

Configureer ISE BYOD met enkele en dubbele SSID in ISE 3.3

Inhoud

[Inleiding](#)

[Achtergrond](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Wat is Single SSID en Dual SSID BYOD op ISE?](#)

[Single SSID BYOD](#)

[Dual SSID BYOD](#)

[WLC-configuratie](#)

[Een WLAN voor CWA maken](#)

[RADIUS-servers configureren](#)

[AAA-servers configureren](#)

[Beveiligingsbeleid voor het WLAN configureren](#)

[Voorafgaande verificatie-ACL configureren](#)

[Beleidsprofiel configureren](#)

[Tags toepassen en implementeren](#)

[Een open/onbeveiligde SSID configureren](#)

[ISE-configuratie](#)

[Voorwaarden](#)

[Certificaten](#)

[DNS-configuratie](#)

[ISE-netwerkapparaat configureren](#)

[Een BYOD-portal maken](#)

[Nieuwste versie Cisco IOS® downloaden](#)

[Een endpointprofiel maken](#)

[Sjabloon voor certificaat](#)

[Een endpointprofiel toewijzen aan de client-provisioningportal](#)

[Configureer ISE-beleidssets voor één SSID-BYOD](#)

[Configureer ISE-beleidssets voor Dual SSID BYOD](#)

[Probleemoplossing](#)

[Logfragment](#)

[Gastenlogboeken](#)

[ISE-PSC-logbestanden](#)

[Downloaden van endpointprofiel](#)

Inleiding

Het document beschrijft hoe u BYOD-problemen op ISE kunt configureren en oplossen.

Achtergrond

BYOD is een functie waarmee gebruikers hun persoonlijke apparaten op ISE aan boord kunnen nemen, zodat de gebruiker de netwerkbron op de omgeving kan gebruiken. Het helpt de netwerkbeheerder ook om te voorkomen dat de gebruiker toegang heeft tot de kritieke bron van de persoonlijke apparaten.

In tegenstelling tot de gaststroom waarbij het apparaat is geverifieerd met de Gastpagina met behulp van de interne Store of Active directory op ISE. Met de BYOD kan de netwerkbeheerder een eindpuntprofiel op het eindpunt installeren om het type EAP-methode te kiezen. In scenario's zoals EAP-TLS wordt het clientcertificaat door de ISE zelf ondertekend om een vertrouwen te creëren tussen het eindpunt en ISE.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- WLC-controller
- Basiskennis over ISE

Gebruikte componenten

Deze gebruikte apparaten zijn niet beperkt tot één bepaalde versie voor de BYOD-stroom:

- Catalyst 9800-CL draadloze controller (17.12.3)
- ISE virtuele machine (3.3)

Wat is Single SSID en Dual SSID BYOD op ISE?

Single SSID BYOD

In een Single SSID BYOD-installatie verbinden gebruikers hun persoonlijke apparaten rechtstreeks met het draadloze bedrijfsnetwerk. Het onboarding proces vindt plaats op dezelfde SSID, waar ISE de registratie, levering en handhaving van het apparaat vergemakkelijkt. Deze benadering vereenvoudigt de gebruikerservaring, maar vereist veilige onboarding en juiste verificatiemethoden om de netwerkbeveiliging te garanderen.

Dual SSID BYOD

In een dubbele opstelling van SSID BYOD, worden twee afzonderlijke SSIDs gebruikt: een voor onboarding (onbeveiligde of beperkte toegang) en een ander voor toegang tot het bedrijfsnetwerk. Gebruikers maken eerst verbinding met de onboarding SSID, voltooien apparaatregistratie en

provisioning via ISE, en vervolgens switches naar de beveiligde zakelijke SSID voor netwerktoegang. Dit biedt een extra beveiligingslaag door onboarding van verkeer te scheiden van productieverkeer.

WLC-configuratie

Een WLAN voor CWA maken

1. Ga naar Configuratie > Tags & profielen > WLAN's.
 2. Klik op Add om een nieuw WLAN te maken.
- Stel een WLAN-naam en SSID in (bijvoorbeeld BYOD-WiFi).
 - Schakel het WLAN in.

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

RADIUS-servers configureren

1. Navigeer naar Configuratie > Beveiliging > AAA > RADIUS > Servers.

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

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

RADIUS

TACACS+

LDAP

Servers Server Groups

Acct Port "Contains" 1814

Name	Address	Auth Port	Acct Port
0			

No items to display

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

2. Klik op Add om ISE te configureren als een RADIUS-server:

- IP-server: IP-adres van ISE.
- Gedeeld geheim: Stem het gedeelde geheim af op ISE.

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 [i](#)

ENABLED ☒

CoA Server Key Type

Clear Text

CoA Server Key [i](#)

Confirm CoA Server Key

Automate Tester

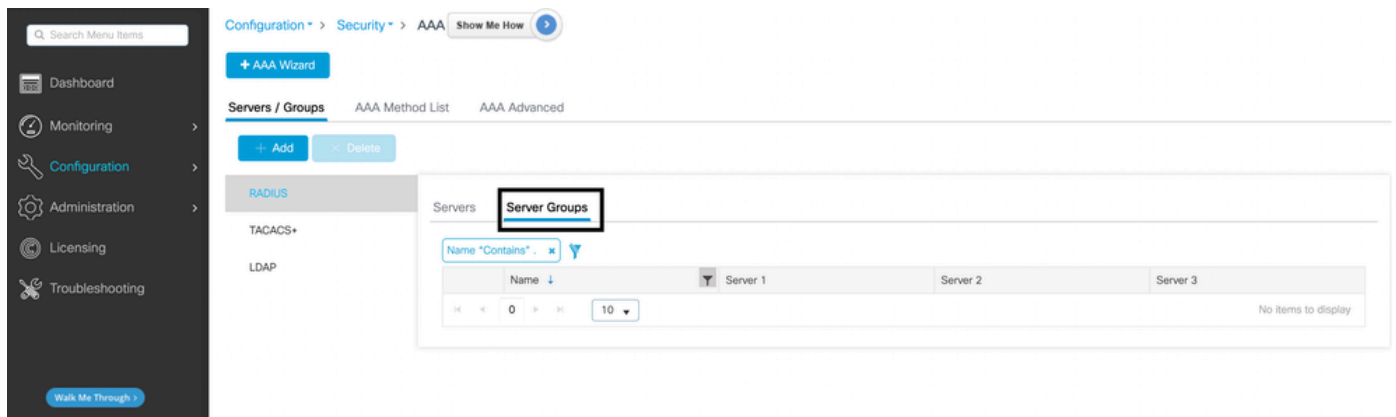
☐

[Cancel](#)

[Apply to Device](#)

AAA-servers configureren

1. Ga naar Configuratie > Beveiliging > AAA > Servers/groepen.



2. Wijs de RADIUS-server toe aan een nieuwe of bestaande servergroep.

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

> < >> <<

Cancel Apply to Device

Beveiligingsbeleid voor het WLAN configureren

1. Navigeer naar Configuratie > Tags en profielen > WLAN's. Bewerk het eerder gemaakte WLAN.
2. Onder het tabblad Security > Layer 2:
 - WPA+WPA2 inschakelen
 - AES (CCMP128) instellen onder WPA2-encryptie
 - Beheer autosleutel 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. Selecteer onder het tabblad Security > Layer 3 de optie global uit de vervolgkeuzelijst voor Web Auth Parameter Map.

⚠ 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

Voorafgaande verificatie-ACL configureren

Maak een ACL om deze omleidingsacties:

- DNS-verkeer.
- HTTP/HTTPS naar het ISE-portal.
- Alle vereiste back-end services.

