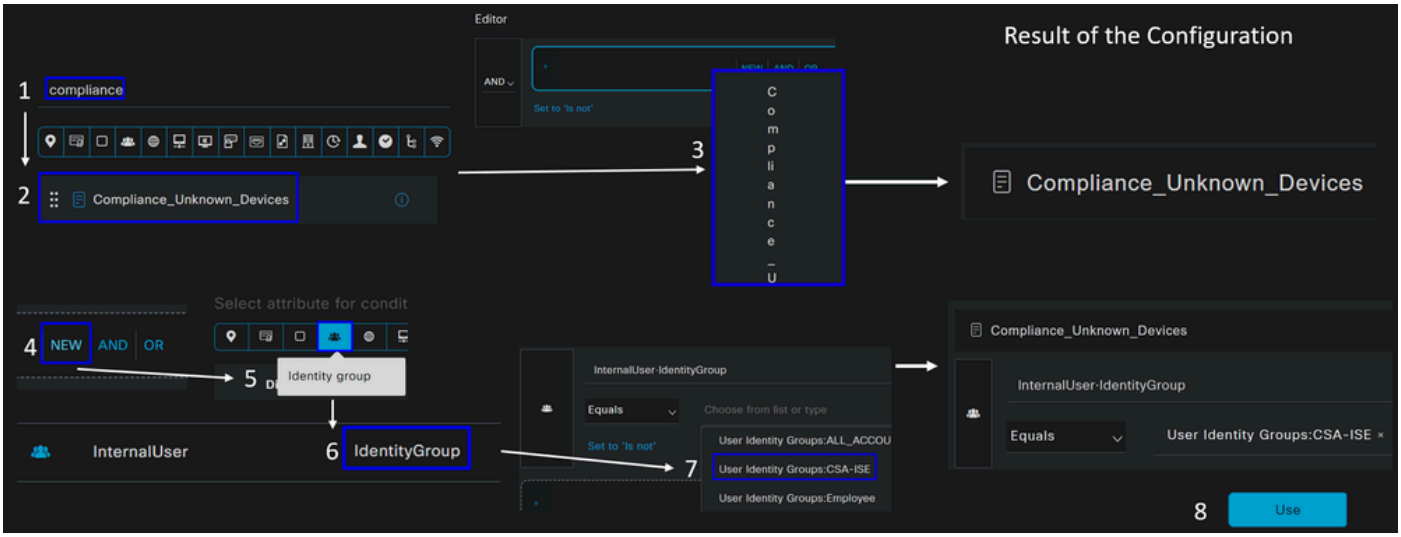


- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles
- Wenn Sie einen Namen **Name** konfigurieren auf **CSA-Unknown-Compliance**

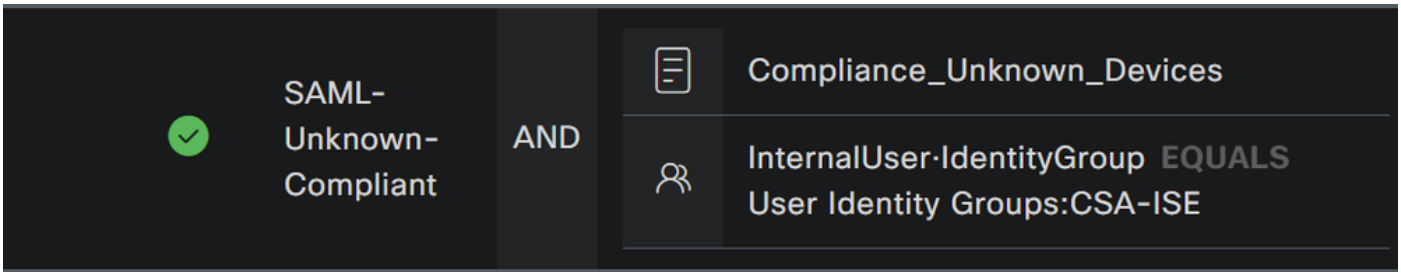
- Um das zu konfigurieren, **Condition**klicken Sie auf die Schaltfläche +
- Unter **Condition Studio**finden Sie die Informationen:



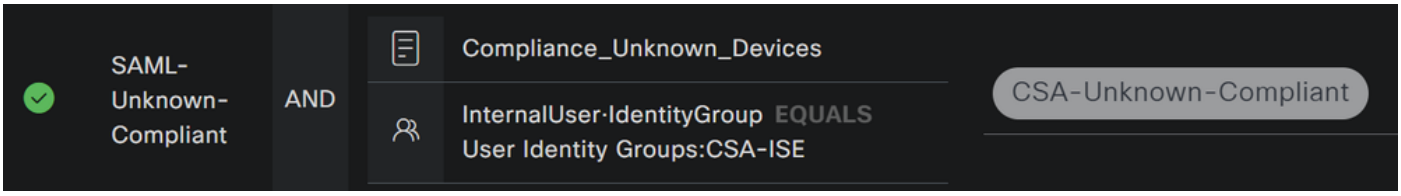
- Um die Bedingung zu erstellen, suchen Sie nach **compliance**
- Sie müssen Folgendes anzeigen: Compliant_Unknown_Devices
- Drag & Drop unter dem **Editor**
- Klicken Sie unter Editor in **New**
- Klicken Sie auf das **Identity Group** Symbol
- Auswählen **Internal User Identity Group**
- Wählen **Equals**Sie unter die **User Identity Group** passende aus.
- Klicken Sie auf **Use**



- Als Ergebnis haben Sie das nächste Bild

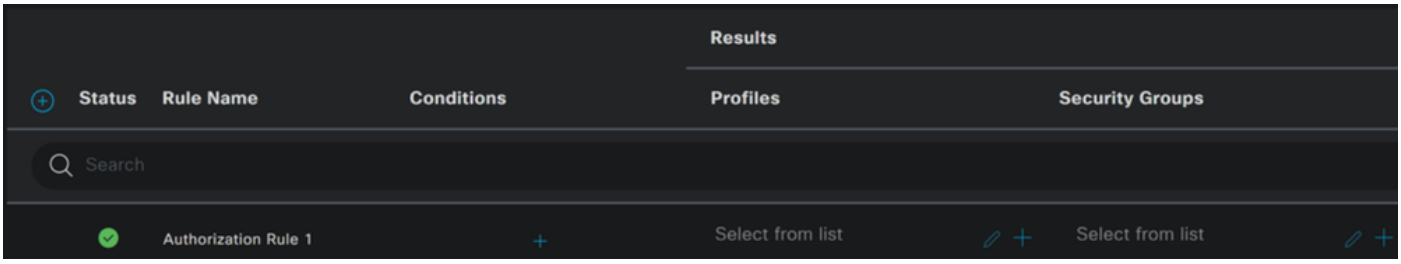


- Klicken Sie unter der Dropdown-Schaltfläche auf **Profile** und wählen Sie das auf dem Schritt konfigurierte Autorisierungsprofil für die Beschwerde aus: Unknown Compliant Authorization Profile (Unbekanntes konformes Autorisierungsprofil)



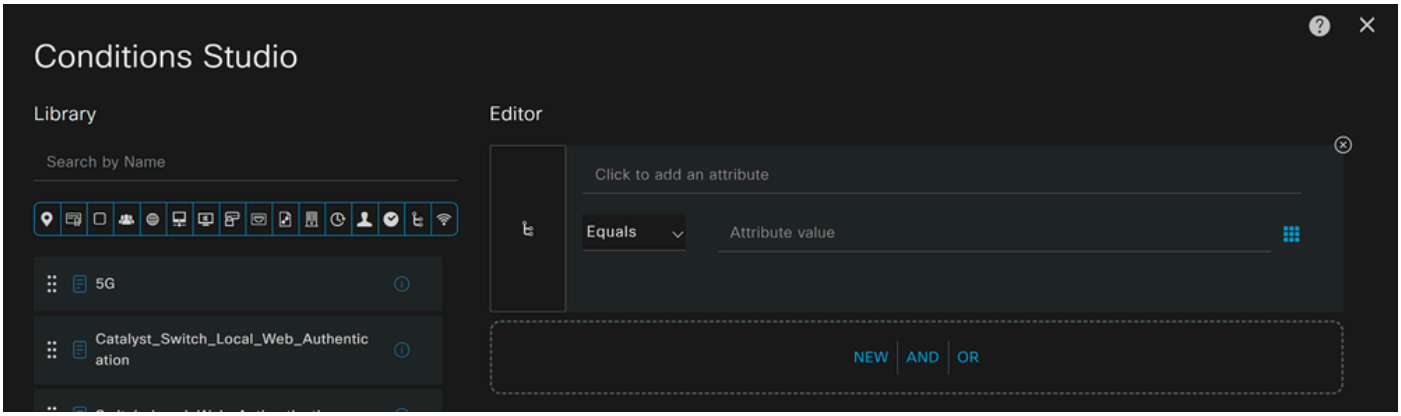
Jetzt haben Sie die konfiguriert **Unknown Compliance Policy Set**.

- Klicken Sie auf, + um die **CSA- Non-Compliant** Richtlinie zu definieren:

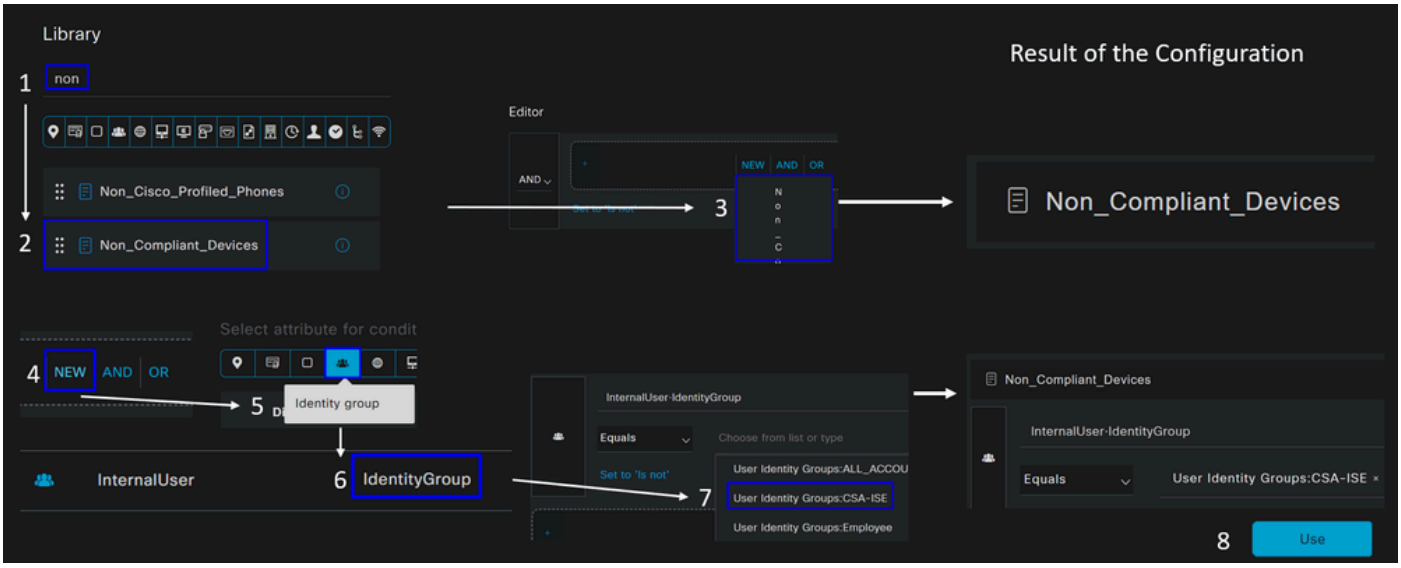


- Im nächsten Schritt ändern Sie das Rule Name, Conditions und Profiles
- Wenn Sie einen Namen **Name** konfigurieren auf **CSA-Non-Compliance**

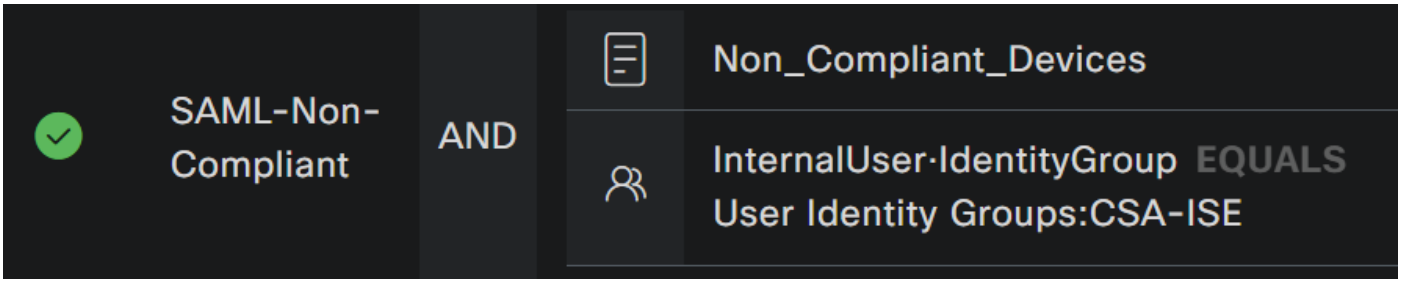
- Um das zu konfigurieren, **Condition**klicken Sie auf die Schaltfläche +
- Unter **Condition Studio**finden Sie die Informationen:



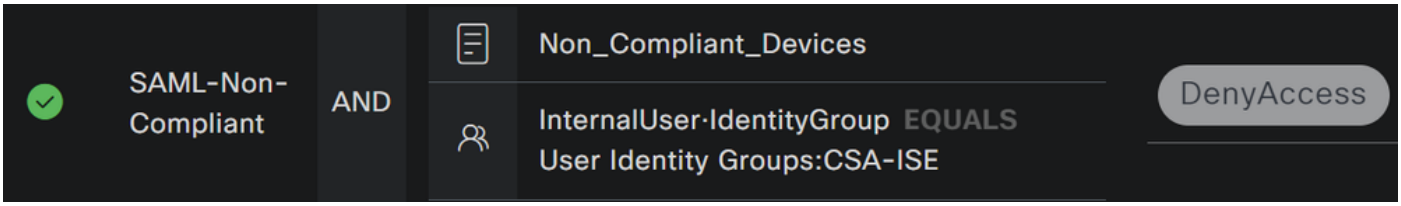
- Um die Bedingung zu erstellen, suchen Sie nach **non**
- Sie müssen Folgendes anzeigen: Non_Compliant_Devices
- Drag & Drop unter dem **Editor**
- Klicken Sie unter Editor in **New**
- Klicken Sie auf das **Identity Group** Symbol
- Auswählen **Internal User Identity Group**
- Wählen **Equals**Sie unter die **User Identity Group** passende aus.
- Klicken Sie auf **Use**



- Als Ergebnis haben Sie das nächste Bild



- Klicken Sie unter **Profile** dem Dropdown-Menü auf das Profil für die Autorisierung der Beschwerde. **DenyAccess**



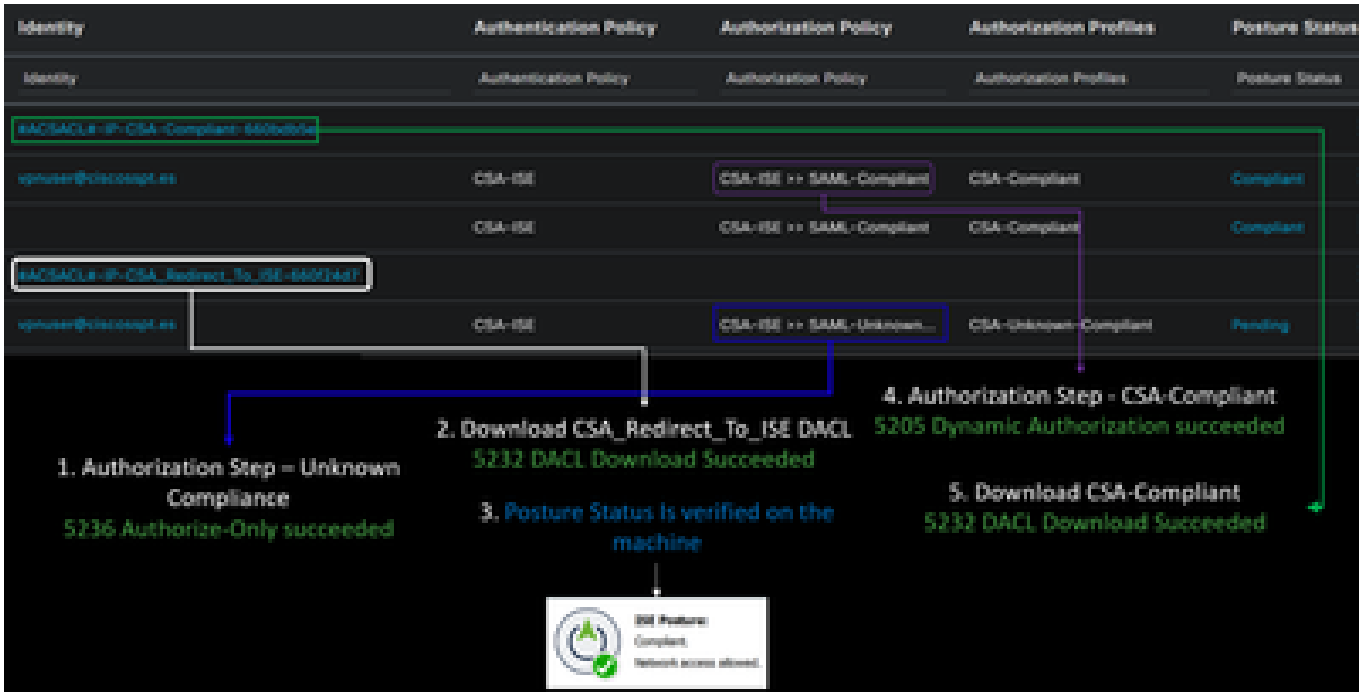
Wenn Sie die Konfiguration der drei Profile abgeschlossen haben, können Sie die Integration mit dem Status testen.

