Configure Single SSID Wireless BYOD on Windows and ISE

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Theory

Configure

- ISE Configuration
- WLC Configuration

Verify

- Authentication Flow Verification
- Check the My Devices Portal

Troubleshoot

- General Information
- Working Log Analysis
  - ISE Logs
  - Client Logs (spw logs)

Introduction

This document describes how to configure Bring Your Own Device on Cisco Identity Services Engine for Windows Machine using both Single-SSID and Dual-SSID.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Configuration of Cisco Identity Services Engine (ISE) Version 3.0
- Configuration of Cisco WLC
- Bring Your Own Device (BYOD) Working

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE Version 3.0
- Windows 10
- WLC and AP

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Theory

In Single SSID BYOD, only one SSID is used for both onboardings of devices and later giving full access to the Registered Devices. First, the user connects to the SSID using the user name and password (MSCHAPv2). Once authenticated successfully on ISE, the user gets redirected to the BYOD Portal. Once the Device Registration is done, the end-client downloads the Native Supplicant Assistant (NSA) from ISE . NSA is installed on the end client and downloads the Profile and certificate from ISE. The NSA configures the Wireless supplicant and the client installs the certificate. Endpoint performs another authentication to the same SSID using the downloaded certificate using EAP-TLS. ISE checks the new request from the client and verifies the EAP Method and Device Registration and gives full access to the device.

Windows BYOD Single SSID Steps

- Initial EAP-MSCHAPv2 authentication
- Redirection to BYOD portal
- Device registration
- NSA download
- Profile download
- Certificate download
- EAP-TLS Authentication

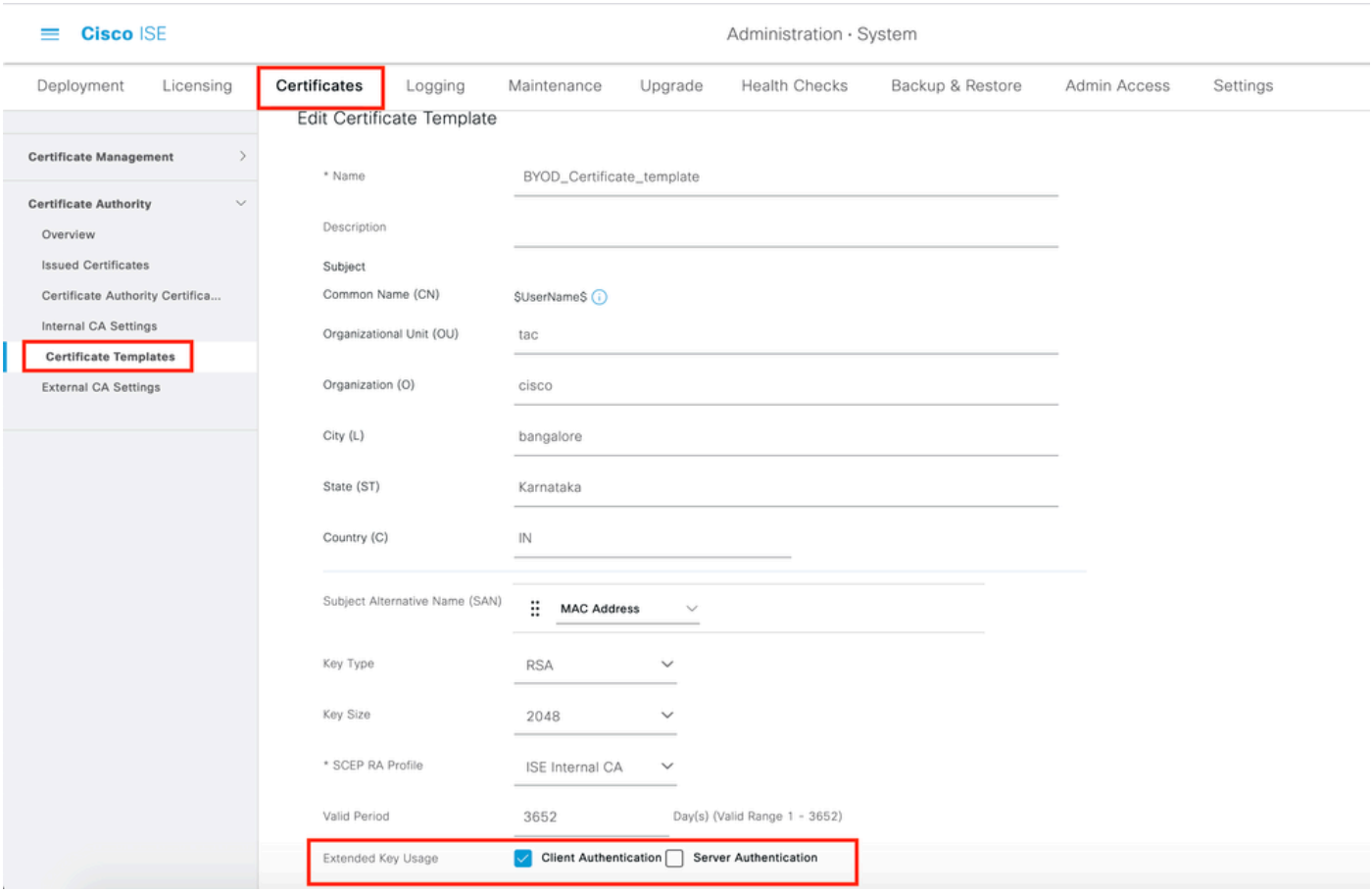
Configure

ISE Configuration

Step 1. Add network Device on ISE and configure RADIUS and shared key.

Navigate to **ISE > Administration > Network Devices > Add Network Device**.

Step 2. Create a **certificate template** for BYOD users. The template must have Client Authentication Enhanced Key Usage. You can use the default EAP_Certificate_Template.

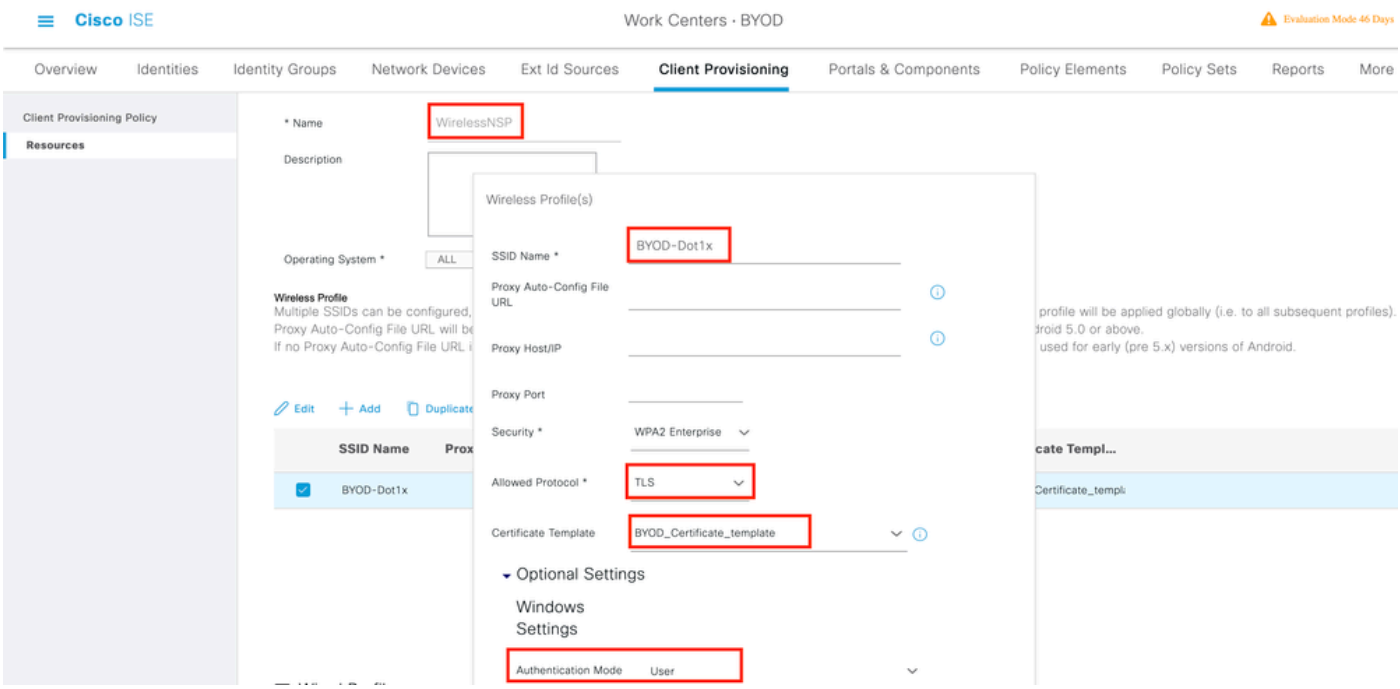


Step 3. Create a **Native Supplicant Profile** for a Wireless profile.

Navigate to **ISE > Work Centres > BYOD > Client Provisioning**. Click **Add** and choose **Native Supplicant Profile (NSP)** from the drop-down.