Dit doet u zo:

1. Ga naar Configuratie > Beveiliging > ACL's > Toegangscontrolelijsten.
2. Maak een nieuwe ACL met regels om noodzakelijk verkeer toe te staan.

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 ⏏

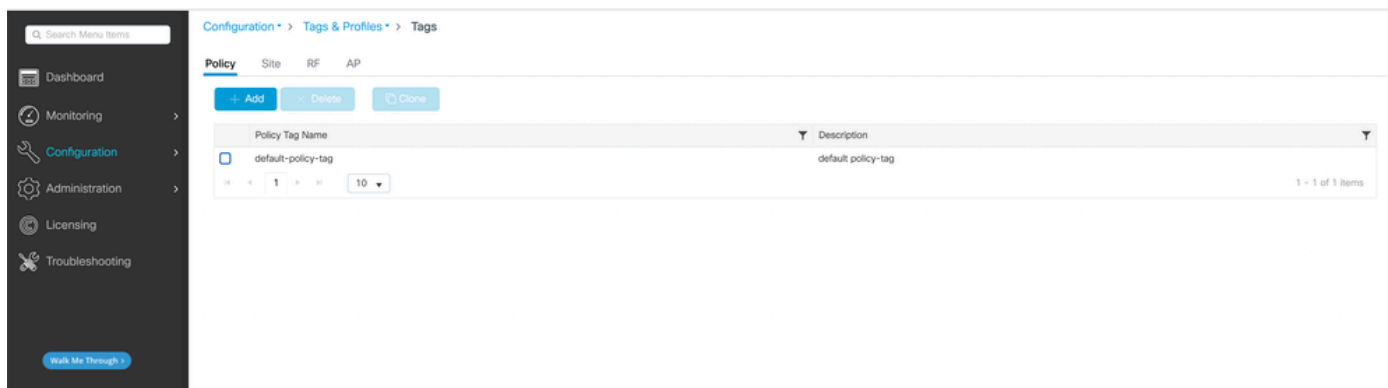
Post Auth

Search or Select ⏏

↶ Cancel

📁 Update & Apply to Device

3. Schakel ook AAA en NAC status toestaan in onder Advanced in het beleid.



Een open/onbeveiligde SSID configureren

De Open SSID wordt alleen gemaakt wanneer u besluit om een Dual SSID BYOD-configuratie op uw omgeving te hebben.

1. Navigeren naar Configuratie > Tags en profielen > WLAN's. Klik op de knop Toevoegen.
2. Geef een SSID-naam op onder het tabblad Algemeen en schakel de WLAN-knop in.

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. Klik in hetzelfde venster op het tabblad Beveiliging. Selecteer het keuzerondje Geen en schakel Mac-filtering in.

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. In Layer 3 onder Security selecteert u de wereldwijde instelling voor Web Auth Parameter Map. Als u een ander web auth profiel geconfigureerd op de WLC, kunt u het hier ook in kaart brengen:

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-configuratie

Voorwaarden

- Zorg ervoor dat Cisco ISE is geïnstalleerd en gelicentieerd voor BYOD-functionaliteit.
- Voeg uw WLC toe aan ISE als netwerkapparaat met het gedeelde RADIUS-geheim.

Certificaten

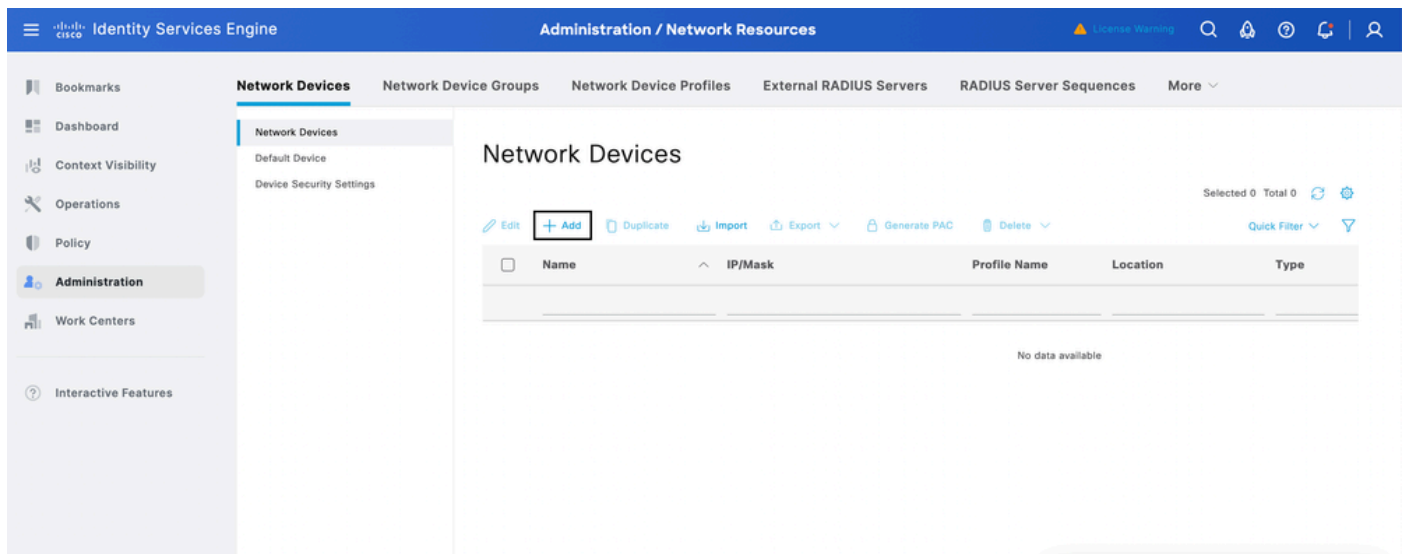
- Installeer een geldig servercertificaat op ISE om beveiligingswaarschuwingen voor de browser te voorkomen.
- Zorg ervoor dat het certificaat wordt vertrouwd door eindpunten (ondertekend door een bekende CA of een interne CA met vertrouwde basis).

DNS-configuratie

- Zorg ervoor dat DNS de ISE-hostnaam voor het BYOD-portal oplost.

