Konfigurieren von ISE BYOD mit einer und zwei SSID in ISE 3.3

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie BYOD-Probleme auf der ISE konfiguriert und behoben werden.

Hintergrund

BYOD ist eine Funktion, mit der Benutzer ihre privaten Geräte an die ISE anbinden können, sodass die Benutzer die Netzwerkressource in der Umgebung nutzen können. Darüber hinaus kann der Netzwerkadministrator den Zugriff auf wichtige Ressourcen über private Geräte einschränken.

Im Gegensatz zu Gastdatenfluss, bei dem das Gerät mithilfe des internen Speichers oder Active Directory auf der ISE über die Gastseite authentifiziert wird. Bei BYOD kann der Netzwerkadministrator ein Endgeräteprofil auf dem Endgerät installieren, um den EAP-Methodentyp auszuwählen. In Szenarien wie EAP-TLS wird das Client-Zertifikat von der ISE selbst signiert, um eine Vertrauensstellung zwischen dem Endpunkt und der ISE zu schaffen.

Voraussetzungen

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

- WLC-Controller
- Grundlegendes zur ISE

Verwendete Komponente

Die folgenden Geräte sind nicht auf eine bestimmte Version für den BYOD-Workflow beschränkt:

- Catalyst Wireless Controller 9800-CL (17.12.3)
- ISE Virtual Machine (3.3)

Was bedeutet Single-SSID und Dual-SSID-BYOD auf der ISE?

BYOD mit einer SSID

In einer Single-SSID-BYOD-Konfiguration verbinden Benutzer ihre privaten Geräte direkt mit dem Wireless-Netzwerk des Unternehmens. Der Onboarding-Prozess erfolgt über dieselbe SSID, über die die ISE die Geräteregistrierung, -bereitstellung und -durchsetzung erleichtert. Dieser Ansatz vereinfacht die Benutzerumgebung, erfordert jedoch ein sicheres Onboarding und geeignete Authentifizierungsmethoden, um die Netzwerksicherheit zu gewährleisten.

Dual-SSID-BYOD

In einer Dual-SSID-BYOD-Konfiguration werden zwei separate SSIDs verwendet: eines für die Einbindung (ungesicherter oder beschränkter Zugriff) und eines für den Zugriff auf das

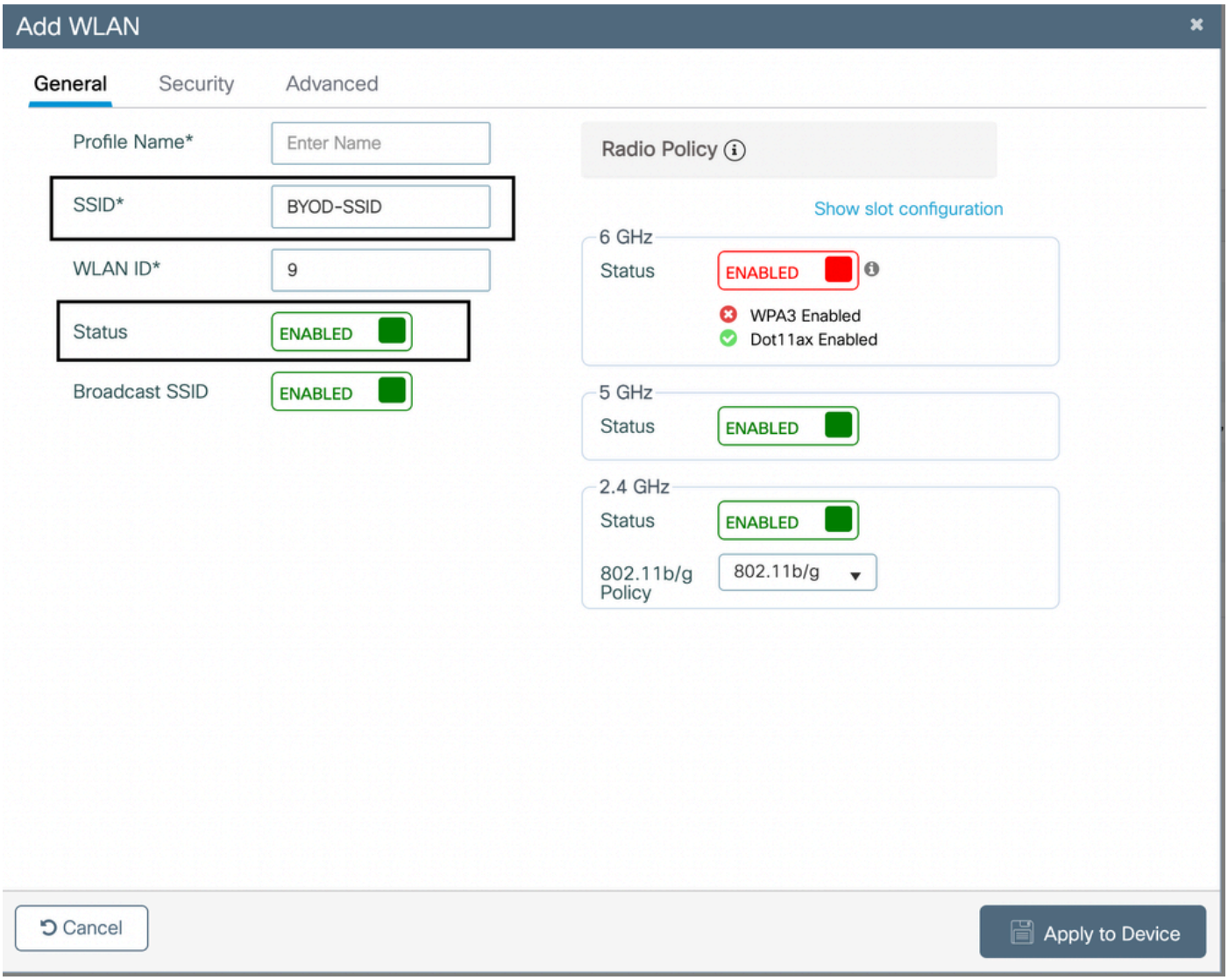
Unternehmensnetzwerk. Die Benutzer stellen zunächst eine Verbindung mit der integrierten SSID her, schließen die Geräteregistrierung und -bereitstellung über die ISE ab und wechseln dann zum sicheren Unternehmens-SSID für den Netzwerkzugriff. Dadurch wird eine zusätzliche Sicherheitsebene geschaffen, indem der Onboarding-Datenverkehr vom Produktionsdatenverkehr getrennt wird.

WLC-Konfiguration

WLAN für CWA erstellen

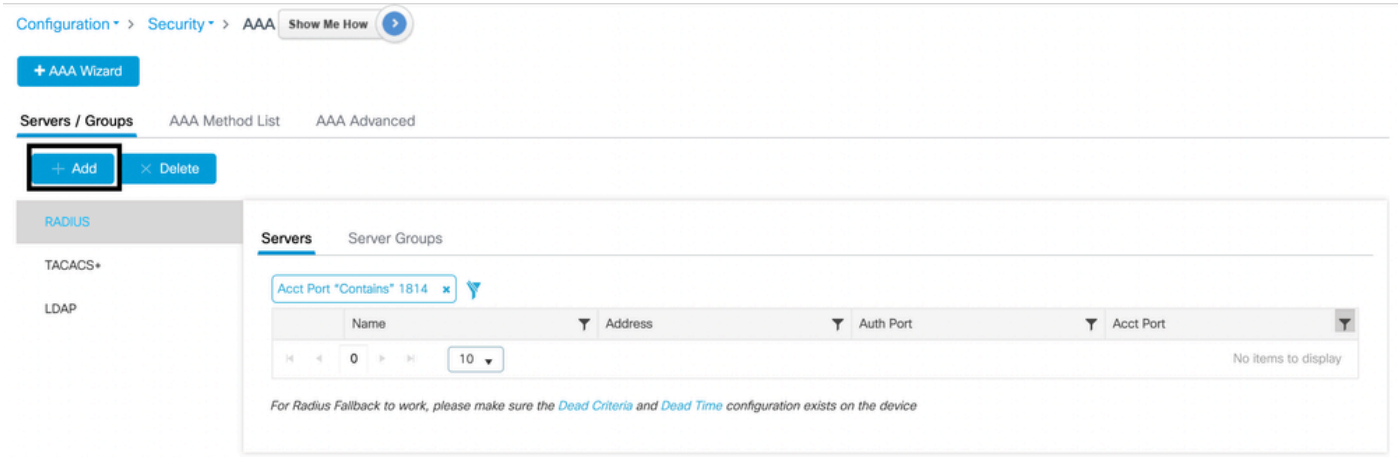
1. Gehen Sie zu Configuration > Tags & Profiles > WLANs.
2. Klicken Sie auf Hinzufügen, um ein neues WLAN zu erstellen.

    - Legen Sie einen WLAN-Namen und eine SSID fest (z. B. BYOD-Wi-Fi).
    - Aktivieren des WLAN

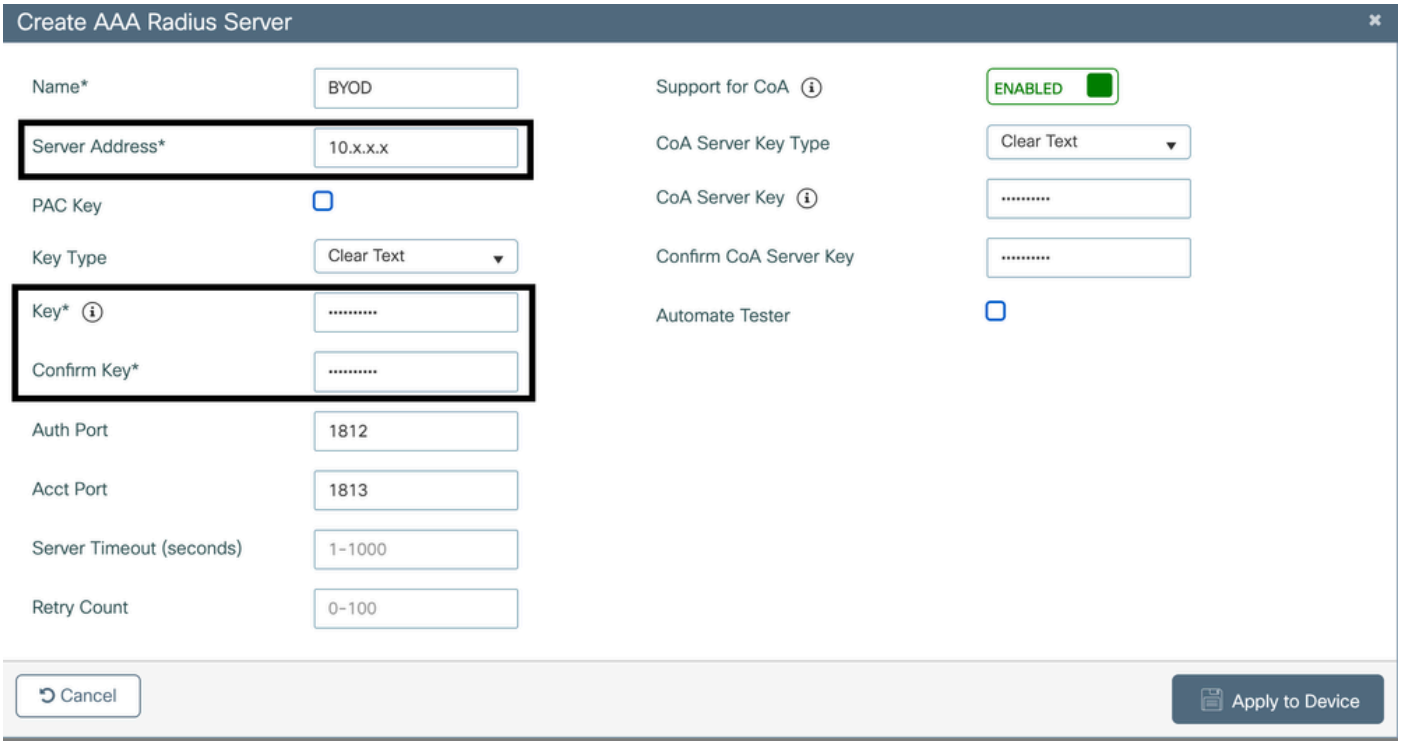


Konfigurieren von RADIUS-Servern

1. Navigieren Sie zu Configuration > Security > AAA > RADIUS > Servers.

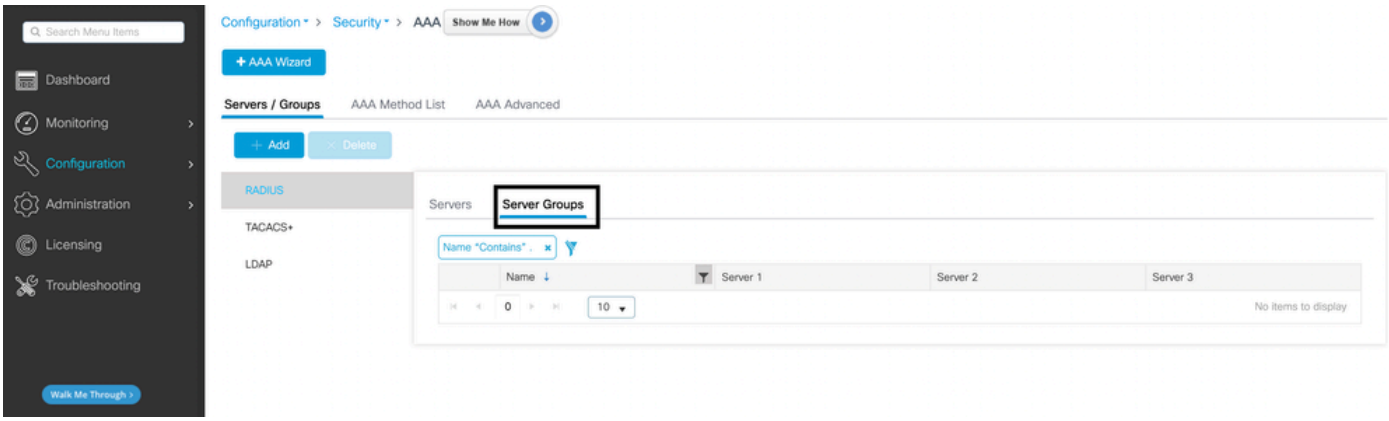


2. Klicken Sie auf Hinzufügen, um ISE als RADIUS-Server zu konfigurieren:
   - Server-IP: IP-Adresse der ISE
   - Gemeinsamer Schlüssel: Ordnen Sie den auf der ISE konfigurierten gemeinsamen geheimen Schlüssel zu.

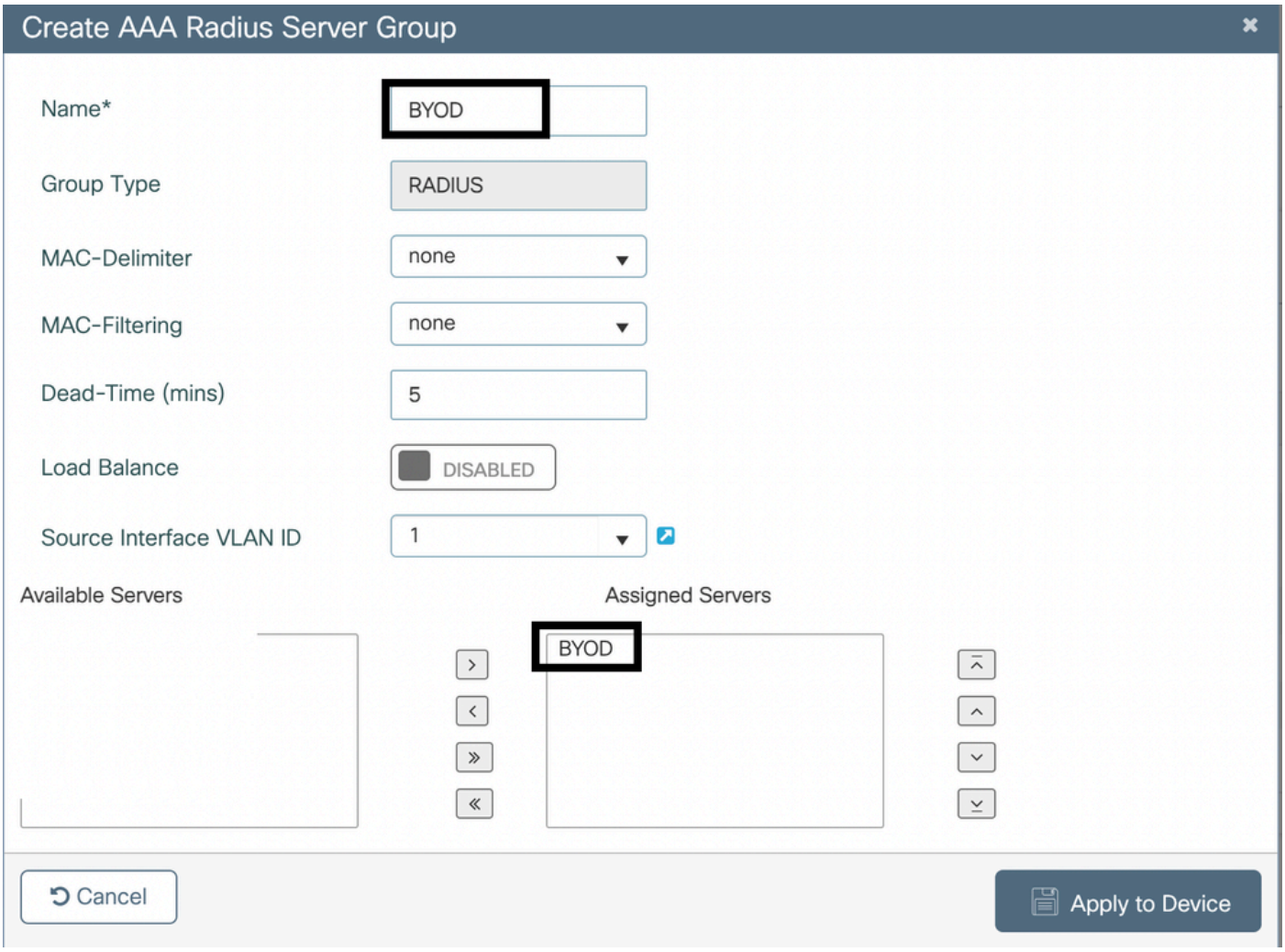


AAA-Server konfigurieren

1. Navigieren Sie zu Configuration > Security > AAA > Servers/Groups (Konfiguration > Sicherheit > AAA > Server/Gruppen).



