Konfigurieren der RADIUS-basierten Administratoranmeldung bei einem Arista-Switch

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Cisco Identity Services Engine (ISE) konfiguriert wird, um Administratoranmeldungen bei Arista-Switches mithilfe von RADIUS zu authentifizieren.

Voraussetzungen

Anforderungen

Bevor Sie fortfahren, stellen Sie sicher, dass

- Die Cisco ISE (Version 3.x empfohlen) ist installiert und betriebsbereit.
- Arista-Switch mit EOS und RADIUS-Unterstützung
- Active Directory (AD) oder interne Benutzerdatenbank in ISE konfiguriert.

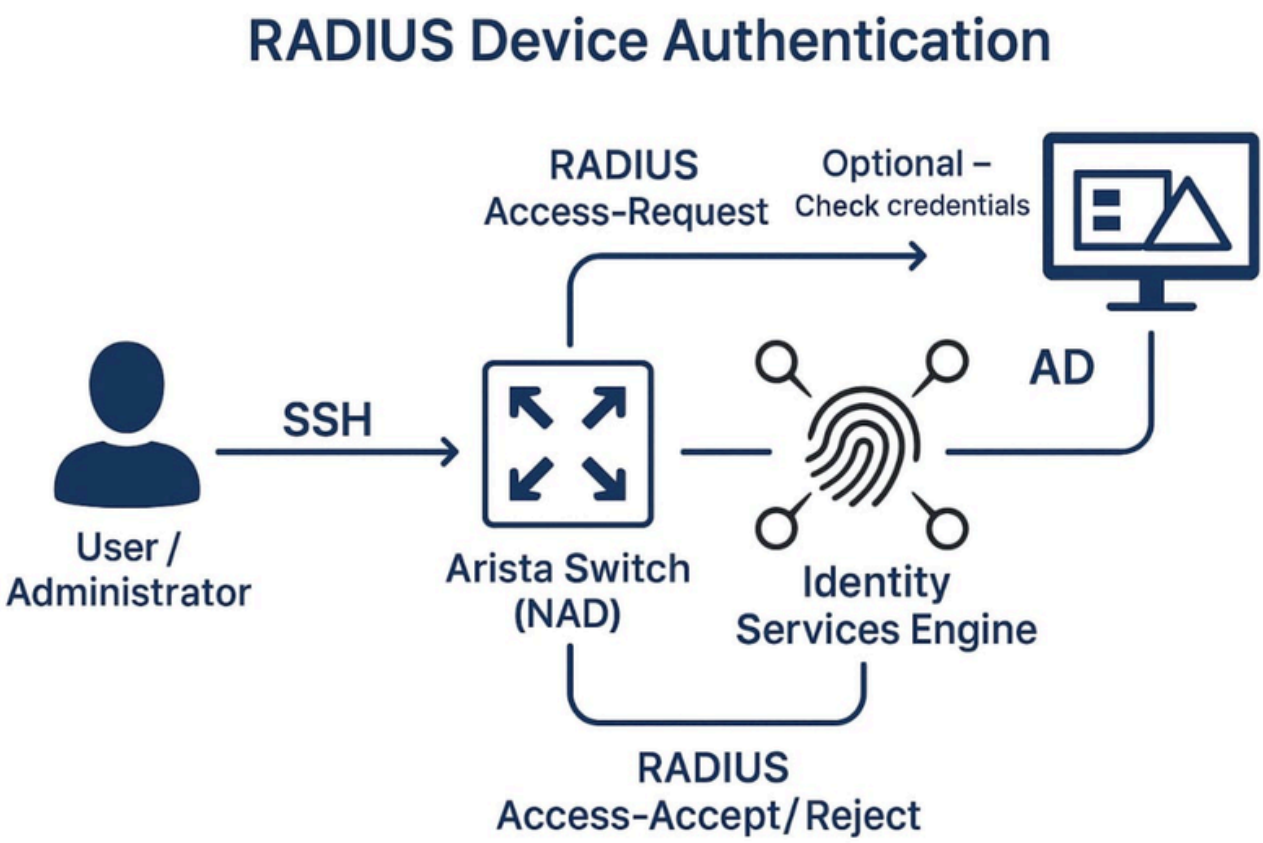
Verwendete Komponenten

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

- Arista Switch Software-Image-Version: 4,33,2 F
- Cisco Identity Services Engine (ISE) Version 3.3 Patch 4

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.

Netzwerkdiagramm



Das folgende Netzwerkdiagramm zeigt die RADIUS-basierte Geräteauthentifizierung für einen

Arista-Switch mit Cisco ISE und Active Directory (AD) als optionale Authentifizierungsquelle.

Das Diagramm enthält:

- Arista Switch (als Netzwerkzugriffsgerät, NAD)
- Cisco ISE (als RADIUS-Server)
- Active Directory (AD) [Optional] (zur Identitätsüberprüfung verwendet)
- Benutzer/Administrator (der sich über SSH anmeldet)

Konfigurieren

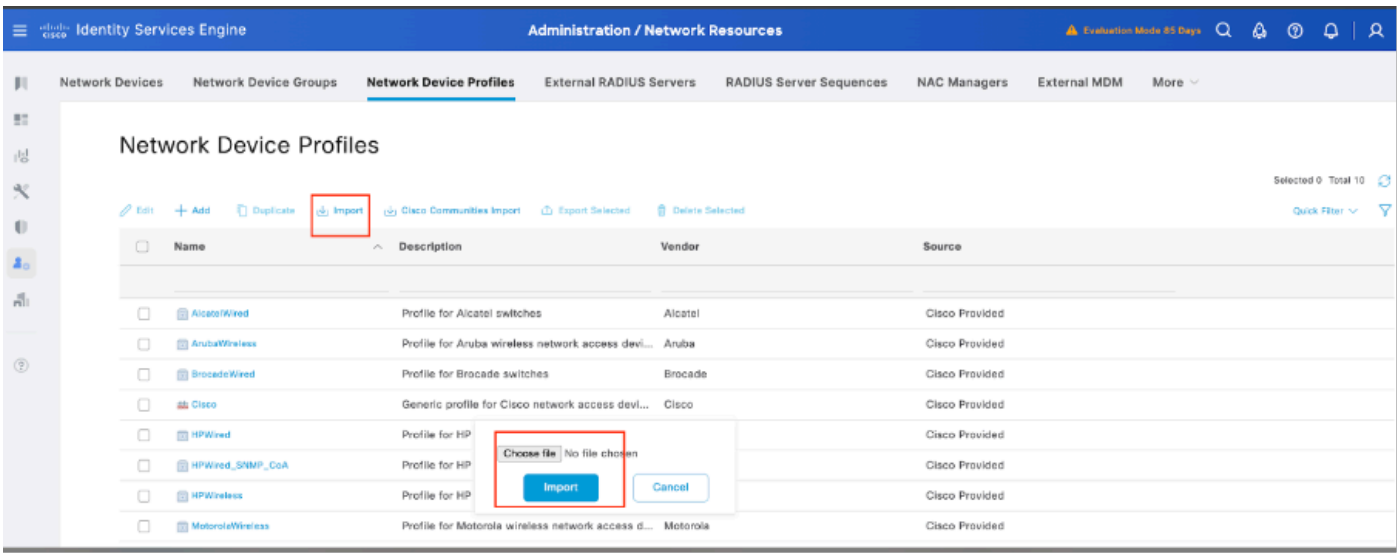
Konfigurieren der Cisco ISE

Schritt 1: Abruf des Arista-Netzwerkgeräteprofils für die Cisco ISE

Die Cisco Community hat ein dediziertes NAD-Profil für Arista-Geräte freigegeben. Dieses Profil, zusammen mit den erforderlichen Wörterbuchdateien, finden Sie im Artikel Arista CloudVision WiFi Dictionary und NAD Profile for ISE Integration. Das Herunterladen und Importieren dieses Profils in Ihre ISE-Konfiguration vereinfacht die Integration

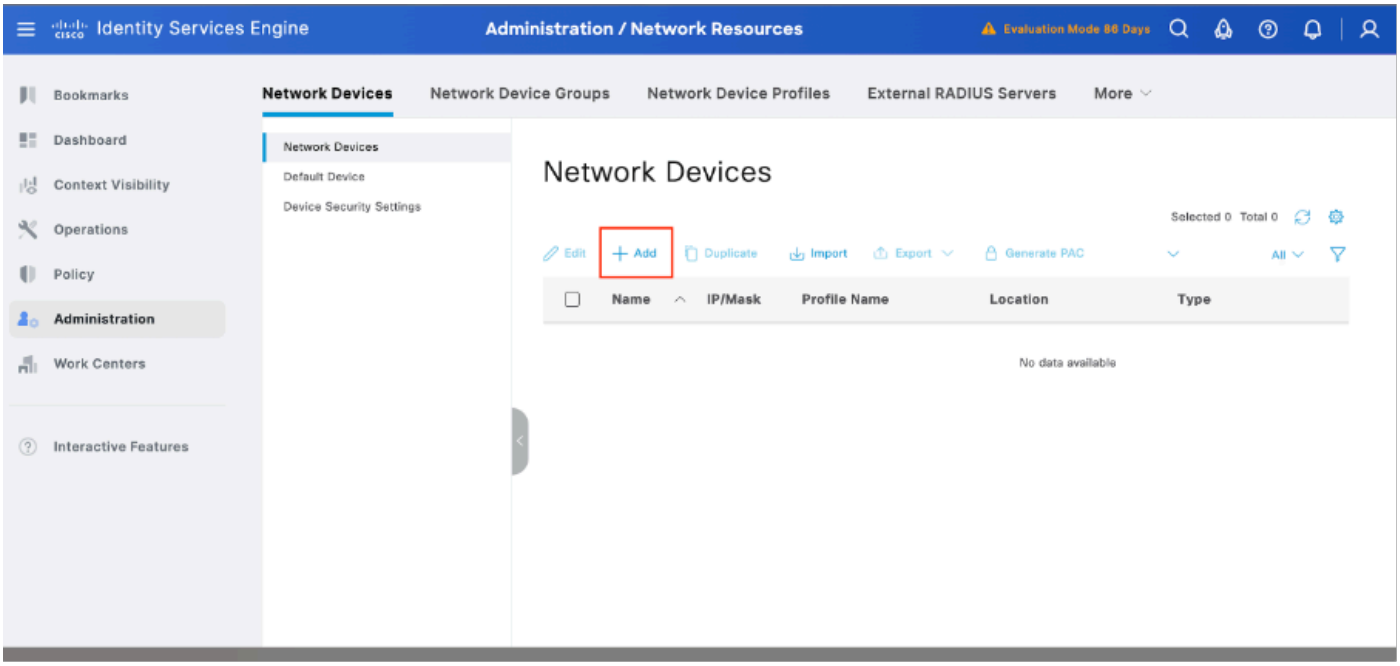
So importieren Sie das Arista NAD-Profil in die Cisco ISE:

1. Profil herunterladen:
    - Rufen Sie das Arista NAD-Profil über den oben angegebenen Link zur Cisco Community Cisco Community.
2. Zugriff auf die Cisco ISE:
    - Melden Sie sich bei Ihrer Cisco ISE-Verwaltungskonsole an
3. NAD-Profil importieren:
    - Navigieren Sie zu Administration > Network Resources > Network Device Profiles..
    - Klicken Sie auf die Schaltfläche Importieren
    - Laden Sie die heruntergeladene Arista NAD-Profildatei hoch.