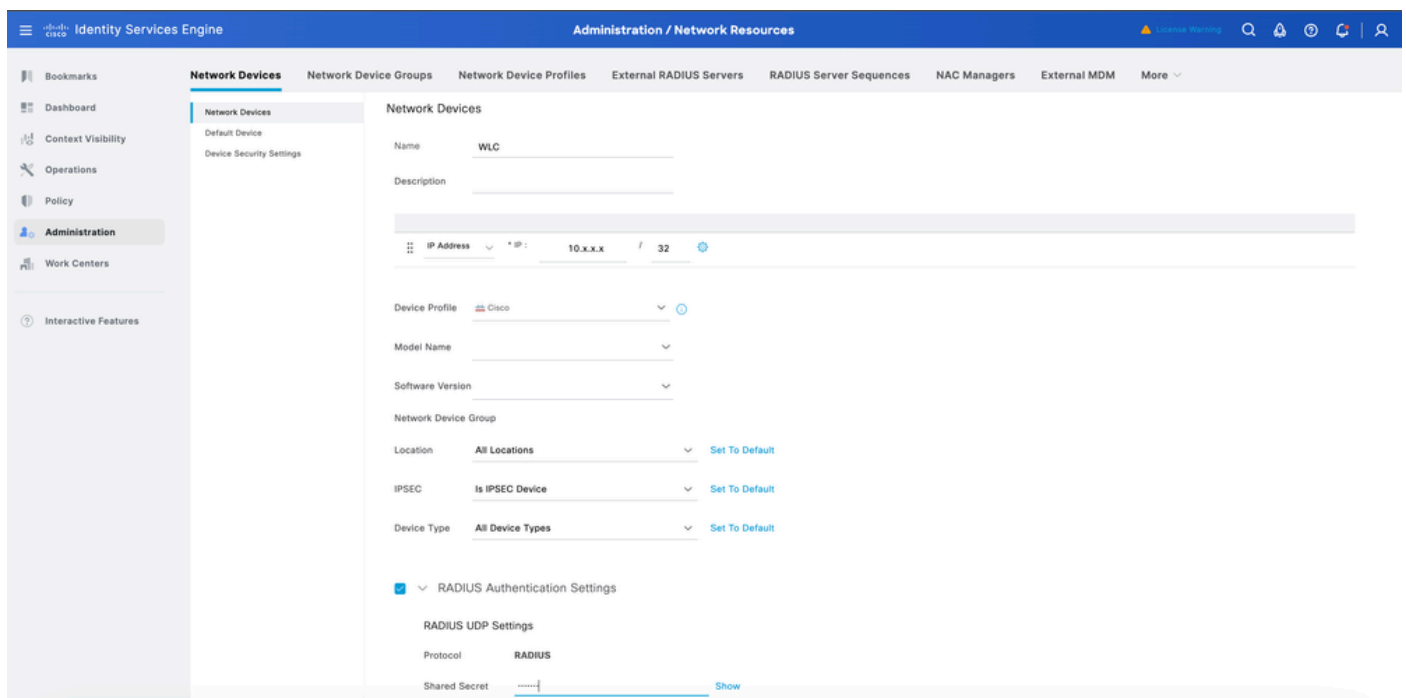
ISE-netwerkapparaat configureren

1. Log in op de ISE web UI.
2. Ga naar Beheer > Netwerkbronnen > Netwerkapparaten.



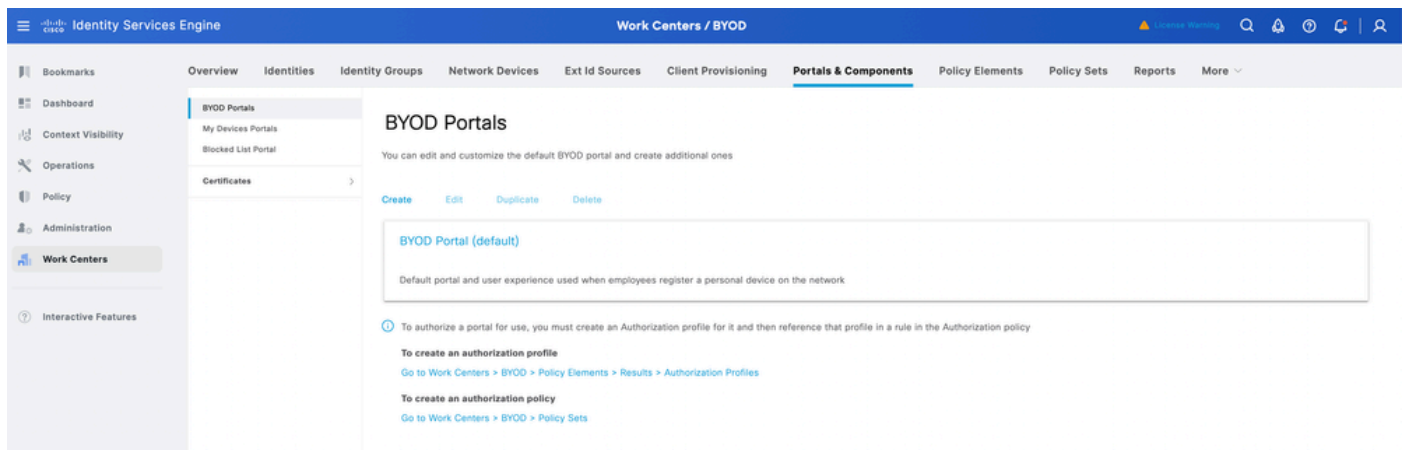
3. Add uw WLC als netwerkapparaat:

- Naam: Voer een naam in voor de WLC.
- IP-adres: Voer het WLC-beheer IP in.
- RADIUS gedeeld geheim: Voer hetzelfde gedeelde geheim in als geconfigureerd op de WLC.
- Klik op Verzenden.



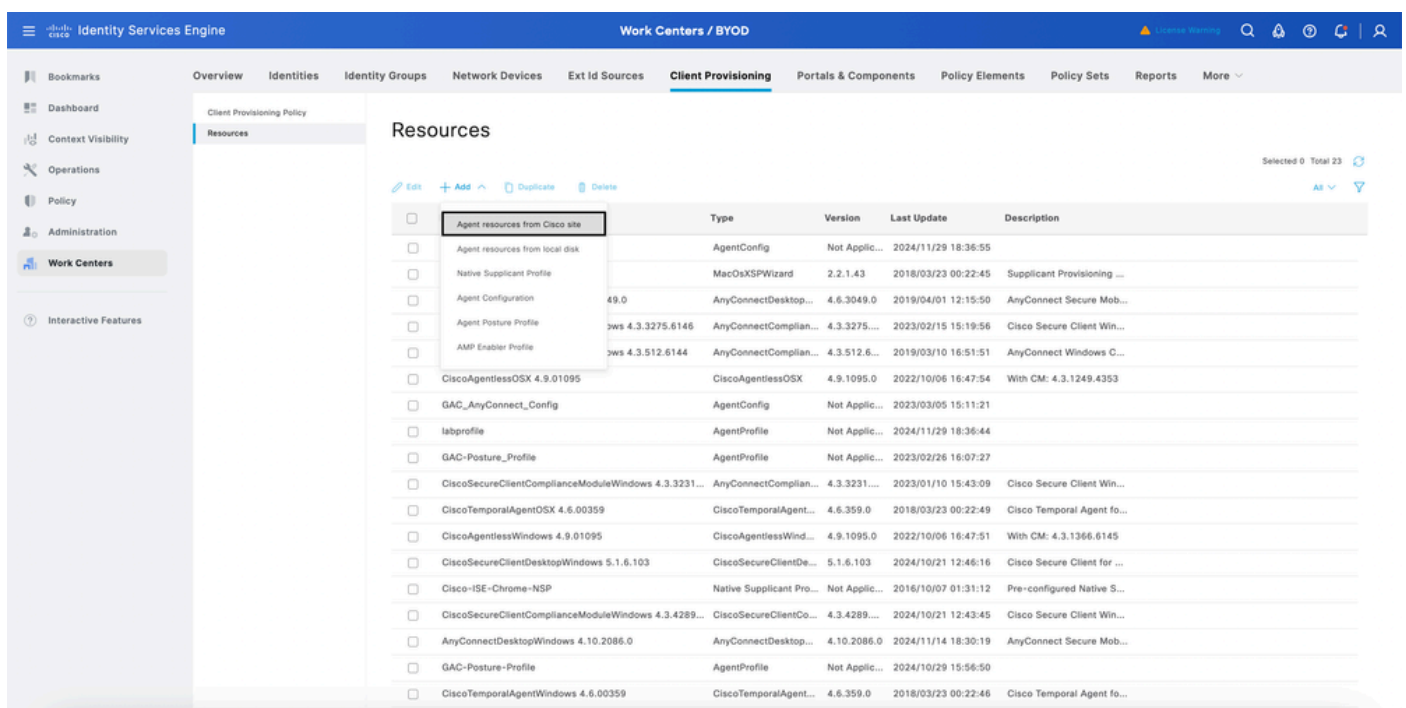
Een BYOD-portal maken

1. Navigeren naar werkcentra > BYOD > Instellingen > Portals & Components > BYOD Portals.
2. Klik op Add om een BYOD-portal te maken of u kunt het bestaande standaardportal op ISE gebruiken.



