Konfigurieren der SWA Second Factor-Authentifizierung mit der ISE als RADIUS-Server

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Authentifizierung des zweiten Faktors auf einer sicheren Web-Appliance mit der Cisco Identity Service Engine als RADIUS-Server konfigurieren.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse in SWA.
- Kenntnis der Konfiguration von Authentifizierungs- und Autorisierungsrichtlinien auf der ISE
- Grundlegendes RADIUS-Wissen

Cisco empfiehlt außerdem Folgendes:

- Administrationszugriff über die Secure Web Appliance (SWA) und die Cisco Identity Service Engine (ISE).
- Ihre ISE ist in Active Directory oder LDAP integriert.
- Active Directory oder LDAP wird mit dem Benutzernamen "admin" konfiguriert, um das SWA-Standardkonto "admin" zu authentifizieren.
- 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 zweite Faktor-Authentifizierung für administrative Benutzer auf SWA aktivieren, überprüft das Gerät nach der Überprüfung der in SWA konfigurierten Anmeldeinformationen die Benutzeranmeldeinformationen beim RADIUS-Server zum zweiten Mal.

Netzwerktopologie

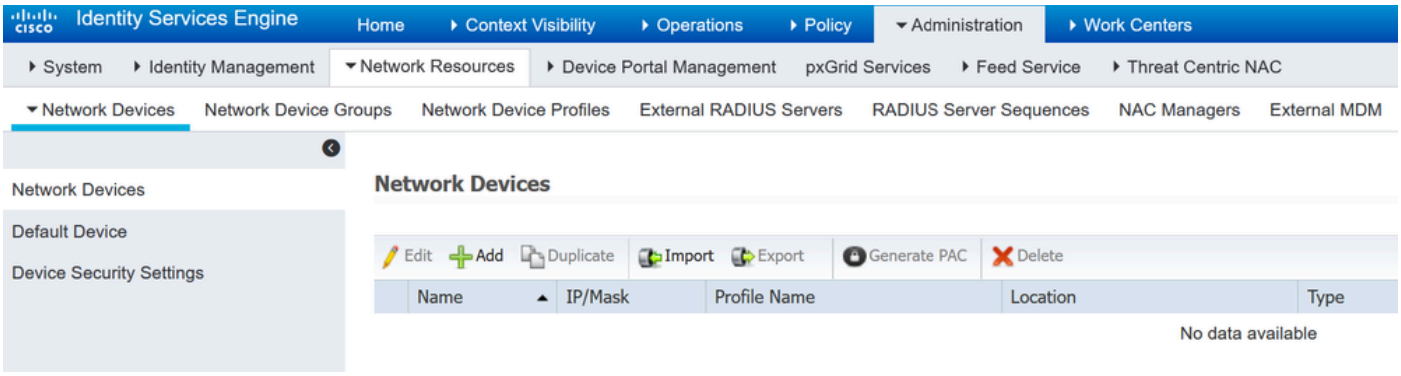
Bild - Netzwerktopologie-Diagramm

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

Konfigurationsschritte

ISE-Konfiguration

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



SWA als Netzwerkgerät in der ISE hinzufügen

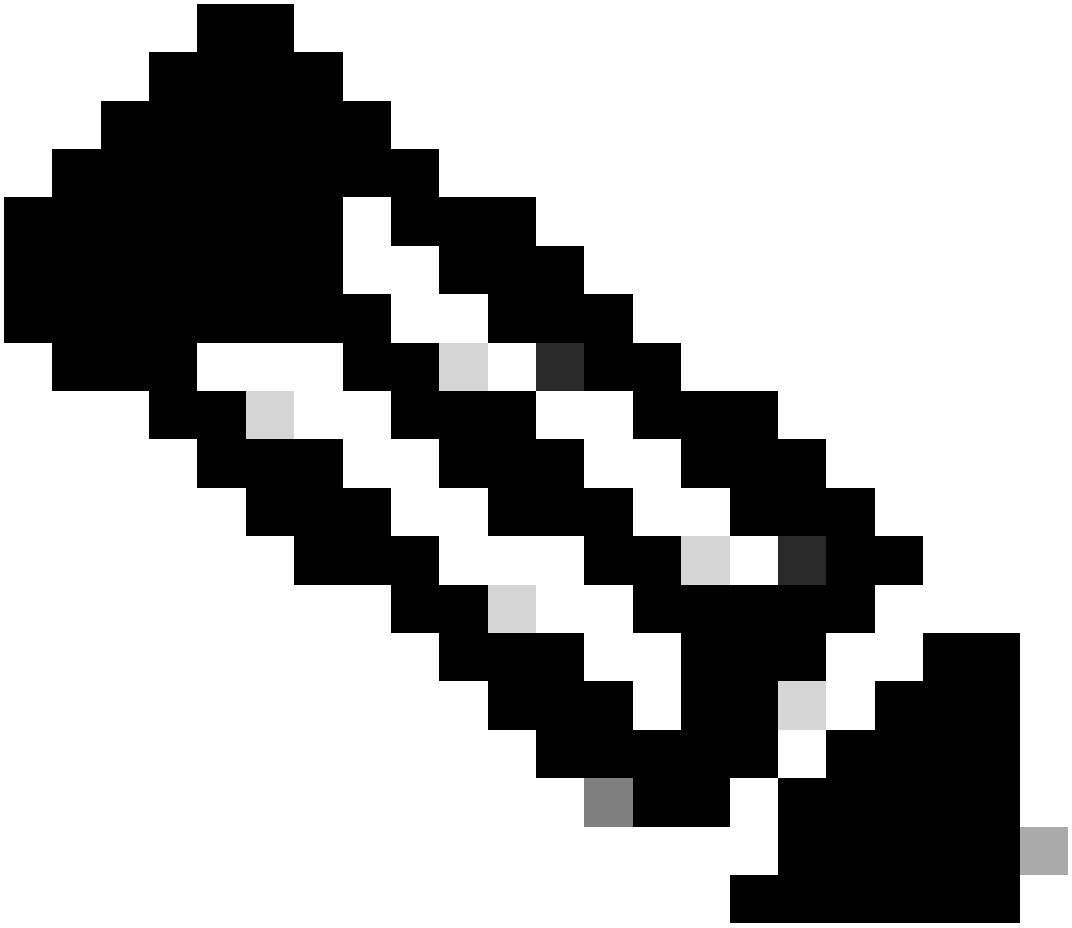
Schritt 2: Konfigurieren von Netzwerkgeräten in der ISE

Schritt 2.1: Weisen Sie dem Netzwerkgeräteobjekt einen Namen zu.

