USER GUIDE

Cisco Small Business

Cisco OnPlus Portal User Guide

Document Part Number: 78-20144-02

Contents

Contents

1

Overview

Welcome to Cisco OnPlus Service. To learn more about Cisco OnPlus, read these sections:

- **About Cisco OnPlus**
- **Cisco OnPlus Scanner**
- **Cisco OnPlus Network Agent**

See **Getting Started with Cisco OnPlus, page 17** to learn how to log in to Cisco OnPlus Portal or register your Cisco OnPlus Partner Account, create customer accounts, and activate Cisco OnPlus Network Agent with the portal.

About Cisco OnPlus

Cisco OnPlus™ Service is an easy-to-deploy, cloud-based platform that enables channel users to economically deliver managed network services through discovery and monitoring of the entire mid-market network, along with reporting and remote management. Users can access their networks from anywhere, at any time, through a secure interface using a PC, tablet, or mobile device.

Cisco OnPlus uses two types of agents to connect networks to the service in the cloud:

- “Cisco OnPlus Scanner — Free, browser-based agent that discovers the inventory of Cisco devices and reports product lifecycle data such as end of sale notices and warranty status.
- “Cisco ON100 — Small, easy-to-use network agent that combines the discovery of the network, both Cisco and non-Cisco, and the Life Management details of Cisco products, with proactive remote monitoring, management, and maintenance.

Cisco OnPlus provides IT administrators of small to mid-sized networks the following:

- Basic network and device monitoring, including the up or down status of supported devices, using simple alerting email or Short Message Service (SMS) text messages and event logging.
- Remote device management access from Cisco OnPlus Portal to customer devices, using Web Hypertext Transfer Protocol (HTTP or HTTPS), Remote Desktop Protocol (RDP), Virtual Network Computing (VCN), or generic tunnel connections.
- Detailed device information (Internet Protocol (IP) address, serial number, firmware version, Media Access Control (MAC) address).
- Ability to upload and manage firmware for supported Cisco devices.
- Ability to back up and restore configuration for supported Cisco devices.
- Customizable reports.
- Integration with professional service automation applications such as ConnectWise and Autotask to automatically generate service tickets based on network and device events monitored through the portal.
- Multiuser account access (authorized agents).
- Mobile access from smartphones or tablets.
- Product support, service contract, and warranty information for Cisco devices.

Cisco OnPlus Scanner

Cisco OnPlus Scanner is a web-based service that can be accessed by registered Cisco users (Customers and Partners). The Cisco OnPlus Scanner allows customers to scan their local networks, discover Cisco devices, and receive lifecycle management information directly from Cisco. This service gives customers the ability to easily maintain current networks. Customers can maintain the discovered information in the cloud, which is more efficient than managing this information locally.

Cisco OnPlus Scanner provides an inventory view of the network that can be either a list or topology view. Cisco OnPlus Scanner also provides the following product support information:

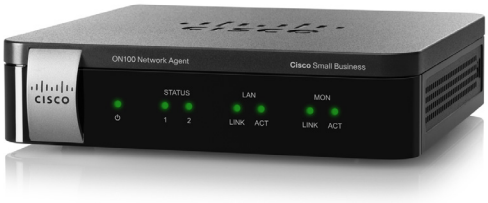
- Current warranty and service contract status
- Product field notices

- End-of-life for hardware and software
- Product security notifications

For information on how to use Cisco OnPlus Scanner on the network, see **Using the OnPlus Scanner to Discover Your Network, page 39**.

Cisco OnPlus Network Agent

Cisco OnPlus Network Agent is a device that is deployed at the customer premises, one per site. Cisco OnPlus Network Agent acts as a local agent that discovers devices on the network and sends and receives data from Cisco OnPlus Portal.



For an overview of the steps required to install and activate the customer's Cisco OnPlus Network Agent with the portal, see **Getting Started with Cisco OnPlus, page 17**.

- For detailed information about installing Cisco OnPlus Network Agent on the customer's network, see *Cisco ON100 Network Agent Quick Start Guide*, available on Cisco.com at www.cisco.com/go/onplus.
- For important information about prerequisites, guidelines, and activation steps, see **Getting Started with Cisco OnPlus, page 17**.