Schritt 2: Hinzufügen eines Arista-Switches als Netzwerkgerät

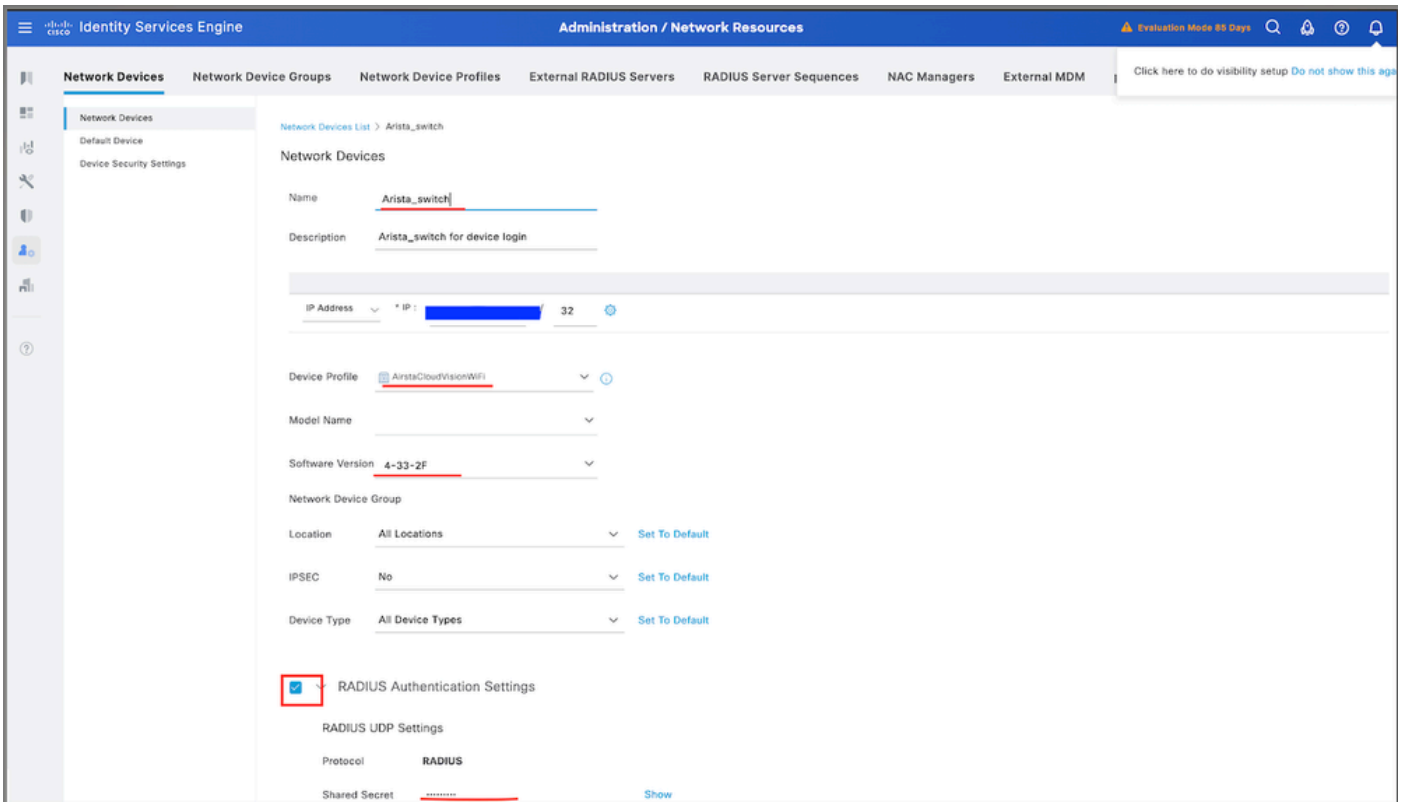
1. Navigieren Sie zu Administration > Network Resources > Network Devices > +Add.



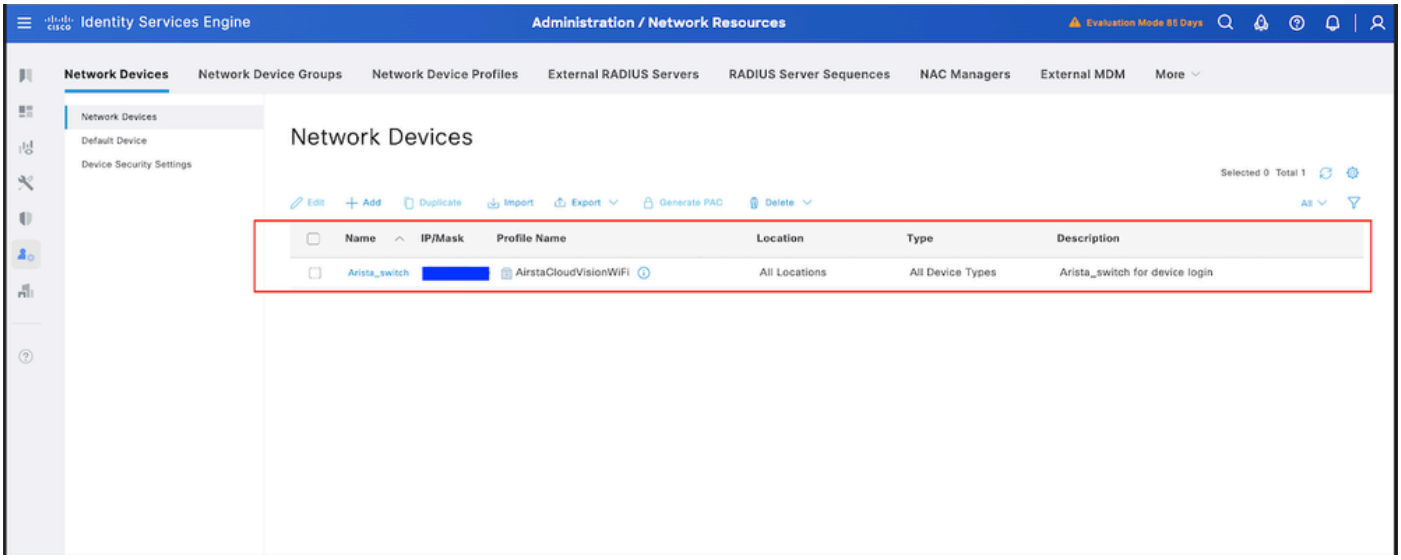
2. Klicken Sie auf Hinzufügen, und geben Sie folgende Details ein:

1. Name: Arista-Switch
2. IP-Adresse: <Switch-IP>
3. Gerätetyp: Andere verkabelte auswählen
4. Netzwerkgeräteprofil: Wählen Sie AirstaCloudVisionWiFi aus.
5. RADIUS-Authentifizierungseinstellungen:
    1. RADIUS-Authentifizierung aktivieren
    2. Geben Sie den gemeinsamen geheimen Schlüssel ein (muss mit der Switch-Konfiguration übereinstimmen).

