Single SSID Wireless BYOD op Windows en ISE configureren

Inhoud

Inleiding

Dit document beschrijft hoe u uw eigen apparaat (BYOD) kunt configureren op Cisco Identity Services Engine (ISE) voor Windows-machine met zowel Single-SSID als Dual-SSID.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Cisco ISE versies 3.0
- Configuratie van Cisco WLC
- BYOD

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.0
- Windows 10
- WLC en AP

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Theorie

In Single SSID BYOD wordt slechts één SSID gebruikt voor zowel het installeren van apparaten als het later volledig toegankelijk maken van de geregistreerde apparaten. Eerst sluit de gebruiker zich aan op SSID met behulp van de gebruikersnaam en het wachtwoord (MSCHAPv2). Zodra deze op ISE is geauthentiseerd, wordt de gebruiker opnieuw naar het BYOD Portal verwezen. Zodra de Apparaatregistratie is uitgevoerd, downloads de Native Supplicant Assistant (NSA) van ISE. NSA wordt geïnstalleerd op de eindclient en downloads van het profiel en certificaat vanaf ISE. De NSA vormt de draadloze leverancier en de client installeert het certificaat. Endpoint voert een andere verificatie uit aan dezelfde SSID met behulp van het gedownload certificaat met behulp van EAP-TLS. ISE controleert het nieuwe verzoek van de cliënt en verifieert de MAP-methode en de apparaatregistratie en geeft volledige toegang tot het apparaat.

Windows BYOD Enkelvoudige SSID’s

- Oorspronkelijke EAP-MSCHAPv2-authenticatie
- Omleiding naar het BYOD-portaal
- Apparaatregistratie
- NSA-download
- Profieldownload
- Downloaden van certificaten
- EAP-TLS-verificatie

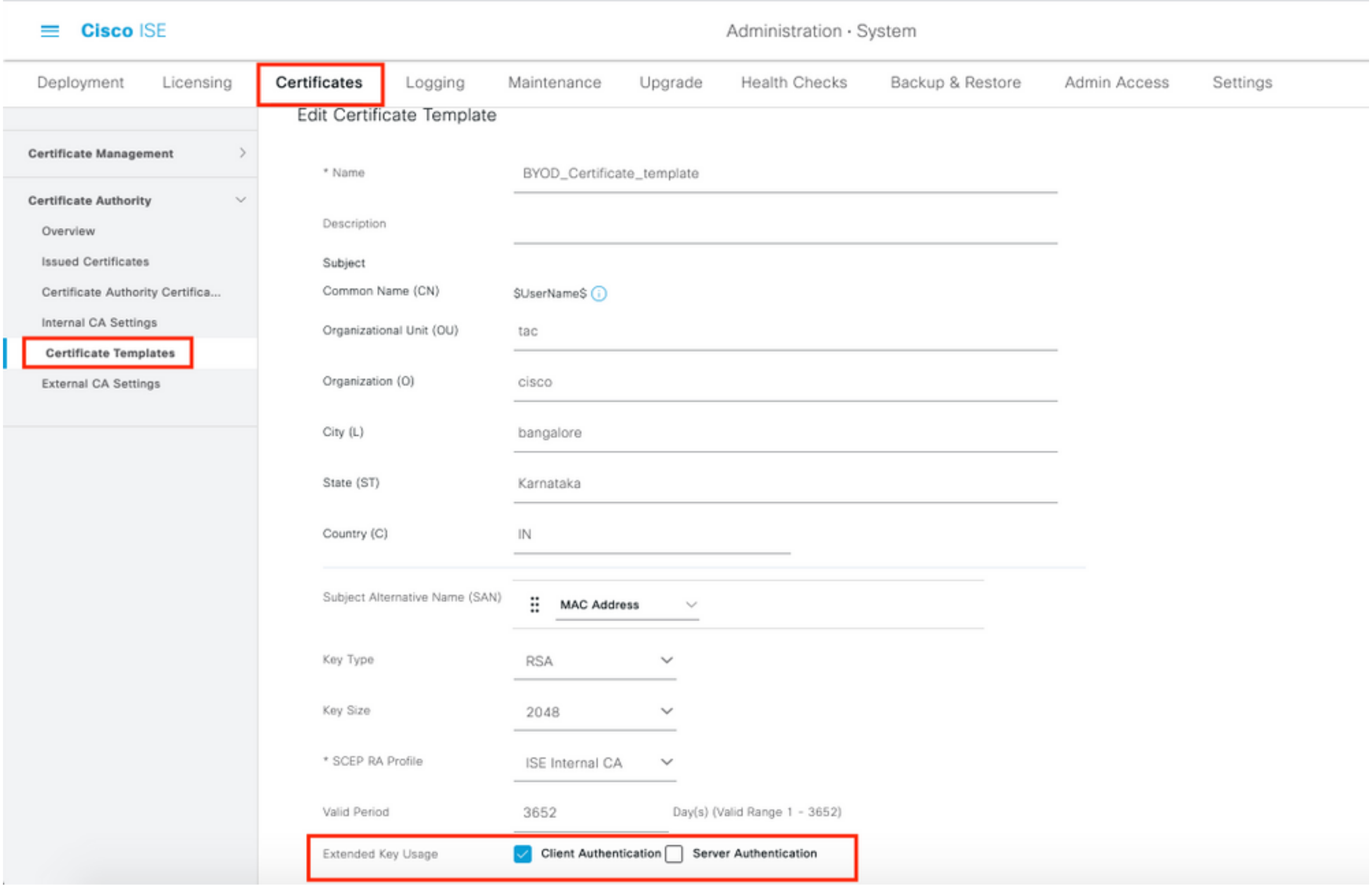
Configureren

ISE-configuratie

Stap 1. Voeg het netwerkapparaat toe op ISE en vorm RADIUS en gedeelde toets.

Navigeer in op **ISE > Administration > Network Devices > Add Network Devices**.

Stap 2. Maak een certificaatsjabloon voor BYOD-gebruikers. De sjabloon moet zijn voorzien van een uitgebreid gebruik van clientverificatie. U kunt de standaard EAP_certificaatsjabloon gebruiken.



Edit Certificate Template

* Name: BYOD_Certificate_template

Description:

Subject

Common Name (CN): $UserName$

Organizational Unit (OU): tac

Organization (O): cisco

City (L): bangalore

State (ST): Karnataka

Country (C): IN

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)

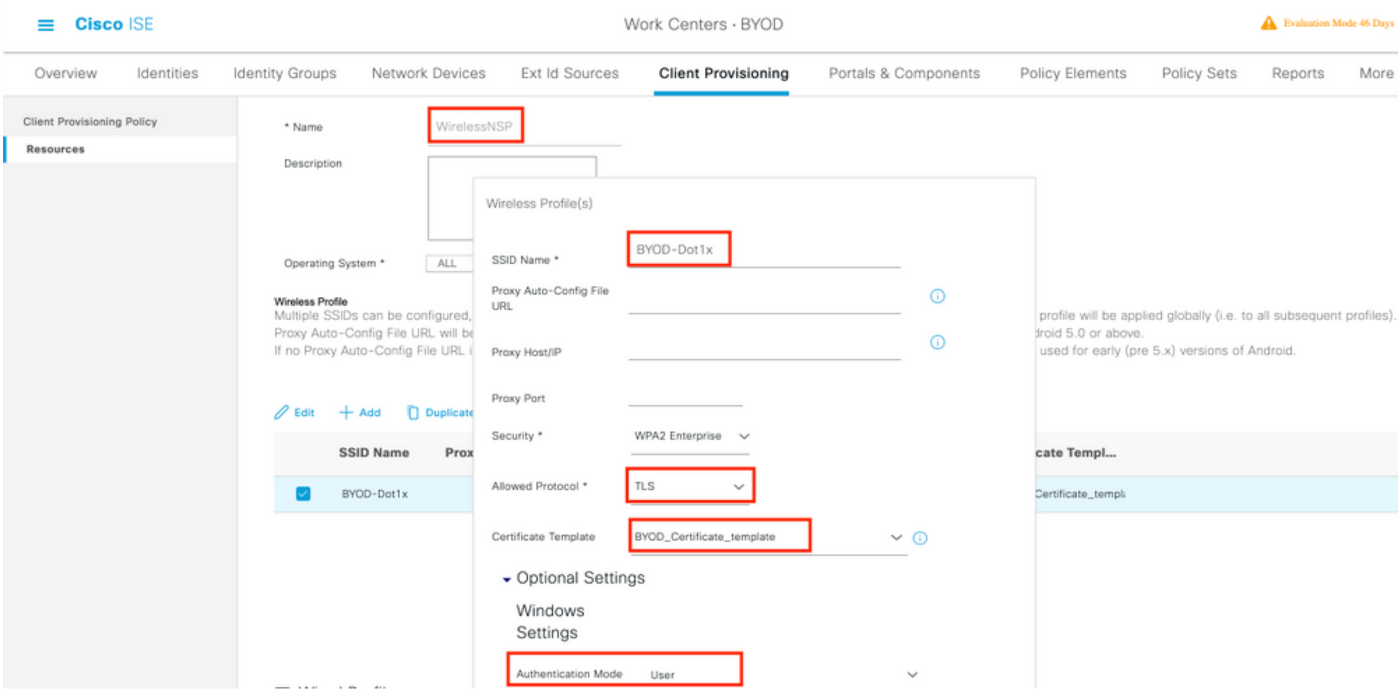
Extended Key Usage: ☑ Client Authentication □ Server Authentication

Stap 3. Maak een standaard flexibel profiel voor een draadloos profiel.

Navigeer naar **ISE > Workcenters > BYOD > Clientprovisioning**. Klik op **Add** en kies **Native Supply Profile (NSP**) uit de vervolgkeuzelijst.

Hier moet de naam van SSID hetzelfde zijn als u verbonden bent voordat u één SSID BYOD doet. Selecteer het Protocol als TLS. Selecteer de certificaatsjabloon zoals deze in de vorige stap is gemaakt, of u kunt de standaard EAP_certificaatsjabloon gebruiken.

Selecteer onder optionele instellingen de gebruiker of User en Machine verificatie volgens uw vereisten. In dit voorbeeld wordt het ingesteld als gebruikersverificatie. Laat andere instellingen standaard staan.



* Name: WirelessNSP

Description

Operating System *: ALL

Wireless Profile
Multiple SSIDs can be configured, ... profile will be applied globally (i.e. to all subsequent profiles).
Proxy Auto-Config File URL will be ...roid 5.0 or above.
If no Proxy Auto-Config File URL i... used for early (pre 5.x) versions of Android.

SSID Name	Prox...	...cate Templ...
☑ BYOD-Dot1x		Certificate_templ...

Wireless Profile(s)

SSID Name *: BYOD-Dot1x

Proxy Auto-Config File URL:

Proxy Host/IP:

Proxy Port:

Security *: WPA2 Enterprise

Allowed Protocol *: TLS

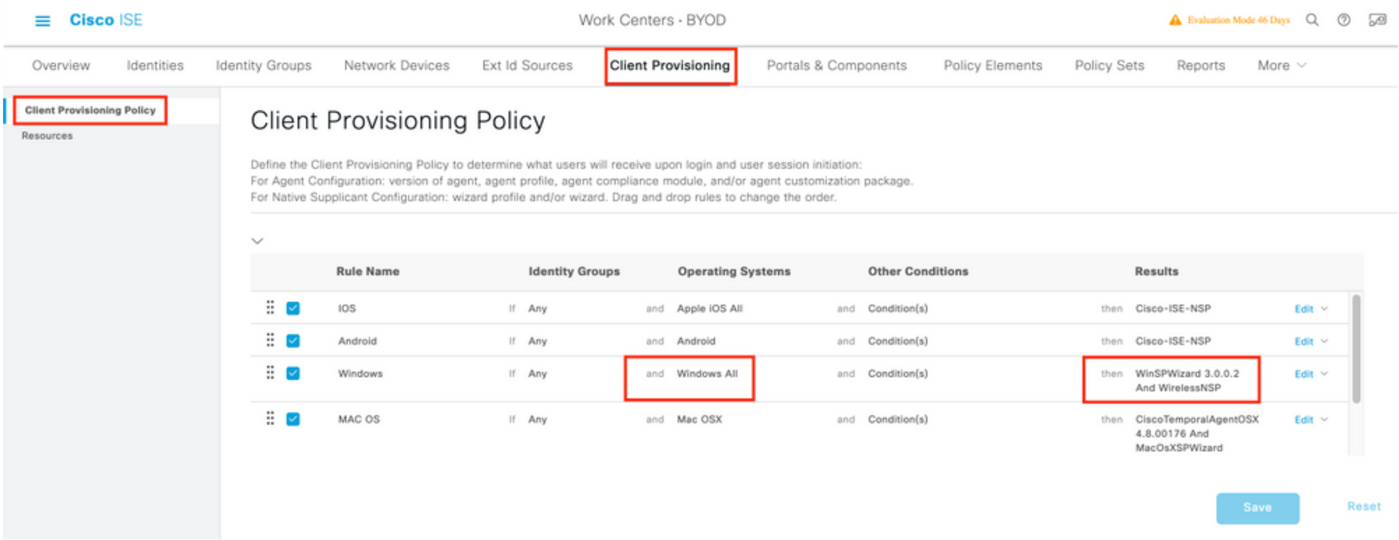
Certificate Template: BYOD_Certificate_template

Windows Settings

Authentication Mode: User

Stap 4. Maak clientprovisioningbeleid voor Windows-apparaat.

Navigatie naar **ISE > Workcenters > BYOD > Clientprovisioning > Clientprovisioningbeleid**. Selecteer het besturingssysteem als **Windows ALLE**. Selecteer **WinSPWizard 3.0.0.2 en NSP** die in de vorige stap zijn gemaakt.



