Konfigurieren der externen SWA-Authentifizierung mit der ISE als RADIUS-Server

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren der externen Authentifizierung für Secure Web Access (SWA) mit der Cisco ISE als RADIUS-Server beschrieben.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der Cisco Secure Web Appliance
- Kenntnis der Konfiguration von Authentifizierungs- und Autorisierungsrichtlinien auf der ISE
- Grundlegendes RADIUS-Wissen

Cisco empfiehlt außerdem Folgendes:

- Administrationszugriff für SWA und ISE.
- Kompatible WSA- und ISE-Versionen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- SWA 14.0.2-012
- ISE 3.0.0

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

Wenn Sie die externe Authentifizierung für administrative Benutzer Ihres SWAs aktivieren, überprüft das Gerät die Benutzeranmeldeinformationen mit einem LDAP- (Lightweight Directory Access Protocol) oder RADIUS-Server, wie in der Konfiguration für die externe Authentifizierung angegeben.

Netzwerktopologie

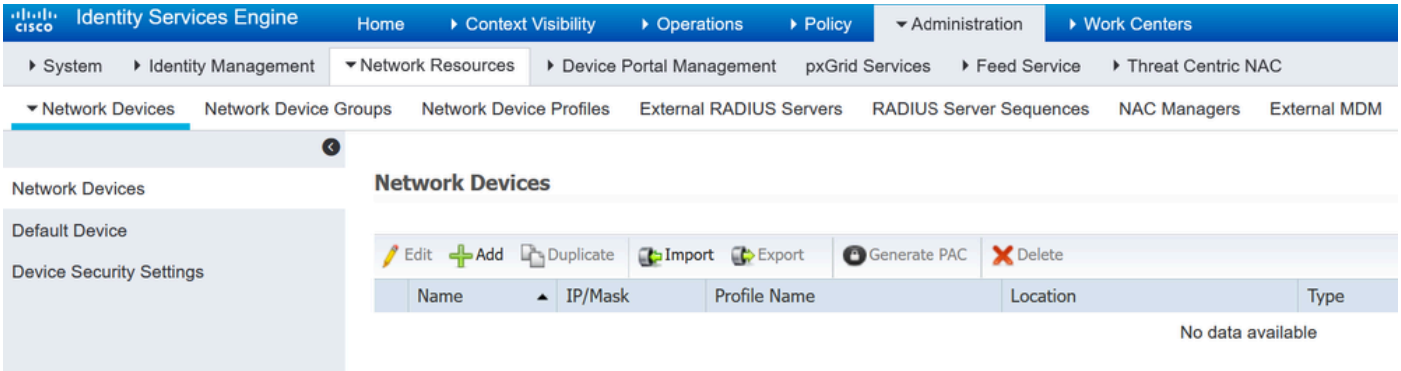
Diagramm der Netzwerktopologie

Administrative Benutzer greifen mit ihren Anmeldeinformationen auf Port 443 auf SWA zu. SWA verifiziert die Anmeldeinformationen mit dem RADIUS-Server.

Konfigurieren

ISE-Konfiguration

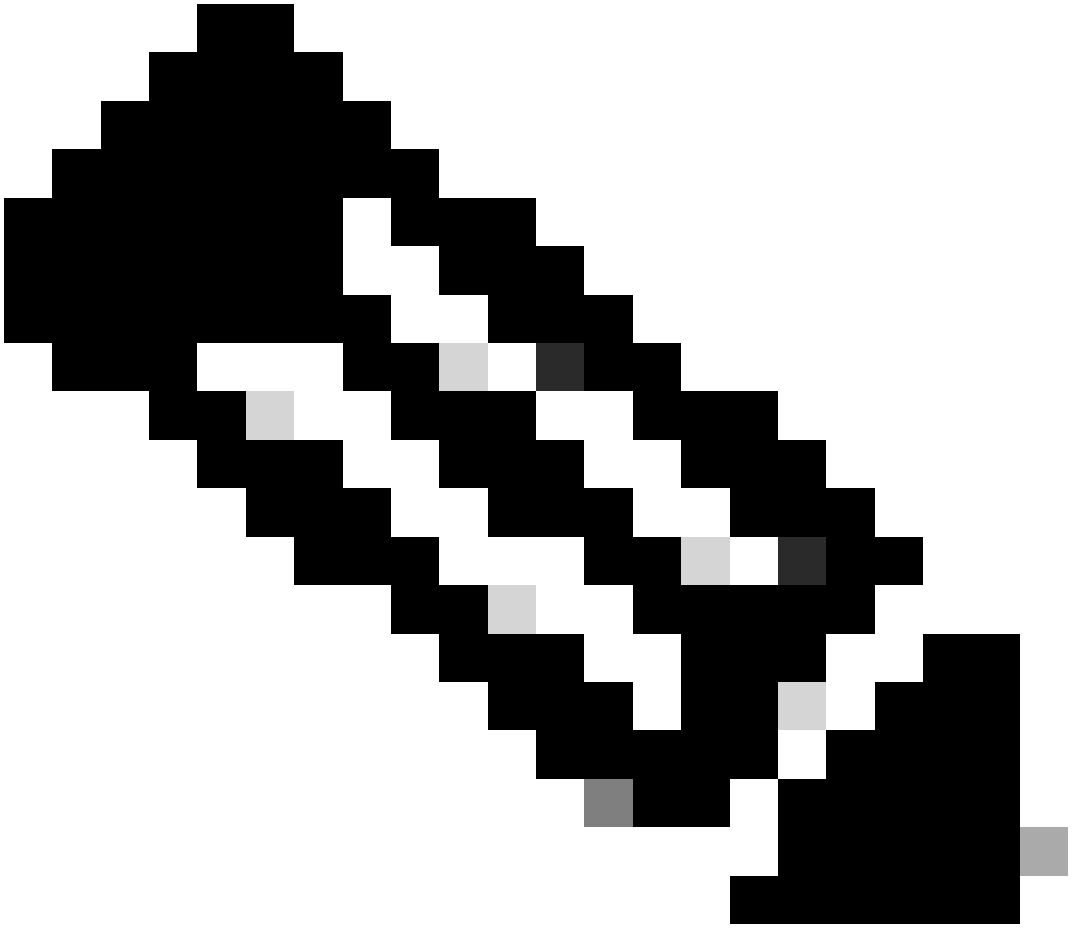
Schritt 1: Hinzufügen eines neuen Netzwerkgeräts Navigieren Sie zu Administration > Network Resources > Network Devices > +Add.



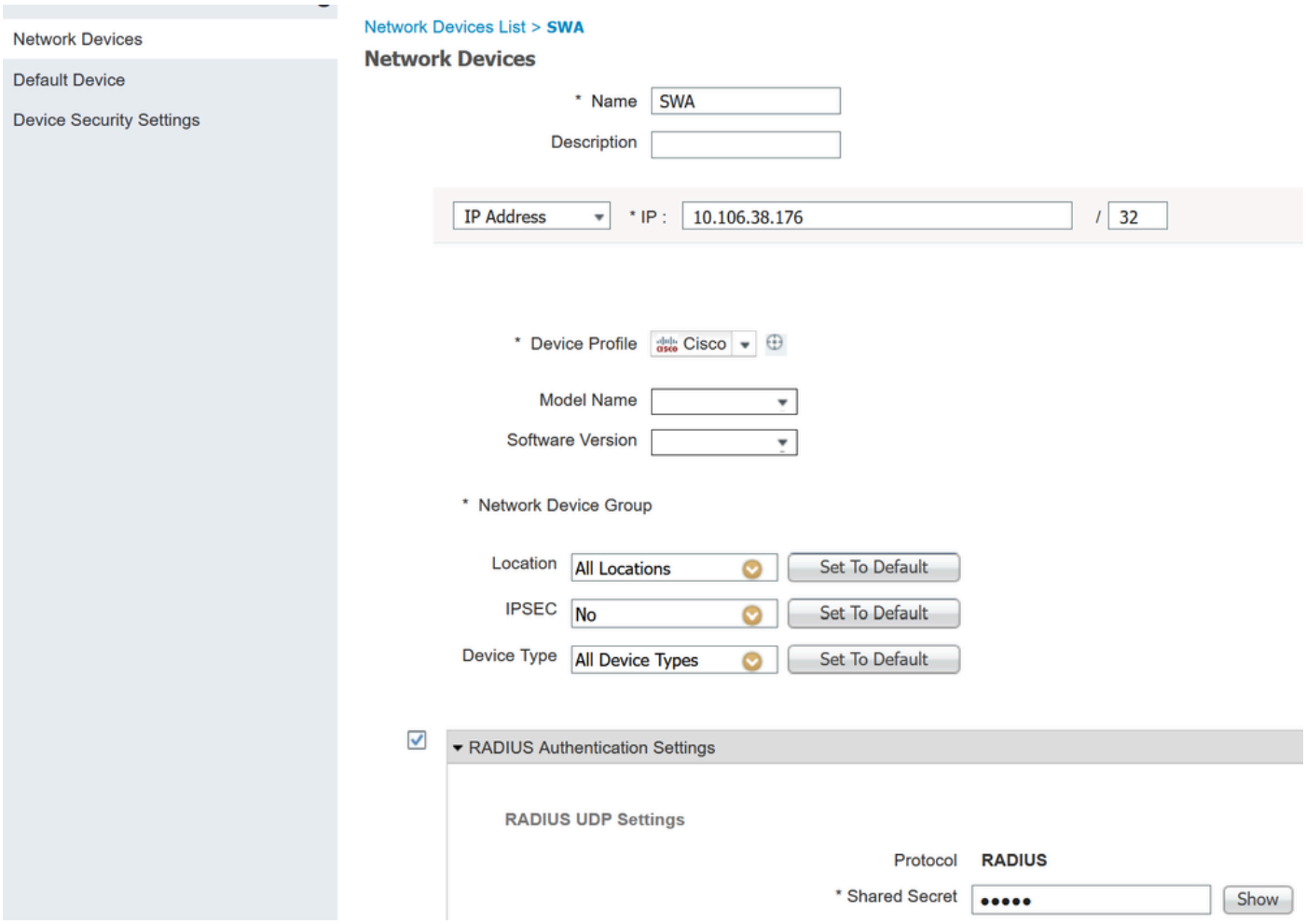
SWA als Netzwerkgerät in der ISE hinzufügen

Schritt 2: Weisen Sie dem Netzwerkgeräteobjekt einen Namen zu, und fügen Sie die SWA-IP-Adresse ein.

Aktivieren Sie das Kontrollkästchen RADIUS, und definieren Sie einen gemeinsamen geheimen Schlüssel.

