Supporting Personal Devices

This chapter provides information about allowing employees to use their personal devices on your corporate network.

This chapter contains the following sections:

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 and their devices. A Cisco ISE Advanced License provides the tools you need to allow employees to securely use personal devices on a corporate network.

Users have two ways of adding their personal devices to the network: using native supplicants 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 necessary supplicant provisioning wizard needed to set up the user's personal device to access the network. Native supplicant profiles are not available for all devices, but users can use the My Devices portal to add those devices manually.

Personal Devices Portals

Cisco ISE provides several web-based portals to support employee-owned personal devices.

Self-Provisioning Portal

Employees access the Self-Provisioning portal when registering personal devices using native supplicants. The first time employees attempt to access the network using a personal device, they will be guided automatically through registering and installing the supplicant. After they have registered a device, they can use the My Devices portal to manage it.

Related Topics

- Supporting Device Registration Using Native Supplicants, page 17-3

My Devices Portal

Some network devices are not supported by native supplicants. If the operating system is not supported or if the devices do not have web browsers (such as printers, Internet radios, and other devices), these devices still need to access the network. To add these types of devices to your company's network, employees need to use 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. The devices are profiled like any other endpoint in Cisco ISE and go through a registration process for network access.

When employees register their devices using the My Devices portal or during native supplicant provisioning, the Device Registration Status and BYOD Registration Status attributes in **Administration > Identity Management > Identities > Endpoints** are updated from NotRegistered and Unknown to Registered and Yes respectively. 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 user (who is not an employee) registers their device using the guest device registration page, because these are BYOD attributes used only during employee device registration.

Regardless of whether or not employees register their devices using the native supplicant or the My Devices portal, all employees can use the My Devices portal to manage their personal devices.

Related Topics

- Setting Up and Customizing End-User Web Portals, page 15-1
- Supporting the My Devices Portal, page 17-4
- Operating Systems Supported by Native Supplicants, page 17-3

Blacklist Portal

Employees can indicate whether they have lost a device, which adds it to the Blacklist endpoint identity group, which prevents others from using the device to obtain unauthorized network access. If users attempt to connect to the network using one of these devices, they are redirected to the Blacklist portal. If the device is found, employees can reinstate it and regain network access without having to register the device again.

You can configure the port settings (default is port 8444) for the Blacklist portal using the Admin portal. Employees do not access this portal directly.

Related Topics

- Setting Up and Customizing End-User Web Portals, page 15-1

Employee Accounts

When you add employees or contractors to Cisco ISE, you can authorize them to use personal devices on the network. Whether you have added them using external identity stores or created internal users, you can authorize them to use personal devices on your network.

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

Cisco ISE includes the Employee user identity group for internal users.

Related Topics

Adding Users, page 14-3

Supporting 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 that user's authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard needed 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 will be guided automatically through 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, page 17-3
- Allowing Employees to Register Personal Devices Using Native Supplicants, page 17-3

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, Vista, and XP

Allowing Employees to Register Personal Devices Using Native Supplicants

The self-provisioning flow enables employees to connect devices to the network directly using native supplicants, which are available for Windows, MacOS, iOS, and Android devices.

If you do not want to enable this feature, employees can still add personal devices using the My Devices portal. By default, this feature is disabled when upgrading and enabled when performing a fresh installation of Cisco ISE.

Before You Begin

You must create the native supplicant profiles.

Step 1 Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations.**

Step 2 Choose a portal and click **Edit**.

Step 3 Click **Operations**.

Step 4 Check **Enable Self-Provisioning Flow**.

Related Topics

- Creating Native Supplicant Profiles, page 22-25
- Configuring Personal Device Registration Behavior, page 22-26

Supporting the My Devices Portal

Employees can use the My Devices portal to register and manage their personal devices. The My Devices portal includes online help that provides employees with assistance in using the portal. However, there are several things you need to do to prepare the portal before employees can access it.

Related Topics

My Devices Portal, page 17-2

Specifying the Identity Store Sequence Used for Employee Authentication

To allow an employee to log into the My Devices portal, you must specify an identity store sequence. This sequence is used with the login credentials of an employee to authenticate and authorize the employee for access to the My Devices portal. Cisco ISE includes a default identity store sequence for employees: MyDevices_Portal_Sequence.

Step 1 Choose **Administration > Web Portal Management > Settings > My Devices > Authentication Source**.

Step 2 Choose an identity store sequence from the **Identity Store Sequence** drop-down list.

Step 3 Click **Save**.

Related Topics

- My Devices Portal Settings, page A-54
- Creating Identity Source Sequences, page 14-38

Enabling the My Devices Portal

By default, the My Devices portal is enabled. If you disable it, a customizable error message notifies users that the portal is unavailable when they attempt to go to the URL.

Step 1 Choose **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.

Step 2 Uncheck the **Enable My Devices Portal** check box.

