# Support Device Access

## Personal Devices on a Corporate Network

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.

Guests can automatically register their devices when logging in to Guest portals. They can also register additional devices up to the maximum limit that you define for their guest type. These devices are registered into endpoint identity groups based on the type of portal used by the guest. For Hotspot Guest portals, the selected endpoint identity group is used, and for credentialed Guest portals, the endpoint identity group is defined by the guest type of the guest.

Users can also add their personal devices to the network using native supplicant provisioning (Bring Your Own Device [BYOD]) or the My Devices portal. You can create native supplicant profiles so that when a user logs in, based on the profile that you associate with that user’s authorization requirements, Cisco ISE provides the native supplicant provisioning wizard (via the BYOD portal) required to set up the device for network access.

Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure BYOD rules to register these devices.

## End-User Device Portals in a Distributed Environment

Cisco ISE end-user web portals depend on the Administration, Policy Services, and Monitoring personas to provide configuration, session support, and reporting functionality.

### Administration Node

Any configuration changes you make to users or devices on the end-user portals are written to the Administration node.

### Policy Services Node

You must run the end-user portals on a Policy Services Node, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If the Policy Service Node is part of a node group, and the node fails, the other nodes detect the failure and reset any pending sessions.

### Monitoring Node

The Monitoring node collects, aggregates, and reports data about the end user and device activity on the My Devices, Sponsor, and Guest portals. If the primary Monitoring node fails, the secondary Monitoring node automatically becomes the primary Monitoring node.

## Limit the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 100 personal devices. Regardless of the portal that employees used to register their personal devices, this setting defines the maximum number of devices registered across all portals.

**Step 1** Choose **Administration** > **Device Portal Management** > **Settings** > **Employee Registered Devices**.

**Step 2** Enter the maximum number of devices that an employee can register in **Restrict employees to**. By default, this value is set to 5 devices.

**Step 3** Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

# Employee Accounts

When you add users such as employees or contractors to Cisco ISE, either by using external identity stores or by creating internal users, you can authorize them to use their personal devices on your network.

Cisco ISE authenticates these users through a local database, or through external Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory (AD) identity stores.

# Personal Device Portals

Cisco ISE provides several web-based portals to support employee-owned personal devices. These Device portals do not participate in the guest or sponsor portal flows.

Use these portals to:

- **Blacklist Portal—**Provide information about personal devices that are "blacklisted" and cannot be used to gain access to the network.
- **BYOD Portals—**Enable employees to register their personal devices using native supplicant provisioning functionality.
- **Client Provisioning Portals—**Force employees to download a posture agent on their devices that checks for compliance.
- **MDM Portals—**Enable employees to enroll their mobile devices with an external Mobile Device Management (MDM) system.
- **My Devices Portals—**Enable employees to add and register personal devices, including those that do not support native supplicant provisioning, and then manage them.

Cisco ISE provides you with the ability to host multiple device portals on the Cisco ISE server, including a predefined set of default portals. The default portal themes have standard Cisco branding that you can customize through the Admin portal. You can also choose to further customize a portal by uploading images, logos and cascading style sheets (CSS) files that are specific to your organization.

## Access Device Portals

**Step 1** To access any of the Device portals, you can either:

- Click **Administration** > **Device Portal Management**. The **Configure and Customize Device Portals** page displays the list of supported Device portals.
- Choose **Administration** > **Device Portal Management**. The supported Device portals display in the drop-down menu.

**Step 2** Select the specific device portal that you want to configure.

## Blacklist Portal

Employees do not access this portal directly, but are redirected to it.

If employees lose their personal device or it is stolen, they can update its status in the My Devices portal, which adds it to the Blacklist endpoint identity group. This prevents others from using the device to obtain unauthorized network access. If anyone attempts to connect to the network using one of these devices, they are redirected to the Blacklist portal which informs them that the device is denied access to the network. If the device is found, employees can reinstate it (in the My Devices portal) and regain network access without having to register the device again. Depending on whether the device was lost or stolen, additional provisioning may be required before the device can be connected to the network.