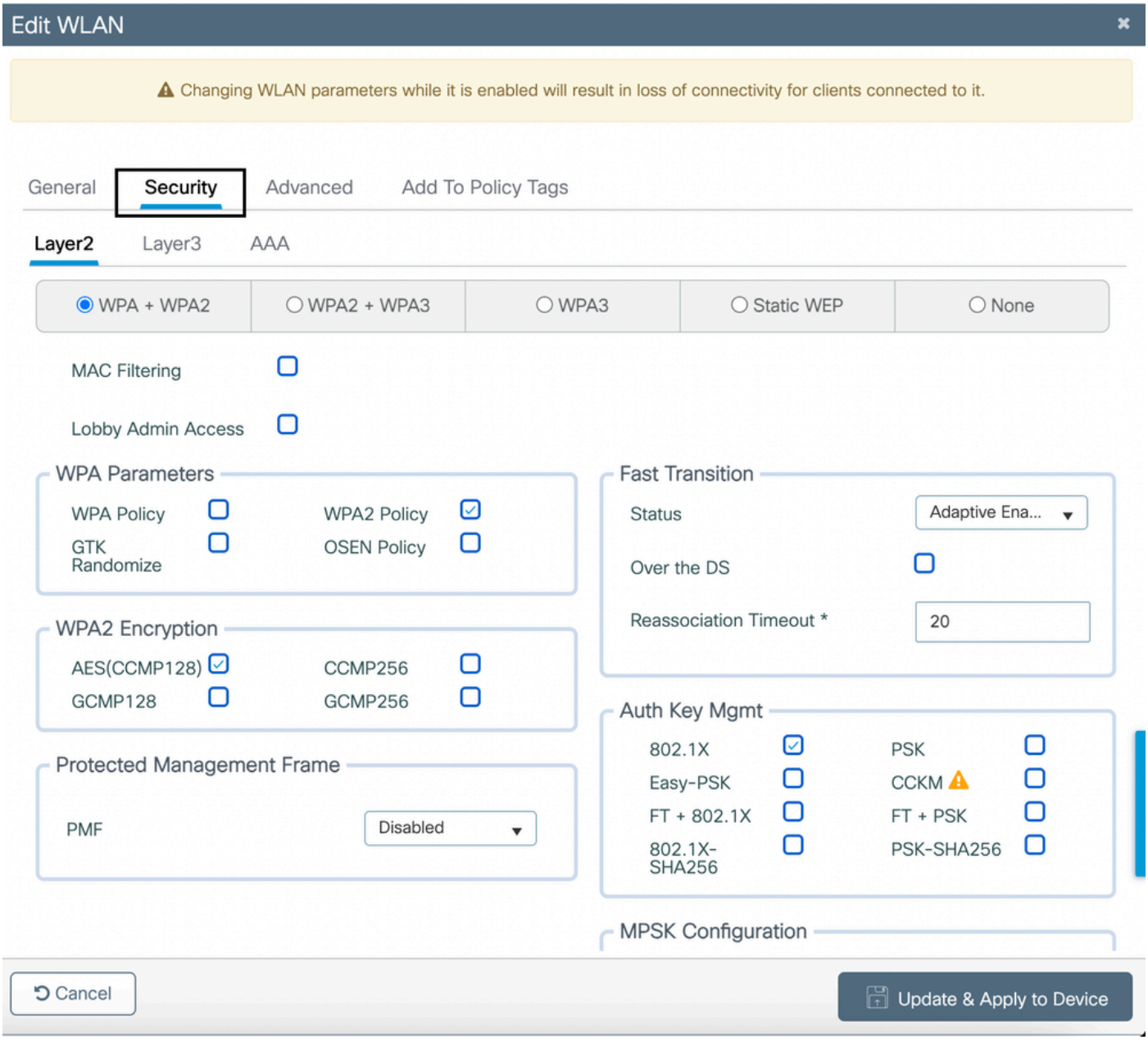
2. Weisen Sie den RADIUS-Server einer neuen oder vorhandenen Servergruppe zu.



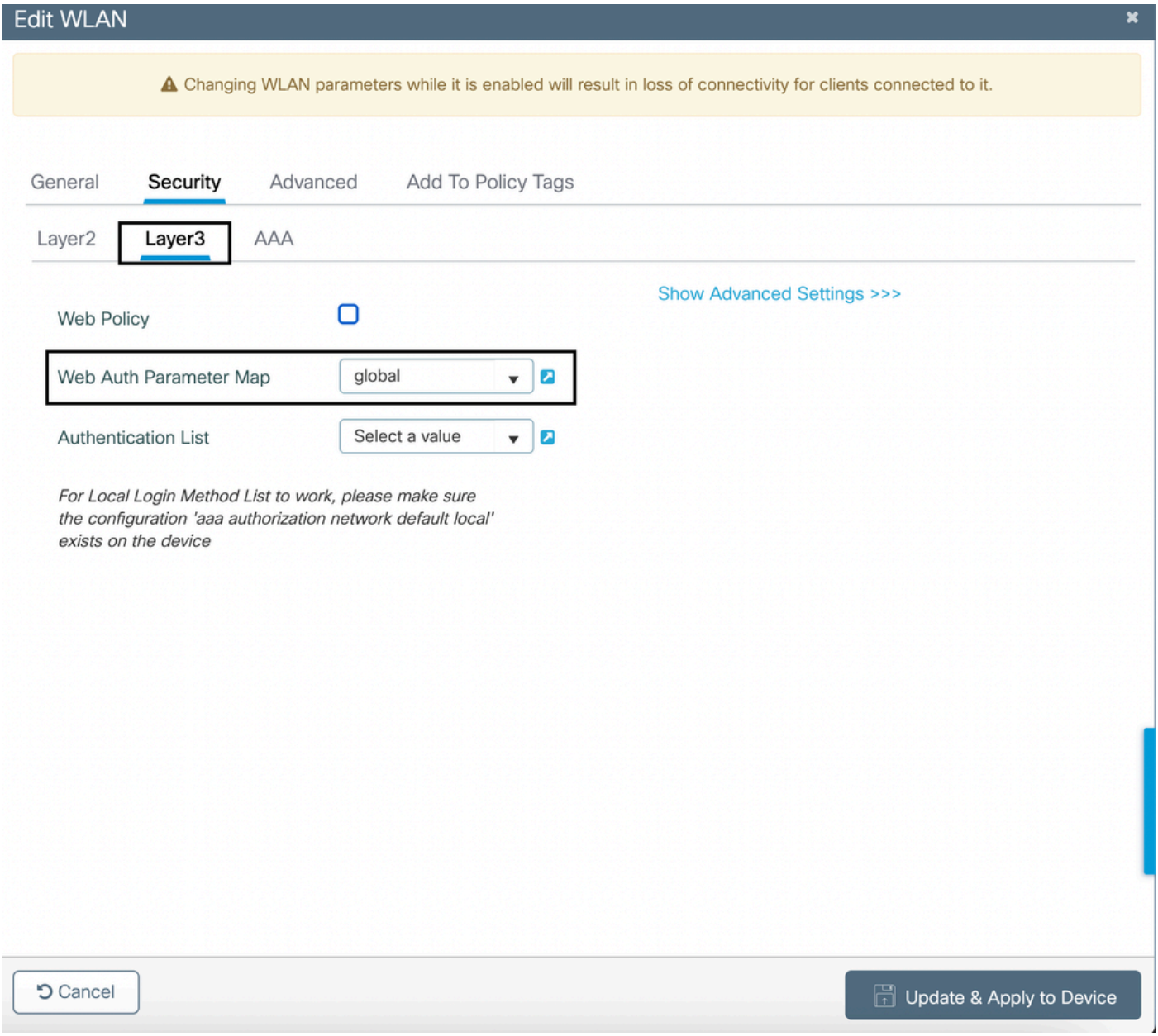
Konfigurieren von Sicherheitsrichtlinien für das WLAN

1. Navigieren Sie zu Konfiguration > Tags & Profile > WLANs. Bearbeiten Sie das zuvor erstellte WLAN.

2. Gehen Sie auf der Registerkarte Security > Layer 2 wie folgt vor:
   - WPA+WPA2 aktivieren
   - Stellen Sie AES(CCMP128) unter WPA2 Encryption ein.
   - Authentifizierungs-Schlüsselverwaltung als 802.1X



3. Wählen Sie auf der Registerkarte Security > Layer 3 im Dropdown-Menü für Web Auth Parameter Map die Option global aus.



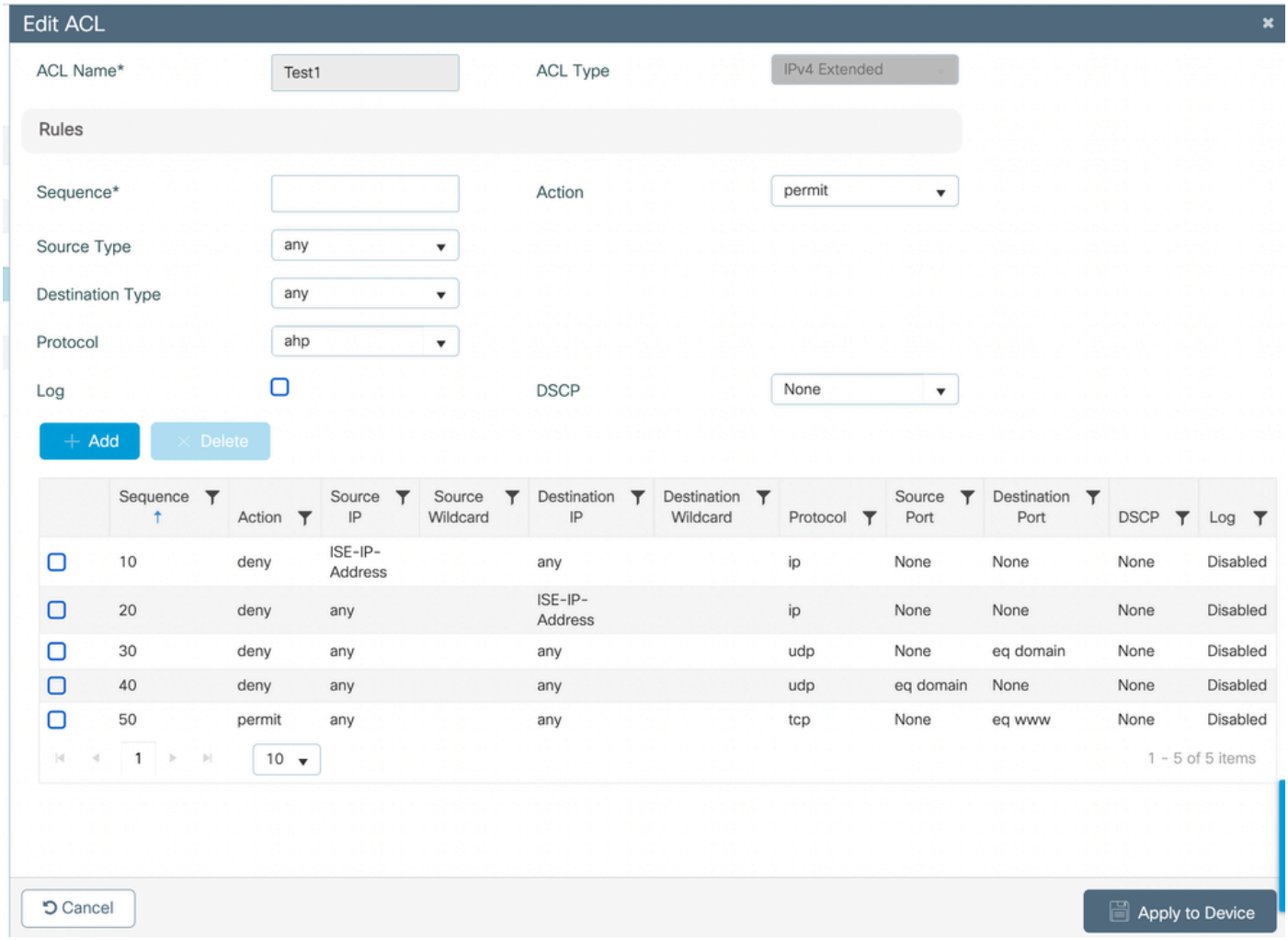
ACL vor der Authentifizierung konfigurieren

Erstellen Sie eine ACL, damit dieAktionen für die Umleitung verwenden:

- DNS-Datenverkehr.
- HTTP/HTTPS an das ISE-Portal.
- Alle erforderlichen Backend-Services.

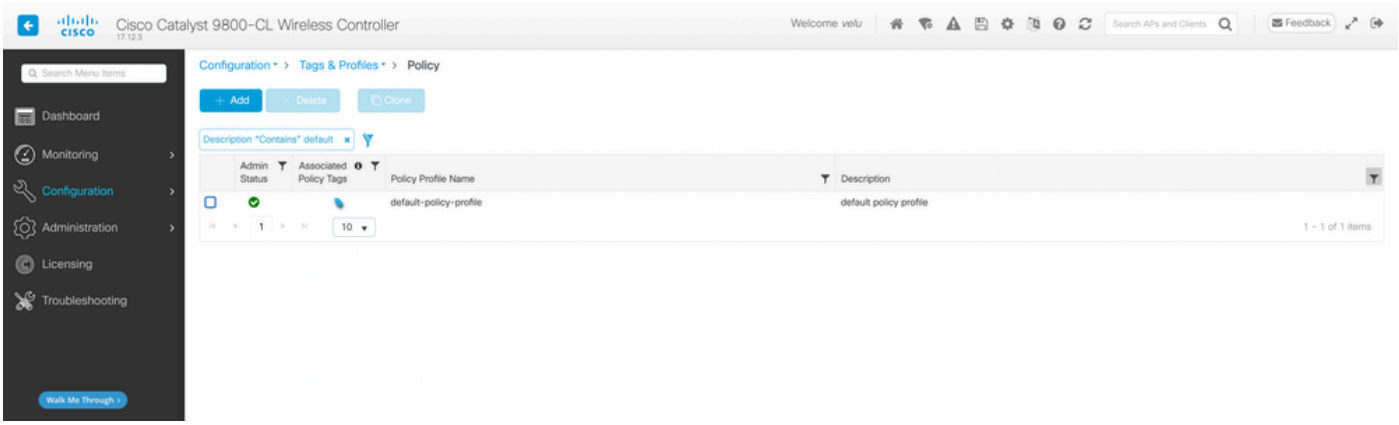
Gehen Sie dazu folgendermaßen vor:

1. Navigieren Sie zu Konfiguration > Sicherheit > ACLs > Zugriffskontrolllisten.
2. Erstellen Sie eine neue ACL mit Regeln, um den erforderlichen Datenverkehr zuzulassen.

