Cisco ISE 2.7 Admin Guide: Integration

Integration

What Is Wireless Setup

Wireless Setup provides an easy way to set up wireless flows for 802.1x, guest, and BYOD. It also provides workflows to configure and customize each portal for guest and BYOD, where appropriate. These workflows are much simpler than configuring the associated portal flow in ISE by providing the most common recommended settings. Wireless Setup does many steps for you that you would have to do yourself in ISE, and on the WLC, so you can quickly create a working environment.

You can use the Wireless Setup created environment to test and develop your flows. Once you get your Wireless Setup environment working, you may want to switch to ISE, so you can support more advanced configurations. For more information about configuring Guest in ISE, see the ISE Administrators Guide for your version of ISE, and the Cisco Community Site https://community.cisco.com/t5/security-documents/ise-guest-amp-web-authentication/ta-p/3657224 . For more information about configuring and using Wireless Setup for ISE, see https://community.cisco.com/t5/security-documents/cisco-ise-secure-access-wizard-saw-guest-byod-and-secure-access/ta-p/3636602.

Note ISE Wireless Setup is beta software - please do not use Wireless Setup in production networks.

- **Wireless Setup is disabled** by default after fresh installation of Cisco ISE. You can enable Wireless Setup from the ISE CLI with the **application configure ise** command (select option 17) or by using the Wireless Setup option in the ISE GUI Home page.
- Wireless Setup does not work if you upgrade ISE from a previous version. Wireless Setup is supported only for new ISE installations.
- Wireless Setup works only on a Standalone node.
- Run only one instance of Wireless Setup at a time; only one person can run Wireless Setup at a time.
- Wireless Setup requires ports 9103 and 9104 to be open. To close those ports, use the CLI to disable Wireless Setup.
- If you would like to start a fresh installation of Wireless Setup after running some flows, you can use the CLI command **application reset-config ise**. This command resets the ISE configuration and clears the ISE database, but keeps the network definitions. So you can reset ISE and Wireless Setup, without having to reinstall ISE and running setup.

  If you would like to start over with Wireless Setup, you can reset both ISE and Wireless Setup's configuration with the following steps:

  - In the CLI, run **application reset-config** to reset all ISE configuration. If you were testing Wireless Setup on a fresh installation, this command removes the configurations done by Wireless Setup in ISE.

- In the CLI, run **application configure ise**, and choose **[18]Reset Config Wi-Fi Setup**. This cleans the Wireless Setup configuration database.
- On the WLC, remove the configurations added by Wireless Setup on the WLC. For information about what Wireless Setup configures on the WLC, see Changes to ISE and WLC by Wireless Setup, on page 10.

You can avoid these steps by taking a snapshot of the VM after you finish a fresh installation of ISE.

For more information about the CLI, see the Cisco Identity Services Engine CLI Reference Guide for your version of ISE.

- You must be an ISE Super Admin user to use Wireless Setup.
- Wireless Setup requires at least two CPU cores and 8 GB or memory.
- Only Active Directory groups and users are supported. After you have created one or more flows in Wireless Configuration, other types of users, groups, and authorizations are available for Wireless Setup, but they must be configured on ISE.
- If you already defined Active Directory in ISE, and you plan to use this AD for Wireless Setup, then:
  - The join name and domain name must be the same. If the names are not the same, then make them the same in ISE before using that AD in Wireless Setup.
  - If your WLC is already configured on ISE, the WLC must have a shared secret configured. If the WLC definition does not have the shared secret, then either add the shared secret, or delete the WLC from ISE, before configuring that WLC in Wireless Setup.
- Wireless Setup can configure ISE components, but it can't delete or modify them after a flow has been started. For a list of all the things that Wireless Setup configures in ISE, see Cisco Identity Services Engine CLI Reference Guide for your version of ISE.
- When you start a flow, you must complete the flow. Clicking a breadcrumb in the flow stops the flow. As you step through a flow, changes are made to the ISE configuration dynamically. Wireless Setup provides a list of configuration changes, so you can manually revert. You can't back up in a flow to make extra changes, with one exception. You can go back to change Guest or BYOD portal customization.
- Multiple WLCs and Active Directory domains are supported, but each flow can only support one WLC and one Active Directory.
- Wireless Setup requires an ISE Basic license to operate. BYOD requires a Plus license.
- If you have configured ISE resources before configuring Wireless Setup, Wireless Setup may have conflicts with an existing policy. If this happens, Wireless Setup advises you to review the authorization policy after running through the tool. We recommended that you start with a clean setup of ISE when running Wireless Setup. Support for a mixed configuration of Wireless Setup and ISE is limited.
- Wireless Setup is available in English, but not other languages. If you want to use other languages with your portal, configure that in ISE after running Wireless Setup.
- Dual SSID is supported for BYOD. The Open SSID used in this configuration does not support guest access, due to conflicts. If you need a portal that supports both guest and BYOD, you cannot use Wireless Setup, and is out of the scope of this document.
- **Email and SMS Notifications**

