



## CHAPTER 22

# Device Access Management

---

This chapter describes customization of the My Devices Portal, and provides information on how enterprise users (employees) can bring in their smart devices into an enterprise network, by using a device registration portal. This portal allows users to register and manage their smart devices through a device registration process.

This chapter contains the following topics:

- [Overview, page 22-1](#)
- [Configuring the My Devices Portal, page 22-2](#)
- [Using the My Devices Portal, page 22-11](#)
- [Managing Devices Added to the My Devices Portal, page 22-14](#)

## Overview

Cisco ISE allows enterprise users (employees) who wish to adopt the capabilities of their feature-rich smart devices to bring in these devices into an enterprise network. These smart devices allow users to communicate and collaborate on the network with high-speed Wi-Fi connectivity, social networking, and other capabilities.

However, adopting these smart devices into an enterprise network for user demands, and protecting network services and enterprise data between an enterprise and user is highly challenging, as these devices have to be properly configured on the network and managed for security. Given the increase in untrusted employee-owned smart devices that request network access, you must ensure that both the employees and their devices are authenticated and authorized for network access.

You might be able to connect your laptop, mobile phone, tablet, printer, and other network devices on your enterprise network, depending on your enterprise policy. You can use a web browser that is installed on your device to log into your enterprise network, and register the device. Once you have registered your devices, you can manage them in the My Devices Portal. If your device does not have web browser support, you must use the MAC address of the device, and add it in the My Devices Portal. The MAC address is the unique device identifier for these devices.

The My Devices Portal allows you to add a device in the portal, where the device goes through a registration process for network access. You can mark as lost any device that you have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device in your absence. You can reinstate a blacklisted device to its previous status in the My Devices Portal, and regain network access without having to register the device again in the My Devices Portal. You can also remove any device in your enterprise network temporarily, then register the device for network access again later.

The My Devices Portal is a standalone portal, which requires employee authentication to log into the portal. The portal allows employees to initiate their smart devices on the network, which displays those devices that they added through the My Devices Portal. You 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. Any attempt to add the same device in the My Devices Portal will fail, and the portal will display the following error message: “Device ID already exists. Please try again.”

We recommend that you register your devices such as laptop and mobile phone through the Guest portal, so that the device appears in your list. In this way, you declare ownership of the device by using your login credentials. This allows you to overwrite the PortalUser property of the device when, for instance, another employee has already added the device through the My Devices Portal using the MAC address. If the device is a Mac Authentication Bypass (MAB) device, such as a printer, then the device must be removed from the other employee’s list, so that you can add the device to your list. For MAB devices, your system administrator must find the other owner of the device; and remove ownership before you can add the device to your list.

Cisco ISE adds devices to the Endpoints page when you add devices in the My Devices Portal, and these are profiled like any other endpoint in Cisco ISE. The device registration portal sets attributes for these endpoints for profiling and supplicant provisioning. These attributes include the endpoint identity group, device registration status, product, device name, operating system version, unique device identifier (UDID) for iPads and iPhones (UDID), certificate serial number, and certificate issuer name, in addition to other attributes that are collected for the endpoints.

## Employee User Identity Group

Employees are network access users that you create and assign to the Employee user identity group in Cisco ISE.

The Employee user identity group is a default network access user identity group for employees. You can create, and assign users to this group. The description of the Employee user identity group is editable, and you can add or delete employees in the Employee user identity group.

For information on user identity groups, see the Configuring User Identity Groups section in the [Cisco Identity Services Engine User Guide, Release 1.1.x](#).

# Configuring the My Devices Portal

You can use the Settings navigation pane to configure the My Devices Portal from the Web Portal Management menu of the Cisco ISE administrator user interface, which is found under:

Administration > Web Portal Management > Settings.

This section contains the following topics:

- [General Settings, page 22-3](#)
- [My Devices Portal Settings, page 22-6](#)
- [Connecting to the My Devices Portal, page 22-11](#)
- [Registering, Editing, Reinstating, and Deleting a New Device, page 22-12](#)
- [Registered Endpoints Report, page 22-15](#)

## General Settings

You can customize the portal theme for the My Devices Portal, configure the port, and specify the default URL that you can use to access the My Devices Portal over Secure Socket Layer (SSL).

