Konfigurieren der RAVPN-Zertifikatauthentifizierung und ISE-Autorisierung auf dem FMC

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von ISE-Server-Autorisierungsrichtlinien für die Zertifikatsauthentifizierung in RAVPN-Verbindungen beschrieben, die von CSF auf FMC verwaltet werden.

Voraussetzungen

Anforderungen

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

- Cisco Secure Firewall (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Zertifikatregistrierung und SSL-Grundlagen
- Zertifizierungsstelle

Verwendete Komponenten

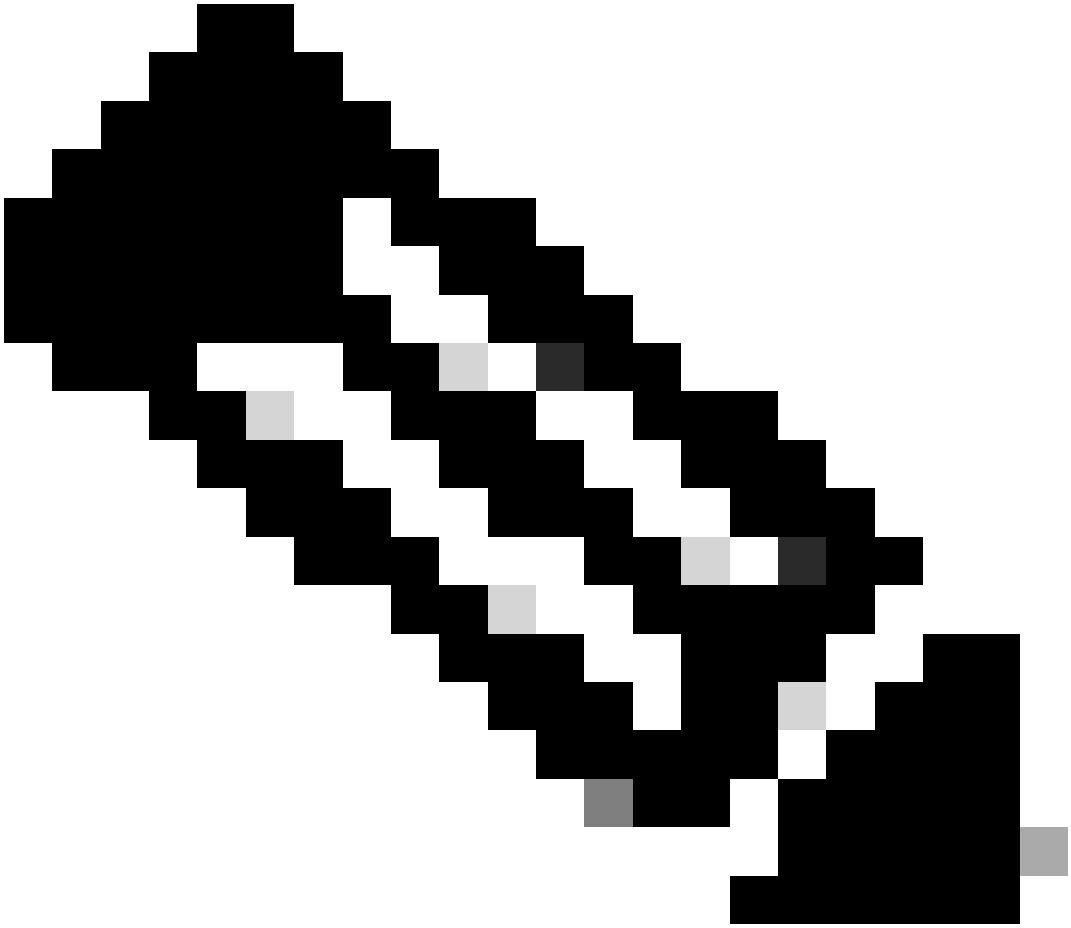
Der Inhalt dieses Dokuments basiert auf den Software- und Hardwareversionen.

- Cisco Secure Client Version 5.1.6
- Cisco Secure Firewall Version 7.2.8
- Cisco Secure Firewall Management Center Version 7.2.8

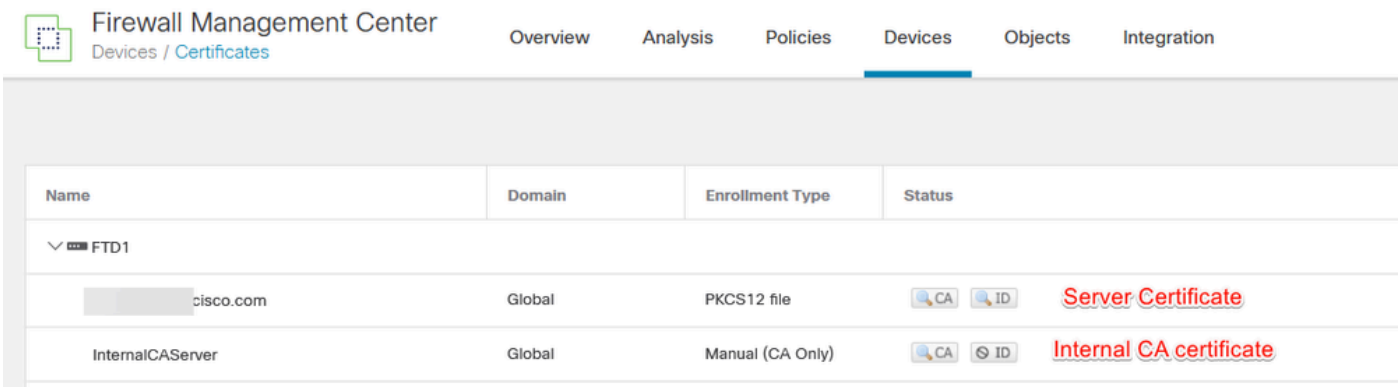
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

Schritt 1: Installieren eines Zertifikats der vertrauenswürdigen Zertifizierungsstelle



Hinweis: Dieser Schritt muss ausgeführt werden, wenn sich das CA-Zertifikat von dem Zertifikat unterscheidet, das für die Serverauthentifizierung verwendet wird. Wenn derselbe CA-Server die Benutzerzertifikate ausstellt, ist es nicht erforderlich, dasselbe CA-Zertifikat erneut zu importieren.

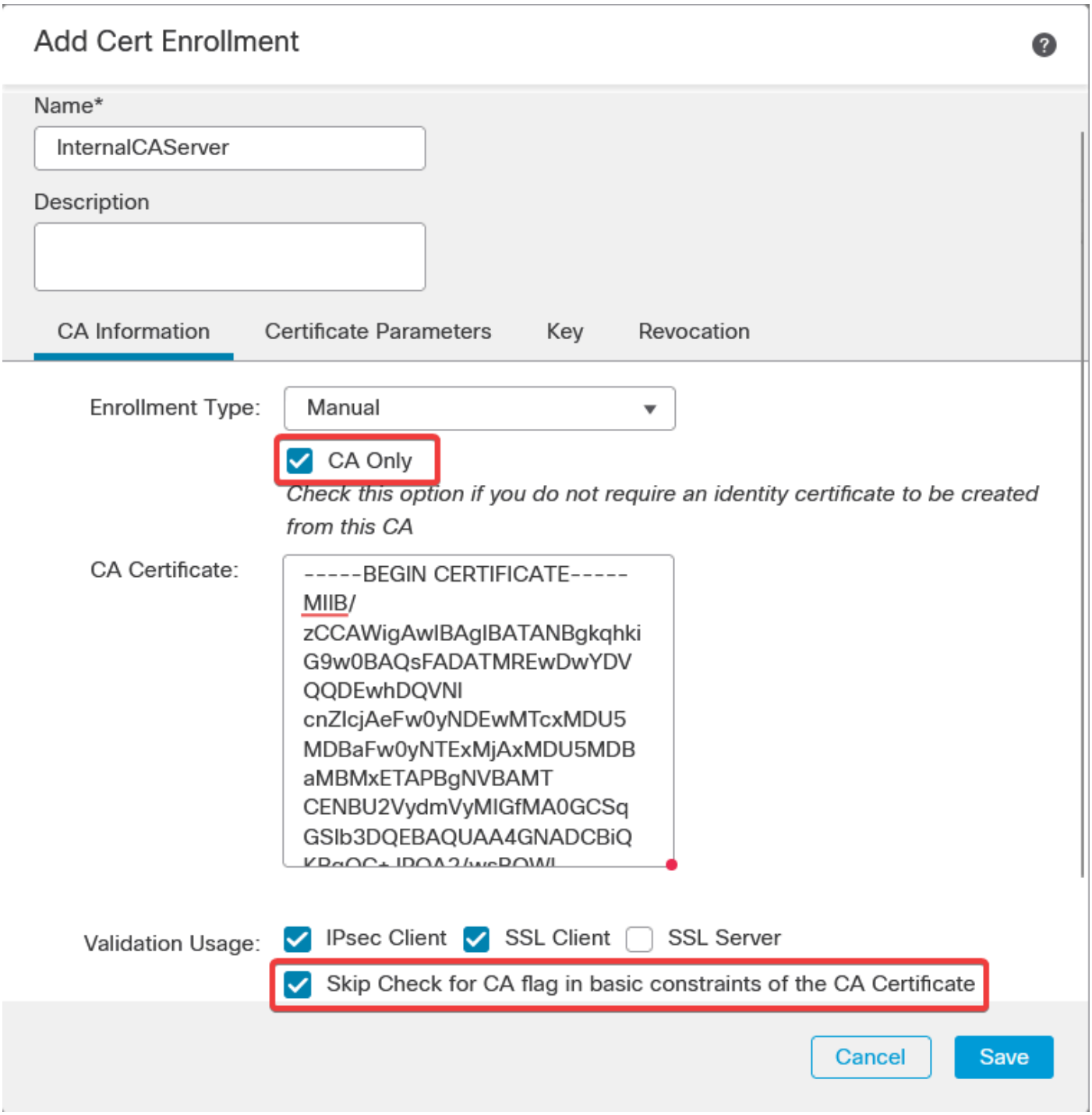


a. Navigieren Sie zu ,Devices > Certificatesund klicken Sie auf **Add**.

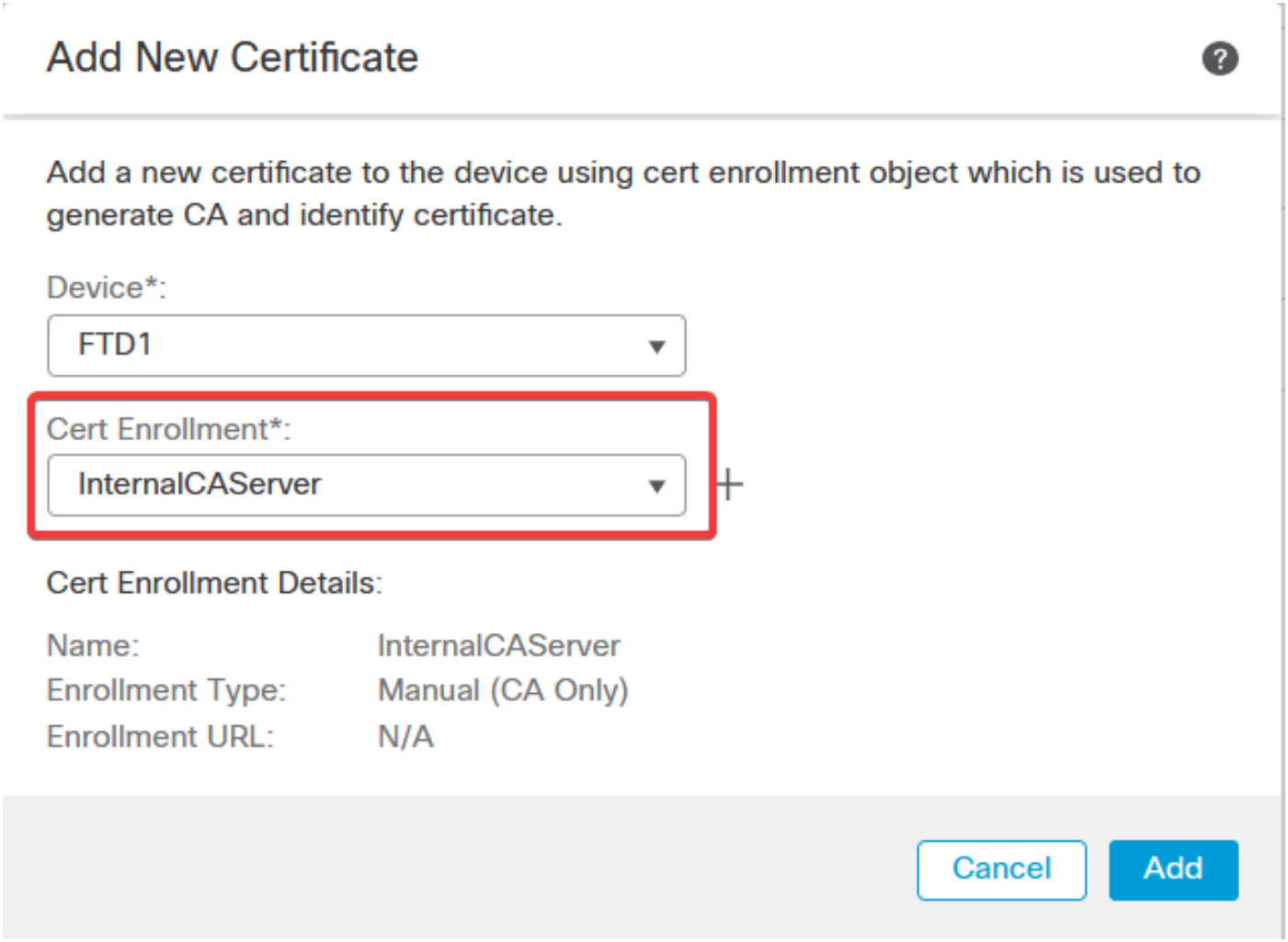
b. Geben Sie einen Wert ein **trustpoint name** und wählen Sie unter "CA-Informationen" Manual als Registrierungstyp aus.

c. AktivierenCA OnlySie das vertrauenswürdige/interne Zertifizierungsstellenzertifikat, und fügen Sie es im PEM-Format ein.

d. Aktivieren **Skip Check for CA flag in basic constraints of the CA Certificate** und klicken Sie auf **Save**.

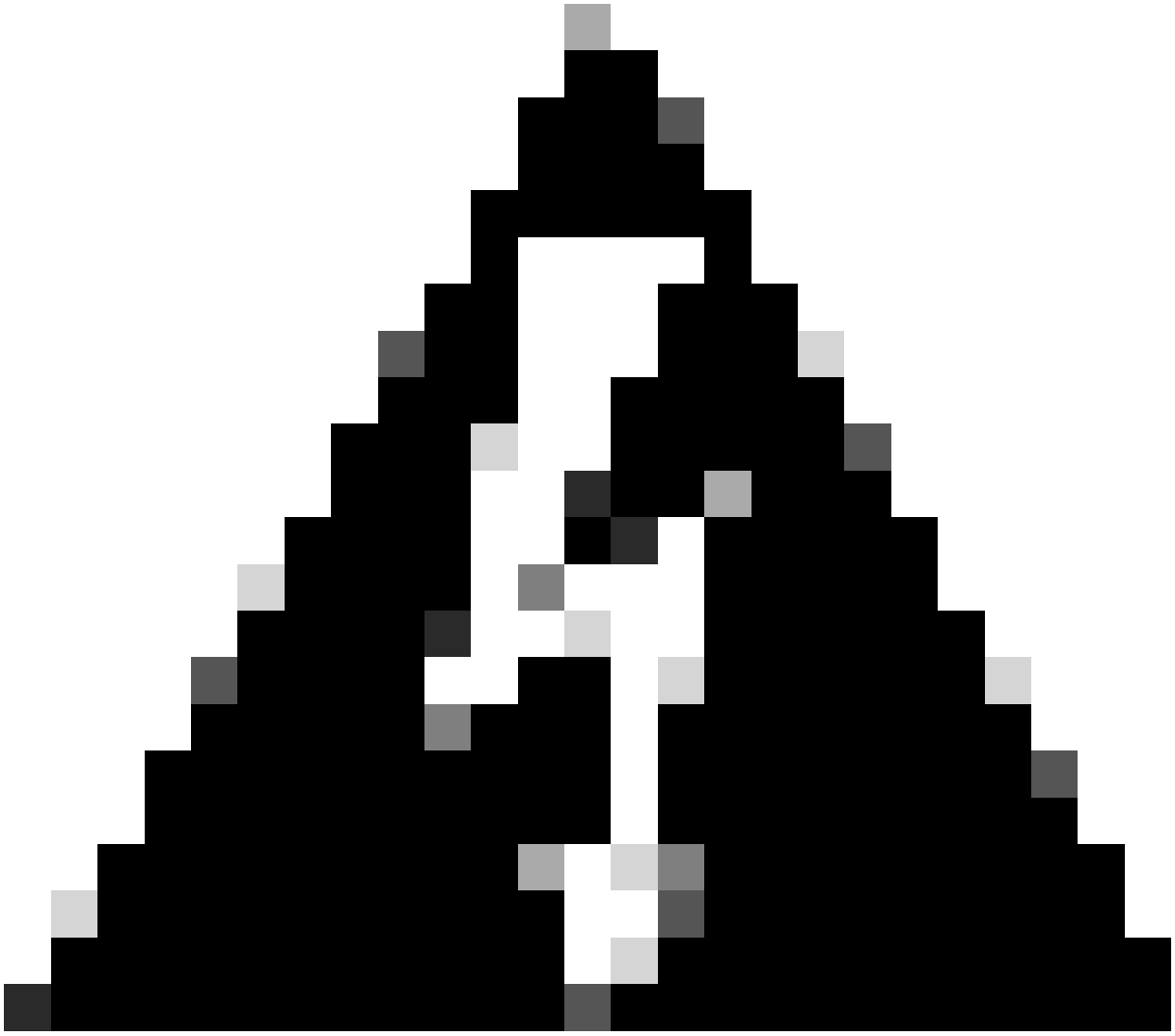


e. Wählen Sie **Cert Enrollment**unter die **trustpoint** aus dem Dropdown-Menü aus, die gerade erstellt wurde, und klicken Sie auf **Add**.