Nieuwste versie Cisco IOS® downloaden

1. Navigeren naar werkcentra > BYOD > Clientprovisioning > Resources.
2. Klik op de knop Add en selecteer agent resources uit de Cisco-site.



3. Selecteer in de softwarelijst de nieuwste Cisco IOS-versie die u wilt downloaden.



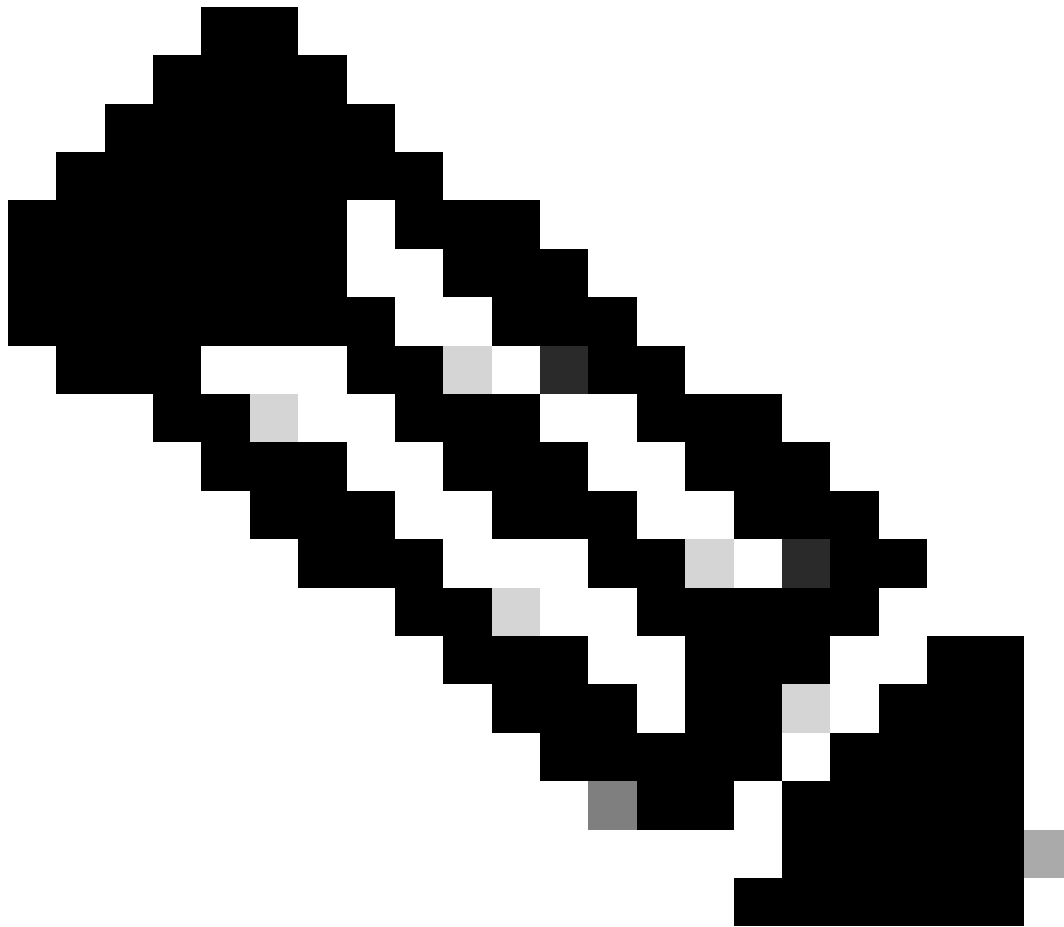
Download Remote Resources

☐	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



Opmerking: Cisco IOS-software wordt gedownload op de ISE voor Windows- en MacOS-endpoints. Voor Apple iPhone IOS, het gebruikt een native supplicant om het apparaat te provisioneren en voor Android-apparaat, je hebt Network setup assistent die moet worden gedownload van Play Store.

Een endpointprofiel maken

1. Navigeren naar werkcentra > BYOD > Clientprovisioning > Resources.
2. Klik op Add, selecteer Native Supplicant-profiel in het keuzemenu.

Identity Services Engine Work Centers / BYOD

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

Client Provisioning Policy

Resources

Selected 0 Total 24

Edit Add Duplicate Delete

Name	Type	Version	Last Update	Description
Agent resources from Cisco site				
Agent resources from local disk				
Native Supplicant Profile	MacOsXSPWizard	2.2.1.43	2018/03/23 00:22:45	Supplicant Provisioning ...
Agent Configuration	AnyConnectDesktop...	4.6.3049.0	2019/04/01 12:15:50	AnyConnect Secure Mob...
Agent Posture Profile	AnyConnectComplan...	4.3.3275...	2023/02/15 15:19:56	Cisco Secure Client Win...
AMP Enabler Profile	AnyConnectComplan...	4.3.512.6...	2019/03/10 16:51:51	AnyConnect Windows C...
CiscoAgentlessOSX 4.9.01095	CiscoAgentlessOSX	4.9.1095.0	2022/10/06 16:47:54	With CM: 4.3.1249.4353
GAC_AnyConnect_Config	AgentConfig	Not Applic...	2023/03/05 15:11:21	
labprofile	AgentProfile	Not Applic...	2024/11/29 18:36:44	
GAC-Posture_Profile	AgentProfile	Not Applic...	2023/02/26 16:07:27	
CiscoSecureClientComplianceModuleWindows 4.3.3231...	AnyConnectComplan...	4.3.3231...	2023/01/10 15:43:09	Cisco Secure Client Win...
CiscoTemporalAgentOSX 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:49	Cisco Temporal Agent fo...
CiscoAgentlessWindows 4.9.01095	CiscoAgentlessWind...	4.9.1095.0	2022/10/06 16:47:51	With CM: 4.3.1366.6145
CiscoSecureClientDesktopWindows 5.1.6.103	CiscoSecureClientDe...	5.1.6.103	2024/10/21 12:46:16	Cisco Secure Client for ...
Cisco-ISE-Chrome-NSP	Native Supplicant Pro...	Not Applic...	2016/10/07 01:31:12	Pre-configured Native S...
CiscoSecureClientComplianceModuleWindows 4.3.4289...	CiscoSecureClientCo...	4.3.4289...	2024/10/21 12:43:45	Cisco Secure Client Win...
AnyConnectDesktopWindows 4.10.2086.0	AnyConnectDesktop...	4.10.2086.0	2024/11/14 18:30:19	AnyConnect Secure Mob...
GAC-Posture_Profile	AgentProfile	Not Applic...	2024/10/29 15:56:50	
CiscoTemporalAgentWindows 4.6.00359	CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:46	Cisco Temporal Agent fo...

3. Selecteer in de uitrollijst van het besturingssysteem het gewenste besturingssysteem op het apparaat of stel het in op ALL voor alle eindpunten in uw omgeving:

Identity Services Engine Work Centers / BYOD

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

Client Provisioning Policy

Resources

Native Supplicant Profile

* Name BYOD profile

Description

Operating System * ALL

Wireless Profile

Multiple SSIDs can be co

Proxy Auto-Config File U

If no Proxy Auto-Config File URL is defined then the Proxy host/

Operating System Groups

Android

Apple iOS All

Chrome OS All

Linux All

Mac OSX

SSID Name Proxy Auto-Conf... Proxy Host/IP

BYOD

Wired Profile

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

4. Klik op Add op de pagina om het eindpuntprofiel te maken om 802.1X te configureren voor het eindpunt:

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](#)

Afhankelijk van uw vereiste dient u het eindpuntprofiel voor het eindpunt in uw omgeving te configureren. Met het profiel voor endpoints kunnen we EAP-PEAP, EAP-TLS configureren.