This section contains the following topics:

- [Customizing the Portal Theme, page 22-3](#)
- [Setting Ports for the My Devices Portal, page 22-5](#)
- [Specifying a Simple URL for the My Devices Portal, page 22-5](#)

## Customizing the Portal Theme

You can customize a portal theme by changing text, banners, background color, and images for the My Devices Portal by setting and applying customized options. This functionality allows you to change the appearance of the portal without having to upload customized HTML files to the Cisco ISE server. You can follow the same steps to modify an existing customized portal theme.

**Note**

Supported image formats include JPG, JPEG, GIF, and PNG.

**To customize a portal theme for the My Devices Portal, complete the following steps:**

- Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.
- Step 2** In the Settings navigation pane, click the arrow next to General, and choose **Portal Theme**. The Portal Theme page appears.
- Step 3** Customize the following for the My Devices Portal:
- Login Page Logo—See Step 4.
  - Login Page Background Image—See Step 5.

**Note**

The login page background image always overrides the login background color, unless the background image is transparent. For example, the default login page background image overrides the login background color default setting (66aaff) or the login background color that you have defined, as described in Step 8.

- Banner Logo—See Step 6.
- Banner Background Image—See Step 7.

**Note**

The banner background image always overrides the banner background color, unless the background image is transparent. For example, the default banner background image overrides the banner background color default setting (66aaff) or the banner background color that you have defined, as described in step 9.

- Login Background Color— See Step 8.
- Banner Background Color—See Step 9.

- Banner Text Color—See Step 10.




---

**Note** The Banner Text Color field applies only to the My Devices Portal.

---

- Banner Link Color—See Step 11.




---

**Note** The Banner Link Color field applies only to the My Devices Portal.

---

- Content Background Color—See step 12.

**Step 4** Select **Upload New File** from the Login Page Logo drop-down list, and click **Browse** to locate the image file and upload the login page logo.

You can use the default Cisco logo, or upload a custom image. When you upload an image, it is automatically resized to fit an image size of 46 pixels (height) by 86 pixels (width). To avoid distortion, resize your image to fit these dimensions.

**Step 5** Select **Upload New File** from the Login Page Background Image drop-down list, and click **Browse** to locate the image file and upload the login page background image.

You can use the default Cisco background, or upload a custom login background image.

**Step 6** Select **Upload New File** from the Banner Logo drop-down list, and click **Browse** to locate the image file, and upload the login banner logo.

You can use the default Cisco login banner, or upload a custom login banner logo. When you upload the image, it is automatically resized to fit an image size of 46 pixels (height) by 86 pixels (width). To avoid distortion, resize your image to fit these dimensions.

**Step 7** Select **Upload New File** from the Login Banner Background Image drop-down list, and click **Browse** to locate the image file, and upload the login banner background image.




---

**Note** Click **Use Uploaded Image** if you want to use an image that was previously uploaded and is available from the location.

---

You can use the default Cisco login banner, or upload a custom login banner background image.




---

**Note** Each pair of hexadecimal digits expresses an RGB (Red Green Blue) value from 0–255.

---

**Step 8** Enter the color value as an RGB hexadecimal value in HTML color format to set the login page background color.

You can use the factory default, or customize the color. Click **Show Color** to display the color that you define in the Login Background Color field.

**Step 9** Enter the color value as an RGB hexadecimal value in HTML color format to set the banner background color.

You can use the factory default, or customize the color. Click **Show Color** to display the color that you define in the Banner Background Color field.

**Step 10** Enter the color value as an RGB hexadecimal value in HTML color format to set the color for text that you want to use in the banner.

You can use the factory default, or customize the color. Click **Show Color** to display the color that you define in the Banner Text Color field.

For example, the Welcome Text appears in the specified color in the banner.

- Step 11** Enter the color value as an RGB hexadecimal value in HTML color format to set the color for links that you want to use in the banner.

You can use the factory default, or customize the color. Click **Show Color** to display the color that you define in the Banner Link Color field.

For example, the Sign Out link appears in the specified color in the banner.

- Step 12** Enter the color value as an RGB hexadecimal value in HTML color format to set the background color for content.