2

Getting Started with Cisco OnPlus

This chapter covers the steps required to get started with Cisco OnPlus, from logging in to the portal to Partner Account sign-up to customer account creation and service activation:

- **Requirements for Accessing the Cisco OnPlus Portal**
- **Logging In to the Cisco OnPlus Portal**
- **Adding Your First Customer**
- **End Customer Agreement Legal Requirement**
- **Installing and Activating the Cisco OnPlus Network Agent at the Customer Premises**
- **Verifying Customer Activation with the Portal**
- **Next Steps**

Requirements for Accessing the Cisco OnPlus Portal

Read this section for important information about prerequisites for accessing the Cisco OnPlus Portal and for web browser compatibility requirements.

Obtain a Cisco.com Login

A Cisco.com login is required for Cisco OnPlus Portal access. If you do not already have a Cisco.com login, you can obtain one by clicking the **Register** link in the upper right corner of the Cisco.com Registration page and following the on-screen instructions. Record your username and password to use to log in to the Cisco OnPlus Portal.

You will receive an email with an Activate Now link. Click the link and a page will display with a message that states: This account has already been activated.

Verify Web Browser Compatibility with the Cisco OnPlus Portal

Recent versions of the Mozilla Firefox, Google Chrome, and Internet Explorer web browsers are recommended for use with the Cisco OnPlus Portal. If you are accessing the portal from a Mac, you can also use the Safari web browser.

NOTE Microsoft Internet Explorer 6 is not recommended.

IMPORTANT In order for the Cisco OnPlus Portal to function correctly, your web browser must not be set to exclude the HTTP referrer header. If the HTTP referrer header is excluded, you may experience issues when saving or updating settings on the portal. Most modern browsers have this set correctly by default.

Adobe Flash Player 10.1 or later is required.

The minimum recommended desktop display resolution for the PC running the web browser used to access the portal is 1024 x 768.

Logging In to the Cisco OnPlus Portal

After you have created your Cisco.com username and password, follow these steps to log in to the portal for the first time:

NOTE You are automatically logged out of the portal after 24 minutes of inactivity.

STEP 1 Open a web browser and go to the following URL to log in for the first time:

www.cisco-onplus.com

STEP 2 Log in.

a. In the **Cisco.com Username** field, enter the Cisco.com username that you requested.

b. In the **Cisco.com Password** field, enter the password for the CIsco.com account that you used when registering for the Cisco OnPlus Portal. You can change this password later.

STEP 3 Create an account.

When logging in to the Cisco OnPlus Portal for the first time, you will be asked to:

- Select **Account Type** from the drop-down list options.

- Enter the **Email Address** to which reports will be sent.
- Select **Geographic Region** from the drop-down list.
- Accept terms and conditions by clicking **Accept.**

STEP 4 Email confirmation.

An email will be sent that welcomes you to the Cisco OnPlus Service and states your portal username along with information about Cisco OnPlus Service, Cisco OnPlus Scanner, and the Cisco OnPlus ON100 Network Agent, as well as links to useful OnPlus resources.

STEP 5 Cisco OnPlus Portal opens.

If you have selected Account Type **Cisco Customer**, your initial Cisco OnPlus Portal page will be the Cisco OnPlus Scanner Page. For information about using the Cisco OnPlus Scanner, see **Using the Cisco OnPlus Scanner, page 45**.

If you have selected Account Type **Registered Partner**, your initial Cisco OnPlus Portal page will be the Overview page. There will be no entries because your first task is to add new customers. To add your first customer, see **Adding Your First Customer, page 19**

Adding Your First Customer

To add a customer account, follow these steps:

STEP 1 On the Overview page, click the + **Add Customer** button on the upper right section of the page, just below the navigation bar.

STEP 2 To upload an optional logo image for the customer, click **Browse**.

TIP The logo upload is optional. Images must be in JPEG, PNG, or GIF format. Images larger than 300x300 pixels in size will be resized. You can add or replace the picture any time after the account is created.

