Konfigurieren des Status auf Catalyst 9800 WLC und ISE

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration eines Status-WLAN auf einem Catalyst 9800 WLC und der ISE über die grafische Benutzeroberfläche (Graphic User Interface, GUI).

Voraussetzungen

Anforderungen

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

- 9800 WLC - allgemeine Konfiguration
- ISE-Richtlinien- und Profilkonfiguration

Verwendete Komponenten

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

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- Identity Service Engine (ISE) v3.2
- Laptop Windows 10 Enterprise

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

Wireless LAN Controller - RADIUS NAC- und CoA-Funktionsablauf

1. Der Client authentifiziert sich mithilfe der 802.1x-Authentifizierung.

2. RADIUS Access Accept beinhaltet die umgeleitete URL für Port 80 und vorab erstellte ACLs, die das Zulassen von IP-Adressen und Ports oder das Quarantäne-VLAN umfasst.

3. Der Client wird auf die unter "access accept" angegebene URL umgeleitet und in einen neuen Zustand versetzt, bis die Statusüberprüfung abgeschlossen ist. Der Client kommuniziert in diesem Zustand mit dem ISE-Server und überprüft sich anhand der auf dem ISE NAC-Server konfigurierten Richtlinien.

4. NAC-Agent auf Client initiiert Statusüberprüfung (Datenverkehr zu Port 80): Der Agent sendet eine HTTP-Erkennungsanforderung an Port 80, die der Controller an die im Zugriffs-Accept angegebene URL umleitet. Die ISE weiß, dass der Client die Verbindung herstellen will und direkt auf den Client reagiert. Auf diese Weise erfährt der Client die IP-Adresse des ISE-Servers und kommuniziert von nun an direkt mit dem ISE-Server.

5. WLC lässt diesen Datenverkehr zu, da die ACL so konfiguriert ist, dass dieser Datenverkehr zugelassen wird. Bei einer VLAN-Übersteuerung wird der Datenverkehr überbrückt, sodass er den ISE-Server erreicht.

6. Nach Abschluss der Bewertung durch den ISE-Client wird ein RADIUS-CoA-Req. mit Büroth-Service an den WLC gesendet. Dadurch wird eine erneute Authentifizierung des Clients (durch Senden von EAP-START) initiiert. Sobald die erneute Authentifizierung erfolgreich ist, sendet die ISE eine Zugriffsbestätigung mit einer neuen ACL (falls vorhanden), ohne URL-Umleitung oder Zugriffs-VLAN.

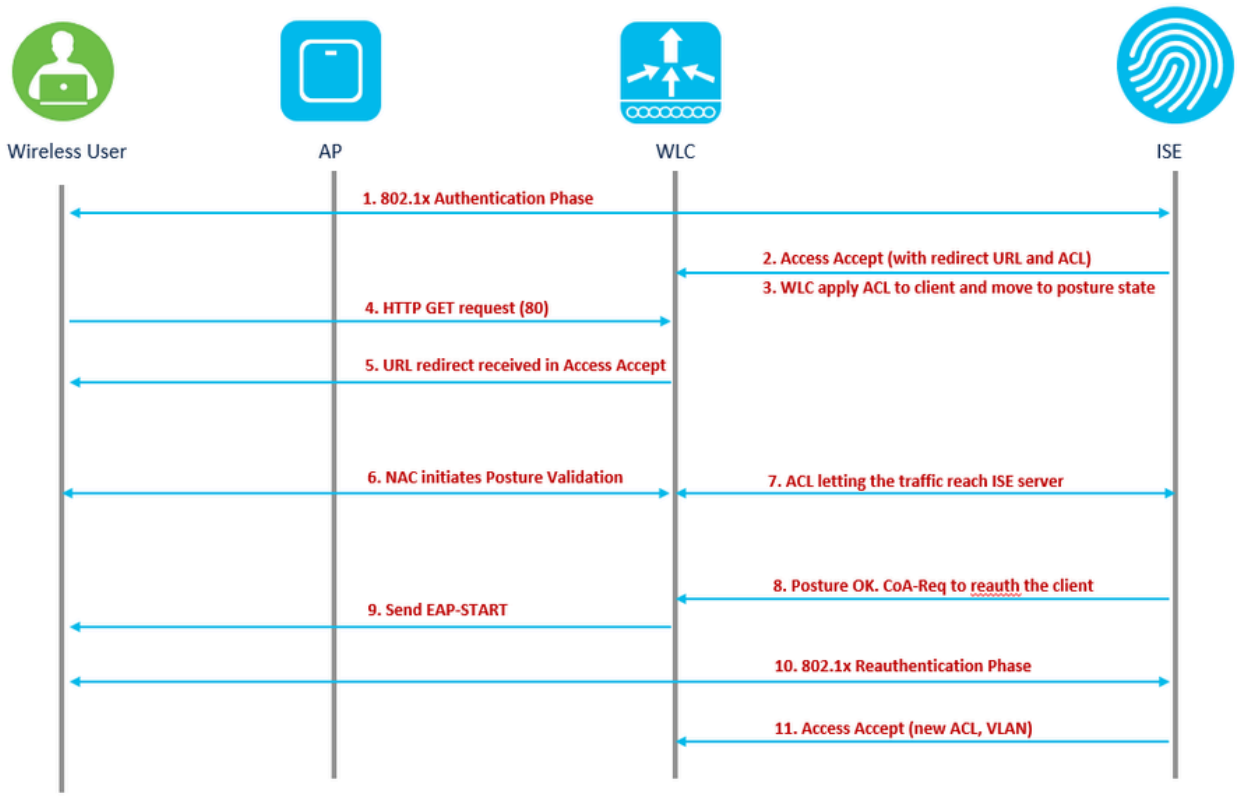
7. WLC unterstützt CoA-Req und Disconnect-Req gemäß RFC 3576. Der WLC muss die CoA-Anforderung für den Authentifizierungsdienst gemäß RFC 5176 unterstützen.

8. Statt herunterladbarer ACLs werden auf dem WLC vorkonfigurierte ACLs verwendet. Der ISE-

Server sendet nur den ACL-Namen, der bereits im Controller konfiguriert ist.

9. Dieses Design eignet sich sowohl für VLAN- als auch für ACL-Gehäuse. Im Fall einer VLAN-Übersteuerung leiten wir nur Port 80 um, der umgeleitet wird und den restlichen Verkehr (Bridge) auf das Quarantäne-VLAN überträgt. Auf die ACL wird die im Accept-Modus vor der Authentifizierung empfangene ACL angewendet.

Diese Abbildung zeigt den Funktionsablauf in visueller Darstellung:



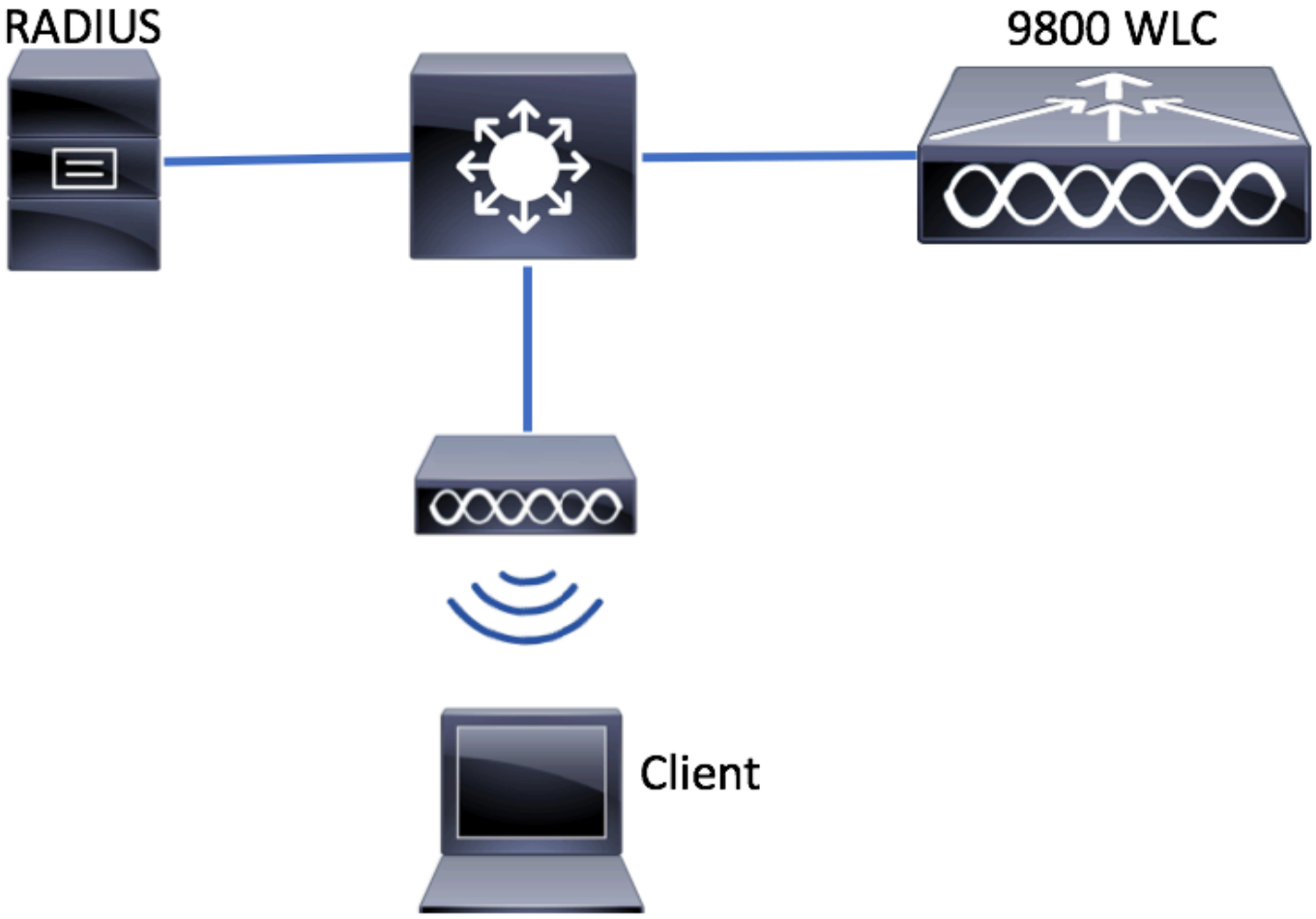
Feature-Workflow

In diesem Anwendungsfall wird eine SSID, die nur für Unternehmensbenutzer verwendet wird, für den Status aktiviert. Andere Anwendungsfälle wie BYOD, Guest oder andere sind für diese SSID nicht verfügbar.

Wenn ein Wireless-Client zum ersten Mal eine Verbindung mit der Posture-SSID herstellt, muss er das Posture-Modul auf das umgeleitete Portal der ISE herunterladen und installieren und schließlich mit den relevanten ACLs basierend auf dem Ergebnis der Statusprüfung (konform/nicht konform) anwenden.

Konfigurieren

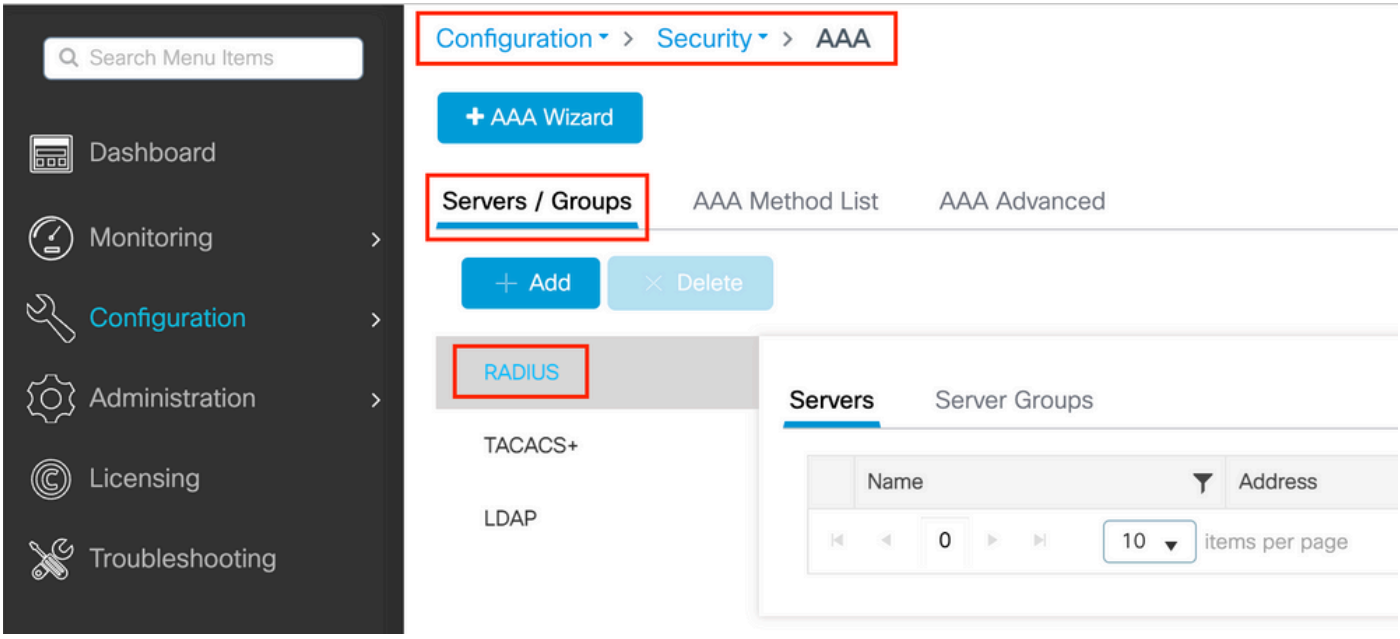
Netzwerkdiagramm



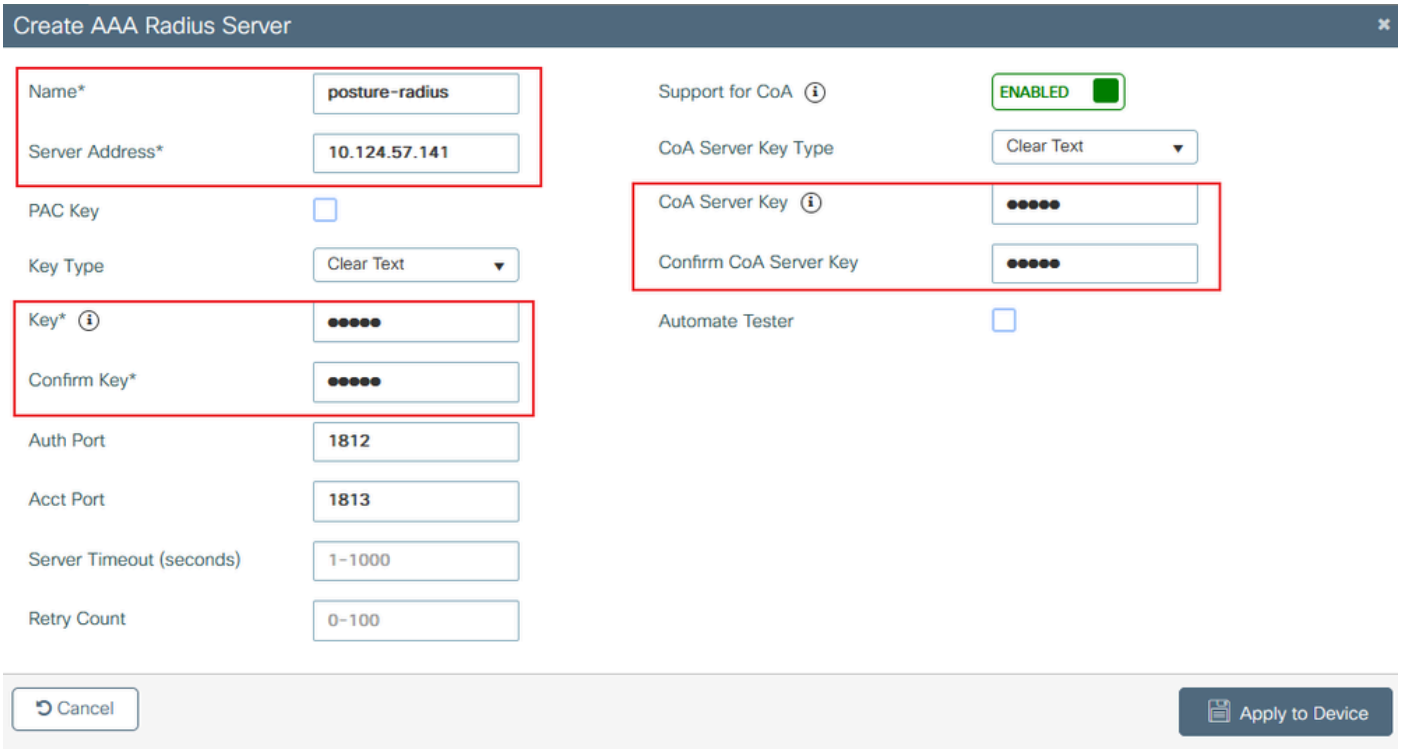
Netzwerkdiagramm

AAA-Konfiguration auf dem 9800 WLC

Schritt 1: Fügen Sie den ISE-Server der 9800 WLC-Konfiguration hinzu. Navigieren Sie zu Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add, und geben Sie die RADIUS-Serverinformationen wie in den Bildern dargestellt ein. Stellen Sie sicher, dass die Unterstützung für CoA für den Status-NAC aktiviert ist.