You can use the factory default, or customize the color. Click **Show Color** to display the color that you define in the Content Background Color field.

- Step 13** Click **Save** to save the changes that you made, or click **Reset** if you do not want to save the changes you made, and you want to restore the previous settings.

- Step 14** Click **Restore to Factory Defaults** to load the Cisco ISE default settings for the My Devices Portal.
- 

## Setting Ports for the My Devices Portal

Employees can get connected to the My Devices Portal through a web interface over HTTPS. The default setting for the My Devices Portal is HTTPS on port 8443.

**To configure the port number for the My Devices Portal, complete the following steps:**

- 
- Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.
- Step 2** In the Settings navigation pane, click the arrow next to General, and choose **Ports**.  
The Guest/Sponsor SSL Settings page appears.
- Step 3** Assign a port number for the My Devices Portal in the My Devices Portal Settings field. Port 8443 is the default, and the valid range for ports is 1 to 65535.
- Step 4** Click **Save**.
- 

### Accessing the My Devices Portal

To access the My Devices Portal, enter the following URL, substituting the IP address variable with the IP address of the Cisco ISE server:

```
https://ip_address:port/mydevices/
```

## Specifying a Simple URL for the My Devices Portal

You can specify a fully qualified domain name (FQDN) URL so that it automatically resolves to the My Devices Portal on a given node in a deployment.

For example, you can set `https://mydevices.company.com` so that it resolves to the My Devices Portal.

**Caution**

Making a change to the ports or FQDN value restarts all the nodes in the deployment that will configure the web server on each node.

**To specify an FQDN URL to the My Devices Portal, complete the following steps:**

- 
- Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.
- Step 2** In the Settings navigation pane, click the arrow next to General, and choose **Ports**.  
The Guest/Sponsor SSL Settings page appears.
- Step 3** Select the **Default My Devices Portal URL** check box under Portal URLs, and enter a fully qualified domain name URL in the text field, such as: mydevices.yourcompany.com
- Step 4** Click **Save**.  
All the nodes in the deployment restart that will configure the web server on each node.

**Note**

You must configure the network Domain Name System (DNS) server so that it resolves the FQDN to the Cisco ISE My Devices Portal node.

**Related Topics:**

[My Devices Portal Settings, page 22-6](#)

[Connecting to the My Devices Portal, page 22-11](#)

[Registering, Editing, Reinstating, and Deleting a New Device, page 22-12](#)

## My Devices Portal Settings

This section includes information on configuring an identity store sequence for authentication, language templates for customization of the My Devices Portal, and portal configuration that enables the My Devices Portal.

- [Authentication Sequence, page 22-6](#)
- [Language Templates, page 22-7](#)
- [Portal Configuration, page 22-10](#)

## Authentication Sequence

You can configure the authentication source, an identity store sequence, which is used with the login credentials of an employee to authenticate and authorize an employee to log into the My Devices Portal.

To allow an employee to log into the My Devices Portal, you have to choose 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. The sequence can include external stores, as well as the local Cisco ISE identity store. The identity store sequence defines which stores should be accessed and in what order they should be accessed to resolve the authentication of an employee.

To set the identity store sequence for an employee authentication, complete the following steps:

- 
- Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.
  - Step 2** In the Settings navigation pane, click the arrow next to My Devices, and choose **Authentication Source**.
  - Step 3** From the Identity Store Sequence drop-down list, choose the identity store sequence to be used for an employee authentication from the Identity Sequence widget that appears.  
For example: MyDevices\_Portal\_Sequence.
  - Step 4** Click **Save**.
- 

## Language Templates

All the Cisco ISE supported language templates are active by default for a given browser locale. You are allowed to add new language templates or edit and duplicate existing templates. A lock is set for all the supported language templates in Cisco ISE, which indicates that you are not allowed to delete supported language templates. You have the option of modifying a standard language template, or creating a custom template for the My Devices Portal user interface.

To add a custom language template, complete the following steps:

- 
- Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.
  - Step 2** In the Settings navigation pane, click the arrow next to My Devices, and click **Language Templates**.  
The My Devices Portal Language Templates page lists standard language templates that are supported and newly created templates.
  - Step 3** Click **Add** to create a new language template.
  - Step 4** Click **Configure Template Definition**, and enter a unique name and description in the Name and Description text boxes for the language template, followed by a valid locale in the Browser Locale Mapping text box.



