

ISE 3.3のシングルおよびデュアルSSIDを使用したISE BYODの設定

内容

[はじめに](#)

[背景](#)

[前提条件](#)

[使用するコンポーネント](#)

[ISEのシングルSSIDおよびデュアルSSID BYODとは何ですか。](#)

[シングルSSID BYOD](#)

[デュアルSSID BYOD](#)

[WLC の設定](#)

[CWA用のWLANの作成](#)

[RADIUS サーバの設定](#)

[AAAサーバの設定](#)

[WLANのセキュリティポリシーの設定](#)

[事前認証ACLの設定](#)

[ポリシープロファイルの設定](#)

[タグの適用と展開](#)

[オープン/非セキュアSSIDの設定](#)

[ISE 設定](#)

[前提条件](#)

[証明書](#)

[DNS 設定](#)

[ISEネットワークデバイスの設定](#)

[BYODポータル作成](#)

[Cisco IOS®最新バージョンのダウンロード](#)

[エンドポイントプロファイルの作成](#)

[証明書テンプレート](#)

[クライアントプロビジョニングポータルへのエンドポイントプロファイルのマッピング](#)

[シングルSSID BYOD用のISEポリシーセットの設定](#)

[デュアルSSID BYOD用のISEポリシーセットの設定](#)

[トラブルシューティング](#)

[ログスニペット](#)

[ゲストログ](#)

[lse-Pscログ](#)

[エンドポイントプロファイルのダウンロード](#)

はじめに

このドキュメントでは、ISEでBYODの問題を設定およびトラブルシューティングする方法について説明します。

背景

BYODは、ユーザが個人所有デバイスをISEにオンボーディングできるようにする機能です。これにより、ユーザは環境内のネットワークリソースを使用できます。また、ネットワーク管理者は、ユーザが個人デバイスから重要なリソースにアクセスするのを制限できます。

ISE上の内部ストアまたはActive Directoryを使用してデバイスがゲストページで認証されるゲストフローとは異なります。BYODでは、ネットワーク管理者がエンドポイントにエンドポイントプロファイルをインストールして、EAP方式のタイプを選択できます。EAP-TLSなどのシナリオでは、クライアント証明書はISE自体によって署名され、エンドポイントとISE間の信頼が作成されます。

前提条件

次の項目に関する知識があることが推奨されます。

- WLCコントローラ
- ISEに関する基礎知識

使用するコンポーネント

使用されるデバイスは、BYODフローの特定のバージョンに限定されません。

- Catalyst 9800-CLワイヤレスコントローラ(17.12.3)
- ISE仮想マシン(3.3)

ISEのシングルSSIDおよびデュアルSSID BYODとは何ですか。

シングルSSID BYOD

シングルSSID BYOD設定では、ユーザは個人デバイスを企業のワイヤレスネットワークに直接接続します。オンボーディングプロセスは同じSSIDで実行され、ISEによりデバイスの登録、プロビジョニング、ポリシー適用が容易になります。このアプローチにより、ユーザエクスペリエンスは簡素化されますが、ネットワークセキュリティを確保するには、セキュアなオンボーディングと適切な認証方式が必要です。

デュアルSSID BYOD

デュアルSSID BYOD設定では、2つの別個のSSIDが使用されます。1つはオンボーディング（非セキュアまたは制限付きアクセス）用で、もう1つは企業ネットワークへのアクセス用です。ユーザは最初にオンボーディングSSIDに接続し、ISE経由でデバイスの登録とプロビジョニングを完

了してから、ネットワークアクセスのためにセキュアな企業SSIDに切り替えます。これにより、オンボーディングトラフィックと実稼働トラフィックが分離されるため、セキュリティがさらに強化されます。

WLC の設定

CWA用のWLANの作成

1. Configuration > Tags & Profiles > WLANsの順に選択します。
2. Addをクリックして、新しいWLANを作成します。

- WLAN名とSSID (BYOD-WiFiなど) を設定します。
- WLANを有効にします。

Add WLAN

GeneralSecurityAdvanced

Profile Name*

Enter Name

SSID*

BYOD-SSID

WLAN ID*

9

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

ENABLED

ⓘ

✖ WPA3 Enabled

✔ Dot11ax Enabled

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

▼

↶ Cancel

📄 Apply to Device

RADIUS サーバの設定

1. Configuration > Security > AAA > RADIUS > Serversの順に移動します。

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

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

RADIUS

TACACS+

LDAP

Servers Server Groups

Acct Port "Contains" 1814

Name	Address	Auth Port	Acct Port
0			10

No items to display

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

2. Addをクリックして、RADIUSサーバとしてISEを設定します。

- サーバIP:ISEのIPアドレス。
- Shared Secret:ISEで設定されている共有秘密に一致します。

Create AAA Radius Server

Name* BYOD

Support for CoA ⓘ

ENABLED

Server Address* 10.x.x.x

CoA Server Key Type

Clear Text

PAC Key ☐

CoA Server Key ⓘ

Key Type Clear Text

Confirm CoA Server Key

Key* ⓘ *****

Automate Tester

☐

Confirm Key* *****

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

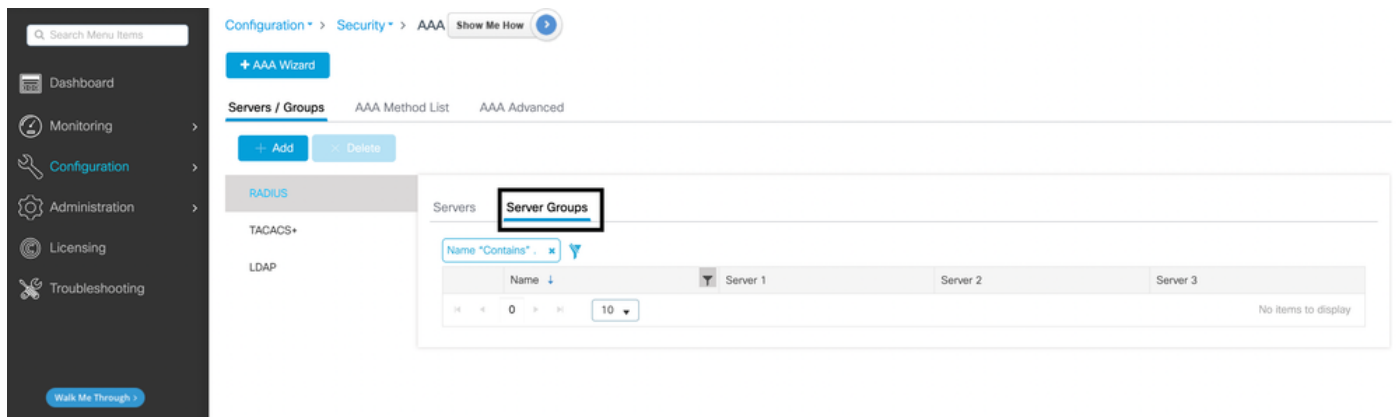
Retry Count 0-100

[Cancel](#)

[Apply to Device](#)

AAAサーバの設定

1. Configuration > Security > AAA > Servers/Groupsの順に選択します。



2. 新規または既存のサーバグループにRADIUSサーバを割り当てます。

Create AAA Radius Server Group

Name*

BYOD

Group Type

RADIUS

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

DISABLED

Source Interface VLAN ID

1

Available Servers

Assigned Servers

BYOD

Cancel

Apply to Device

WLANのセキュリティポリシーの設定

- Configuration > Tags & Profiles > WLANsの順に選択します。先ほど作成したWLANを編集します。
- Security > Layer 2タブで、次の操作を実行します。
 - WPA+WPA2を有効にする
 - WPA2 EncryptionでAES(CCMP128)を設定する
 - 802.1Xとしての認証キー管理