5. Klik op Opslaan en vervolgens op Indienen in het eindpuntprofiel.

Sjabloon voor certificaat

Het eindpuntprofiel is vooraf geconfigureerd om EAP-TLS uit te voeren. Er moet een certificaatsjabloon aan het profiel worden toegevoegd. Standaard heeft ISE twee vooraf gedefinieerde sjablonen die uit de vervolgkeuzelijst kunnen worden gekozen.

Wireless Profile(s)

SSID Name *

Proxy Auto-Config File URL ⓘ

Proxy Host/IP ⓘ

Proxy Port

Security * WPA2 Enterprise ▼

Allowed Protocol * TLS ▼

Certificate Template EAP_Authentication_Certificate_Template ⓘ

▼ Optional Settings

- EAP_Authentication_Certificate_Template
- pxGrid_Certificate_Template

Save

Voer de volgende stappen uit om een nieuwe certificaatsjabloon te maken:

1. Ga naar Beheer > Systeem > Certificaten > Certificaatautoriteit > Certificaatsjablonen.

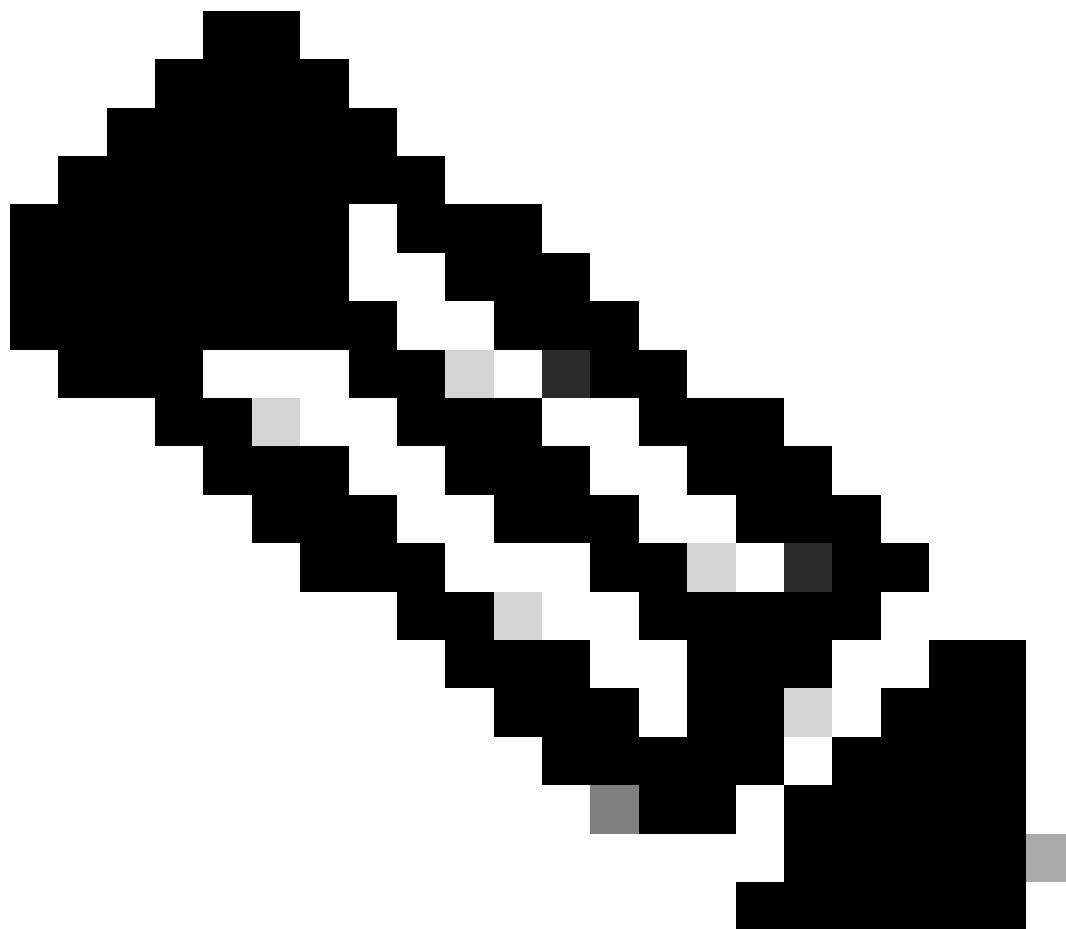
2. Klik op de knop Toevoegen op de pagina.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The top navigation bar includes Deployment, Licensing, Certificates (selected), Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area is titled 'Certificate Templates' and features a table with columns: Template Name, Description, Key Type, Key Size, and Curve Type. The table lists three templates: CA_SERVICE_Certificate_Template, EAP_Authentication_Certificate_Tem..., and pxGrid_Certificate_Template. Above the table, there are buttons for Edit, Add (highlighted with a red box), Duplicate, and Delete.

3. Vul de gegevens in die zijn afgestemd op de specifieke behoeften van uw organisatie.

The screenshot shows the 'Add Certificate Template' form in the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar and top navigation bar are the same as in the previous screenshot. The main content area is titled 'Add Certificate Template' and contains the following fields: * Name, Description, Subject (Common Name (CN) with a dropdown menu showing '\$UserName\$'), Organizational Unit (OU), Organization (O), City (L), State (ST), Country (C), Subject Alternative Name (SAN) (with a dropdown menu showing 'MAC Address'), Key Type (RSA), Key Size (2048), * SCEP RA Profile (ISE Internal CA), Valid Period (3652 days, with a note 'Valid Range 1 - 3652'), and Extended Key Usage (Client Authentication checked, Server Authentication unchecked). At the bottom right, there are 'Submit' and 'Cancel' buttons.

4. Klik op Indienen om de wijzigingen op te slaan.



Opmerking: De certificaatsjabloon kan nuttig zijn in een scenario wanneer u verschillende domeinen hebt en de gebruiker segmenteert door een andere waarde toe te voegen in de OE van het certificaat.

Een endpointprofiel toewijzen aan de client-provisioningportal

1. Navigeren naar werkcentra > BYOD > Clientprovisioning > Clientprovisioningbeleid.
2. Klik op v.n van de regels om een nieuwe regel voor clientprovisioning te maken.

Client Provisioning Policy

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 CiscoISE: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

3. Plaats de nieuwe regel op de pagina

4. Voeg de identiteitsgroep toe als u bepaalde gebruikers wilt beperken om het BYOD-portaal te gebruiken

5. Voeg het besturingssysteem toe dat u toegang wilt hebben tot het BYOD-portaal

6. Breng de Cisco IOS-versie uit de vervolgkeuzelijst in kaart en selecteer ook het eindpuntprofiel dat u op basis van het resultaat hebt gemaakt

Client Provisioning Policy

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 CiscoISE:ExternalGroups EQUALS ITSLMY:ITSLDomain.com/Users/Domain Users	then AnyConnect5.1
BYOD	If Any	and Windows All	and Condition(s)	then Result
iOS	If Any	and Apple iOS All	and Condition(s)	then
Android	If Any	and Android	and Condition(s)	then

