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

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

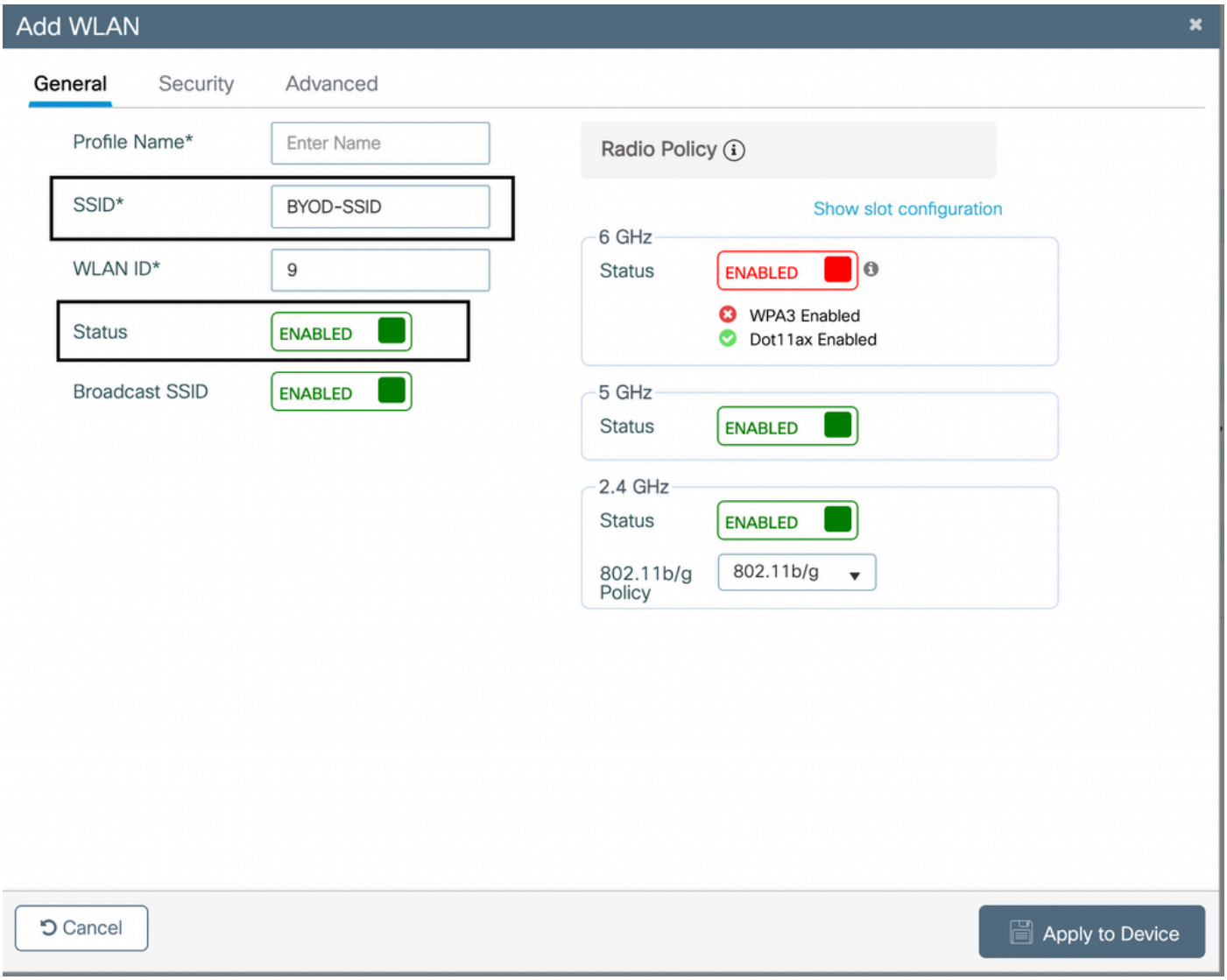
了してから、ネットワークアクセスのためにセキュアな企業SSIDに切り替えます。これにより、オンボーディングトラフィックと実稼働トラフィックが分離されるため、セキュリティがさらに強化されます。

WLC の設定

CWA用のWLANの作成

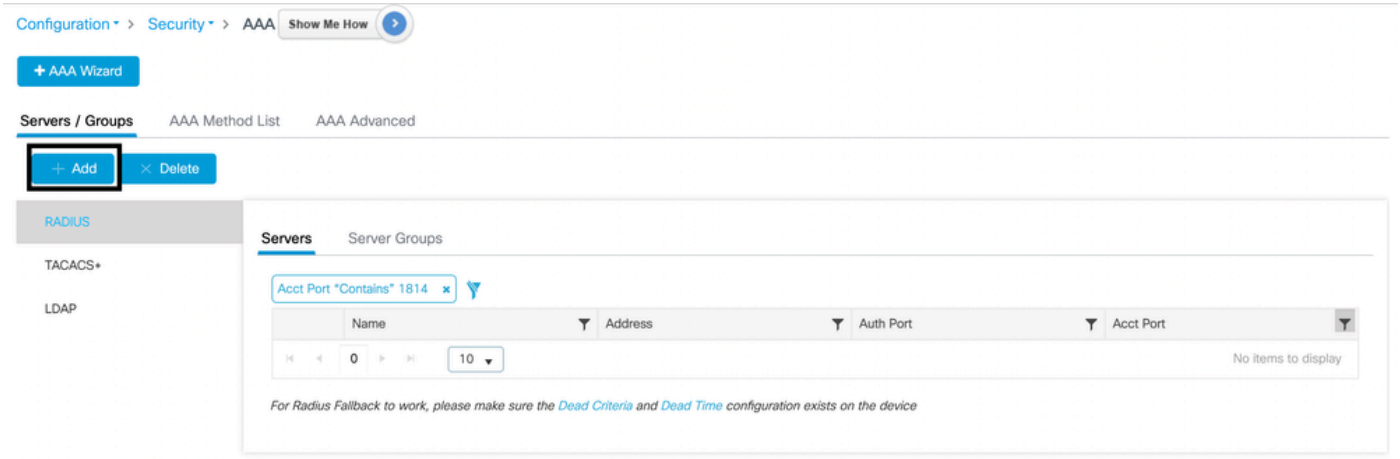
1. Configuration > Tags & Profiles > WLANsの順に選択します。
2. Addをクリックして、新しいWLANを作成します。