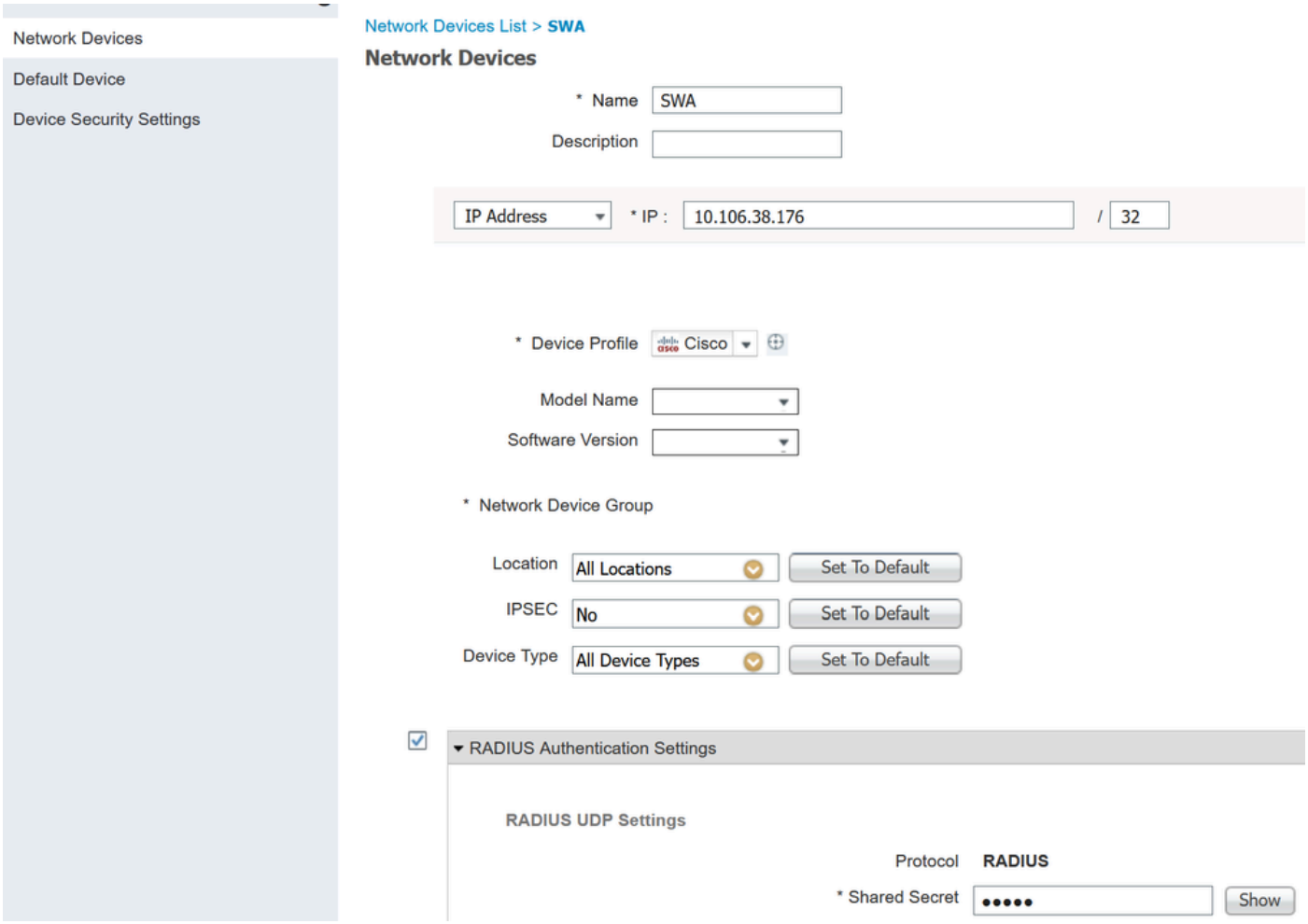
Schritt 2.2: Geben Sie die SWA-IP-Adresse ein.

Schritt 2.3: Aktivieren Sie das Kontrollkästchen RADIUS.

Schritt 2.4: Definieren Sie einen gemeinsamen geheimen Schlüssel.

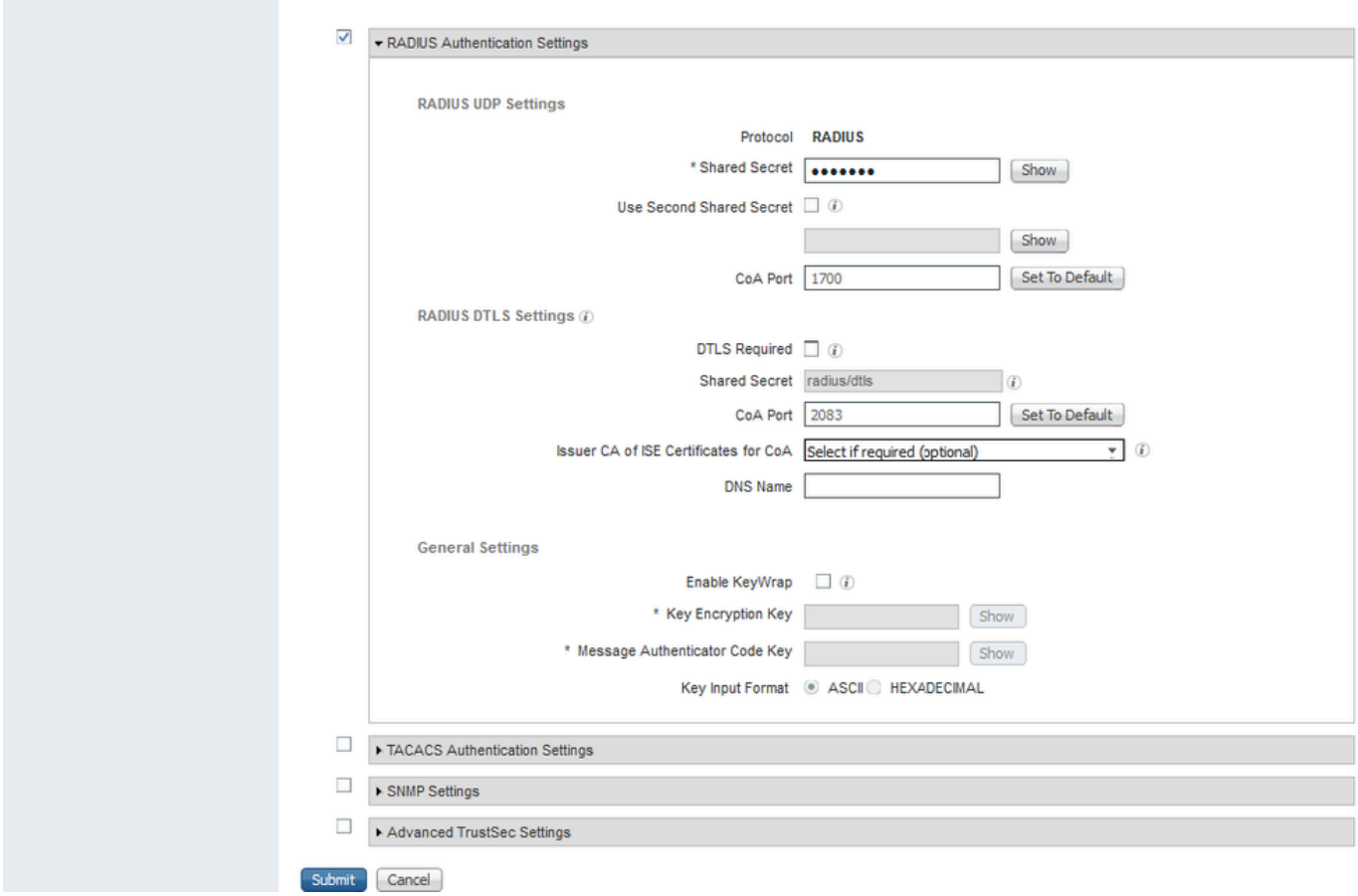


Hinweis: Derselbe Schlüssel muss später zur Konfiguration der SWA verwendet werden.



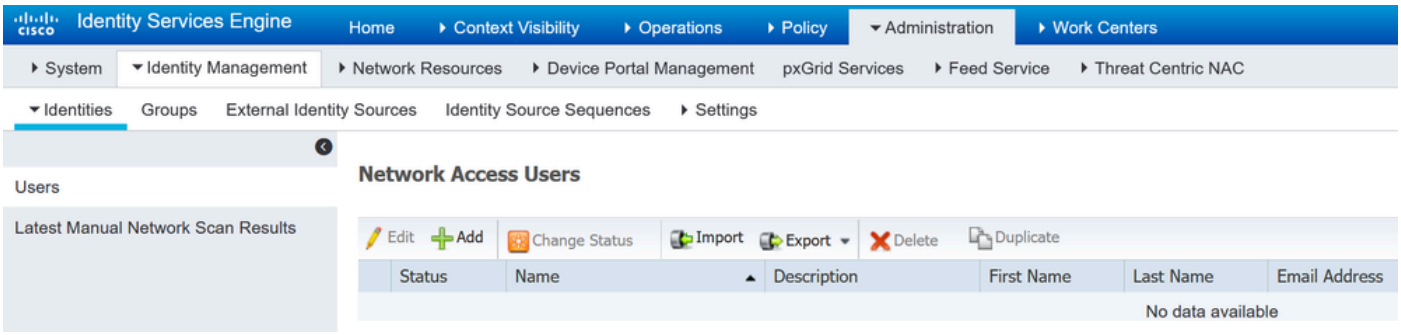
Gemeinsamer SWA-Schlüssel für Netzwerkgerät konfigurieren

Schritt 2.5: Klicken Sie auf Senden.



