

# WindowsおよびISEでのシングルSSIDワイヤレスBYODの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[理論](#)

[設定](#)

[ISE の設定](#)

[WLC の設定](#)

[確認](#)

[認証フローの検証](#)

[\[My Devices\]ポータルの確認](#)

[トラブルシュート](#)

[一般情報](#)

[作業ログ分析](#)

[ISEログ](#)

[クライアントログ \( spwログ \)](#)

## 概要

このドキュメントでは、シングルSSIDとデュアルSSIDの両方を使用して、Cisco Identity Services Engine(ISE)for WindowsマシンでBring Your Own Device(BYOD)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ISEバージョン3.0の設定
- Cisco WLCの設定
- BYOD作業

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.0
- Windows 10

- WLCとAP

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 理論

シングルSSIDでは、BYODは1つのSSIDのみをデバイスの両方のオンボーディングに使用し、それ以降は登録済みデバイスへのフルアクセスを提供します。まず、ユーザ名とパスワード(MSCHAPv2)を使用してSSIDに接続します。ISEで正常に認証されると、ユーザはBYODポータルにリダイレクトされます。デバイス登録が完了すると、エンドクライアントはISEからネイティブサブリカントアシスタント(NSA)をダウンロードします。NSAはエンドクライアントにインストールされ、ISEからプロファイルと証明書をダウンロードします。NSAはワイヤレスサブリカントを設定し、クライアントは証明書をインストールします。エンドポイントは、EAP-TLSを使用して、ダウンロードされた証明書を使用して、同じSSIDに対して別の認証を実行します。ISEはクライアントからの新しい要求をチェックし、EAP方式とデバイス登録を確認し、デバイスへのフルアクセスを提供します。

Windows BYODシングルSSIDの手順：

- 初期EAP-MSCHAPv2認証
- BYODポータルへのリダイレクト
- デバイス登録
- NSAダウンロード
- プロファイルのダウンロード
- 証明書のダウンロード
- EAP-TLS 認証

## 設定

### ISE の設定

ステップ1: ISEでネットワークデバイスを追加し、RADIUSと共有キーを設定します。

[ISE] > [Administration] > [Network Devices] > [Add Network Device]に移動します。

ステップ2: BYODユーザの証明書テンプレートを作成します。テンプレートには、クライアント認証拡張キーの使用が必要です。デフォルトのEAP\_Certificate\_Templateを使用できます。

Cisco ISE Administration · System

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

**Certificate Management** >

**Certificate Authority** v

Overview

Issued Certificates

Certificate Authority Certifica...