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☒ WPA + WPA2☐ WPA2 + WPA3☐ WPA3☐ Static WEP☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☒GTK
Randomize☐

OSEN Policy

☐

WPA2 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Disabled ▼

Fast Transition

Status

Adaptive Ena... ▼

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

802.1X

☒

PSK

☐

Easy-PSK

☐

CCKM ⚠

☐

FT + 802.1X

☐

FT + PSK

☐802.1X-
SHA256☐

PSK-SHA256

☐

MPSK Configuration

↶ Cancel



Update & Apply to Device

3. Security > Layer 3タブで、Web Auth Parameter Mapのドロップダウンからglobalを選択します。

Edit WLAN ✕

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

Web Policy

☐

Show Advanced Settings >>>

Web Auth Parameter Map

global

▼

🔗

Authentication List

Select a value

▼

🔗

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

↶ Cancel

🔄 Update & Apply to Device

事前認証ACLの設定

ACLを作成して、リダイレクトの操作を使用する：

- DNS トラフィック.
- ISEポータルへのHTTP/HTTPS。
- 必要なバックエンドサービス

これを行うには、

1. Configuration > Security > ACLs > Access Control Listsの順に選択します。
2. 必要なトラフィックを許可するルールを持つ新しいACLを作成します。

Edit ACL

ACL Name*

Test1

ACL Type

IPv4 Extended

Rules

Sequence*

Action

permit

Source Type

any

Destination Type

any

Protocol

ahp

Log

☐

DSCP

None

+ Add

✕ Delete

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
☐	10	deny	ISE-IP-Address		any		ip	None	None	None	Disabled
☐	20	deny	any		ISE-IP-Address		ip	None	None	None	Disabled
☐	30	deny	any		any		udp	None	eq domain	None	Disabled
☐	40	deny	any		any		udp	eq domain	None	None	Disabled
☐	50	permit	any		any		tcp	None	eq www	None	Disabled

1

10

1 - 5 of 5 items

Cancel

Apply to Device

ポリシープロファイルの設定

1. [設定 (Configuration)] > [タグとプロファイル (Tags & Profiles)] > [ポリシー (Policy)] に移動します。デフォルトポリシーを作成または使用できます

Cisco Catalyst 9800-CL Wireless Controller

17.12.3

Welcome velu

Search APs and Clients

Feedback

Configuration

Tags & Profiles

Policy

+ Add

✕ Delete

Clone

Description "Contains" default

▼

Admin Status	Associated Policy Tags	Policy Profile Name	Description
☐	☒	default-policy-profile	default policy profile

1

10

1 - 1 of 1 items

2. アクセスポリシーで適切なVLANを割り当てます

Edit Policy Profile

⌵

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

☒

HTTP TLV Caching

☒

DHCP TLV Caching

☒

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

▼

🔗

VLAN

VLAN/VLAN Group

VLAN0097

▼

ⓘ

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select

▼

🔗

IPv6 ACL

Search or Select

▼

🔗

URL Filters

ⓘ

Pre Auth

Search or Select

▼

🔗

Post Auth

Search or Select

▼

🔗

↶ Cancel

📁

Update & Apply to Device

3. ポリシーのAdvancedで、Allow AAA OverrideとNAC stateを有効にします。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)
28800 ⓘ

Idle Timeout (sec)
300

Idle Threshold (bytes)
0

Client Exclusion Timeout (sec)
☒ 60

Guest LAN Session Timeout
☐

DHCP

IPv4 DHCP Required
☐

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override
☒

NAC State
☒

Policy Name
default-aaa-policy ✕ ▼ ⓘ

Accounting List
Test ✕ ▼ ⓘ

Fabric Profile
☐ Search or Select ⓘ

Link-Local Bridging
☐

mDNS Service Policy
default-mdns-ser... ▼ ⓘ Clear

Hotspot Server
Search or Select ⓘ

User Defined (Private) Network

Status
☐

Drop Unicast
☐

DNS Layer Security

DNS Layer Security Parameter Map
Not Configured ▼ Clear

Flex DHCP Option for DNS
ENABLED ☒

Flex DNS Traffic Redirect
☐ IGNORE

WLAN Flex Policy

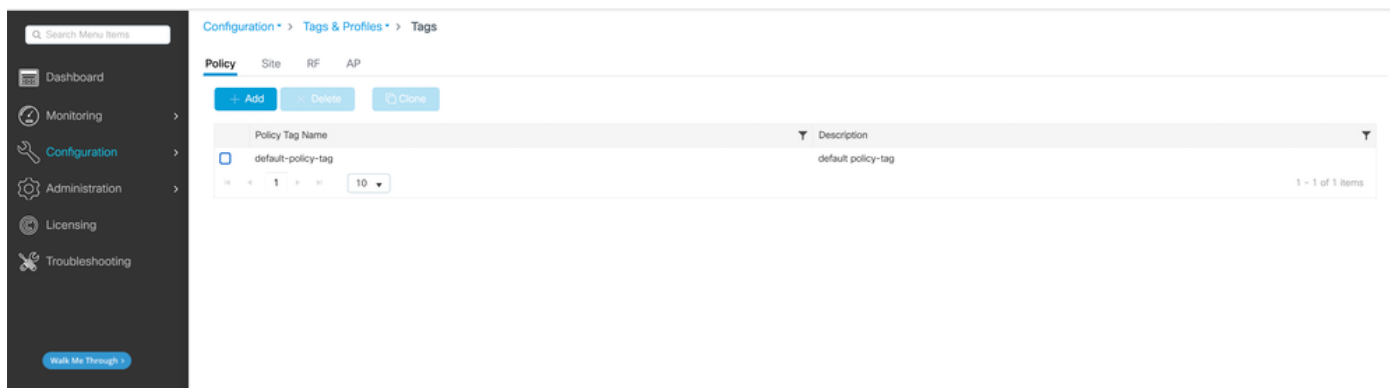
VLAN Central Switching
☐

Split MAC ACL
Search or Select ⓘ

Cancel
Update & Apply to Device

タグの適用と展開

- Configuration > Tags & Profiles > Tagsの順に移動します。
- タグを作成または編集して、WLANとポリシープロファイルを含めます。
- アクセスポイントにタグを割り当てます。



オープン/非セキュアSSIDの設定

オープンSSIDは、環境内にデュアルSSID BYOD設定を設定した場合にのみ作成されます。

1. Configuration > Tags & Profiles > WLANsの順に選択します。[Add] ボタンをクリックします。
2. GeneralタブでSSID名を指定し、WLANボタンを有効にします。

Add WLAN

GeneralSecurityAdvanced

Profile Name*BYOD-Open

SSID*BYOD-Open

WLAN ID*10

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

ENABLED

WPA3 Enabled

Dot11ax Enabled

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

Cancel

Apply to Device

3. 同じウィンドウでSecurityタブをクリックします。Noneオプションボタンを選択して、MACフィルタリングを有効にします。

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. The 'Layer2' sub-tab is also selected. In the security options row, the 'None' radio button is selected. The 'MAC Filtering' checkbox is checked. The 'Authorization List*' dropdown is set to 'default'. The 'OWE Transition Mode' checkbox is checked, and the 'Transition Mode WLAN ID*' text box contains '0-4096'. The 'Lobby Admin Access' checkbox is unchecked. A 'Fast Transition' section is expanded, showing 'Status' as 'Disabled', 'Over the DS' as unchecked, and 'Reassociation Timeout *' as '20'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

General		Security		Advanced	
Layer2 Layer3 AAA					
☐ WPA + WPA2 ☐ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☒ None					
MAC Filtering ☒		Authorization List*		default ▼ ⓘ	
OWE Transition Mode ☒		Transition Mode WLAN ID*		0-4096	
Lobby Admin Access ☐					
Fast Transition					
Status		Disabled ▼			
Over the DS		☐			
Reassociation Timeout *		20			