**Note** You are not allowed to create a new language template that uses the same browser locale mapping as an existing language template. Each language template must use a unique browser locale mapping.

---

- Step 5** Click **Configure Login Page**, and enter the captions in the text boxes.  
The Configure Login Page allows you to configure captions for the following text boxes for a specific locale, which appear in the login page of the My Devices Portal: Username Field, Password Field, and the Login Button.
- Step 6** Click **Configure Device Management Page**, and enter captions in the text boxes.  
The Configure Device Management Page allows you to configure captions for the following text boxes for a specific locale, which appear in the devices registration page of the My Devices Portal: Page Title, Page Description, MAC Address Field, Description Field, Submit Button, Cancel Button, Table Title,

State Column, MAC Address Column, Description Column, Action Column, Edit Action, Blacklist Action, Reinstate Action, Delete Action, Save Action, Cancel Action, Unknown Status (Not Registered), Pending Status, Registered Status, and Blacklisted Status.



**Note** The user who is logging into the network can enter only a maximum of 256 characters in the Page Description text box.

**Step 7** Click **Configure Acceptable Use Policy Page**, and enter a caption for the Acceptable Use Policy (AUP) title, and configure the AUP text.

The Configure Acceptable Use Policy Page allows you to configure the caption for the AUP Title and AUP for a specific locale, which appear in both the login page and the device registration page of the My Devices Portal.

**Step 8** Click **Configure Info/Error Messages**, and configure the responses that the My Devices Portal prompts to the user.

The Configure Information/Error Messages page allows you to configure the responses that provide information, and to guide users in the actions that they perform on the My Devices Portal.

**Step 9** Click **Configure Miscellaneous Items**, and configure the captions for the following miscellaneous items for a specific locale, which appear in the My Devices Portal.

The Configure Miscellaneous Items page allows you to configure the captions for the following text boxes for a specific locale for the My Devices Portal: Product Name, Portal Name, Contact Link, Online Help Link, Logout Link, Welcome Text, Server Response, Help Desk Title, Help Desk Email Address Field, Help Desk Phone Number Field, Yes Button, No Button, and Ok Button.

**Step 10** Click **Configure the Blackhole Portal Items**, and configure the My Devices Portal to respond to the blacklisted devices during log in.

The Configure the Blackhole Portal Items page allows you to configure the captions for the following text boxes for a specific locale, which appear in the portal for blacklisted devices: Blackhole Portal Name and Blackhole Message.

**Step 11** Click **Submit**.

---

**To edit and duplicate a language template, complete the following steps:**

**Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.

**Step 2** In the Settings navigation pane, click the arrow next to My Devices, and click **Language Templates**.

The My Devices Portal Language Templates page lists the language templates that are supported in Cisco ISE and newly created templates.

**Step 3** Select a language template from the list in the My Devices Portal Language Templates page.

- Click **Edit** to modify the description and the locale in the Configure Template Definition page. You can also configure Configure Login Page, Configure Device Management Page, Configure Acceptable Use Policy Page, Configure Info/Error Messages, Configure Miscellaneous Items, and Configure Blackhole Portal Items for a specific language template.



- Click **Duplicate** to enter a unique name and description for the language template, followed by a valid locale in the Configure Template Definition page. You can also configure Configure Login Page, Configure Device Management Page, Configure Acceptable Use Policy Page, Configure Info/Error Messages, Configure Miscellaneous Items, and Configure Blackhole Portal Items for the language template.

**Step 4** Click **Submit**.

---

**To filter language templates, complete the following steps:**

---

**Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.

**Step 2** In the Settings navigation pane, click the arrow next to My Devices, and click **Language Templates**. The My Devices Portal Language Templates page lists all the language templates that are supported in Cisco ISE and newly created templates.

**Step 3** In the My Devices Portal Language Templates page, click the Show drop-down list to choose the filter options.

You can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering.

**Step 4** Click the Show drop-down list, and click **Quick Filter** or click the filter icon to invoke the quick filter.

