Konfigurieren der externen RADIUS-Authentifizierung für DNA Center und ISE 3.1

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der externen RADIUS-Authentifizierung auf dem Cisco DNA Center mit einem Cisco ISE-Server mit Version 3.1 beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco DNA Center und Cisco ISE sind bereits integriert, und die Integration hat den Status "Aktiv".

Verwendete Komponenten

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

- Cisco DNA Center Version 2.3.5.x
- Cisco ISE Version 3.1

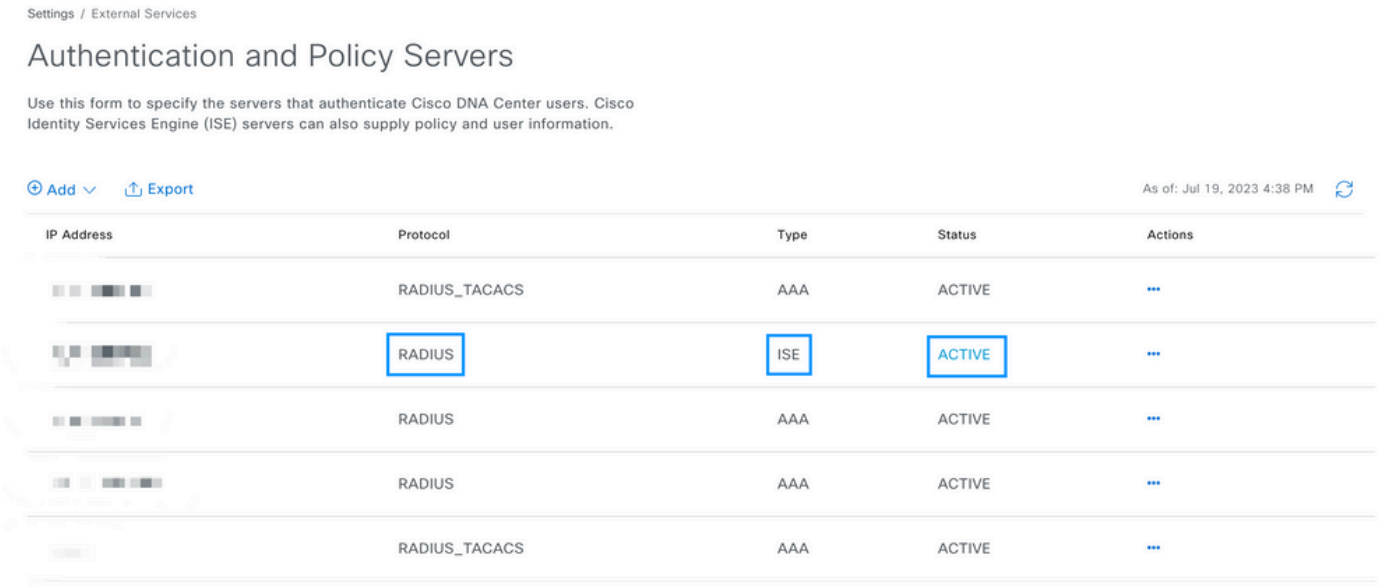
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

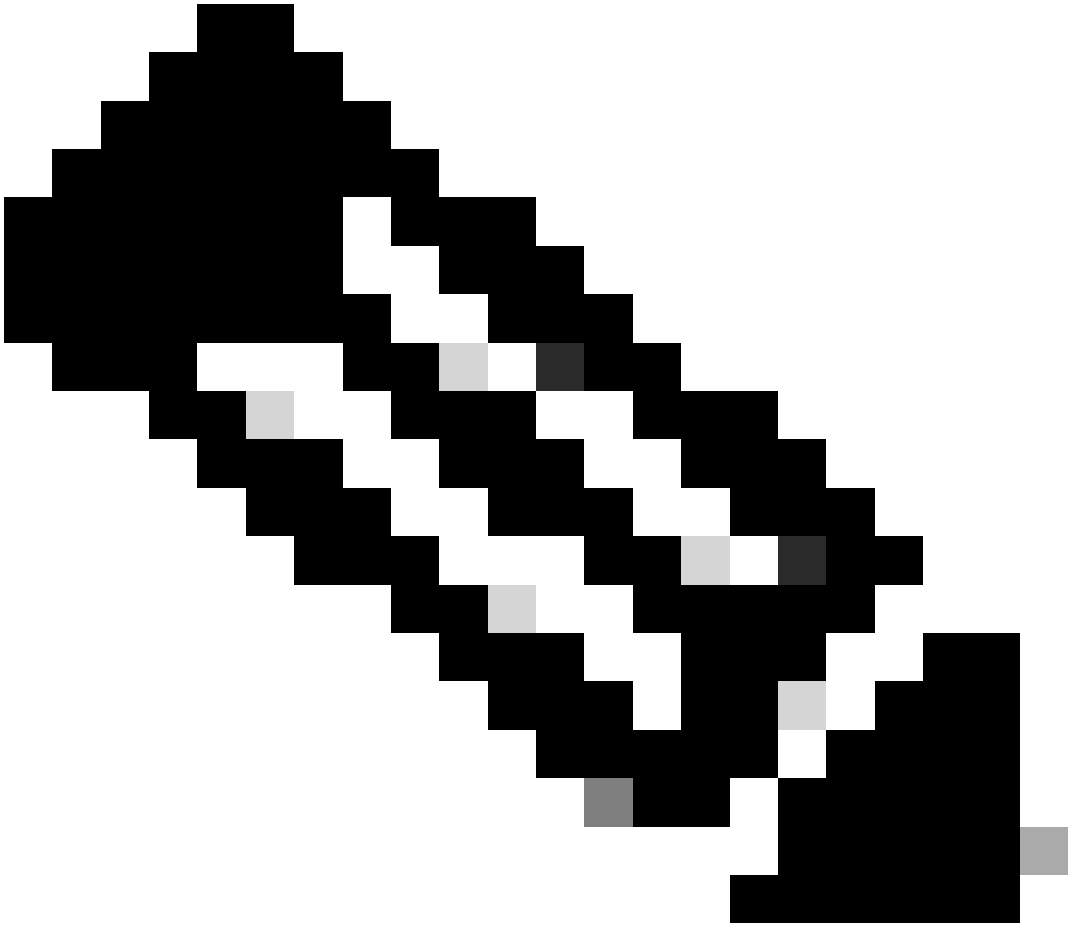
Konfigurieren

Schritt 1: Melden Sie sich bei der Cisco DNA Center-GUI an, und navigieren Sie zu System >

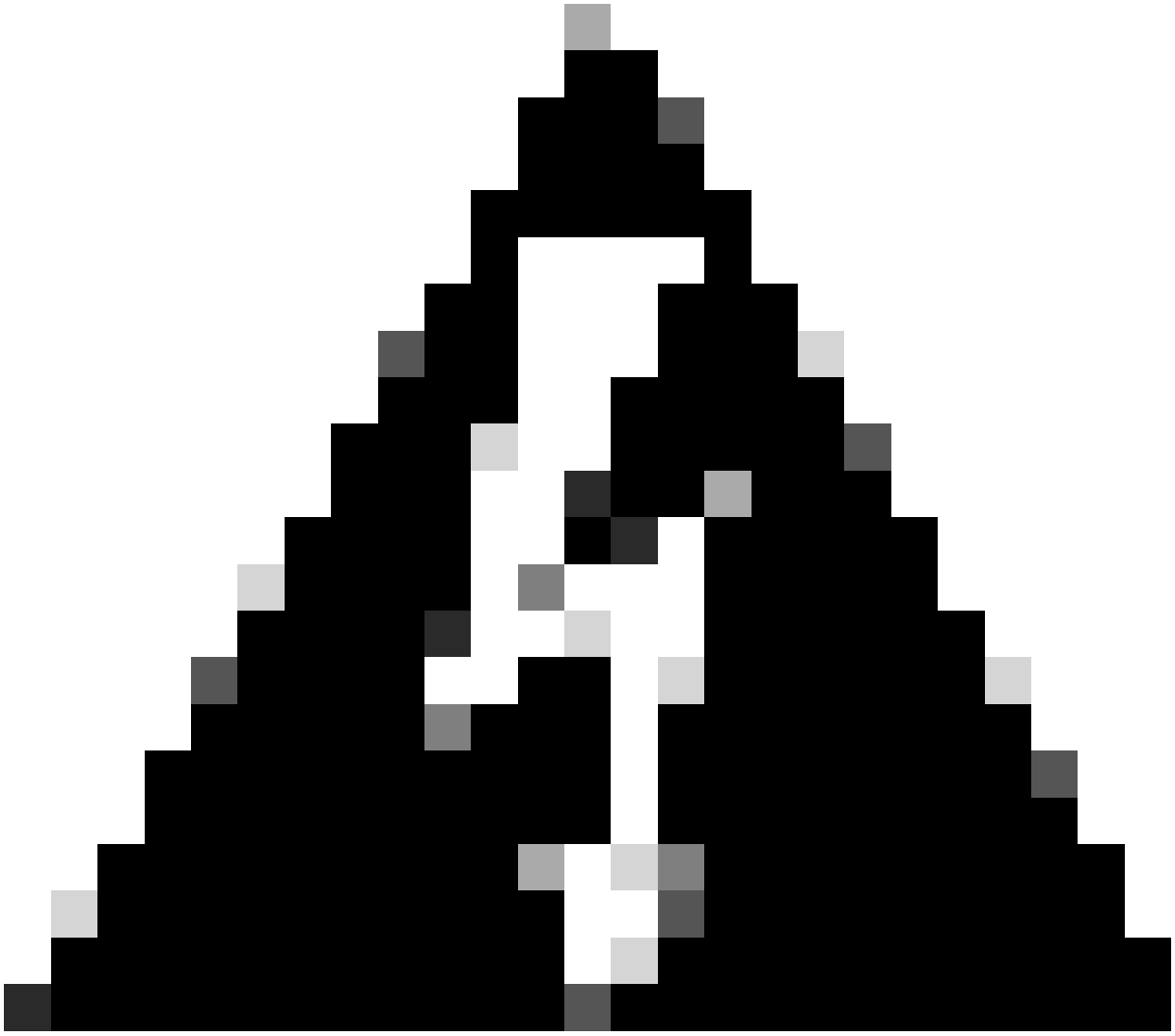
Settings > Authentication and Policy Servers.

Überprüfen Sie, ob das RADIUS-Protokoll konfiguriert ist und der ISE-Status für den ISE-Typ-Server Aktiv ist.





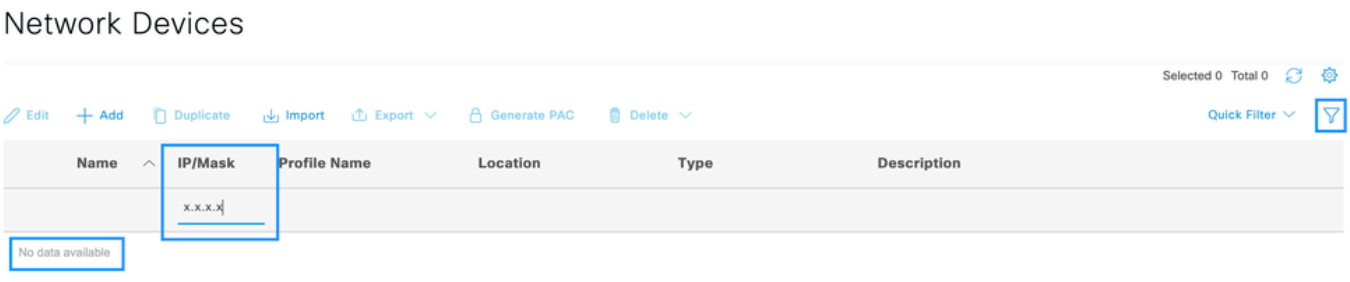
Hinweis: Der Protokolltyp RADIUS_TACACS funktioniert für dieses Dokument.



