Bring Your Own Device (BYOD)

Personal Devices on a Corporate Network (BYOD)

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 the Guest portals. Guests can register additional devices up to the maximum limit that you define in their guest type. These devices are registered into endpoint identity groups based on the portal configuration.

Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. You can create native supplicant profiles, which determine the proper native supplicant provisioning wizard to use, based on the operating system.

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.

Cisco ISE Community Resource

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.

- **Policy Administration node (PAN)**: Configuration changes that you make to the users, devices, and end-user portals are written to the PAN.
- **Policy Service node (PSN)**: The end-user portals run on a PSN, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If a PSN is part of a node group, and one node fails, the other nodes detect the failure and reset any pending sessions.

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

Global Settings for Device Portals

Choose **Work Centers** > **BYOD** > **Settings** > **Employee Registered Devices** or **Administration** > **Device Portal Management** > **Settings**.

You can configure the following general settings for the BYOD and My Devices portals:

- **Employee Registered Devices**: Enter the maximum number of devices that an employee can register in **Restrict employees to**. By default, this value is set to **5** devices.
- **Retry URL**: Enter a URL that can be used to redirect the device back to Cisco ISE in **Retry URL for onboarding**.

Once you configure these general settings, they apply to all BYOD and My Devices portals that you set up for your company.

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.

- **Blacklist Portal**: Provides information about personal devices that are block listed and cannot be used to gain access to the network.
- **BYOD Portals**: Enables employees to register their personal devices using native supplicant provisioning functionality.
- **Certificate Provisioning Portal**: Enables administrators and employees to request for user or device certificate(s) for devices that cannot go through the BYOD flow.
- **Client Provisioning Portals**: Forces employees to download a posture agent on their devices that checks for compliance.
- **MDM Portals**: Enables employees to enroll their mobile devices with an external Mobile Device Management (MDM) system.
- **My Devices Portals**: Enables 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 Administrators portal (**Administration** > **Device Portal Management**). 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

You can access any of the Personal Device Portals from the Cisco ISE GUI as follows:

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

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 13.

Certificate Provisioning Portal

Employees can access the Certificate Provisioning portal directly.

The Certificate Provisioning portal allows employees to request certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals cannot go through the BYOD flow and need to be issued certificates manually. The Certificate Provisioning portal allows a privileged set of users to upload a certificate request for such devices, generate key pairs (if required), and download the certificate.

Employees can access this portal and request for a single certificate or make a bulk certificate request using a CSV file.

ISE Community Resource

For information about the functionality and configuration of Cisco ISE Certificate Provisioning Portal, see ISE 2.0: Certificate Provisioning Portal.

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.

If you're using Microsoft Edge 93 or Microsoft Edge 94 as your web browser for downloading NSA and AnyConnect wizards, copy-paste the **redirected URL** or **download link** in a new tab and click **Enter** on your keyboard.

Alternatively, you can click on **Download icon** > **right click on downloaded file** > **Keep file** on your Microsoft Edge 93 or Microsoft Edge 94 browser.

If you are using Google Chrome 93 or Google Chrome 95 as your web browser for downloading Network Setup Assistant (NSA) and AnyConnect wizards, click the **Keep** option in the download notification to keep and install the NSA and AnyConnect packages on your system.

Note

- BYOD flow is not supported when a device is connected to a network using Network Access Manager (NAM).
- If you are using the BYOD flow for Android devices, upgrade to Android 11 or enable the Broadcast SSID option in WLAN configuration.

Related Topics

Create a BYOD Portal, on page 15
Personal Devices on a Corporate Network (BYOD), on page 1

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.

Related Topics

Create a Client Provisioning Portal, on page 18

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 Cisco ISE, see Create an MDM Portal, on page 19.

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 window (**Administration** > **Context Visibility** > **Endpoints**) 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 Cisco 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 **DeviceRegistrationStatus** and **BYODRegistration** attributes change to **Not Registered** and **No**, respectively. However, these attributes remain unchanged when a guest (who is not an employee) registers a device using the Guest Device Registration window in the credentialed Guest portals, because these BYOD attributes are 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.

Note The My Devices portal is not available when the Administrator's portal is down.

When endpoints are imported from Context visibility, they are not automatically linked to BYOD user accounts. They must follow the usual BYOD registration process to be added to the My Devices portal.

Related Topics

Create a My Devices Portal, on page 20

BYOD Deployment Options and Status Flow

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

- Single or dual SSID: With single SSID, the same Wireless Local Area Network (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. The process diverges based on the device type.