3. Klicken Sie auf Speichern.

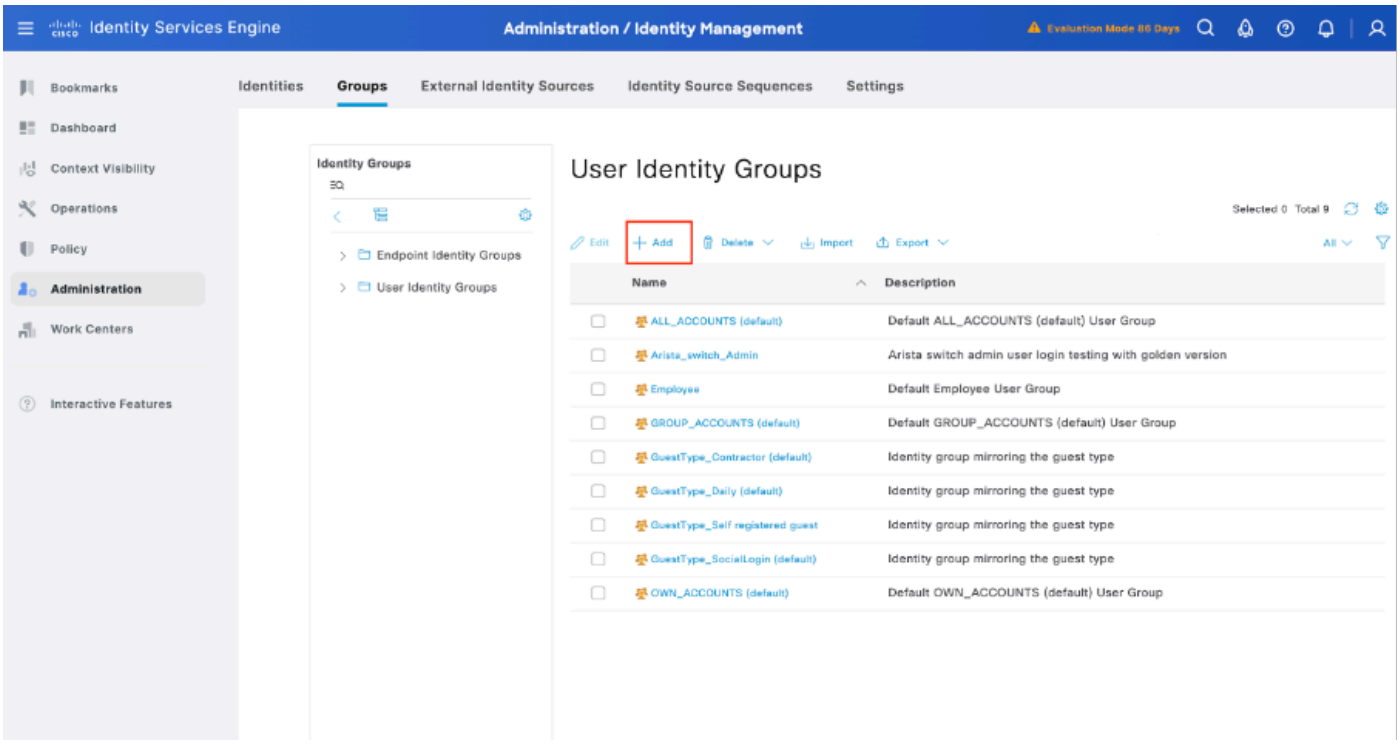


Schritt 3: Überprüfen, ob das neue Gerät unter "Netzwerkgeräte" angezeigt wird



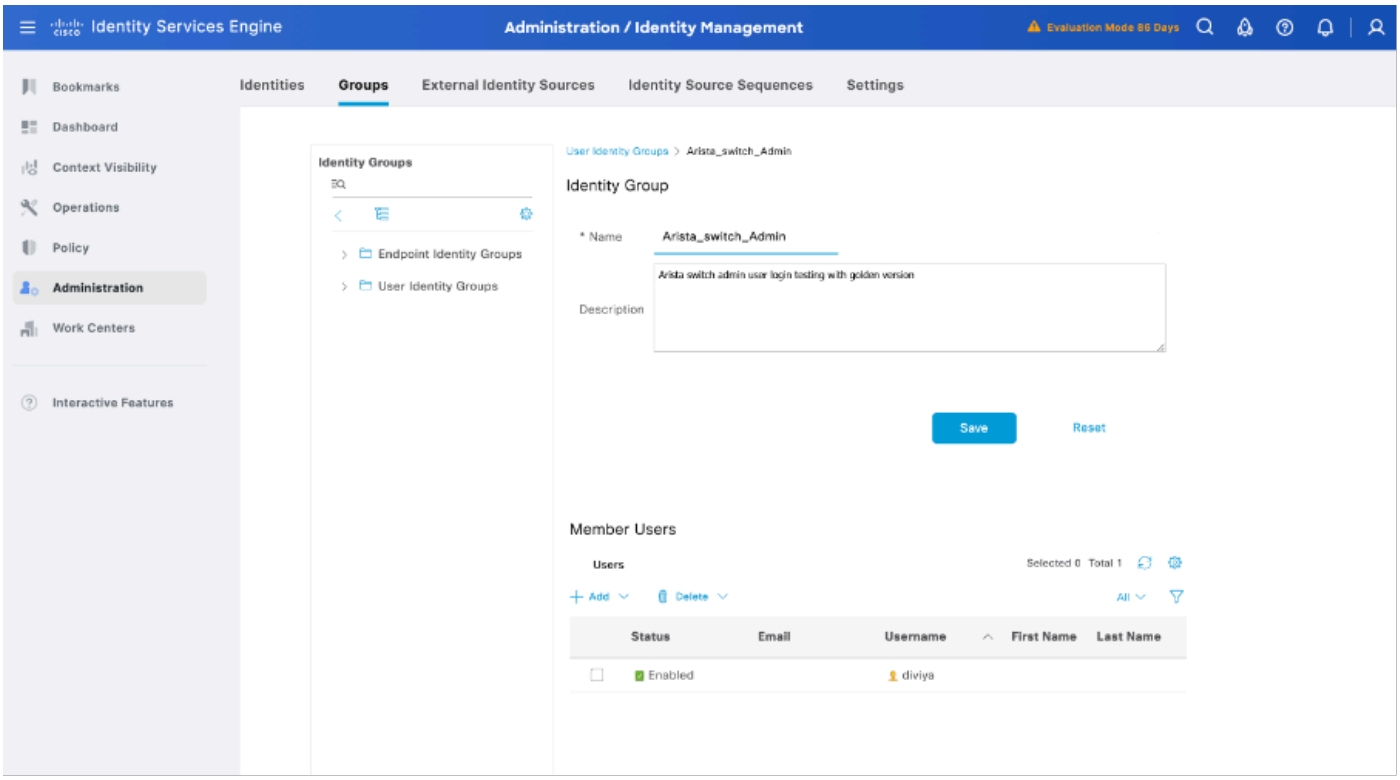
Schritt 4: Erstellen der erforderlichen Benutzeridentitätsgruppen

Navigieren Sie zu Administration > Identity Management > Groups > User Identity Groups > + Add:



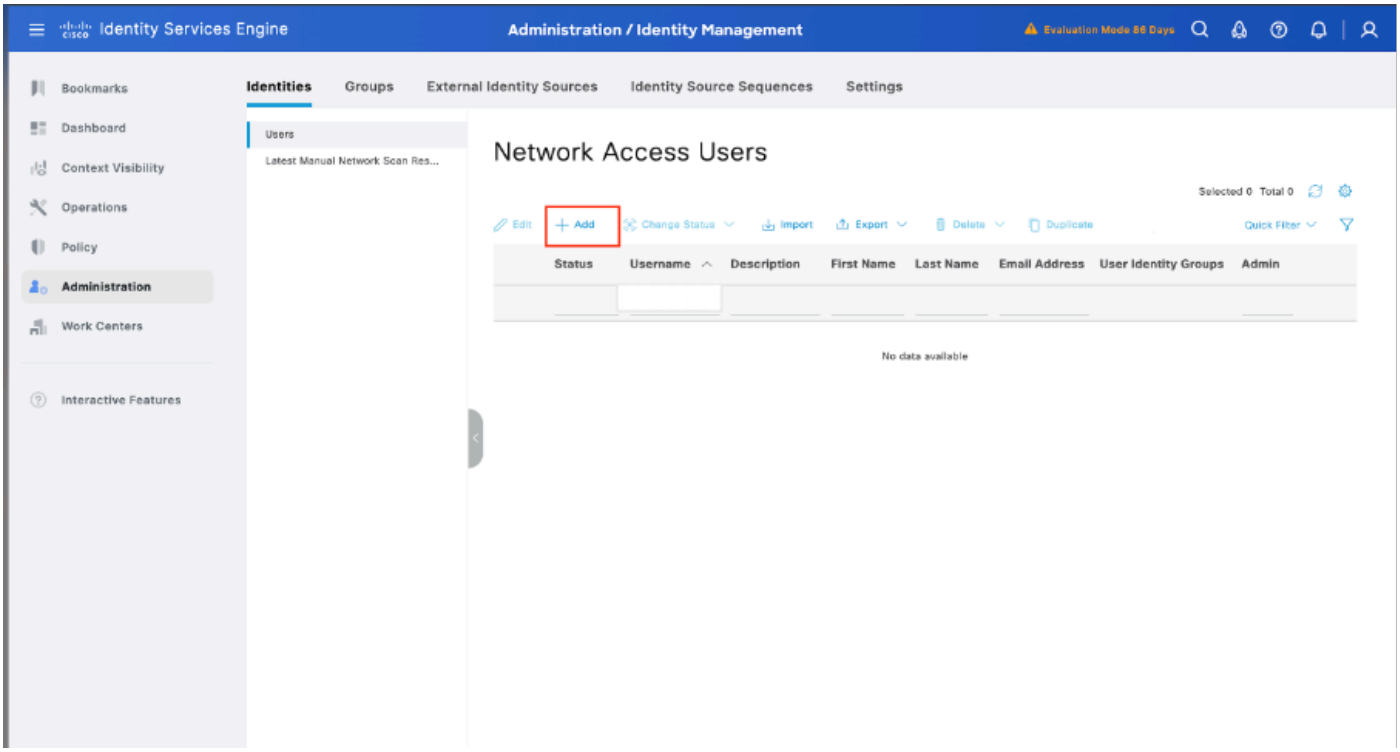
Schritt 5: Legen Sie einen Namen für die Benutzeridentitätsgruppe des Administrators fest.

Klicken Sie auf Senden, um die Konfiguration zu speichern:

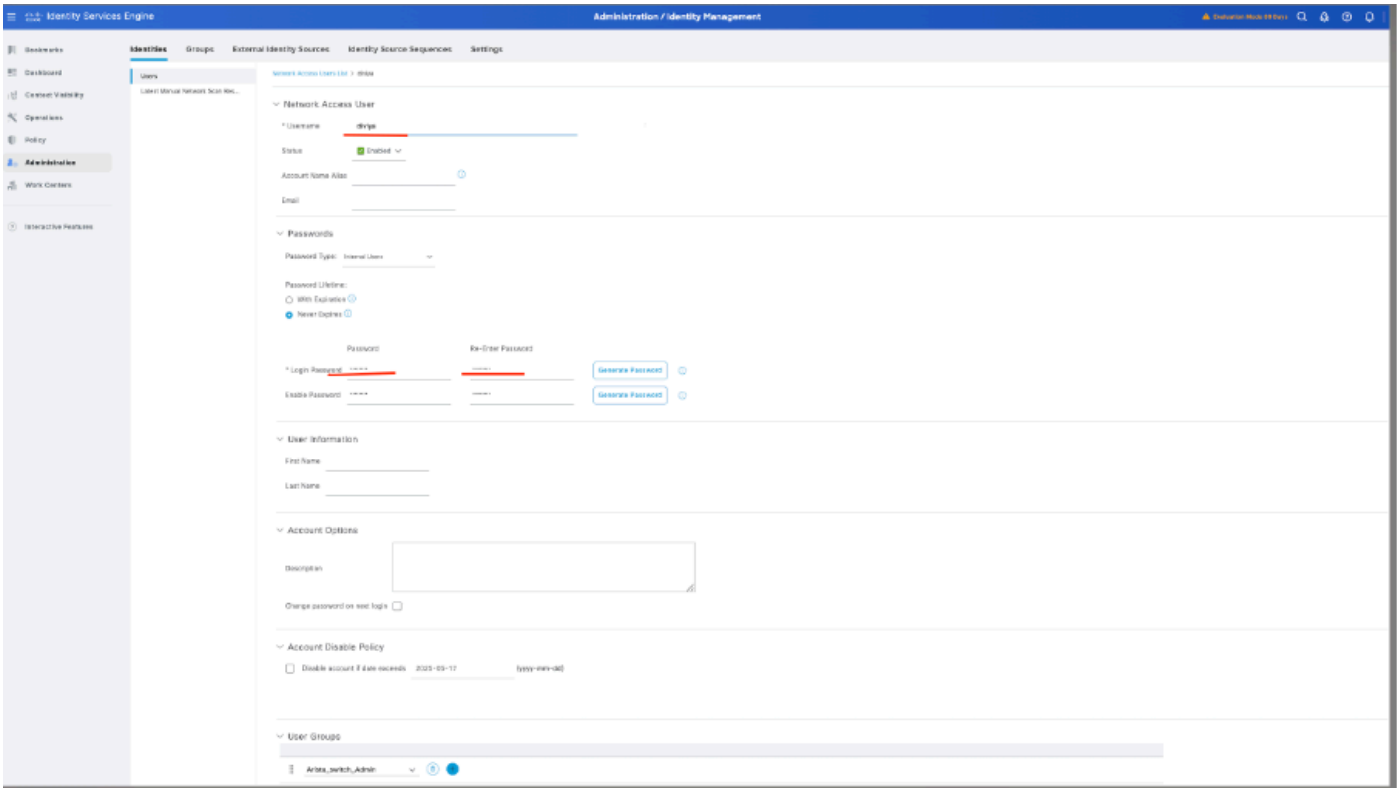


Schritt 6: Lokale Benutzer erstellen und sie ihrer Korrespondenzgruppe hinzufügen

