

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

Inhalt

[Einleitung](#)

[Hintergrund](#)

[Voraussetzungen](#)

[Verwendete Komponente](#)

[Was bedeutet Single-SSID und Dual-SSID-BYOD auf der ISE?](#)

[BYOD mit einer SSID](#)

[Dual-SSID-BYOD](#)

[WLC-Konfiguration](#)

[WLAN für CWA erstellen](#)

[Konfigurieren von RADIUS-Servern](#)

[AAA-Server konfigurieren](#)

[Konfigurieren von Sicherheitsrichtlinien für das WLAN](#)

[ACL vor der Authentifizierung konfigurieren](#)

[Richtlinienprofil konfigurieren](#)

[Tags anwenden und bereitstellen](#)

[Konfigurieren einer offenen/ungesicherten SSID](#)

[ISE-Konfiguration](#)

[Voraussetzungen](#)

[Zertifikate](#)

[DNS-Konfiguration](#)

[Konfigurieren des ISE-Netzwerkgeräts](#)

[Erstellung eines BYOD-Portals](#)

[Cisco IOS® aktuelle Version herunterladen](#)

[Endgeräteprofil erstellen](#)

[Zertifikatvorlage](#)

[Zuordnen eines Endgeräteprofils zum Client-Bereitstellungsportal](#)

[Konfigurieren von ISE-Richtliniensätzen für BYOD mit einer SSID](#)

[Konfigurieren von ISE-Richtliniensätzen für Dual-SSID-BYOD](#)

[Fehlerbehebung](#)

[Protokollausschnitt](#)

[Gastprotokolle](#)

[ISE-PSC-Protokolle](#)

[Endgeräteprofil-Download](#)

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

Add WLAN

GeneralSecurityAdvanced

Profile Name*

Enter Name

SSID*

BYOD-SSID

WLAN ID*

9

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

ENABLED

WPA3 Enabled

Dot11ax Enabled

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

Cancel

Apply to Device

Konfigurieren von RADIUS-Servern

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

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

[+ Add](#) [- Delete](#)

RADIUS

TACACS+

LDAP

Servers Server Groups

Acct Port "Contains" 1814 x				
Name	Address	Auth Port	Acct Port	
0 10				

No items to display

For Radius fallback to work, please make sure the [Dead Criteria](#) and [Dead Time](#) configuration exists on the device

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.

Create AAA Radius Server

Name* BYOD

Server Address* 10.x.x.x

PAC Key ☐

Key Type Clear Text

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ⓘ

ENABLED ☒

CoA Server Key Type

Clear Text

CoA Server Key ⓘ

.....

Confirm CoA Server Key

.....

Automate Tester

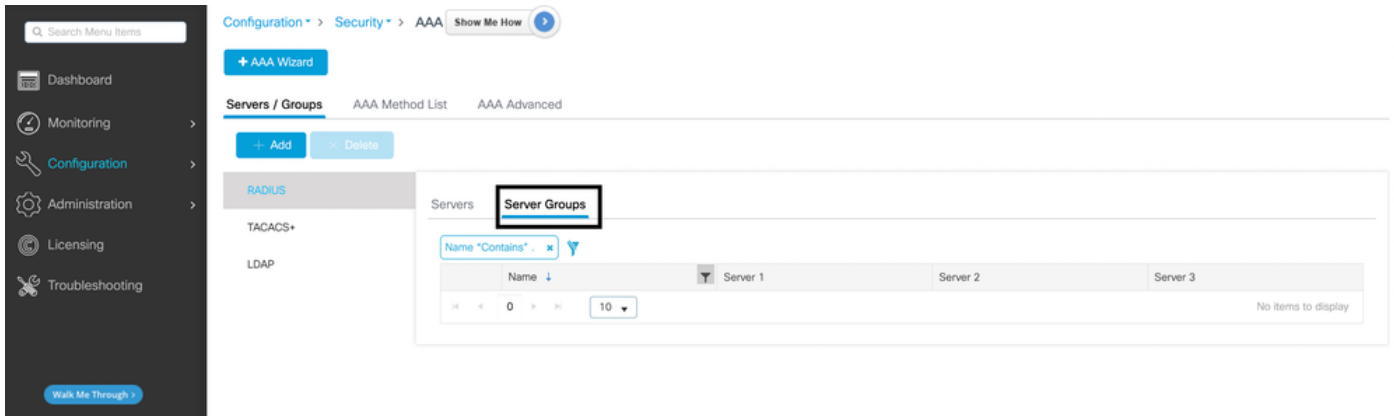
☐

[Cancel](#)

[Apply to Device](#)

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.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance ☐ DISABLED

Source Interface VLAN ID

Available Servers

Assigned Servers

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

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☒ WPA + WPA2☐ WPA2 + WPA3☐ WPA3☐ Static WEP☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☒GTK
Randomize☐

OSEN Policy

☐

WPA2 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Disabled ▼

Fast Transition

Status

Adaptive Ena... ▼

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

802.1X

☒

PSK

☐

Easy-PSK

☐

CCKM ⚠

☐

FT + 802.1X

☐

FT + PSK

☐802.1X-
SHA256☐

PSK-SHA256

☐

MPSK Configuration

Cancel



Update & Apply to Device

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

Edit WLAN ✕

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

Web Policy

☐

Show Advanced Settings >>>

Web Auth Parameter Map

global

▼

🔗

Authentication List

Select a value

▼

🔗

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

↶ Cancel

📄 Update & Apply to Device

ACL vor der Authentifizierung konfigurieren

Erstellen Sie eine ACL, damit die Aktionen 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.

Edit Policy Profile

⌵

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling☒

HTTP TLV Caching☒

DHCP TLV Caching☒

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ⌵ ⓘ

VLAN

VLAN/VLAN Group

VLAN0097 ⌵ ⓘ

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ⌵ ⓘ

IPv6 ACL

Search or Select ⌵ ⓘ

URL Filters

ⓘ

Pre Auth

Search or Select ⌵ ⓘ

Post Auth

Search or Select ⌵ ⓘ

↶ Cancel

📁 Update & Apply to Device

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

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)
28800 ⓘ

Idle Timeout (sec)
300

Idle Threshold (bytes)
0

Client Exclusion Timeout (sec)
☒ 60

Guest LAN Session Timeout
☐

DHCP

IPv4 DHCP Required
☐

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override
☒

NAC State
☒

Policy Name
default-aaa-policy ✕ ▼ ⓘ

Accounting List
Test ✕ ▼ ⓘ

Fabric Profile
☐ Search or Select ▼ ⓘ

Link-Local Bridging
☐

mDNS Service Policy
default-mdns-ser... ▼ ⓘ Clear

Hotspot Server
Search or Select ▼ ⓘ

User Defined (Private) Network

Status
☐

Drop Unicast
☐

DNS Layer Security

DNS Layer Security Parameter Map
Not Configured ▼ Clear

Flex DHCP Option for DNS
ENABLED ☒

Flex DNS Traffic Redirect
☐ IGNORE

WLAN Flex Policy

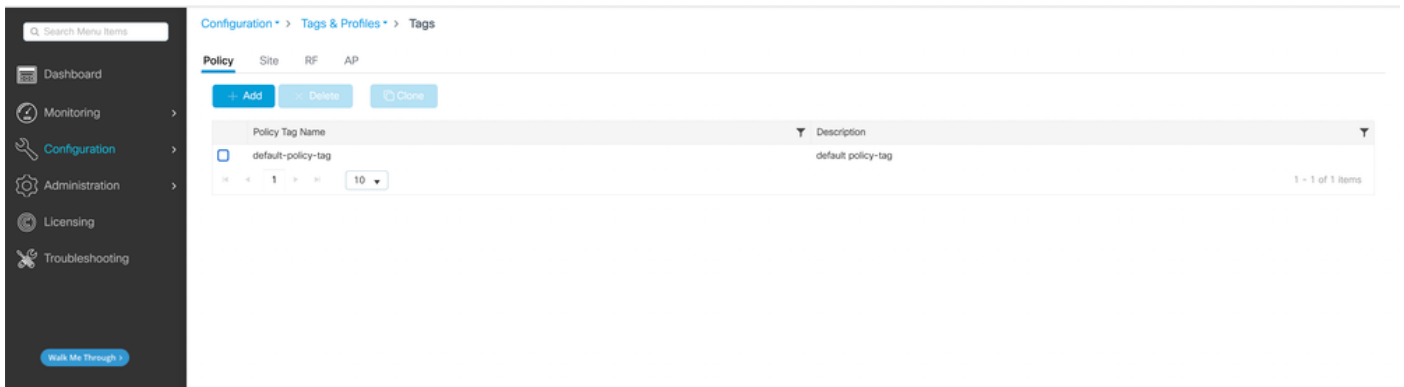
VLAN Central Switching
☐

Split MAC ACL
Search or Select ▼ ⓘ

Cancel
Update & Apply to Device

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.