Employee Connects to Network

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

2. The device is redirected to the BYOD portal. The device's MAC address field is preconfigured, and the user can add a device name and description.
3. The native supplicant is configured (MacOS, Windows, iOS, Android) 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 (Network Setup Assistant), which configures the supplicant and provides the certificate (if necessary) used for EAP-TLS certificate-based authentication. The issued certificate is embedded with the device's MAC address and employee's username.

     Starting with version MacOS 10.15, the user must allow download of the Supplicant Provisioning Wizard (SPW). A window displays on the user's device asking them to allow or deny downloads from the Cisco ISE server.

Note Network Setup Assistant cannot be downloaded to a Windows device, unless the user of that device has administrative privileges. If you cannot grant end users administrative privileges, then use your Group Policy object (GPO) to push the certificate to the user's device, instead of using the 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 (if configured) is embedded with the iOS device's MAC address and employee's username.
     - A Wi-Fi supplicant profile that enforces the use of EAP-TLS for 802.1X authentication. An additional profile can be installed on the endpoint device to protect Over-The-Air (OTA) communication.

     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 or SSID is used for both onboarding and connectivity).
   - Android devices: Cisco ISE prompts and routes employee to download the Network Setup Assistant (NSA) from the Google Play store. After installing the application, the employee can open NSA and start the setup wizard, which generates the supplicant configuration and issued certificate used to configure the device.
4. After the user goes through the on boarding flow, Cisco ISE initiates a Change of Authorization (CoA). This causes the MacOS, Windows, and Android devices to reconnect 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.

You can configure a BYOD flow that does not use supplicants. For more information, see the Cisco ISE Community Resource document.

Note Mac randomization is not enabled for this flow.

As Android 10 generates a random MAC address whenever a new connection profile is created, you must modify the default rule to remove *BYOD_is_Registered* and *MAC_in_SAN* conditions from the authorization profile for the BYOD flow to work with Android clients.

BYOD Session Endpoint Attribute

The state of the endpoint attribute *BYODRegistration* changes during the BYOD flow to the following states.

- *Unknown*: The device has not been through a BYOD flow.
- *Yes*: The device has been through BYOD flow, and is registered.
- *No*: The device has been through BYOD flow, but is not registered. This means that the device was deleted.

Device Registration Status Endpoint Attribute

The state of the endpoint attribute *DeviceRegistrationStatus* changes during device registration to the following states.

- *Registered*: The device has been through BYOD flow, and it is registered. There is a 20-minute delay before the attribute changes from pending to registered.
- *Pending*: The device has been through BYOD flow, and it is registered. But, Cisco ISE has not seen it on the network.
- *Not Registered*: The device has not been through BYOD flow. *Not Registered* is the default state of the *DeviceRegistrationStatus* attribute.
- *Stolen*: The user logs onto the My Devices portal, and marks a currently onboarded device as Stolen. This happens:
  - If the device was onboarded by provisioning a certificate and a profile, Cisco ISE revokes the certificate that was provisioned to the device, and assigns the device's MAC address to the Blacklist endpoint identity group. That device no longer has network access.
  - If the device was onboarded by provisioning a profile (no certificate), Cisco ISE assigns the device to the Blacklist endpoint identity group. The device still has network access, unless you create an authorization policy for this situation. For example, **IF Endpoint Identity Group is Blacklist AND BYOD_is_Registered THEN DenyAccess**.

  An administrator performs an action that disables network access for several devices, such as deleting or revoking a certificate.

  If a user reinstates a stolen device, the status reverts to *Not Registered*. The user must delete that device, and add it back. This starts the onboarding process.
- *Lost*: The user logs on to the My Devices portal, and marks a currently onboarded device as *Lost* that causes the following actions:
  - The device is assigned to Blacklist identity group.

- Certificates provisioned to the device are not revoked.
- The device status is updated to *Lost*.
- *BYODRegistration* status is updated to *No*.

A lost device still has network access unless you create an authorization policy to block lost devices. You can use the Blacklist identity group or the *endpoint:BYODRegistration* attribute in your rule. For example, **IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD**. For more granular access, you can also add *NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST" , InternalUser:IdentityGroup Equals <<group>>* to the IF part of the rule.

Limit the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 999 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 the **Restrict employees to** field. 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.

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 the registration and supplicant configuration. After they have registered the device, they can use the My Devices portal to manage their devices.

Operating Systems Supported by Native Supplicants

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

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 **Work Centers** > **Guest Access** > **Portals & Components** > **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 Click the **Portal Behavior and Flow Settings** tab.

Step 4 Under **BYOD Settings**, check the **Allow employees to use personal devices on the network** check box.

Step 5 Click **Save**.

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 In the **Retry URL for Onboarding** field, enter the URL to be used to redirect the device back to Cisco ISE.