Internal CA Settings

**Certificate Templates**

External CA Settings

### Edit Certificate Template

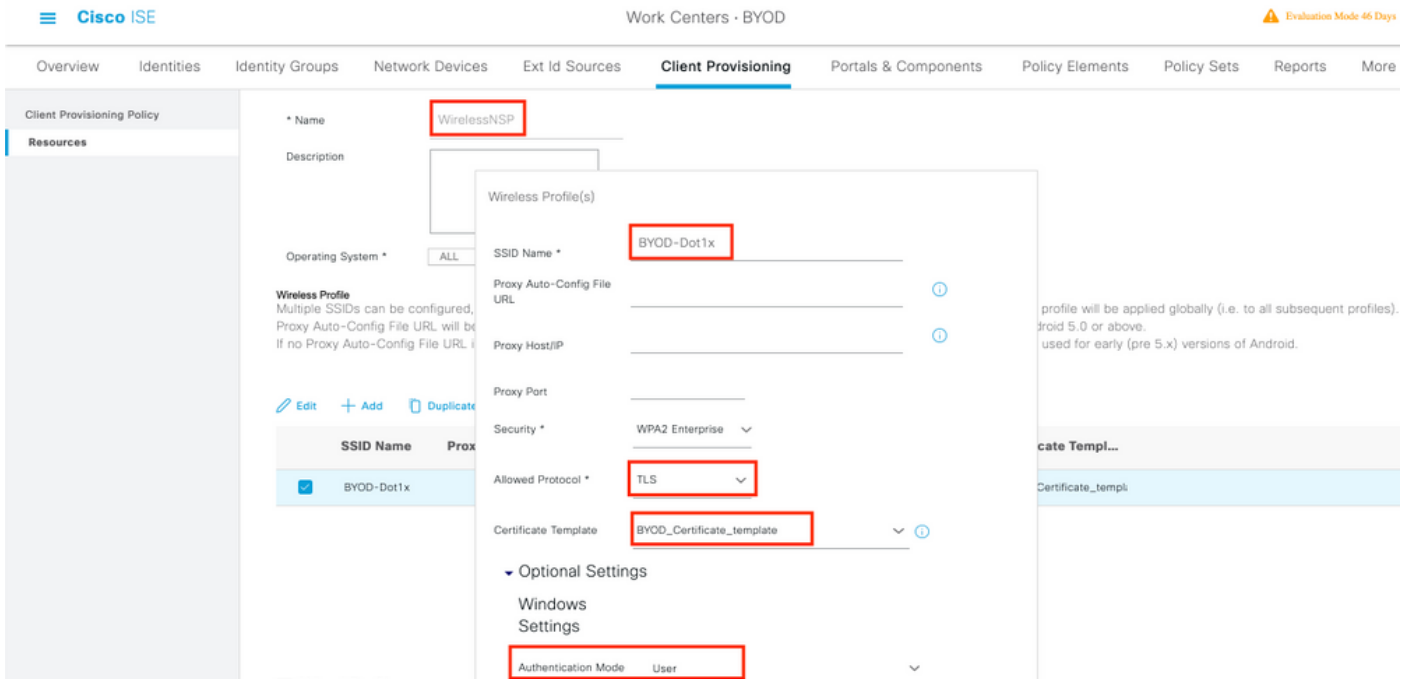
* Name	BYOD_Certificate_template
Description	
Subject	
Common Name (CN)	\$UserName\$ ⓘ
Organizational Unit (OU)	tac
Organization (O)	cisco
City (L)	bangalore
State (ST)	Karnataka
Country (C)	IN
Subject Alternative Name (SAN)	⋮ MAC Address v
Key Type	RSA v
Key Size	2048 v
* SCEP RA Profile	ISE Internal CA v
Valid Period	3652 Day(s) (Valid Range 1 - 3652)
Extended Key Usage	<input checked="" type="checkbox"/> Client Authentication <input type="checkbox"/> Server Authentication

ステップ3 : ワイヤレスプロファイルのネイティブサブリカントプロファイルを作成します。

[ISE] > [Work Centers] > [BYOD] > [Client Provisioning]に移動します。[Add]をクリックし、ドロップダウンから[Native Supplciant Profile (NSP)]を選択します。

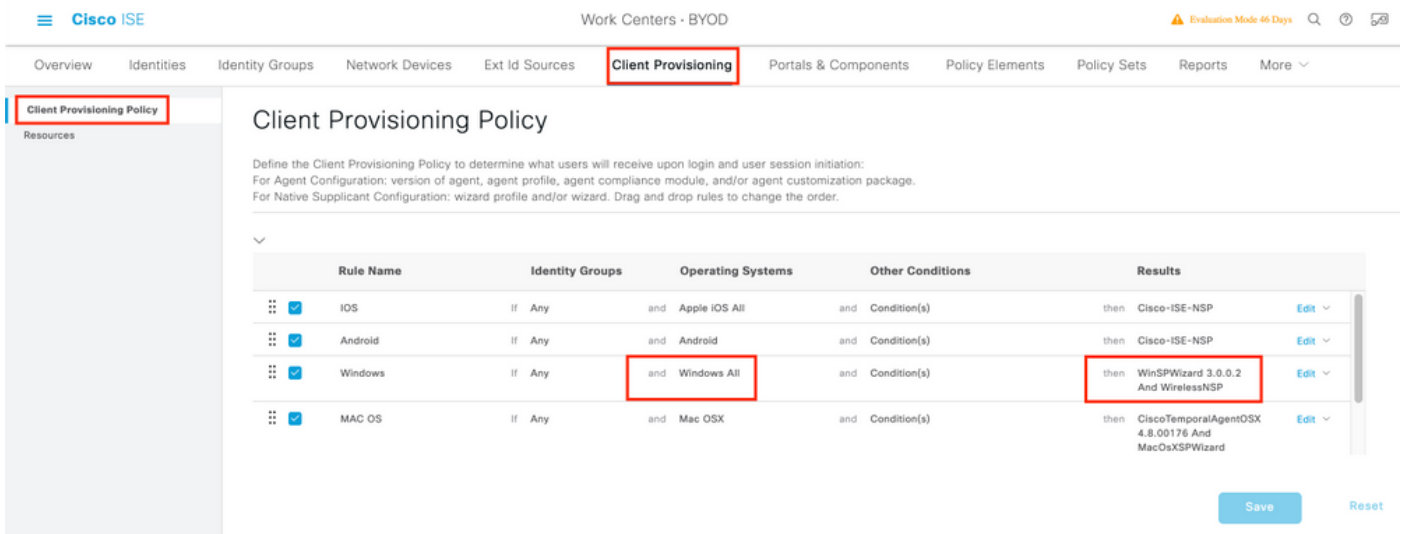
ここで、SSID名は、1つのSSID BYODを実行する前に、接続しているSSID名と同じである必要があります。[Protocol]で[TLS]を選択します。前の手順で作成した[Certificate template]を選択するか、デフォルトの[EAP\_Certificate\_Template]を使用できます。

