

# Konfigurieren von Single-SSID Wireless BYOD unter Windows und ISE

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Theorie](#)

[Konfiguration](#)

[ISE-Konfiguration](#)

[WLC-Konfiguration](#)

[Überprüfung](#)

[Überprüfung des Authentifizierungsflusses](#)

[Überprüfen Sie das My Devices-Portal.](#)

[Fehlerbehebung](#)

[Allgemeine Informationen](#)

[Arbeitsprotokollanalyse](#)

[ISE-Protokolle](#)

[Clientprotokolle \(spw-Protokolle\)](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie Bring Your Own Device (BYOD) auf der Cisco Identity Services Engine (ISE) für Windows-Systeme mithilfe von Single-SSID und Dual-SSID konfigurieren.

## Voraussetzungen

### Anforderungen

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

- Konfiguration der Cisco ISE Version 3.0
- Konfiguration des Cisco WLC
- BYOD

### Verwendete Komponenten

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

- Cisco ISE Version 3.0

- Windows 10
- WLC und AP

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Theorie

In einer einzigen SSID wird BYOD nur noch eine SSID für die Integration von Geräten verwendet. Später wird der uneingeschränkte Zugriff auf die registrierten Geräte gewährt. Zuerst stellt der Benutzer über den Benutzernamen und das Kennwort ( MSCHAPv2 ) eine Verbindung zur SSID her. Nach erfolgreicher Authentifizierung auf der ISE wird der Benutzer zum BYOD-Portal umgeleitet. Nach Abschluss der Geräteregistrierung lädt der Endclient den Native Supplicant Assistant (NSA) von der ISE herunter. NSA wird auf dem Endclient installiert und lädt das Profil und das Zertifikat von der ISE herunter. Die NSA konfiguriert die Wireless-Komponente, und der Client installiert das Zertifikat. Endpunkt führt eine weitere Authentifizierung für dieselbe SSID mithilfe des heruntergeladenen Zertifikats mithilfe von EAP-TLS durch. Die ISE überprüft die neue Anfrage vom Client und verifiziert die EAP-Methode und die Geräteregistrierung und gewährt vollständigen Zugriff auf das Gerät.

Windows BYOD Einzelne SSID-Schritte -

- Ursprüngliche EAP-MSCHAPv2-Authentifizierung
- Umleitung zum BYOD-Portal
- Geräteregistrierung
- NSA-Download
- Profildownload
- Zertifikatdownload
- EAP-TLS-Authentifizierung

## Konfiguration

### ISE-Konfiguration

Schritt 1: Hinzufügen eines Netzwerkgeräts in der ISE und Konfigurieren von RADIUS und gemeinsam genutztem Schlüssel

Navigieren Sie zu **ISE > Administration > Network Devices > Add Network Device**.

Schritt 2: Erstellen Sie eine Zertifikatsvorlage für BYOD-Benutzer. Die Vorlage muss über eine Client Authentication Enhanced Key Usage verfügen. Sie können die Standard-Vorlage EAP\_Certificate\_Template verwenden.

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

**Edit Certificate Template**

Certificate Management >

Certificate Authority v

Overview

Issued Certificates

Certificate Authority Certifica...

Internal CA Settings

**Certificate Templates**

External CA Settings

\* 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 v

Key Type RSA v

Key Size 2048 v

\* SCEP RA Profile ISE Internal CA v

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

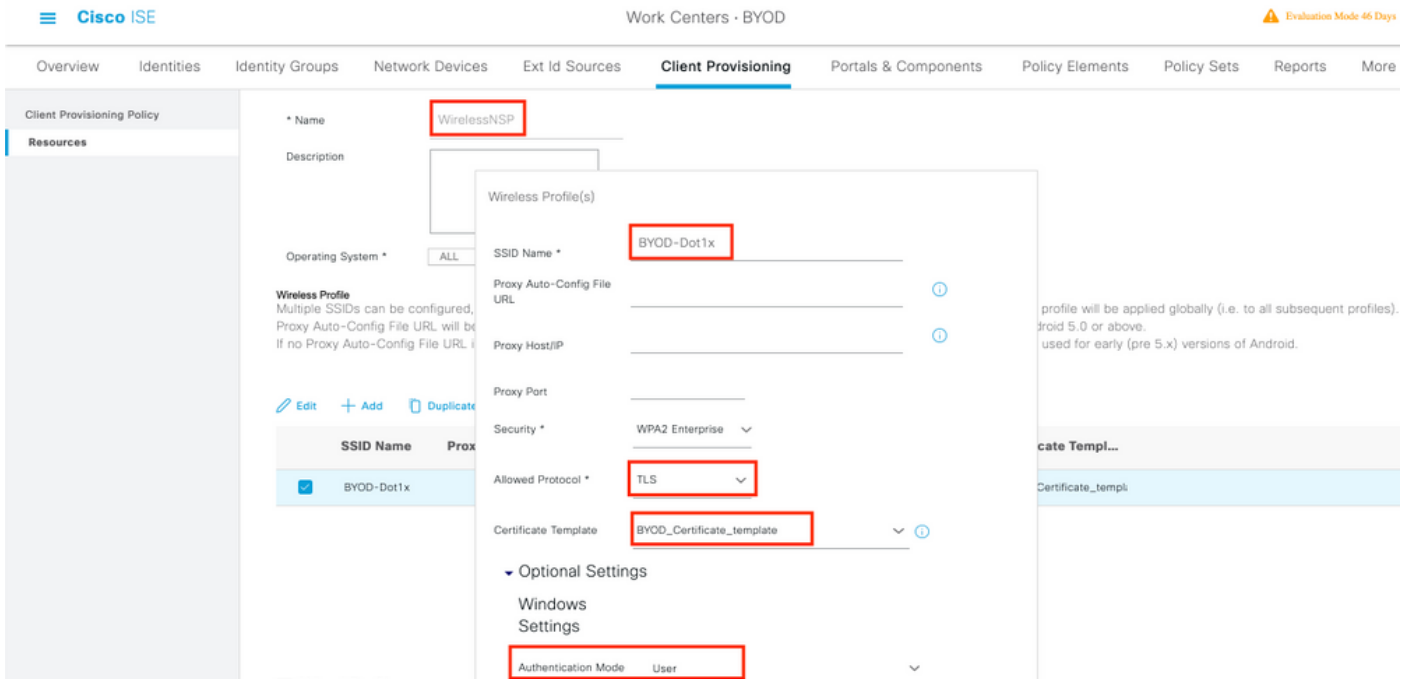
Extended Key Usage  Client Authentication  Server Authentication

