

Frequently Asked Questions



My Devices Portal FAQs

[My Devices FAQ](#) 2

[Additional References](#) 4

[Communications, Services, and Additional Information](#) 4

[Full Cisco Trademarks with Software License](#) ?

My Devices FAQ

My Devices Portal

Q. Why do I need to use the My Devices Portal?

A. Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network.

When you use a laptop computer, mobile phone, or tablet to access the Internet, you typically use a web browser on the device itself. The first time you try to do so using your company's network, the system will automatically guide you through registering and installing the required software. You may not need to use the My Devices Portal to register those types of devices. However, once you register them, you can use the My Devices Portal to perform operations such as remove them, mark them as lost, or reinstate devices that were marked as lost, once they are found.

Other network devices do not have web browsers on them because they need access to the network only to allow you to perform activities such as listen to music, print documents, and watch videos. If you want to add these types of devices to your company's network, you need to use the My Devices portal.

Q. Why do I see different types of information display for Device ID?

A. When you add a personal device, it displays on the **Manage Devices** page and is listed according to the device ID you entered when registering the device. However, devices often have multiple device IDs (for example, a different value for wired and wireless connections). In this case, a device with multiple MAC addresses will display its host name for the device ID.

Adding New Devices

Q. Where do I find the device ID?

A. It depends on your device. All network-ready devices have a unique identifier that makes sure that all network communication goes to the right device. This identifier is typically called a MAC address, Wi-Fi address, or network address. It includes six pairs of alphanumeric characters separated by hyphens, such as: 00-01-0b-42-8f-82. Check the documentation for the device you are adding or request assistance from your help desk.

Q. I just added a device. Why does it display as Pending?

A. A status of **Pending** indicates that the device is still not provisioned. It may take up to twenty minutes for the provisioning process, which prepares the device to gain network access, to complete. After it connects to the network and it is registered in Cisco ISE, the status changes to **Registered**.

Q. When I try to add a device, I get an error that says that the device already exists, but I do not see it listed as one of my devices. How can I add this device?

A. That error means that someone has already added the device to the system. If it does not appear on your list, one of your coworkers has registered the device already.

You have several options for resolving this situation:

- If you are attempting to add a device such as a printer, you will need to contact your help desk to locate the current owner and to resolve this issue for you.

- Regardless of the device type, you can contact your help desk so that they can verify who registered the device previously and delete it from the database so you can re-register it.

- Q.** When I try to add another device, I get an error telling me I have already reached the maximum number of devices. How can I add this device?
- A.** Your system administrator determines the number of devices each person can add to the network. If you have reached that limit, you need to delete a device before adding a new one.
- Q.** I made a mistake entering the ID for my device. How can I change it?
- A.** You can only **Edit** the Description of the device. If you want to change the Device Name or the Device ID, you should **Delete** the device first and then **Add** it back into the portal.

Removing Lost, Stolen and Unused Devices

- Q.** What do I do if I lose one of my devices?
- A.** You should first contact your help desk to verify your company's policies. To immediately prevent anyone who finds the device from accessing your company's network, select the device on the list and click **Lost**. When you identify a device as lost, the system prevents the device from connecting to the network and changes its status from **Registered** to **Lost**. In addition, if this device is enrolled in the Mobile Device Management (MDM) system, you can unenroll it.
- Q.** I've recently found a lost device. How do I get it back on the network?
- A.** You should first contact your help desk to verify your company's policies. To allow the device to access the network again, select the device on the list and click **Reinstate**. The next time you try to connect to the network with your reinstated device, your device will go through the BYOD provisioning process again.
- Q.** What do I do if one of my devices is stolen?
- A.** You should first contact your help desk to verify your company's policies. To immediately prevent the stolen device from accessing your company's network, select the device on the list and click **Stolen**. When you identify a device as stolen, the system prevents the device from connecting to the network and changes its status from **Registered** to **Stolen**.
- Q.** How can I get a stolen device that has been returned to me back on the network?
- A.** You should first contact your help desk to verify your company's policies. To allow the stolen device to access the network again, select the device on the list and click **Reinstate**. The reinstated device displays as **Not Registered** and has to be provisioned before it can connect to the network. The next time you try to connect to the network with your reinstated device, your device will go through the BYOD provisioning process again.
- Q.** How do I delete a device that I'm not using anymore?
- A.** Select the device on the list and click **Delete**. Click **Refresh** to view any updates to the list.

Managing Mobile Devices

- Q.** What is the difference between **Full Wipe** and **Unenroll**?
- A.** These options are available only if your company has integrated the My Devices portal with an MDM system that supports these features. Many companies use an MDM system to manage employees' mobile devices. Choose the appropriate option:
- **Full Wipe** resets your mobile device to its default factory settings, removing installed apps and data. You might choose this option if you have lost your device or are replacing it with a new one.
 - **Unenroll** removes only those applications and settings installed by your company. Your other apps and data remain installed on your device. You might choose this option if you no longer need to use the device at work.



Note If you enrolled your device into the MDM system to access departmental applications, you will lose access to these applications once you unenroll your device.

- Q.** What is the difference between choosing PIN Lock on the My Devices portal or doing it directly from my device?
- A.** PIN Lock is available only if your company has integrated with an MDM system and if this feature is supported by your MDM system and mobile device.

Mobile devices typically include a locking feature that enables you to lock your screen after a set time period to prevent unauthorized access. To use this feature, you must define an access code, or PIN, which is required to unlock the device. If you do not enable this locking feature on your mobile device, you cannot lock your device using PIN Lock from the My Devices Portal.

If this feature is enabled, you can use the PIN Lock feature from the My Devices portal to immediately lock your phone remotely. So, if you lose the device, you can prevent others from using it. However, you cannot set your PIN from the My Devices portal; you must set a PIN on your mobile device in advance to use this feature.

Additional References

The following link contains additional resources that you can use when working with Cisco ISE: https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit [Cisco DevNet](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.