オプションの設定で、要件に応じて[user]または[User and Machine authentication]を選択します。この例では、ユーザ認証として設定されています。他の設定はデフォルトのままにします。



ステップ4:Windowsデバイスのクライアントプロビジョニングポリシーを作成します。

[ISE] > [Work Centers] > [BYOD] > [Client Provisioning] > [Client Provisioning Policy] に移動します。オペレーティング・システムをWindows ALLとして選択します。前のステップで作成したWinSPWizard 3.0.0.2およびNSPを選択します。



ステップ5:BYODデバイスとして登録されていないデバイスの許可プロファイルを作成します。

[ISE] > [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] > [Add]に移動します。

[共通タスク]で、[Native Supplicant Provisioning]を選択します。WLCで作成されるリダイレクトACL名を定義し、BYODポータルを選択します。ここでは、デフォルトポータルを使用します。カスタムBYODポータルを作成できます。[ISE] > [Work Centers] > [BYOD] > [Portals and components]に移動し、[Add]をクリックします。

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)

ステップ6：証明書プロファイルを作成します。

[ISE] > [Administration] > [External Identity Sources] > [Certificate Profile]に移動します。ここでは、新しい証明書プロファイルを作成するか、デフォルトの証明書プロファイルを使用します。

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

External Identity Sources

Certificate Authentication F

**cert\_profile**

Preloaded\_Certificate\_Prof

Active Directory

ADJooint

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 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

ステップ7：アイデンティティソースシーケンスを作成し、前のステップで作成した証明書プロファイルを選択するか、デフォルトの証明書プロファイルを使用します。これは、ユーザがBYOD登録後にEAP-TLSを実行してフルアクセスを取得するときに必要です。

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

## Identity Source Sequence

## Identity Source Sequence

\* Name

Description

## Certificate Based Authentication

Select Certificate Authentication Profile

## Authentication Search List

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

Available	Selected
Internal Endpoints	Internal Users
Guest Users	ADJoioint

ステップ8 : ポリシーセット、認証ポリシー、および許可ポリシーを作成します。

[ISE] > [Policy] > [Policy Sets]に移動します。ポリシーセットを作成して保存します。

認証ポリシーを作成し、前の手順で作成したアイデンティティソースシーケンスを選択します。

認可ポリシーの作成.2つのポリシーを作成する必要があります。

1. BYOD登録されていないデバイスの場合。ステップ5で作成したリダイレクトプロファイルを指定します。
2. BYODが登録され、EAP-TLSを実行しているデバイス。これらのデバイスへのフルアクセスを許可します。

Authentication Policy (1)

Status	Rule Name	Conditions	Use
+	Search		
+	Default		BYOD_id_Store > Options

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results	Profiles	Security Groups
+	Search				
+	Full_Access	AND Network Access-EapAuthentication EQUALS EAP-TLS EndPoints-BYODRegistration EQUALS Yes	PermitAccess x		Select from list
+	BYOD_Redirect	EndPoints-BYODRegistration EQUALS Unknown	BYOD_Wireless_Redire... x		Select from list

## WLC の設定

手順1:WLCでRADIUSサーバを設定します。

[Security] > [AAA] > [Radius] > [Authentication]に移動します。

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

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

[Security] > [AAA] > [Radius] > [Accounting]に移動します。

The screenshot shows the Cisco configuration interface for RADIUS Accounting Servers. The left sidebar shows a navigation tree with 'AAA' expanded to 'RADIUS' and 'Accounting'. The main content area is titled 'RADIUS Accounting Servers > Edit'. The configuration details for server index 7 are as follows:

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	<input type="checkbox"/>
Port Number	1813
Server Status	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

ステップ2:Dot1x SSIDを設定します。

The screenshot shows the Cisco configuration interface for WLANs. The left sidebar shows a navigation tree with 'WLANs' expanded to 'Advanced'. The main content area is titled 'WLANs > Edit 'BYOD-Dot1x''. The configuration details for the 'BYOD-Dot1x' profile are as follows:

Profile Name	BYOD-Dot1x
Type	WLAN
SSID	BYOD-Dot1x
Status	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none
Lobby Admin Access	<input type="checkbox"/>



WLANs

- WLANs
- Advanced

WLANs > Edit 'BYOD-Dot1x'

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

- Layer 2** Layer 3 AAA Servers

Layer 2 Security [e](#) 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 [19](#)

802.1X-SHA1  Enable

WLANs

- WLANs
- Advanced

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

Authentication Servers

Accounting Servers

Server	Enabled	IP:Port	Enabled	IP:Port
Server 1	<input checked="" type="checkbox"/>	IP:10.106.32.119, Port:1812	<input checked="" type="checkbox"/>	IP:10.106.32.119, Port:1813
Server 2	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 3	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 4	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 5	<input type="checkbox"/>	None	<input type="checkbox"/>	None
Server 6	<input type="checkbox"/>	None	<input type="checkbox"/>	None

EAP Parameters

Enable

Authorization ACA Server

Accounting ACA Server

Enabled  Enabled

ステップ3 : デバイスをプロビジョニングするための制限付きアクセスを提供するようにリダイレクトACLを設定します。

- DHCPおよびDNSへのUDPトラフィックを許可します ( DHCPはデフォルトで許可されています )。
- ISEへの通信。
- 他のトラフィックを拒否します。

[Name] : BYOD-Initial ( または認可プロファイルのACLに手動で名前を付けたもの )

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

## 確認

### 認証フローの検証

Live Logs Live Sessions

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

Refresh Never Show Latest 20 records Within Last 5 minutes

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Identity Group	Authenti...	Authorization Policy	Authorization Profiles	Ei
Nov 29, 2020 11:13:47.4...	<span style="color: blue;">●</span>		0	dot1xuser	50:3E:AA:E4:8...		Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:13:47.2...	<span style="color: green;">■</span>			dot1xuser	50:3E:AA:E4:8...	RegisteredDevices	Wireless >...	Wireless >> Full_Access	PermitAccess	W
Nov 29, 2020 11:10:57.9...	<span style="color: green;">■</span>			dot1xuser	50:3E:AA:E4:8...	Profiled	Wireless >...	Wireless >> BYOD_Redirect	BYOD_Wireless_Redirect	TF

1.最初のログイン時に、ユーザ名とパスワードを使用してPEAP認証を実行します。ISEで、ユーザは[Redirect Rule BYOD-Redirect]にヒットします。

## Cisco ISE

### 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. BYOD登録後、ユーザが登録済みデバイスに追加され、EAP-TLSが実行されてフルアクセスが取得されます。

### 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

## [My Devices]ポータルの確認

[MyDevices Portal]に移動し、クレデンシャルを使用してログインします。デバイス名と登録ステータスを確認できます。

MyDevicesポータルのURLを作成できます。

[ISE] > [Work Centers] > [BYOD] > [Portal and Components] > [My Devices Portal] > [Login Settings]に移動し、[Enter the Fully Qualified URL]を選択します。