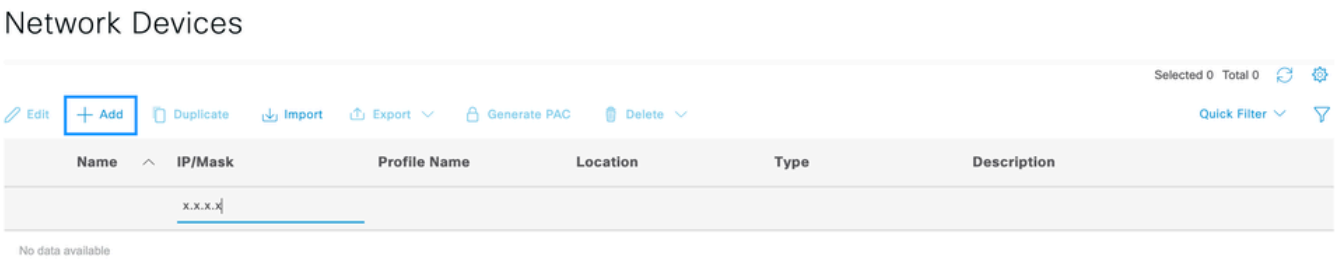
Warnung: Wenn sich der ISE-Server nicht im aktiven Status befindet, müssen Sie zuerst die Integration reparieren.

Schritt 2: Navigieren Sie auf dem ISE-Server zu Administration > Network Resources > Network Devices, klicken Sie auf das Filter-Symbol, schreiben Sie die Cisco DNA Center-IP-Adresse, und bestätigen Sie, ob ein Eintrag vorhanden ist. Wenn dies der Fall ist, fahren Sie mit Schritt 3 fort.

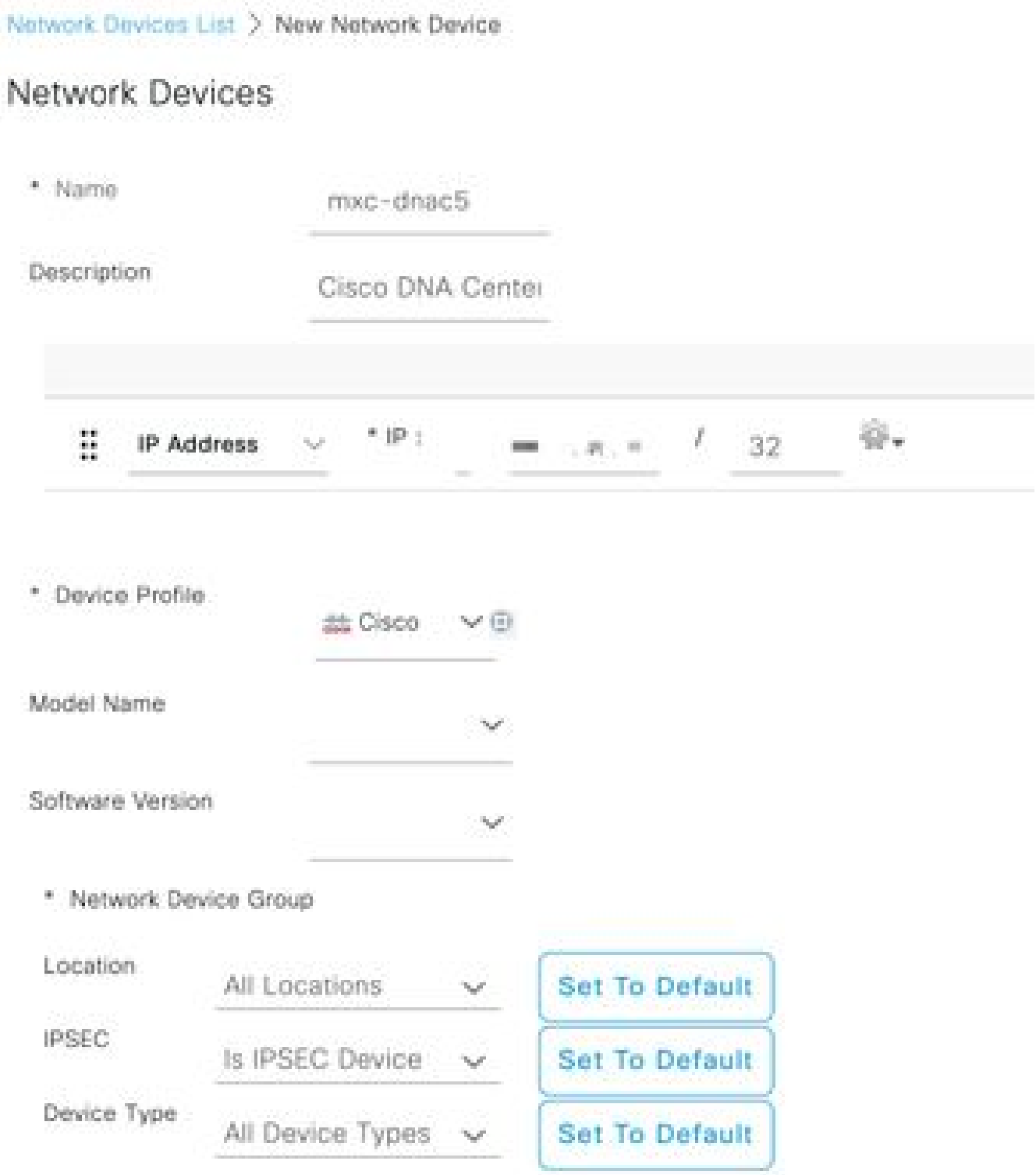
Wenn der Eintrag fehlt, muss die Meldung Keine Daten verfügbar angezeigt werden.



In diesem Fall müssen Sie ein Netzwerkgerät für Cisco DNA Center erstellen. Klicken Sie dazu auf die Schaltfläche Hinzufügen.



Konfigurieren Sie den Namen, die Beschreibung und die IP-Adresse (oder die Adressen) von Cisco DNA Center. Alle anderen Einstellungen sind auf Standardwerte festgelegt und werden für die Zwecke dieses Dokuments nicht benötigt.



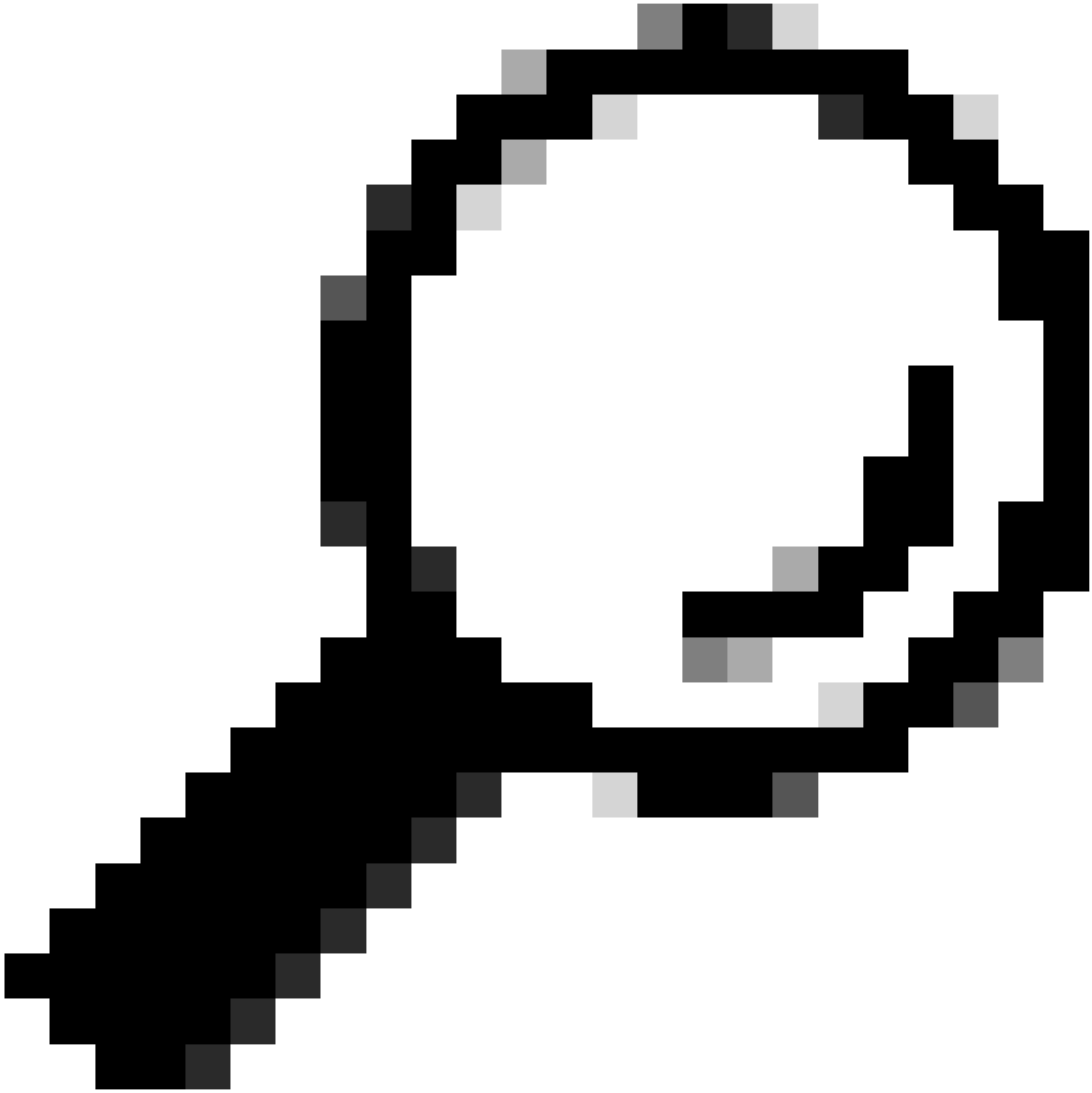
Blättern Sie nach unten, und aktivieren Sie die RADIUS-Authentifizierungseinstellungen, indem Sie auf das entsprechende Kontrollkästchen klicken und einen gemeinsamen geheimen Schlüssel konfigurieren.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret ••••••••• Show