Schritt 3: Erstellen Sie ein systemeigenes Supplicant-Profil für ein Wireless-Profil.

Navigieren Sie zu **ISE > Work Center > BYOD > Client Provisioning**. Klicken Sie auf **Hinzufügen**, und wählen Sie **Native Supplicant Profile (NSP)** aus dem Dropdown-Menü aus.

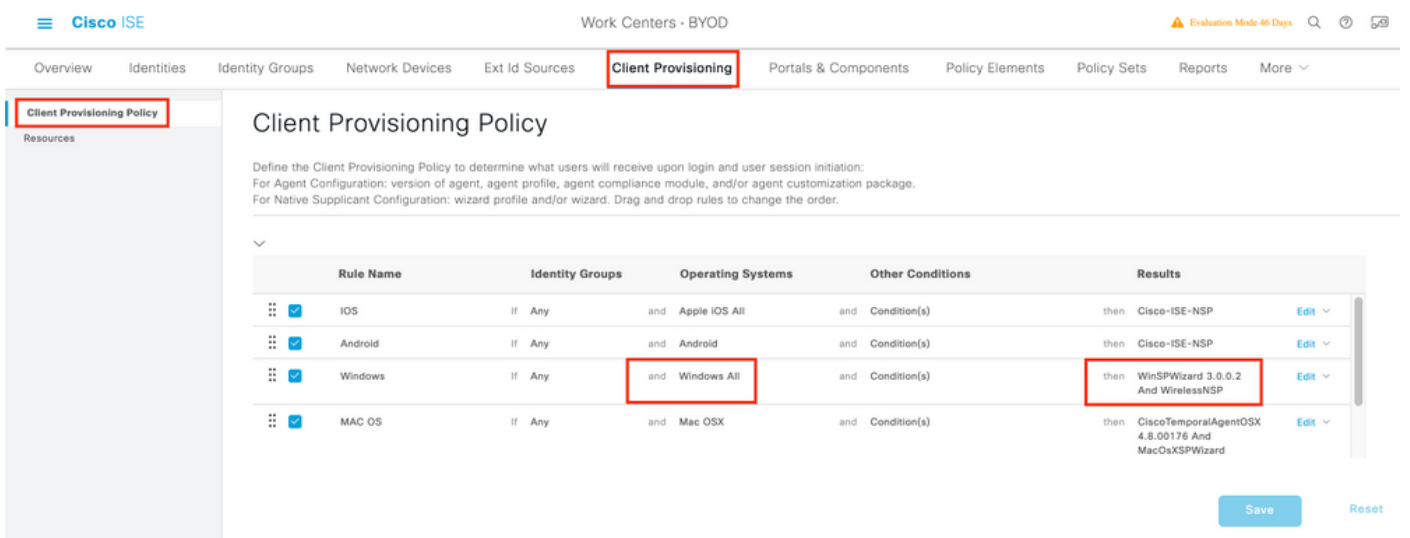
Hier muss der SSID-Name mit dem SSID übereinstimmen, mit dem Sie eine Verbindung hergestellt haben, bevor Sie ein SSID-BYOD durchführen. Wählen Sie das Protokoll als TLS aus. Wählen Sie eine Zertifikatsvorlage aus, wie im vorherigen Schritt erstellt, oder Sie können die Standard-Vorlage EAP\_Certificate\_Template verwenden.