Überprüfung

Statusüberprüfung

Verbindung am Rechner

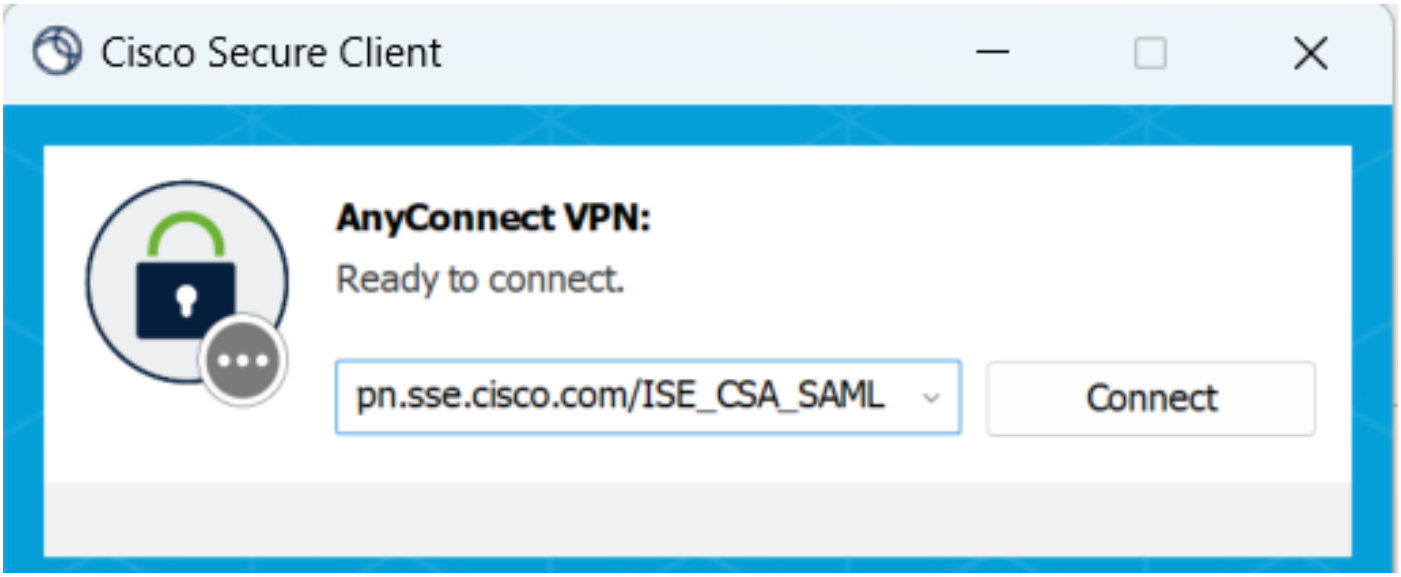
Stellen Sie über Secure Client eine Verbindung zu Ihrer FQDN RA-VPN-Domäne bei sicherem Zugriff her.



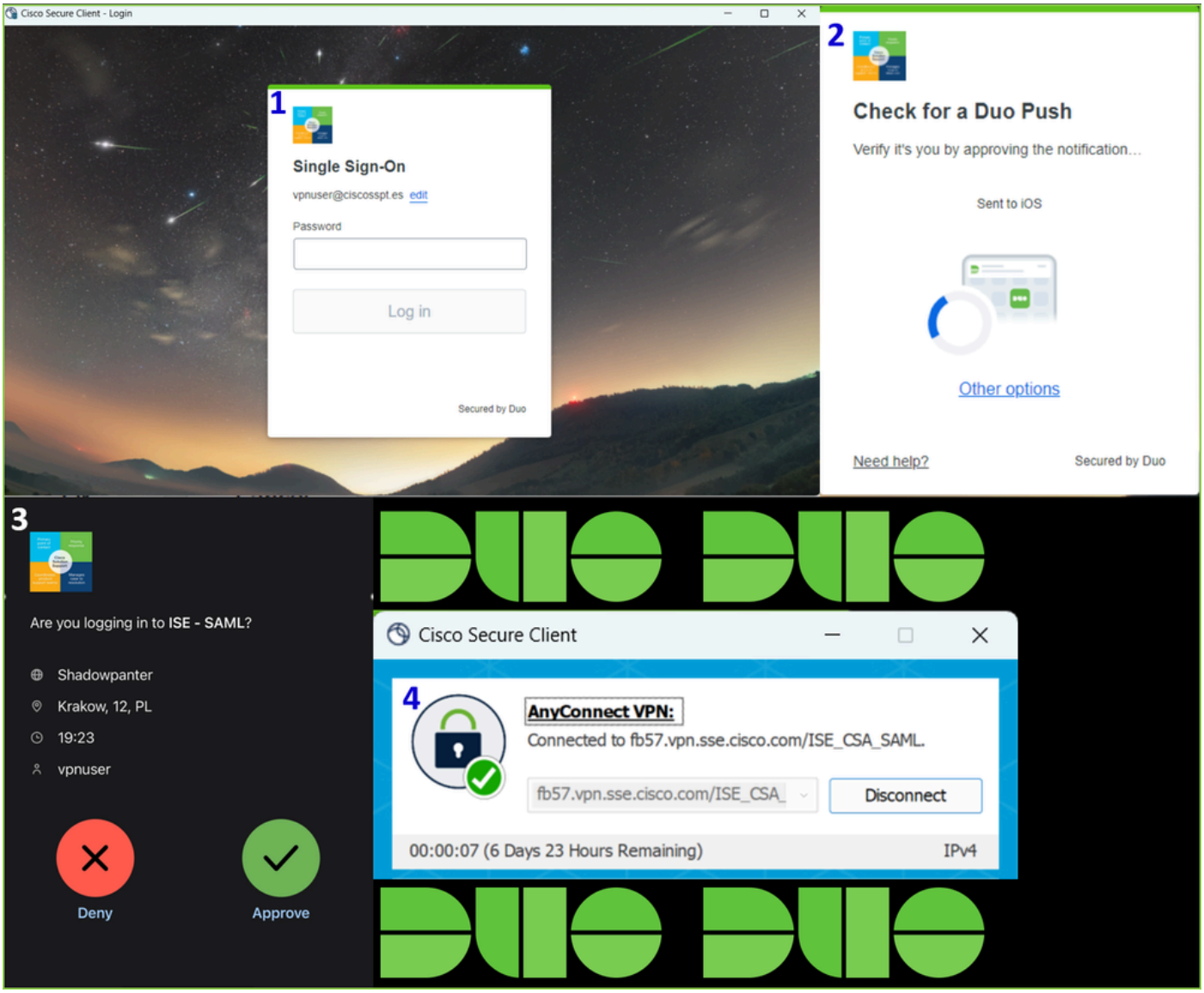
Hinweis: Für diesen Schritt muss kein ISE-Modul installiert werden.

---

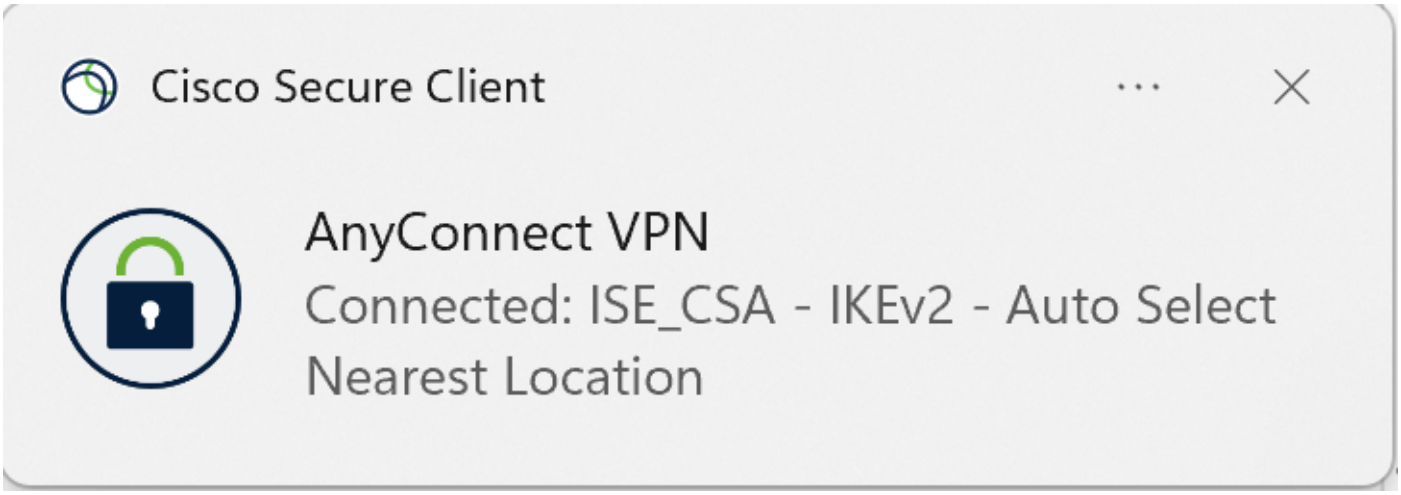
1. Verbindung über Secure Client herstellen.

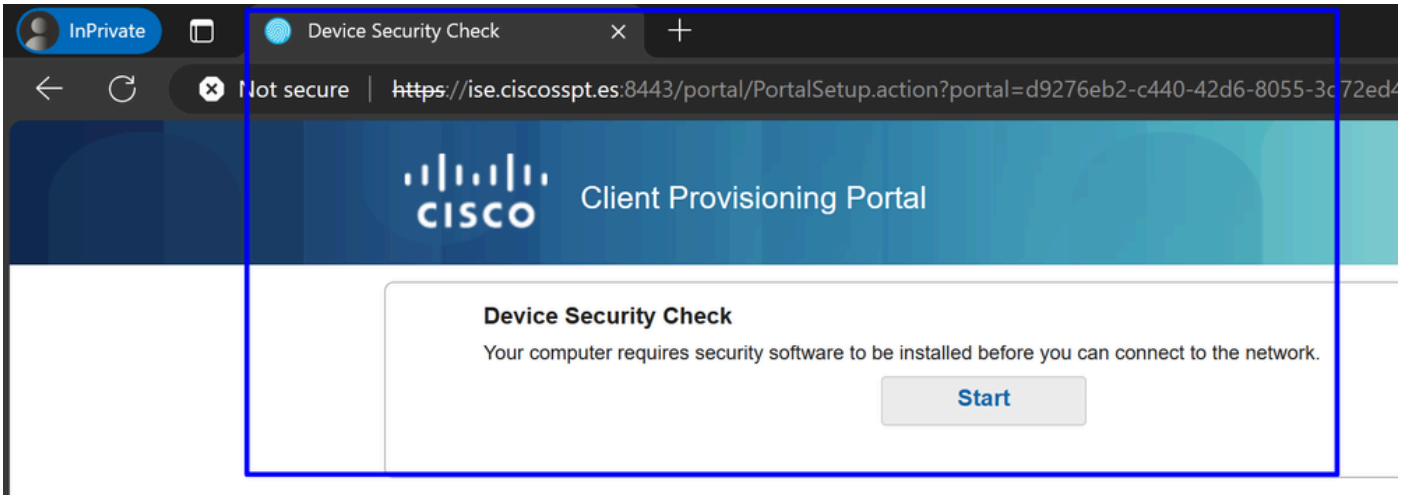


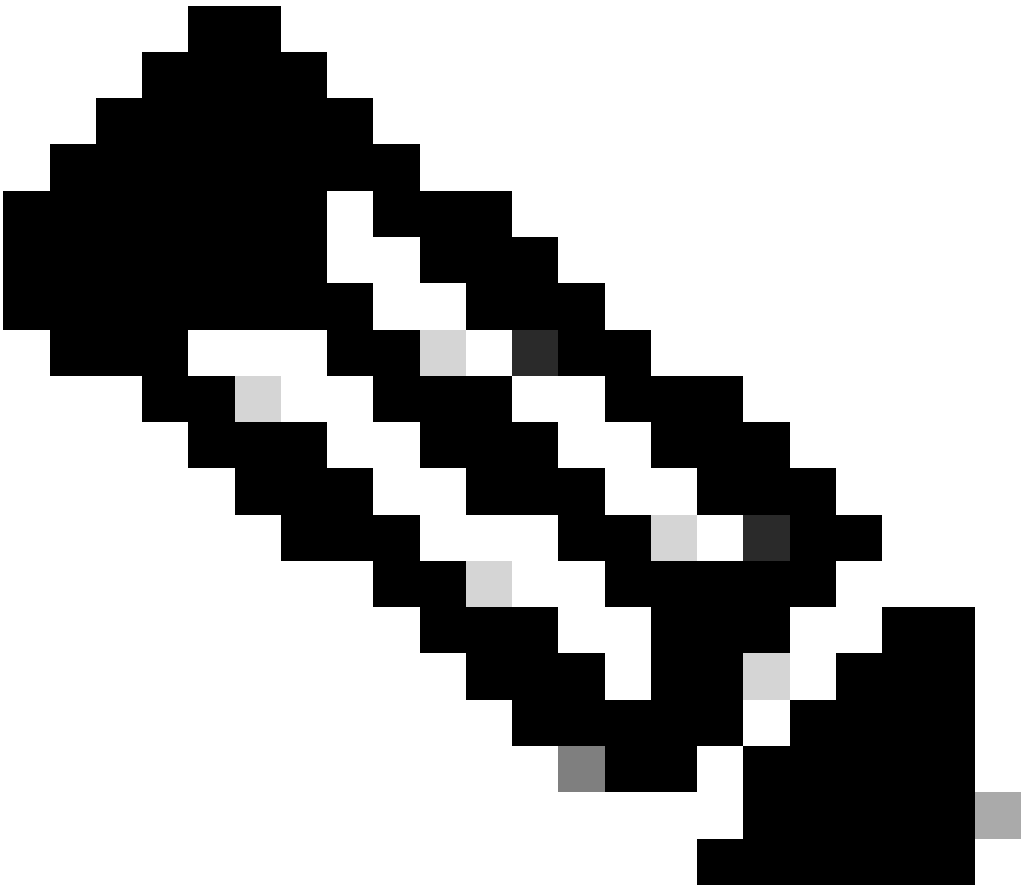
2. Geben Sie die Anmeldeinformationen für die Authentifizierung über Duo an.



3. An diesem Punkt werden Sie mit dem VPN verbunden, und meistens werden Sie wahrscheinlich zur ISE umgeleitet; wenn nicht, können Sie versuchen, zu navigieren **http:1.1.1.1**.