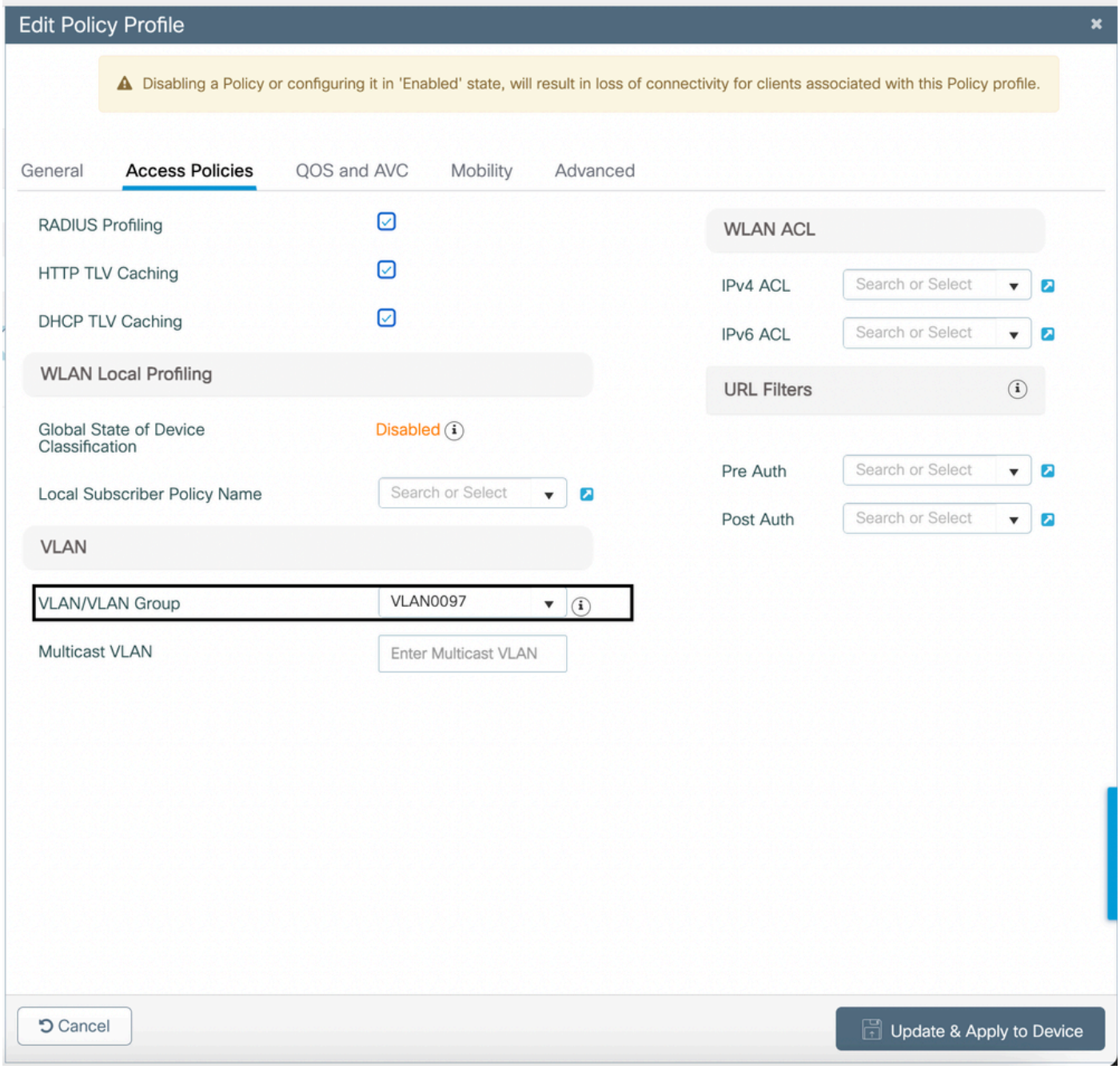


Richtlinienprofil konfigurieren

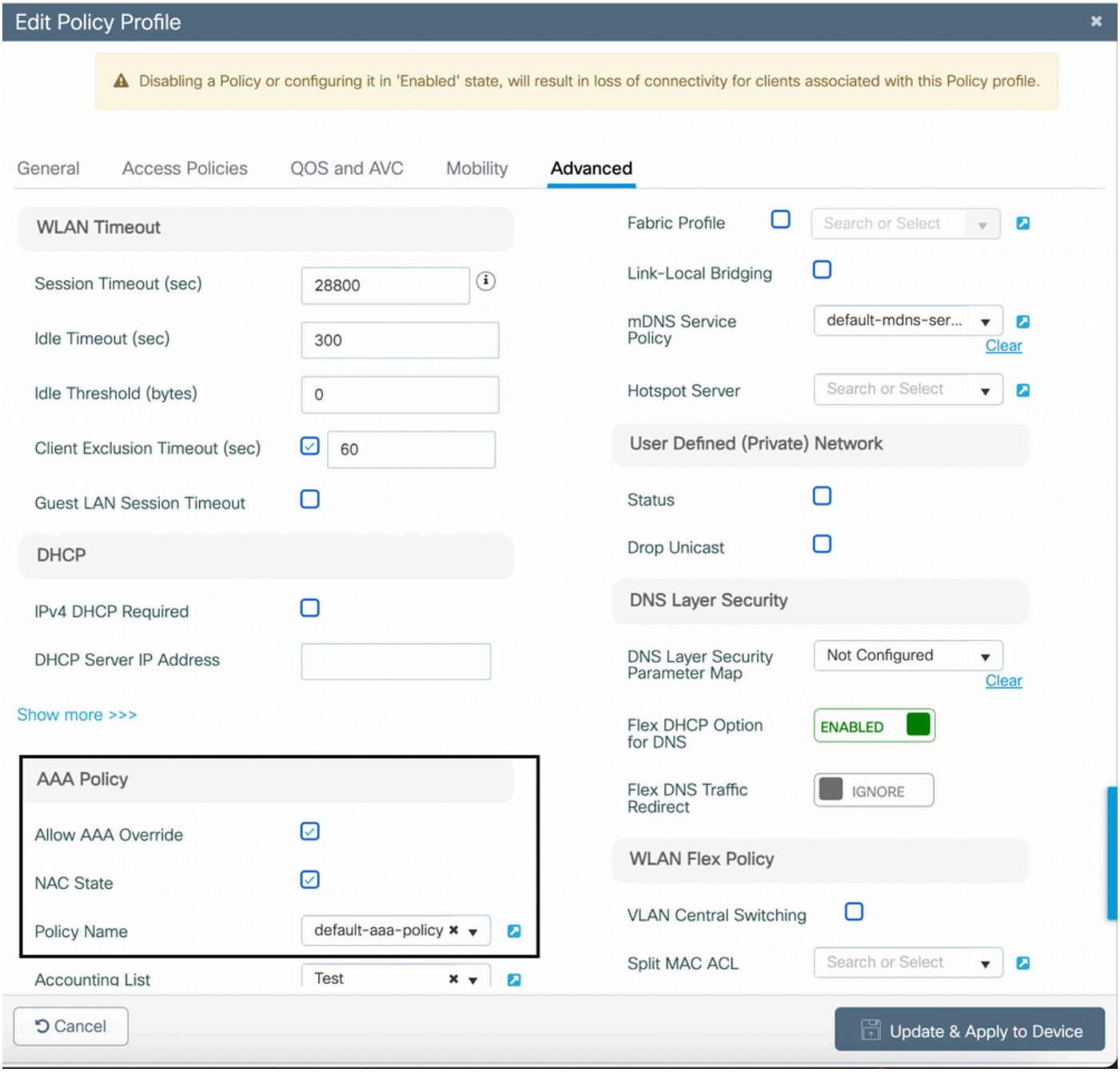
1. Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie. Sie können die Standardrichtlinie erstellen oder verwenden.



2. Zuweisen des entsprechenden VLANs unter "Access Policies"

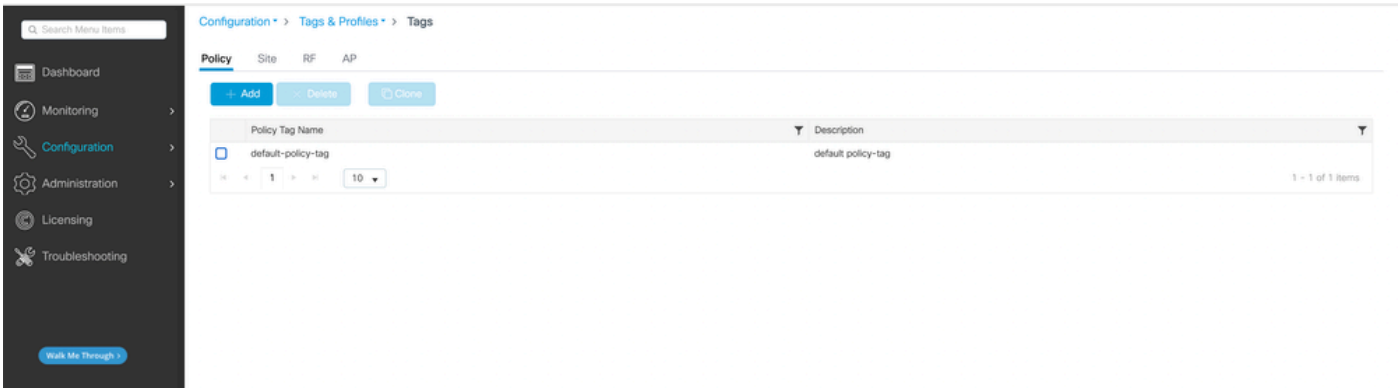


3. Aktivieren Sie außerdem unter "Erweitert" der Richtlinie "AAA-Außerkraftsetzung und NAC-Status zulassen"



Tags anwenden und bereitstellen

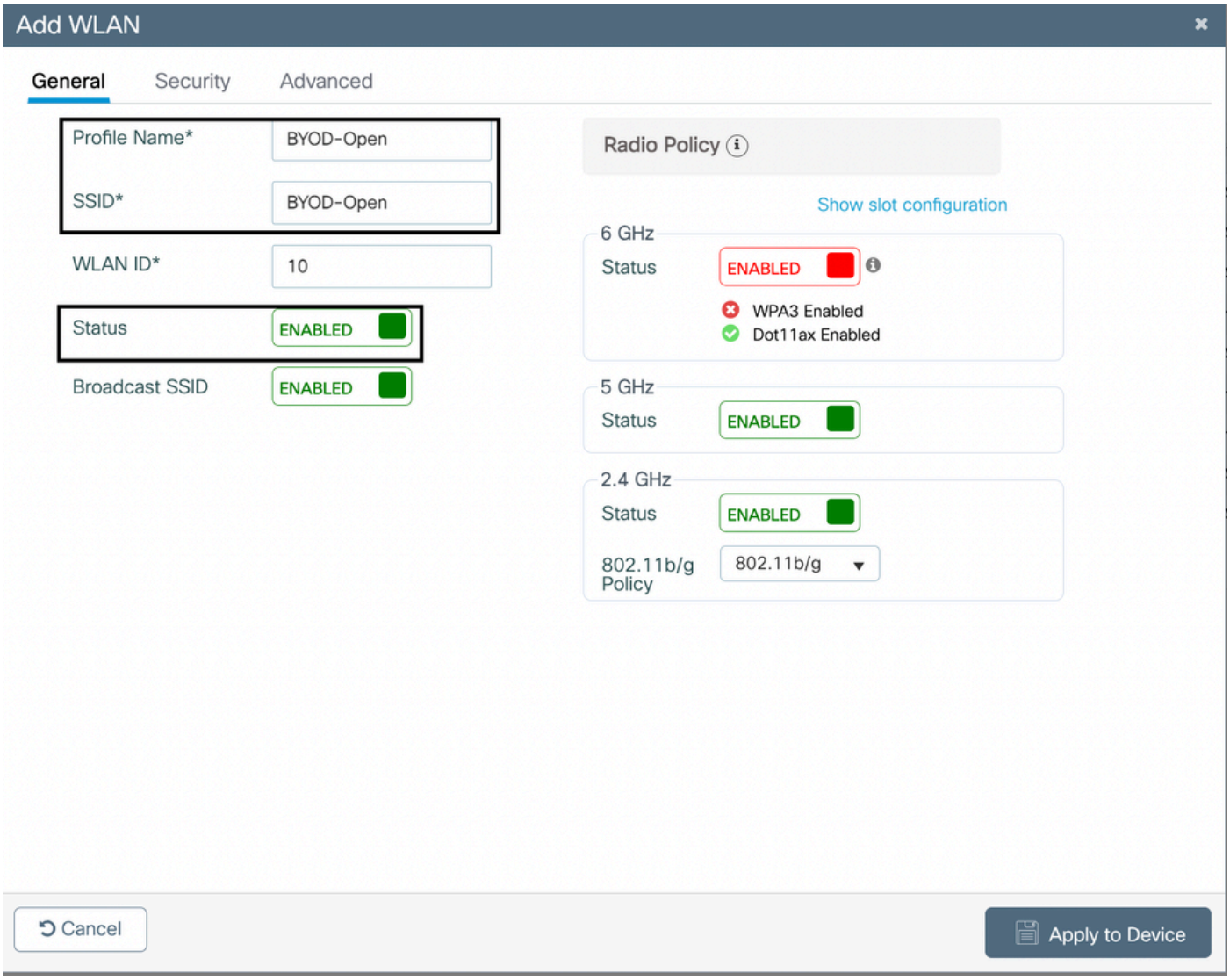
- Navigieren Sie zu Konfiguration > Tags & Profile > Tags.
- Erstellen oder bearbeiten Sie einen Tag, der das WLAN und das Richtlinienprofil enthält.
- Weisen Sie den Access Points das Tag zu.



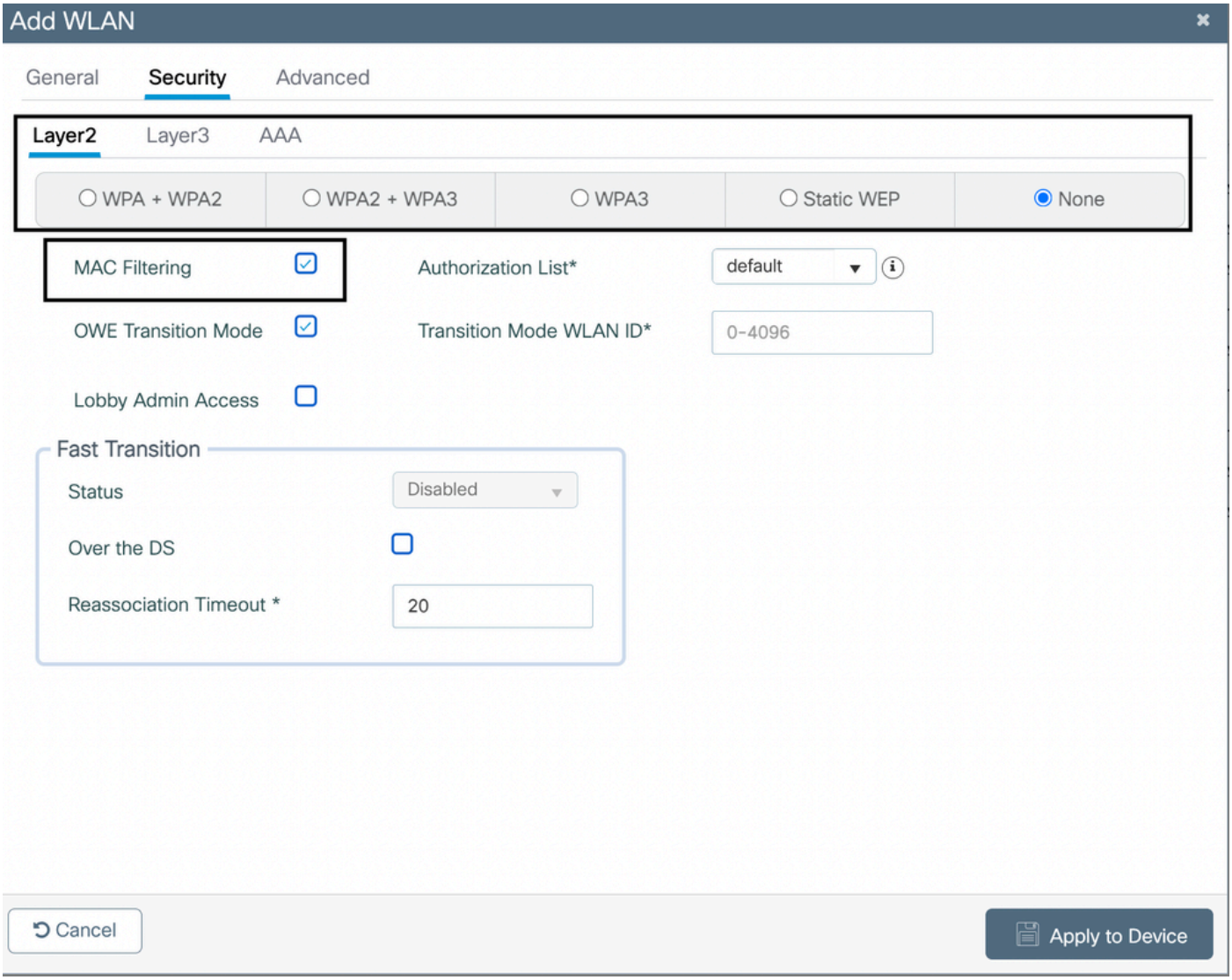
Konfigurieren einer offenen/ungesicherten SSID

Die offene SSID wird nur erstellt, wenn Sie sich für eine Dual-SSID-BYOD-Konfiguration in Ihrer Umgebung entscheiden.

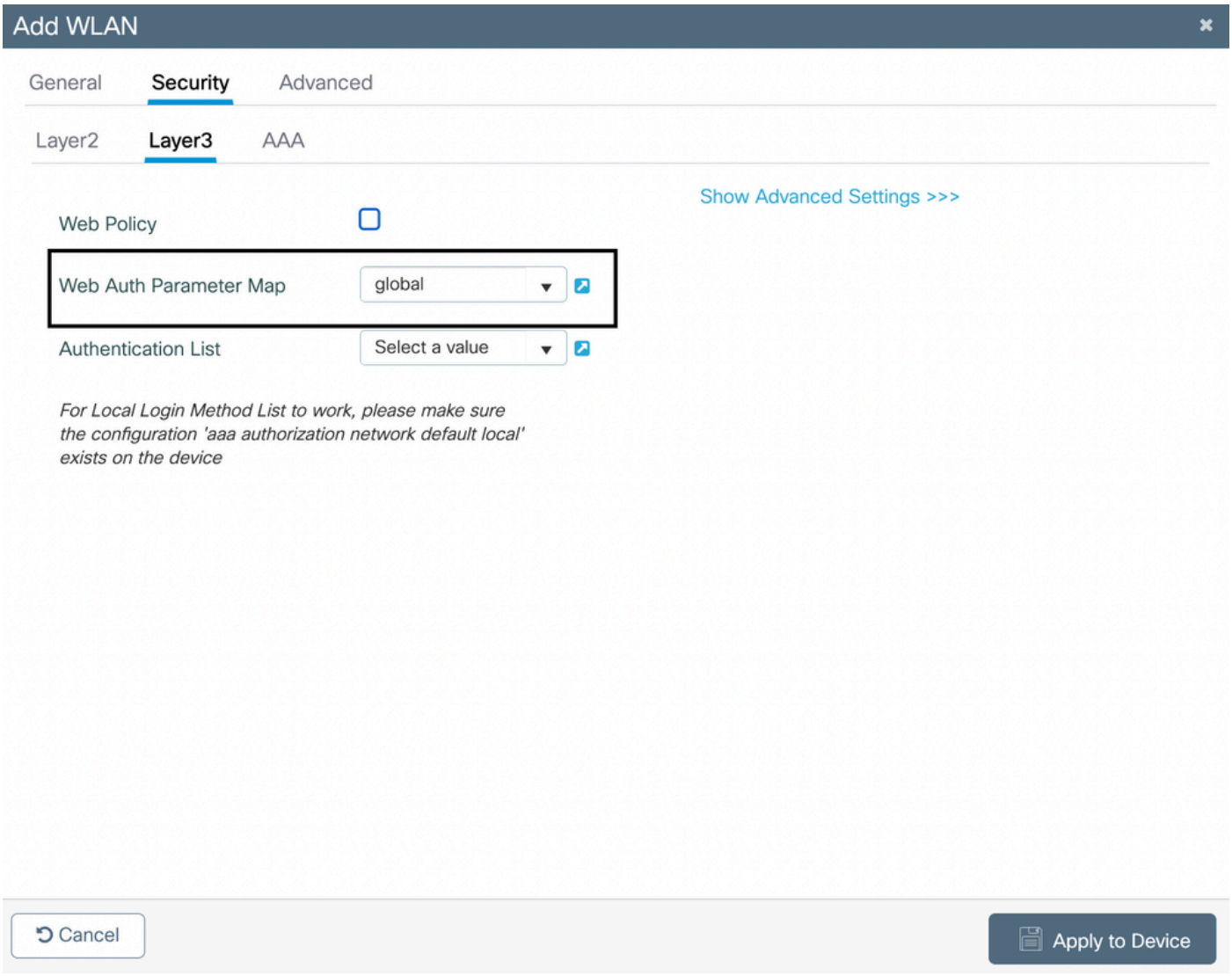
1. Navigieren Sie zu Konfiguration > Tags & Profile > WLANs. Klicken Sie auf die Schaltfläche Hinzufügen.
2. Geben Sie auf der Registerkarte General (Allgemein) einen SSID-Namen ein, und aktivieren Sie die Schaltfläche WLAN.



3. Klicken Sie im gleichen Fenster auf die Registerkarte Sicherheit. Aktivieren Sie das Optionsfeld Keine, und aktivieren Sie die Mac-Filterung.



4. Wählen Sie in Layer 3 unter Sicherheit die globale Einstellung für Web Auth Parameter Map aus. Wenn Sie ein anderes Webauthentifizierungsprofil auf dem WLC konfiguriert haben, können Sie es auch hier zuordnen:



ISE-Konfiguration

Voraussetzungen

- Stellen Sie sicher, dass die Cisco ISE installiert und für BYOD-Funktionen lizenziert ist.
- Fügen Sie Ihren WLC der ISE als Netzwerkgerät mit dem gemeinsamen geheimen RADIUS-Schlüssel hinzu.