You can configure the port settings (default is port 8444) for the Blacklist portal. If you change the port number, make sure it is not being used by another end-user portal.

For information about configuring a Blacklist portal, see Edit the Blacklist Portal, on page 12.

# Bring Your Own Device Portal

Employees do not access this portal directly.

Employees are redirected to the Bring Your Own Device (BYOD) portal when registering personal devices using native supplicants. The first time employees attempt to access the network using a personal device, they may be prompted to manually download and launch the Network Setup Assistant (NSA) wizard and be guided through registering and installing the native supplicant. After they have registered a device, they can use the My Devices portal to manage it.

**Note** BYOD flow is not supported when a device is connected to a network using AnyConnect Network Access Manager (NAM).

# Client Provisioning Portal

Employees do not access this portal directly, but are redirected to it.

The Client Provisioning system provides posture assessments and remediations for devices that are attempting to gain access to your corporate network. When employees request network access using their devices, you can route them to a Client Provisioning portal and require them to first download the posture agent. The posture agent scans the device for compliance, such as verifying that virus protection software is installed on it and that its operating system is supported.

# Mobile Device Management Portal

Employees do not access this portal directly, but are redirected to it.

Many companies use a Mobile Device Management (MDM) system to manage employees' mobile devices.

Cisco ISE allows integration with external MDM systems that employees can use to enroll their mobile device and gain access to your corporate network. Cisco provides an external MDM interface that employees can enroll in to register their devices and then connect to the network.

The MDM portal enables employees to enroll in an external MDM system.

Employees can then use the My Devices portal to manage their mobile devices, such as lock their devices with a pin code, reset their device to its default factory settings, or remove applications and settings that were installed when registering the device.

Cisco ISE allows you to have a single MDM portal for all external MDM systems, or a portal for each individual MDM system.

For information about configuring MDM servers to work with ISE, see Create an MDM Portal, on page 15.

## My Devices Portal

Employees can access the My Devices portal directly.

Some network devices that need network access are not supported by native supplicant provisioning and cannot be registered using the BYOD portal. However, employees can add and register personal devices, whose operating systems are not supported or do not have web browsers (such as printers, Internet radios, and other devices), using the My Devices portal.

Employees can add and manage new devices by entering the MAC address for the device. When employees add devices using the My Devices portal, Cisco ISE adds the devices to the Endpoints page as members of the **RegisteredDevices** endpoint identity group (unless already statically assigned to a different endpoint identity group). The devices are profiled like any other endpoint in Cisco ISE and go through a registration process for network access.

When two MAC addresses from one device are entered into the My Devices Portal by a user, profiling determines that they have the same hostname, and they are merged together as a single entry in ISE. For example, a user registers a laptop with wired and wireless addresses. Any operations on that device, such as delete, acts on both addresses.

When a registered device is deleted from the portal, the Device Registration Status and BYOD Registration Status attributes change to NotRegistered and No, respectively. However, these attributes remain unchanged when a guest (who is not an employee) registers a device using the Guest Device Registration page in the credentialed Guest portals, because these are BYOD attributes used only during employee device registration.

Regardless of whether employees register their devices using the BYOD or the My Devices portals, they can use the My Devices portal to manage them.

# Support Device Registration Using Native Supplicants

You can create native supplicant profiles to support personal devices on the Cisco ISE network. Based on the profile that you associate with a user's authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard to set up the user's personal device to access the network.

The first time employees attempt to access the network using a personal device, they are guided automatically through registration and supplicant configuration. After they have registered the device, they can use the My Devices portal to manage their devices.

## BYOD Deployment Scenarios for Personal Devices Using Native Supplicants

The BYOD deployment flows that support personal devices using native supplicants vary slightly based on these factors:

- Single or dual SSID—With single SSID, the same WLAN is used for certificate enrollment, provisioning, and network access. In a dual SSID deployment, there are two SSIDs: one provides enrollment and provisioning, and the other provides secure network access.
- Windows, MacOS, iOS, or Android device—The native supplicant flow starts similarly, regardless of the device type, by redirecting employees using a supported personal device to the BYOD portal to confirm their device information. At this point, the process diverges based on device type.