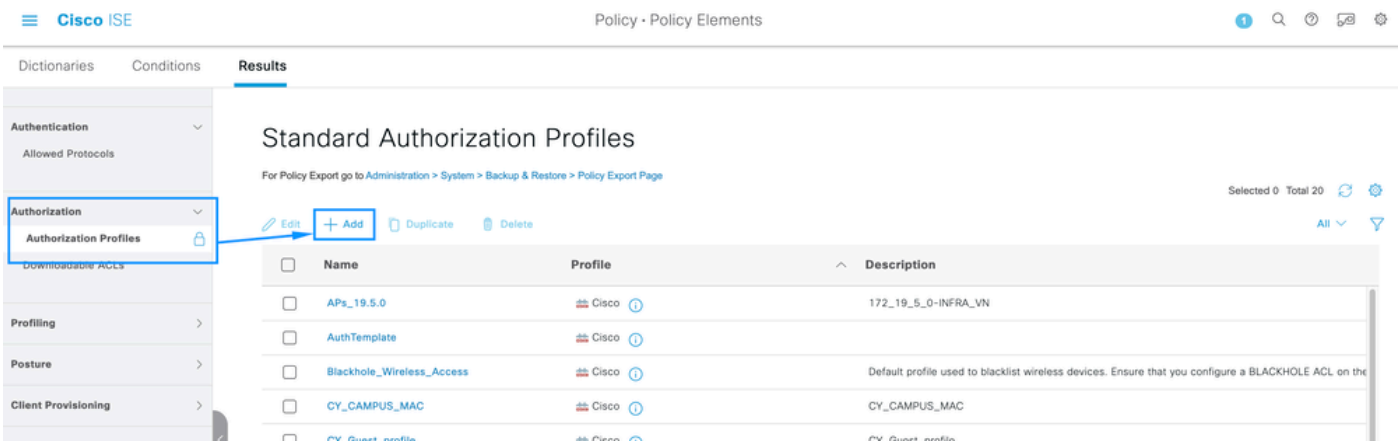


Tipp: Dieser gemeinsame geheime Schlüssel wird zu einem späteren Zeitpunkt benötigt. Speichern Sie ihn also an einer anderen Stelle.

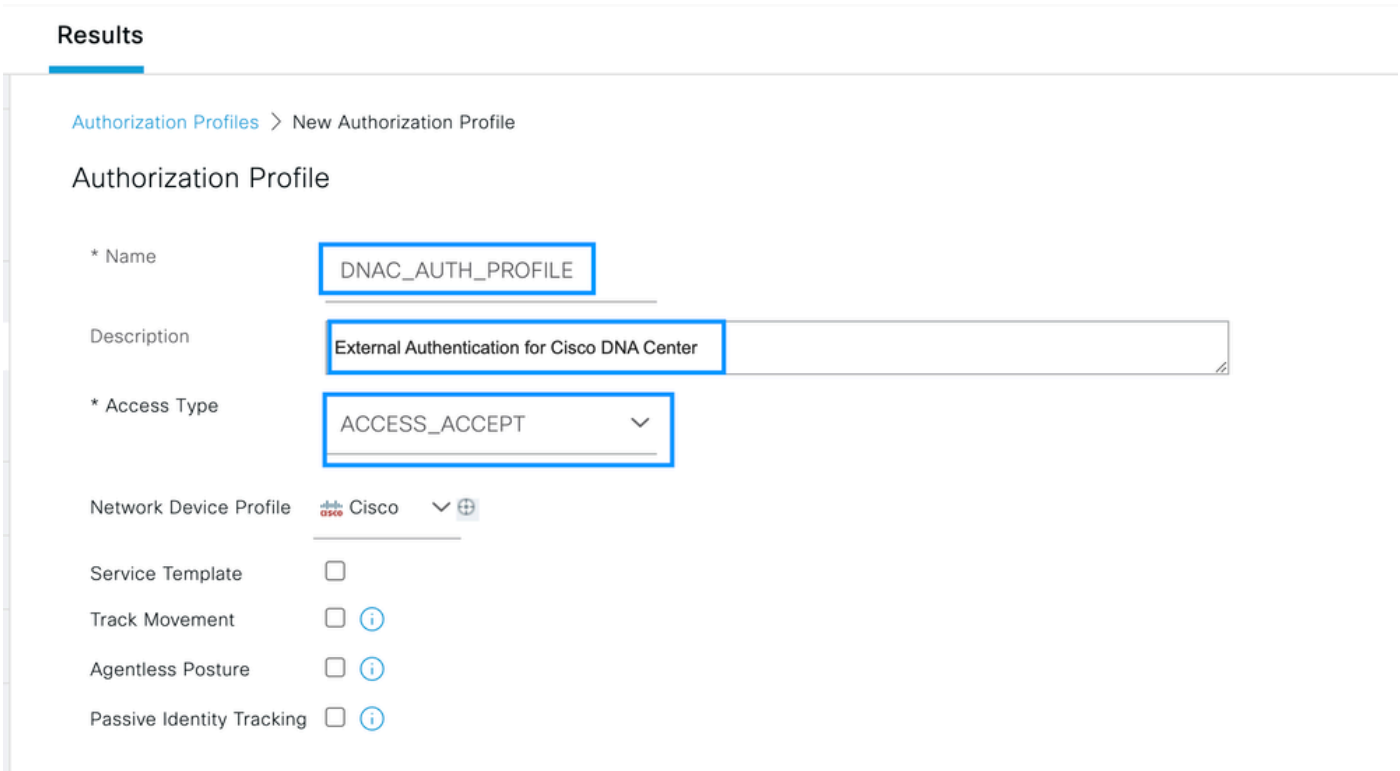
Klicken Sie dann auf Senden.

Schritt 3: Navigieren Sie auf dem ISE-Server zu Policy > Policy Elements > Results (Richtlinie > Richtlinienelemente > Ergebnisse), um das Autorisierungsprofil zu erstellen.

Vergewissern Sie sich, dass Sie unter Autorisierung > Autorisierungsprofile sind, und wählen Sie dann die Option Hinzufügen aus.



Name konfigurieren, eine Beschreibung hinzufügen, nur um das neue Profil zu speichern und sicherzustellen, dass der Zugriffstyp auf ACCES_ACCEPT gesetzt ist.

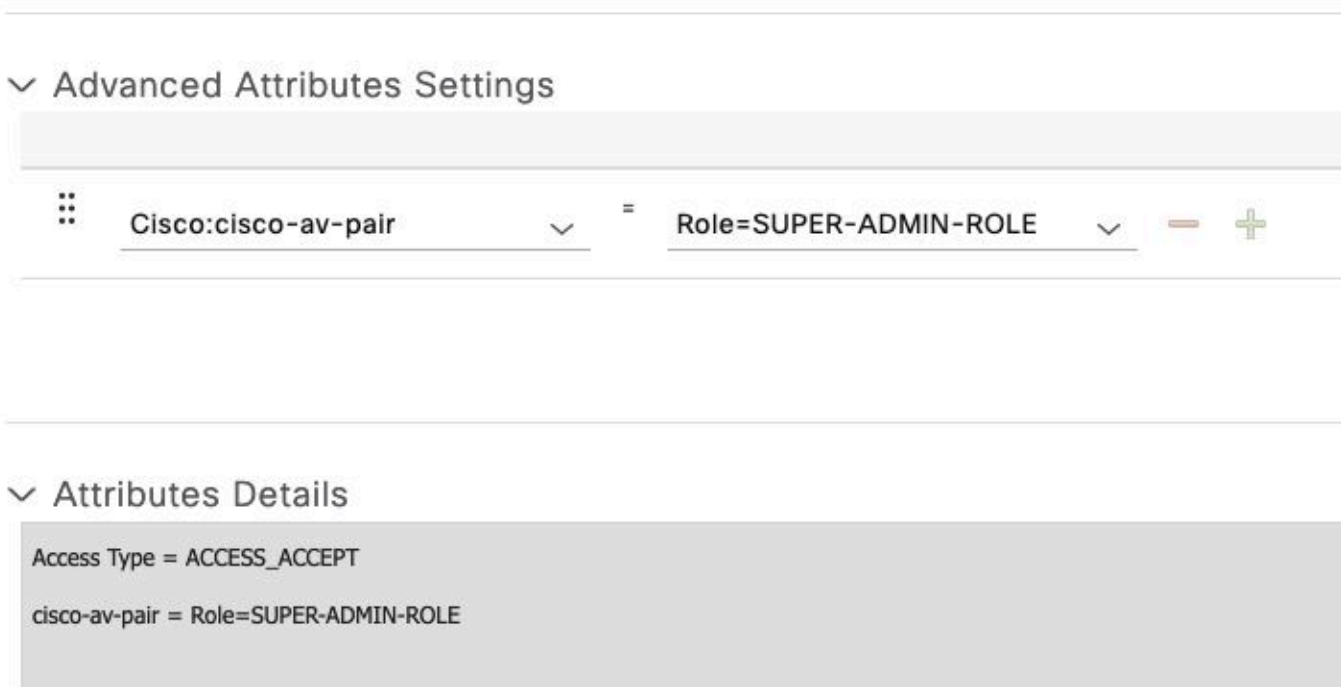


Blättern Sie nach unten, und konfigurieren Sie die erweiterten Attributeinstellungen.

Suchen Sie in der linken Spalte nach der Option cisco-av-pair, und wählen Sie sie aus.

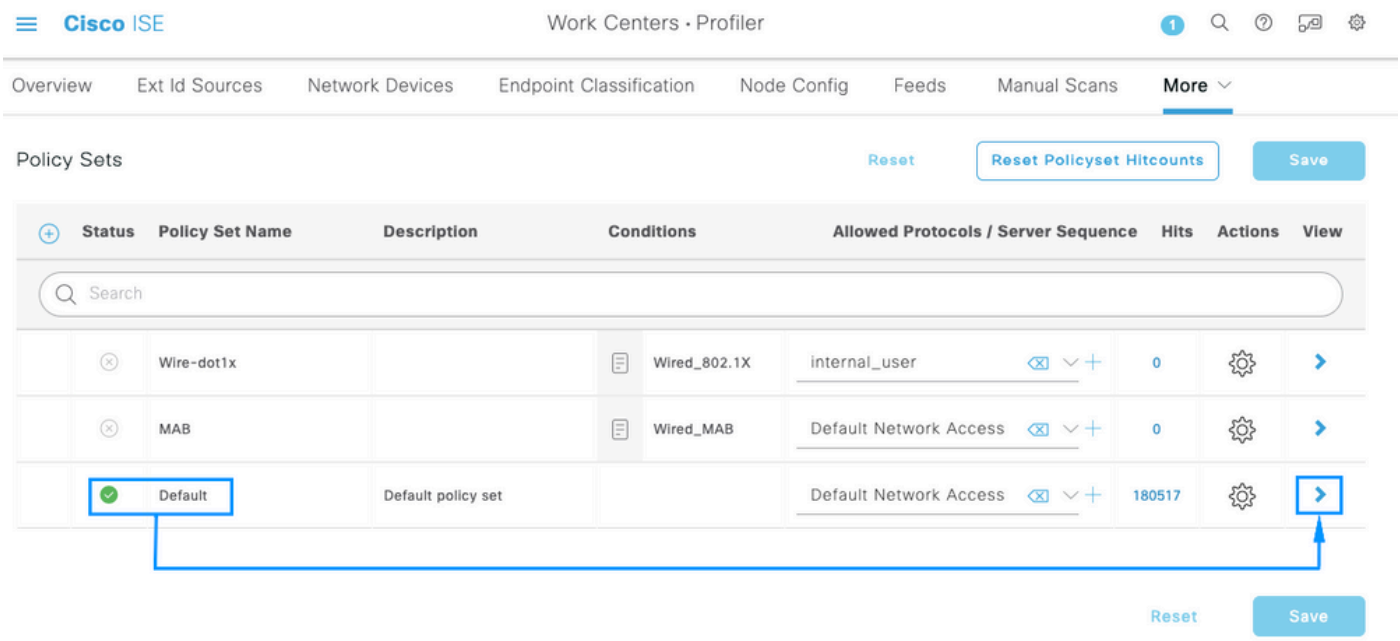
Geben Sie in der rechten Spalte manuell Role=SUPER-ADMIN-ROLE ein.