Cancel Apply to Device

4. Layer 3のSecurityで、Web Auth Parameter Mapのグローバル設定を選択します。WLCに他のWeb認証プロファイルが設定されている場合は、次の場所にマッピングすることもできます。

Add WLAN



General

Security

Advanced

Layer2

Layer3

AAA

[Show Advanced Settings >>>](#)

Web Policy



Web Auth Parameter Map

global



Authentication List

Select a value



For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Cancel

Apply to Device

ISE 設定

前提条件

- Cisco ISEがインストールされ、BYOD機能のライセンスを取得していることを確認します。
- RADIUS共有秘密を使用して、WLCをネットワークデバイスとしてISEに追加します。

証明書

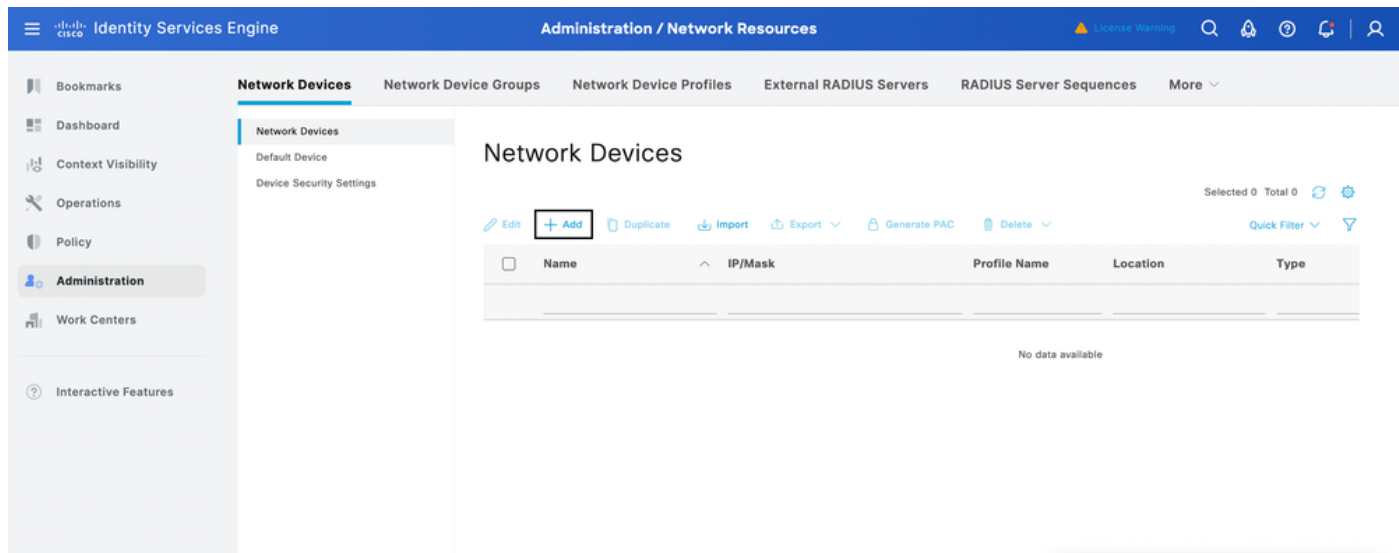
- ブラウザのセキュリティ警告を回避するために、有効なサーバ証明書をISEにインストールします。
- 証明書がエンドポイントによって信頼されていること（既知のCAまたは信頼されたルートを持つ内部CAによって署名されていること）を確認します。