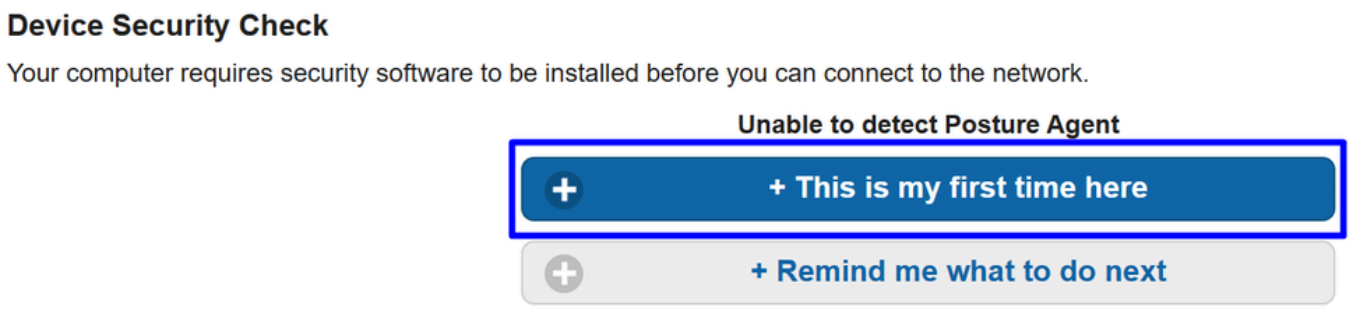


Hinweis: An diesem Punkt fallen Sie unter die Autorisierung - Richtlinienset CSA-Unknown-Compliance, da Sie den ISE Posture

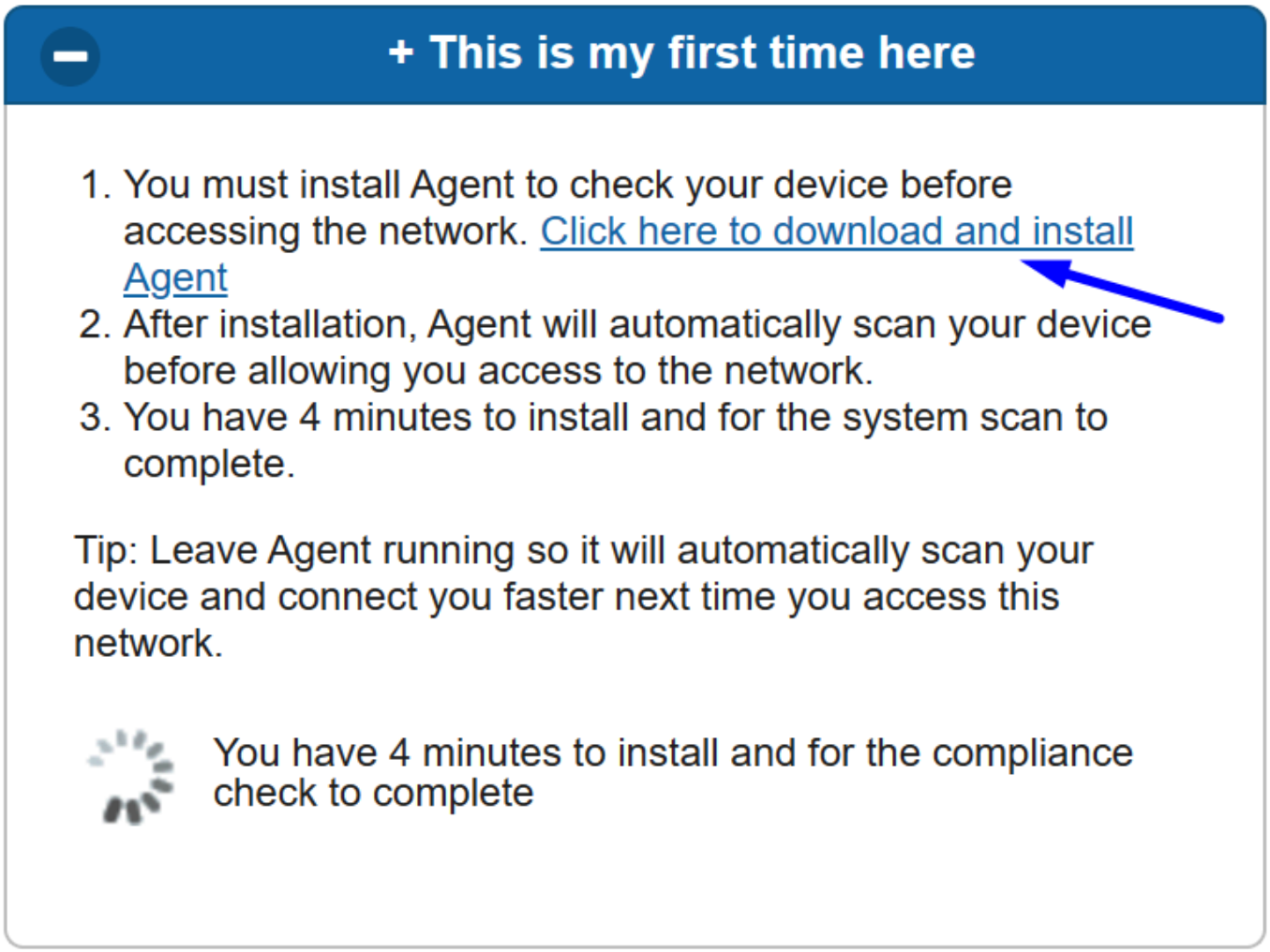
Agent nicht auf dem Computer installiert haben, und Sie werden zum ISE-Bereitstellungsportal umgeleitet, um den Agenten zu installieren.

4. Klicken Sie auf Start, um mit der Agentenbereitstellung fortzufahren.

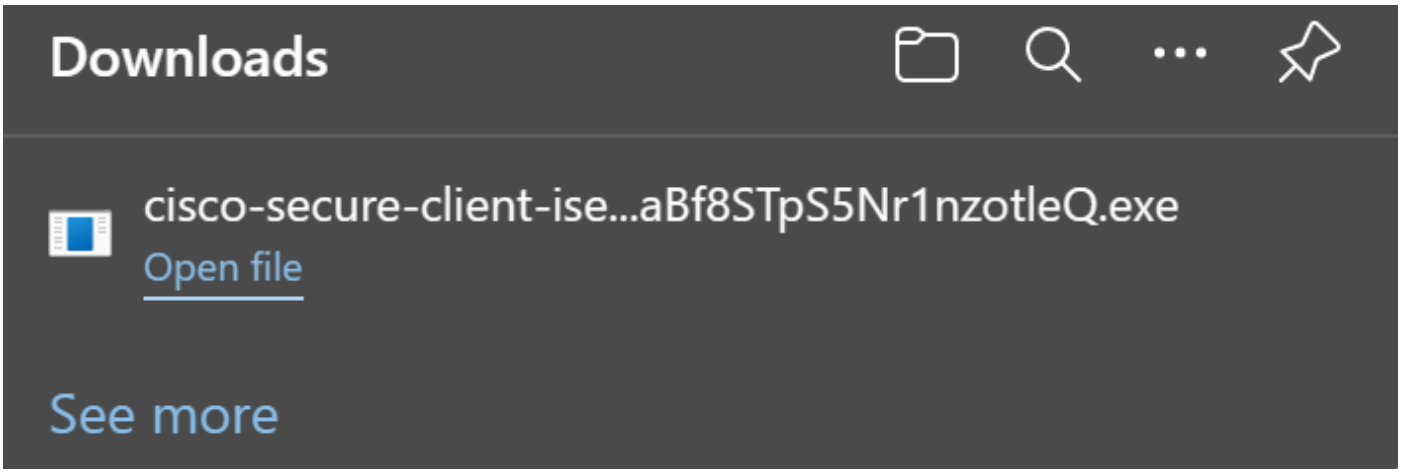
5. Klicken Sie auf **+ This is my first time here**.