Wählen Sie unter Optionale Einstellungen die Benutzer- oder Benutzer- und Systemauthentifizierung gemäß Ihren Anforderungen aus. In diesem Beispiel wird es als Benutzerauthentifizierung konfiguriert. Lassen Sie andere Standardeinstellungen unverändert.



Schritt 4: Erstellen von Client-Bereitstellungsrichtlinien für Windows-Geräte.

Navigieren Sie zu ISE > Work Center > BYOD > Client Provisioning > Client Provisioning Policy (ISE > Work Center > BYOD > Client Provisioning > Client Provisioning Policy (Client-Bereitstellungsrichtlinie). Wählen Sie das Betriebssystem als **Windows ALL** aus. Wählen Sie WinSPWizard 3.0.0.2 und NSP aus, die im vorherigen Schritt erstellt wurden.



Schritt 5: Erstellen Sie ein **Autorisierungsprofil** für Geräte, die nicht als BYOD-Geräte registriert sind.

Navigieren Sie zu ISE > Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add.

Wählen Sie unter "**Allgemeine Aufgabe**" die Option **Bereitstellung systemeigener Komponenten** aus. Definieren Sie einen Namen für die Weiterleitungskontrollliste, der auf dem WLC erstellt wird, und wählen Sie das BYOD-Portal aus. Hier wird das Standardportal verwendet. Sie können ein benutzerdefiniertes BYOD-Portal erstellen. Navigieren Sie zu ISE > Work Center > BYOD > Portale und Komponenten, und klicken Sie auf **Hinzufügen**.

Dictionarys Conditions **Results**

Authentication >

Authorization >

**Authorization Profiles**

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

\* 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)

Schritt 6: Erstellen Sie ein Zertifikatprofil.

Navigieren Sie zu ISE > Administration > External Identity Sources > Certificate Profile. Erstellen Sie hier ein neues Zertifikatprofil, oder verwenden Sie das standardmäßige Zertifikatprofil.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

## External Identity Sources

- <
- Certificate Authentication F
- cert\_profile**
- Preloaded\_Certificate\_Prof
- Active Directory
- ADJoloint
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Certificate Authentication Profiles List &gt; cert\_profile

## Certificate Authentication Profile

\* Name **cert\_profile**

Description

Identity Store [not applicable]

Use Identity From  Certificate Attribute Subject - Common N: ⓘ

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

Schritt 7: Erstellen Sie eine Identitätsquellensequenz, und wählen Sie das im vorherigen Schritt erstellte Zertifikatprofil aus, oder verwenden Sie das Standardzertifikatprofil. Dies ist erforderlich, wenn Benutzer nach der BYOD-Registrierung EAP-TLS durchführen, um vollständigen Zugriff zu erhalten.

[Identity Source Sequences List](#) > For\_Teap

## Identity Source Sequence

## Identity Source Sequence

\* Name

BYOD\_id\_Store

Description

## Certificate Based Authentication



Select Certificate Authentication Profile

cert\_profile



## Authentication Search List

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

## Available

Internal Endpoints

Guest Users

## Selected

Internal Users

ADJoiint

Schritt 8: Erstellen eines Policy Set, einer Authentifizierungsrichtlinie und einer Autorisierungsrichtlinie.

Navigieren Sie zu ISE > Policy > Policy Sets (ISE > Richtlinien > Richtlinienansätze). Erstellen Sie einen Richtlinienansatz, und **speichern Sie ihn**.

Erstellen Sie eine Authentifizierungsrichtlinie, und wählen Sie die im vorherigen Schritt erstellte Identitätsquellensequenz aus.

Erstellen einer Autorisierungsrichtlinie. Sie müssen zwei Richtlinien erstellen.

1. Für Geräte, die nicht für BYOD registriert sind. Geben Sie ein in Schritt 5 erstelltes Redirect-Profil ein.

2. BYOD-registrierte Geräte, die EAP-TLS ausführen. Ermöglichen Sie vollständigen Zugriff auf diese Geräte.



**CISCO** MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Auth Cached Users
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
    - LDAP
    - Local Net Users
    - MAC Filtering
  - Disabled Clients
    - User Login Policies
    - AP Policies
    - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec
  - Local Policies
  - Umbrella
  - Advanced

**RADIUS Authentication Servers > Edit**

Server Index: 7

Server Address(Ipv4/Ipv6): 10.106.32.119

Shared Secret Format: ASCII

Shared Secret: [REDACTED]

Confirm Shared Secret: [REDACTED]

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

Navigieren Sie zu **Security > AAA > Radius > Accounting**.

**CISCO** MONITOR WLANS CONTROLLER WIRELESS SECURITY **MANAGEMENT** COMMANDS HELP FEEDBACK

**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Auth Cached Users
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
    - LDAP
    - Local Net Users
    - MAC Filtering
  - Disabled Clients
    - User Login Policies
    - AP Policies
    - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec

**RADIUS Accounting Servers > Edit**

Server Index: 7

Server Address(Ipv4/Ipv6): 10.106.32.119

Shared Secret Format: ASCII

Shared Secret: [REDACTED]

Confirm Shared Secret: [REDACTED]

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

Schritt 2: Konfigurieren Sie eine 802.1x-SSID.