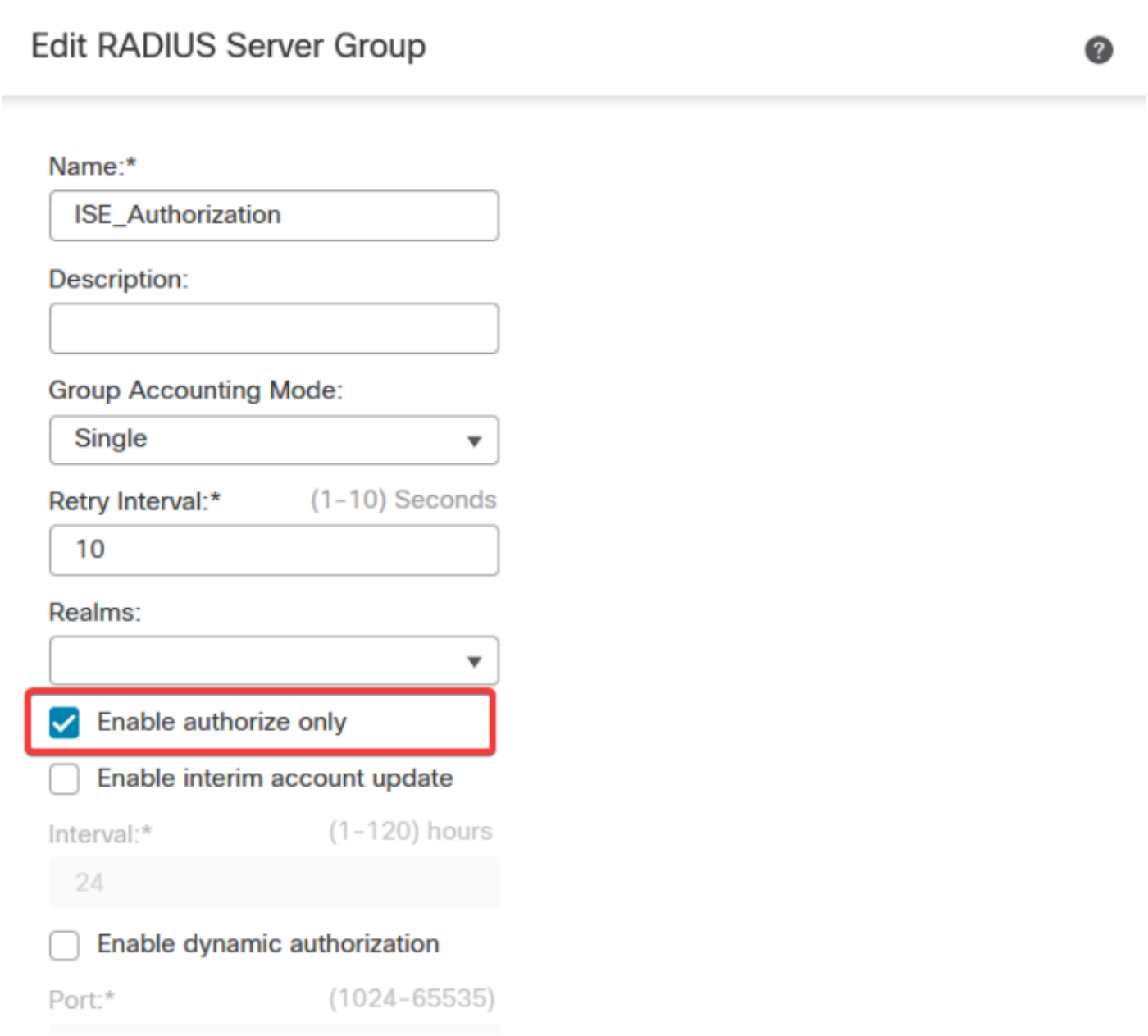


Schritt 2: Konfigurieren von ISE/Radius-Servergruppe und Verbindungsprofil

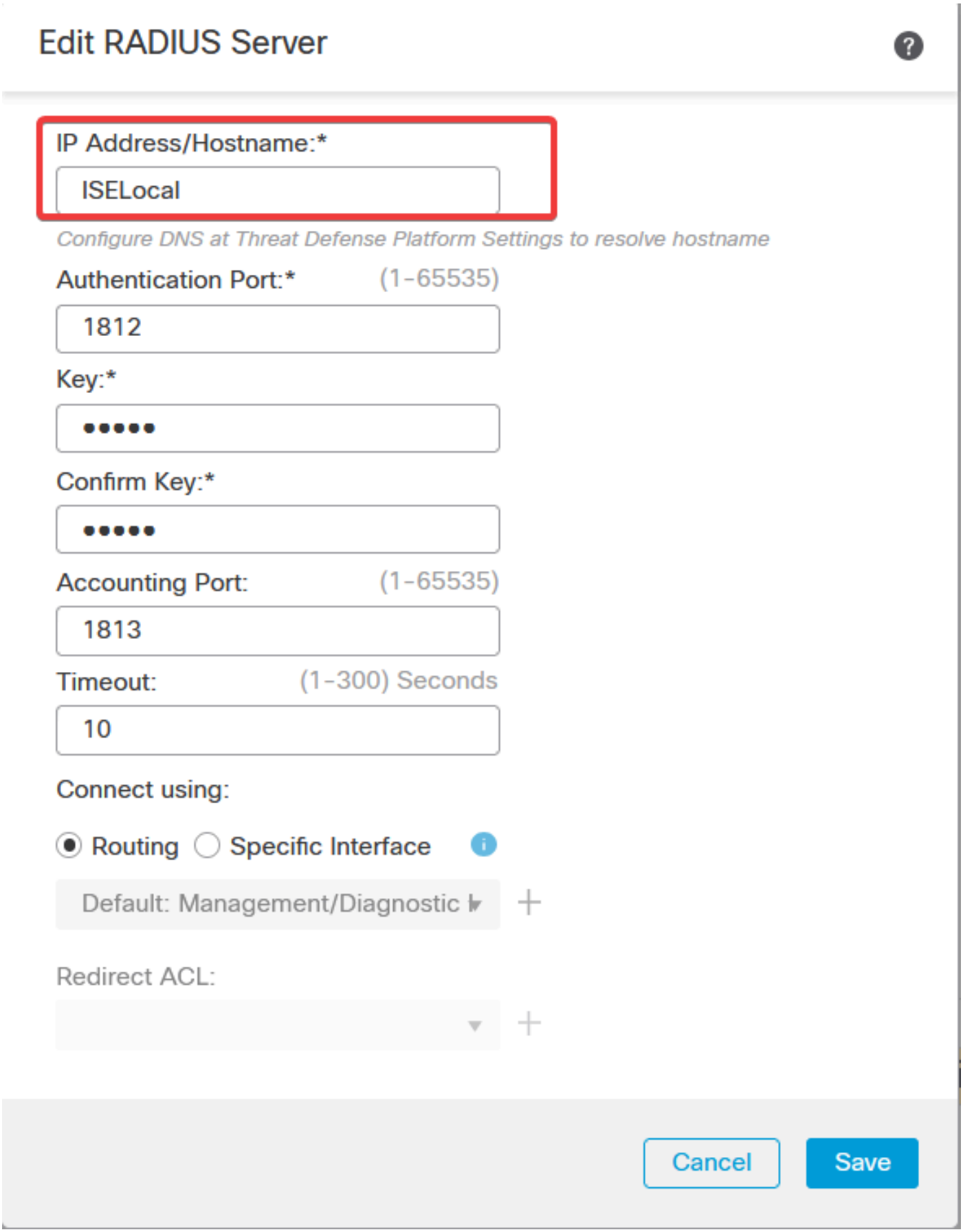
a. Navigieren Sie zu , **Objects > AAA Server > RADIUS Server Group** und klicken Sie auf **Add RADIUS Server Group**. Aktivieren Sie **Enable authorize only** Option.



Warnung: Wenn die Option Nur Autorisierung aktivieren nicht aktiviert ist, sendet die Firewall eine Authentifizierungsanforderung. Die ISE erwartet jedoch, mit dieser Anforderung einen Benutzernamen und ein Kennwort zu erhalten, und in Zertifikaten wird kein Kennwort verwendet. Daher markiert die ISE die Anforderung als fehlgeschlagen.

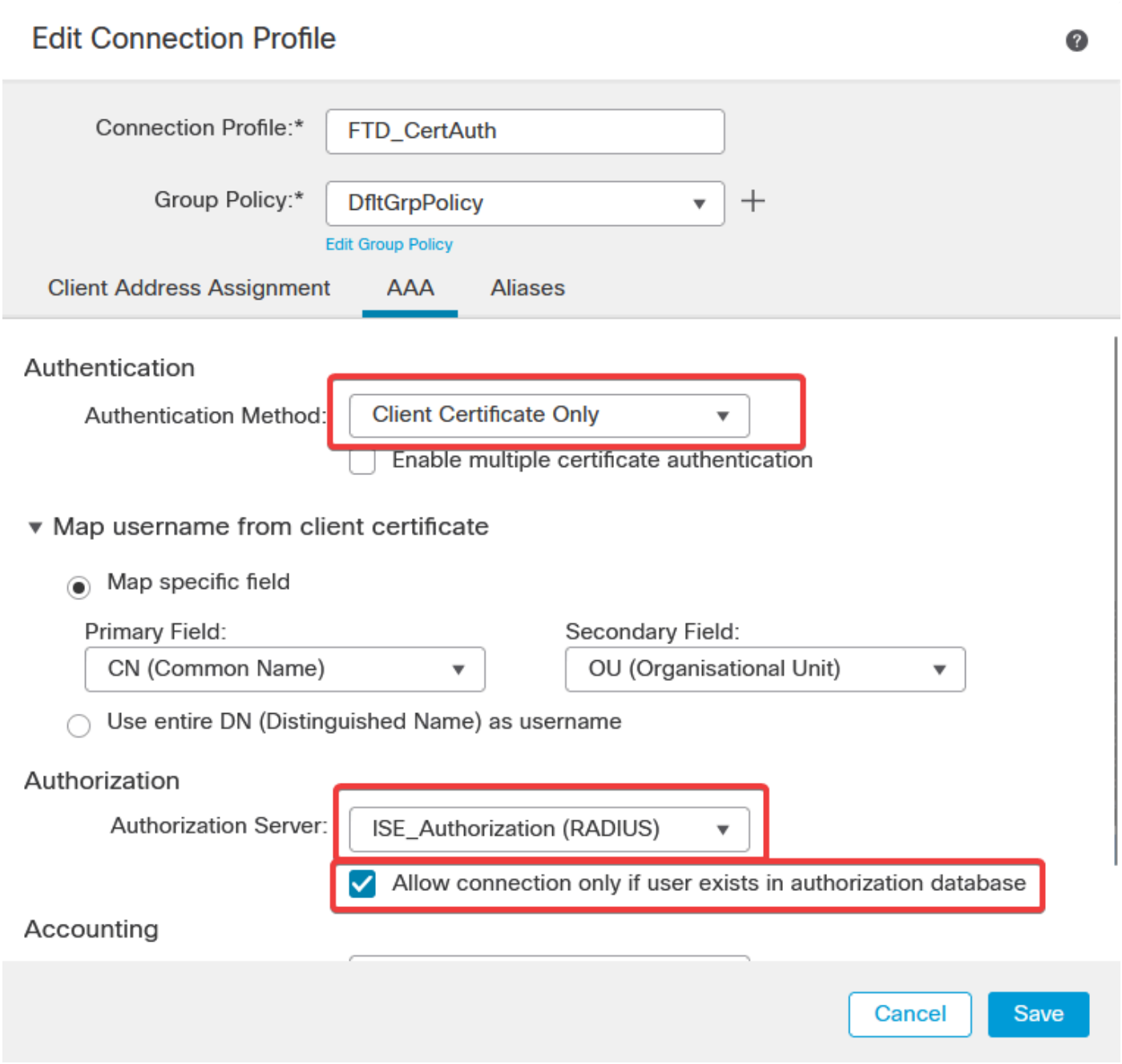


b. Klicken Sie auf **Add (+)** das Symbol, und fügen Sie dann dieRadius server/ISE serverunter Verwendung der IP-Adresse oder eines Hostnamens hinzu.



c. Navigieren Sie zu **Devices** > **Remote Access configuration** . Erstellen Sie einenew connection profile, und legen Sie die Authentifizierungsmethode aufClient Certificate Onlyfest. Wählen Sie für den Autorisierungsserver den Server aus, der mit den vorherigen Schritten erstellt wurde.

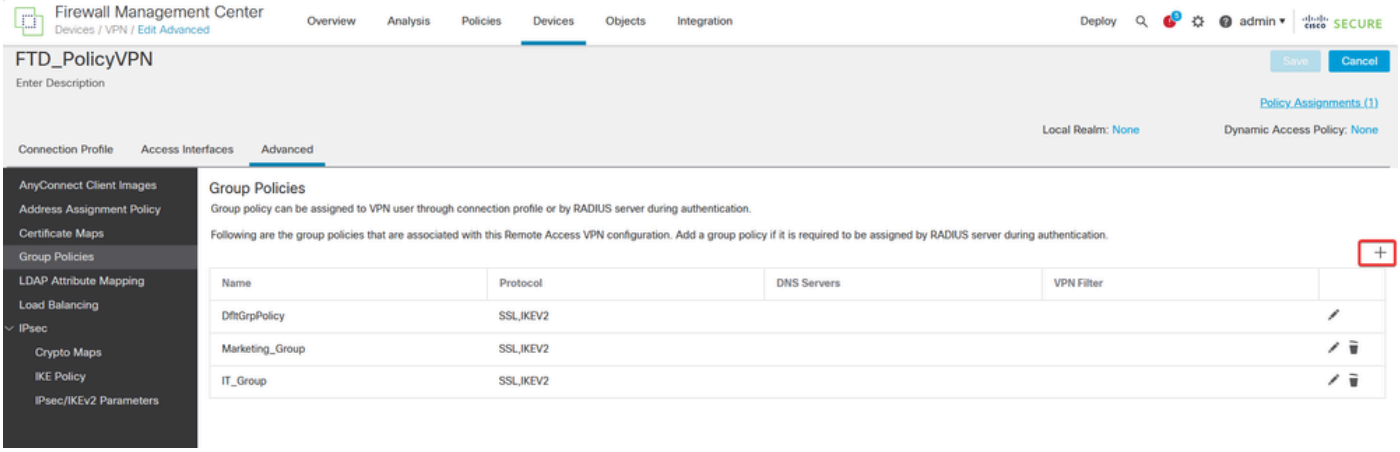
Stellen Sie sicher, dass Sie die **Allow connection only if user exists in authorization database** Option aktivieren. Mit dieser Einstellung wird sichergestellt, dass die Verbindung zum RAVPN nur dann hergestellt wird, wenn die Autorisierung zulässig ist.