Client Provisioning Policy

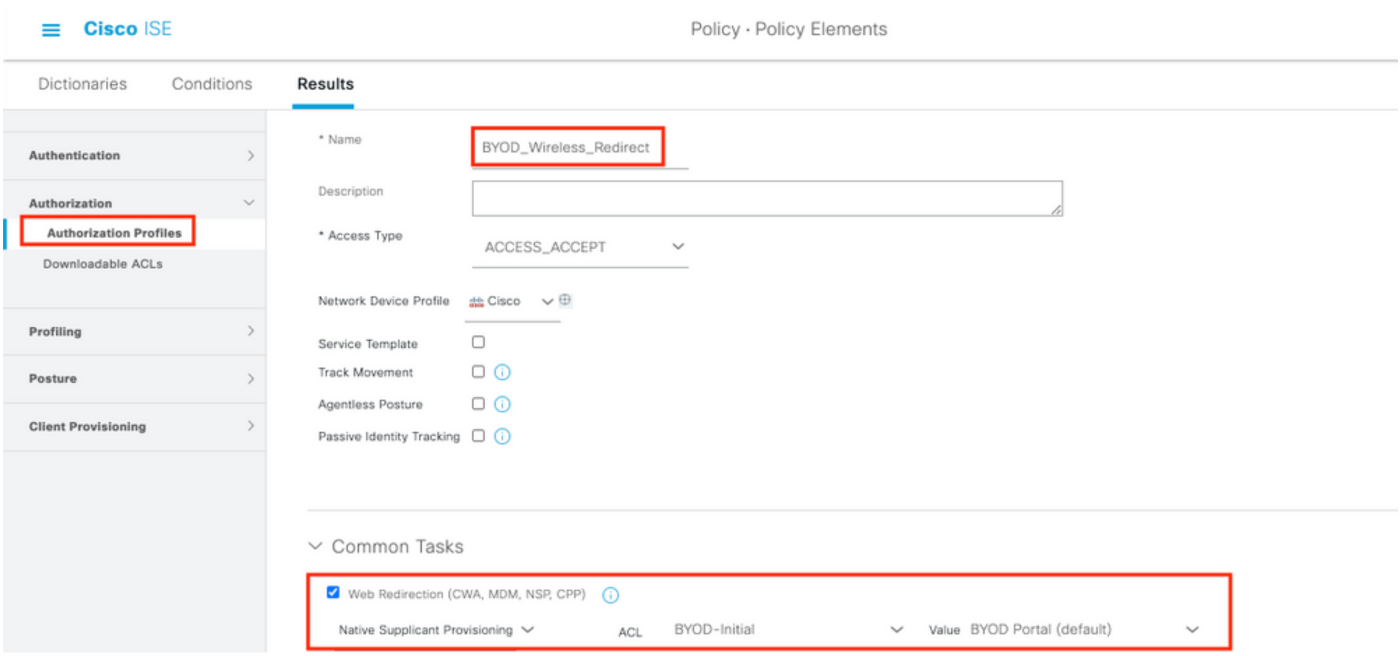
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.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

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP	Edit
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	WinSPWizard 3.0.0.2 And WirelessNSP	Edit
☑	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	CiscoTemporalAgentOSX 4.8.00176 And MacOsXSPWizard	Edit

Stap 5. Maak een **vergunningsprofiel** voor apparaten die niet als BYOD-apparaten zijn geregistreerd.

Navigeren in op **ISE > Policy > Policy Elementen > Resultaten > > Authorificatie > autorisatieprofielen > Add**.

Selecteer onder **Gemeenschappelijke taak** de optie **Provisioning**. Definieer een ACL-naam (omleiden) die op WLC is gemaakt en selecteer de BYOD-portal. Hier wordt Default Portal gebruikt. U kunt een aangepaste BYOD-portal maken. Navigeer naar **ISE > Workcenters > BYOD > Portals** en onderdelen en klik op **Add**.



* Name: BYOD_Wireless_Redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

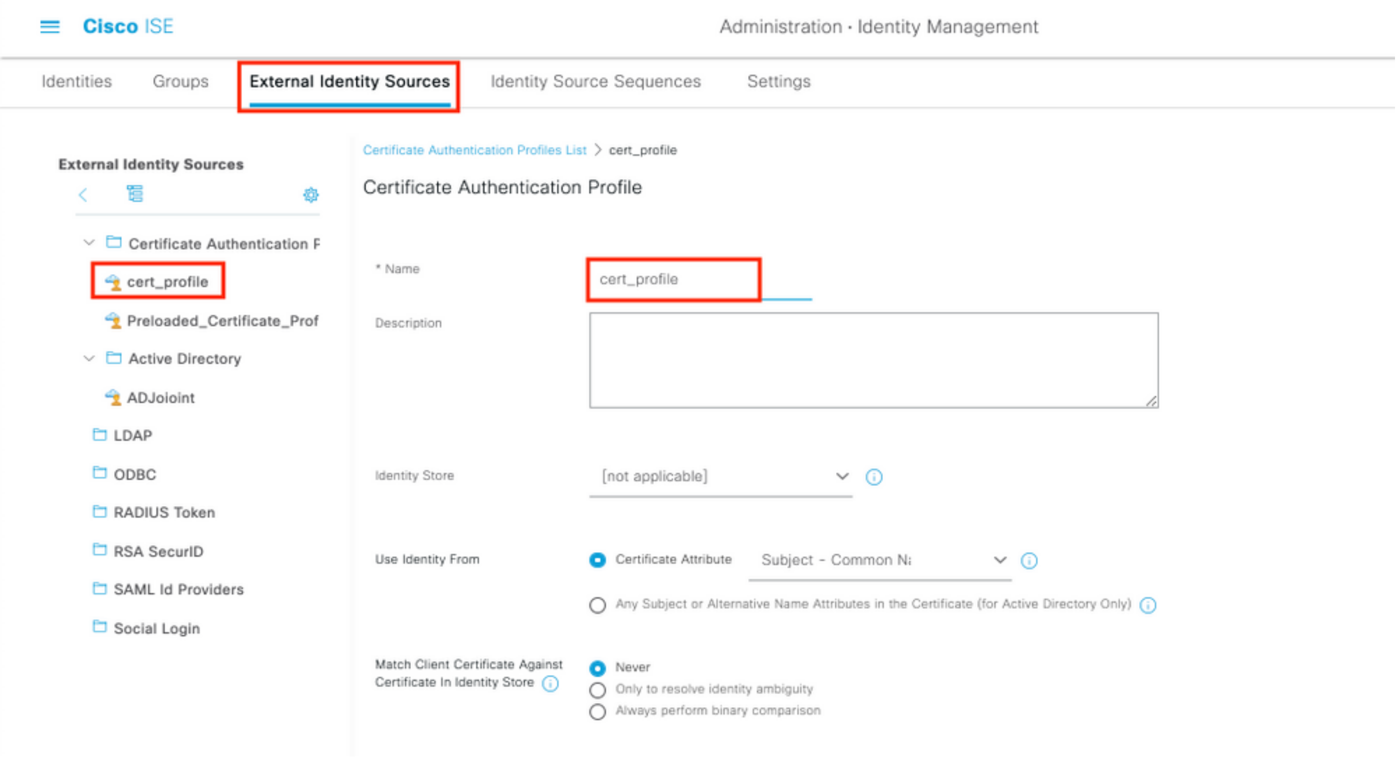
Common Tasks

☑ Web Redirection (CWA, MDM, NSP, CPP)

Native Supplicant Provisioning ACL BYOD-Initial Value BYOD Portal (default)

Stap 6. Maak een certificaatprofiel.

Navigeer naar **ISE > Administratie > Externe Identity Services > certificaatprofiel**. Maak hier een nieuw certificaatprofiel of gebruik het standaardcertificaatprofiel.


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication F
cert_profile
Preloaded_Certificate_Prof
Active Directory
ADJoioint
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
Certificate Authentication Profiles List > cert_profile

Certificate Authentication Profile

* Name: cert_profile

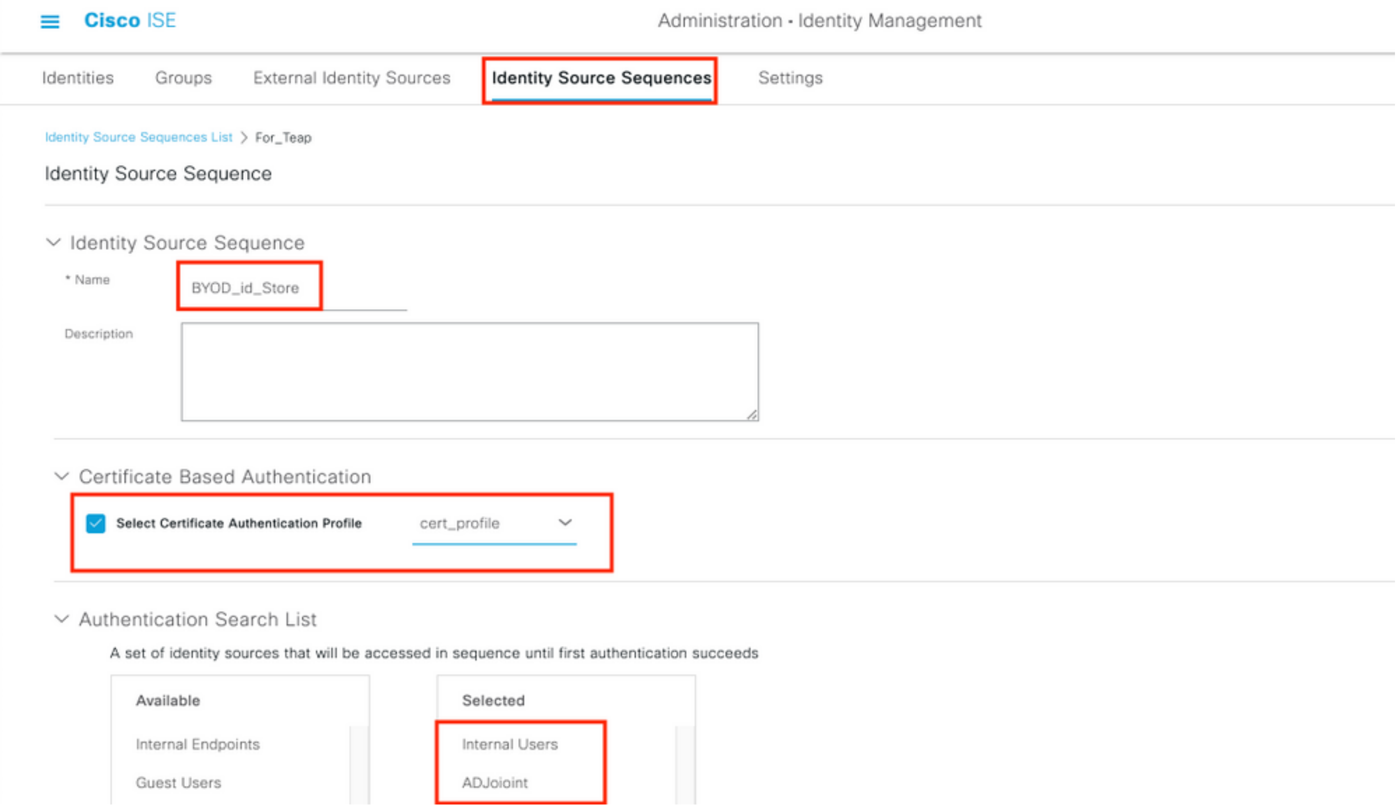
Description:

Identity Store: [not applicable]

Use Identity From: ● Certificate Attribute Subject - Common Na
○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store: ● Never
○ Only to resolve identity ambiguity
○ Always perform binary comparison

Stap 7. Maak een reeks van identiteitsbronnen en selecteer het certificeringsprofiel dat in de vorige stap is gemaakt of gebruik het standaardcertificaatprofiel. Dit is vereist wanneer gebruikers MAP-TLS uitvoeren na BYOD-registratie om volledige toegang te krijgen.


Cisco ISE
Administration • Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Source Sequences List > For_Teap
Identity Source Sequence
Identity Source Sequence
Certificate Based Authentication
Authentication Search List
Available
Internal Endpoints
Guest Users
Selected
Internal Users
ADJoioint

* Name: BYOD_id_Store

Description:

☑ Select Certificate Authentication Profile: cert_profile

A set of identity sources that will be accessed in sequence until first authentication succeeds

Stap 8. Maak een beleids-, verificatie- en autorisatiebeleid.

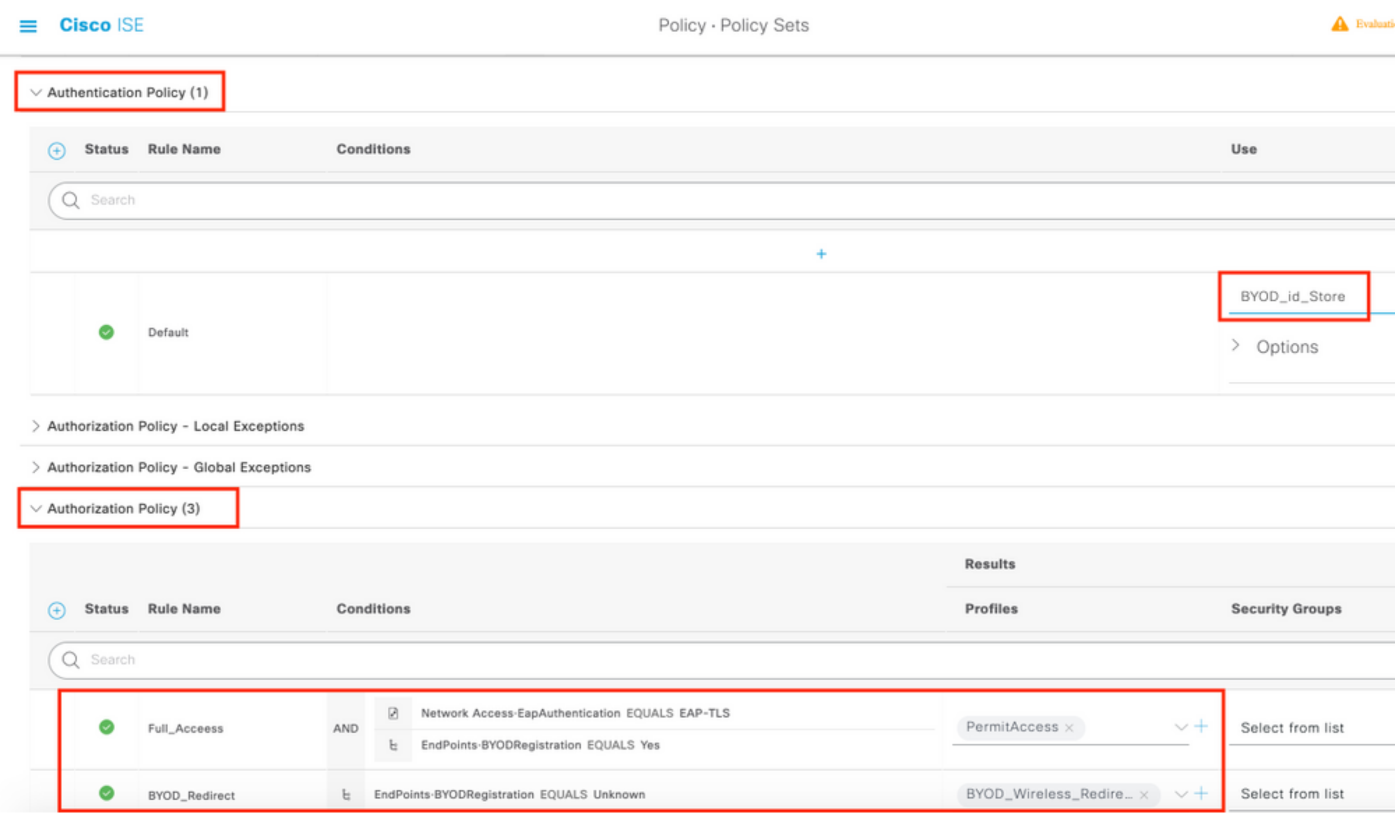
Navigeer naar **ISE > Policy > Policy Sets**. Een beleidsset maken en **opslaan**.