### Employee Connects to Network

- Single SSID—Employees connect the device to the 802.1X SSID by entering their corporate username and password.
- Dual SSID—Employees connect to the open guest provisioning SSID and are redirected to the credentialed Guest portal. You must check **Allow employees to use personal devices on the network** in **BYOD Settings** in the credentialed Guest portal to enable this functionality.

### Employee Credentials Are Authenticated

Cisco ISE authenticates the employee against the corporate Active Directory or other corporate identity stores and provides an authorization policy.

### Device Is Redirected to the BYOD Portal

The device is redirected to the BYOD portal. The device's MAC address is automatically preconfigured, but employees can verify and add a description.

### 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, which configures the supplicant and provides the certificate (if required).
- 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 (if configured) embedded 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 Google Play. After installing the app, the employee can open NSA and start the setup wizard, which generates authentication parameters and initiates a certificate request (if required) for device certification.

### Change of Authorization Issued

Cisco ISE initiates a Change of Authorization (CoA) and connects the MacOS X, Windows, and Android devices to the secure 802.1X network. For single SSID, iOS devices also connect automatically, but for dual SSID, the wizard prompts iOS users to manually connect to the new network.

**Note** You must check the **Enable if Target Network is Hidden** check box only when the actual Wi-Fi network is hidden. Otherwise, Wi-Fi network configuration may not be provisioned properly for certain iOS devices, especially in the single SSID flow (where the same Wi-Fi network/SSID is used for both onboarding and connectivity).

# Operating Systems Supported by Native Supplicants

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 and 8 (excluding RT), Vista, and XP

# Allow Employees to Register Personal Devices Using Credentialed Guest Portals

Employees using credentialed Guest portals can register their personal devices. The self-provisioning flow supplied by the BYOD portal enables employees to connect devices to the network directly using native supplicants, which are available for Windows, MacOS, iOS, and Android devices.

### Before You Begin

You must create the native supplicant profiles.

**Step 1** Choose **Guest Access** > **Configure** > **Guest Portals**.

**Step 2** Choose the credentialed Guest portal that you want to allow employees to use to register their devices using native supplicants and click **Edit**.

**Step 3** On the **Portal Behavior and Flow Settings** tab and in **BYOD Settings**, check **Allow employees to use personal devices on the network**.

**Step 4** Click **Save** and then **Close**.

# Provide a URL to Reconnect with BYOD Registration

You can provide information that enables employees, who encounter a problem while registering their personal devices using the BYOD portal to reconnect with the registration process.

**Step 1** Choose **Administration** > **Device Portal Management** > **Settings** > **Retry URL**.

**Step 2** Change the IP address or enter a URL that can be used to redirect the device back to Cisco ISE in **Retry URL for onboarding**.

When the employee's device encounters a problem during the registration process, it will try to reconnect to the Internet automatically. At this point, the IP address or domain name that you enter here will redirect the device to Cisco ISE, which will reinitiate the onboarding process. The default value is 1.1.1.1.

**Step 3** Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

# Device Portals Configuration Tasks

You can use a default portal and its default settings such as certificates, endpoint identity group, identity source sequence, portal themes, images, and other details provided by Cisco ISE. If you do not want to use the default settings, you should create a new portal or edit an existing one to meet your needs. You can duplicate a portal if you want to create multiple portals with the same settings.

After creating a new portal or editing a default one, you must authorize the portal for use. Once you authorize a portal for use, any subsequent configuration changes you make are effective immediately.

You do not need to authorize the My Devices portal for use.

If you choose to delete a portal, you must first delete any authorization policy rules and authorization profiles associated with it or modify them to use another portal.