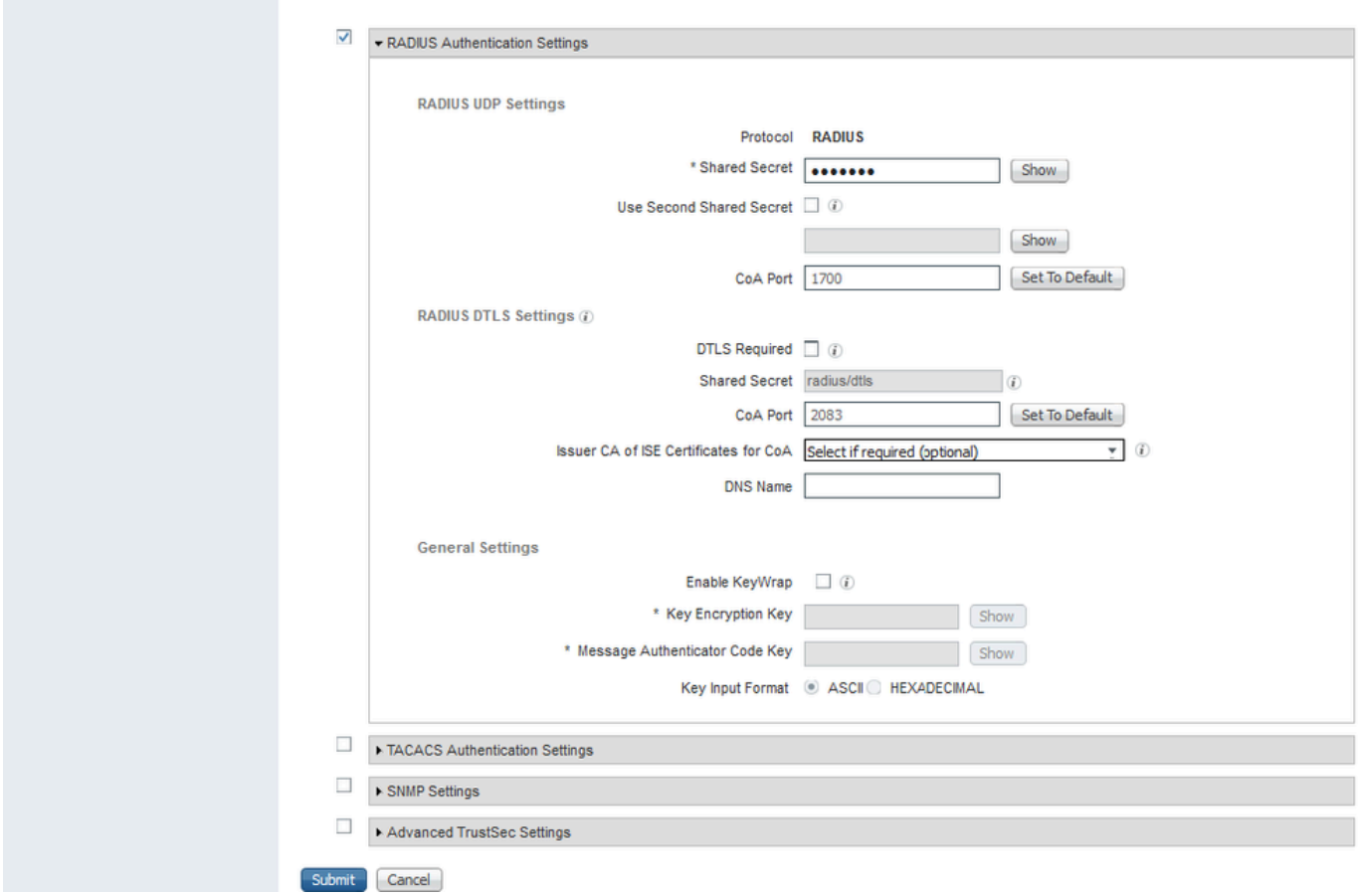


Hinweis: Derselbe Schlüssel muss später zum Konfigurieren des RADIUS-Servers in SWA verwendet werden.



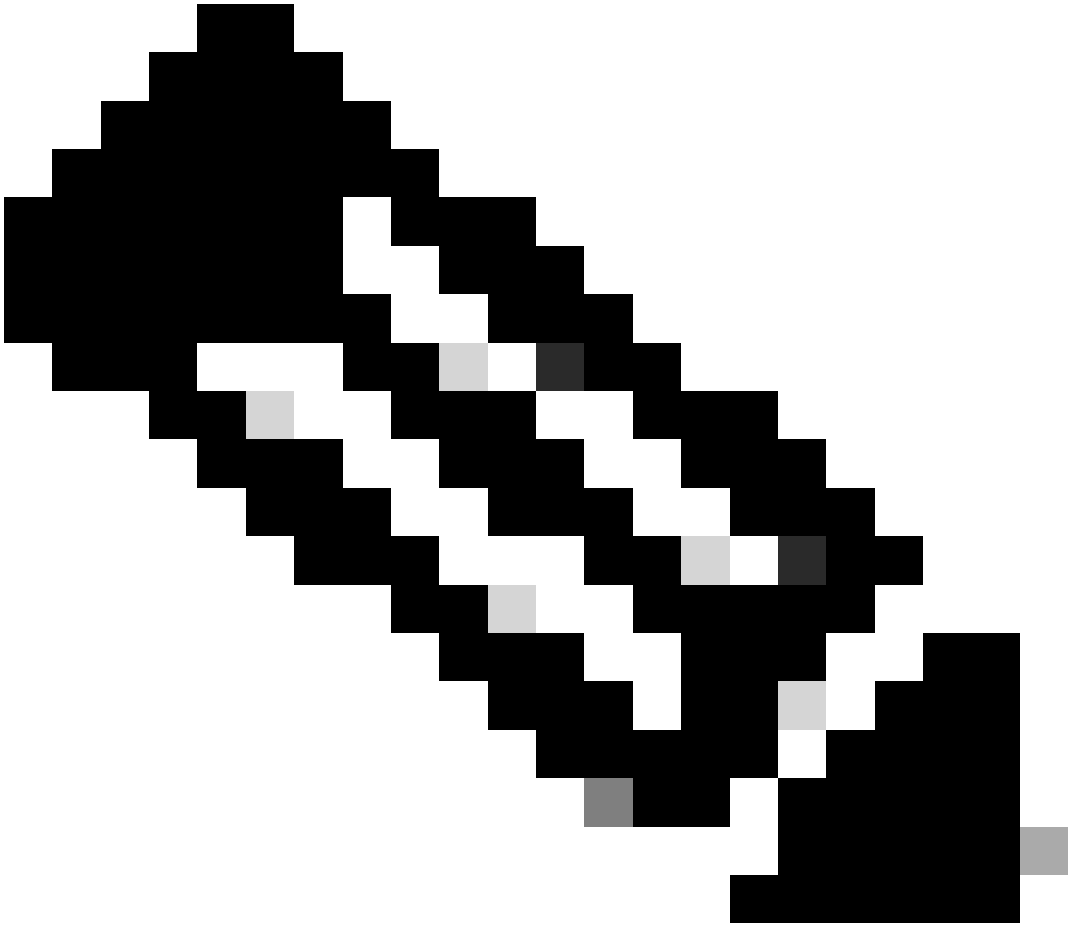
Gemeinsamer SWA-Schlüssel für Netzwerkgerät konfigurieren

Schritt 2.1: Klicken Sie auf Senden.

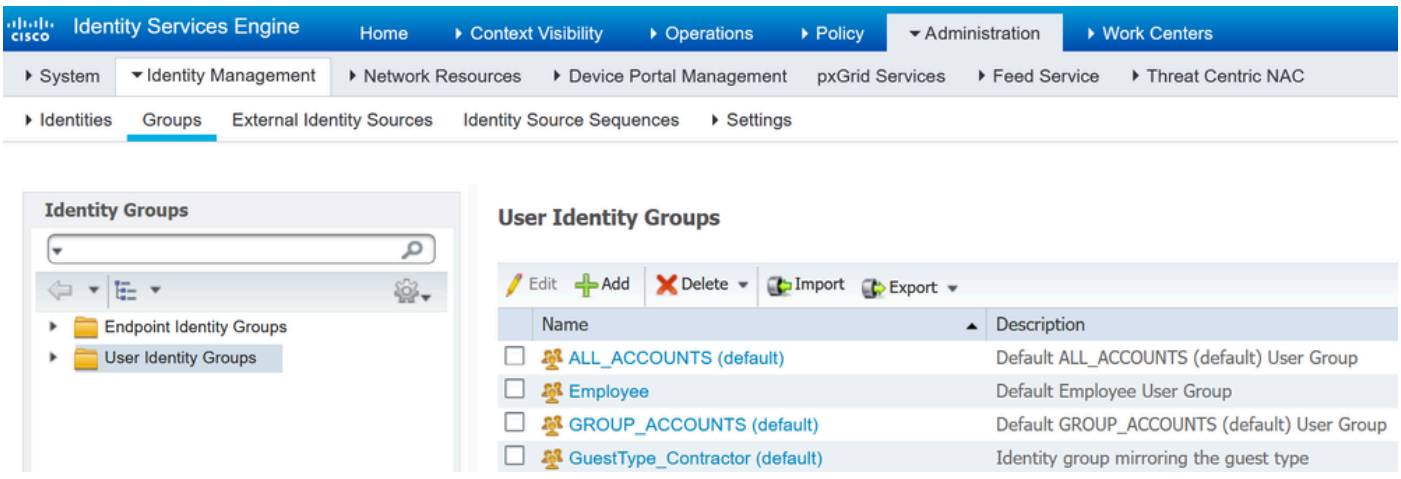


Konfiguration des Netzwerkgeräts senden

Schritt 3: Erstellen Sie die erforderlichen Benutzeridentitätsgruppen. Navigieren Sie zu Administration > Identity Management > Groups > User Identity Groups > + Add.



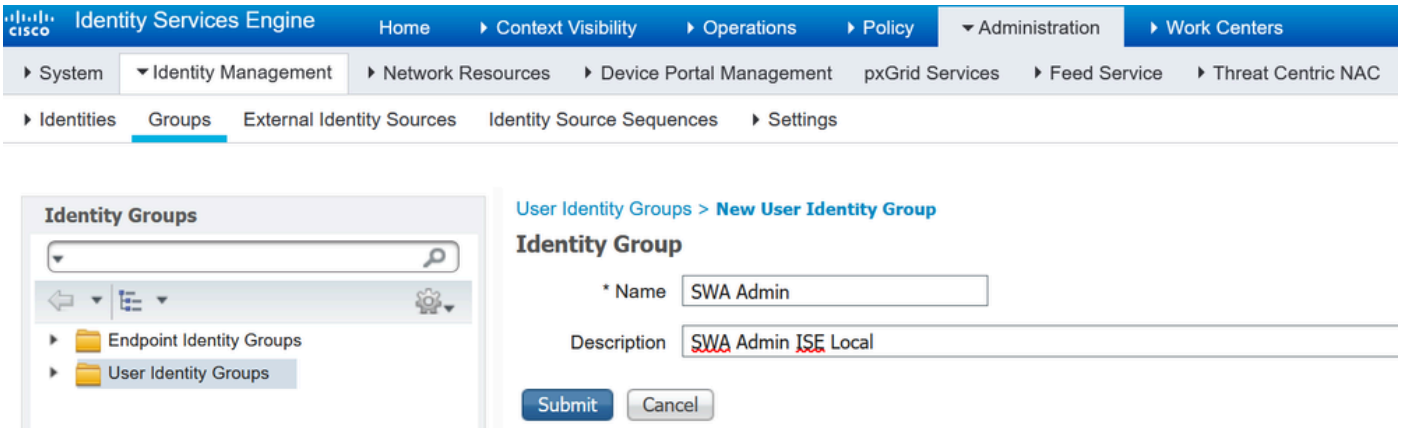
Hinweis: Sie müssen verschiedene Benutzergruppen konfigurieren, um unterschiedlichen Benutzertypen gerecht zu werden.