Navigieren Sie zu Administration > Identity Management > Identities > + Add:



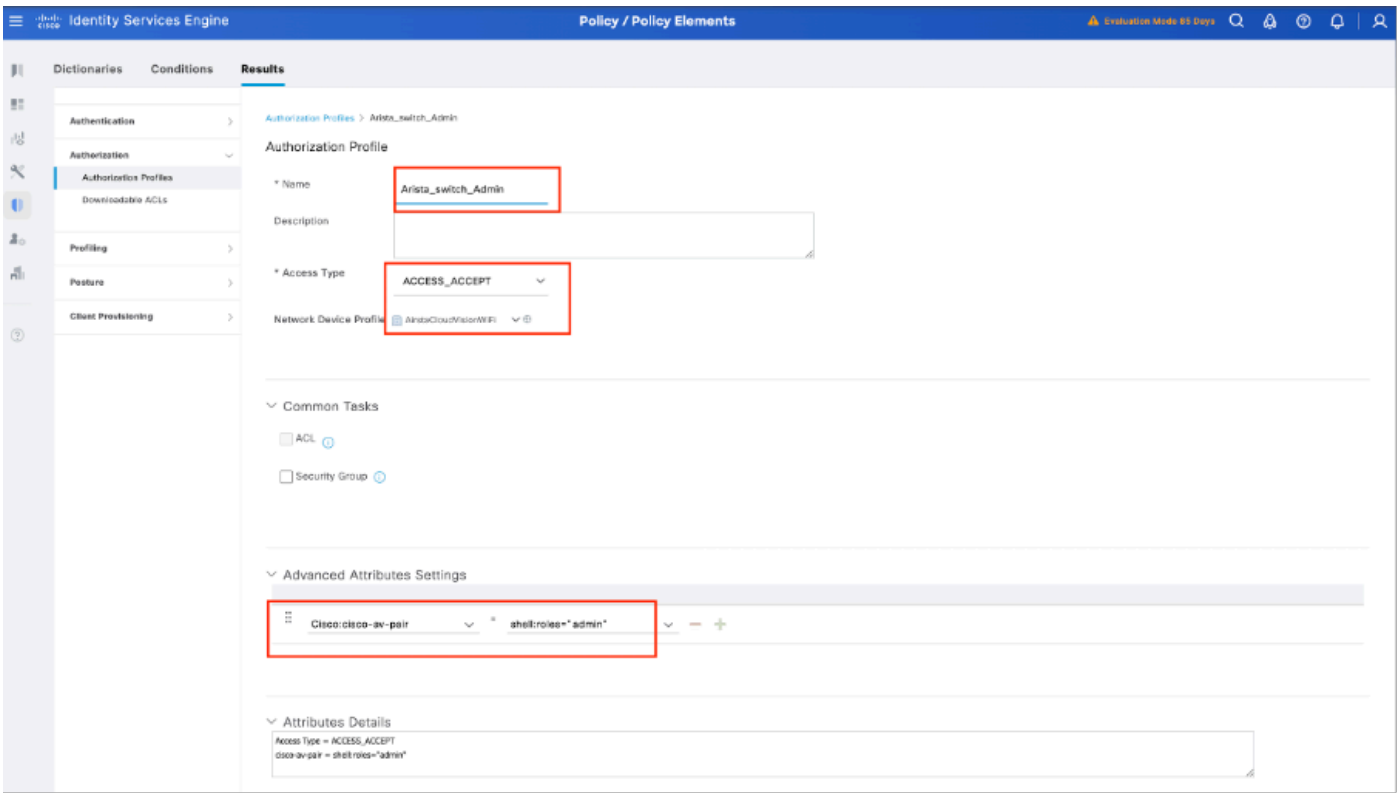
6.1. Fügen Sie den Benutzer mit Administratorrechten hinzu. Legen Sie einen Namen und ein Kennwort fest, und weisen Sie sie Arista_switch_Admin zu. Scrollen Sie nach unten, und klicken Sie auf Submit (Senden), um die Änderungen zu speichern.



Schritt 7. Erstellen des Autorisierungsprofils für den Administrator-Benutzer

Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > +Hinzufügen.

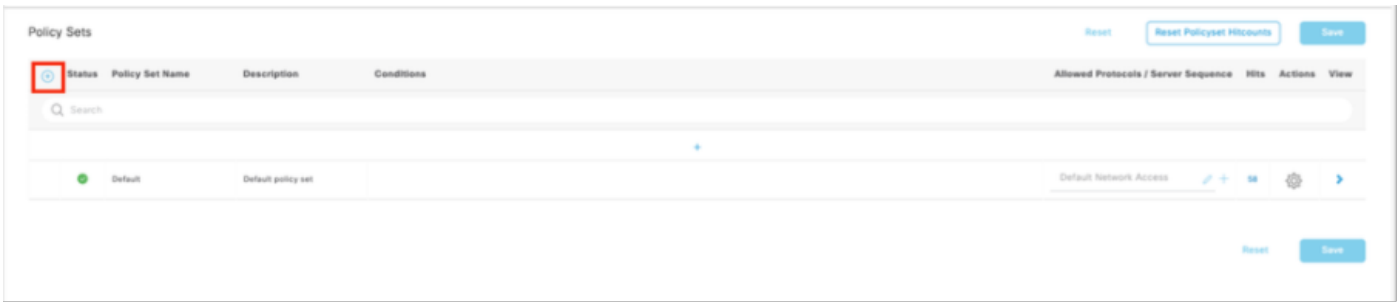
Definieren Sie einen Namen für das Autorisierungsprofil, belassen Sie den Zugriffstyp ACCESS_ACCEPT, und fügen Sie unter Erweiterte Attributeinstellungen cisco-av-pair=shell:roles="admin" mit hinzu, und klicken Sie auf "Senden".



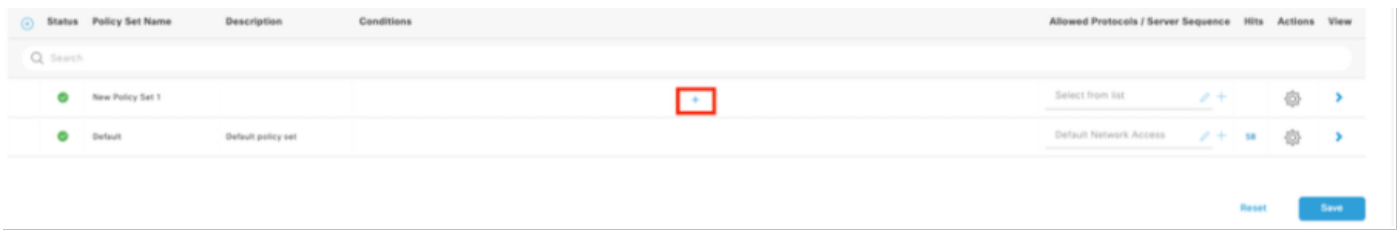
Schritt 8: Erstellen eines Policy Sets, das mit der IP-Adresse des Arista Switches übereinstimmt

Auf diese Weise wird verhindert, dass andere Geräte den Benutzern Zugriff gewähren.

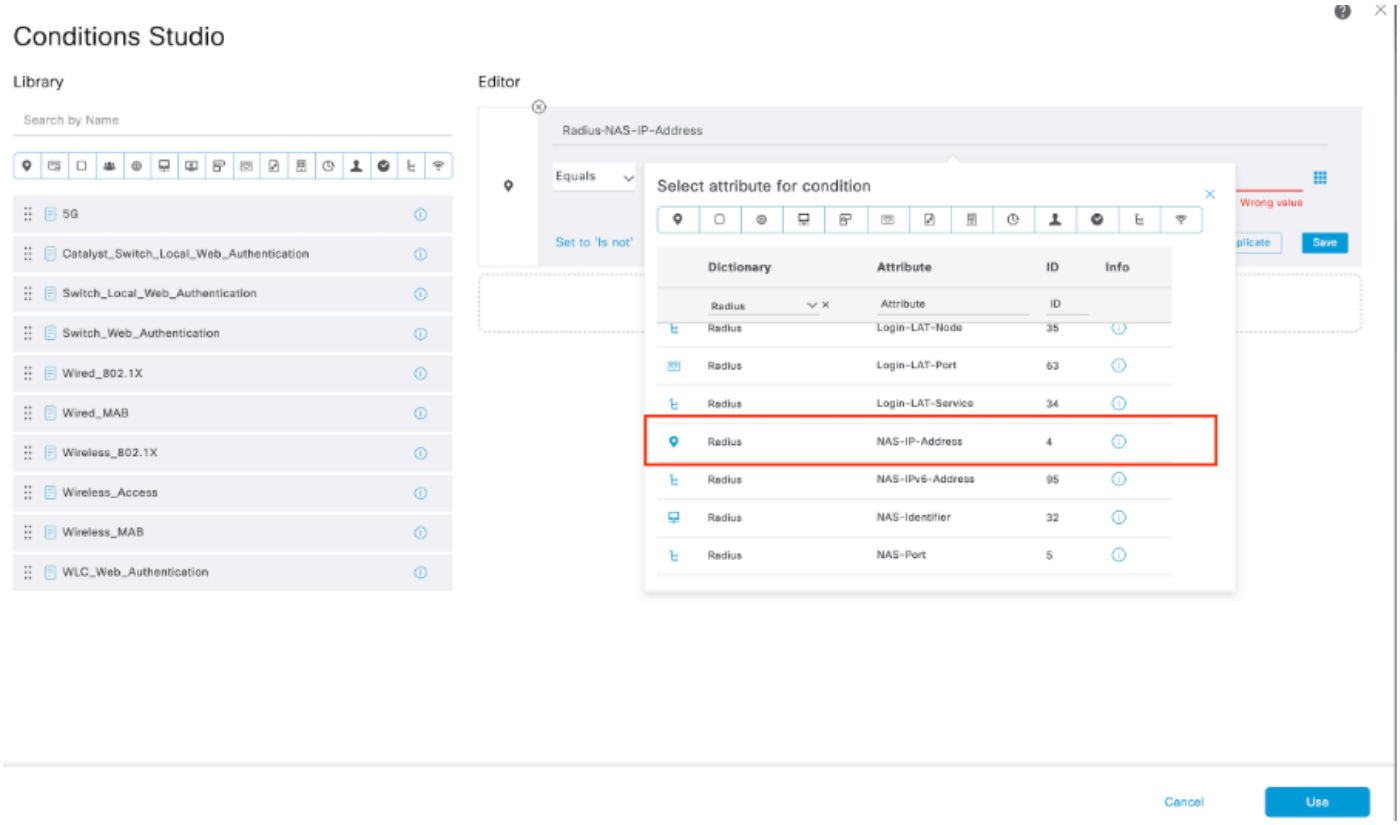
Navigieren Sie zu Policy > Policy Sets > Add icon sign in der oberen linken Ecke.