A checkmark and the text **Image OK** appears if the upload is successful. The uploaded image is not displayed here. After the customer is created, you can view the logo from the customer list. See **Viewing Customer Contact and Location Information, page 36**.

STEP 3 Enter the required information for the customer on the **Profile** section and click **Next**. You can add or edit the customer profile later.

STEP 4 In the **Contact** section, enter the required contact information for this customer or uncheck the **Add a Contact** option to continue without adding a contact.

Contacts are used for delivering event notifications. You can add or edit contacts later. See **Adding and Managing Delivery Contacts, page 112**.

STEP 5 On the **Summary** tab, review the information that you entered and correct errors that are highlighted.

Use the **Back** and **Next** buttons to move between sections.

STEP 6 Click **Save**.

The portal updates to display the Status for the customer you just added.

The customer's **Activation ID** is displayed in three locations:

- On the customer's Dashboard page in the ON100 drop-down list
- On the **Profile** page for the customer (click the customer, then choose **Profile** > **Profile**)
- In the customers actions drawer associated.

You can copy and paste this ID into a text editor or other program for later use.

This ID is used for activating the customer's Cisco OnPlus Network Agent with the portal.

An entry for the new customer is also added to the Overview page. The **Status** column indicates that the customer is **Unknown** because the Cisco OnPlus Scanner has not been used or because the Cisco OnPlus Network Agent has not yet been installed and activated at the customer premises.

 Indicates a Customer with an activated ON100.

 Indicates a Customer with a scanned network.

 Indicates a Customer that has not scanned the network or activated a Cisco ON100 Network Agent.

After you have added your first customer, continue with **Installing and Activating the Cisco OnPlus Network Agent at the Customer Premises, page 21**.

End Customer Agreement Legal Requirement

When you install a Cisco OnPlus Network Appliance at a customer site, you must get written approval for Cisco monitoring capabilities by having the customer sign Attachment A of the Cisco OnPlus Terms & Conditions. Per the Cisco OnPlus Service Terms & Conditions, Cisco has the right to review your records to ensure that you are complying with this requirement.

Attachment A of the Terms & Conditions ("End User's Consent and Obligations,") is appended to the PDF version of this guide.

Installing and Activating the Cisco OnPlus Network Agent at the Customer Premises

Follow the procedures in this section to install the Cisco OnPlus Network Agent and activate the Network Agent with the Cisco OnPlus Portal. These topics are covered:

- **Before You Begin**
- **Where to Place the Cisco OnPlus Network Agent in the Customer Network**
- **Port and Protocol Access Requirements**
- **Installing the Cisco OnPlus Network Agent**
- **Activating the Cisco OnPlus Network Agent**

Before You Begin

The Cisco OnPlus Network Agent must be installed at the customer premises.

The computer or mobile device that is used to activate the Cisco OnPlus Network Agent with the Cisco OnPlus Portal must be connected to the local area network (LAN) or wireless local area network (WLAN) at the customer premises.

NOTE Multiple simultaneous network connections on the device being used to access the portal or the Cisco OnPlus Network Agent can cause connection problems. For example, if your computer has a dual network interface card (NIC) with a wired and a wireless interface, and you are having problems connecting to the portal, disable one of the interfaces, then retry the connection.

Only one Cisco OnPlus Network Agent is installed per customer account.

Before installing the Cisco OnPlus Network Agent, make sure that you have:

- Cisco OnPlus Portal activation information for this customer: Customer name and **Activation ID**.

  To locate the customer's **Activation ID**, log into the portal, click the customer's entry in the list on the Overview page, then choose **ON100 > Activate** from the Customer's Dashboard page. Prior to activation, the Activation ID will be displayed here as well as in the action drawer and on the customer Profile page.

- A power source for the Cisco OnPlus Network Agent, either a Power over Ethernet (PoE) LAN port or a 100-240VAC, 50-60 Hz power receptacle.
- An active Internet connection at the customer premises.
- A Windows PC, Mac, or Linux computer with a web browser.
- A DHCP server on the customer LAN.