Add WLAN

General
Security
Advanced

Profile Name*
BYOD-Open

SSID*
BYOD-Open

WLAN ID*
10

Status
ENABLED

Broadcast SSID
ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status
ENABLED ⓘ

WPA3 Enabled
Dot11ax Enabled

5 GHz

Status
ENABLED

2.4 GHz

Status
ENABLED

802.11b/g Policy
802.11b/g

Cancel
Apply to Device

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

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. The 'Layer2' section is highlighted with a black box. Inside this section, the 'None' radio button is selected, and the 'MAC Filtering' checkbox is checked. Other options like 'WPA + WPA2', 'WPA2 + WPA3', 'WPA3', and 'Static WEP' are unselected. Below the 'Layer2' section, the 'Authorization List*' dropdown is set to 'default', and the 'Transition Mode WLAN ID*' is '0-4096'. The 'OWE Transition Mode' checkbox is checked, and 'Lobby Admin Access' is unchecked. A 'Fast Transition' section is also visible, with 'Status' set to 'Disabled', 'Over the DS' unchecked, and 'Reassociation Timeout *' set to '20'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

☐ WPA + WPA2 ☐ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☒ None

MAC Filtering ☒ Authorization List* default ⓘ

OWE Transition Mode ☒ Transition Mode WLAN ID* 0-4096

Lobby Admin Access ☐

Fast Transition

Status Disabled ▼

Over the DS ☐

Reassociation Timeout * 20

Cancel Apply to Device

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:

Add WLAN



General

Security

Advanced

Layer2

Layer3

AAA

Web Policy

☐

[Show Advanced Settings >>>](#)

Web Auth Parameter Map

global



Authentication List

Select a value



For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Cancel

Apply to Device

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

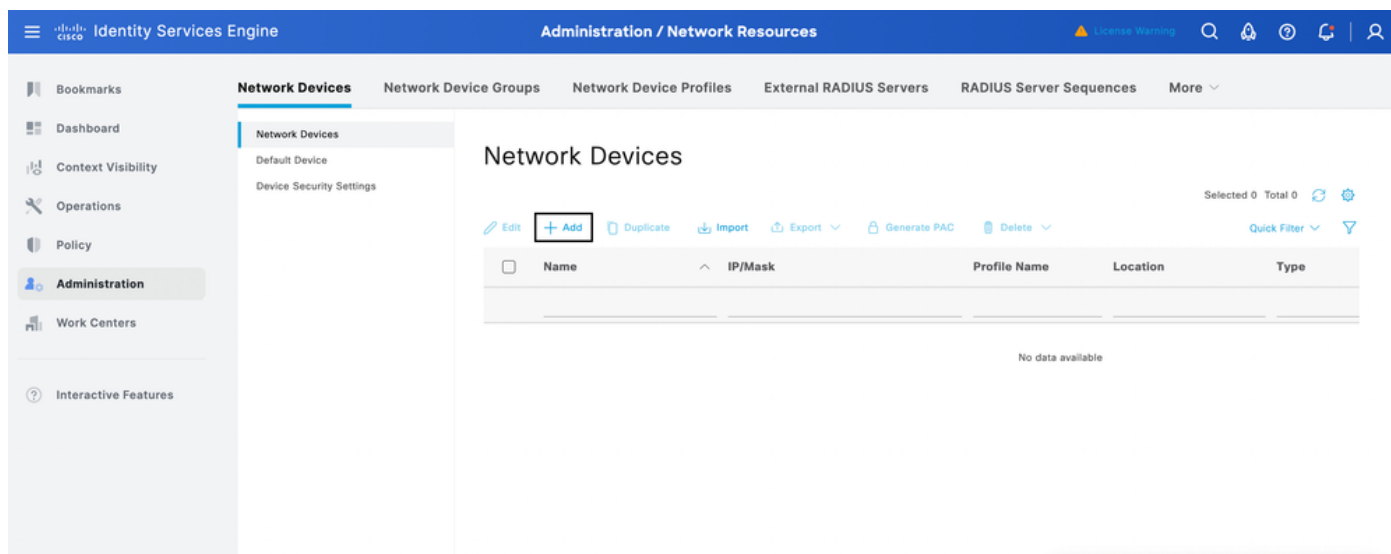
- Installieren Sie ein gültiges Serverzertifikat auf der ISE, um Sicherheitswarnungen im Browser zu vermeiden.
- Stellen Sie sicher, dass das Zertifikat von den Endpunkten als vertrauenswürdig eingestuft wird (signiert von einer bekannten Zertifizierungsstelle oder einer internen Zertifizierungsstelle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