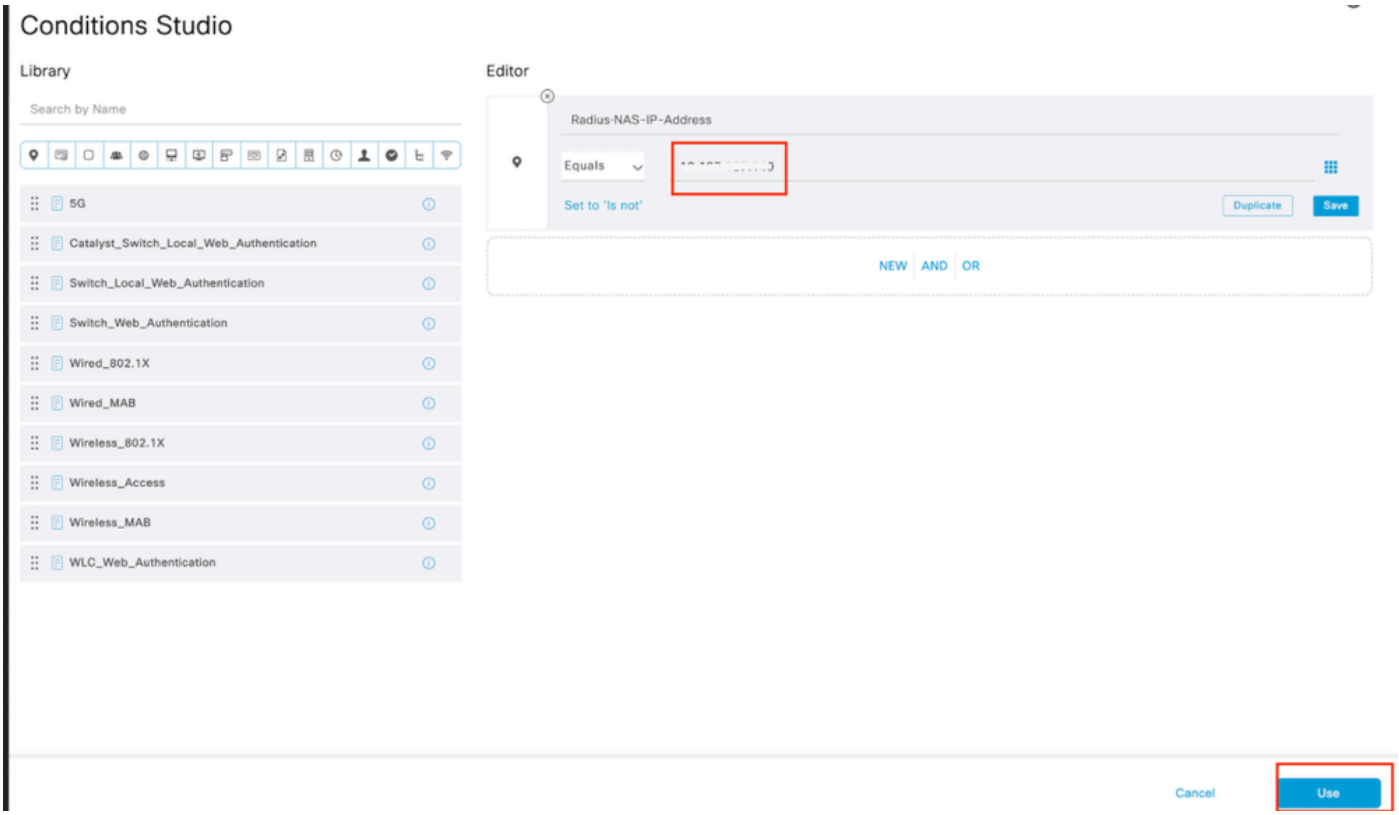


8.1 Eine neue Zeile wird an die Spitze Ihrer Policy Sets gesetzt. Klicken Sie auf das Symbol Hinzufügen, um eine neue Bedingung zu konfigurieren.

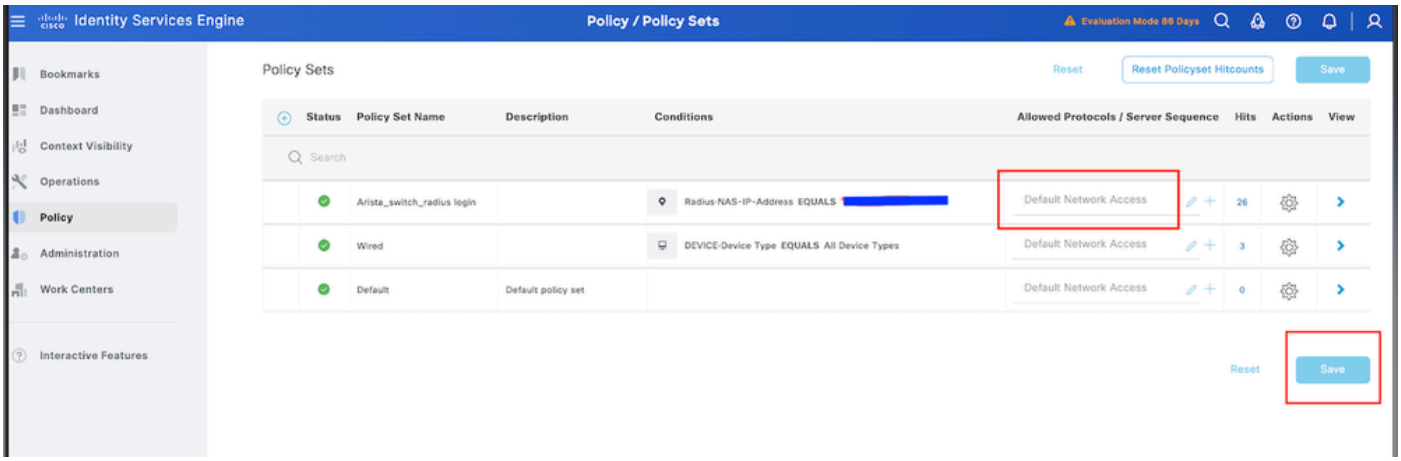


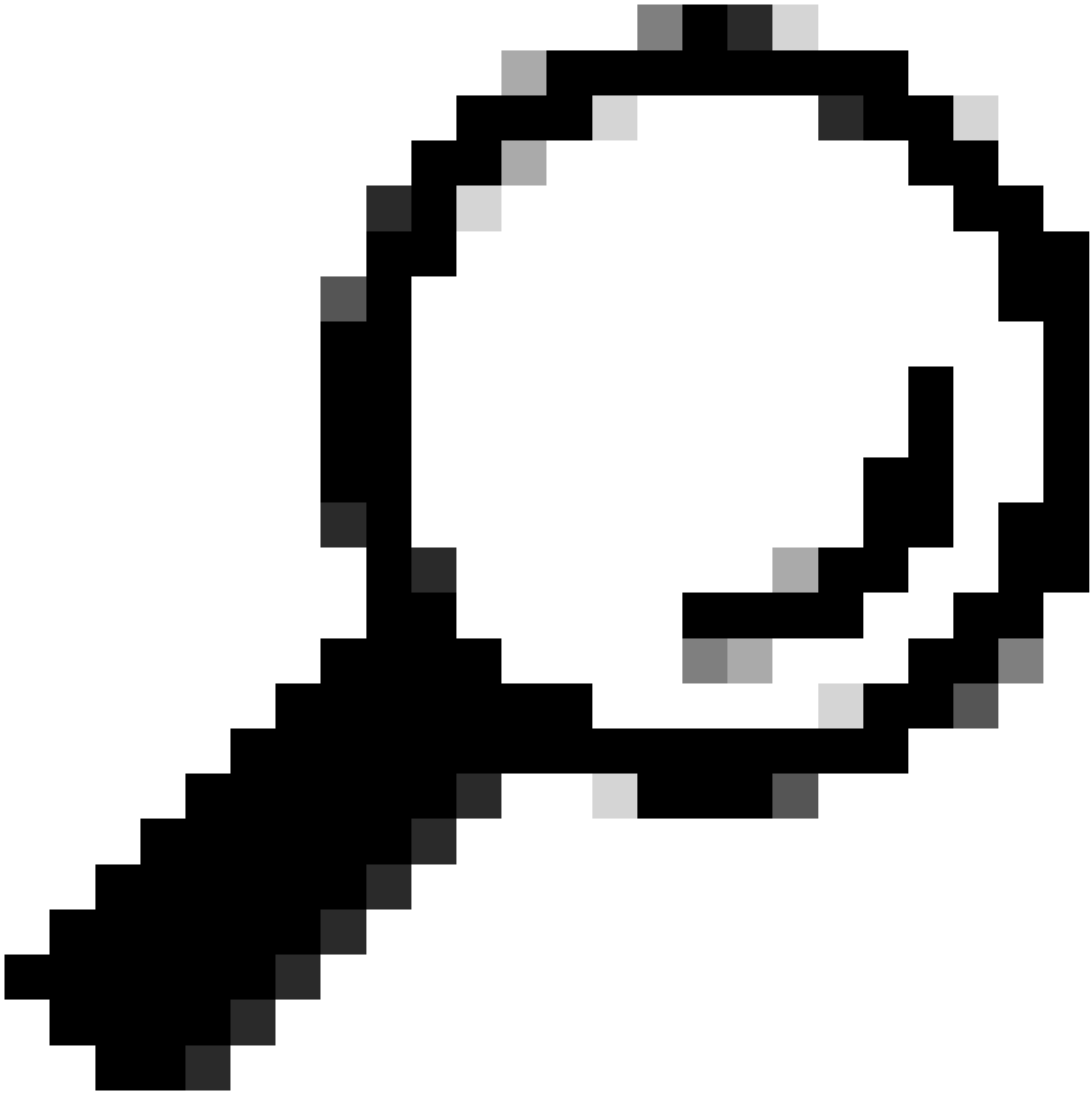
8.2 Fügen Sie eine Top-Bedingung für das RADIUS NAS-IP-Address-Attribut hinzu, das mit der IP-Adresse des Arista-Switches übereinstimmt, und klicken Sie dann auf Verwenden.