NOTE If there is no DHCP server at the customer site, you can pre-stage the Cisco OnPlus Network Agent by activating the customer on your local network before deploying it at the customer site.

Activate the customer's Cisco OnPlus Network Agent on the local network, then configure a static IP on the network agent. When the Cisco OnPlus Network Agent is installed and connected to the customer's network, it will boot up with the static IP address.

After connecting to the customer's network, navigate to that customer's Dashboard, hover over the Actions icon on the toolbar, then click **Data Reset** > **Rediscover Network** to remove all existing discovery information and discover the customer's network and devices.

Where to Place the Cisco OnPlus Network Agent in the Customer Network

The success and accuracy of the device discovery process and network topology representation is affected by the location of the Cisco OnPlus Network Agent in the network.

Follow these guidelines when determining where to place the Cisco OnPlus Network Agent in the customer's network:

- To ensure the most accurate device discovery and topology representation, connect the Cisco OnPlus Network Agent to a LAN port on a Cisco OnPlus-supported Cisco router or switch. For a list of Cisco OnPlus-supported Cisco devices, see **Device Feature Summary, page 241**.
- Non-CDP capable switches may flood Cisco Discovery Protocol (CDP) messages, resulting in inaccurate topology representation. To correct the topology, manually re-parent devices. See **Manually Adding Child Devices, page 74**.
- Switches that are CDP-capable, but not supported by the Cisco OnPlus Portal consume CDP messages from devices connected behind them. As a result, this limits the ability of the Cisco OnPlus Network Agent to see devices behind the switch if those devices use CDP as their only discovery method (for example, Cisco 7900 Series IP Phones).
- As a best practice, place the Cisco OnPlus Network Agent on the LAN side of all devices in the customer network. For example, if a UC300 is deployed in an existing network behind an SA500 security appliance and the Cisco OnPlus Network Agent is placed on the WAN side of the UC300, discovery success and topology accuracy will be severely limited. In this scenario, place the Cisco OnPlus Network Agent on the LAN side of the UC300.
- Non-OnPlus-supported routers and switches can be discovered. However, these non-OnPlus-supported devices may severely limit Cisco OnPlus Network Agent discovery and topology accuracy. Manual driver selection and topology adjustments will be needed. For more information, see **Manually Adding Child Devices, page 74** and **Device Driver, page 93**.

Port and Protocol Access Requirements

The Cisco OnPlus Network Agent and Cisco OnPlus Portal do not need special configuration and will communicate with the portal through the firewall. However, we recommend that you ensure that the following ports are opened for outbound-initiated traffic (no inbound ports need to be opened on the firewall):

- Outboard-initiated traffic that must be permitted on the network hosting the Cisco OnPlus Network Agent device:

  - Port 53 UDP (DNS)
  - Port 80 TCP (HTTP)
  - Port 123 UDP (NTP)
  - Port 443 TCP (HTTPS)
  - Ports 11300 (TCP) and 11400 (TCP)
  - Port 14931 (UDP), WAN network performance monitoring through the Cisco OnPlus Network Agent

- Outbound-initiated traffic that must be permitted to successfully use the Cisco OnPlus Portal from a web browser:
  - Port 53 UDP (DNS)
  - Port 80 TCP (HTTP)
  - Port 443 TCP (HTTPS)
  - Ports 11305 (TCP) and 11700 through 11800 (TCP), remote tunnel connections through the Cisco OnPlus Portal
  - Port 12330 (TCP), real-time dashboard and Topology communication

NOTE Outbound-initiated traffic on these ports would only be blocked in a highly restrictive network environment. By default, most routers do not block outbound-initiated traffic.

Installing the Cisco OnPlus Network Agent

To avoid exposure of site data, we recommend that you limit physical access to the Cisco OnPlus Network Agent device. Use the physical locking slot and a security cable to secure the device and protect against unauthorized removal. Unauthorized, privileged access can be gained through hardware modification, which violates the warranty. Since the AUX port on the device is not supported, nothing should be connected to that port.

Follow the *Cisco ON100 Network Agent Quick Start Guide* to install the Network Agent hardware, connect it to your customer's network, and apply power.