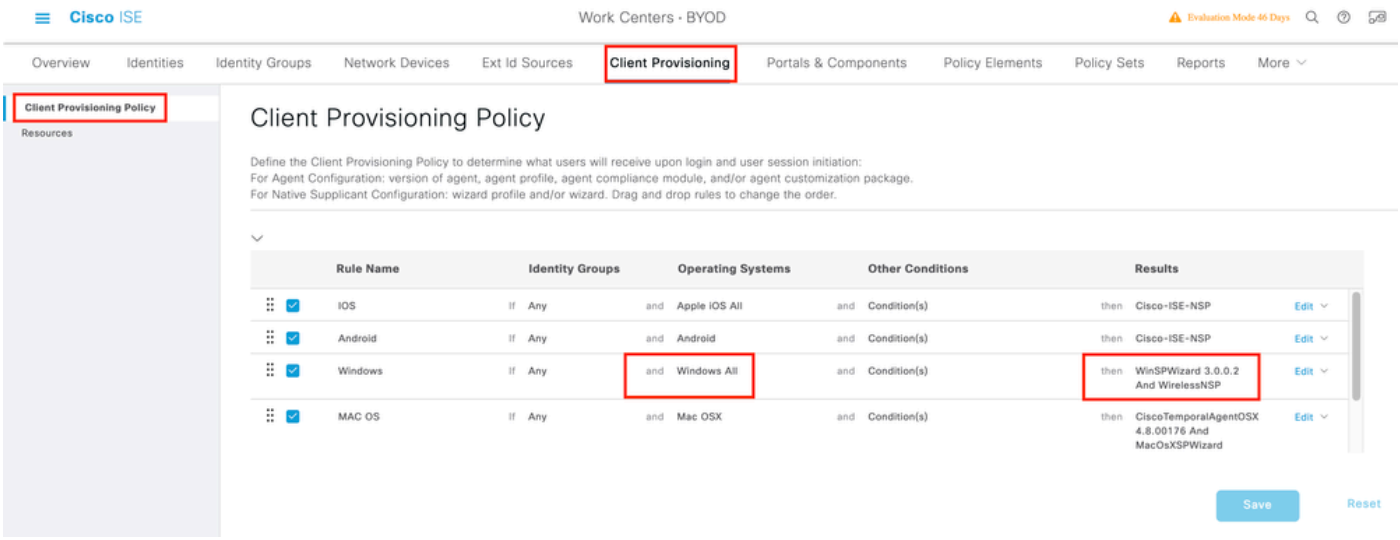
Here, the SSID name must be the same as you connected before you did a single SSID BYOD. Select the **Protocol** as TLS. Chose **Certificate template** as created in the previous step or you can use the default EAP_Certificate_Template.

Under **optional settings**, select **user** or **User and Machine authentication** as per your requirement. In this example, it is configured as user authentication. Leave other settings as default.



Step 4. Create **Client Provisioning Policy** for Windows Device.

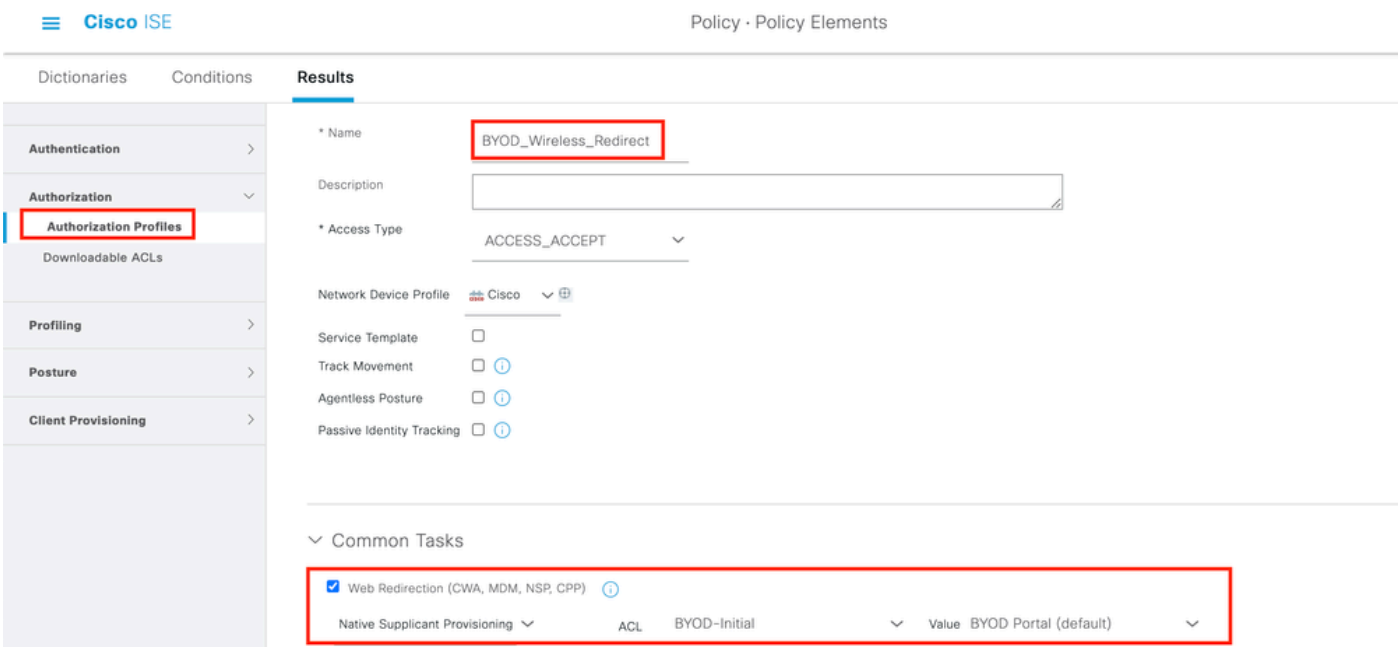
Navigate to **ISE > Work Centres > BYOD > Client Provisioning > Client Provisioning Policy**. Select the Operating System as **Windows ALL**. Select **WinSPWizard 3.0.0.2 and NSP** created in the previous step.



Step 5. Create an **Authorization Profile** for devices not registered as BYOD devices.

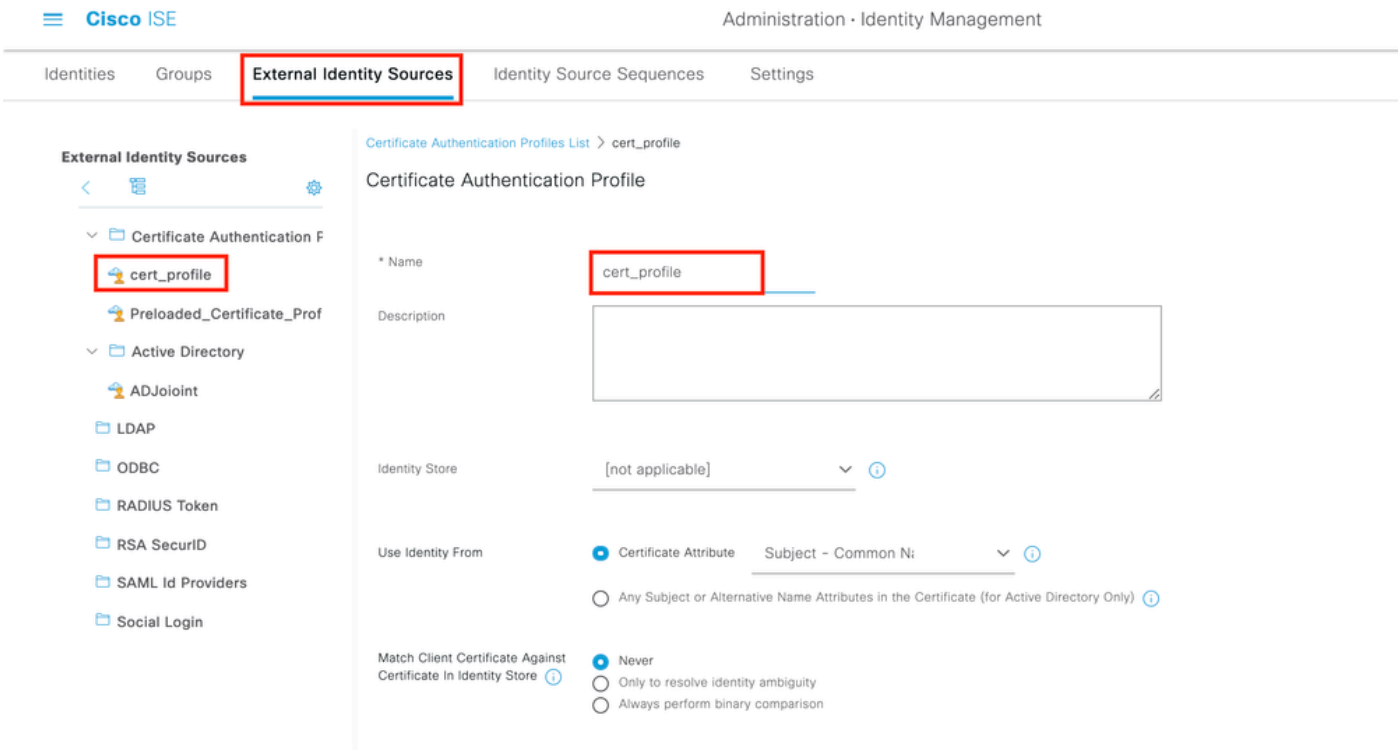
Navigate to **ISE > Policy > Policy Elements > Results> Authorization > Authorization Profiles > Add**.

Under **Common Task**, select **Native Supplicant Provisioning**. Define a Redirect ACL Name that is created on WLC and select the **BYOD Portal**. Here, Default Portal is used. You can create a custom BYOD Portal. Navigate to **ISE > Work Centres > BYOD > Portals and components** and click **Add**.