When a device encounters a problem during the registration process, it tries to reconnect to the internet automatically. At this point, the URL that you enter here is used to redirect the device back to Cisco ISE (which reinitiates 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 11	Required	Required	Required	Required	Required
Add Certificates to the Device Portal, on page 11	Required	Required	Required	Required	Required
Create External Identity Sources, on page 12	Not Required	Not Required	Not Required	Not Required	Required
Create Identity Source Sequences, on page 12	Not Required	Not Required	Not Required	Not Required	Required
Create Endpoint Identity Groups, on page 13	Not Required	Required	Not Required	Required	Required
Edit the Blacklist Portal	Required	Not applicable	Not applicable	Not applicable	Not applicable
Create a BYOD Portal, on page 15	Not applicable	Required	Not applicable	Not applicable	Not applicable
Create a Client Provisioning Portal, on page 18	Not applicable	Not applicable	Required	Not applicable	Not applicable
Create an MDM Portal, on page 19	Not applicable	Not applicable	Not applicable	Required	Not applicable
Create a My Devices Portal, on page 20	Not applicable	Not applicable	Not applicable	Not applicable	Required

Task	Blacklist Portal	BYOD Portal	Client Provisioning Portal	MDM Portal	My Devices Portal
Create Authorization Profiles, on page 22	Not applicable	Required	Required	Required	Not Required
Customize Device Portals, on page 23	Optional	Optional	Optional	Optional	Optional

Enable Policy Services

To support the Cisco ISE end-user web portals, you must enable the 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 Under the **General Settings** tab, check the **Policy Service** check box.

Step 4 Check the **Enable Session Services** check box.

Step 5 Click **Save**.

Add Certificates to the Device Portal

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 Choose **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 portal)** > **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.

Note

- BYOD does not support certificate chains longer than three certificates.
- During BYOD onboarding, certificates are issued twice for iOS devices.

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 include certificate authentication profiles that you need for certificate-based authentications.

Note To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers.

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.
- **Social Login** to add a Social Login, such as Facebook, as an external identity source. See Social Login for Self-Registered Guests 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** field.

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

Step 6 If a selected identity store cannot be accessed for authentication, 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**

- **Treat as if the user was not found and proceed to the next store in the sequence**

  While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list field 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** window. 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 block listed 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 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal test URL** link to open a new browser tab that displays the URL for this portal. Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are disabled, the PSN only displays the Admin portal.

Note The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work. If you have more than one PSN, Cisco ISE chooses the first active PSN.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, 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 with port values outside this range, they are honored until you modify this window. If you modify this window, 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 appears.

  For posture assessments and remediation only, the Client Provisioning portal also uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - Valid combinations include, using the Sponsor portal as an example:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A** and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blacklist portal: Port **8444**, Interface **0**, Certificate group **B**.
  - Invalid combinations include:
    - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
    - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blacklist portal: Port **8444**, Interface **0**, Certificate group **A**.

  Note We recommend that you use interface 0 for Guest services for best performance. You can either configure only interface 0 in the **Portal Settings**, or you can use the CLI command **ip host** to map a hostname or FQDN to the IP address of interface 0.

- **Allowed Interfaces**: Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, 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 or Alternate Subject Name must resolve to the interface IP address.

- Configure **ip host x.x.x.x yyy.domain.com** in Cisco ISE CLI to map the secondary interface IP address to the FQDN, which is used to match the certificate Subject Name or Alternate Subject Name.
- If only the bonded NIC is selected, when the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will not try to start the portal on the physical interface.
- NIC Teaming or bonding is a configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based in the **Portal Settings** configuration. If both physical NICs and the corresponding bonded NIC are configured, when the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

- **Certificate Group tag**: Pick a certificate group tag that specifies the certificate to be used for the portal's HTTPS traffic.
- **Display Language**
  - **Use Browser Locale**: Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by Cisco ISE, then the **Fallback Language** is used as the language portal.
  - **Fallback Language**: Choose the language to use when the language cannot be obtained from the browser locale, or if the browser locale language is not supported by Cisco ISE.
  - **Always Use**: Choose the display language to use for the portal. This setting overrides the **User Browser Locale** option.

Step 6 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 7 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 the 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 **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it from the flow.

Before you begin

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

Step 1 Choose **Administration** > **Device Portal Management** > **BYOD** > **Create**.

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

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

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **Support Information Page Settings**. Update the required information here to help employees provide information that the Help Desk can use to troubleshoot network access issues.

Step 7 Click the **Portal Page Customization** tab. Scroll down to the **Page Customizations** area to customize the following end user portal windows. Choose the portal window you want to customize by clicking the corresponding option listed under **Pages**in the left side menu.