Zertifikate

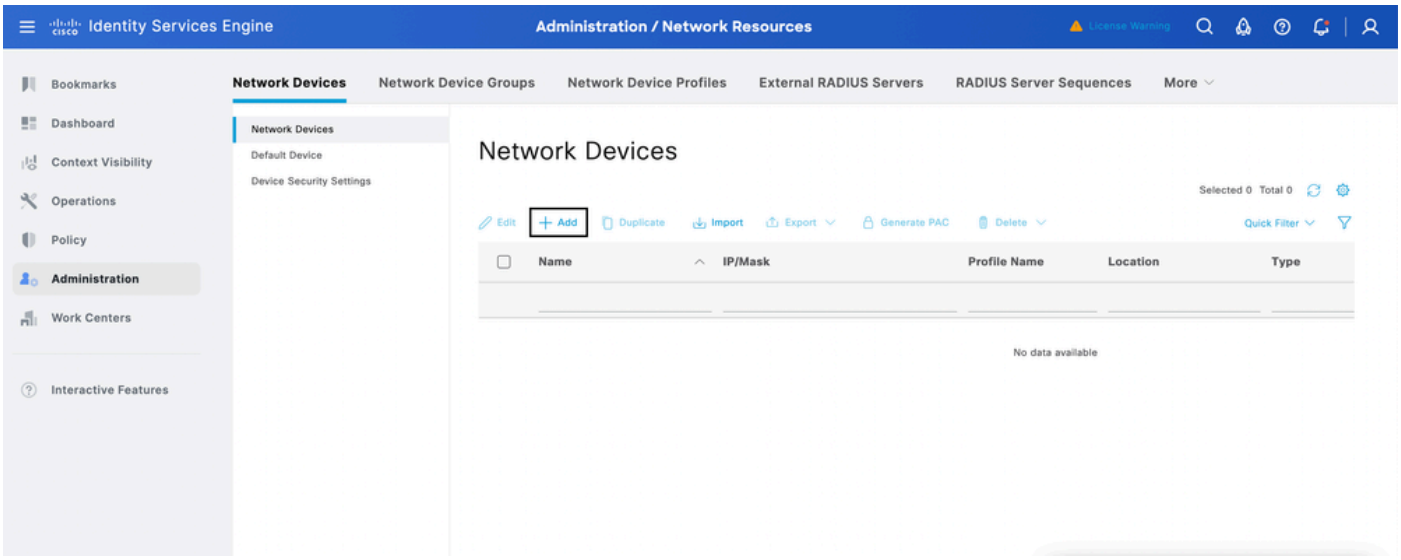
- Installieren Sie ein gültiges Serverzertifikat auf der ISE, um Sicherheitswarnungen im Browser zu vermeiden.
- Stellen Sie sicher, dass das Zertifikat von den Endpunkten als vertrauenswürdig eingestuft wird (signiert von einer bekannten Zertifizierungsstelle oder einer internen Zertifizierungsstelle mit vertrauenswürdigem Root).

DNS-Konfiguration

- Stellen Sie sicher, dass DNS den ISE-Hostnamen für das BYOD-Portal auflöst.

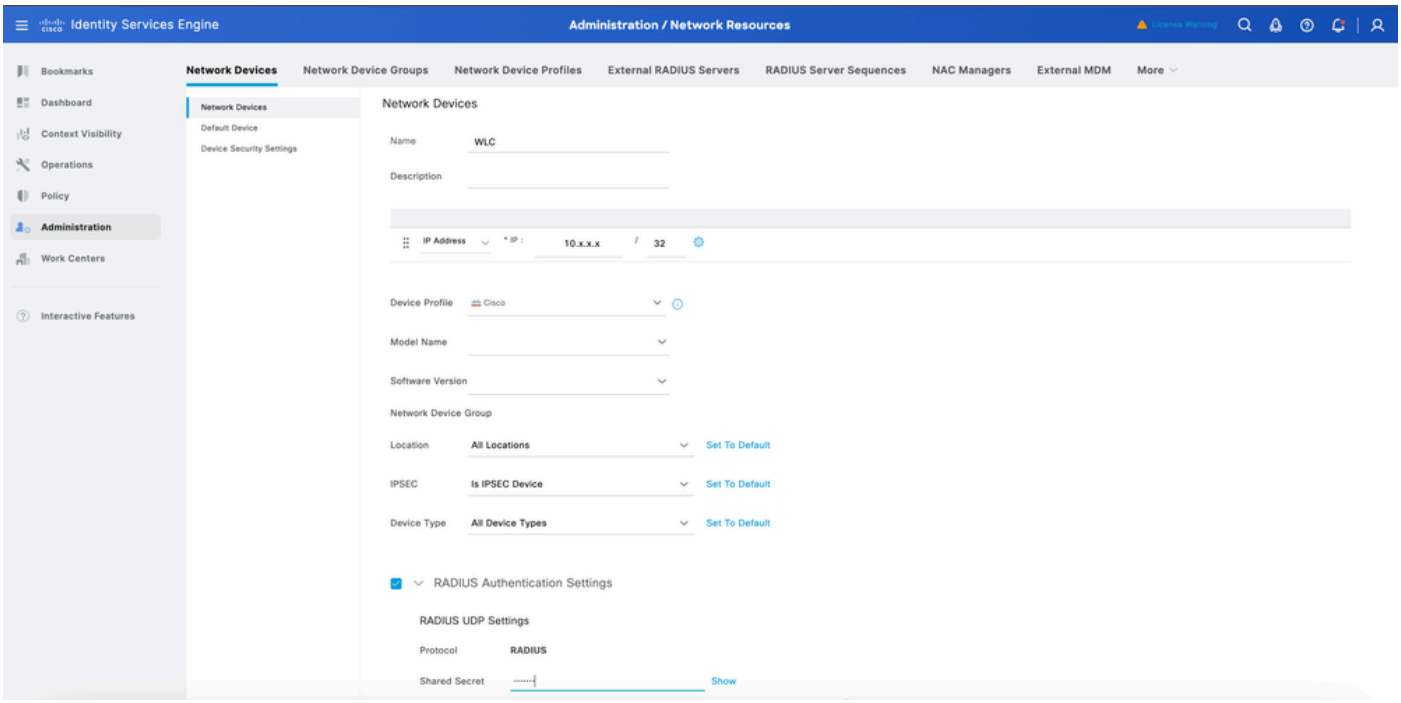
Konfigurieren des ISE-Netzwerkgeräts

1. Melden Sie sich bei der ISE-Webbenutzeroberfläche an.
2. Navigieren Sie zu Administration > Network Resources > Network Devices.



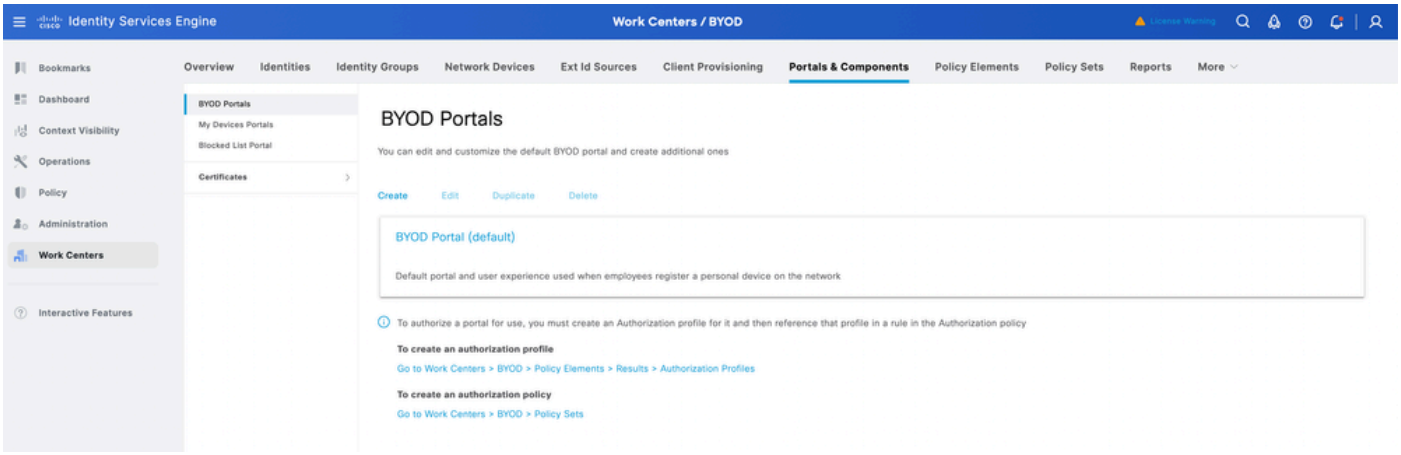
3. Fügen Sie Ihren WLC als Netzwerkgerät hinzu:

- Name: Geben Sie einen Namen für den WLC ein.
- IP-Adresse: Geben Sie die WLC-Verwaltungs-IP ein.
- Gemeinsamer RADIUS-Schlüssel: Geben Sie den gleichen gemeinsamen geheimen Schlüssel ein, der auf dem WLC konfiguriert wurde.
- Klicken Sie auf Senden.



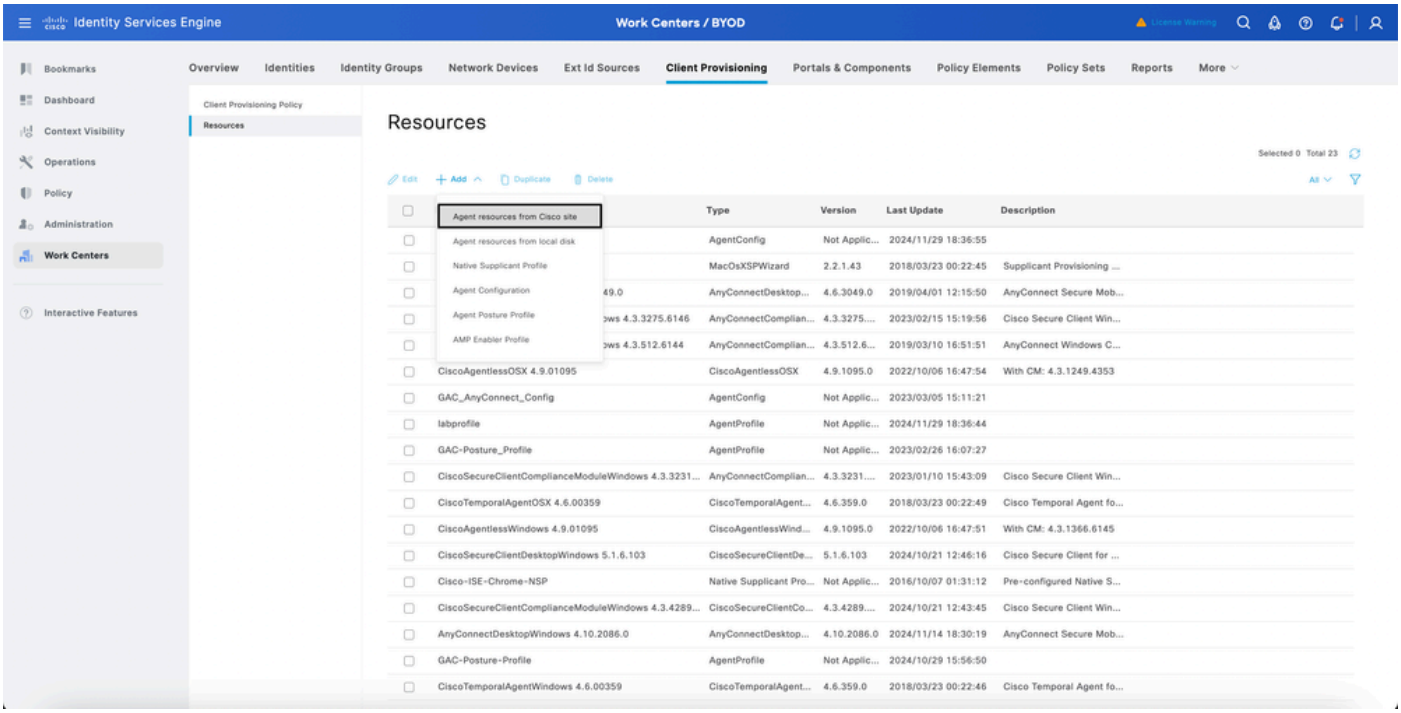
Erstellung eines BYOD-Portals

1. Navigieren Sie zu Work Centers > BYOD > Settings > Portals & Components > BYOD Portals.
2. Klicken Sie auf Hinzufügen, um ein BYOD-Portal zu erstellen, oder verwenden Sie das vorhandene Standardportal auf der ISE.



Cisco IOS® aktuelle Version herunterladen

1. Navigieren Sie zu Work Centers > BYOD > Client provisioning > Resources.
2. Klicken Sie auf die Schaltfläche Hinzufügen, und wählen Sie die Agenten-Ressourcen von der Cisco Website aus.



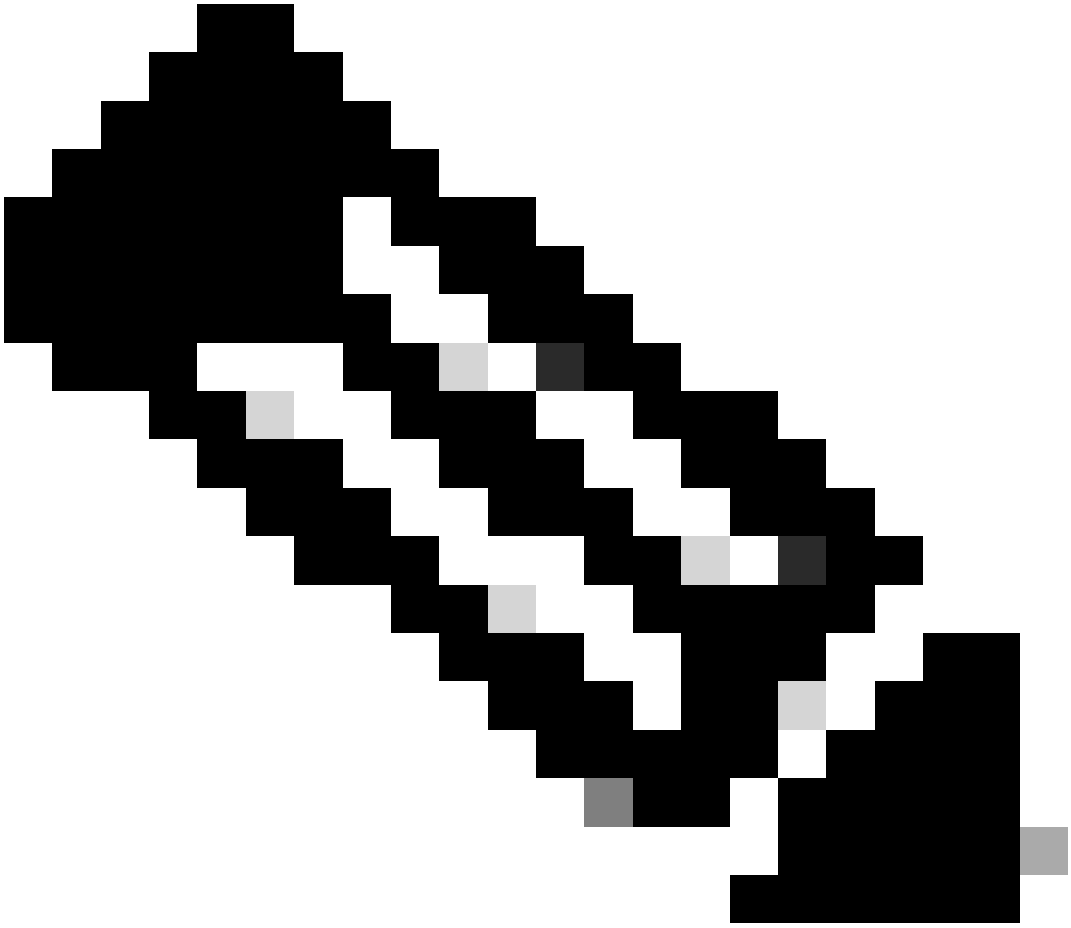
3. Wählen Sie in der Softwareliste die neueste Cisco IOS-Version aus, die heruntergeladen werden soll.

Download Remote Resources

	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☑	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from http://cisco.com/go/ciscosecureclient. Use the "Agent resource from local disk" add option, to import into ISE

Cancel Save

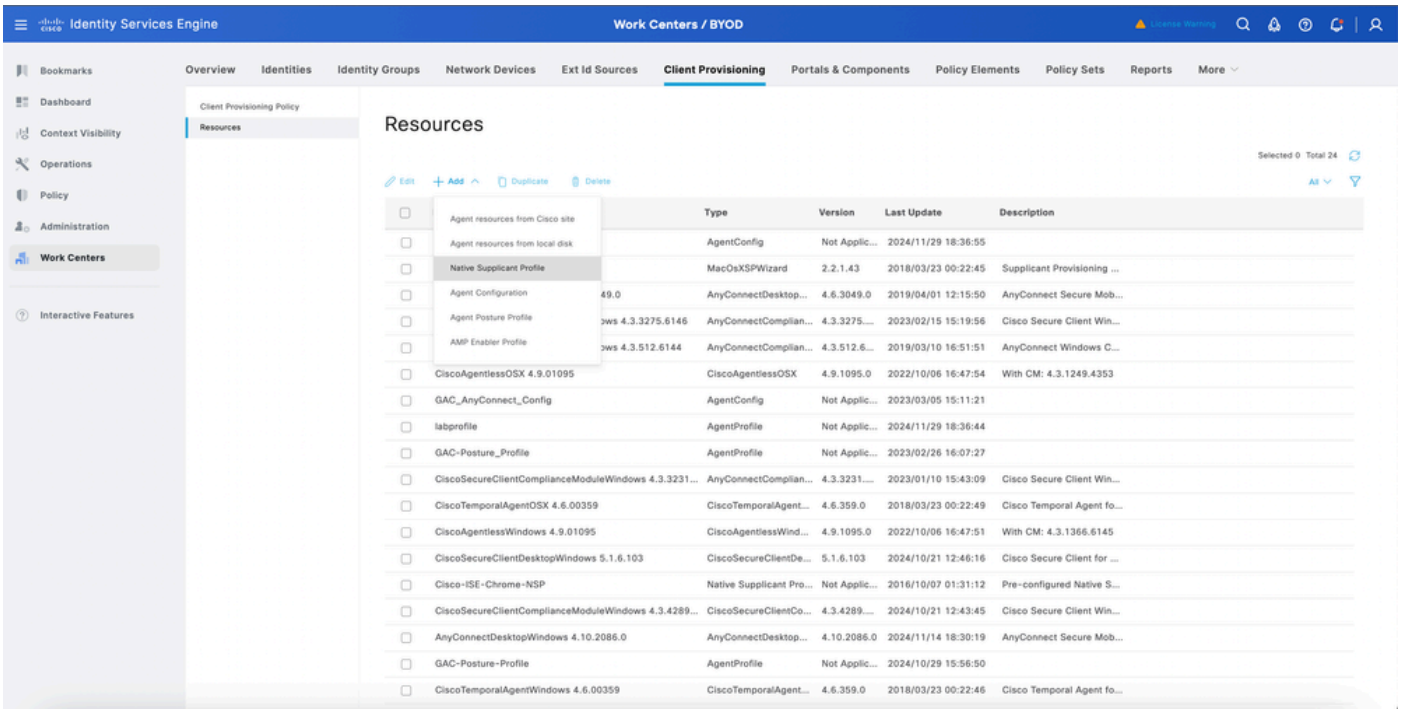


Anmerkung: Die Cisco IOS Software kann für Windows- und MacOS-Endgeräte von der ISE heruntergeladen werden. Für Apple iPhone IOS, es verwendet eine native Supplicant, um das Gerät bereitzustellen und Für Android-Gerät, haben Sie Netzwerk-Setup-Assistent, die aus dem Play Store heruntergeladen werden muss.