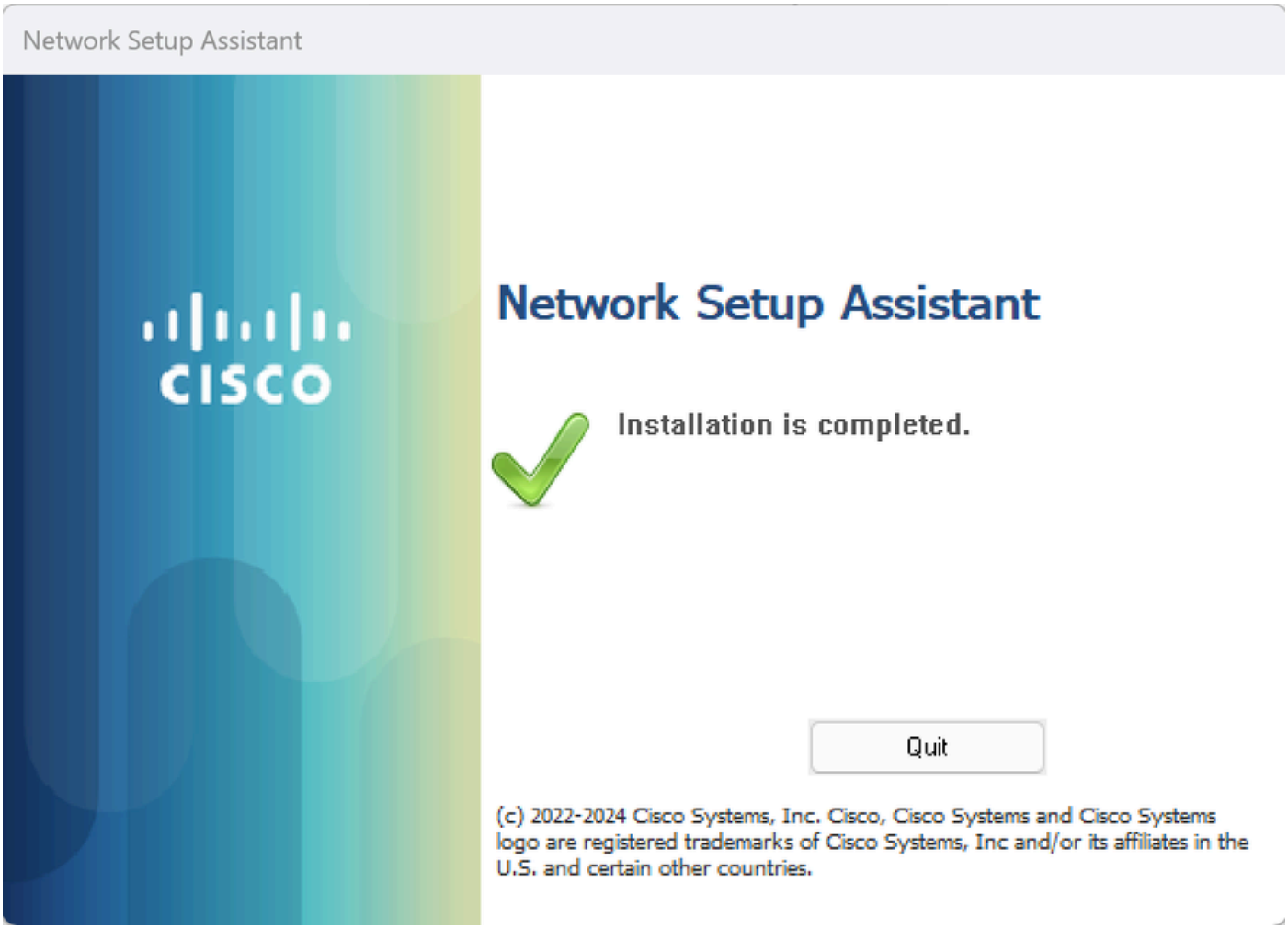


6. Klicken Sie **Click here to download and install agent**

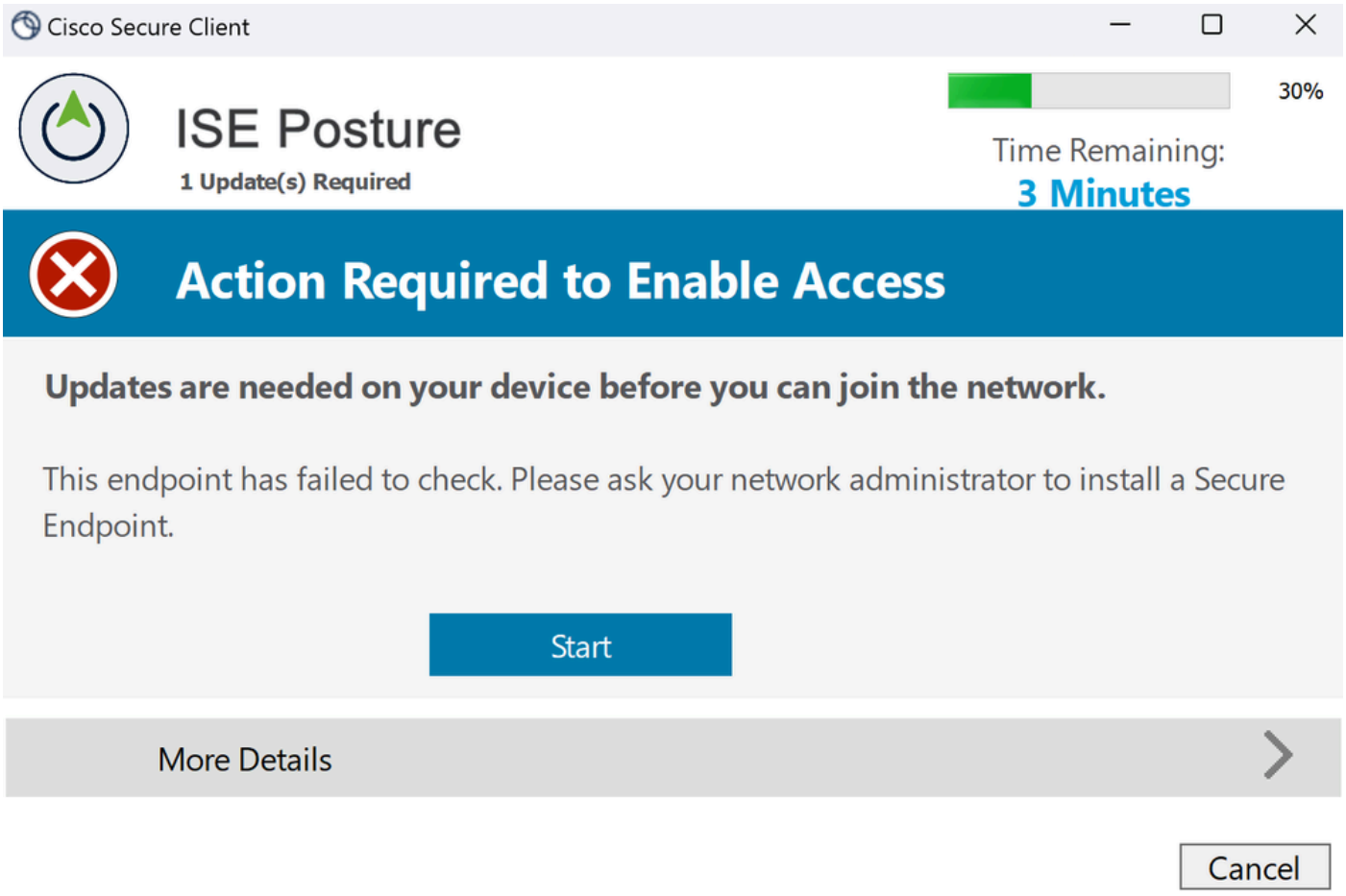


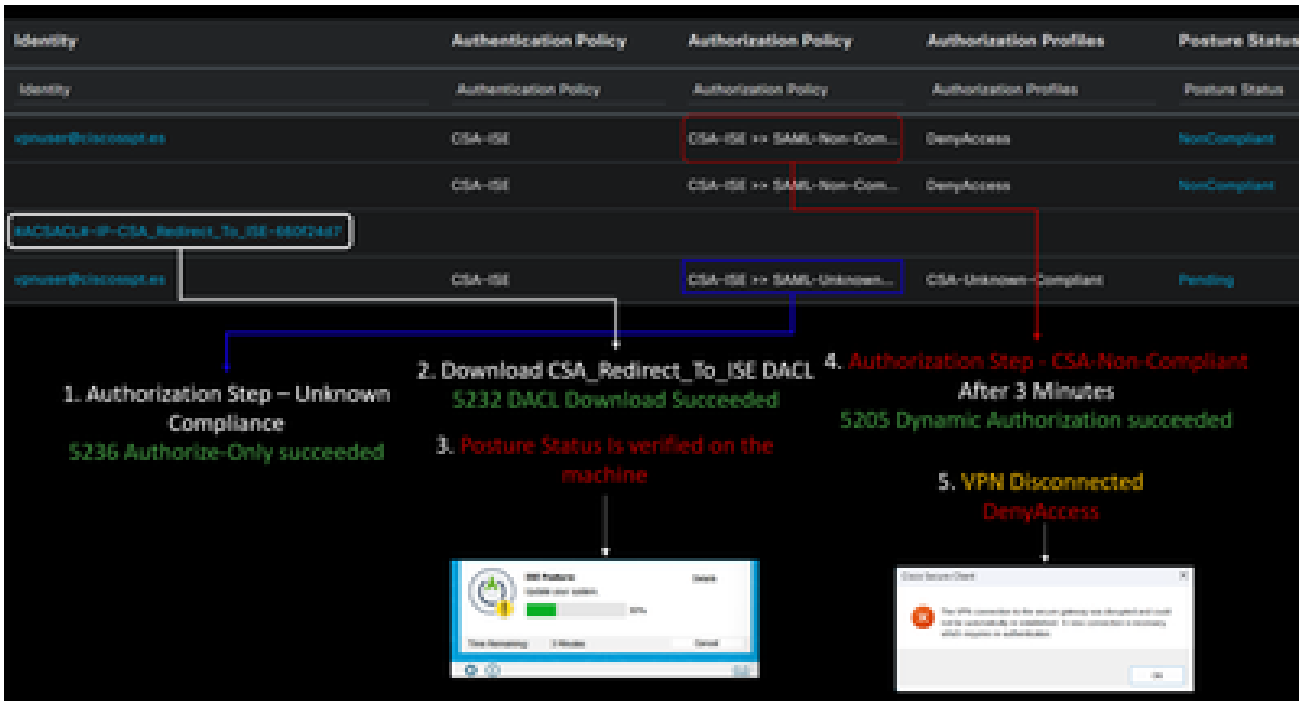
7. Installieren Sie den Agenten





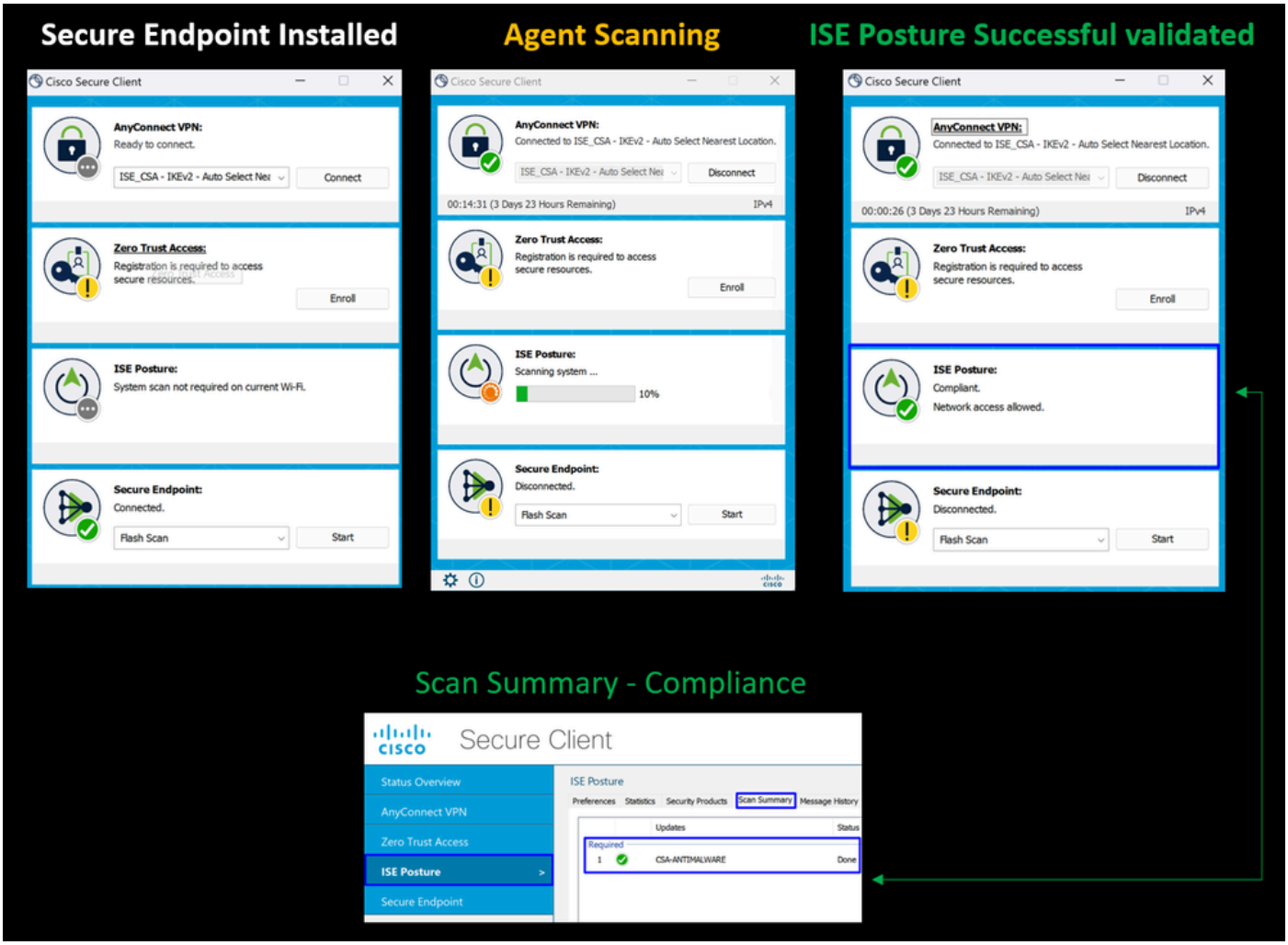
8. Nach der Installation des Agenten beginnt die ISE-Statusüberprüfung mit der Überprüfung des aktuellen Systemstatus. Wenn die Richtlinienanforderungen nicht erfüllt werden, wird ein Popup-Fenster angezeigt, das Sie auf die Einhaltung der Richtlinien hinweist.


Cisco Secure Client
ISE Posture
1 Update(s) Required
30%
Time Remaining:
3 Minutes
Action Required to Enable Access
Updates are needed on your device before you can join the network.
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.
Start
More Details
Cancel

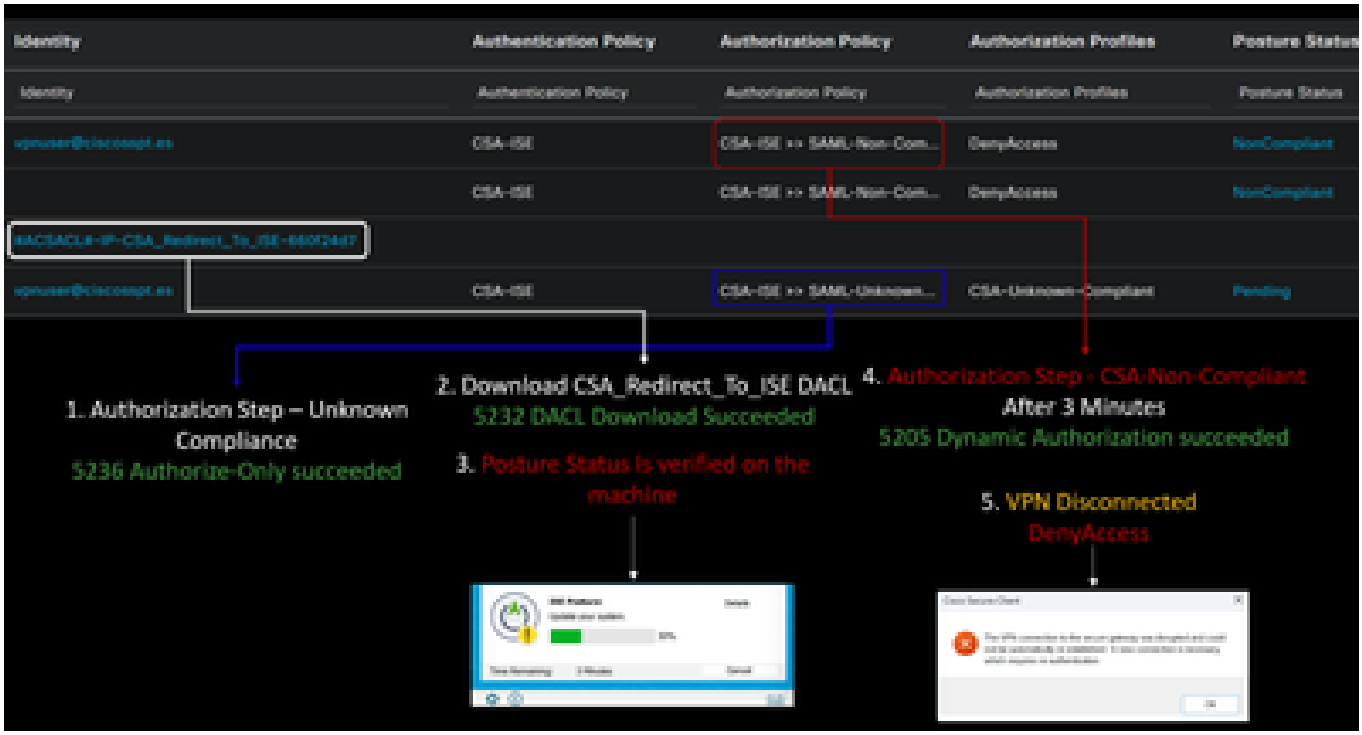

Identity
Authentication Policy
Authorization Policy
Authorization Profiles
Posture Status
CSA-ISE
CSA-ISE >> SAML-Non-Com...
DenyAccess
NonCompliant
CSA-ISE >> SAML-Unknown...
CSA-Unknown-Compliant
Pending
1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status is verified on the machine
4. Authorization Step - CSA-Non-Compliant
After 3 Minutes
5205 Dynamic Authorization succeeded
5. VPN Disconnected
DenyAccess

Hinweis: Wenn Sie Cancel oder die verbleibende Zeit endet, werden Sie automatisch nicht konform, fallen unter den Autorisierungsrichtliniensatz CSA-Non-Compliance und werden sofort vom VPN getrennt.

9. Installieren Sie den Secure Endpoint Agent, und stellen Sie erneut eine Verbindung mit dem VPN her.



10. Nachdem der Agent überprüft hat, dass der Computer die Anforderungen erfüllt, ändert sich Ihr Status, sodass er eine Beschwerde auslöst und Zugriff auf alle Ressourcen im Netzwerk erhält.

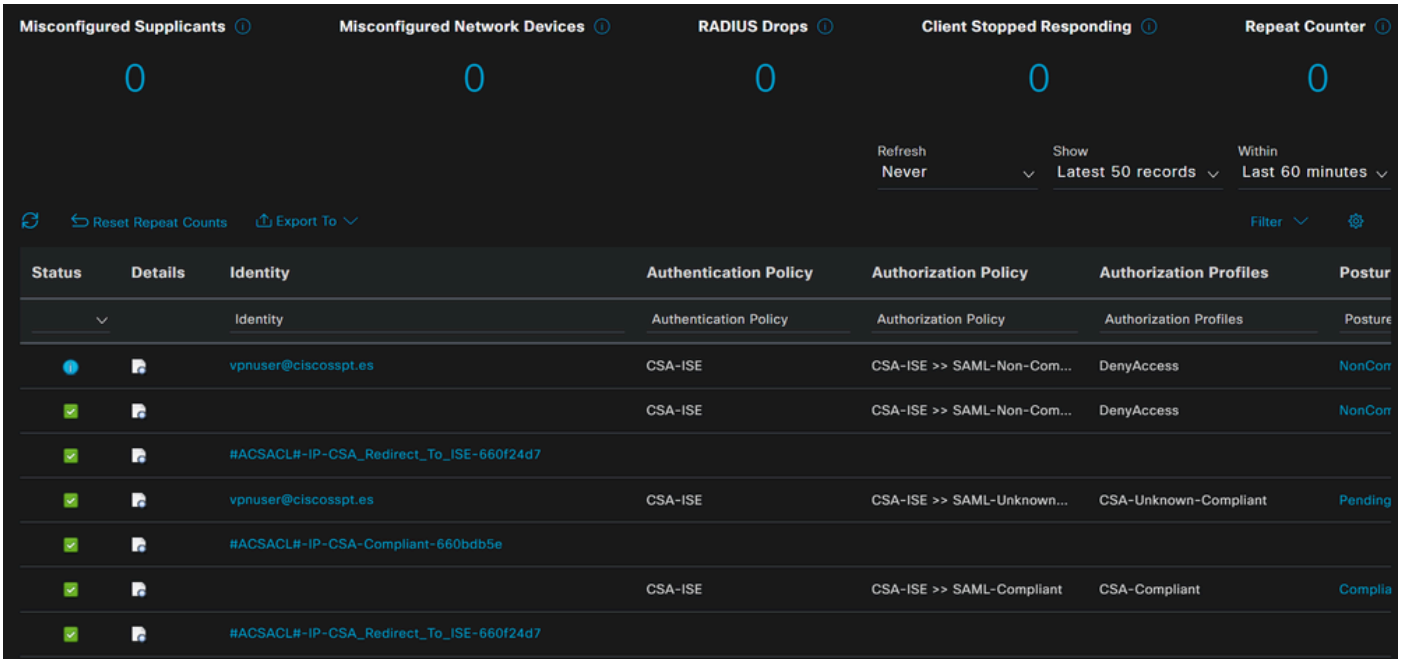


Hinweis: Sobald die CSA-Konformität für Sie erreicht ist, unterliegen Sie der Autorisierungsrichtlinie, und Sie haben sofort Zugriff auf alle Netzwerkressourcen.

So überprüfen Sie die Protokolle in der ISE

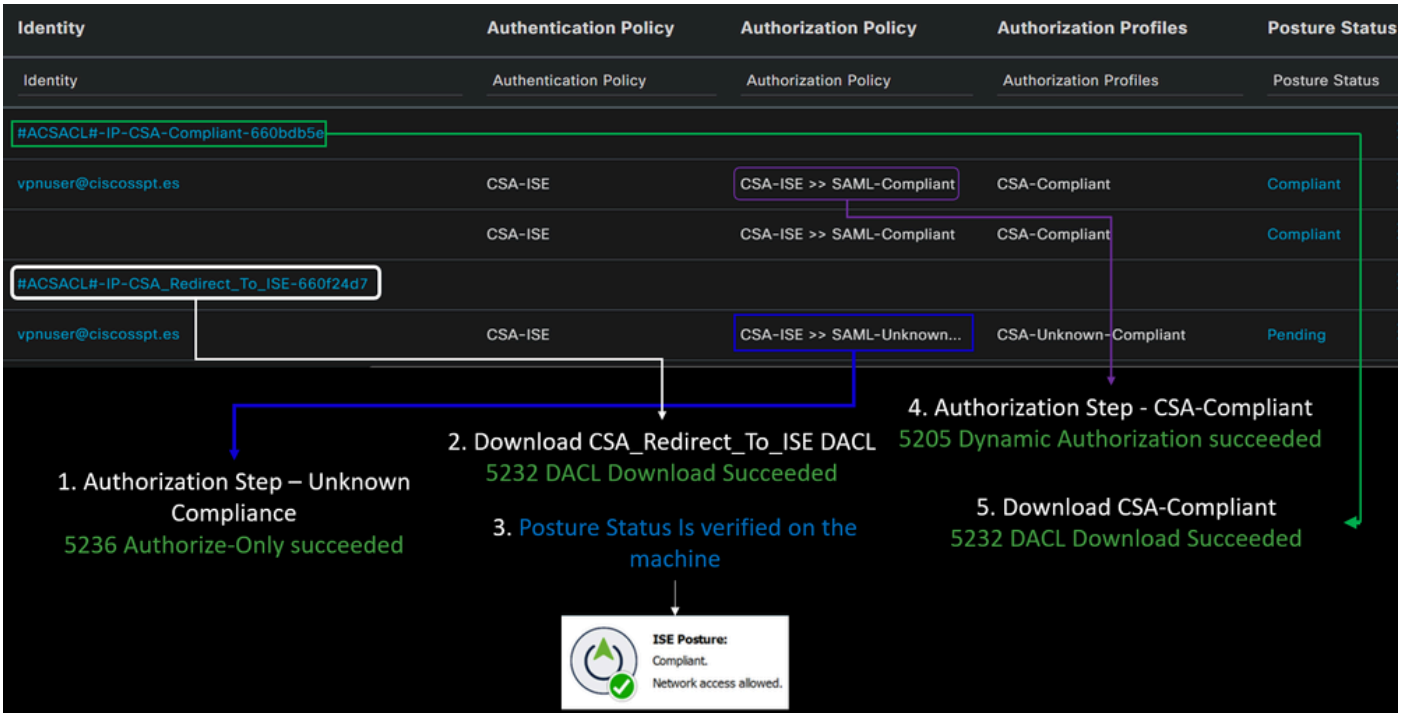
Um das Authentifizierungsergebnis für einen Benutzer zu überprüfen, gibt es zwei Beispiele für Compliance und Nichtkonformität. Um es in der ISE zu überprüfen, befolgen Sie die folgenden Anweisungen:

- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie Operations > Live Logs

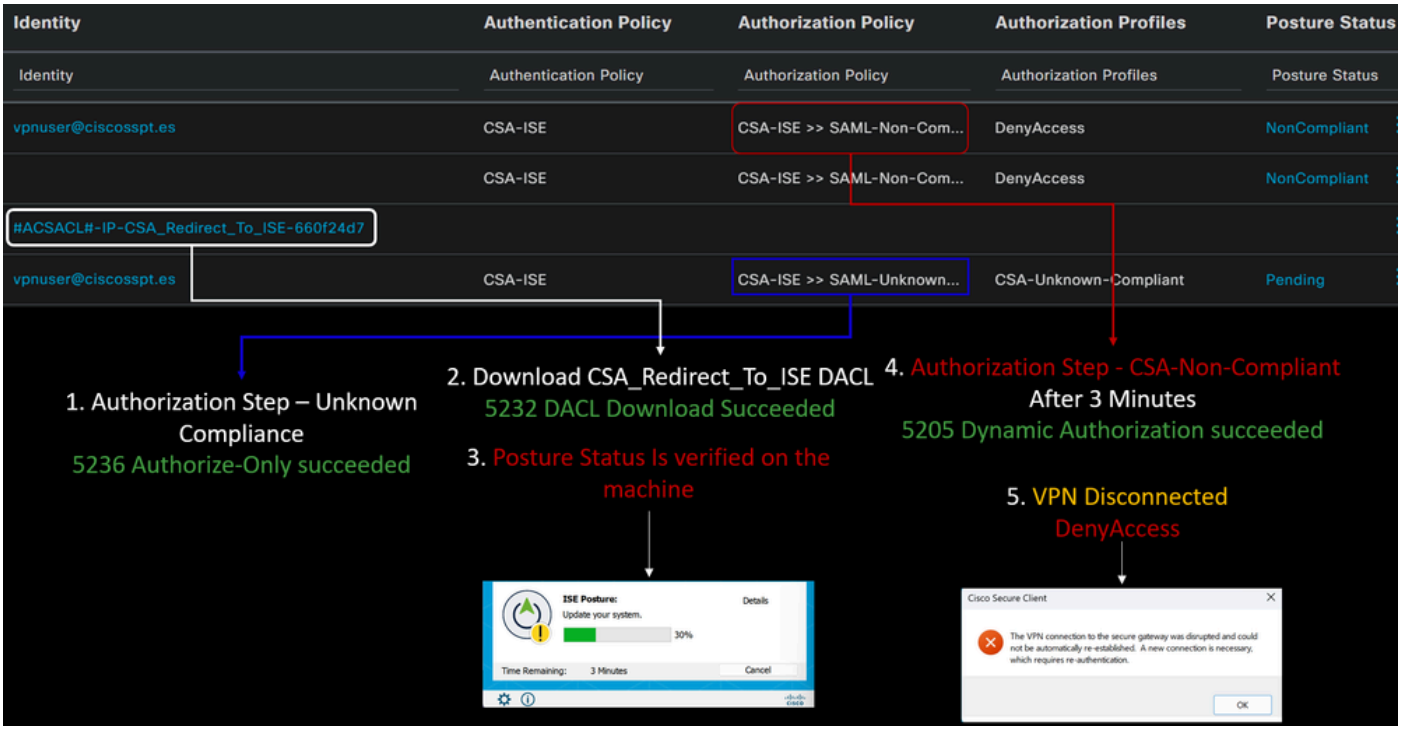


Das nächste Szenario zeigt, wie erfolgreiche Compliance- und Nicht-Compliance-Ereignisse angezeigt werden unter **Live Logs**:

Einhaltung



Nichteinhaltung



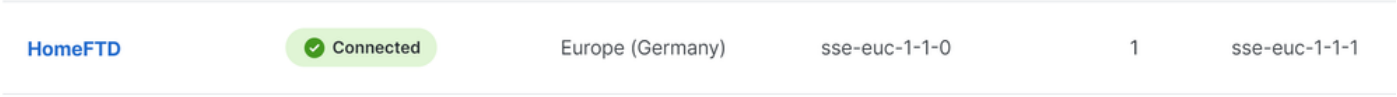
Erste Schritte mit sicherem Zugriff und ISE-Integration

Im nächsten Beispiel befindet sich die Cisco ISE unter dem Netzwerk 192.168.10.0/24, und die Konfiguration der Netzwerke, die über den Tunnel erreichbar sind, muss unter der Tunnelkonfiguration hinzugefügt werden.