Sobald es wie das Bild unten aussieht, klicken Sie auf Senden.

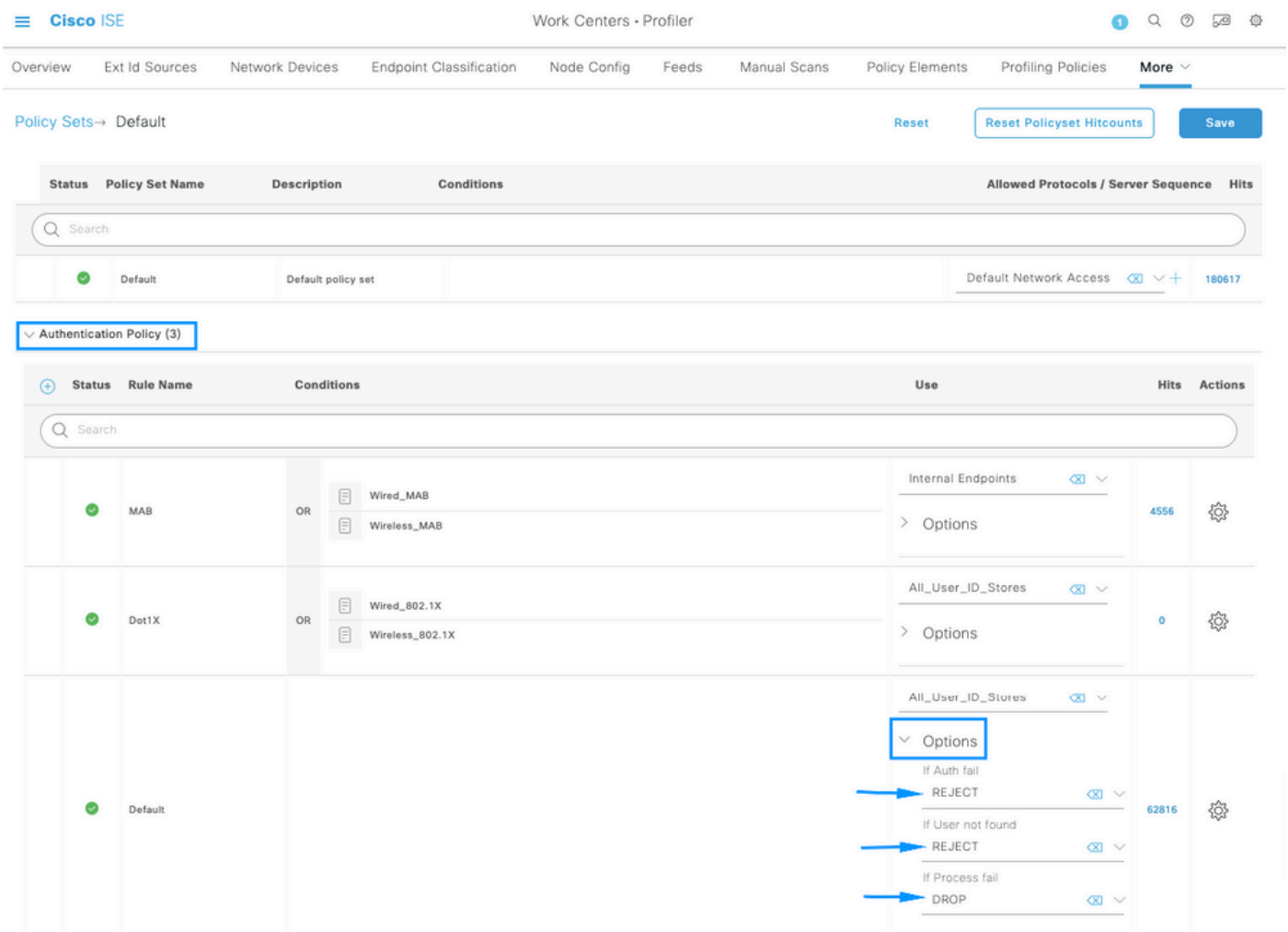


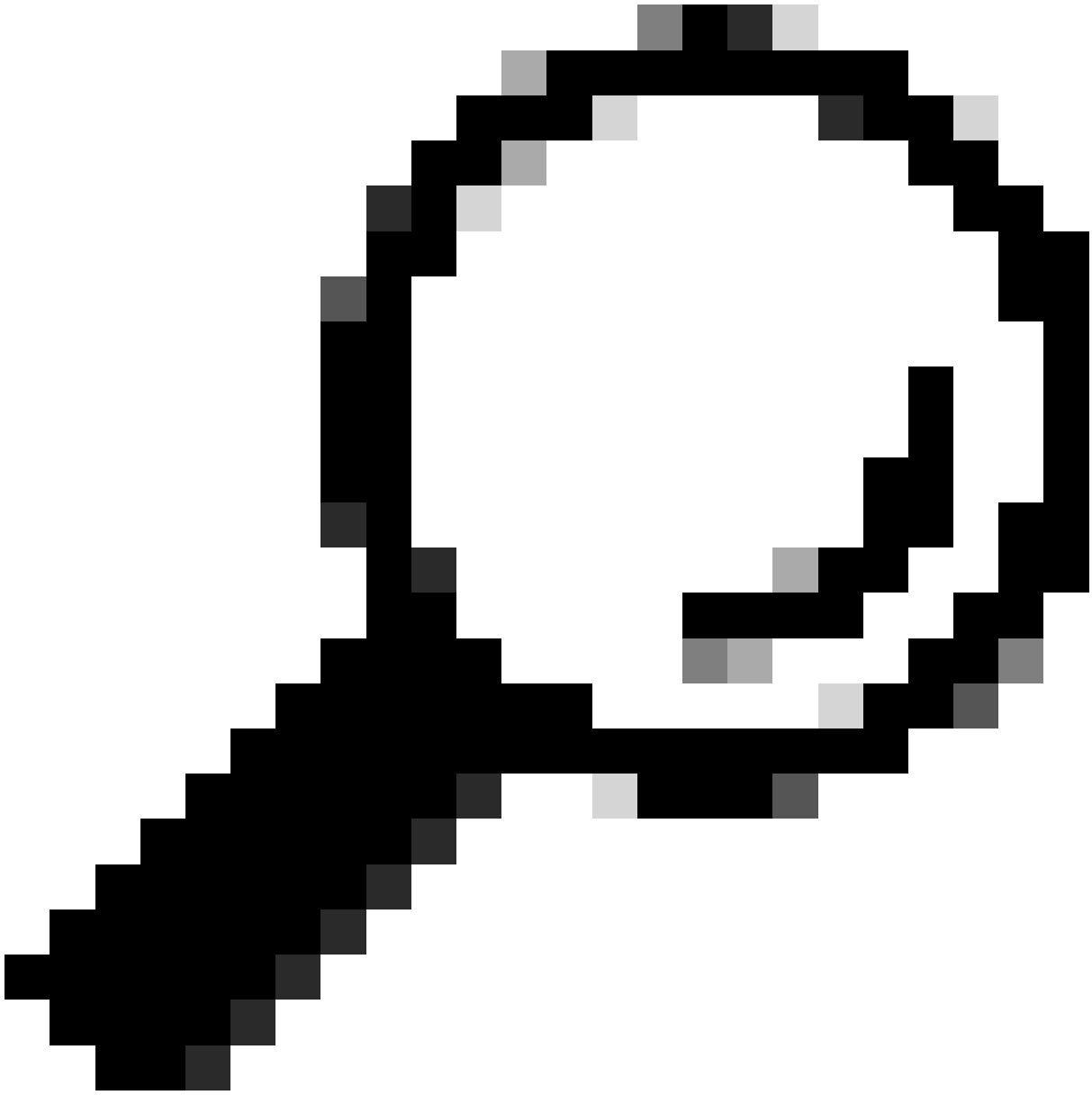
Schritt 4: Navigieren Sie auf dem ISE-Server zu Work Centers > Profiler > Policy Sets, um die Authentifizierungs- und Autorisierungsrichtlinie zu konfigurieren.

Identifizieren Sie die Standard-Richtlinie, und klicken Sie auf den blauen Pfeil, um sie zu konfigurieren.



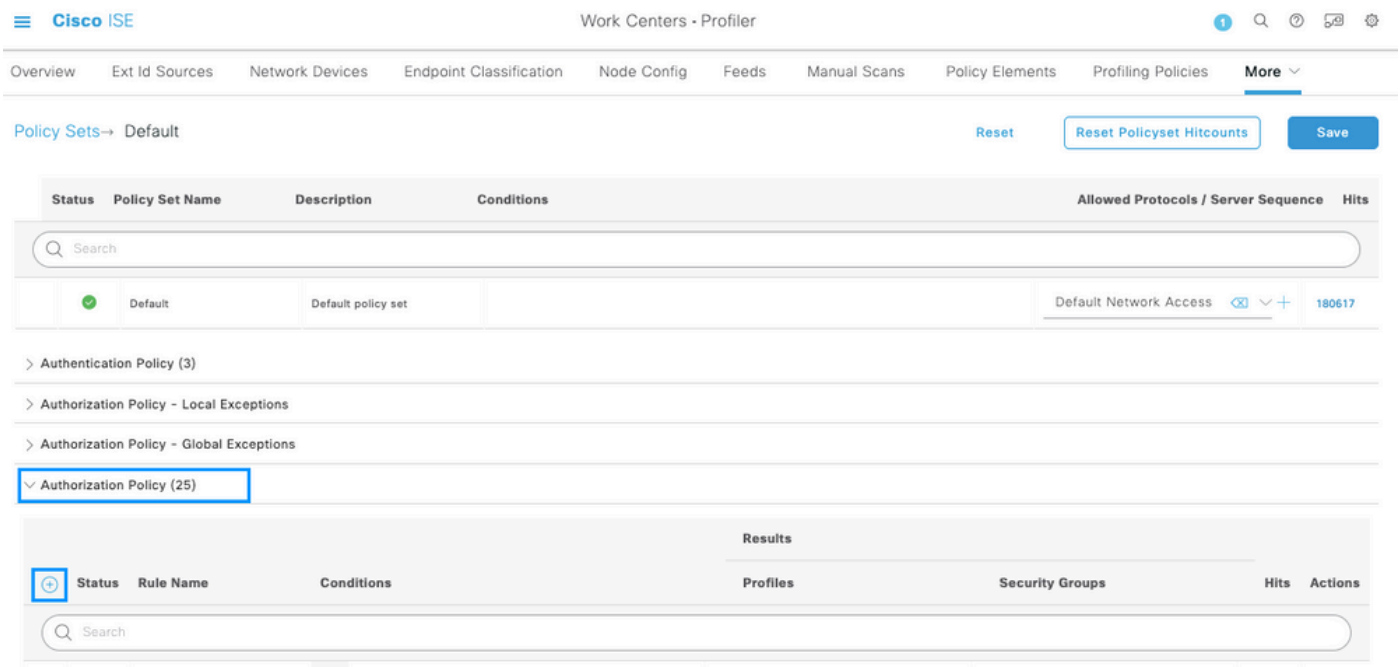
Erweitern Sie innerhalb des Standardrichtliniensatzes die Authentifizierungsrichtlinie, und erweitern Sie im Abschnitt Standard die Optionen, und stellen Sie sicher, dass sie mit der unten stehenden Konfiguration übereinstimmen.