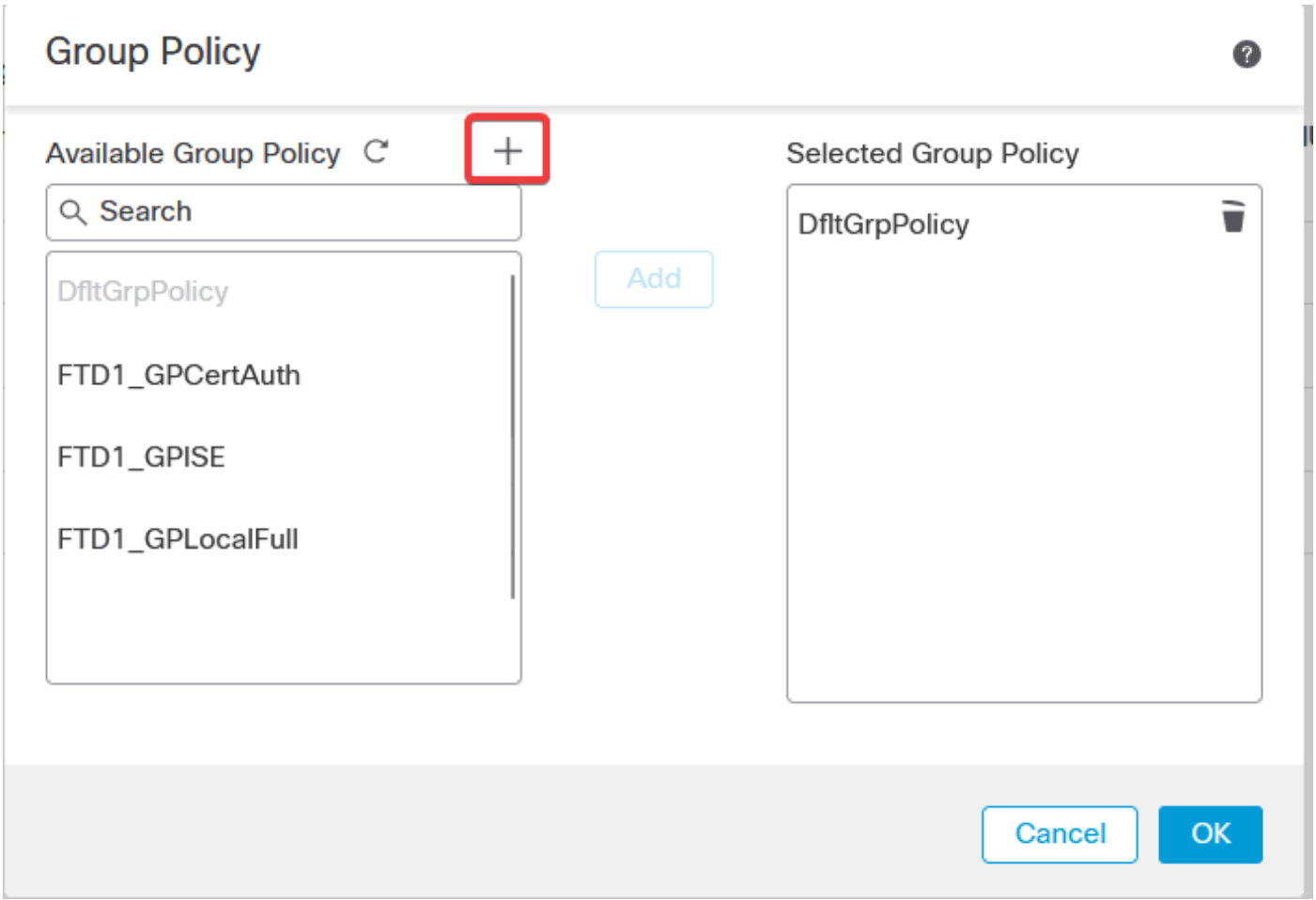
Der Zuordnungsbenutzername aus dem Clientzertifikat bezieht sich auf die Informationen, die aus dem Zertifikat abgerufen werden, um den Benutzer zu identifizieren. In diesem Beispiel behalten Sie die Standardkonfiguration bei, sie kann jedoch geändert werden, je nachdem, welche Informationen zum Identifizieren der Benutzer verwendet werden.

Klicken Sie auf .**Save**

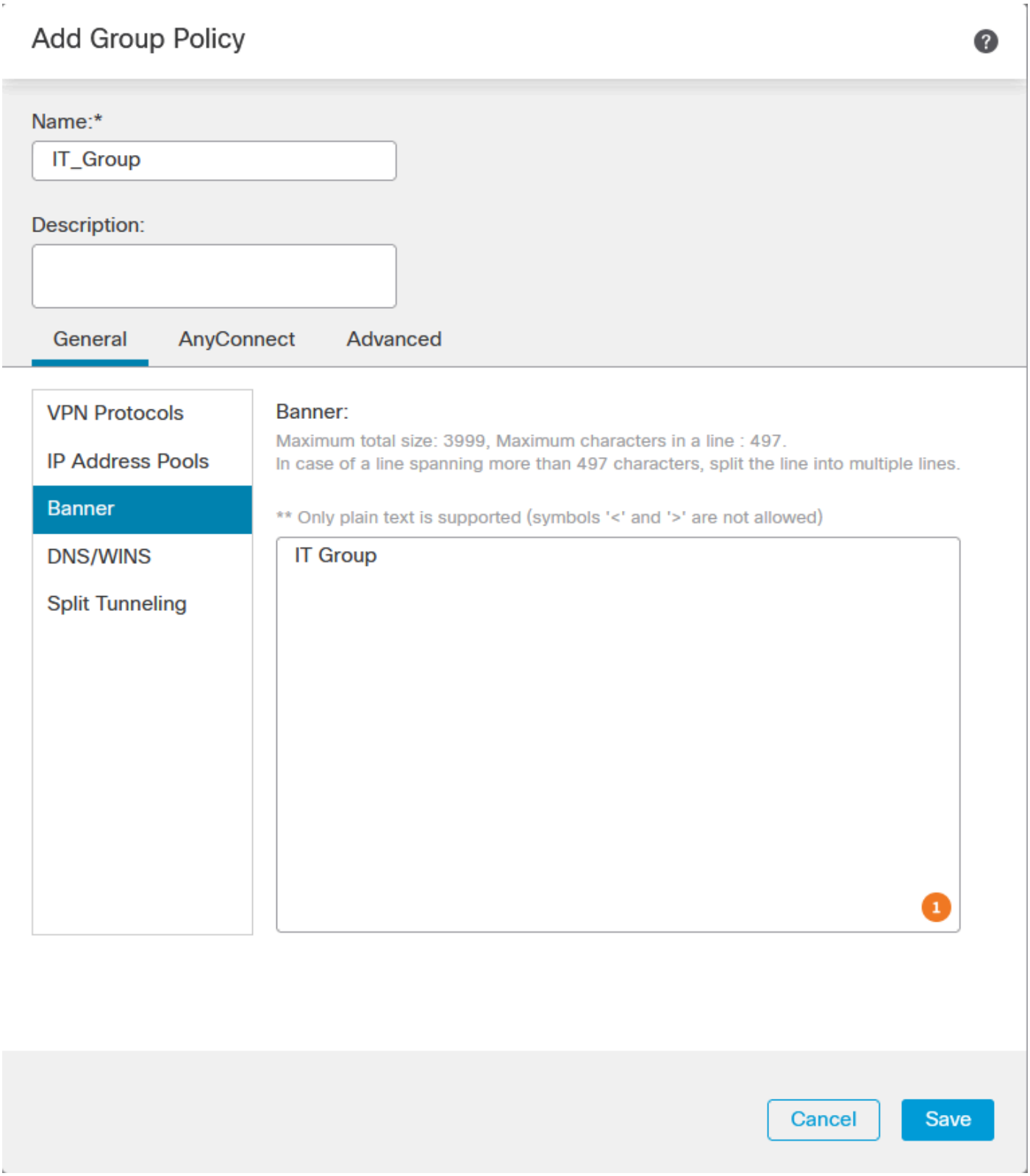
d. Navigieren Sie zu **Advanced** > **Group Policies**. Klicken Sie auf **Add (+)** das Symbol rechts.



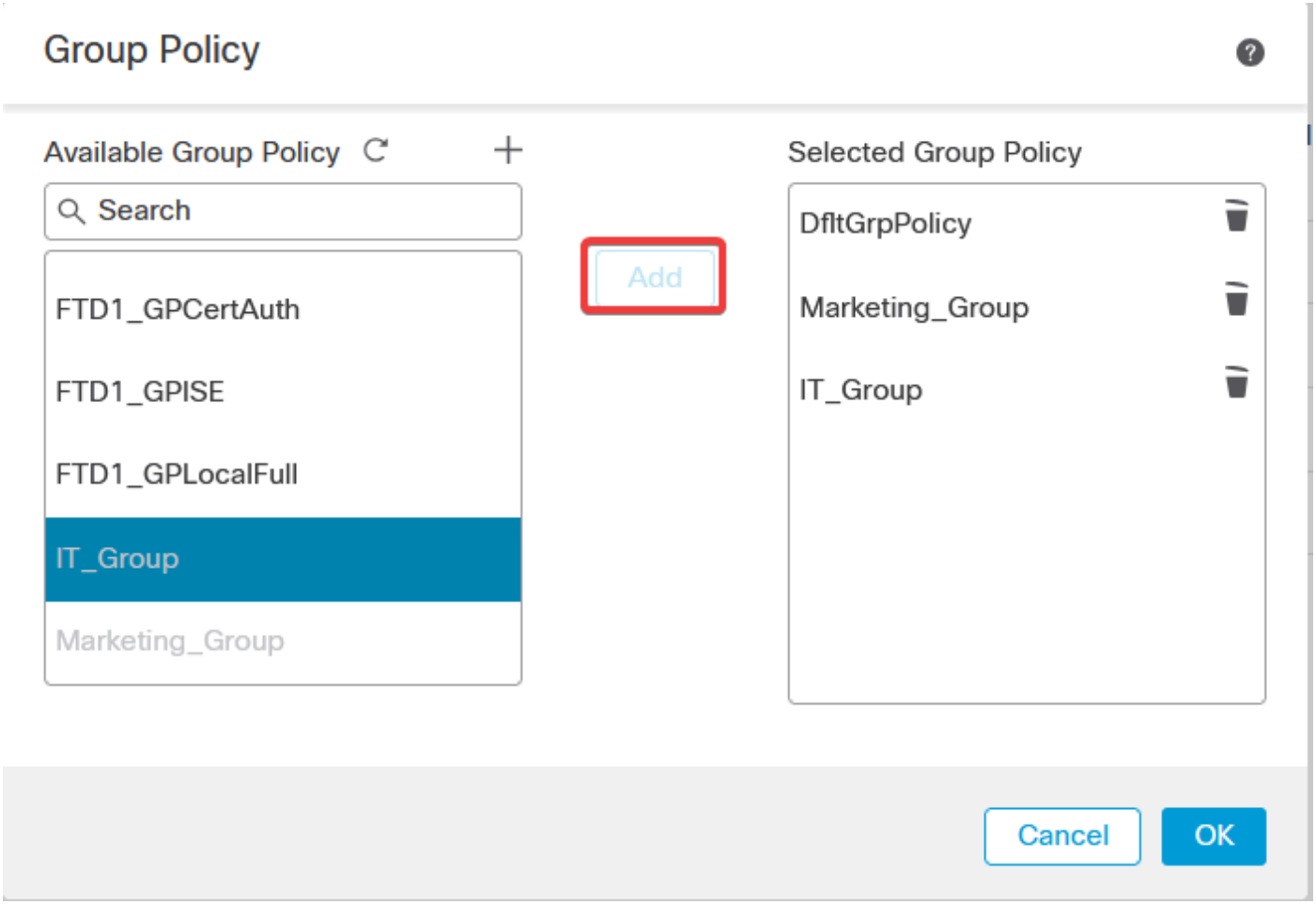
e. Erstellen Sie die **group policies**. Jede Gruppenrichtlinie wird auf Grundlage der Organisationsgruppen und der Netzwerke konfiguriert, auf die jede Gruppe zugreifen kann.



f. Führen Sie in der Gruppenrichtlinie die für jede Gruppe spezifischen Konfigurationen aus. Eine Bannernachricht kann hinzugefügt werden, um sie nach einer erfolgreichen Verbindung anzuzeigen.



g. Wählen Sie die **group policies** auf der linken Seite aus, und klicken SieAddauf, um sie zur rechten Seite zu verschieben. Legt fest, welche Gruppenrichtlinien in der Konfiguration verwendet werden.

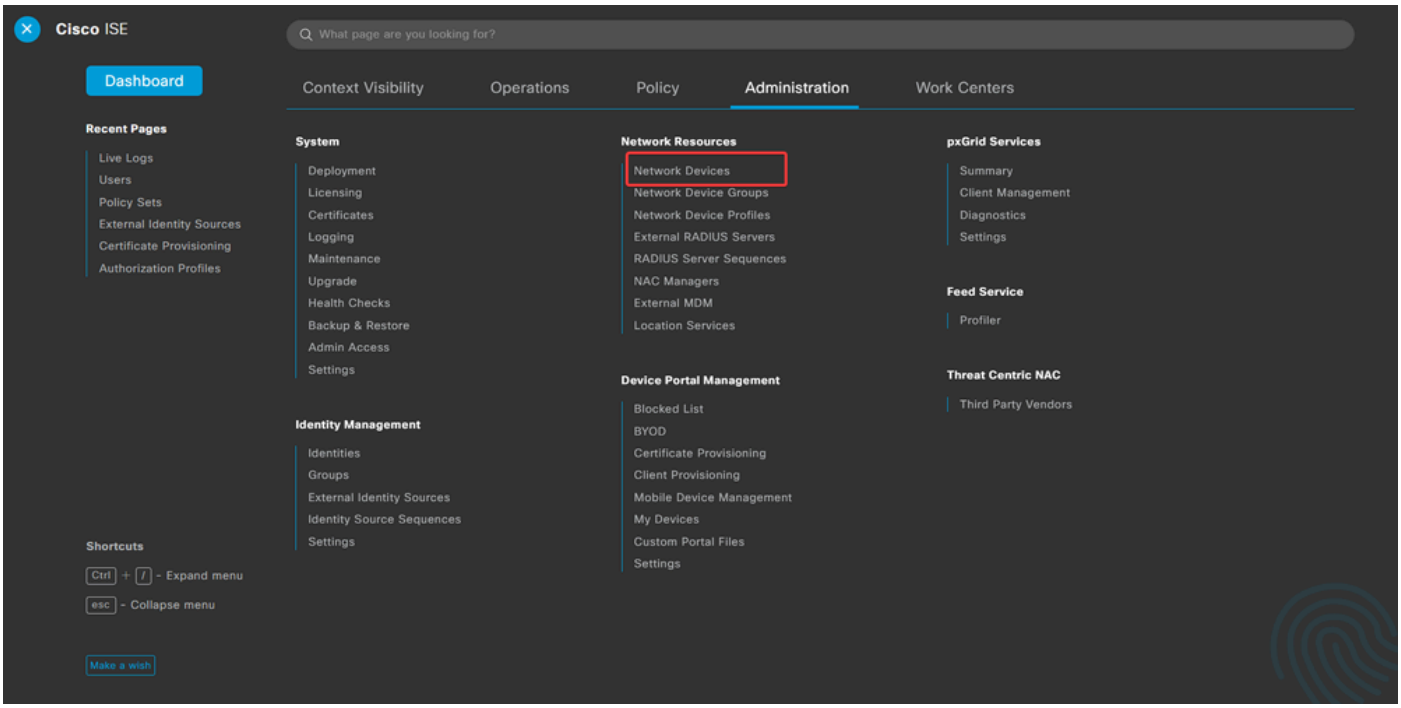


e. Stellen Sie die Änderungen bereit.