DNS-Konfiguration

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

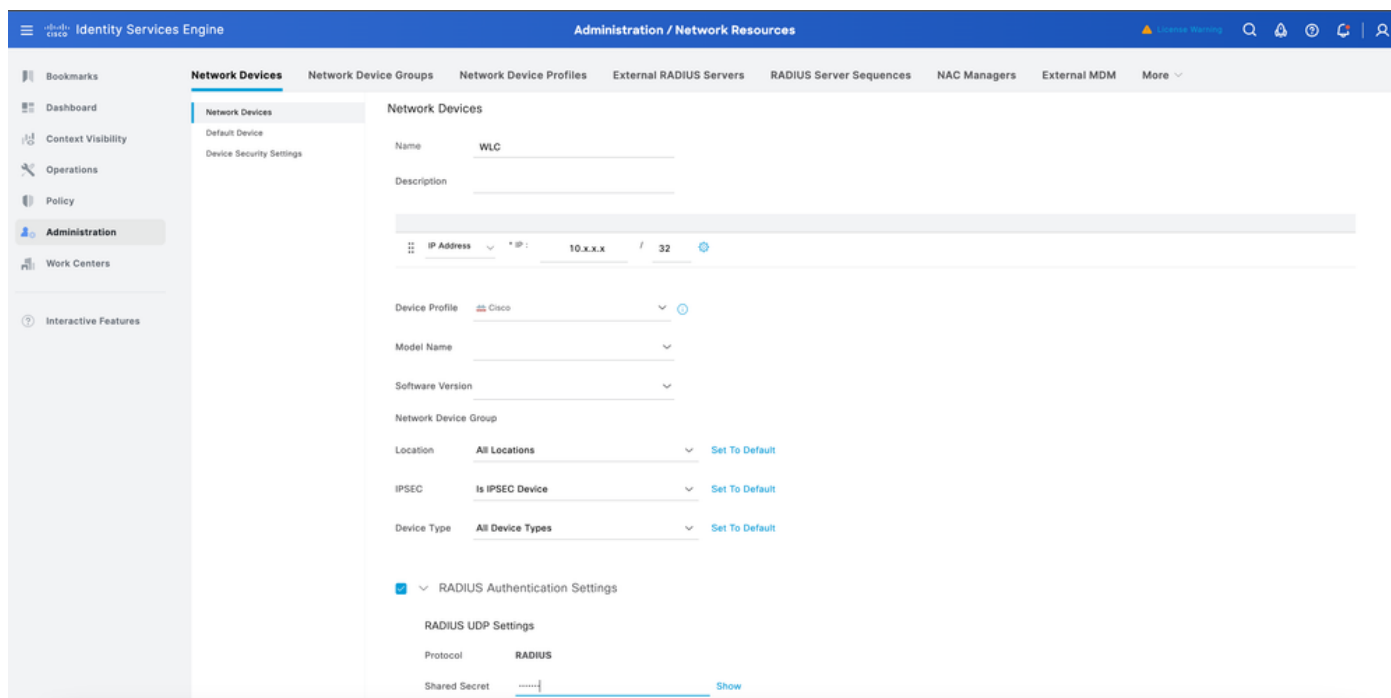
Konfigurieren des ISE-Netzwerkgeräts

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



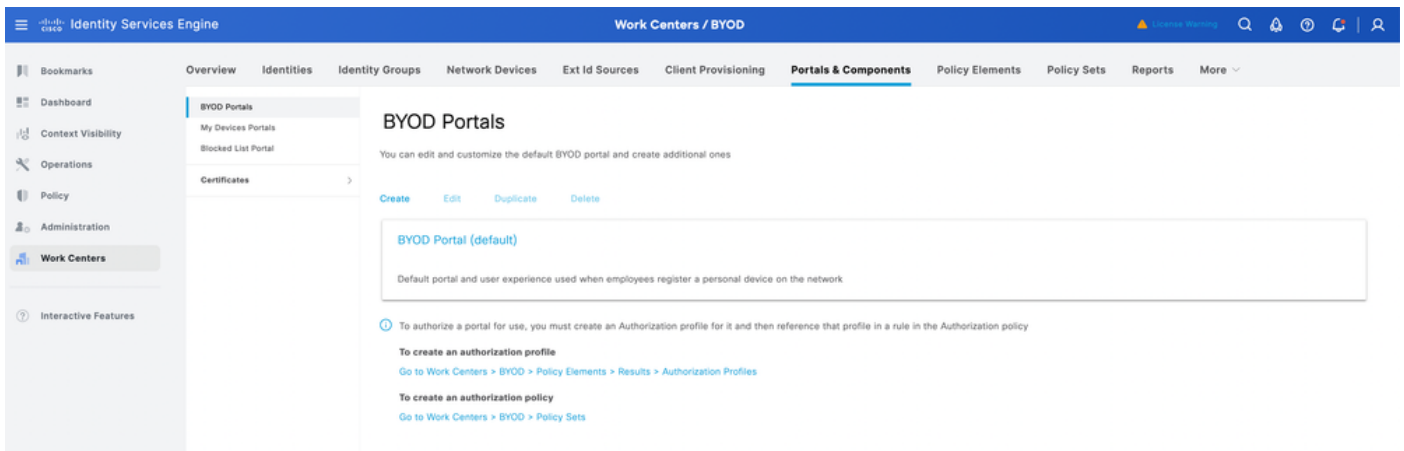
3. Fügen Sie Ihren WLC als Netzwerkgerät hinzu:

- 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.



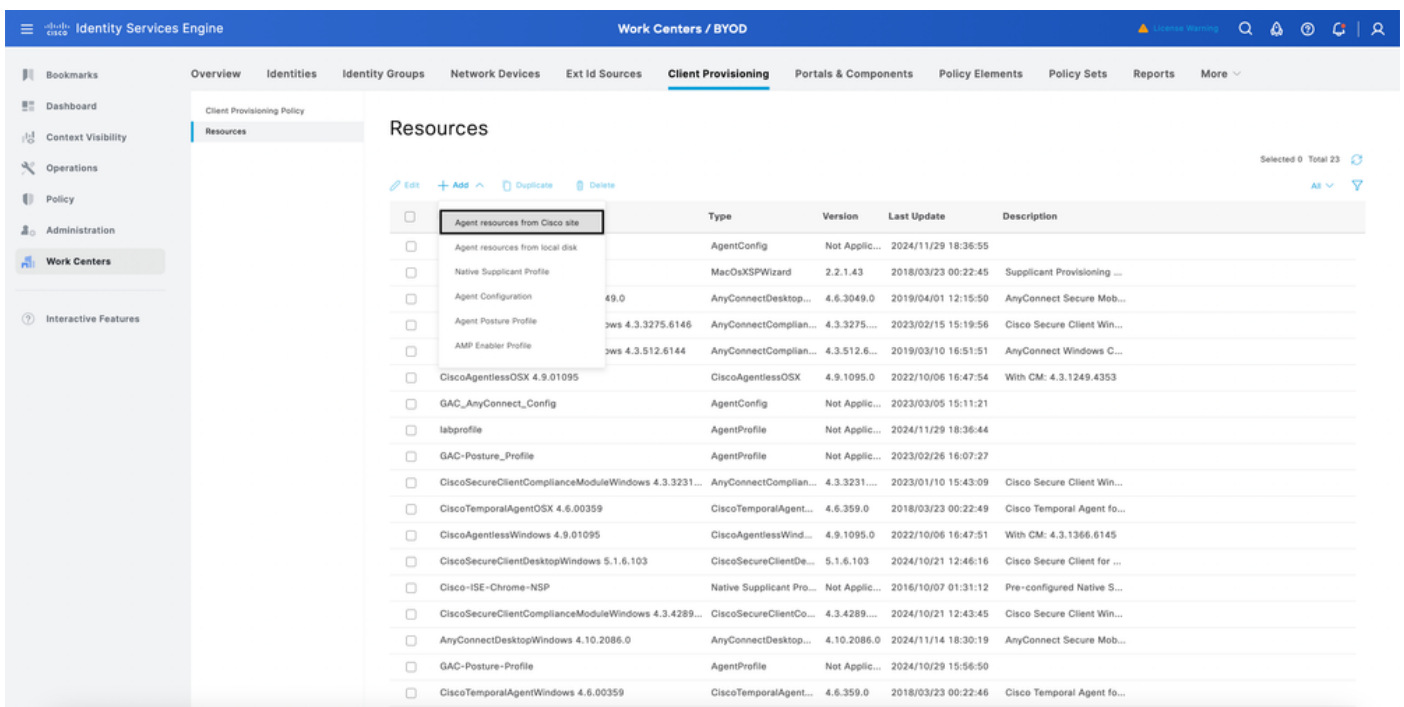
Erstellung eines BYOD-Portals

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.