### 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













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

## トラブルシューティング

### 一般情報

BYODプロセスでは、PSNノードのデバッグでこれらのISEコンポーネントを有効にする必要があります。

**scep:scep** ログメッセージ。ターゲットログファイル **guest.log** および **ise-psc.log**。

**client-webapp** : インフラストラクチャメッセージを処理するコンポーネント。ターゲットログファイル : **ise-psc.log**

**portal-web-action** : クライアントプロビジョニングポリシーの処理を担当するコンポーネント。ターゲットログファイル : **guest.log**。

**portal** : すべてのポータル関連イベント。ターゲットログファイル : **guest.log**

**portal-session-manager** -ターゲットログファイル – ポータルセッション関連デバッグメッセージ – **gues.log**

**ca-service** - ca-service messages – ターゲットログファイル – **caservice.log** および **caservice-misc.log**

**ca-service-cert** - ca-service certificate messages – ターゲットログファイル – **caservice.log** および **caservice-misc.log**

**admin-ca** - ca-service admin messages – ターゲットログファイル **ise-psc.log**、**caservice.log** および **caservice-misc.log**

**certprovisioningportal** : 証明書プロビジョニングポータルメッセージ – ターゲットログファイル **ise-psc.log**

**nsf**:NSF関連メッセージ – ターゲットログファイル **ise-psc.log**

**nsf-session**:Session cache-related messages – ターゲットログファイル **ise-psc.log**

**runtime-AAA** : すべてのランタイムイベント。ターゲットログファイル : **prrt-server.log**。

クライアント側のログの場合：

%temp%\spwProfileLog.txt (例：C:\Users\\AppData\Local\Temp\spwProfileLog.txt)

## 作業ログ分析

### ISEログ

BYODポータルのリダイレクトACLとリダイレクトURLを使用した初期アクセス許可

Prrt-server.log-

```
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{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
```

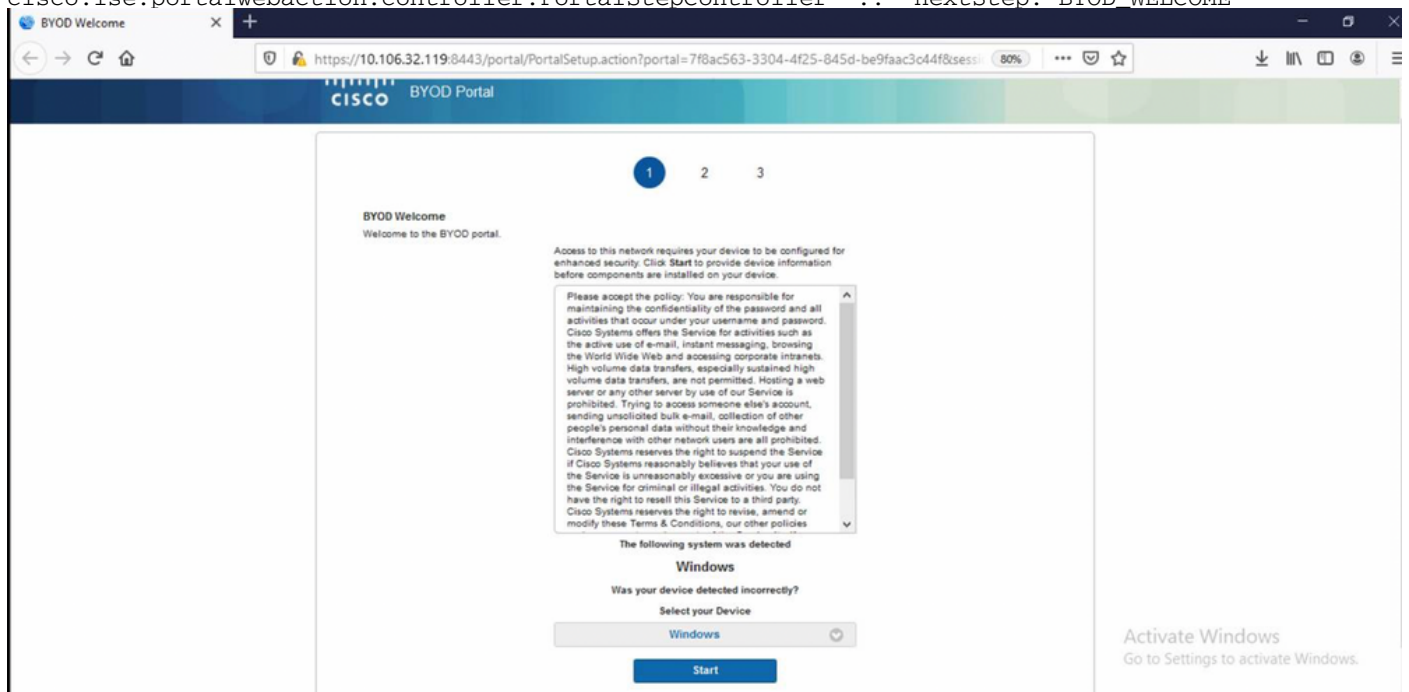
エンドユーザがWebサイトに移動しようとして、WLCによってISEリダイレクトURLにリダイレ  
クトされた場合。