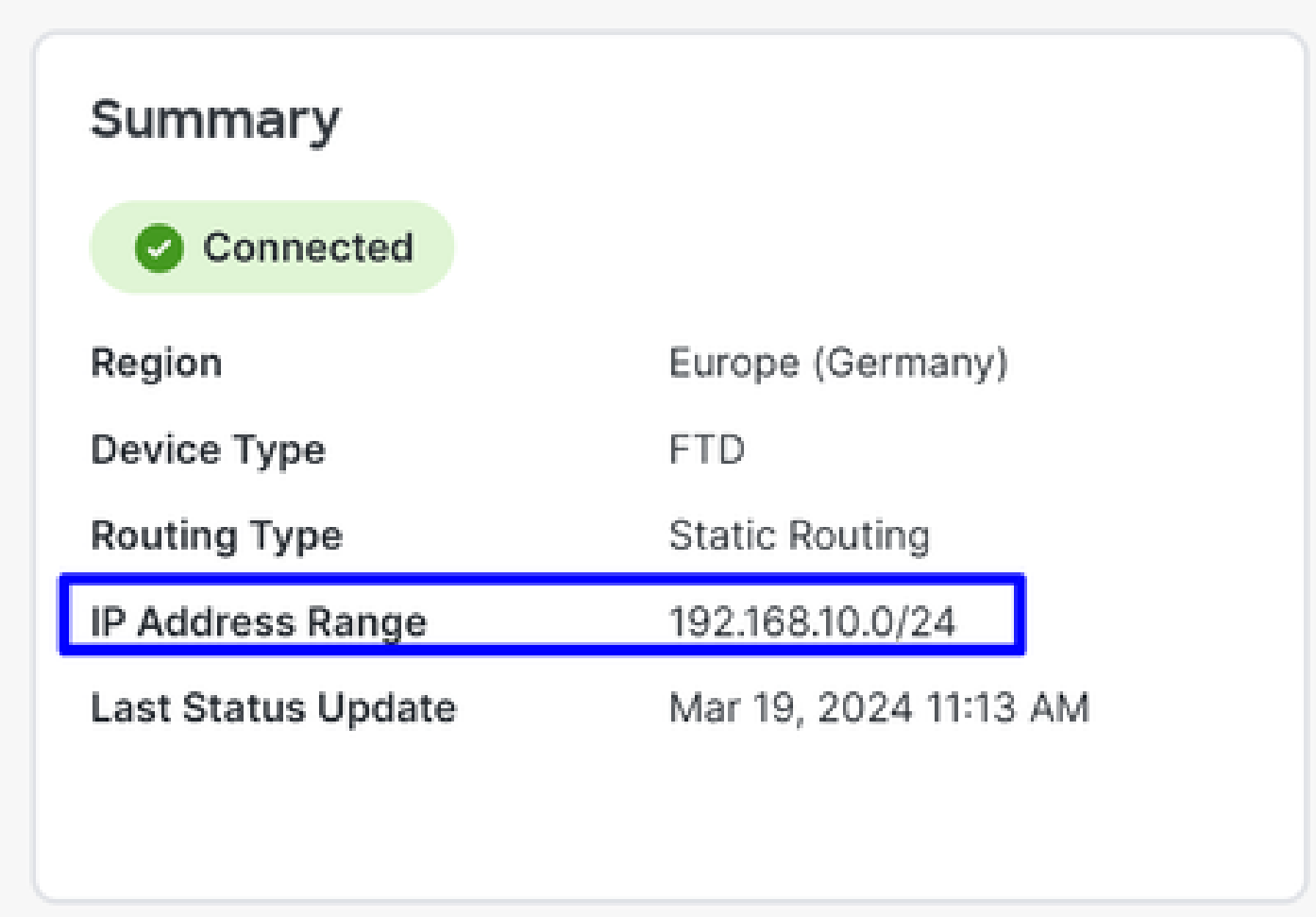
Step 1: Überprüfen Sie Ihre Tunnelkonfiguration:

Navigieren Sie zu Ihrem Secure Access Dashboard, um dies zu überprüfen.

- Klicken Sie **Connect > Network Connections**
- Klicken Sie auf **Network Tunnel Groups** > Ihr Tunnel



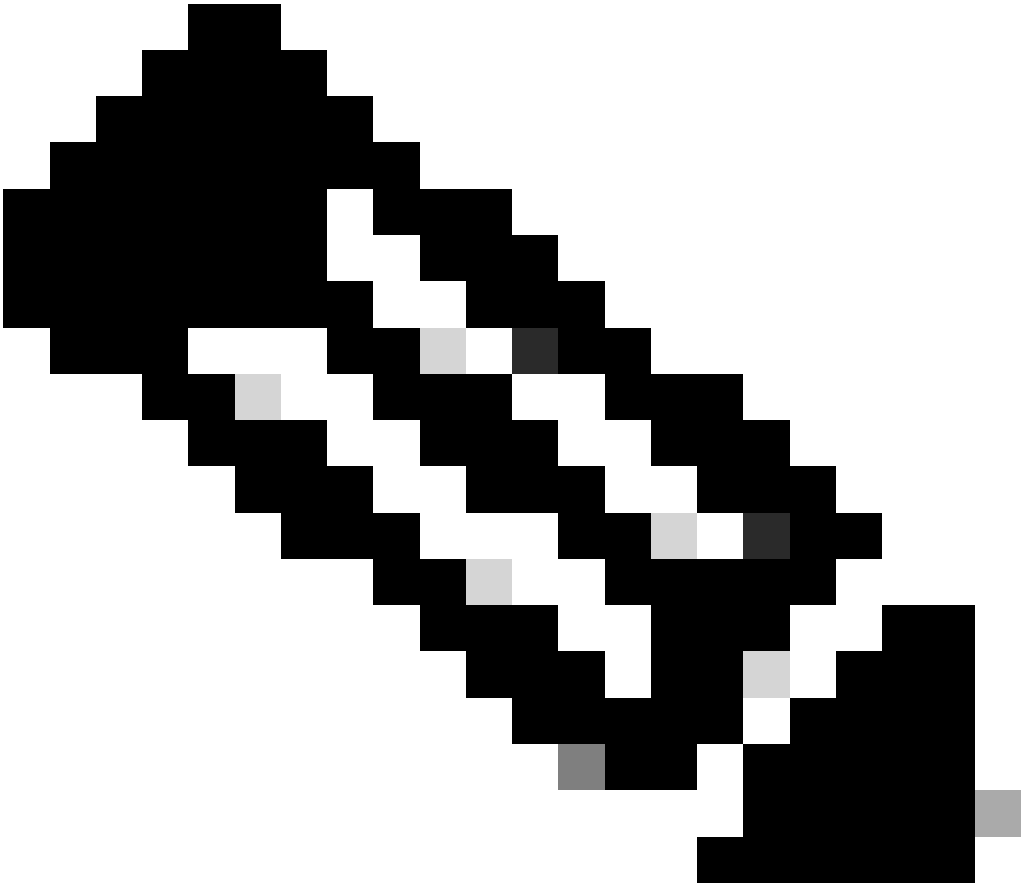
- Prüfen Sie unter Zusammenfassung, ob der Tunnel den Adressraum konfiguriert hat, in dem sich Ihre Cisco ISE befindet:



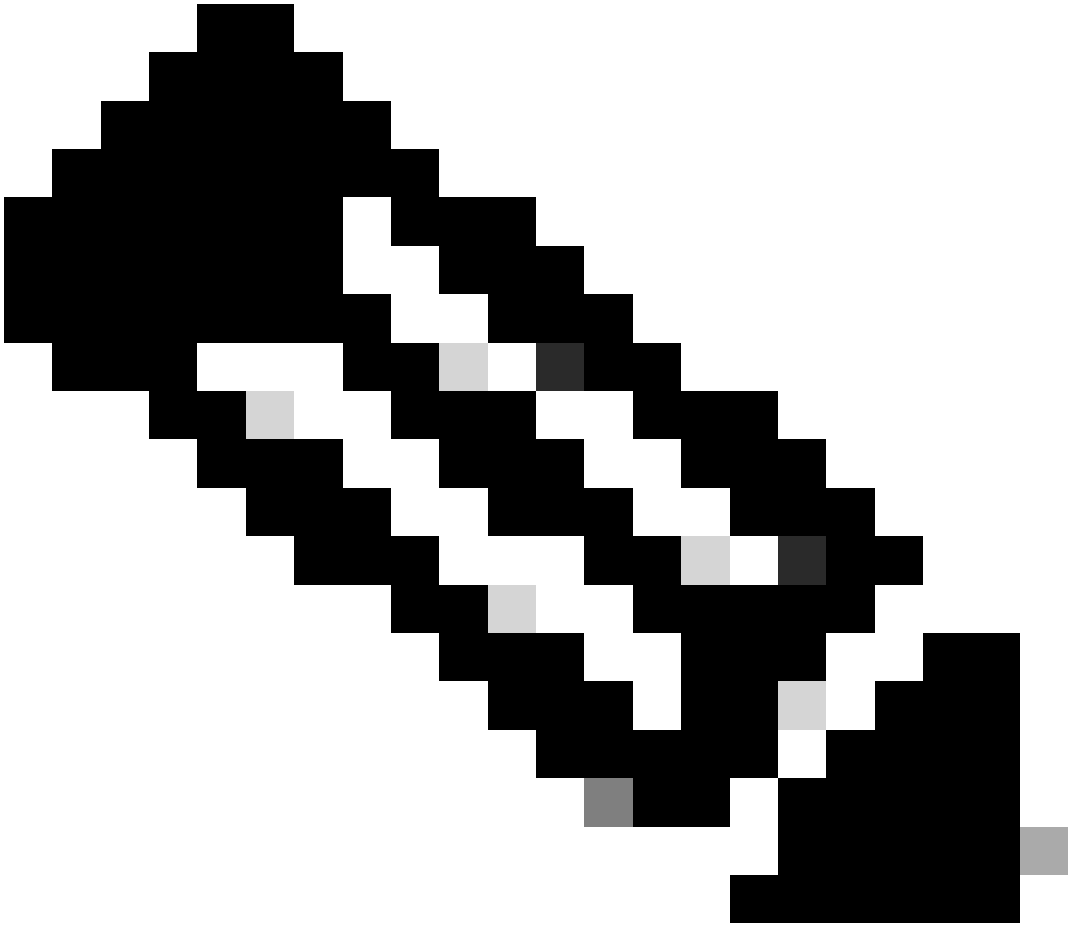
Step 2: Den Verkehr auf Ihrer Firewall zulassen.

Damit Secure Access das ISE-Gerät für die Radius-Authentifizierung verwenden kann, müssen Sie eine Regel von Secure Access für Ihr Netzwerk mit den erforderlichen Radius-Ports konfiguriert haben:

Regel	Quelle	Ziel	Zielport
ISE für sicheren Zugriff **Management-Pool**	ISE-Server	Management-IP-Pool (RA-VPN)	**KAO** UDP 1700 (Standard-Port)
Sicherer Access Management-IP-Pool zur ISE	Management-IP-Pool	ISE-Server	**Authentifizierung, Autorisierung** UDP 1812 (Standard-Port) **Buchhaltung** UDP 1813 (Standard-Port)
IP-Pool für sicheren Zugriff auf ISE	Endpunkt-IP-Pool	ISE-Server	**Bereitstellungsportal** TCP 8443 (Standard-Port)
IP-Pool für sicheren Zugriff auf DNS-SERVER	Endpunkt-IP-Pool	DNS-Server	**DNS** UDP und TCP 53



Hinweis: Weitere Informationen zu ISE-Ports finden Sie im Benutzerhandbuch - Port-Referenz.



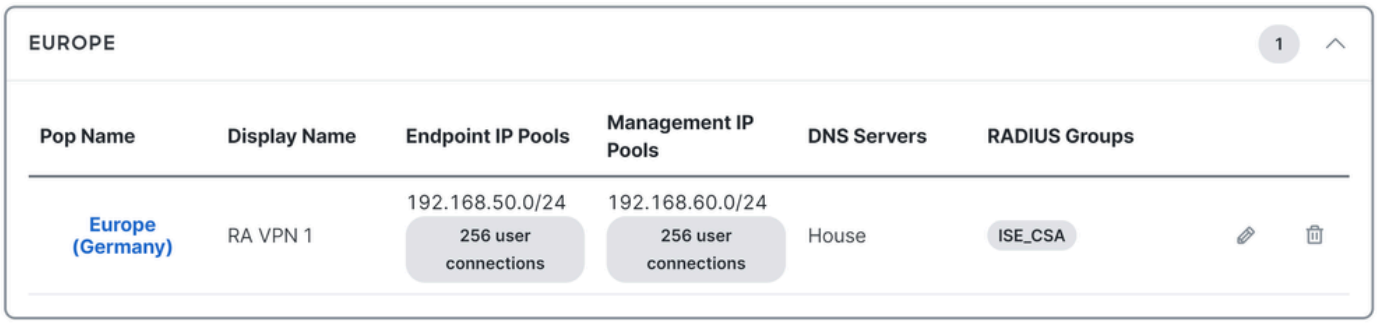
Hinweis: Wenn Sie Ihre ISE so konfiguriert haben, dass sie über einen Namen wie ise.ciscosspt.es erkannt wird, ist eine DNS-Regel erforderlich.