WLANs

- WLANs
- Advanced

WLANs > Edit 'BYOD-Dot1x'

- General**
- Security
- QoS
- Policy-Mapping
- Advanced

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

- WLANs
- Advanced

WLANs > Edit 'BYOD-Dot1x'

- General
- Security**
- QoS
- Policy-Mapping
- Advanced

- Layer 2**
- Layer 3
- AAA Servers

Layer 2 Security: WPA2+WPA3

Security Type: Enterprise

MAC Filtering:

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

802.1X-SHA1:  Enable

WLANs > Edit 'BYOD-Dot1x'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

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

Server	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.106.32.119, Port:1812	<input checked="" type="checkbox"/> Enabled 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

Authorization ACA Server  Enabled

Accounting ACA Server  Enabled

EAP Parameters  Enable

WLANs > Edit 'BYOD-Dot1x'

General Security QoS Policy-Mapping **Advanced**

Allow AAA Override  Enabled

Coverage Hole Detection  Enabled

Enable Session Timeout  1800  
Session Timeout (secs)

Aironet IE  Enabled

Diagnostic Channel  Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion  Enabled  
Timeout Value (secs) 180

Maximum Allowed Clients 0

Static IP Tunneling  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 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

Schritt 3: Konfigurieren Sie die Umleitungszugriffskontrollliste so, dass der Zugriff auf das Gerät eingeschränkt wird.

- Zulassen von UDP-Datenverkehr zu DHCP und DNS (standardmäßig ist DHCP zulässig).
- Kommunikation mit der ISE.
- Andere Zugriffe ablehnen.

Name: BYOD-Initial (ODER was auch immer Sie die ACL manuell im Autorisierungsprofil genannt haben)

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security 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

# Überprüfung

## Überprüfung des Authentifizierungsflusses

Cisco ISE Operations - RADIUS Evaluation Mode 46 Days

Live Logs Live Sessions

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	Ei
Nov 29, 2020 11:13:47.4...	●	🔒	0	dot1kuser	50:3E-AA-E4.8...	Wireless >...	Wireless >> Full_Access	PermitAccess		W
Nov 29, 2020 11:13:47.2...	■	🔒		dot1kuser	50:3E-AA-E4.8...	RegisteredDevices	Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:10:57.9...	■	🔒		dot1kuser	50:3E-AA-E4.8...	Profiled	Wireless >...	Wireless >> BYOD_Redirect	BYOD_Wireless_Redirect	TF

1. Bei der ersten Anmeldung führt der Benutzer eine PEAP-Authentifizierung mit Benutzernamen und Kennwort durch. Auf der ISE trifft der Benutzer auf die Umleitungsregel BYOD-Redirect.

## 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

**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. Nach der BYOD-Registrierung wird der Benutzer dem registrierten Gerät hinzugefügt. Er führt nun EAP-TLS durch und erhält vollständigen Zugriff.

## 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_Access
Authorization Result	PermitAccess

**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

**Überprüfen Sie das My Devices-Portal.**

Navigieren Sie zum MyDevices-Portal, und melden Sie sich mit den Anmeldeinformationen an. Sie sehen den Gerätenamen und den Registrierungsstatus.

Sie können eine URL für das MyDevices-Portal erstellen.

Navigieren Sie zu **ISE > Work Center > BYOD > Portal and Components > My Devices Portal > Login Settings** und geben Sie dann die vollqualifizierte URL ein.

**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

**Add** **Refresh**

MAC Address...

**Lost** **Stolen** **Edit** **PIN Lock** **Full Wipe** **Unenroll** **Reinstate** **Delete**

<input type="checkbox"/>	MAC Address	Device Name	Description	Status
<input type="checkbox"/>	50:3E:AA:E4:81:B6	<a href="#">MyWindows_Device</a>		Registered

## Fehlerbehebung

### Allgemeine Informationen

Für den BYOD-Prozess müssen diese ISE-Komponenten beim Debuggen auf PSN-Knoten aktiviert werden:

Signaltonprotokolle Ziellog-Dateien **Guest.log** und **ise-psc.log**.

**client-webapp**: die Komponente, die für Infrastrukturmeldungen verantwortlich ist.  
 Zielprotokolldatei - **ise-psc.log**

**portal-web-action**: Die Komponente, die für die Verarbeitung von Client-Bereitstellungsrichtlinien verantwortlich ist. Zielprotokolldatei - **guest.log**.