- **BYOD Welcome**:
  - **Device Configuration Required**: Enter the content to be displayed when the device is redirected to the BYOD portal for the first time and requires certificate provisioning.
  - **Certificate Needs Renewal**: Enter the content to be displayed when the previous certificate needs to be renewed.
- **BYOD Device Information**:
  - **Maximum Devices Reached**: Enter the content to be displayed when the maximum limit of devices that an employee can register is reached.
  - **Required Device Information**: Enter the content to be displayed when requesting device information that is required to enable an employee to register the device.
- **BYOD Installation**:
  - **Desktop Installation**: Enter the content to be displayed when providing installation information for a desktop device.
  - **iOS Installation**: Enter the content to be displayed when providing installation instructions for an iOS mobile device.
  - **Android Installation**: Enter the content to be displayed when providing installation instructions for an Android mobile device.
- **BYOD Success**:
  - **Success**: Enter the content to be displayed when the device is configured and automatically connected to the network.
  - **Success: Manual Instructions**: Enter the content to be displayed when the device is successfully configured and an employee must manually connect to the network.
  - **Success: Unsupported Device**: Enter the content to be displayed when an unsupported device is allowed to connect to the network.

Step 8 Click **Save** and then click **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 Certificate Provisioning Portal

Cisco ISE provides a Certificate Provisioning portal that allows you to request for certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals. You can request for a single certificate or make a bulk certificate request using a CSV file.

You can edit the default portal settings and customize the messages that appear on the portal. You can also create, duplicate, and delete the Certificate Provisioning portal.

There are two types of users who can access the Certificate Provisioning portal:

- Internal or external users with administrative privileges: Can generate certificates for themselves as well as for others.
- All other users: Can generate certificates only for themselves.

Users (network access users) who are assigned the Super Admin or ERS Admin role have access to this portal and can request certificates for others. However, if you create a new internal admin user and assign the Super Admin or ERS Admin role, the internal admin user will not have access to this portal. You must first create a network access user and then add the user to the Super Admin or ERS Admin group. Any existing network access users who are added to the Super Admin or ERS Admin group will have access to this portal.

For other users to be able to access the portal and to generate certificates for themselves, configure the Certificate Provisioning Portal Settings. The navigation path for this window is **Administration** > **Device Portal Management** > **Certificate Provisioning** > **Edit** > **Portal Behavior and Flow Settings** > **Portal Settings**. Ensure that you choose the appropriate identity source or identity source sequence under **Authentication Method** and choose the user group under **Configure Authorized Groups**. All users who belong to the groups that you choose will have access to the portal and can generate certificates for themselves.

Before you begin

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

Step 1 Choose **Administration** > **Device Portal Management** > **Certificate Provisioning** > **Create**.

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

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

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Click the **Portal Page Customization** tab. Customize the page title and the message text that appears in the portal.

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

Create a Client Provisioning Portal

You can provide a Client Provisioning portal to enable employees to download the Cisco AnyConnect posture component, that 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.

Users (network access users) who are assigned the Super Admin or ERS Admin role have access to this portal. However, if you create a new internal admin user and assign the Super Admin or ERS Admin role, the internal admin user will not have access to this portal. You must first create a network access user and then add the user to the Super Admin or ERS Admin group. Any existing network access users who are added to the Super Admin or ERS Admin group will have access to this portal.

For other users to be able to access the portal and to generate certificates for themselves, configure the Certificate Provisioning Portal settings. The navigation path for this window is **Administration** > **Device Portal Management** > **Client Provisioning** > **Edit** > **Portal Behavior and Flow Settings** > **Portal Settings**. Ensure that you choose the appropriate identity source or identity source sequence under **Authentication Method** and choose the user group under **Configure Authorized Groups**. All users who belong to the groups that you choose will have access to the portal and can generate certificates for themselves.

Any changes that you make to the **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it 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** > **Create**.

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

Ensure that the portal name

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **Support Information Page Settings**. Update the required information here to help employees provide information that the Help Desk can use to troubleshoot network access issues.

Step 7 Click the **Portal Page Customization** tab. Scroll down to the **Page Customizations** area to customize the following end user portal windows. Choose the portal window you want to customize by clicking the corresponding option listed under **Pages**in the left side menu.

- **Client Provisioning Portals**:

- **Agent Unknown**: Enter the content to be displayed when the agent is unknown.
- **Checking**, **Scanning** and **Compliant**: Enter the content to be displayed when the posture agent is successfully installed and checks, scans and verifies that the device is compliant with posture requirements.
- **Non-compliant**: Enter the content to be displayed when the posture agent determines that the device is not compliant with posture requirements.