Maak een verificatiebeleid en selecteer de reeks van de identiteitsbron die in de vorige stap is gemaakt.

Maak een autorisatiebeleid. Je moet twee beleidslijnen uitstippelen.

1. Voor apparaten die niet zijn geregistreerd. Geef profiel omleiden dat is gemaakt in stap 5.

2. Apparaten die BYOD-geregistreerd zijn en MAP-TLS uitvoeren. Geef volledige toegang tot deze apparaten.



Authentication Policy (1)

Status	Rule Name	Conditions	Use
✓	Default		BYOD_id_Store Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

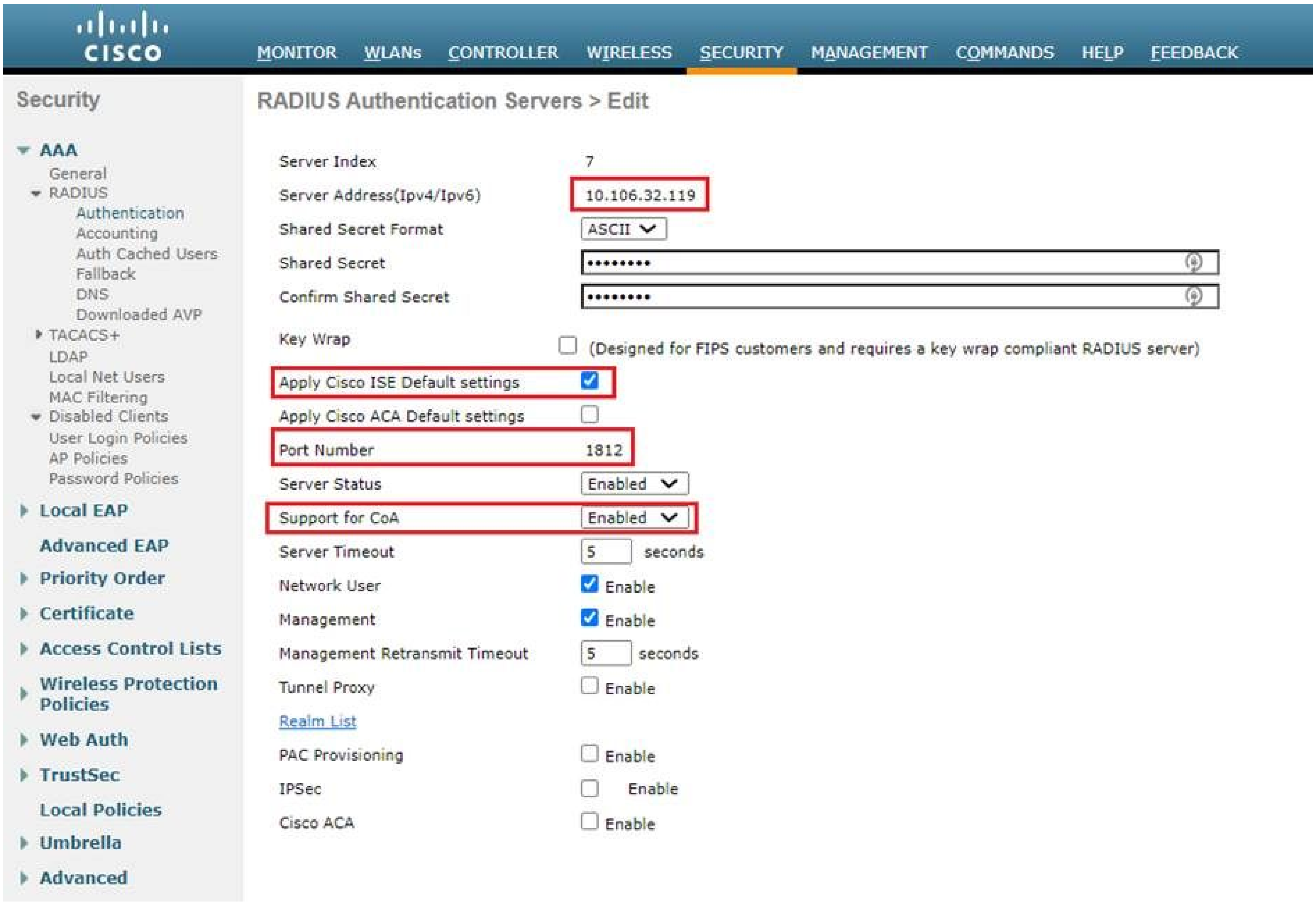
Authorization Policy (3)

Status	Rule Name	Conditions	Results: Profiles	Security Groups
✓	Full_Acceess	AND Network Access·EapAuthentication EQUALS EAP-TLS EndPoints·BYODRegistration EQUALS Yes	PermitAccess	Select from list
✓	BYOD_Redirect	EndPoints·BYODRegistration EQUALS Unknown	BYOD_Wireless_Redire...	Select from list

WLC-configuratie

Stap 1. Configureer de RADIUS-server op WLC.

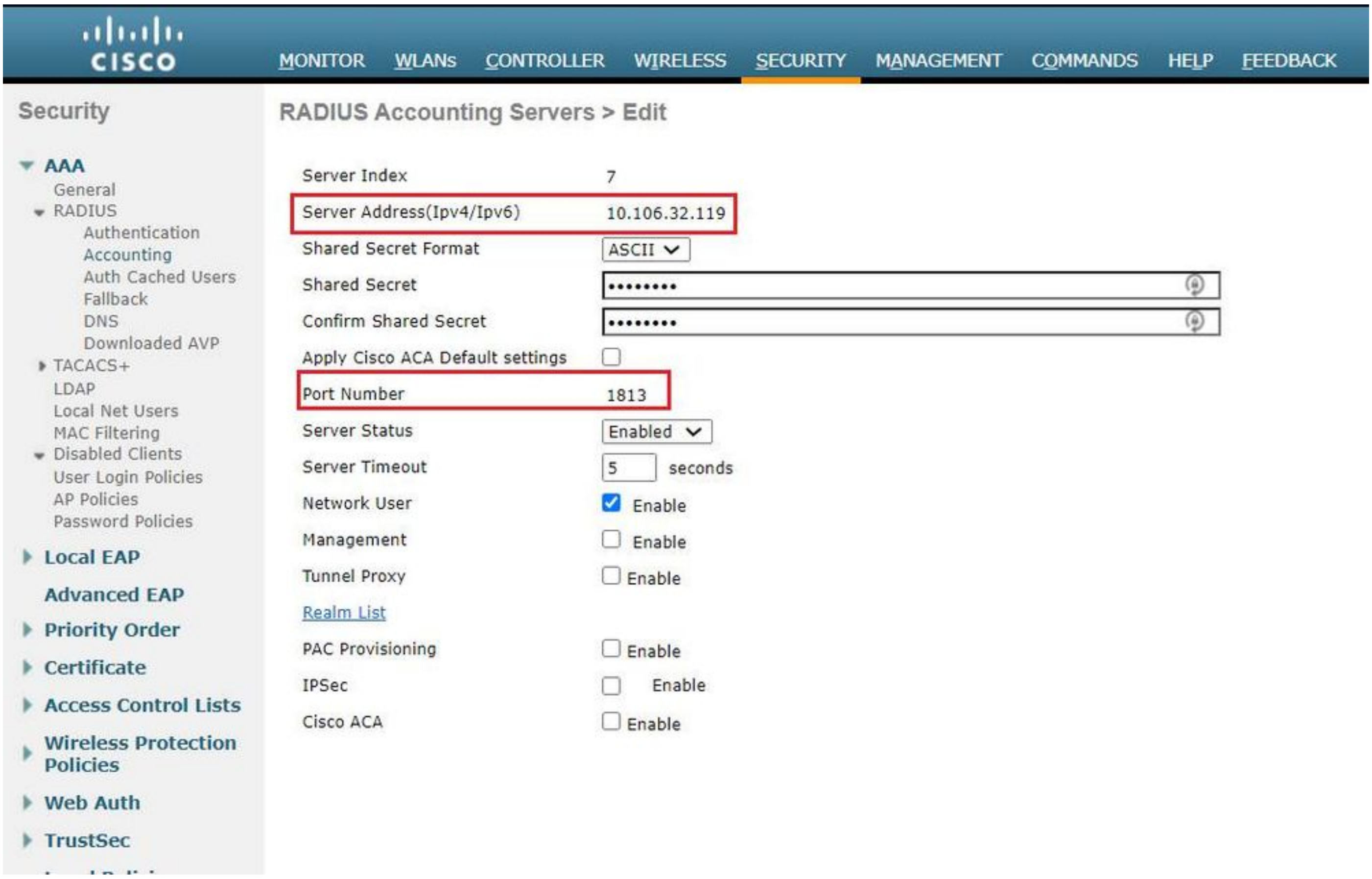
Navigeer naar **Security > AAA > Straal > Verificatie**.



RADIUS Authentication Servers > Edit

Server Index	7
Server Address(Ipv4/Ipv6)	10.106.32.119
Shared Secret Format	ASCII
Shared Secret	••••••••
Confirm Shared Secret	••••••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	☑
Apply Cisco ACA Default settings	□
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	5 seconds
Network User	☑ Enable
Management	☑ Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	□ Enable
Realm List	
PAC Provisioning	□ Enable
IPSec	□ Enable
Cisco ACA	□ Enable

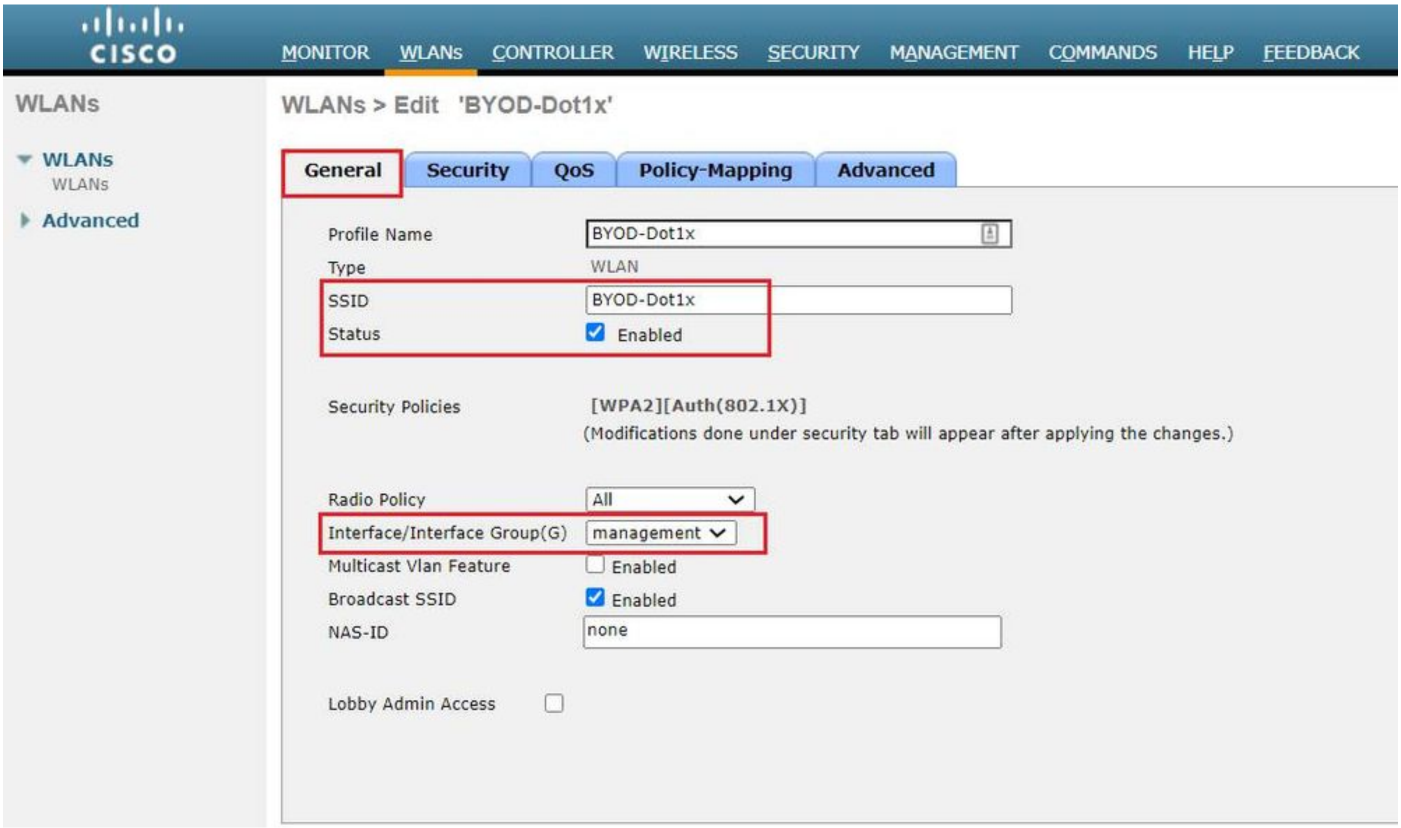
Navigeer in op **Security > AAA > Straal > Accounting**.