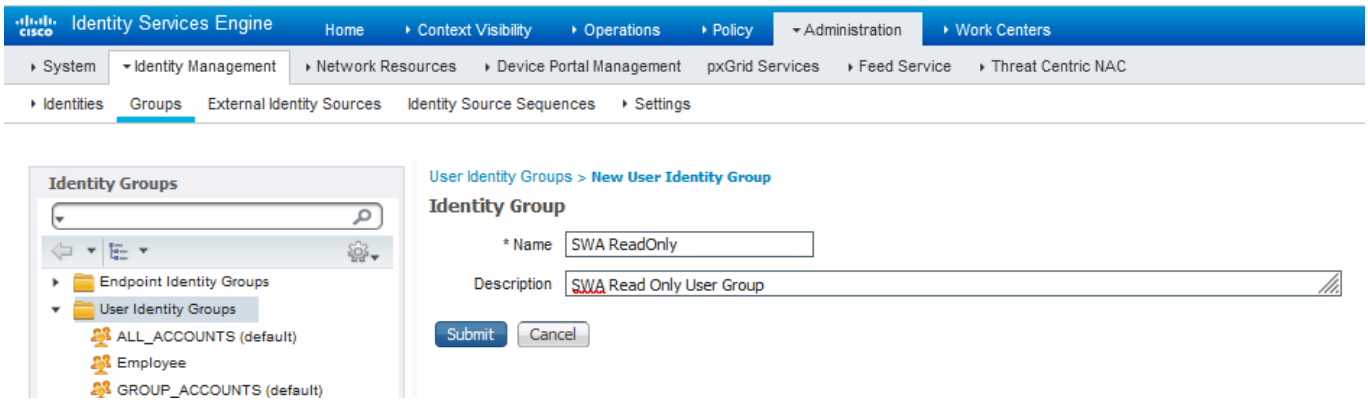
Benutzeridentitätsgruppe hinzufügen

Schritt 4: Geben Sie den Gruppennamen, die Beschreibung (optional) und die Übermittlungsoption

ein. Wiederholen Sie diese Schritte für jede Gruppe. In diesem Beispiel erstellen Sie eine Gruppe für Administrator-Benutzer und eine weitere Gruppe für schreibgeschützte Benutzer.



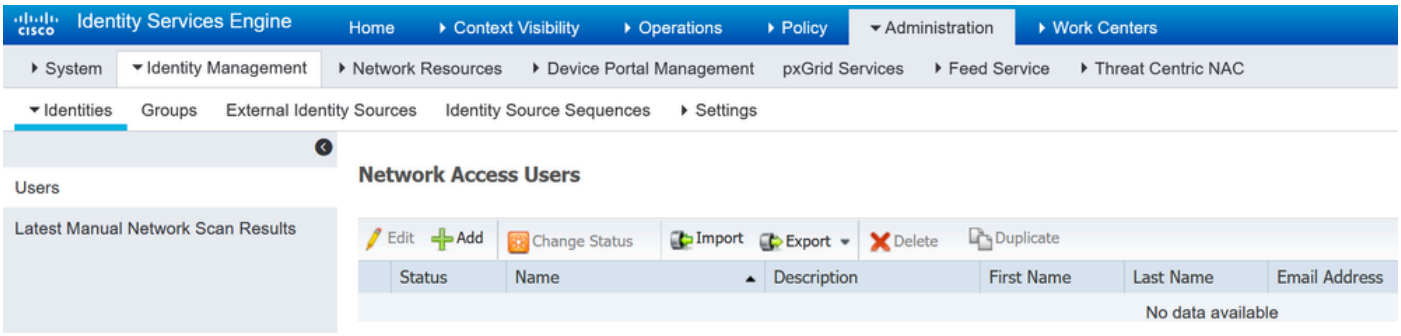
Benutzeridentitätsgruppe hinzufügenBenutzeridentitätsgruppe



für schreibgeschützte SWA-Benutzer hinzufügen

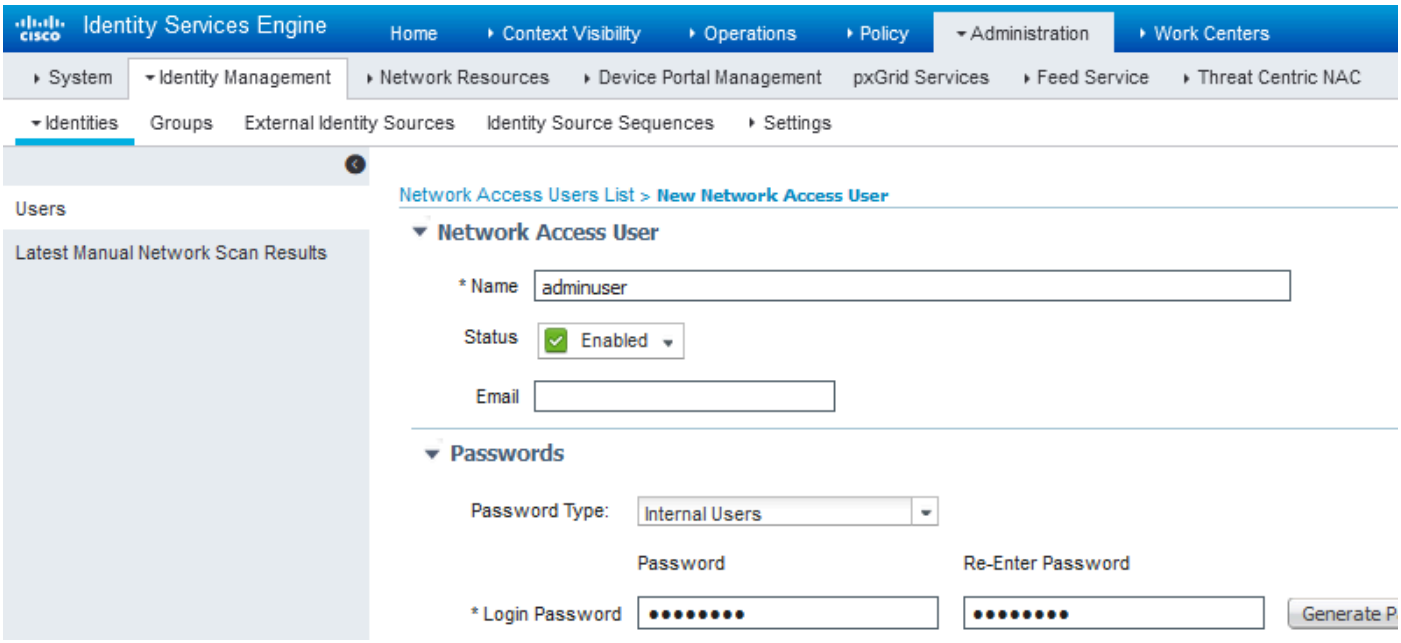
Schritt 5: Sie müssen Netzwerkzugriffsbenutzer erstellen, die mit dem in SWA konfigurierten Benutzernamen übereinstimmen.

Erstellen Sie die Netzwerkzugriffsbenutzer, und fügen Sie sie der entsprechenden Gruppe hinzu. Navigieren Sie zu Administration > Identity Management > Identities > + Add.



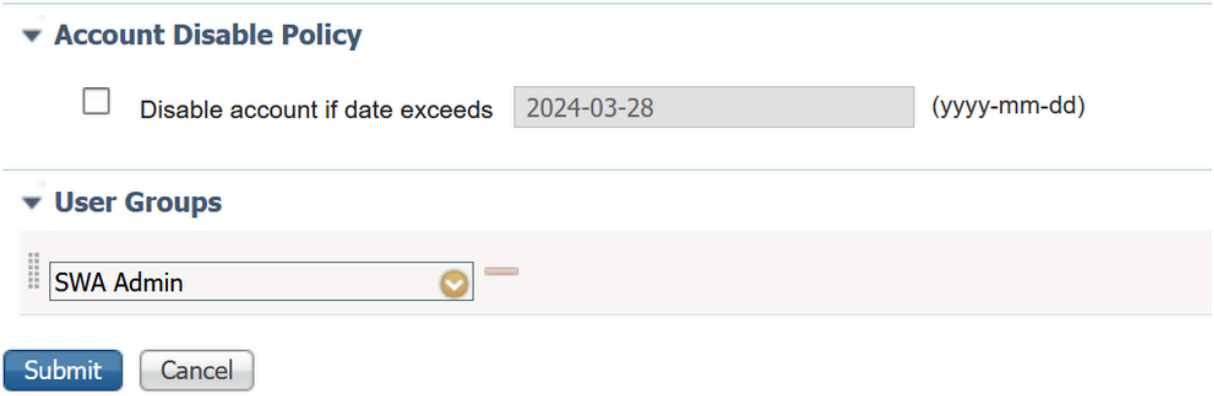
Hinzufügen lokaler Benutzer zur ISE

Schritt 5.1: Sie müssen einen Netzwerkzugriffsbenutzer mit Administratorrechten erstellen. Weisen Sie einen Namen und ein Kennwort zu.



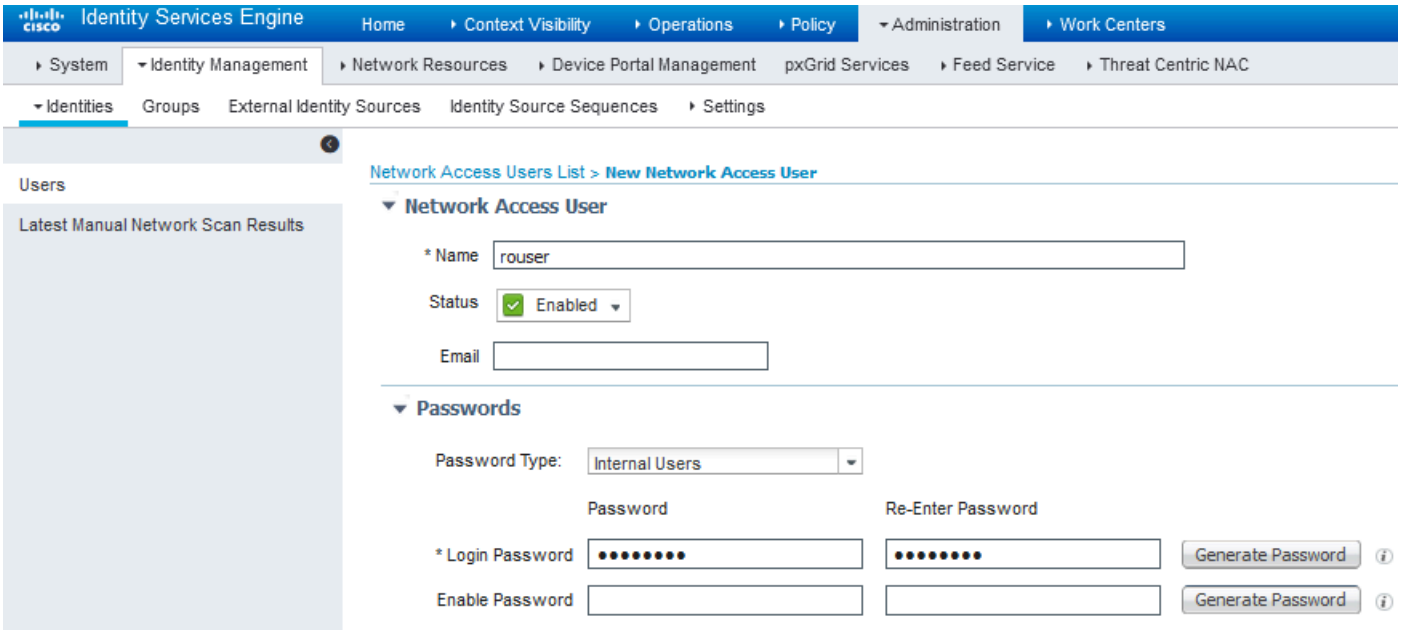
Administrator-Benutzer hinzufügen

Schritt 5.2: Wählen Sie im Abschnitt "User Groups" (Benutzergruppen) die Option SWA Admin



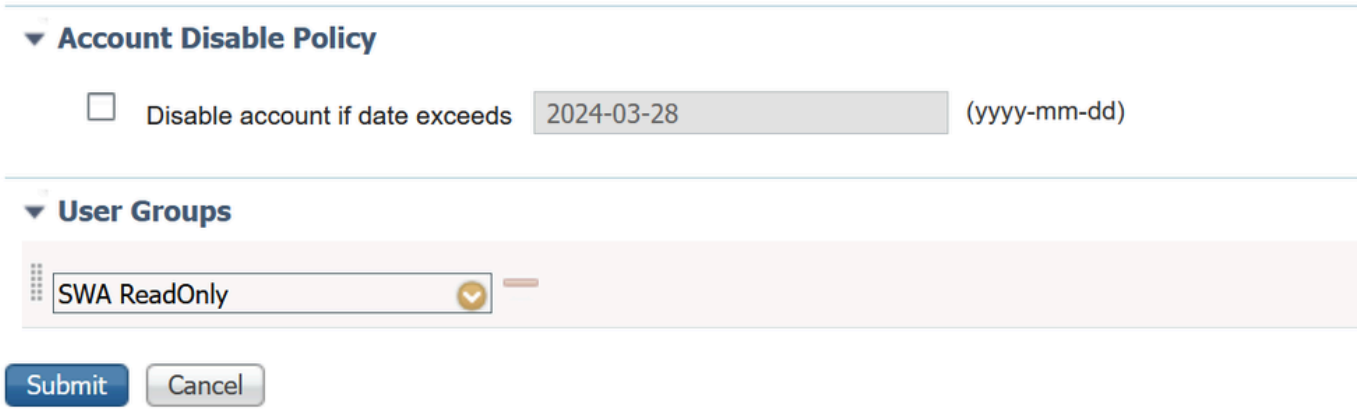
(Admin-Gruppe)
aus. Weisen Sie dem Admin-Benutzer eine Admin-Gruppe zu.