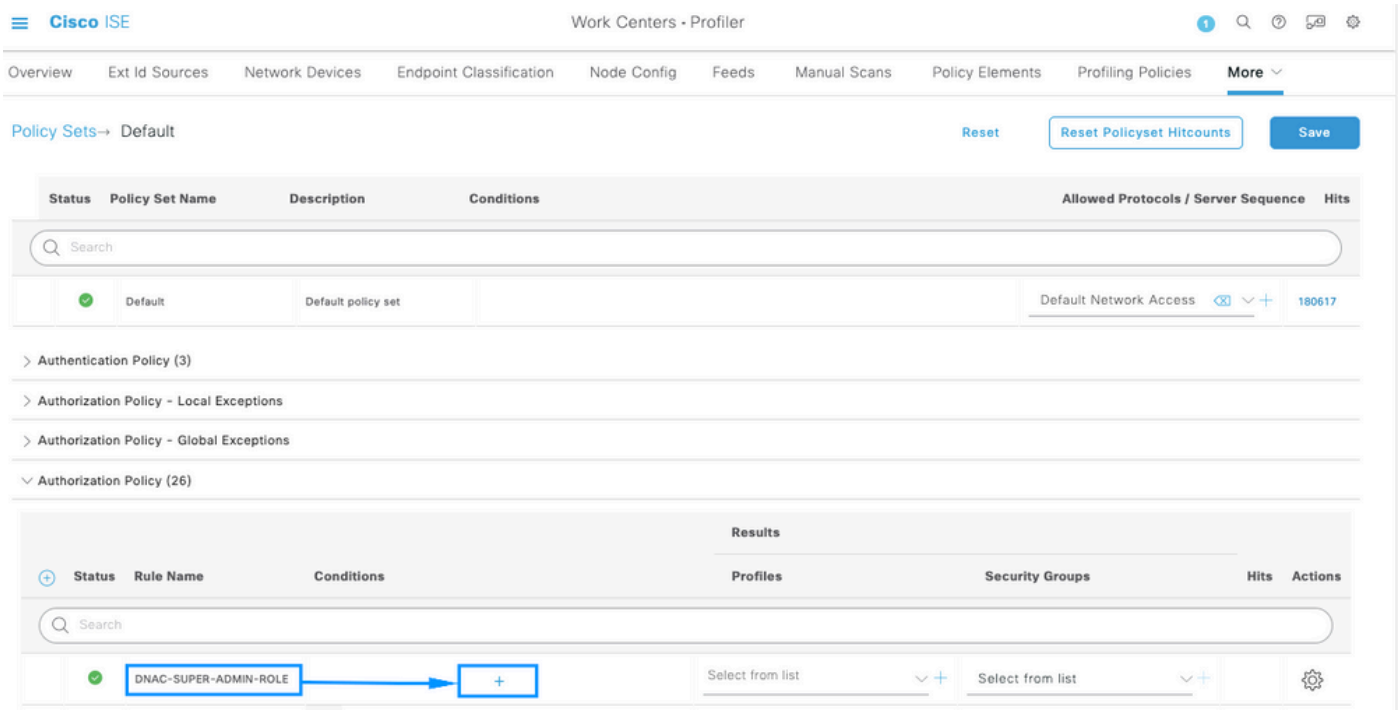


Tipp: REJECT, das für die 3 Optionen konfiguriert wurde, funktioniert auch

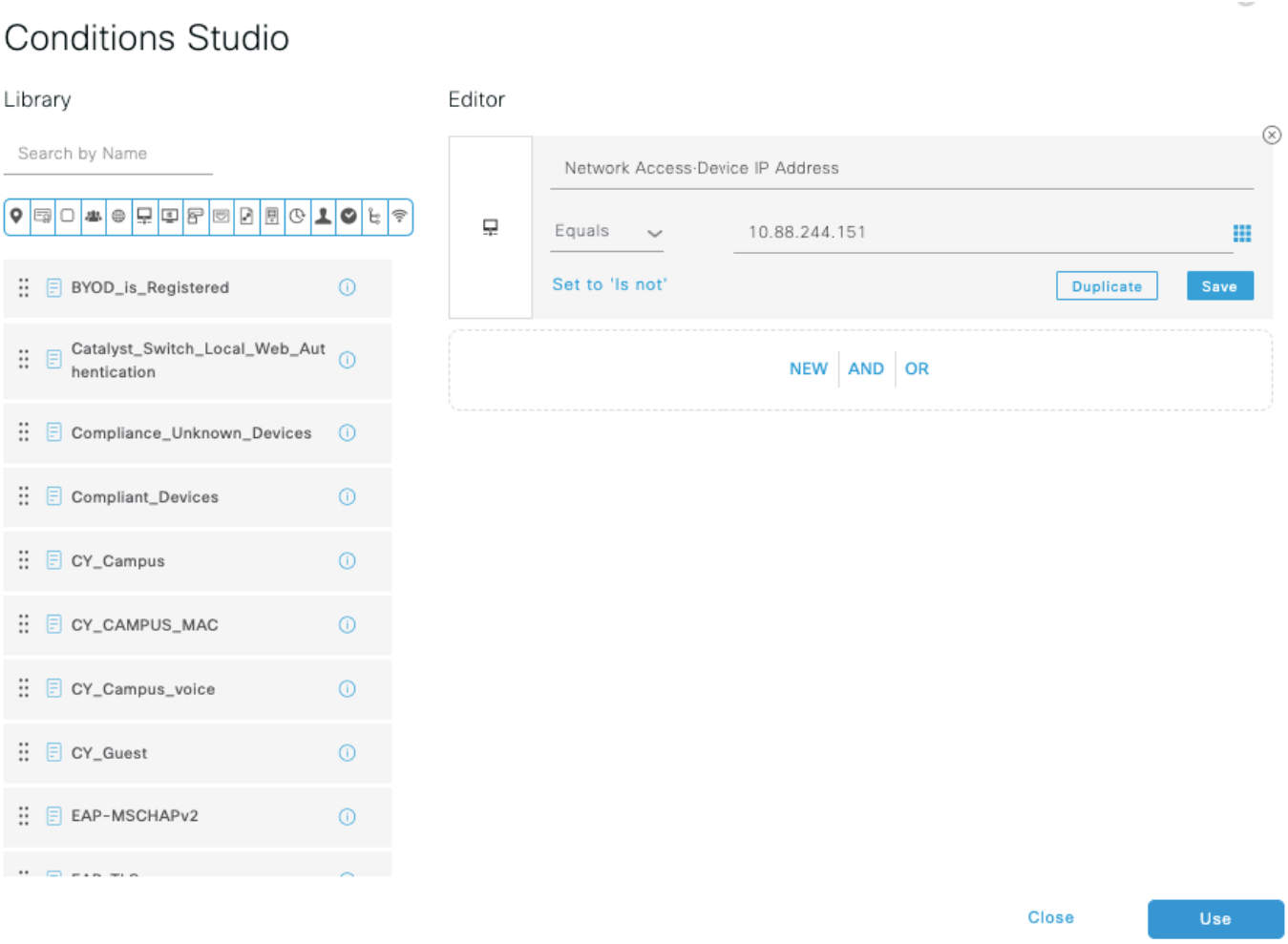
Erweitern Sie innerhalb des Standardrichtliniensatzes die Autorisierungsrichtlinie, und wählen Sie das Symbol Hinzufügen aus, um eine neue Autorisierungsbedingung zu erstellen.



Konfigurieren Sie einen Regelnamen, und klicken Sie auf das Symbol Hinzufügen, um die Bedingung zu konfigurieren.

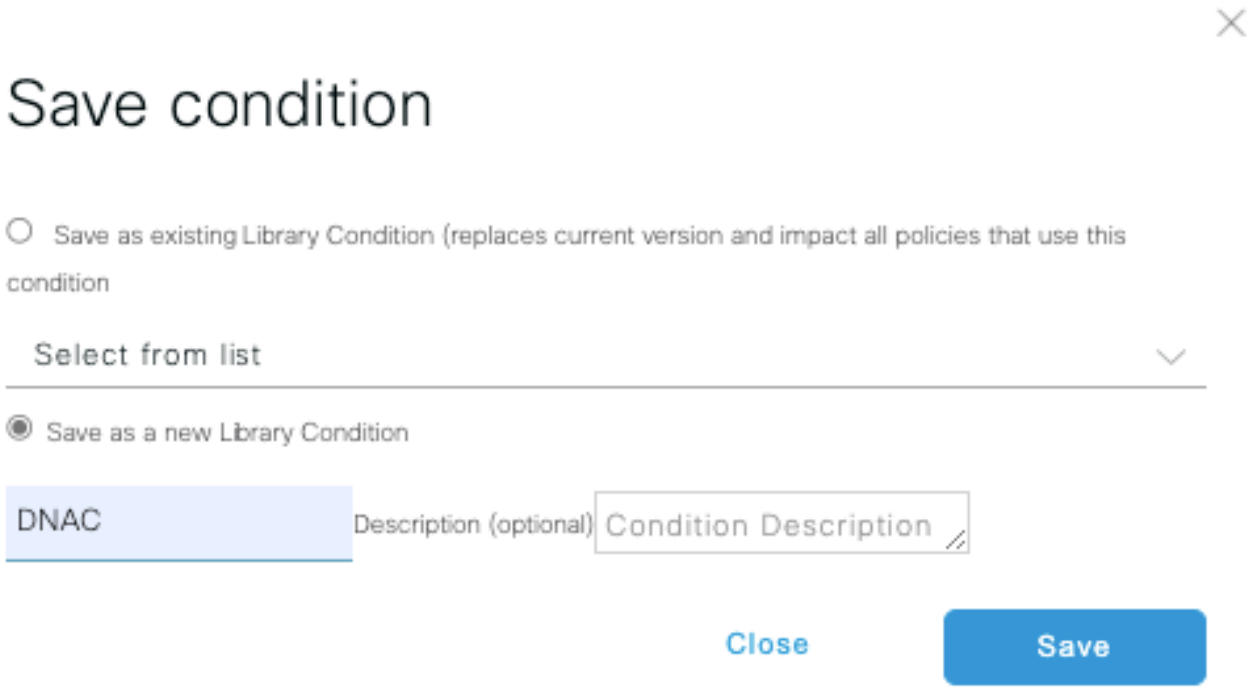


Ordnen Sie sie als Teil der Bedingung der IP-Adresse des Netzwerkgeräts zu, die in Schritt 2 konfiguriert wurde.