- For self-registered guests, SMS and email notification is supported. These notifications are configured in the portal customization notification section. You must configure an SMTP server to support SMS and email notifications. The cellular providers built in to ISE, which include AT&T, T Mobile, Sprint, Orange and Verizon, are pre-configured, and are free email to SMS gateways.
- A guest chooses their cell provider in the portal. If their provider is not in the list, then they can't receive a message. You can also configure a global provider, but that is outside of the scope of this guide. If the guest portal is configured for SMS and email notification, then they must enter values for both those services.
- The Sponsored guest flow does not provide configuration for SMS or email notification in Wireless Setup. For that flow, you must configure notification services in ISE.
- Do not select the SMS provider *Global Default* when configuring notifications for a portal. This provider is not configured (by default).

- Wireless setup only supports a standalone setup without HA. If you decide to use extra PSNs for authentication, then add the ISE IP address of those PSNs to your WLC's RADIUS configuration.

Wireless Setup Support for Apple Mini-Browser (Captive Network Assistant)

- **Guest Flows**—Auto popup of the Apple pseudo browser works with all Guest Flows. A guest may go through the flow using Apple's Captive Network Assistant browser. When an Apple user connects to the OPEN network, the minibrowser pops-up automatically, which allows them to accept an AUP (hotspot), or to go through self-registration or login with their credentials.
- **BYOD**
  - **Single SSID**—ISE 2.2 added support for the apple minibrowser. However, to limit potential problems with SSID flows on Apple devices, we suppressed the minibrowser by adding captive.apple.com to the redirection ACL. This causes the Apple device to think it has access to the Internet. The user must manually launch Safari to be redirected to the portal for web authentication or device onboarding.
  - **Dual SSID**—For Dual SSID flow that starts with an initial OPEN network WLAN to start guest access, or to allow your employees to go through Device Onboarding (BYOD), and redirects to a secured SSID, the minibrowser is also suppressed.

For more information about the Apple CAN minibrowser, see https://communities.cisco.com/docs/DOC-71122.

Configuring WLCs in Wireless Network

When you first log on to Wireless Setup and select a flow, you are asked to configure a wireless controller. Wireless Setup pushes the necessary settings to the WLC to support the type of flow you are configuring.

- The WLC must be a Cisco WLC running AireOS 8.x or higher.
- vWLC doesn't support DNS based ACLs
- Configure your WLC for the interface VLANS (networks) that you plan to use in your Wireless Setup deployment. By default, the WLC has a management interface, but we recommend that you configure other interfaces for your guest and secure access (employee) networks.

- For Guest flow, an ACL_WEBAUTH_REDIRECT ACL is used to redirect guest devices to either a Hotspot or Credentialed Portal to acceptance of an AUP (hotspot), to log in, or to create credentials. After the Guest is authorized, they are permitted access (ACCESS-ACCEPT). You can use ACLs on the WLC to restrict guest permissions: create an ACL on the WLC, and use that ACL in your guest permission authz profile. To allow access to the ISE success page, add this ACL to the WLC. For more information about creating restrictive ACLs, see https://communities.cisco.com/docs/DOC-68169.
- Wireless Setup configures a WLAN for each flow. Once you have configured a WLAN for a flow, that WLAN is not available for any other flow. The only exception to this is if you configured a WLAN for self-registration flow, and later you decided to use this WLAN for a Sponsored Guest Flow, which handles both self-registration and sponsoring of guests.

  If you run Wireless Setup in a production environment, your configurations may disconnect some existing users.
- If you configure a flow in Wireless Setup with a WLC, do not remove that WLC in ISE.
- If you have already configured a WLC in ISE, but you didn't configure a shared secret in the RADIUS Options, then you must add a shared secret before using that WLC in Wireless Setup.
- If you already configured a WLC in ISE, and you configured a shared secret, then don't configure a different shared secret with Wireless Setup. The Wireless Setup and the ISE secret passwords must match. The WLAN that you select is disabled throughout the flow, but it can be re-enabled at the end of the flow by clicking the **Go Live** button.
- **Remote LAN**—If your network has a remote LAN, Wireless Setup fails when it tries to use a VLAN ID that is already assigned to your remote LAN. To work around this, either remove the remote LAN, or create the VLANs that you plan to use on the WLC before you run Wireless Setup. In Wireless Setup, you can enable those existing VLANs for flows.
- **FlexConnect**—Flexconnect Local Switch and Flexconnect ACLs are configured by Wireless Setup, but they are not used or supported. Wireless Setup only works with Flexconnect Centralized or Local Mode Aps and SSIDs.