Schritt 5.3: Sie müssen einen Benutzer mit Lesezugriff erstellen. Weisen Sie einen Namen und ein Kennwort zu.



Schreibgeschützten Benutzer hinzufügen

Schritt 5.4: Wählen Sie im Abschnitt User Groups (Benutzergruppen) die Option SWA ReadOnly aus.

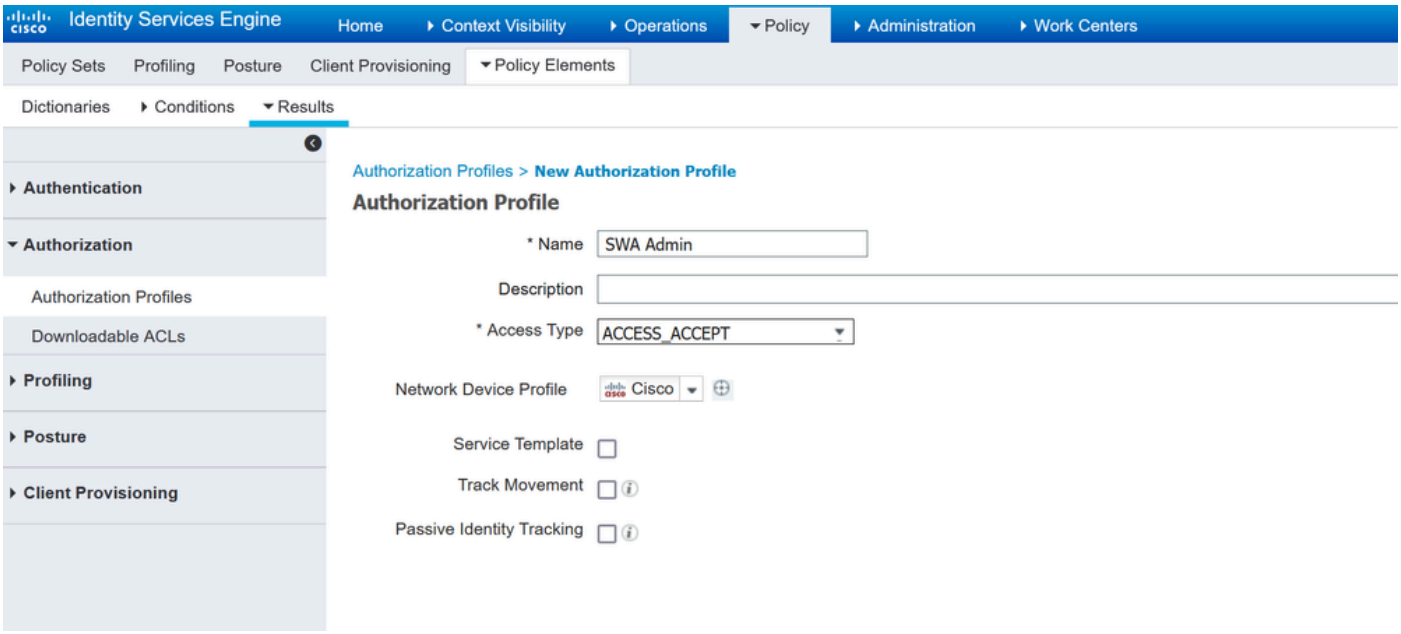


Weisen Sie dem schreibgeschützten Benutzer eine schreibgeschützte Benutzergruppe zu.

Schritt 6: Erstellen Sie das Autorisierungsprofil für den Admin-Benutzer.

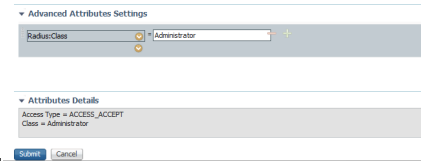
Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > +Hinzufügen.

Definieren Sie einen Namen für das Autorisierungsprofil, und stellen Sie sicher, dass der Zugriffstyp auf ACCESS_ACCEPT festgelegt ist.



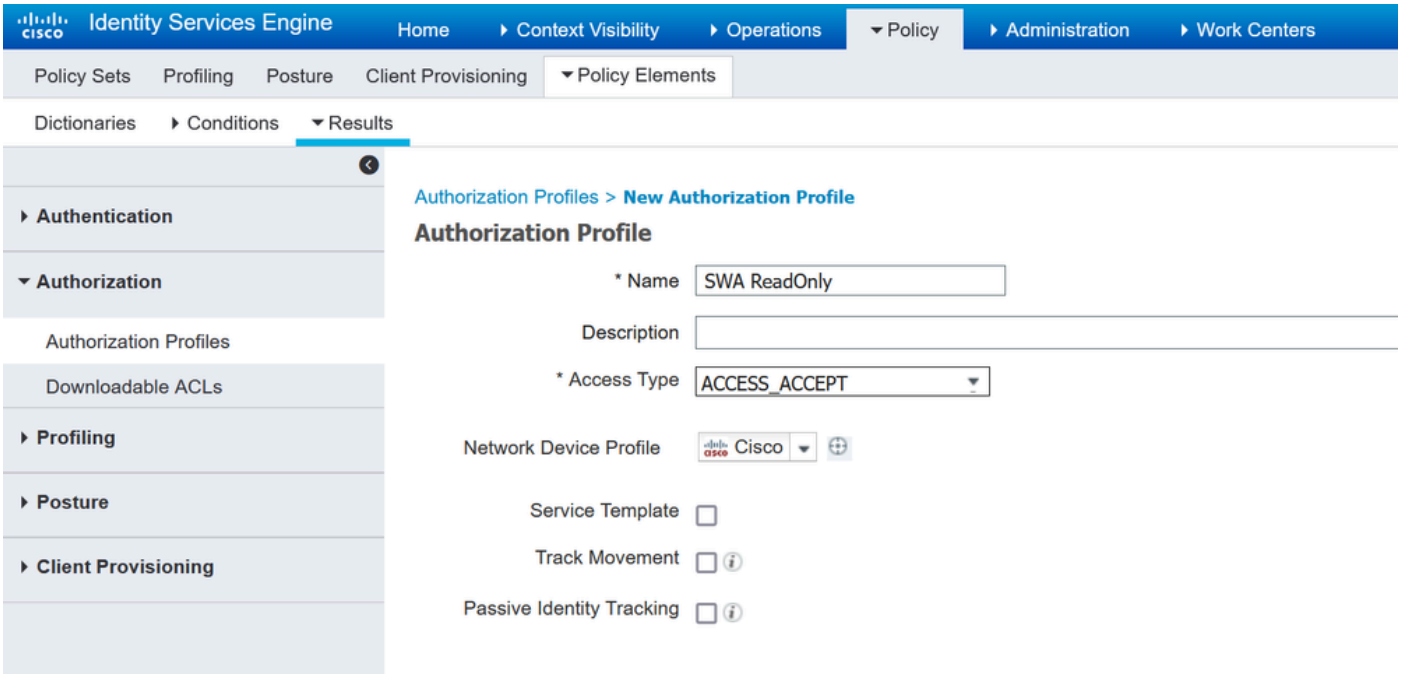
Autorisierungsprofil für Administratorbenutzer hinzufügen

Schritt 6.1: Navigieren Sie in den erweiterten Attributeinstellungen zu Radius > Class—[25], geben



Sie den Wert Administrator ein, und klicken Sie auf Submit (Senden). Add Authorization Profile for Admin Users (Autorisierungsprofil für Administratorbenutzer hinzufügen).

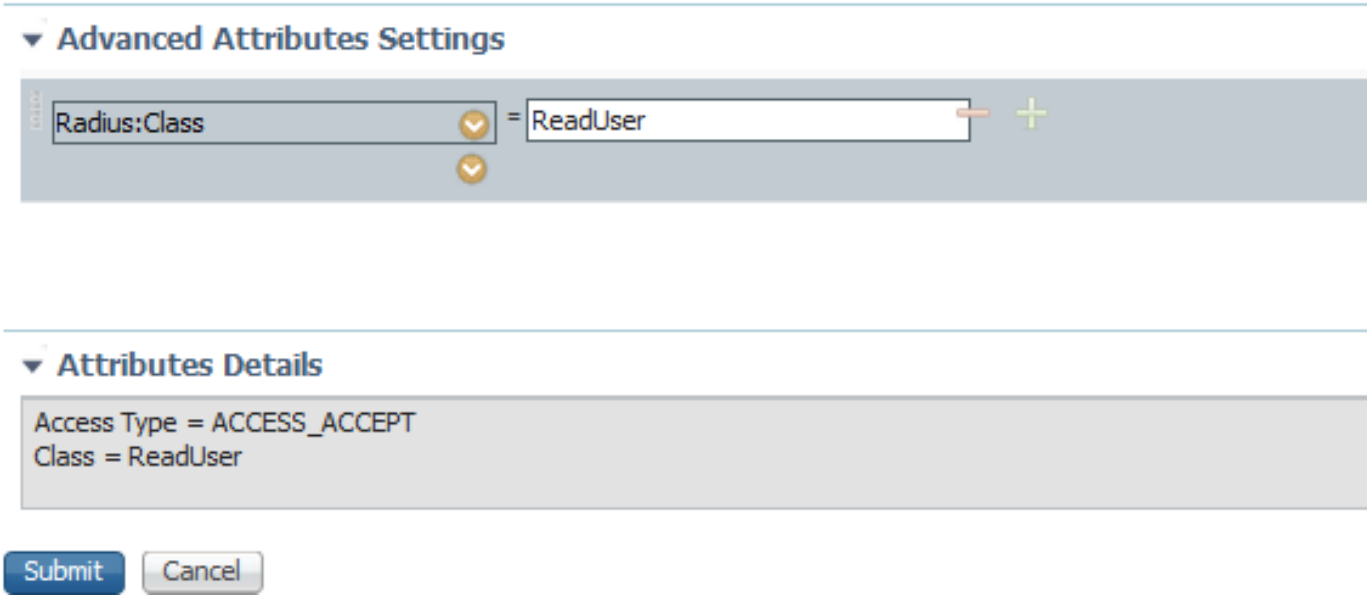
Schritt 7. Wiederholen Sie Schritt 6, um das Autorisierungsprofil für den schreibgeschützten Benutzer zu erstellen.