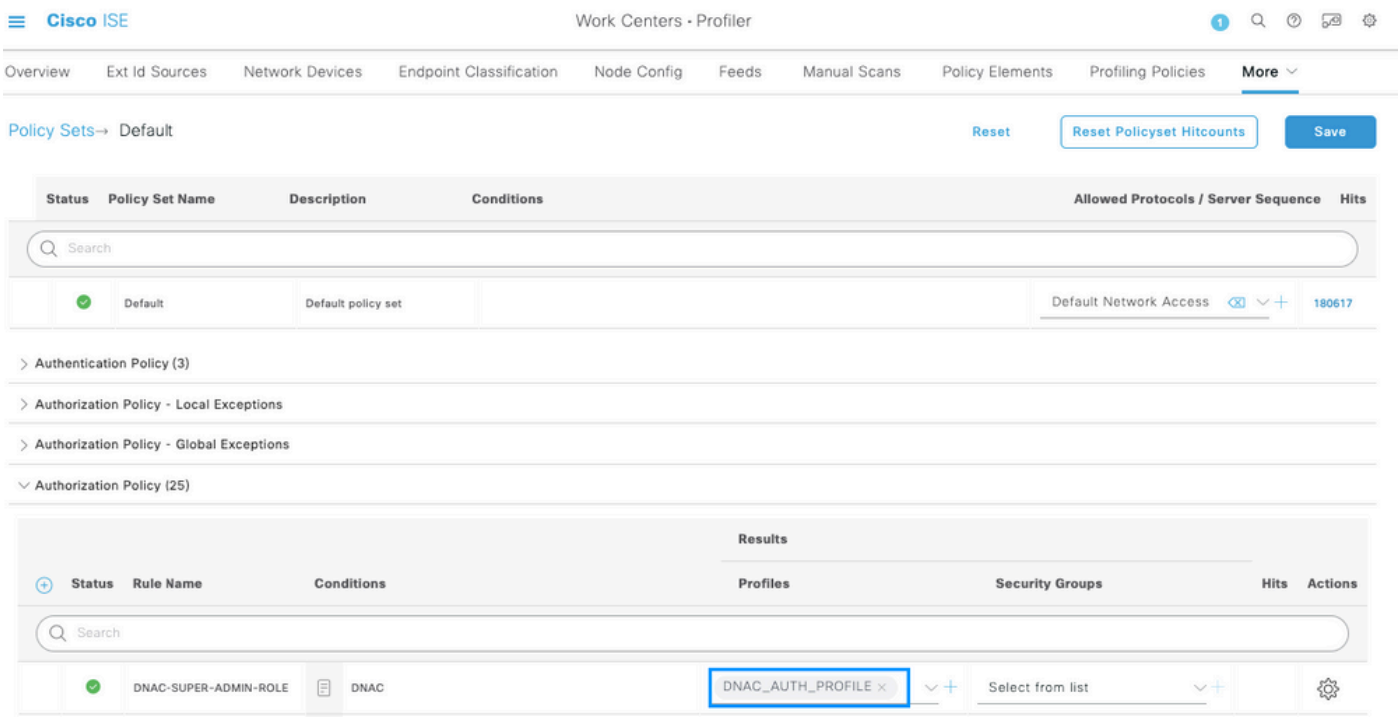


Klicken Sie auf Speichern.

Speichern Sie sie als neue Bibliotheksbedingung, und nennen Sie sie, wie Sie möchten, in diesem Fall wird sie alsDNACbenannt.



Konfigurieren Sie abschließend das in Schritt 3 erstellte Profil.

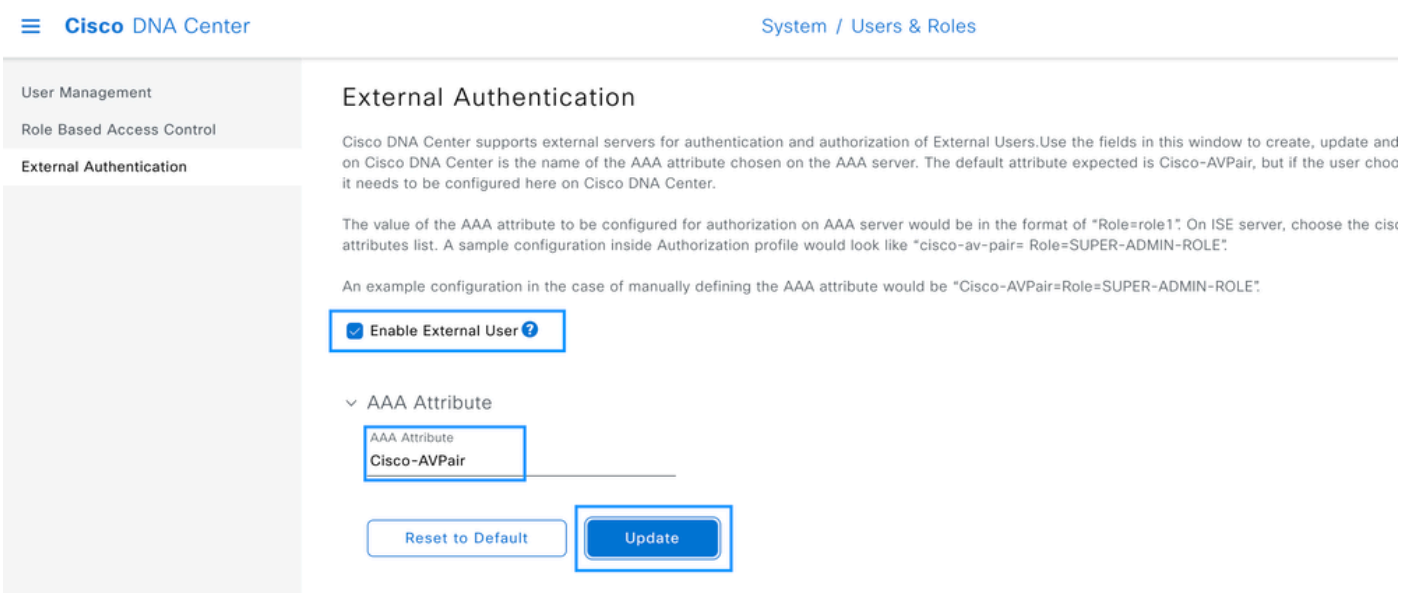


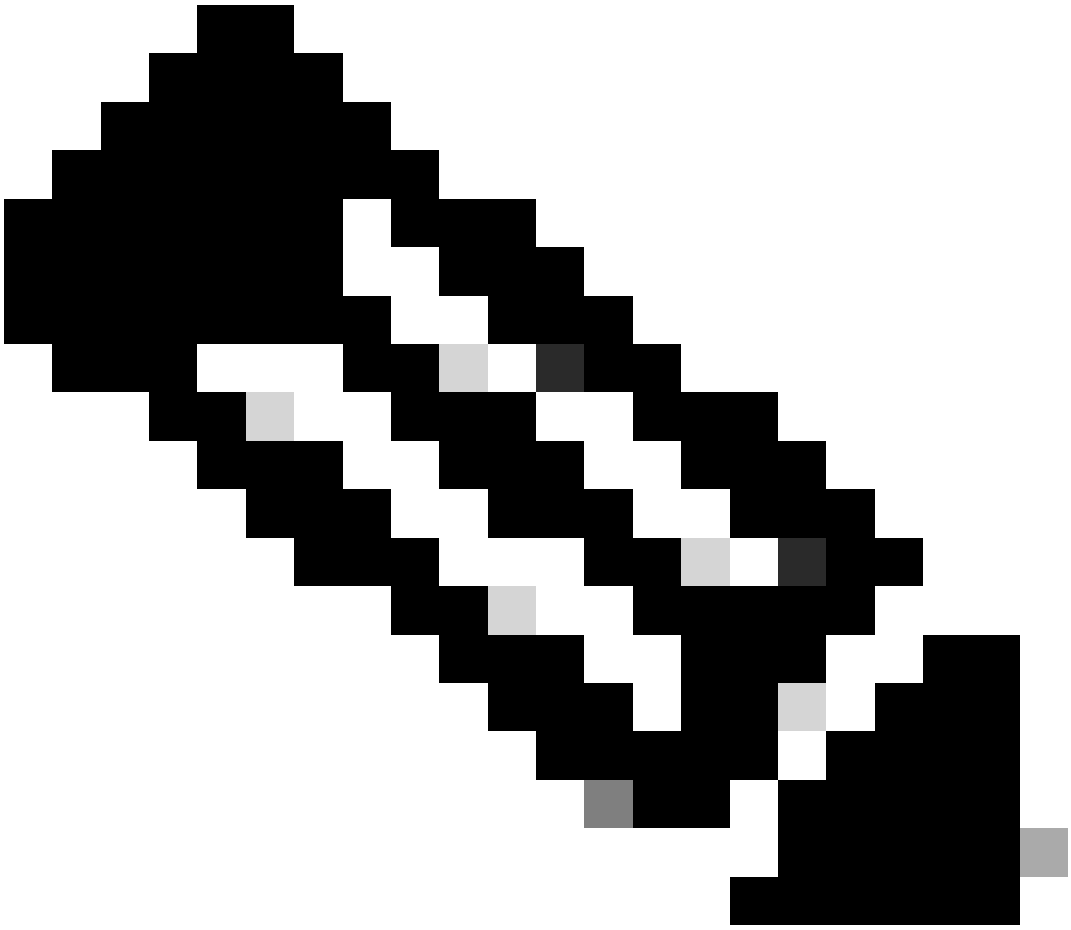
Klicken Sie auf Speichern.

Schritt 5: Melden Sie sich bei der Cisco DNA Center-GUI an, und navigieren Sie zu System > Users & Roles > External Authentication.

Klicken Sie auf die Option Externen Benutzer aktivieren, und legen Sie das AAA-Attribut als Cisco-

AVPair fest.