DNS 設定

- DNSがBYODポータルのISEホスト名を解決することを確認します。

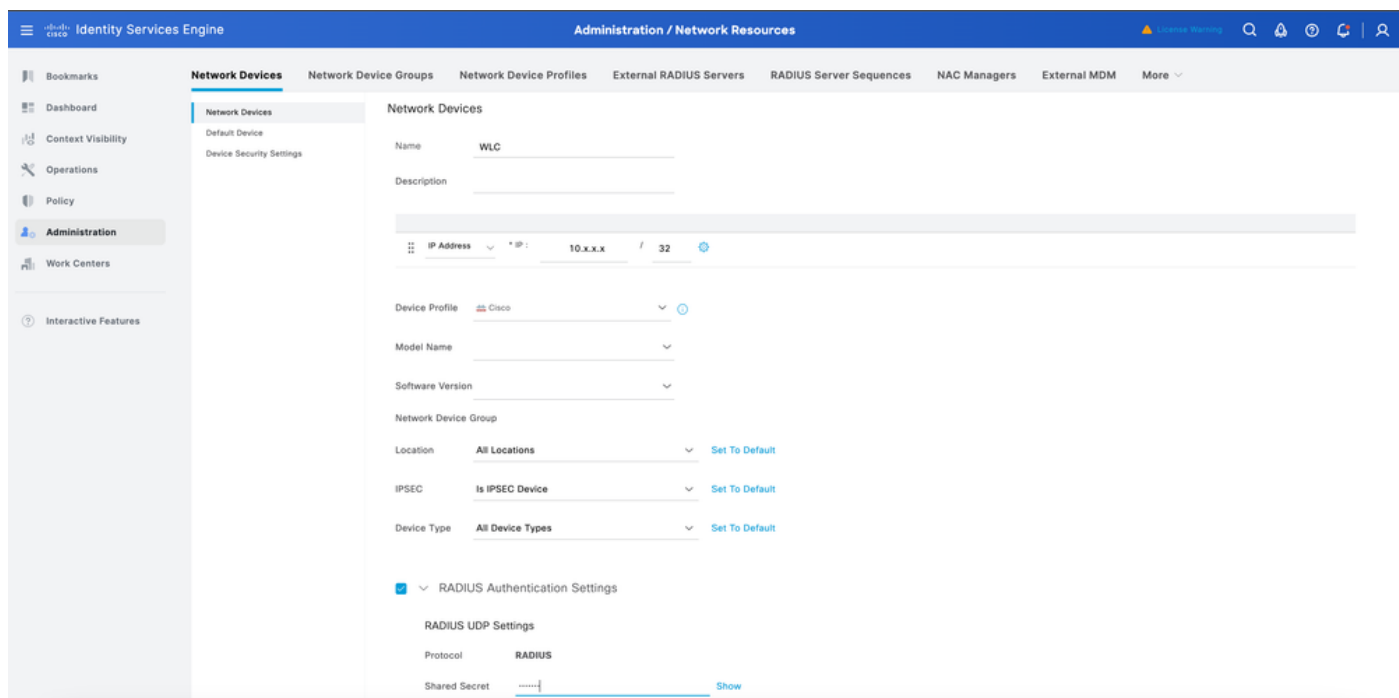
ISEネットワークデバイスの設定

1. ISE Web UIにログインします。
2. [管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] に移動します。



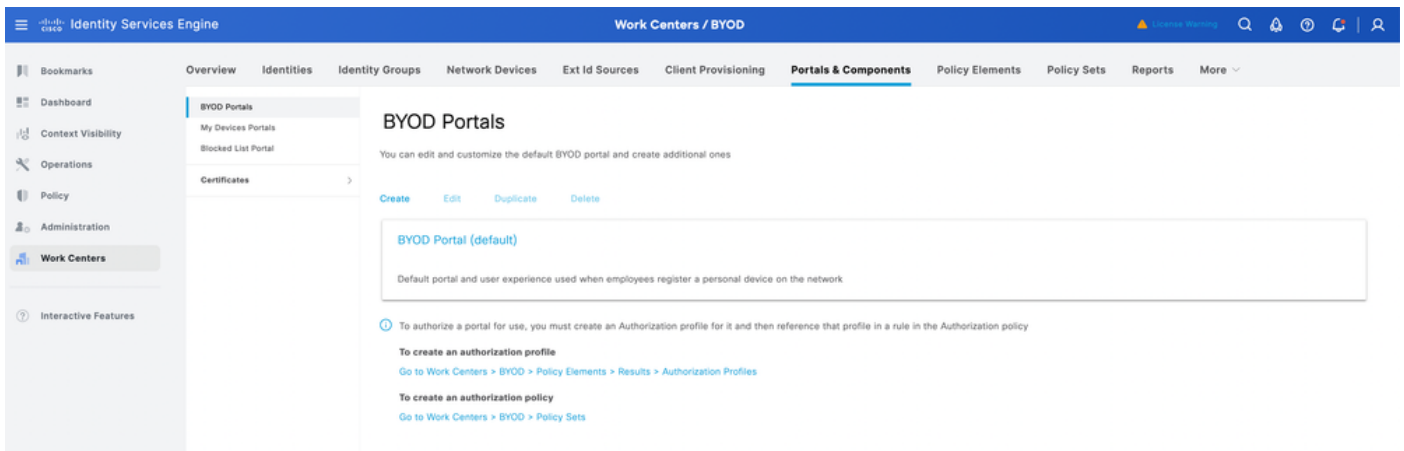
3. WLCをネットワークデバイスとして追加します。

- Name:WLCの名前を入力します。
- IP Address:WLC管理IPを入力します。
- RADIUS共有秘密:WLCに設定されているものと同じ共有秘密を入力します。
- [Submit] をクリックします。



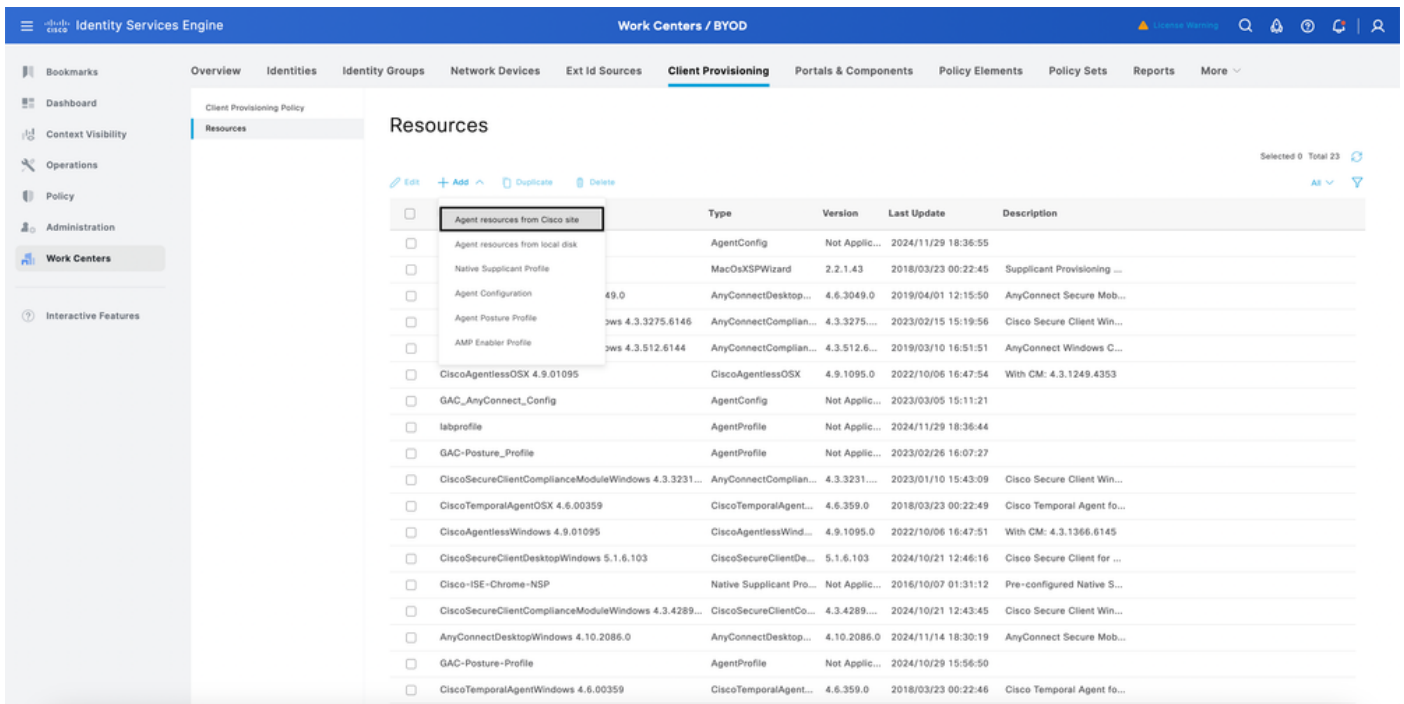
BYODポータルを作成

1. Work Centers > BYOD > Settings > Portals & Components > BYOD Portalsの順に移動します。
2. AddをクリックしてBYODポータルを作成するか、ISEの既存のデフォルトポータルを使用できます。



Cisco IOS®最新バージョンのダウンロード

1. Work Centers > BYOD > Client provisioning > Resourcesの順に移動します。
2. Addボタンをクリックして、シスコのサイトからエージェントリソースを選択します。



3. ソフトウェアリストで、ダウンロードする最新のCisco IOSバージョンを選択します。



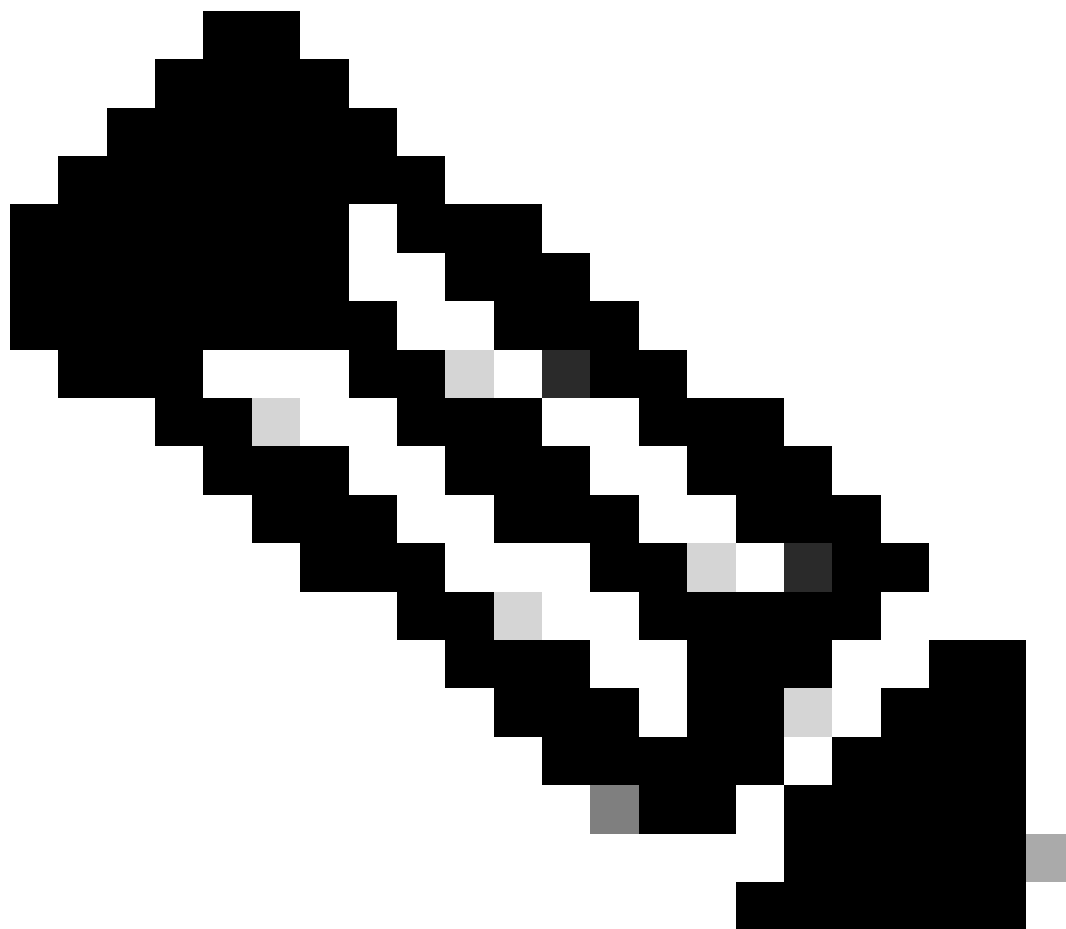
Download Remote Resources

☐	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☒	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save