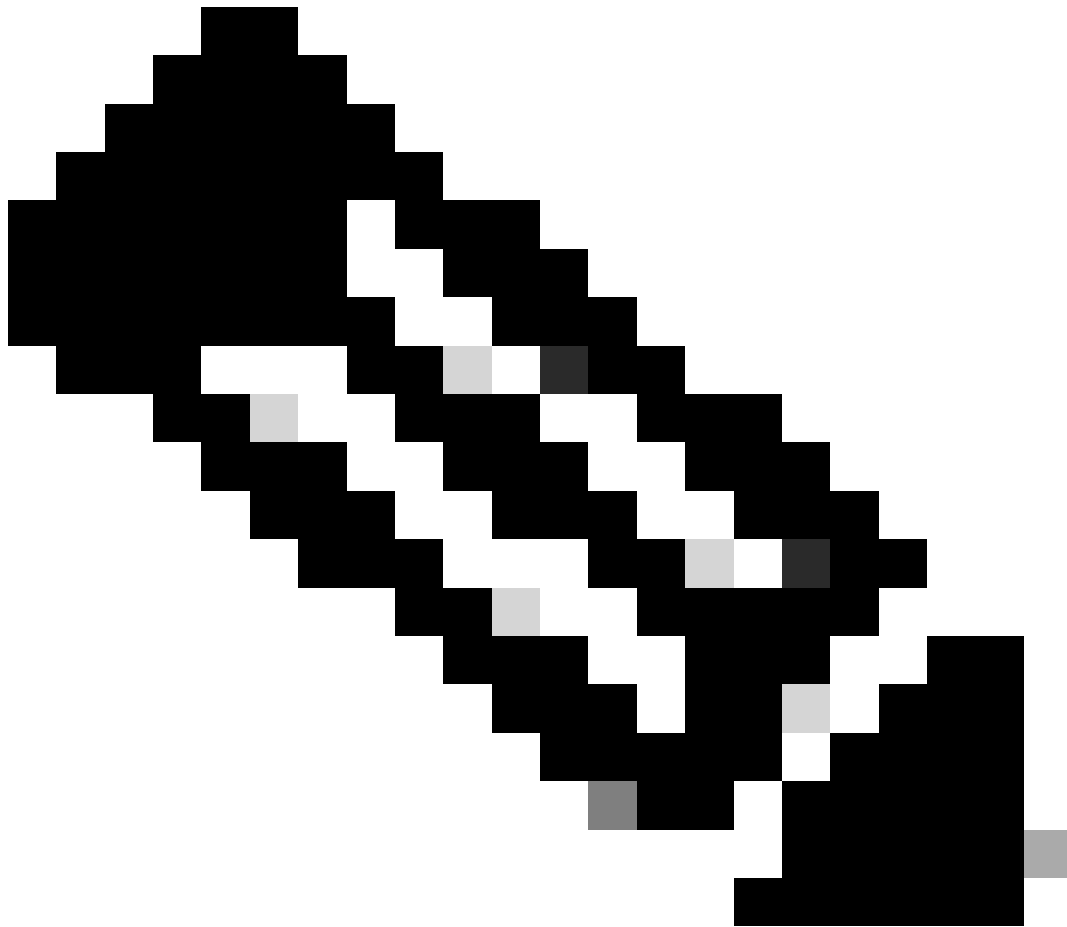
Download Remote Resources

☐	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

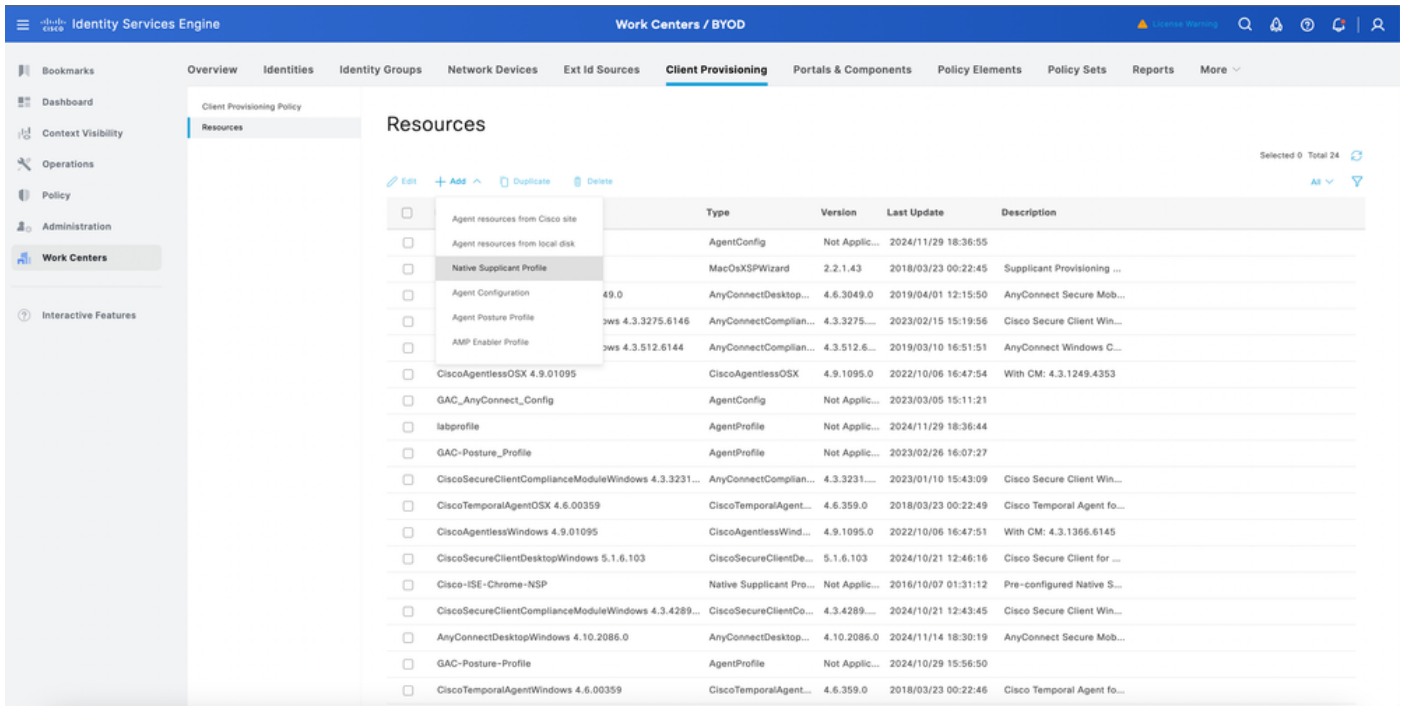
Save



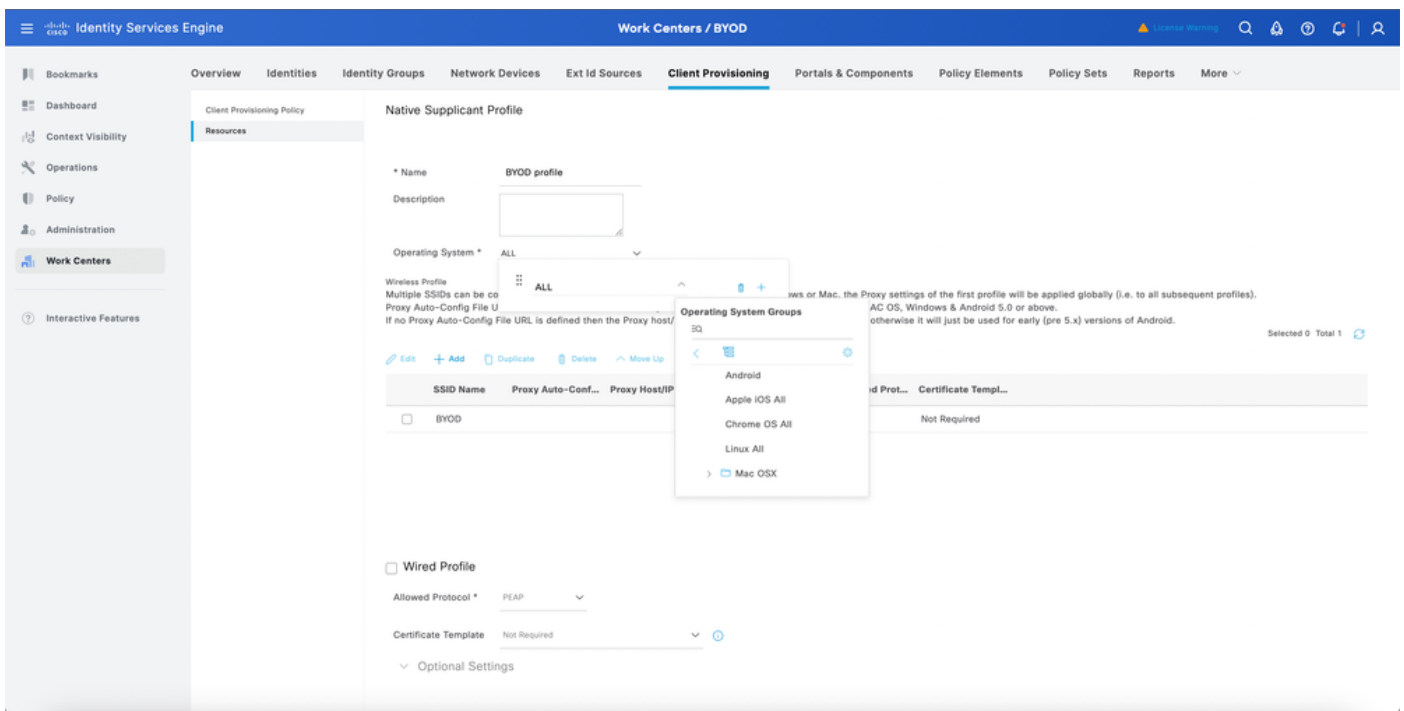
Anmerkung: Die Cisco IOS Software kann für Windows- und MacOS-Endgeräte von der ISE heruntergeladen werden. Für Apple iPhone IOS, es verwendet eine native Supplicant, um das Gerät bereitzustellen und Für Android-Gerät, haben Sie Netzwerk-Setup-Assistent, die aus dem Play Store heruntergeladen werden 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		i
Proxy Host/IP		i
Proxy Port		
Security *	WPA2 Enterprise	▼
Allowed Protocol *	PEAP	▼
Certificate Template	Not Required	▼ i

▼ Optional Settings

Windows Settings

Authentication Mode	User or Computer	▼
☐ Automatically use logon name and password (and domain if any)		
☒ 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		
☒ Connect even if the network is not broadcasting its name (SSID)		

iOS Settings

☐ Enable if target network is hidden

Android Settings

Certificate Enrollment Protocol: [i](#)

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..

Wireless Profile(s)

SSID Name *

Proxy Auto-Config File URL

i

Proxy Host/IP

i

Proxy Port

Security *

WPA2 Enterprise

▼

Allowed Protocol *

TLS

▼

Certificate Template

EAP_Authentication_Certificate_Template

▼

i

▼ Optional Settings

EAP_Authentication_Certificate_Template

pxGrid_Certificate_Template

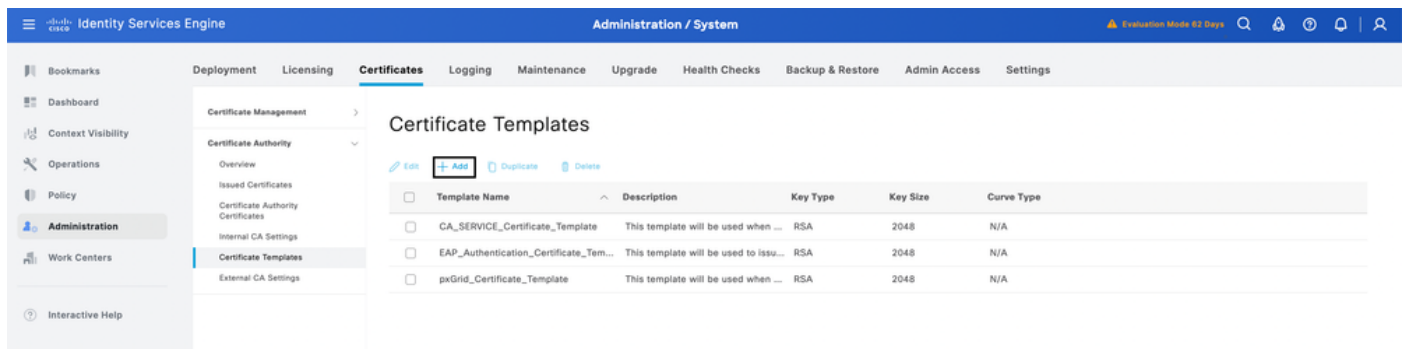
Save

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

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

Templates.