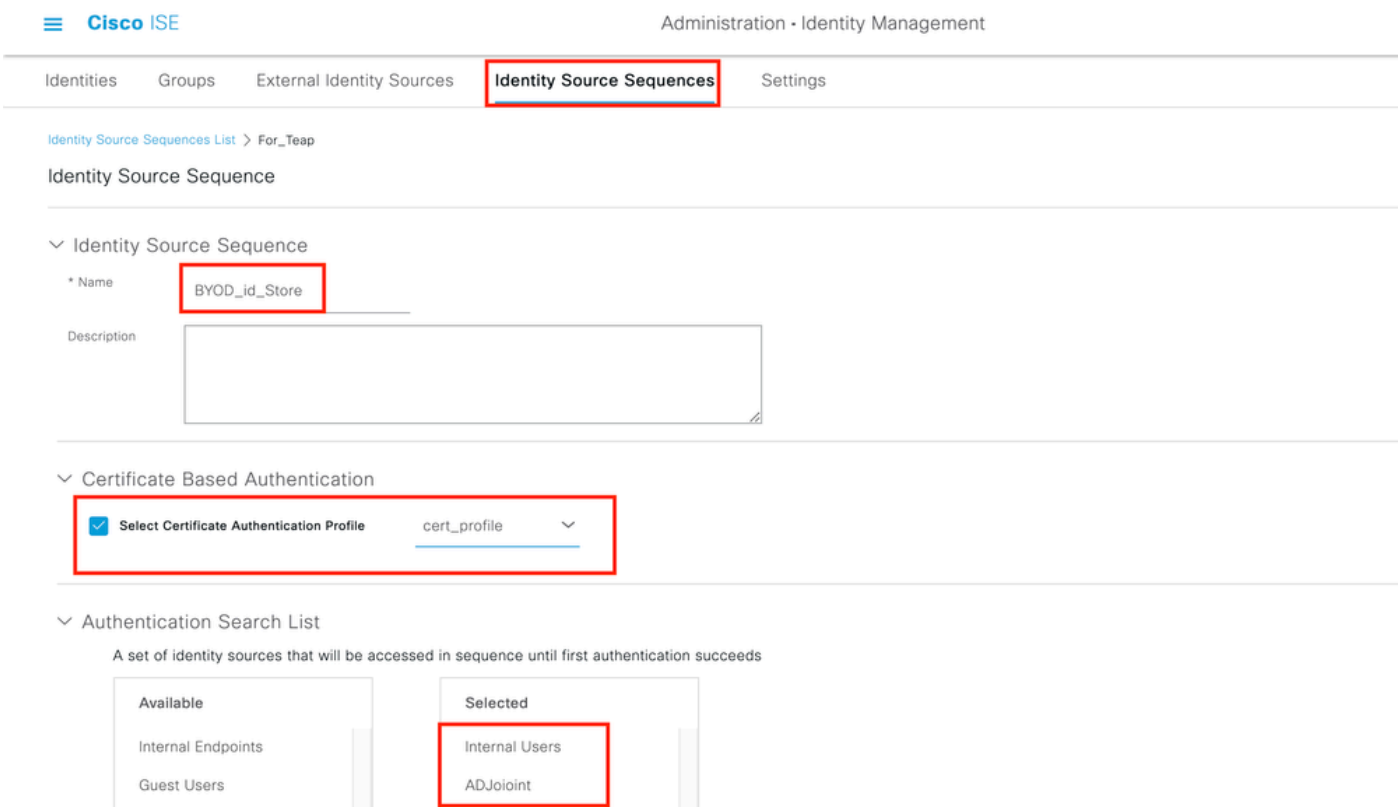


Step 6. Create a **certificate profile**.

Navigate to **ISE > Administration > External Identity Sources > Certificate Profile**. Here create a **new certificate profile** or use the **default certificate profile**.



Step 7. Create an **identity source sequence** and select the **certificate profile** created in the previous step or use the **default certificateprofile**. This is required when users perform EAP-TLS after BYOD registration to get full access.



Step 8. Create a **Policy Set**, **authentication Policy**, and **Authorization Policy**.

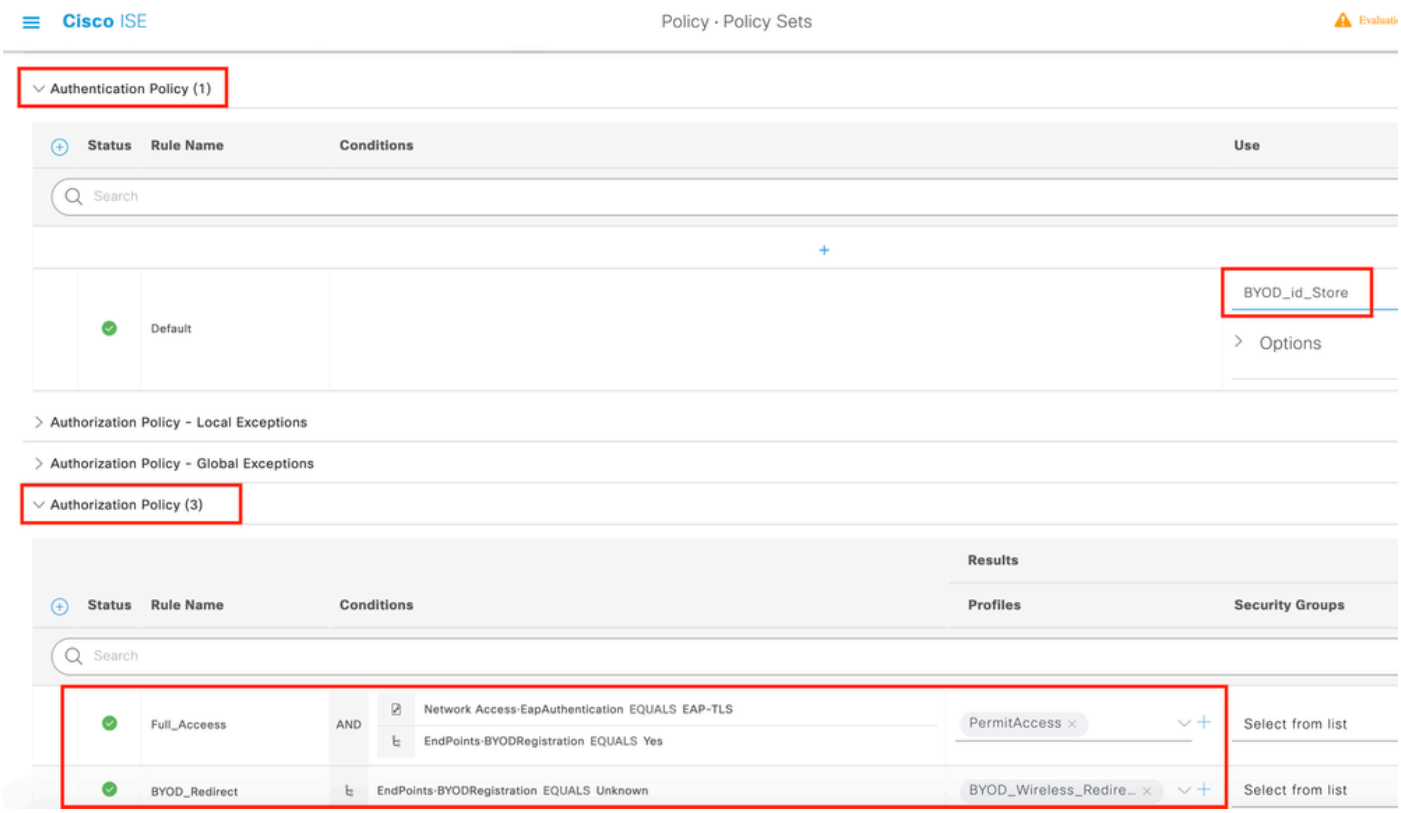
Navigate to **ISE > Policy > Policy Sets**. Create a **Policy Set** and **Save**.

Create an **Authentication Policy** and select the **identity source sequence** created in the previous step.

Create an **Authorization Policy**. You must create two policies.

1. For devices that are not BYOD Registered, give redirect profile created in step 5.

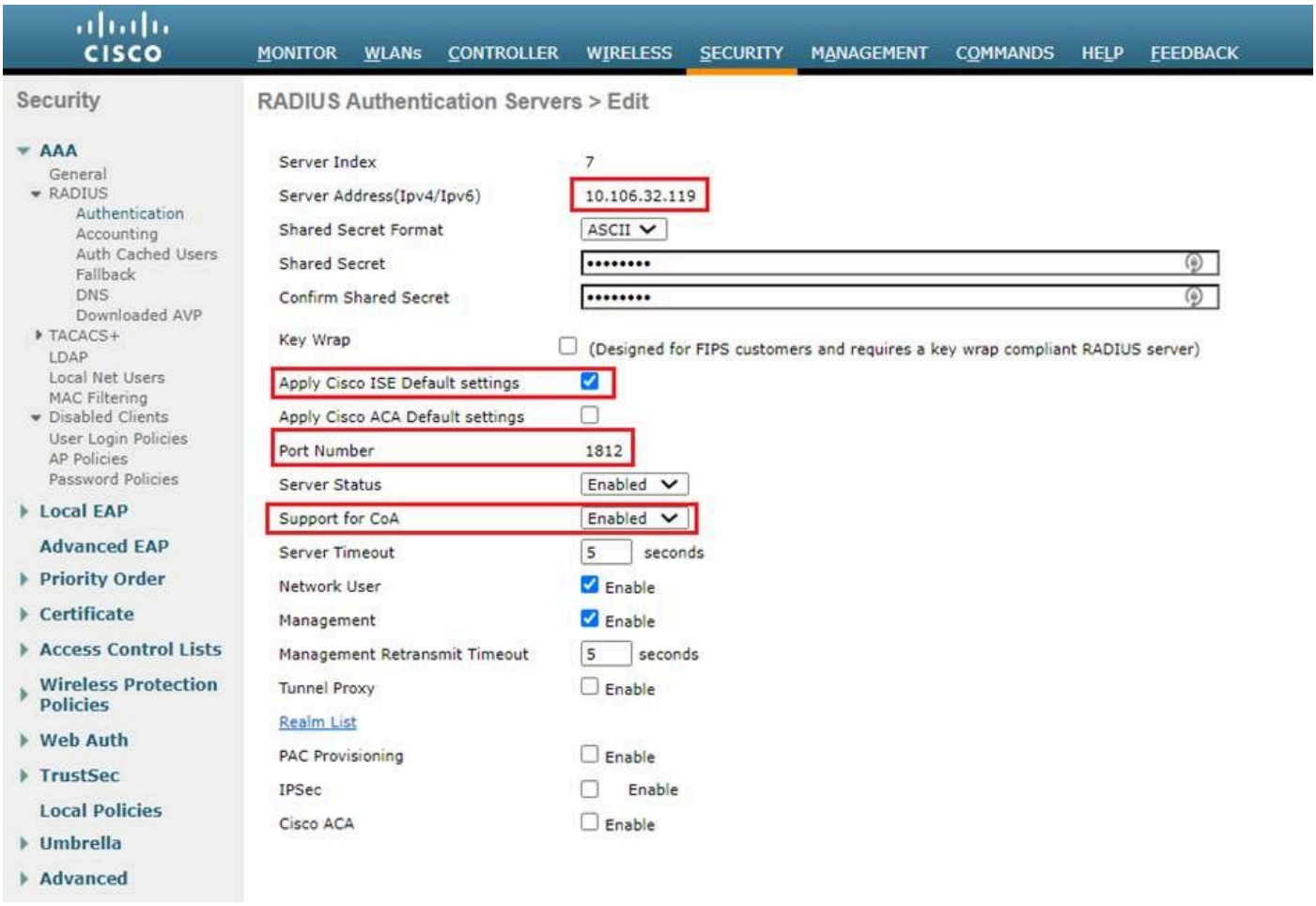
2. For devices that are BYOD registered and doing EAP-TLS, give full access to these devices.