注: Cisco IOSソフトウェアは、WindowsおよびMacOSエンドポイント用のISEでダウンロードできます。Apple iPhone IOSの場合は、ネイティブサブリカントを使用してデバイスをプロビジョニングします。Androidデバイスの場合は、Play Storeからダウンロードする必要があるネットワークセットアップアシスタントがあります。

エンドポイントプロファイルの作成

1. Work Centers > BYOD > Client provisioning > Resourcesの順に移動します。
2. Addをクリックし、ドロップダウンメニューからNative supplicant profileを選択します。

Type	Version	Last Update	Description
AgentConfig	Not Applic...	2024/11/29 18:36:55	
MacOsXSPWizard	2.2.1.43	2018/03/23 00:22:45	Supplicant Provisioning ...
AnyConnectDesktop...	4.6.3049.0	2019/04/01 12:15:50	AnyConnect Secure Mob...
AnyConnectComplan...	4.3.3275...	2023/02/15 15:19:56	Cisco Secure Client Win...
AnyConnectComplan...	4.3.512.6...	2019/03/10 16:51:51	AnyConnect Windows C...
CiscoAgentlessOSX	4.9.1095.0	2022/10/06 16:47:54	With CM: 4.3.1249.4353
AgentConfig	Not Applic...	2023/03/05 15:11:21	
AgentProfile	Not Applic...	2024/11/29 18:36:44	
AgentProfile	Not Applic...	2023/02/26 16:07:27	
AnyConnectComplan...	4.3.3231...	2023/01/10 15:43:09	Cisco Secure Client Win...
CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:49	Cisco Temporal Agent fo...
CiscoAgentlessWind...	4.9.1095.0	2022/10/06 16:47:51	With CM: 4.3.1366.6145
CiscoSecureClientDe...	5.1.6.103	2024/10/21 12:46:16	Cisco Secure Client for ...
Native Supplicant Pro...	Not Applic...	2016/10/07 01:31:12	Pre-configured Native S...
CiscoSecureClientCo...	4.3.4289...	2024/10/21 12:43:45	Cisco Secure Client Win...
AnyConnectDesktop...	4.10.2086.0	2024/11/14 18:30:19	AnyConnect Secure Mob...
AgentProfile	Not Applic...	2024/10/29 15:56:50	
CiscoTemporalAgent...	4.6.359.0	2018/03/23 00:22:46	Cisco Temporal Agent fo...

3. [Operating system]ドロップダウンで、デバイスをオンボードする必要のあるオペレーティングシステムを選択するか、または環境内のすべてのエンドポイントをオンボードするためのALLとして設定します。

Native Supplicant Profile

* Name: BYOD profile

Description: [Empty text box]

Operating System: ALL

Wireless Profile

Multiple SSIDs can be co

Proxy Auto-Config File U

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

Operating System Groups

Android

Apple iOS All

Chrome OS All

Linux All

Mac OSX

Wired Profile

Allowed Protocol: PEAP

Certificate Template: Not Required

Optional Settings

4. ページからAddをクリックして、エンドポイントのプロファイルを作成し、エンドポイントの802.1Xを設定します。

Wireless Profile(s)

SSID Name *	BYOD	
Proxy Auto-Config File URL		i
Proxy Host/IP		i
Proxy Port		
Security *	WPA2 Enterprise	▼
Allowed Protocol *	PEAP	▼
Certificate Template	Not Required	▼ i

▼ Optional Settings

Windows Settings

Authentication Mode	User or Computer	▼
☐ Automatically use logon name and password (and domain if any)		
☒ Enable fast reconnect		
☐ Enable quarantine checks		
☐ Disconnect if server does not present cryptobinding TLV		
☐ Do not prompt user to authorize new servers or trusted certification authorities		
☒ Connect even if the network is not broadcasting its name (SSID)		

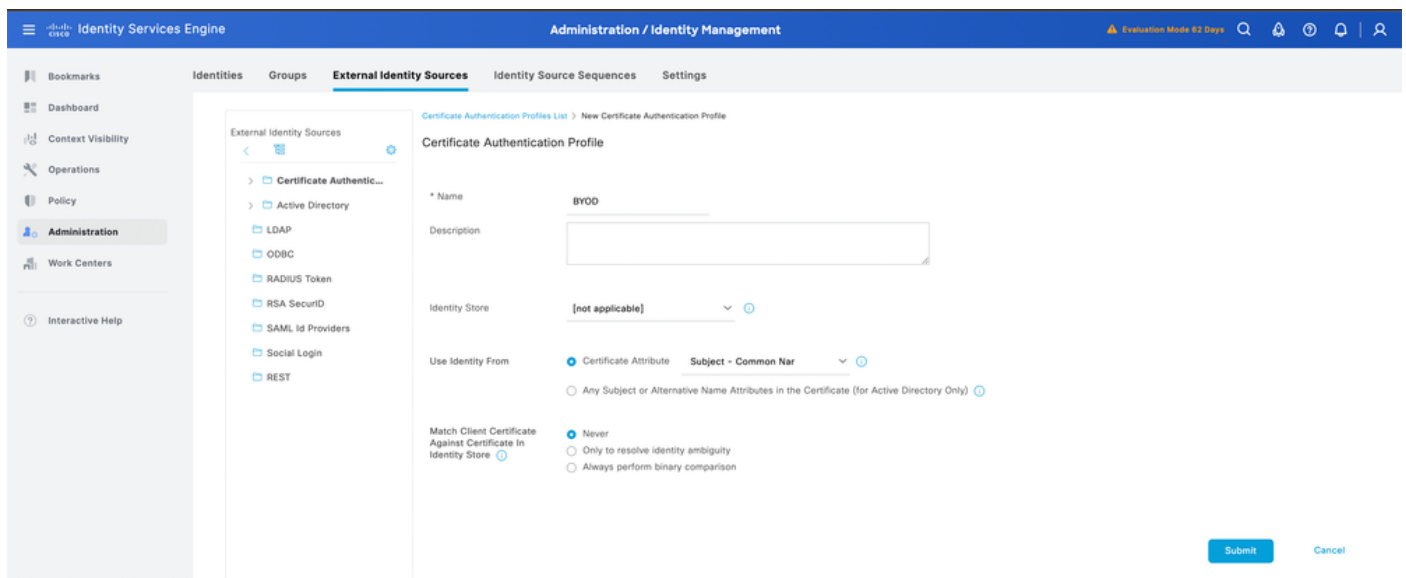
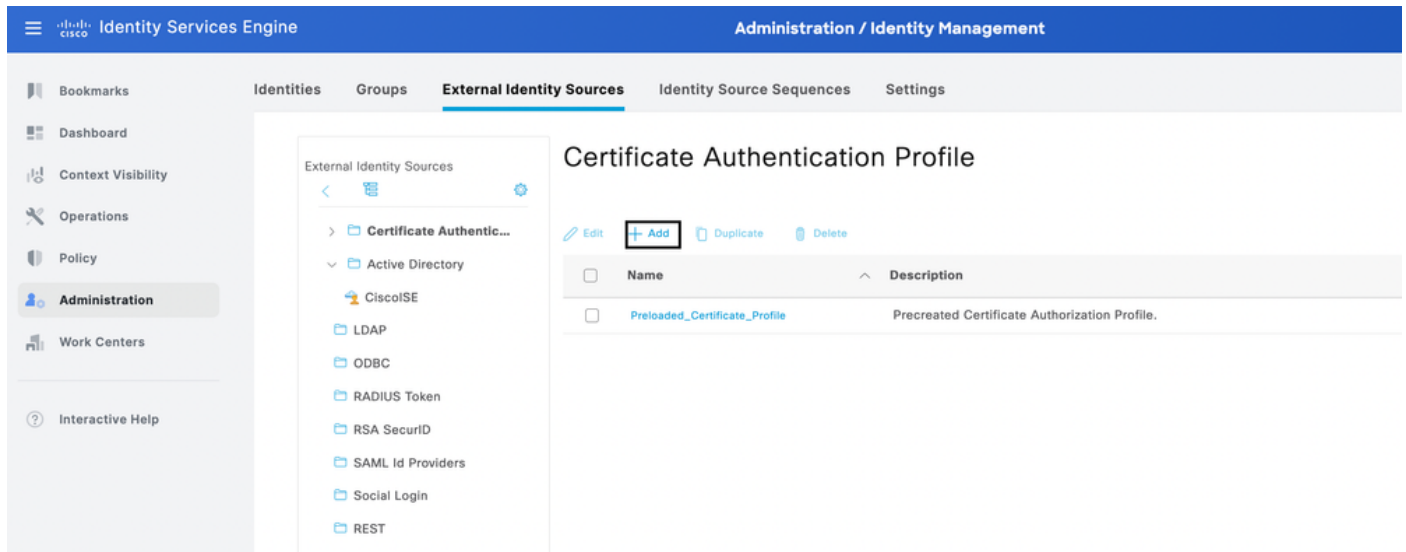
iOS Settings