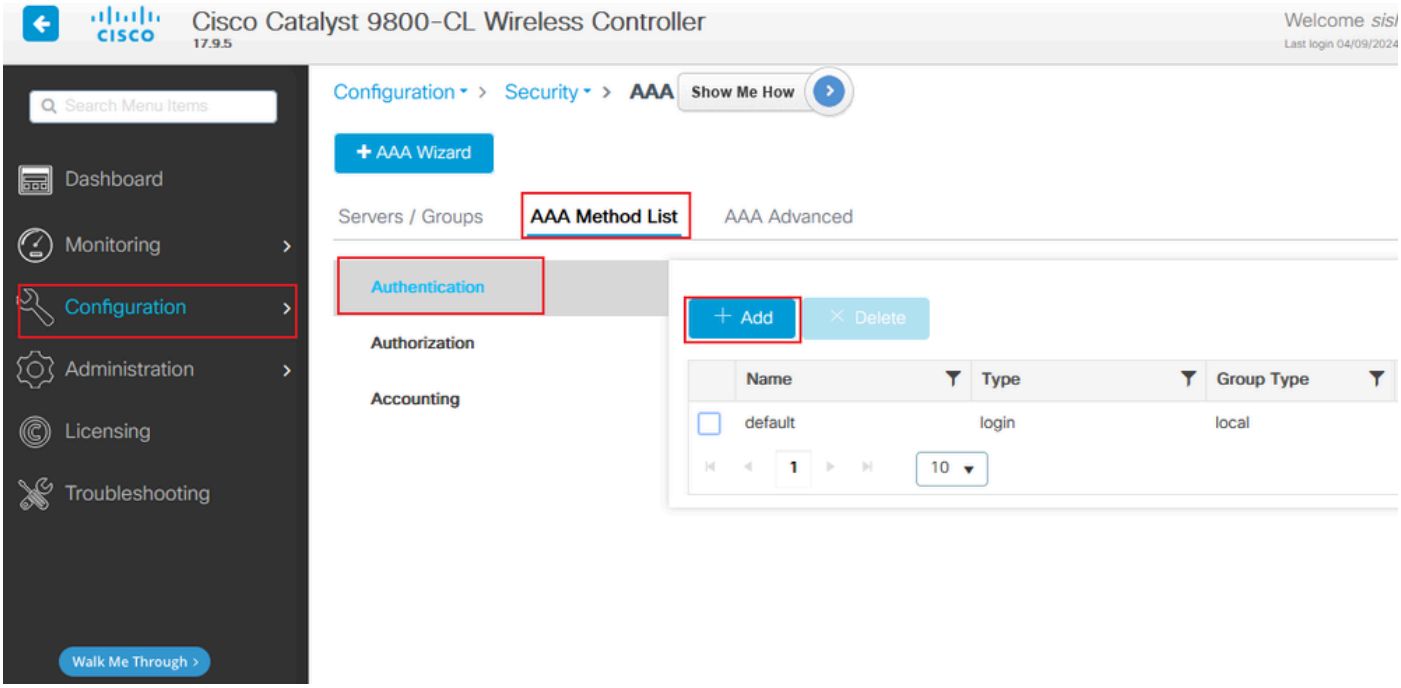


9800 Radius-Server erstellen

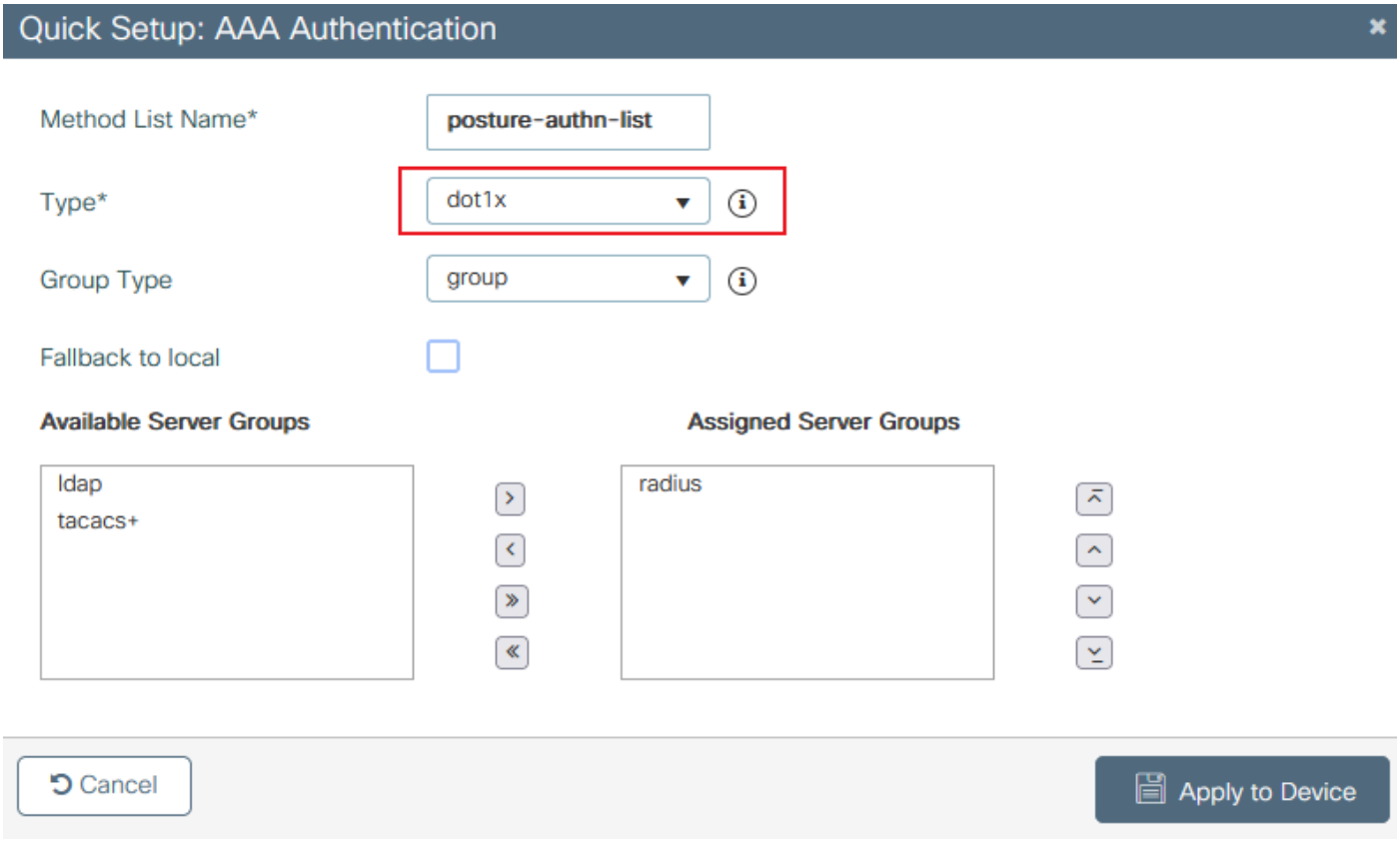


9800 Radius-Details erstellen

Schritt 2: Erstellen Sie eine Liste der Authentifizierungsmethoden. Navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authentication > + Add, wie im Bild dargestellt:

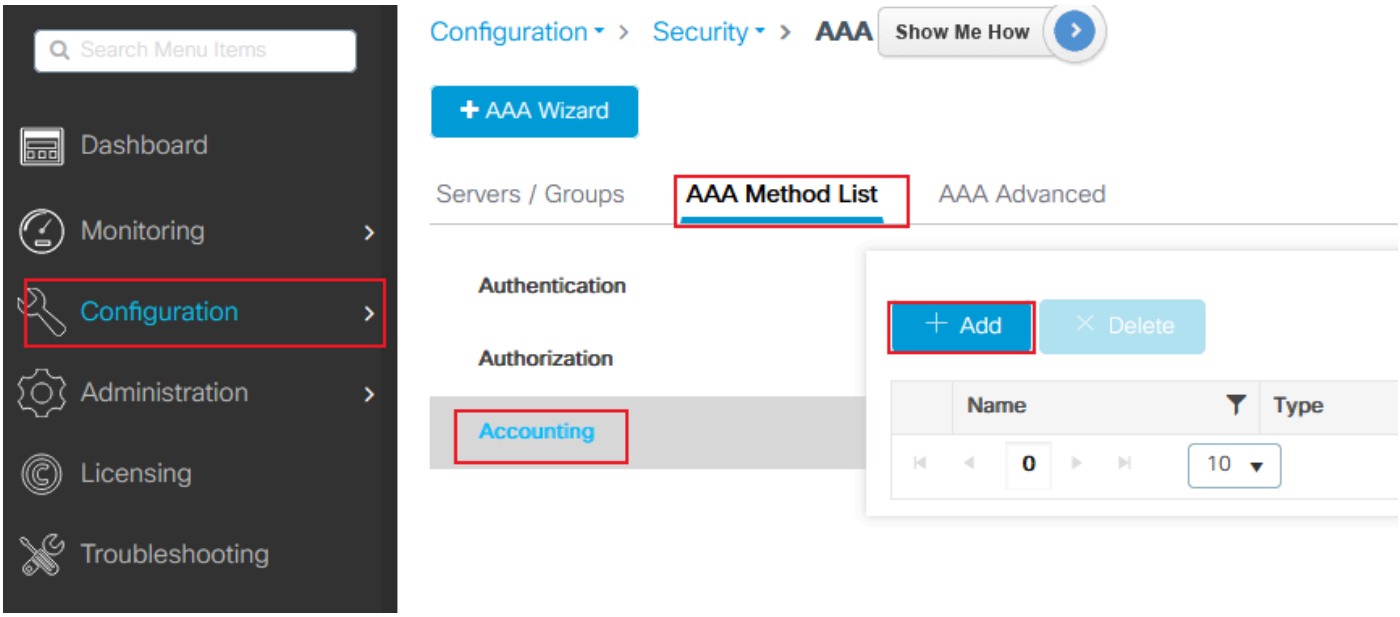


9800 - Authentifizierungsliste hinzufügen

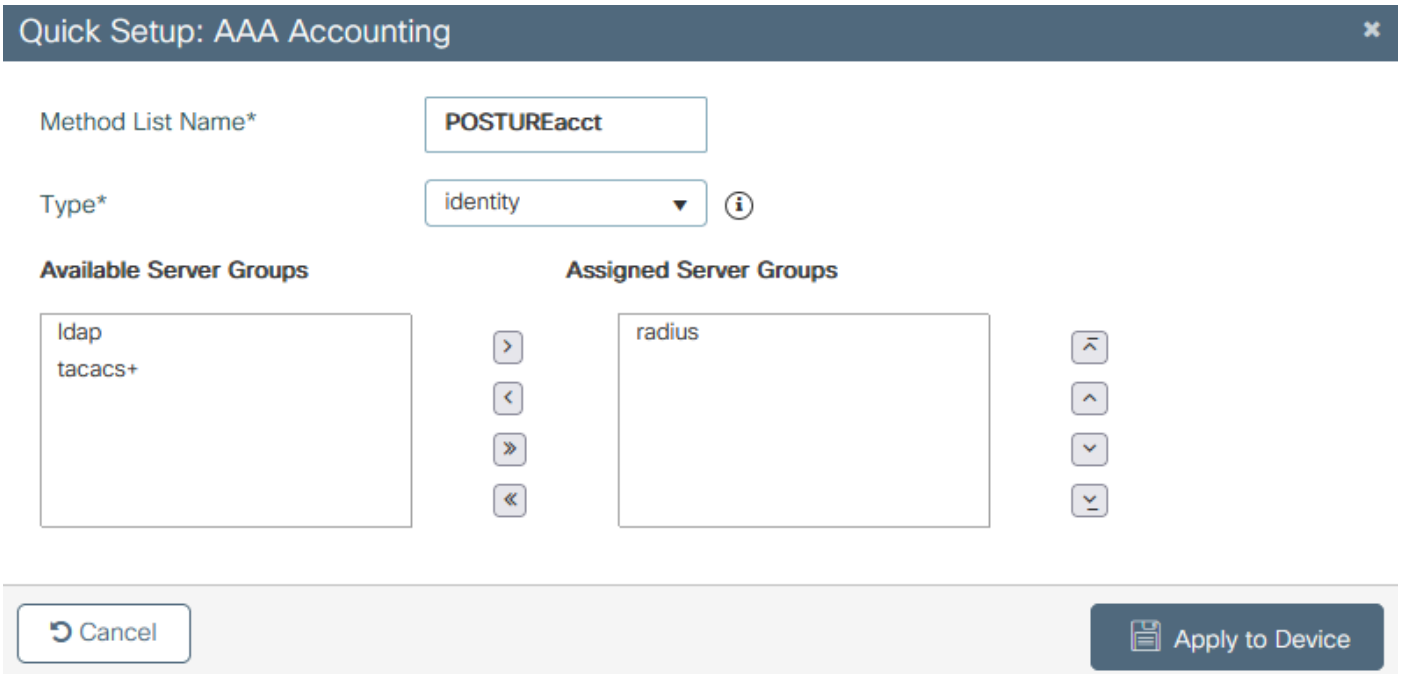


9800 - Authentifizierungslistendetails erstellen

Schritt 3. (Optional) Erstellen Sie eine Abrechnungsmethodenliste, wie in der Abbildung dargestellt:



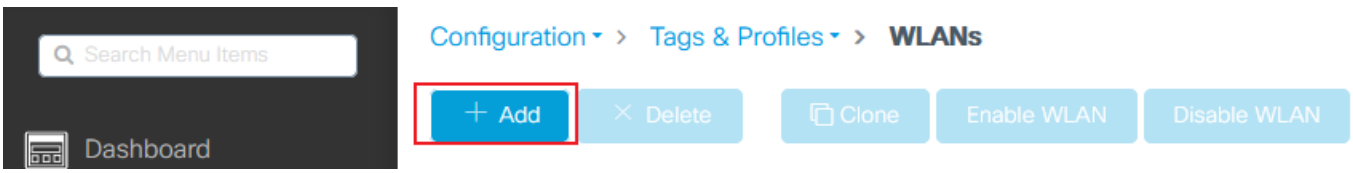
9800 Kundenliste hinzufügen



9800 Kundenlistendetails erstellen

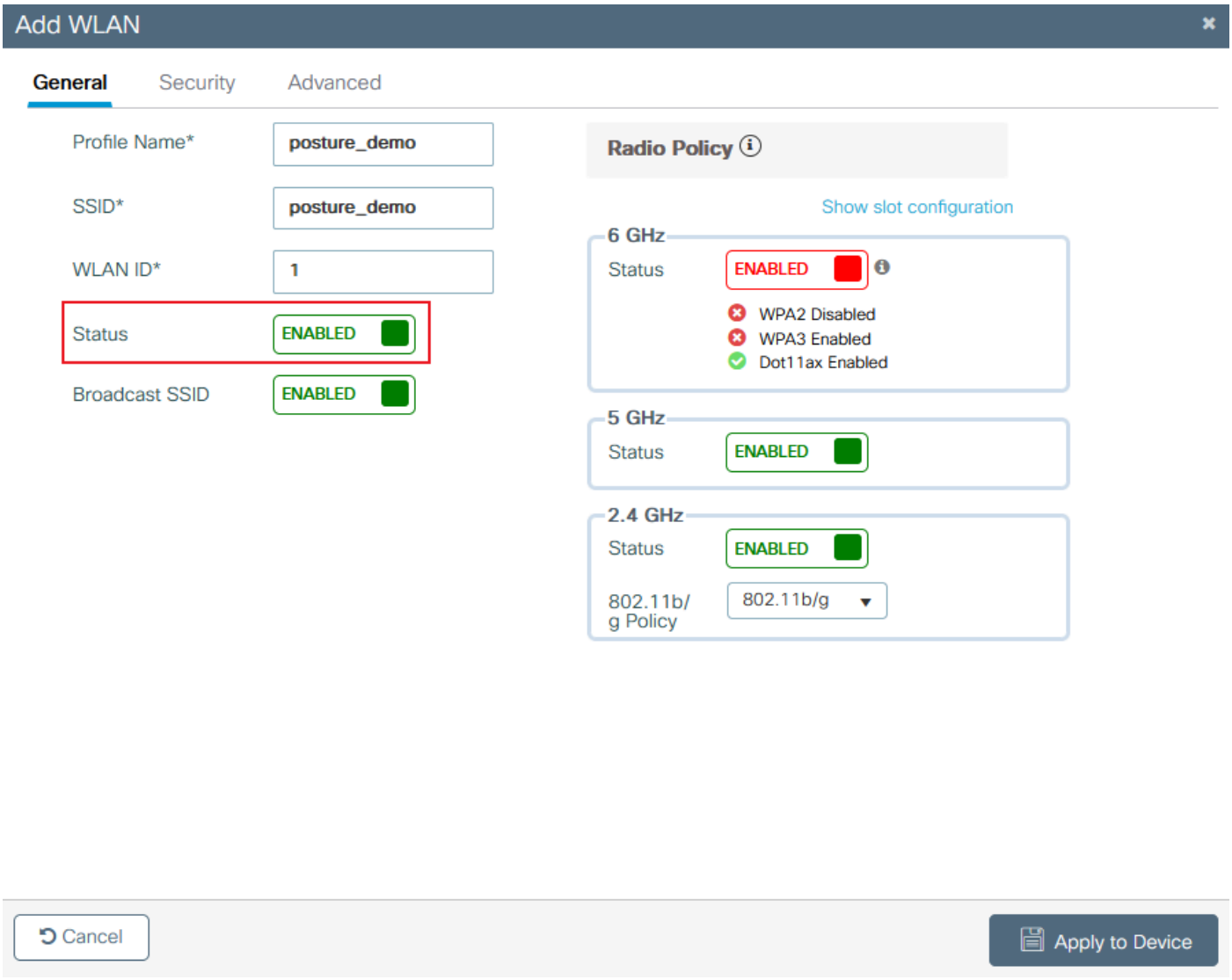
WLAN-Konfiguration

Schritt 1: Erstellen Sie das WLAN. Navigieren Sie zu Configuration > Tags & Profiles > WLANs > + Add, und konfigurieren Sie das Netzwerk nach Bedarf:



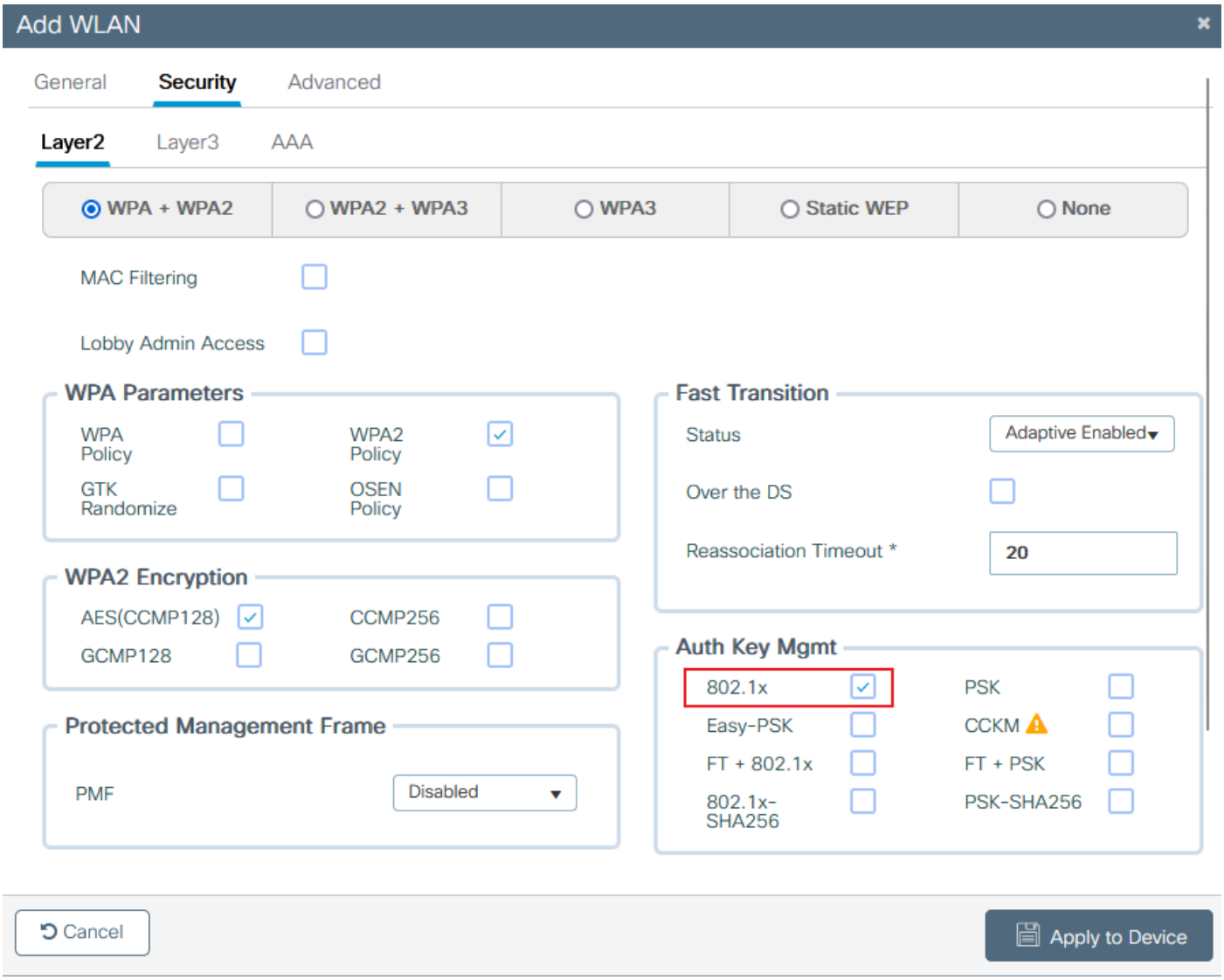
9800 WLAN hinzufügen

Schritt 2: Geben Sie die allgemeinen WLAN-Informationen ein.