Autorisierungsprofil für schreibgeschützte Benutzer hinzufügen

SCHRITT 7.1: Erstellen Sie diesmal Radius:Class mit dem Wert ReadUser anstelle von

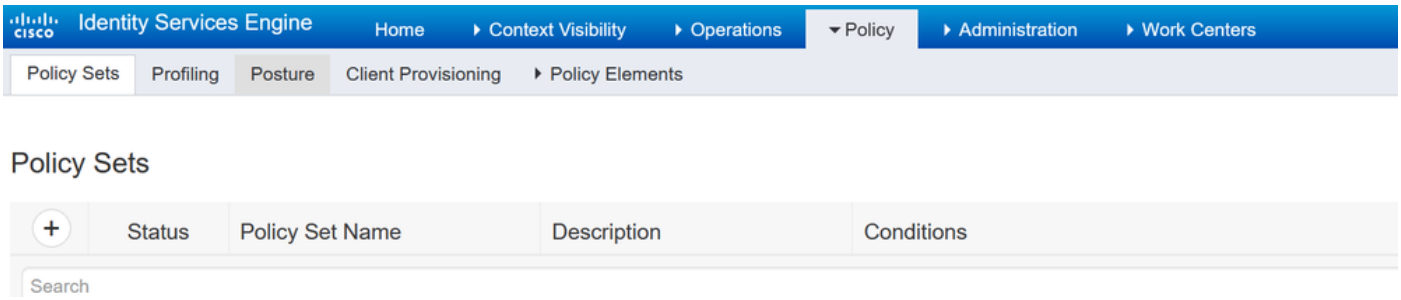
Administrator.



Autorisierungsprofil für schreibgeschützte Benutzer hinzufügen

Schritt 8: Erstellen Sie Richtliniensätze, die mit der SWA-IP-Adresse übereinstimmen. Dadurch wird der Zugriff auf andere Geräte mit diesen Benutzeranmeldeinformationen verhindert.

Navigieren Sie zu Policy > PolicySets, und klicken Sie in der linken oberen Ecke auf das Symbol +.

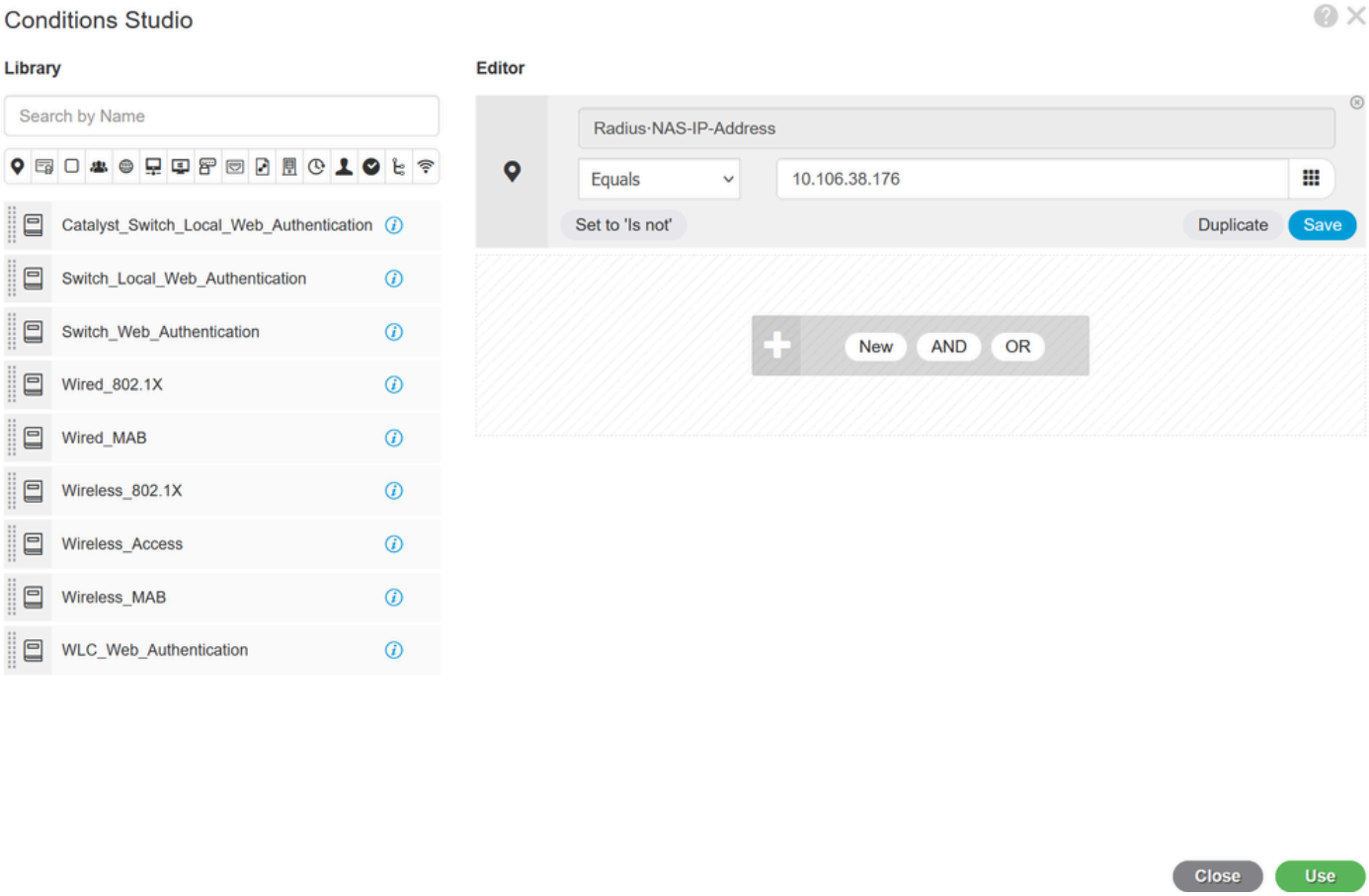


Richtliniensatz in ISE hinzufügen

Schritt 8.1: Eine neue Zeile wird oben in Ihren Richtliniensätzen platziert.

Geben Sie der neuen Richtlinie einen Namen, und fügen Sie eine Bedingung für das RADIUS NAS-IP-Address-Attribut hinzu, damit es mit der SWA-IP-Adresse übereinstimmt.

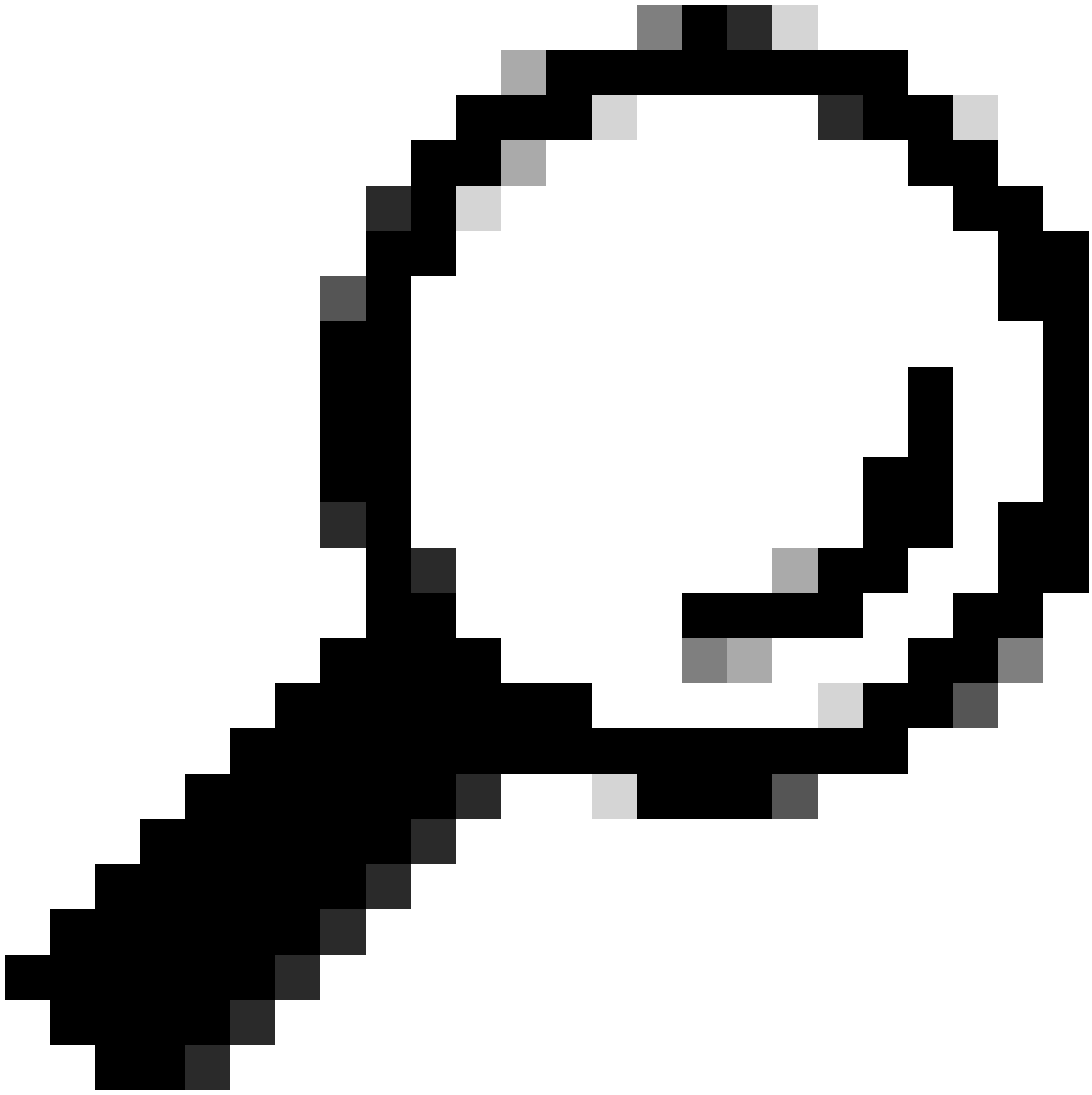
Klicken Sie auf Verwenden, um die Änderungen beizubehalten und den Editor zu beenden.



Hinzufügen einer Richtlinie zum Zuordnen eines SWA-Netzwerkgeräts

Schritt 8.2: Klicken Sie auf Speichern.

Richtlinie speichern

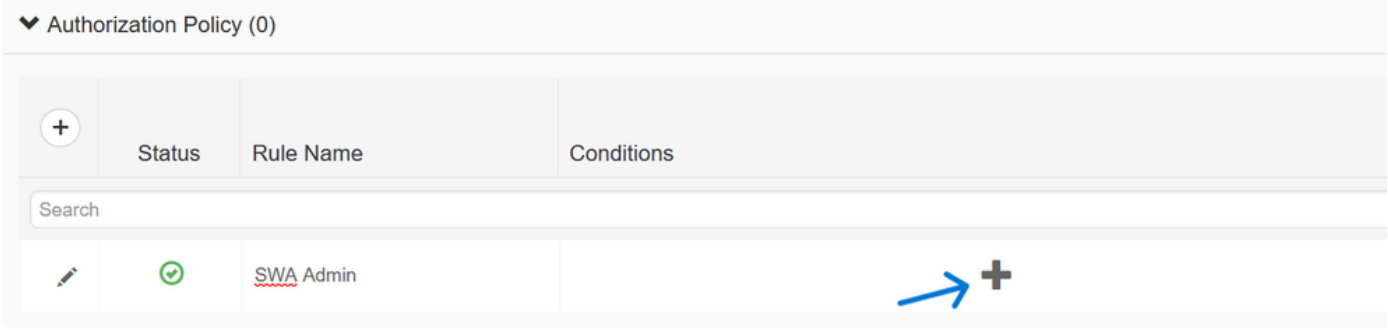


Tipp: In diesem Artikel ist die Liste der Standardprotokolle für den Netzwerkzugriff zulässig. Sie können eine neue Liste erstellen und diese nach Bedarf eingrenzen.

Schritt 9. Um die neuen Richtliniensätze anzuzeigen, klicken Sie in der Spalte Ansicht auf das Symbol >. Erweitern Sie das Menü Autorisierungsrichtlinie, und klicken Sie auf das Symbol +, um eine neue Regel hinzuzufügen, die den Zugriff für Benutzer mit Administratorrechten ermöglicht.