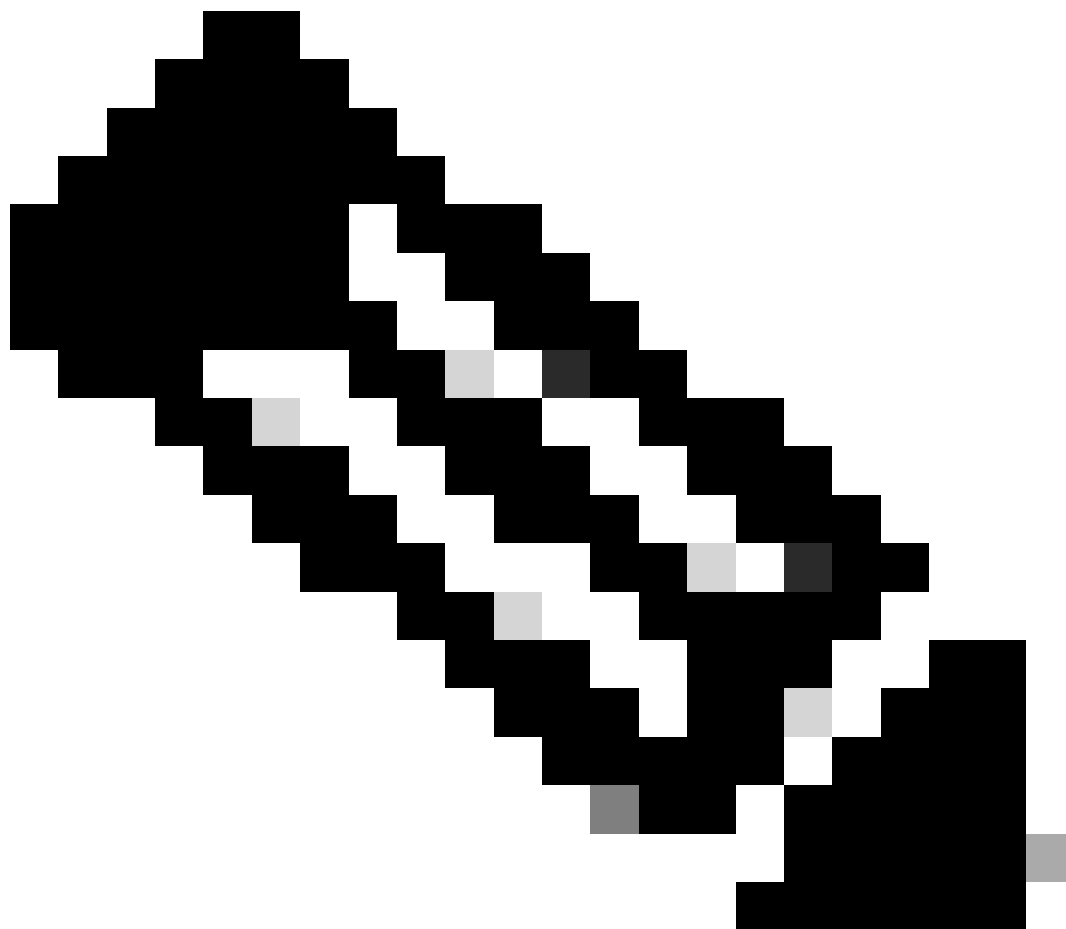
☐ Enable if target network is hidden

Android Settings

Certificate Enrollment Protocol: [i](#)

Administration > Identity Management > External Identity Sources > Certificate Authentication Profileの順に移動します。Addボタンをクリックして、証明書プロファイルを作成します。





注:IDストアでは、ISEに統合されているActive Directoryをいつでも選択できます。これにより、追加のセキュリティのために証明書からユーザ検索を実行できます。

3. Submit をクリックして、設定を保存します。次に、証明書プロファイルをBYODのポリシーセットにマッピングします。

4. BYODフロー後のBYODリダイレクトとフルアクセスの許可プロファイルを設定します。
[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] の順に選択します。

5. Addをクリックし、認可プロファイルを作成します。Webリダイレクション(CWA、MDM、NSP、CPP)を確認し、BYODポータルページをマッピングします。また、WLCからプロファイルにリダイレクションACL名を追加します。Full accessプロファイルの場合は、プロファイル内のそれぞれの社内VLANでpermit accessを設定します。

6. 認可プロファイルを認可ルールにマッピングします。ユーザがBYODフロー後にネットワークにフルアクセスできるように、BYODフルアクセスにはルールEndPoints・BYODRegistrationをyesに設定する必要があります。

Policy Sets → BYOD

Reset Reset Policy Set Hit Counts Save

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

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

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

デュアルSSID BYOD用のISEポリシーセットの設定

デュアルSSID BYOD設定では、2ポリシーセットがISEで設定されます。最初のポリシーセットはオープン/非セキュアSSID用で、ポリシーセット設定はオープン/非セキュアSSIDへの接続時にユーザをBYODページにリダイレクトします

1. Policy > Policy Setに移動し、ISE上でBYODフローのポリシーを作成します。
2. ISE上で登録されたBYODユーザを認証するオープン/非セキュアSSIDと社内SSIDのポリシーセットを作成します。

Policy Sets

Reset Reset Policy Set Hit Counts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	BYOD_Devices	BYOD_Devices	Wireless_802.1X	Default Network Access	0	Edit Add Delete Gear	>
On	Onboard_Personal_Devices	Onboard_Personal_Devices	Wireless_MAB	Default Network Access	0	Edit Add Delete Gear	>
On	Default	Default policy set		Default Network Access	0	Edit Add Delete Gear	>