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

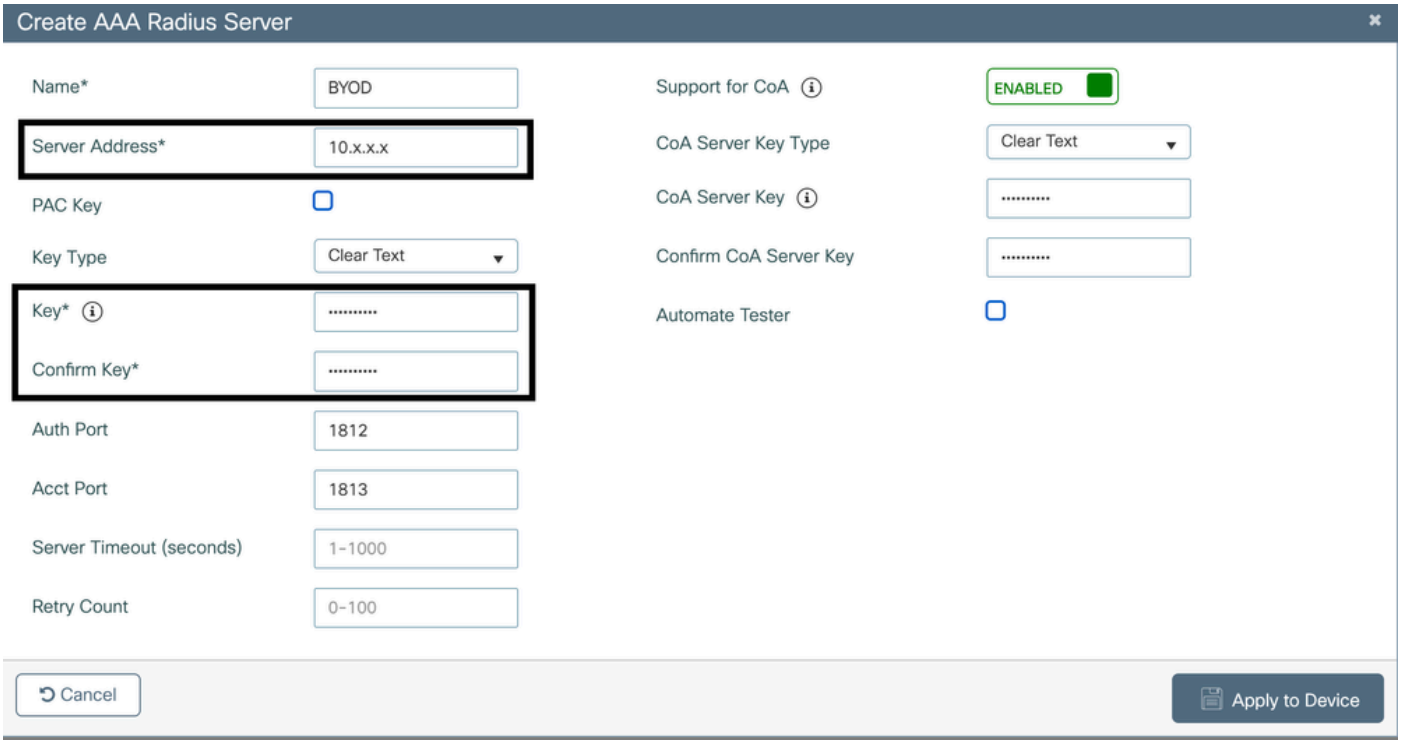


RADIUS サーバの設定

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

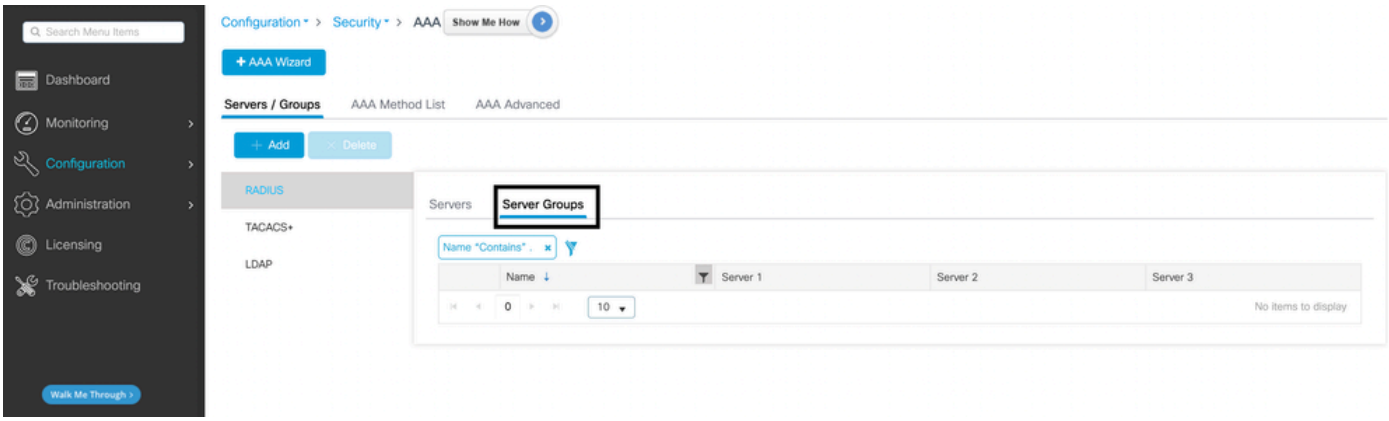


2. Addをクリックして、RADIUSサーバとしてISEを設定します。
    - サーバIP:ISEのIPアドレス。
    - Shared Secret:ISEで設定されている共有秘密に一致します。

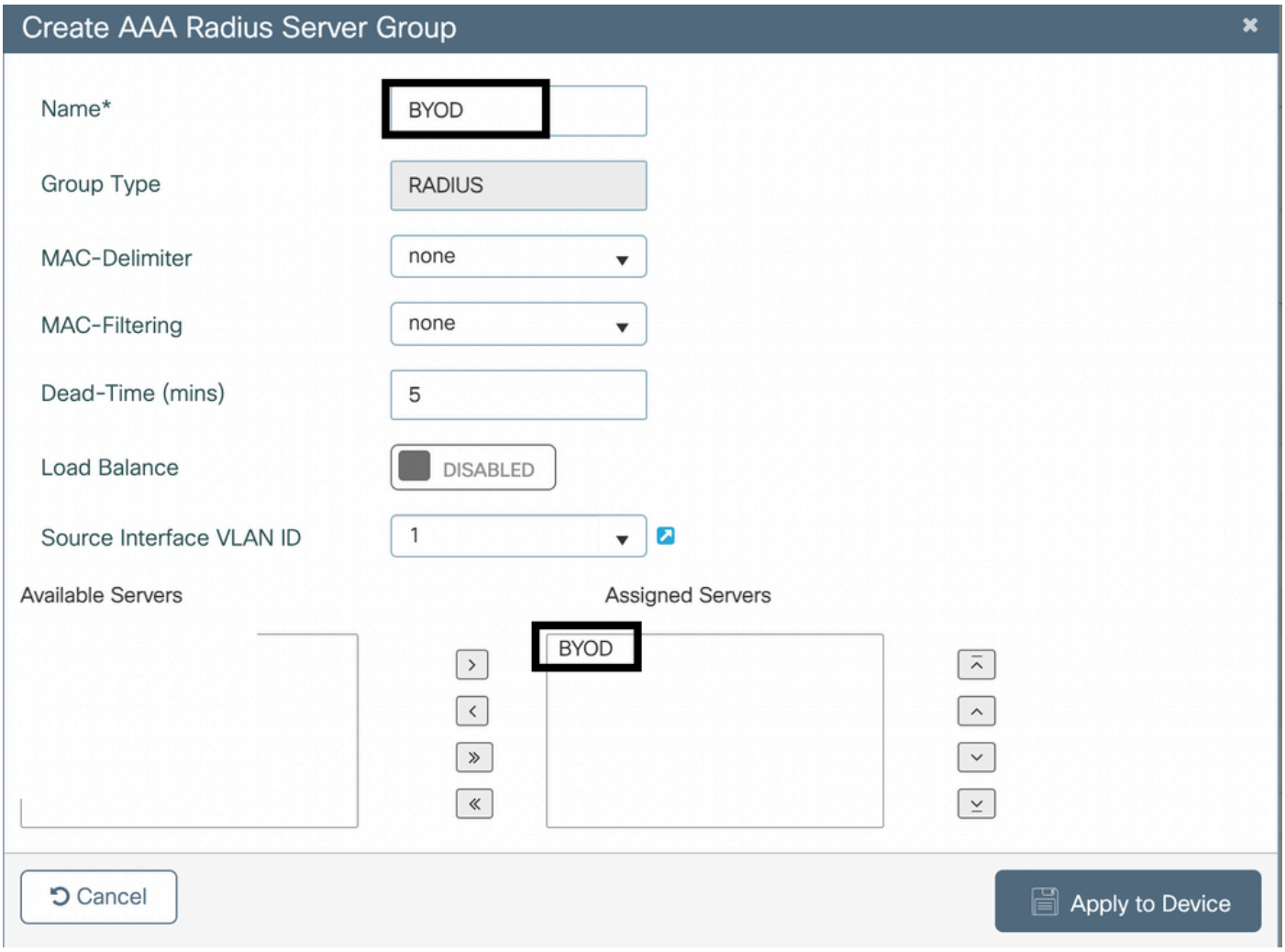


AAAサーバの設定

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



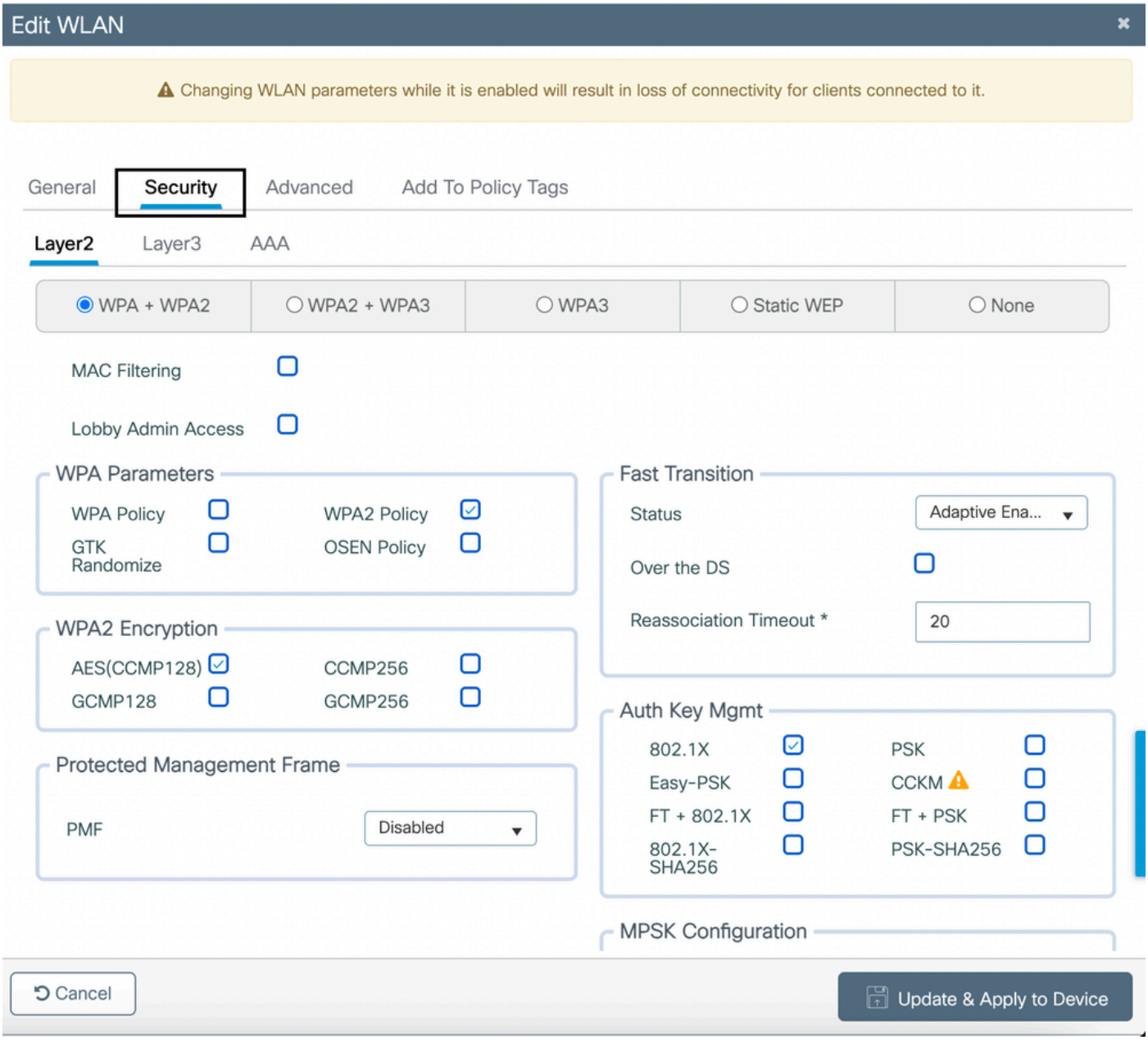
2. 新規または既存のサーバグループにRADIUSサーバを割り当てます。



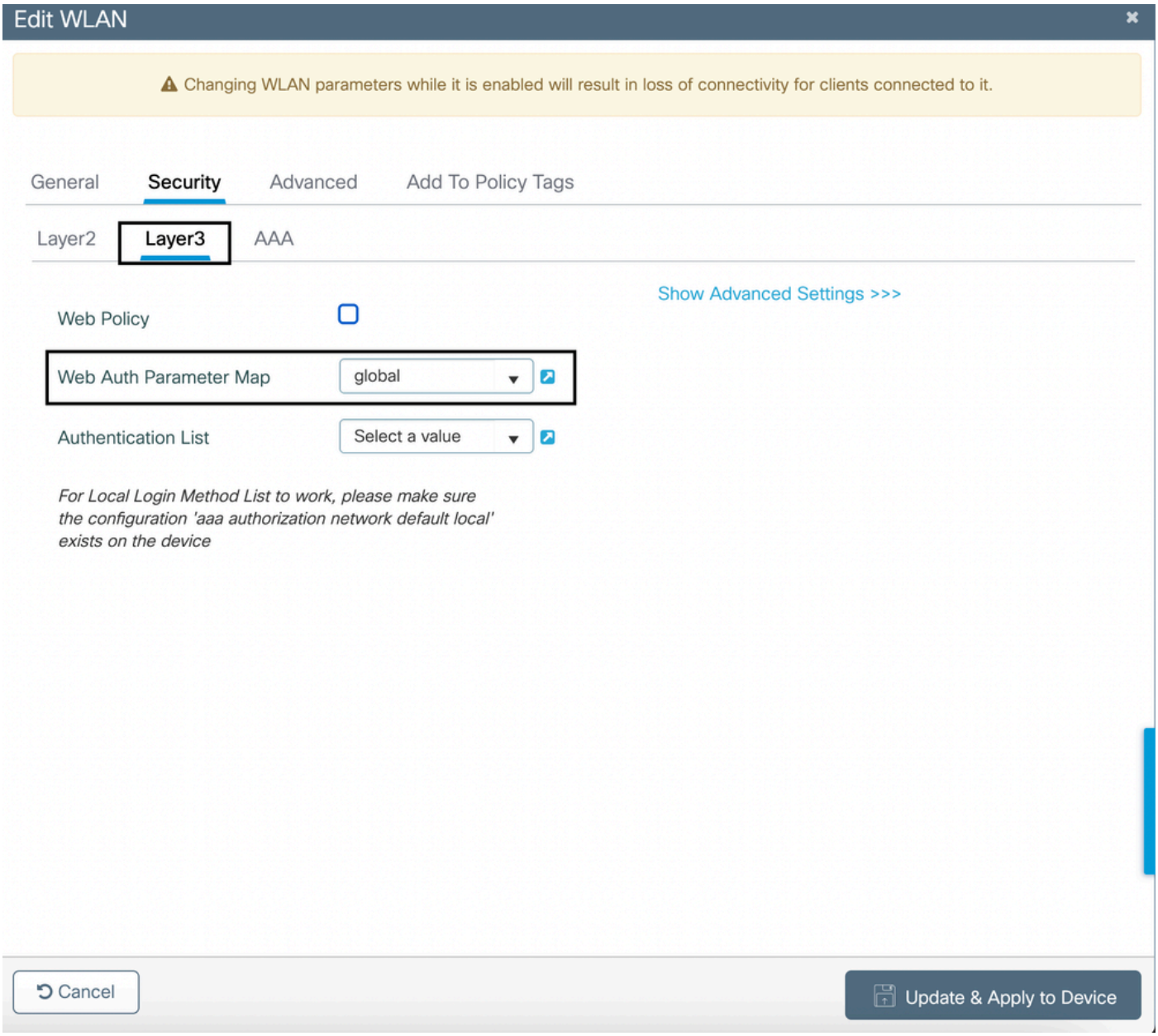
WLANのセキュリティポリシーの設定

1. 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。

2. 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



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。