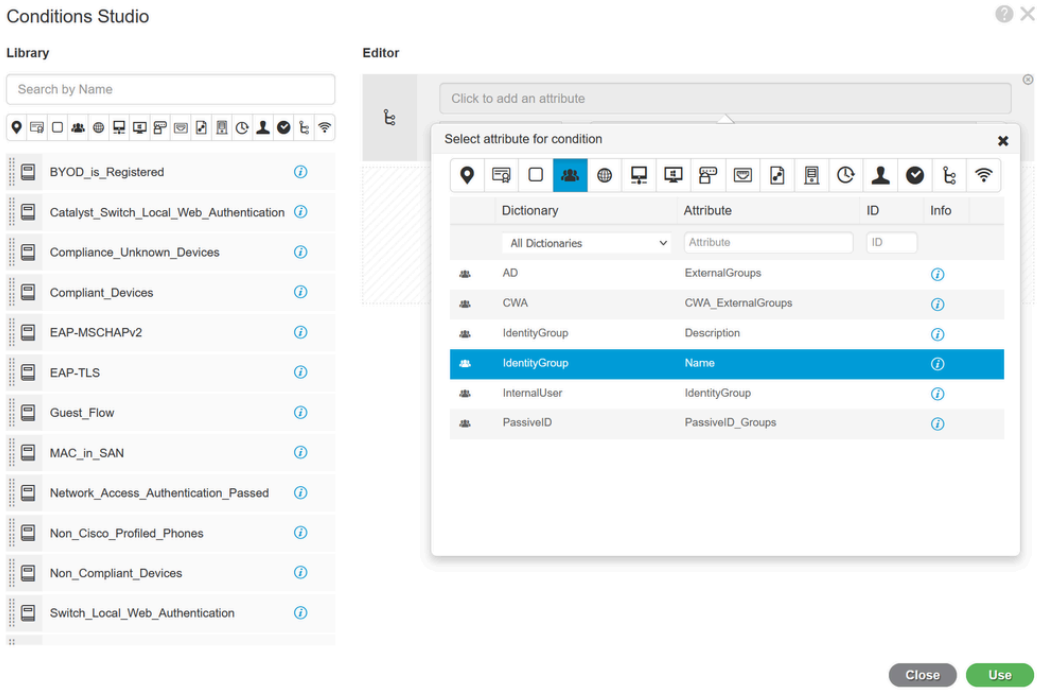
Legen Sie einen Namen fest.

Schritt 9.1: Um eine Bedingung zu erstellen, die mit der Admin-Benutzergruppe übereinstimmt, klicken Sie auf + Symbol



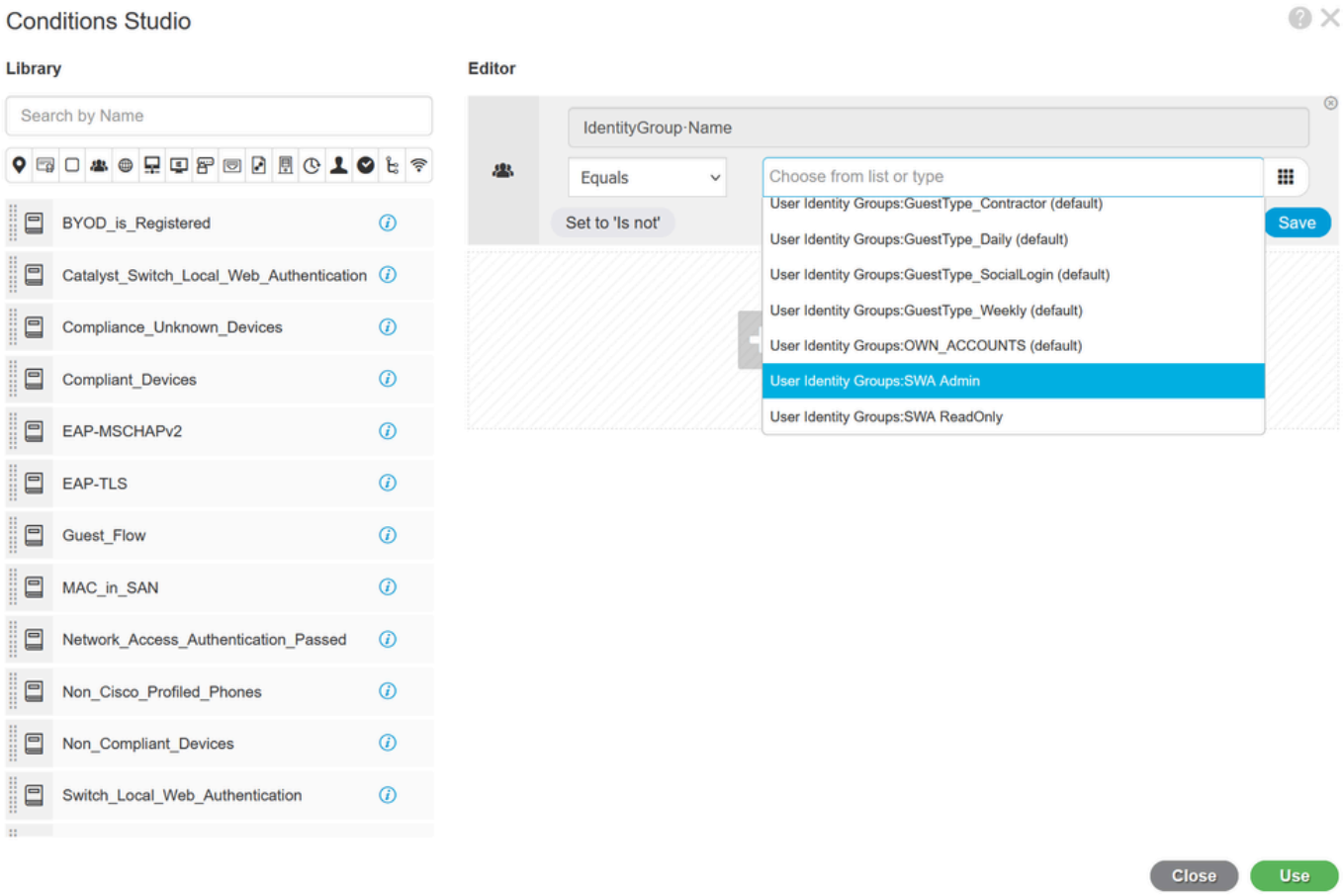
Autorisierungsrichtlinienbedingung hinzufügen

Schritt 9.2: Legen Sie die Bedingungen fest, die der Dictionary-Identitätsgruppe mit dem Attributnamen gleich den Benutzeridentitätsgruppen entsprechen: SWA admin.



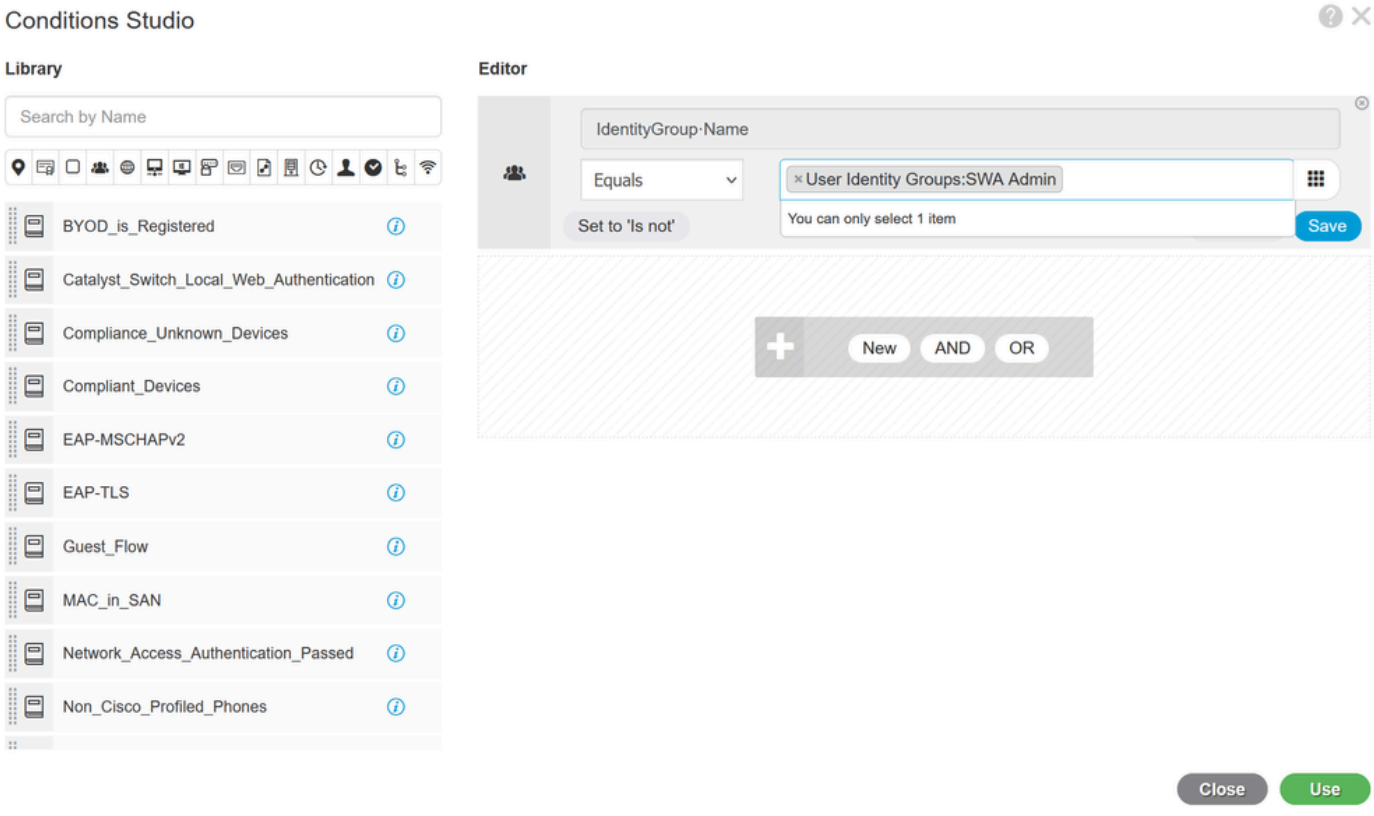
Identitätsgruppe als Bedingung auswählen

Schritt 9.3: Blättern Sie nach unten, und wählen Sie Benutzeridentitätsgruppen: SWA admin.



Blättern Sie nach unten und wählen Sie Identitätsgruppenname aus.

Schritt 9.4: Klicken Sie auf Verwenden.