The *Cisco ON100 Network Agent Quick Start Guide* is available on Cisco.com at www.cisco.com/go/onplus.

Activating the Cisco OnPlus Network Agent

After the STATUS 1 and STATUS 2 LEDs on the Cisco OnPlus Network Agent indicate that the device is ready for activation (STATUS 1 is lit Green and STATUS 2 is Off), follow the instructions in this section to locate the Cisco OnPlus Network Agent on the network and launch the Activation page.

STEP 1 On the computer connected to the customer LAN, open a web browser and log in to the Cisco OnPlus Portal.

STEP 2 If you have not yet created an entry for this customer, go to the Partner Account Overview page and click **+ Add Customer**. After you add the customer, an Activation ID is generated.

STEP 3 Navigate to the customer's **Dashboard** page and choose **ON100 > Activate**.

STEP 4 On the **Activate Cisco OnPlus Network Agent** page, select the MAC address that corresponds to the Cisco OnPlus Network Agent that you are installing, then click **Proceed to this Cisco OnPlus Network Agent**.

The Activation page on the Cisco OnPlus Network Agent is displayed. The customer's Activation ID is automatically inserted for you.

If the MAC address for the customer's Cisco OnPlus Network Agent is not displayed:

- Make sure that the Cisco OnPlus Network Agent is powered on and connected to the customer LAN.
- If the message "Unable to determine a local IP address for any Cisco OnPlus Network Agent on your current network." appears, read the onscreen troubleshooting information and make sure that your network environment meets the requirements for using this feature:
  - The Cisco OnPlus Network Agent must be located on the same public WAN IP address block as the web browser you are using to perform the activation.
  - Check that DHCP service is running on the local network so that the Cisco OnPlus Network Agent is able to acquire an IP address using DHCP. You will be able to set a static IP address for the Cisco OnPlus Network Agent later if you choose, but DHCP service is required to initially access the Cisco OnPlus Network Agent.
  - Check that DHCP clients can route to the Internet.

- Make sure that the firewall on the customer network is not blocking outbound-initiated HTTP or HTTPS traffic on the port that the Cisco OnPlus Network Agent uses to communicate with the portal.
- Make sure that you are not connected to the network through a VPN during activation.

If the **Activate** method described here does not work, see **Alternate Methods for Activating the Cisco OnPlus Network Agent, page 27** for additional ways to discover the Network Agent and launch the activation page.

STEP 5 If needed, configure optional network settings. These include IP addressing (DHCP or static), DNS servers, and NTP servers. See **Configuring Additional Network Settings on the Cisco OnPlus Network Agent, page 26**.

STEP 6 Click **Activate**.

STEP 7 Confirm that the customer information matches the customer you are installing.

STEP 8 Click **Complete Activation**.

The system will automatically update the Cisco OnPlus Network Agent with the customer's profile information and upgrade the software as needed. Status messages are displayed so that you can track system setup progress. The Cisco OnPlus Network Agent may restart twice during the process, which can take up to 20 minutes, depending on broadband connection speed.

When the Cisco OnPlus Network Agent is activated and connected to the portal, both Status LEDs on the device are lit steady Green.

Continue with the section, **Verifying Customer Activation with the Portal, page 28**.

Configuring Additional Network Settings on the Cisco OnPlus Network Agent

You can configure the following optional network settings for the Cisco OnPlus Network Agent:

- **IP Address**—Choose either DHCP or Static.
- **DNS Servers**—Use DHCP-assigned DNS servers or specify different DNS servers.
- **NTP Servers**—Use DHCP-assigned NTP servers or specify different NTP servers.

To configure optional network settings for the Cisco OnPlus Network Agent during activation, click **Configure additional network settings** on the Activation page.

When you finish making changes, click **Apply network settings**.

After you change the IP address of the Cisco OnPlus Network Agent, the device will restart. When the device has finished restarting, click the link provided to access the Cisco OnPlus Network Agent at its new IP address.

You can change these settings later, if needed. To modify these settings after activation, log in to the Cisco OnPlus Network Agent, click the **Configuration** link at the top of the page, then click **Configure additional settings**. The username and password for the Cisco OnPlus Network Agent are listed on the customer's Profile page on the portal.

