What Is Wireless Setup

Wireless Setup provides an easy way to set up wireless flows for 802.1X, Guest and BYOD services. It also provides workflows to configure and customize each portal for Guest and BYOD services, where appropriate. These workflows are much simpler than configuring the associated portal flow in Cisco ISE by providing the most common recommended settings. Wireless Setup does many steps for you that you would have to do yourself in Cisco ISE, and on the Wireless Controller, 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 Cisco ISE, so you can support advanced configurations. For more information about configuring Guest services in Cisco ISE, see the ISE Administrators Guide for your version of Cisco 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 Cisco ISE, see https://community.cisco.com/t5/security-documents/cisco-ise-secure-access-wizard-saw-guest-byod-and-secure-access/ta-p/3636602.

Note Cisco 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 Cisco ISE CLI with the **application configure ise** command (select option 17) or by using the **Wireless Setup** option ( ) available in the top right-hand corner in the Cisco ISE GUI home page.
- Run only one instance of Wireless Setup at a time. Only one person can run Wireless Setup at a time.
- If you upgrade Cisco ISE from a previous version, the Wireless Setup menu does not appear. This is because Wireless Setup is only supported for new Cisco ISE installations. You can enable Wireless Setup in the Cisco ISE CLI with the command **application configure ise**, picking the option to enable Wireless Setup.
- Wireless Setup requires ports 9103 and 9104 to be open. To close these 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 Cisco ISE configuration and clears the Cisco ISE database, but keeps the network definitions. So you can reset Cisco ISE and Wireless Setup, without having to reinstall Cisco ISE and running setup.

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

- In the CLI, run **application reset-config** to reset all Cisco ISE configuration. If you were testing Wireless Setup on a fresh installation, this command removes the configurations done by Wireless Setup in Cisco 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 Wireless Controller, remove the configurations added by Wireless Setup on the Wireless Controller. For information about what Wireless Setup configures on the Wireless Controller, see Changes on Cisco ISE and Wireless Controller by the Wireless Setup flow, on page 10.

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

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

- You must be a Cisco ISE Super Admin user to use Wireless Setup.
- Wireless Setup requires at least two CPU cores and 8 GB of memory.
- Only Active Directory (AD) groups and users are supported. After you have created one or more flows in Wireless Setup, 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 Cisco 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 Cisoc ISE before using that AD in Wireless Setup.
  - If your Wireless Controller is already configured on Cisco ISE, the Wireless Controller must have a shared secret configured. If the Wireless Controller definition does not have the shared secret, then either add the shared secret, or delete the Wireless Controller from Cisco ISE, before configuring that Wireless Controller in Wireless Setup.
- Wireless Setup can configure Cisco 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 Cisco ISE, see Cisco Identity Services Engine CLI Reference Guide for your version of Cisco 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 Cisco 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 Wireless Controllers and Active Directory domains are supported, but each flow can only support one Wireless Controller and one Active Directory.
- Wireless Setup requires a Cisco ISE Basic license to operate. BYOD requires a Cisco ISE Plus license.
- We recommend that you run Wireless Setup in a standalone setup, with optionally a second node. For more information about what defines a standalone setup, see the Cisco Identity Services Engine Installation Guide for your version of Cisco ISE.
- If you have configured Cisco 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 Ciisco ISE when running Wireless Setup. Support for a mixed configuration of Wireless Setup and Cisco 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 Cisco 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 Cisco ISE, which include AT&T, T Mobile, Sprint, Orange and Verizon, are pre-configured, and are free to email to the 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 Cisco 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 Cisco ISE IP address of those PSNs to your Wireless Controller'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**: Cisco ISE Release 2.2 added support for the Apple minibrowser. However, to limit potential problems with the 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 the Safari browser 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.

- Configure Wireless Controllers in the Wireless Network, on page 4

Configure Wireless Controllers in the Wireless Network

When you first launch Wireless Setup and select a flow, you are asked to configure a Wireless Controller. Wireless Setup pushes the necessary settings to the Wireless Controller to support the type of flow you are configuring.