Management-Pool und Endpunkt-IP-Pools

Um Ihren Management- und Endpunkt-IP-Pool zu überprüfen, navigieren Sie zu Ihrem Secure Access Dashboard:

- Klicken Sie **Connect > End User Connectivity**
- Klicken Sie Virtual Private Network

- Unter **Manage IP Pools**
- Klicken Sie **Manage**

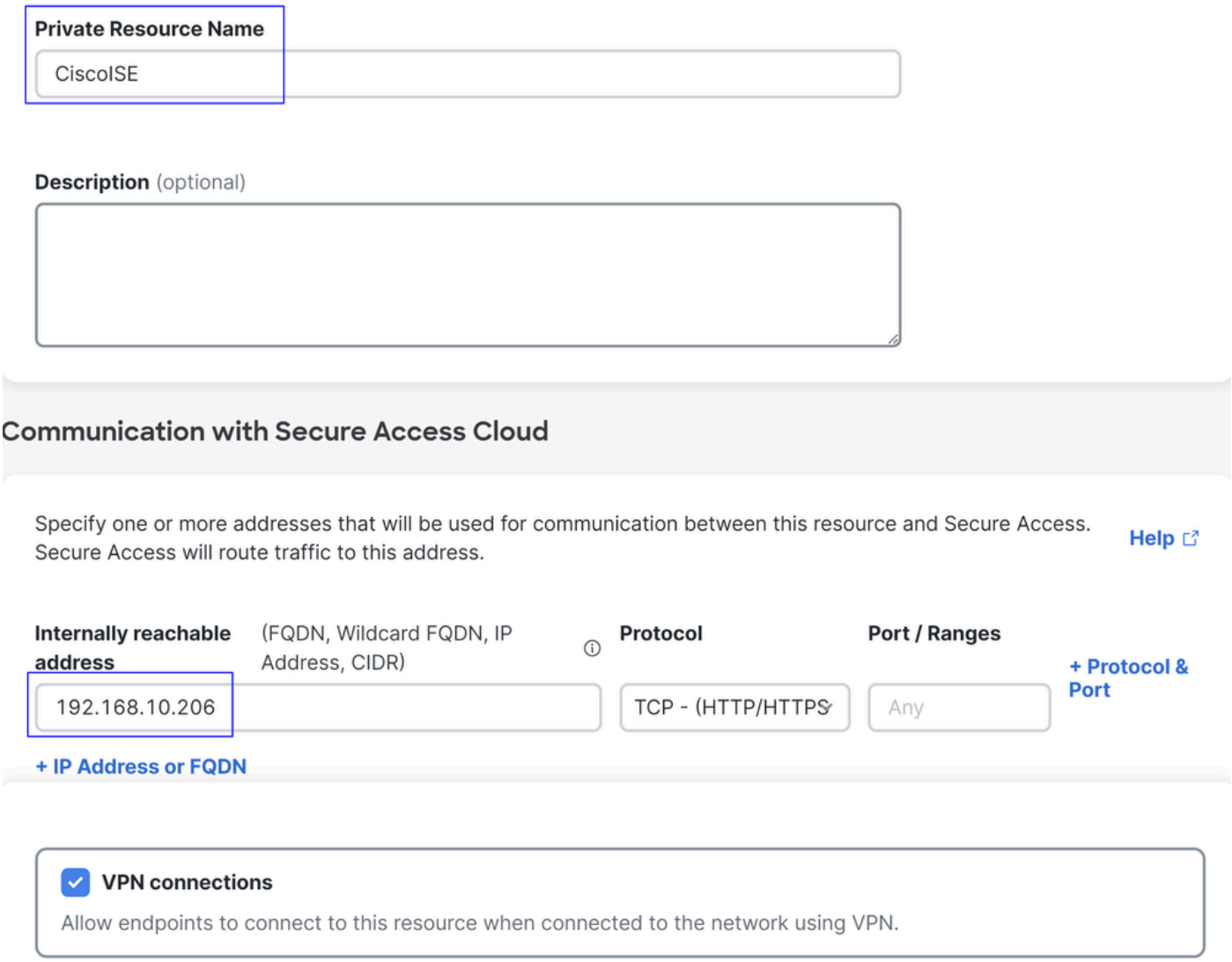


Schritt 3: Überprüfen der ISE-Konfiguration unter "Private Resources" (Private Ressourcen)

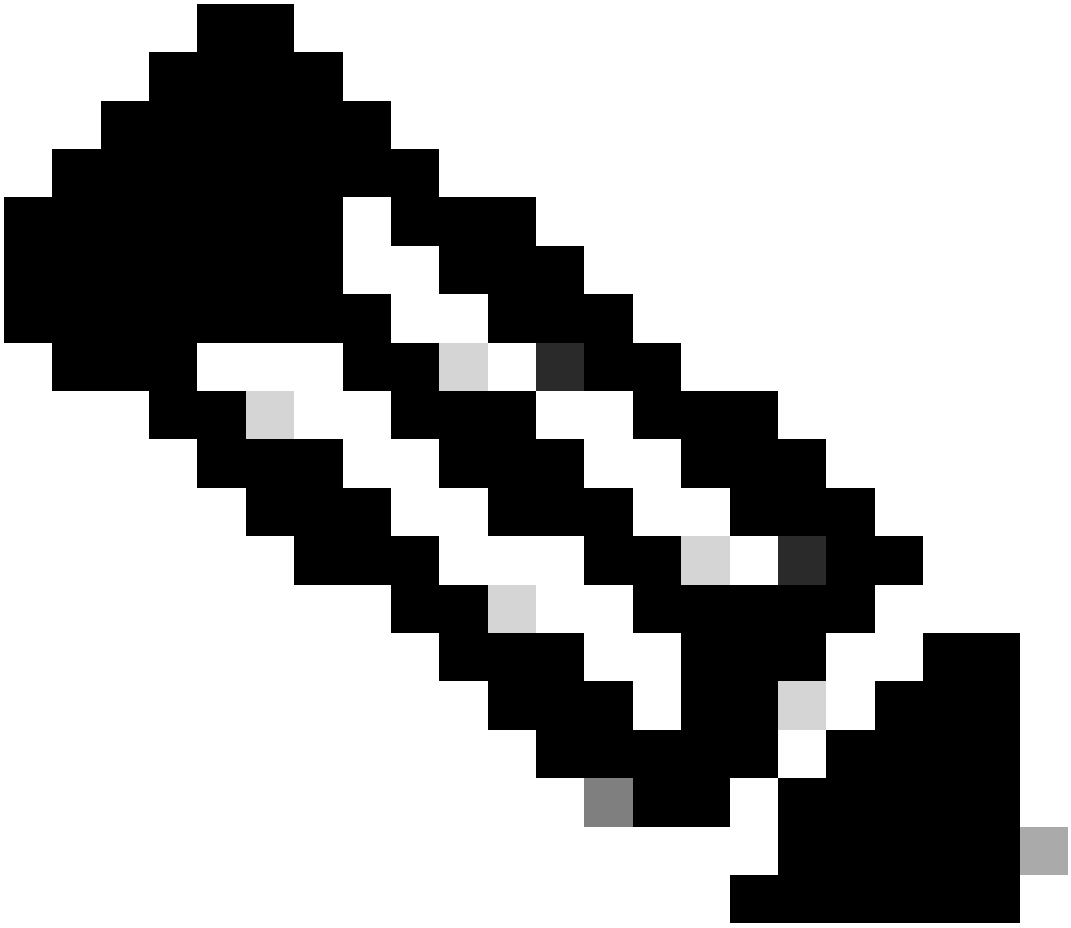
Damit die Benutzer, die über das VPN verbunden sind, zu navigieren **ISE Provisioning Portal**können, müssen Sie das Gerät als private Ressource konfiguriert haben, die den Zugriff ermöglicht. Damit wird die automatische Bereitstellung des Geräts über das VPN ermöglichtISE Posture Module.

Um zu überprüfen, ob ISE korrekt konfiguriert ist, navigieren Sie zu Ihrem Secure Access Dashboard:

- Klicken Sie **Resources > Private Resources**
- Klicken Sie auf die ISE-Ressource



Bei Bedarf können Sie die Regel auf den Bereitstellungsportal-Port (8443) beschränken.



Hinweis: Stellen Sie sicher, dass Sie das Kontrollkästchen für VPN-Verbindungen aktiviert haben.

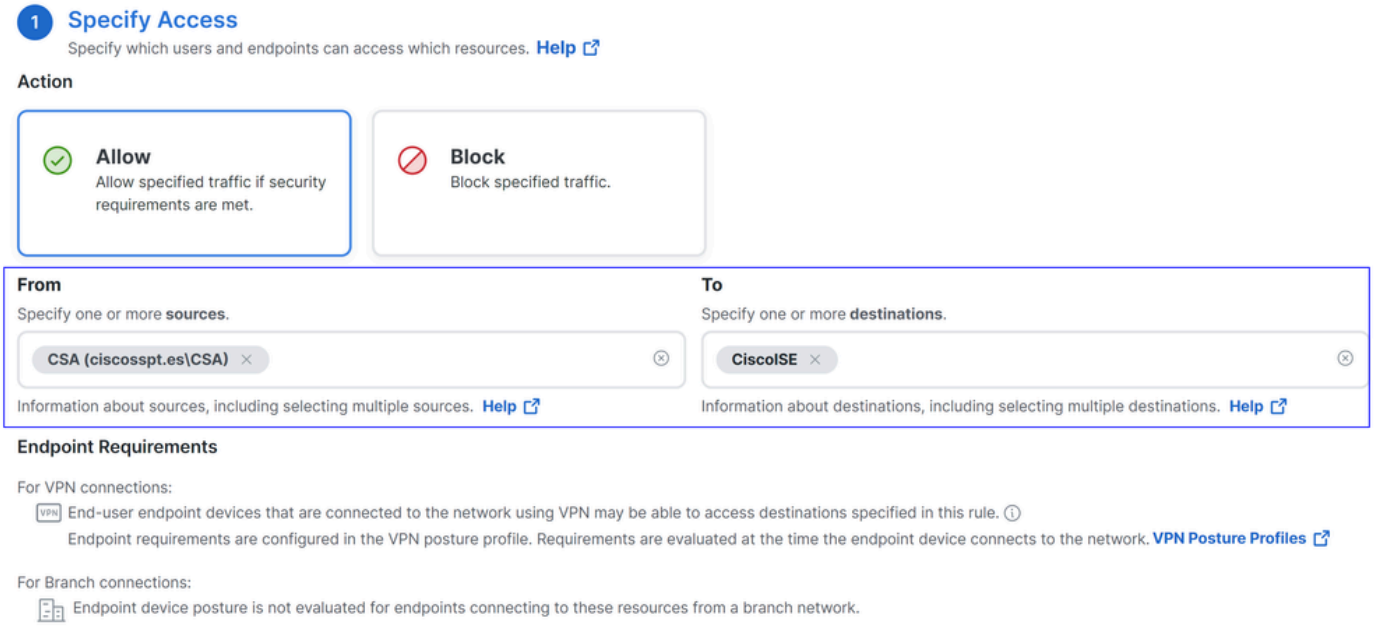
Schritt 4: Zulassen des ISE-Zugriffs gemäß der Zugriffsrichtlinie

Damit die Benutzer, die über das VPN verbunden sind, zu navigieren **ISE Provisioning Portal**können, müssen Sie sicherstellen, dass Sie eine konfiguriert haben, **Access Policy** damit die Benutzer, die unter dieser Regel konfiguriert sind, auf die in konfigurierte private Ressource zugreifen könnenStep3.

Um zu überprüfen, ob ISE korrekt konfiguriert ist, navigieren Sie zu Ihrem Secure Access Dashboard:

- Klicken Sie **Secure > Access Policy**

- Klicken Sie auf die konfigurierte Regel, um den Zugriff für die VPN-Benutzer auf die ISE zuzulassen.

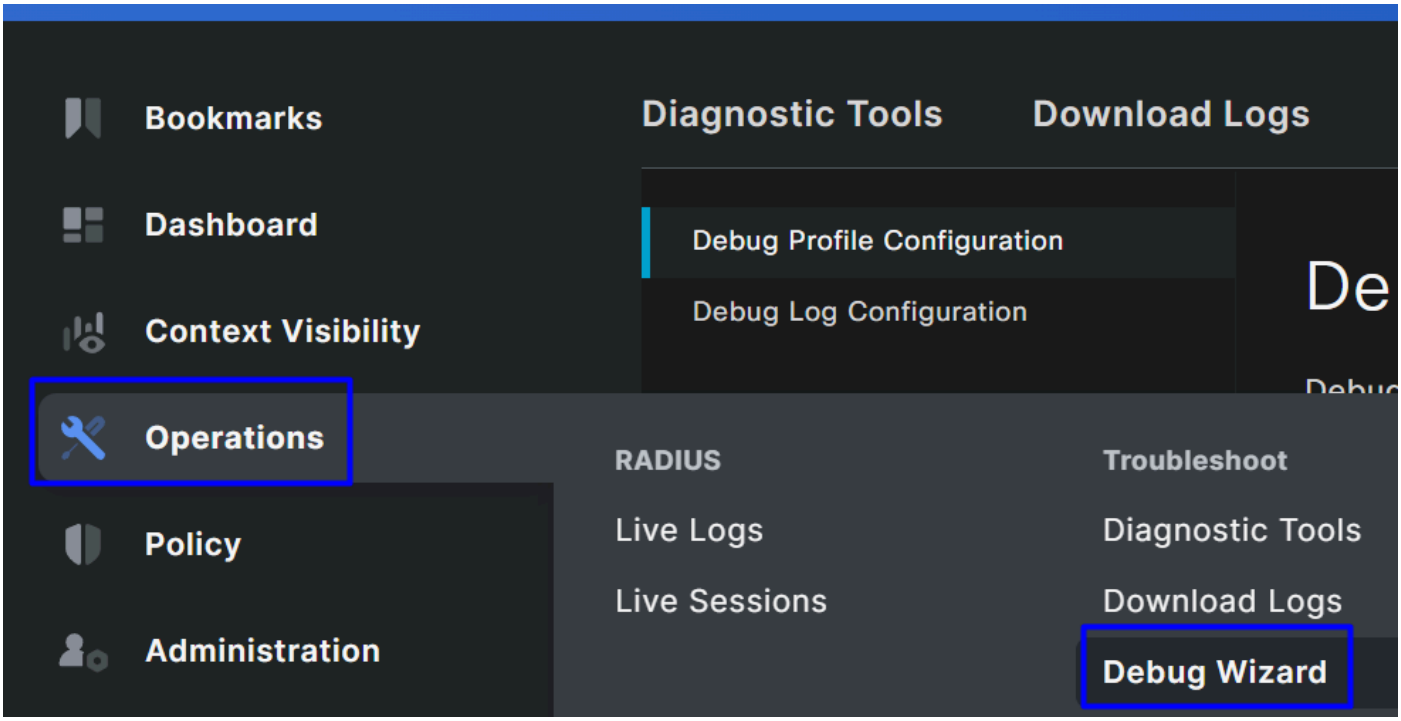


Fehlerbehebung

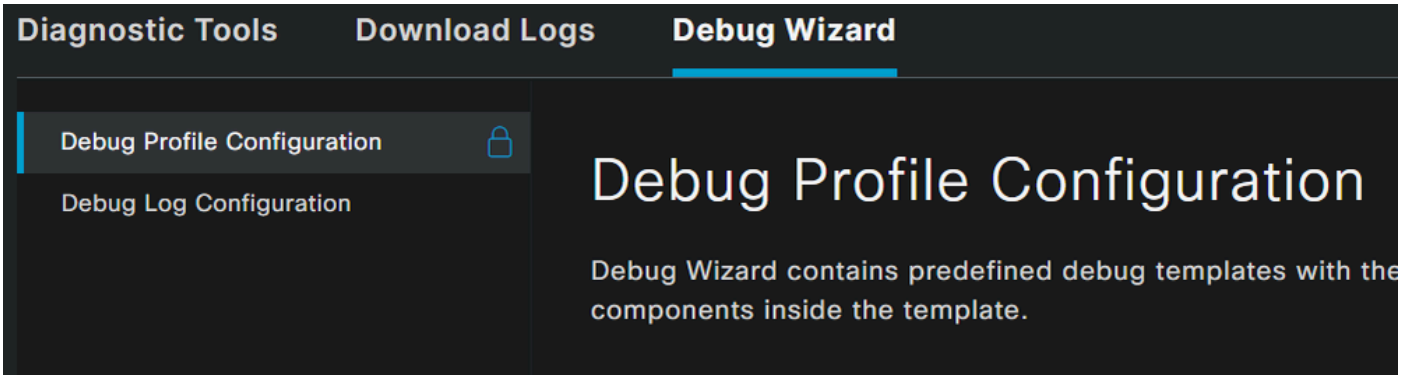
Herunterladen von ISE Posture Debug-Protokollen

So laden Sie ISE-Protokolle herunter, um ein Statusproblem zu überprüfen:

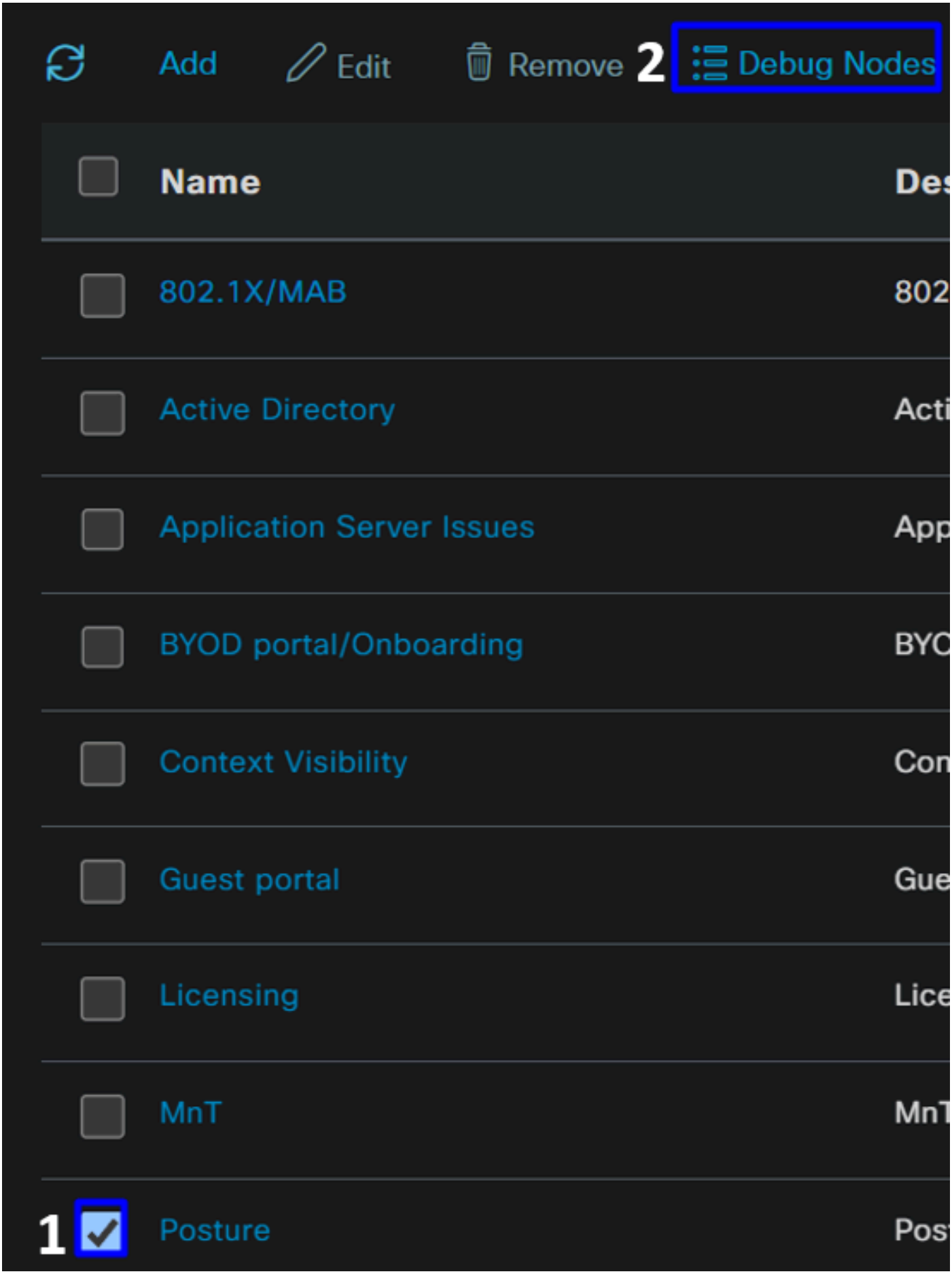
- Rufen Sie Ihr ISE Dashboard auf.
- Klicken Sie Operations > Troubleshoot > Debug Wizard



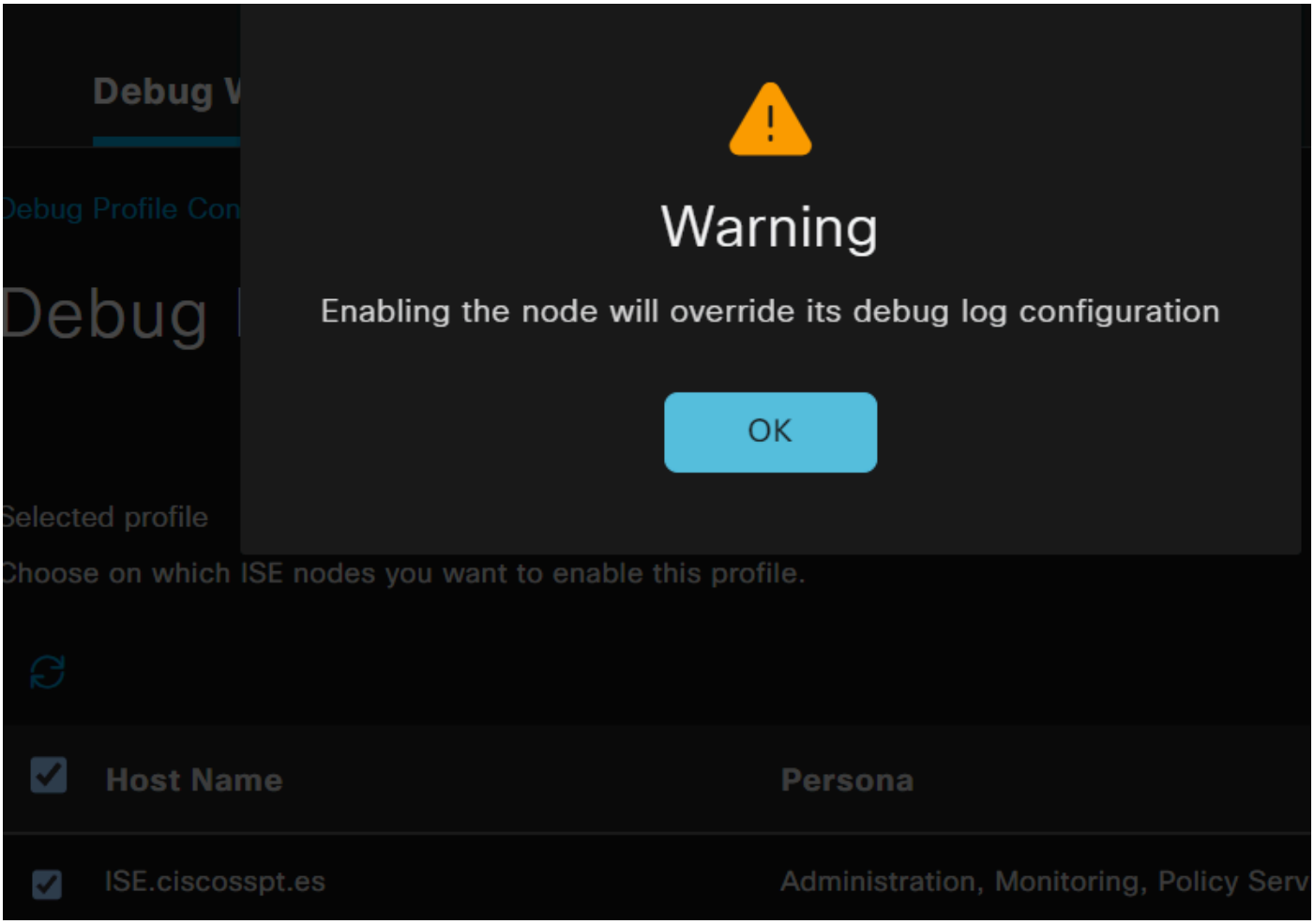
- Klicken Sie Debug Profile Configuration



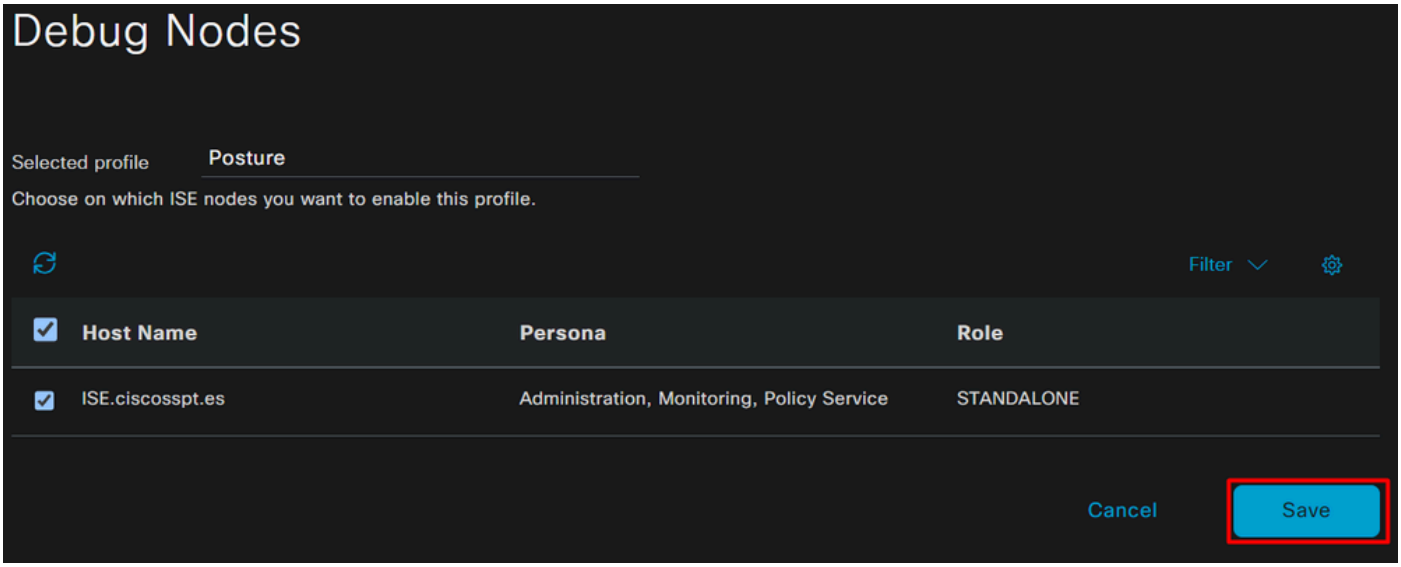
- Aktivieren Sie das Kontrollkästchen für **Posture > Debug Nodes**

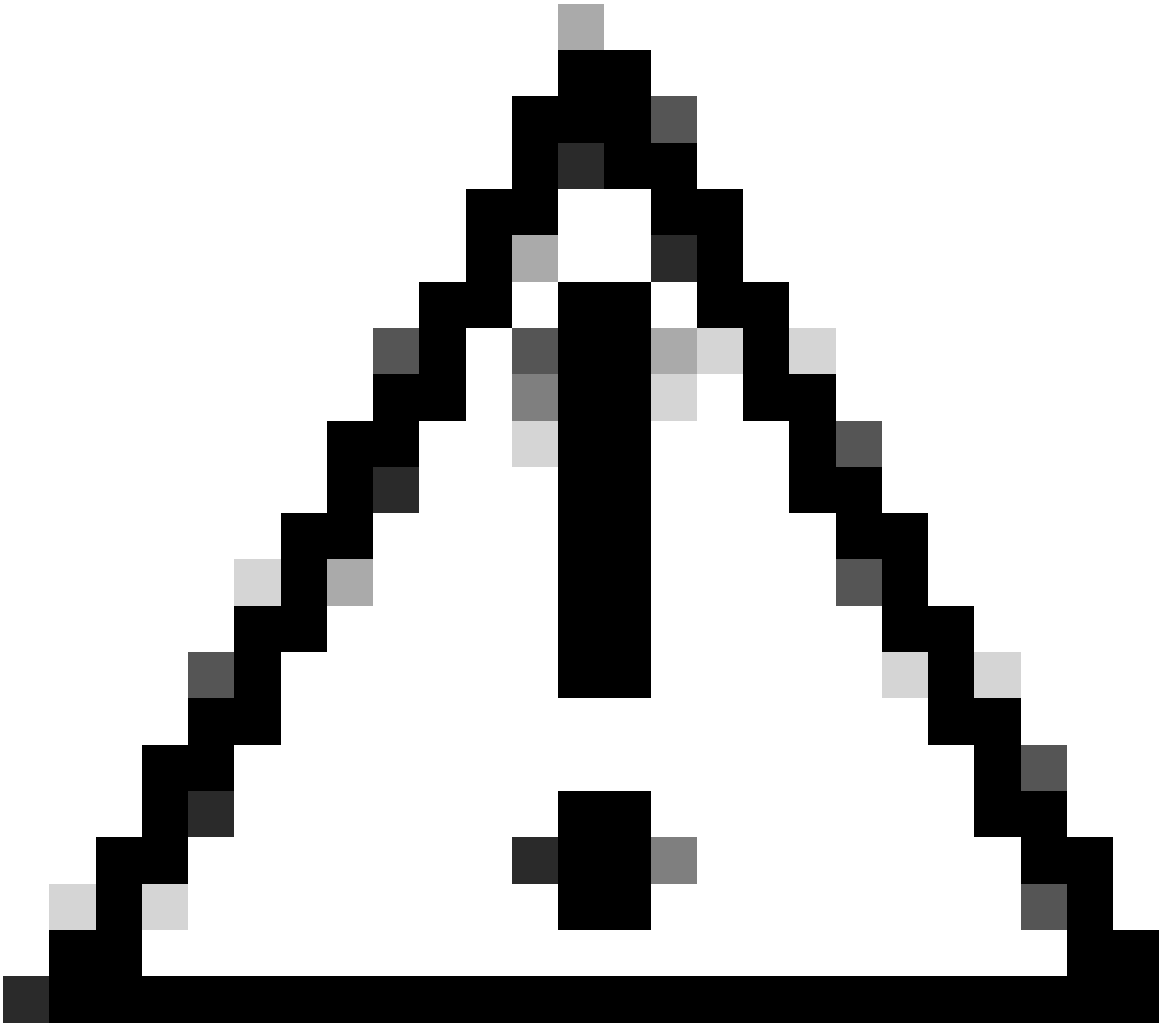

Add
Edit
Remove
2
Debug Nodes
Name
Des
802.1X/MAB
802
Active Directory
Acti
Application Server Issues
App
BYOD portal/Onboarding
BYO
Context Visibility
Con
Guest portal
Gue
Licensing
Lice
MnT
MnT
1
Posture
Post

- Aktivieren Sie das Kontrollkästchen für die ISE-Knoten, auf denen Sie den Debugmodus aktivieren möchten, um das Problem zu beheben.



- Klicken Sie auf Save

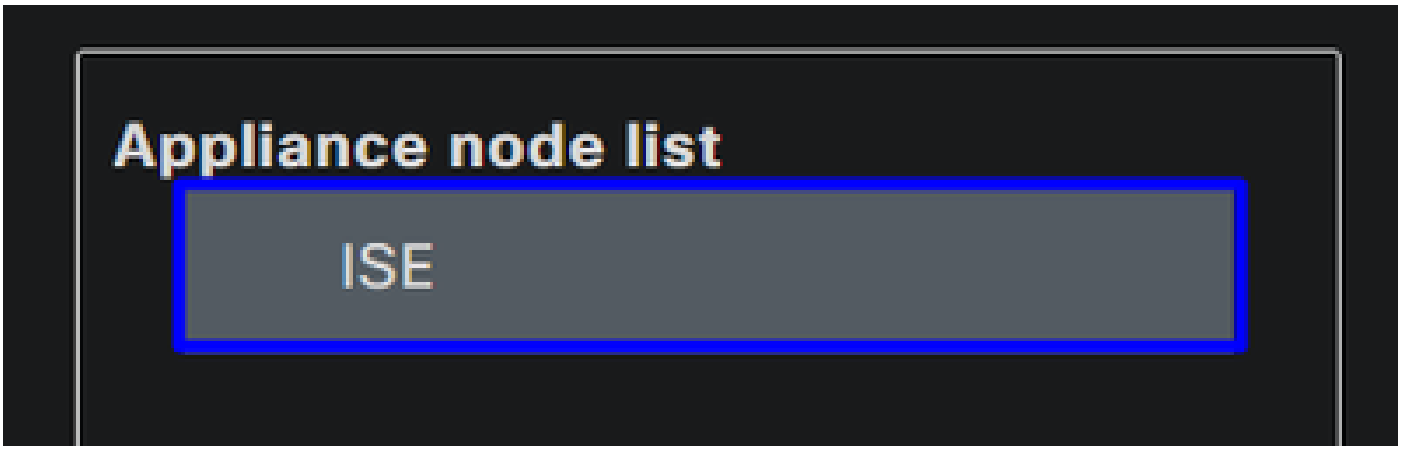

Debug Nodes
Selected profile
Posture
Choose on which ISE nodes you want to enable this profile.
Filter
Host Name
Persona
Role
ISE.ciscosspt.es
Administration, Monitoring, Policy Service
STANDALONE
Cancel
Save



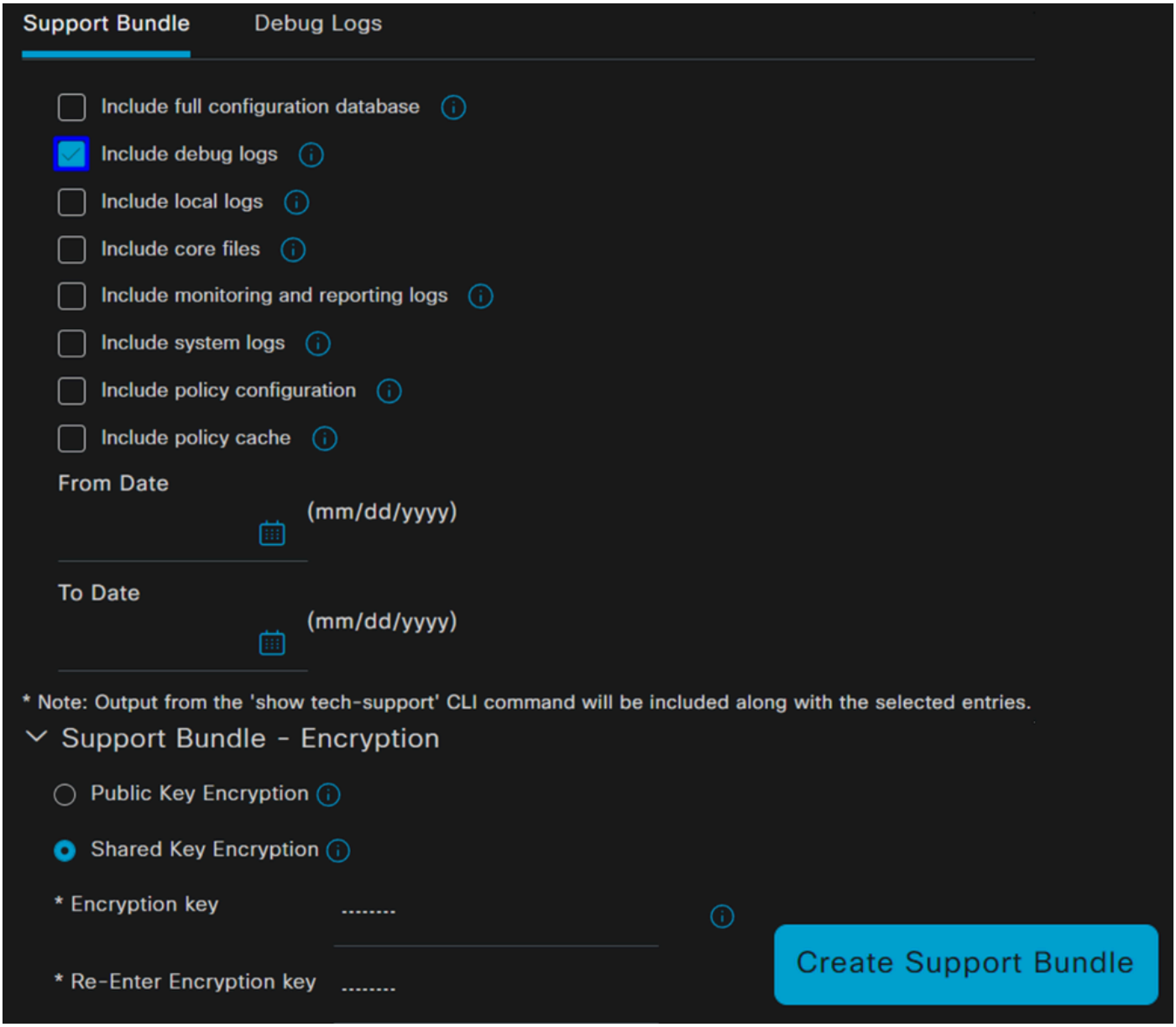
Vorsicht: Nach diesem Punkt müssen Sie anfangen, das Problem zu reproduzieren; **the debug logs can affect the performance of your device**.