**portal** - alle Veranstaltungen rund um das Portal. Zielprotokolldatei - **guest.log**

**portal-session-manager** - Zielprotokolldateien - **Portal-Session-Debug-Meldungen** - **gues.log**

**ca-service**- ca-service-Meldungen -Zielprotokolldateien - **caservice.log** und **caservice-misc.log**

**ca-service-cert**- ca-service-Zertifikatmeldungen - Zielprotokolldateien - **caservice.log** und **caservice-misc.log**

**admin-ca**- ca-service Admin-Meldungen -Ziel-Protokolldateien **ise-psc.log**, **caservice.log** und **caservice-misc.log**

**certprovisioning portal**- Nachrichten des Zertifikats Provisioning Portal - Zielprotokolldateien **ise-psc.log**

**nsf**- NSF-bezogene Meldungen - Zielprotokolldateien **ise-psc.log**

**nsf-session**- Nachrichten im Sitzungscache -Zielprotokolldateien **ise-psc.log**

**Runtime-AAA**: Alle Laufzeitergebnisse. Zielprotokolldatei - **prrt-server.log**.

Für clientseitige Protokolle:



Suchen Sie %temp%\spwProfileLog.txt (z. B.:  
C:\Users\\AppData\Local\Temp\spwProfileLog.txt)

## Arbeitsprotokollanalyse

### ISE-Protokolle

Erstmalige Zugriffsgenehmigung mit Umleitung der ACL und Umleitung der URL für das BYOD-Portal.

#### Port-Server.log-

```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-  
primary/392215758/699,CPMSessionID=0a6a21b20000009f5fc770c7,user=dotlxuser,CallingStationID=50-  
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=254 Length=459 [1] User-Name -  
value: [dotlxuser] [25] Class - value: [****] [79] EAP-Message - value: [ñ [80] Message-  
Authenticator - value: [.2{wëbÜ"Åp05<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
```

Wenn ein Endbenutzer versucht, zu einer Website zu navigieren und von WLC an die ISE-Umleitungs-URL umgeleitet wurde.

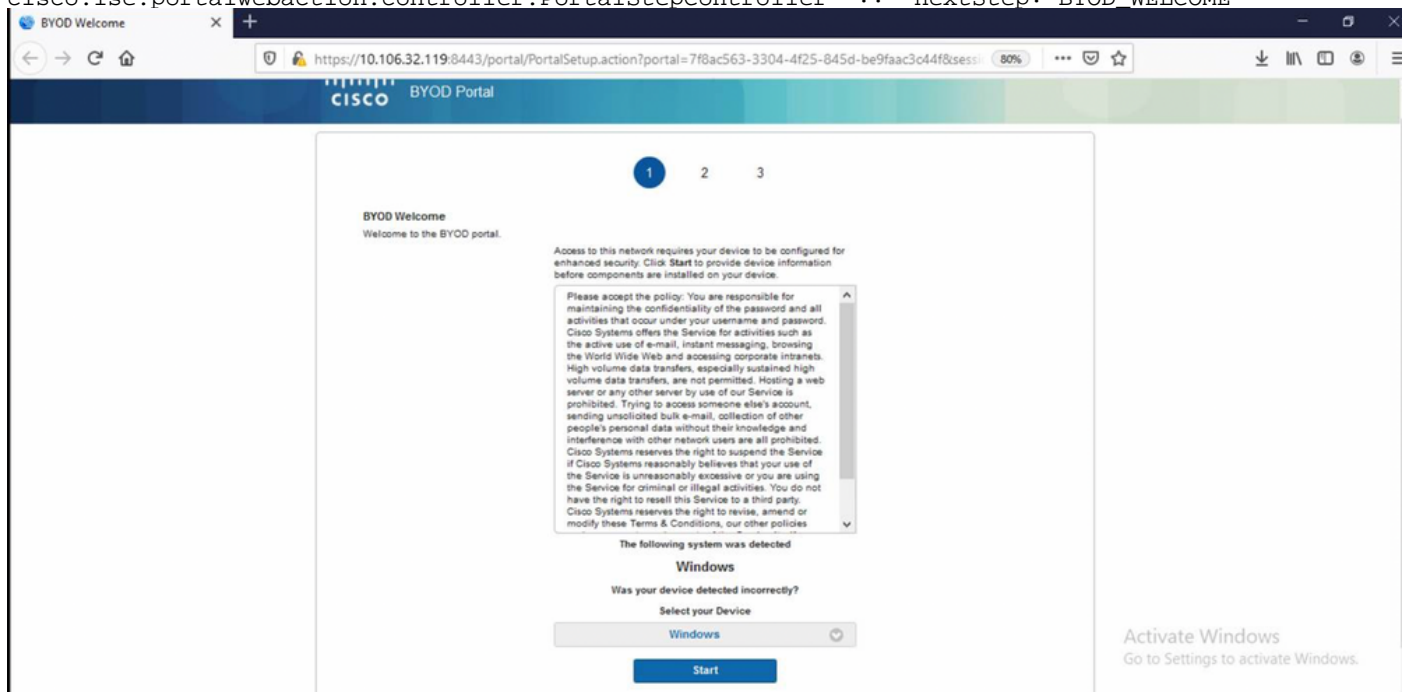
#### Guest.log -

```
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 'dotlxuserin
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

```



Klicken Sie auf der BYOD-Willkommensseite auf **Start**.

```

2020-12-02 05:44:01,926 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][[]
cisco.ise.portalwebaction.actions.BasePortalAction -::dotlxuser:- 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 -::dotlxuser:-
currentStep: BYOD_WELCOME