Agent Configuration

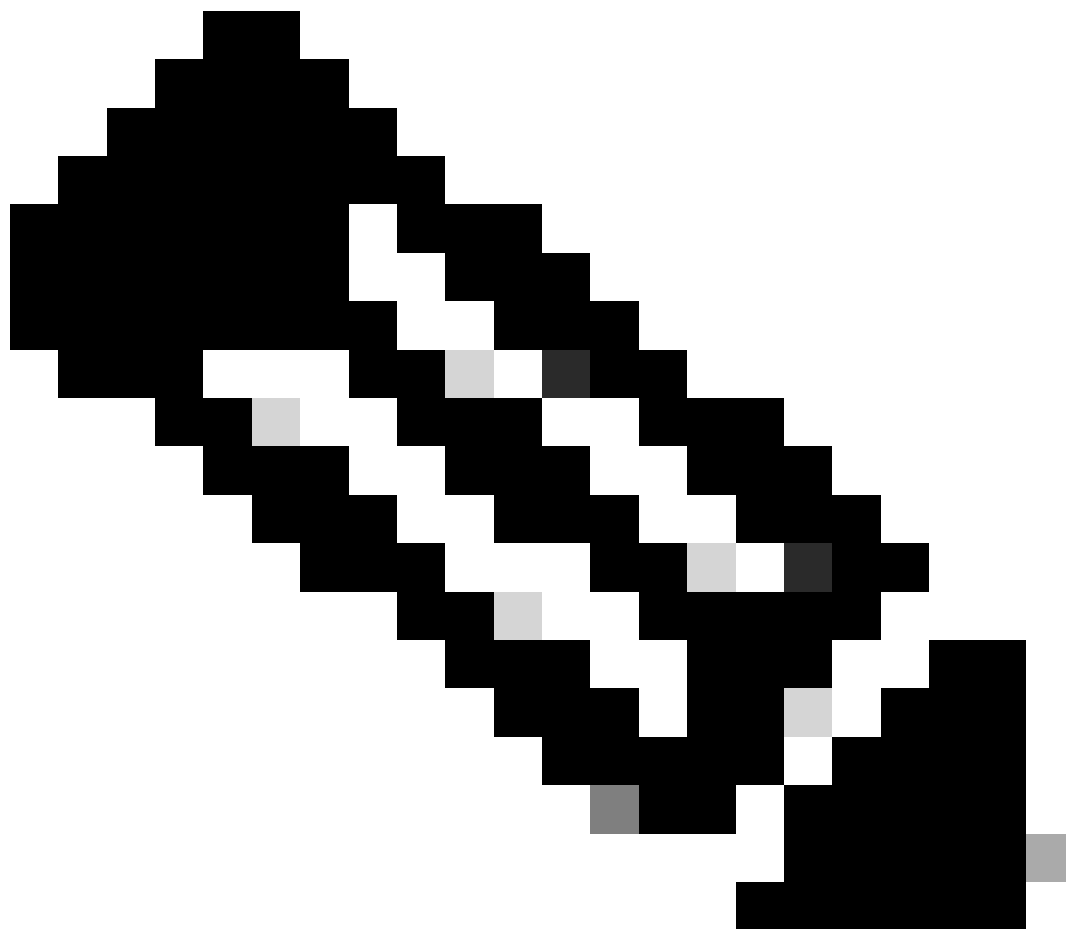
Choose an Agent: Is Upgrade Mandatory: ☐

Native Supplicant Configuration

WinSPWizard 3.2.0.1

Cisco-ISE-NSP

7. Klik op Gereed en vervolgens op de knop Opslaan.



Opmerking: Dit beleid heeft invloed op zowel postuur client provisioning en BYOD provisioning, waar de Agent Configuration sectie bepaalt de postuur agent en compliance module afgedwongen voor postuur controles, terwijl de Native Supplicant Configuration sectie instellingen beheert voor BYOD provisioning stromen

Configureer ISE-beleidssets voor één SSID-BYOD

1. Navigeren naar Policy > Policy Set en een beleid maken voor BYOD flow op 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. Navigeer vervolgens naar Beheer > Identity Management > Externe Identiteitsbronnen > Certificaatverificatieprofiel. Klik op de knop Add om het certificaatprofiel te maken:

Identity Services Engine Administration / Identity Management

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Identities Groups External Identity Sources Identity Source Sequences Settings

External Identity Sources

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

Certificate Authentication Profile

Edit Add Duplicate Delete

Name	Description
Preloaded_Certificate_Profile	Precreated Certificate Authorization Profile.

Identity Services Engine Administration / Identity Management Evaluation Mode 63 Days

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Identities Groups External Identity Sources Identity Source Sequences Settings

External Identity Sources

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

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name BYOD

Description

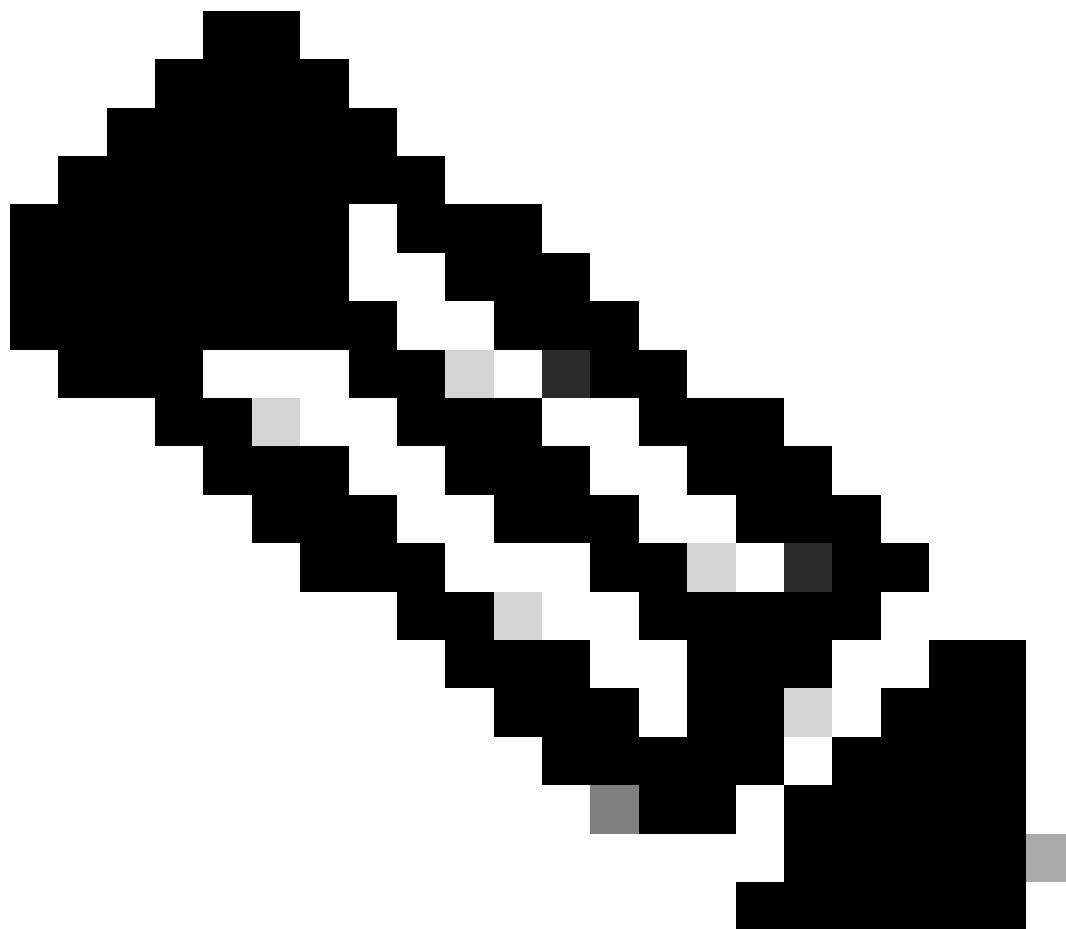
Identity Store [not applicable]

Use Identity From Certificate Attribute Subject - Common Name

Match Client Certificate Against Certificate In Identity Store

Never Only to resolve identity ambiguity Always perform binary comparison

Submit Cancel



Opmerking: In de Identity Store kunt u altijd uw Active Directory selecteren die is geïntegreerd in ISE om een gebruikersraadpleging uit te voeren vanuit het certificaat voor extra beveiliging.