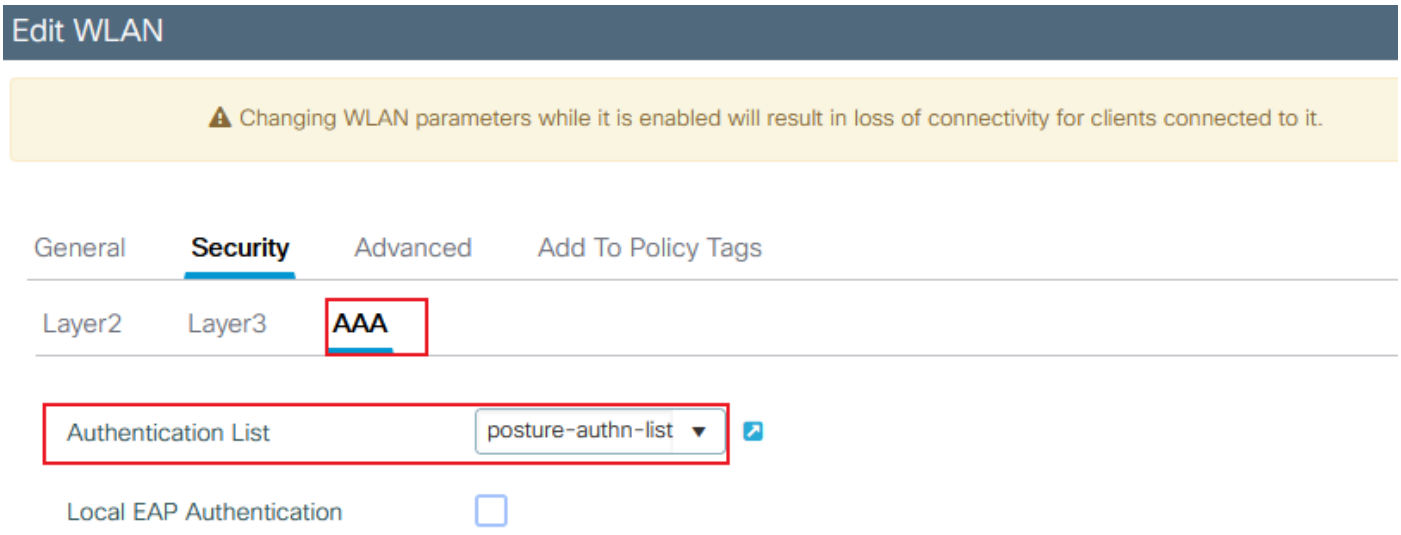


9800 WLAN erstellen allgemein

Schritt 3: Navigieren Sie zur Registerkarte Sicherheit, und wählen Sie die gewünschte Sicherheitsmethode aus. Wählen Sie in diesem Fall "802.1x" aus, und die AAA-Authentifizierungsliste (die Sie in Schritt 2 im Abschnitt zur AAA-Konfiguration erstellt haben) wird benötigt:



9800 erstellen WLAN-Sicherheit L2

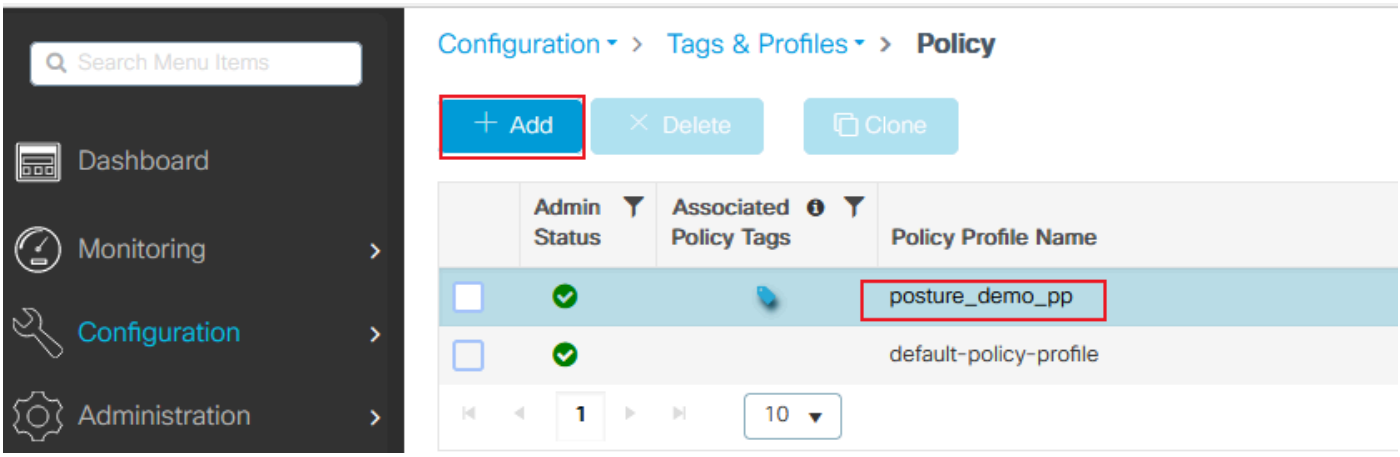


9800 erstellt WLAN-Sicherheit AAA

Richtlinienprofilkonfiguration

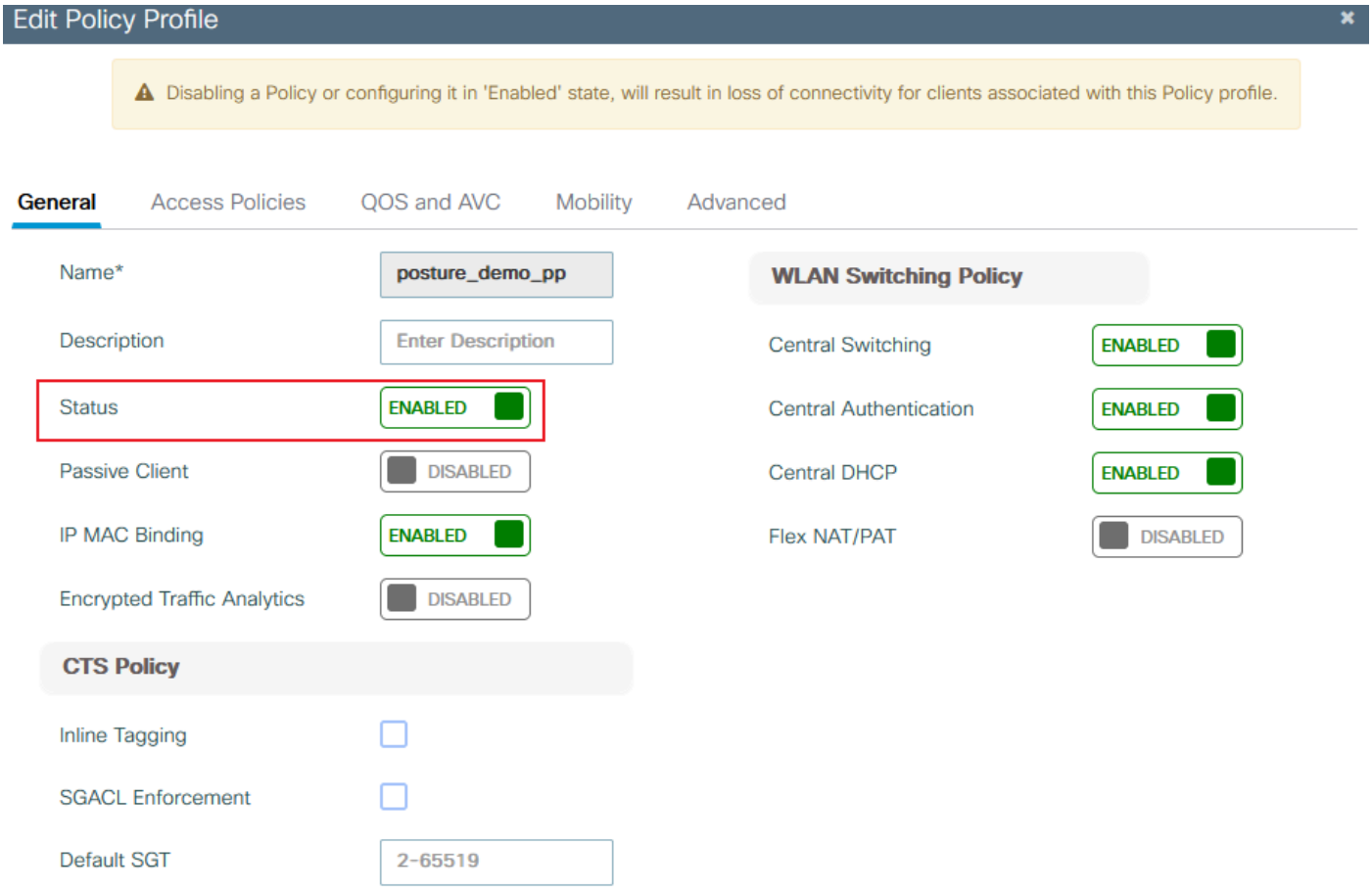
In einem Richtlinienprofil können Sie den Clients neben anderen Einstellungen (wie Zugriffskontrolllisten (ACLs), Quality of Service (QoS), Mobility Anchor, Timer usw.) festlegen, welchem VLAN sie zugewiesen werden sollen. Sie können entweder Ihr Standardrichtlinienprofil verwenden oder ein neues erstellen.

Schritt 1: Erstellen eines neuen Richtlinienprofils. Navigieren Sie zu Configuration > Tags & Profiles > Policy, und erstellen Sie eine neue:



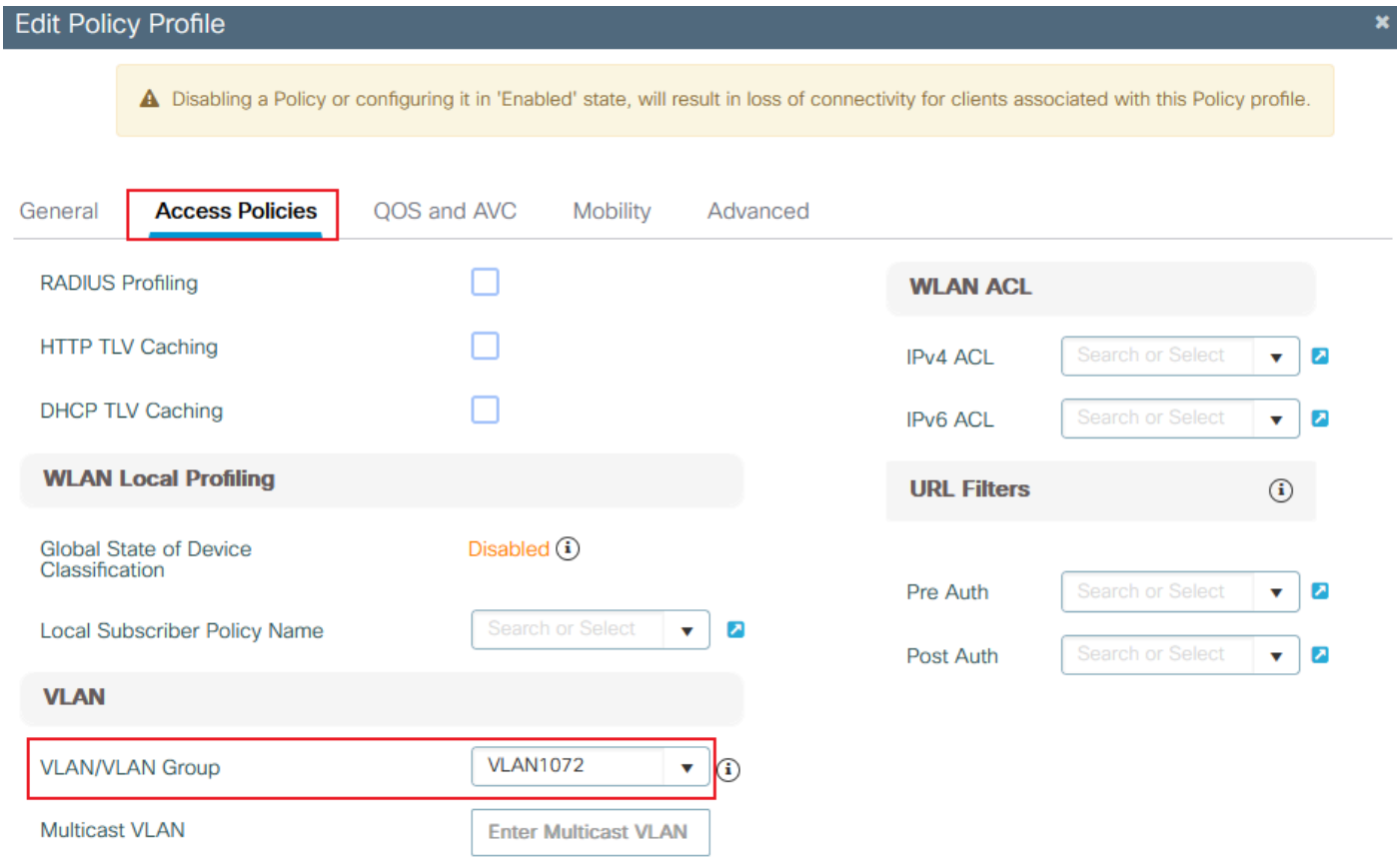
9800 Richtlinienprofil hinzufügen

Stellen Sie sicher, dass das Profil aktiviert ist.



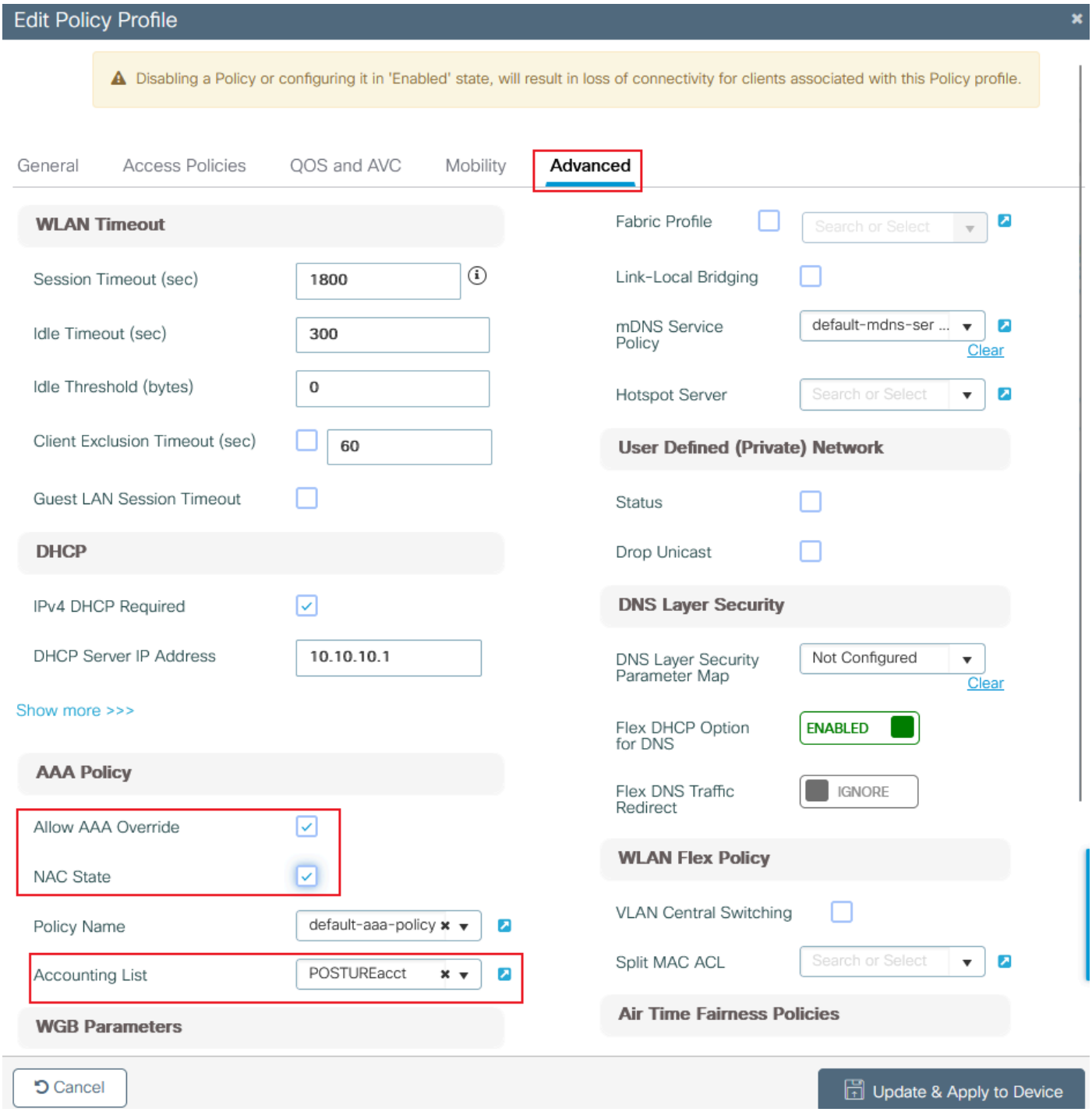
9800 Richtlinienprofil erstellen (allgemein)