RADIUS Accounting Servers > Edit

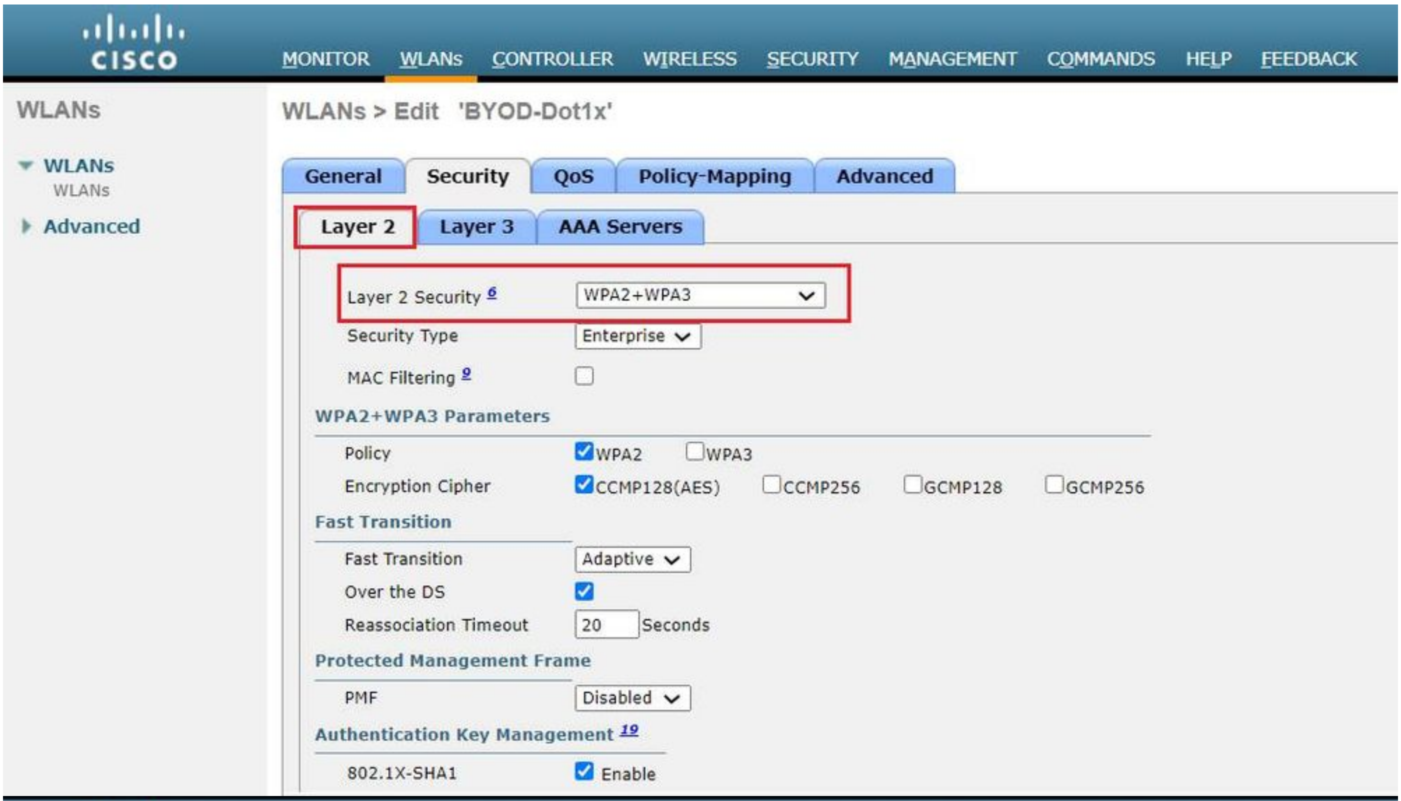
Server Index	7
Server Address(Ipv4/Ipv6)	10.106.32.119
Shared Secret Format	ASCII
Shared Secret	••••••••
Confirm Shared Secret	••••••••
Apply Cisco ACA Default settings	□
Port Number	1813
Server Status	Enabled
Server Timeout	5 seconds
Network User	☑ Enable
Management	□ Enable
Tunnel Proxy	□ Enable
Realm List	
PAC Provisioning	□ Enable
IPSec	□ Enable
Cisco ACA	□ Enable

Stap 2. Configureer een Dot1x SSID.



WLANs > Edit 'BYOD-Dot1x'

Profile Name	BYOD-Dot1x
Type	WLAN
SSID	BYOD-Dot1x
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none
Lobby Admin Access	□



WLANs > Edit 'BYOD-Dot1x'

Layer 2 Security [6]: WPA2+WPA3

Security Type: Enterprise

MAC Filtering [9]: □

WPA2+WPA3 Parameters

Policy: ☑ WPA2 □ WPA3

Encryption Cipher: ☑ CCMP128(AES) □ CCMP256 □ GCMP128 □ GCMP256

Fast Transition

Fast Transition: Adaptive

Over the DS: ☑

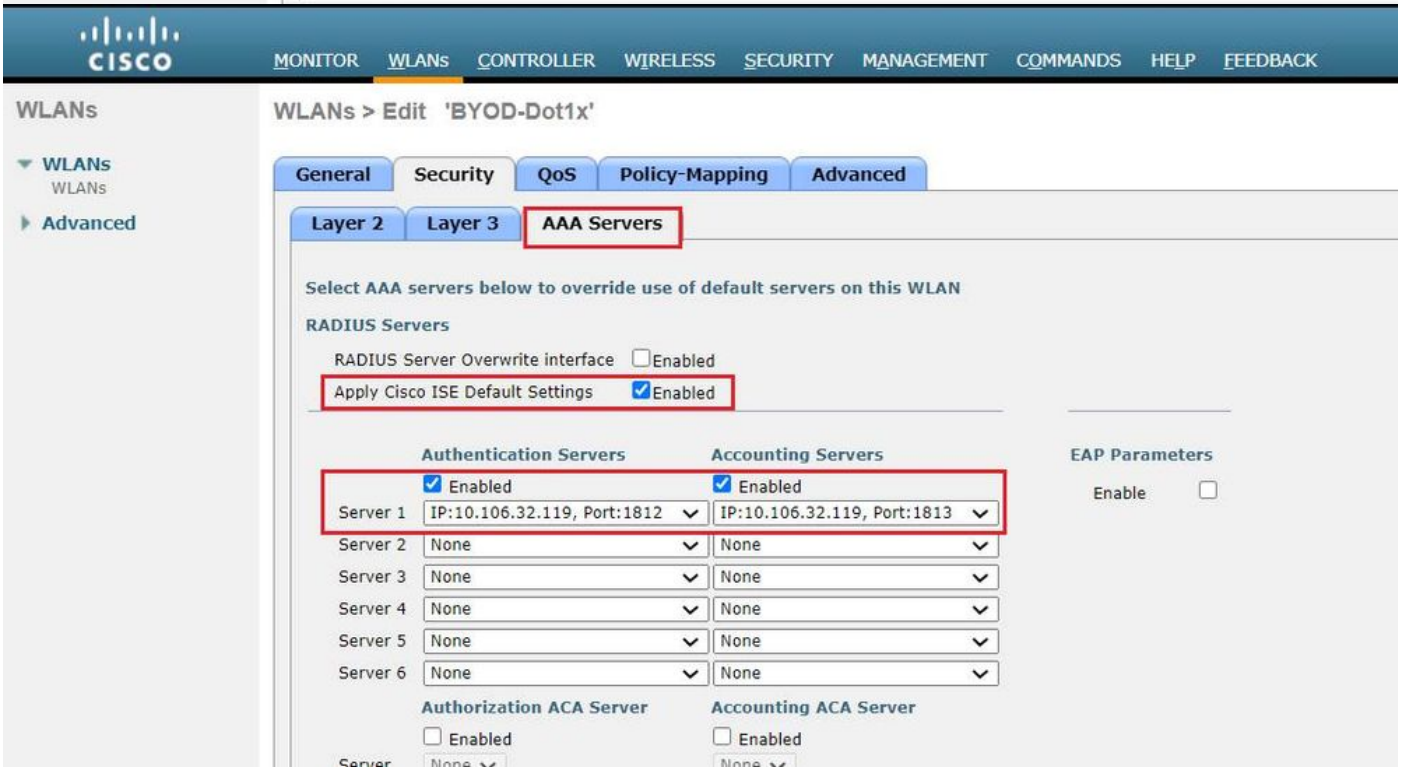
Reassociation Timeout: 20 Seconds

Protected Management Frame

PMF: Disabled

Authentication Key Management [19]

802.1X-SHA1: ☑ Enable



WLANs > Edit 'BYOD-Dot1x'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface: □ Enabled

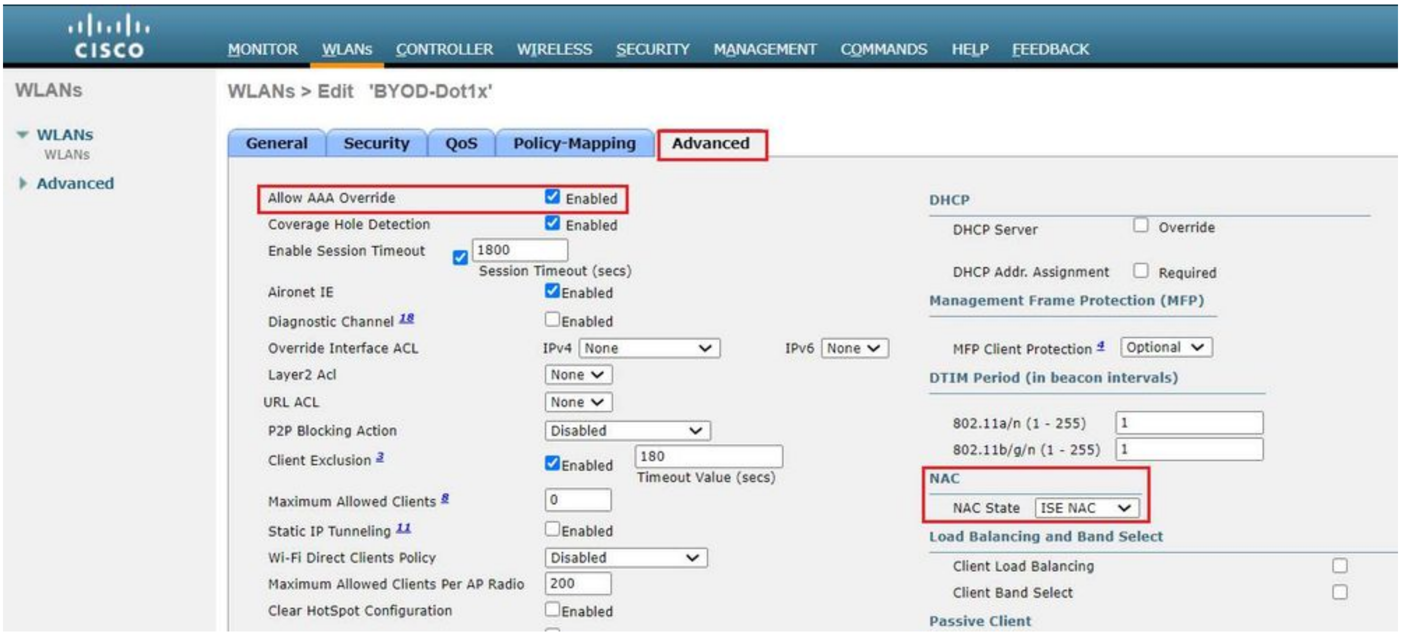
Apply Cisco ISE Default Settings: ☑ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.106.32.119, Port:1812	IP:10.106.32.119, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable: □

	Authorization ACA Server	Accounting ACA Server
	□ Enabled	□ Enabled
Server	None	None



WLANs > Edit 'BYOD-Dot1x'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel 18 □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion 3 ☑ Enabled 180 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □ Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State ISE NAC

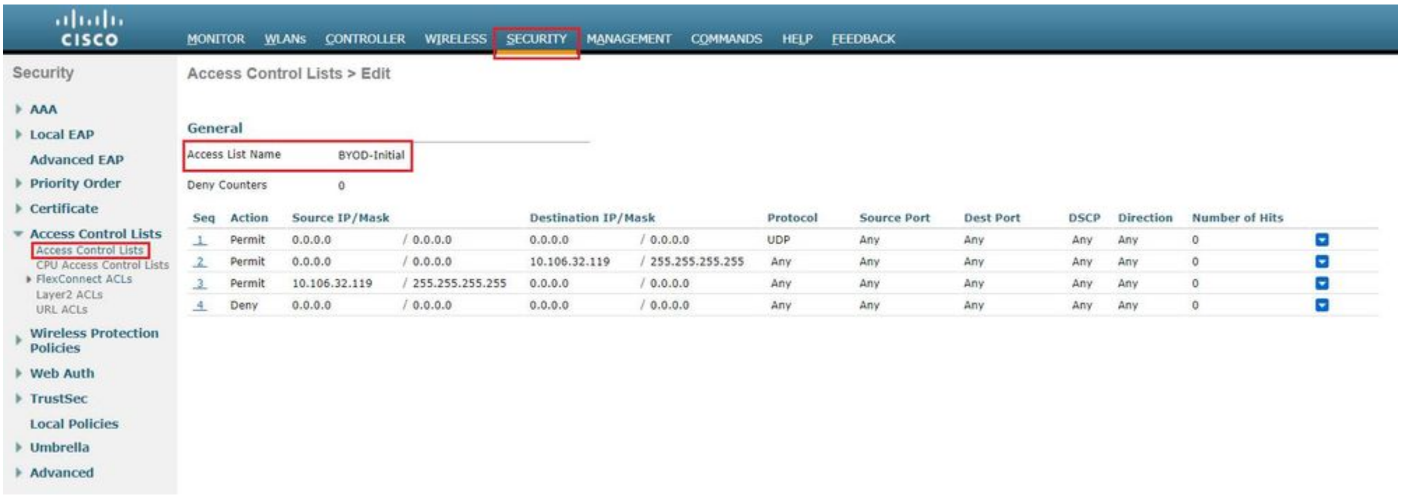
Load Balancing and Band Select
Client Load Balancing □
Client Band Select □

Passive Client

Stap 3. Configureer ACL om beperkte toegang te bieden voor het leveren van het apparaat.

- Hiermee kan UDP-verkeer naar DHCP en DNS worden toegestaan (DHCP is standaard toegestaan).
- Communicatie met ISE.
- Ontken ander verkeer.

Name: BYOD-Initiaal (OF iets wat u handmatig de ACL’s noemt in het machtigingsprofiel)



Access Control Lists > Edit

General

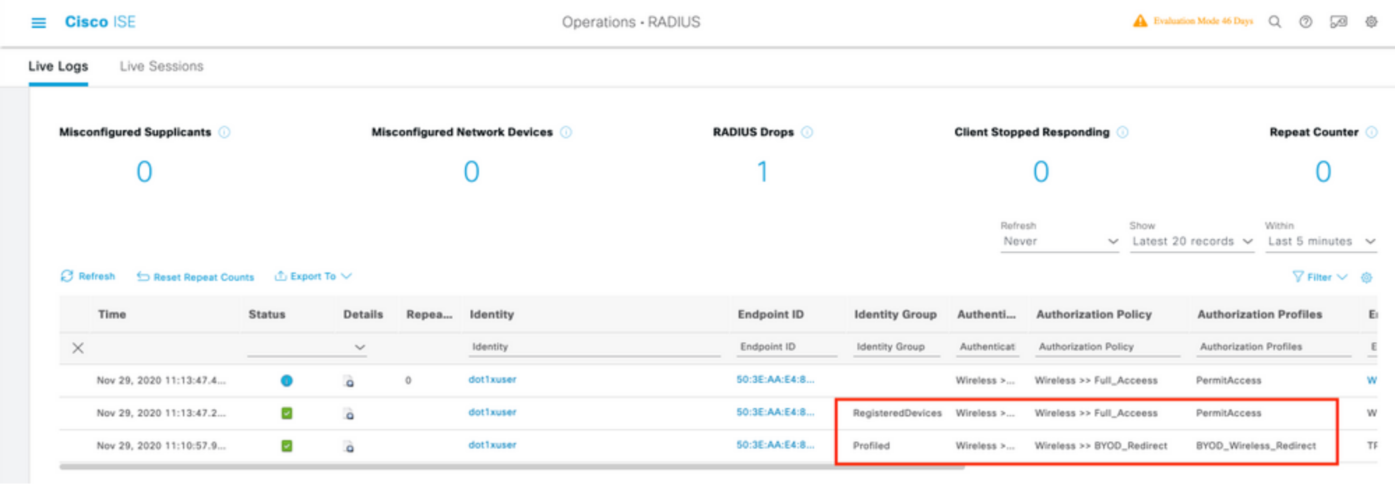
Access List Name BYOD-Initial

Deny Counters 0

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	Any	Any	Any	0
2	Permit	0.0.0.0	/ 0.0.0.0	10.106.32.119	/ 255.255.255.255	Any	Any	Any	Any	Any	0
3	Permit	10.106.32.119	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	0
4	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	0