Use this table for the tasks related to configuring the different Device portals.

| Task | Blacklist Portal | BYOD Portal | Client Provisioning Portal | MDM Portal | My Devices Portal |
|---|---|---|---|---|---|
| Enable Policy Services, on page 9 | Required | Required | Required | Required | Required |
| Add Certificates, on page 10 | Required | Required | Required | Required | Required |
| Create External Identity Sources, on page 10 | Not Required | Not Required | Not Required | Not Required | Required |
| Create Identity Source Sequences, on page 10 | Not Required | Not Required | Not Required | Not Required | Required |
| Create Endpoint Identity Groups, on page 11 | Not Required | Required | Not Required | Required | Required |
| Edit the Blacklist Portal, on page 12 | Required | Not applicable | Not applicable | Not applicable | Not applicable |

| Task | Blacklist Portal | BYOD Portal | Client Provisioning Portal | MDM Portal | My Devices Portal |
|---|---|---|---|---|---|
| Create a BYOD Portal, on page 13 | Not applicable | Required | Not applicable | Not applicable | Not applicable |
| Create a Client Provisioning Portal, on page 14 | Not applicable | Not applicable | Required | Not applicable | Not applicable |
| Create an MDM Portal, on page 15 | Not applicable | Not applicable | Not applicable | Required | Not applicable |
| Create a My Devices Portal, on page 16 | Not applicable | Not applicable | Not applicable | Not applicable | Required |
| Authorize Portals, on page 17 | Not applicable | Required | Required | Required | Not Required |
| Customize Device Portals, on page 19 | Optional | Optional | Optional | Optional | Optional |

## Enable Policy Services

To support the Cisco ISE end-user web portals, you must enable portal-policy services on the node on which you want to host them.

**Step 1** Choose **Administration** > **System** > **Deployment**

**Step 2** Click the node and click **Edit**.

**Step 3** On the General Settings tab, check **Policy Service**.

**Step 4** Check the **Enable Session Services** option.

**Step 5** Click **Save**.

# Add Certificates

If you do not want to use the default certificates, you can add a valid certificate and assign it to a certificate group tag. The default certificate group tag used for all end-user web portals is Default Portal Certificate Group.

**Step 1** Chose **Administration** > **System** > **Certificates** > **System Certificates**.

**Step 2** Add a system certificate and assign it to a certificate group tag that you want to use for the portal.
This certificate group tag will be available to select during portal creation or editing.

**Step 3** Choose **Administration** > **Device Portal Management** > **(any portals)** > **Create or Edit** > **Portal Settings**.

**Step 4** Select the specific certificate group tag from the **Certificate Group Tag** drop-down list that is associated with the newly added certificate.

# Create External Identity Sources

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also includes certificate authentication profiles that you need for certificate-based authentications.

**Step 1** Choose **Administration** > **Identity Management** > **External Identity Sources**.

**Step 2** Choose one of these options:

- **Certificate Authentication Profile** for certificate-based authentications.
- **Active Directory** to connect to an Active Directory as an external identity source (see Active Directory as an External Identity Source for more details).
- **LDAP** to add an LDAP identity source (see LDAP for more details).
- **RADIUS Token** to add a RADIUS Token server (see RADIUS Token Identity Sources for more details).
- **RSA SecurID** to add an RSA SecurID server (see RSA Identity Sources for more details).
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager (see SAMLv2 Identity Provider as an External Identity Source for more details).

# Create Identity Source Sequences

## Before You Begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest Portal authentication source and the identity source sequence to contain the same identity stores.

**Step 1** Choose **Administration** > **Identity Management** > **Identity Source Sequences** > **Add**.

**Step 2** Enter a name for the identity source sequence. You can also enter an optional description.

**Step 3** Check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile for certificate-based authentication.

**Step 4** Choose the database or databases that you want to include in the identity source sequence in the **Selected List** box.

**Step 5** Rearrange the databases in the **Selected list** in the order in which you want Cisco ISE to search the databases.

**Step 6** Choose one of the following options in the **Advanced Search List** area:

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError —**If you want Cisco ISE to discontinue the search, if the user is not found in the first selected identity source.
- **Treat as if the user was not found and proceed to the next store in the sequence —**If you want Cisco ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.