Schritt 2: Wählen Sie das VLAN aus. Navigieren Sie zur Registerkarte Access Policies (Zugriffsrichtlinien), und wählen Sie den VLAN-Namen aus dem Dropdown-Menü aus, oder geben Sie die VLAN-ID manuell ein. Konfigurieren Sie keine ACL im Richtlinienprofil:



9800 erstellt Richtlinienprofil-VLAN

Schritt 3: Konfigurieren Sie das Richtlinienprofil so, dass ISE-Außerkraftsetzungen (AAA-Außerkraftsetzung zulassen) und Autorisierungsänderung (CoA) (NAC-Status) akzeptiert werden. Sie können optional auch eine Abrechnungsmethode angeben:

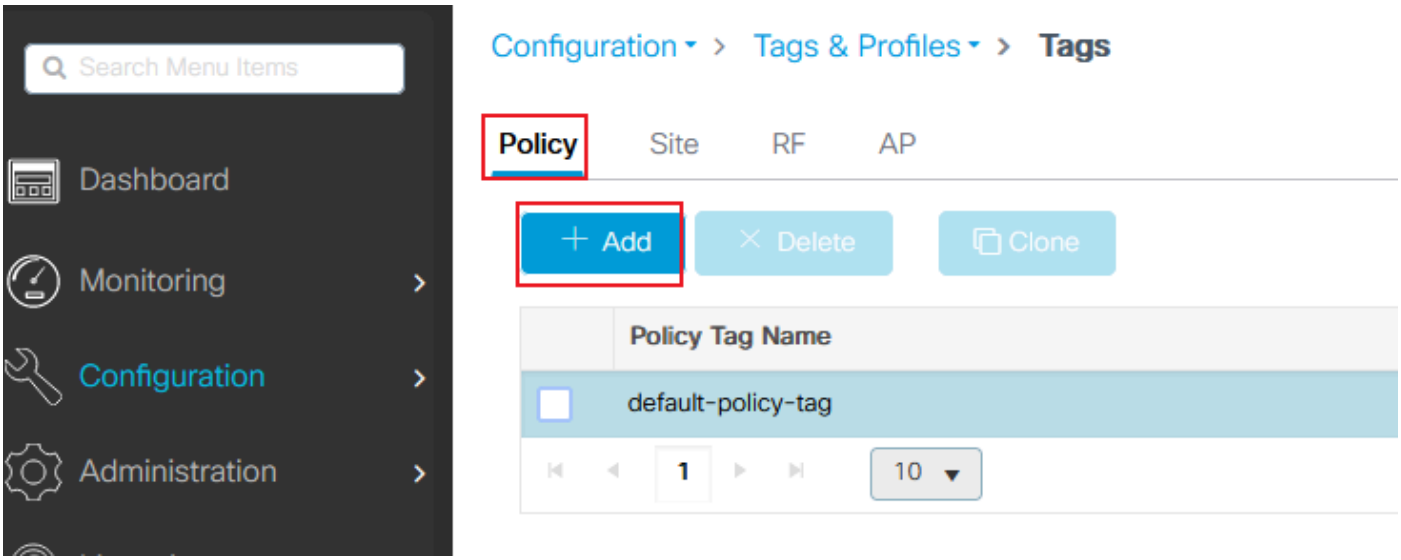


9800 Richtlinienprofil erstellen Erweitert

Richtlinien-Tag-Konfiguration

Sie verbinden Ihre SSID innerhalb des Richtlinien-Tags mit Ihrem Richtlinienprofil. Sie können entweder ein neues Richtlinien-Tag erstellen oder das Standard-Richtlinien-Tag verwenden.

Navigieren Sie zu Configuration > Tags & Profiles > Tags > Policy, und fügen Sie bei Bedarf eine neue hinzu, wie im Bild gezeigt:



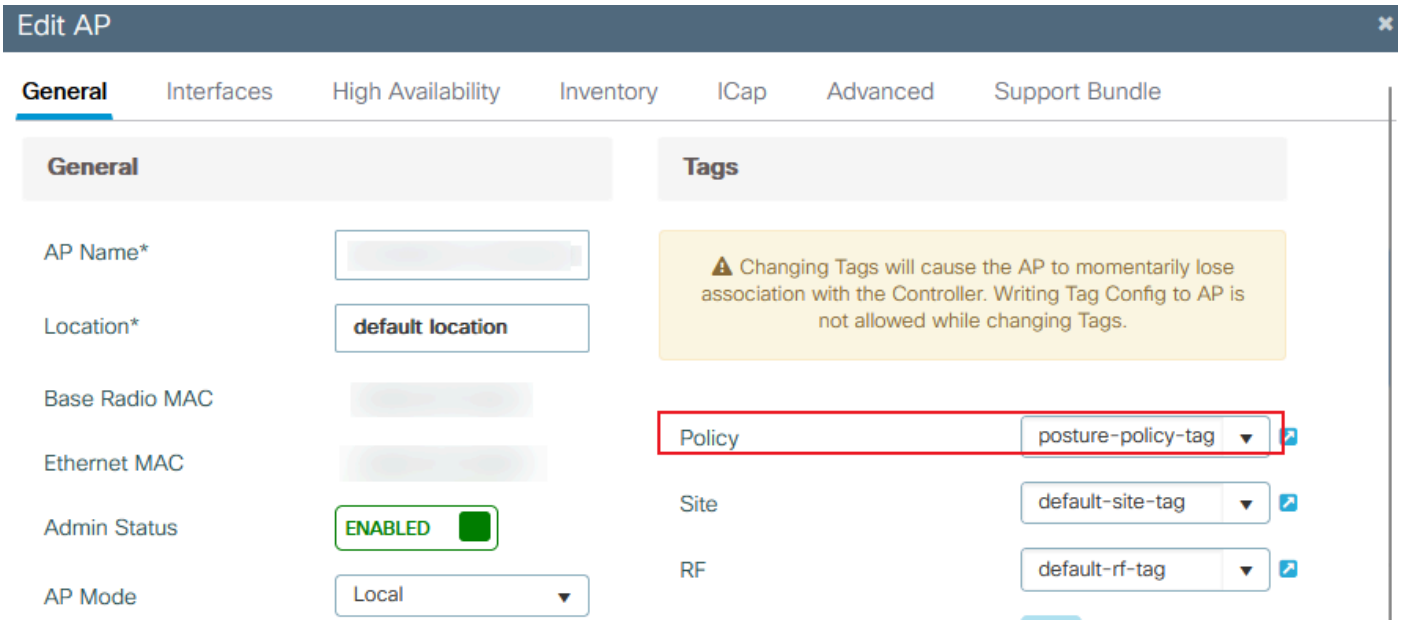
9800 policy tag add

Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil:

Details zu 9800-Richtlinien-Tags

Richtlinien-Tag-Zuweisung

Weisen Sie den erforderlichen APs das Richtlinien-Tag zu. Navigieren Sie zu Configuration > Wireless > Access Points > AP Name > General Tags, nehmen Sie die erforderliche Zuweisung vor, und klicken Sie dann auf Update & Apply to Device .



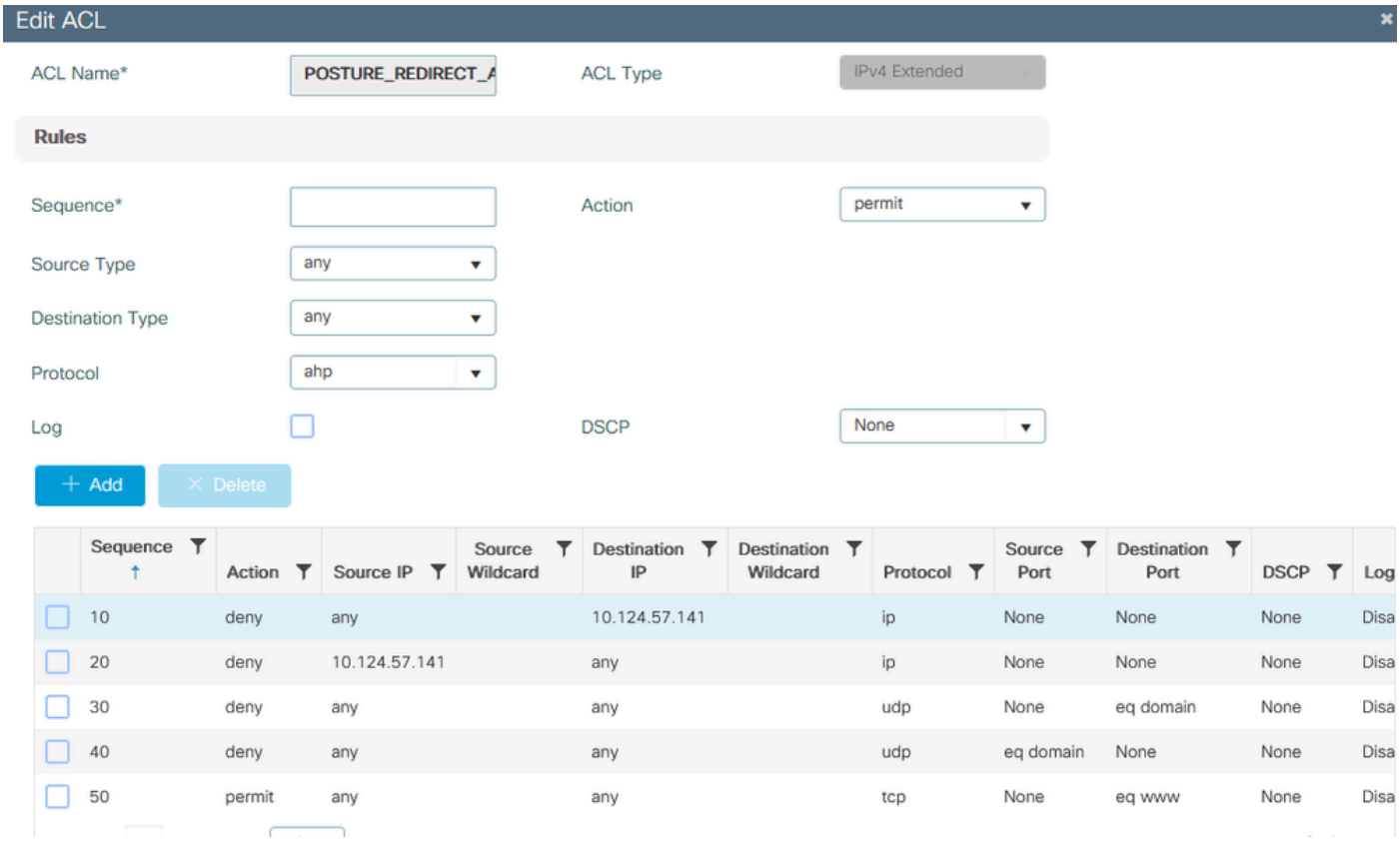
9800-Zuweisen von Richtlinientags

Umleiten der ACL-Konfiguration

Navigieren Sie zu Configuration > Security > ACL > + Add (Konfiguration > Sicherheit > ACL > + Hinzufügen), um eine neue ACL zu erstellen.

Die für die Posture Portal Redirect verwendete ACL erfüllt dieselben Anforderungen wie die CWA (Central Web Authentication).

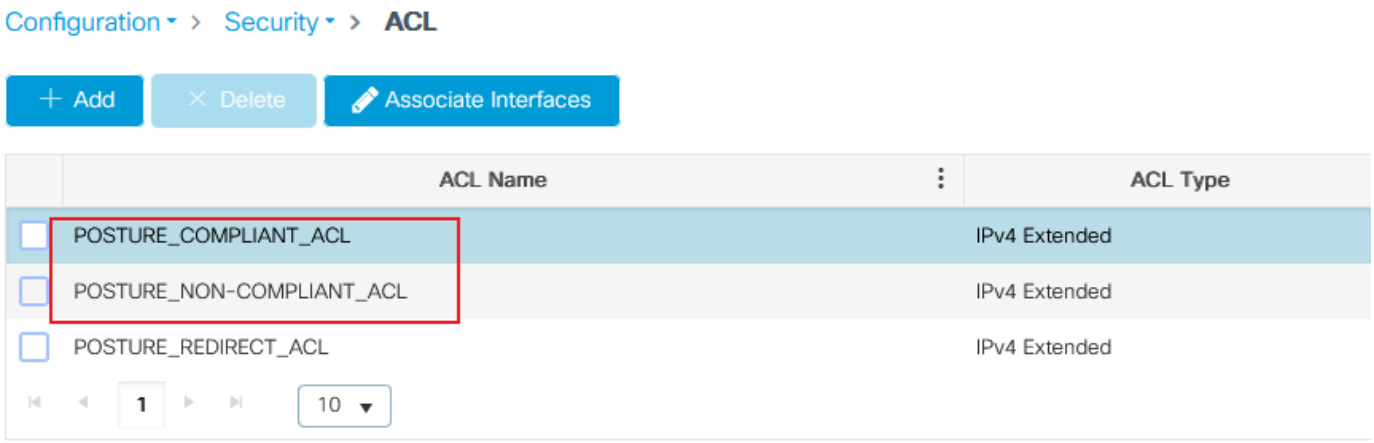
Sie müssen den Traffic zu Ihren ISE-PSNs-Knoten sowie DNS verweigern und den Rest zulassen. Bei dieser Umleitungs-ACL handelt es sich nicht um eine Sicherheits-ACL, sondern um eine Punkt-ACL, die festlegt, welcher Datenverkehr zur Weiterbehandlung (z. B. Umleitung) an die CPU weitergeleitet wird (bei entsprechender Berechtigung) und welcher Datenverkehr auf der Datenebene verbleibt (bei Ablehnung), um eine Umleitung zu vermeiden. Die ACL muss wie folgt aussehen (ersetzen Sie in diesem Beispiel 10.124.57.141 durch Ihre ISE-IP-Adresse):



ACL-Details für 9800-Umleitung

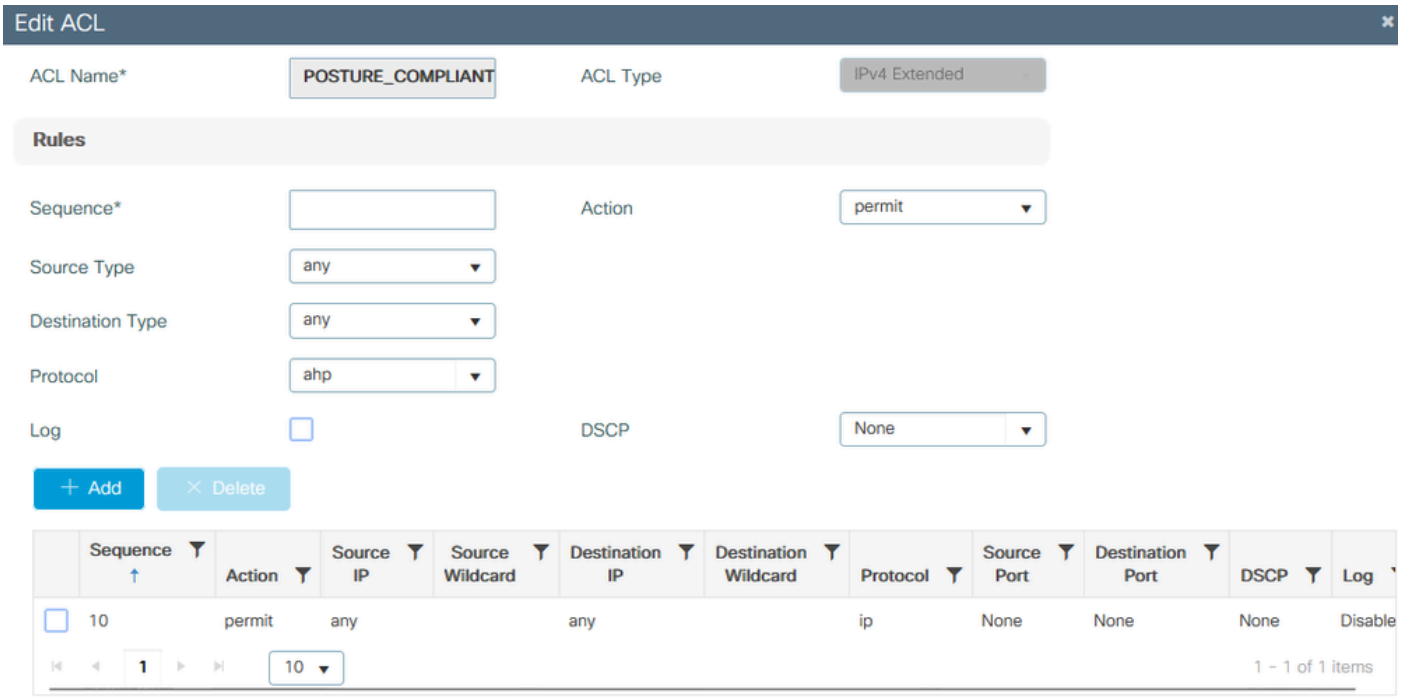
Richtlinien-ACL-Konfiguration

In diesem Fall müssen Sie separate ACLs für den 9800 WLC für die ISE definieren, um die konformen und nicht konformen Szenarien basierend auf dem Ergebnis der Port-Prüfung zu autorisieren.