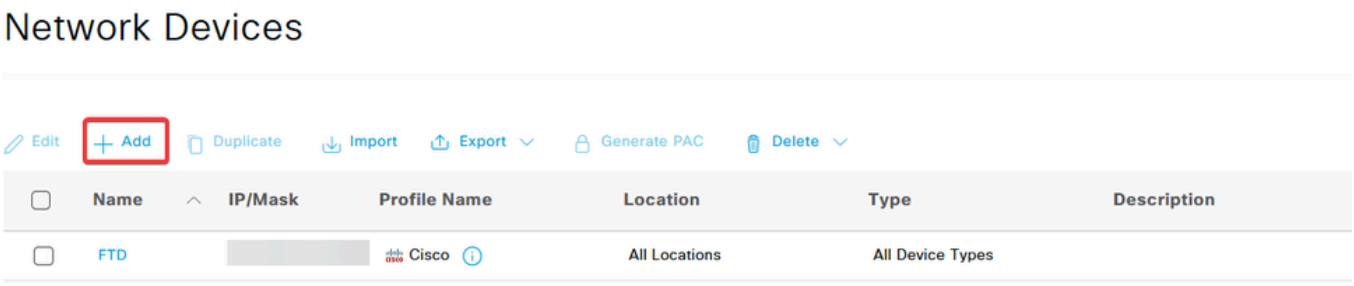
Schritt 3: Konfigurieren der ISE

Schritt 3.1: Erstellen von Benutzern, Gruppen und Zertifikatauthentifizierungsprofilen

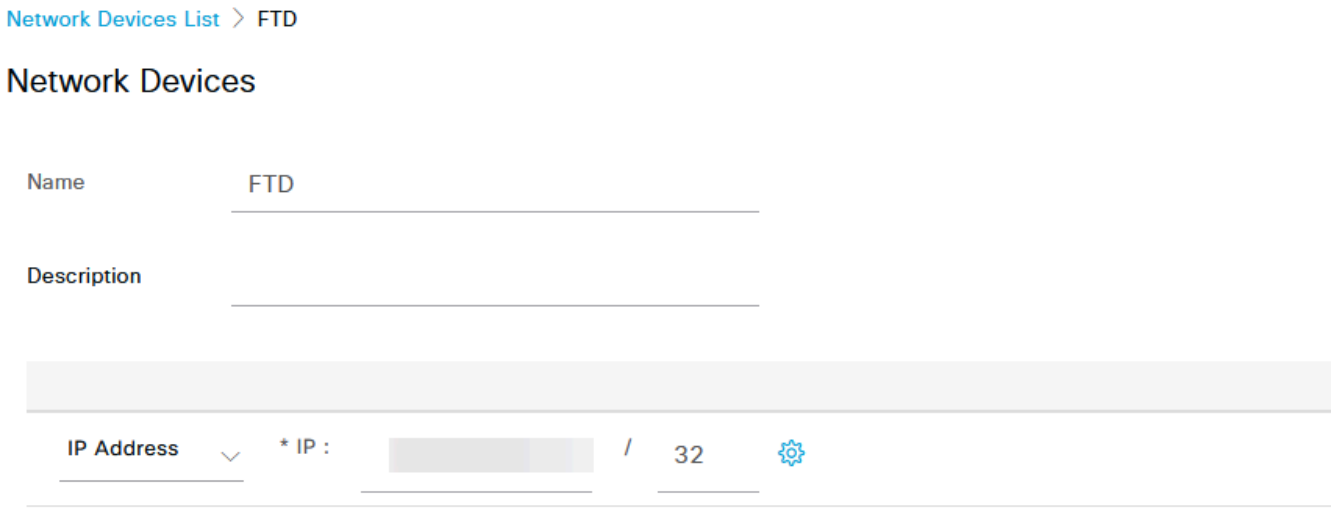
a. Melden Sie sich beim ISE-Server an, und navigieren Sie zu **Administration > Network Resources > Network Devices.**

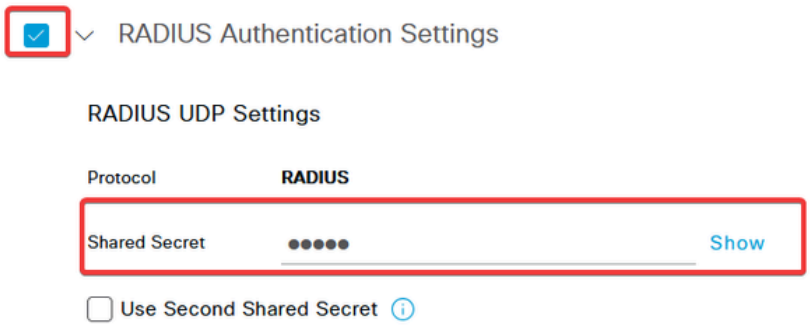


b. Klicken Sie auf **Add** , um die Firewall als AAA-Client zu konfigurieren.

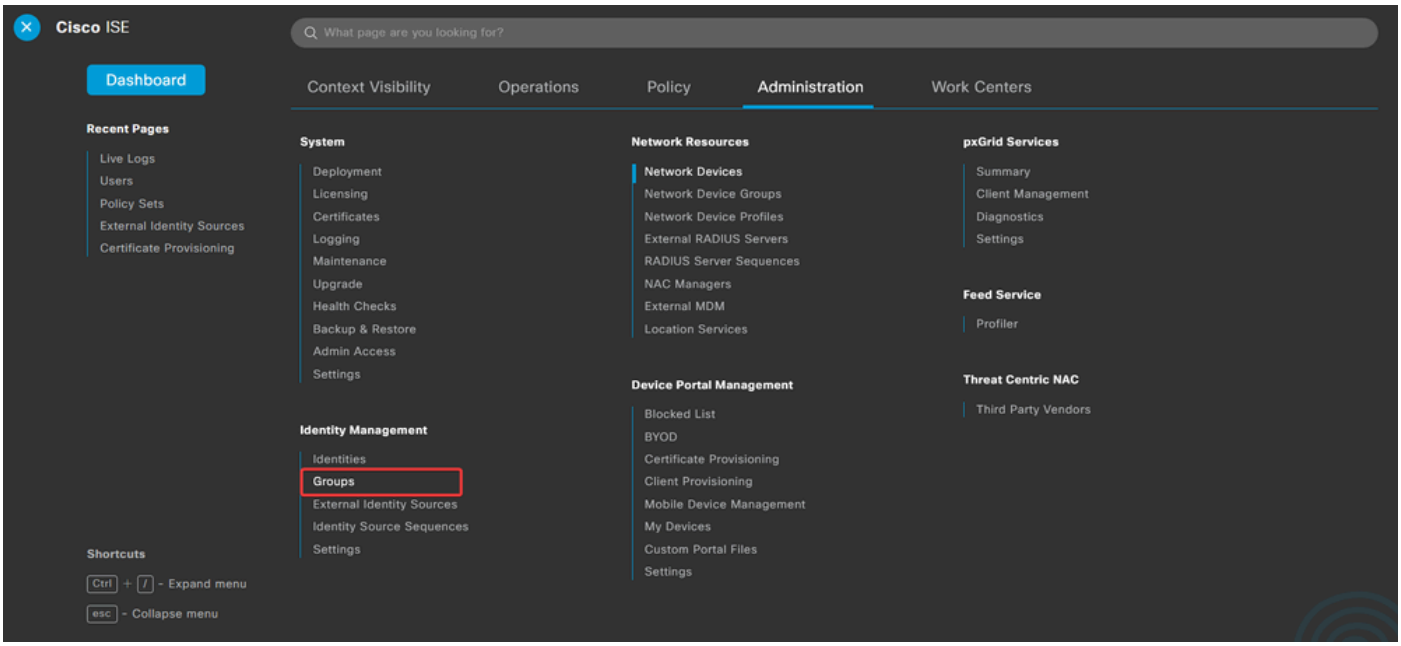


c. Geben Sie die Felder für den Netzwerkgerätenamen und die IP-Adresse ein, aktivieren Sie **RADIUS Authentication Settings** dann das Kontrollkästchen, und fügen Sie den **Shared Secret**. Wert Dieser muss derselbe sein, der beim Erstellen des RADIUS-Serverobjekts auf dem FMC verwendet wurde. Klicken Sie auf .Save



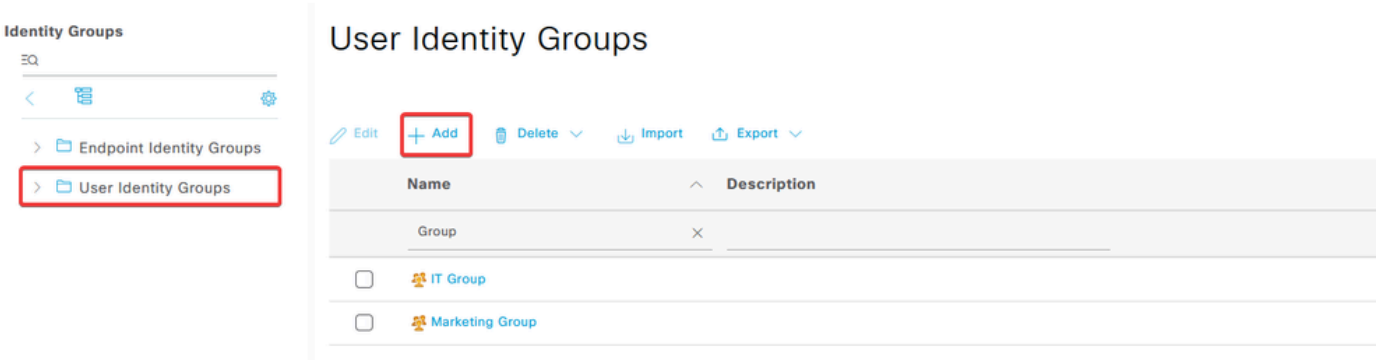


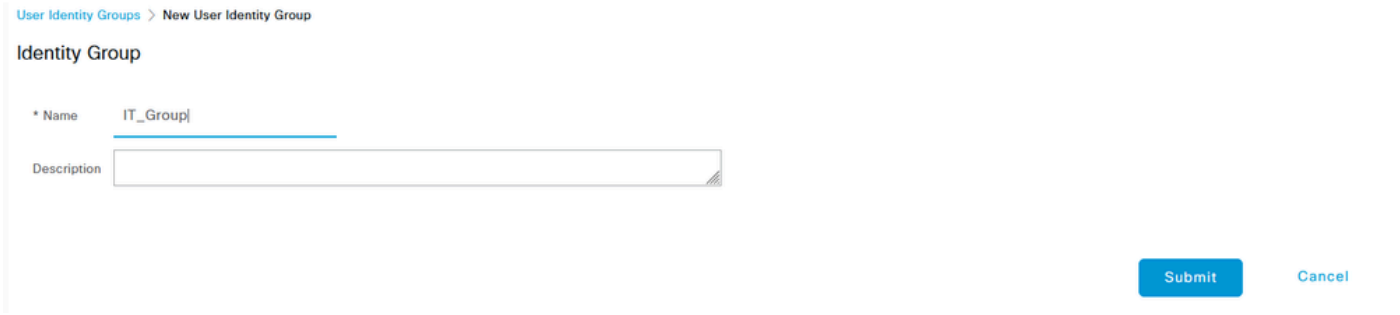
d. Navigieren Sie zuAdministration > Identity Management > Groups.

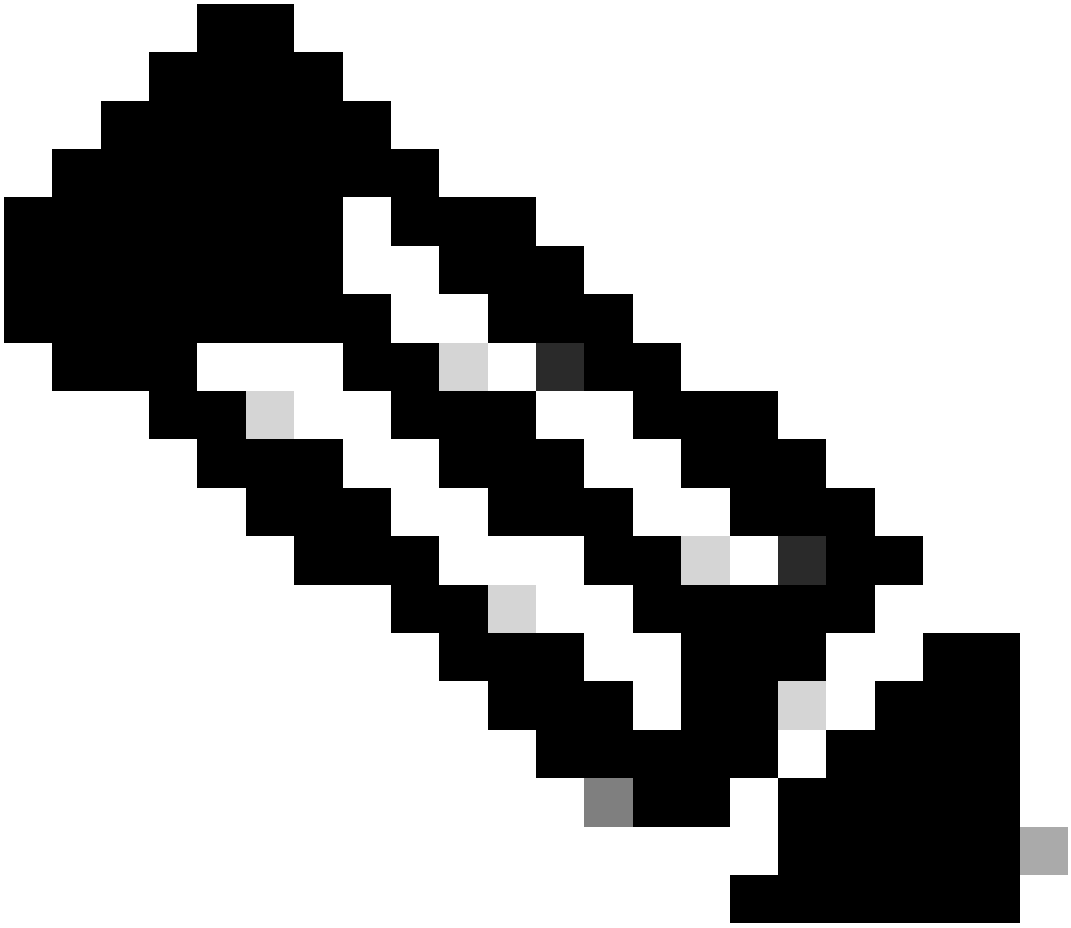


e. Klicken Sie aufUser Identity Groupsund dann auf **Add**.

Geben Sie den Gruppennamenein, und klicken Sie aufSubmit.

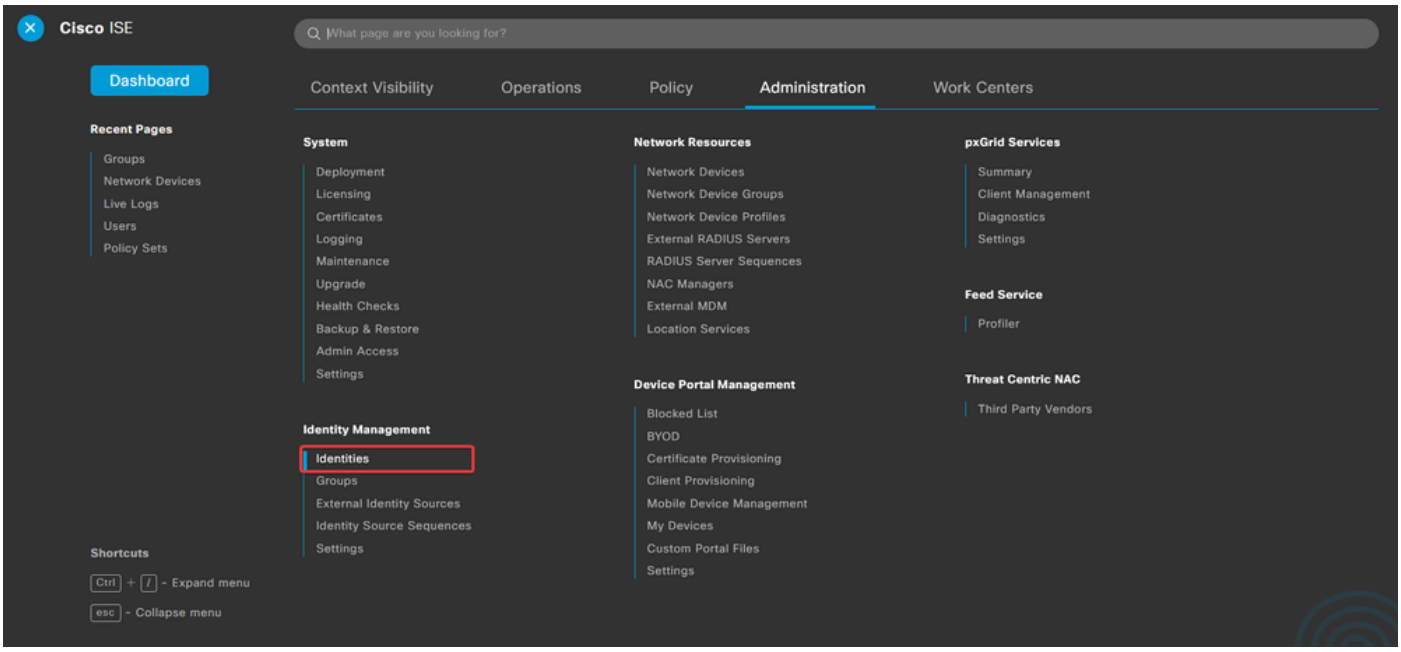






Hinweis: Wiederholen Sie den Vorgang, um so viele Gruppen wie nötig zu erstellen.