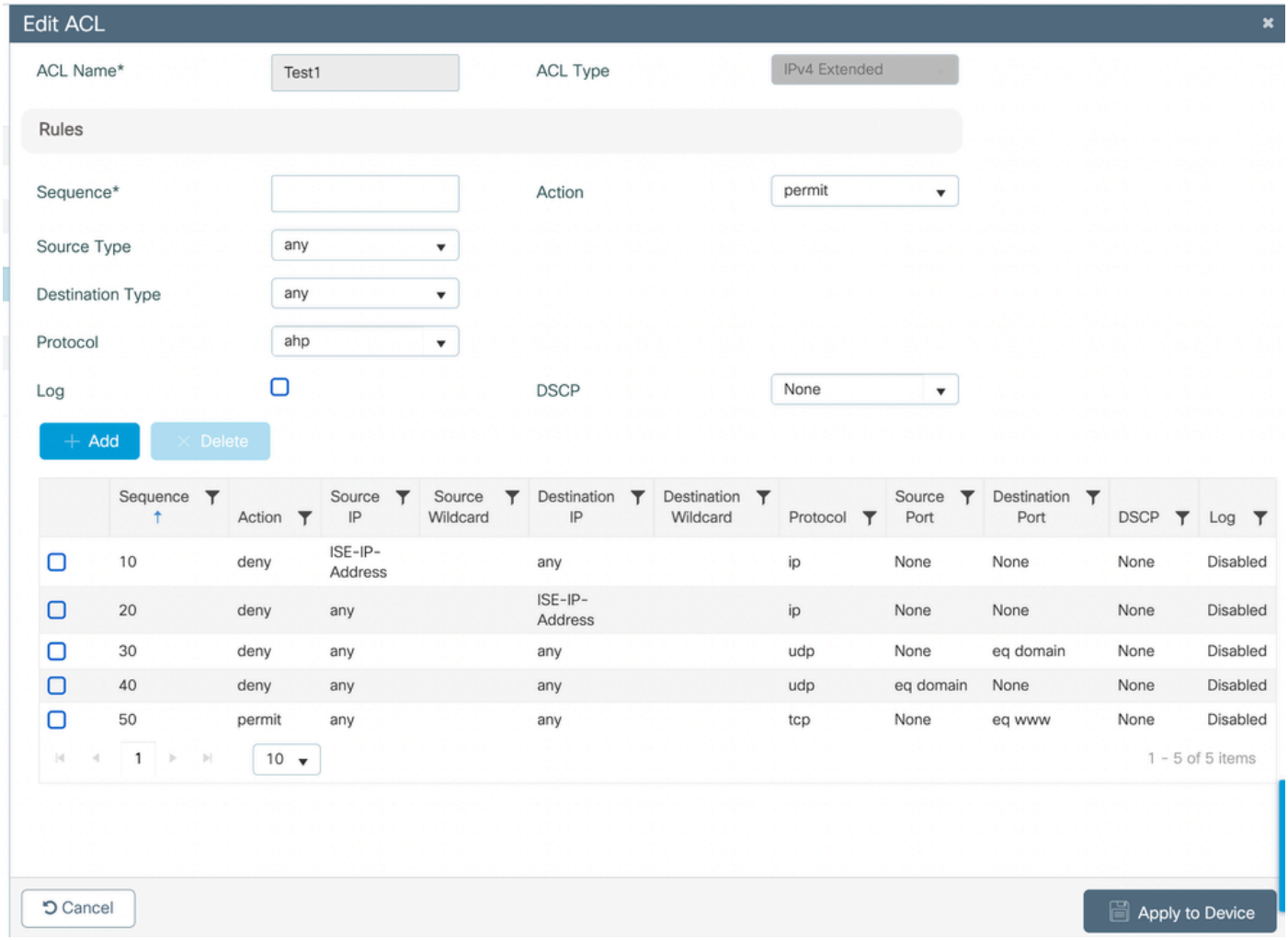
事前認証ACLの設定

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

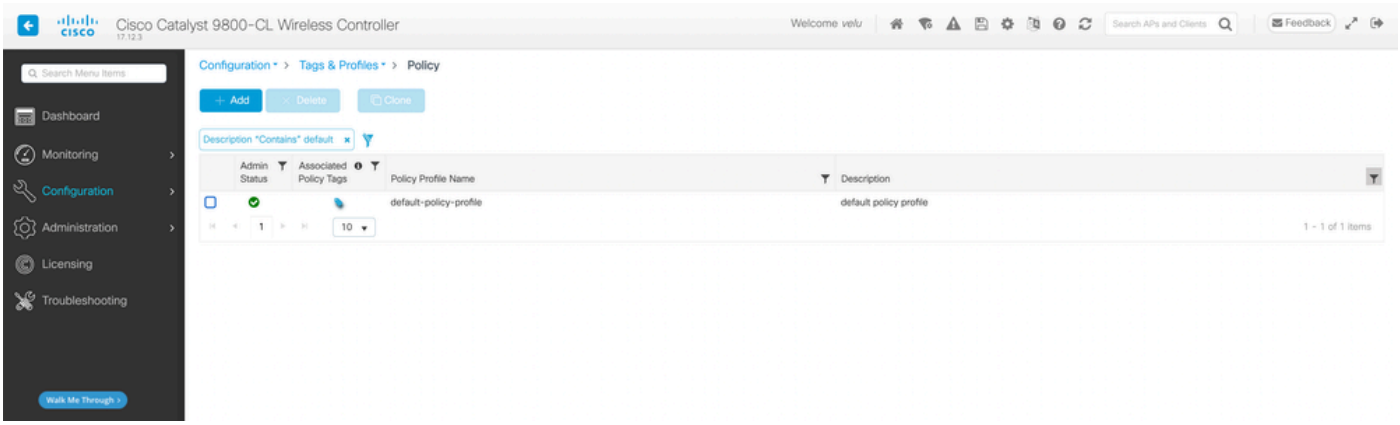
これを行うには、

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。

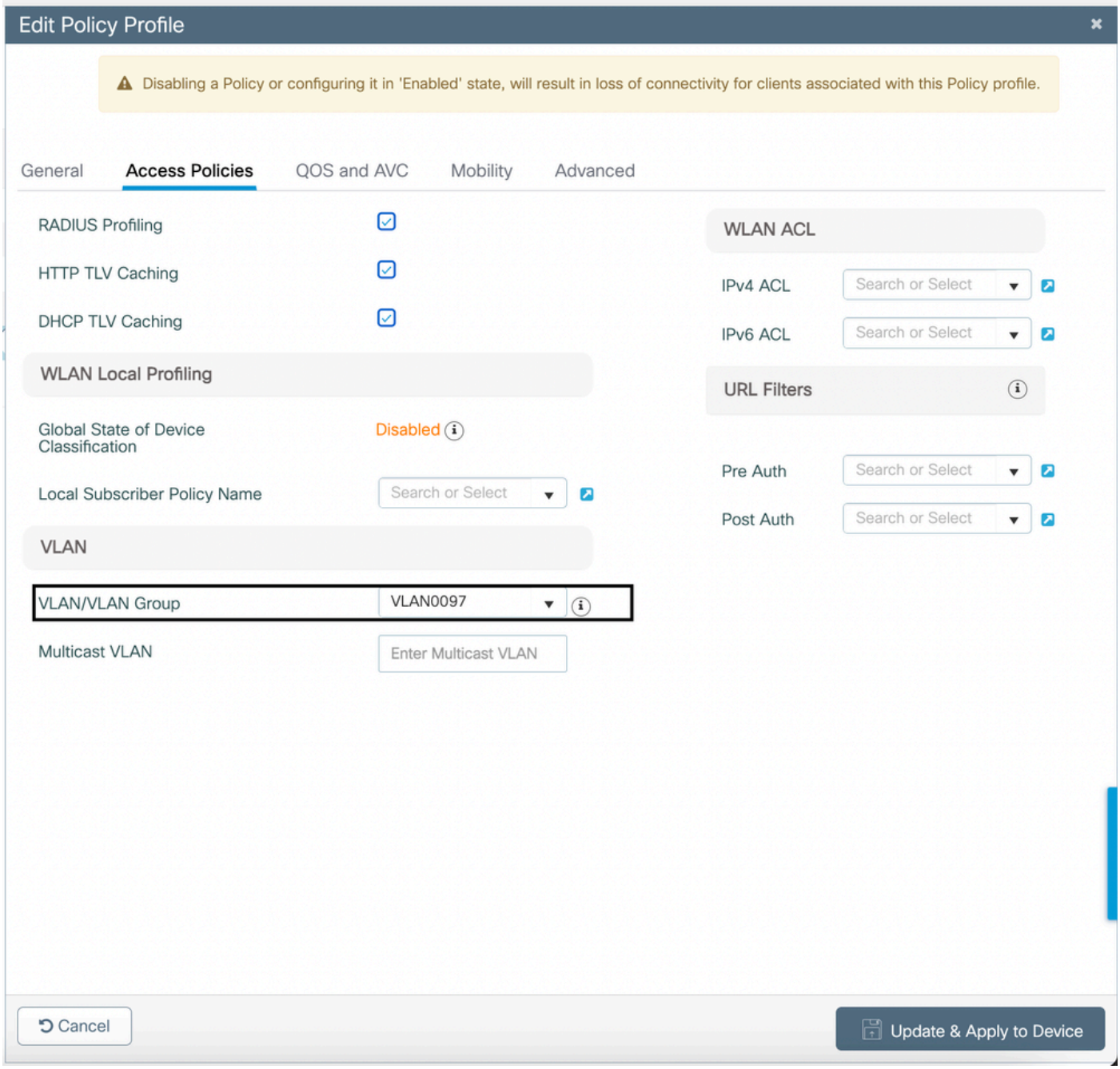


ポリシープロファイルの設定

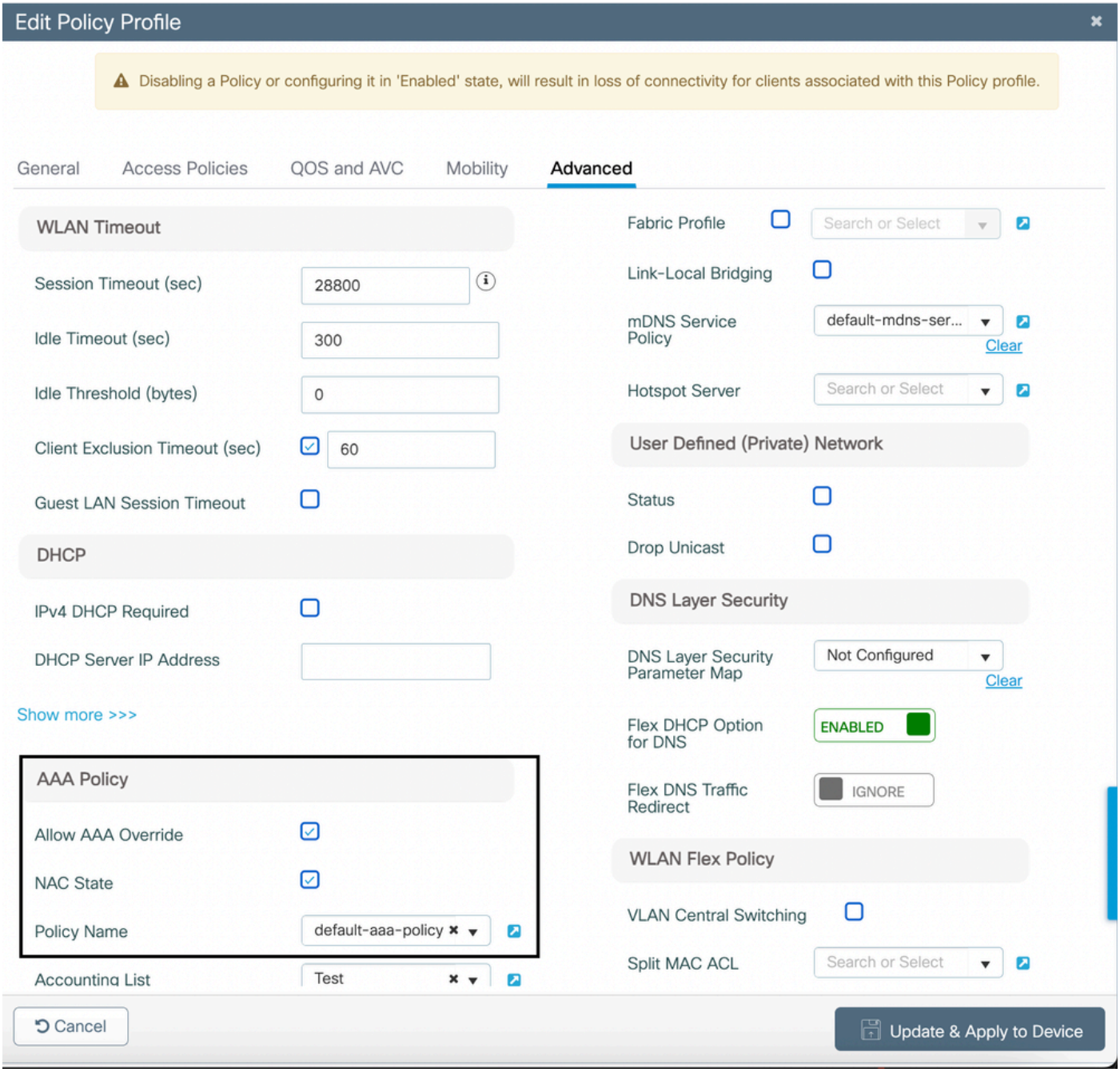
1. [設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [ポリシー（Policy）] に移動します。デフォルトポリシーを作成または使用できます



2. アクセスポリシーで適切なVLANを割り当てます

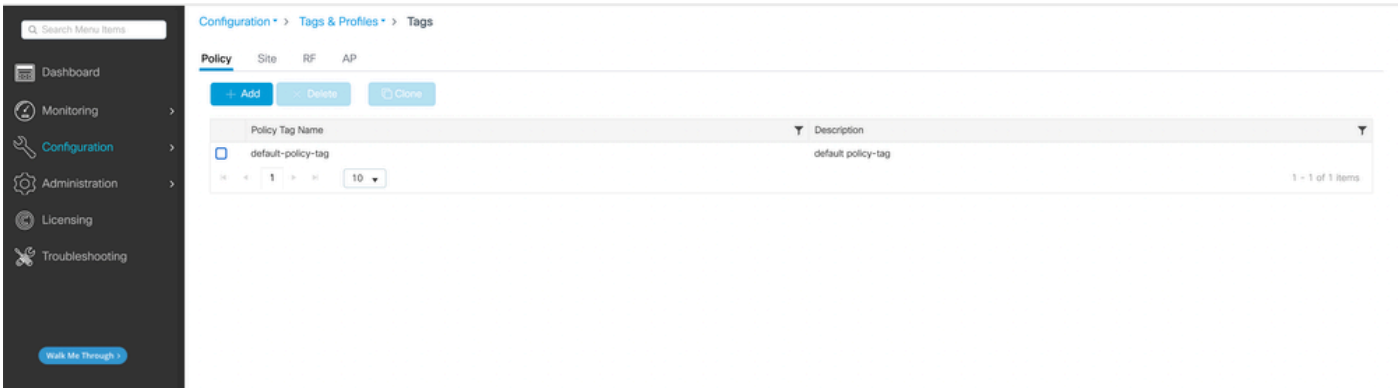


3. ポリシーのAdvancedで、Allow AAA OverrideとNAC stateを有効にします。



タグの適用と展開

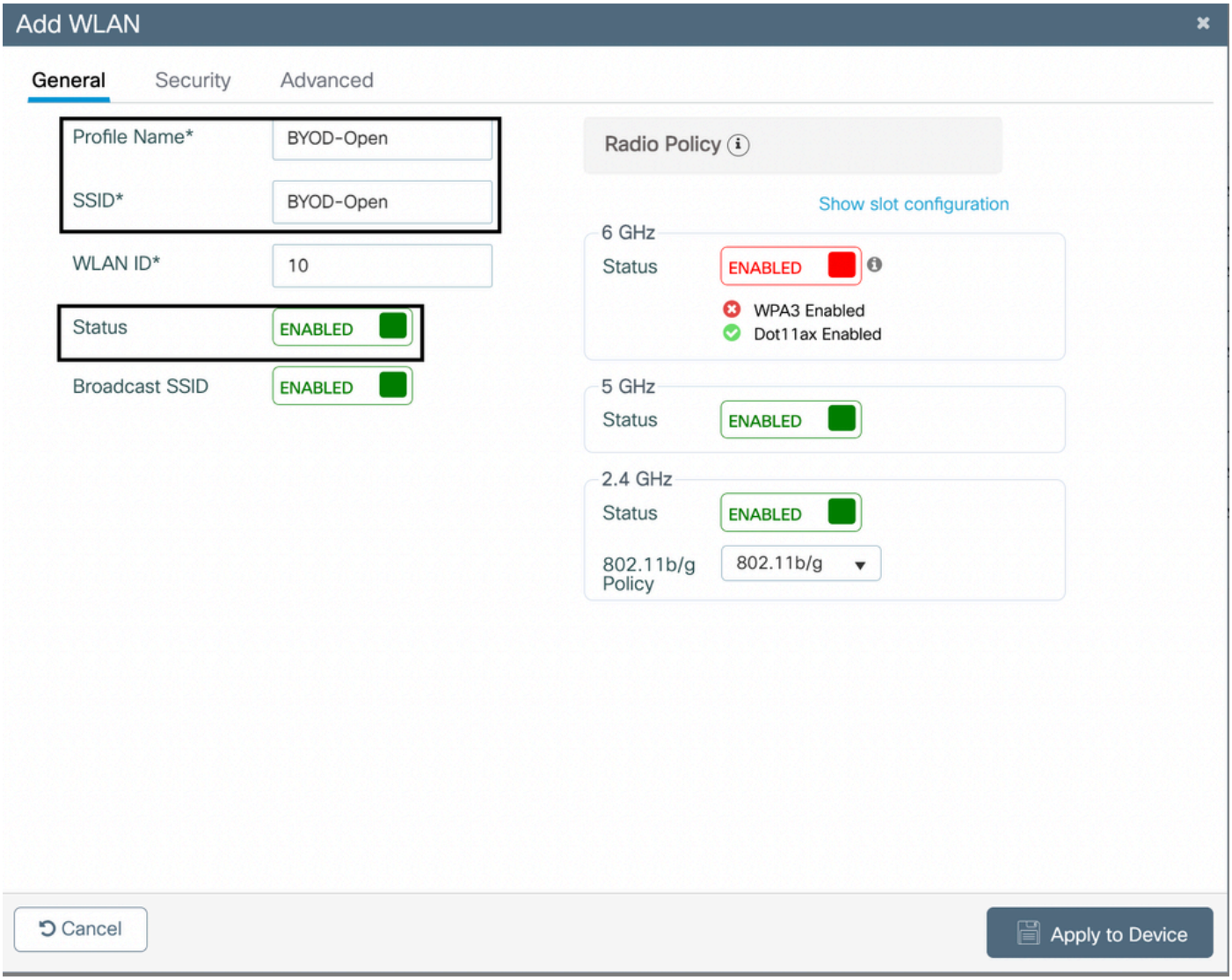
- Configuration > Tags & Profiles > Tagsの順に移動します。
- タグを作成または編集して、WLANとポリシープロファイルを含めます。
- アクセスポイントにタグを割り当てます。