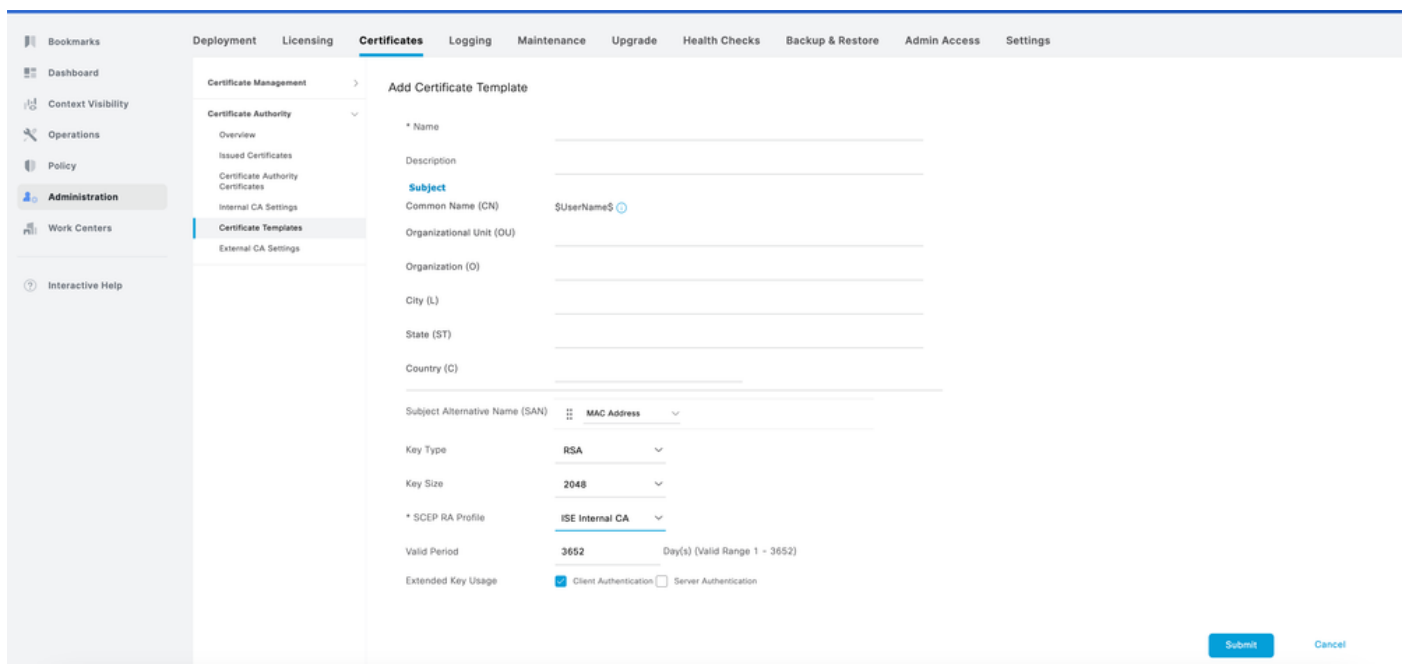
2. Klicken Sie auf der Seite auf die Schaltfläche Hinzufügen.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains the navigation menu, with 'Administration' selected. The main content area displays the 'Certificate Templates' section. The 'Add' button is highlighted with a red box.

Template Name	Description	Key Type	Key Size	Curve Type
CA_SERVICE_Certificate_Template	This template will be used when ...	RSA	2048	N/A
EAP_Authentication_Certificate_Tem...	This template will be used to issu...	RSA	2048	N/A
pxGrid_Certificate_Template	This template will be used when ...	RSA	2048	N/A

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



The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page, specifically the 'Add Certificate Template' form. The left sidebar contains the navigation menu, with 'Administration' selected. The main content area displays the 'Add Certificate Template' form with various fields for configuration.

Add Certificate Template

* Name: _____

Description: _____

Subject

Common Name (CN): \$UserName\$ ⓘ

Organizational Unit (OU): _____

Organization (O): _____

City (L): _____

State (ST): _____

Country (C): _____

Subject Alternative Name (SAN): ⓘ MAC Address ▾

Key Type: RSA ▾

Key Size: 2048 ▾

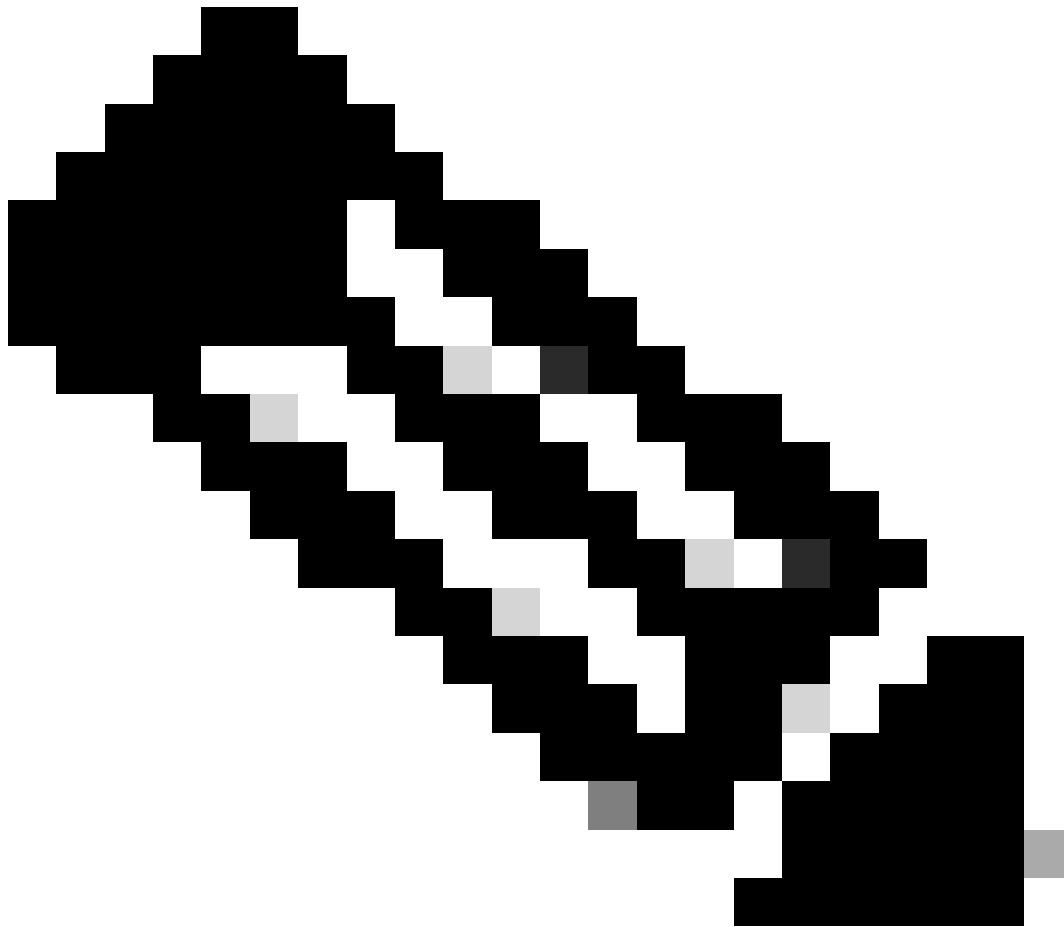
* SCEP RA Profile: ISE Internal CA ▾

Valid Period: 3652 Day(s) (Valid Range 1 - 3652)

Extended Key Usage: ☒ Client Authentication ☐ Server Authentication

Submit **Cancel**

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.

Identity Services Engine Work Centers / BYOD Evaluation Mode 63 Days

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy Resources

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM64 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session as follows:
1 Session-OS-Architecture EQUALS arm64, or
2 Cisco-av-pair EQUALS mdm-tlv=device-platform=win-arm64.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AnyConnect	If Any	and Windows All	and CiscoSE:ExternalGroups EQUALS ITSLMY:ITSLDomain.com/Users/Domain Users	then AnyConnect5.1
iOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
DownloadAnyConnect	If Any	and Windows All	and Condition(s)	then AnyConnect5.1

Actions: Duplicate above, Duplicate below, Insert new policy above, Insert new policy below, Delete

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.