  While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list box listed in the order in which you want Cisco ISE to search them.

**Step 7** Click **Submit** to create the identity source sequence that you can then use in policies.

# Create Endpoint Identity Groups

Cisco ISE groups endpoints that it discovers in to the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the Endpoint Identity Groups page. You can edit or delete the endpoint identity groups that you have created. You can only edit the description of the system-defined endpoint identity groups; you cannot edit the name of these groups or delete them.

**Step 1** Choose **Administration** > **Identity Management** > **Groups** > **Endpoint Identity Groups**.

**Step 2** Click **Add**.

**Step 3** Enter the name for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).

**Step 4** Enter the description for the endpoint identity group that you want to create.

**Step 5** Click the **Parent Group** drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.

**Step 6** Click **Submit**.

# Edit the Blacklist Portal

Cisco ISE provides a single Blacklist portal that displays information when a lost or stolen device that is blacklisted in Cisco ISE is attempting to access your corporate network.

You can only edit the default portal settings and customize the default message that displays for the portal. You cannot create a new Blacklist portal, or duplicate or delete the default portal.

### Before You Begin

Ensure that you have the required certificates configured for use with this portal.

**Step 1** Choose **Administration** > **Device Portal Management** > **Blacklist Portal** > **Edit**.

**Step 2** Provide a unique **Portal Name** and a **Description** for the portal.
Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 3** Use the **Languages** menu to export and import language files to use with the portal.

**Step 4** Update the default values for certificate group tags, languages and so on in **Portal Settings**, and define behavior that applies to the overall portal.

- **HTTPS Port—**Enter a Port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded ISE and were using Port values outside this range, they are honored until you make any change to this page. If you do change this page, you must update the Port setting to comply with this restriction.

  If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

- **Allowed interfaces—**Select the PSN interfaces where this portal can run. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.

  - The Ethernet interfaces must use IP addresses on different subnets.

  - The interfaces you enable here must be available on all the PSNs that are running portals, including VM-based ones (when Policy Services turned on). This is required because any of these PSNs can be used for a redirect at the start of the guest session.

  - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP. If the interface IP is not the same as the domain, then configure **ip host x.x.x.x yyy.domain.com** in the ISE CLI to map your interface IP to FQDN in the certificate.

- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.

- **Display Language—**Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

**Step 5** On the **Portal Page Customization** tab, customize the page title and message text that appears in the portal when an unauthorized device is attempting to gain access to the network.

**Step 6** Click **Save** and then **Close**.

# Create a BYOD Portal

You can provide a Bring Your Own Device (BYOD) portal to enable employees to register their personal devices, so that registration and supplicant configuration can be done before allowing access to the network.

You can create a new BYOD portal, or you can edit or duplicate an existing one. You can delete any BYOD portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

### Before You Begin

Ensure that you have the required certificates and endpoint identity groups configured for use with this portal.

**Step 1** Choose **Administration** > **Device Portal Management** > **BYOD Portals** > **Create, Edit or Duplicate**.

**Step 2** Provide a unique **Portal Name** and a **Description** for the portal.
Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 3** Use the **Language File** drop-down menu to export and import language files to use with the portal.

**Step 4** Update the default values for ports, certificate group tags, endpoint identity groups and so on in **Portal Settings**, and define behavior that applies to the overall portal.

**Step 5** Update the **Support Information Page Settings** to help employees provide information that the Help Desk can use to troubleshoot network access issues.

**Step 6** On the **Portal Page Customization** tab, customize the **Content Area** message text that appears on the following pages during the provisioning process:

- BYOD Welcome page:
    - Device Configuration Required—When the device is redirected to the BYOD portal for the first time and requires certificate provisioning.
    - Certificate Needs Renewal—When the previous certificate needs to be renewed.
- BYOD Device Information page:
    - Maximum Devices Reached—When the maximum limit of devices that an employee can register is reached.
    - Required Device Information—When requesting device information that is required to enable an employee to register the device.
- BYOD Installation page:
    - Desktop Installation—When providing installation information for a desktop device.
    - iOS Installation—When providing installation instructions for an iOS mobile device.
    - Android Installation—When providing installation instructions for an Android mobile device
- BYOD Success page:

- ◦ Success—When the device is configured and automatically connected to the network.
- ◦ Success: Manual Instructions—When the device is successfully configured and an employee must manually connect to the network.
- ◦ Success: Unsupported Device—When an unsupported device is allowed to connect to the network.