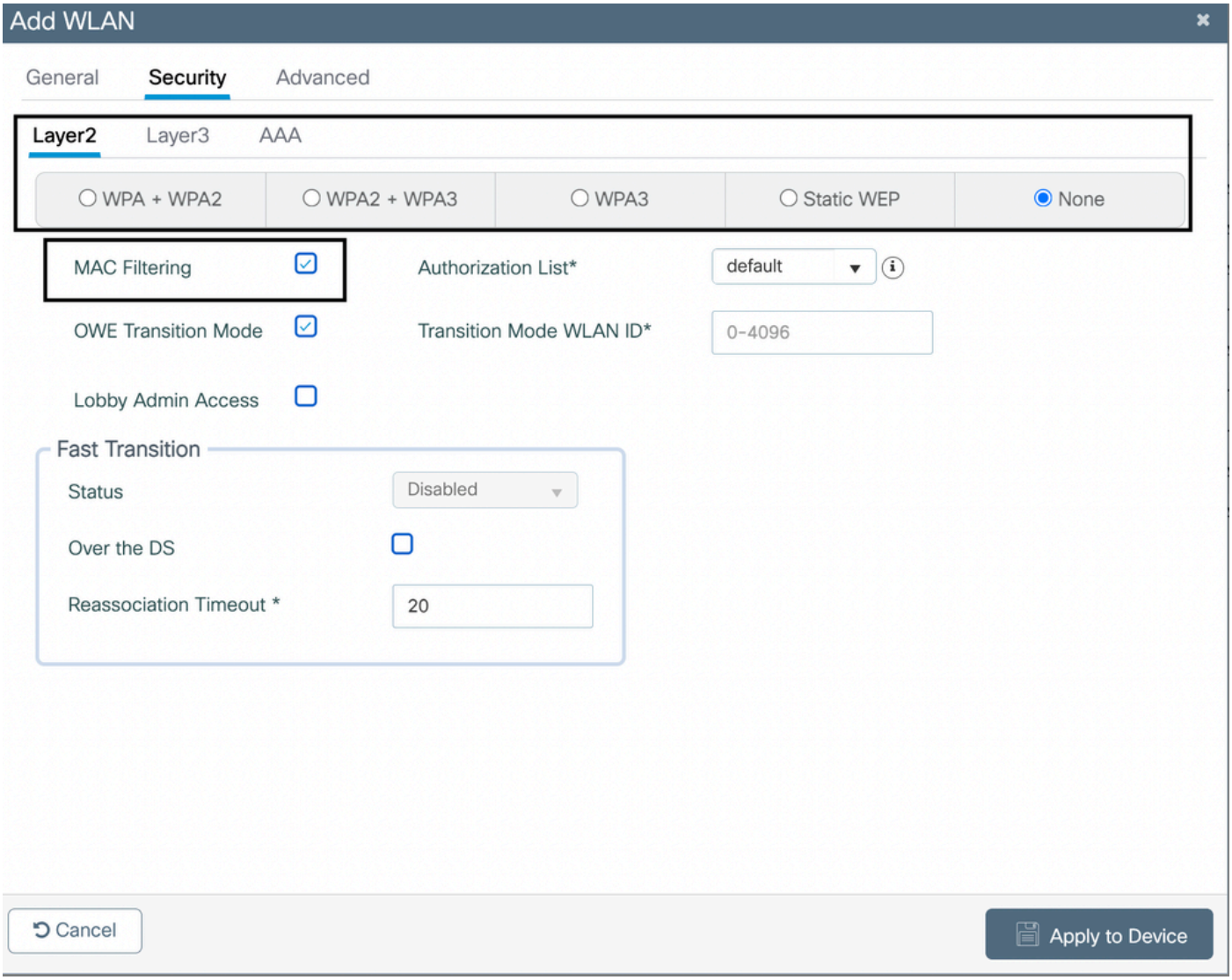
オープン/非セキュアSSIDの設定

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。

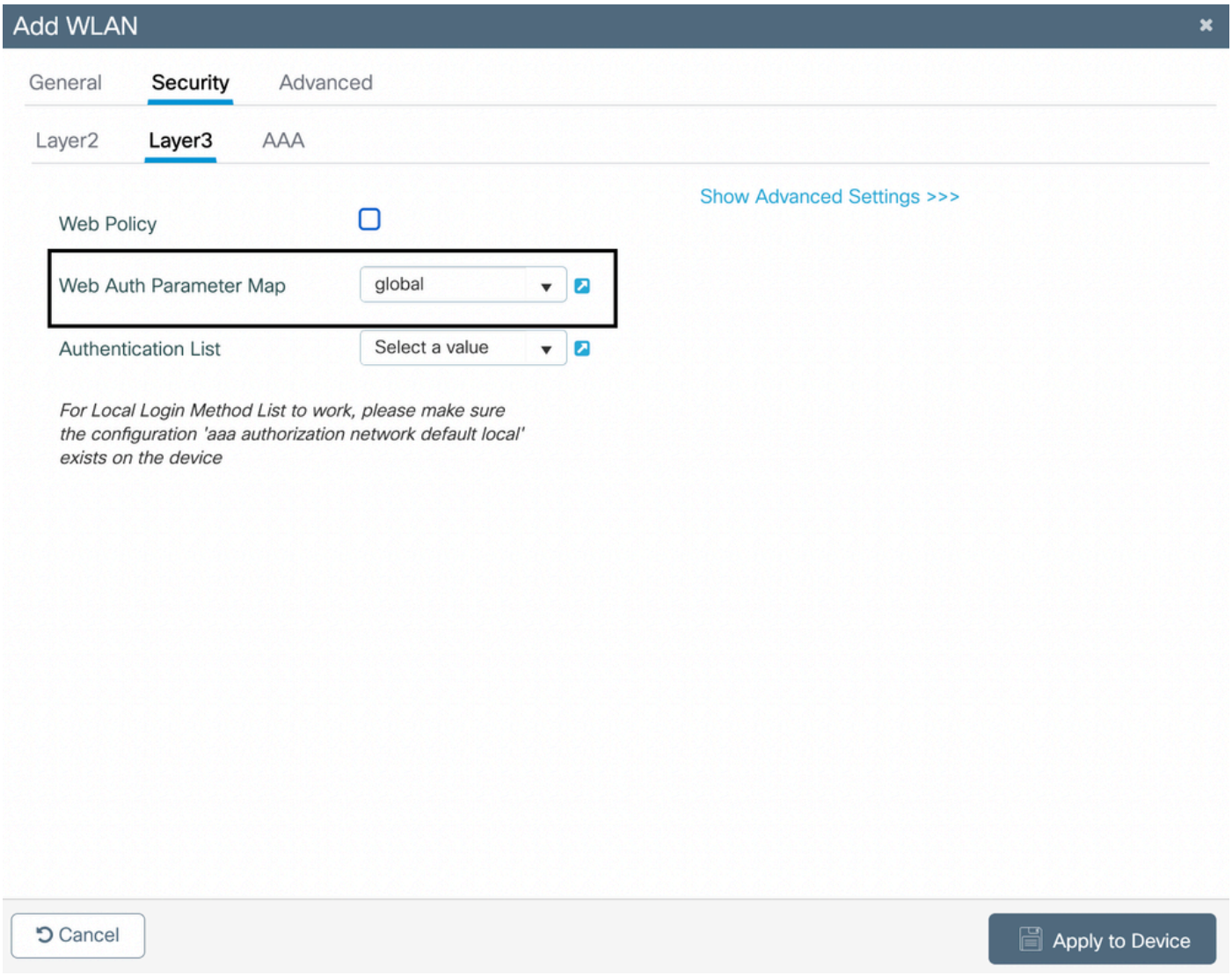
1. Configuration > Tags & Profiles > WLANsの順に選択します。[Add] ボタンをクリックします。
2. GeneralタブでSSID名を指定し、WLANボタンを有効にします。



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。



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。



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

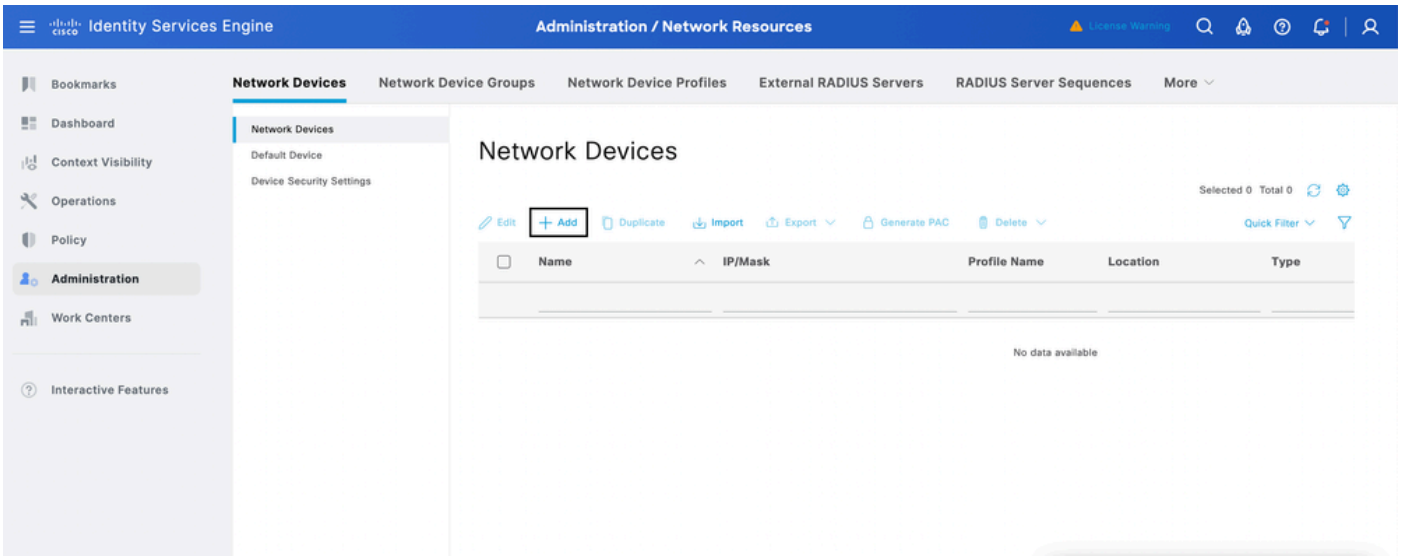
- ブラウザのセキュリティ警告を回避するために、有効なサーバ証明書をISEにインストールします。
- 証明書がエンドポイントによって信頼されていること（既知のCAまたは信頼されたルートを持つ内部CAによって署名されていること）を確認します。