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 'dotluserin
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
```



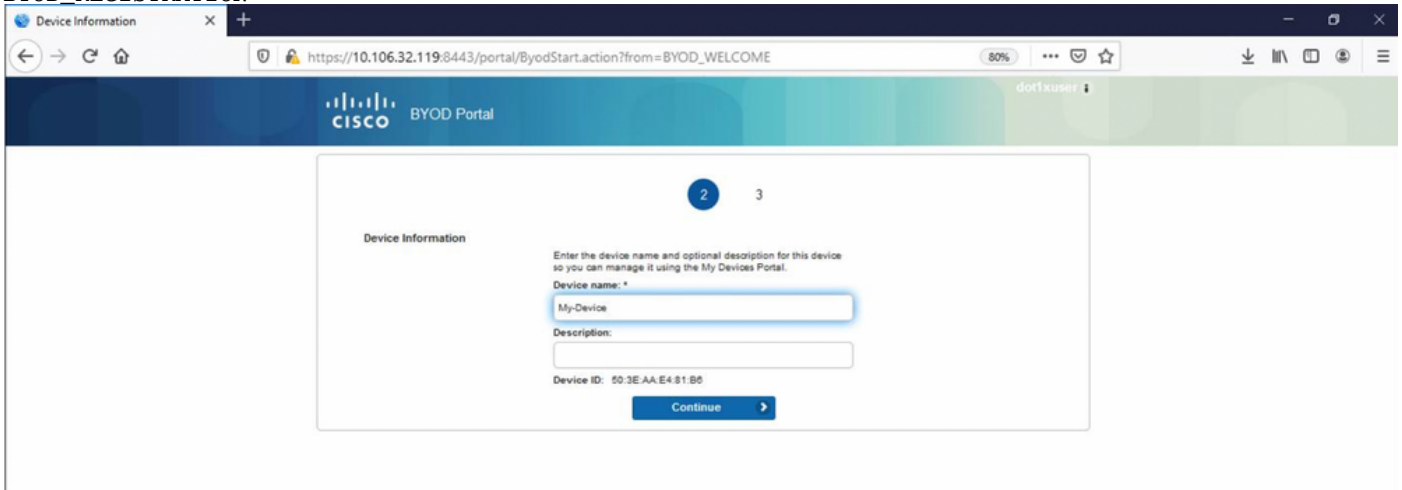
BYODウェルカムページの[スタート]をクリックします。

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

この時点で、ISEはBYODに必要なファイルまたはリソースが存在するかどうかを評価し、自身をBYOD INIT状態にします。

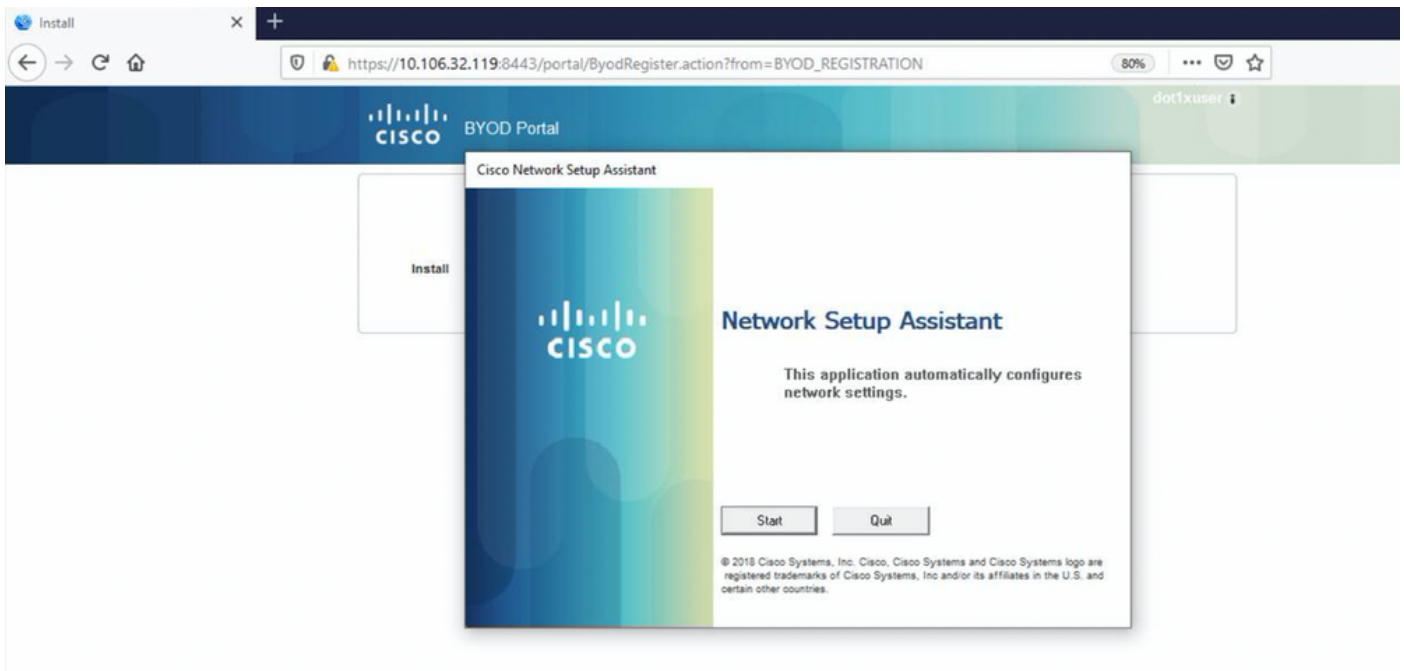
```
2020-12-02 05:44:01,936 DEBUG [https-jsse-nio-10.106.32.119-8443-exec-3][ ]
guestaccess.flowmanager.step.guest.ByodWelcomeStepExecutor -:dotluser:- userAgent=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0, os=Windows 10 (All),
nspStatus=SUCCESS 2020-12-02 05:44:01,936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