A quick filter filters language templates based on each field description in the My Devices Portal Language Templates page. When you click inside any field, and as you enter the search criteria in the field, the quick filter refreshes the My Devices Portal Language Templates page with the results in the Endpoint Policies page. If you clear the field, the quick filter displays the list of all the language templates in the My Devices Portal Language Templates page.

- Click **Go** within each field to filter, and refresh the My Devices Portal Language Templates page with the results.
- Click **Clear** within each field to clear the field.

**Step 5** Click the Show drop-down list, and click **Advanced Filter**.

An advanced filter enables you to filter language templates by using variables that are more complex. It contains one or more filters that filter language templates based on the values that match the field descriptions. A filter on a single row filters language templates based on each field description and the value that you define in the filter. Multiple filters can be used to match the values and filter profiling policies by using any one or all of the filters within a single advanced filter.

- To choose the field description, click the drop-down arrow.
- To choose the operator, click the drop-down arrow.
- Enter the value for the field description that you selected.
- Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.
- Click **Go** to start filtering.
- Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save** or click **Cancel** to clear the filter. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

- Click **Clear Filter** after filtering.

**Note**

To return to the My Devices Portal Language Templates list, choose **All** from the Show drop-down list to display all the language templates without filtering.

**Step 6** Click the Show drop-down list, and click **Manage Preset Filters**.

The Manage Preset Filters dialog appears, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results in the My Devices Portal Language Templates page. Once you have created and saved a preset filter, you can choose a preset filter from the list. You can also edit preset filters and remove them from the preset filters list.

- Click the Select a filter drop-down list, and select a preset filter that you have already saved.
- Click **Edit** to change preset filter criteria, and save the filter as new.
- Click **Remove** to remove the preset filter from the list.
- Click **Cancel** to close the Manage Preset Filters dialog.

## Portal Configuration

You can configure the My Devices Portal in the My Devices Portal Settings page from the Cisco ISE administrator user interface, which allows an employee to access the My Devices Portal.

The My Devices Portal Settings page contains the following: settings that enable the My Devices Portal through the web user interface over HTTPS, links that allow the user to accept the Acceptable Use Policy page and the Help Desk page in the My Devices Portal, and the number of devices that the user can register through the My Devices Portal.

**To configure the My Devices Portal, complete the following steps:**

**Step 1** From the Cisco ISE administrator user interface, choose **Administration > Web Portal Management > Settings**.

**Step 2** In the Settings navigation menu, click the arrow next to My Devices, and click **Portal Configuration**.  
The My Devices Portal Settings page appears.

**Step 3** Select the **Enable My Devices Portal** check box, which allows an employee to access the My Devices Portal. By default, this setting is enabled in Cisco ISE.

**Note**

If you have disabled the Enable My Devices Portal check box, your attempt to log into the My Devices Portal displays the following message: “The My Devices Portal Service is not available.”

**Step 4** Select the **Enable the Acceptable Use Policy Link** check box, which displays an Acceptable Use Policy link on both the login page and the device registration page of the My Devices Portal.

**Note**

If you enable Acceptable Use Policy (AUP) in the My Devices Portal Settings page, then you must set the AUP text in the Configure Acceptable Use Policy Page for all the language templates.

**Step 5** In the text box for **Device Management**, enter the maximum number of smart devices that an employee can register and manage in the My Devices Portal.

The maximum number of smart devices that you can register is 20, as the valid range that can be configured in this field is between 1 and 20. By default, the number of devices that you can register is set to 5 devices in Cisco ISE.

**Step 6** Enter the help desk contact information in the My Devices Portal Settings page.

Help Desk:

- Email Address
- Phone Number

This setting allows you to display the help desk information from the Contact link on both the login page and the device registration page of the My Devices Portal.

---

**Related Topics:**

[General Settings, page 22-3](#)

[Connecting to the My Devices Portal, page 22-11](#)

[Registering, Editing, Reinstating, and Deleting a New Device, page 22-12](#)

## Using the My Devices Portal

Employees access the My Devices portal to register and manage their personal devices. These sections provide details about using this portal:

- [Connecting to the My Devices Portal, page 22-11](#)
- [Registering, Editing, Reinstating, and Deleting a New Device, page 22-12](#)

## Connecting to the My Devices Portal

You can open a web browser and get connected to the My Devices Portal through the web user interface over HTTPS.