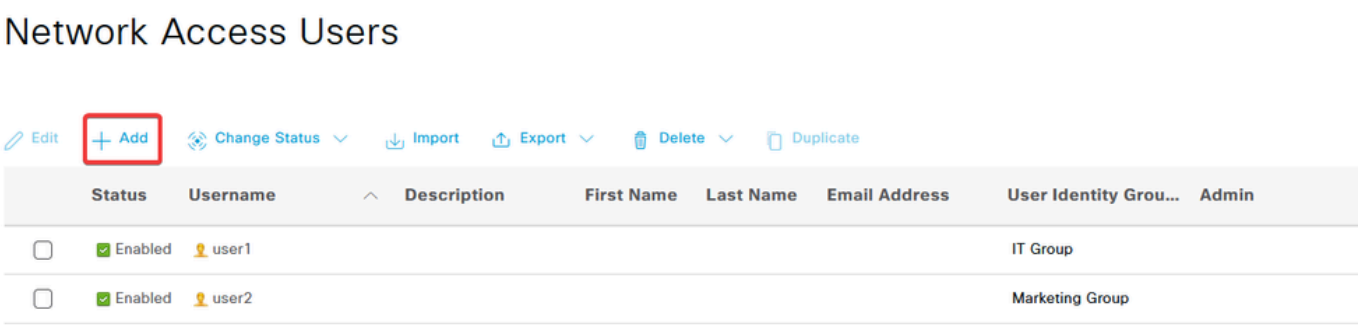
d. Navigieren Sie zu **Administration > Identity Management > Identities.**

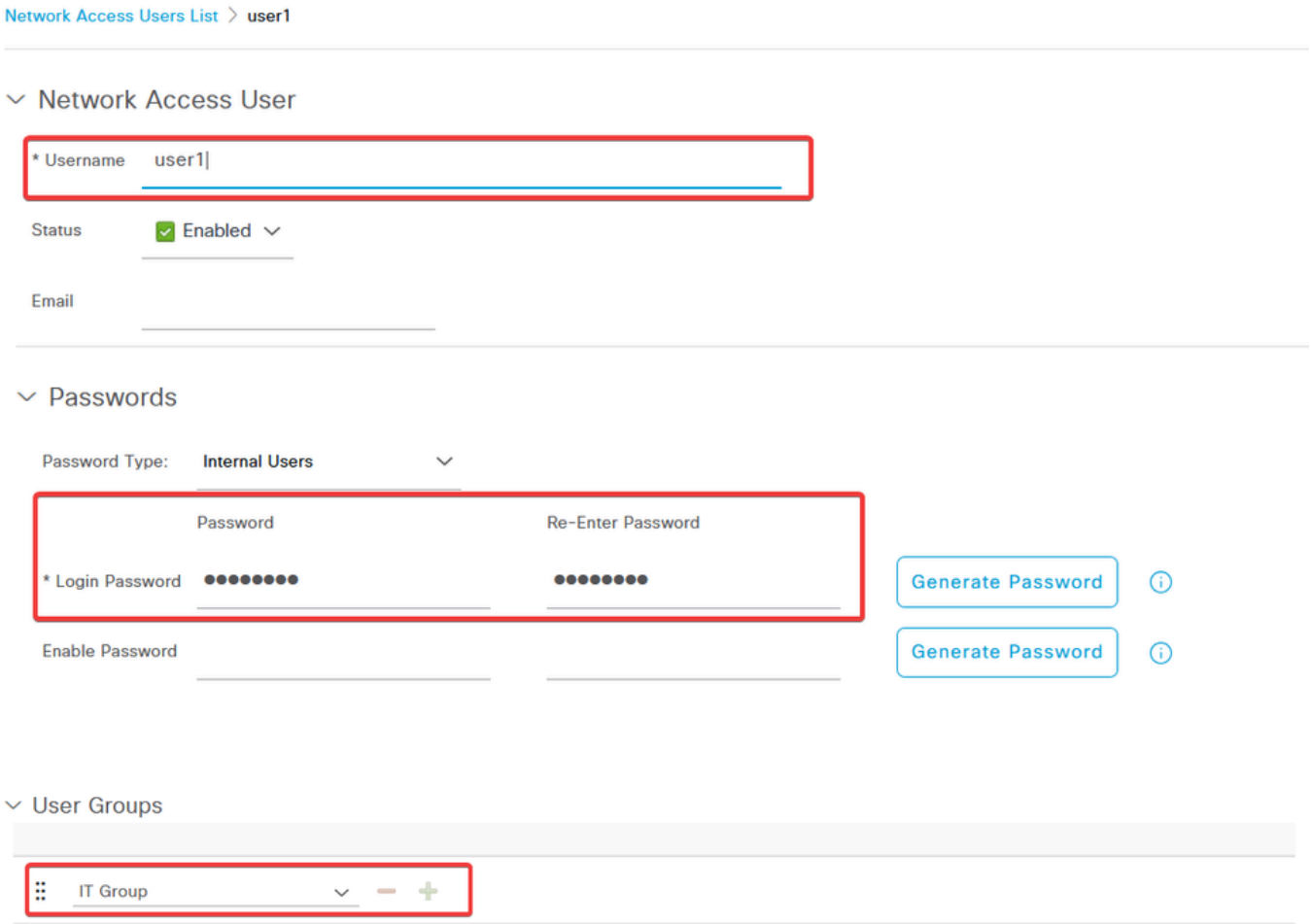


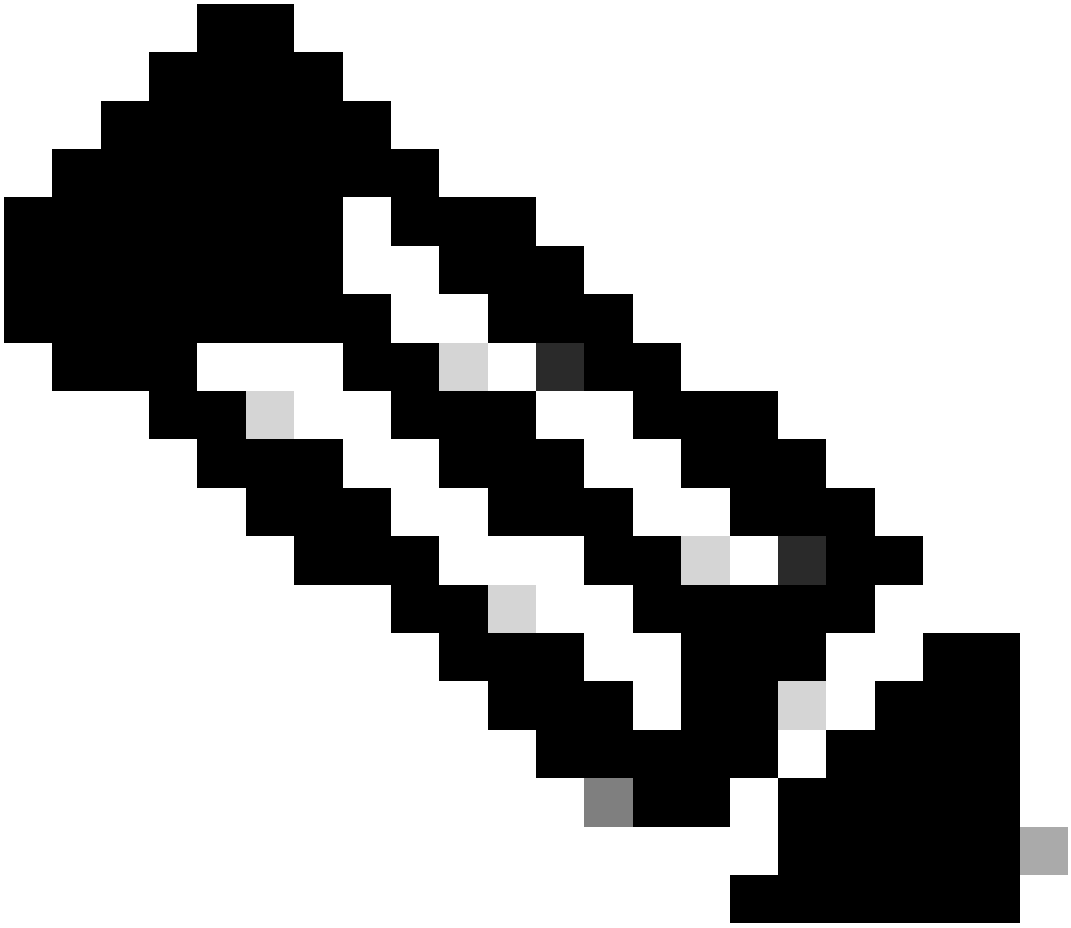
e. Klicken Sie auf Add, um einen neuen Benutzer in der lokalen Serverdatenbank zu erstellen.

Geben Sie das Username und **Login Password** ein. Navigieren Sie dann zum Ende dieser Seite, und wählen Sie die User Group.

Klicken Sie auf **Save**.



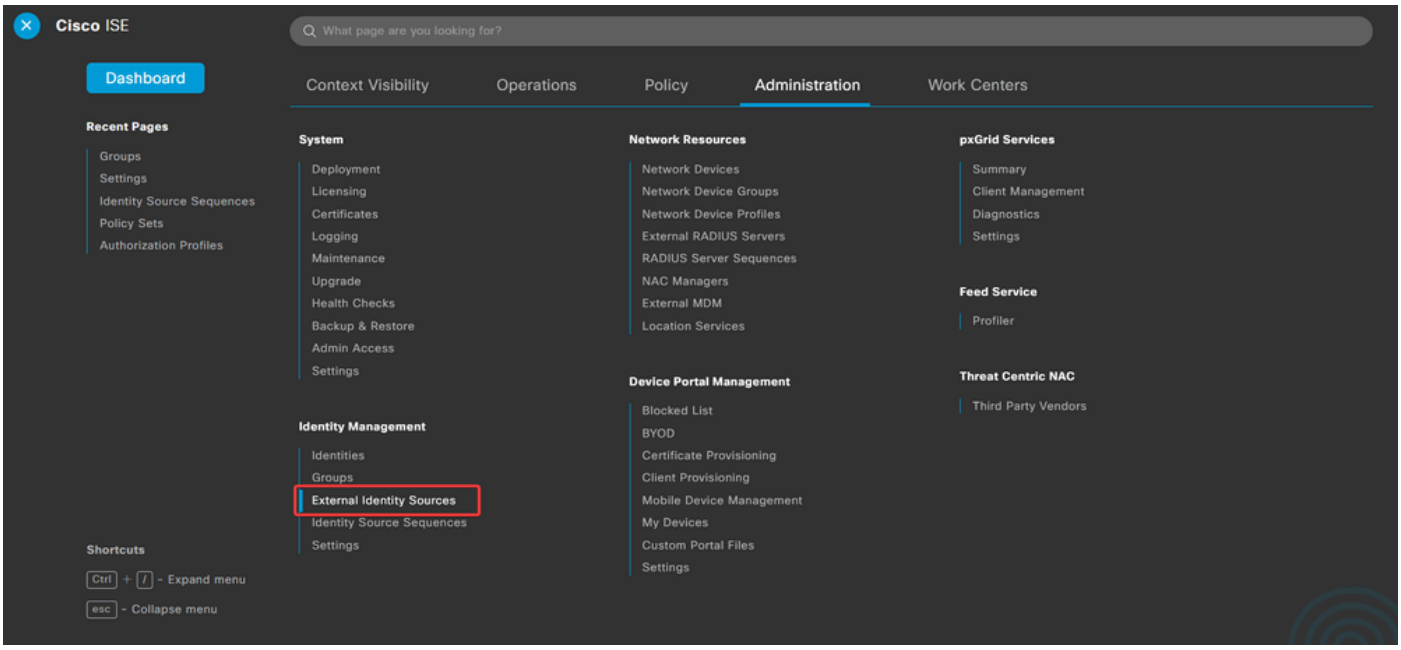

Network Access Users List
user1
Network Access User
* Username
user1
Status
Enabled
Email
Passwords
Password Type:
Internal Users
Password
Re-Enter Password
* Login Password
Generate Password
Enable Password
Generate Password
User Groups
IT Group



Hinweis: Sie müssen einen Benutzernamen und ein Kennwort konfigurieren, um interne Benutzer zu erstellen. Auch wenn dies für die RAVPN-Authentifizierung mithilfe von Zertifikaten nicht erforderlich ist, können diese Benutzer für andere interne Dienste verwendet werden, für die ein Kennwort erforderlich ist. Verwenden Sie daher ein sicheres Kennwort.

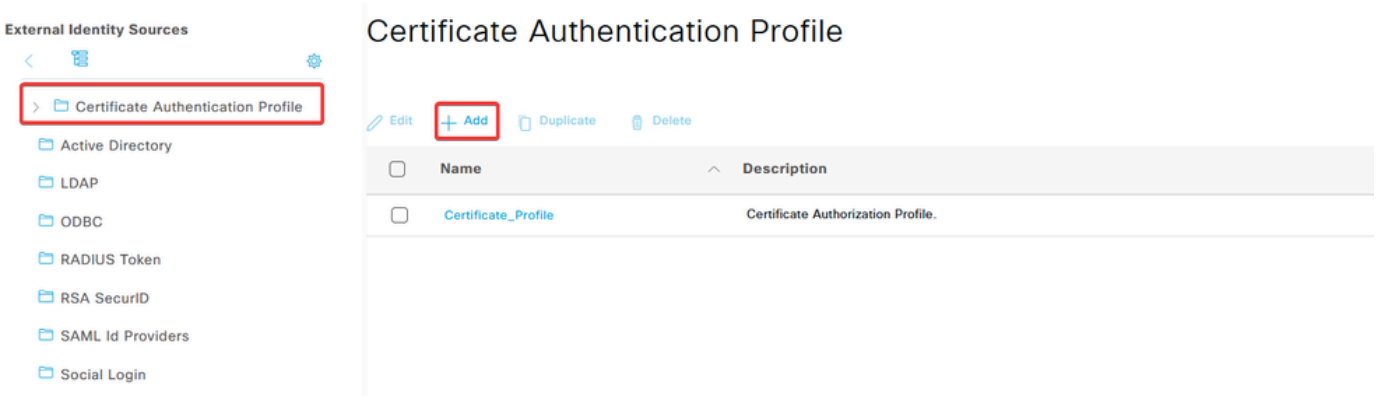
---

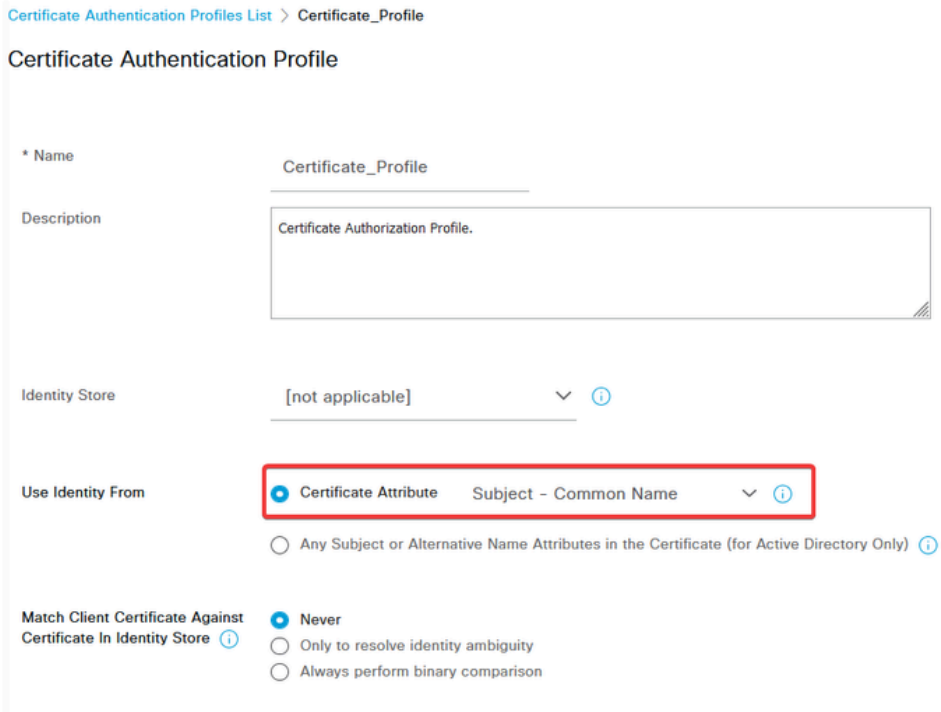
f. Navigieren Sie zu **Administration** > **Identity Management** > **External Identify Sources**.



g. Klicken Sie auf`Add`, um eine **Certificate Authentication Profile**zu erstellen.

Das Zertifikatauthentifizierungsprofil legt fest, wie Clientzertifikate validiert werden. Dazu gehört auch, welche Felder im Zertifikat überprüft werden können (alternativer Name des Antragstellers, allgemeiner Name usw.).