Example of Wireless Configuration

The following extraction from a WLC log shows an example of the configuration that Wireless Setup does when you configure a flow.

```
"config radius auth add 1 192.168.201.228 1812 ascii cisco"
"config radius auth disable 1"
"config radius auth rfc3576 enable 1"
"config radius auth management 1 disable"
"config radius auth enable 1"
"config radius acct add 1 192.168.201.228 1813 ascii cisco"
"config radius acct enable 1"
"config acl create ACL_WEBAUTH_REDIRECT"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
```

```
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl apply ACL_WEBAUTH_REDIRECT"
"show flexconnect acl summary"
"config flexconnect acl create ACL_WEBAUTH_REDIRECT"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config flexconnect acl apply ACL_WEBAUTH_REDIRECT"
```

Active Directory with Wireless Setup

An Active Directory Domain is required to create Sponsored Guest, 802.1x, and BYOD flows. Active Directory identifies users for the sponsor groups to access the Sponsor portal, 802.1x Secure Access and associated VLANs, and BYOD and device on boarding. After configuring any of these flows in Wireless Setup, you can optionally go into ISE Identities and add:

- A internal sponsor account mapped to sponsor group, such as ALL_ACCOUNTS. This is not required if you are using Active Directory.
- An employee who is part of the ISE internal employee group. Make sure that the internal Employee group is added to your Authorization Policy and ISE internal employee group.

Guest Portals in Wireless Setup

When people visiting your company wish to use your company's network to access the internet, or resources and services on your network, you can provide them network access through a Guest portal. Employees can use these Guest portals to access your company's network, if configured.

There are three default Guest portals:

- Hotspot Guest portal—Network access is granted without requiring any credentials. Usually, an Acceptance of User Policy (AUP) must be accepted before network access is granted.

  Requiring an access code logon is supported by Wireless Setup for the Hotspot and Self-Registration portals.
- Sponsored-Guest portal—Network access is granted by a sponsor who creates accounts for guests, and provides the Guest with login credentials.
- Self-Registered Guest portal—Guests can create their own accounts credentials, and may need sponsor approval before they are granted network access.

Cisco ISE can host multiple Guest portals, including a predefined set of default portals.

Guest Portal Workflow

1. After you choose the type of portal, you are asked which controller to use. Configure a new wireless network for each flow. You can choose an existing WLAN that you haven't already used in Wireless Setup, or create a new one.

   Flows that require redirection have the option of redirecting the user to an Originating URL, success page, or specific URL (for example, www.cisco.com). Originating URL requires support from the WLC.

Note Originating URL is not supported until WLC version 8.4 is release.

2. Customize the appearance and change the basic settings of the portal.
3. When you're done with customization, follow the URL link to the test portal. The test portal shows you a preview of a test version of the portal. You can continue through the flow, and make more changes, if desired. Note, the only successful redirection that works to the Success Page. Original URL and Static URL do not work, since they require a wireless session to support the redirect. The test portal does not support RADIUS sessions, so you won't see the entire portal flow. If you have more than one PSN, ISE chooses the first active PSN.
4. Configuration is done. You can download and view the steps that Wireless Setup did for you in ISE and the WLC during the workflow.

Note Location is not used for basic guest access in Wireless Setup. Locations are required if you want to control access based on local time. For information about configuring time zones in ISE, see the section "SMS Providers and Services" in Chapter Guest and BYOD in *Cisco ISE Administrator Guide* .

Wireless Network Self-Registration Portal

A Self-Registered Guest portal enables guests to register themselves and create their own accounts so they can access the network.

We recommend that you do not choose logon success page, which displays logon credentials to the user on screen. The best practice is to require the user to get their credentials via email or SMS, which associates them with something unique for audit purposes.

Wireless Network Sponsored Guest Flow

Sponsors use the Sponsor portal to create and manage temporary accounts for authorized visitors to securely access the corporate network or the Internet. After creating a guest account, sponsors can also use the Sponsor portal to provide account details to the guest by printing, emailing, or texting. Before providing self-registering guests access to the company network, sponsors may be requested via email to approve their guests' accounts.