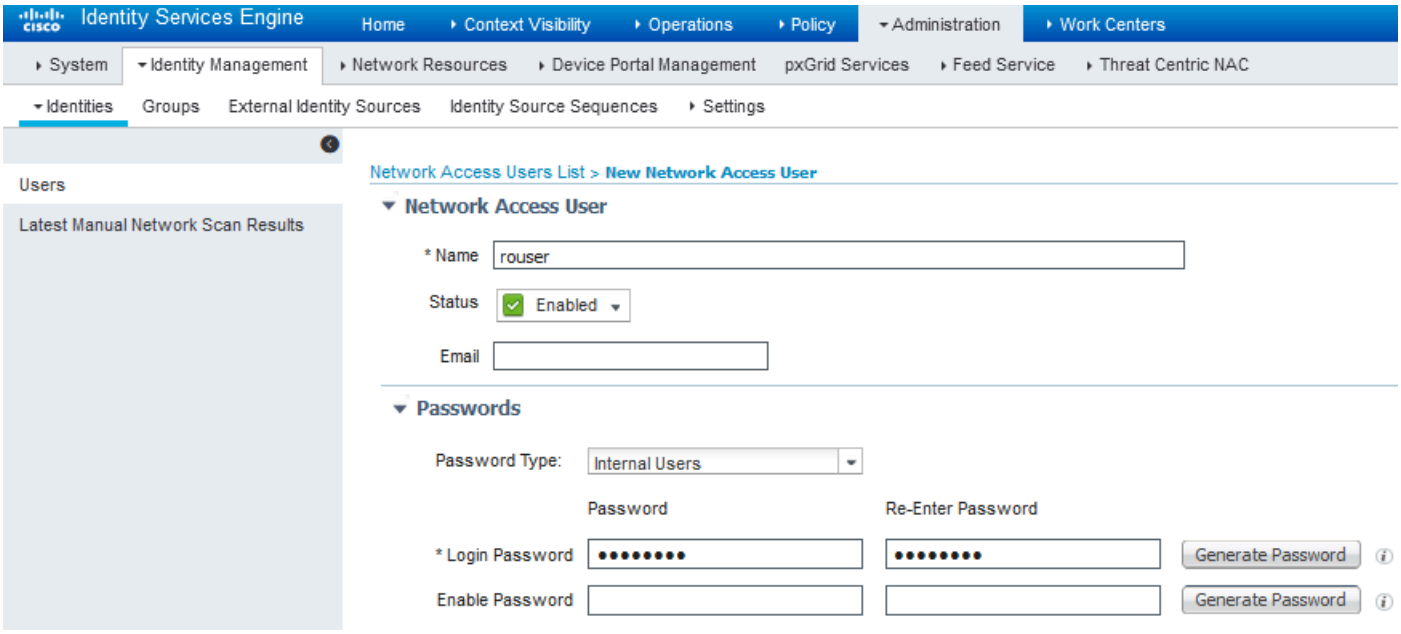
Konfiguration des Netzwerkgeräts senden

Schritt 3: Sie müssen Netzwerkzugriffsbenutzer erstellen, die mit dem in SWA konfigurierten Benutzernamen übereinstimmen. Navigieren Sie zu Administration > Identity Management > Identities > + Add.



Hinzufügen lokaler Benutzer zur ISE

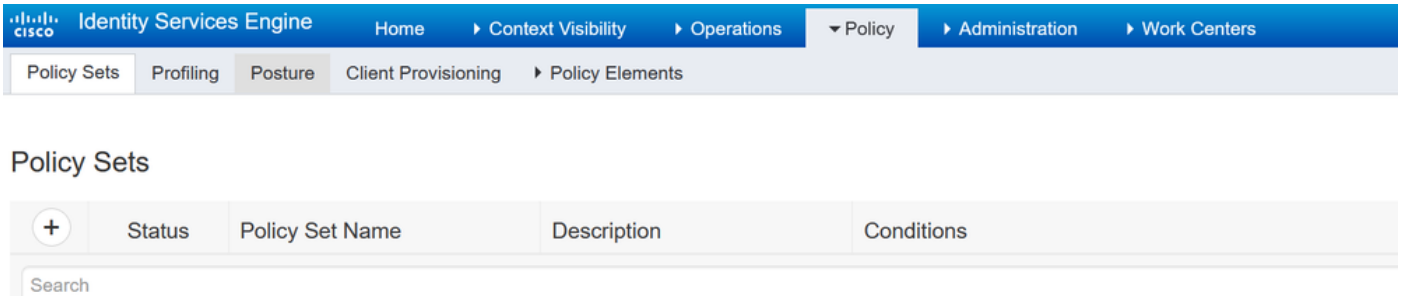
Schritt 3.1: Weisen Sie einen Namen zu.
Schritt 3.2. (Optional) Geben Sie die E-Mail-Adresse des Benutzers ein.
Schritt 3.3: Passwort festlegen.
Schritt 3.4: Klicken Sie auf Speichern.



Hinzufügen eines lokalen Benutzers zur ISE

Schritt 4: Erstellen Sie einen Richtliniensatz, der der SWA-IP-Adresse entspricht. 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 +.