3. Klik op **Indienen** om de configuratie op te slaan. Vervolgens brengt u het certificaatprofiel in kaart met de beleidsset voor BYOD:

4. Het autorisatieprofiel voor BYOD-omleiding en volledige toegang na de BYOD-stroom configureren. Navigeer naar **Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen**.

5. Klik op **Add** en maak een autorisatieprofiel aan. Controleer de webomleiding (CWA, MDM, NSP, CPP) en breng de pagina van het BYOD-portaal in kaart. Voeg ook de Redirectie ACL-naam van WLC toe aan het profiel. Voor het volledige toegangsprofiel configureer je een vergunningstoegang met het betreffende zakelijke VLAN in het profiel.

6. Het autorisatieprofiel in kaart brengen aan de autorisatieregel. De BYOD volledige toegang moet de regel EndPoints·BYOD registratie gelijk ja hebben, zodat de gebruiker volledige toegang krijgt tot het netwerk na de BYOD-stroom.

Identity Services Engine Policy / Policy Sets Evaluation Mode 62 Days

Policy Sets → BYOD

Reset Reset Policy Set Hit Counts Save

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

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

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

Configureer ISE-beleidssets voor Dual SSID BYOD

In Dual SSID BYOD configuratie, wordt de twee-beleid set geconfigureerd op ISE. De eerste beleidsset is voor de open/onbeveiligde SSID, waar de Policy Set-configuratie de gebruiker omleidt naar de BYOD-pagina bij het verbinden met de open/onbeveiligde SSID

1. Ga naar Policy > Policy Set en maak een Policy voor BYOD-flow op ISE.
2. Maak een Policy set voor de Open/Unsecure SSID en Corporate SSID die de geregistreerde BYOD-gebruiker op ISE authenticceert.

Policy Sets

Reset Reset Policy Set Hit Counts Save

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		

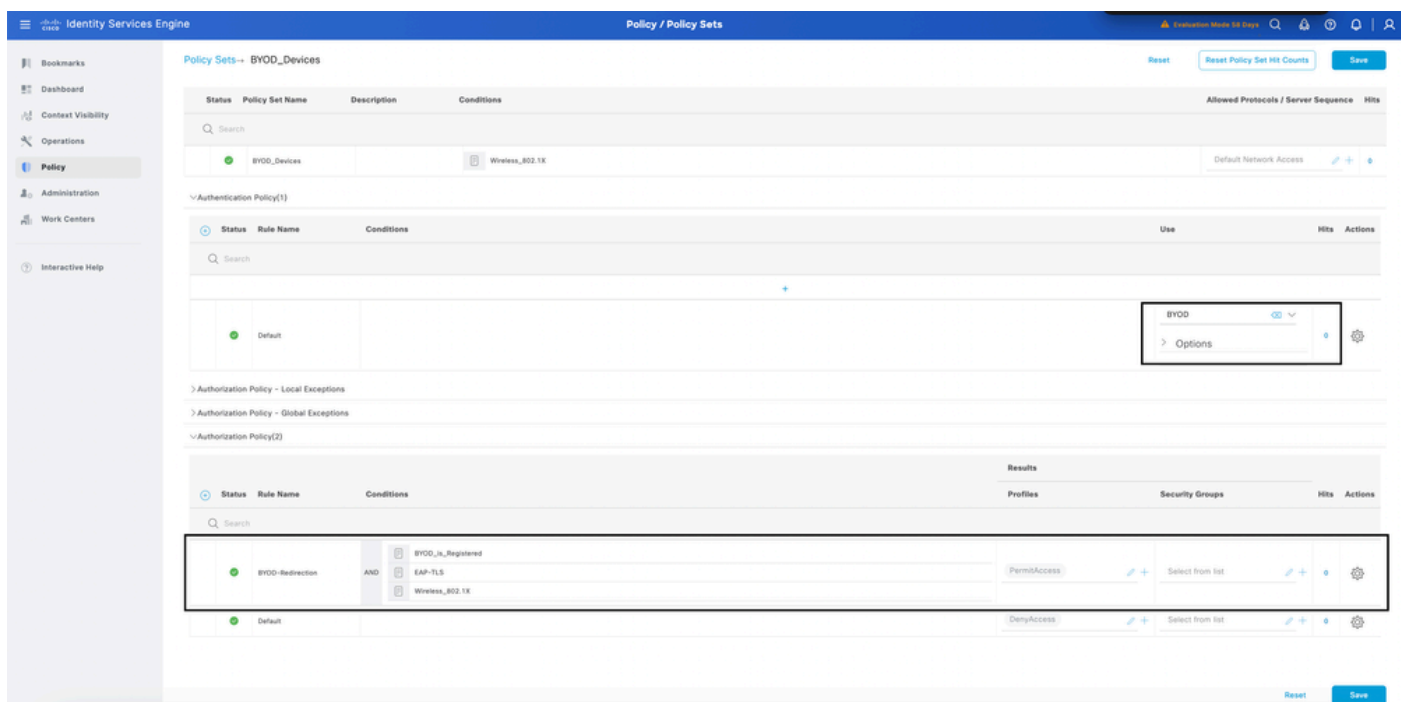
Reset Save

3. Zoek in de reeks Onboarding Policy de optie Doorgaan onder de opties. Voor het autorisatiebeleid moet u een voorwaarde maken en het omleidingsautorisatieprofiel toewijzen. Dezelfde stappen zijn nodig bij het opstellen van het vergunningsprofiel, dat onder punt 4 kan worden gevonden.



4. In de BYOD Registered Policy Set moet u het verificatiebeleid configureren met hetzelfde certificaatprofiel als u hebt gevonden.

in het configureren van ISE Policy Sets voor Single SSID BYOD in punt 2. Maak ook een voorwaarde voor autorisatiebeleid en breng het volledige toegangsprofiel in kaart met het beleid.



Logboekregistratie

Vanuit het live-logbestand van ISE zou de gebruikersverificatie succesvol zijn en worden doorgestuurd naar de BYOD Portal-pagina. Na voltooiing van de BYOD-stroom, zou de gebruiker toegang tot het netwerk moeten verlenen

↶ 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...	

CISCO

test

BYOD Portal

123

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

Nadat u op de knop Volgende hebt geklikt, wordt u naar een pagina geleid waar de gebruiker wordt gevraagd de naam van het apparaat en de beschrijving in te voeren

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 a user profile 'test' 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.

Plaats dat de gebruiker wordt gevraagd om het Network Assistant-programma te downloaden voor het downloaden van het Endpoint-profiel en het EAP TLS-certificaat voor verificatie als het profiel is geconfigureerd voor het uitvoeren van EAP-TLS-verificatie

The screenshot shows the next step in the Cisco BYOD Portal, titled 'Install'. The progress indicator now shows step 3 as the active step, highlighted with a blue circle. The instruction reads: '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.' There is no visible button or action on this screen.