Wireless Setup configures a sponsor portal and a sponsored guest portal during the sponsored flow.

Approval flow it not supported with Wireless Setup.

You map Active Directory groups to your Sponsor Groups during the workflow. The workflow maps the AD Groups you select to the ALL_ACCOUNTS Sponsor group. It does not configure the GROUP or OWN account sponsor groups. Optionally, if you want to add other identity sources (such as internal or LDAP settings) you may do this in the ISE admin UI. For more information, see the Sponsor Groups section in the *Cisco ISE Admin Guide: Guest and BYOD* .

Wireless Setup BYOD Flow - For Native Supplicant and Certificate Provisioning

The Bring Your Own Device (BYOD) portal enables employees to register their personal devices. Native supplicant and certificate provisioning can be done before allowing access to the network. Employees do not access the BYOD portal directly, they are redirected to this portal when registering personal devices. The first time employees attempt to access the network using a personal device, they may be prompted to manually download (for non-iOS devices) and launch the Network Setup Assistant (NSA) wizard. The NSA guides them through registering and installing the native supplicant. After they have registered a device, they can use the My Devices portal to manage it.

Wireless Setup configures ISE and the controller for native supplicant and certificate provisioning. The user makes a PEAP connection to the controller, provides credentials, and the connection is switched to EAP-TLS (certificate).

The following devices are supported with Wireless Setup: Apple Devices (MAC and iOS), Windows Desktop OS (but not mobile), and Android. Chrome OS on boarding is not supported by Wireless Setup.

In the case of Android devices, ensure that the basic authentication access policy is enabled for single or dual EAP-TLS-based BYOD flows to be successful. Go to **Policy** > **Policy Sets** > **Default** > **Authorization Policy** and ensure that the **Basic_Authenticated_Access** rule is active.

Note Dual SSID flow consists of an open network for onboarding, and a TLS certificate-based secure network for authenticated access. A device can connect to the secure network without onboarding. This is because the basic_authenticated_access default rule allows any valid authentication to pass. When the device connects to the secure network, they don't match the BYOD secured authorization rule, the match falls to the bottom of the list to basic_authenticated_access.

The fix is to disable the Basic_Authenticated_Access rule under authorization policies, or edit the rule to match a specific SSID (WLAN). Both changes block PEAP connections to those that shouldn't allow it.

Note Wireless Setup does not have an authorization rule to redirect devices that are marked as lost. This is called blacklisting, which is managed by the blacklist portal. For information about managing lost and stolen devices, see http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.pdf.

BYOD Flow in Wireless Setup

BYOD Configuration in Wireless Setup consists of the following steps:

1. Choosing or Registering a wireless LAN controller
2. Adding a wireless network: For Dual SSID, this step runs twice.

Note A new ISE installation includes a default wireless network. With dual SSID BYOD, when the user is redirected to the second SSID, they will also see the default network SSID in their network profile. You can delete the default SSID, or tell your users to ignore it.

3. Choosing or joining an Active Directory (AD): You can override default VLAN settings for both the onboarding VLAN and the final access VLAN. The final access VLAN is mapped to the Active Directory groups.
4. Customizing your BYOD Portals: You can customize BYOD and My Devices Portal here. You can customize all the pages that ISE supports in this step. In this step, all the portal customization is submitted, policies are created and the profiles are linked to the respective policies.

Note My Devices portal uses the basic customization from BYOD portal customization; you cannot customize My Devices portal in Wireless Setup.

5. Preview the configuration changes made, and select Done.

For Dual SSID BYOD

Fast SSID must be enabled to support dual SSID BYOD. When Fast SSID changing is enabled, the wireless controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced. For more information about configuring Fast SSID on a Cisco WLC, see the Cisco Wireless Controller Configuration Guide.

Recommended WLC Timer Settings

We recommend setting the following timers on the WLC that you plan to use with Wireless Setup. The settings are shown in CLI.

```
config radius auth retransmit-timeout {SERVER_INDEX} 5
config radius aggressive-failover disable
config radius fallback-test mode passive
config wlan exclusionlist {WLAN ID} 180
config wlan exclusionlist {WLAN ID} enabled
```

802.1X Wireless Flow

Wireless Setup flow configures an 802.1x Wireless LAN controller with PEAP (username and password credentials).

Part of the flow asks you to specify an Active Directory (AD). You can map employee AD groups to a VLAN. You can configure different employee groups to different VLANs, if you want to separate your groups by VLAN. Click the drop-down next to **Access** to see the AD groups available in the AD you configured.