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。

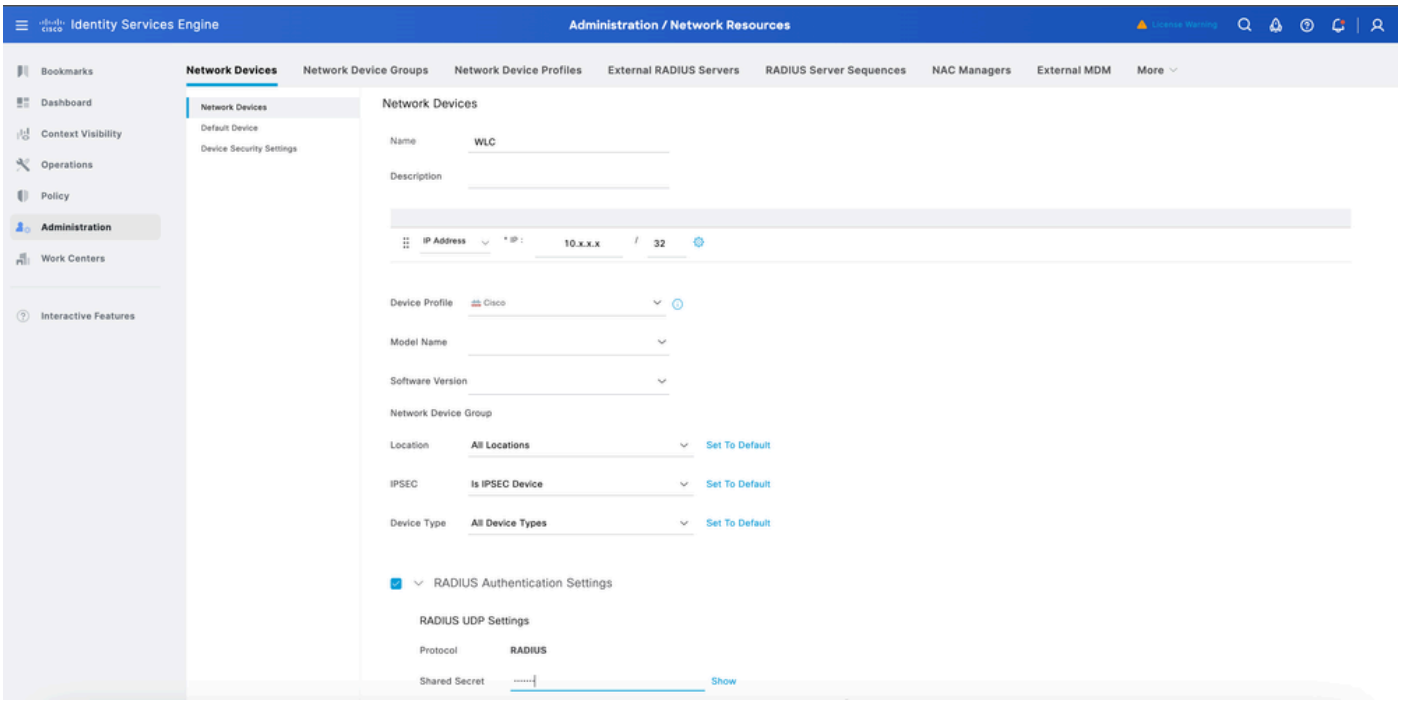
ISEネットワークデバイスの設定

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。



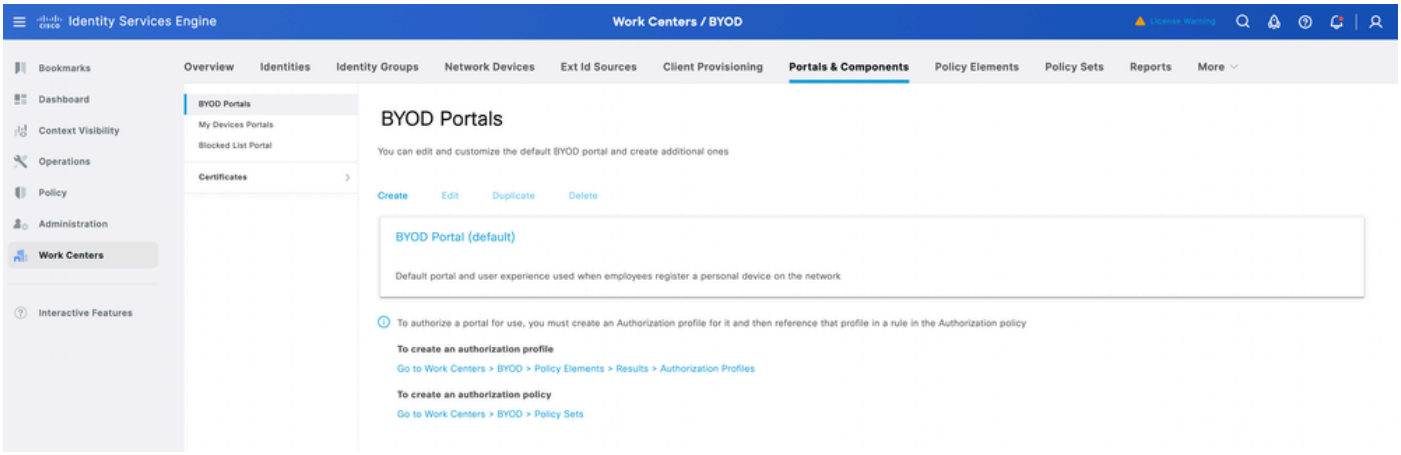
3. WLCをネットワークデバイスとして追加します。

- 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。



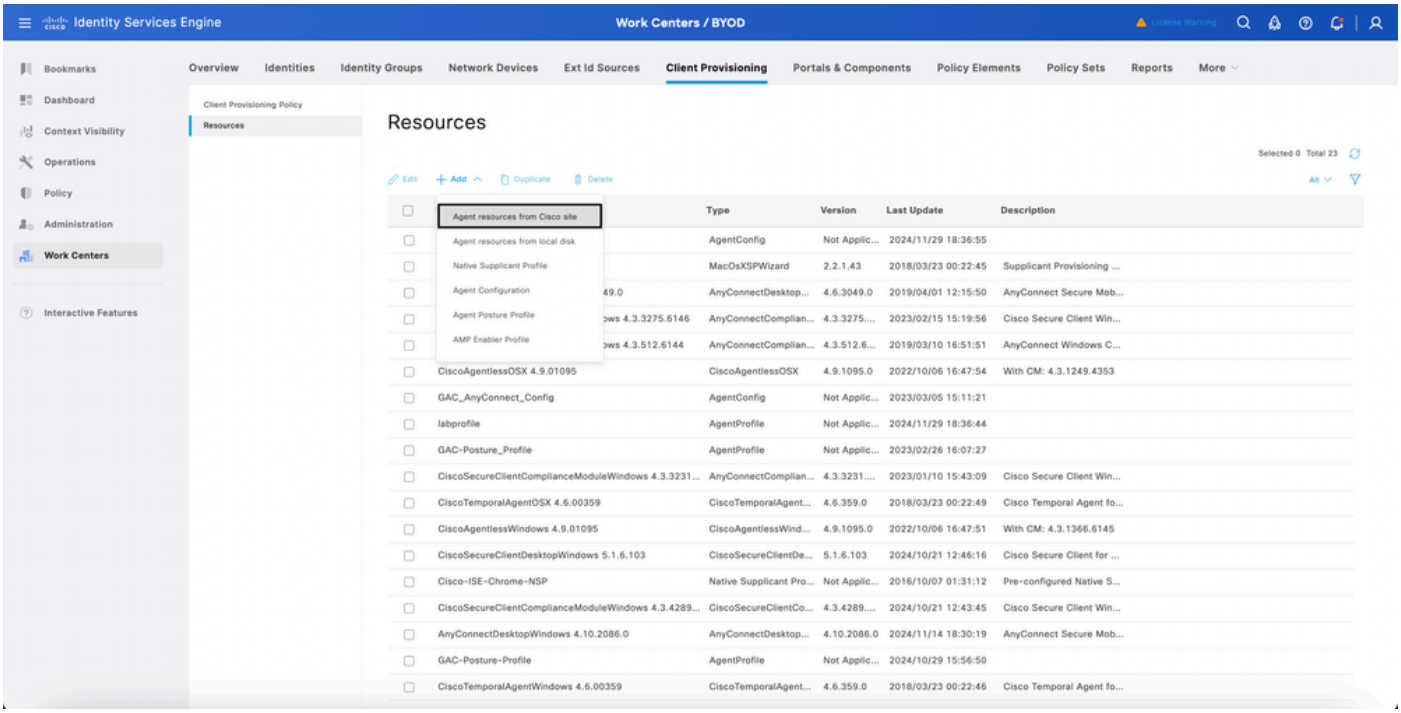
BYODポータルの作成

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。



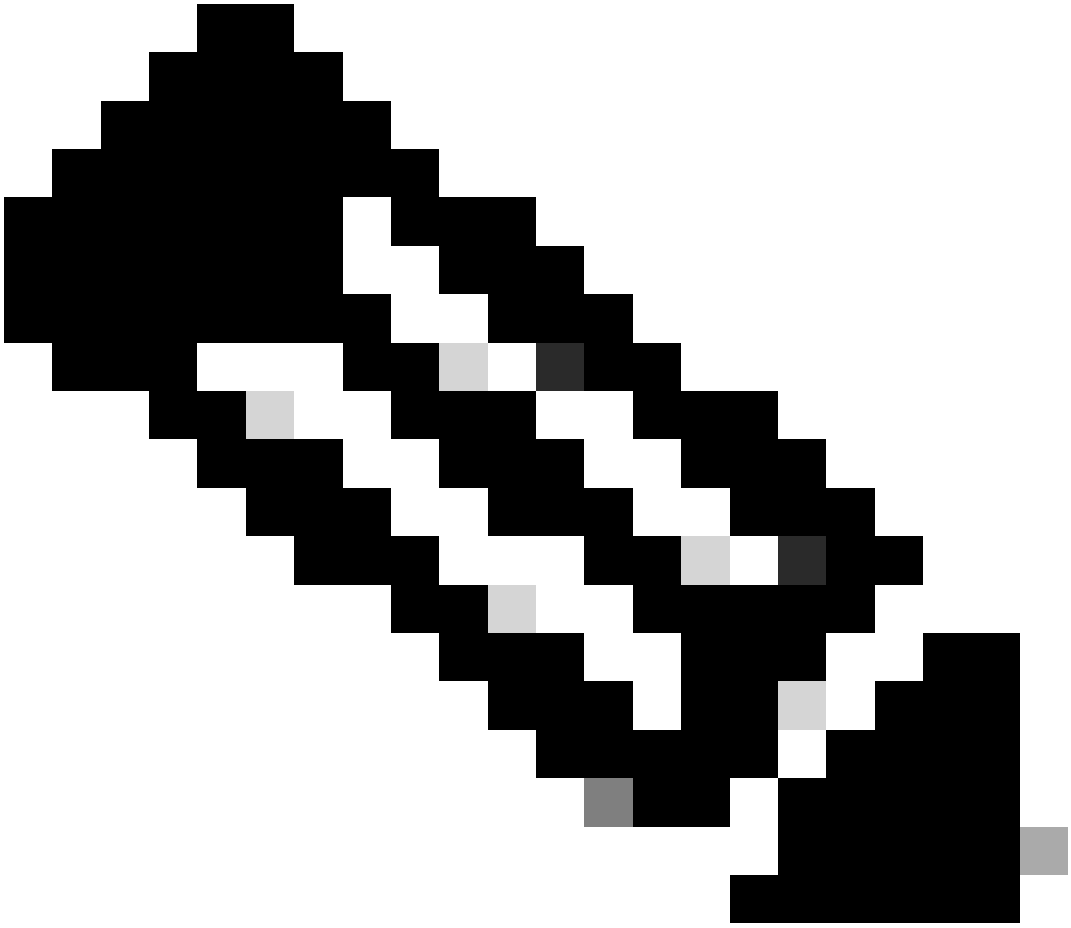
3. ソフトウェアリストで、ダウンロードする最新のCisco IOSバージョンを選択します。

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

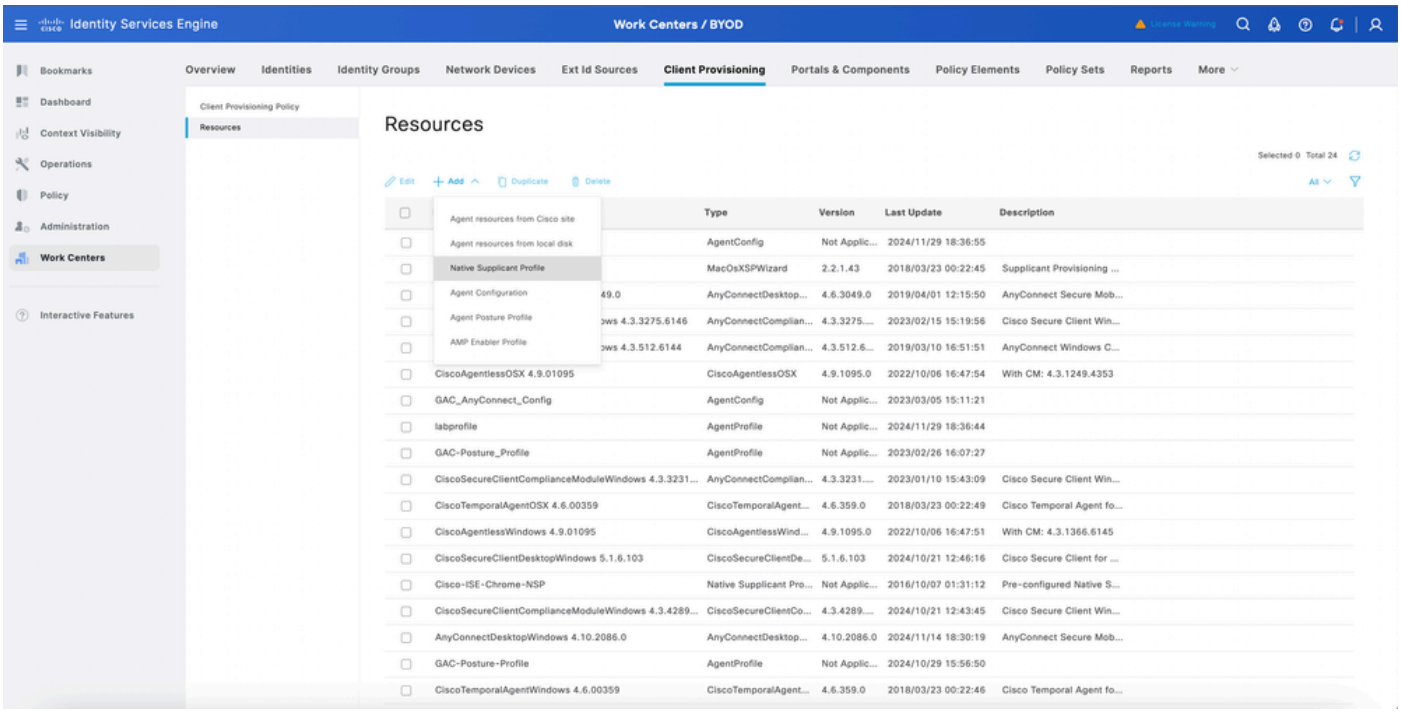


注:Cisco IOSソフトウェアは、WindowsおよびMacOSエンドポイント用のISEでダウンロードできます。Apple iPhone IOSの場合は、ネイティブサプリカントを使用してデバイスをプロビジョニングします。Androidデバイスの場合は、Play Storeからダウンロードする必要があるネットワークセットアップアシスタントがあります。

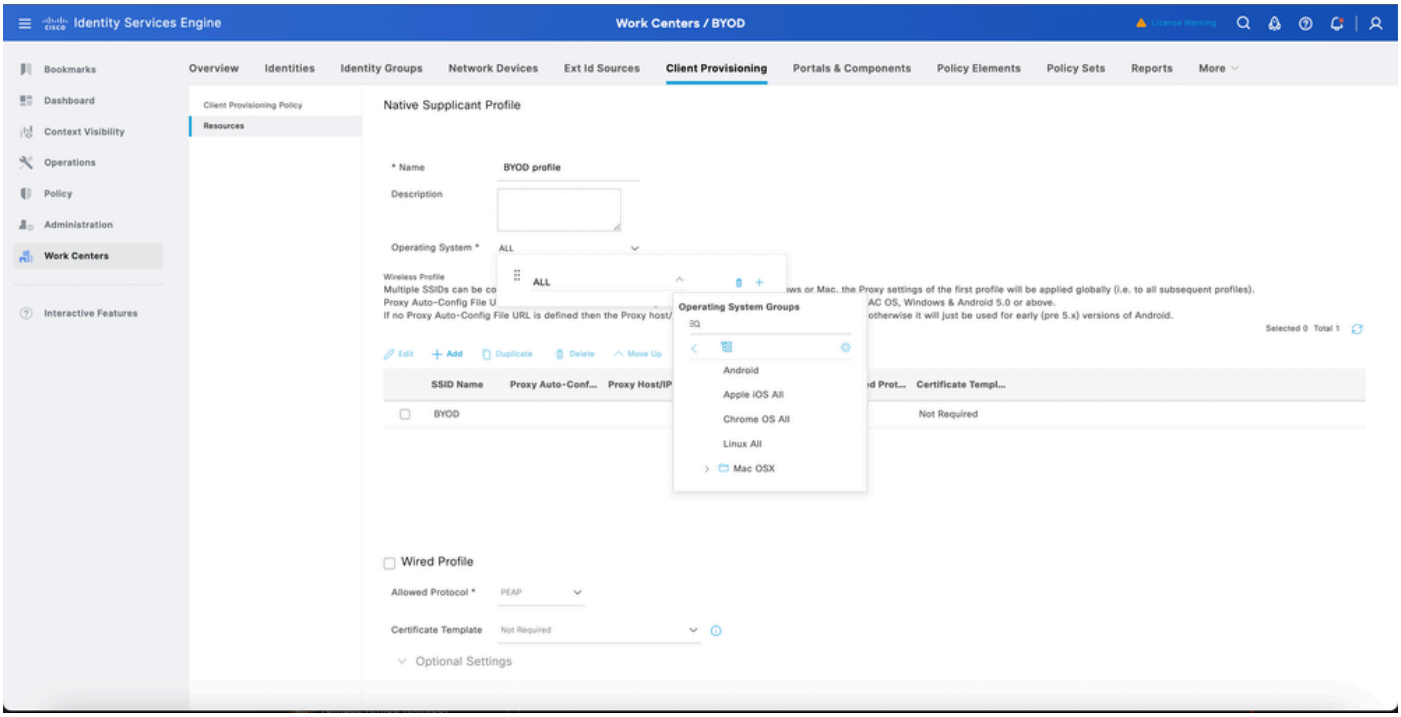
エンドポイントプロファイルの作成

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。



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。



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

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

Windows Settings

Authentication Mode User or Computer

- [ ] Automatically use logon name and password (and domain if any)
- [x] 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
- [x] Connect even if the network is not broadcasting its name (SSID)