デバイス名を入力し、[register]をクリックします。

```
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
```

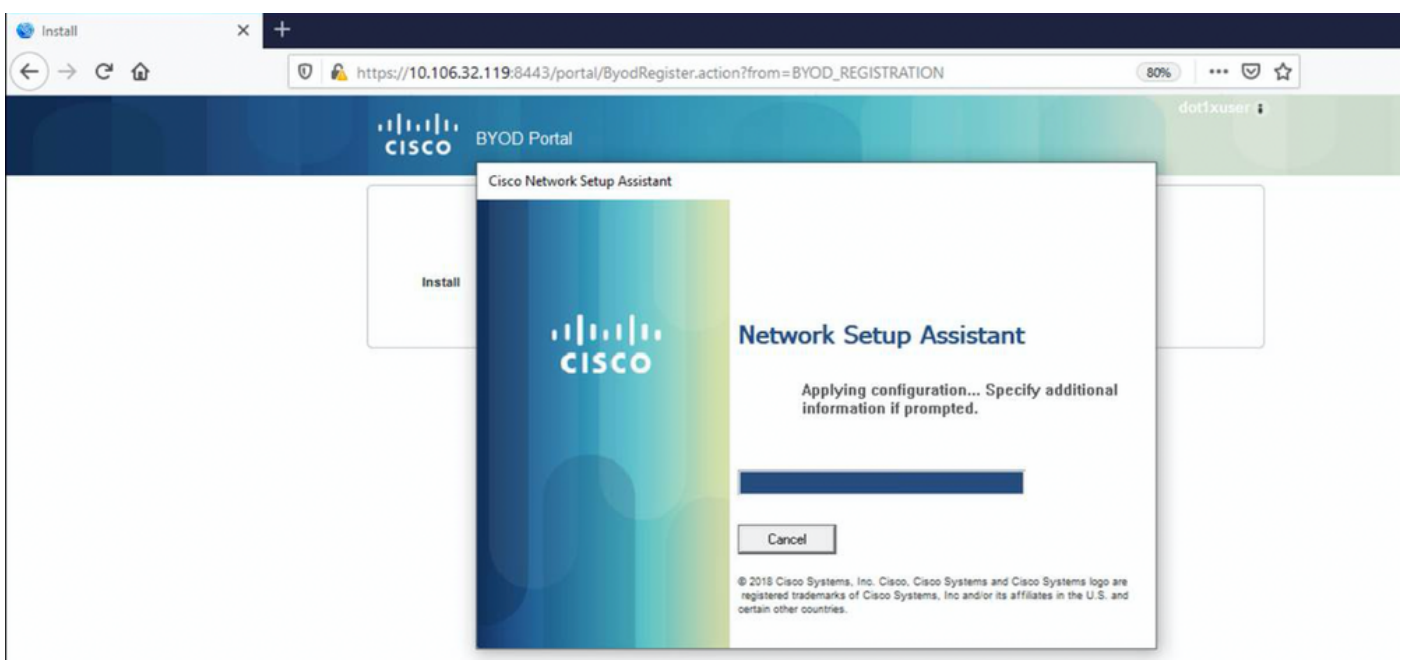


ここで、ユーザがNSAの[Start]をクリックすると、**spwProfile.xml**という名前のファイルがクライアントに一時的に作成され、TCPポート8905でダウンロードしたCisco-ISE-NSP.xmlからコンテンツがコピーされます。