If you choose AD groups in Wireless Setup, each group is mapped to VLAN. If an AD group is not mapped to a VLAN, then the user matches the basic access policy, which allows any valid AD user to login.

Employee Connects to Network

1. **Employee Credentials Are Authenticated**—Cisco ISE authenticates the employee against the corporate Active Directory and provides an authorization policy.
2. **Device Is Redirected to the BYOD Portal**—The device is redirected to the BYOD portal. The device's MAC address field is populated, and the user can add a device name and description.
3. **Native Supplicant Is Configured (MacOS, Windows, iOS, Android)**—The native supplicant is configured; but the process varies by device:
   - MacOS and Windows devices—Employee clicks **Register** in the BYOD portal to download and install the supplicant provisioning wizard. The wizard configures the supplicant, and installs the certificate for EAP-TLS certificate-based authentication. The issued certificate is embedded with the device's MAC address and employee's username.

     

     Note For MacOS, except for Apple certificates, the certificate shows as "unsigned" on the Mac. This does not affect BYOD flow.

   - iOS devices—The Cisco ISE policy server sends a new profile using Apple's iOS over the air to the IOS device, which includes:
     - The issued certificate is stored with the IOS device's MAC address and employee's username.
     - A Wi-Fi supplicant profile that enforces the use of MSCHAPv2 or EAP-TLS for 802.1X authentication.
   - Android devices—Cisco ISE prompts and routes employee to download the Cisco Network Setup Assistant (NSA) from the Google Play store. After installing the app, the employee can open NSA and start the setup wizard. The startup wizard generates the supplicant configuration and issued certificate that is used, which is to configure the device.
   - **Change of Authorization Issued**—After the user goes through the on boarding flow, Cisco ISE initiates a Change of Authorization (CoA). This causes the MacOS X, Windows, and Android devices to reconnect to the secure 802.1X network using EAP-TLS. For single SSID, iOS devices also connect automatically, but for dual SSID, the wizard prompts iOS users to manually connect to the new network.

Native supplicants are supported for these operating systems:

- Android (excluding Amazon Kindle, B&N Nook)
- Mac OS X (for Apple Mac computers)
- Apple iOS devices (Apple iPod, iPhone, and iPad)
- Microsoft Windows 7, 8 (excluding RT), Vista, and 10

Changes to ISE and WLC by Wireless Setup

Wireless Setup configures ISE and the controller as you step through a flow. Wireless Setup lists the changes it made at the end of each flow. The changes for each flow are listed here as a reference to help you find all the changes that Wireless Setup made to ISE, to review or change them.

- **Hotspot**
  - **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Hotspot Portal**
  - **Work Centers** > **Guest Access** > **Policy Elements** > **Results** > **Authorization Profiles**
  - **Work Centers** > **Guest Access** > **Policy Sets**
- **Self-Registration**
  - **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Self-reg Portal**
  - **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Types** > **Guest Types**
  - **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**
  - **Work Centers** > **Guest Access** > **Policy Sets**
  - **Aministration** > **System** > **Settings** > **SMTP Server**
  - **Aministration** > **System** > **Settings** > **SMTP Gateway**
- **Sponsored**
  - **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Sponsored Guest Portal** >
  - **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > > **Sponsor Portal** >
  - **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**
  - **Work Centers** > **Guest Access** > **Authorization Policy**
  - **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor** > **Sponsor Groups**
  - **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Types** > **Guest Types**
  - **Work Centers** > **Guest Access** > **Ext ID Sources** > **Active Directory**
- **BYOD**
  - **Work Centers** > **BYOD** > **Portals & Components** > **BYOD Portals** > **BYOD Portal**
  - **Work Centers** > **BYOD** > **Portals & Components** > **My Devices Portals** > **My Devices Portal**
  - **Work Centers** > **BYOD** > **Policy Elements** > **Authorization** > **Authorization Profiles**
  - **Work Centers** > **BYOD** > **Authorization Policy**
  - **Work Centers** > **BYOD** > **Ext ID Sources** > **Active Directory**

- **Work Centers** > **BYOD** > **Ext ID Sources** > **Active Directory**, then select your AD, then the **Groups** tab.

- **Secure Access**
  - **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**
  - **Policy** > **Policy Sets**
  - **Work Centers** > **Guest Access** > **Ext ID Sources** > **Active Directory**, then select your AD, then the **Groups** tab.