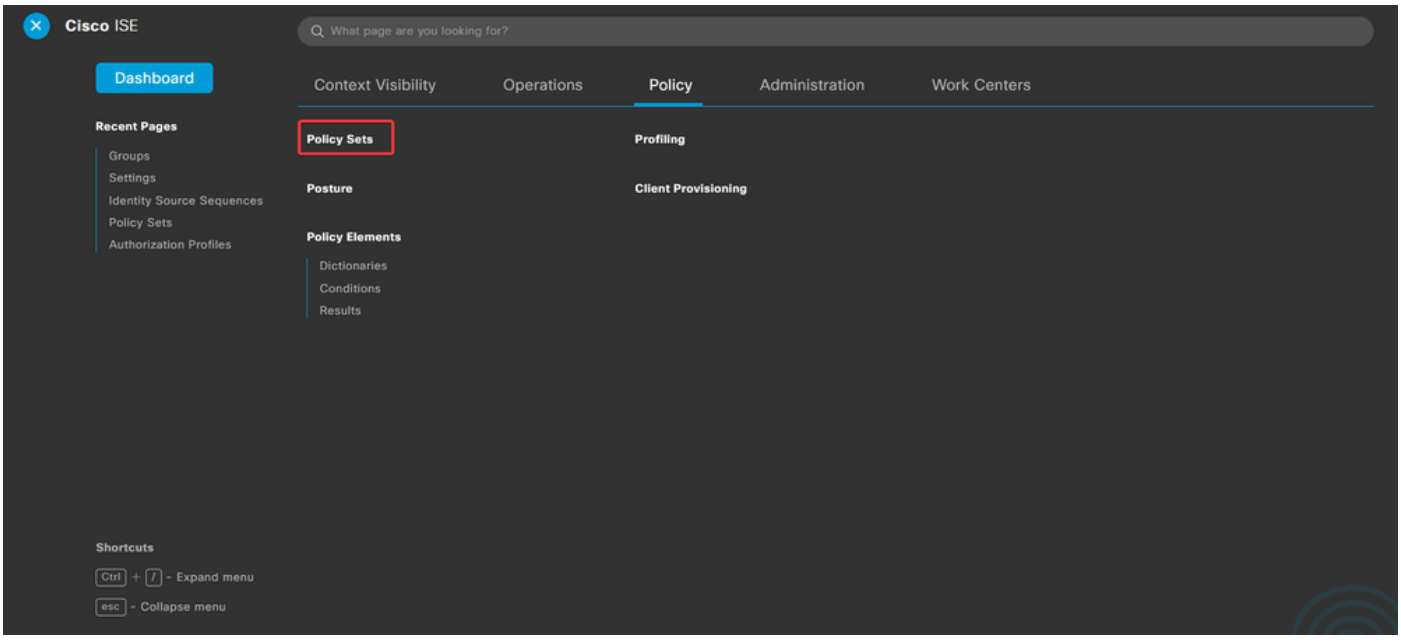




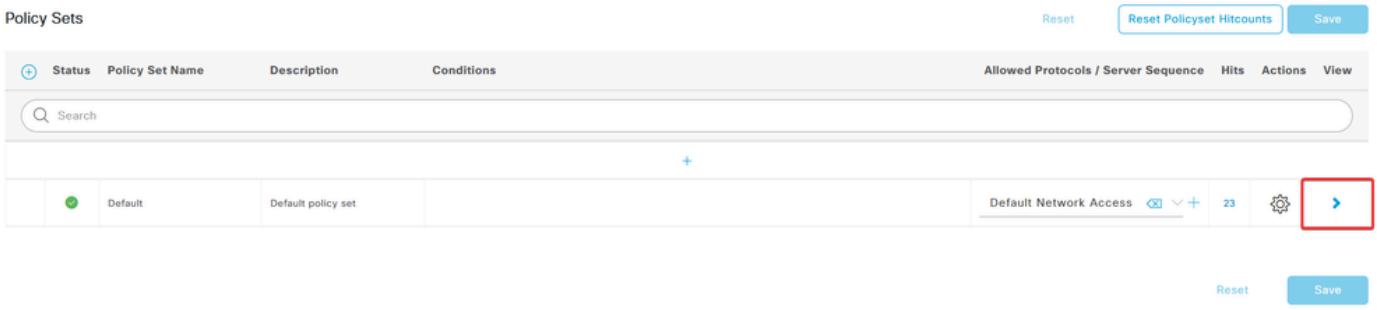
Schritt 3.2: Konfigurieren der Authentifizierungsrichtlinie

Die Authentifizierungsrichtlinie wird verwendet, um zu authentifizieren, dass die Anforderung von der Firewall und dem spezifischen Verbindungsprofil stammt.

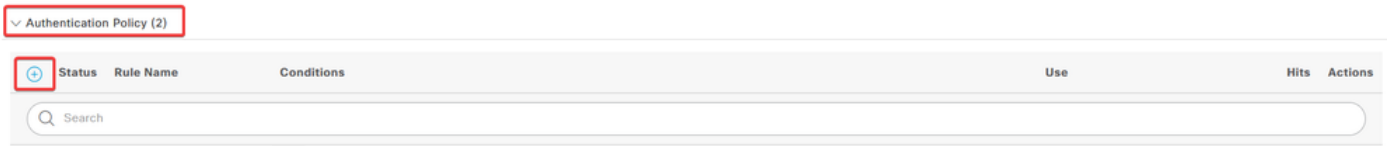
a. Navigieren Sie zu **Policy > Policy Sets.**



Wählen Sie die Standard-Autorisierungsrichtlinie aus, indem Sie auf den Pfeil rechts im Bildschirm klicken:

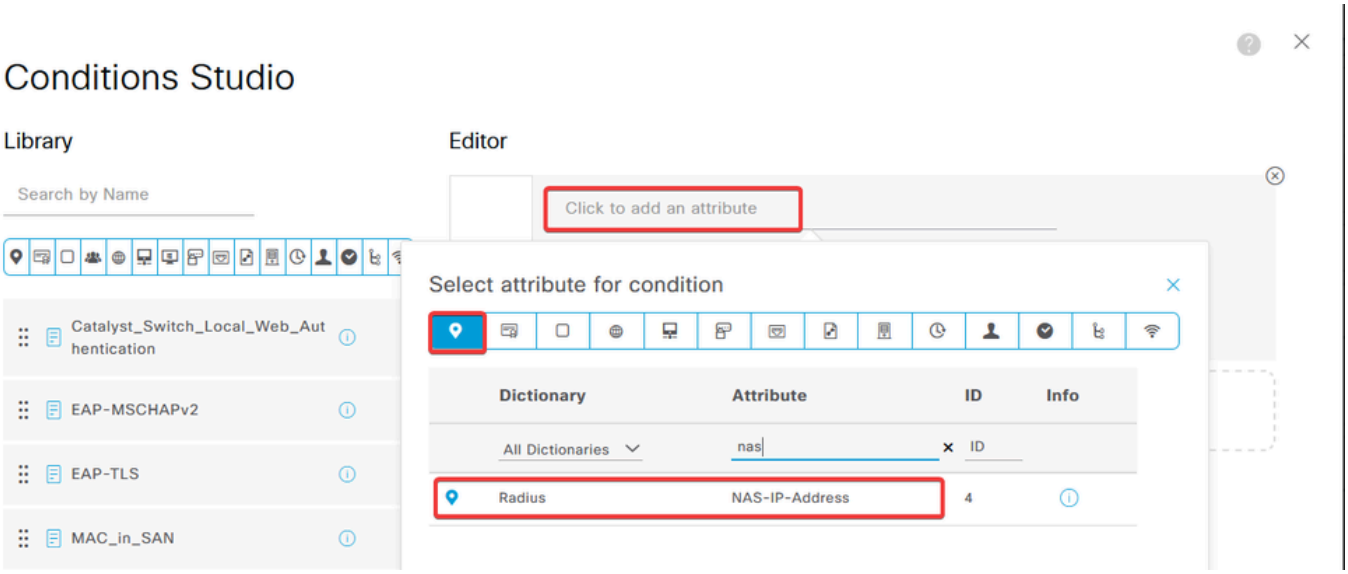


b. Klicken Sie auf den Dropdown-Menüpfeil nebenAuthentication Policy, um ihn zu erweitern. Klicken Sie dann auf das **add (+)** Symbol, um eine neue Regel hinzuzufügen.

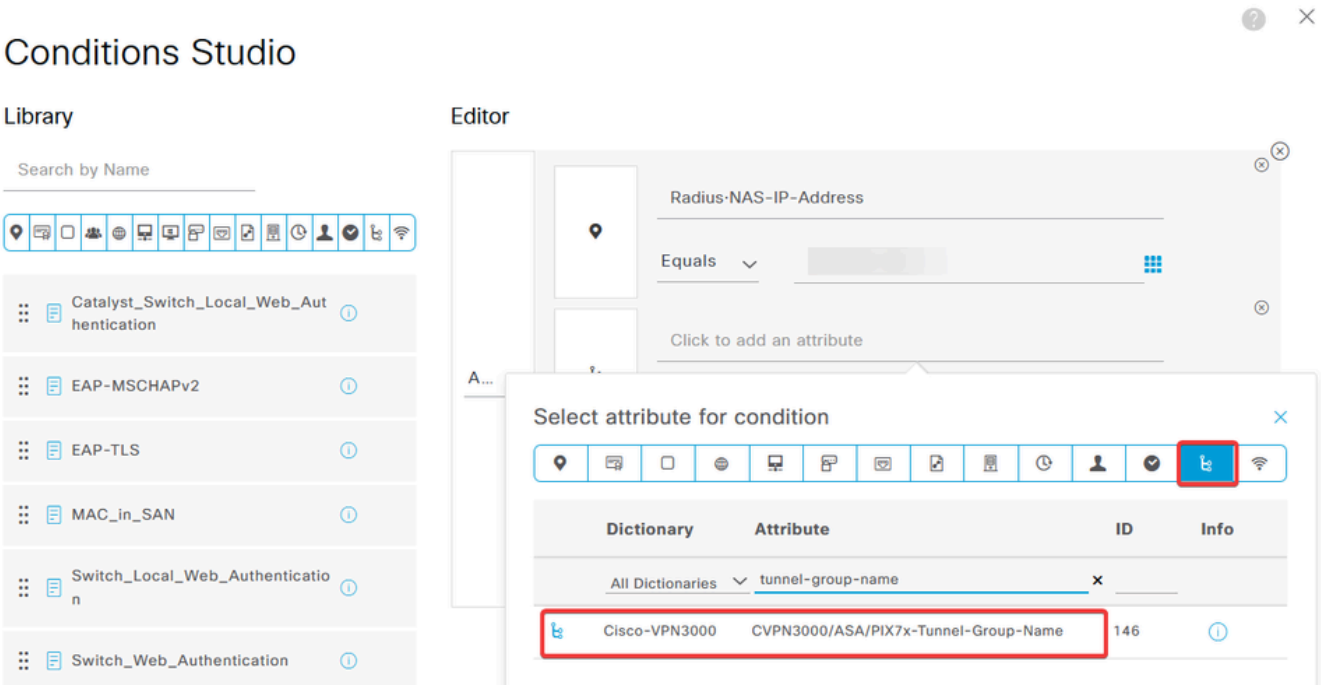


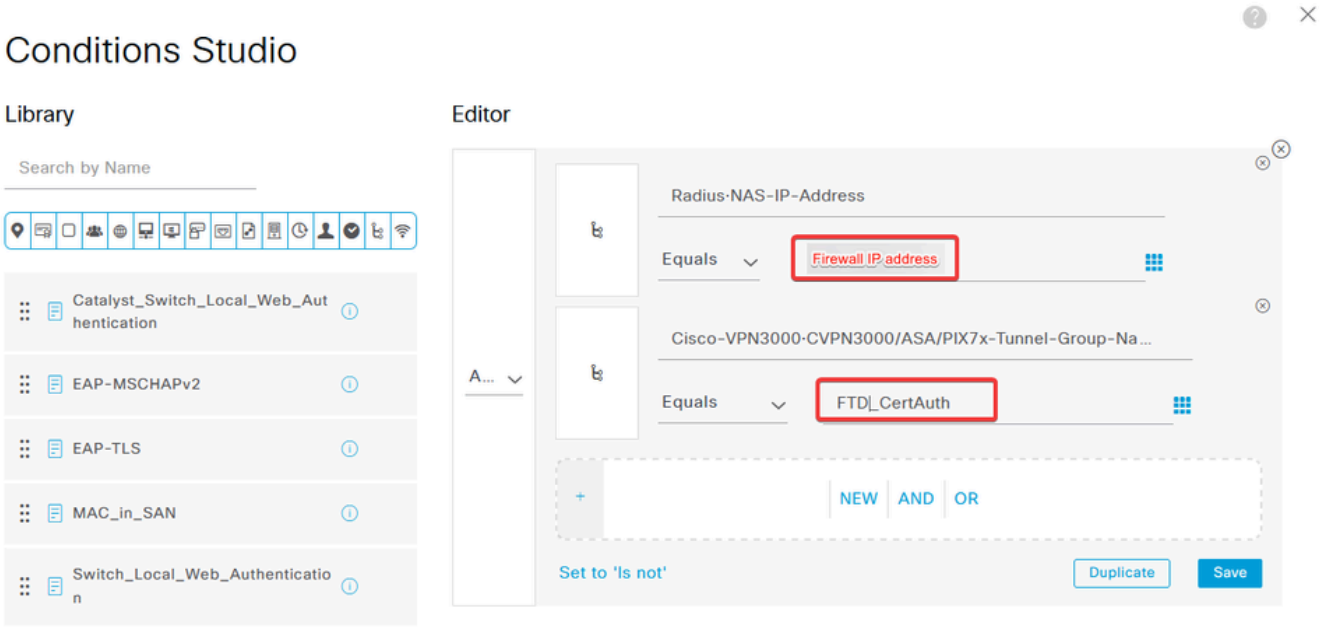
add (+)Geben Sie den Namen für die Regel ein, und wählen Sie das Symbol in der Spalte Bedingungen aus.

c. Klicken Sie auf das Textfeld Attribute-Editor und anschließend auf dasNAS-IP-AddressSymbol. Geben Sie die IP-Adresse der Firewall ein.

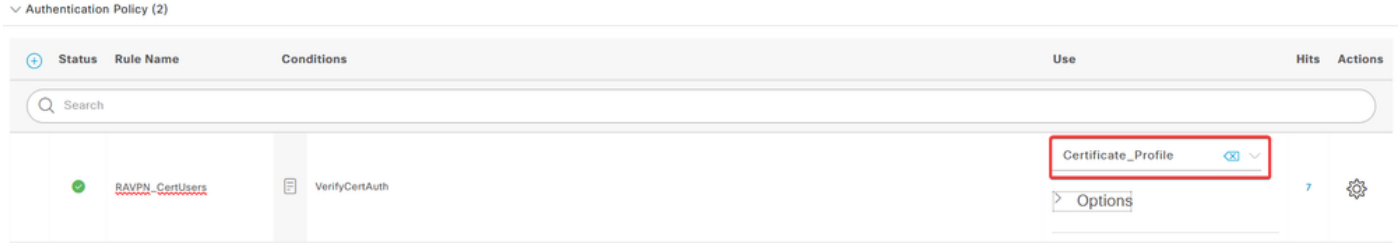


d. Klicken Sie auf **New** , und fügen Sie dann das andere AttributTunnel-Group-namehinzu. Geben Sie denConnection ProfileNamen ein, der auf dem FMC konfiguriert wurde.





e. Wählen Sie in der Spalte "Verwenden" die **Certificate Authentication Profile** erstellte aus. Auf diese Weise werden die im Profil definierten Informationen angegeben, die zur Identifizierung der Benutzer verwendet werden.

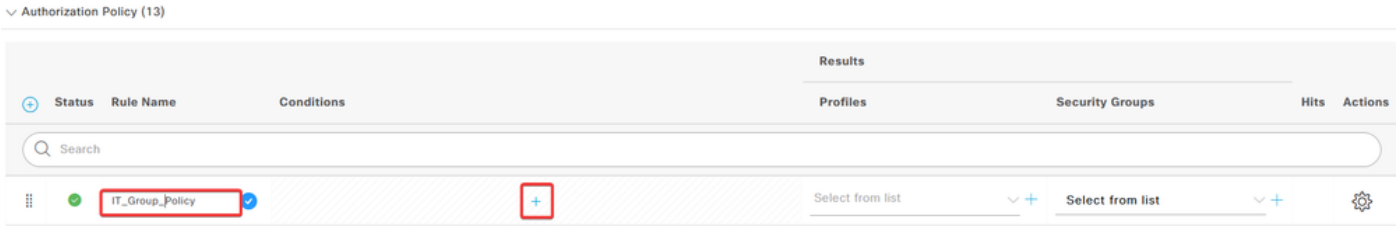


Klicken Sie auf .Save

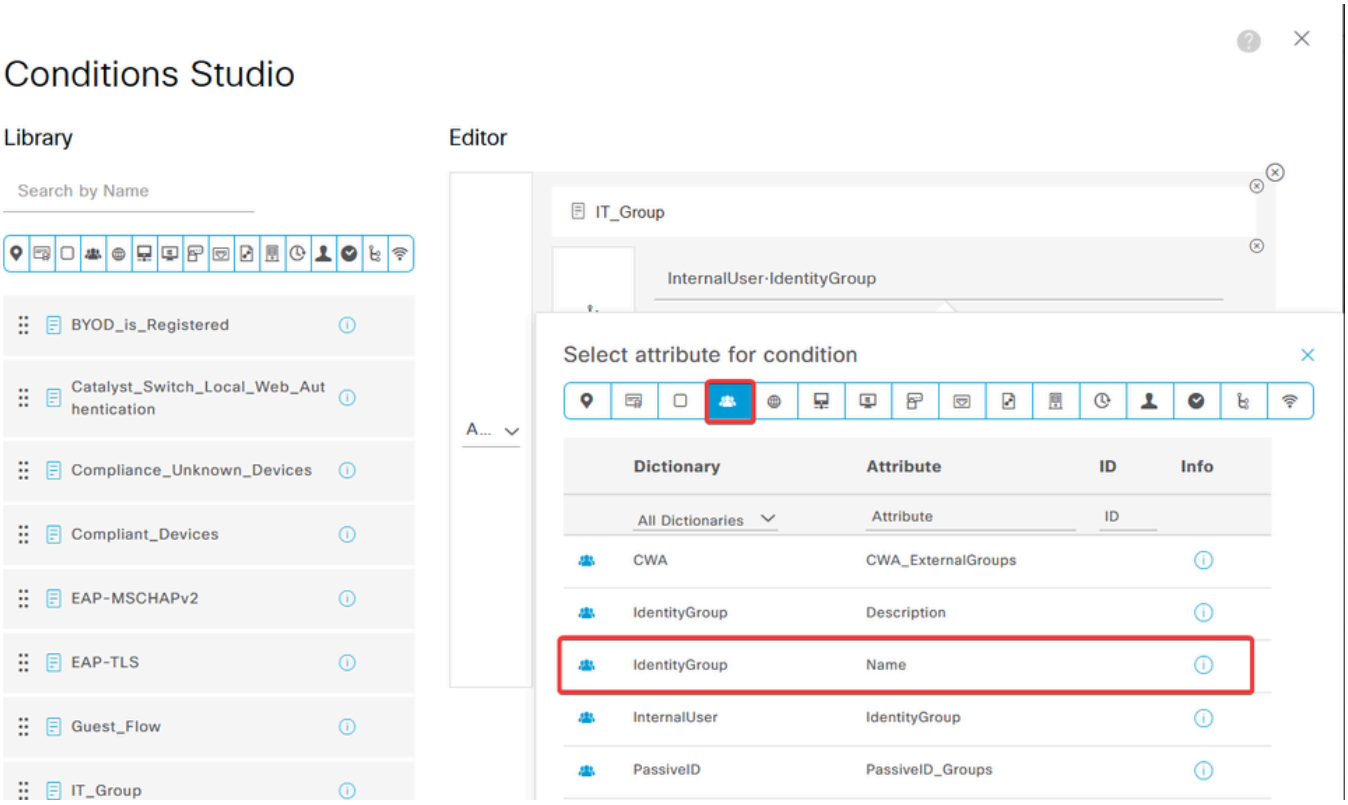
Schritt 3.3: Konfigurieren der Autorisierungsrichtlinie

a. Klicken Sie auf den Dropdown-Menüpfeil nebenAuthorization Policy, um ihn zu erweitern. Klicken Sie dann auf das **add (+)** Symbol, um eine neue Regel hinzuzufügen.