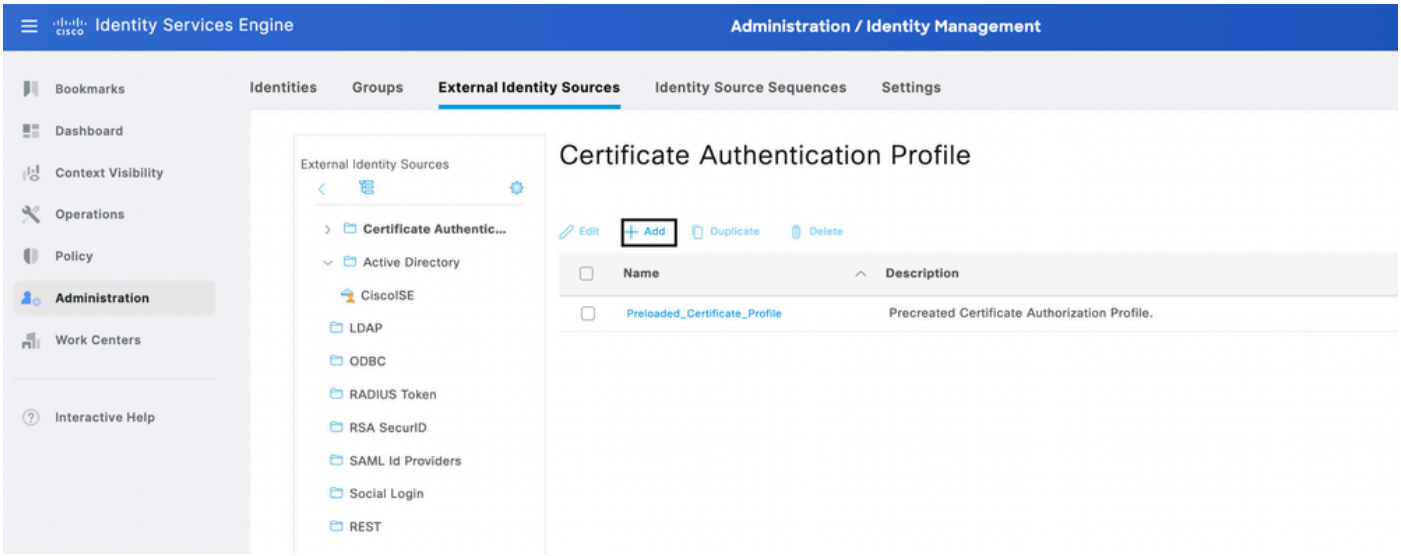
iOS Settings

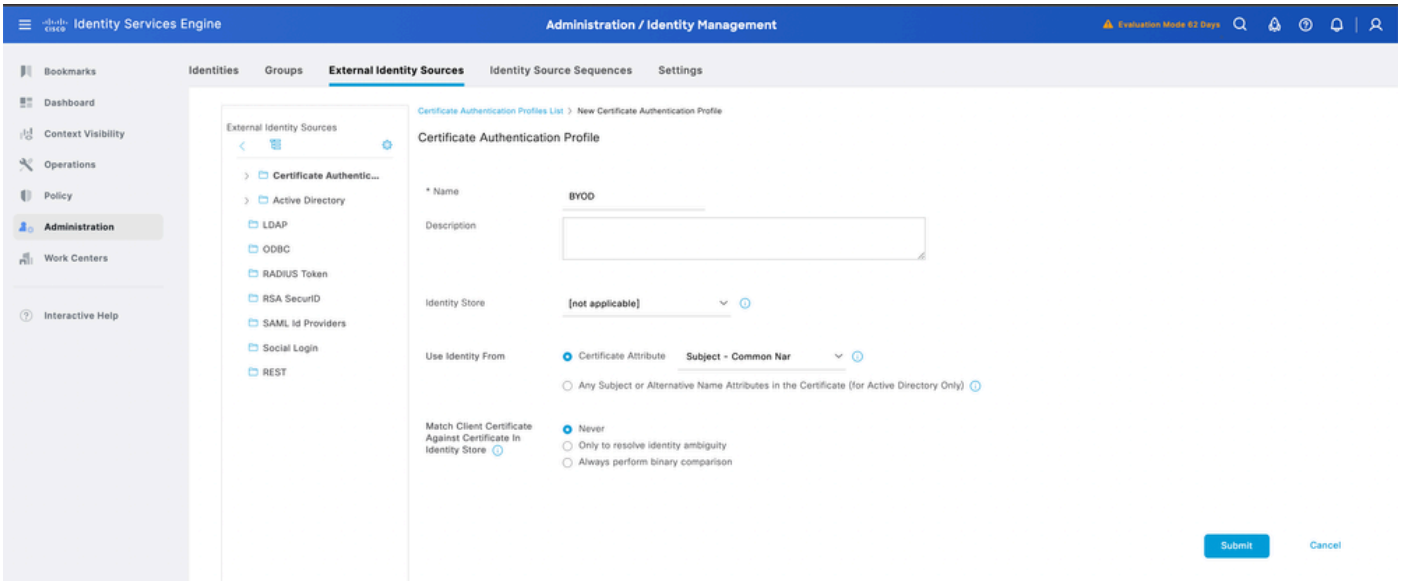
- [ ] Enable if target network is hidden

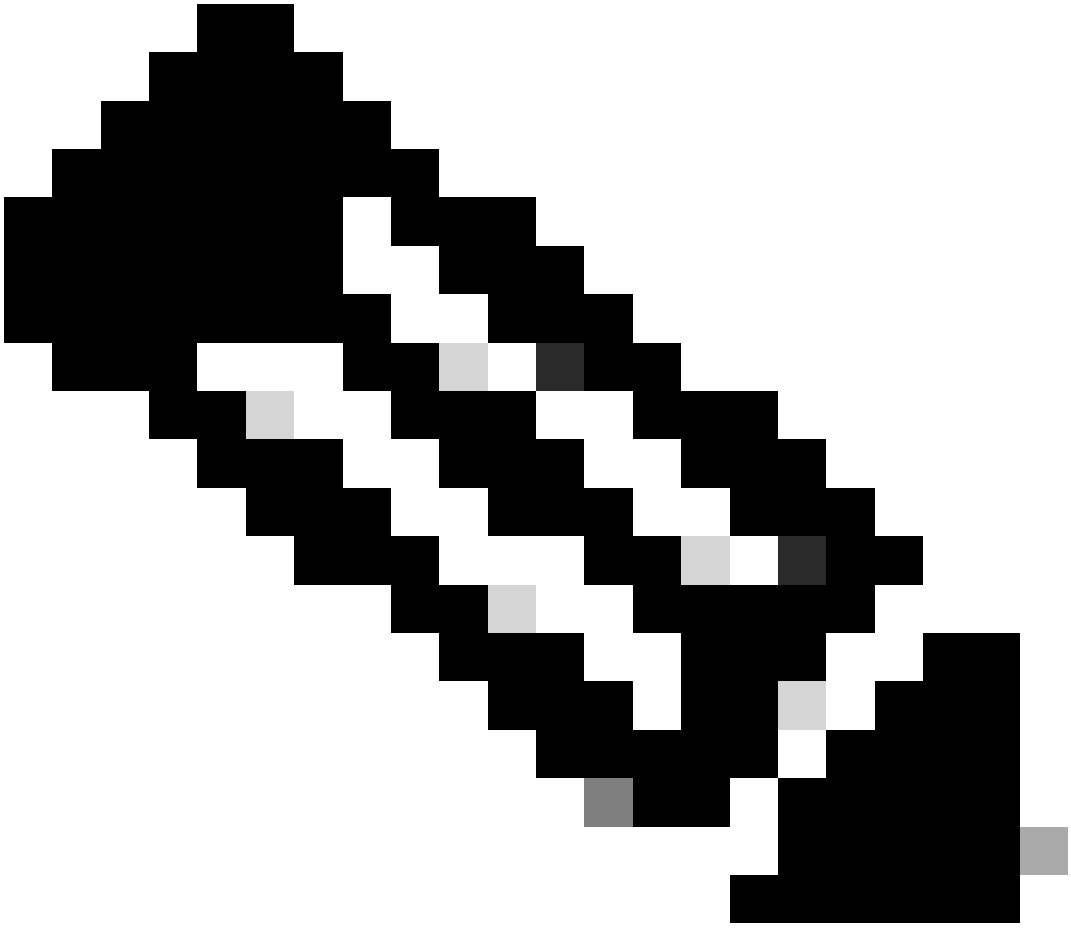
Android Settings

Certificate Enrollment Protocol:

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。

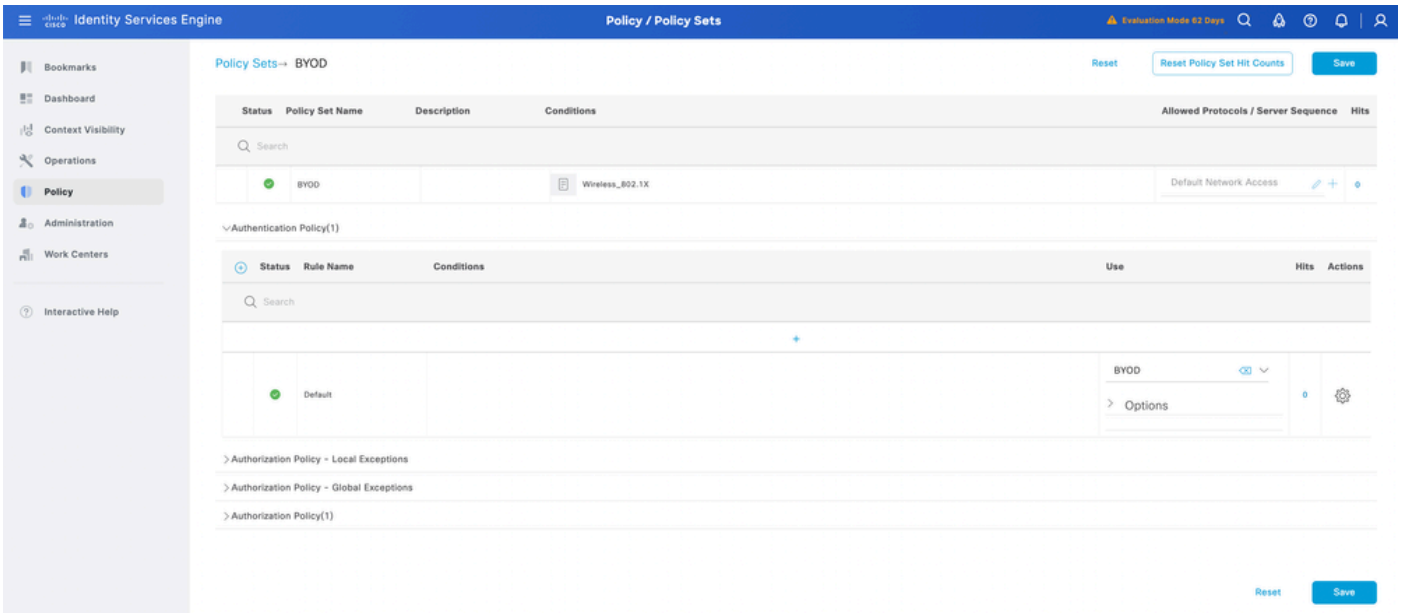






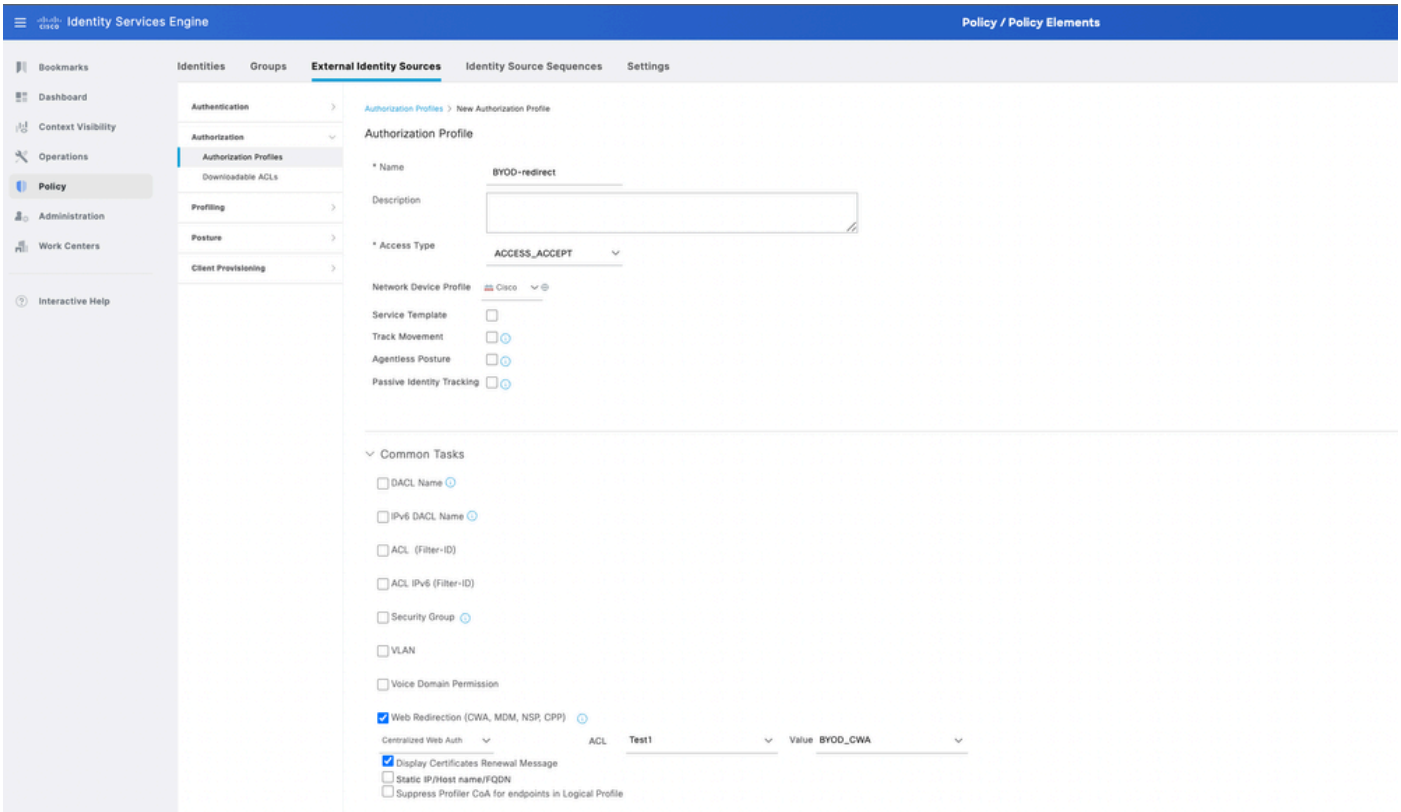
注:IDストアでは、ISEに統合されているActive Directoryをいつでも選択できます。これにより、追加のセキュリティのために証明書からユーザ検索を実行できます。