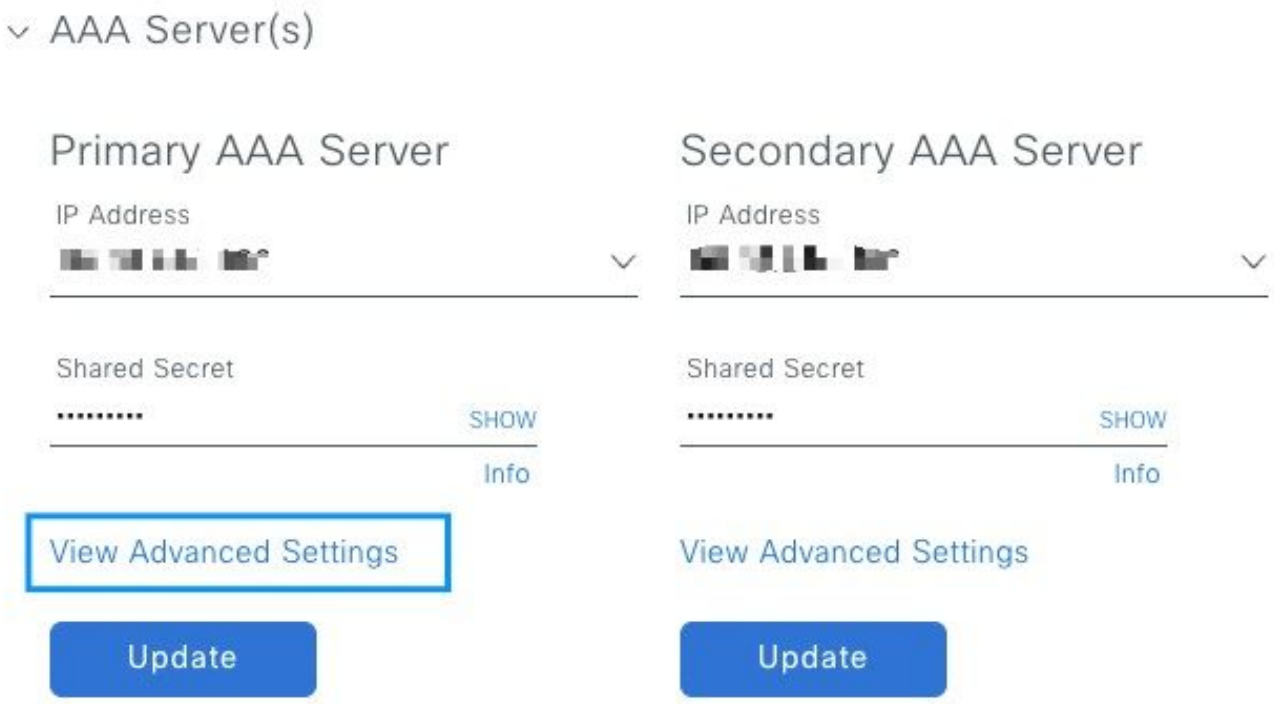

Cisco DNA Center
System / Users & Roles
User Management
Role Based Access Control
External Authentication
External Authentication
Cisco DNA Center supports external servers for authentication and authorization of External Users.Use the fields in this window to create, update and
on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choo
it needs to be configured here on Cisco DNA Center.
The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cis
attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".
An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".
Enable External User
AAA Attribute
AAA Attribute
Cisco-AVPair
Reset to Default
Update



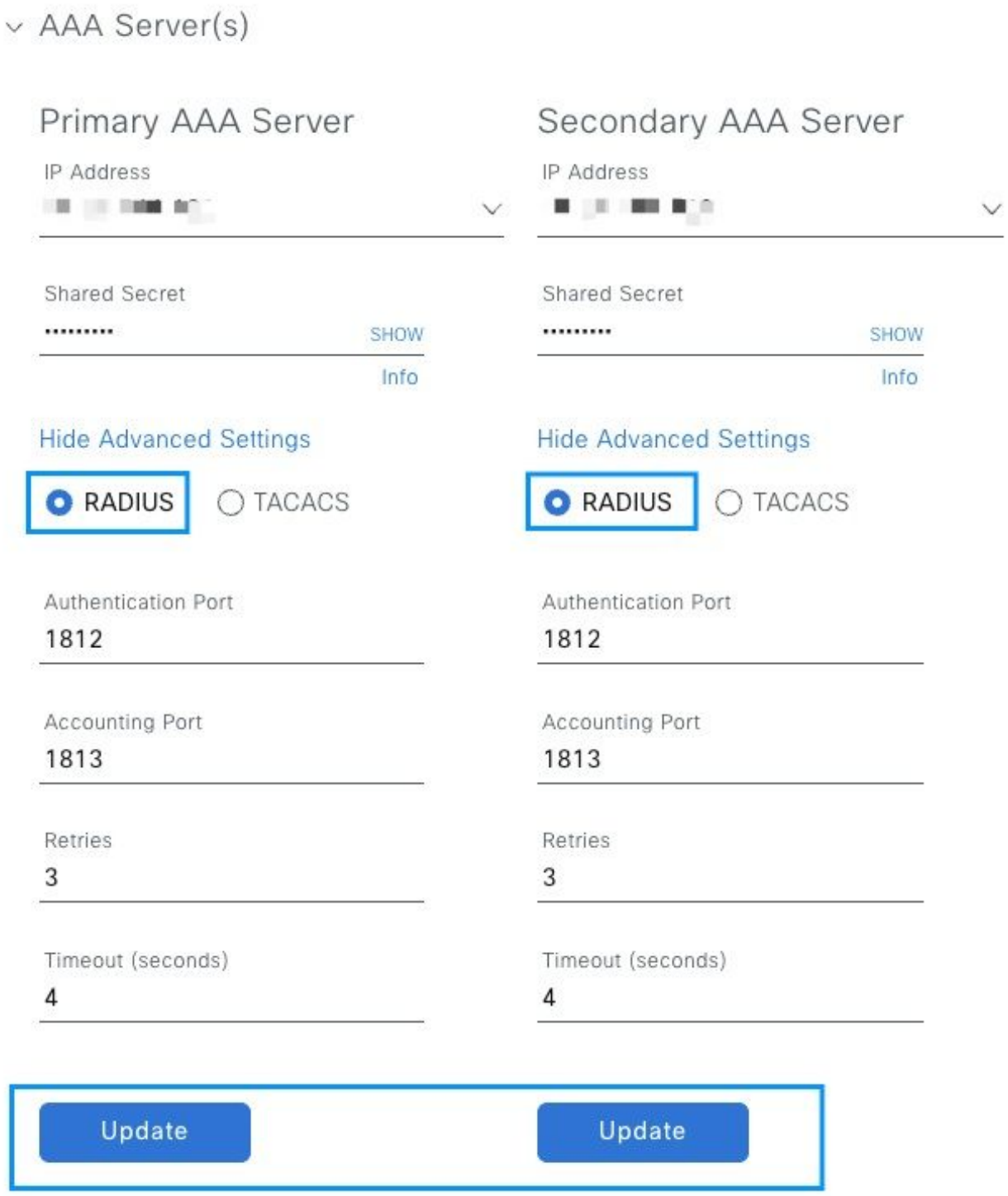
Hinweis: ISE-Server verwenden das Attribut Cisco-AVPair am Backend, sodass die Konfiguration in Schritt 3 gültig ist.

Blättern Sie nach unten, um den Konfigurationsabschnitt für AAA-Server anzuzeigen. Konfigurieren Sie die IP-Adresse des ISE-Servers in Schritt 1 und den unter Schritt 3 konfigurierten gemeinsamen geheimen Schlüssel.

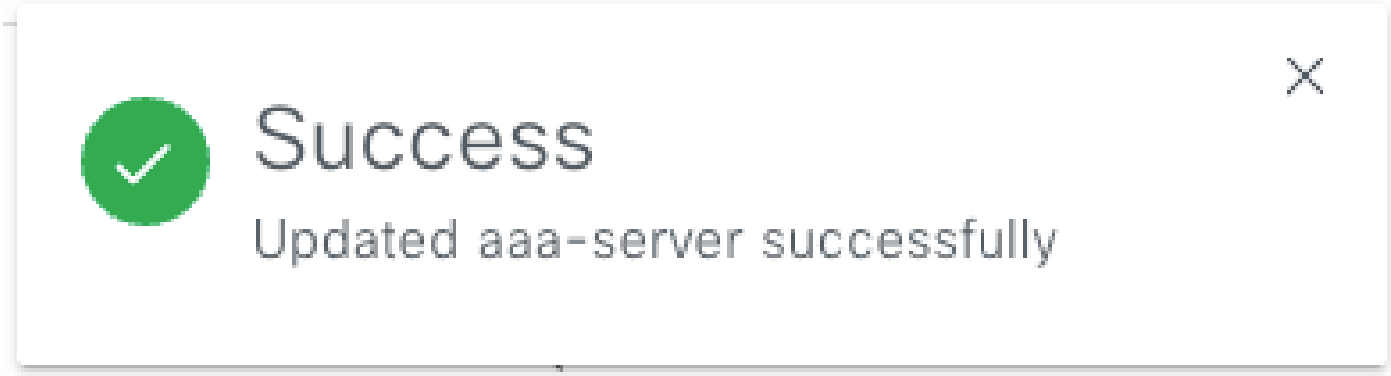
Klicken Sie dann auf Erweiterte Einstellungen anzeigen.

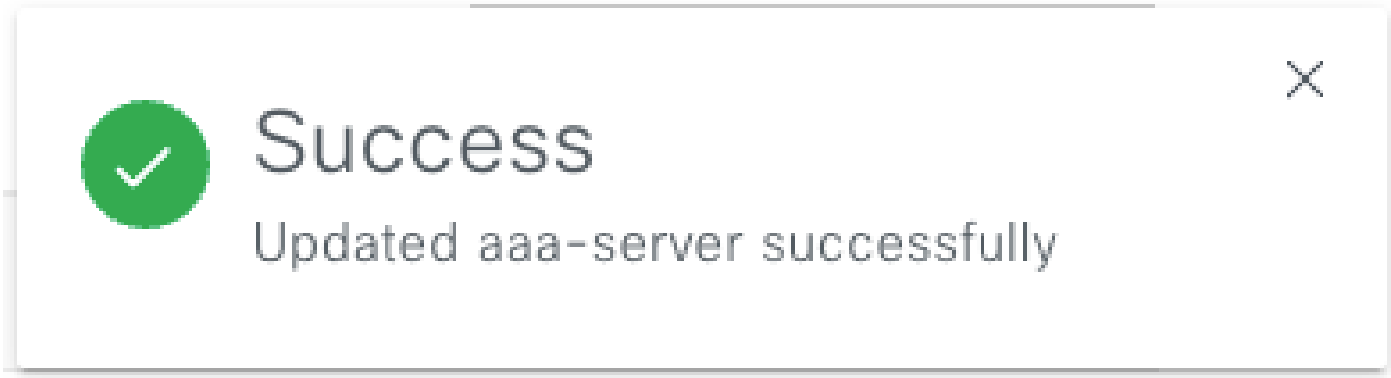


Vergewissern Sie sich, dass die RADIUS-Option aktiviert ist, und klicken Sie auf die Schaltfläche Aktualisieren auf beiden Servern.



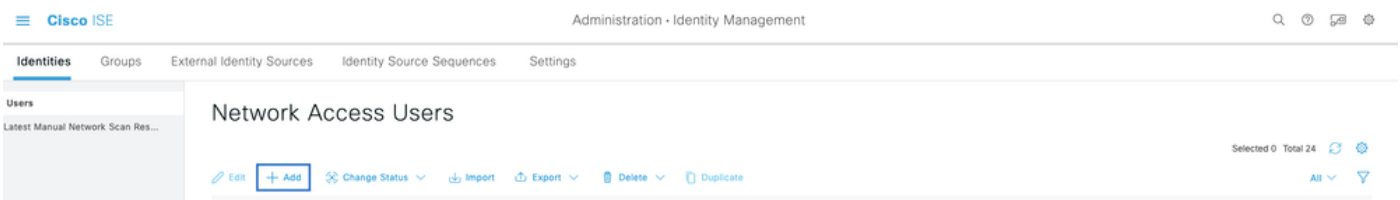
Sie müssen jeweils eine Erfolgsmeldung anzeigen.