Geben Sie den Namen für die Regel ein, und wählen Sie das **add (+)** Symbol in der Spalte Bedingungen aus.

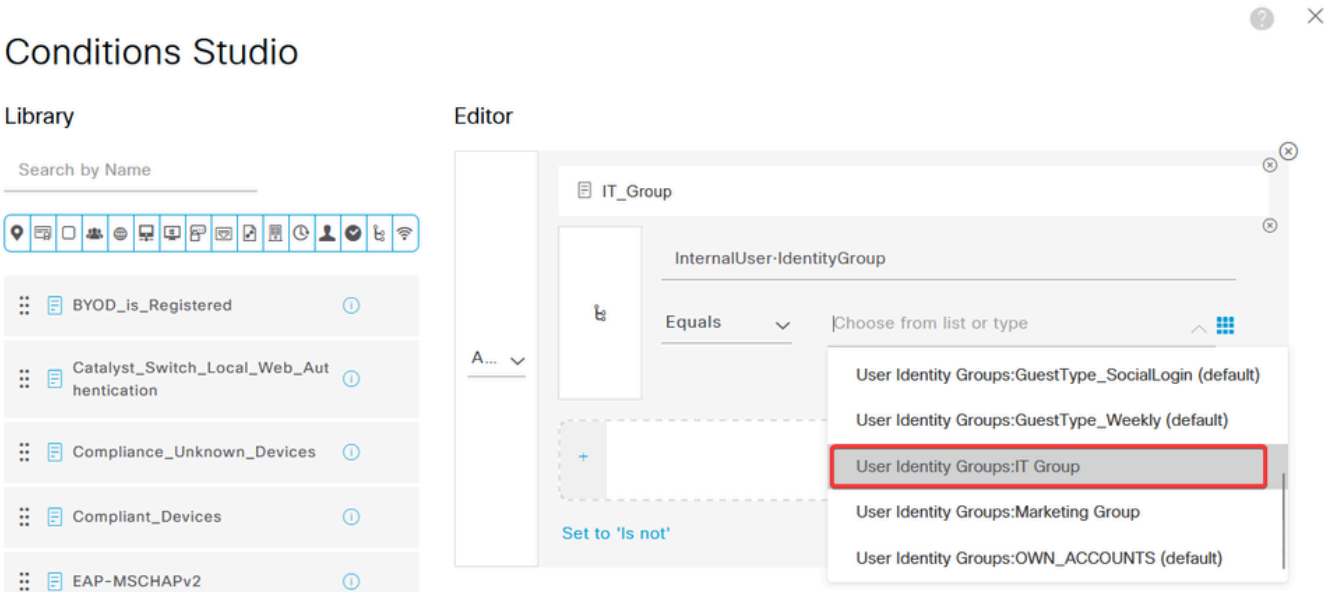


b. Klicken Sie auf das Textfeld Attribute-Editor und anschließend auf dasIdentity groupSymbol. Wählen Sie das **Identity group - Name** Attribut aus.

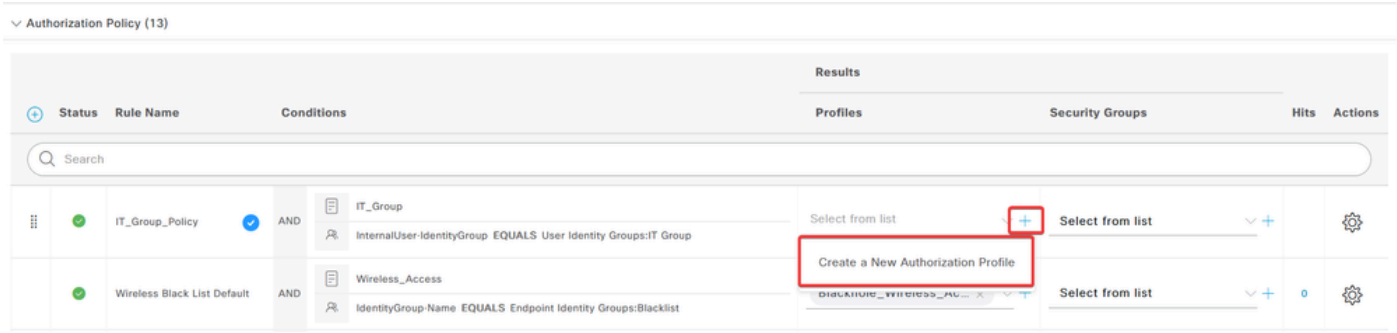


Wählen SieEqualsals Operator aus, klicken Sie auf den Pfeil des Dropdown-Menüs, um die verfügbaren Optionen anzuzeigen, und wählen Sie **User Identity Groups:**

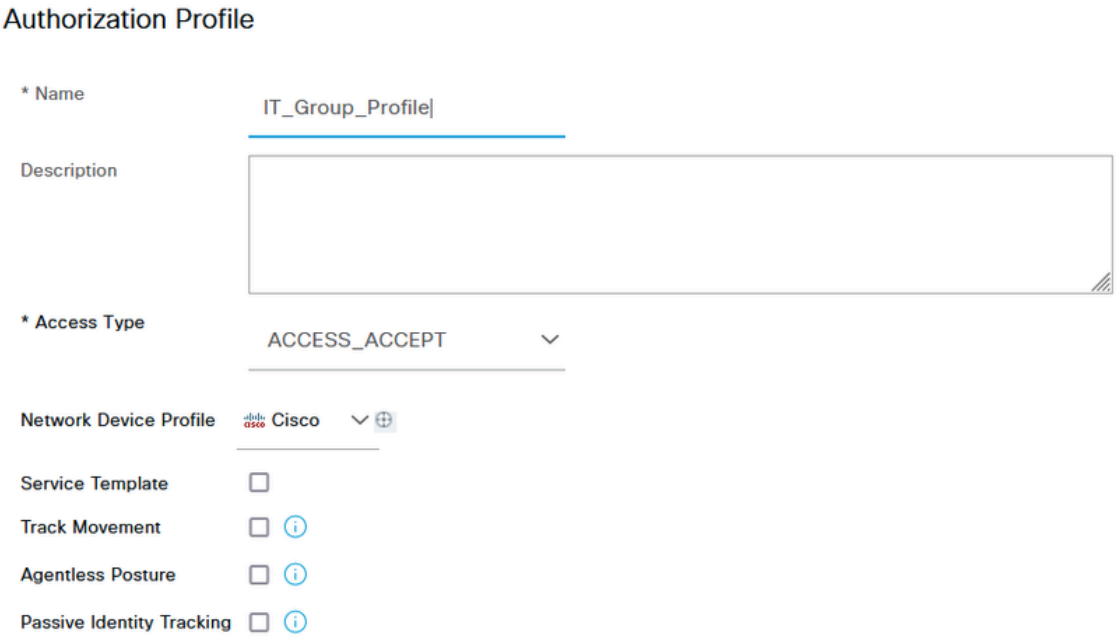
.



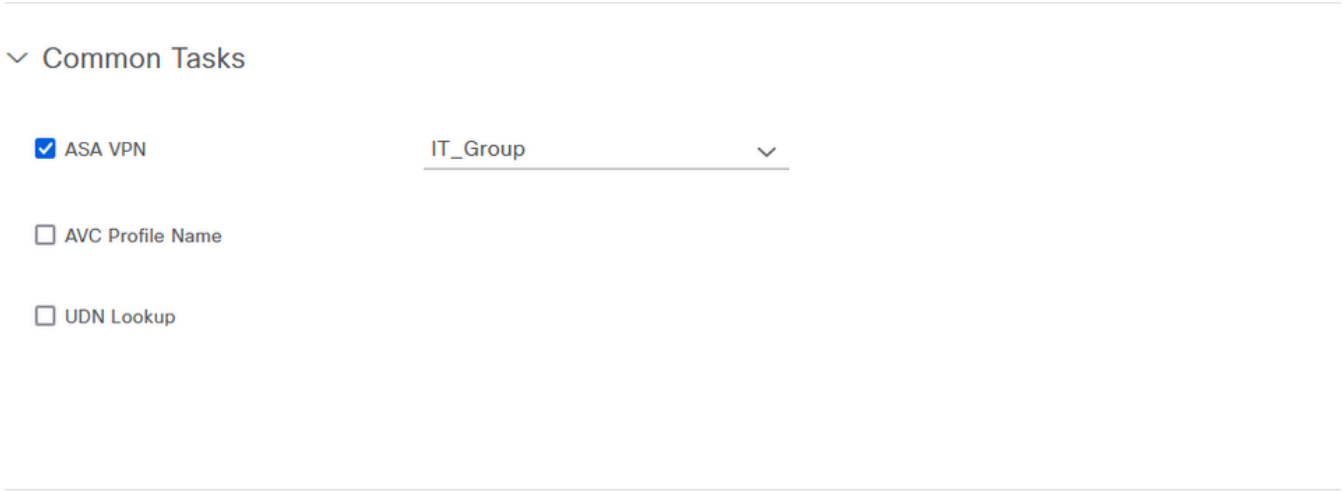
c. Klicken Sie in der Spalte Profile auf das add (+) Symbol, und wählen Sie **Create a New Authorization Profile**.



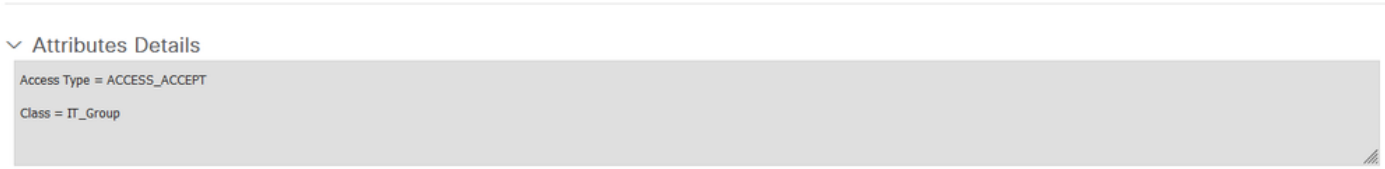
Geben Sie das Profil **Name** ein.



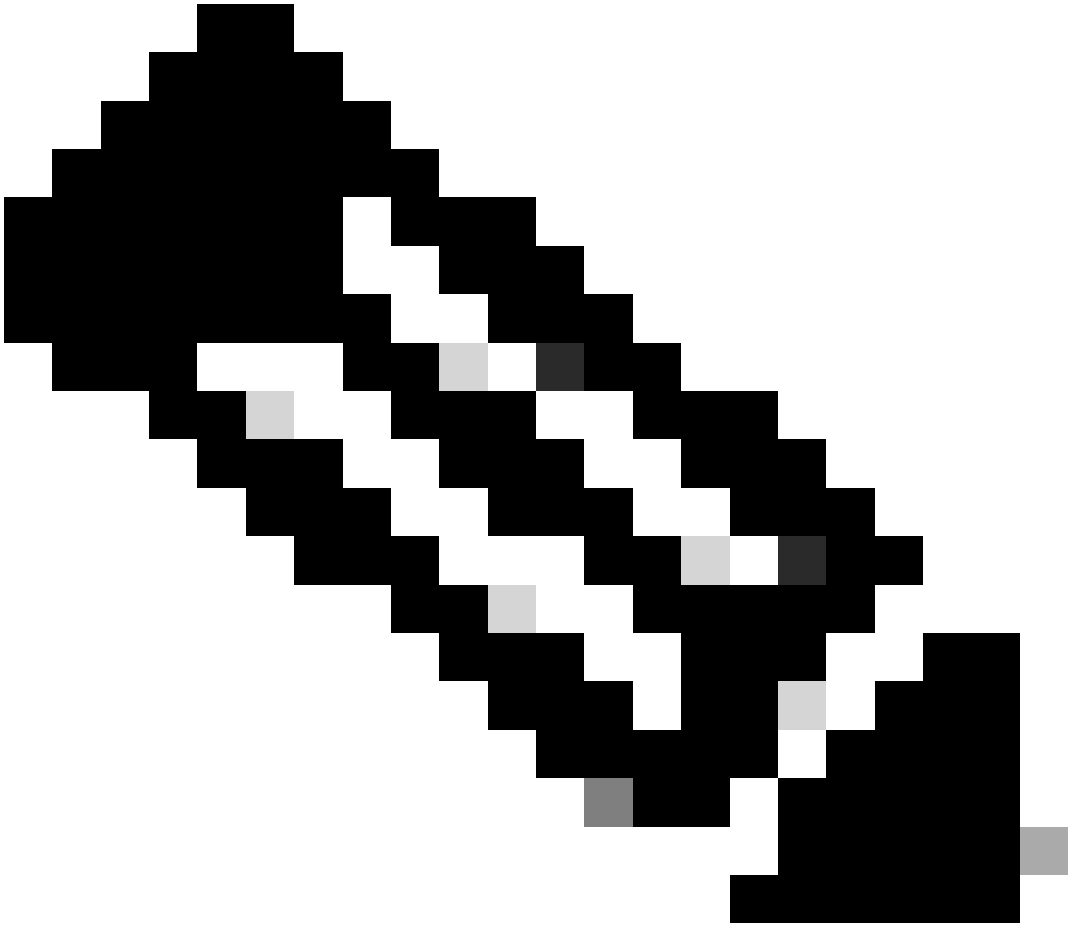
Navigieren Sie zu, **Common Tasks** und aktivieren Sie **ASA VPN**. Geben Sie dann den Befehl **group policy name**ein, der mit dem auf dem FMC erstellten identisch sein muss.



Die Attribute, die als Nächstes folgen, wurden jeder Gruppe zugewiesen:



Klicken Sie auf Speichern.



Hinweis: Wiederholen Sie Schritt 3.3: Konfigurieren Sie die Autorisierungsrichtlinie für jede erstellte Gruppe.