Verifiëren

Verificatie van verificatie van verificatiestromen

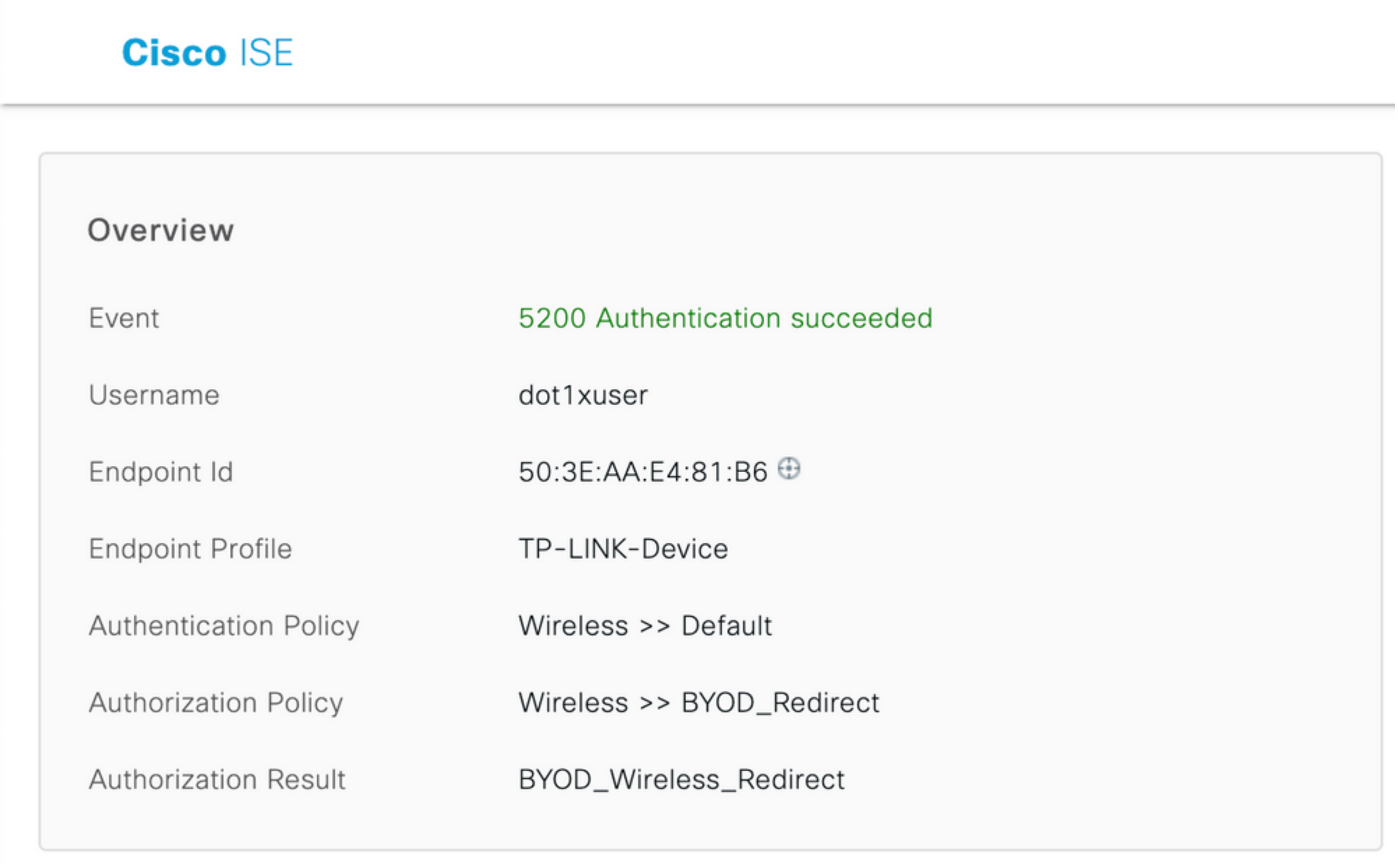


Misconfigured Supplicants: 0
Misconfigured Network Devices: 0
RADIUS Drops: 1
Client Stopped Responding: 0
Repeat Counter: 0

Refresh: Never
Show: Latest 20 records
Within: Last 5 minutes

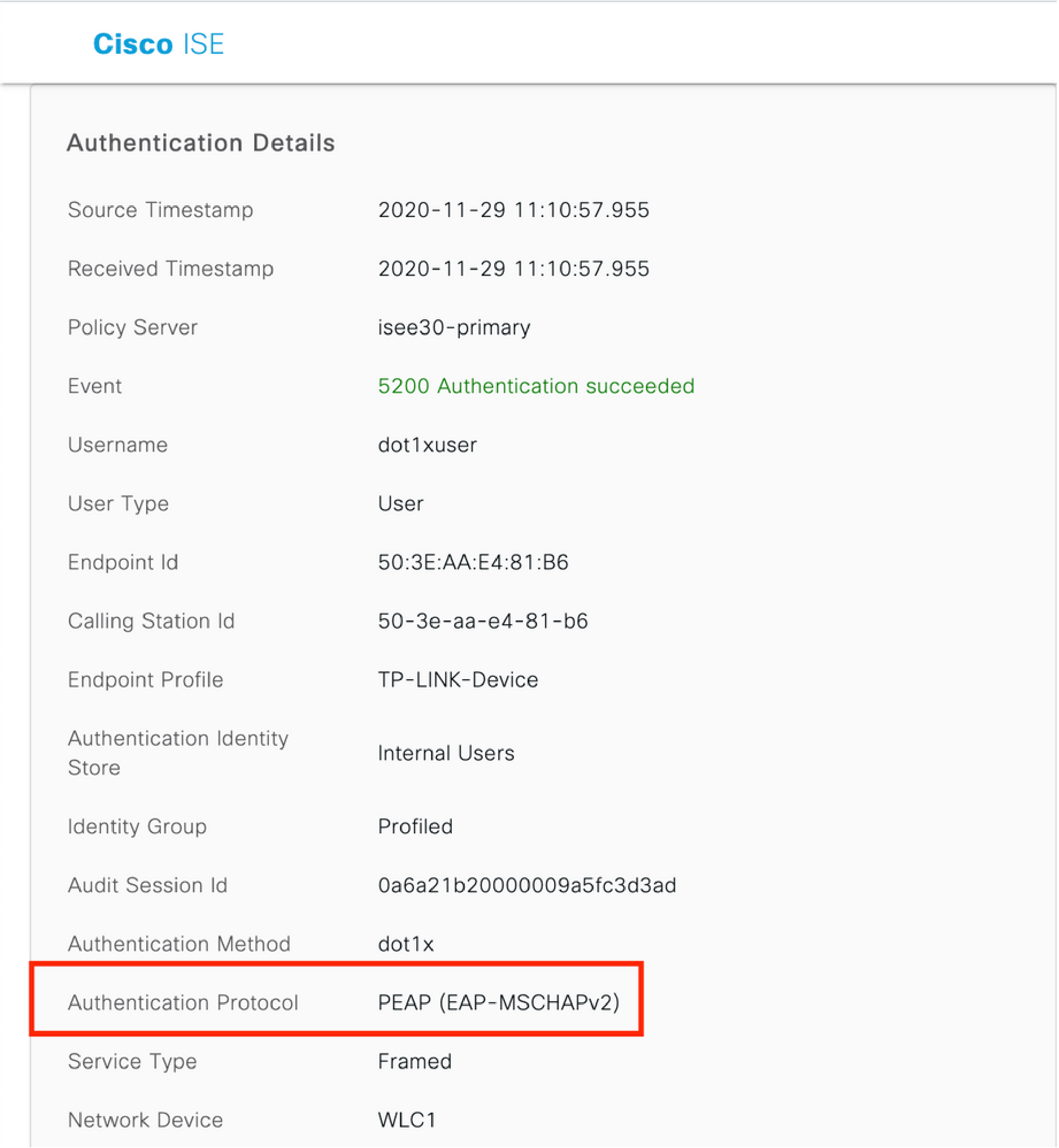
Time	Status	Details	Repea...	Identity	Endpoint ID	Identity Group	Authenti...	Authorization Policy	Authorization Profiles	E
Nov 29, 2020 11:13:47.4...	●		0	dot1xuser	50:3E:AA:E4:8...		Wireless >...	Wireless >> Full_Acceess	PermitAccess	W
Nov 29, 2020 11:13:47.2...	✓			dot1xuser	50:3E:AA:E4:8...	RegisteredDevices	Wireless >...	Wireless >> Full_Acceess	PermitAccess	W
Nov 29, 2020 11:10:57.9...	✓			dot1xuser	50:3E:AA:E4:8...	Profiled	Wireless >...	Wireless >> BYOD_Redirect	BYOD_Wireless_Redirect	TF

1. Bij de eerste inlog voert de gebruiker PEAP-verificatie uit met behulp van een gebruikersnaam en een wachtwoord. Op ISE slaat gebruiker regel BYOD-Redirect in.



Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	TP-LINK-Device
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> BYOD_Redirect
Authorization Result	BYOD_Wireless_Redirect

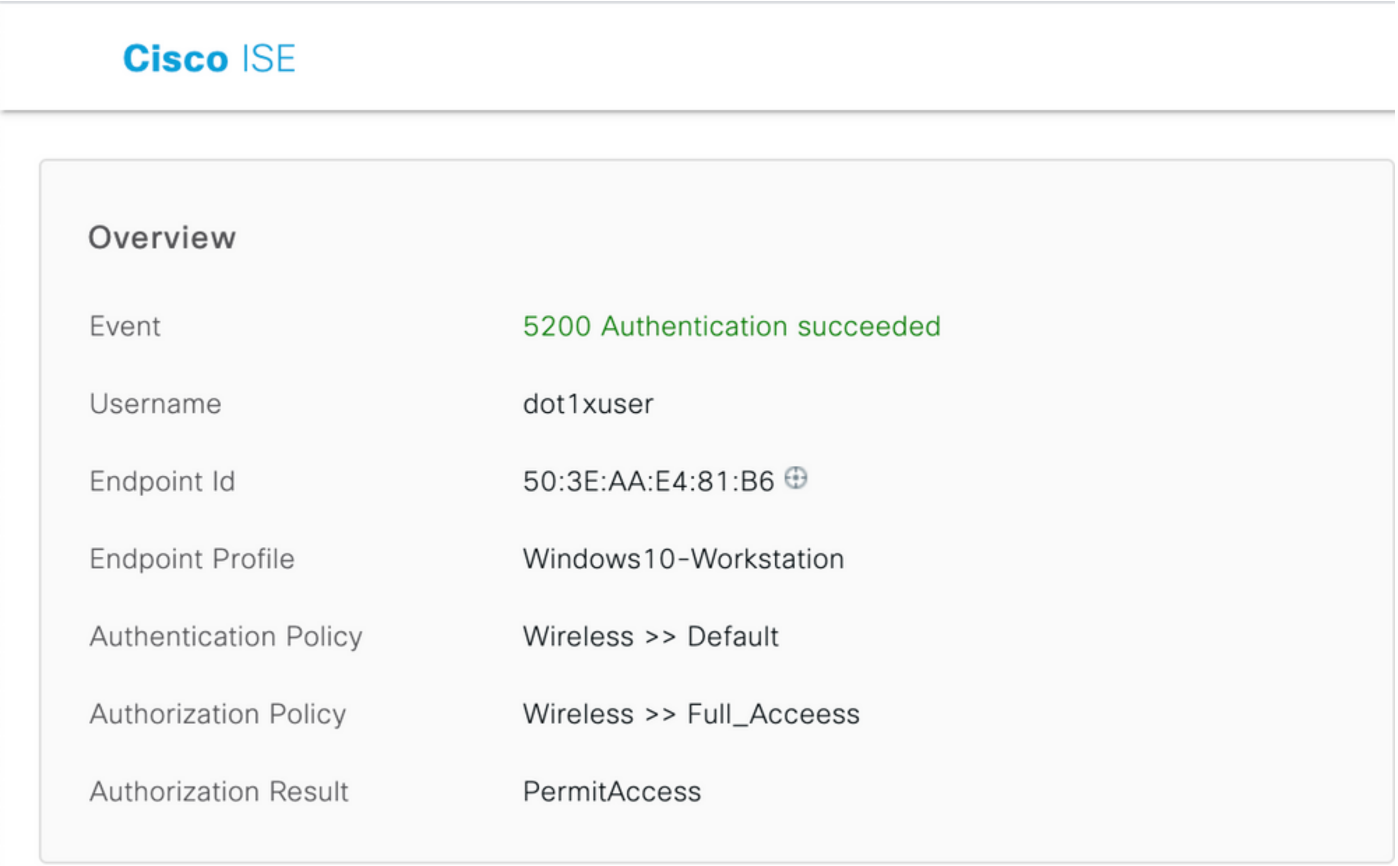


Cisco ISE

Authentication Details

Source Timestamp	2020-11-29 11:10:57.955
Received Timestamp	2020-11-29 11:10:57.955
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
User Type	User
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	TP-LINK-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WLC1