- **Wireless LAN Controller**
  - **WLANs**
  - **Security** > **Access Control Lists**—Wireless Setup creates the following ACL:
    - Redirect ACL for guest and BYOD
  - Wireless setup also creates entries under **Security** > **AAA** > **Authentication and Accounting**

Enable Your Switch to Support Standard Web Authentication

Ensure that you include the following commands in your switch configuration to enable standard Web Authenticating functions for Cisco ISE, including provisions for URL redirection upon authentication:

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

Local Username and Password Definition for Synthetic RADIUS Transactions

Enter the following command to enable the switch to talk to the Cisco ISE node as though it is the RADIUS server for this network segment:

```
username test-radius password 0 abcde123
```

NTP Server Configuration to Ensure Accurate Log and Accounting Timestamps

Ensure that you specify the same NTP server as you have set in Cisco ISE at **Administration** > **System** > **Settings** > **System Time** by entering the following command:

ntp server *<IP_address>|<domain_name>*

Command to Enable AAA Functions

Enter the following commands to enable the various AAA functions between the switch and Cisco ISE, including 802.1X and MAB authentication functions:

```
aaa new-model

! Creates an 802.1X port-based authentication method list

aaa authentication dot1x default group radius

! Required for VLAN/ACL assignment

aaa authorization network default group radius

! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius

! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius

!

aaa session-id common

!

aaa accounting update periodic 5


! Update AAA accounting information periodically every 5 minutes


aaa accounting system default start-stop group radius

!
```

RADIUS Server Configuration on the Switch

Configure the switch to interoperate with Cisco ISE acting as the RADIUS source server by entering the following commands:

```
!
radius-server attribute 6 on-for-login-auth

! Include RADIUS attribute 8 in every Access-Request

radius-server attribute 8 include-in-access-req

! Include RADIUS attribute 25 in every Access-Request

radius-server attribute 25 access-request include

! Wait 3 x 30 seconds before marking RADIUS server as dead

radius-server dead-criteria time 30 tries 3


! Use RFC-standard ports (1812/1813)
radius-server host <Cisco_ISE_IP_address> auth-port 1812 acct-port 1813 test
username test-radius key 0 <RADIUS-KEY>

!
radius-server vsa send accounting
!
radius-server vsa send authentication
!
! send RADIUS requests from the MANAGEMENT VLAN

ip radius source-interface <VLAN_number>
```

Note We recommend that you configure a dead-criteria time of 30 seconds with 3 retries to provide longer response times for RADIUS requests that use Active Directory for authentication.

Configure the Switch to Send RADIUS Accounting Start/Stop to Inline Posture Nodes

The network access device should be configured to send RADIUS accounting "Start" and "Stop" messages at the beginning and end of a session, respectively, with the remote device's IP address in those messages to the Inline Posture nodes. The Inline Posture node associates the device IP address to any relevant authorization profiles downloaded over the life of a session. For example, a remote device may have an "unknown-compliance-state" authorization profile at initial login, then switch to a "compliant" authorization profile following CoA (assuming successful device posture assessment).

Command to Enable RADIUS Change of Authorization (CoA)

Specify the settings to ensure the switch is able to appropriately handle RADIUS Change of Authorization behavior supporting Posture functions from Cisco ISE by entering the following commands:

```
aaa server radius dynamic-author

client <ISE-IP> server-key 0 abcde123
```

Note

- Cisco ISE uses port 1700 (Cisco IOS software default) versus RFC default port 3799 for CoA. Existing Cisco Secure ACS 5.x customers may already have this set to port 3799 if they are using CoA as part of an existing ACS implementation.
- Shared secret key should be the same as the one configured on Cisco ISE while adding a network device and the IP address should be a PSN IP address.

Command to Enable Device Tracking and DHCP Snooping

To help provide optional security-oriented functions from Cisco ISE, you can enable device tracking and DHCP snooping for IP substitution in dynamic ACLs on switch ports by entering the following commands:

```
! Optional

ip dhcp snooping

! Required!

! Configure Device Tracking Policy!
device-tracking policy <DT_POLICY_NAME>
no protocol ndp
tracking enable

! Bind it to interface!
interface <interface_id>
device-tracking attach-policy<DT_POLICY_NAME>
```

In RADIUS Accounting, the DHCP attributes are not sent by IOS sensor to Cisco ISE even when dhcp snooping is enabled. In such cases, the dhcp snooping should be enabled on the VLAN to make the DHCP active.