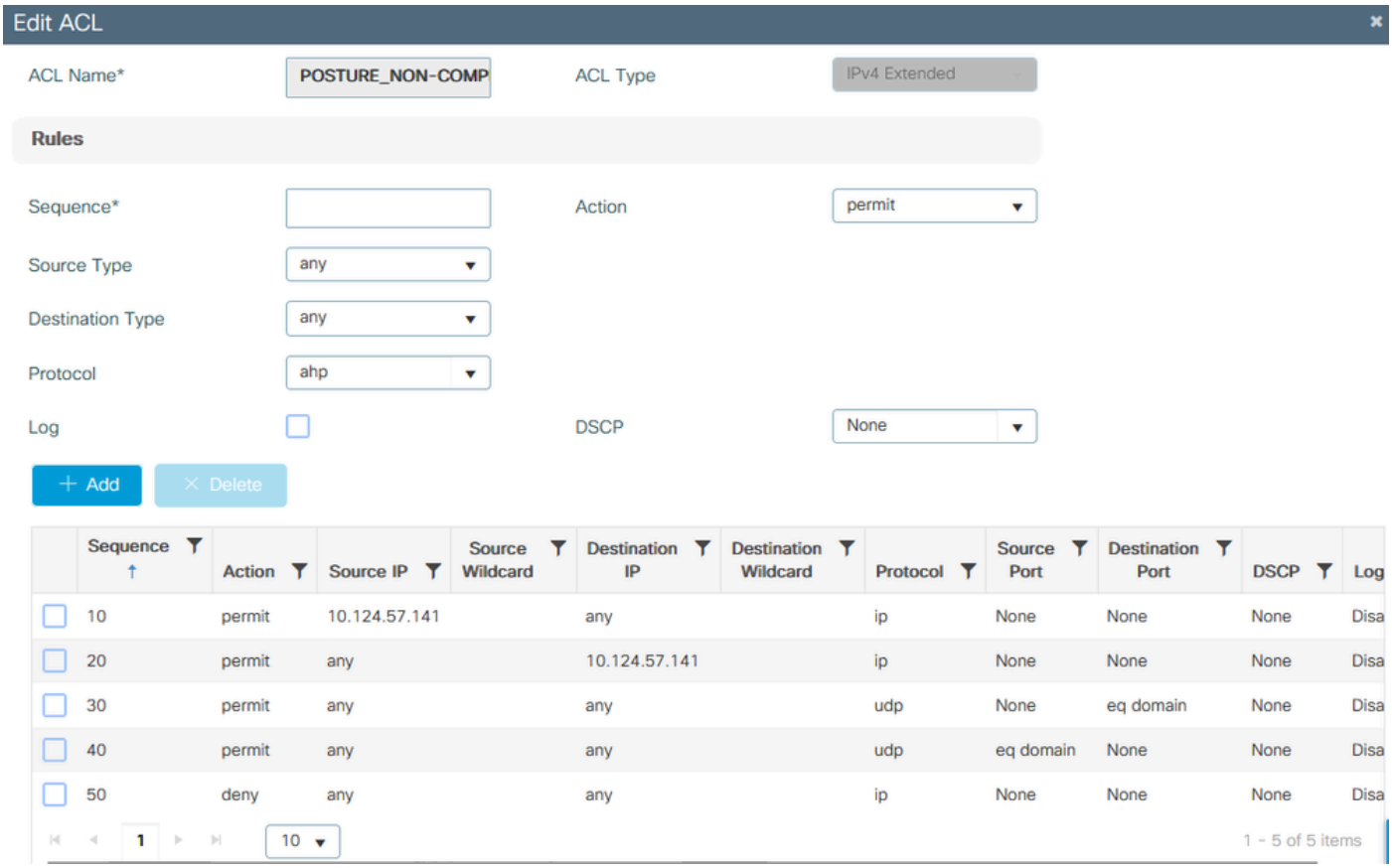
9800 ACL allgemein

Verwenden Sie in diesem Fall einfach permit all (Alle zulassen). Eine weitere gängige Konfiguration besteht darin, dass die ISE keine ACL im konformen Ergebnis autorisiert. Dies entspricht der Erlaubnis aller ACLs auf der 9800-Seite:



9800 ACL-konform

Bei einem nicht konformen Szenario erlaubt der Client nur Zugriff auf bestimmte Netzwerke, in der Regel den Behebungsserver (in diesem Fall die ISE selbst):

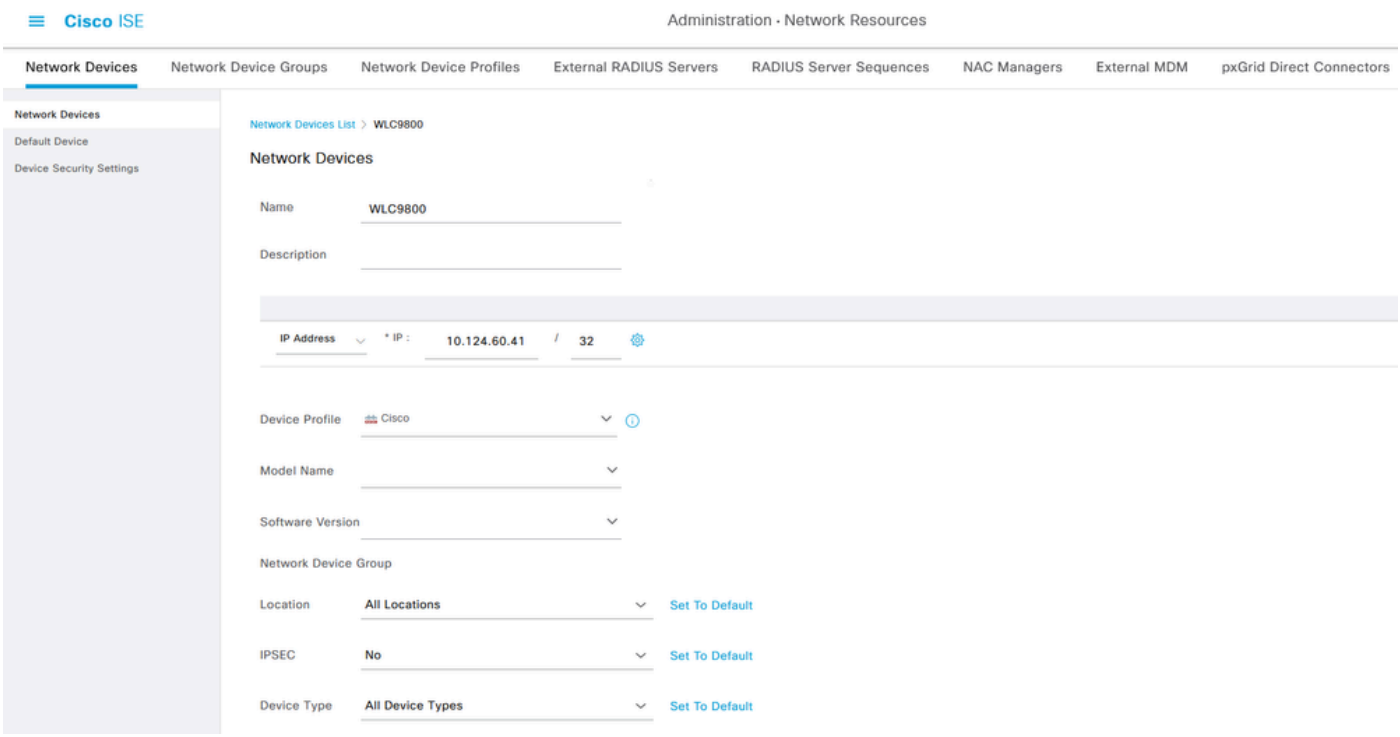


9800 ACL - nicht konform

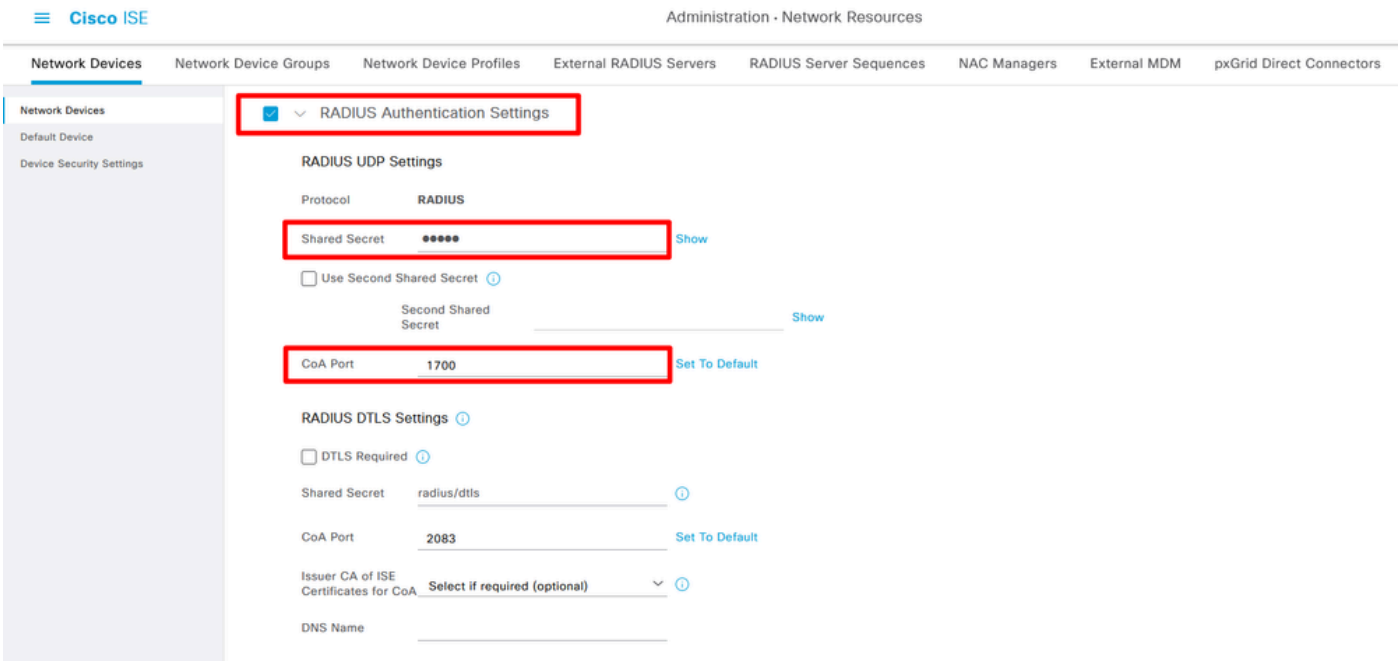
AAA-Konfiguration und Statuseinstellung auf der ISE

Statusanforderung: In diesem Beispiel besteht die Anforderung zum Ermitteln der Konformität darin, zu ermitteln, ob auf dem Desktop, auf dem Windows-PC getestet wird, eine bestimmte Testdatei vorhanden ist.

Schritt 1: Hinzufügen des WLC 9800 als NAD auf der ISE Navigieren Sie zu Administration > Network Resources > Network Devices > Add:



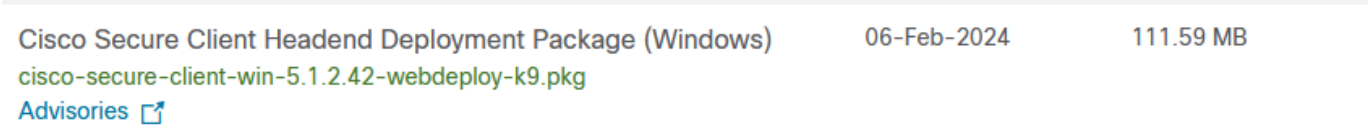
Netzwerkgerät hinzufügen 01



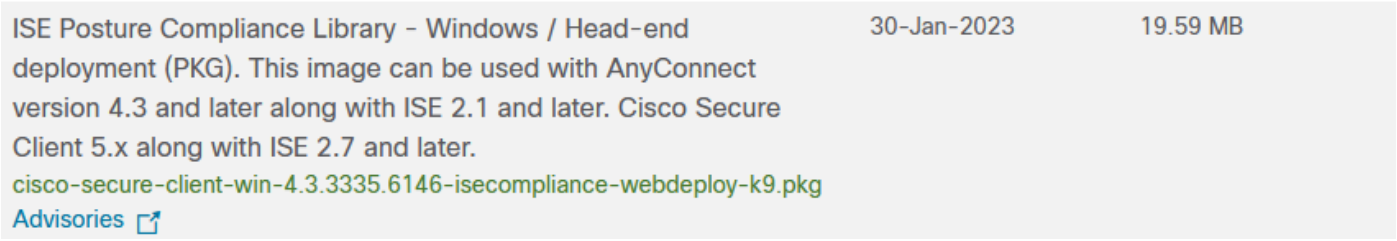
Netzwerkgerät hinzufügen 02

Schritt 2: Laden Sie das Cisco Secure Client Headend-Bereitstellungspaket und das Compliance-Modul auf die Cisco Software CCO-Website herunter.

Zugriff auf und Suche nach Cisco Secure Client:

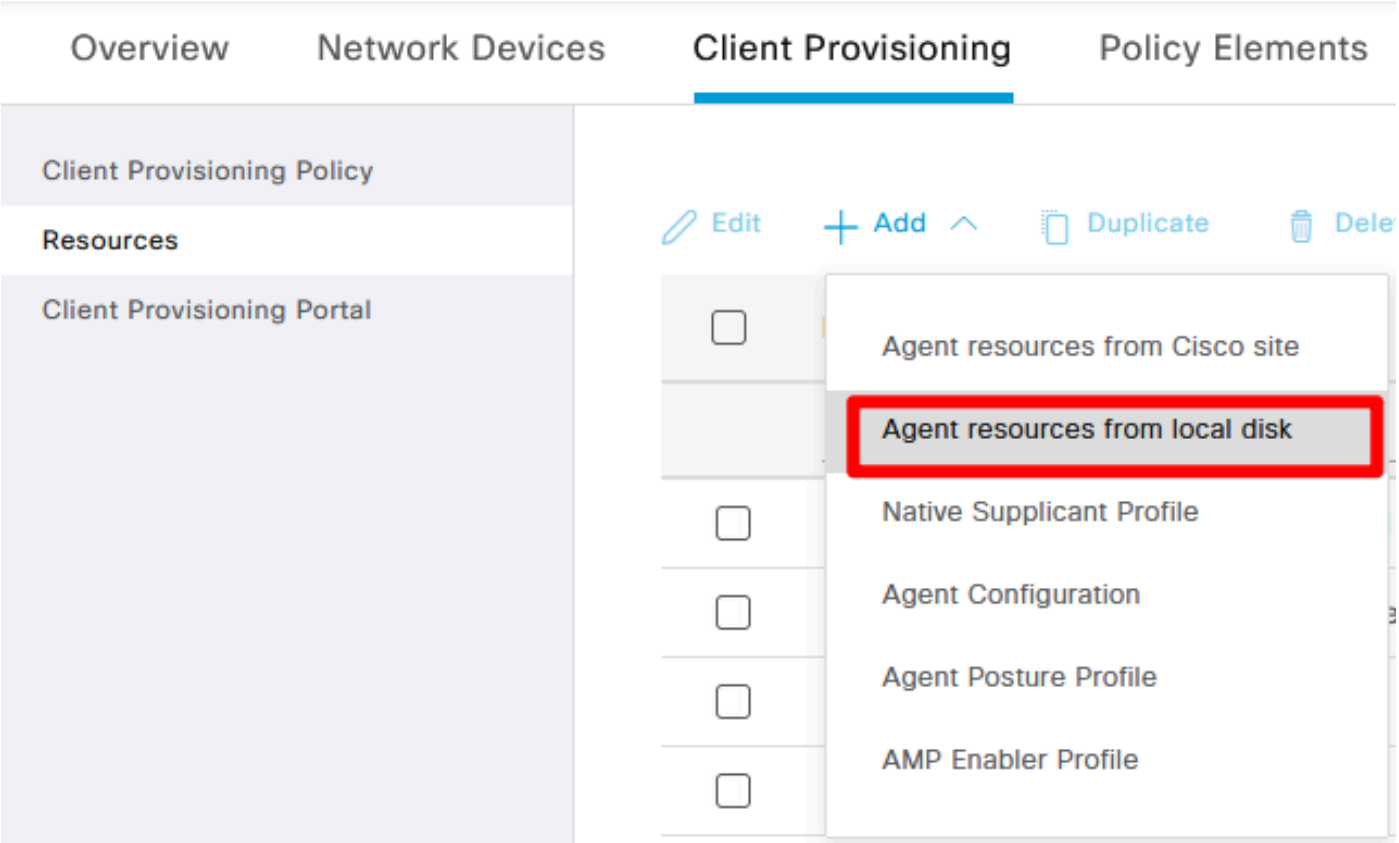


Sicherer Client 5.1.2.42

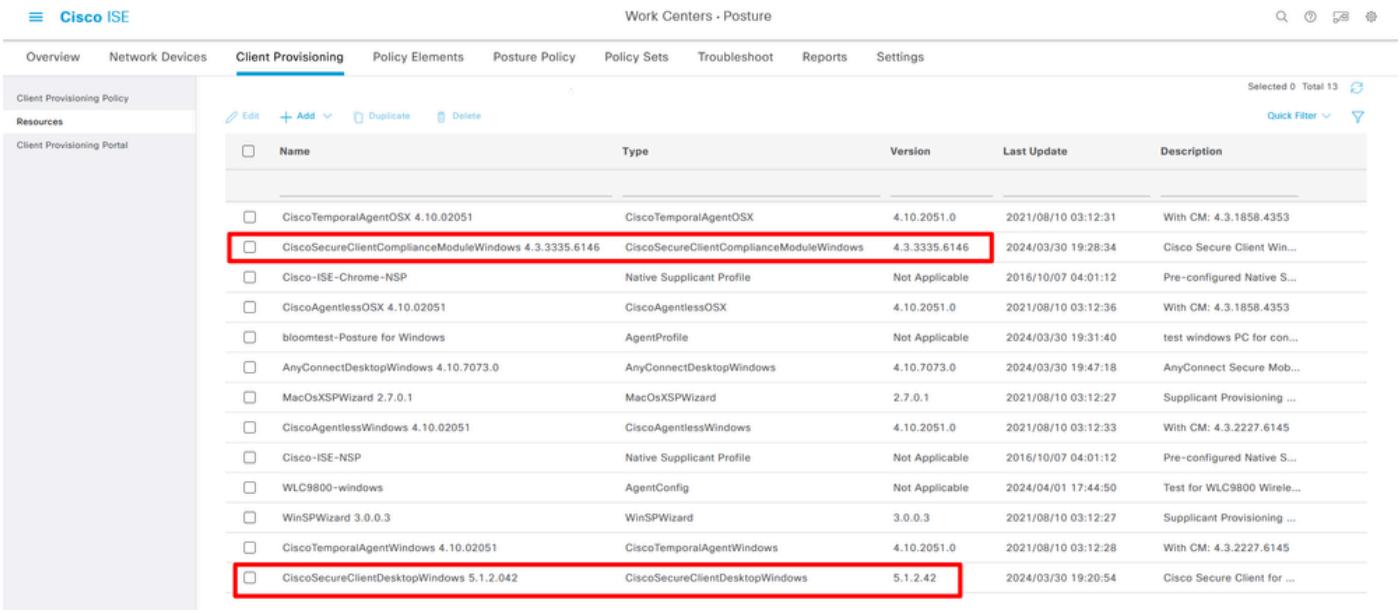


ISE Compliance-Modul 4.3

Schritt 3: Laden Sie das Cisco Secure Client Headend-Bereitstellungspaket und das Compliance-Modulpaket in ISE Client Provisioning hoch. Navigieren Sie zu Work Centers> Status> Client Provisioning> Resources . Klicken Sie auf Add, wählen Sie Agent-Ressourcen von der lokalen Festplatte aus dem Dropdown-Feld:

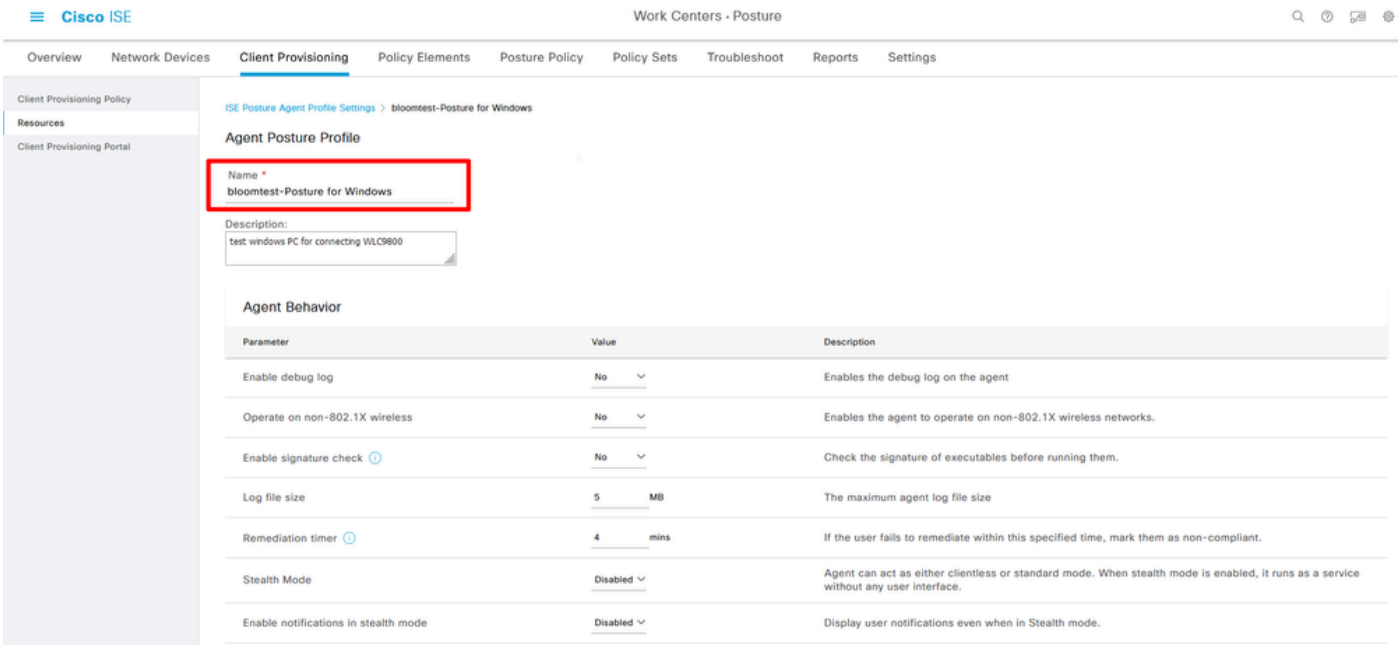


Sicheren Client hochladen



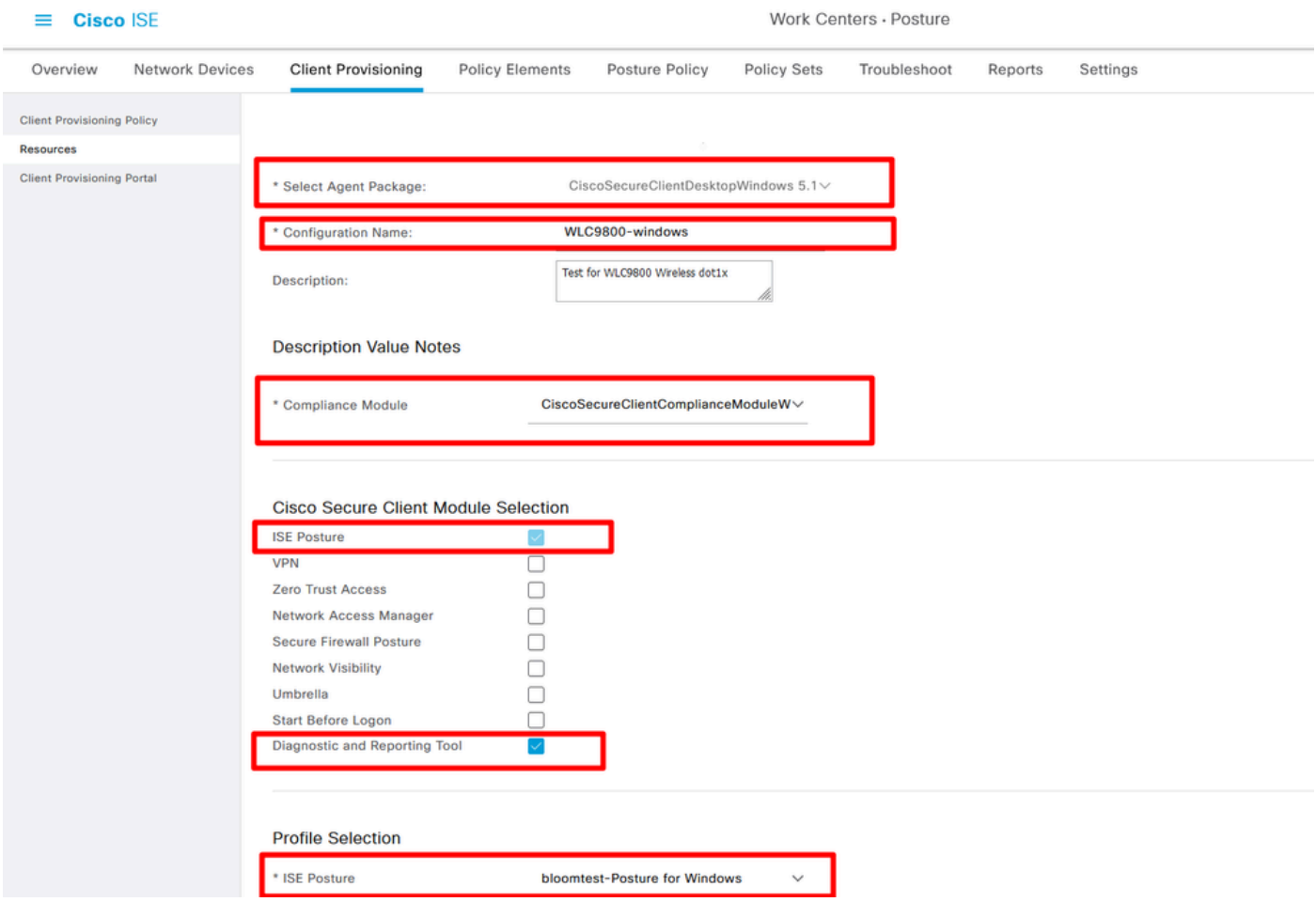
Hochladen des sicheren Clients und des Compliance-Moduls erfolgreich

Schritt 4: Erstellen eines Agentenstatusprofils Navigieren Sie zu Work Centers> Posture> Client Provisioning> Resources> Add> Agent Posture Profile:



Agentenstatusprofil

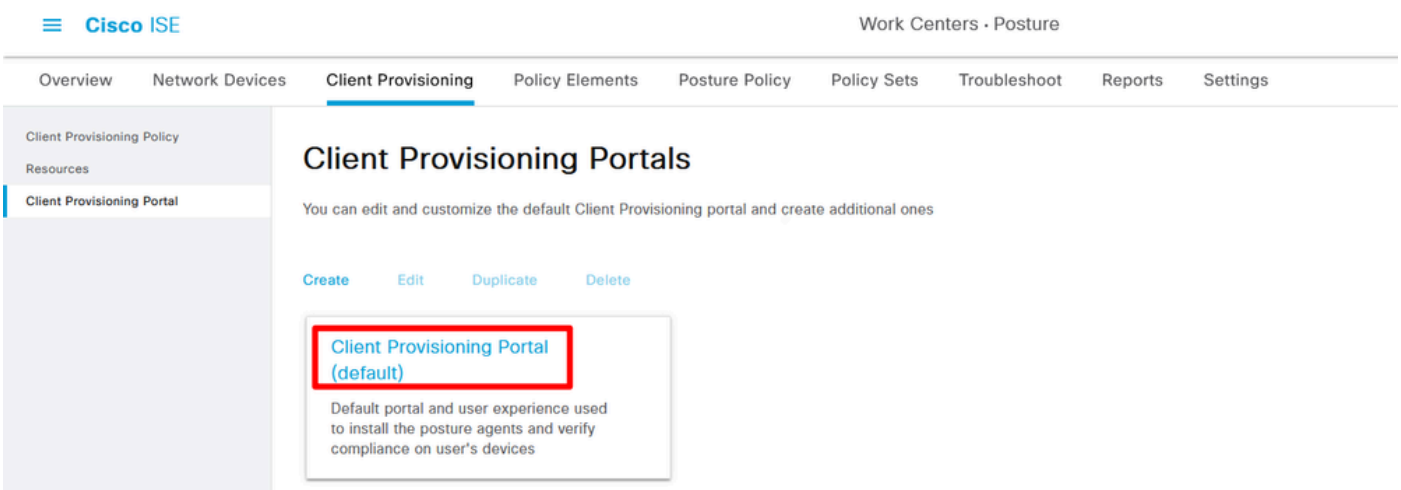
Schritt 5: Agentenkonfiguration erstellen Navigieren Sie zu Work Centers > Status > Client-Bereitstellung > Ressourcen > Hinzufügen > Agentenkonfiguration:



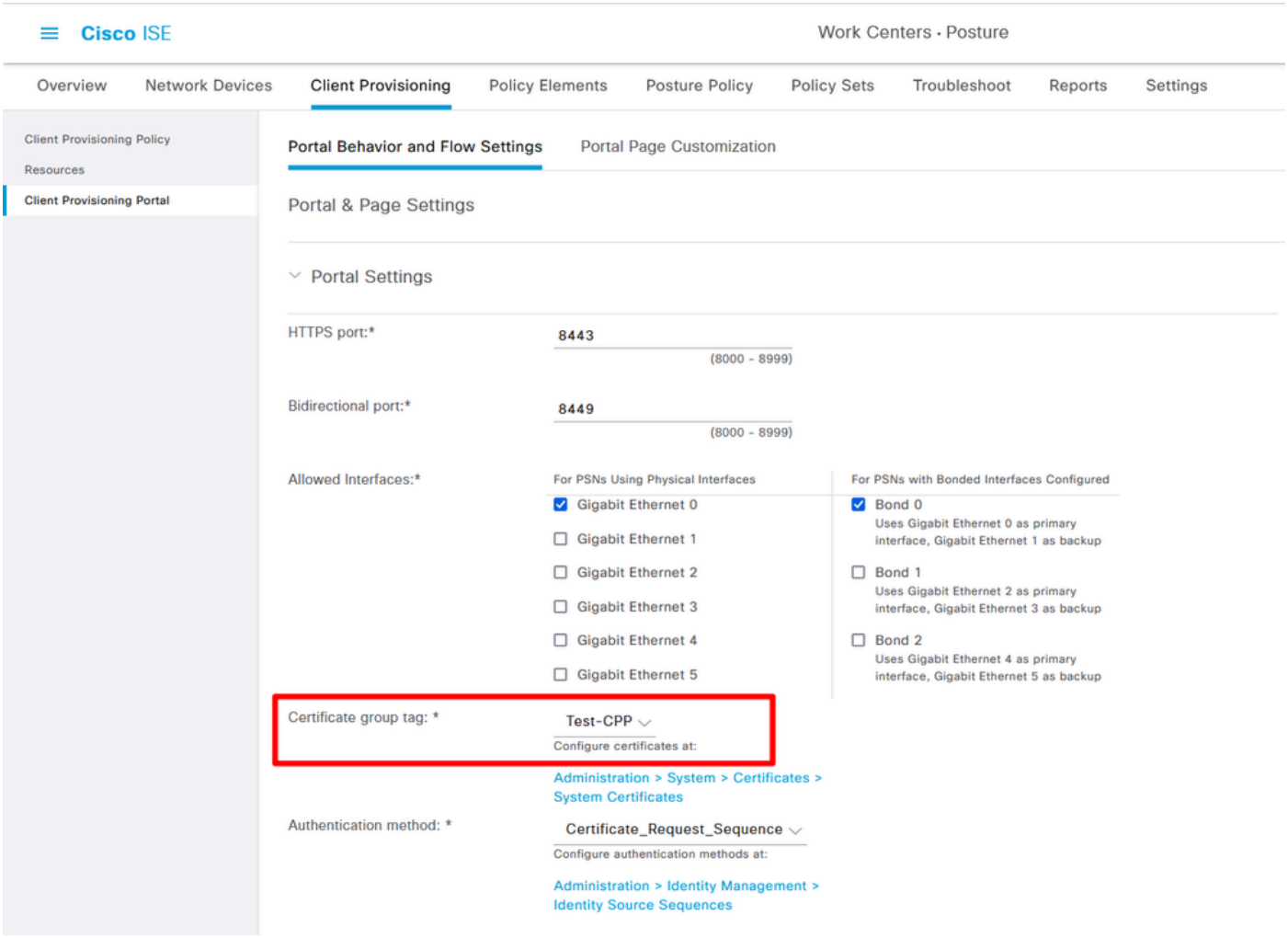
Agent-Konfiguration hinzufügen

Schritt 6. Bestätigen Sie das Client-Bereitstellungsportal, verwenden Sie das Standardportal für Tests ist OK. (Generieren Sie CSR und beantragen Sie ein SSL-Zertifikat vom CA-Server, und ersetzen Sie das Zertifikatgruppen-Tag in diesem Portal Einstellungen. Andernfalls tritt während des Testprozesses eine nicht vertrauenswürdige Warnung für das Zertifikat auf.)

Navigieren Sie zu Work Centers> Status> Client Provisioning> Client Provisioning Portals:

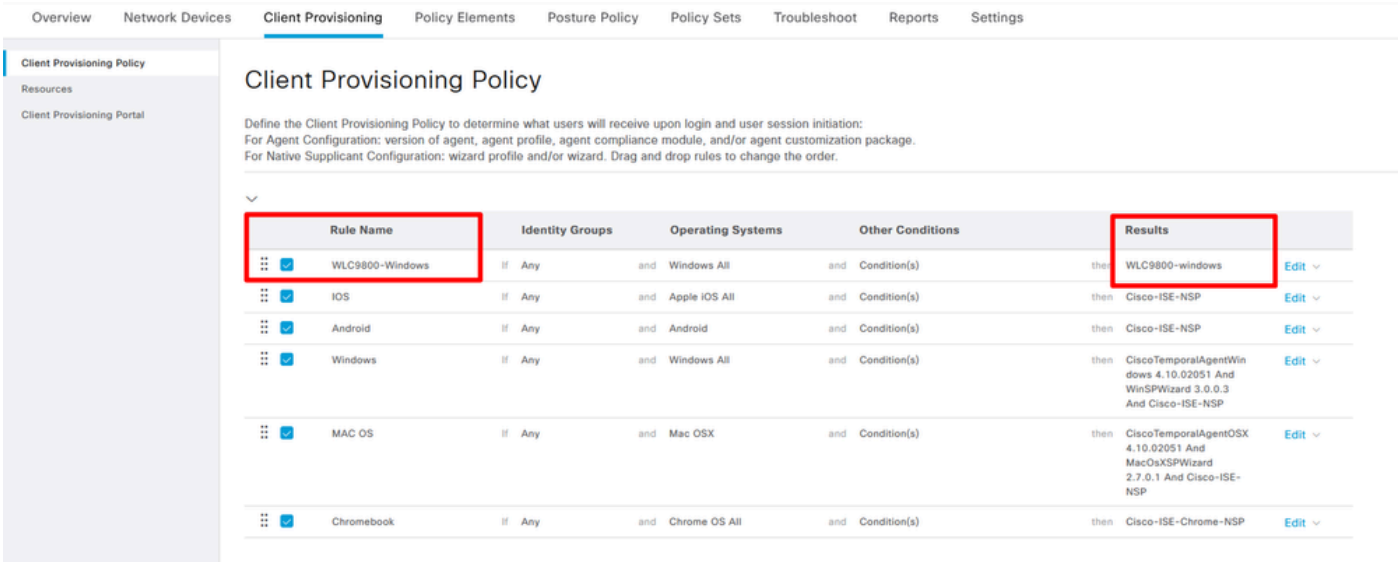


Client-Bereitstellungsportal 01 auswählen



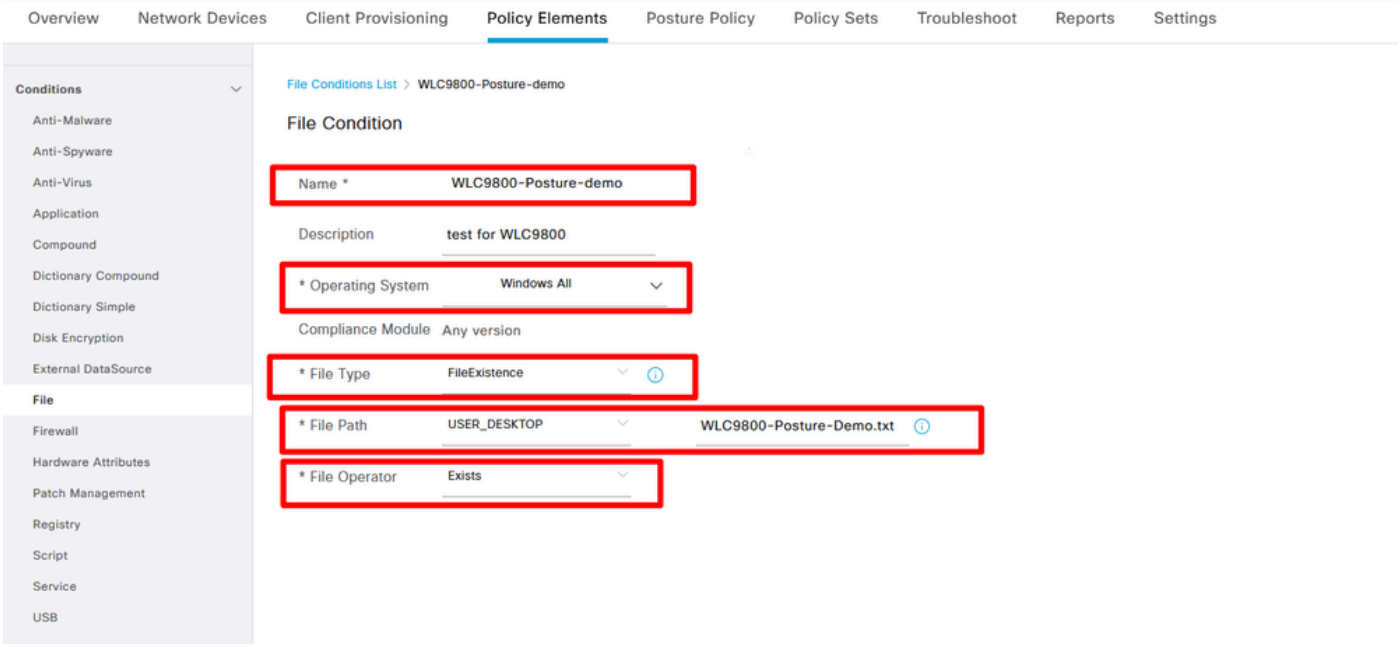
Client-Bereitstellungsportal 02 auswählen

Schritt 7: Erstellen einer Client-Bereitstellungsrichtlinie Navigieren Sie zu Work Centers > Status > Client Provisioning > Client Provisioning Policy > Edit > Insert new policy above.