Identity Services Engine Work Centers / BYOD Evaluation Mode 63 Days

Overview Identities Identity Groups Network Devices Ext Id Sources **Client Provisioning** Portals & Components Policy Elements Policy Sets Reports More

Client Provisioning Policy Resources

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

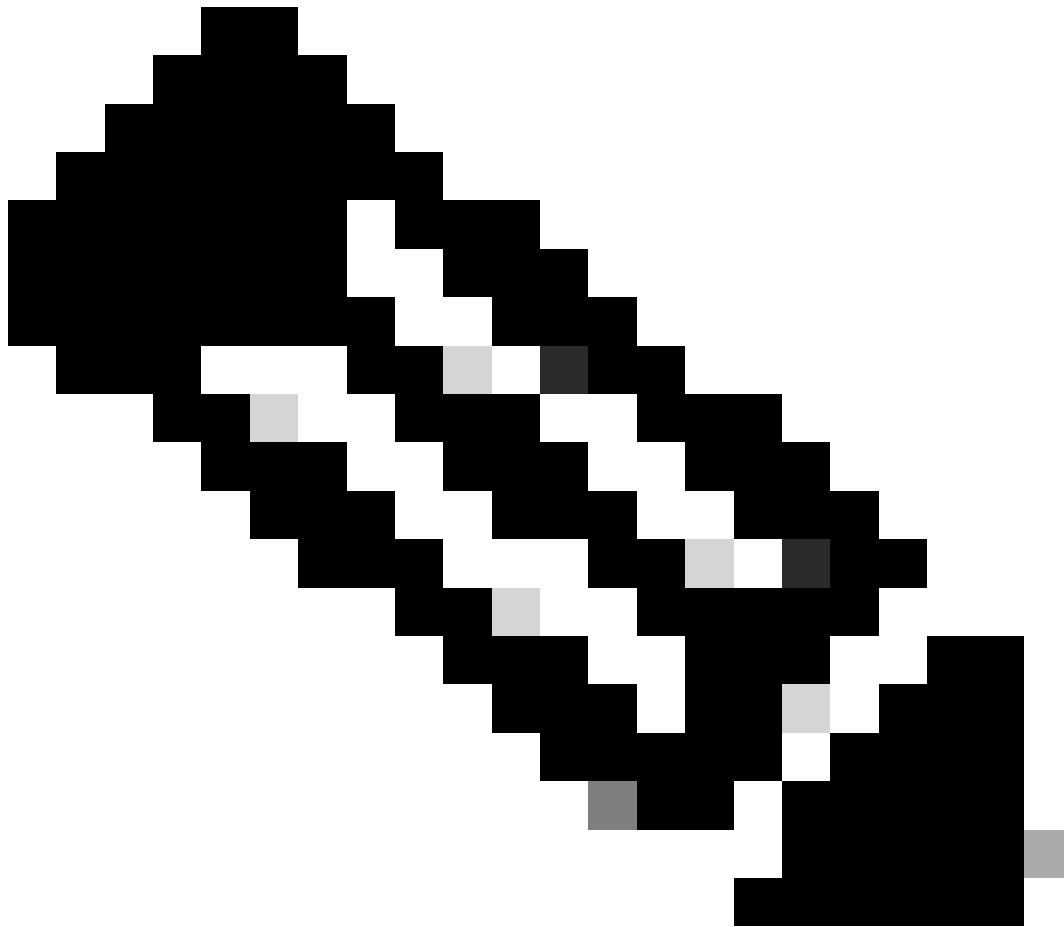
Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM64 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session as follows:
1 Session-OS-Architecture EQUALS arm64, or
2 Cisco-av-pair EQUALS mdm-tlv=device-platform=win-arm64.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
AnyConnect	If Any	and Windows All	and CiscoSE:ExternalGroups EQUALS ITSLMY:ITSLDomain.com/Users/Domain Users	then AnyConnect5.1
BYOD	If Any +	and Windows All +	and Condition(s) +	then Result X Done
iOS	If Any	and Apple iOS All	and Condition(s)	then
Android	If Any	and Android	and Condition(s)	then

Agent Configuration: Choose an Agent, Is Upgrade Mandatory

Native Supplicant Configuration: WinSPWizard 3.2.0.1, Cisco-ISE-NSP

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:

Policy Sets

Reset

Reset Policy Set Hit Counts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search							
	BYOD		Wireless_802.1X	Default Network Access	+ 0		
	Default	Default policy set		Default Network Access	+ 0		

Reset

Save

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:

Identity Services Engine Administration / Identity Management

External Identity Sources

Certificate Authentication Profile

External Identity Sources

- Certificate Authentic...
- Active Directory
- CiscoSE
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST

Actions: Edit, Add, Duplicate, Delete

Name	Description
Preloaded_Certificate_Profile	Precreated Certificate Authorization Profile.

Identity Services Engine Administration / Identity Management

External Identity Sources

Certificate Authentication Profile

* Name: BYOD

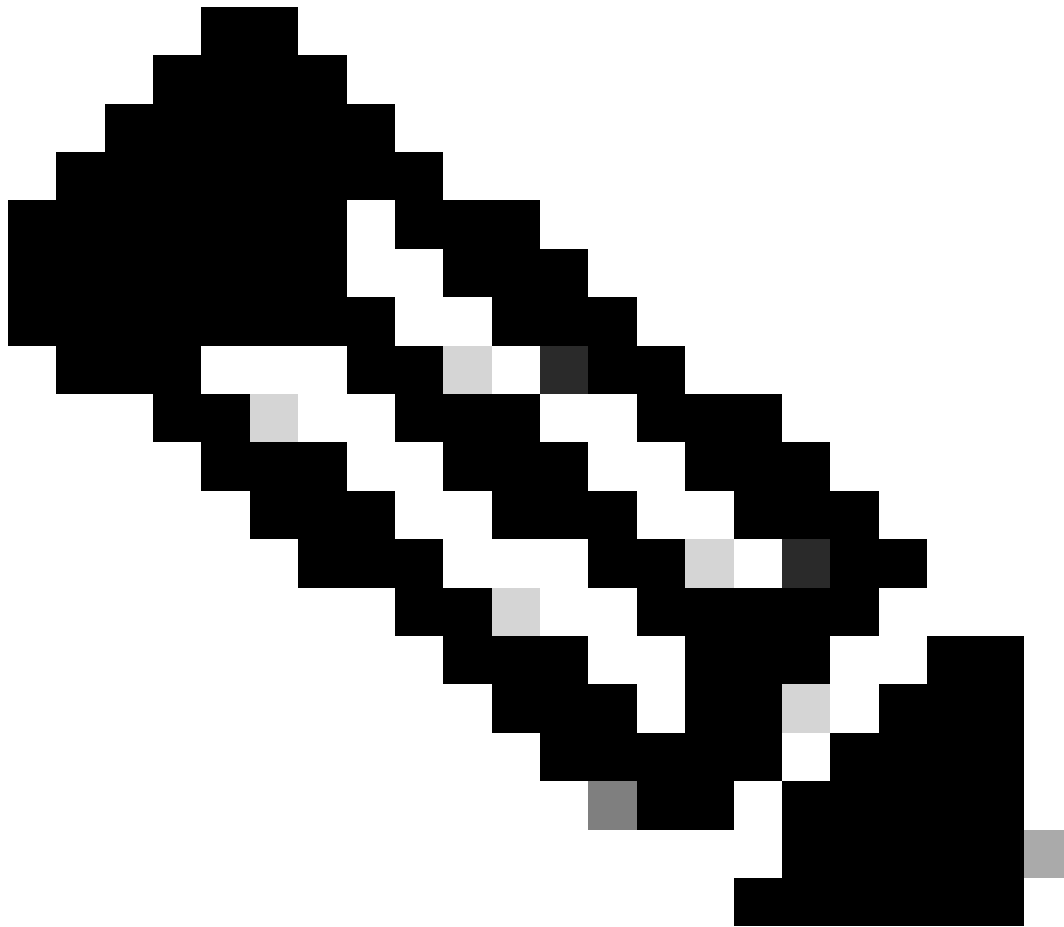
Description: [Text Field]

Identity Store: [not applicable]