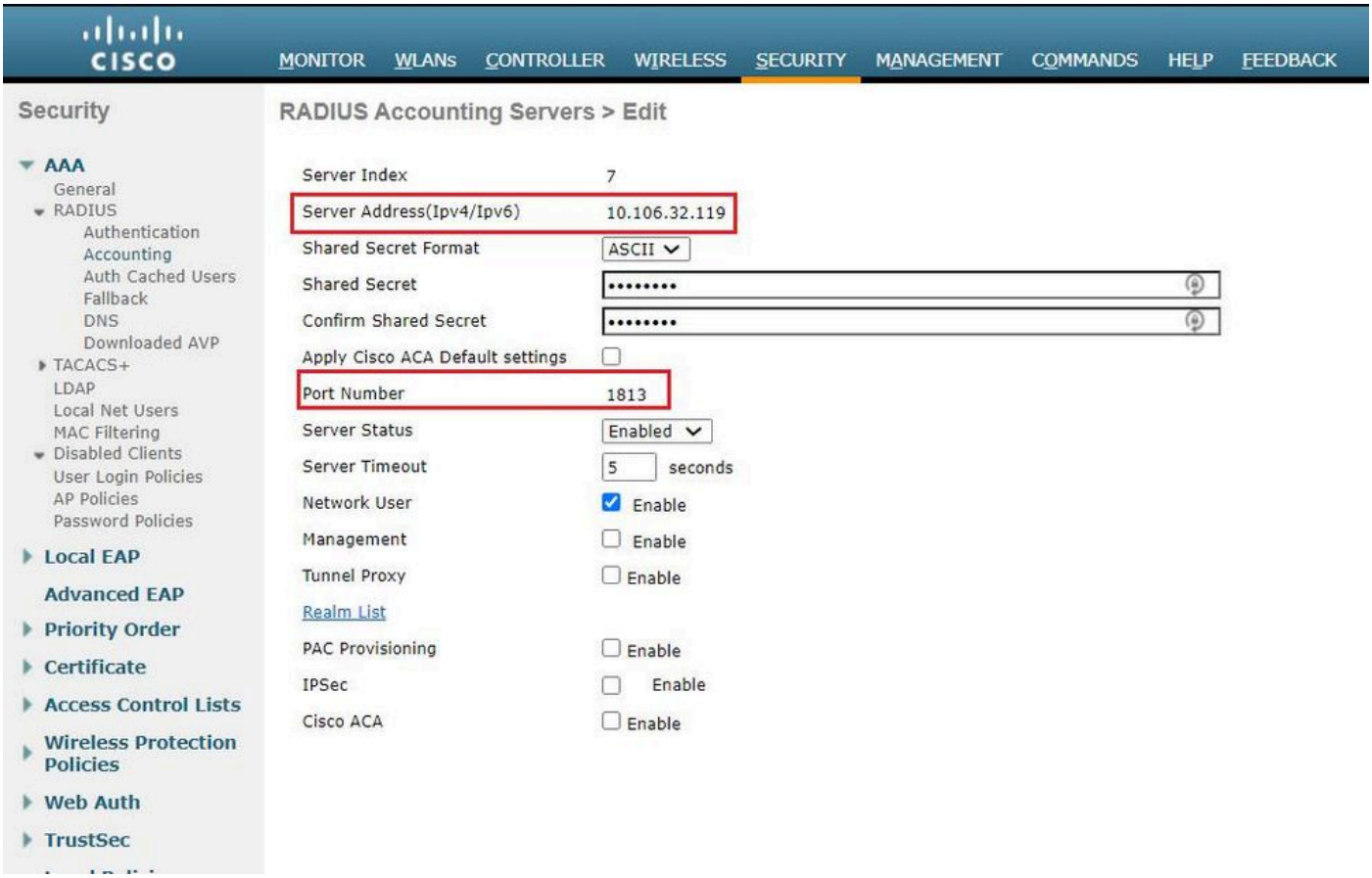
WLC Configuration

Step 1. Configure Radius Server on WLC.

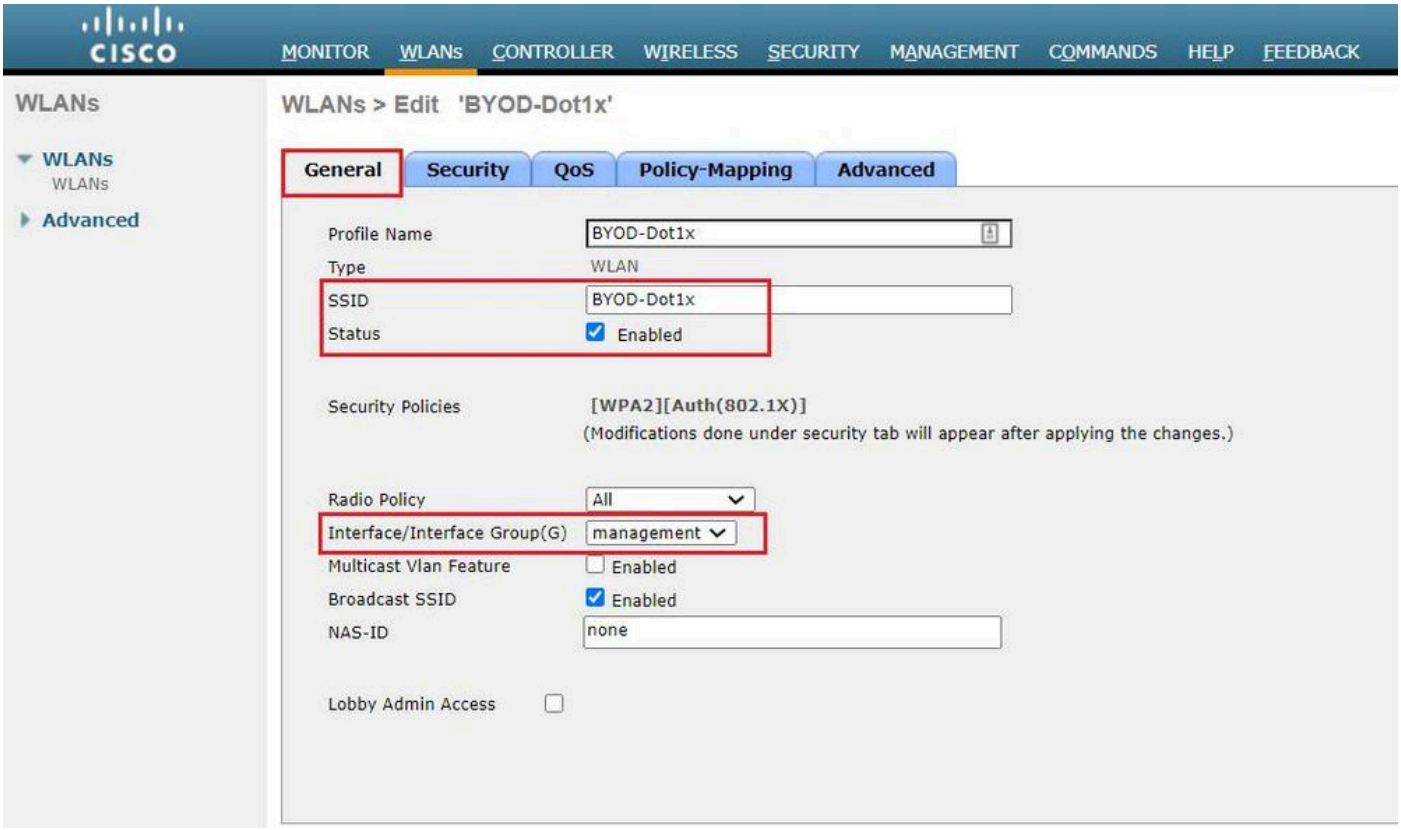
Navigate to **Security > AAA > Radius > Authentication**.



Navigate to **Security > AAA > Radius > Accounting**.