```

Die ISE bewertet nun, ob die für BYOD erforderlichen Dateien/Ressourcen vorhanden sind oder nicht, und setzt sich in den BYOD-INIT-Status ein.

```

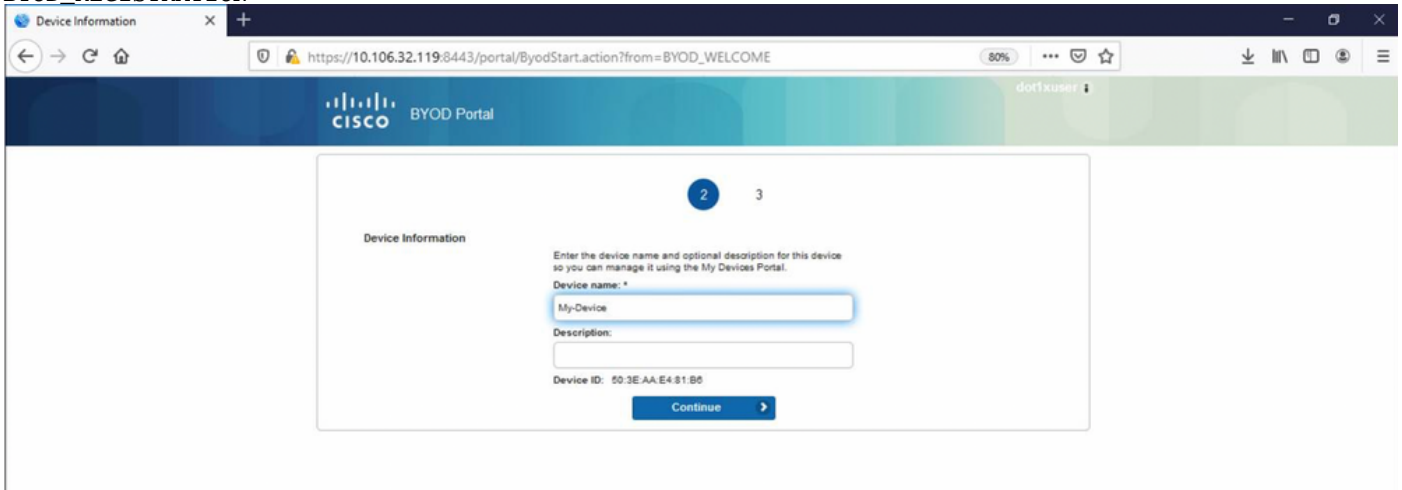
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][[]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -::dotlxuser:- userAgent=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All),
nspStatus=SUCCESS 2020-12-02 05:44:01,936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

```

```

https://10.106.32.119:8443/auth/provisioning/download/a2b317ee-df5a-4bda-abc3-
e4ec38ee188c/WirelessNSP.xml?sessionId=0a6a21b2000009f5fc770c7&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 -:dotlxuser:-
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 -:dotlxuser:- 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 -:dotlxuser:- ++++ 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 -:dotlxuser:- nextStep:
BYOD_REGISTRATION