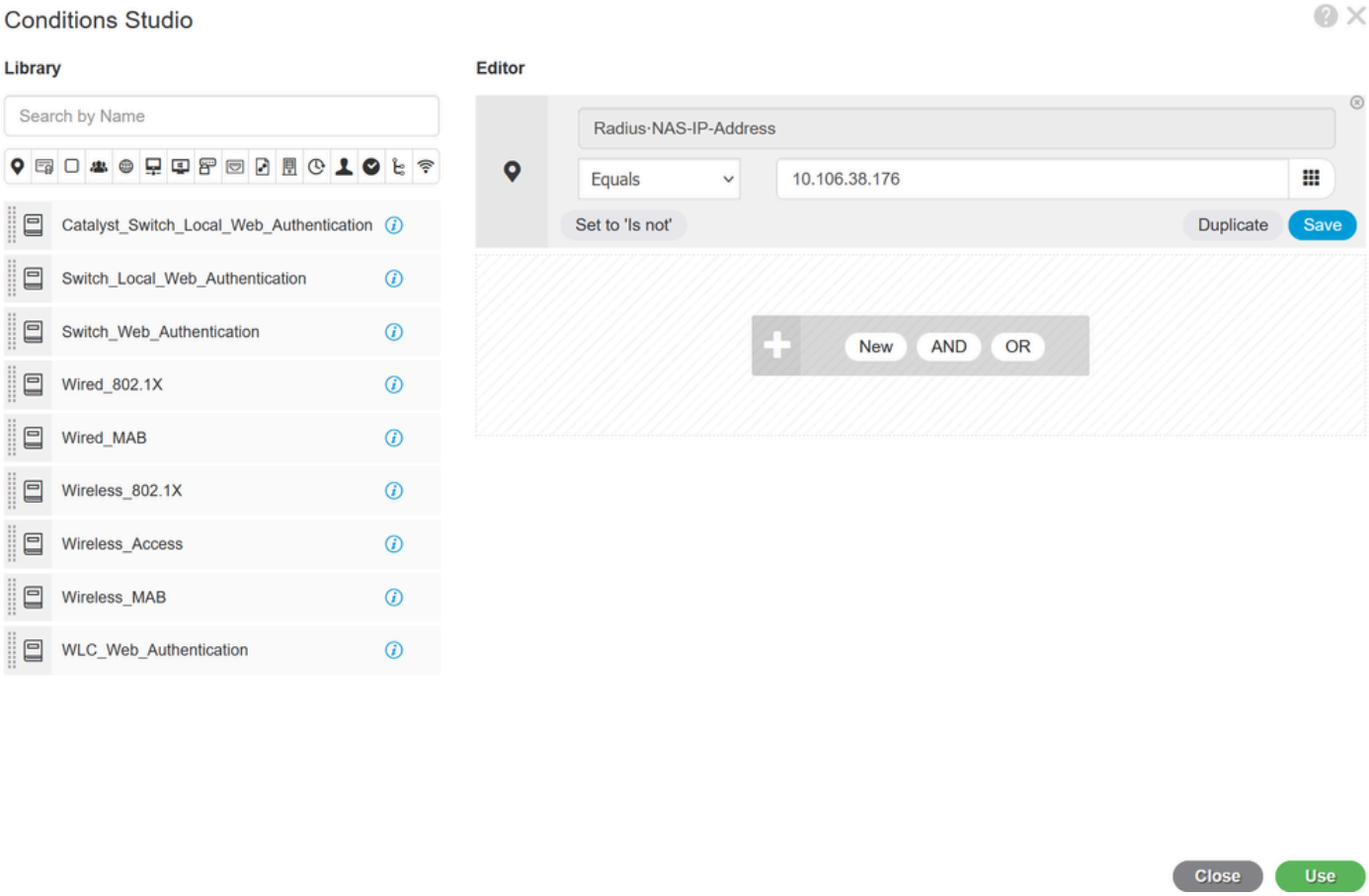


Richtliniensatz in ISE hinzufügen

Schritt 4.1: Eine neue Zeile wird oben in Ihren Richtliniensätzen platziert. Geben Sie einen Namen für die neue Richtlinie ein.

Schritt 4.2: Fügen Sie eine Bedingung für das RADIUS NAS-IP-Address-Attribut hinzu, damit es mit der SWA-IP-Adresse übereinstimmt.

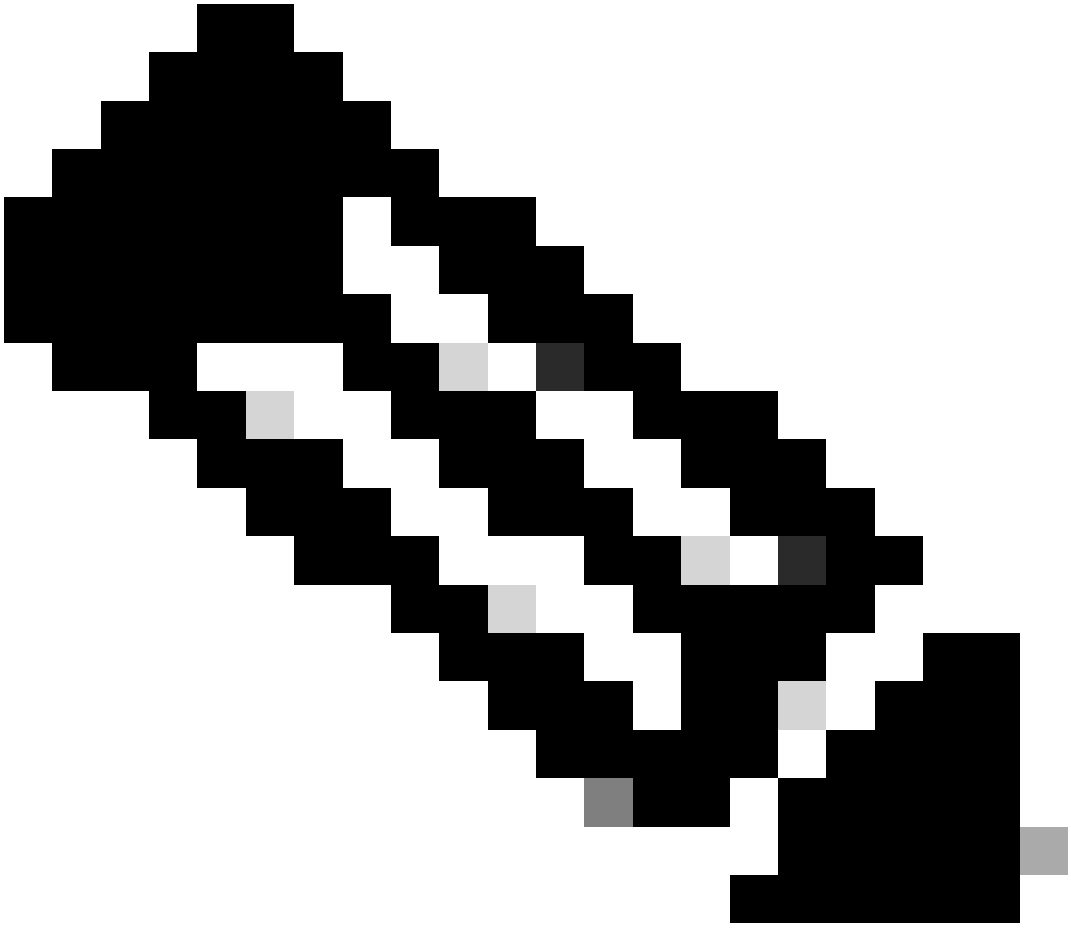
Schritt 4.3: Klicken Sie auf Verwenden, um die Änderungen beizubehalten und den Editor zu beenden.



Hinzufügen einer Richtlinie zum Zuordnen eines SWA-Netzwerkgeräts

Schritt 4.4: Klicken Sie auf Speichern.

Richtlinie speichern



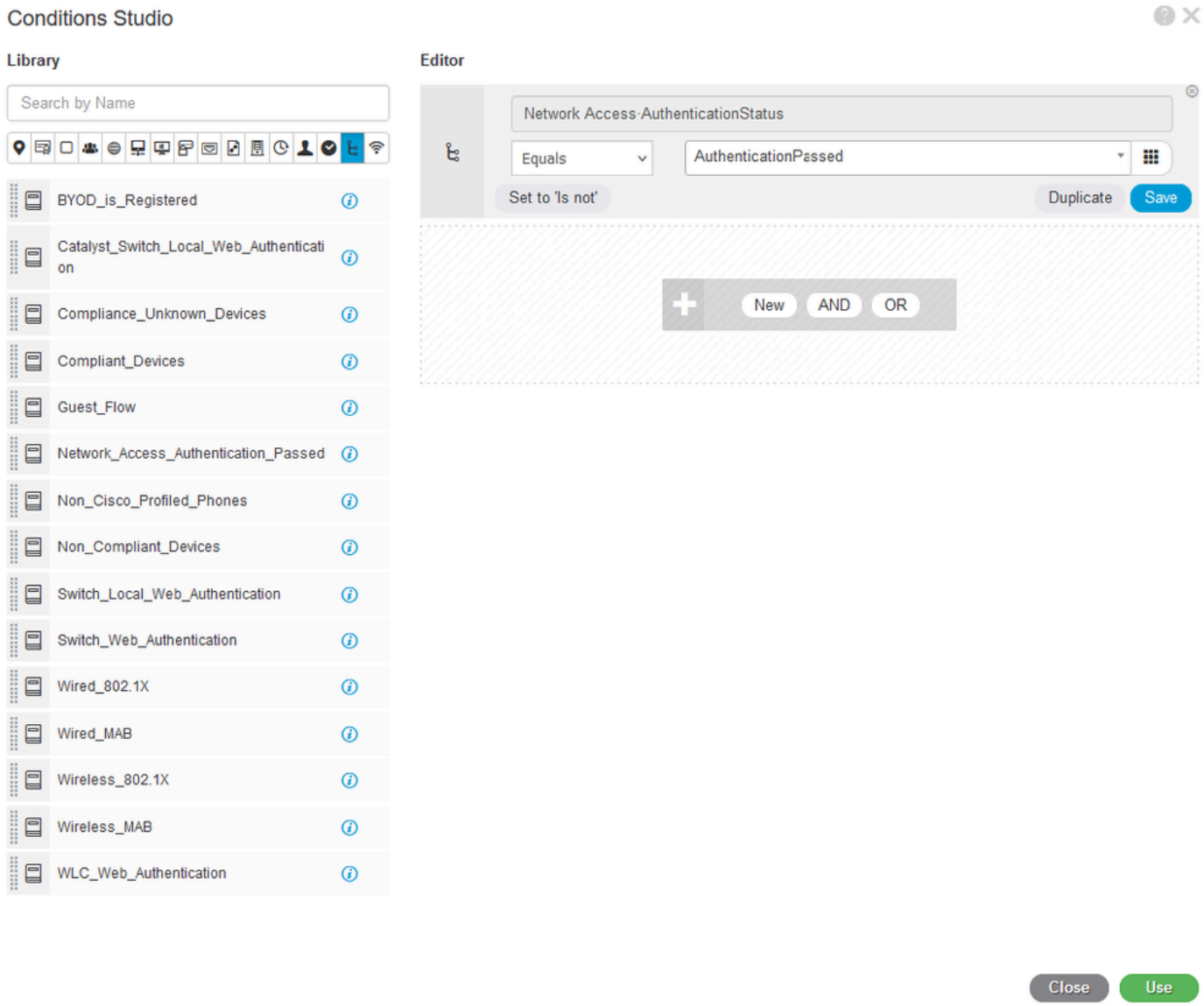
Hinweis: In diesem Beispiel wurde die Liste der Standardprotokolle für den Netzwerkzugriff zugelassen. Sie können eine neue Liste erstellen und sie nach Bedarf eingrenzen.