8.3 Klicken Sie abschließend auf Speichern:

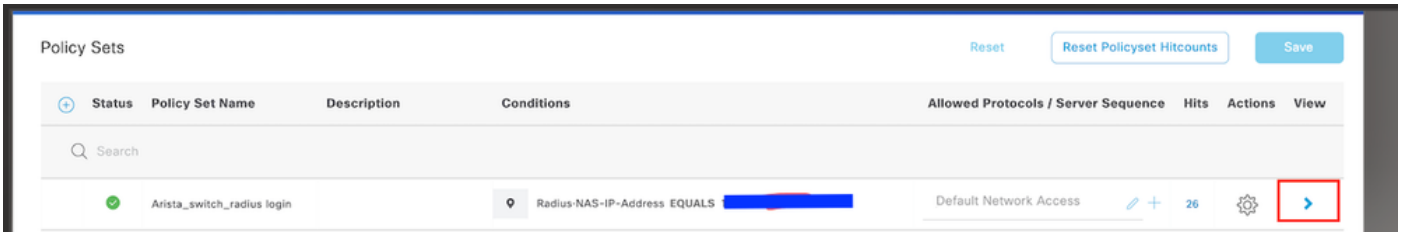




Tipp: Für diese Übung wurde die Liste der Standardprotokolle für den Netzwerkzugriff zugelassen. Sie können eine neue Liste erstellen und sie nach Bedarf eingrenzen.

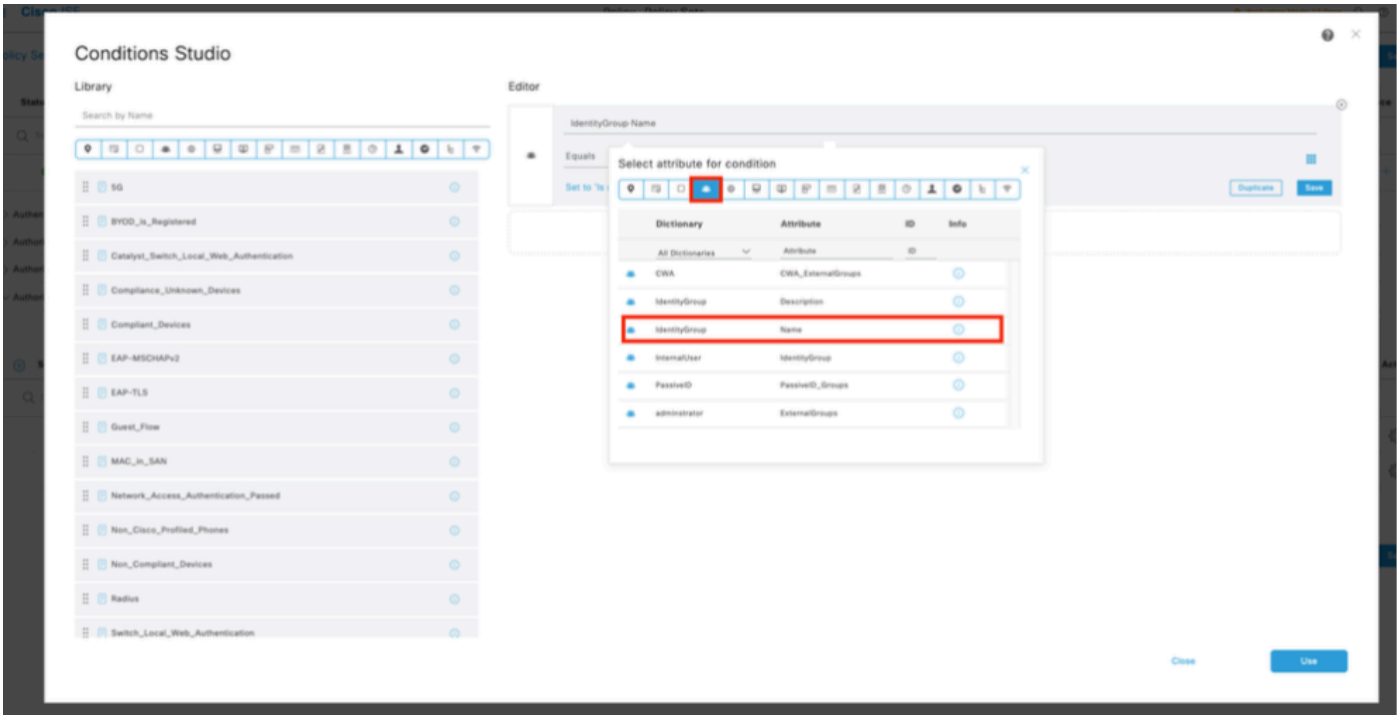
Schritt 9. Neuen Richtliniensatz anzeigen

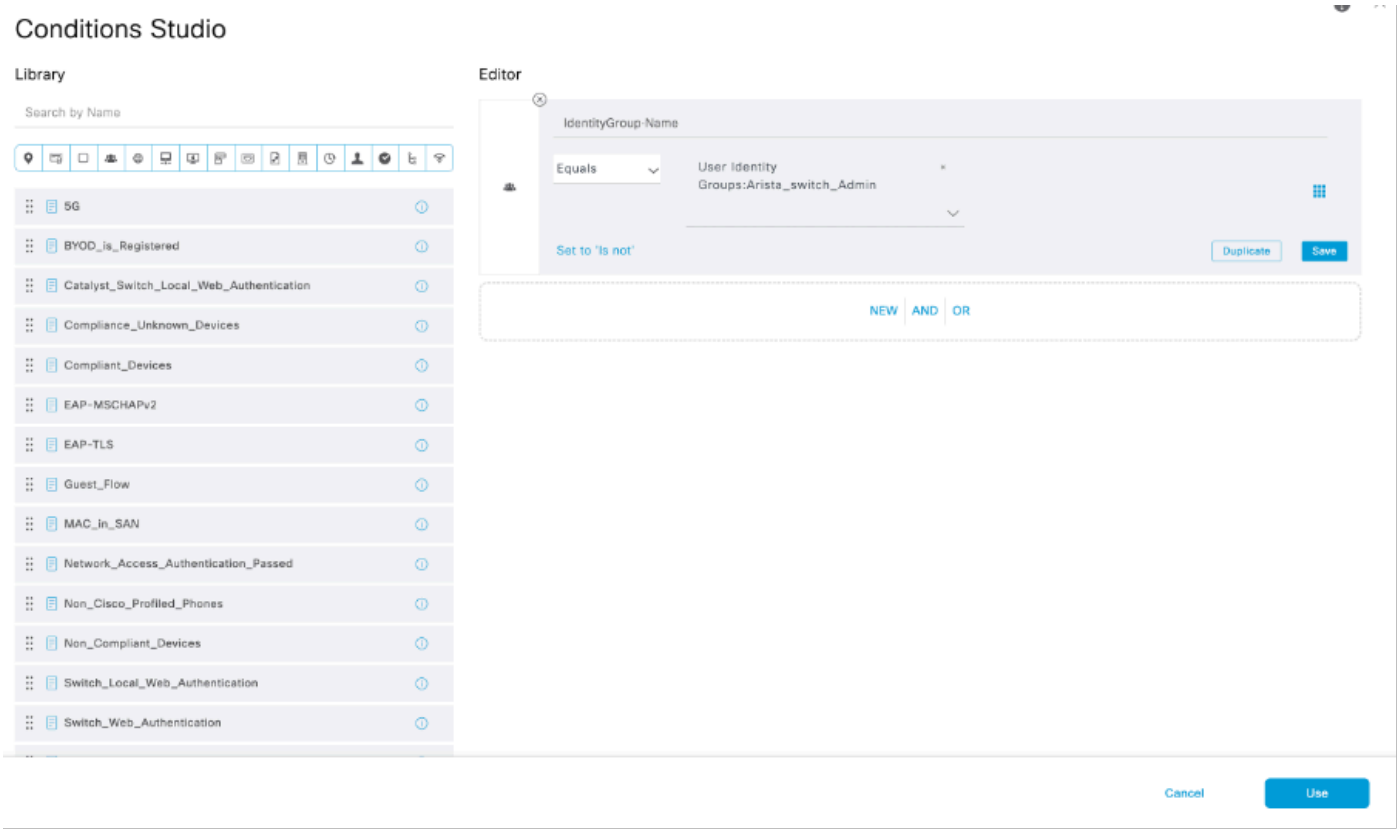
Klicken Sie auf das > Symbol am Ende der Zeile:



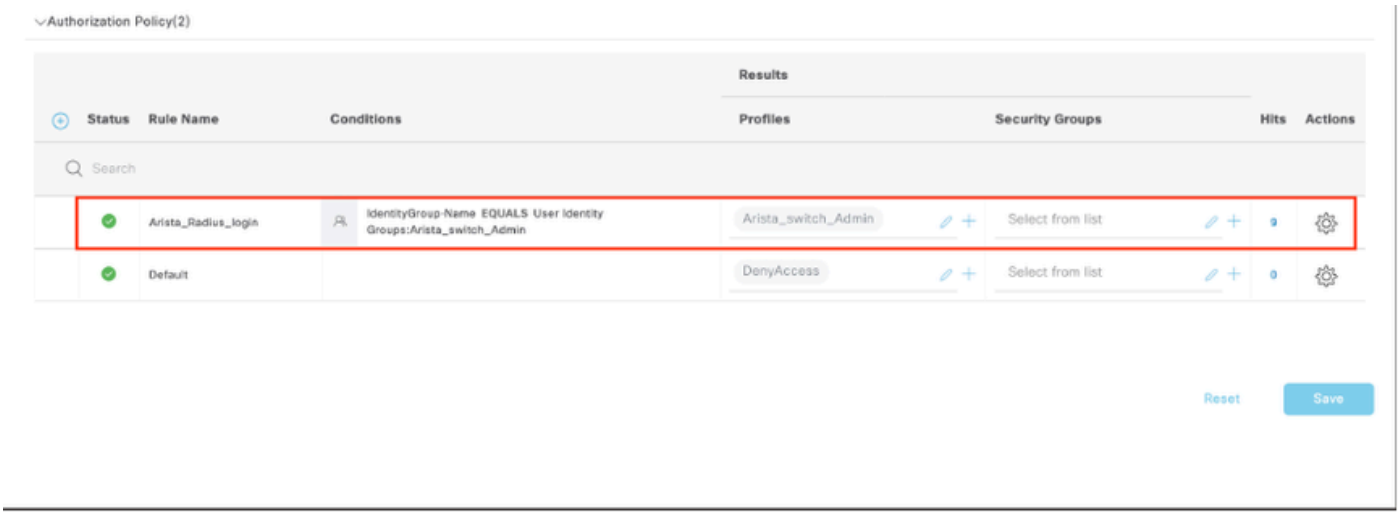
9.1 Erweitern Sie das Menü Autorisierungsrichtlinie, und klicken Sie auf (+), um eine neue Bedingung hinzuzufügen.