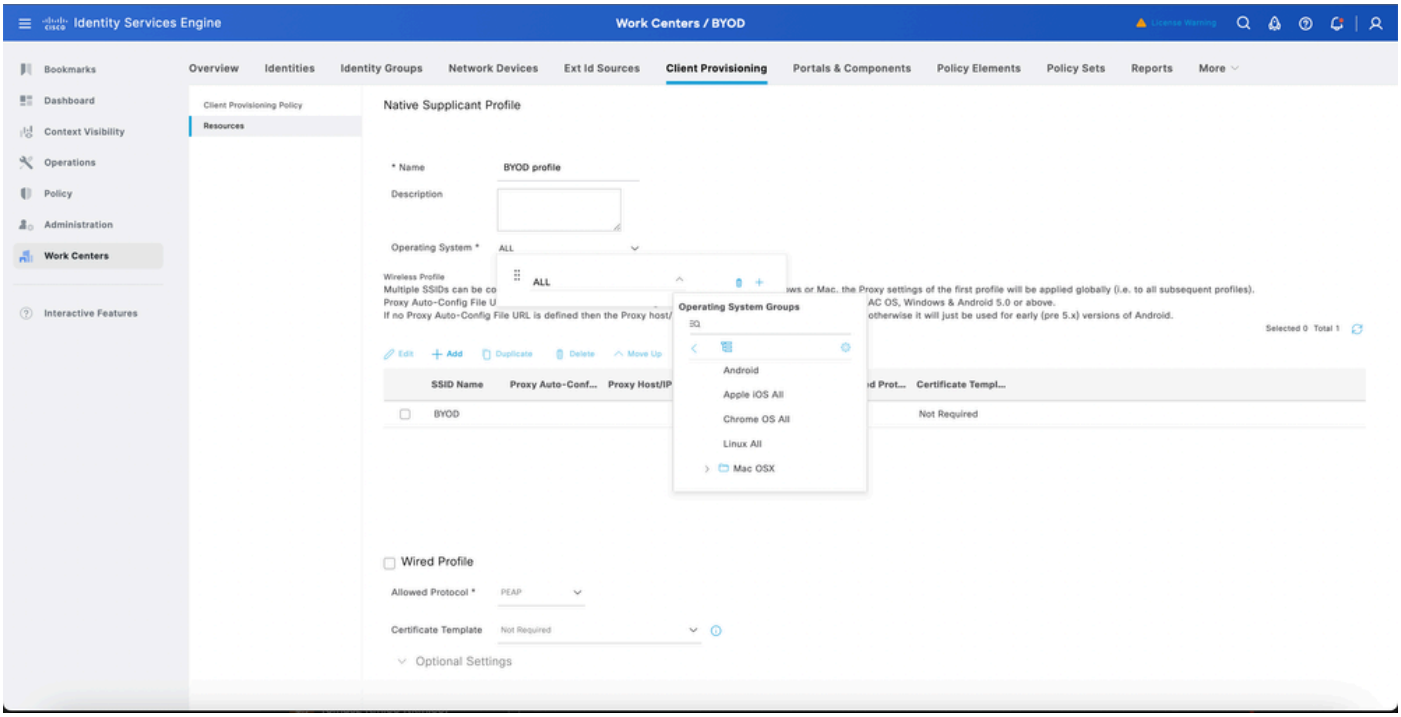
Endgeräteprofil erstellen

1. Navigieren Sie zu Work Centers > BYOD > Client provisioning > Resources.

2. Klicken Sie auf Hinzufügen, wählen Sie Natives Komponentenprofil aus dem Dropdown-Menü aus.



3. Wählen Sie im Dropdown-Menü Operating System (Betriebssystem) das Betriebssystem aus, das Sie in das Gerät integrieren möchten, oder legen Sie es als ALL (ALLE) für alle Endgeräte in Ihrer Umgebung fest:



4. Klicken Sie auf Hinzufügen von der Seite, um das Endgeräteprofil zu erstellen und 802.1X für das Endgerät zu konfigurieren:

Wireless Profile(s)

SSID Name * BYOD

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

Windows Settings

Authentication Mode User or Computer

- [ ] Automatically use logon name and password (and domain if any)
- [x] Enable fast reconnect
- [ ] Enable quarantine checks
- [ ] Disconnect if server does not present cryptobinding TLV
- [ ] Do not prompt user to authorize new servers or trusted certification authorities
- [x] Connect even if the network is not broadcasting its name (SSID)

iOS Settings

- [ ] Enable if target network is hidden

Android Settings

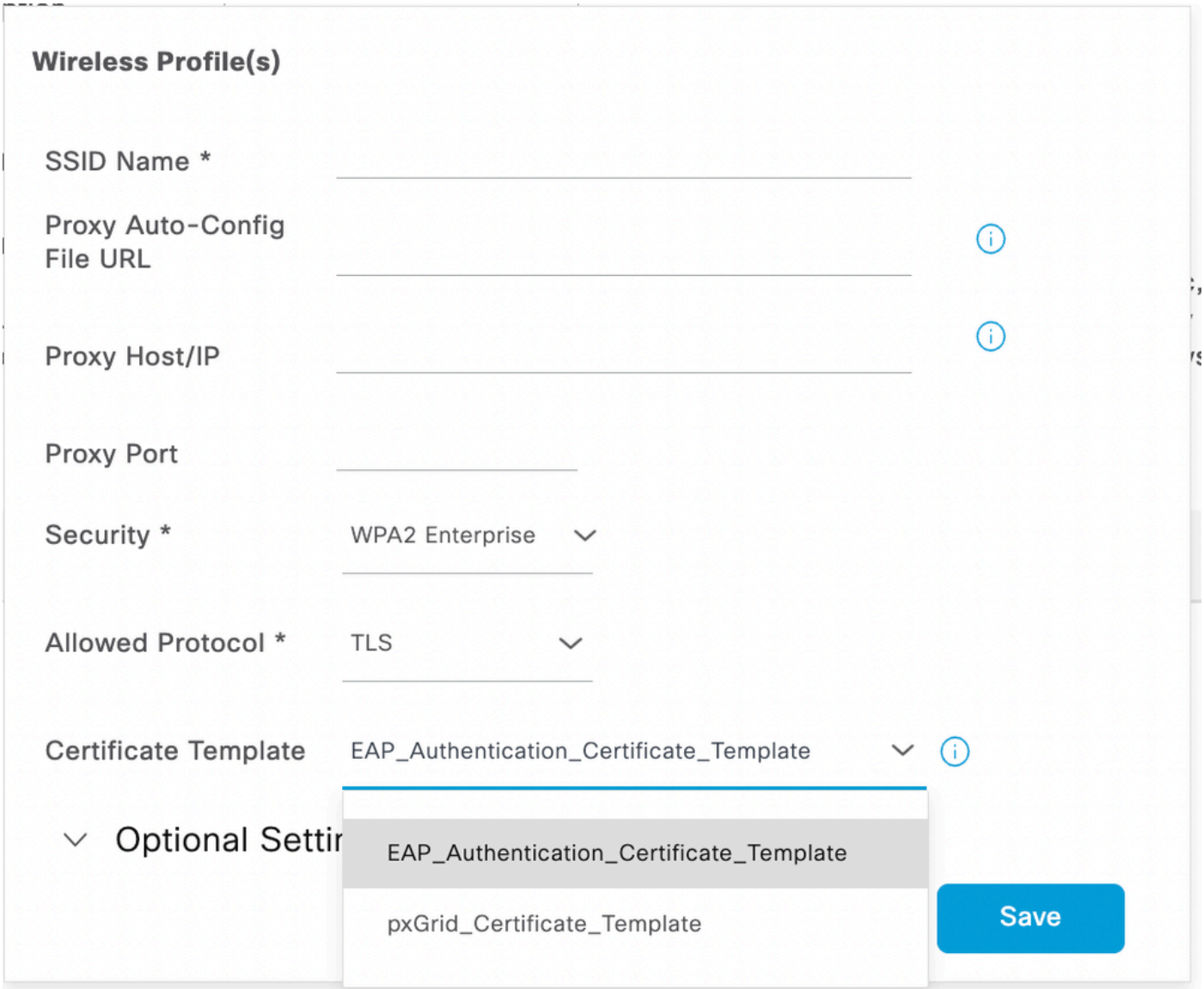
Certificate Enrollment Protocol:

Konfigurieren Sie je nach Ihren Anforderungen das Endgeräteprofil für den Endpunkt in Ihrer Umgebung. Das Endgeräteprofil ermöglicht die Konfiguration von EAP-PEAP und EAP-TLS.

5. Klicken Sie im Endpunktprofil auf Speichern und dann auf Senden.

Zertifikatvorlage

Das Endgeräteprofil ist für die Ausführung von EAP-TLS vorkonfiguriert. Dem Profil muss eine Zertifikatvorlage hinzugefügt werden. Standardmäßig sind für die ISE zwei Vorlagen vordefiniert, die in der Dropdown-Liste ausgewählt werden können..

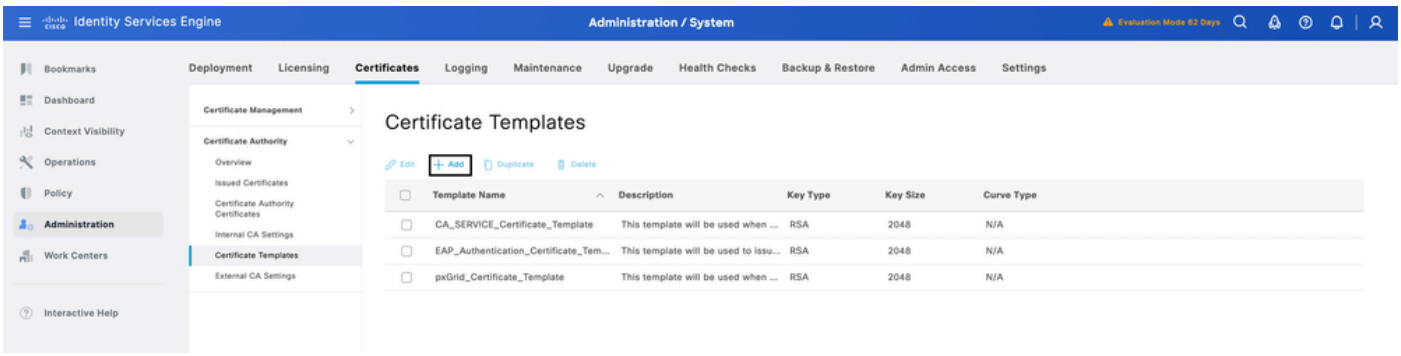


Um eine neue Zertifikatvorlage zu erstellen, gehen Sie wie folgt vor:

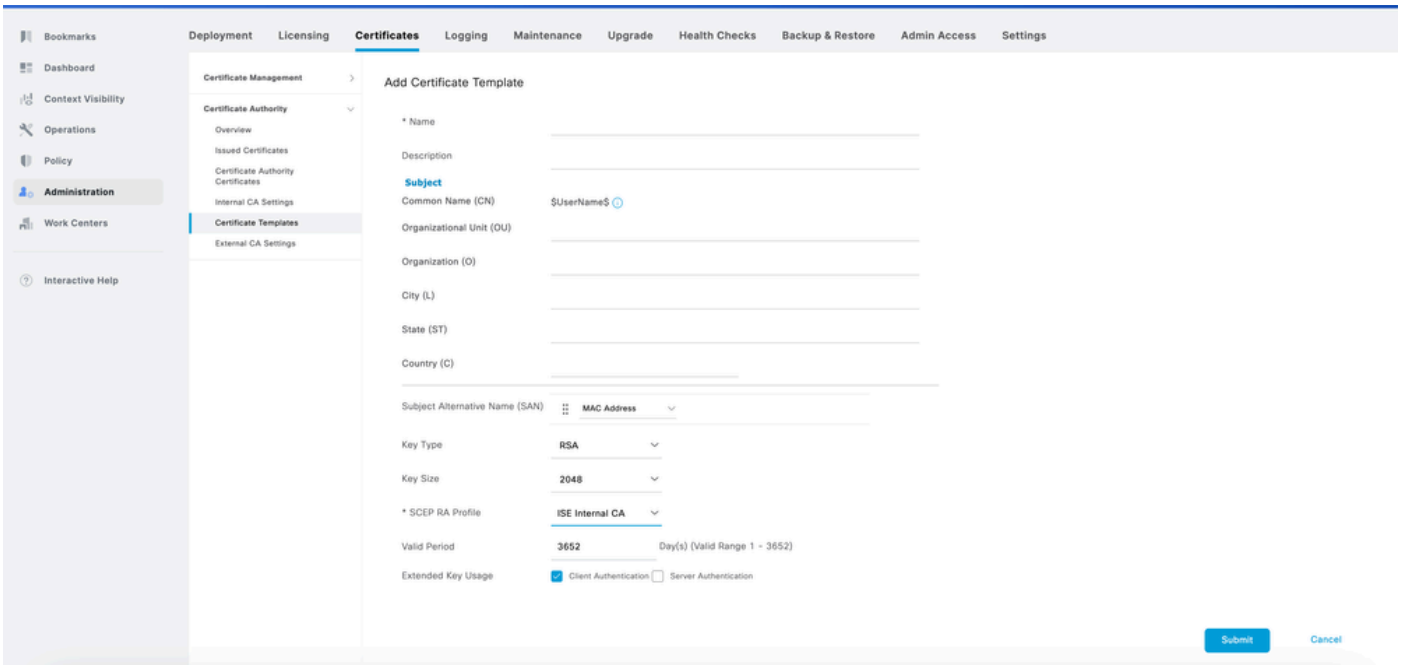
1. Navigieren Sie zu Administration > System > Certificates > Certificate Authority > Certificate

Templates.

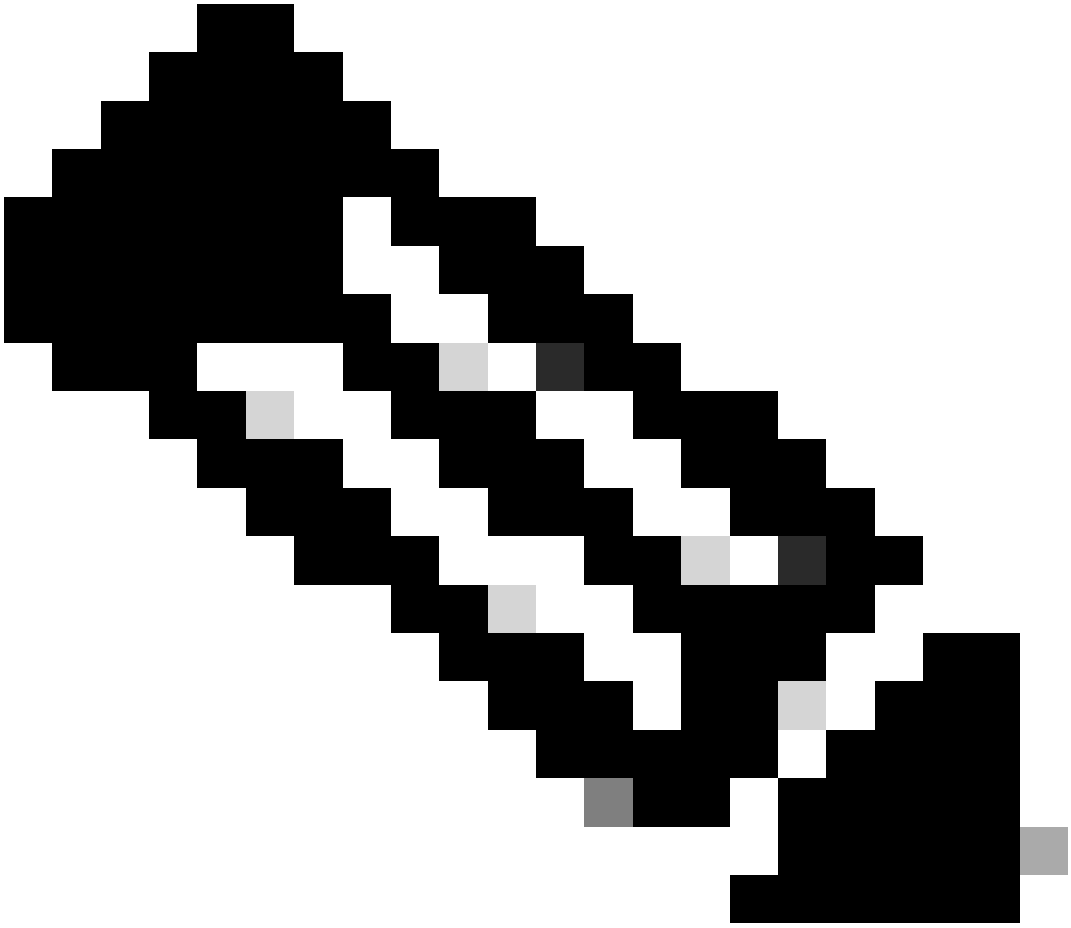
2. Klicken Sie auf der Seite auf die Schaltfläche Hinzufügen.



3. Geben Sie die Details ein, die auf die spezifischen Anforderungen Ihres Unternehmens zugeschnitten sind.



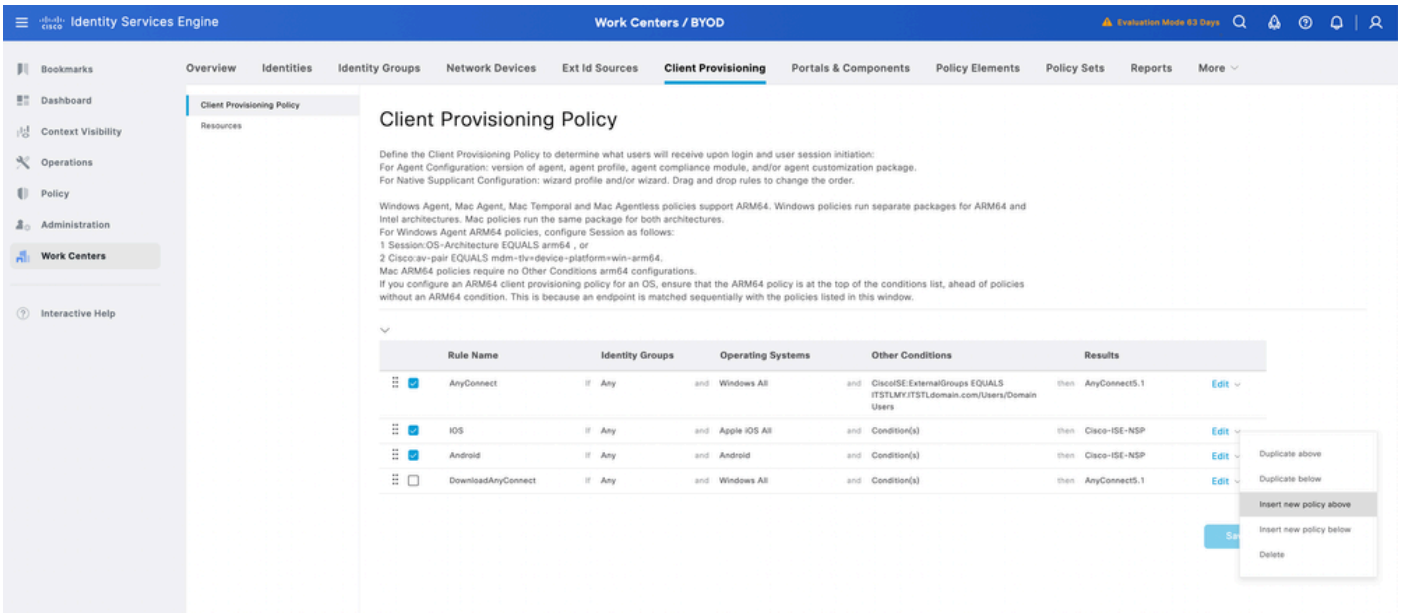
4. Klicken Sie auf Senden, um die Änderungen zu speichern.