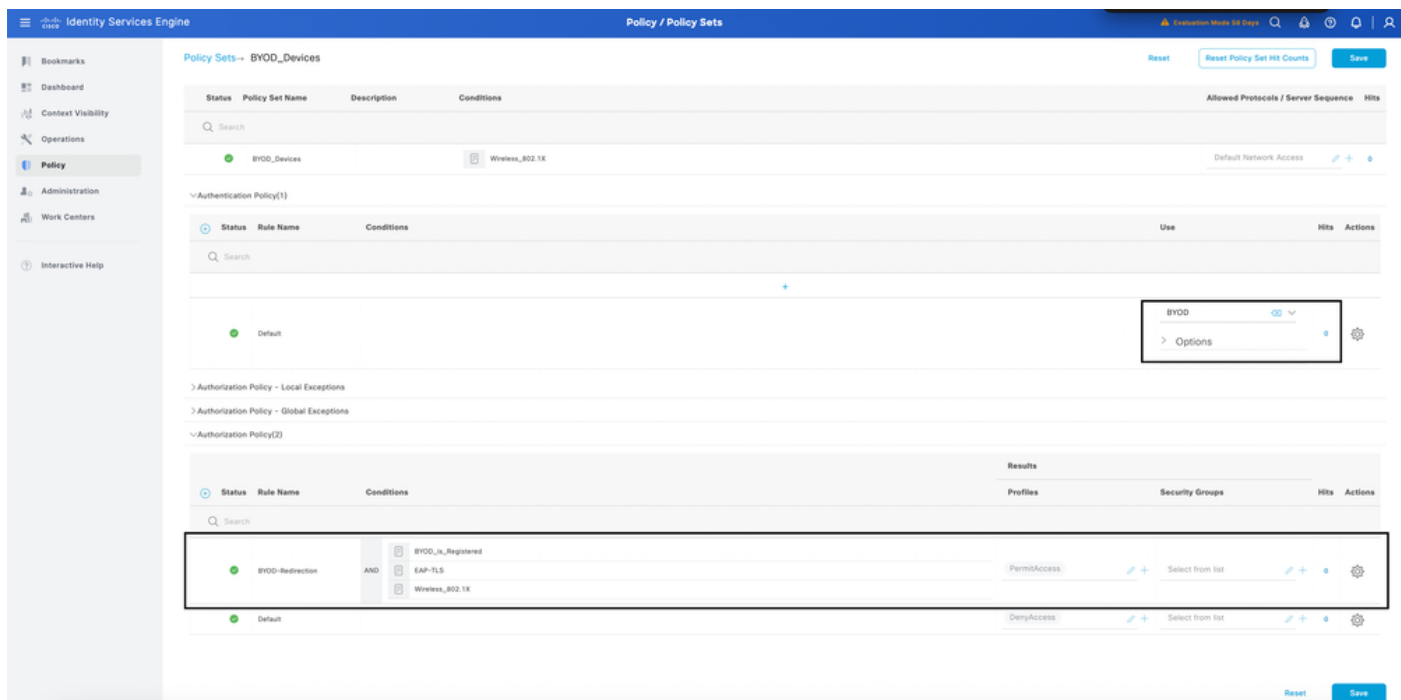
Reset Save

3. オンボーディングポリシーセットで、オプションの下Continue selectedを見つけます。認可ポリシーについて、条件を作成し、リダイレクション認可プロファイルのマッピングします。認可プロファイルの作成にも同じ手順が含まれます。これはポイント4で確認できます。



4. BYOD登録済みポリシーセットで、見つかったのと同じ証明書プロファイルを使用して認証ポリシーを設定します。

「ポイント2のシングルSSID BYOD用のISEポリシーセットの設定」で説明します。また、認可ポリシーの条件を作成し、フルアクセスプロファイルをポリシーにマッピングします。



Logging

ISEからのライブログから、ユーザ認証が成功し、BYODポータルページにリダイレクトされます。BYODフローが完了すると、ユーザはネットワークへのアクセスを許可されます

Reset Repeat Counts

Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authorization Policy	Authoriz...	IP Address	Network De...	Device	
X		▼		Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorization Policy	Authorizatic	IP Address	▼	Network Device	Device
Feb 24, 2025 12:30:18.1...			0	test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD	PermitAcc...	10.127.196.2...			TenGig...
Feb 24, 2025 12:06:43.0...				test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...		BYOD-Switch	TenGig...
Feb 24, 2025 12:06:37.9...				test	B4:96:91:22:65:A5	Windows1...	Test >> D...	Test >> BYOD_redirect	BYOD_Re...	10.127.196.2...		BYOD-Switch	TenGig...

ユーザの観点からは、最初にBYODページにリダイレクトされ、Webページから適切なデバイスを選択する必要があります。テストでは、Windows 10デバイスが使用されました

BYOD Portal

test

1

2

3

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

The following system was detected

Windows

Was your device detected incorrectly?

Select your Device

Windows

▼

Start

[Next] (次へ) ボタンをクリックすると、デバイスの名前と説明を入力するように求められるページが表示されます

The screenshot shows the Cisco BYOD Portal interface. At the top, there is a header with the Cisco logo on the left, 'BYOD Portal' in the center, and a user profile 'test' with a dropdown arrow on the right. Below the header, a progress indicator shows two steps: step 2 is active and highlighted with a blue circle, and step 3 is shown as a plain circle. The main content area is titled 'Device Information' and contains the instruction: 'Enter the device name and optional description for this device so you can manage it using the My Devices Portal.' There are three input fields: 'Device name: *' (required), 'Description:', and 'Device ID:'. The 'Device ID' field is pre-filled with a blacked-out string. At the bottom of the form is a blue 'Continue' button with a right-pointing arrow.

プロファイルがEAP-TLS認証を実行するように設定されている場合、認証のためにエンドポイントプロファイルとEAP TLS証明書をダウンロードするためのNetwork Assistantツールをダウンロードするようにユーザに要求することを示す投稿。

The screenshot shows the Cisco BYOD Portal interface at the 'Install' step. The header is identical to the previous screenshot. The progress indicator now shows step 3 as the active step, highlighted with a blue circle, while step 2 is a plain circle. The main content area is titled 'Install' and contains the instruction: 'Please wait while we download the Cisco Network Setup Assistant. You will then need to manually run the Setup Assistant and follow the instructions to finish registering this device.'