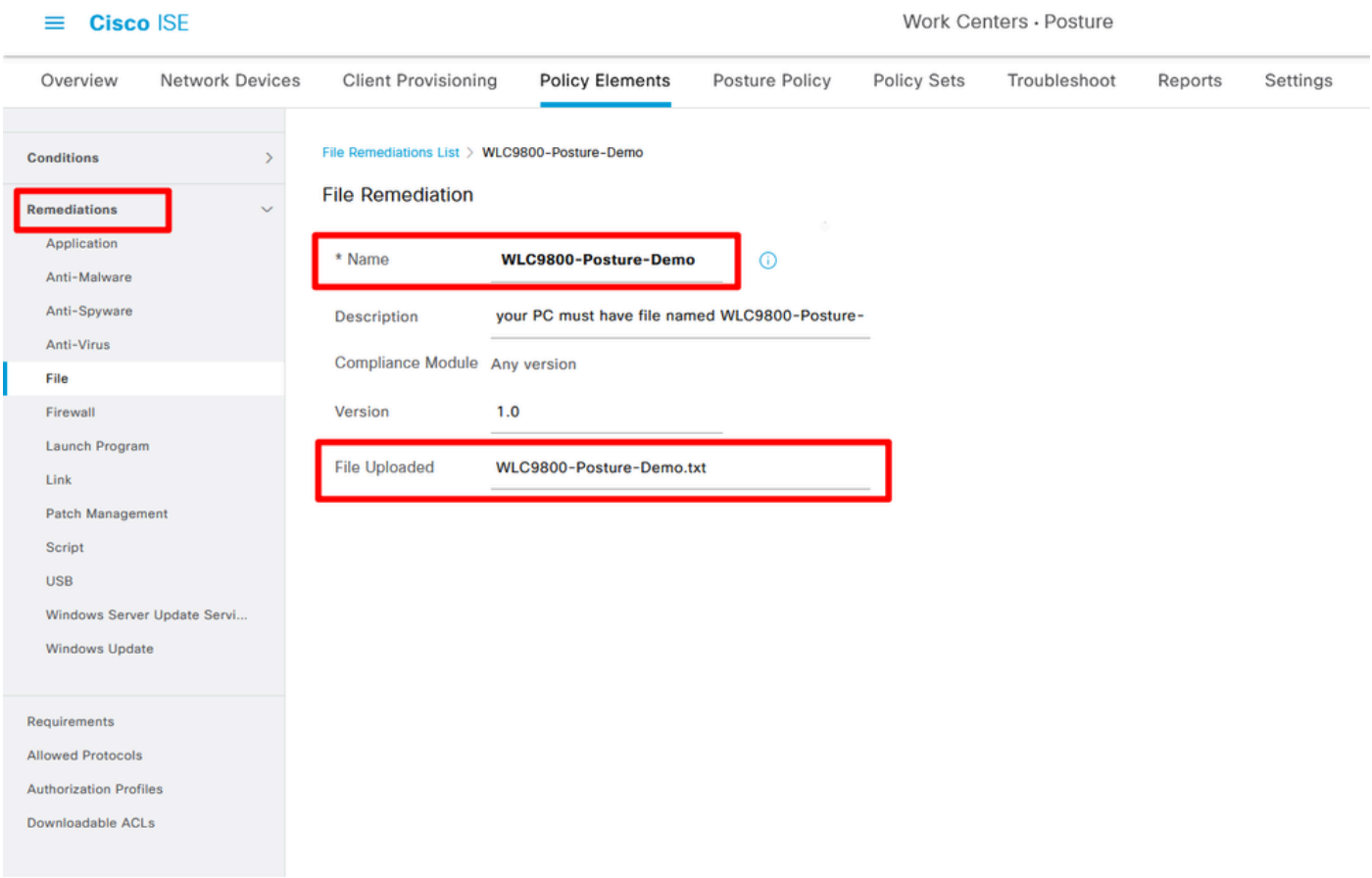
Client-Bereitstellungsrichtlinie erstellen

Schritt 8: Erstellen von Dateibedingungen Navigieren Sie zu Work Centers> Status> Policy Elements> Conditions> File> File Conditions> Add:



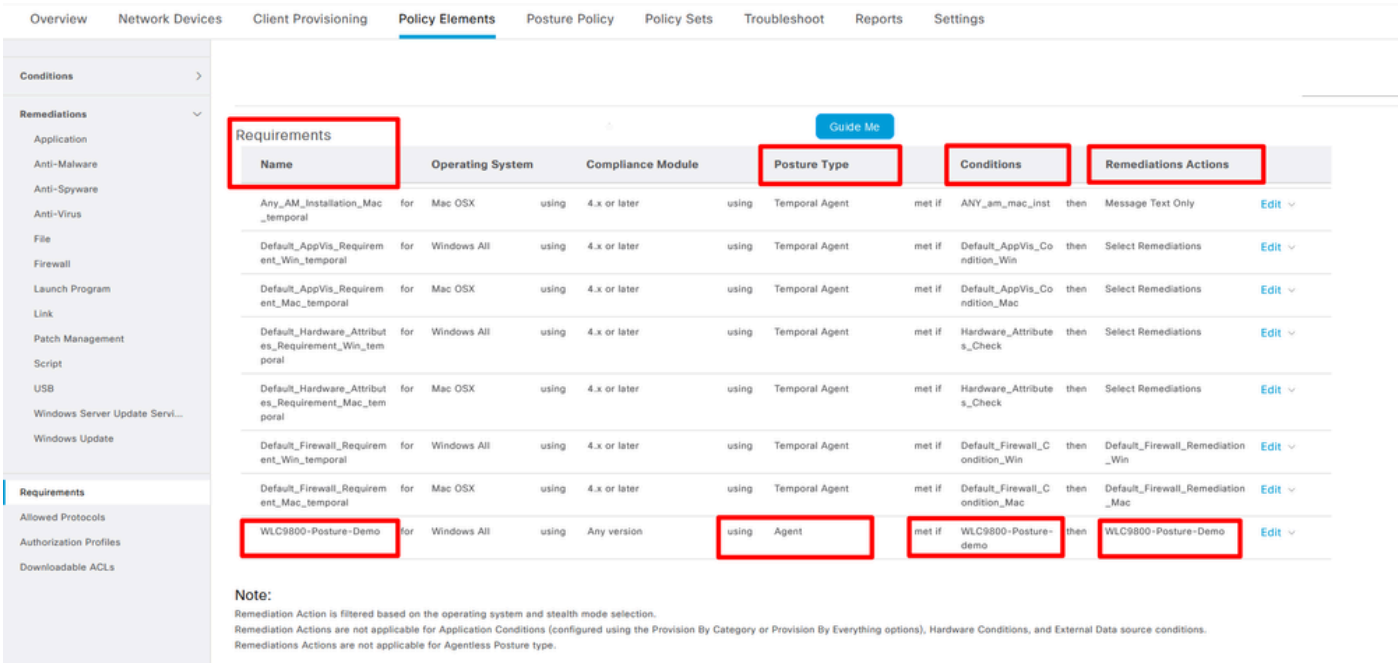
Dateibedingung erstellen

Schritt 9: Korrekturen erstellen Navigieren Sie zu Work Centers > Status > Policy Elements > Remediations > File > Add:



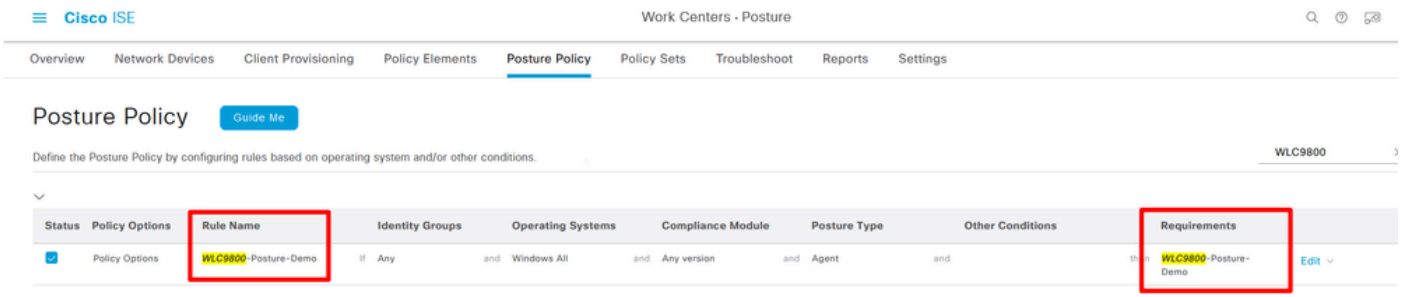
Dateibereinigung erstellen

Schritt 10: Anforderung erstellen. Navigieren Sie zu Work Centers> Status> Policy Elements> Requirements> Insert new Requirement:



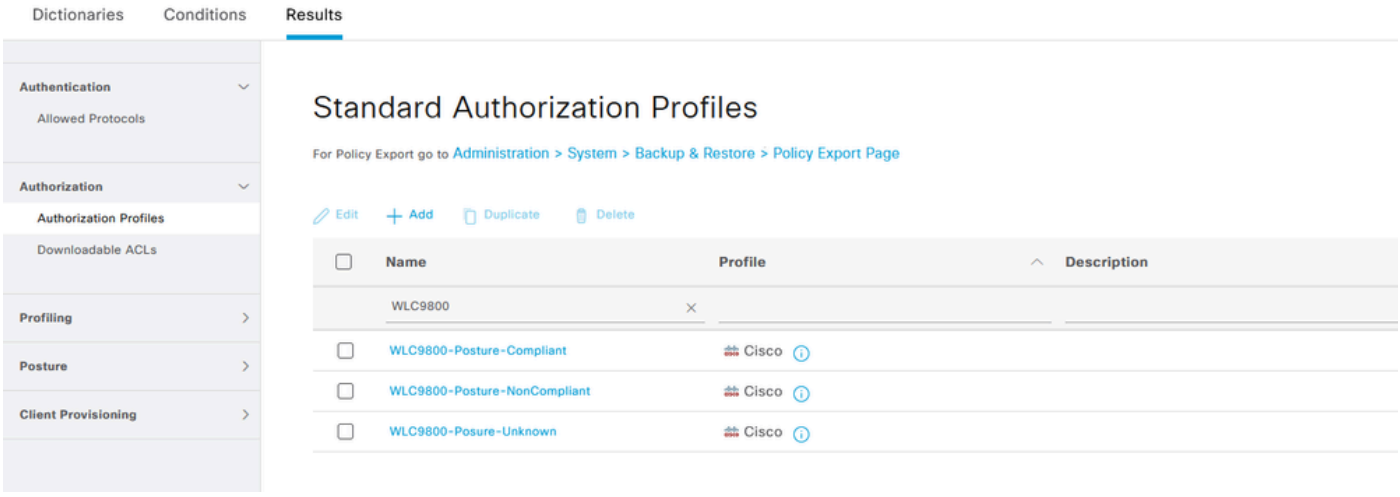
Statusanforderung erstellen

Schritt 11: Erstellen einer Statusrichtlinie Navigieren Sie zu Work Centers > Posture > Insert new policy:

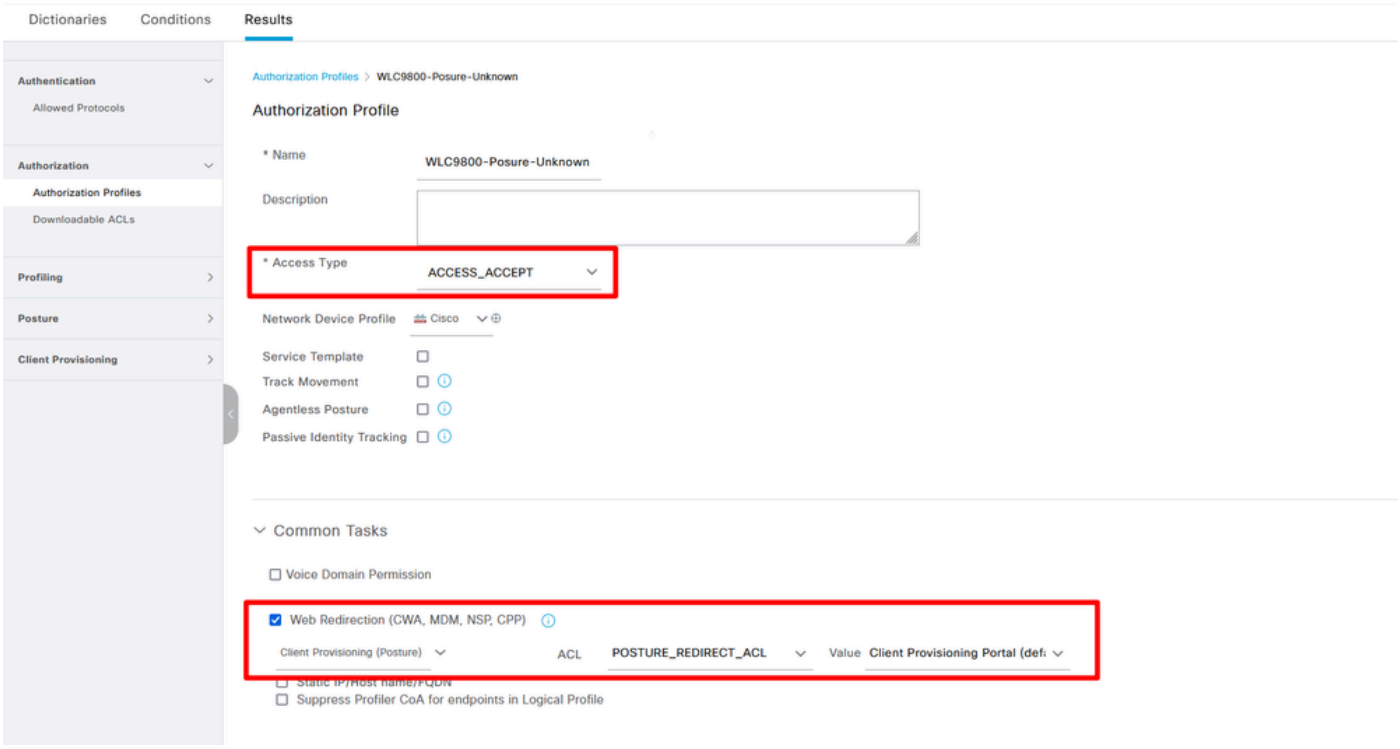


Statusrichtlinie erstellen

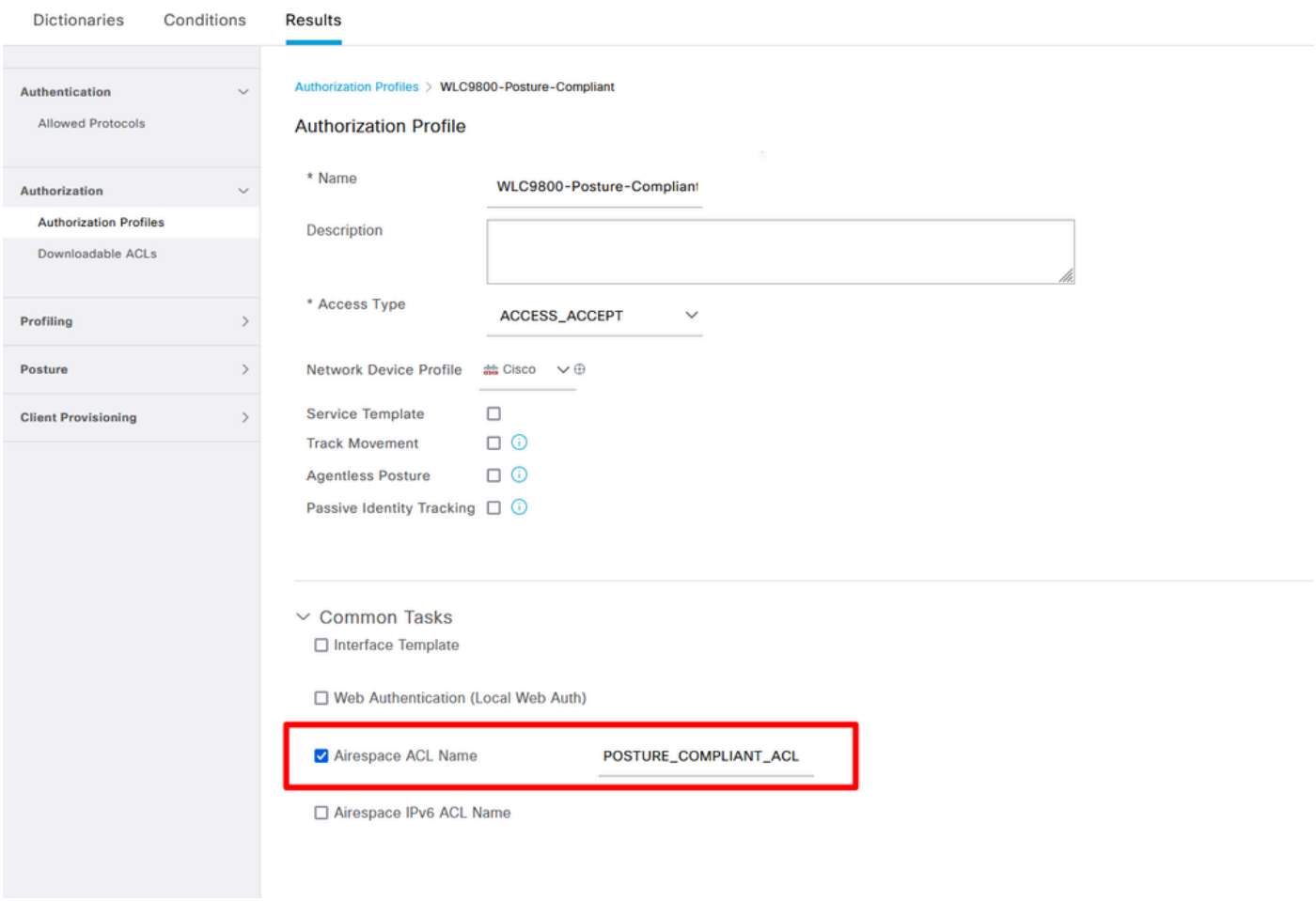
Schritt 12: Erstellen Sie drei Autorisierungsprofile: Der Status lautet "Unbekannt". Der Status "Status" ist "Nicht konform". Der Statusstatus ist "Konformität". Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile> Hinzufügen:



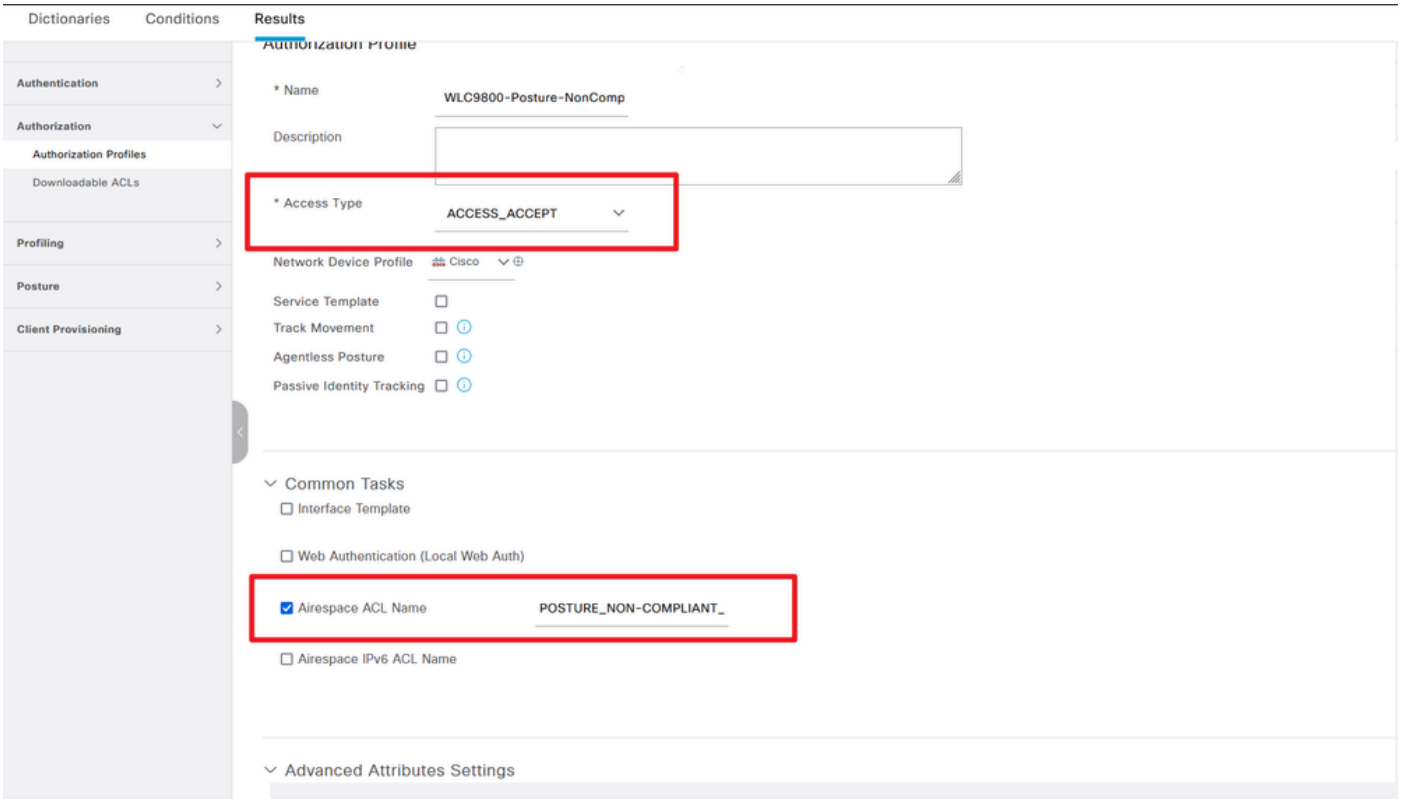
Autorisierungsprofile erstellen 01



Erstellen von Autorisierungsprofilen 02



Erstellen von Autorisierungsprofilen 03

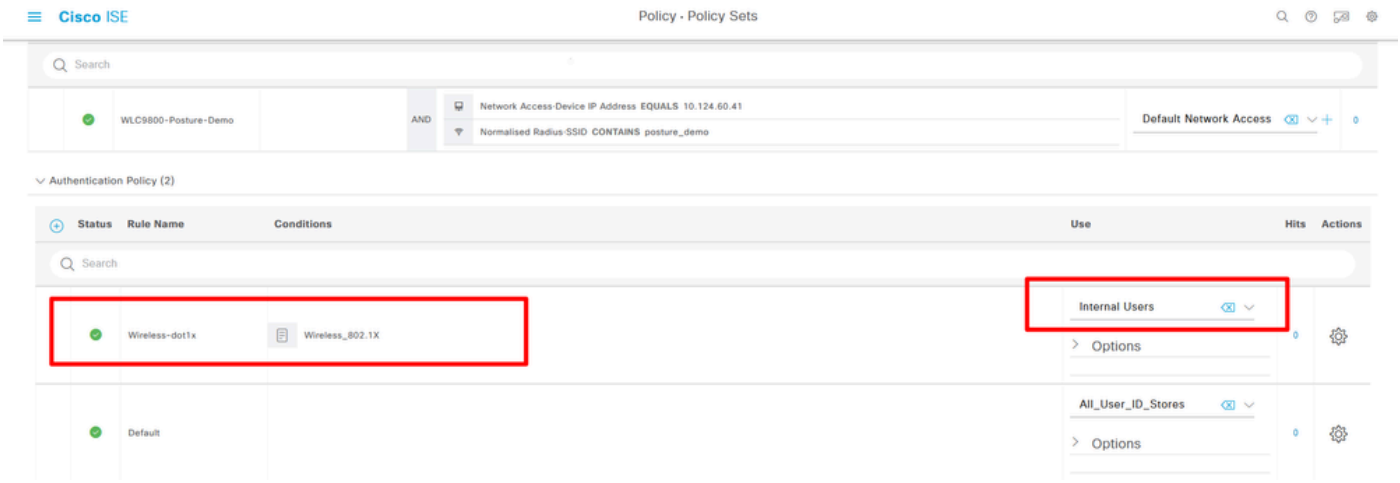


Schritt 13: Erstellen von PolicySets Navigieren Sie zu Richtlinie > Richtlinie.

Policy Sets erstellen

Sets> Symbol hinzufügen:

Schritt 14: Erstellen einer Authentifizierungsrichtlinie Navigieren Sie zu Richtlinie> Richtliniensätze> Erweitern Sie "WLC9800-Posture-Demo"> Authentifizierungsrichtlinie> Hinzufügen:



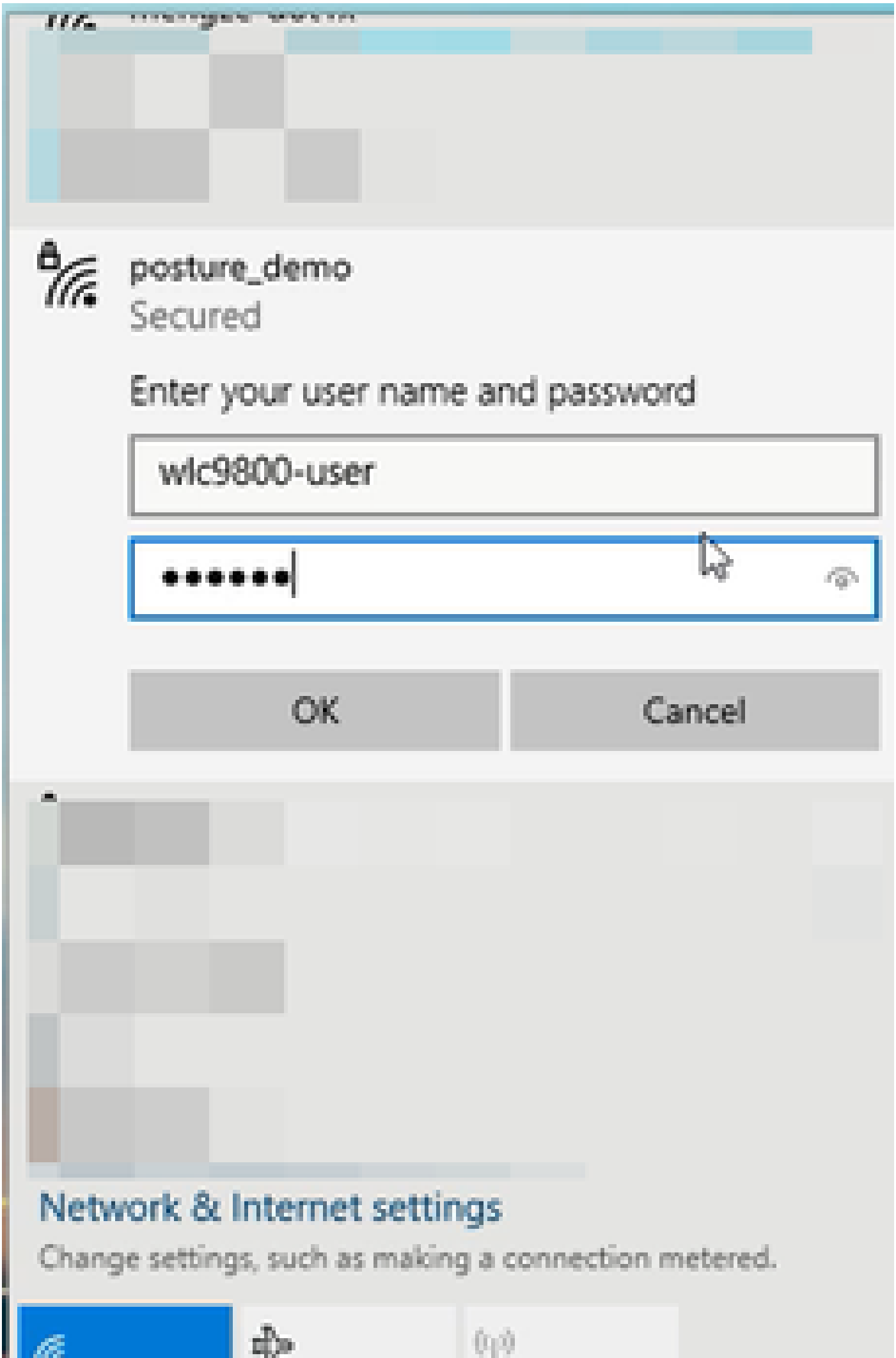
Authentifizierungsrichtlinie erstellen

Schritt 15: Autorisierungsrichtlinie erstellen Navigieren Sie zu Richtlinie> Richtliniensätze> Erweitern Sie "WLC9800-Posture-Demo"> Autorisierungsrichtlinie> Hinzufügen:

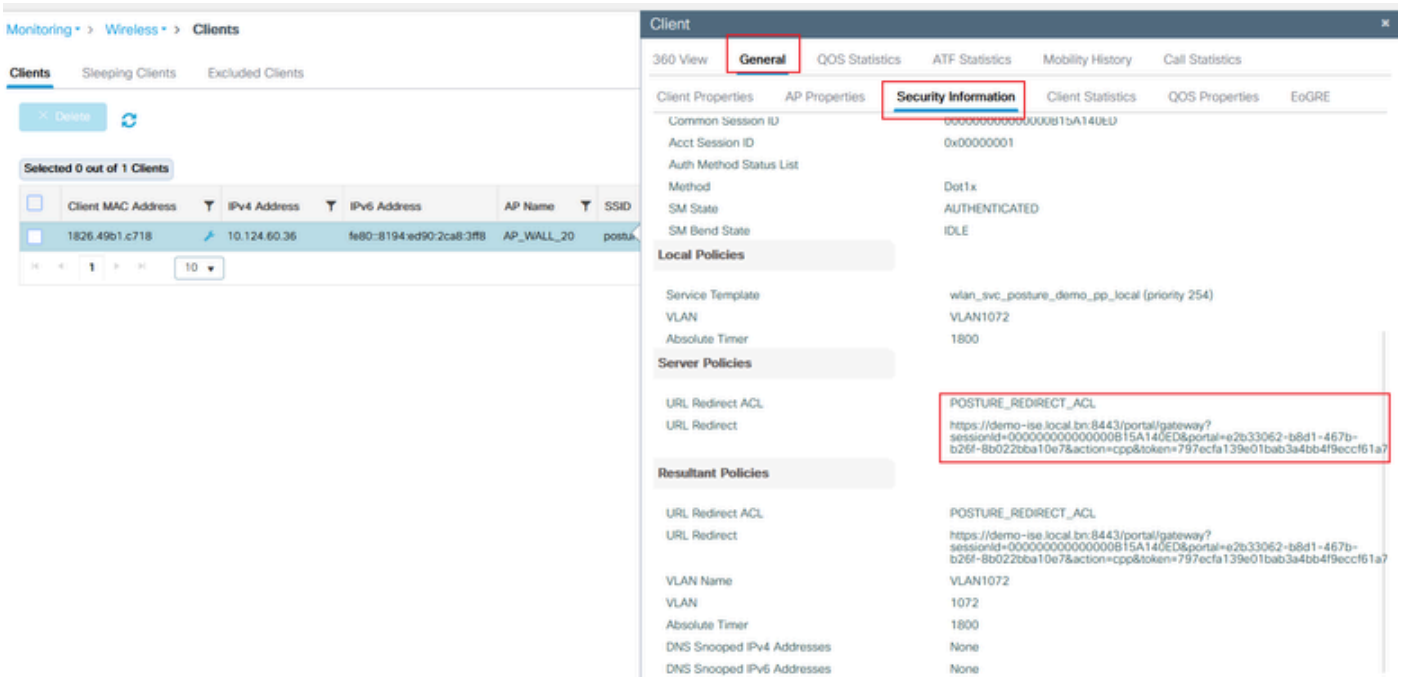
Autorisierungsrichtlinie erstellen

Beispiele

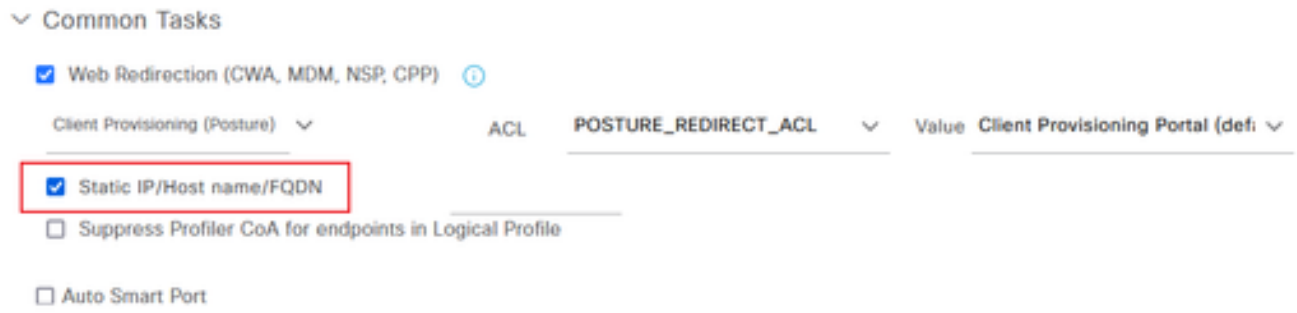
1. Verbundener Test-SSID stature_demo mit korrekten 802.1X-Anmeldedaten.


posture_demo
Secured
Enter your user name and password
wlc9800-user
OK
Cancel
Network & Internet settings
Change settings, such as making a connection metered.

- Stellen Sie sicher, dass der WLC die richtige Umleitungs-URL und ACL von der ISE erhält. Sie können es über die GUI überprüfen:



- Wenn die Umleitung nicht automatisch erfolgt, öffnen Sie einen Browser, und versuchen Sie eine zufällige IP-Adresse. Beispiel: 10.0.0.1. Wenn die Umleitung funktioniert, liegt möglicherweise ein DNS-Auflösungsproblem vor. Stellen Sie sicher, dass Sie über DHCP einen gültigen DNS-Server bereitgestellt haben und dass dieser Hostnamen auflösen kann.
- Wenn der Browser zur ISE-Portal-URL umgeleitet wurde, die Seite jedoch nicht geladen werden kann, überprüfen Sie, ob der ISE-Domänenname nicht zum DNS-Server hinzugefügt wurde. Der Client kann die Portal-URL daher nicht auflösen. Um dieses Problem schnell zu beheben, markieren Sie die Option Static IP/Host name/FQDN (Statischer IP-/Hostname/FQDN) unter dem Autorisierungsprofil, um die IP-Adresse in der Umleitungs-URL anzugeben. Dies kann jedoch ein Sicherheitsrisiko darstellen, da die IP-Adresse der ISE offen gelegt wird.



Debuggen sammeln

[Aktivieren von Debuggen auf C9800]

Debuggen auf ISE aktivieren

Referenzen

- Konfigurieren von CWA auf Catalyst 9800 WLC und ISE - Cisco
- Wireless BYOD mit Identity Services Engine
- ISE-Status bereitstellen
- Fehlerbehebung bei ISE-Sitzungsmanagement und Status
- ISE-Statusumleitungsfluss mit ISE-Statusumleitungslosem Fluss vergleichen

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.