**Step 7** Click **Save** and then **Close**.

### What to Do Next

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

# Create a Client Provisioning Portal

You can provide a Client Provisioning portal to enable employees to download either the Cisco AnyConnect posture component or the Cisco NAC agent, which verifies the posture compliance of the device before allowing access to the network.

You can create a new Client Provisioning portal, or you can edit or duplicate an existing one. You can delete any Client Provisioning portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

### Before You Begin

Ensure that you have the required certificates and client provisioning policies configured for use with this portal.

**Step 1** Choose **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Create, Edit or Duplicate**.

**Step 2** Provide a unique **Portal Name** and a **Description** for the portal.
Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 3** Use the **Language File** drop-down menu to export and import language files to use with the portal.

**Step 4** Update the default values for ports, certificate group tags, endpoint identity groups and so on in **Portal Settings**, and define behavior that applies to the overall portal.

**Step 5** Update the **Support Information Page Settings** to help employees provide information that the Help Desk can use to troubleshoot network access issues.

**Step 6** On the **Portal Page Customization** tab, customize the **Content Area** message text that appears in the Client Provisioning portal during the provisioning process:

a) On the Client Provisioning page:

- Checking, Scanning and Compliant—When the posture agent is successfully installed and checks, scans and verifies that the device is compliant with posture requirements.

- Non-compliant—When the posture agent determines that the device is not compliant with posture requirements.

b) On the Client Provisioning (Agent Not Found) page:

- Agent Not Found—When the posture agent is not detected on the device.
- Manual Installation Instructions—When devices do not have Java or Active X software installed on them, instructions on how to manually download and install the posture agent.
- Install, No Java/ActiveX—When devices do not have Java or Active X software installed on them, instructions on how to download and install the Java plug-in.
- Agent Installed—When the posture agent is detected on the device, instructions on how to start the posture agent, which checks the device for compliance with posture requirements .

**Step 7** Click **Save** and then **Close**.

### What to Do Next

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

## Create an MDM Portal

You can provide a Mobile Device Management (MDM) portal to enable employees to manage their mobile devices that are registered for use on your corporate network.

You can create a new MDM portal, or you can edit or duplicate an existing one. You can have a single MDM portal for all of your MDM systems or you can create a portal for each system. You can delete any MDM portal, including the default portal provided by Cisco ISE. The default portal is for third-party MDM providers.

You can create a new MDM portal, or you can edit or duplicate an existing one. You can delete any MDM portal, including the default portal provided by Cisco ISE. The default portal is for third-party MDM providers.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

### Before You Begin

Ensure that you have the required certificates and endpoint identity groups configured for use with this portal.

**Step 1** Choose **Administration** > **Device Portal Management** > **MDM Portals** > **Create, Edit or Duplicate**.

**Step 2** Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 3** Use the **Language File** drop-down menu to export and import language files to use with the portal.

**Step 4** Update the default values for ports, certificate group tags, endpoint identity groups and so on in **Portal Settings**, and define behavior that applies to the overall portal.

**Step 5** Update the following settings that apply to each of the specific pages:

- In **Employee Mobile Device Management Settings**, access the link provided to configure third-party MDM providers and then define the acceptance policy behavior for employees using the MDM portals.
- **Support Information Page Settings** to help guests provide information that the Help Desk can use to troubleshoot network access issues.