9.2 Bedingungen festlegen, die der Dictionary Identity Group mit Attributname gleich Benutzeridentitätsgruppen entsprechen: Arista_switch_Admin (der in Schritt 7 erstellte Gruppenname), und klicken Sie auf Verwenden.





9.3 Überprüfen Sie, ob die neue Bedingung in der Autorisierungsrichtlinie konfiguriert ist, und fügen Sie dann unter "Profiles" (Profile) ein Benutzerprofil hinzu:



Konfigurieren des Arista-Switches

Schritt 1: Aktivieren der RADIUS-Authentifizierung

Melden Sie sich beim Arista-Switch an, und wechseln Sie in den Konfigurationsmodus:

konfigurieren

!

radius-server host <ISE-IP> key <RADIUS-SECRET>

Radius-Server-Timeout 5

Radius-Server-Neuübertragung 3

Radius-Server-Totzeit 30

!

aaa Gruppenserver-Radius ISE

  server <ISE-IP>

!

aaa Authentifizierung Anmeldung Standardgruppe ISE lokal

aaa, Autorisierung, exec, Standardgruppe, ISE lokal

aaa accounting exec default start-stop group ISE

aaa accounting-Befehle 15 standardmäßige Start-Stopp-Gruppe ISE

aaa Abrechnungssystem Standard Start-Stopp-Gruppe ISE

!

end

Schritt 2: Konfiguration speichern

So behalten Sie die Einstellungen bei Neustarts bei:

Schreibspeicher

Oder

copy running-config startup-config

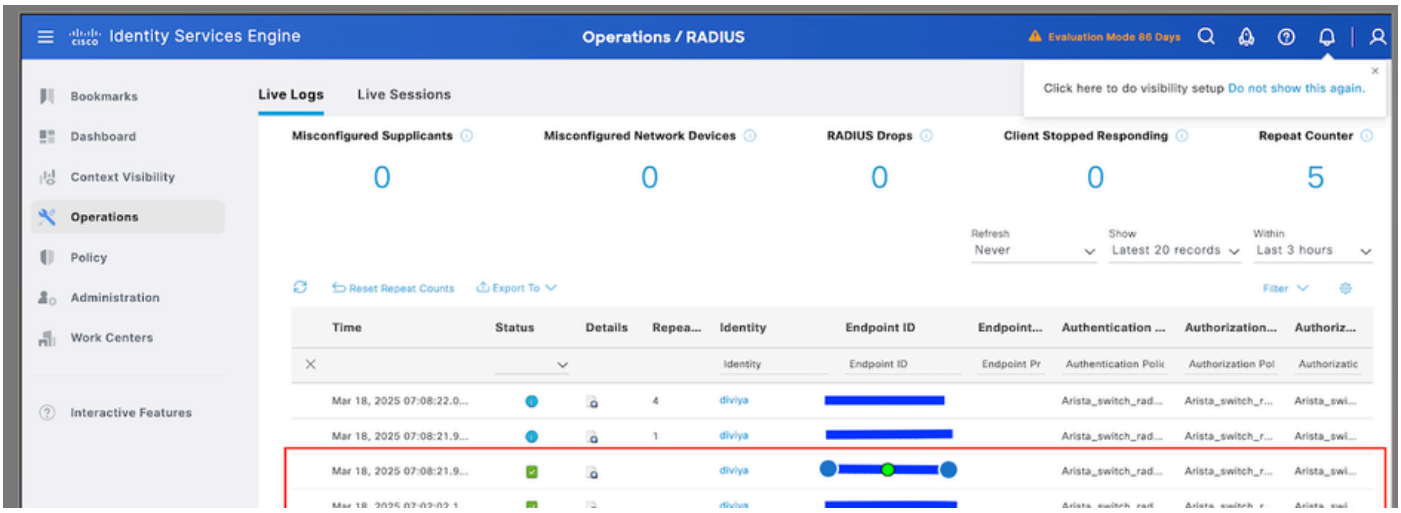
Überprüfung

ISE-Prüfung

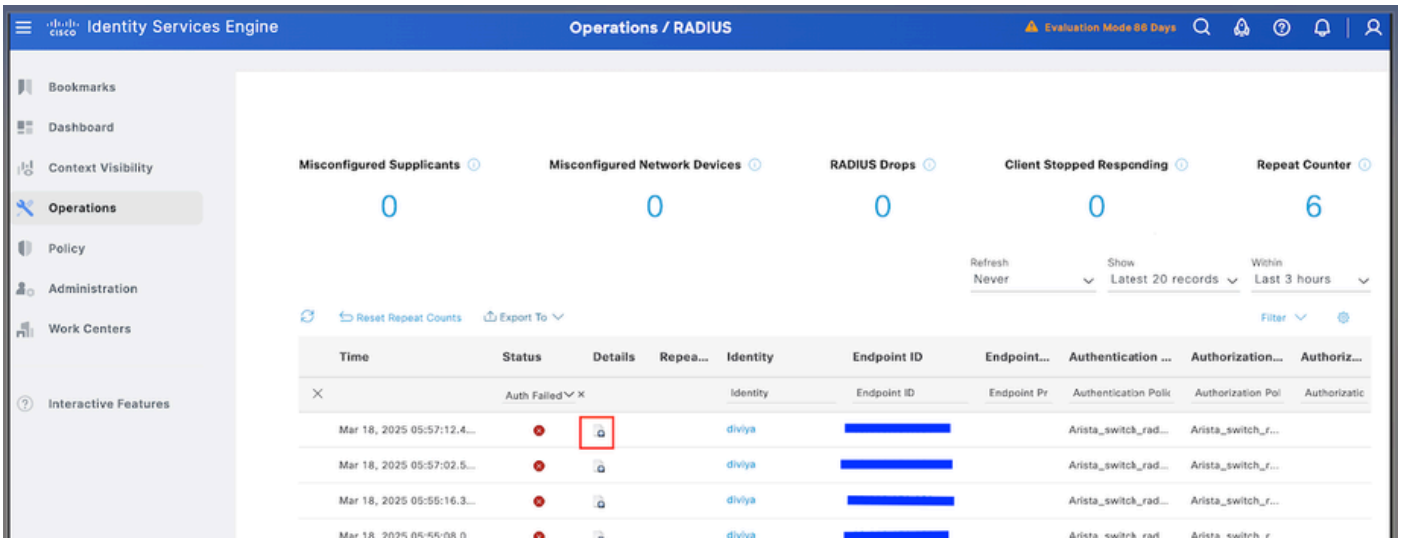
1. Versuchen Sie, sich mit den neuen RADIUS-Anmeldeinformationen beim Arista Switch anzumelden:

    1.1 Navigieren Sie zu Operationen > Radius > Live-Protokolle.

    1.2 Die angezeigten Informationen zeigen an, ob ein Benutzer erfolgreich angemeldet wurde.



2. Wenn der Status "Fehlgeschlagen" angezeigt wird, überprüfen Sie die Sitzungsdetails:

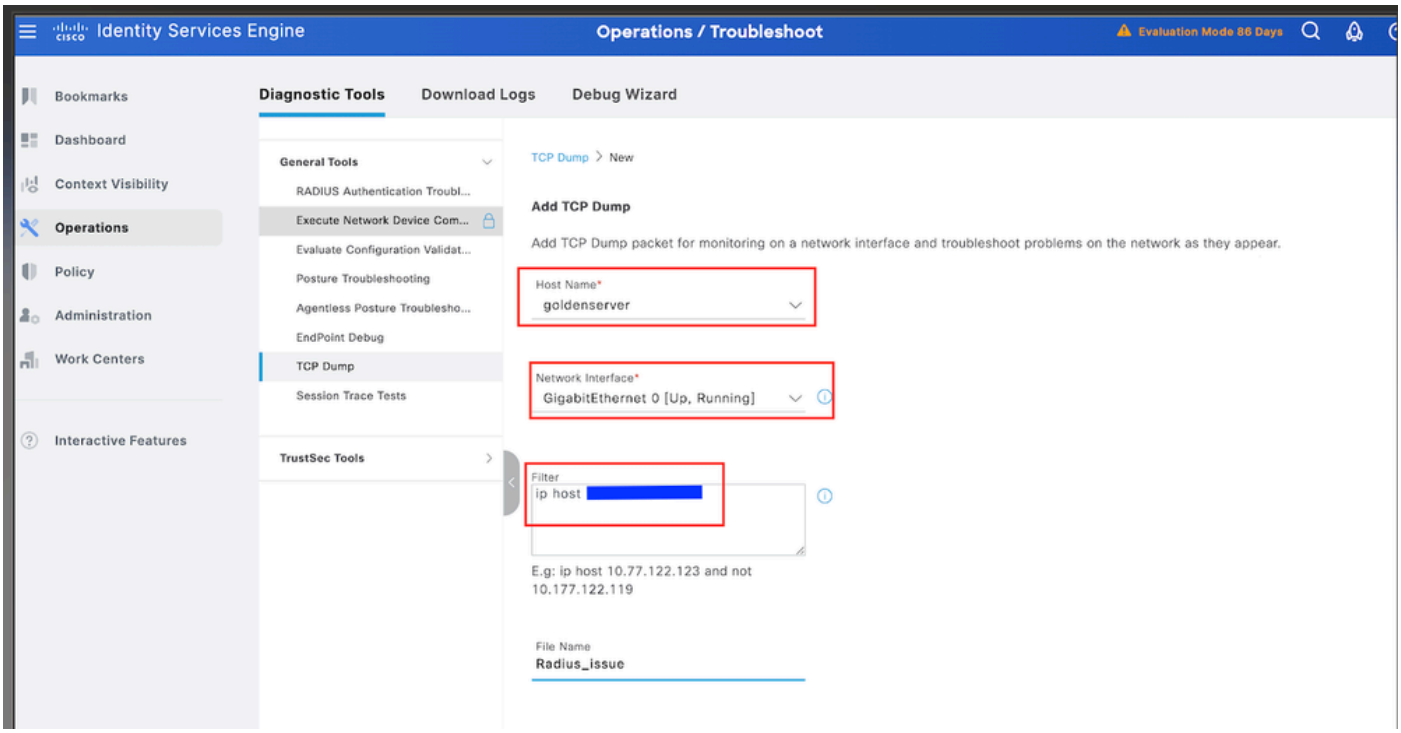


3. Überprüfen Sie bei Anfragen, die nicht in Radius Live-Protokollen angezeigt werden, ob die UDP-Anfrage den ISE-Knoten über eine Paketerfassung erreicht.