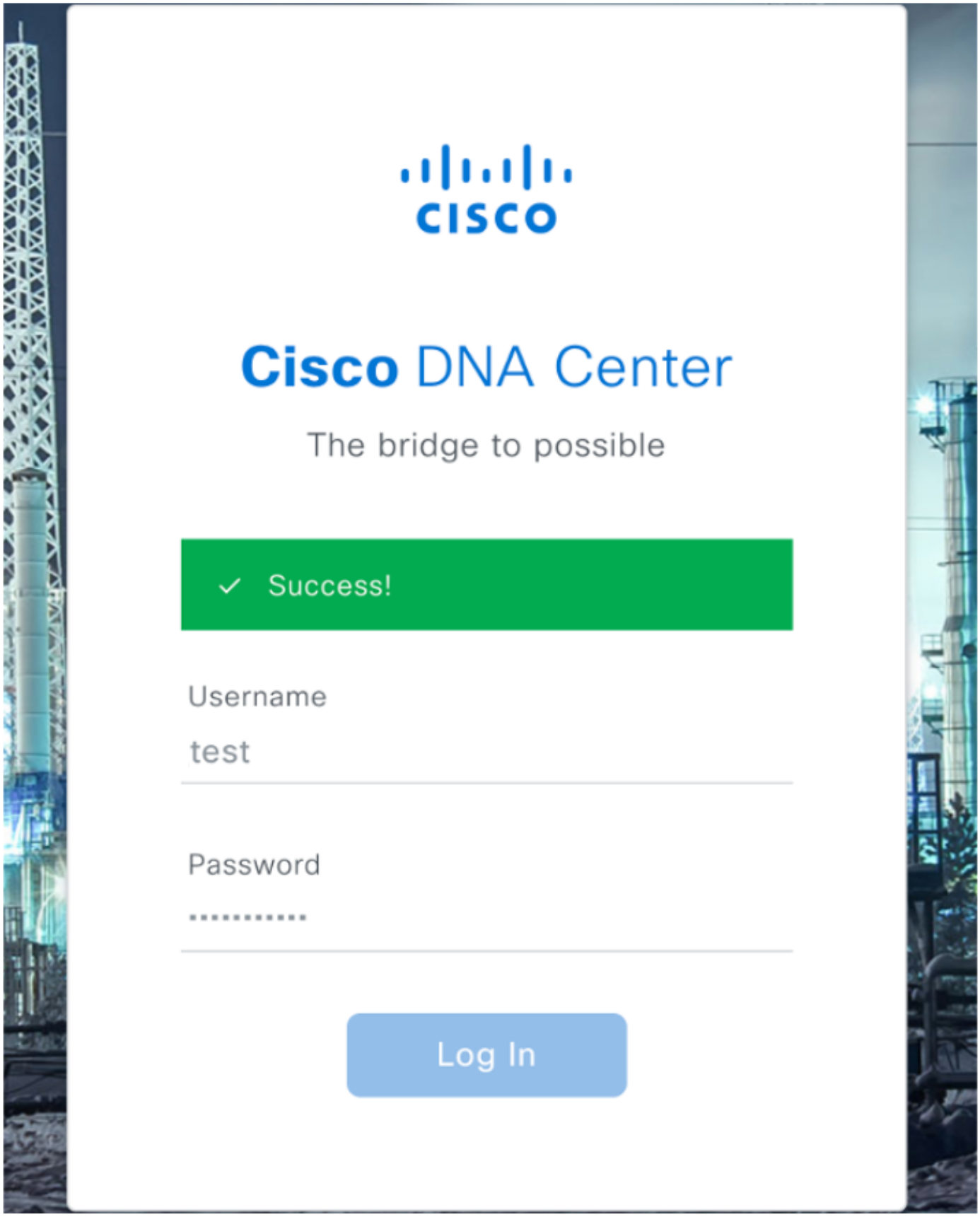
Jetzt können Sie sich mit jeder ISE-Identität anmelden, die im Menü "ISE" unter "Administration" > "Identity Management" > "Identities" > "Users" (Benutzer) erstellt wurde.

Falls Sie noch keine erstellt haben, melden Sie sich bei der ISE an, navigieren Sie zum obigen Pfad, und fügen Sie einen neuen Netzwerkzugriffsbenutzer hinzu.

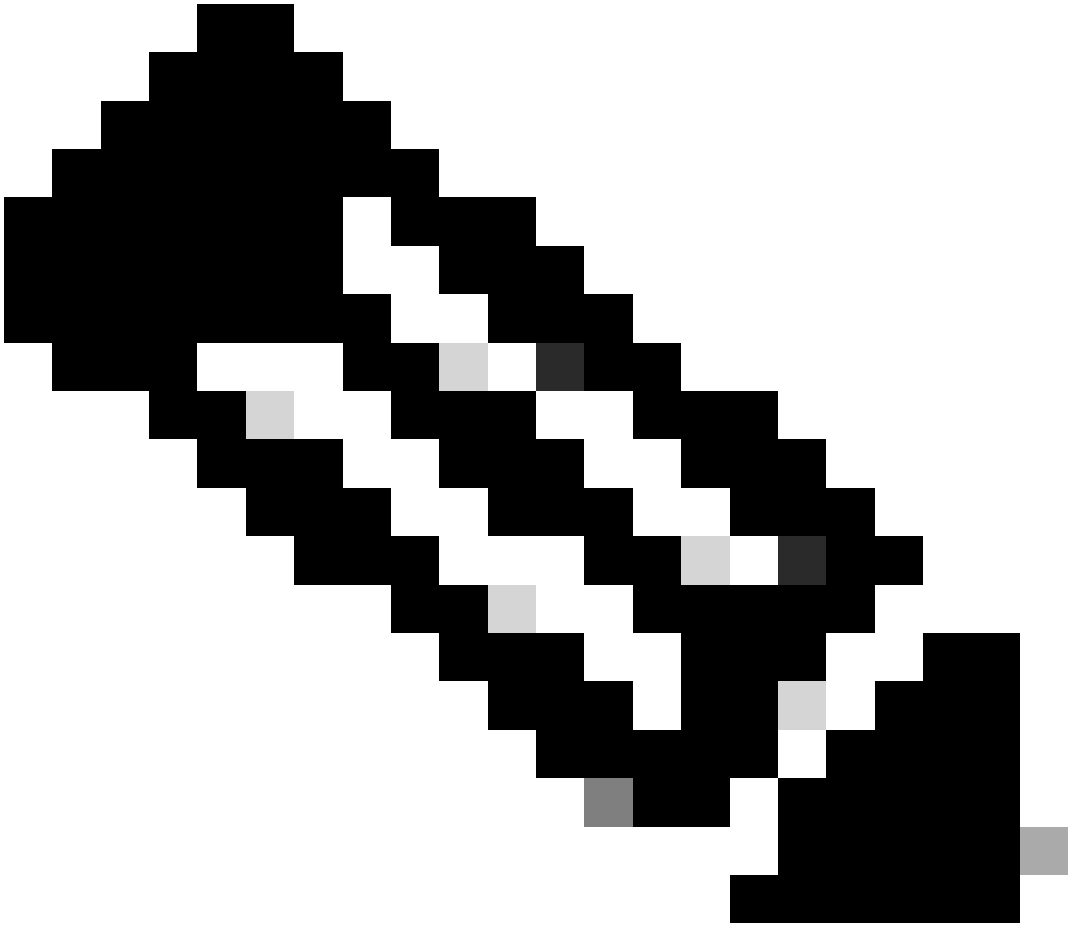


Überprüfung

Laden der Benutzeroberfläche von Cisco DNA Center und melden Sie sich mit einem Benutzer von der ISE an.

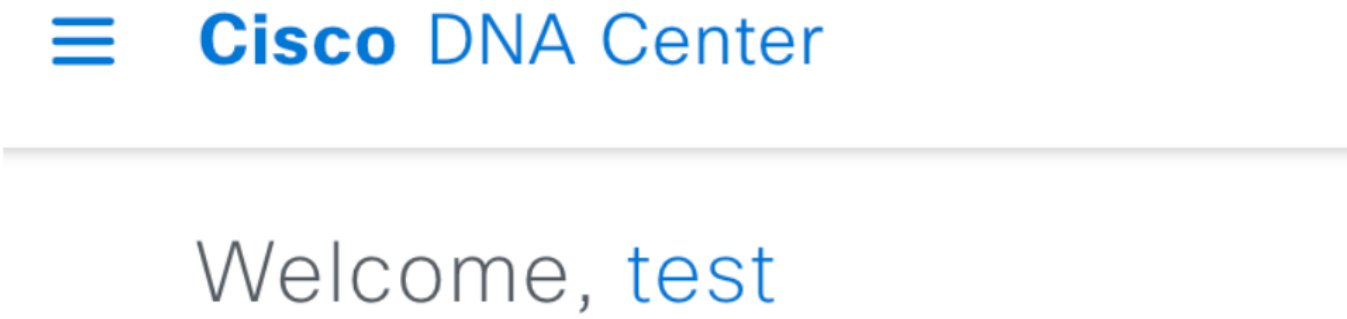


Anmeldung beim DNS-Center



Hinweis: Jeder Benutzer mit ISE-ID kann sich jetzt anmelden. Sie können die Authentifizierungsregeln auf dem ISE-Server detaillierter gestalten.

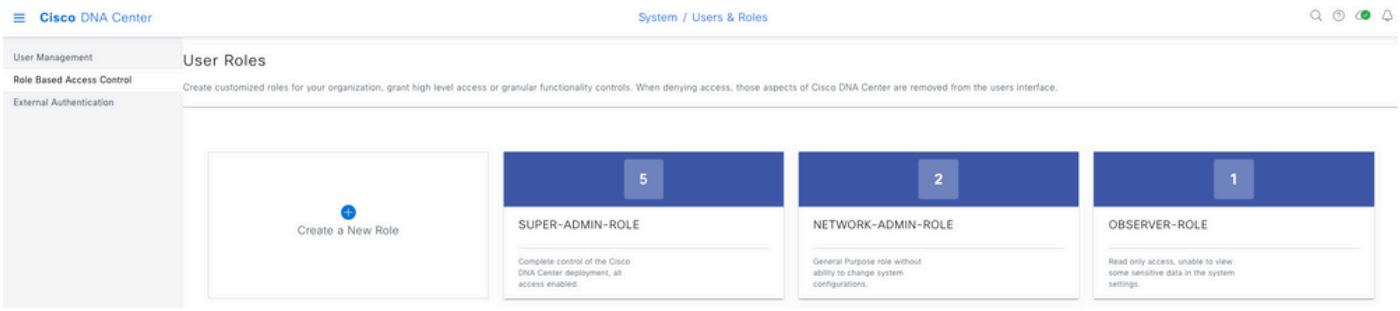
Nach erfolgreicher Anmeldung wird der Benutzername in der Cisco DNA Center-GUI angezeigt.



Willkommensseite

Weitere Rollen

Sie können diese Schritte für jede Funktion im Cisco DNA Center wiederholen. Standardmäßig haben wir folgende Funktionen: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE und OBSERVER-ROLE.



In diesem Dokument wird das Rollenbeispiel SUPER-ADMIN-ROLE verwendet. Sie können jedoch für jede Rolle in Cisco DNA Center ein Autorisierungsprofil auf der ISE konfigurieren. Die einzige Überlegung hierbei ist, dass die in Schritt 3 konfigurierte Rolle genau (unter Berücksichtigung der Groß-/Kleinschreibung) mit dem Rollennamen in Cisco DNA Center übereinstimmen muss.

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.