Schritt 5: Um die neuen Richtliniensätze anzuzeigen, klicken Sie in der Spalte Ansicht auf das Symbol ">".

Schritt 5.1: Erweitern Sie das Menü Authorization Policy (Autorisierungsrichtlinie), und klicken Sie auf das +-Symbol, um eine neue Regel hinzuzufügen, die den Zugriff für alle authentifizierten Benutzer ermöglicht.

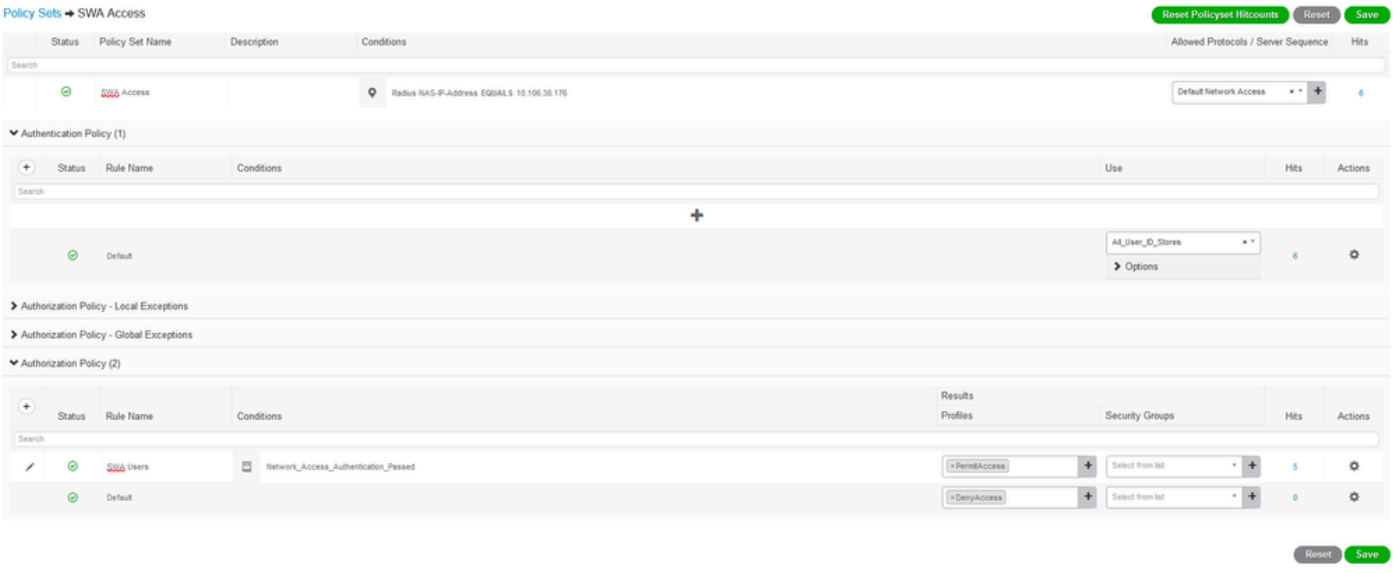
Schritt 5.2: Legen Sie einen Namen fest.

Schritt 5.3: Legen Sie die Bedingungen fest, die dem Dictionary Network Access mit dem Attribut AuthenticationStatus gleich AuthenticationPassed entsprechen, und klicken Sie auf Use (Verwenden).



Autorisierungsbedingung auswählen

Schritt 6: Legen Sie PermitAccess als Autorisierungsprofil fest, und klicken Sie auf Speichern.