- **Client Provisioning (Agent Not Found)**:
  - **Agent Not Found**: Enter the content to be displayed when the posture agent is not detected on the device.
  - **Manual Installation Instructions**: Enter the content to be displayed 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**: Enter the content to be displayed 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**: Enter the content to be displayed 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 8 Click **Save** and then click **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.

Related Topics

Authorize Portals
Customize Device Portals, on page 23

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 **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it 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** > **Mobile Device Management** > **Create, Edit or Duplicate**.

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

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

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings**. Update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **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.

Step 7 Expand **Support Information Page Settings**. Update the required information here to help employees provide information that the help desk can use to troubleshoot network access issues.

Step 8 Click the **Portal Page Customization** tab.

Step 9 Customize the **Content Area** messages that appears in the MDM portal during the device enrollment process.

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

Step 10 Click **Save** and then click **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 to the Device Portal, on page 11
- Create Endpoint Identity Groups, on page 13
- Create Authorization Profiles, on page 22
- Customize Device Portals, on page 23

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 **Portal & Page Settings** under the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the device portal flow diagram. If you enable a window, such as the **Support Information** window, the window appears in the flow and the employee experiences it in the portal. Disabling the window removes it 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** > **Create**.

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

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

Step 3 From the **Language File** drop-down list, choose the desired action to import or export language files to be used with the portal.

Step 4 Click the **Portal Behavior and Flow Settings** tab.

Step 5 Expand **Portal Settings** to update the default values for ports, certificate group tags, endpoint identity groups, and so on, and define behavior that applies to the overall portal.

Step 6 Expand **Login Page Settings** to specify employee credential and login guidelines.

Step 7 Expand **Acceptable Use Policy (AUP) Page Settings** to add a separate AUP page and define the acceptable use policy behavior for employees.

Step 8 Expand **Post-Login Banner Page Settings** to notify employees of additional information after they log into the portal.

Step 9 Expand **Employee Change Password Settings** to allow employees to change their own passwords. This option is enabled only if the employee is part of the internal users database.

Step 10 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 11 Click **Save** and then click **Close**.

What to do next

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

Related Topics

Customize Device Portals, on page 23
My Devices Portal, on page 5
Display Devices Added by an Employee, on page 23

Create Authorization Profiles

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.

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** > **Policy Sets** to create a new authorization policy rule under **Standard** policies.

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 Reauthenticate and Terminate CoA types are supported by Hotspot Guest portals. You can use Network Access:UseCase EQUALS Guest Flow as one of the validation conditions in the Hotspot Guest authorization policy only when Reauthentication CoA type is chosen in the Hotspot Guest Portal.

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

Note While creating an authorization condition using a dictionary attribute with the MAC option enabled, such as RADIUS.Calling-Station-ID, you must use a Mac operator (for example, Mac_equals) to support different MAC formats.

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 are displayed to the users. For more information about customizing portals, see Customization of End-User Web Portals.

Manage Personal Devices Added by Employees

When employees register a device using the Bring Your Own Device (BYOD) or the My Devices portals, the registered device is displayed 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 window. 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 **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Step 2 Click the **Settings** icon available on the top right corner of the endpoints list, below the dashlets.

Step 3 Check the **Portal User** check boxEnable the **Portal User** toggle button to display this information in the endpoints listing.

Step 4 Click **Go**.

Step 5 Click the **Filter** drop-down list and choose **Quick Filter**.

Step 6 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 that was already added by another employee, and that device is still in the endpoints database.

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

- We recommend adding the device through the BYOD portal, if it supports native supplicant provisioning. This overwrites 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 first resolve the ownership of the device. If appropriate, you can remove the device from the endpoints database using the Administrator's portal, so that the new owner can successfully add the device using the My Devices portal.

Note The My Devices portal is not available when the Administrator's portal is down.

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 is displayed in the **Endpoints** list.

You can permanently delete the device from the Endpoints window. The navigation path for this window is **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

Limit the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 999 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 the **Restrict employees to** field. 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.

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.

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

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

Step 2 Choose **Guest** or **Endpoints and Users** to view the various guest, sponsor, and endpoint related reports

Step 3 Choose the data with which you want to search using the **Filters** drop-down list.

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** > **Reports** > **Guest** > **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** > **Reports** > **Endpoints and Users** > **Registered Endpoints**. You can filter on attributes such as **Identity**, **Endpoint ID**, **Identity Group**, **Endpoint Profile** and you can generate a report.

You can query the endpoint database for endpoints that are assigned to the **Registered Devices** 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.