Anmerkung: Die Zertifikatvorlage kann in einem Szenario nützlich sein, wenn Sie unterschiedliche Domänen haben und den Benutzer segmentieren, indem Sie einen anderen Wert in der OU des Zertifikats hinzufügen.

Zuordnen eines Endgeräteprofils zum Client-Bereitstellungsportal

1. Navigieren Sie zu Work Centers > BYOD > Client provisioning > Client provisioning Policy.
2. Klicken Sie auf v on der Regeln, um eine neue Client-Bereitstellungsregel zu erstellen.

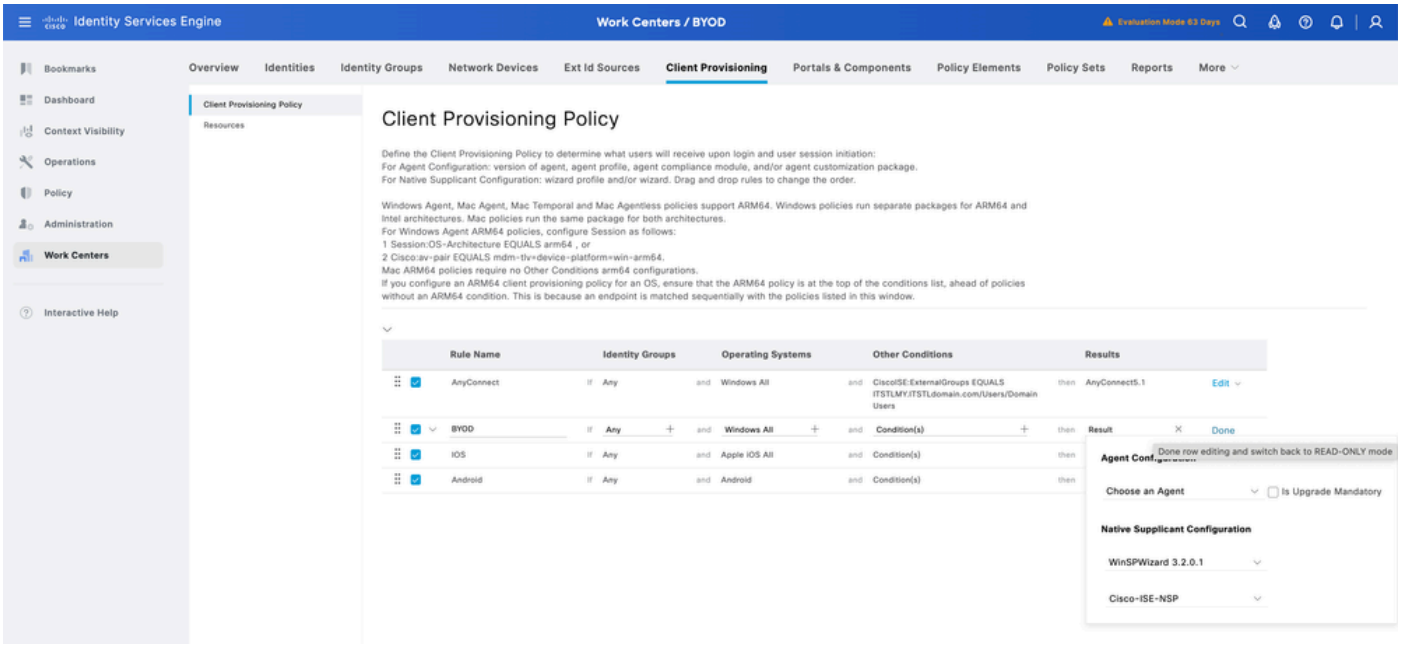


3. Erstellen Sie die neue Regel auf der Seite

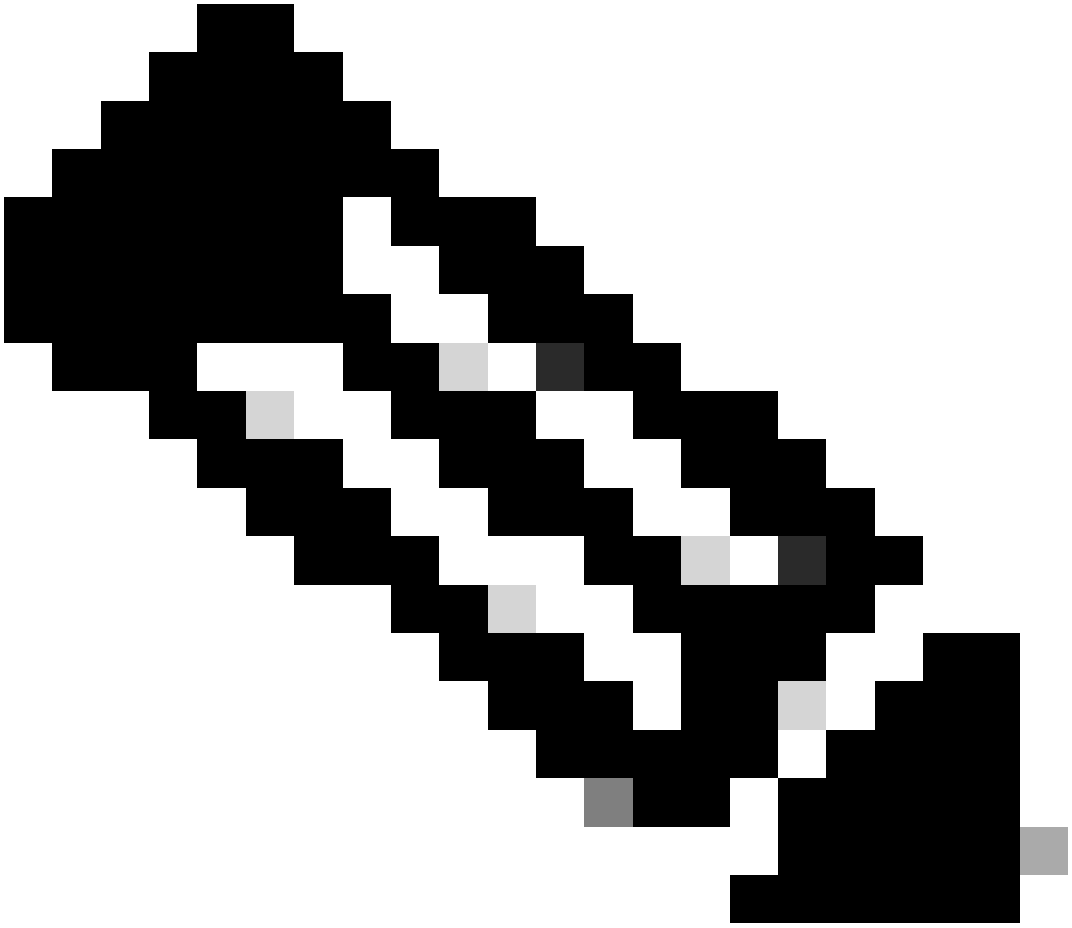
4. Fügen Sie die Identitätsgruppe hinzu, wenn Sie die Nutzung des BYOD-Portals durch bestimmte Benutzer einschränken möchten.

5. Fügen Sie das Betriebssystem hinzu, auf das Sie Zugriff auf das BYOD-Portal erhalten möchten.

6. Ordnen Sie die Cisco IOS-Version aus dem Dropdown-Menü zu, und wählen Sie auch das Endgeräteprofil aus, das Sie anhand des Ergebnisses erstellt haben.



7. Klicken Sie auf Fertig und dann auf die Schaltfläche Speichern.

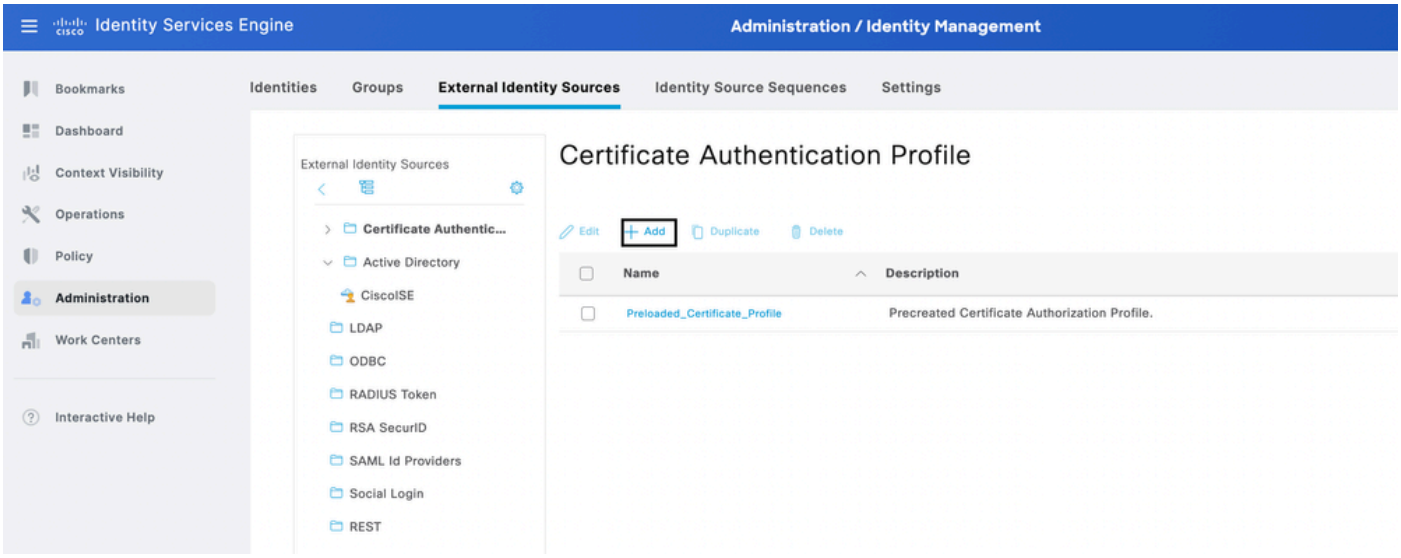


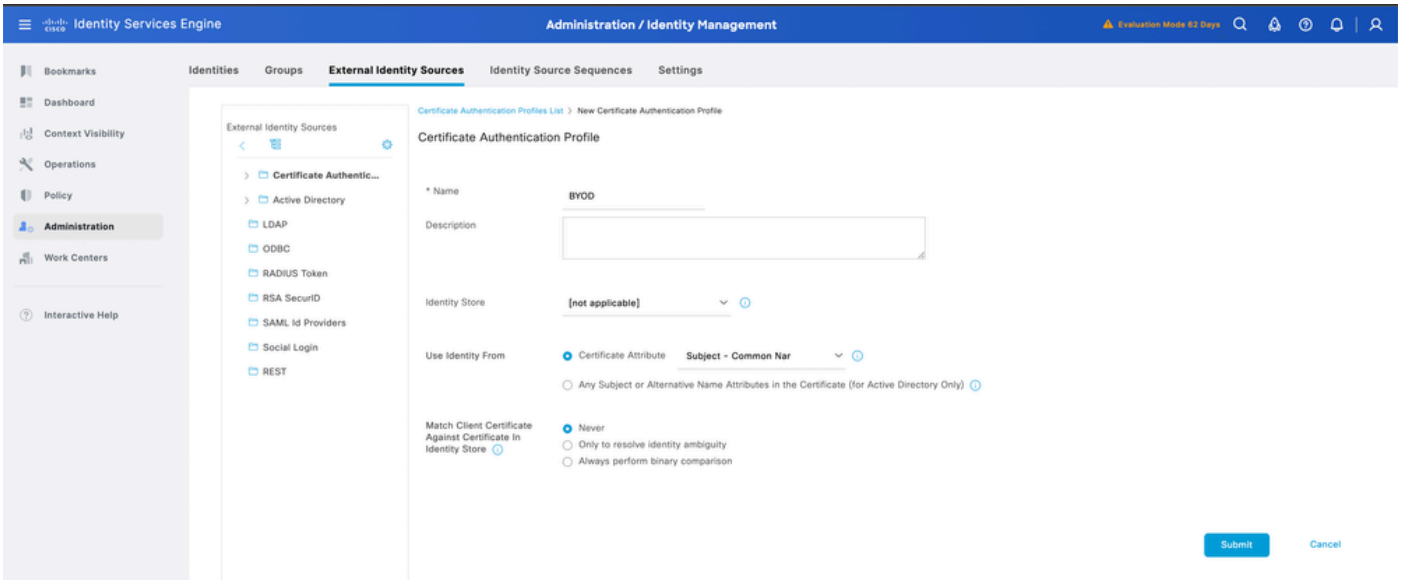
Anmerkung: Diese Richtlinie wirkt sich sowohl auf die Statusclientbereitstellung als auch auf die BYOD-Bereitstellung aus, wobei im Abschnitt "Agentenkonfiguration" der Status-Agent und das Compliance-Modul für Statusprüfungen festgelegt werden, während im Abschnitt "Konfiguration der nativen Komponente" die Einstellungen für BYOD-Bereitstellungsabläufe verwaltet werden

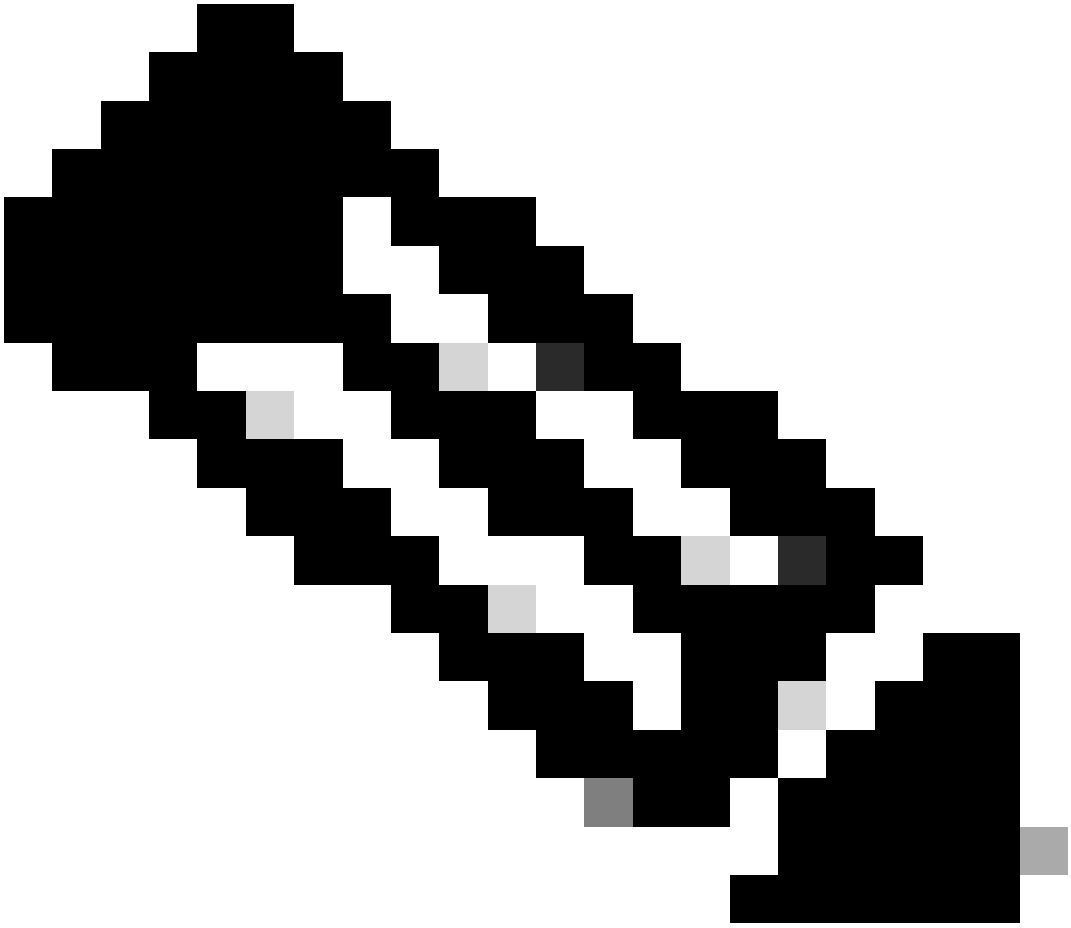
Konfigurieren von ISE-Richtliniensätzen für BYOD mit einer SSID

1. Navigieren Sie zu Policy > Policy Set, und erstellen Sie eine Richtlinie für BYOD-Fluss auf der ISE:

2. Navigieren Sie dann zu Administration > Identity Management > External Identity Sources > Certificate Authentication Profile. Klicken Sie auf die Schaltfläche Hinzufügen, um das Zertifikatprofil zu erstellen:

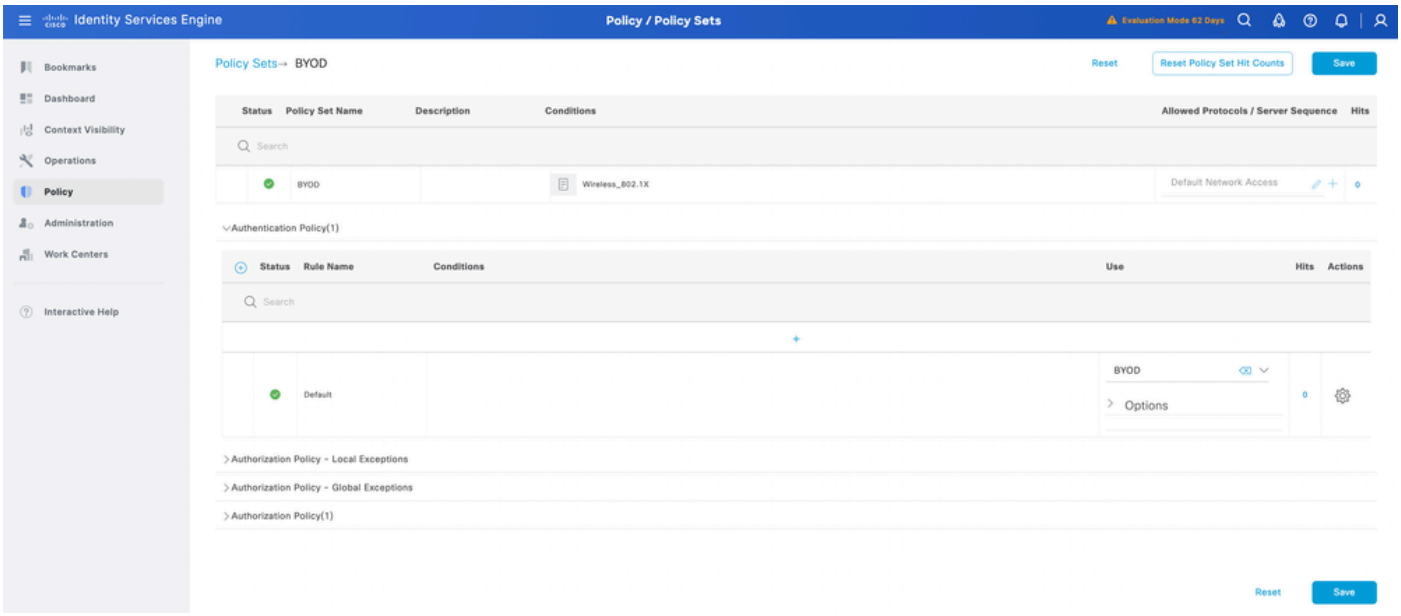






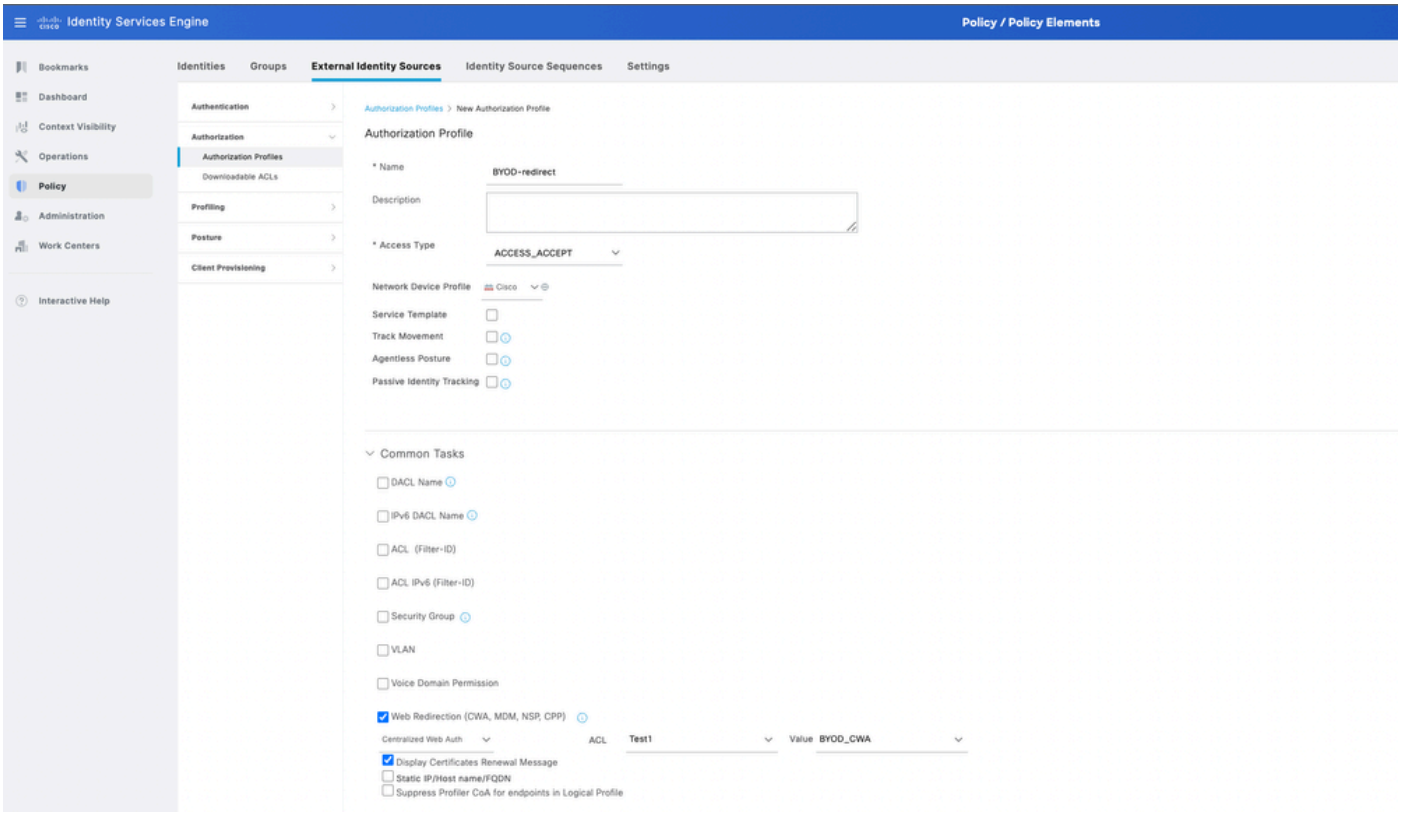
Anmerkung: Im Identity Store können Sie Ihr Active Directory, das in die ISE integriert wurde, immer auswählen, um eine Benutzersuche aus dem Zertifikat für zusätzliche Sicherheit durchzuführen.

3. Klicken Sie auf Senden, um die Konfiguration zu speichern. Ordnen Sie dann das Zertifikatprofil dem für BYOD festgelegten Richtliniensatz zu:



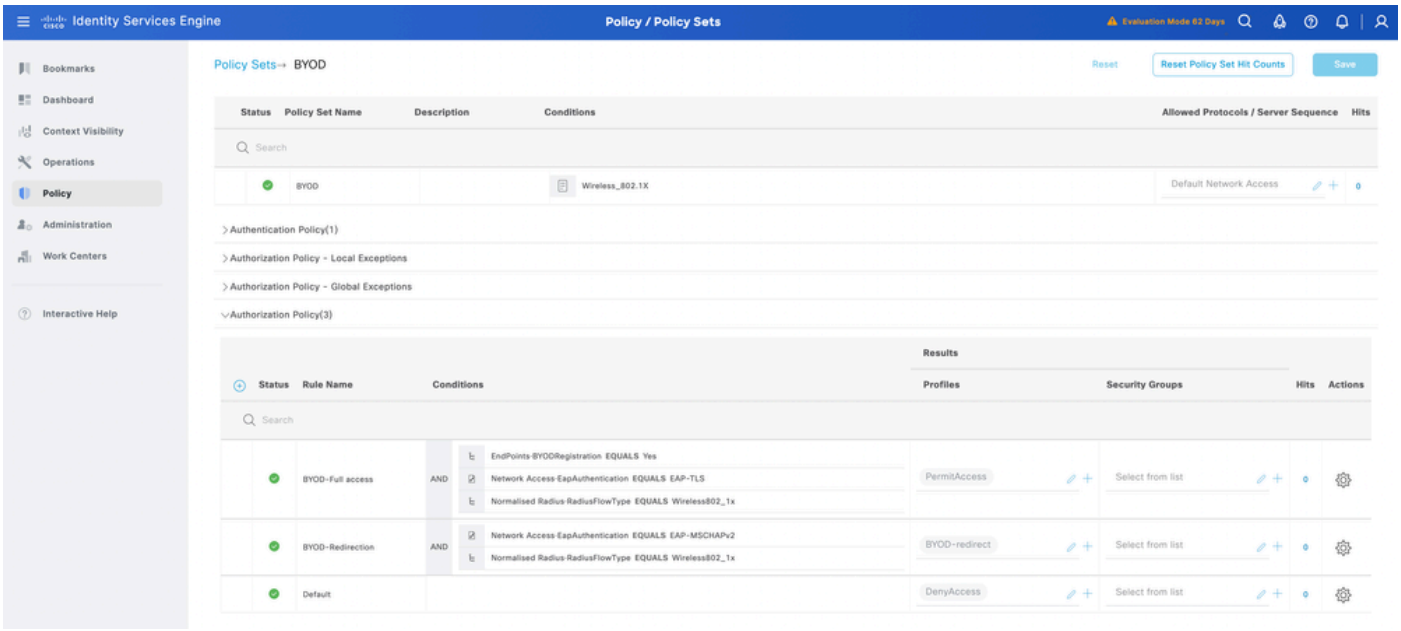
4. Konfigurieren Sie das Autorisierungsprofil für die BYOD-Umleitung und den vollständigen Zugriff nach dem BYOD-Fluss. Navigieren Sie zu Policy > Policy Elements > Results > Authorization > Authorization Profiles (Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile).

5. Klicken Sie auf Hinzufügen, und erstellen Sie ein Autorisierungsprofil. Überprüfen Sie die Web Redirection (CWA, MDM, NSP, CPP), und ordnen Sie die BYOD-Portalseite zu. Fügen Sie dem Profil außerdem den Namen der Umleitungs-ACL vom WLC hinzu. Konfigurieren Sie für das Profil "Vollständiger Zugriff" einen Zulassen-Zugriff mit dem entsprechenden Unternehmens-VLAN im Profil.



6. Das Autorisierungsprofil der Autorisierungsregel zuordnen. Für den vollständigen BYOD-Zugriff

muss die Regel Endpunkte· BYOD-Registrierung "yes" (Ja) lauten, damit der Benutzer nach dem BYOD-Fluss vollständigen Zugriff auf das Netzwerk erhält.

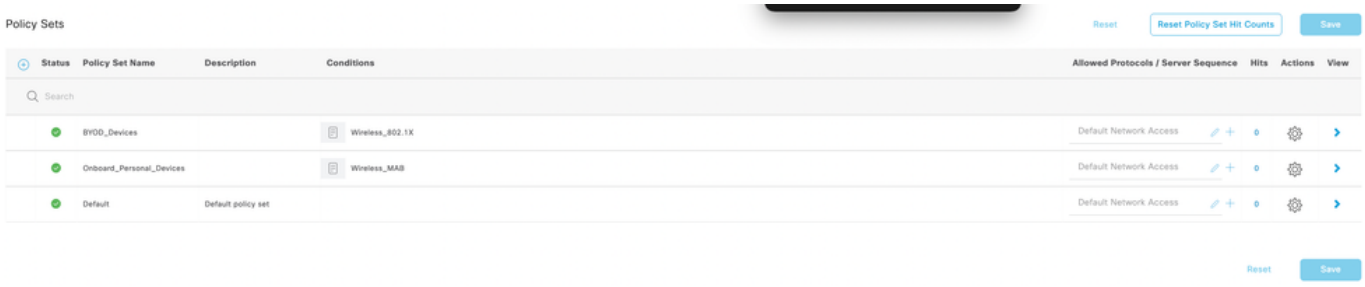


Konfigurieren von ISE-Richtliniensätzen für Dual-SSID-BYOD

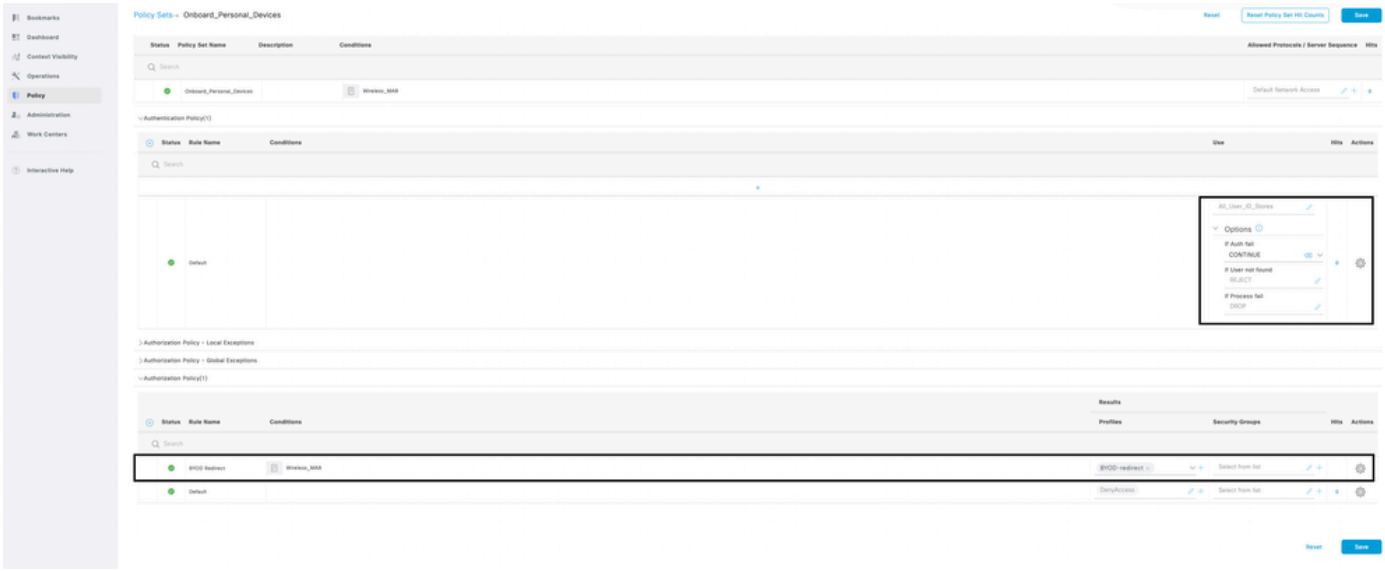
Bei einer BYOD-Konfiguration mit zwei SSIDs wird der Satz mit zwei Richtlinien auf der ISE konfiguriert. Der erste Richtliniensatz gilt für die offene/nicht gesicherte SSID, wobei die Konfiguration des Richtliniensatzes den Benutzer beim Herstellen einer Verbindung mit der offenen/nicht gesicherten SSID auf die BYOD-Seite umleitet.

1. Navigieren Sie zu Policy > Policy Set (Richtlinie > Richtliniensatz), und erstellen Sie eine Richtlinie für BYOD-Fluss auf der ISE.

2. Erstellen Sie einen Richtliniensatz für die offene/ungesicherte SSID und die Unternehmens-SSID, die den registrierten BYOD-Benutzer auf der ISE authentifiziert.

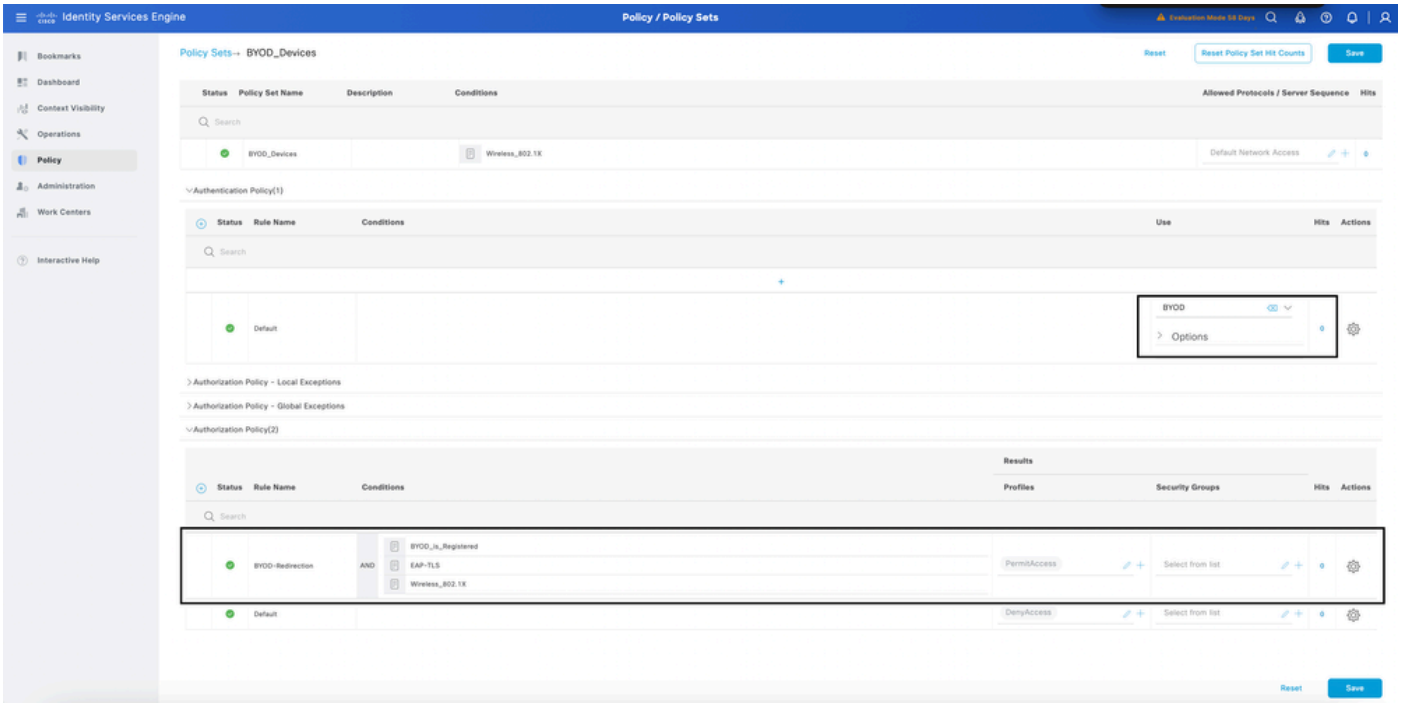


3. Wählen Sie im Onboarding Policy Set unter den Optionen die Option "Weiter" aus. Erstellen Sie für die Autorisierungsrichtlinie eine Bedingung, und ordnen Sie das Autorisierungsprofil für die Umleitung zu. Die gleichen Schritte sind bei der Erstellung des Autorisierungsprofils erforderlich, wie unter Nummer 4 beschrieben.



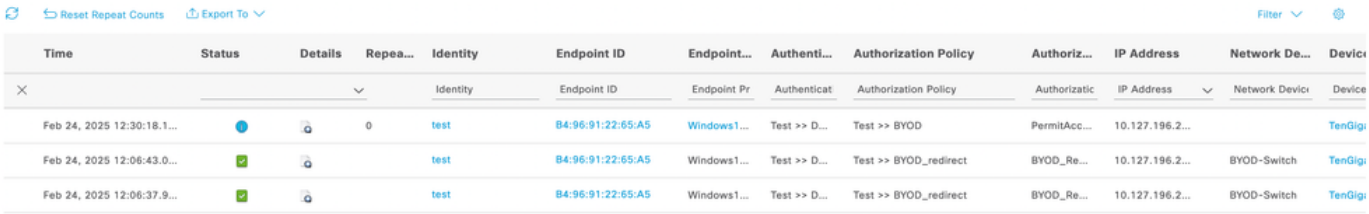
4. Konfigurieren Sie im registrierten BYOD-Richtliniensatz die Authentifizierungsrichtlinie mit dem gleichen Zertifikatprofil wie gefunden.

in Konfigurieren von ISE-Richtliniensätzen für BYOD mit einer SSID in Abschnitt 2. Erstellen Sie auch eine Bedingung für eine Autorisierungsrichtlinie, und ordnen Sie der Richtlinie das vollständige Zugriffsprofil zu.