To connect to the My Devices Portal, enter the URL as provided by your network administrator.

---

**Step 1** Enter the My Devices Portal URL in the web browser, for example, `https://ip_address:port/mydevices`. The port number is configurable in the Cisco ISE administrator user interface.



---

**Note** The default port for the My Devices Portal is 8443.

---

**Step 2** Click **Acceptable Use Policy**.

The My Devices Portal displays the Acceptable Use Policy page on the login page, as well as the device registration page for a specific locale from the language template.

For example, the Acceptable Use Policy appears in English that you have configured in the following location: Administration > Web Portal Management > Settings > My Devices > Language Template > English > Configure Acceptable Use Policy Page in Cisco ISE.

**Step 3** Click **Contact**.

The My Devices Portal displays the Help Desk window on both the login page, as well as the device registration page for a specific locale.

For example, the Help Desk window appears in English that you have configured in the following location: Administration > Web Portal Management > Settings > My Devices > Portal Configuration in Cisco ISE.

**Step 4** Enter your employee username and password in the My Devices Portal login page, and click **Login**.

Use the employee login credentials that were created by your network administrator in the New Network Access User page in Cisco ISE.

The portal device registration page is a single page that displays devices that are added only by you. You cannot view devices that are added by other users. The device registration page title is configurable in Cisco ISE in the following location:

Administration > Web Portal Management > Settings > My Devices > Language Template > English > Configure Device Management Page > Page Title.

For example, the Add a New Device page appears in the My Devices Portal.

**Step 5** Click **Sign Out** to log out of from the My Devices Portal.**Related Topics**

[Registering, Editing, Reinstating, and Deleting a New Device, page 22-12](#)

## Registering, Editing, Reinstating, and Deleting a New Device

You can connect to the My Devices Portal through the web user interface over HTTPS.

**Step 1** Enter the My Devices Portal URL in the web browser.

For example, you might enter https://ip\_address:port/mydevices. Enter the IP address of the Cisco ISE server, along with the port number that you have configured for the My Devices Portal.

**Step 2** Enter your employee username and password in the My Devices Portal login page, and click **Login**.

You can use the network access user login credentials of an employee to log into the My Devices Portal.

The device registration page appears with the page title that you have configured in the following location: Administration > Web Portal Management > Settings > My Devices > Language Template > English > Configure Device Management Page > Page Title.

For example, the Add a New Device is the device registration page that allows you to add devices in the My Devices Portal.

**Figure 22-1 Adding a New Device in the My Devices Portal**

302147

**Step 3** Enter the MAC address of the device that you want to add in the My Devices Portal.



**Note** The MAC Address of the device is not editable after you have added the device into the My Devices Portal.




**Step 4** Enter the description of the device. (The user who is logging into the network can enter only a maximum of 256 characters in the Description text box.)

**Step 5** Click **Submit**.

You can view in a table all the devices that you have added in the My Devices Portal. The table title is configurable from the Configure Device Management Page for a specific locale. This table provides you the status of all the devices and allows you to edit the description of the devices, reinstate the devices and delete the devices from the network.

For example, Your Devices is a table that displays all the devices that you add in the My Devices Portal, which allows you to edit the description of the devices, reinstate the devices and delete the devices.

Icons represent the status of the devices, such as Pending, Registered, and Blacklisted in the device registration page.

- —The status appears pending when you add a device in the My Devices Portal.
- —The status appears registered when you connect the device to an enterprise network, and the device is provisioned with a supplicant and authorized to access the network.
- —The status appears blacklisted when you mark the device in the My Devices Portal as lost. You can reinstate the device to its previous the status by registering it again through the My Devices Portal that allows the device to access the network.



**Note** You can find the PortalUser and DeviceRegistrationStatus attributes of the devices in the attributes list in Cisco ISE that you have added in the My Devices Portal.