Alternate Methods for Activating the Cisco OnPlus Network Agent

If the **Activate** link does not work, try these alternate methods to discover the Cisco OnPlus Network Agent and launch the activation page.

STEP 1 Use one of the following methods to discover the Cisco OnPlus Network Agent.

- If you are using a web browser with built-in Bonjour support (for example, Safari) or you have a Bonjour browser plug-in installed, use the Bonjour browser to locate the Cisco OnPlus Network Agent. The Bonjour name for the Cisco OnPlus Network Agent is **onplus***<Last_6_digits_of_LAN_port_MAC_address>*.
- If you are using a Windows PC with UPnP enabled, look for the Cisco OnPlus Network Agent on the Network Panel in Windows Explorer.
- If you have access to a DHCP server on the customer LAN, use it to determine the IP address of the Cisco OnPlus Network Agent. If you need to refer to the Cisco OnPlus Network Agent by its MAC address, use the LAN port MAC address listed on the back panel of the device.

STEP 2 To launch the Activation page:

- If you used Bonjour or UPnP to locate the Cisco OnPlus Network Agent, double-click its name (**onplus***<Last_6_digits_of_LAN_port_MAC_address>).*
- If you know the IP address of the Cisco OnPlus Network Agent, enter it in your web browser address bar (for example, 192.168.10.25).

STEP 3 On the Activation page, enter the Cisco OnPlus Portal Activation ID.

The Activation ID is displayed on the **Profile** page for the customer on the Cisco OnPlus Portal. Prior to activation, the Activation ID is also displayed on the customer's **Dashboard** when you choose **ON100** on the Cisco OnPlus Portal.

Copy and paste the Activation ID into the field provided or enter it manually.

Continue with Step 6, see **Activating the Cisco OnPlus Network Agent, page 25**.

Verifying Customer Activation with the Portal

To verify the customer site is active on the portal, follow these steps:

STEP 1 Log in to the Cisco OnPlus Portal.

STEP 2 On the Overview page, locate the customer you just installed and click the entry to go to the Customer Dashboard.

STEP 3 Choose **ON100**. If the customer site has been successfully activated, the status will be shown as Activated, Online.

When you first log in to the portal after the initial activation, no discovery information will be available on the customer's Dashboard until the device discovery process finishes. The message "No discovery information currently available" is displayed.

After several minutes, the Network Topology and Device Listing views on the customer Dashboard will update to show the devices discovered on the network.

NOTE Depending on the size of your network, it can take several minutes to discover devices and display them in the Network Topology. Device discovery on a larger, more complex network can take 15 minutes or longer.

Click items in the **To-Do** list on the customer Dashboard to view a list of recommended actions. When you click an item, the page updates to display only the devices that require attention for that item.

For example, if devices present on the network are not displayed as expected, you may need to provide access credentials for devices such as Cisco routers, switches, or access points to enable discovery of additional devices.

After your customer is activated and you can view their network using the Network Topology, you can begin exploring the features of the Cisco OnPlus Portal.

Continue with the section **Next Steps, page 29**.

Next Steps

The remaining chapters of this guide provide detailed information about how to use each of these Cisco OnPlus Portal features.

Chapter	Description
Cisco OnPlus Partner Account Overview, page 31	How to navigate the customer list and menus on the Overview page and manage customers' accounts.
Using the OnPlus Scanner to Discover Your Network, page 39	How to use the Cisco OnPlus Scanner to discover devices in your network and view and access them from a network topology.
Viewing Customer Networks, page 57	How to use the Network Topology and Device Listing Dashboard views to explore and view each customer's network topology and devices.
Working with Customer Devices, page 85	How to view device information and perform actions on remote devices using the Cisco OnPlus Portal.
Monitoring and Notifications, page 107	How to set up device monitors, delivery rules, and delivery contacts to enable notifications for events monitored through the portal.
Connecting to Devices from the Portal, page 137	How to connect to devices remotely through the portal.
Cisco Device Management and Maintenance, page 151	How to upgrade firmware and how to back up and restore device configuration for supported Cisco devices. Instructions for performing a factory reset, rebooting the Cisco OnPlus Network Agent, deactivating a customer, and other maintenance operations for the Cisco OnPlus Network Agent are also covered.
Adding and Managing Authorized Agents, page 157	How to invite and manage accounts for your authorized agents on the Cisco OnPlus Portal.
Reports, page 169	Describes Lifecycle Digest, available reports, and how to generate and schedule them.