**Step 6** On the **Portal Page Customization** tab, customize the **Content Area** messages that appears in the MDM portal during the device enrollment process:

- Unreachable—When the selected MDM system cannot be reached.
- Non-compliant—When the device being enrolled is not compliant with the requirements of the MDM system.
- Continue—When the device should try connecting to the network in case of connectivity issues.
- Enroll—When the device requires the MDM agent and needs to be enrolled in the MDM system.

**Step 7** Click **Save** and then **Close**.

### What to Do Next

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use. Also see the following topics:

- Add Certificates, on page 10
- Create Endpoint Identity Groups, on page 11
- Authorize Portals, on page 17
- Customize Device Portals, on page 19

# Create a My Devices Portal

You can provide a My Devices portal to enable employees to add and register their personal devices that do not support native supplicants and cannot be added using the Bring Your Own Device (BYOD) portal. You can then use the My Devices portal to manage all devices that have been added using either portal.

You can create a new My Devices portal, or you can edit or duplicate an existing one. You can delete any My Devices portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

### Before You Begin

Ensure that you have the required certificates, external identity stores, identity source sequences, and endpoint identity groups configured for use with this portal.

**Step 1** Choose **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate**.

**Step 2** Provide a unique **Portal Name** and a **Description** for the portal.
Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 3** Use the **Language File** drop-down menu to export and import language files to use with the portal.

**Step 4** Update the default values for ports, certificate group tags, identity source sequences, endpoint identity groups, and so on in **Portal Settings**, and define behavior that applies to the overall portal.

**Step 5** Update the following settings that apply to each of the specific pages:

- **Login Page Settings—**Specify employee credential and login guidelines.
- **Acceptable Use Policy (AUP) Page Settings—**Add a separate AUP page and define the acceptable use policy behavior for employees.
- **Post-Login Banner Page Settings—**Notify employees of additional information after they log into the portal.
- **Employee Change Password Settings—**Allow employees to change their own passwords. This option is enabled only if the employee is part of the Internal Users database.

**Step 6** In the **Portal Page Customization** tab, customize the following information that appears in the My Devices portal during registration and management:

- Titles, instructions, content, field and button labels
- Error messages and notification messages

**Step 7** Click **Save** and then **Close**.

### What to Do Next

You can customize the portal if you want to change its appearance.

## Authorize Portals

When you authorize a portal, you are setting up the network authorization profiles and rules for network access.

### Before You Begin

You must create a portal before you can authorize it.

**Step 1** Set up a special authorization profile for the portal.

**Step 2** Create an authorization policy rule for the profile.

## Create Authorization Profiles

Each portal requires that you set up a special authorization profile for it.

### Before You Begin

If you do not plan to use a default portal, you must first create the portal so you can associate the portal name with the authorization profile.

**Step 1** Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

**Step 2** Create an authorization profile using the name of the portal that you want to authorize for use.

### What to Do Next

You should create a portal authorization policy rule that uses the newly created authorization profile.

## Create Authorization Policy Rules

To configure the redirection URL for a portal to use when responding to the users' (guests, sponsors, employees) access requests, define an authorization policy rule for that portal.

The url-redirect takes the following form based on the portal type, where:

*ip:port* = the IP address and port number

*PortalID* = the unique portal name

For a Hotspot Guest portal:
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

For a Mobile Device Management (MDM) portal:
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

**Step 1** Choose **Policy** > **Authorization** to create a new authorization policy rule under **Standard** policies.
If you enabled Policy Sets, choose **Policy** > **Policy Set**, pick the Policy Set you plan to use for this portal, expand Authorization Policy, and add a new rule.

**Step 2** For **Conditions**, select an endpoint identity group that you want to use for the portal validation. For example, for the Hotspot Guest portal, select the default **GuestEndpoints** endpoint identity group and, for the MDM portal, select the default **RegisteredDevices** endpoint identity group.