管理者権限でNetwork Assistantアプリケーションを実行し、開始ボタンをクリックしてオンボーディングフローを開始します。



Network Setup Assistant

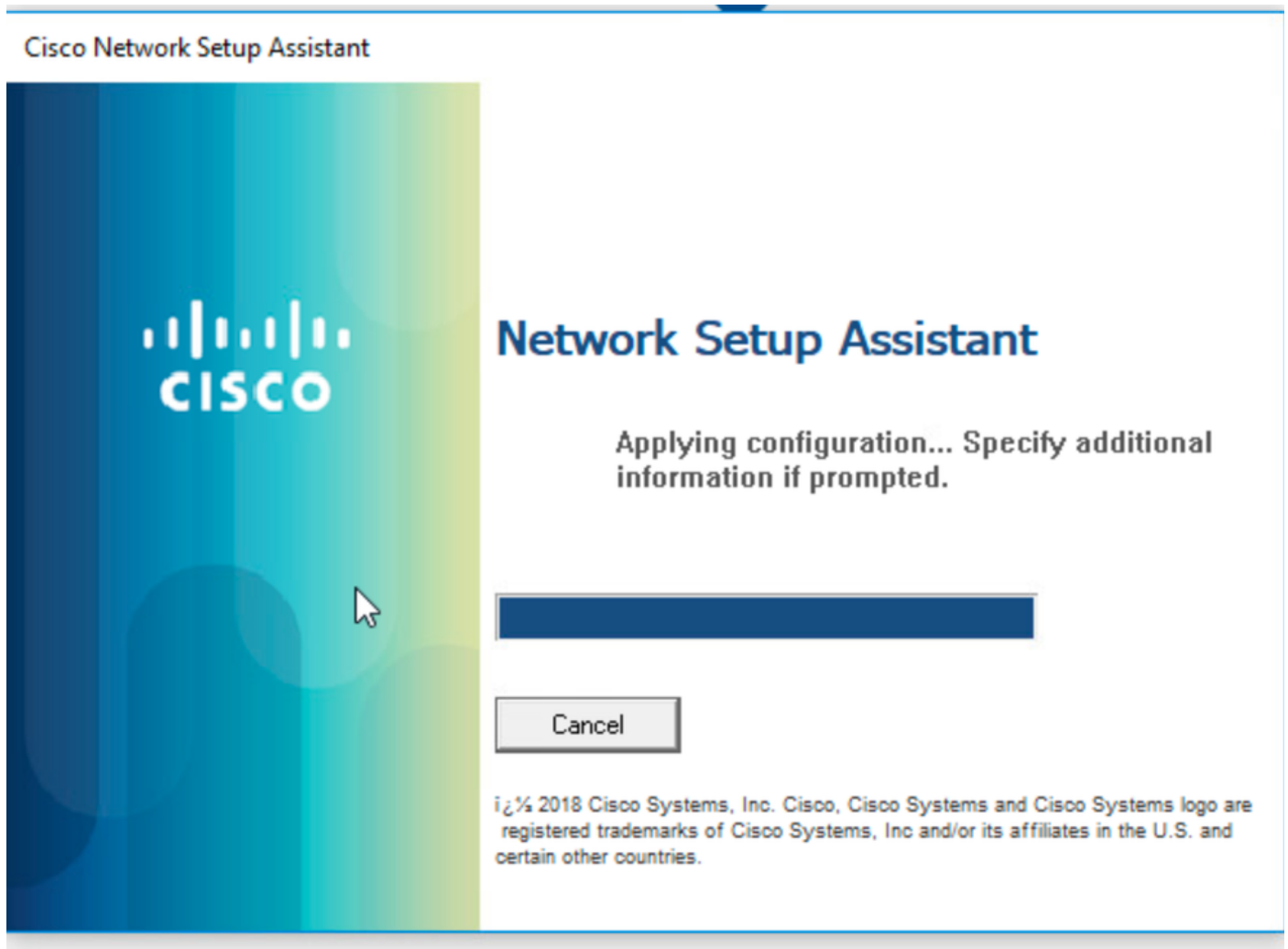


This application automatically configures network settings.

Start

Quit

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



ユーザは、リソースにアクセスするための個人用デバイスを使用してネットワークに正常にオンボーディングされました。

トラブルシューティング

BYODの問題をトラブルシューティングするには、ISEでこのデバッグを有効にしてください

デバッグレベルに設定する属性：

- クライアント(guest.log)
- client-webapp(guest.log)
- scep(ise-psc.log)
- caサービス(ise-psc.log)
- admin-ca(ise-psc.log)
- ランタイムAAA (prrt-server.log)
- nsf(ise-psc.log)
- nsf-session(ise-psc.log)
- プロファイラ(profiler.log)

ログスニペット

ゲストログ

これらのログは、ユーザがページに正常にリダイレクトされ、Network Assistantアプリケーションをダウンロードしたことを示しています。

```
2025-02-24 12:06:08,053情報[https-jsse-nio-10.127.196.172-8443-exec-4][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-ア
クション転送で見つかったマッピングパス : pages/byodWelcome.jsp // BYODウェルカムページ
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
pTranSteps:1のサイズ
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, pTranSteps:[id: 2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, stepTran:d251 3b7b-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-
mapping path found in-action-forwarding: pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
pTranSteps:1のサイズ
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, pTranSteps:[f:[id: 203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
cpm.guestaccess.flowmanager.step.StepExecutor -:0000000000000000B30D59CC5::test:-
getNextFlowStep, stepTran:f203 b757-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]]
portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5:::-
mapping path found in-action-forwarding: pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5:::- Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5:::-
portalSessionId = null
2025-02-24 12:06:14,713デバッグ[https-jsse-nio-10.127.196.172-8443 -exec-10][[]]
cisco.cpm.client.provisioning.StreamingServlet -:0000000000000000B30D59CC5:::-
StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-
bbb91e8828da/NetworkSetupAssistant.exe //ネットワーク支援アプリケーションがエンドポイン
トに送信されました
```

Isc-Pscログ

アプリケーションがエンドポイントにダウンロードされると、アプリケーションはSCEPフローを開始してISEからクライアント証明書を取得します。

```
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- CertStoreには4つの証明書が含まれています :
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=Certificate Services Root CA - iseguest;
serial=32281512738768960628252532784663302089]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA -
iseguest; serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- 3. '[issuer=CN=Certificate Services Root CA - iseguest;
serial=68627620160586308685849818775100698224]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- 4. '[issuer=CN=Certificate Services Node CA - iseguest;
serial=72934767698603097153932482227548874953]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 暗号化証明書の選択
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- keyEncipherment keyUsageによる証明書の選択
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- keyEncipherment keyUsageを含む1つの証明書が見つかりました
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- [issuer=CN=Certificate Services Endpoint Sub CA -
iseguest serial=131900858749761727853768227590303808637]を使用してメッセージを暗号化
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 検証証明書の選択
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- digitalSignature keyUsageを使用した証明書の選択
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- digitalSignature keyUsageを含む1つの証明書が見つかりました
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- [issuer=CN=Certificate Services Endpoint Sub CA -
iseguest serial=131900858749761727853768227590303808637]を使用したメッセージの検証
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 発行者証明書の選択
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Selecting certificate with basicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- basicConstraintsを持つ3つの証明書が見つかりました
```

2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- [issuer=CN=Certificate Services Endpoint Sub CA -
iseguest serial=131900858749761727853768227590303808637]を発行者に使用
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][]
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- SCEPサーバのパフォーマンスメトリック
: name[live/dead、total reqs、total failures、inflight reqs、Average RTT]
[http://127.0.0.1:9444/caservice/scep\[live,96444,1,0,120\]](http://127.0.0.1:9444/caservice/scep[live,96444,1,0,120])

エンドポイントプロファイルのダウンロード

SCEPプロセスが完了し、エンドポイントが証明書をインストールすると、アプリケーションは以降の認証用にエンドポイントプロファイルをダウンロードします。このプロファイルはデバイスによって実行されます。

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Referrer = Windows // Windowsデバイスが
Webページに基づいて検出されました
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][]
cisco.cpm.client.provisioning.EvaluationServlet -::::- nspプロファイルのプロビジョニング
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][]
cisco.cpm.client.provisioning.StreamingServlet -::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][]
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionId = null
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][]
cisco.cpm.client.provisioning.StreamingServlet -::::- StreamingServlet
URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-
NSP.xml//NSPプロファイルがエンドポイントにダウンロードされます
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][]
cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming to ip: file type: NativeSPProfile
name:Cisco-ISE-NSP.xml //The Network Assistant Application
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][]
cisco.cpm.client.provisioning.StreamingServlet -::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][]
cisco.cpm.client.provisioning.StreamingServlet -::::- userId has been set to test
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][]
cisco.cpm.client.provisioning.StreamingServlet -::::: リダイレクトの種類は : SUCCESS_PAGE、
リダイレクトurlは : mac:

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。