Use the following commands to enable dhcp snooping on VLAN:

```
ip dhcp snooping

ip dhcp snooping vlan 1-100
```

(VLAN range should include used for data and vlan)

Command to Enable 802.1X Port-Based Authentication

Enter the following commands to turn 802.1X authentication on for switch ports, globally:

```
dot1x system-auth-control
```

Command to Enable EAP for Critical Authentications

To support supplicant authentication requests over the LAN, enable EAP for critical authentications (Inaccessible Authentication Bypass) by entering the following command:

```
dot1x critical eapol
```

Command to Throttle AAA Requests Using Recovery Delay

When a critical authentication recovery event takes place, you can configure the switch to automatically introduce a delay (in seconds) to ensure Cisco ISE is able to launch services again following recovery by entering the following command:

```
authentication critical recovery delay 1000
```

VLAN Definitions Based on Enforcement States

Enter the following commands to define the VLAN names, numbers, and SVIs based on known enforcement states in your network. Create the respective VLAN interfaces to enable routing between networks. This can be especially helpful to handle multiple sources of traffic passing over the same network segments—traffic from both PCs and the IP phone through which the PC is connected to the network, for example.

Note The first IP helper goes to the DHCP server and the second IP helper sends a copy of the DHCP request to the inline posture node for profiling.

```
vlan <VLAN_number>

name ACCESS!

vlan <VLAN_number>

name VOICE

!

interface <VLAN_number>

description ACCESS

ip address 10.1.2.3 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

ip helper-address <Cisco_ISE_IP_address>

!

interface <VLAN_number>

description VOICE
```

```
ip address 10.2.3.4 255.255.255.0

ip helper-address <DHCP_Server_IP_address>
```

Local (Default) ACLs Definition on the Switch

Enable these functions on older switches (with Cisco IOS software releases earlier than 12.2(55)SE) to ensure Cisco ISE is able to perform the dynamic ACL updates required for authentication and authorization by entering the following commands:

```
ip access-list extended ACL-ALLOW

 permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain

  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal

permit tcp any host <Cisco_ISE_IP_address> eq www


permit tcp any host <Cisco_ISE_IP_address> eq 443


permit tcp any host <Cisco_ISE_IP_address> eq 8443
```

```
permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest
  deny ip any any log
!
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
```

Note This configuration on the WLC my increase CPU utilization and raises the risk of system instability. This is an IOS issue and does not adversely affect Cisco ISE.

Enable Switch Ports for 802.1X and MAB

To enable switch ports for 802.1X and MAB:

Procedure

Step 1 Enter configuration mode for all of the access switch ports:

interface range FastEthernet0/1-8

Step 2 Enable the switch ports for access mode (instead of trunk mode):

switchport mode access

Step 3 Statically configure the access VLAN. This provides local provisioning the access VLANs and is required for open-mode authentication:

switchport access vlan <*VLAN_number*>

Step 4 Statically configure the voice VLAN:

switchport voice vlan <*VLAN_number*>

Step 5 Enable open-mode authentication. Open-mode allows traffic to be bridged onto the data and voice VLANs before authentication is completed. We strongly recommend using a port-based ACL in a production environment to prevent unauthorized access.

! Enables pre-auth access before AAA response; subject to port ACL

authentication open

Step 6 Apply a port-based ACL to determine which traffic should be bridged by default from unauthenticated endpoints onto the access VLAN. Because you should allow all access first and enforce policy later, you should apply ACL-ALLOW to permit all traffic through the switch port. You have already created a default ISE authorization to allow all traffic for now because we want complete visibility and do not want to impact the existing end-user experience yet.

! An ACL must be configured to prepend dACLs from AAA server.

ip access-group ACL-ALLOW in

Note Prior to Cisco IOS software Release 12.2(55)SE on DSBU switches, a port ACL is required for dynamic ACLs from a RADIUS AAA server to be applied. Failure to have a default ACL will result in assigned dACLs being ignored by the switch. With Cisco IOS software Release12.2(55)SE, a default ACL will be automatically generated and applied.

Note We are using ACL-ALLOW at this point in the lab because we want to enable 802.1X port-based authentication, but without any impact to the existing network. In a later exercise, we will apply a different ACL-DEFAULT, which blocks undesired traffic for a production environment.

Step 7 Enable Multi-Auth host mode. Multi-Auth is essentially a superset of Multi-Domain Authentication (MDA). MDA only allows a single endpoint in the data domain. When multi-auth is configured, a single authenticated phone is allowed in the voice domain (as with MDA) but an unlimited number of data devices can be authenticated in the data domain.

! Allow voice + multiple endpoints on same physical access port

authentication host-mode multi-auth

Note Multiple data devices (whether virtualized devices or physical devices connected to a hub) behind an IP phone can exacerbate the access ports' physical link-state awareness.