- The Wireless Controller must be a Cisco Wireless Controller running AireOS 8.x or higher.
- Virtual Wireless Controller doesn’t support DNS based ACLs.
- Configure your Wireless Controller for the interface VLANS (networks) that you plan to use in your Wireless Setup deployment. By default, the Wireless Controller has a management interface, but we recommend that you configure other interfaces for your guest and secure access (employee) networks.
- For the 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 Wireless Controller to restrict guest permissions. To do so, create an ACL on the Wireless Controller, and use that ACL in your guest permission authorization profile. To allow access to the Cisco ISE success page, add this ACL to the Wireless Controller. 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 Wireless Controller, do not remove that Wireless Controller in Cisco ISE.
- If you have already configured a Wireless Controller in Cisco ISE, but you didn't configure a shared secret in the RADIUS Options, then you must add a shared secret before using that Wireless Controller in Wireless Setup.
- If you already configured a Wireless Controller in Cisco ISE, and you configured a shared secret, then don't configure a different shared secret with Wireless Setup. The Wireless Setup and the Cisco 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 Wireless Controller 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 Access Points and SSIDs.

Example of Wireless Configuration

The following extraction from a Wireless Controller 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 onboarding. After configuring any of these flows in Wireless Setup, you can optionally go into Cisco ISE Identities and add:

- An internal sponsor account mapped to a sponsor group, such as ALL_ACCOUNTS. This is not required if you are using Active Directory.
- An employee who is part of the Cisco ISE internal employee group. Make sure that the internal employee group is added to your authorization policy.

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.
- 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 account 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.

The default portal themes have standard Cisco branding that you can customize through the Admin portal.

Wireless Setup has its own default theme (CSS) and you are able to modify some basic settings such as logo, banner, background image, coloring and fonts. In Cisco ISE, you can also choose to further customize your portal by changing more settings and going into advanced customizations.

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 Wireless Controller.

Note Originating URL is not supported until Wireless Controller version 8.4.

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 is for the success page. The originating URL and static URL do not work in the test portal, 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, Cisco ISE chooses the first active PSN.

4. The configuration is complete. You can download and view the steps that Wireless Setup did for you in Cisco ISE and the Wireless Controller 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 Cisco ISE, see SMS Providers and Services.

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 the logon success page, which displays logon credentials to the user on the screen. The best practice is to get the user 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-registration guest 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 Cisco ISE admin UI. For more information, see Sponsor Groups.

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 Cisco 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 onboarding 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 the **Basic_Authenticated_Access** rule.

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 has an authorization rule to redirect devices that are marked as lost. This is done through by blocking the devices, 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. Choose or register a wireless LAN controller.
2. Add a wireless network.

Note A new Cisco 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. Choose or join Cisco ISE to 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. Customize your BYOD Portals: You can customize BYOD and My Devices Portal here. You can customize all the pages that Cisco 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 The My Devices portal uses basic customization from BYOD portal customization. You cannot customize the My Devices portal in Wireless Setup.

5. Preview the configuration changes made, and click **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 Wireless Controller, see the Cisco Wireless Controller Configuration Guide.

Recommended WLC Timer Settings

We recommend setting the following commands on the Wireless Controller that you plan to use in the Wireless Setup.

```
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 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 a 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 MacOS. 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 onboarding flow, Cisco ISE initiates a Change of Authorization (CoA). This causes the MacOSX, 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)
- MacOS (for Apple Mac computers)
- Apple iOS devices (Apple iPod, iPhone, and iPad)
- Microsoft Windows 7, 8 (excluding RT), Vista, and 10

Changes on Cisco ISE and Wireless Controller by the Wireless Setup flow

Wireless Setup configures Cisco 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 Cisco 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** > **Authorization Policy**
- **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** > **Authorization Policy**
- **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** > **Authorization** > **Authorization Policy**
  - **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**