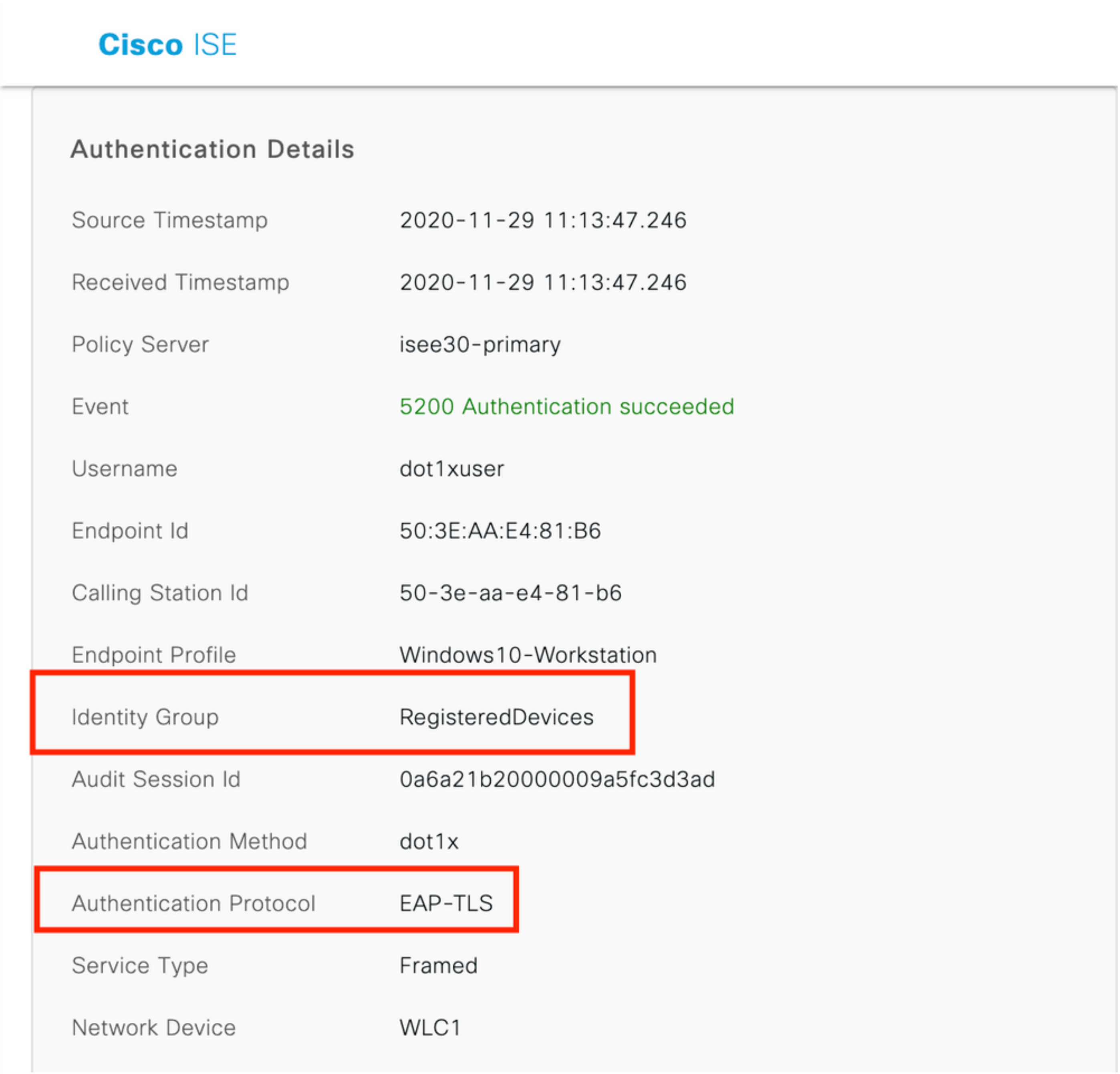
2. Na de BYOD-registratie wordt de gebruiker aan het geregistreerde apparaat toegevoegd, voert nu een MAP-TLS uit en krijgt volledige toegang.



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Endpoint Profile	Windows10-Workstation
Authentication Policy	Wireless >> Default
Authorization Policy	Wireless >> Full_Acceess
Authorization Result	PermitAccess



Cisco ISE

Authentication Details

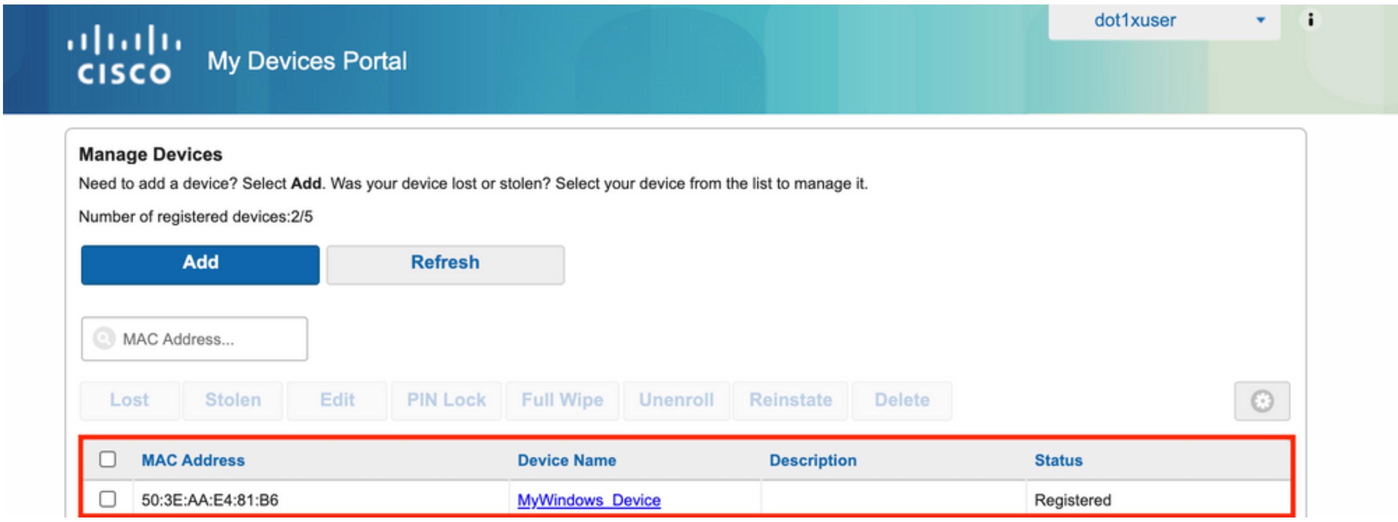
Source Timestamp	2020-11-29 11:13:47.246
Received Timestamp	2020-11-29 11:13:47.246
Policy Server	isee30-primary
Event	5200 Authentication succeeded
Username	dot1xuser
Endpoint Id	50:3E:AA:E4:81:B6
Calling Station Id	50-3e-aa-e4-81-b6
Endpoint Profile	Windows10-Workstation
Identity Group	RegisteredDevices
Audit Session Id	0a6a21b20000009a5fc3d3ad
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	WLC1

Controleer het My Devices Portal

Blader naar MyDevices Portal en Meld u aan bij de aanmeldingsgegevens. U kunt de naam van het apparaat en de Registratiestatus zien.

U kunt een URL maken voor MyDevices Portal.

Navigeer naar **ISE > Workcenters > BYOD > Portal en Componenten > My Devices Portal > Aanmelden-instellingen** en voer vervolgens de volledig gekwalificeerde URL in.



Manage Devices

Need to add a device? Select **Add**. Was your device lost or stolen? Select your device from the list to manage it.

Number of registered devices:2/5

☐	MAC Address	Device Name	Description	Status
☐	50:3E:AA:E4:81:B6	MyWindows_Device		Registered

Problemen oplossen

Algemene informatie

Voor het BYOD-proces moeten deze ISE-componenten worden ingeschakeld in debug op PSN-knooppunten -

scep - scep logberichten. Doellogbestand **filesgage.log en ise-psc.log**.

client-webapp: de component verantwoordelijk voor infrastructuurberichten. Bestandslogbestand - **ise-psc.log**

portal-web-action: de component die verantwoordelijk is voor de verwerking van het clientvoorzieningsbeleid. Bestandslogbestand -**gast.log**.

portal - alle aan portal gerelateerde evenementen . Bestandslogbestand -**gast.log**

portal-sessie-manager -Target logbestanden - **Portal sessie-gerelateerde debug-berichten - gues.log**

ca-service- ca-service berichten -Target logbestanden - **caservice.log en caservice-misc.log**

ca-service-cert- ca-service certificaatberichten - Target-logbestanden - **caservice.log en caservice-misc.log**

admin-ca- ca-service admin-berichten -Target logbestanden **ise-psc.log**, **caservice.log en casrvice-misc.log**

portal voor levering- certificaatprovisioningportal -berichten van het Target-**logbestand ise-psc.log**

nsf- NSF-gerelateerde berichten -Target logbestanden **ise-psc.log**

nsf-sessie- Session cache-gerelateerde berichten - Target logbestanden **ise-psc.log**

Runtime-AAA-alle Runtime gebeurtenissen. Doel logbestand -**prrt-server.log**.

Voor de logbestanden van de klant:

Zoek %temp%\spwProfileLog.txt (bijvoorbeeld: C:\Users\<gebruikersnaam>\AppData\Local\Temp\spwProfileLog.txt)

Analyse van het werklogboek

ISE-logboek

Initiële toegang-Accept met doorsturen van ACL en omgekeerde URL voor BYOD-portal

Port Server.log-7

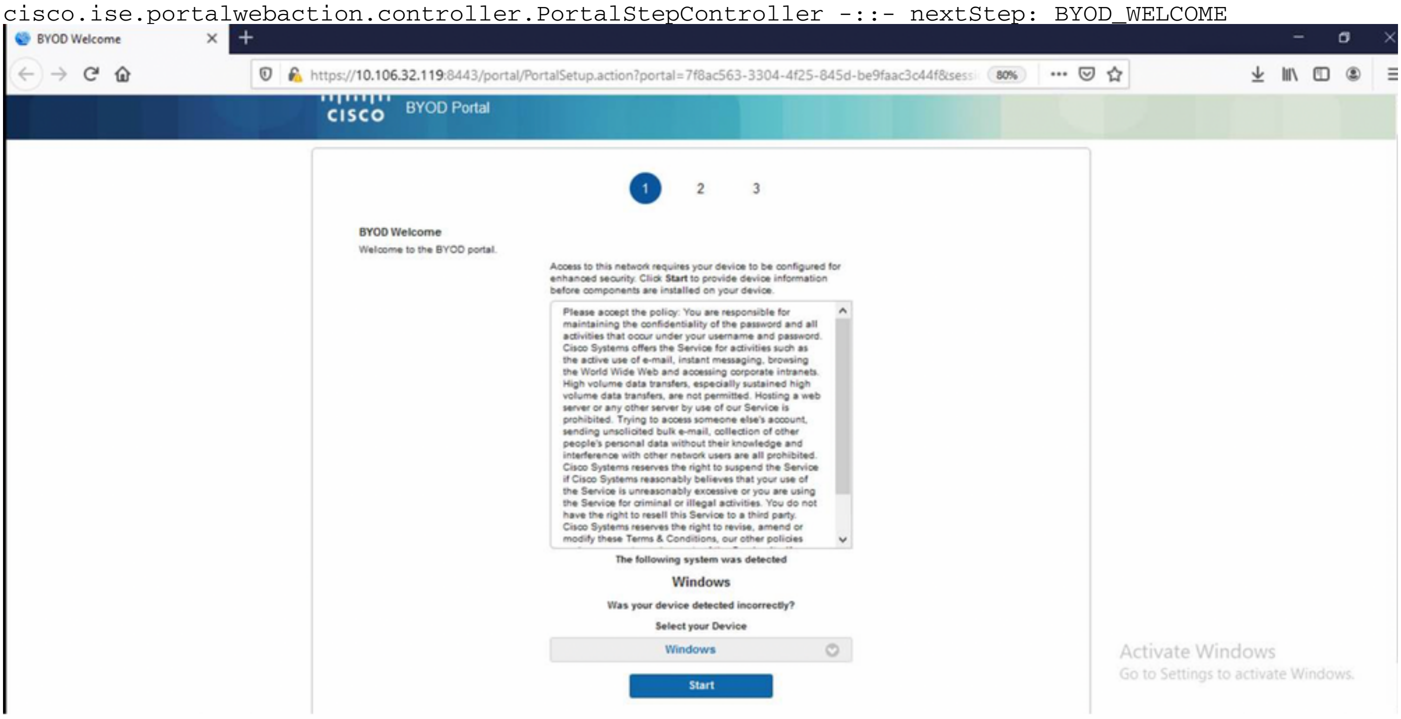
```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-
primary/392215758/699,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name -
value: [dot1xuser] [25] Class - value: [****] [79] EAP-Message - value: [ñ [80] Message-
Authenticator - value: [.2{wëbÙ¨ÅþO5‹Z] [26] cisco-av-pair - value: [url-redirect-acl=BYOD-
Initial] [26] cisco-av-pair - value: [url-
redirect=https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009f5fc770c7&portal=7f8
ac563-3304-4f25-845d-be9faac3c44f&action=nsp&token=53a2119de6893df6c6fca25c8d6bd061] [26] MS-
MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

Wanneer een eindgebruiker probeert om naar een website te navigeren en door WLC werd omgeleid naar de ISE om URL.

Guest.log -

```
2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][]
com.cisco.ise.portal.Gateway -::- Gateway Params (after update):
redirect=www.msftconnecttest.com/redirect client_mac=null daysToExpiry=null ap_mac=null
switch_url=null wlan=null action=nsp sessionId=0a6a21b20000009f5fc770c7 portal=7f8ac563-3304-
4f25-845d-be9faac3c44f isExpired=null token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02
05:43:58,339 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][]
cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- sessionId=0a6a21b20000009f5fc770c7 :
token=53a2119de6893df6c6fca25c8d6bd061 2020-12-02 05:43:58,339 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.utils.RadiusSessionUtil -::- Session
token successfully validated. 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-5][] cisco.ise.portal.util.PortalUtils -::- UserAgent : Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0 2020-12-02 05:43:58,344 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-5][] cisco.ise.portal.util.PortalUtils -::- isMozilla: true 2020-12-02
05:43:58,344 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gateway -
::- url: /portal/PortalSetup.action?portal=7f8ac563-3304-4f25-845d-
be9faac3c44f&sessionId=0a6a21b20000009f5fc770c7&action=nsp&redirect=www.msftconnecttest.com%2Fre
direct 2020-12-02 05:43:58,355 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.controller.PortalFlowInterceptor -::- start guest flow interceptor...
2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Executing action PortalSetup via request
/portal/PortalSetup.action 2020-12-02 05:43:58,356 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cisco.ise.portalwebaction.actions.PortalSetupAction -::- executeAction... 2020-12-02
05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Result from action, PortalSetup: success
2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cisco.ise.portalwebaction.actions.BasePortalAction -::- Action PortalSetup Complete for request
/portal/PortalSetup.action 2020-12-02 05:43:58,360 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -::- Current flow step:
INIT, otherInfo=id: 226ea25b-5e45-43f5-b79d-fb59cab96def 2020-12-02 05:43:58,361 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- Getting
next flow step for INIT with TranEnum=PROCEED 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- StepTran for
```