```

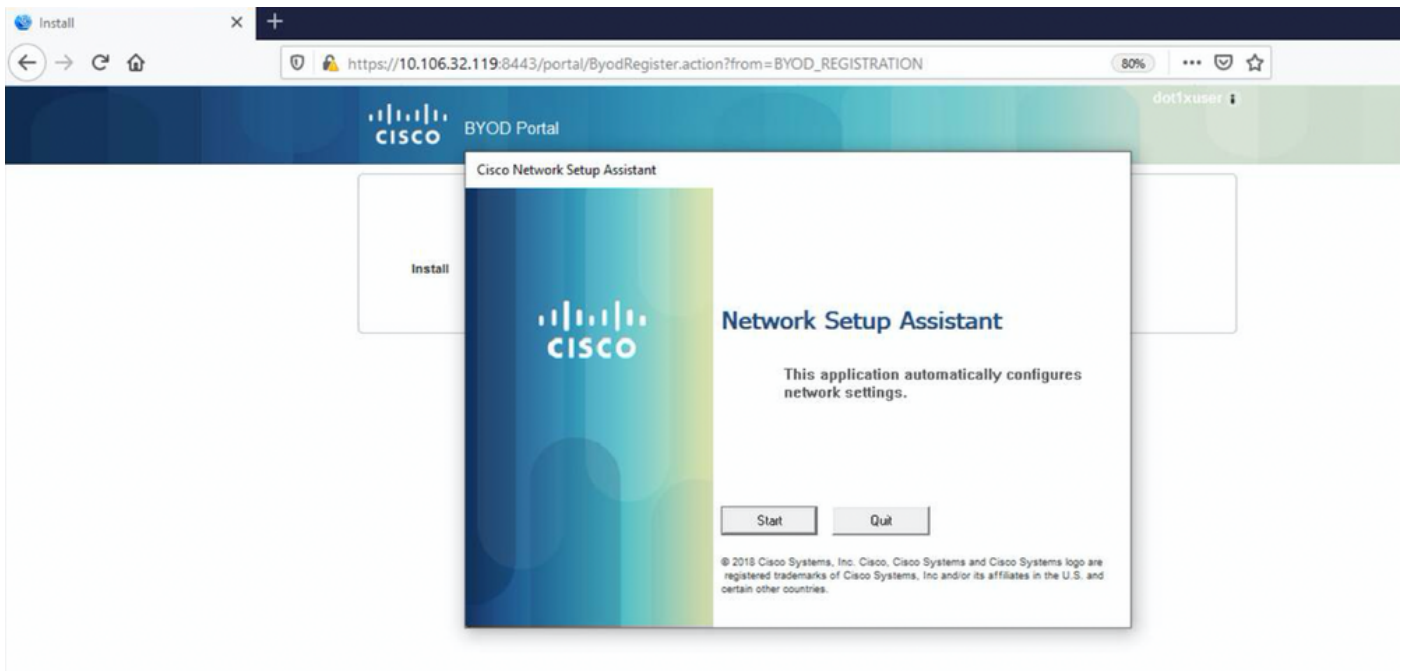


Geben Sie den Gerätenamen ein, und klicken Sie auf Registrieren.

```

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- 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 -:dotlxuser:- executeAction... 2020-12-02
05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][]
cisco.ise.portalwebaction.actions.BasePortalAction -:dotlxuser:- 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 -:dotlxuser:- 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 -
:dotlxuser:- Register Device : 50:3E:AA:E4:81:B6 username= dotlxuser idGroupID= aal3bb40-8bff-
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 -:dotlxuser:-
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 -:dotlxuser:- ++++
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 -:dotlxuser:- 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 -:dotlxuser:- StreamingServlet
URI:/auth/provisioning/download/90a6dc9c-4aae-4431-a453-81141ec42d2d/NetworkSetupAssistant.exe

```

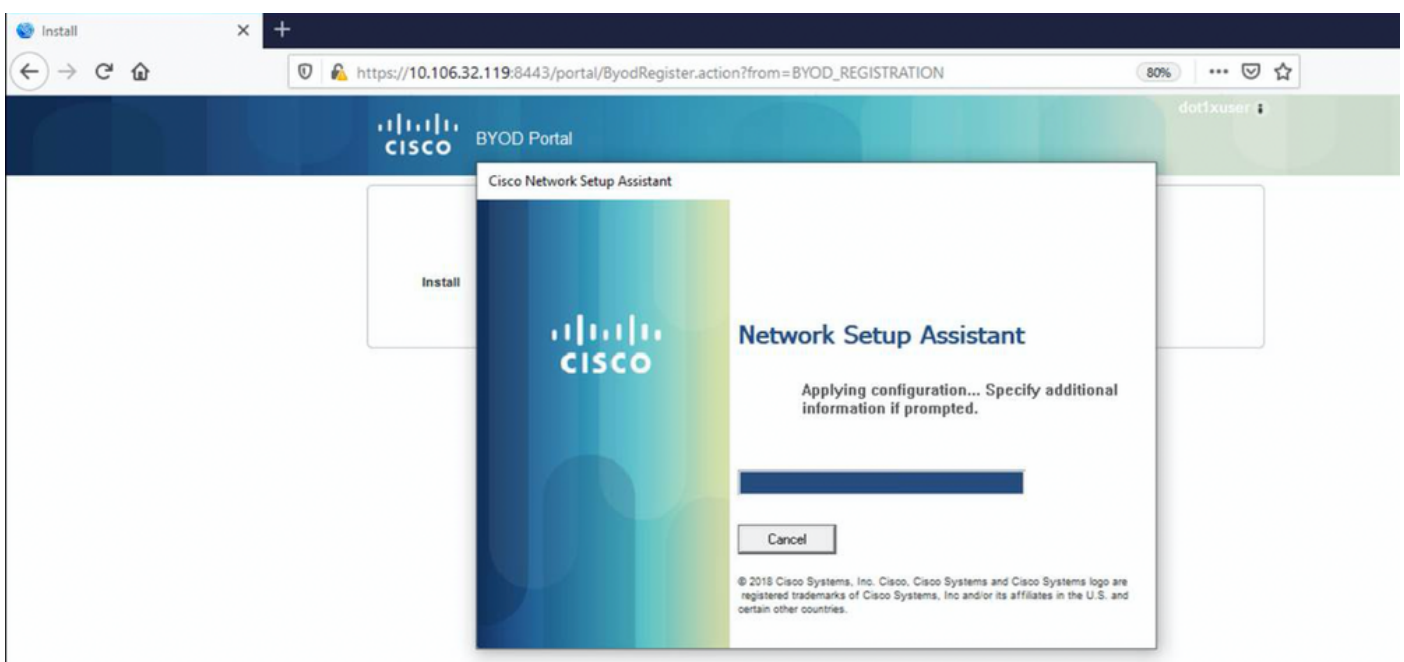


Wenn der Benutzer auf Start in der NSA klickt, wird eine Datei mit dem Namen **spwProfile.xml** temporär auf dem Client erstellt, die den Inhalt von Cisco-ISE-NSP.xml kopiert, der auf dem TCP-Port 8905 heruntergeladen wurde.