Chapter	Description
Viewing Cisco Product Support Information, page 181	How to view product support information for supported Cisco devices through the Cisco OnPlus Portal This information includes service contracts, product warranties, field notices, hardware and software end-of-life notices, and product security advisories.
Mobile Device Access to the OnPlus Portal, page 231	How to access and use the features of the Cisco OnPlus Portal from a mobile device with a web browser.
Cisco Device Feature Support, page 241	Lists Cisco devices supported by the Cisco OnPlus Portal, along with the portal features available for each device, and any limitations or constraints that apply.

3

Cisco OnPlus Partner Account Overview

This chapter provides information about using the Partner Account Overview area of the portal to view customer status, manage customers, and access global features associated with your Partner Account.

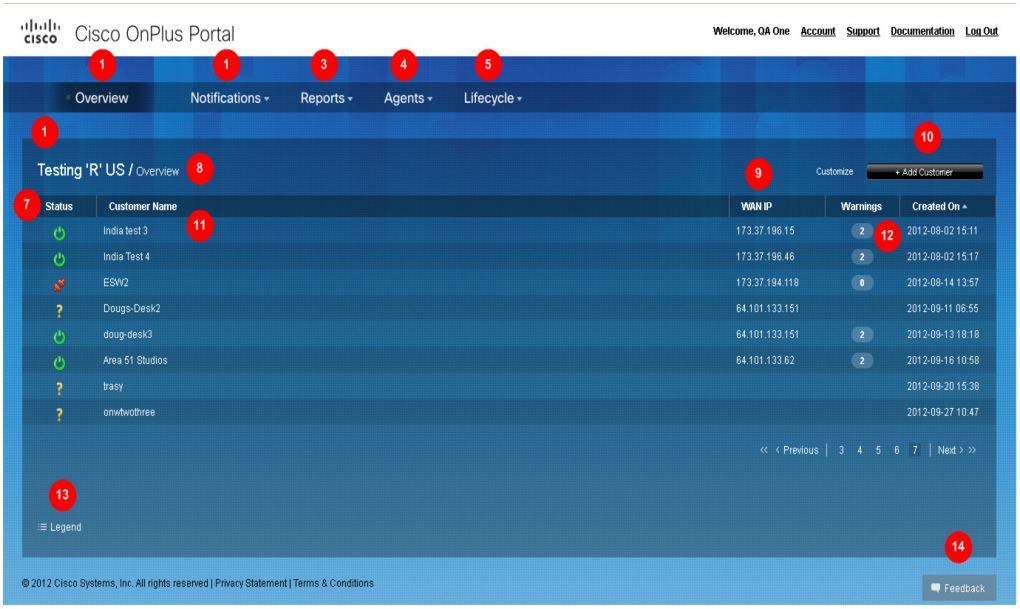
- **Overview Page and Feature Menus**
- **Managing Customers**
- **Updating Your OnPlus Partner Account Information**

Overview Page and Feature Menus

When you first log in to your Cisco OnPlus Portal Account, the Overview page appears. From this page you can:

- View a list of all your customers that includes status, 24-hour alert count, and location information for each customer.
- Add and manage your customers.
- Click any customer in the list to open that customer's Dashboard. From the Dashboard, you can view their network topology and monitor or interact with devices remotely through the portal.
- Access reporting, notification delivery, authorized agent management, firmware upload listing, and lifecycle product support information.

Here is a sample page that shows the available features and areas of interest on the Overview page.