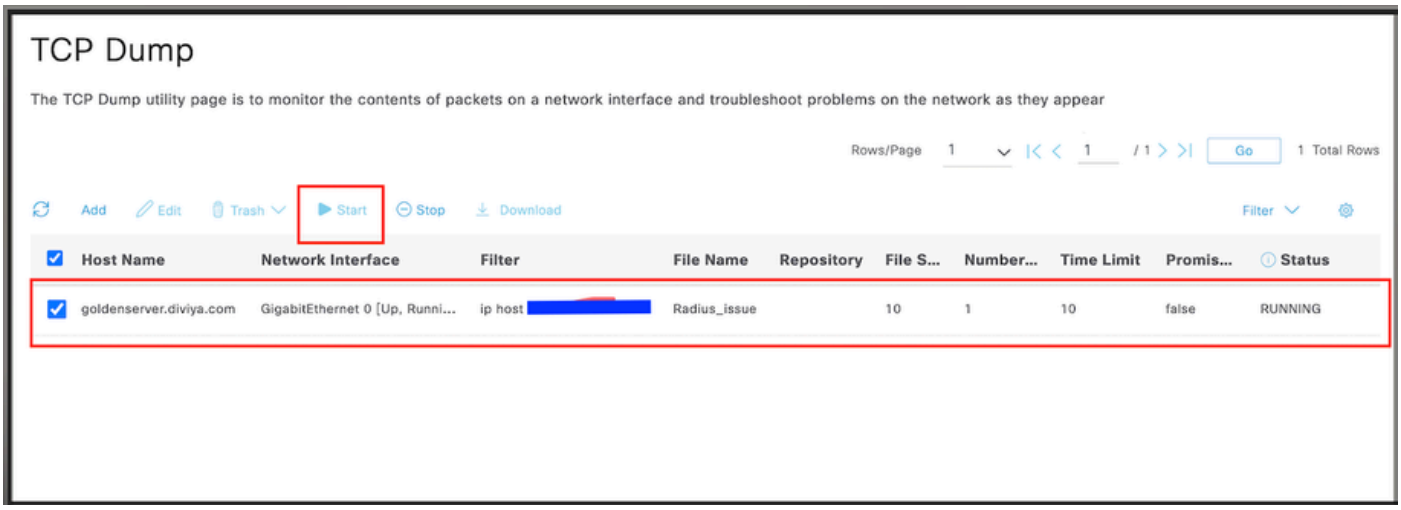
3.1. Navigieren Sie zu Vorgänge > Fehlerbehebung > Diagnosetools > TCP-Dump.

3.2. Fügen Sie eine neue Erfassung hinzu, und laden Sie die Datei auf Ihren lokalen Computer herunter, um zu überprüfen, ob die UDP-Pakete beim ISE-Knoten eintreffen.

3.3. Füllen Sie die erforderlichen Informationen aus, scrollen Sie nach unten und klicken Sie auf Speichern.



3.4. Wählen Sie die Erfassung aus, und starten Sie sie.



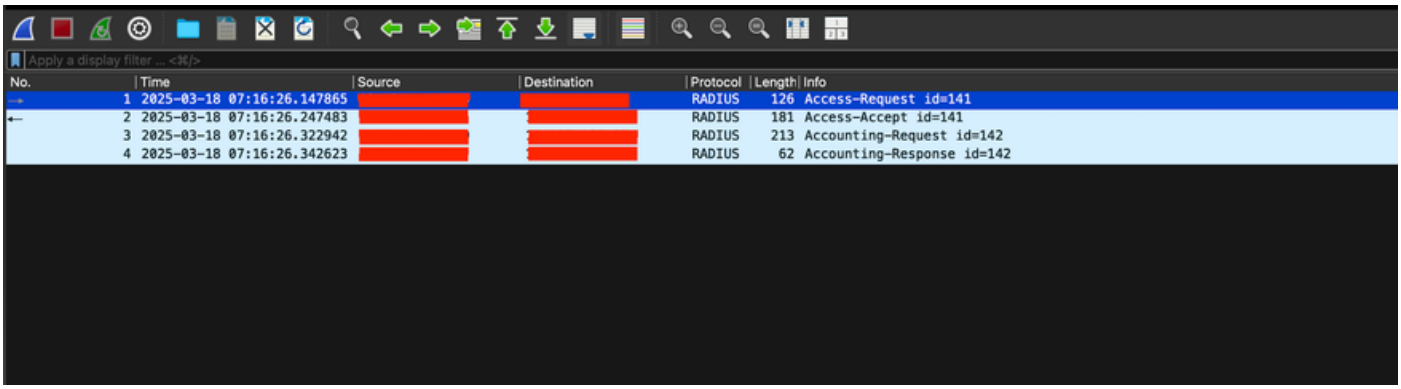
3.5. Versuchen Sie, sich beim Arista Switch anzumelden, während die ISE-Erfassung ausgeführt wird.

3.6. Stoppen Sie den TCP-Dump in der ISE, und laden Sie die Datei auf einen lokalen Computer herunter.

3.7. Datenverkehrsausgabe überprüfen

Erwartete Ausgabe:

Paket Nr.1. Anforderung vom Arista Switch an den ISE-Server über Port 1812 (RADIUS).
Paket Nr. 2. ISE-Serverantwort, die die ursprüngliche Anforderung akzeptiert.



Fehlerbehebung

Szenario 1. "5405 RADIUS-Anforderung wurde verworfen"

Problem

Dieses Szenario beinhaltet die Fehlerbehebung für den Fehler "5405 RADIUS Request droppt" (5405 RADIUS-Anforderung verworfen) mit dem Grund "11007 Could not locate Network Device or AAA Client" (konnte Netzwerkgerät oder AAA-Client nicht finden) in Cisco ISE, wenn ein Netzwerkgerät (z. B. ein Arista-Switch) versucht, sich zu authentifizieren.

Mögliche Ursachen

- Die Cisco Identity Services Engine (ISE) kann den Arista-Switch nicht identifizieren, da seine IP-Adresse nicht unter bekannten Netzwerkgeräten aufgeführt ist.
- Die RADIUS-Anforderung stammt von einer IP-Adresse, die von der ISE nicht als gültiges Netzwerkgerät oder AAA-Client erkannt wird.
- Zwischen dem Switch und der ISE kann eine Diskrepanz in der Konfiguration bestehen (z. B. eine falsche IP oder ein gemeinsamer geheimer Schlüssel).

Lösung

- Fügen Sie den Switch der Cisco ISE-Liste der Netzwerkgeräte mit der richtigen IP-Adresse hinzu.
- Überprüfen Sie, ob die IP-Adresse und der gemeinsame geheime Schlüssel, die in der ISE konfiguriert wurden, mit den Angaben auf dem Switch übereinstimmen.
- Nach der Korrektur muss die RADIUS-Anforderung ordnungsgemäß erkannt und verarbeitet werden.

Szenario 2: Arista-Switch schlägt Failover zum Backup von ISE PSN fehl

Problem

Ein Arista-Switch wird so konfiguriert, dass er die Cisco ISE für die RADIUS-Authentifizierung verwendet. Wenn der primäre ISE Policy Service Node (PSN) nicht mehr verfügbar ist, erfolgt für den Switch kein automatisches Failover zu einem Backup-PSN. Daher werden Authentifizierungsprotokolle nur vom primären ISE PSN angezeigt, und es gibt keine Protokolle vom sekundären/Backup-PSN, wenn das primäre ausfällt.

Mögliche Ursachen

- Die RADIUS-Serverkonfiguration des Arista-Switches verweist nur auf den primären ISE-Knoten, sodass keine Backup-Server verwendet werden.
- Die RADIUS-Serverpriorität ist nicht richtig festgelegt, oder die ISE-Backup-IP-Adresse fehlt in der Konfiguration.
- Die Einstellungen für Zeitüberschreitung und Neuübertragung auf dem Switch sind zu niedrig eingestellt, um ein erfolgreiches Fallback auf das Backup-PSN zu verhindern.
- Der Switch verwendet einen FQDN für das PSN, aber die DNS-Auflösung gibt nicht alle A-Einträge zurück, sodass nur der primäre Server kontaktiert wird.

Lösung

- Stellen Sie sicher, dass mehrere ISE PSN-IPs in die RADIUS-Servergruppenkonfiguration des Switches eingegeben werden. Auf diese Weise kann der Switch das Backup-ISE-PSN verwenden, wenn der primäre Switch nicht erreichbar ist.

  Beispielkonfiguration:

  radius-server host <ISE1-IP> key <geheim>

  radius-server host <ISE2-IP> key <geheim>

- Überprüfen Sie, ob die RADIUS-Serverprioritäts-, Timeout- und Neuübertragungs-Werte ordnungsgemäß für ein zuverlässiges Failover konfiguriert sind.
- Bei Verwendung von FQDNs überprüfen Sie die DNS-Einstellungen und die Auflösung, um sicherzustellen, dass alle PSN-IP-Adressen zurückgegeben und vom Switch verwendet werden.

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.