```
Step=INIT=> tranEnum=PROCEED, toStep=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager.step.StepExecutor -::- Find Next
Step=BYOD_WELCOME 2020-12-02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Step : BYOD_WELCOME will be visible! 2020-12-
02 05:43:58,361 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Returning next step =BYOD_WELCOME 2020-12-02
05:43:58,362 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -::- Looking up Guest user with
uniqueSubjectId=5f5592a4f67552b855ecc56160112db42cf7074e 2020-12-02 05:43:58,365 DEBUG [https-
jsse-nio-10.106.32.119-8443-exec-7][]
cpm.guestaccess.flowmanager.adaptor.PortalUserAdaptorFactory -::- Found Guest user 'dot1xuserin
DB using uniqueSubjectID '5f5592a4f67552b855ecc56160112db42cf7074e'. authStoreName in
DB=Internal Users, authStoreGUID in DB=9273fe30-8c01-11e6-996c-525400b48521. DB ID=bab8f27d-
c44a-48f5-9fe4-5187047bffc0 2020-12-02 05:43:58,366 DEBUG [https-jsse-nio-10.106.32.119-8443-
exec-7][] cisco.ise.portalwebaction.controller.PortalStepController -::- ++++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is INITIATED and current step
is BYOD_WELCOME 2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][]
com.cisco.ise.portalSessionManager.PortalSession -::- Setting the portal session state to ACTIVE
2020-12-02 05:40:35,611 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-6][]
cisco.ise.portalwebaction.controller.PortalStepController -::- nextStep: BYOD_WELCOME
```



https://10.106.32.119:8443/portal/PortalSetup.action?portal=7f8ac563-3304-4f25-845d-be9faac3c44f&sessi

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

The following system was detected

Windows

Was your device detected incorrectly?

Select your Device

Windows

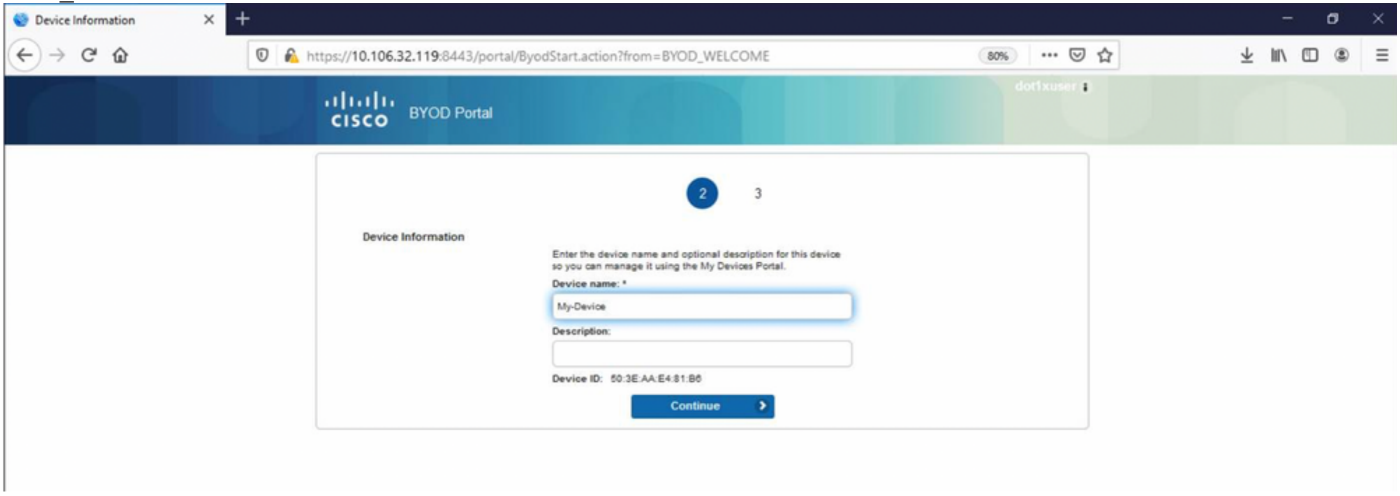
Klik op **Start** op de BYOD-welkomstpagina.

```
020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Executing action ByodStart via
request /portal/ByodStart.action 2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][] cisco.ise.portalwebaction.controller.PortalPreResultListener -:dot1xuser:-
currentStep: BYOD_WELCOME
```

Op dit punt evalueert ISE of de benodigde bestanden/bronnen die voor BYOD vereist zijn, aanwezig zijn of niet, en stelt deze zichzelf in op de BYOD INIT-status.

```
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- userAgent=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All),
nspStatus=SUCCESS 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dot1xuser:- NSP Downloadalble
Resource data=>, resource=DownloadableResourceInfo :WINDOWS_10_ALL
https://10.106.32.119:8443/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
```

```
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009f5fc770c7&os=WINDOWS_10_ALL null null
https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/ null
null https://10.106.32.119:8443/auth/provisioning/download/90a6dc9c-4aae-4431-a453-
81141ec42d2d/NetworkSetupAssistant.exe, coaType=NoCoa 2020-12-02 05:44:01,936 DEBUG [https-jsse-
nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager.utils.NSPProvAccess -:dot1xuser:-
It is a WIN/MAC! 2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cpm.guestaccess.flowmanager.step.StepExecutor -:dot1xuser:- Returning next step
=BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- ++++ updatePortalState:
PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE and current step is
BYOD_REGISTRATION 2020-12-02 05:44:01,950 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][]
cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- nextStep:
BYOD_REGISTRATION
```


Device Information
https://10.106.32.119:8443/portal/ByodStart.action?from=BYOD_WELCOME
80%
dot1xuser
cisco
BYOD Portal
2
3
Continue

Device Information

Enter the device name and optional description for this device so you can manage it using the My Devices Portal.

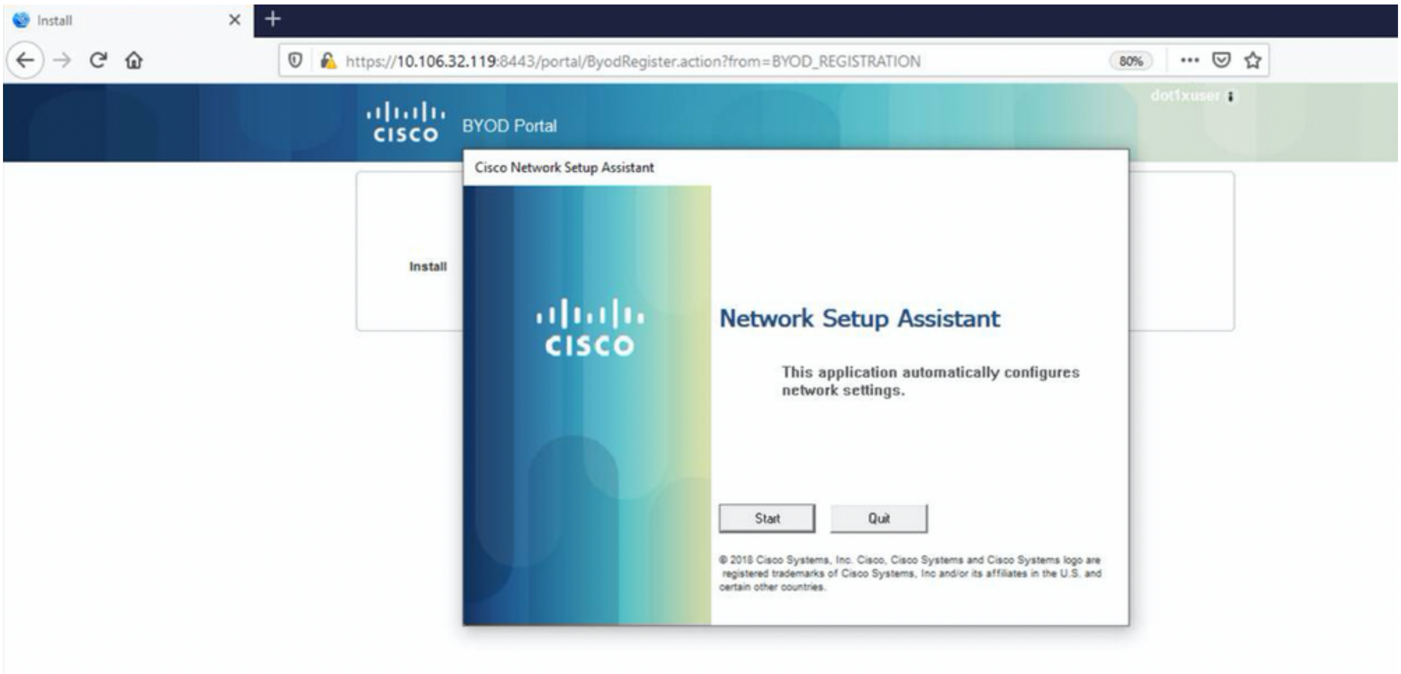
Device name: * My-Device

Description:

Device ID: 50:3E:AA:E4:81:B6

Voer de naam van het apparaat in en klik op in register.

```
2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Executing action ByodRegister
via request /portal/ByodRegister.action Request Parameters: from=BYOD_REGISTRATION
token=PZBMFBHX3FBPXT8QF98U717ILNOTD68D device.name=My-Device device.description= 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portal.actions.ByodRegisterAction -:dot1xuser:- executeAction... 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Result from action,
ByodRegister: success 2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dot1xuser:- Action ByodRegister Complete
for request /portal/ByodRegister.action 2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices.mydevices.MyDevicesServiceImpl -
:dot1xuser:- Register Device : 50:3E:AA:E4:81:B6 username= dot1xuser idGroupID= aa13bb40-8bff-
11e6-996c-525400b48521 authStoreGUID= 9273fe30-8c01-11e6-996c-525400b48521 nadAddress=
10.106.33.178 isSameDeviceRegistered = false 2020-12-02 05:44:14,900 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cpm.guestaccess.flowmanager.step.StepExecutor -:dot1xuser:-
Returning next step =BYOD_INSTALL 2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-1][] cisco.ise.portalwebaction.controller.PortalStepController -:dot1xuser:- ++++
updatePortalState: PortalSession (e0d457d9-a346-4b6e-bcca-5cf29e12dacc) current state is ACTIVE
and current step is BYOD_INSTALL 2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-
8443-exec-3][] cisco.ise.portalwebaction.controller.PortalFlowInterceptor -:dot1xuser:- result:
success 2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe
```


Install
https://10.106.32.119:8443/portal/ByodRegister.action?from=BYOD_REGISTRATION
80%
BYOD Portal
dot1xuser
Install
Cisco Network Setup Assistant
Network Setup Assistant
Start
Quit

This application automatically configures network settings.

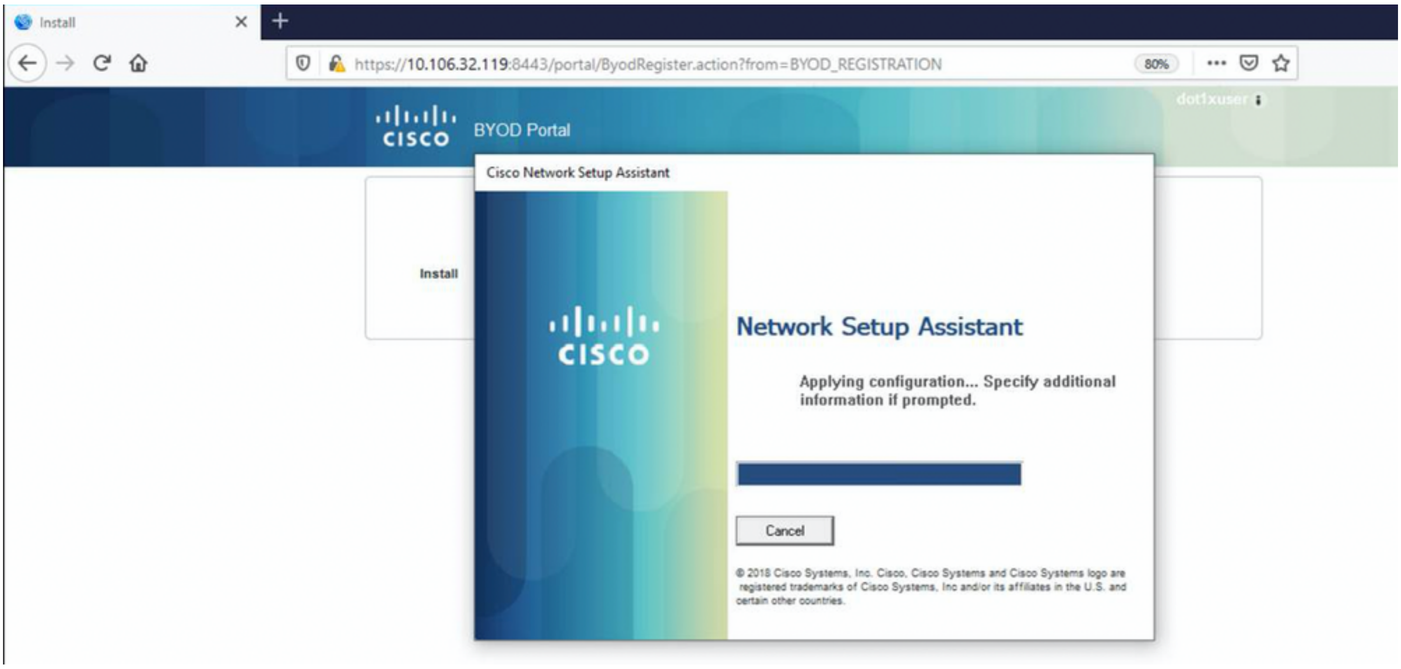
© 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

Wanneer de gebruiker op Start op de NSA klikt, wordt er tijdelijk een bestand met de naam **spwProfile.xml** gecreëerd op de client die de inhoud kopieert van de download van Cisco-ISE-NSP.xml op TCP-poort 8905.

Guest.log -

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][]
cisco.cpm.client.provisioning.StreamingServlet -::- StreamingServlet
URI:/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-e4ec38ee188c/WirelessNSP.xml 2020-12-02
05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-
Streaming to ip:10.106.33.167 file type: NativeSPProfile file name:WirelessNSP.xml 2020-12-02
05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet -::-
SPW profile :: 2020-12-02 05:45:03,308 DEBUG [portal-http-service15][]
cisco.cpm.client.provisioning.StreamingServlet -::-
```

Nadat u de inhoud uit de **spwProfile.xml** hebt gelezen, vormt NSA het netwerkprofiel en genereert u een CSR, en stuurt u het naar ISE om een certificaat te krijgen met de URL https://10.106.32.119:8443/auth/pkiclient.exe


Install
https://10.106.32.119:8443/portal/ByodRegister.action?from=BYOD_REGISTRATION
80%
BYOD Portal
dot1xuser
Install
Cisco Network Setup Assistant
Network Setup Assistant
Cancel

Applying configuration... Specify additional information if prompted.