Use Identity From: Certificate Attribute Subject - Common Name

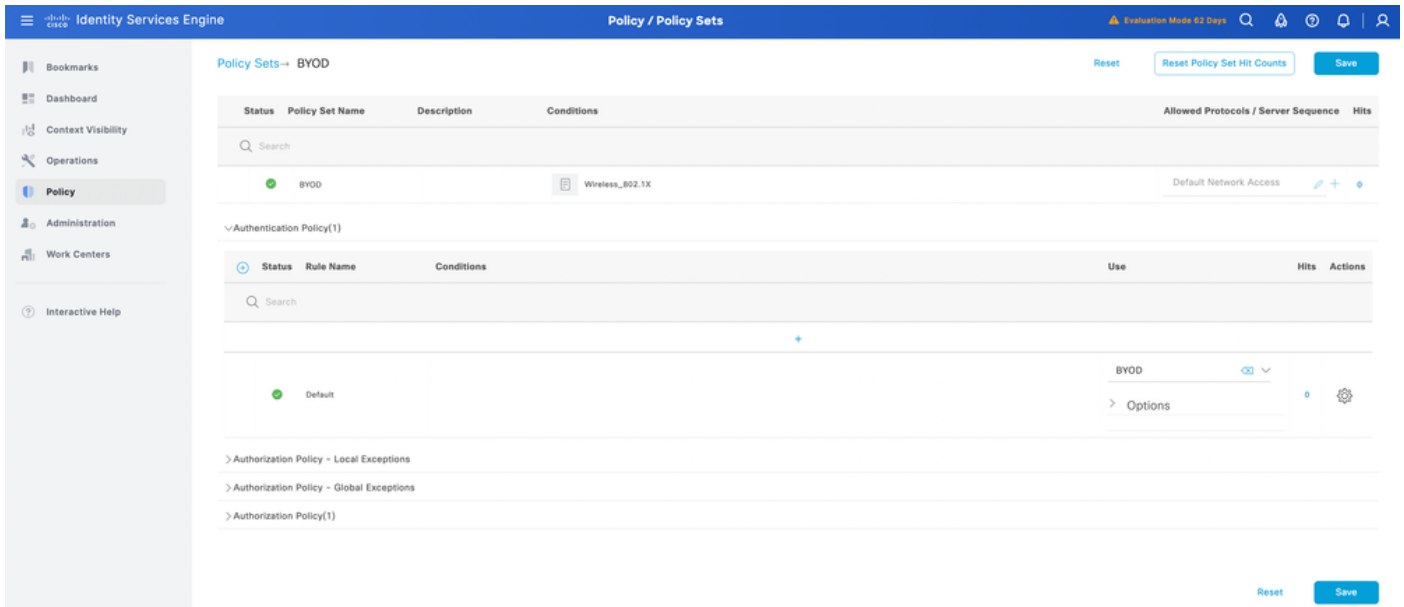
Match Client Certificate Against Certificate in Identity Store: Never

Submit Cancel



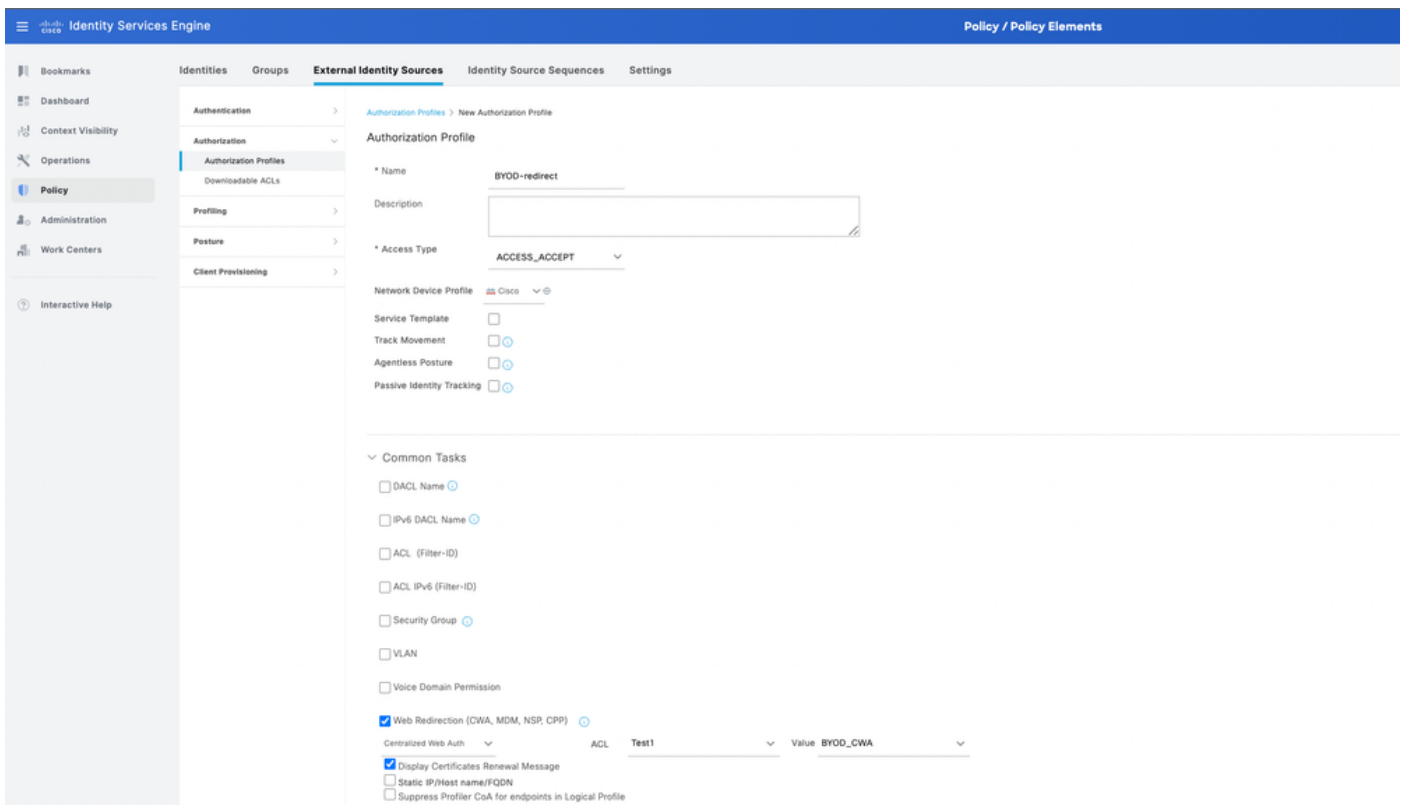
Anmerkung: Im Identity Store können Sie Ihr Active Directory, das in die ISE integriert wurde, immer auswählen, um eine Benutzersuche aus dem Zertifikat für zusätzliche Sicherheit durchzuführen.

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

The screenshot shows the Cisco Identity Services Engine (ISE) Policy / Policy Sets configuration page. The page is titled "Policy / Policy Sets" and has a sidebar with navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Help. The main content area shows the "Policy Sets" configuration for "BYOD".

The "Policy Sets" table lists the following Policy Sets:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	BYOD		Wireless_802.1X	Default Network Access	0

The "BYOD" Policy Set is expanded, showing its details:

- Authentication Policy(1)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy(3)

The "Authorization Policy(3)" is expanded, showing the following rules:

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
●	BYOD-Full access	AND EndPoints-BYODRegistration EQUALS Yes Network Access-EapAuthentication EQUALS EAP-TLS Normalised Radius-RadiusFlowType EQUALS Wireless802_1x	PermitAccess		Select from list	0	
●	BYOD-Redirection	AND Network Access-EapAuthentication EQUALS EAP-MSCHAPv2 Normalised Radius-RadiusFlowType EQUALS Wireless802_1x	BYOD-redirect		Select from list	0	
●	Default		DenyAccess		Select from list	0	

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Policy / Policy Sets configuration page. The page is titled "Policy Sets" and has a sidebar with navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Help. The main content area shows the "Policy Sets" configuration for "BYOD".

The "Policy Sets" table lists the following Policy Sets:

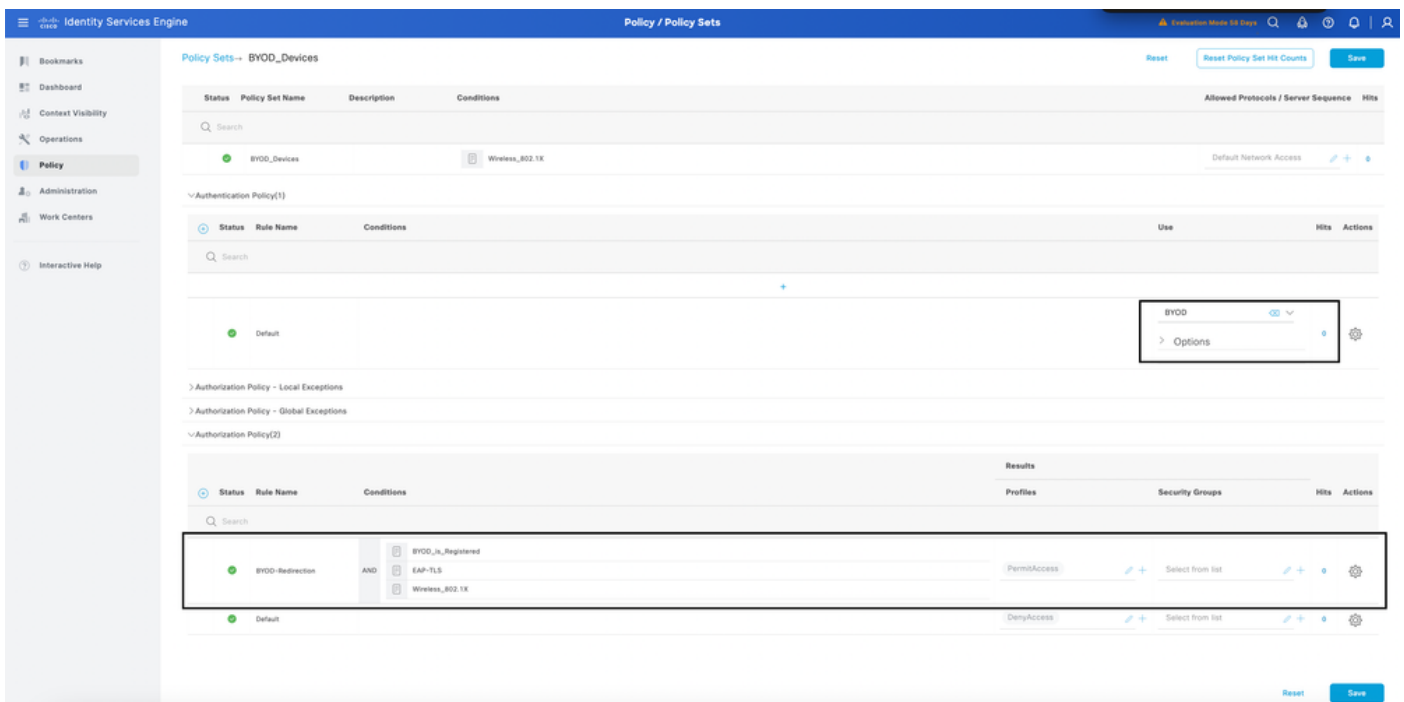
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	BYOD_Devices		Wireless_802.1X	Default Network Access	0		
●	Onboard_Personal_Devices		Wireless_MAB	Default Network Access	0		
●	Default	Default policy set		Default Network Access	0		

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.

↺ Reset Repeat Counts ↗ Export To										Filter			⚙
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authorization Policy	Authoriz...	IP Address	Network De...	Device	
×		▼		Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorization Policy	Authorizatic	IP Address	▼	Network Device	Device
Feb 24, 2025 12:30:18.1...	ⓘ	🔍	0	test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD	PermitAcc...	10.127.196.2...			TenGig...
Feb 24, 2025 12:06:43.0...	✅	🔍		test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...	BYOD-Switch		TenGig...
Feb 24, 2025 12:06:37.9...	✅	🔍		test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...	BYOD-Switch		TenGig...

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

BYOD Portal

test

1
2
3

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

The following system was detected

Windows

Was your device detected incorrectly?

Select your Device

Windows

Start

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.

The screenshot shows the Cisco BYOD Portal interface. At the top, there is a header with the Cisco logo on the left, 'BYOD Portal' in the center, and 'test' with a user icon on the right. Below the header, a progress indicator shows two steps: step 2 is active and highlighted with a blue circle, and step 3 is shown as a plain circle. The main content area is titled 'Device Information' and contains the instruction: 'Enter the device name and optional description for this device so you can manage it using the My Devices Portal.' There are three input fields: 'Device name: *' (required), 'Description:', and 'Device ID:'. The 'Device ID' field is pre-filled with a blacked-out value. At the bottom of the form is a blue 'Continue' button with a right-pointing arrow.

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

The screenshot shows the next step in the Cisco BYOD Portal. The header is identical to the previous screen. The progress indicator now shows step 3 as the active step, highlighted with a blue circle. The main content area is titled 'Install' and contains the instruction: 'Please wait while we download the Cisco Network Setup Assistant. You will then need to manually run the Setup Assistant and follow the instructions to finish registering this device.'

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



Network Setup Assistant

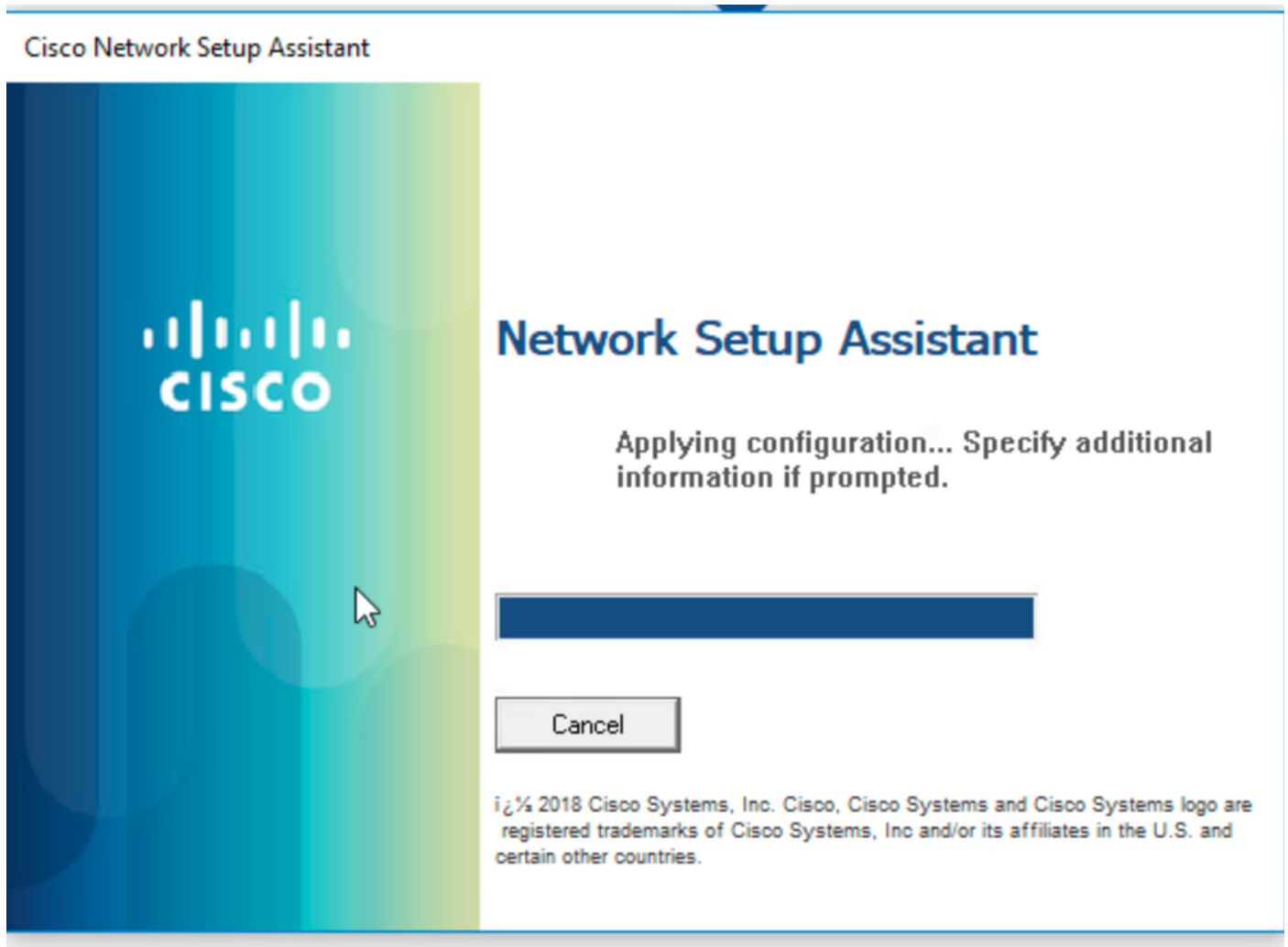


This application automatically configures network settings.

Start

Quit

© 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 -:0000000000000000B30D59CC5:::-
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 -:0000000000000000B30D59CC5:::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 -:0000000000000000B30D59CC5:::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 -:0000000000000000B30D59CC5:::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 -:0000000000000000B30D59CC5:::-
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 -:0000000000000000B30D59CC5:::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 -:0000000000000000B30D59CC5:::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 -:0000000000000000B30D59CC5:::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 -:0000000000000000B30D59CC5:::-
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 -:0000000000000000B30D59CC5:::- 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 -:0000000000000000B30D59CC5:::-
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 -:0000000000000000B30D59CC5:::-
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=32281512738768960628252532784663302089]'
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=68627620160586308685849818775100698224]'
24.02.2025 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::: 4. '[emittent=CN=Certificate Services Node CA - iseguest;
serial=72934767698603097153932482227548874953]'
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\[live,96444,1,0,120\]](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 = 0000000000000000B30D59M KV 5
24.02.2025, 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::: Sitzung = 0000000000000000B30D59M 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 = 0000000000000000B30D55 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 SPPProfile-
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.