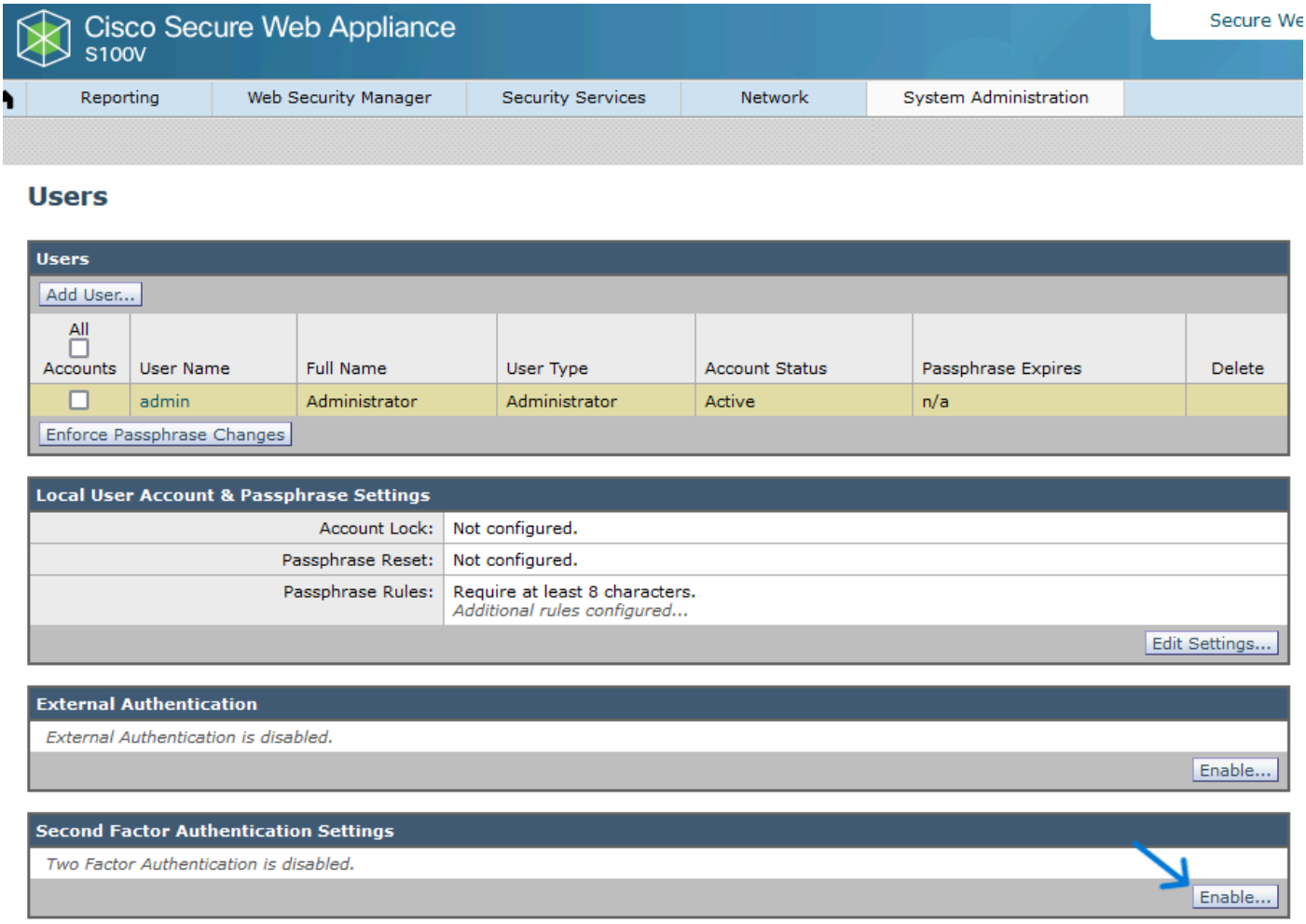


Autorisierungsprofil auswählen

SWA-Konfiguration

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

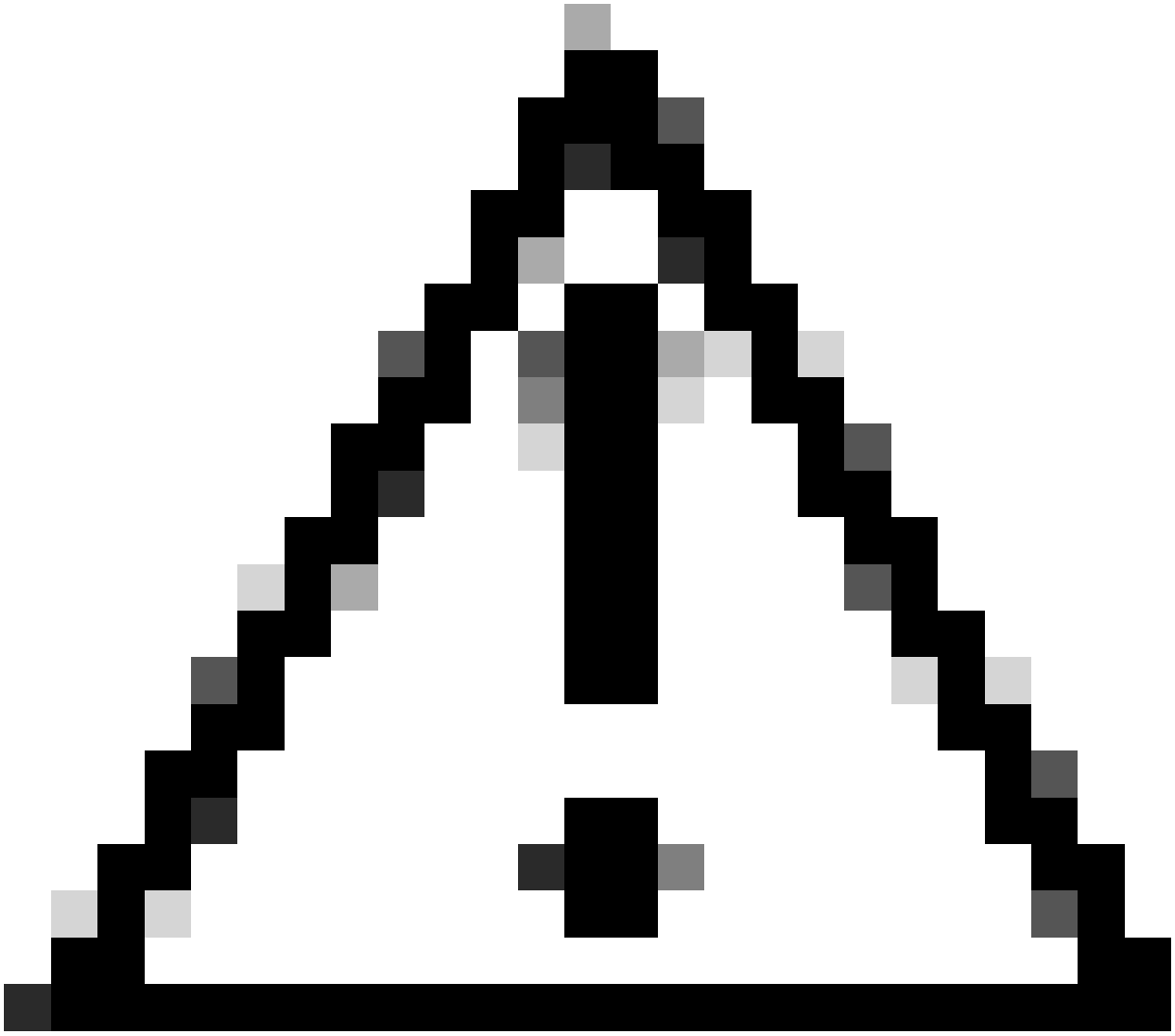
Schritt 2: Klicken Sie in den Second Factor Authentication-Einstellungen auf Aktivieren.



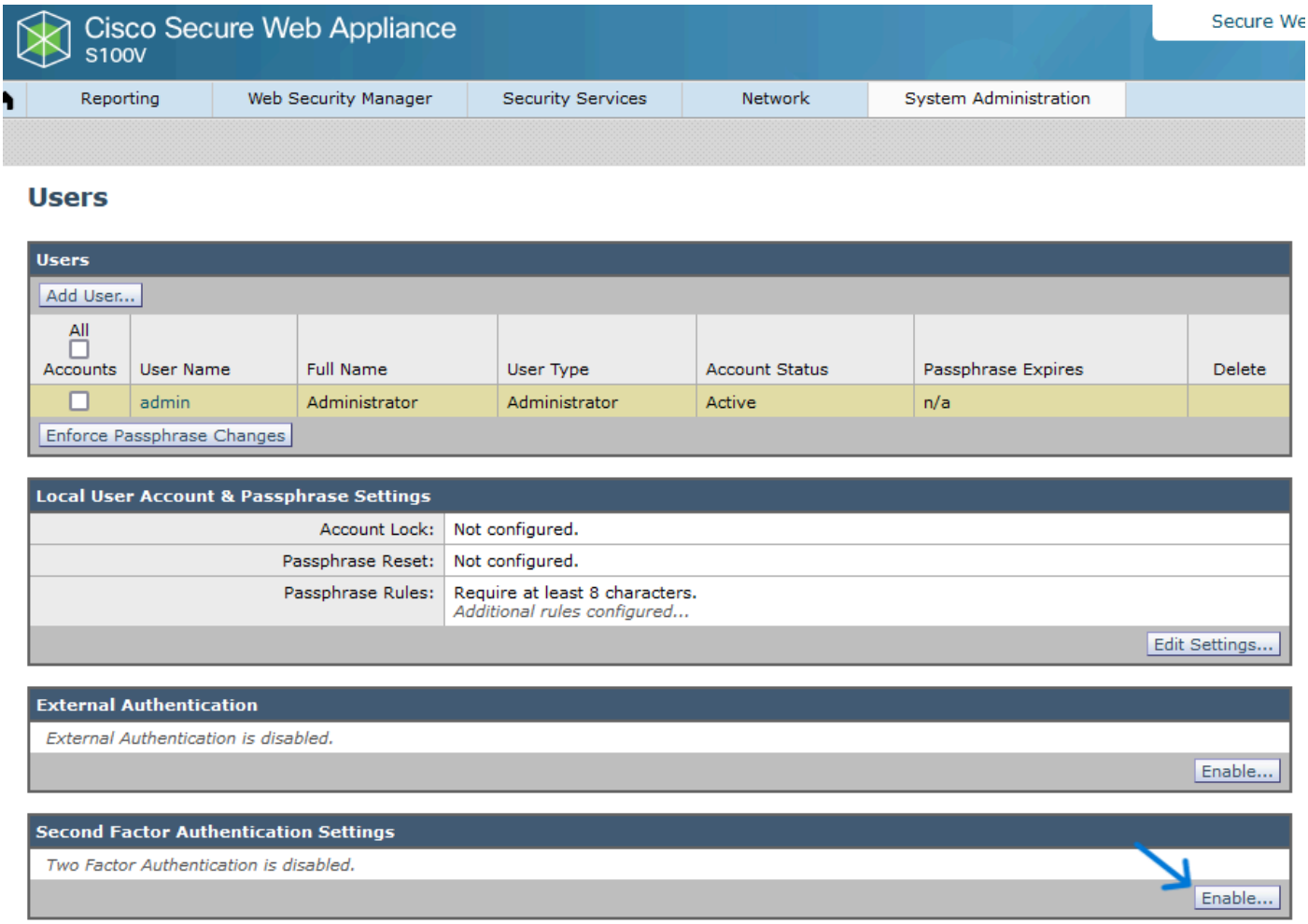
Second Factor Authentication in SWA aktivieren