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。

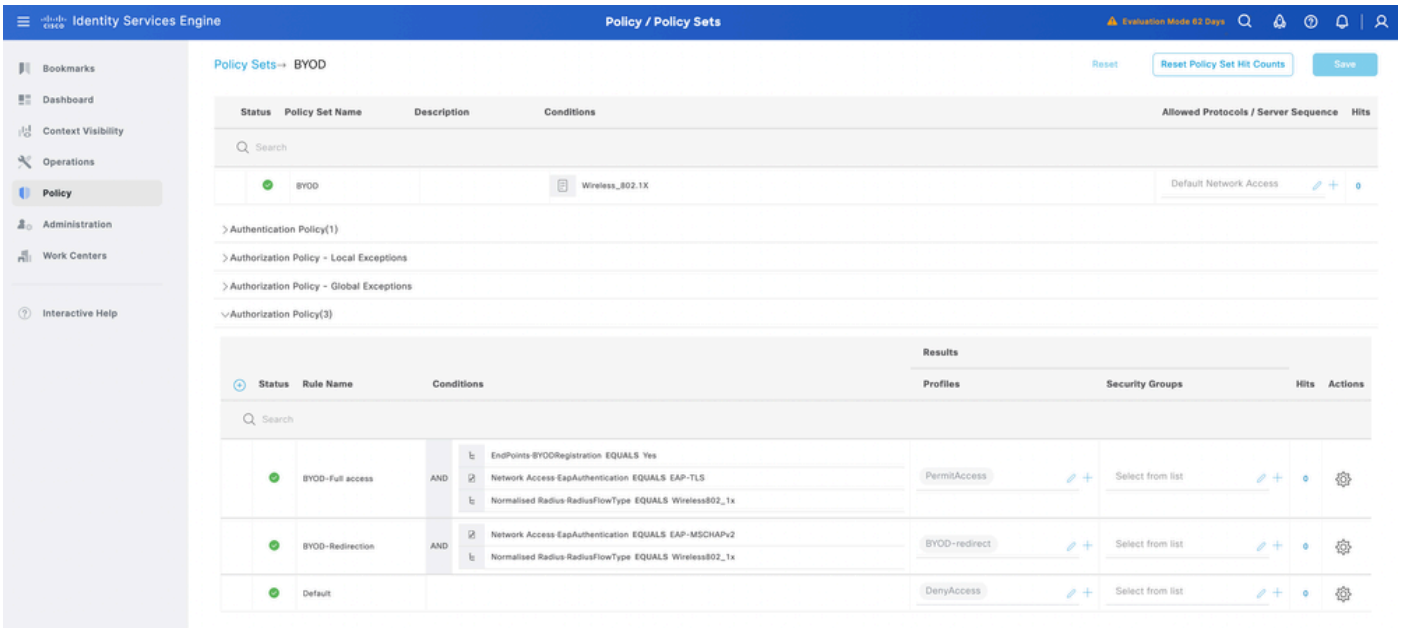


4. BYODフロー後のBYODリダイレクトとフルアクセスの許可プロファイルを設定します。[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] の順に選択します。

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。

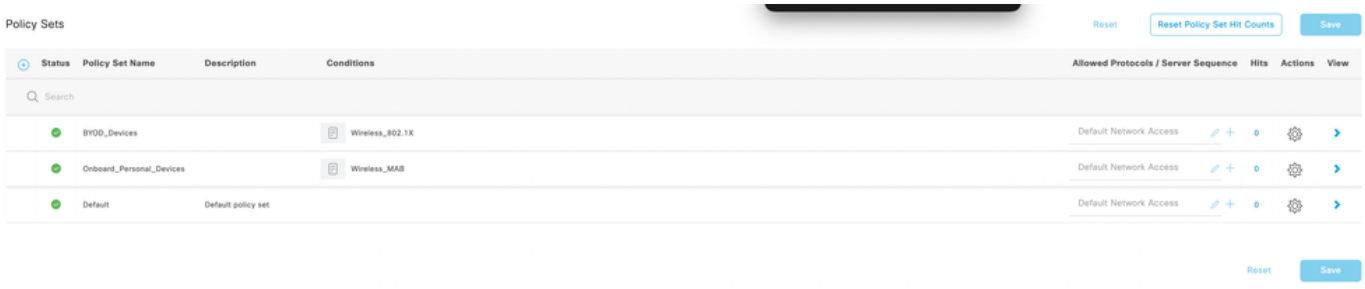


デュアルSSID BYOD用のISEポリシーセットの設定

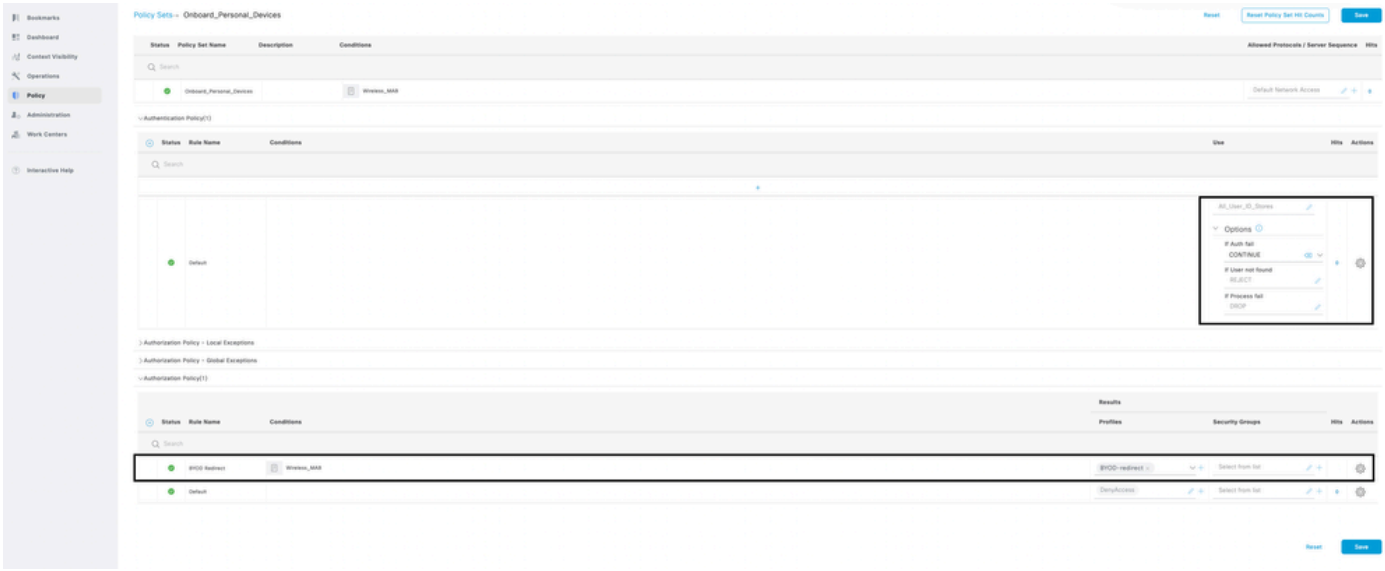
デュアルSSID BYOD設定では、2ポリシーセットがISEで設定されます。最初のポリシーセットはオープン/非セキュアSSID用で、ポリシーセット設定はオープン/非セキュアSSIDへの接続時にユーザをBYODページにリダイレクトします

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。

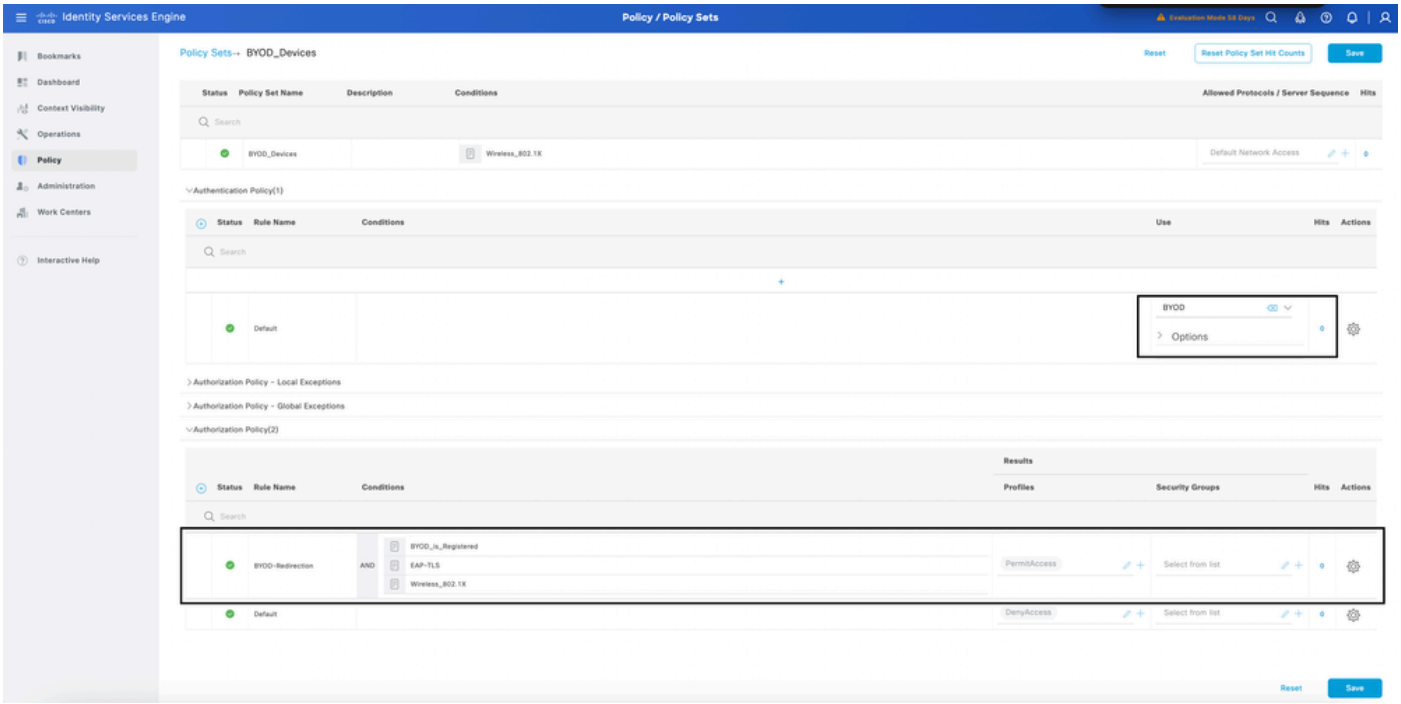


3. オンボーディングポリシーセットで、オプションの下のContinue selectedを見つけます。認可ポリシーについて、条件を作成し、リダイレクション認可プロファイルをマッピングします。認可プロファイルの作成にも同じ手順が含まれます。これはポイント4で確認できます。



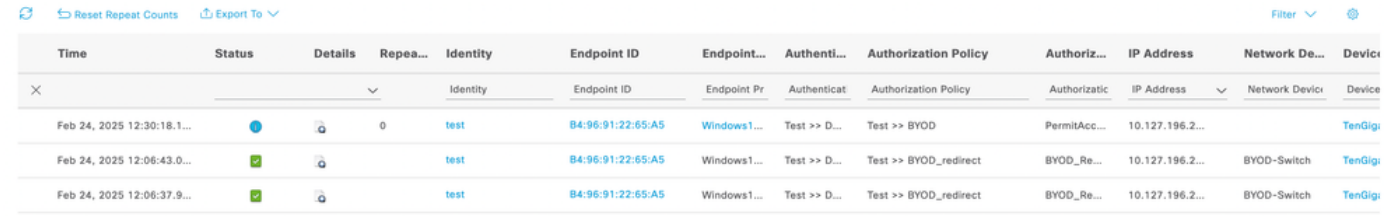
4. BYOD登録済みポリシーセットで、見つかったのと同じ証明書プロファイルを使用して認証ポリシーを設定します。