**Step 6** In the device registration page, click **Edit**.

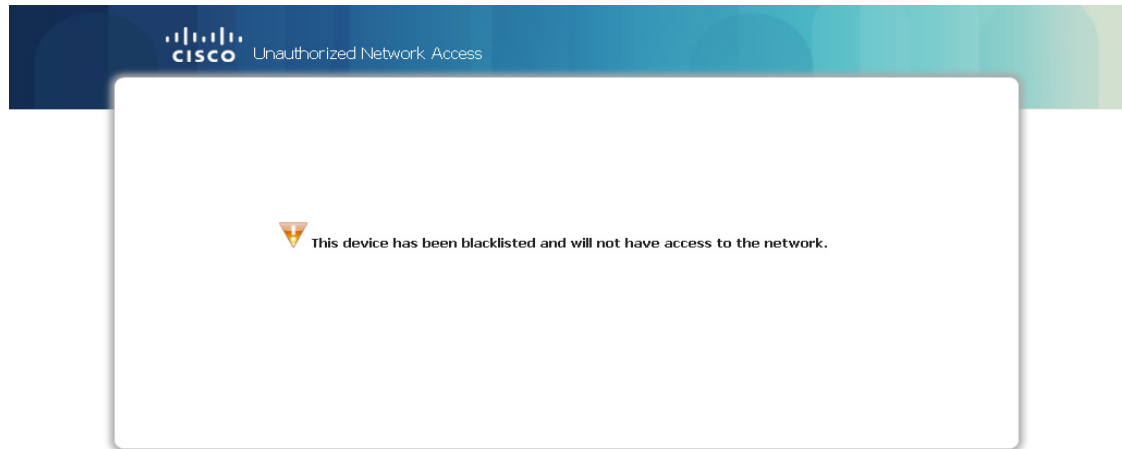
You can edit only the description of the device; the MAC address of the device is not editable. (The user who is logging into the network can enter only a maximum of 256 characters in the Description text box).

**Step 7** In the device registration page, click **Lost?**.

When you mark the device in the My Devices Portal as lost, the portal blacklists the device until the device is reinstated again through the My Devices Portal.

You will see the following default portal page when you access the network with devices that are blacklisted in the device registration portal.

**Figure 22-2** *Unauthorized Network Access to a Blacklisted Device*



**Step 8** In the device registration page, click **Reinstate** for the device in the My Devices Portal to allow the device to resume network access.

When you reinstate the blacklisted device in the My Devices Portal, the device returns to its previous state, such as Registered or Pending, as it was before it was blacklisted.

**Step 9** Click  to delete the device.

Deleting removes a device from the portal until the device is registered again in the My Devices Portal, but such devices exist as endpoints in the Cisco ISE endpoints database. If you delete endpoints in the RegisteredDevices endpoint identity group in Cisco ISE, then those devices are removed from the My Devices Portal.

## Managing Devices Added to the My Devices Portal

When an employee 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.

These sections provide you with tips for managing these devices:

- [Displaying Devices Added by Employees, page 22-15](#)
- [Registered Endpoints Report, page 22-15](#)

## Displaying Devices Added by Employees

You can locate devices added by employees using the Portal User field displayed on the Endpoints listing page. 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.
- 

## Registered Endpoints Report

The Registered Endpoints Report in Cisco ISE 1.1.x 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 in Cisco ISE, page 19-48](#).)

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.

This report provides the following information:

- Logged in Date and Time
- Portal User (who registered the device)
- MAC Address
- Identity Group
- Endpoint Policy
- Static Assignment
- Static Group Assignment
- Endpoint Policy ID
- NMAP Subnet Scan ID
- Device Registration Status

**Note**

When you register a device in the My Devices Portal, the device moves to the “Pending” state. After posture assessment, the device moves to the “Registered” or “Not Registered” state. The Registered Endpoints report does not list the devices that are in the “Not Registered” state. However, you can view these devices in the My Devices Portal.

---

To run the Registered Endpoints Report, complete the following steps:

- 
- 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**.

The Registered Endpoints Report appears on your screen.

You can use the Run drop-down list to generate the report for a specified period of time and for the following time periods:

- Last 30 Minutes
- Last Hour
- Last 12 Hours
- Today
- Yesterday
- Last 7 days
- Last 30 days

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

---