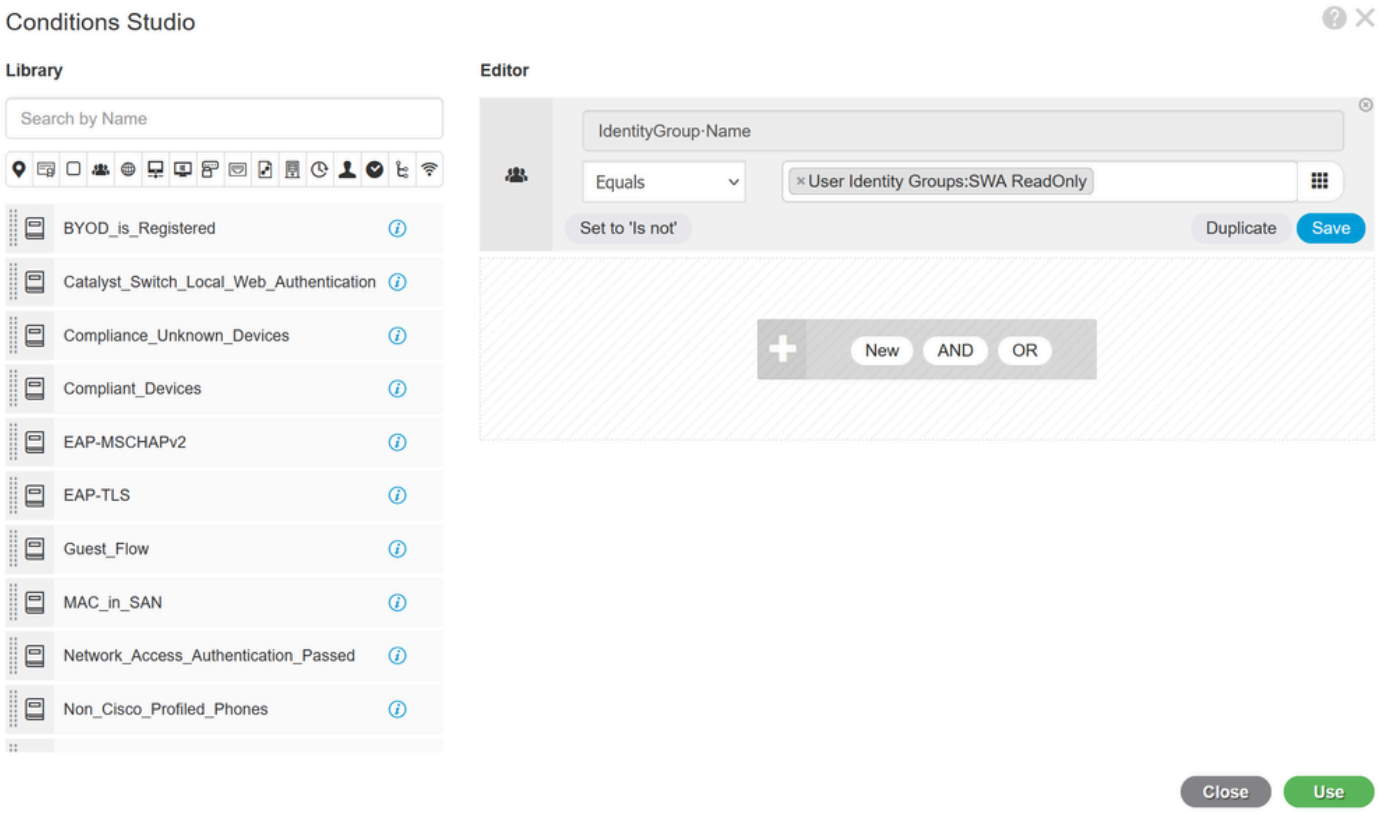


Autorisierungsrichtlinie für SWA-Admin-Benutzergruppe auswählen

Schritt 10. Klicken Sie auf das Symbol +, um eine zweite Regel hinzuzufügen, um Benutzern mit schreibgeschützten Rechten den Zugriff zu gestatten.

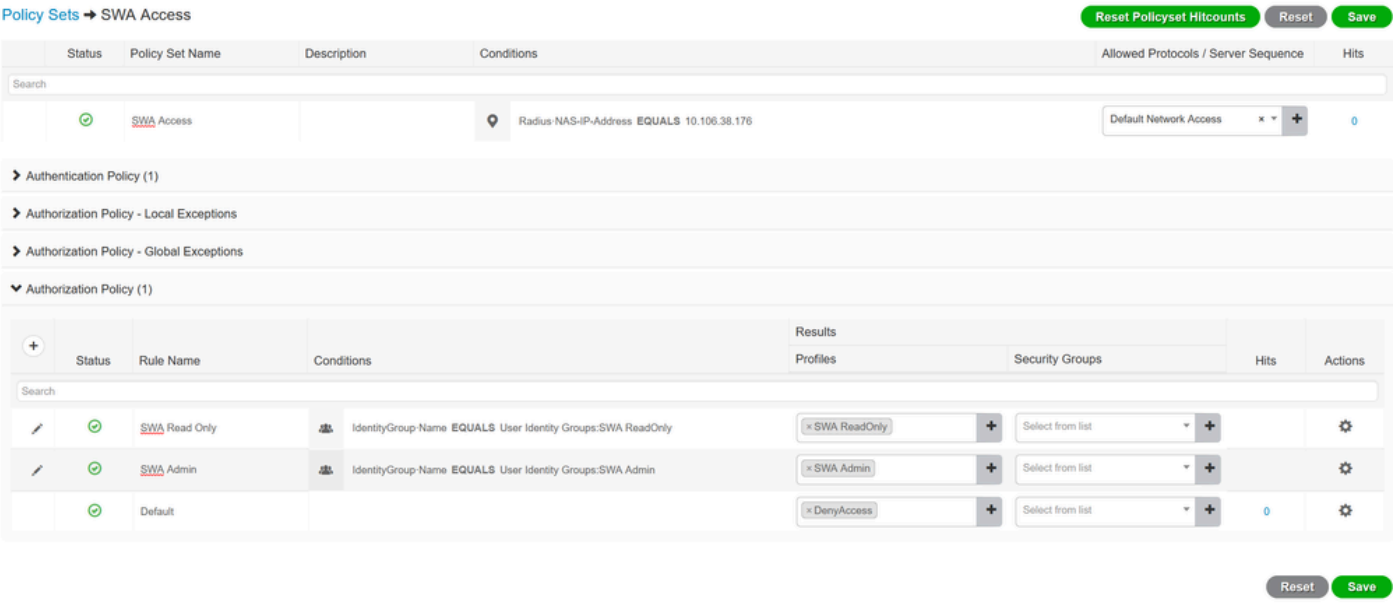
Legen Sie einen Namen fest.

Legen Sie die Bedingungen fest, die der Dictionary-Identitätsgruppe mit dem Attributnamen gleich den Benutzeridentitätsgruppen: SWA ReadOnly (Nur SWA lesen) entsprechen, und klicken Sie auf Verwenden.



Autorisierungsrichtlinie für schreibgeschützte Benutzergruppe auswählen

Schritt 11. Legen Sie das Autorisierungsprofil für jede Regel fest, und klicken Sie auf Speichern.

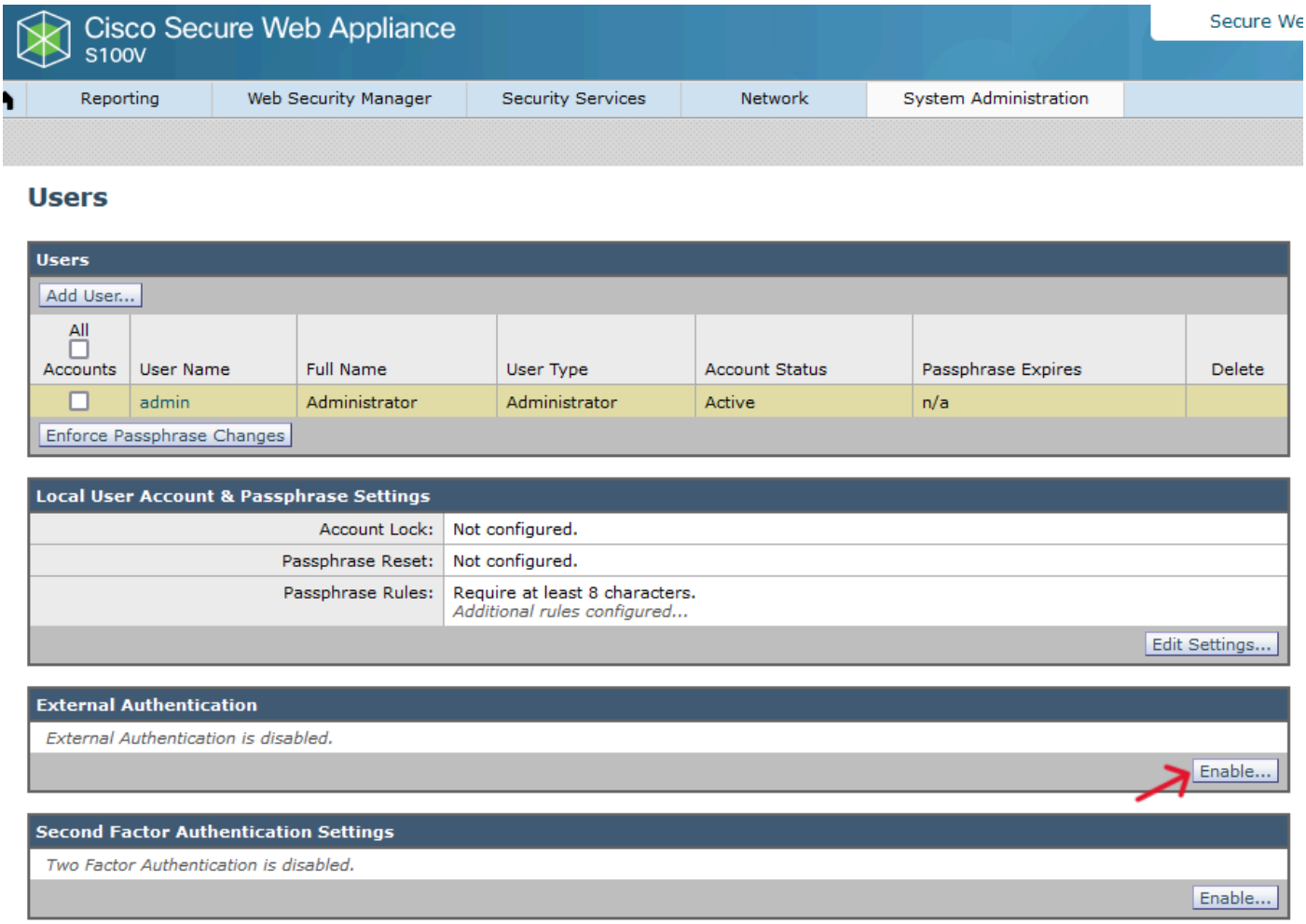


Autorisierungsprofil auswählen

SWA-Konfiguration

Schritt 1: Navigieren Sie in der SWA-GUI zu Systemverwaltung, und klicken Sie auf Benutzer.

Schritt 2: Klicken Sie in Externe Authentifizierung auf Aktivieren.