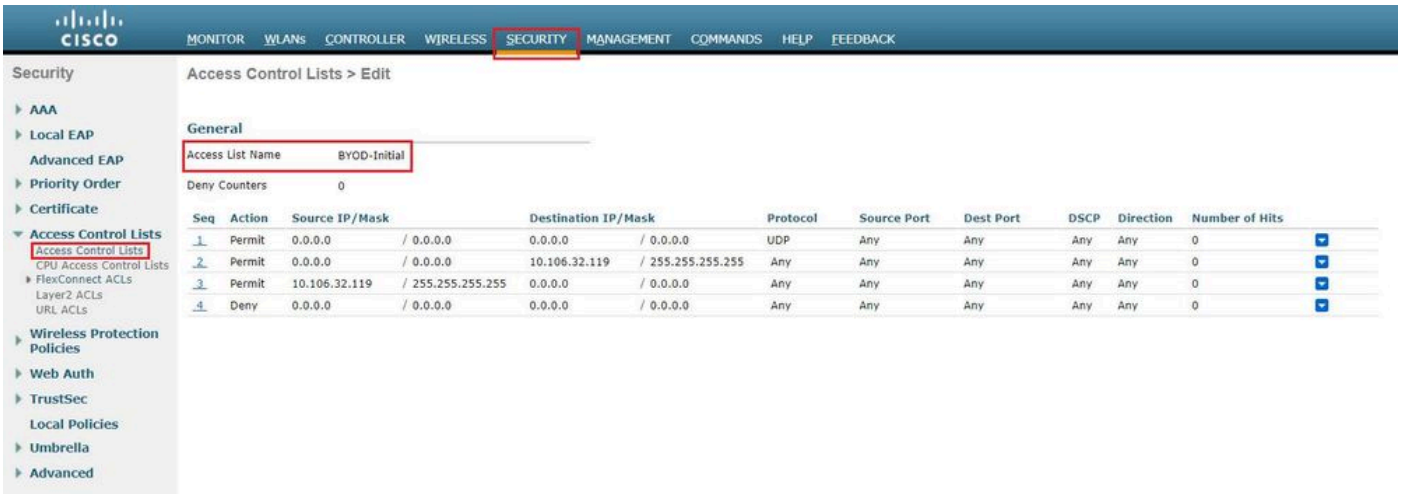
Step 2. Configure a Dot1x SSID.



Step 3. Configure Redirect ACL to provide limited access for provisioning the device.

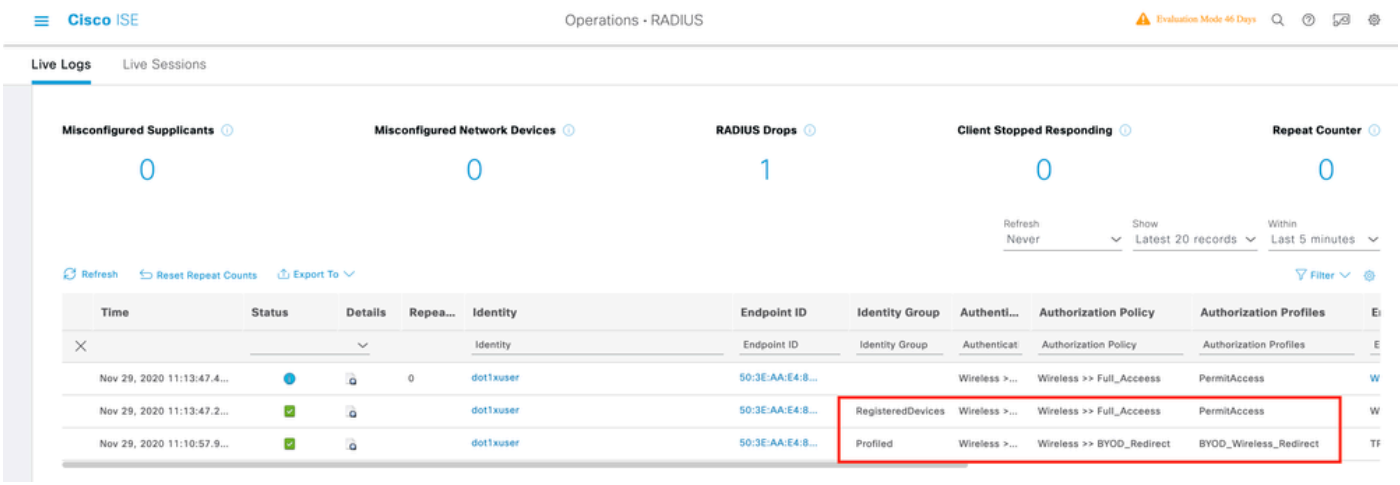
- Permit UDP traffic to DHCP and DNS (DHCP is allowed by default).
- Communication to ISE.
- Deny other traffic.

Name: BYOD-Initial (OR whatever you manually named the ACL in the Authorization Profile)

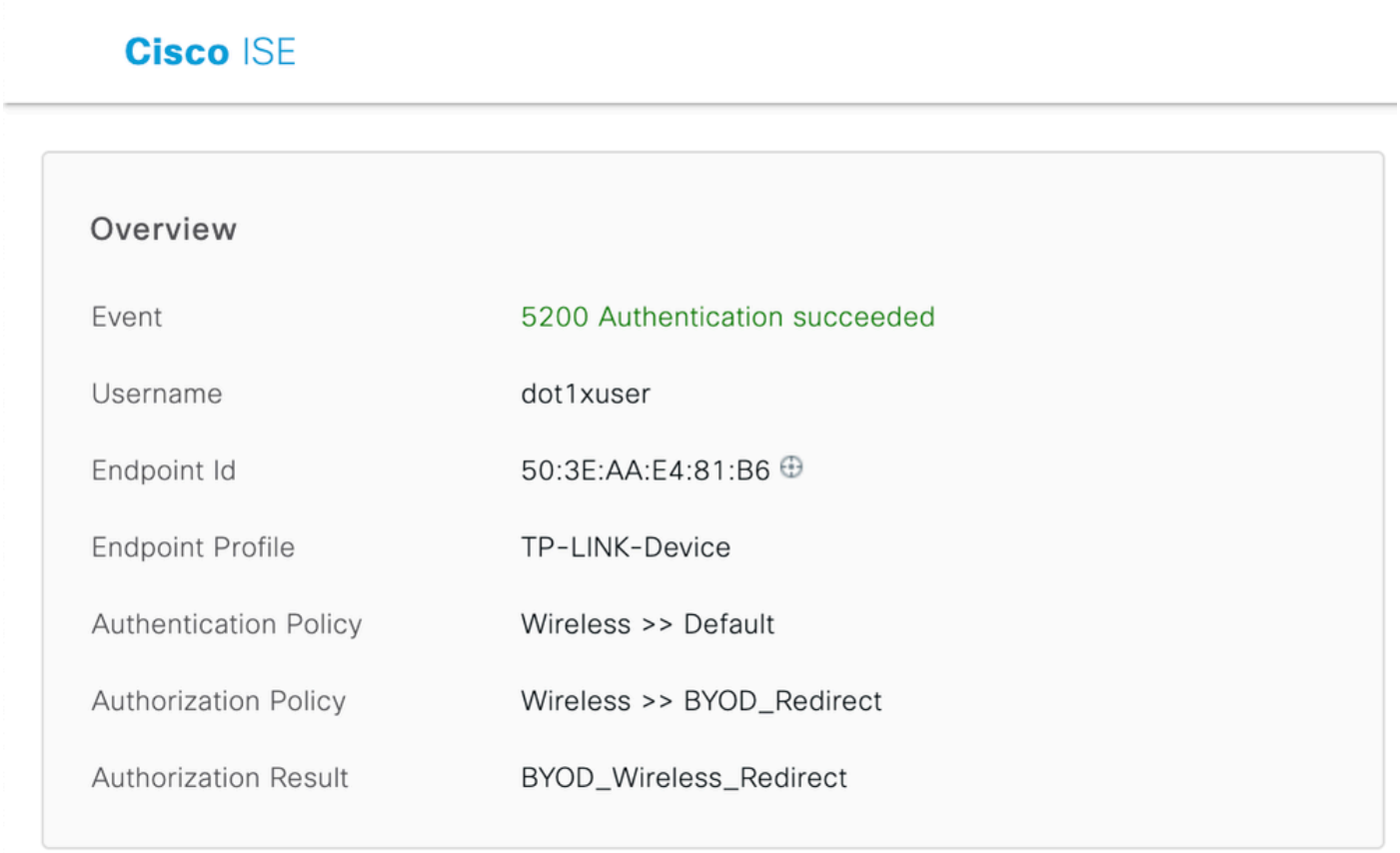


Verify

Authentication Flow Verification



1. At first log in, user performs PEAP authentication using a username and password. On ISE, user hits the Redirect Rule BYOD-Redirect.