© 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.

ise-psc.log-

```
2020-12-02 05:45:11,298 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Found incoming certifcate request for
internal CA. Increasing Cert Request counter. 2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Key type
is RSA, retrieving ScepCertRequestProcessor for caProfileName=ISE Internal CA 2020-12-02
05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.provisioning.cert.CertRequestValidator -::::- Session user has been set to = dot1xuser
2020-12-02 05:45:11,331 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.cpm.scep.util.ScepUtil -::::- Algorithm OID in CSR: 1.2.840.113549.1.1.1 2020-12-02
05:45:11,331 INFO [https-jsse-nio-10.106.32.119-8443-exec-1][]
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- About to forward certificate request
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser with transaction id n@P~N6E to server
http://127.0.0.1:9444/caservice/scep 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Encoding message:
org.jscep.message.PkcsReq@5c1649c2[transId=4d22d2e256a247a302e900ffa71c35d75610de67,messageType=
PKCS_REQ,senderNonce=Nonce
[7d9092a9fab204bd7600357e38309ee8],messageData=org.bouncycastle.pkcs.PKCS10CertificationRequest@
4662a5b0] 2020-12-02 05:45:11,332 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkcsPkiEnvelopeEncoder -::::- Encrypting session key using key belonging to
[issuer=CN=Certificate Services Endpoint Sub CA - isee30-primary;
serial=162233386180991315074159441535479499152] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- Signing message using
key belonging to [issuer=CN=isee30-primary.anshsinh.local;
serial=126990069826611188711089996345828696375] 2020-12-02 05:45:11,333 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessageEncoder -::::- SignatureAlgorithm
SHA1withRSA 2020-12-02 05:45:11,334 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
org.jscep.message.PkiMessageEncoder -::::- Signing
org.bouncycastle.cms.CMSProcessableByteArray@5aa9dfcc content
```

ca. service.log -

```
2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request] com.cisco.cpm.caservice.CrValidator -:::::- performing certificate request
validation: version [0] subject [C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser] ---
output omitted--- 2020-12-02 05:45:11,379 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request validation]
com.cisco.cpm.caservice.CrValidator -:::::- RDN value = dot1xuser 2020-12-02 05:45:11,379 DEBUG
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request]
com.cisco.cpm.caservice.CrValidator -:::::- request validation result CA_OK
```

caservice-misc.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request issuance] cisco.cpm.scep.util.ScepUtil -:::::- Algorithm OID in CSR:
1.2.840.113549.1.1.1 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.scep.CertRequestInfo -:::::- Found challenge password with cert template ID.
```

caservice.log -

```
2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67
0x67ee11d5 request issuance] cisco.cpm.caservice.util.CaServiceUtil -:::::- Checking cache for
certificate template with ID: e2c32ce0-313d-11eb-b19e-e60300a810d5 2020-12-02 05:45:11,380 DEBUG
[CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -:::::- CA SAN Extensions = GeneralNames: 1: 50-3E-
AA-E4-81-B6 2020-12-02 05:45:11,380 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -:::::- CA : add SAN extension... 2020-12-02
```

```
05:45:11,380 DEBUG [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5
request issuance] com.cisco.cpm.caservice.CertificateAuthority -:::::- CA Cert Template name =
BYOD_Certificate_template 2020-12-02 05:45:11,395 DEBUG [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
cisco.cpm.caservice.util.CaServiceUtil -:::::- Storing certificate via REST for serial number:
518fa73a4c654df282ffdb026080de8d 2020-12-02 05:45:11,395 INFO [CAService-Scep][scep job
4d22d2e256a247a302e900ffa71c35d75610de67 0x67ee11d5 request issuance]
com.cisco.cpm.caservice.CertificateAuthority -:::::- issuing Certificate Services Endpoint
Certificate: class [com.cisco.cpm.caservice.CaResultHolder] [1472377777]: result: [CA_OK]
subject [CN=dot1xuser, OU=tac, O=cisco, L=bangalore, ST=Karnataka, C=IN] version [3] serial
[0x518fa73a-4c654df2-82ffdb02-6080de8d] validity [after [2020-12-01T05:45:11+0000] before [2030-
11-27T07:35:10+0000]] keyUsages [ digitalSignature nonRepudiation keyEncipherment ]
```

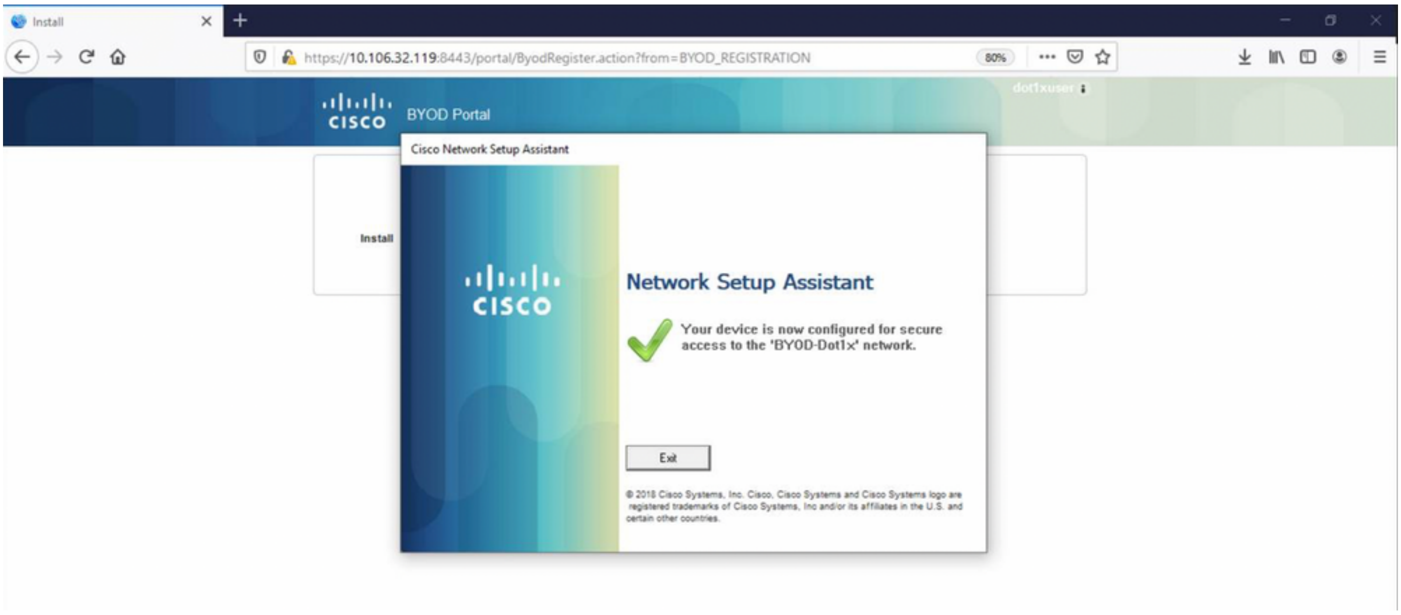
ise-psc.log -

```
2020-12-02 05:45:11,407 DEBUG [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder -
::::- Verifying message using key belonging to 'CN=Certificate Services Endpoint RA - isee30-
primary'
```

caservice.log -

```
2020-12-02 05:45:11,570 DEBUG [Infra-CAServiceUtil-Thread][]
cisco.cpm.caservice.util.CaServiceUtil -:::::- Successfully stored endpoint certificate.
```

ise-psc.log -


Install
https://10.106.32.119:8443/portal/ByodRegister.action?from=BYOD_REGISTRATION
80%
dot1xuser
cisco
BYOD Portal
Cisco Network Setup Assistant
Install
Exit

Network Setup Assistant

Your device is now configured for secure access to the 'BYOD-Dot1x' network.

© 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.

```
2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- Performing doGetCertInitial found
Scep certificate processor for txn id n@P~N6E 2020-12-02 05:45:13,381 DEBUG [https-jsse-nio-
10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCertRequestProcessor -::::- Polling
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser for certificate request n@P~N6E with
id {} 2020-12-02 05:45:13,385 INFO [https-jsse-nio-10.106.32.119-8443-exec-10][]
com.cisco.cpm.scep.ScepCertRequestProcessor -::::- Certificate request Complete for
C=IN,ST=Karnataka,L=bangalore,O=cisco,OU=tac,CN=dot1xuser Trx Idn@P~N6E 2020-12-02 05:45:13,596
DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][]
cisco.cpm.provisioning.cert.CertProvisioningFactory -::::- BYODStatus:COMPLETE_OTA_NSP
```

Na de installatie van het certificaat initiëren cliënten een andere echtheidscontrole met behulp van EAP-TLS en krijgen volledige toegang.

Port Server.log -

```
Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,CallingStationID=50-3e-aa-e4-81-
b6,EAP: Recv EAP packet, code=Response, identifier=64, type=EAP-TLS, length=166
,EapParser.cpp:150 Radius,2020-12-02
05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-
primary/392215758/701,CPMSessionID=0a6a21b20000009f5fc770c7,user=dot1xuser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=5 Length=231 [1] User-Name -
value: [dot1xuser] [25] Class - value: [****] [79] EAP-Message - value: [E [80] Message-
Authenticator - value: [Ù(ØyËöžö|kÔ,¸}] [26] MS-MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-
Key - value: [****] ,RADIUSHandler.cpp:2216
```

Clientvastlegging (spw-logs)

De client start om het profiel te downloaden.

```
[Mon Nov 30 03:34:27 2020] Downloading profile configuration... [Mon Nov 30 03:34:27 2020]
Discovering ISE using default gateway [Mon Nov 30 03:34:27 2020] Identifying wired and wireless
network interfaces, total active interfaces: 1 [Mon Nov 30 03:34:27 2020] Network interface -
mac:50-3E-AA-E4-81-B6, name: Wi-Fi 2, type: unknown [Mon Nov 30 03:34:27 2020] Identified
default gateway: 10.106.33.1 [Mon Nov 30 03:34:27 2020] Identified default gateway: 10.106.33.1,
mac address: 50-3E-AA-E4-81-B6 [Mon Nov 30 03:34:27 2020] DiscoverISE - start [Mon Nov 30
03:34:27 2020] DiscoverISE input parameter : strUrl [http://10.106.33.1/auth/discovery] [Mon Nov
30 03:34:27 2020] [HTTPConnection] CrackUrl: host = 10.106.33.1, path = /auth/discovery, user =
, port = 80, scheme = 3, flags = 0 [Mon Nov 30 03:34:27 2020] [HTTPConnection] HttpSendRequest:
header = Accept: */* headerLength = 12 data = dataLength = 0 [Mon Nov 30 03:34:27 2020] HTTP
Response header: [HTTP/1.1 200 OK Location:
https://10.106.32.119:8443/portal/gateway?sessionId=0a6a21b20000009c5fc4fb5e&portal=7f8ac563-
3304-4f25-845d-
be9faac3c44f&action=nsp&token=29354d43962243bcb72193cbf9dc3260&redirect=10.106.33.1/auth/discove
ry [Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path =
/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b20000009c5fc4fb5e&os=WINDOWS_10_ALL, user = , port
= 8443, scheme = 4, flags = 8388608 Mon Nov 30 03:34:36 2020] parsing wireless connection
setting [Mon Nov 30 03:34:36 2020] Certificate template: [keytype:RSA, keysize:2048,
subject:OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN, SAN:MAC] [Mon Nov 30 03:34:36 2020] set
ChallengePwd
```

Clientcontroles als WLAN-service wordt uitgevoerd.

```
[Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - Start [Mon Nov 30 03:34:36 2020]
Wlansvc service is in Auto mode ... [Mon Nov 30 03:34:36 2020] Wlansvc is running in auto
mode... [Mon Nov 30 03:34:36 2020] WirelessProfile::StartWLanSvc - End [Mon Nov 30 03:34:36
2020] Wireless interface 1 - Desc: [TP-Link Wireless USB Adapter], Guid: [{65E78DDE-E3F1-4640-
906B-15215F986CAA}]... [Mon Nov 30 03:34:36 2020] Wireless interface - Mac address: 50-3E-AA-E4-
81-B6 [Mon Nov 30 03:34:36 2020] Identifying wired and wireless interfaces... [Mon Nov 30
03:34:36 2020] Found wireless interface - [ name:Wi-Fi 2, mac address:50-3E-AA-E4-81-B6] [Mon
Nov 30 03:34:36 2020] Wireless interface [Wi-Fi 2] will be configured... [Mon Nov 30 03:34:37
2020] Host - [ name:DESKTOP-965F94U, mac addresses:50-3E-AA-E4-81-B6]
```

De cliënt past profiel toe -

```
[Mon Nov 30 03:34:37 2020] ApplyProfile - Start... [Mon Nov 30 03:34:37 2020] User Id:
dot1xuser, sessionid: 0a6a21b20000009c5fc4fb5e, Mac: 50-3E-AA-E4-81-B6, profile: WirelessNSP
[Mon Nov 30 03:34:37 2020] number of wireless connections to configure: 1 [Mon Nov 30 03:34:37
2020] starting configuration for SSID : [BYOD-Dot1x] [Mon Nov 30 03:34:37 2020] applying
certificate for ssid [BYOD-Dot1x]
```

Clientinstallatiecertificaat.

```
[Mon Nov 30 03:34:37 2020] ApplyCert - Start... [Mon Nov 30 03:34:37 2020] using ChallengePwd
[Mon Nov 30 03:34:37 2020] creating certificate with subject = dot1xuser and subjectSuffix =
OU=tac;O=cisco;L=bangalore;ST=Karnataka;C=IN [Mon Nov 30 03:34:38 2020] Self signed certificate
[Mon Nov 30 03:34:44 2020] Installed [isee30-primary.anshsinh.local, hash: 5b a2 08 1e 17 cb 73
5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b ] as rootCA [Mon Nov 30 03:34:44 2020] Installed CA cert
for authMode machineOrUser - Success Certificate is downloaded . Omitted for brevity - [Mon Nov
30 03:34:50 2020] creating response file name C:\Users\admin\AppData\Local\Temp\response.cer
[Mon Nov 30 03:34:50 2020] Certificate issued - successfully [Mon Nov 30 03:34:50 2020]
ScepWrapper::InstallCert start [Mon Nov 30 03:34:50 2020] ScepWrapper::InstallCert: Reading scep
response file [C:\Users\admin\AppData\Local\Temp\response.cer]. [Mon Nov 30 03:34:51 2020]
ScepWrapper::InstallCert GetCertHash -- return val 1 [Mon Nov 30 03:34:51 2020]
ScepWrapper::InstallCert end [Mon Nov 30 03:34:51 2020] ApplyCert - End... [Mon Nov 30 03:34:51
2020] applied user certificate using template id e2c32ce0-313d-11eb-b19e-e60300a810d5
```

ISE-configuratie van draadloos profiel

```
[Mon Nov 30 03:34:51 2020] Configuring wireless profiles... [Mon Nov 30 03:34:51 2020]
Configuring ssid [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] WirelessProfile::SetWirelessProfile -
Start [Mon Nov 30 03:34:51 2020] TLS - TrustedRootCA Hash: [ 5b a2 08 1e 17 cb 73 5f ba 5b 9f a2
2d 3b fc d2 86 0d a5 9b]
```

profiel

```
Wireless interface succesfully initiated, continuing to configure SSID [Mon Nov 30 03:34:51
2020] Currently connected to SSID: [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020] Wireless profile:
[BYOD-Dot1x] configured successfully [Mon Nov 30 03:34:51 2020] Connect to SSID [Mon Nov 30
03:34:51 2020] Successfully connected profile: [BYOD-Dot1x] [Mon Nov 30 03:34:51 2020]
WirelessProfile::SetWirelessProfile. - End [Mon Nov 30 03:35:21 2020]
WirelessProfile::IsSingleSSID - Start [Mon Nov 30 03:35:21 2020] Currently connected to SSID:
[BYOD-Dot1x], profile ssid: [BYOD-Dot1x], Single SSID [Mon Nov 30 03:35:21 2020]
WirelessProfile::IsSingleSSID - End [Mon Nov 30 03:36:07 2020] Device configured successfully.
```