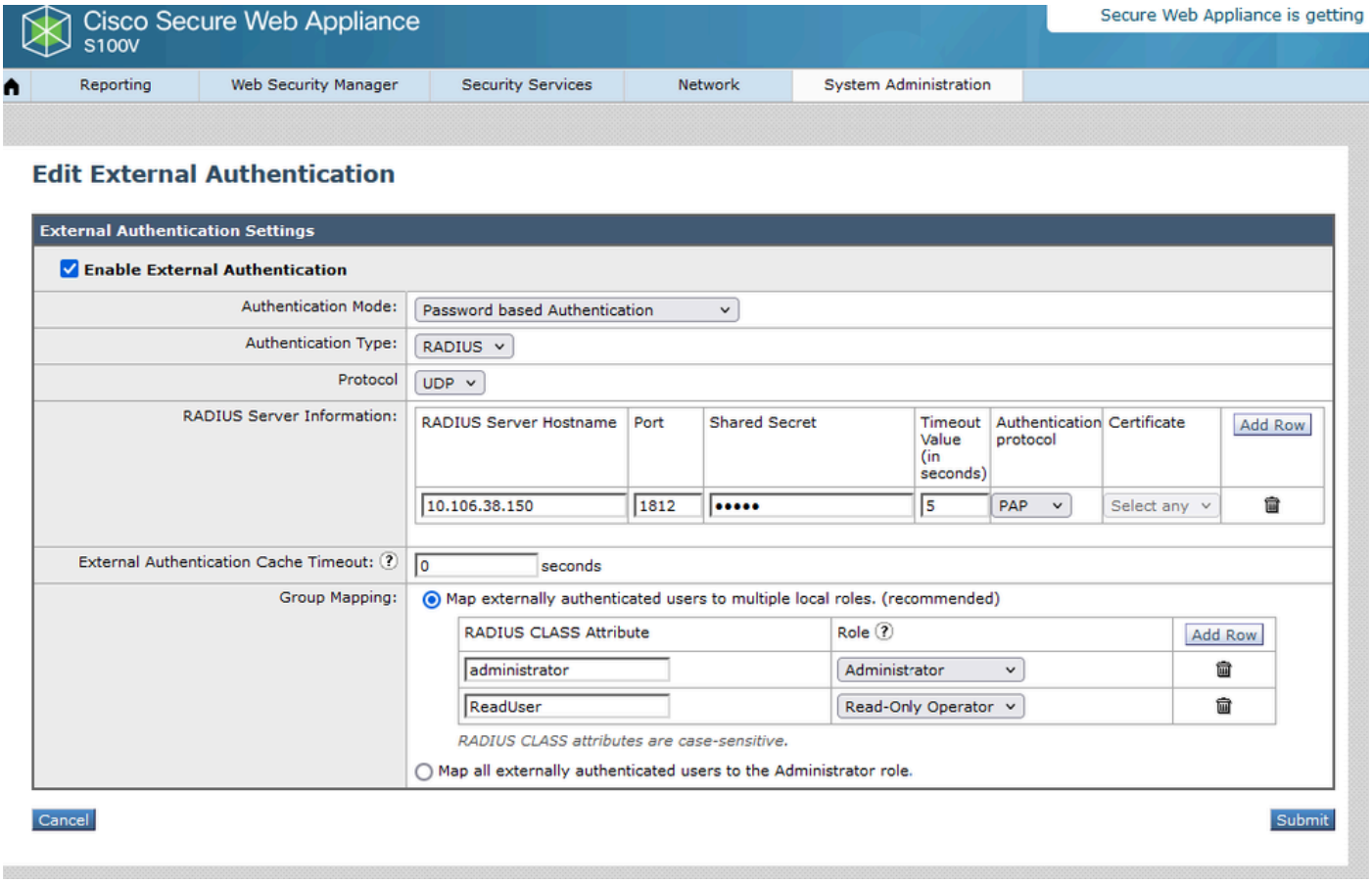
Externe Authentifizierung in SWA aktivieren

Schritt 3: Geben Sie die IP-Adresse oder den FQDN der ISE in das Feld RADIUS Server Hostname ein, und geben Sie den gleichen Shared Secret ein, der in Schritt 2, ISE-Konfiguration, konfiguriert wurde.

Schritt 4: Wählen Sie Extern authentifizierte Benutzer mehreren lokalen Rollen in der Gruppenzuordnung zuordnen.

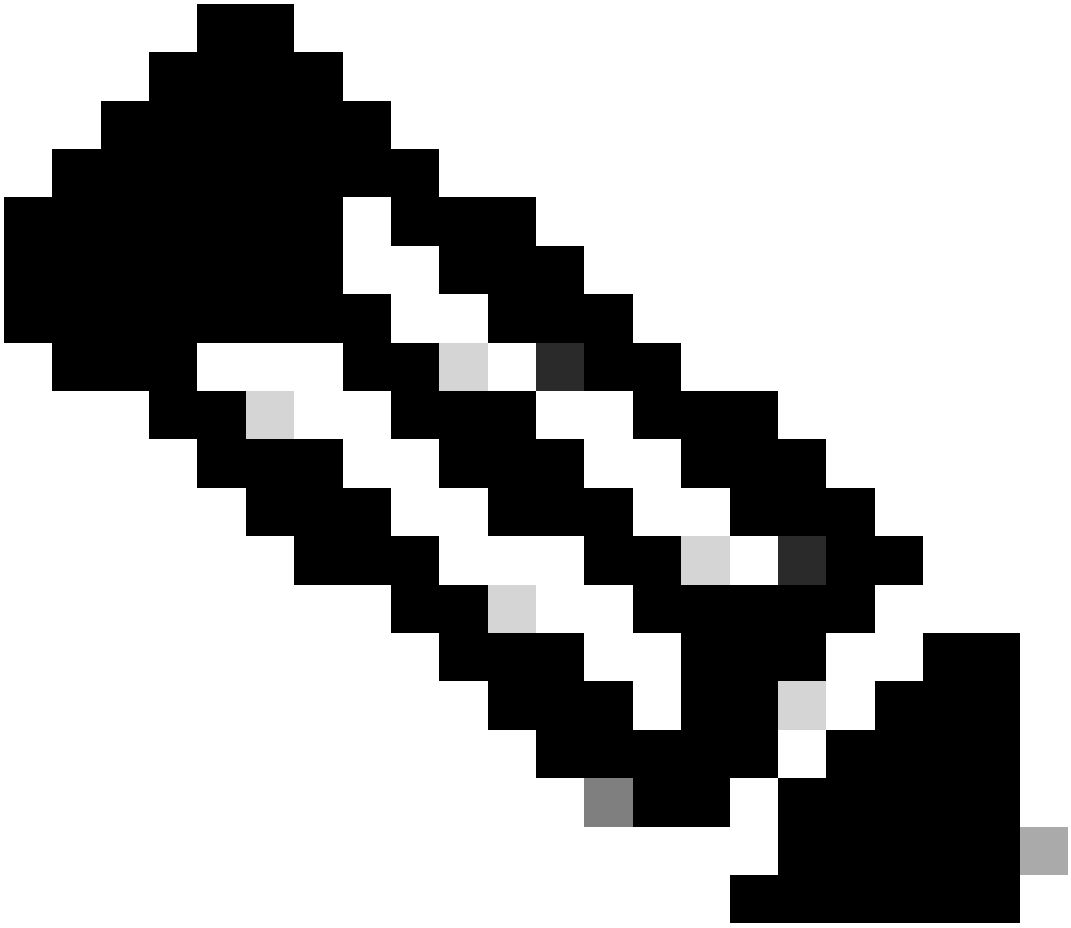
Schritt 4.1: Geben Sie Administrator in das Feld RADIUS CLASS Attribute ein, und wählen Sie Role Administrator aus.

Schritt 4.2: Geben Sie ReadUser in das Feld RADIUS CLASS Attribute ein, und wählen Sie den Role Read-Only Operator aus.

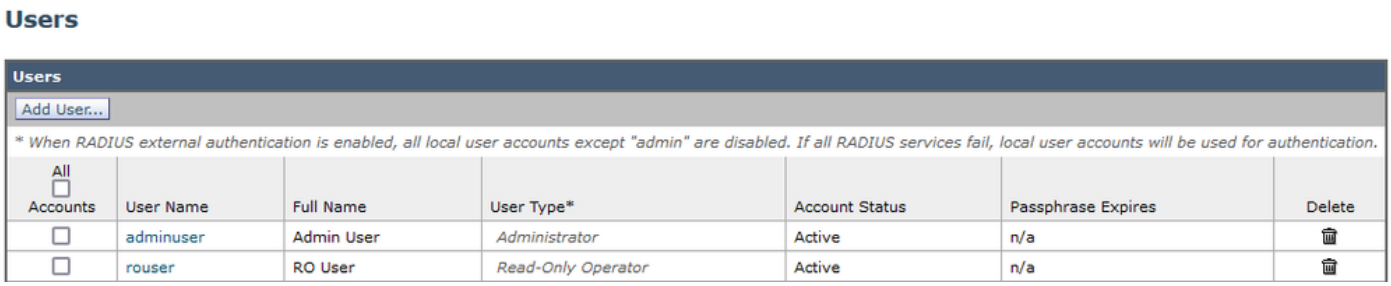


Konfiguration für die externe Authentifizierung für RADIUS-Server

Schritt 5: Um Benutzer in SWA zu konfigurieren, klicken Sie auf Benutzer hinzufügen. Geben Sie den Benutzernamen ein, und wählen Sie den für die gewünschte Rolle erforderlichen Benutzertyp aus. Geben Sie die Passphrase ein, und geben Sie sie erneut ein. Dies ist für den GUI-Zugriff erforderlich, wenn die Appliance keine Verbindung zu einem externen RADIUS-Server herstellen kann.



Hinweis: Wenn die Appliance keine Verbindung zu einem externen Server herstellen kann, versucht sie, den Benutzer als lokalen Benutzer zu authentifizieren, der auf der sicheren Webappliance definiert ist.

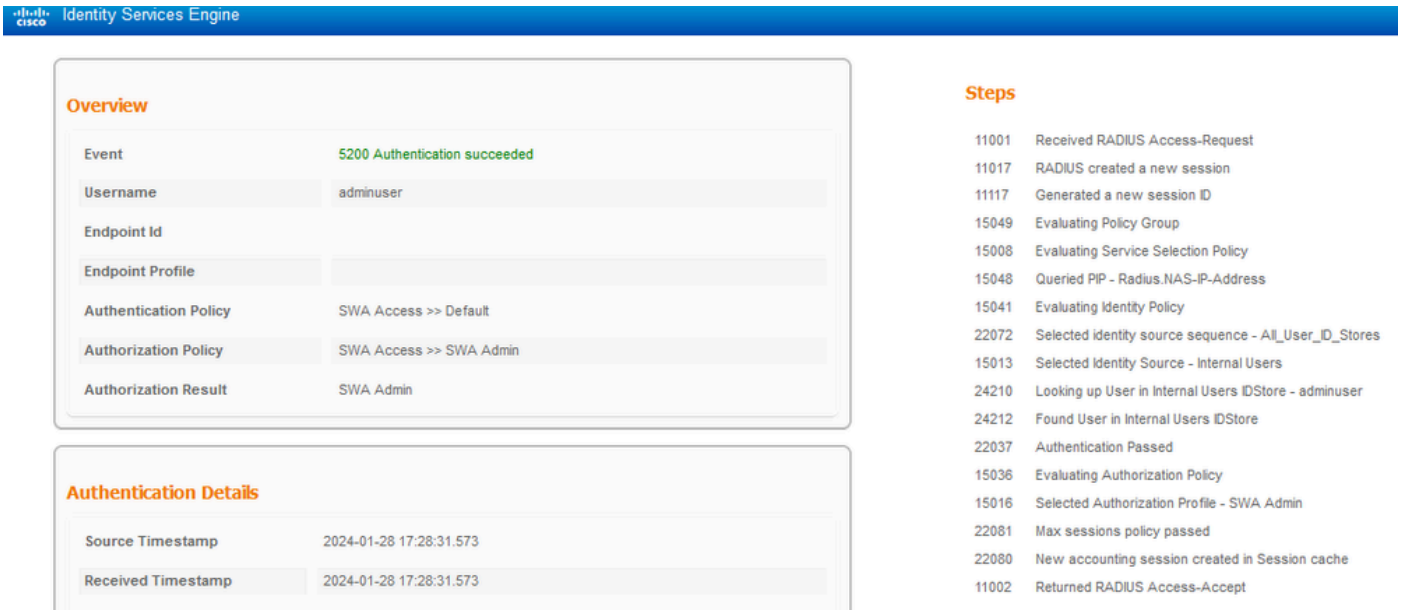


Benutzerkonfiguration in SWA

Schritt 6: Klicken Sie auf Senden und Änderungen bestätigen.

Überprüfung

Zugriff auf die SWA-GUI mit den konfigurierten Benutzeranmeldeinformationen und Überprüfung der Live-Protokolle in der ISE Um die Live-Protokolle in der ISE zu überprüfen, navigieren Sie zu Operations > Live Logs:



Benutzeranmeldung bei ISE überprüfen

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 14.0 für Cisco Secure Web Appliance
- ISE 3.0 - Administratorhandbuch
- ISE-Kompatibilitätsmatrix für Secure Web Appliance
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

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