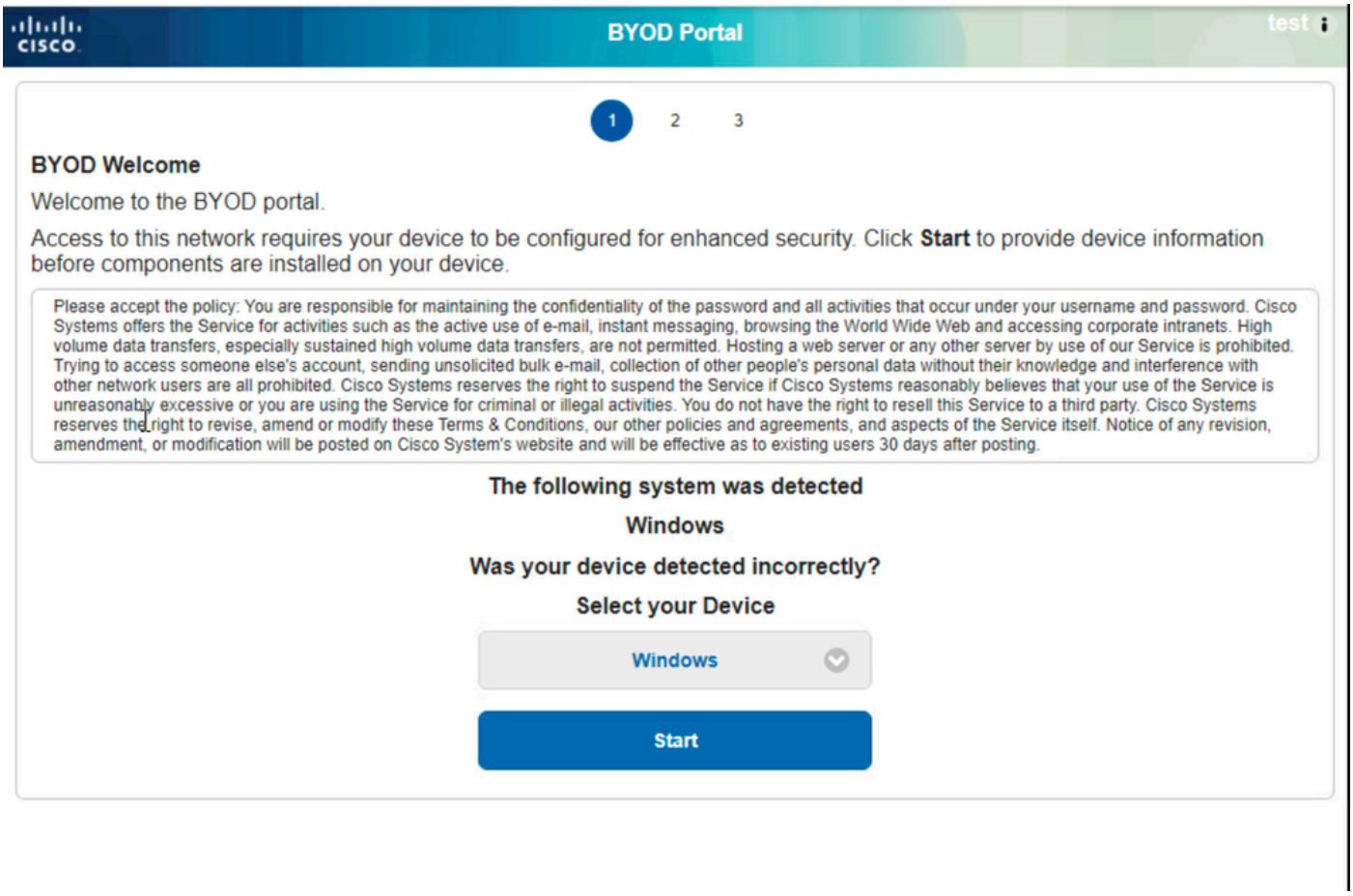


Protokollieren

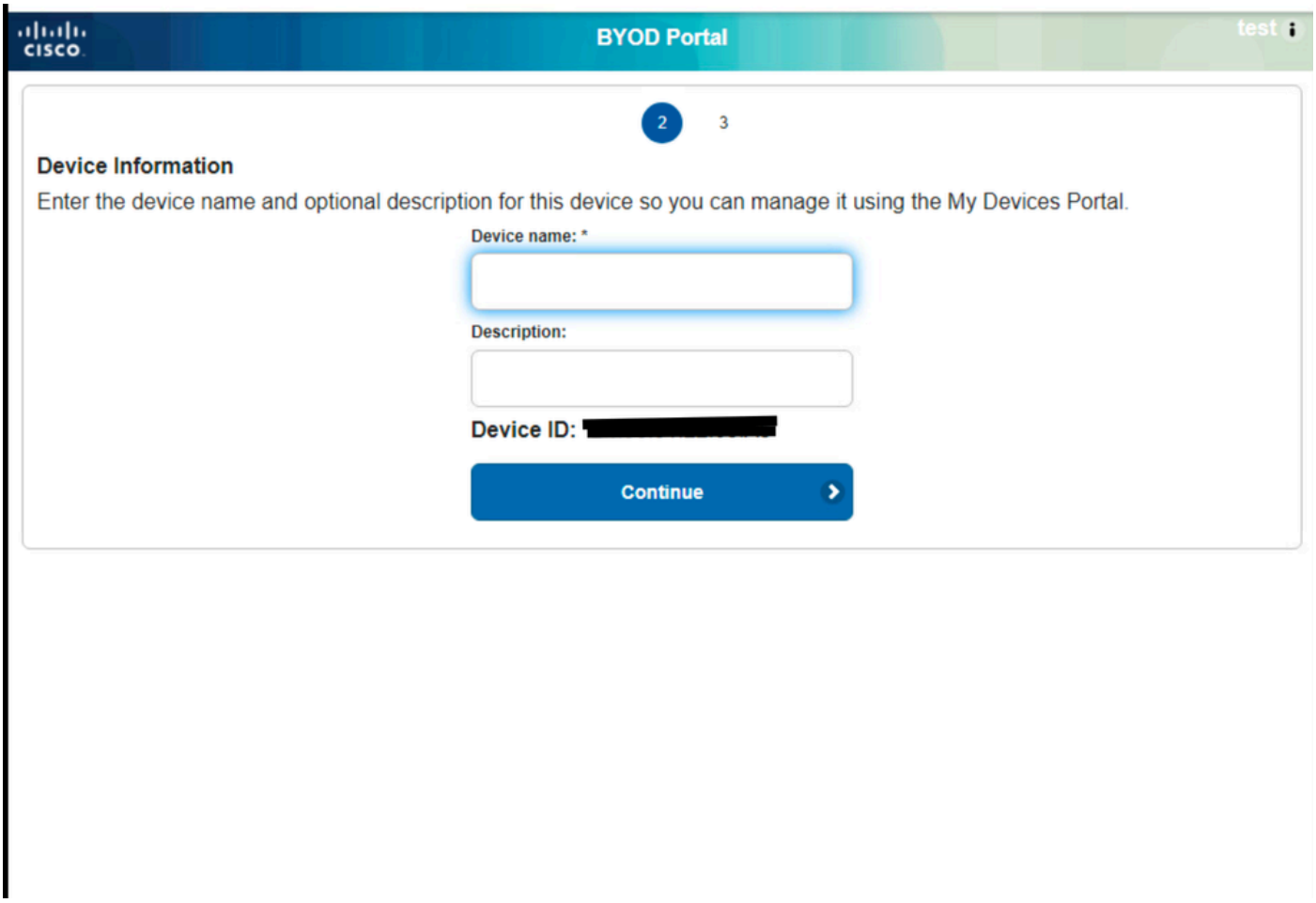
Die Benutzerauthentifizierung über das Live-Protokoll der ISE war erfolgreich und wird auf die Seite des BYOD-Portals umgeleitet. Nach Abschluss des BYOD-Prozesses erhält der Benutzer Zugriff auf das Netzwerk.



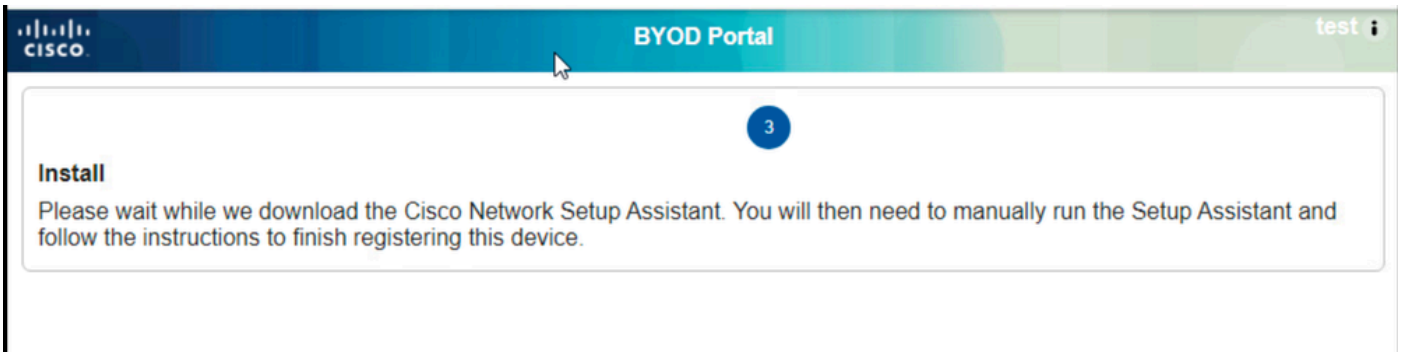
Aus Benutzersicht werden sie zunächst auf die BYOD-Seite weitergeleitet, und das entsprechende Gerät muss auf der Webseite ausgewählt werden. Zum Testen wurde ein Windows 10-Gerät verwendet



Nach dem Klicken auf die Schaltfläche Weiter werden Sie zu einer Seite weitergeleitet, auf der der Benutzer aufgefordert wird, den Namen des Geräts und eine Beschreibung einzugeben.

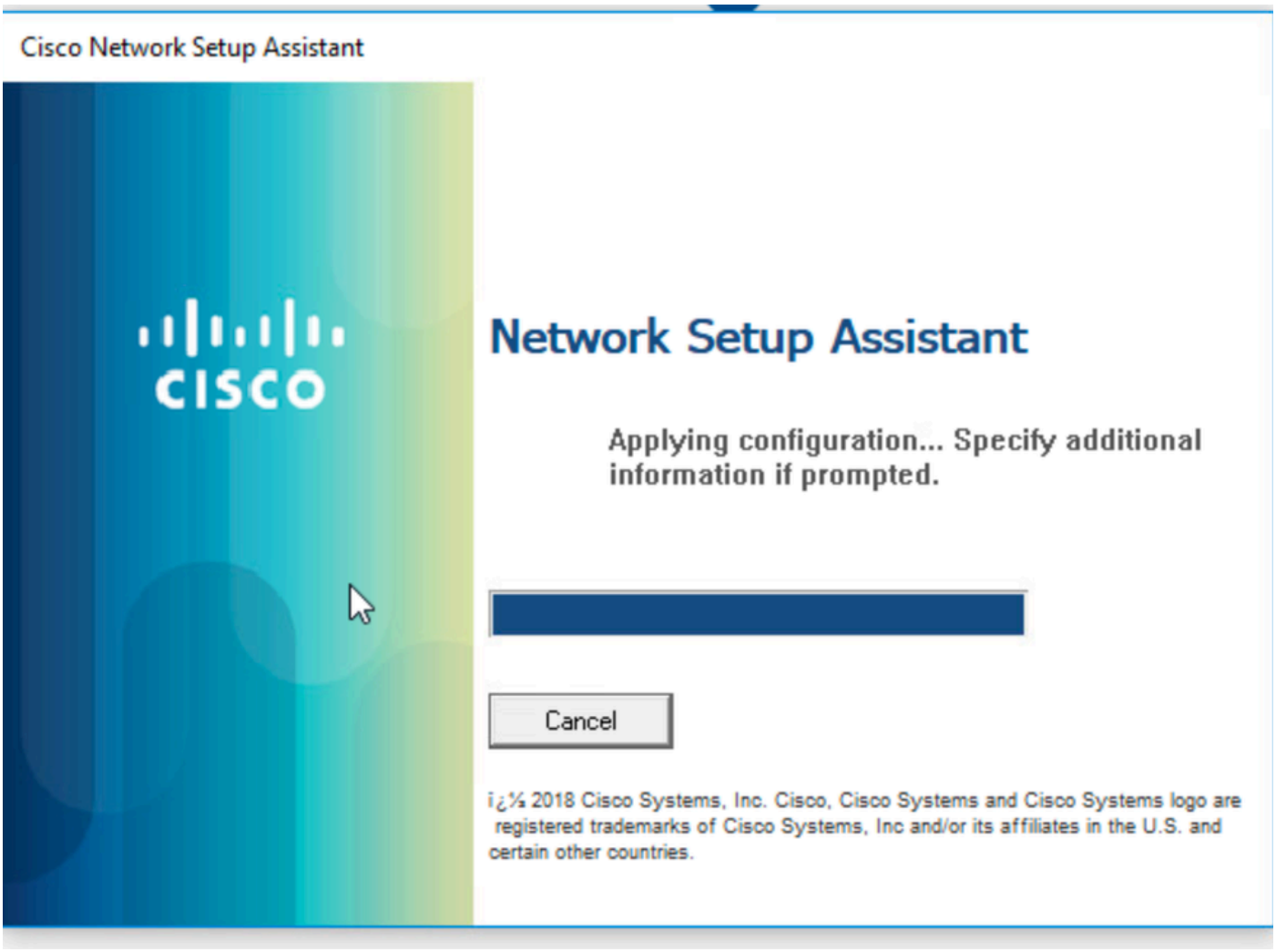


Bereitstellen, dass der Benutzer aufgefordert wird, das Tool Network Assistant zum Herunterladen des Endpunktprofils und des EAP-TLS-Zertifikats für die Authentifizierung herunterzuladen, wenn das Profil für die Durchführung der EAP-TLS-Authentifizierung konfiguriert ist



Führen Sie die Network Assistant-Anwendung mit Administratorberechtigungen aus, und klicken Sie auf die Schaltfläche Start, um den Onboarding-Fluss zu starten:


Cisco Network Setup Assistant
Network Setup Assistant
This application automatically configures network settings.
Start
Quit
i¿¼ 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



Der Benutzer wurde erfolgreich mit seinem privaten Gerät in das Netzwerk integriert, um auf die Ressourcen zuzugreifen.

Fehlerbehebung

Aktivieren Sie dieses Debugging auf der ISE, um das Problem mit BYOD zu beheben.

Auf Debugging-Ebene festzulegende Attribute:

- Client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)
- Profiler (profiler.log)

Protokollausschnitt

Gastprotokolle

Diese Protokolle zeigen an, dass der Benutzer erfolgreich auf die Seite umgeleitet und die Network Assistant-Anwendung heruntergeladen hat:

2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][[]] portalwebaction.utils.portal.spring.ISS EPortalControllerUtils -:000000000000000B30D59CC5:::- Zuordnungspfad gefunden in action-forwards, Weiterleitung an: pages/byodWelcome.jsp // The BYOD Welcome Page
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- Größe von pTranSchritte:1
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep, pTranSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep, stepTran:d2513b7b-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[[]] portalwebaction.utils.portal.spring.ISEP ortalControllerUtils -:000000000000000B30D59CC5:::- Zuordnungspfad in "action-forwards" gefunden, Weiterleitung an: pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- Größe von pTranSchritte:1
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep, pTranSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5:::test:- getNextFlowStep, stepTran:f203b757-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[[]] portalwebaction.utils.portal.spring.ISEP ortalControllerUtils -:000000000000000B30D59CC5:::- Zuordnungspfad in "action-forwards" gefunden, Weiterleitung an: pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[] cisco.cpm.client.provisioning.Streaming Servlet -:000000000000000B30D59CC5::- Sitzung = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[] cisco.cpm.client.provisioning.Streaming Servlet -:000000000000000B30D59CC5:::- portalSessionId = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5:::- StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-bbb91e8828da/NetworkSetupAssistant.exe // Die Netzwerkunterstützung wurde an den Endpunkt gesendet.

ISE-PSC-Protokolle

Wenn die Anwendung auf den Endpunkt heruntergeladen wird, initiiert die Anwendung einen SCEP-Fluss, um das Clientzertifikat von der ISE abzurufen.

24.02.2025 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- CertStore enthält 4 Zertifikate:
24.02.2025 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- 1. '[emittent=CN=Certificate Services Root CA - iseguest; serial=322815127387689606282525327846633020 89]"
24.02.2025 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- 2. '[emittent=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637]"
24.02.2025 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- 3. '[emittent=CN=Certificate Services Root CA - iseguest; serial=686276201605863086858498187751006982 24]"
24.02.2025 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- 4. '[emittent=CN=Certificate Services Node CA - iseguest; serial=729347676986030971539324822275488749 53]"
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Auswählen des Verschlüsselungszertifikats
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Auswählen des Zertifikats mit dem SchlüsselVerschlüsselungsschlüsselVerwendung
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Gefunden 1 Zertifikat(e) mit SchlüsselVerschlüsselungsschlüsselVerwendung
24.02.2025, 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Using [emitter=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] für Nachrichtenverschlüsselung
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Auswählen des Verifiziererzertifikats
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Auswählen des Zertifikats mit dem DigitalSignature-SchlüsselVerwendung
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Gefunden 1 Zertifikat(e) mit digitalemSignaturschlüsselVerwendung
24.02.2025, 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Using [emitter=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] für die Nachrichtenüberprüfung
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Auswählen des Ausstellerzertifikats
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::- Auswählen des Zertifikats mit basicConstraints

24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::- Gefunden 3 Zertifikat(e) mit basicConstraints
24.02.2025, 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -:::- Using [emitter=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] für Aussteller
24.02.2025 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -:::- Leistungsmetriken der SCEP-Server: name[live/tot, Anforderungen gesamt, Fehler gesamt, Anforderungen Flug, Durchschnittliche RTT] http://127.0.0.1:9444/caservice/scep[live,96444,1,0,120]

Endgeräteprofil-Download

Nachdem der SCEP-Prozess abgeschlossen ist und der Endpunkt das Zertifikat installiert hat, lädt die Anwendung das Endpunktprofil für die zukünftige Authentifizierung herunter, die vom Gerät ausgeführt wird:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::- Refferer = Windows // The Windows device wurde basierend auf der Webseite erkannt.
24.02.2025, 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::- Sitzung = 000000000000000B30D59M KV 5
24.02.2025, 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::- Sitzung = 000000000000000B30D59M KV 5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::- provisionieren nsp profile
24.02.2025, 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::- Sitzung = 000000000000000B30D55 9KV5
24.02.2025, 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::- portalSessionId = null
24.02.2025, 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-NSP.xml //Das NSP-Profil wird auf den Endpunkt heruntergeladen.
24.02.2025, 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::- Streaming to ip: Dateityp: Nativer SPProfile-Dateiname:Cisco-ISE-NSP.xml //The Network Assistant Application
24.02.2025, 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::- BYODStatus:INIT_PROFILE
24.02.2025, 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::- userId has been set to test
24.02.2025, 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::- Weiterleitungstyp: SUCCESS_PAGE, URL für Umleitung: für Mac:

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.