Wenn Sie das Problem reproduziert haben, fahren Sie mit den folgenden Schritten fort:

- Klicken Sie Operations > Download Logs
- Wählen Sie den Knoten aus, von dem Sie die Protokolle übernehmen möchten.

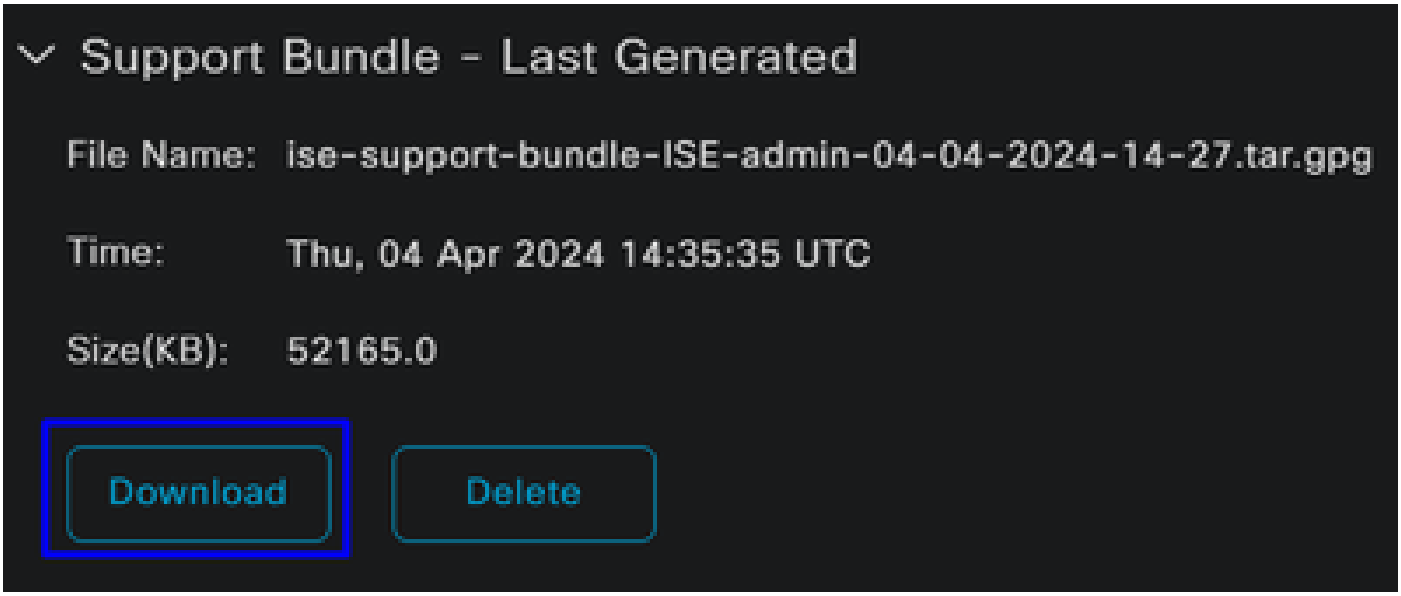


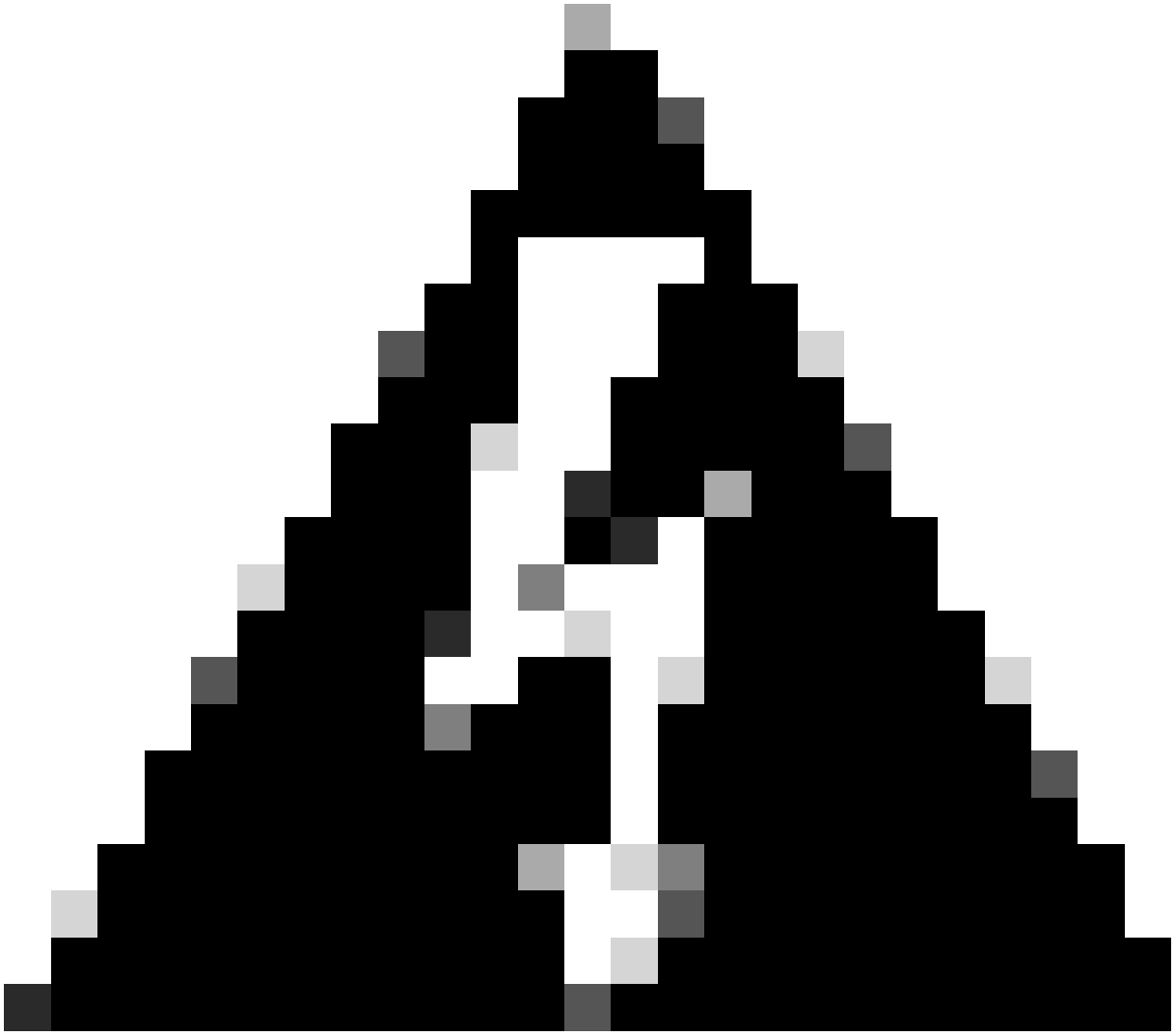
- Wählen Sie unter **Support Bundle** den folgenden Optionen aus:



- Include debug logs
- Unter **Support Bundle Encryption**
    - **Shared Key Encryption**
        - Füllen **Encryption key** und **Re-Enter Encryption key**

- Klicken Sie auf **Create Support Bundle**
- Klicken Sie auf **Download**



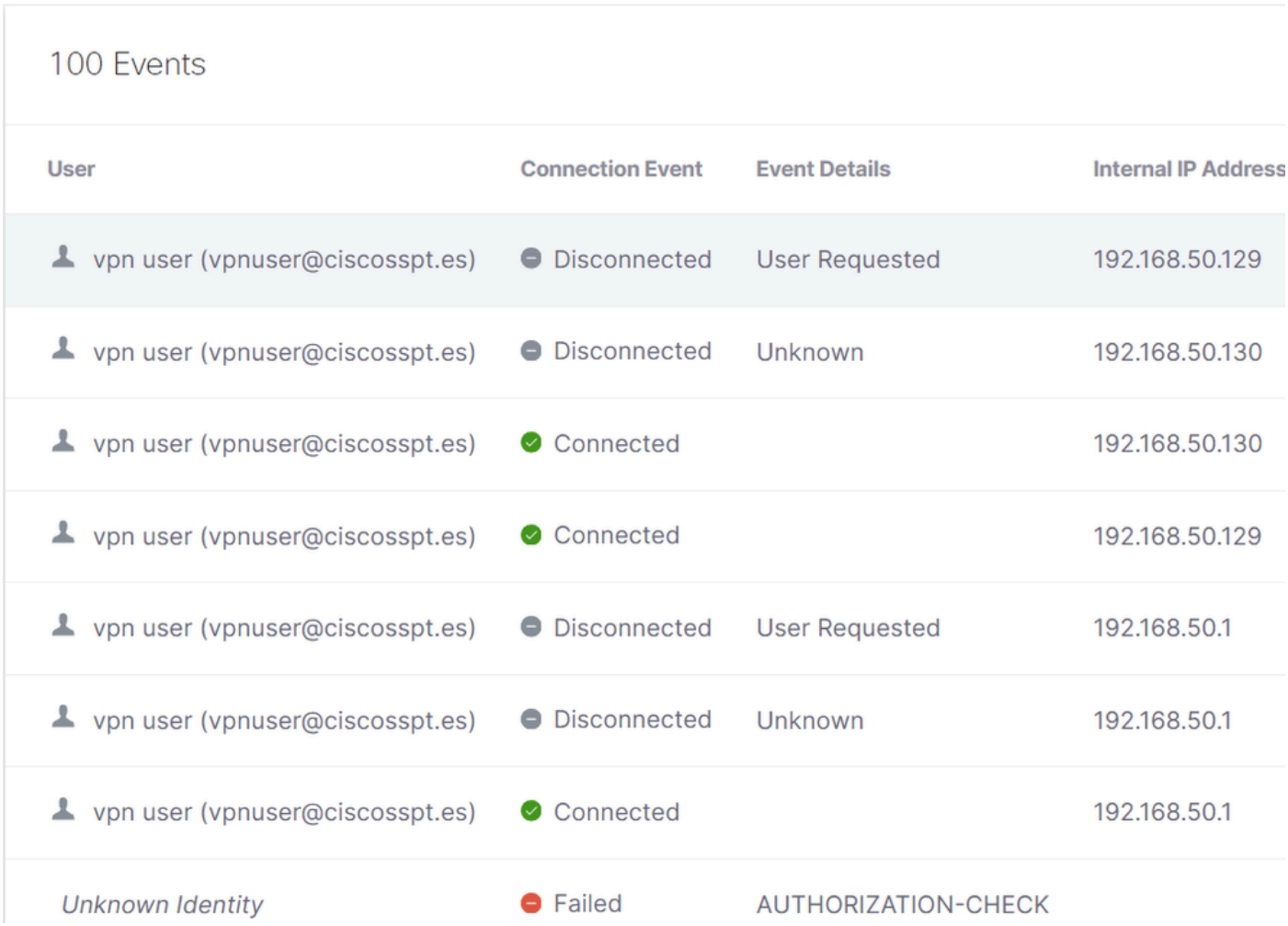


Warnung: Deaktivieren Sie den Debug-Modus, der im Schritt "Debug Profile Configuration" aktiviert ist.

So überprüfen Sie Protokolle für den sicheren Zugriff auf Remote-Zugriff

Navigieren Sie zu Ihrem Secure Access Dashboard:

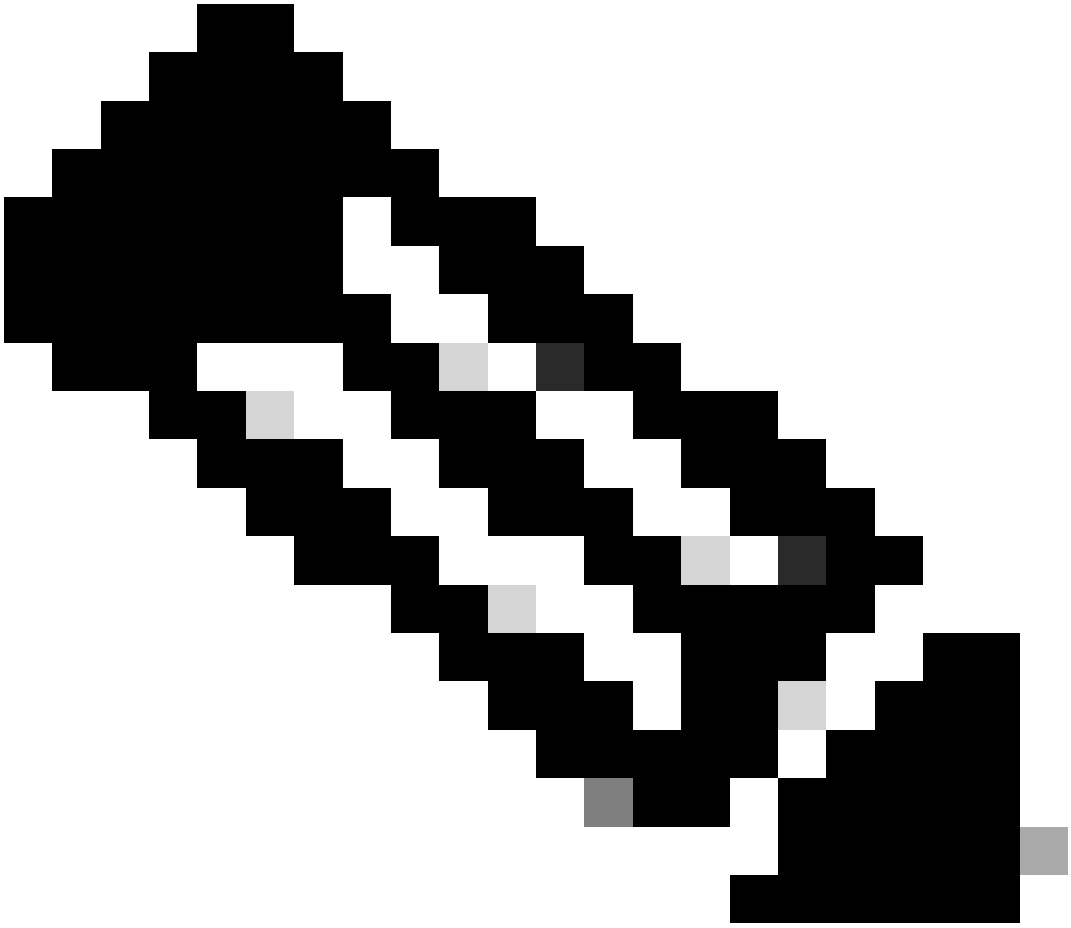
- Klicken Sie Monitor > Remote Access Logs



DART-Paket auf sicherem Client generieren

Überprüfen Sie den folgenden Artikel, um das DART-Paket auf Ihrem Computer zu generieren:

Cisco Secure Client Diagnostic and Reporting Tool (DART)



Hinweis: Nachdem Sie die im Abschnitt zur Fehlerbehebung angegebenen Protokolle gesammelt haben, öffnen Sie ein Ticket bei , **TAC** um mit der Analyse der Informationen fortzufahren.

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**
- **Secure Access-Dokumentation und Benutzerhandbuch**

- **Software-Download für Cisco Secure Client**
- **Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3**

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.