**Note** Because the Hotspot Guest portal only issues a Termination CoA, do not use Network Access:UseCase EQUALS Guest Flow as one of the validation conditions in the Guest authorization policy. Instead, match the Identity Group that the endpoint belongs to for validation. For example,

- If "GuestEndpoint" + Wireless MAB then Permit Access
- If Wireless MAB then HotSpot Redirect

**Step 3** For **Permissions**, select the portal authorization profile that you created.

## Customize Device Portals

You can customize the portal appearance and user (guests, sponsors, or employees as applicable) experience by customizing the portal themes, changing UI elements on the portal pages, and editing error messages and notifications that display to the users.

# Manage Personal Devices Added by Employees

When employees register a device using the Bring Your Own Device (BYOD) or the My Devices portals, it displays in the Endpoints list. Although employees can disassociate a device from their account by deleting it, the device remains in the Cisco ISE database. As a result, employees might need your assistance in resolving errors they encounter when working with their devices.

## Display Devices Added by an Employee

You can locate devices added by a specific employee using the Portal User field displayed on the Endpoints listing page. This might be useful if you need to delete devices registered by a specific user. By default, this field does not display, so you must enable it first before searching.

**Step 1** Choose **Administration** > **Identity Management** > **Identities** > **Endpoints**.

**Step 2** Click the **Settings** icon and choose **Columns**.

**Step 3** Select **Portal User** to display this information in the Endpoints listing.

**Step 4** Click the **Show** drop-down list and choose **Quick Filter**.

**Step 5** Enter the user’s name in the **Portal User** field to display only the endpoints that are assigned to that particular user.

## Errors When Adding Devices to My Devices Portal

Employees cannot add a device, if another employee has previously added it such that the device already exists in the Cisco ISE endpoints database.

If employees attempt to add a device that already exists in the Cisco ISE database:

- And it supports native supplicant provisioning, we recommend adding the device through the BYOD portal. This will overwrite any registration details that were created when it was initially added to the network.
- If the device is a MAC Authentication Bypass (MAB) device, such as a printer, then you must resolve ownership of the device first. If appropriate, you can remove the device from the endpoints database

using the Admin portal, so that the new owner can successfully add the device using the My Devices portal.

## Devices Deleted from My Devices Portal Remain in Endpoints Database

When an employee deletes a device from the My Devices portal, the device is removed from the employee's list of registered devices, but the device remains in the Cisco ISE endpoints database and displays in the Endpoints list.

To permanently delete the device from the Endpoints page, choose **Administration** > **Identity Management** > **Identities** > **Endpoints**.

# Monitor My Devices Portals and Endpoints Activity

Cisco ISE provides various reports and logs that allow you to view endpoint and user management information and guest and sponsor activity. Some of the Cisco ISE 1.2 reports have been deprecated, but the information can be viewed in other reports.

You can run these reports either on demand or on a scheduled basis.

**Step 1** Choose **Operations** > **Reports**.

**Step 2** Under the Report Selector, expand the **Guest Access Reports** and **Endpoints and Users** selections to view the various guest, sponsor, and endpoint related reports.

**Step 3** Select the report and choose the data with which you want to search using the **Filters** drop-down list.
You can use filters on username, portal name, device name, endpoint identity group and other such data.

**Step 4** Select the **Time Range** during which you want to view the data.

**Step 5** Click **Run**.

## My Devices Login and Audit Report

The My Devices Login and Audit report is a combined report that tracks:

- Login activity by employees at the My Devices portal.
- Device-related operations performed by the employees in the My Devices portal.

This report is available at: **Operations** > **Reports** > **Guest Access Reports** > **My Devices Login and Audit**.

## Registered Endpoints Report

The Registered Endpoints report provides information about all the endpoints that are registered by employees. This report is available at: **Operations** > **Reports** > **Endpoints and Users** > **Registered Endpoints**. You can run a query on the following: identity, endpoint ID, identity profile, and the like, and you can generate a report. For information on supplicant provisioning statistics and related data, see Viewing Client Provisioning Reports.

You can query the endpoint database for endpoints that are assigned to the RegisteredDevices endpoint identity group. You can also generate reports for specific users that have the Portal User attribute set to a non-null value.

The Registered Endpoints Report provides information about a list of endpoints that are registered through device registration portals by a specific user for a selected period of time.