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 -::-
```

**spwProfile.xml**から内容を読み取った後、NSAはネットワークプロファイルを設定し、CSRを生成し、URL <https://10.106.32.119:8443/auth/pkclient.exe>を使用して証明書を取得するためにISEに送信します



## 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 = 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 ]
```

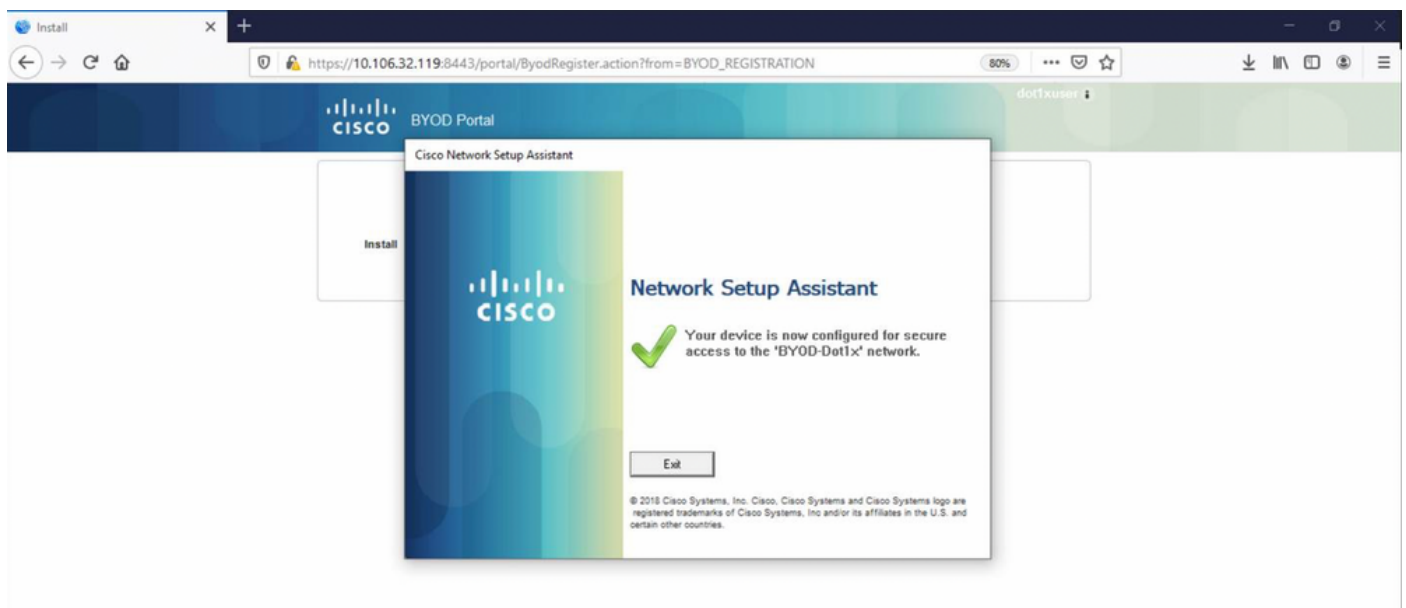
ise-psc.log-

```
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-



```
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
```

証明書のインストール後、クライアントはEAP-TLSを使用して別の認証を開始し、フルアクセスを取得します。

prrt-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: [Û(ØyËöžö|kÔ,.)] [26] MS-MPPE-Send-Key - value: [****] [26] MS-MPPE-Recv-
Key - value: [****] ,RADIUSHandler.cpp:2216
```

## クライアントログ ( spwログ )

クライアントがプロファイルのダウンロードを開始します。

```
[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
```

クライアントは、WLANサービスが実行されているかどうかを確認します。

```
[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]
```

クライアントがプロファイルの適用を開始します。

```
[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]
```

クライアントインストール証明書。



```
[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によるワイヤレスプロファイルの設定

```
[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]
```

### profile

```
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.
```