「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。

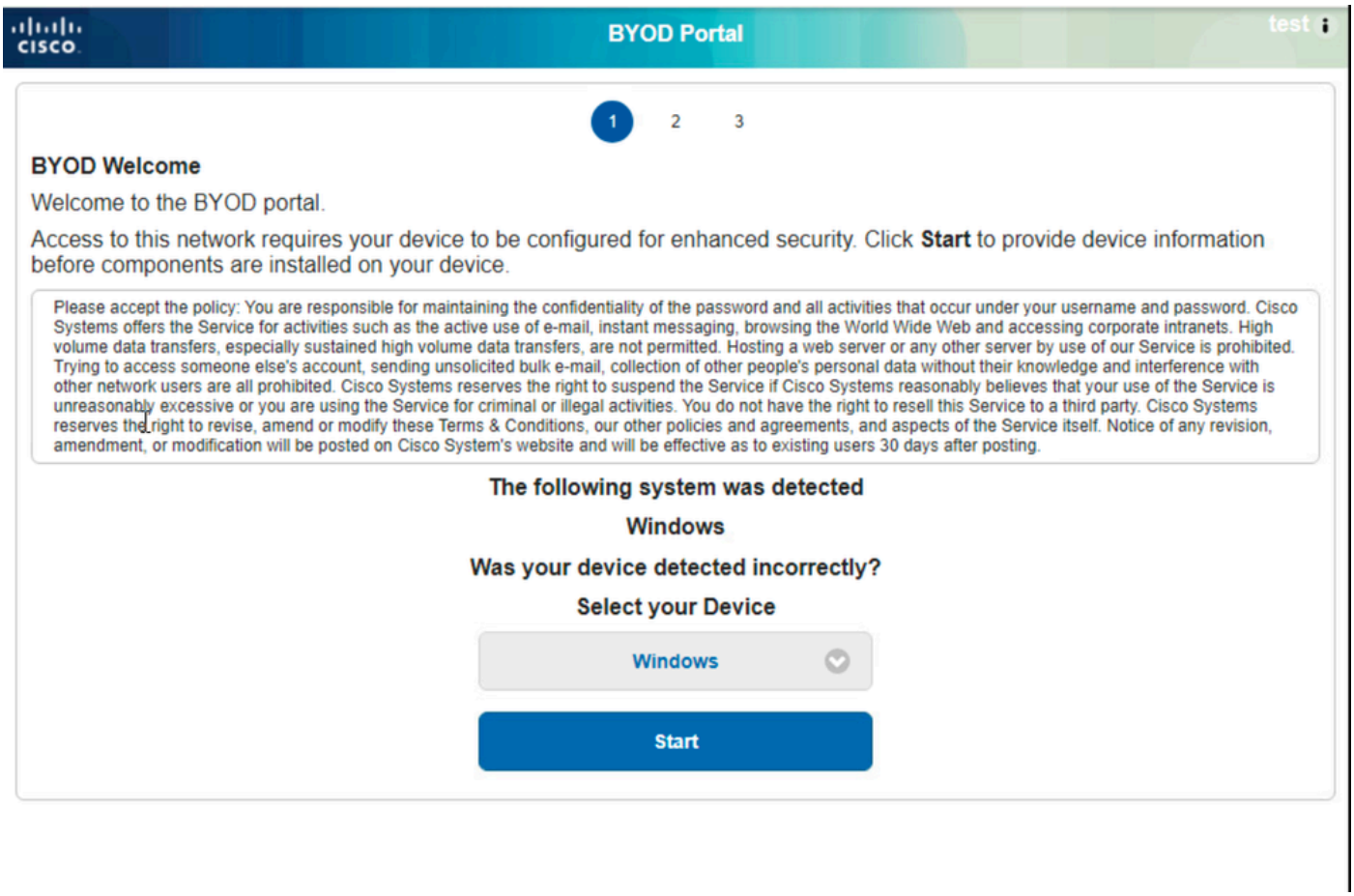


Logging

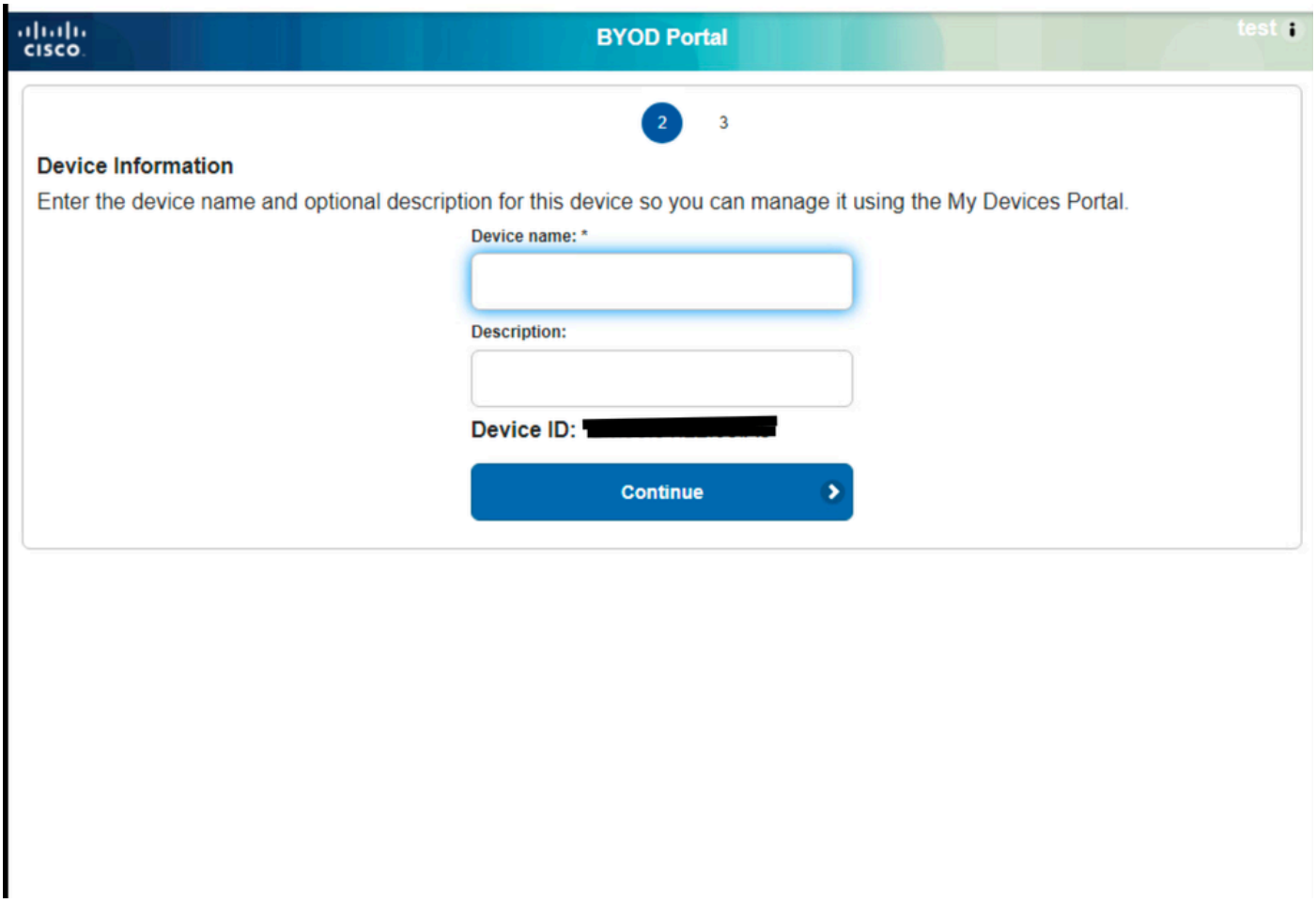
ISEからのライブログから、ユーザ認証が成功し、BYODポータルページにリダイレクトされます。BYODフローが完了すると、ユーザはネットワークへのアクセスを許可されます



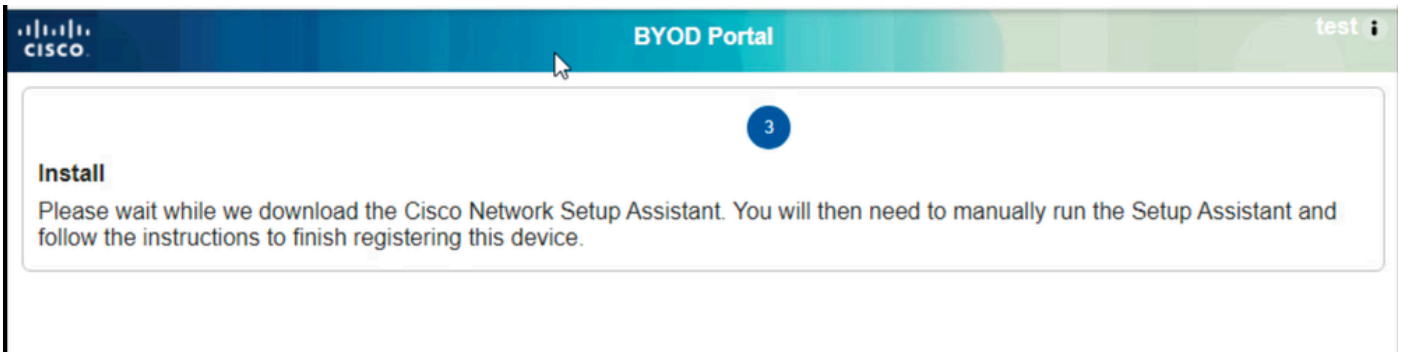
ユーザの観点からは、最初にBYODページにリダイレクトされ、Webページから適切なデバイスを選択する必要があります。テストでは、Windows 10デバイスが使用されました



[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

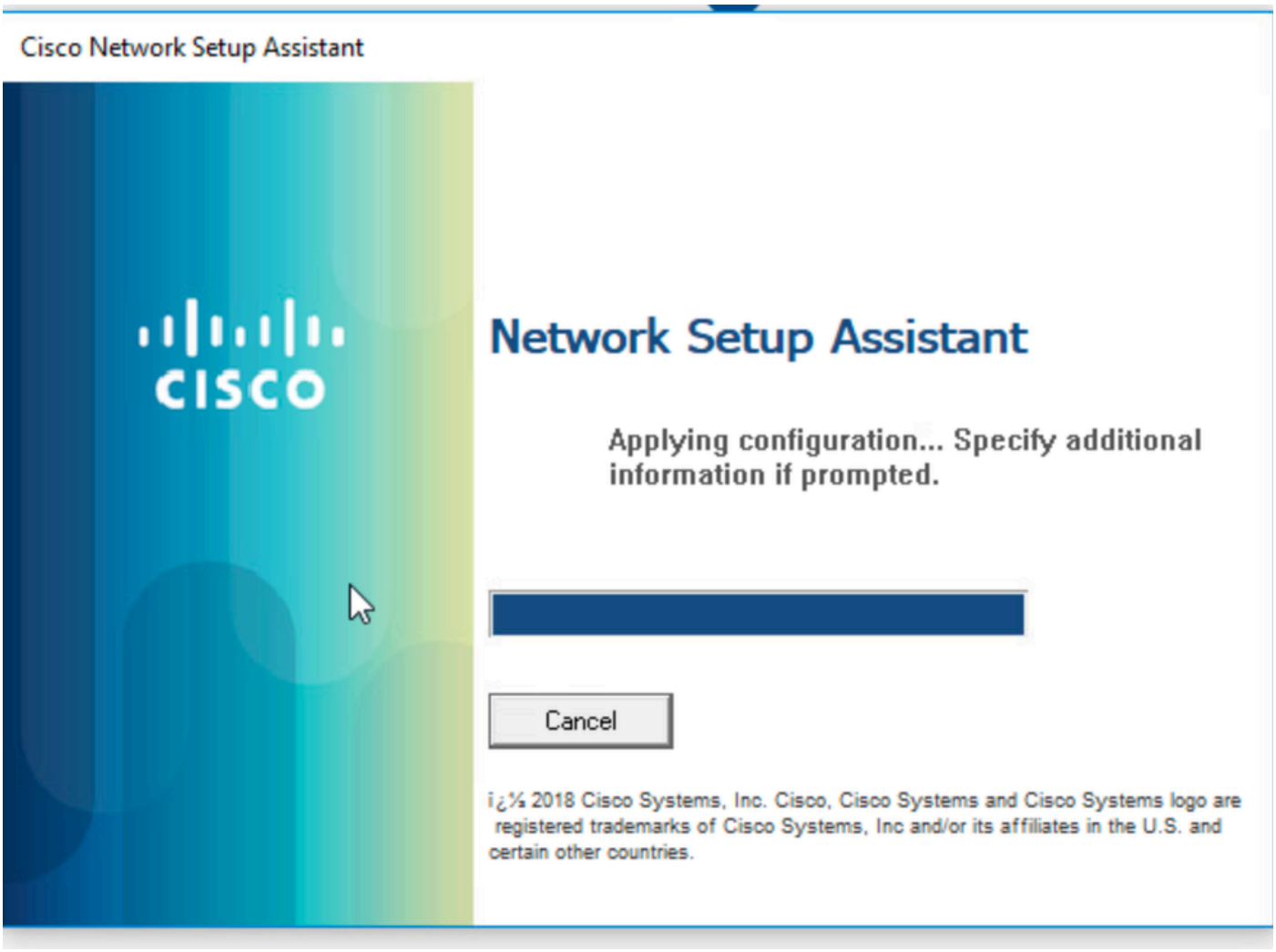


プロファイルがEAP-TLS認証を実行するように設定されている場合、認証のためにエンドポイントプロファイルとEAP TLS証明書をダウンロードするためのNetwork Assistantツールをダウンロードするようにユーザに要求することを示す投稿。



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。


Cisco Network Setup Assistant
Network Setup Assistant
This application automatically configures network settings.
Start
Quit
i¿¼ 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 -:000000000000000B30D59CC5:::-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 -:000000000000000B30D59CC5::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 -:000000000000000B30D59CC5::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 -:000000000000000B30D59CC5::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 -:000000000000000B30D59CC5::::- 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 -:000000000000000B30D59CC5::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 -:000000000000000B30D59CC5::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 -:000000000000000B30D59CC5::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 -:000000000000000B30D59CC5::::- 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 -:000000000000000B30D59CC5::::- 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 -:000000000000000B30D59CC5::::- 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 -:000000000000000B30D59CC5:::- 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

Ise-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=322815127387689606282525327846633020 89]'
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=686276201605863086858498187751006982 24]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][]
org.jscep.client.CertStoreInspector -::::- 4. '[issuer=CN=Certificate Services Node CA - iseguest; serial=729347676986030971539324822275488749 53]'
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]

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。