Voer de Network Assistant-toepassing uit met beheerdersrechten en klik op de knop Start om het onboarding te starten:



Network Setup Assistant

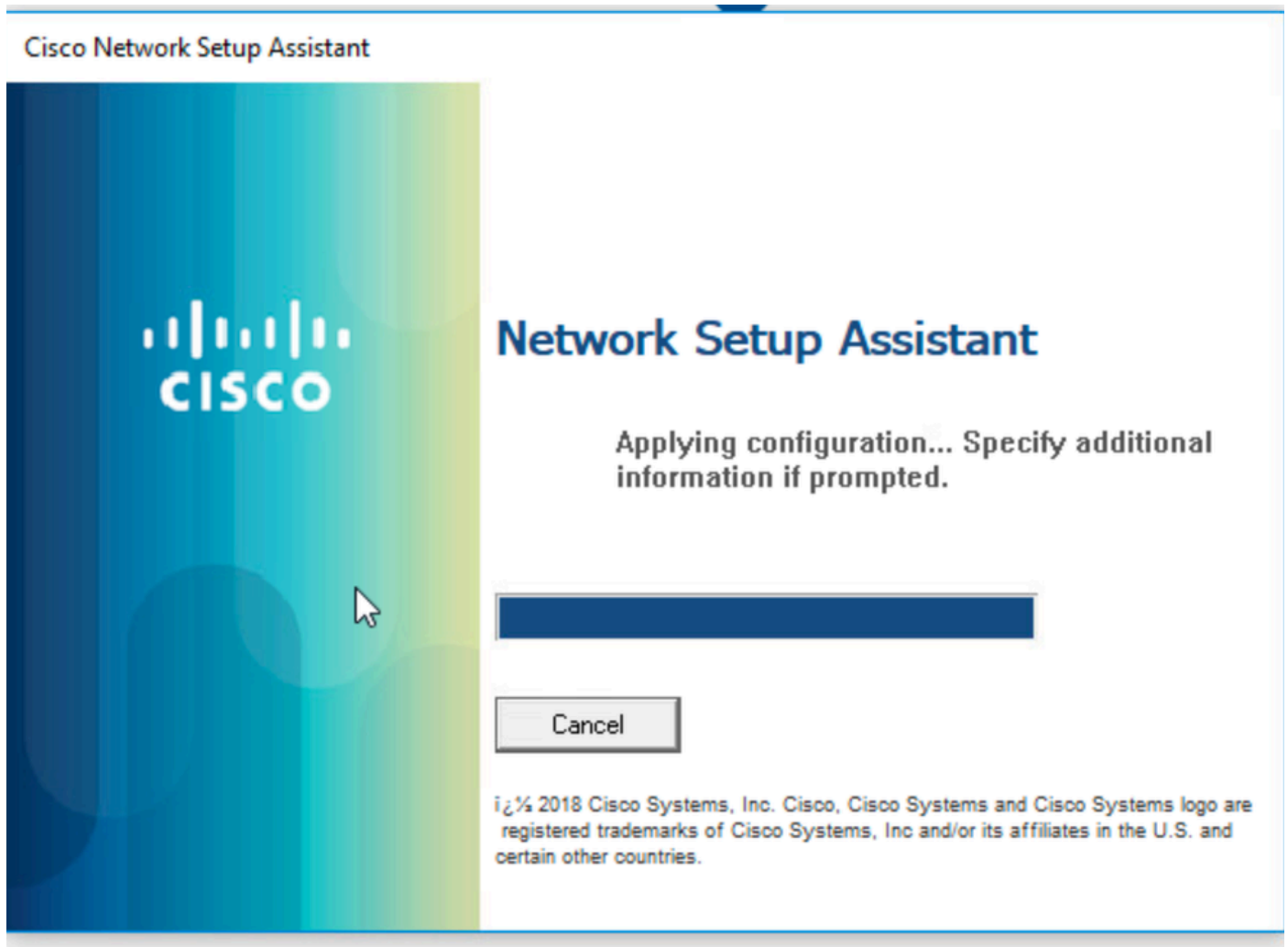


This application automatically configures network settings.

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.



De gebruiker is met succes op het netwerk met hun persoonlijk apparaat aan boord gegaan om tot de middelen toegang te hebben.

Probleemoplossing

Als u het probleem met BYOD wilt oplossen, schakelt u deze debug in op ISE

Kenmerken die moeten worden ingesteld om debug niveau:

- client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (poortserver.log)
- nsf (ise-psc.log)
- nsf-sessie (ise-psc.log)
- profiler (profiler.log)

Logfragment

Gastenlogboeken

Deze logbestanden geven aan dat de gebruiker met succes naar de pagina is doorgestuurd en de Network Assistant-toepassing heeft gedownload:

```
2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-
kartering gevonden in actie-forwards, doorsturen naar: pages/byodWelcome.jsp // De
welkomstpagina van BYOD
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:- Grootte
van pTranStappen: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, pTranStps:[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:d2513b IE-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.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-
kartering pad gevonden in actie-forwards, doorsturen naar: 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:- Grootte
van pTranStappen: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, pTranStps:[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:f203b7 7-9e8a-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.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-
kartering pad gevonden in actie-forwards, doorsturen naar: 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.StreamingServlet -:0000000000000000B30D59CC5:::- Session = 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:::-
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 // De netwerk bijstandsaplicatie is naar het netwerk
verzonden
```


ISE-PSC-logbestanden

Aangezien de toepassing aan het eindpunt wordt gedownload, stelt de toepassing een stroom SCEP in werking om het cliëntcertificaat van ISE te krijgen.

```
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- CertStore bevat 4 certificaat(s):
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1. "[issuer=CN=Certificate Services Root CA - iseguest;
seriële=32281512738768960628252532784663302089]"
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 2. "[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest; seriële=131900858749761727853768227590303808637]"
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 3. "[issuer=CN=Certificate Services Root CA - iseguest;
seriële=68627620160586308685849818775100698224]"
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 4. "[issuer=CN=Certificate Services Node CA - iseguest;
seriële=72934767698603097153932482227548874953]"
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selecteren van encryptie certificaat
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Certificaat selecteren met sleutelEncipherment
keyGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Gevonden 1 certificaat(en) met keyEncipherment
keyGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Gebruik [issuer=CN=Certificate Services Endpoint Sub
CA - Inquest; seriële=131900858749761727853768227590303808637] voor berichtversleuteling
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selecteren van verificateur certificaat
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Certificaat selecteren met digitaleHandtekening
sleutelGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Gevonden 1 certificaat(en) met digitaleSignature
sleutelGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Gebruik [issuer=CN=Certificate Services Endpoint Sub
CA - Inquest; seriële=131900858749761727853768227590303808637] voor berichtverificatie
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selecteren van emittentencertificaat
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Certificaat selecteren met basisBeperkingen
```

2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Gevonden 3 certificaat(s) met basisBeperkingen
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Gebruik [issuer=CN=Certificate Services Endpoint Sub
CA - Inquest; seriële=131900858749761727853768227590303808637] voor de emittent
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- SCEP servers prestatie maatstaven:
naam[levend/dood, totale vereisten, totale mislukkingen, inflight-vereisten, gemiddelde RTT]
<http://127.0.0.1:9444/caservice/scep/live,96444,1,0,120>

Downloaden van endpointprofiel

Nadat het SCEP-proces is voltooid en het eindpunt het certificaat installeert, downloadt de toepassing het eindpuntprofiel voor toekomstige verificatie die door het apparaat zou worden uitgevoerd:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Refferer = Windows // Het Windows-apparaat is gedetecteerd op basis van de webpagina
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 0000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 0000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Voorziening nsp profiel
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Session = 0000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionID = null
2025-02-24 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//Het NSP profiel wordt gedownload naar het eindpunt
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming naar ip: bestandstype: NativeSPP-
bestandsnaam:Cisco-ISE-NSP.xml //The Network Assistant-toepassing
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- userID is ingesteld om te testen
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- omleiden type is: SUCCESS_PAGE, omleiden
url is: mac:

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.