



Mobile Application User Guide for Cisco Network Plug and Play

First Published: 2015-10-30

Last Updated: 2016-2-25



The Cisco Network Plug and Play mobile application helps you deploy Cisco network devices using the Cisco Network Plug and Play Solution.

For more detailed information about the solution, see the [Solution Guide for Cisco Network Plug and Play](#).

Set Up Server Address

You must set up the Cisco Network Plug and Play mobile app with the Cisco APIC-EM controller IP address before using it to deploy devices.

1. Tap **Settings** on the main menu.
2. In the Server URL field, enter the IP address of the APIC-EM controller.
3. In the Username and Password fields, enter the username and password credentials for a user account configured with the Installer role. Get this information from the APIC-EM controller administrator.
4. Tap **Test Connection** to test the APIC-EM controller connection and show the status.
5. If the connection is successful, tap **Save** in the upper right corner, then **Done** in the upper left corner, to return to the main screen.

An icon at the top right side of the main menu shows with a green check mark  if the server connection is good or a red X  if there is no connectivity. While connecting, the icon is orange.

The mobile app must be able to connect through 3G, 4G, or WiFi to the Cisco Network Plug and Play application to download device bootstrap configurations.

Deploy Devices

Deploying a device means to deliver a bootstrap configuration file to the network device. The device then contacts the Cisco Network Plug and Play application, which completes device configuration automatically.

1. Use the special serial console cable to connect your mobile device to the Cisco network device console port.

The following console cable is needed, depending on whether your mobile device is an iOS or Android device:



- iOS device: Redpark Lightning Console Cable ([L2-RJ45V](#)), for iOS devices with the Lightning (8-pin) connector, or Redpark Console Cable ([C2-RJ45V](#)), for iOS devices with the older 30-pin connector.
- Android device: [Airconsole bluetooth adapter](#)

View Deployment Status

2. Tap **Deploy Devices** on the main menu.
3. Select a Site.
4. If the network administrator has preconfigured the device serial number, deployment starts automatically.
5. If deployment does not start automatically, select the device from the Devices list and then tap **Deploy Bootstrap**.

If there is no bootstrap configuration defined for the device, the device deployment status is displayed and you will not see the Deploy Bootstrap button.

To view any installation notes that the network administrator has set for you, tap **Notes**, below the device list.

An icon at the top left side of the main menu shows with a green check mark  if the device connection is good or a red X  if there is no connectivity. While connecting, the icon is orange.

Note: After disconnecting the console cable from the network device, if you want to connect it to a different network device, you must first manually refresh the mobile app to reflect the correct status when connecting to the new device.

IMPORTANT: If you have an iOS mobile device with a Redpark cable and are deploying multiple network devices, after you are done with one device, you must unplug the Redpark cable from both your mobile device and the network device to close the serial connection. If you do not disconnect the cable from your mobile device, the serial session is not closed and the wrong configuration could be deployed on the next device.

Note: This function is not supported for Cisco wireless access point devices.

View Deployment Status

You can view deployment status for any pre-provisioned device from the Cisco Network Plug and Play application. A console cable does not need to be connected to a device, as the status comes from the server.

1. Tap **Deployment Status** on the main menu.
2. Tap **Site Provisioning** at the top.
3. Select a site to see the deployed and pending devices for the site.
4. Select a device to see details.

The mobile app displays the device details, provisioning status, and history of provisioning operations.

To see unplanned device status, follow these steps:

1. Tap **New/Unclaimed** Devices at the top.
2. Select a time range to see devices added within the selected period.

Note: This function is not supported for Cisco wireless access point devices.

Register Device Serial Numbers

You can register device serial numbers with the Cisco Network Plug and Play application without deploying the devices.

1. Tap **Register Device** on the main menu.
2. Tap **Scan for Serial Barcode** and then hold the mobile device camera about three inches from the network device barcode and tap the scanning screen to read the barcode. The camera must have a resolution of 3 megapixels or better.

Troubleshooting

3. If you are unable to scan the device barcode, you can enter the device serial number manually and tap **Register Device**.

Troubleshooting

You can do the following troubleshooting operations:

- Check the status of the Cisco Plug and Play IOS Agent
- Check the status of the APIC-EM controller connection
- Use the mobile app as a terminal console to enter device CLI commands
- Perform a factory reset on the device
- View and email log files

Checking the Status of the Cisco Plug and Play IOS Agent

Ensure that your mobile device is connected to the Cisco network device with the special serial console cable.

1. Tap **Troubleshooting** on the main menu.
2. Tap **Check Agent Status**.
3. Tap **View Current Status**.

Checking the Status of the APIC-EM Controller Connection

1. Tap **Troubleshooting** on the main menu.
2. Tap **Check Ping Server Status**.

Entering CLI Commands on the Network Device

Ensure that your mobile device is connected to the Cisco network device with the special serial console cable.

1. Tap **Troubleshooting** on the main menu.
2. Tap **Advanced**.
3. Enter CLI commands in the field at the bottom and tap **Send** to send the commands to the device.

Factory Resetting a Device

Ensure that your mobile device is connected to the Cisco network device with the special serial console cable.

1. Tap **Troubleshooting** on the main menu.
2. Tap **Factory Reset** to send the CLI commands write erase and reload to the device.

The device configuration will be erased and the device will reload. Once the device is finished reloading you can reconnect to it again through the mobile app.

Viewing and Emailing Log Files

To view a log file, follow these steps:

1. Tap **Troubleshooting** on the main menu.
2. Tap **View Logs**.
3. Tap a session log to view the log of a session with the Cisco Network Plug and Play application, or tap a serial log to view the log of a serial session with a network device.

To email a log file, ensure that your mobile device has an email account configured, and follow these steps:

1. Tap **Troubleshooting** on the main menu.
2. Tap **Email Logs**.
3. Select one or more session or serial log files to email.
4. Tap **Email Selected Attachments** at the bottom of the screen.
5. Enter the email address information, subject, and optionally add note text.
6. Tap **Send** to send the email.

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Legal Information

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015-2016 Cisco Systems, Inc. All rights reserved.