Step 8 Enable various authentication method options:

! Enable re-authentication

authentication periodic

! Enable re-authentication via RADIUS Session-Timeout

authentication timer reauthenticate server

authentication event fail action next-method

! Configure Critical authentication vlan method in case of dead server

authentication event server dead action reinitialize vlan *<VLAN_number>*
authentication event server alive action reinitialize
! IOS Flex-Auth authentication 802.1X and MAB
authentication order dot1x mab
authentication priority dot1x mab

Step 9 Enable 802.1X port control on the switchport:
! Enables port-based authentication on the interface
authentication port-control auto
authentication violation restrict

Step 10 Enable MAC Authentication Bypass (MAB):
! Enable MAC Authentication Bypass (MAB)
mab

Step 11 Enable 802.1X on the switchport
! Enables 802.1X authentication on the interface
dot1x pae authenticator

Step 12 Set the retransmit period to 10 seconds:
dot1x timeout tx-period *10*

Note The dot1x tx-period timeout should be set to 10 seconds. Do not change this unless you understand the implications.

Step 13 Enable the portfast feature:
spanning-tree portfast

Command to Enable EPM Logging

Set up standard logging functions on the switch to support possible troubleshooting/recording for Cisco ISE functions:

```
epm logging
```

Command to Enable SNMP Traps

Ensure the switch is able to receive SNMP trap transmissions from Cisco ISE over the appropriate VLAN in this network segment:

```
snmp-server community public RO
```

```
snmp-server trap-source <VLAN_number>
```

Command to Enable SNMP v3 Query for Profiling

Configure the switch to ensure SNMP v3 polling takes place as intended to support Cisco ISE profiling services. First, configure the SNMP settings in Cisco ISE by choosing **Administration** > **Network Resources** > **Network Devices** > **Add | Edit** > **SNMP Settings**.

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>

snmp-server group  <group> v3 priv

snmp-server group <group> v3 priv context vlan-1
```

Note The **snmp-server group** *<group>* **v3 priv context** *vlan-1* command must be configured for each context. The **snmp show context** command lists all the context information.

If the SNMP Request times out and there is no connectivity issue, then you can increase the Timeout value.

Command to Enable MAC Notification Traps for Profiler to Collect

Configure your switch to transmit the appropriate MAC notification traps so that the Cisco ISE Profiler function is able to collect information on network endpoints:

```
mac address-table notification change

mac address-table notification mac-move

snmp trap mac-notification change added

snmp trap mac-notification change removed
```

RADIUS Idle-Timeout Configuration on the Switch

To configure the RADIUS Idle-timeout on a switch, use the following command:

```
Switch(config-if)# authentication timer inactivity
```

where *inactivity* is interval of inactivity in seconds, after which client activity is considered unauthorized.

In Cisco ISE, you can enable this option for any Authorization Policies to which such a session inactivity timer should apply from **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Wireless LAN Controller Configuration for iOS Supplicant Provisioning

For Single SSID

To support Apple iOS-based devices (iPhone/iPad) switching from one SSID to another on the same wireless access point, configure the Wireless LAN Controller (WLC) to enable the "FAST SSID change" function. This function helps ensure iOS-based devices are able to more quickly switch between SSIDs.

For Dual SSID BYOD

Fast SSID must be enabled to support dual SSID BYOD. When Fast SSID changing is enabled, the wireless controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced. For more information about configuring Fast SSID on a Cisco WLC, see the Cisco Wireless Controller Configuration Guide.

Example WLC Configuration

```
WLC (config)# FAST SSID change
```

You might see the following error message while trying to connect to a wireless network for some of the Apple iOS-based devices:

```
Could not scan for Wireless Networks.
```

You can ignore this error message because this does not affect the authentication of the device.

Configuring ACLs on the Wireless LAN Controller for MDM Interoperability

You must configure ACLs on the wireless LAN controller for use in authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs should be in the following sequence.

Procedure

Step 1 Allow all outbound traffic from server to client.

Step 2 (Optional) Allow ICMP inbound traffic from client to server for troubleshooting.

Step 3 Allow access to MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.

Step 4 Allow all inbound traffic from client to server to ISE for Web Portal and supplicant, and certificate provisioning flows.

Step 5 Allow inbound DNS traffic from client to server for name resolution.

Step 6 Allow inbound DHCP traffic from client to server for IP addresses.

Step 7 Deny all inbound traffic from client to server to corporate resources for redirection to ISE (as per your company policy).

Step 8 (Optional) Permit the rest of the traffic.

Example

The following example shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE ip address is 10.35.50.165, the internal corporate network ip address is 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

Figure 1: ACLs for Redirecting Nonregistered Device

General

Access List Name: NSP-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819