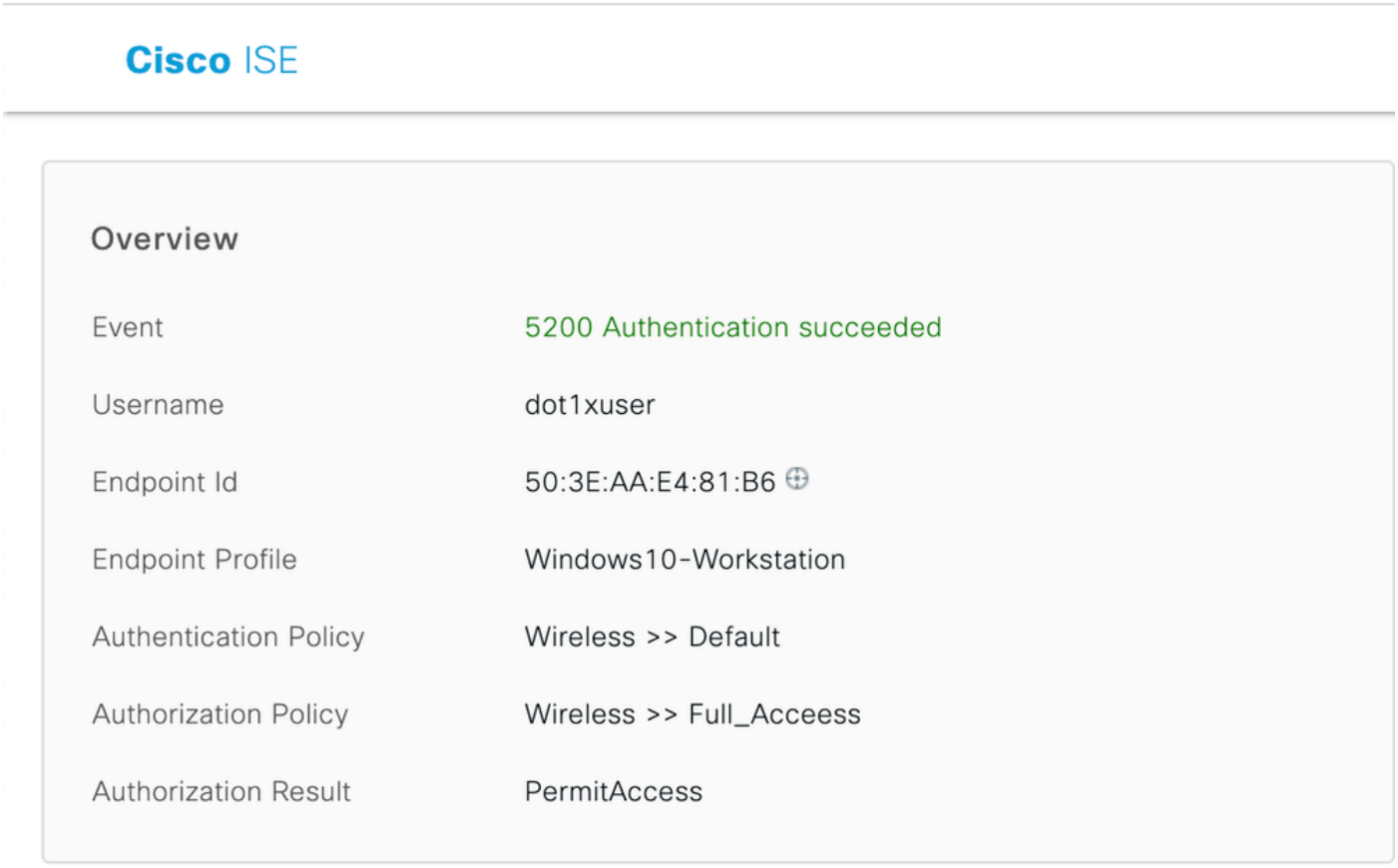


Cisco ISE

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. After the BYOD Registration, user is added to the Registered Device and now performs EAP-TLS and gets Full Access.

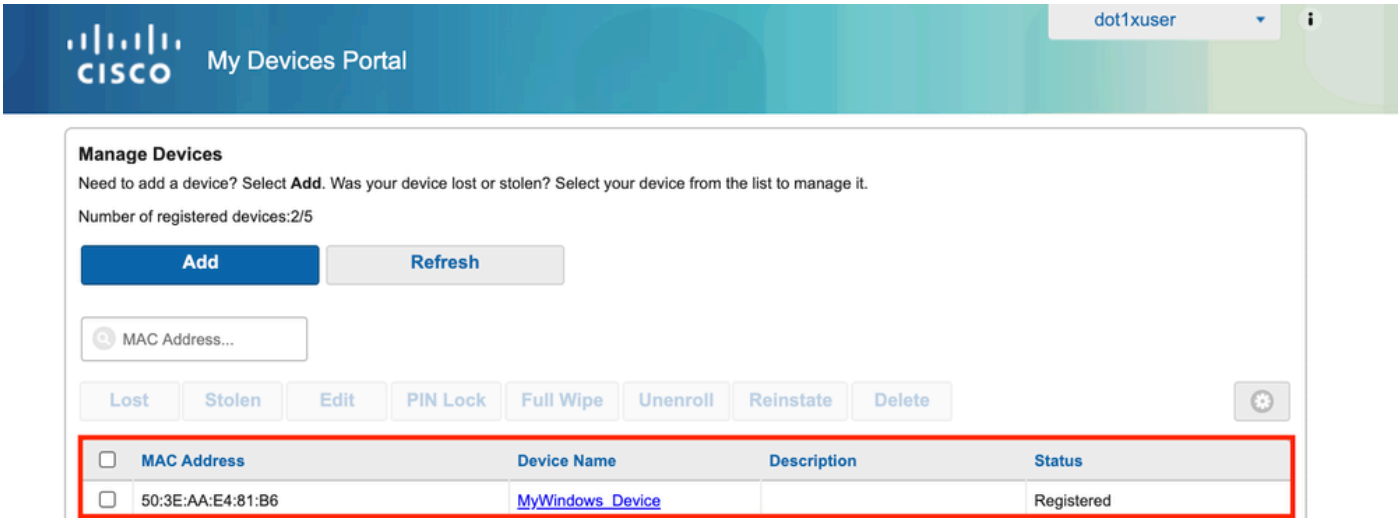


Check the My Devices Portal

Navigate to **MyDevices Portal** and **Log In** with the credentials. You can see the device name and the Registration status.

You can create a **URL** for the MyDevices Portal.

Navigate to **ISE > Work Centres > BYOD > Portal and Components > My Devices Portal > Login Settings** and then Enter the **Fully Qualified URL**.



Troubleshoot

General Information

For BYOD process, these ISE components have to be enabled in debug on PSN nodes.

scep - scep log messages. Target log files guest.log and ise-psc.log.

client-webapp – the component responsible for infrastructure messages. Target log file – ise-psc.log

portal-web-action - the component responsible for client provisioning policy processing. Target log file - guest.log.

portal - all Portal related events. Target log file - guest.log

portal-session-manager -Target log files - Portal session related debug messages - gues.log

ca-service- ca-service messages -Target log files -caservice.log and caservice-misc.log

ca-service-cert - ca-service certificate messages - Target log files - caservice.log and caservice-misc.log

admin-ca- ca-service admin messages -Target log files ise-psc.log, caservice.log and casrvice-misc.log

certprovisioningportal - certificate provisioning portal messages -Target log files ise-psc.log

nsf- NSF related messages -Target log files ise-psc.log

nsf-session - Session cache-related messages -Target log files ise-psc.log

runtime-AAA – All Runtime events. Target log file – prrt-server.log .

For the client-side logs :

Look for %temp%\spwProfileLog.txt (ex: C:\Users\<username>\AppData\Local\Temp\spwProfileLog.txt)

Working Log Analysis

ISE Logs

Initial Access-Accept with redirect ACL and Redirect URL for BYOD Portal.

Prrt-server.log

```
Radius,2020-12-02 05:43:52,395,DEBUG,0x7f433e6b8700,cntx=0008590803,sesn=isee30-primary/392215758/699,C

     [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=0a6a

     [26] MS-MPPE-Send-Key - value: [****]

     [26] MS-MPPE-Recv-Key - value: [****] ,RADIUSHandler.cpp:2216
```

When an end-user tries to navigate to a website and was redirected by WLC to the ISE redirect 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

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.u


2020-12-02 05:43:58,339 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portalwebaction.u


2020-12-02 05:43:58,344 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portal.util.Porta

2020-12-02 05:43:58,344 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] cisco.ise.portal.util.Porta

2020-12-02 05:43:58,344 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-5][] com.cisco.ise.portal.Gateway


2020-12-02 05:43:58,355 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.c


2020-12-02 05:43:58,356 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a


2020-12-02 05:43:58,356 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a


2020-12-02 05:43:58,360 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a
```

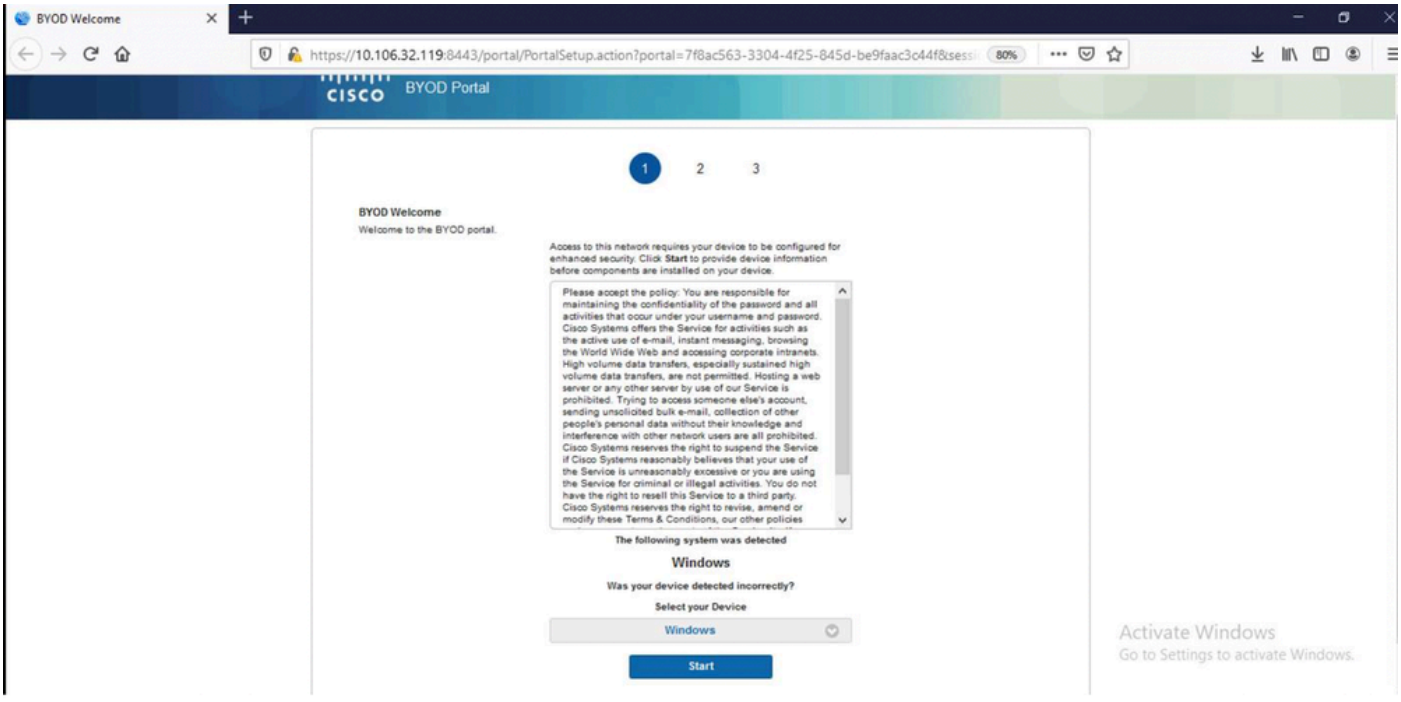
```
2020-12-02 05:43:58,360 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.a

2020-12-02 05:43:58,360 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,361 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,362 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager
2020-12-02 05:43:58,365 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cpm.guestaccess.flowmanager

2020-12-02 05:43:58,366 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-7][] cisco.ise.portalwebaction.c
2020-12-02 05:40:35,611 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-6][] com.cisco.ise.portalSession
2020-12-02 05:40:35,611 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-6][] cisco.ise.portalwebaction.c
```



Click **Start** on the BYOD Welcome page.