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

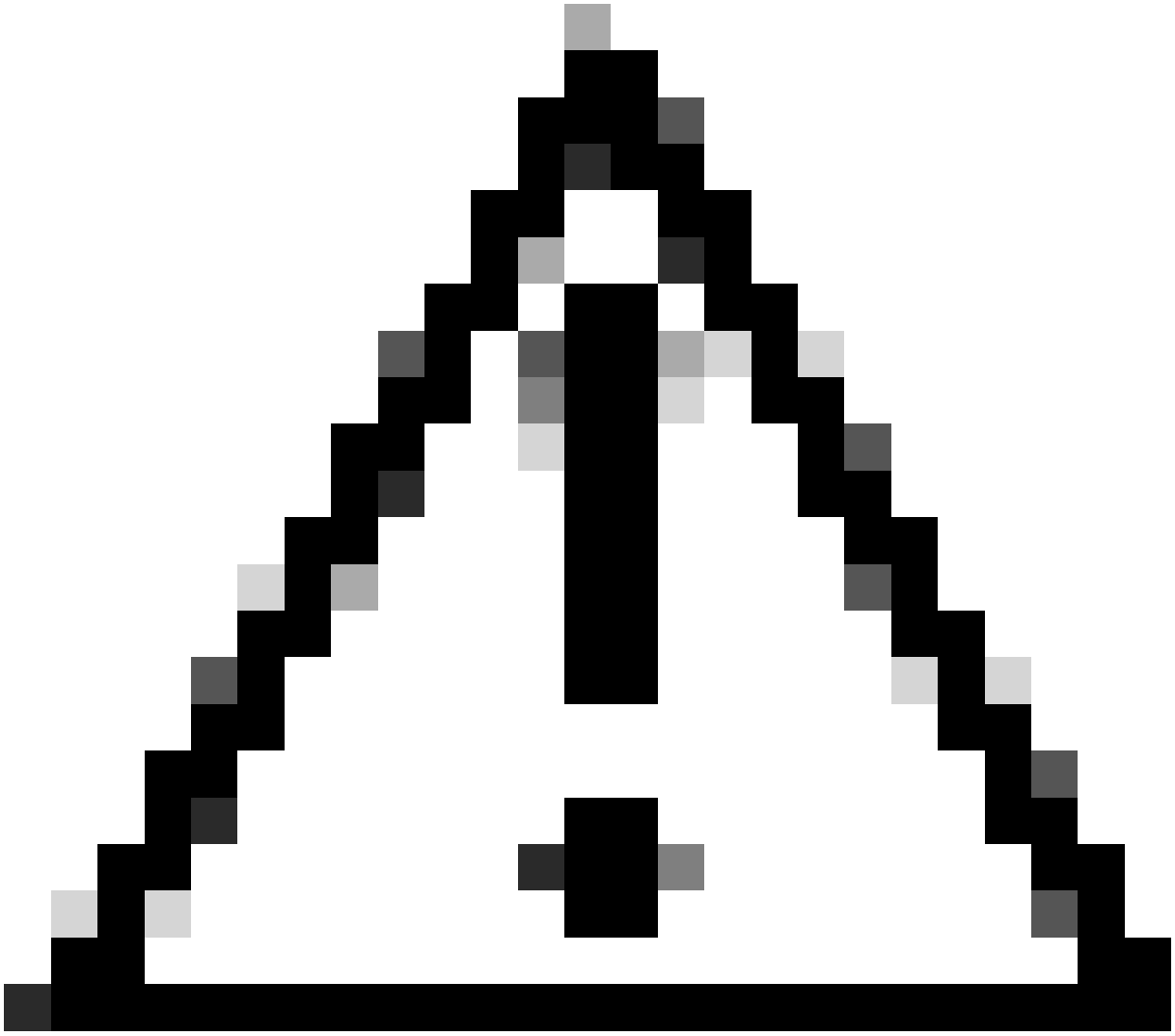
Schritt 4: Wählen Sie die erforderlichen vordefinierten Rollen aus, für die die Durchsetzung des zweiten Faktors aktiviert werden soll.



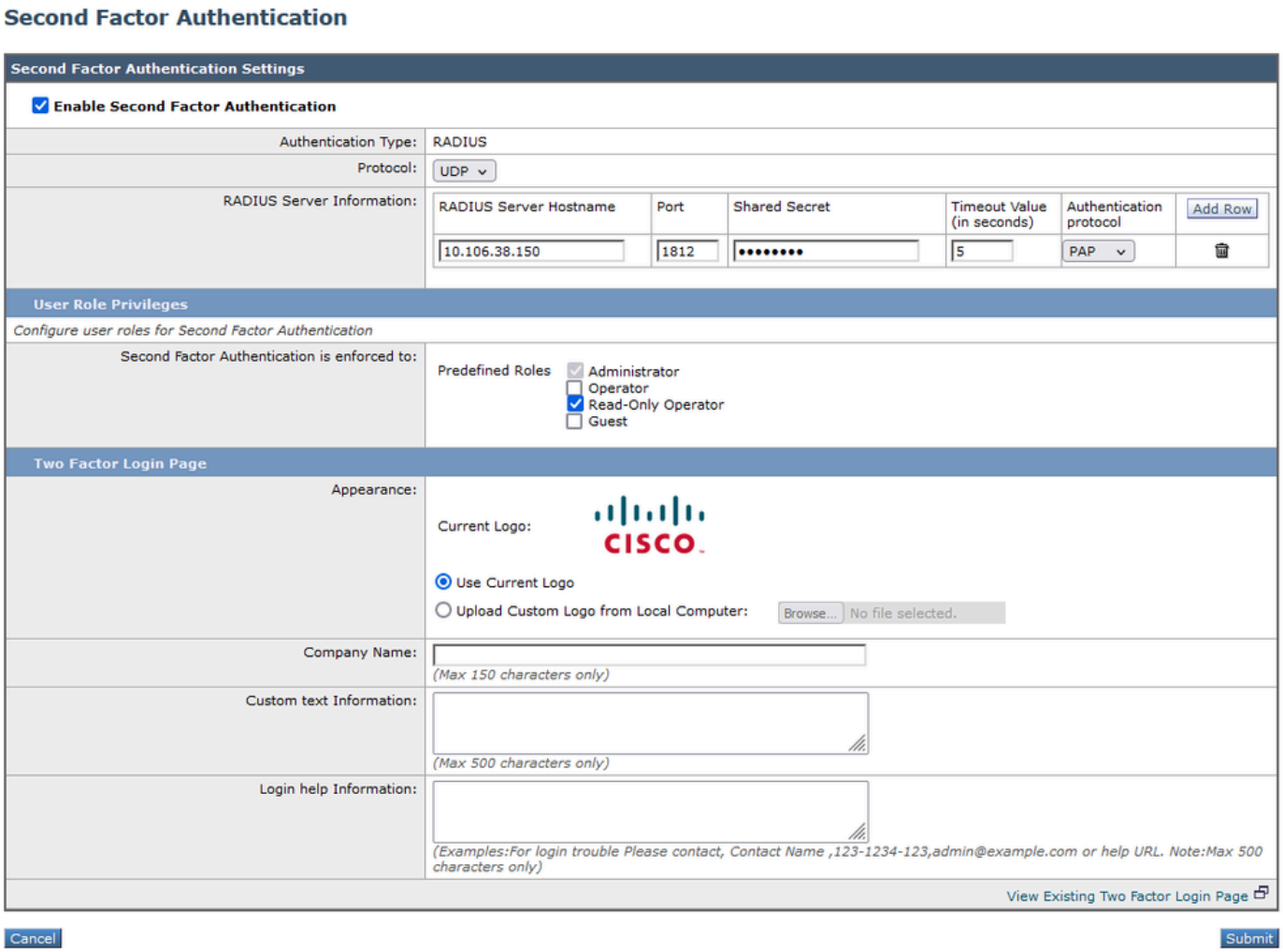
Vorsicht: Wenn Sie die zweite Faktor-Authentifizierung in SWA aktivieren, wird das Standard-Admin-Konto auch mit Second Factor-Durchsetzung aktiviert. Sie müssen die ISE in LDAP oder Active Directory (AD) integrieren, um die Anmeldeinformationen "admin" zu authentifizieren, da die ISE es Ihnen nicht erlaubt, "admin" als Netzwerkzugriffsbenutzer zu konfigurieren.