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 -::-
```

Nachdem Sie den Inhalt von **spwProfile.xml** gelesen haben, konfiguriert die NSA das Netzwerkprofil und generiert eine CSR-Nummer. Anschließend sendet sie diesen an die ISE, um mithilfe der URL <https://10.106.32.119:8443/auth/pkclient.exe> ein Zertifikat zu erhalten.



## 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 certificate 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 = dotlxuser
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=dotlxuser 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=dotlxuser] ---
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 = dotlxuser 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=dotlxuser, 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 ]
```

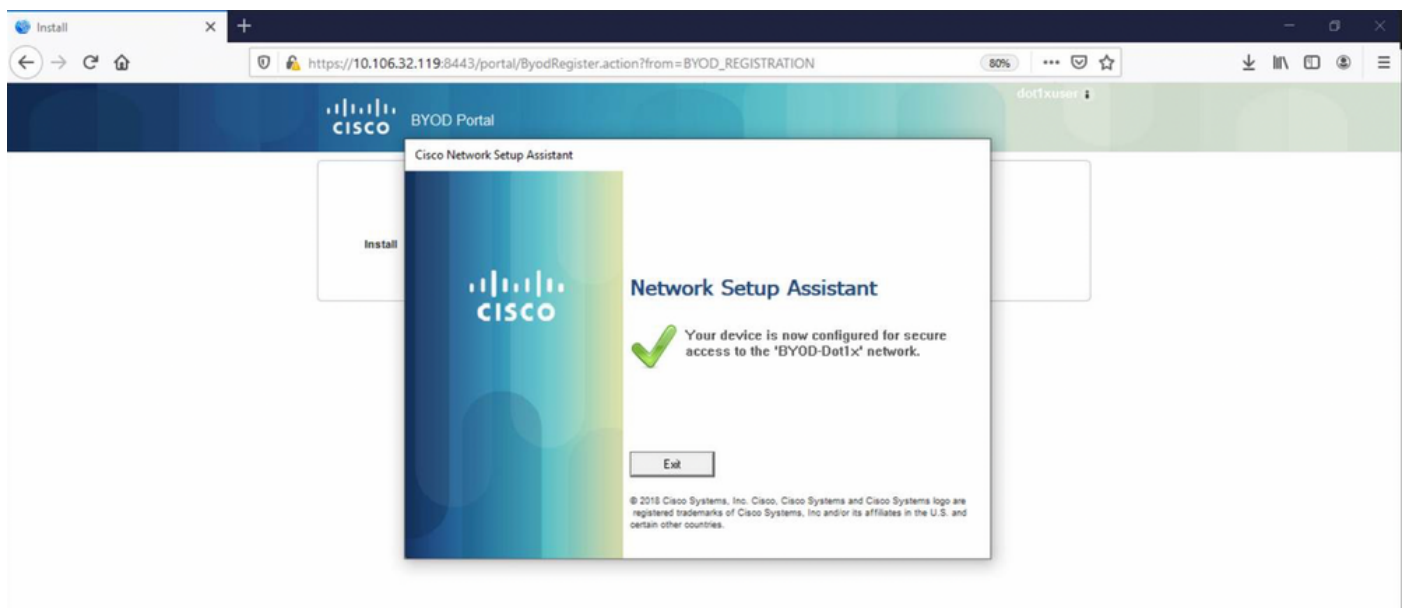
ise-psc.log -

```
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 -



```
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=dotlxuser 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=dotlxuser 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
```

Nach der Zertifikatsinstallation initiieren die Clients eine weitere Authentifizierung mithilfe von EAP-TLS und erhalten vollständigen Zugriff.

prt-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=dotluser,CallingStationID=50-
3e-aa-e4-81-b6,RADIUS PACKET:: Code=2(AccessAccept) Identifier=5 Length=231 [1] User-Name -
value: [dotluser] [25] Class - value: [****] [79] EAP-Message - value: [E [80] Message-
Authenticator - value: [Û(ØyËöžö|kÔ,.)] [26] MS-MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-
Key - value: [****] ,RADIUSHandler.cpp:2216
```

## Clientprotokolle (spw-Protokolle)

### Der Client initiiert den Download des Profils.

```
[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
```

### Der Client überprüft, ob der WLAN-Dienst ausgeführt wird.

```
[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]
```

### Der Client beginnt mit der Anwendung des Profils -

```
[Mon Nov 30 03:34:37 2020] ApplyProfile - Start... [Mon Nov 30 03:34:37 2020] User Id:
dotluser, 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]
```

### Zertifikat für die Client-Installation.

```
[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 = dotlxuser 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 konfiguriert Wireless-Profil

```
[Mon Nov 30 03:34:51 2020] Configuring wireless profiles... [Mon Nov 30 03:34:51 2020]
Configuring ssid [BYOD-Dotlx] [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]
```

## Profil

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