Step 3 Click **Save**.

Related Topics

My Devices Portal Settings, page A-54

Implementing an Acceptable Use Policy for Employees

You can require employees to acknowledge an acceptable use policy when using the My Devices portal.

Customizing the Acceptable Use Policy for Employees

If you require employees to acknowledge an acceptable use policy, you must update the templates to reflect your company’s policy.

Step 1 Choose **Administration > Web Portal Management > Settings > My Devices > Language Template**.

Step 2 Click the language for which you want to apply the policy.

Step 3 Click **Configure Acceptable Use Policy Page** and update the title and text to follow your company’s policy.

Step 4 Click **Save**.

Related Topics

- Requiring an Acceptable Use Policy for Employees, page 17-5
- My Devices Portal Language Template Settings, page A-53

Requiring an Acceptable Use Policy for Employees

You can display an acceptable use policy on the login page and the device registration page of the My Devices portal.

Before You Begin

Update the Acceptable Use text with your company’s policy.

Step 1 Choose **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.

Step 2 Check the **Enable the Acceptable Use Policy Link** check box.

Step 3 Click **Save**.

Related Topics

- Customizing the Acceptable Use Policy for Employees, page 17-5
- My Devices Portal Settings, page A-54

Limiting the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 100 personal devices.

Step 1 Choose **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.

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

Step 3 Click **Save**.

Related Topics

My Devices Portal Settings, page A-54

Customizing Help Desk Contact Details

This setting allows you to customize the e-mail address and phone number associated with the Contact link on the login and main page of the My Devices portal.

Before You Begin

If you want to change the Contact link name, you need to update the name in the My Devices Language Template settings (**Administration > Web Portal Management > Settings > My Devices > Language Template > Configure Miscellaneous Items**).

Step 1 Choose **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.

Step 2 Enter the help desk contact information in the **Email Address** and **Phone Number** fields.

Step 3 Click **Save**.

Related Topics:

My Devices Portal Settings, page A-54

My Devices Portal Language Template Settings, page A-53

Managing Personal Devices Added by Employees

When an employee registers a device using a native supplicant or adds a device to the My Devices portal, 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.

Displaying 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 any devices registered by a specific user. By default, this field does not display so you must enable it first before searching by it.

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 assigned to that particular user.

Related Topics

Filtering Data on Listing Pages, page 2-8

Registered Endpoints Report

The Registered Endpoints report provides information about the endpoints that are registered through the device registration portal. (For information on supplicant provisioning statistics and related data, see Viewing Client Provisioning Reports, page 22-30.)

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

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

Step 1 Log into your Cisco ISE user interface.

Step 2 Choose **Operations > Reports > Catalog**.

Step 3 In the Reports navigation pane, click **My Devices**.

Step 4 Choose **Registered Endpoints**.

Step 5 Click **Run**.

You can run a query on the following: Users, MAC address of a registered device, identity group, endpoint policy, and generate a report.

Errors When Adding Devices to My Devices Portal

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

If employees are attempting to add a device that supports a native supplicant, recommend that they use that instead. That registration process will overwrite the original registration and switch ownership to the new user.

If the device is a MAC Authentication Bypass (MAB) device, such as a printer, then you must resolve ownership of the device, and if appropriate, remove the device from the endpoints database so that the new owner can successfully add the device.

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 their list of registered devices, but the device remains in the Cisco ISE endpoints database and display in the RegisteredDevices endpoint identity group. You can permanently delete the device from the Endpoints page (**Administration > Identity Management > Identities > Endpoints**).

Deployment Scenarios for Personal Devices Using Native Supplicants

The deployment flows to 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 device type by redirecting employees using a supported personal device to the Self-Provisioning portal to confirm their device information. At this point, the process diverges based on device type.

Employe Connects to Network

- Single SSID—Employee connects the device to the 802.1x SSID by entering the corporate username and password.
- Dual SSID—Employees connect to the open guest provisioning SSID, are redirected to the Guest portal, and enter theiruser credentials in the standard Guest portal.

Employee's Credentials are Authenticated

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

Device is Redirected to the Self-Provisioning Portal

The device is redirected to the Self-Provisioning portal. The device's MAC address is automatically pre-configured, but employees can verify and add a description..

Native Supplicant is Configured (MacOS, Windows, iOS)

The native supplicant is configured; the process varies by device.

- MacOS and Windows devices—user clicks on the **Register** button on the Self-Provisioning 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 iPad, which includes:
  - The issued certificate (if configured) embedded with the iPad's MAC address and employee's Active Directory username
  - A Wi-Fi supplicant profile that enforces the use of MSCHAPv2 or EAP-TLS for 802.1X authentication.
- Android devices—users are prompted to download the Cisco ISE prompts and routes employee to download the Cisco Network Setup Assistant from Google Play. After installing the app, the employee opens it, and starts 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 dot1x 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.