```
020-12-02 05:44:01,926 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.ac

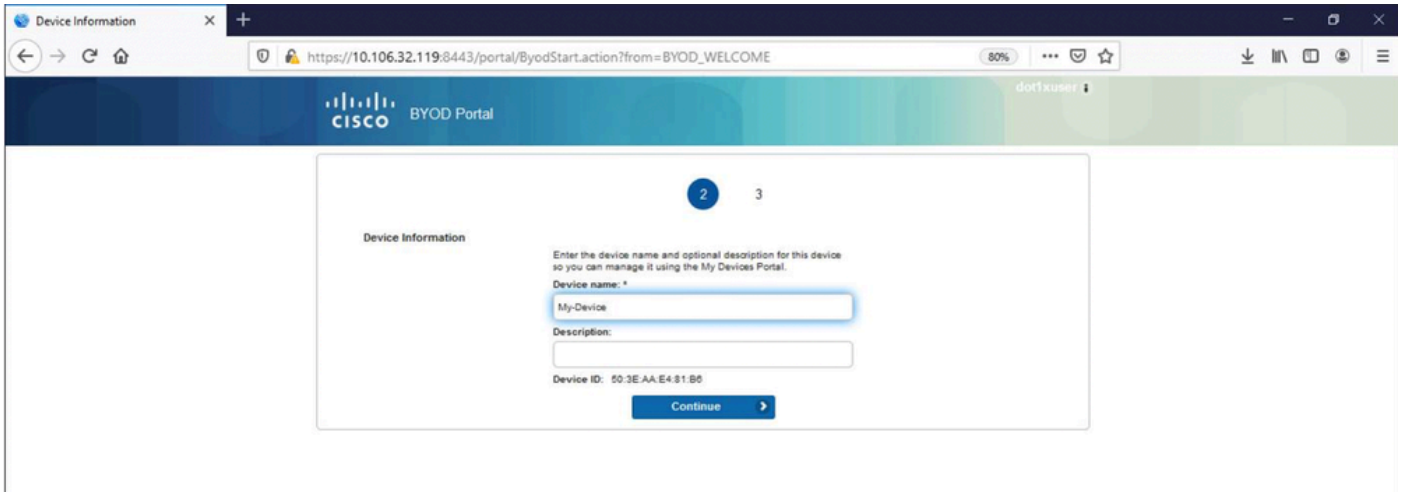
2020-12-02 05:44:01,926 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c
```

At this point, ISE evaluates if the necessary files/resources required for BYOD are present or not, and sets itself to BYOD INIT state.

```
2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.ste

2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] guestaccess.flowmanager.ste
2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager
2020-12-02 05:44:01,936 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cpm.guestaccess.flowmanager


2020-12-02 05:44:01,950 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c
2020-12-02 05:44:01,950 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c
```



Enter the **device name** and click **register**.

```
2020-12-02 05:44:14,682 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a

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.By

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a

2020-12-02 05:44:14,682 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.a

2020-12-02 05:44:14,683 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.apiservices

username= dot1xuser

idGroupID= aa13bb40-8bff-11e6-996c-525400b48521

authStoreGUID= 9273fe30-8c01-11e6-996c-525400b48521

nadAddress= 10.106.33.178

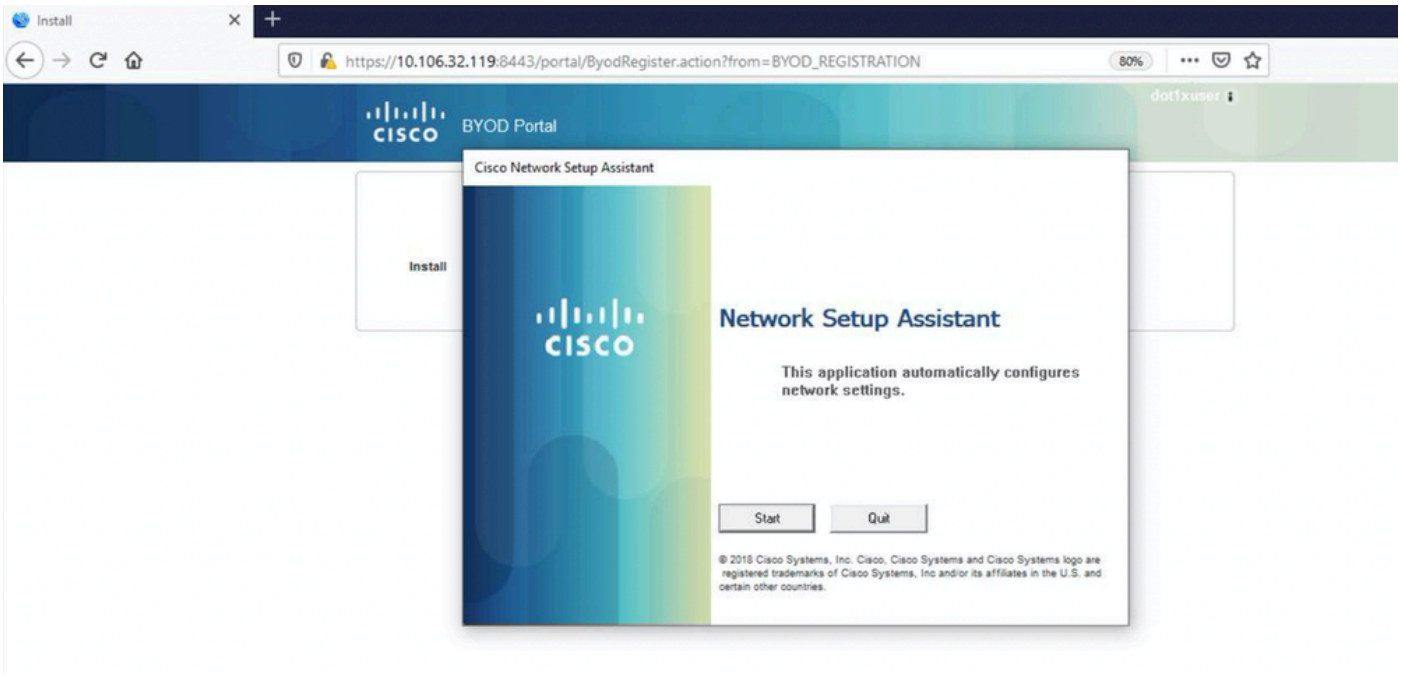
isSameDeviceRegistered = false

2020-12-02 05:44:14,900 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cpm.guestaccess.flowmanager

2020-12-02 05:44:14,902 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.ise.portalwebaction.c

2020-12-02 05:44:01,954 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][] cisco.ise.portalwebaction.c

2020-12-02 05:44:14,969 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.client.provision



Now, when the user clicks **Start** on the NSA, a file named **spwProfile.xml** is temporarily created on the client copying the content from Cisco-ISE-NSP.xml downloaded on TCP port 8905.

Guest.log

```
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
2020-12-02 05:45:03,275 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet

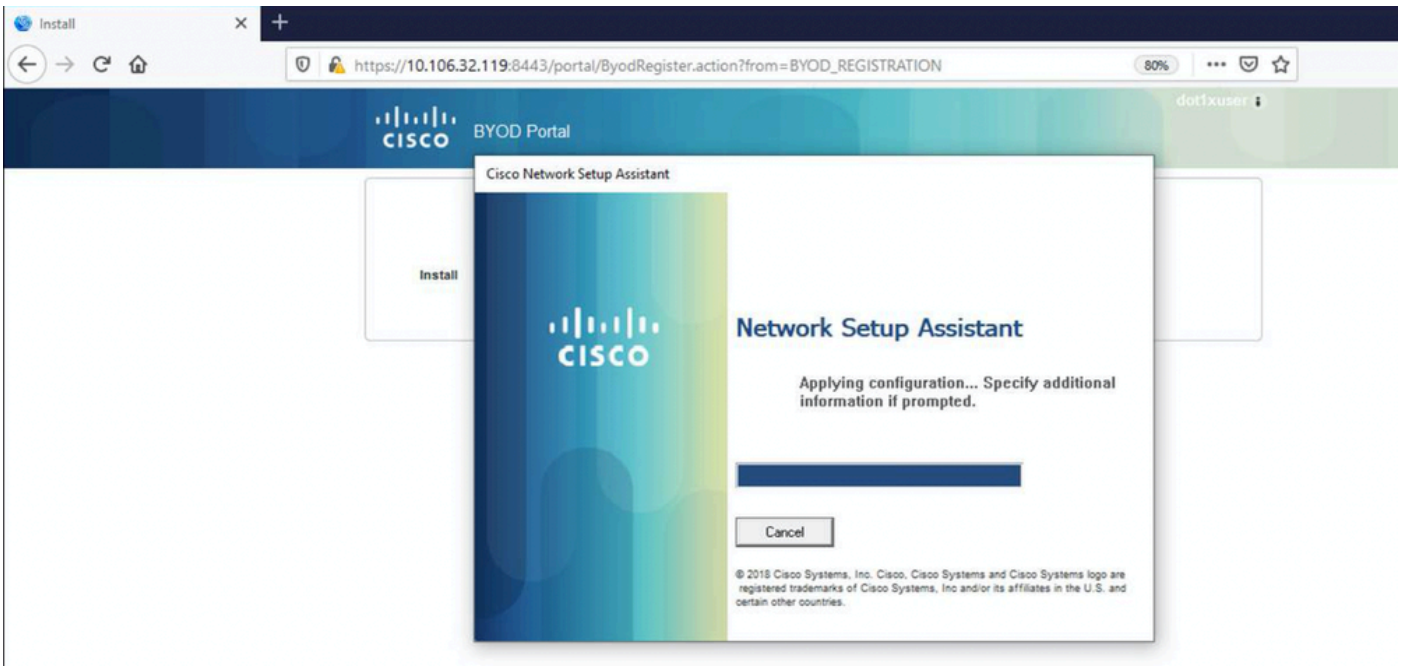


2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
2020-12-02 05:45:03,308 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
<name>WirelessNSP</name>
<spw_xml_version>2.0</spw_xml_version>
<description/>
<OSs>
<os>ALL</os>
</OSs>
<ConnectionSetting>
<connectionTypes>
<connectionType>wireless</connectionType>
</connectionTypes>
<wifiSSIDs>
<SSID>BYOD-Dot1x</SSID>
</wifiSSIDs>
<EAPConfig>
<EncryptionTunnel>
<SecurityType>WPA2</SecurityType>
<OuterEAPMethod xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="TLS">
<EAPType>TLS</EAPType>
<enableServerCertValidation>false</enableServerCertValidation>
</OuterEAPMethod>
</EncryptionTunnel>
</EAPConfig>
<CertTemplateInfo>
<certTemplateId>e2c32ce0-313d-11eb-b19e-e60300a810d5</certTemplateId>

---output omitted---
```

```
2020-12-02 05:45:03,310 DEBUG [portal-http-service15][] cisco.cpm.client.provisioning.StreamingServlet
```