Second Factor Authentication in SWA aktivieren

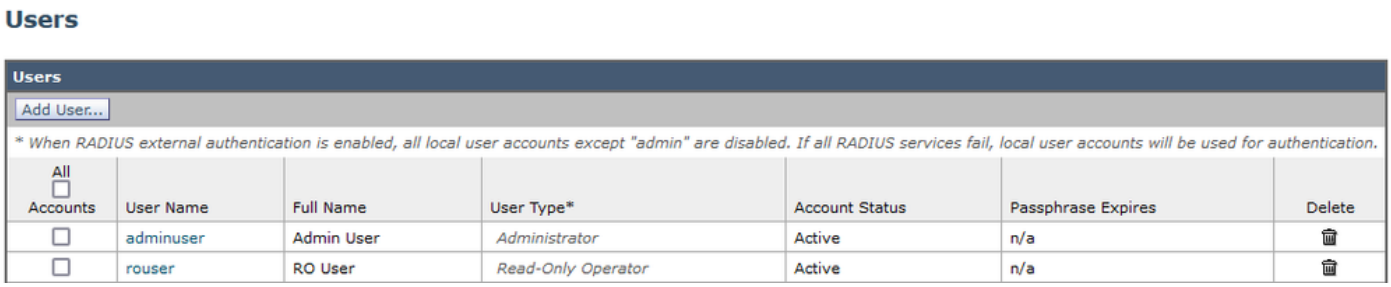


Vorsicht: Wenn Sie die zweite Faktor-Authentifizierung in SWA aktivieren, wird das Standard-Admin-Konto auch mit Second Factor-Durchsetzung aktiviert. Sie müssen die ISE in LDAP oder Active Directory (AD) integrieren, um die Anmeldeinformationen "admin" zu authentifizieren, da die ISE es Ihnen nicht erlaubt, "admin" als Netzwerkzugriffsbenutzer zu konfigurieren.



Zweite Faktorauthentifizierung konfigurieren

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.

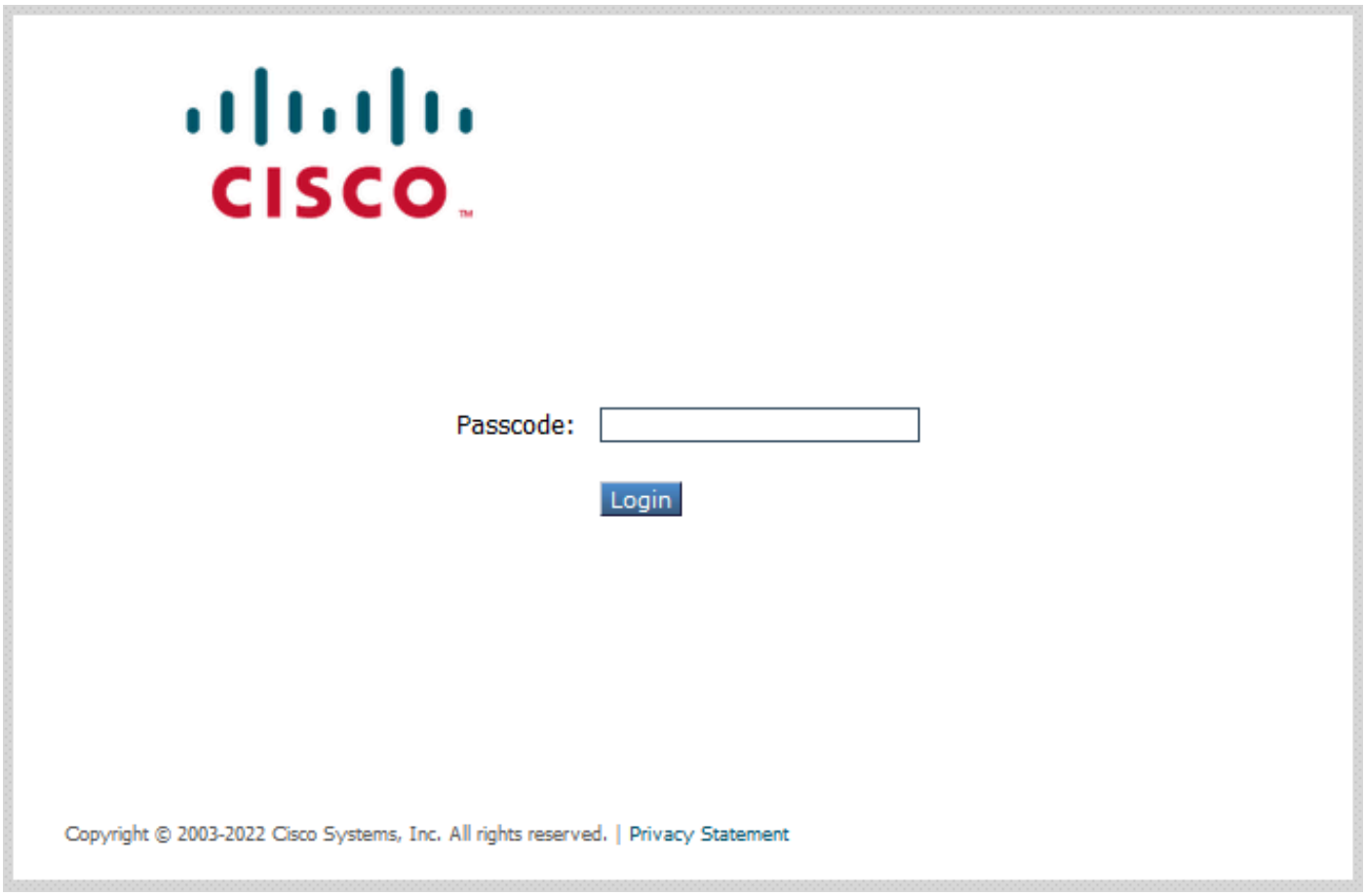


Benutzerkonfiguration in SWA

Schritt 6: Klicken Sie auf Senden und Änderungen bestätigen.

Überprüfung

Zugriff auf die SWA-GUI mit den konfigurierten Benutzeranmeldeinformationen Nach erfolgreicher Authentifizierung werden Sie zur sekundären Authentifizierungsseite weitergeleitet. Hier müssen Sie die sekundären, in ISE konfigurierten Authentifizierungsdaten eingeben.



Zweite Faktoranmeldung überprüfen

Referenzen

- Bedienungsanleitung für AsyncOS 14.0 für Cisco Secure Web Appliance
- ISE 3.0 - Administratorhandbuch
- ISE-Kompatibilitätsmatrix für Secure Web Appliance
- AD für ISE-GUI und CLI integrieren Anmelden

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.