Überprüfung

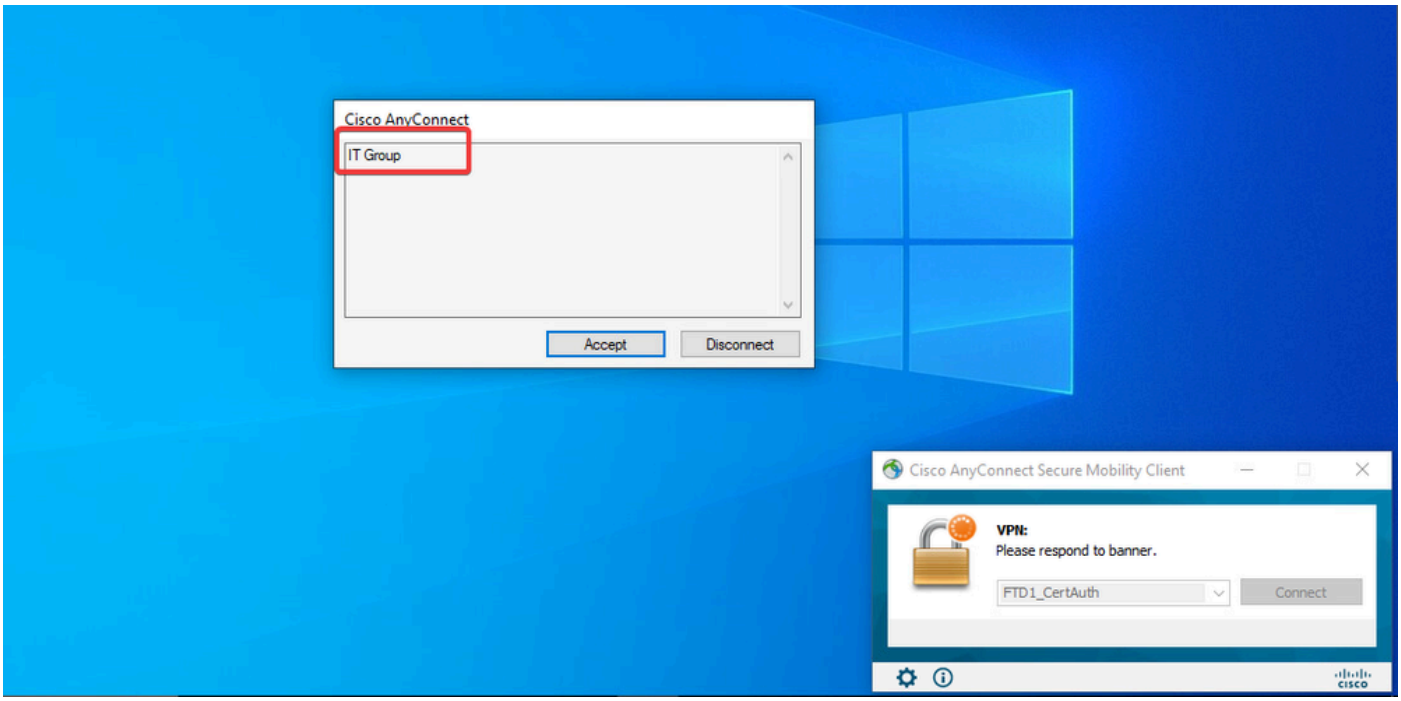
1. Führen Sie den Befehl`show vpn-sessiondb anyconnect`aus, und überprüfen Sie, ob der Benutzer die richtige Gruppenrichtlinie verwendet.

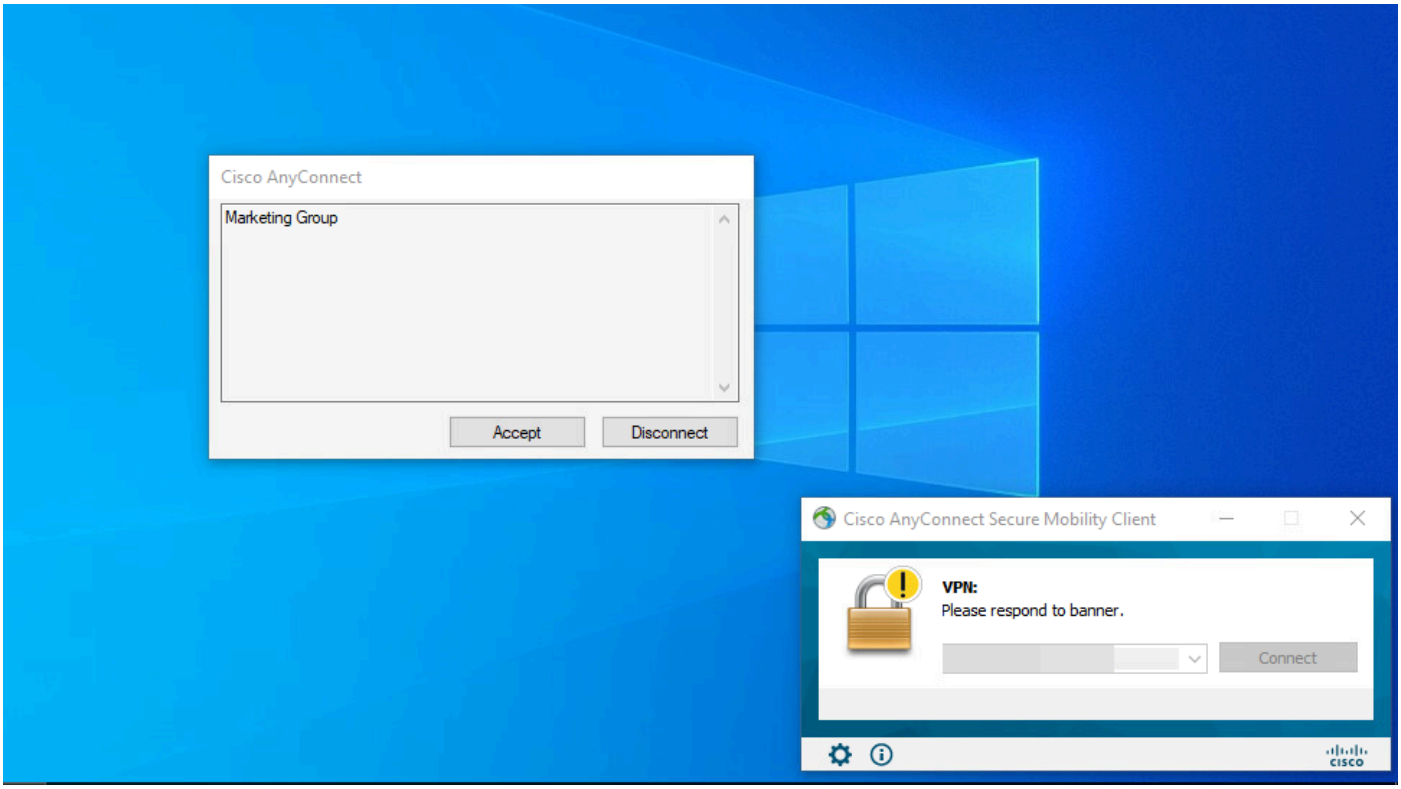
<#root>

```
firepower#
show vpn-sessiondb anyconnect


Session Type : AnyConnect
Username     : user1
```

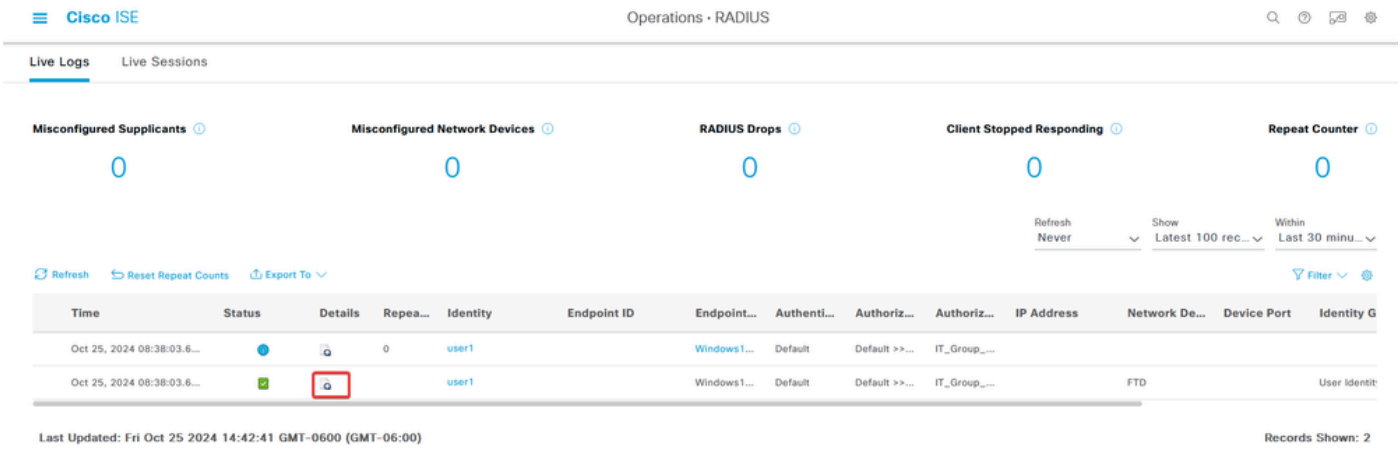
```
                Index        : 64
Assigned IP   : 192.168.55.2           Public IP    :
Protocol      : AnyConnect-Parent
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none
Hashing       : AnyConnect-Parent: (1)none
Bytes Tx      : 15084                  Bytes Rx     : 99611

Group Policy  : IT_Group               Tunnel Group : FTD_CertAuth


Login Time    : 22:21:43 UTC Tue Oct 22 2024
Duration      : 3h:03m:50s
Inactivity    : 0h:41m:44s
VLAN Mapping  : N/A                    VLAN         : none
Audt Sess ID  : 96130a0f0004000067182577
Security Grp  : none                   Tunnel Zone  : 0


Username      : User2

                  Index        : 70
Assigned IP   : 192.168.55.3           Public IP    :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 15112                  Bytes Rx     : 19738

Group Policy  : Marketing_Group        Tunnel Group : FTD_CertAuth


Login Time    : 01:23:08 UTC Wed Oct 23 2024
Duration      : 0h:02m:25s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                    VLAN         : none
Audt Sess ID  : 96130a0f0004600067184ffc
Security Grp  : none                   Tunnel Zone  : 0

firepower#
```

2. In der Gruppenrichtlinie können Sie eine Bannermeldung konfigurieren, die angezeigt wird, wenn der Benutzer eine Verbindung herstellen kann. Jedes Banner kann verwendet werden, um die Gruppe zu identifizieren, die über eine Autorisierung verfügt.





3. Überprüfen Sie in Live-Protokollen, ob für die Verbindung die entsprechende Autorisierungsrichtlinie verwendet wird. Klicken Sie auf,Detailsund zeigen Sie den Authentifizierungsbericht an.



Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. Debugs können über die Diagnose-CLI des CSF für die Zertifikatauthentifizierung ausgeführt werden.

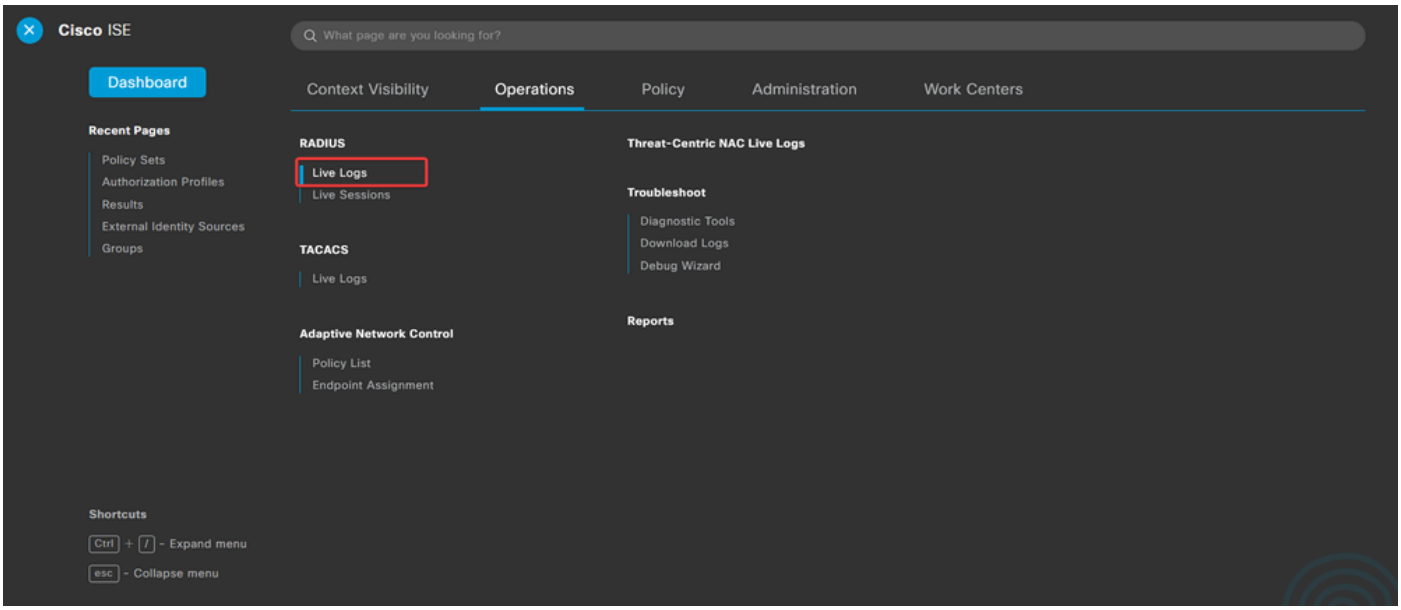
```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

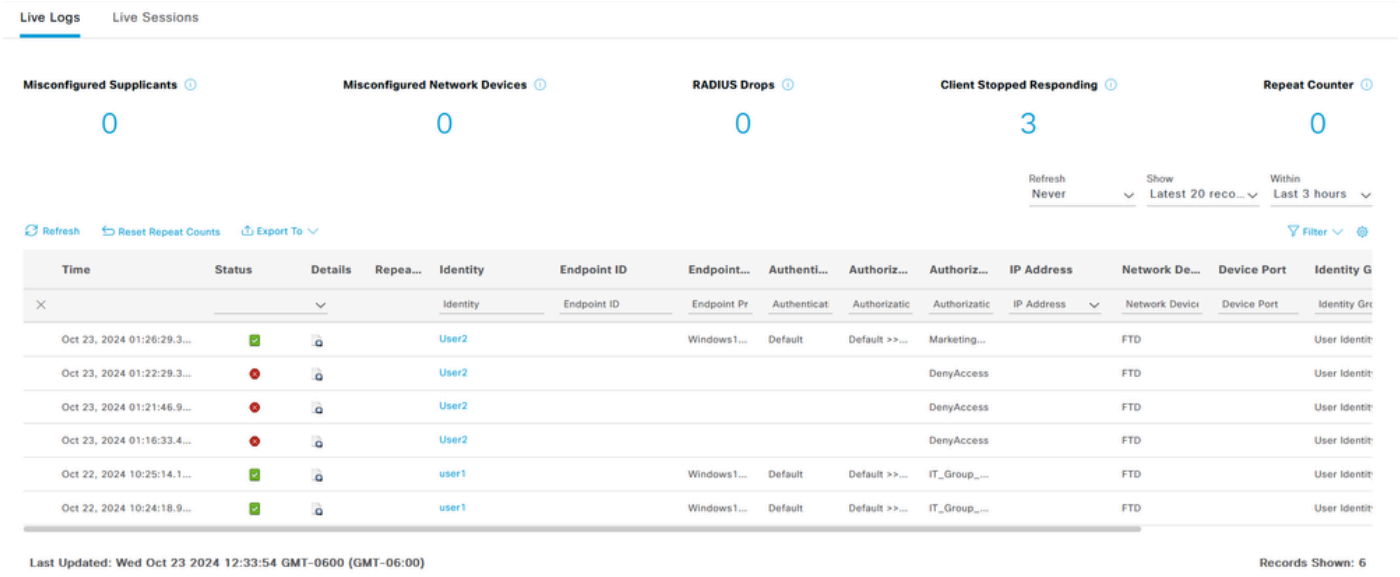
2. Verwenden Sie AAA-Debugs, um die Zuweisung von lokalen und/oder Remote-Attributen zu überprüfen.

```
debug aaa common 255
debug aaa shim 255
debug aaa authentication
debug aaa authorization
debug radius all
```

Auf der ISE:

1. Navigieren Sie zuOperations > RADIUS > Live Logs.


Cisco ISE
What page are you looking for?
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Recent Pages
Policy Sets
Authorization Profiles
Results
External Identity Sources
Groups
RADIUS
Live Logs
Live Sessions
TACACS
Live Logs
Adaptive Network Control
Policy List
Endpoint Assignment
Threat-Centric NAC Live Logs
Troubleshoot
Diagnostic Tools
Download Logs
Debug Wizard
Reports
Shortcuts
Ctrl + / - Expand menu
esc - Collapse menu


Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
3
Repeat Counter
0
Refresh
Never
Show
Latest 20 reco...
Within
Last 3 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authenti...
Authoriz...
Authoriz...
IP Address
Network De...
Device Port
Identity G
Oct 23, 2024 01:26:29.3... User2 Windows1... Default Default >>... Marketing... FTD User Identit
Oct 23, 2024 01:22:29.3... User2 DenyAccess FTD User Identit
Oct 23, 2024 01:21:46.9... User2 DenyAccess FTD User Identit
Oct 23, 2024 01:16:33.4... User2 DenyAccess FTD User Identit
Oct 22, 2024 10:25:14.1... user1 Windows1... Default Default >>... IT_Group_... FTD User Identit
Oct 22, 2024 10:24:18.9... user1 Windows1... Default Default >>... IT_Group_... FTD User Identit
Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00)
Records Shown: 6

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.