After you read the content from the spwProfile.xml, NSA configures the network profile and generates a CSR, and sends it to the ISE to get a certificate using the URL PKI Client



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

2020-12-02 05:45:11,331 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert

2020-12-02 05:45:11,331 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.provisioning.cert

2020-12-02 05:45:11,331 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] cisco.cpm.scep.util.ScepUti
2020-12-02 05:45:11,331 INFO   [https-jsse-nio-10.106.32.119-8443-exec-1][] com.cisco.cpm.scep.ScepCert
2020-12-02 05:45:11,332 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
2020-12-02 05:45:11,332 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkcsPkiEn
2020-12-02 05:45:11,333 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
2020-12-02 05:45:11,333 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
2020-12-02 05:45:11,334 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-1][] org.jscep.message.PkiMessag
```

ca-service.log

```
2020-12-02 05:45:11,379 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
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 0x67e
2020-12-02 05:45:11,379 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
```

caservice-misc.log

```
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
```

caservice.log

```
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
    1: 50-3E-AA-E4-81-B6

2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
2020-12-02 05:45:11,380 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e

2020-12-02 05:45:11,395 DEBUG  [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
2020-12-02 05:45:11,395 INFO   [CAService-Scep][scep job 4d22d2e256a247a302e900ffa71c35d75610de67 0x67e
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 ]
```

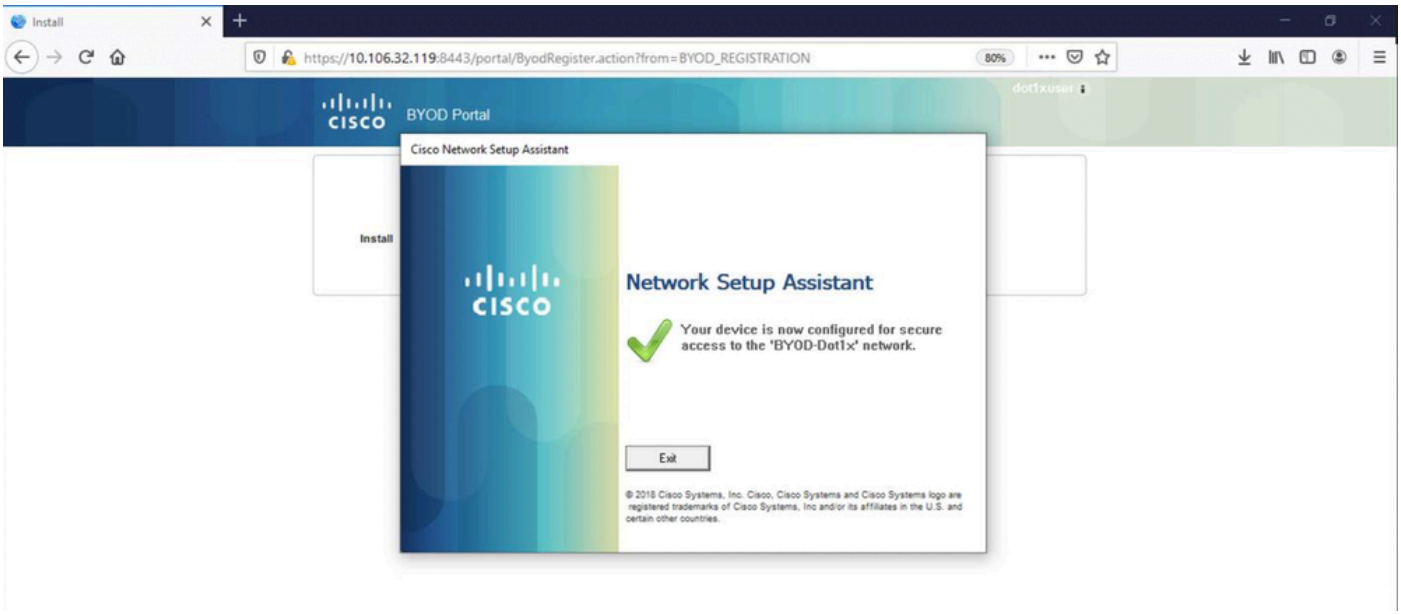
ise-psc.log

```
2020-12-02 05:45:11,407 DEBUG  [AsyncHttpClient-15-9][] org.jscep.message.PkiMessageDecoder -::::- Veri
```

caservice.log

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

ise-psc.log




```
2020-12-02 05:45:13,381 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cer
2020-12-02 05:45:13,381 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCer
2020-12-02 05:45:13,385 INFO   [https-jsse-nio-10.106.32.119-8443-exec-10][] com.cisco.cpm.scep.ScepCer
2020-12-02 05:45:13,596 DEBUG  [https-jsse-nio-10.106.32.119-8443-exec-10][] cisco.cpm.provisioning.cer
```

After certificate installation, clients initiate another authentication using EAP-TLS and get full access.

prrt-server.log

```
Eap,2020-12-02 05:46:57,175,INFO ,0x7f433e6b8700,cntx=0008591342,sesn=isee30-primary/392215758/701,CPMS
```

```
,EapParser.cpp:150

Radius,2020-12-02 05:46:57,435,DEBUG,0x7f433e3b5700,cntx=0008591362,sesn=isee30-primary/392215758/701,C
     [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
```

Client Logs (spw logs)

The client initiates to download the Profile.

```
[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:
[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 =
[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-

[Mon Nov 30 03:34:36 2020] [HTTPConnection] CrackUrl: host = 10.106.32.119, path = /auth/provisioning/d

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=b
[Mon Nov 30 03:34:36 2020] set ChallengePwd
```

Client Checks if WLAN Service is running.

```
[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: [{65E78DD
[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]
```

The client starts applying profile.

```
[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
[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]
```

Client install certificate.

```
[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=c
```

```
[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

] 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\AppDat

[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-e60300a81
```

ISE Configures Wireless Profile

```
[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
```

Profile

```
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">

<name>BYOD-Dot1x</name><SSIDConfig>

<SSID>
```

<name>BYOD-Dot1x</name>

</SSID>

<nonBroadcast>true</nonBroadcast>

</SSIDConfig>

<connectionType>ESS</connectionType>

<connectionMode>auto</connectionMode>

<autoSwitch>false</autoSwitch>

<MSM>

<security>

<authEncryption>

<authentication>WPA2</authentication>

<encryption>AES</encryption>

<useOneX>true</useOneX>

</authEncryption>

<OneX xmlns="http://www.microsoft.com/networking/OneX/v1">

<cacheUserData>true</cacheUserData>

<authMode>user</authMode>

<EAPConfig>

<EapHostConfig xmlns="http://www.microsoft.com/provisioning/EapHostConfig"

xmlns:eapCommon="http://www.microsoft.com/provisioning/EapCommon"

xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapMethodConfig">

<EapMethod>

<eapCommon:Type>13</eapCommon:Type>

<eapCommon:AuthorId>0</eapCommon:AuthorId>

</EapMethod>

<Config xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"

xmlns:eapTls="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV1">

<baseEap:Eap>

<baseEap:Type>13</baseEap:Type>

<eapTls:EapType>

<eapTls:CredentialsSource>

<eapTls:CertificateStore>

<eapTls:SimpleCertSelection>true</eapTls:SimpleCertSelection>

</eapTls:CertificateStore>

</eapTls:CredentialsSource>

<eapTls:ServerValidation>

<eapTls:DisableUserPromptForServerValidation>false</eapTls:DisableUserPromptForServerValidation>

<eapTls:ServerNames />

<eapTls:TrustedRootCA>5b a2 08 1e 17 cb 73 5f ba 5b 9f a2 2d 3b fc d2 86 0d a5 9b

</eapTls:TrustedRootCA>

</eapTls:ServerValidation>

<eapTls:DifferentUsername>false</eapTls:DifferentUsername>

</eapTls:EapType>

</baseEap:Eap>

</Config>

</EapHostConfig>

</EAPConfig>

</OneX>

</security>

</MSM>

</WLANProfile>

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], Singl

[Mon Nov 30 03:35:21 2020] WirelessProfile::IsSingleSSID - End

[Mon Nov 30 03:36:07 2020] Device configured successfully.