1	Displays the main Overview page that lists all customers.
2	Create, edit, or remove delivery rules and contacts for Cisco OnPlus event notifications.
3	Create, schedule, and view reports.
4	Invite and manage agents account.
5	View information about software for supported Cisco devices that you have uploaded to the portal. View product support service and warranty information for Cisco devices.
6	Identifies the current Partner Account.
7	Status shows an ON100 activated account, an account that is off-line, and an account that has not been activated or scanned. a Cisco OnPlus scanned network account. There are two other account status types, scanned accounts and accounts that have been suspended.
8	Summary information about the customer Status, Customer Name, WAN IP, Warnings, and the date the account was created.
9	Move your mouse over the **Customize** link to add or remove information from the display.
10	Create new customer accounts.

11	Move your mouse over the customer data to access a drawer that provides contact and location information about the customer. From this drawer, you can also activate a newly installed ON100.
12	Click an entry in the list to go to the Dashboard for the selected customer.
13	Move your mouse over the Legend icon to view information about Status icons displayed on the Overview page.
14	Provide feedback and request enhancements for the Cisco Portal.

Customizing the Overview Page

You can customize the information that is displayed for your customers on the Overview page.

To do this, move your cursor over the **Customize** link to open the Customize Overview flyout menu and select the information to display in the custom list.

Your changes are applied as soon as you move the cursor out of the flyout menu.

These custom settings are applied on a per-browser basis to all customers. Your selections are saved across sessions for the Web browser you are currently using. If you use a different device to access the portal or change Web browsers, you must reset these options.

You can choose whether or not to display the WAN IP address, the date created, the date last updated, and the number of events with a severity level of Warning or above for the last 24 hours. You can also specify the number of records displayed per page for the site.

Managing Customers

Read the following sections for instructions on how, as a Partner, you can manage your customers:

- **Adding a Customer**
- **Deleting a Customer**
- **Suspending and Resuming a Customer Account**
- **Viewing Customer Contact and Location Information**
- **Editing a Customer Profile or Address**

Adding a Customer

Each customer that you add represents a single customer with a Cisco OnPlus Scanner or a single Cisco OnPlus Network Agent.

To add a customer account, follow these steps:

STEP 1 On the Overview page, click the + **Add Customer** button on the upper right section of the page, just below the navigation bar.

STEP 2 To upload an optional logo image for the customer, click **Browse**.

TIP The logo upload is optional. Images must be in JPEG, PNG, or GIF format. Images over 300x300 pixels in size will be resized. You can add or replace the picture any time after the account is created.

A checkmark and the text **Image OK** appears if the upload is successful. The uploaded image is not displayed here. After the customer is created, you can view the logo from the customer list. See **Viewing Customer Contact and Location Information, page 36**.

STEP 3 Enter the required information for the customer in the **Profile** section and click **Next**. You can add or edit the customer profile later.

STEP 4 In the **Contact** section, enter the required contact information for this customer or uncheck the **Add a Contact** option to continue without adding a contact.

You can add or edit contacts later. See **Adding and Managing Delivery Contacts, page 112**.

STEP 5 On the **Summary** tab, review the information you entered and correct errors that are highlighted.

Use the **Back** and **Next** buttons to move between sections.

STEP 6 Click **Save**.

The Overview page updates to display an entry for the new customer. The **Status** column indicates that the customer is **Unknown**, because the Customer has not yet scanned the network or the Cisco OnPlus Network Agent has not yet been installed and activated at the customer premises.

IMPORTANT The customer's Activation ID is displayed on the Customer Dashboard page by choosing **ON100 > Activate**. The Activation ID is always displayed on the **Profile** page for the customer.

See **Installing and Activating the Cisco OnPlus Network Agent at the Customer Premises, page 21**.

Deleting a Customer

When a customer is deleted, all information for that customer is removed from the portal and cannot be retrieved. This action cannot be undone.

The deleted customer's Cisco OnPlus Network Agent can be factory reset and reactivated with another customer (see **Transferring a Cisco OnPlus Network Agent to a Different Customer, page 195**).

To delete a customer on the Cisco OnPlus Portal, follow these steps:

STEP 1 Before deleting a customer, it is a good practice to perform a factory reset on the customer's Cisco OnPlus Network Agent. This action removes all customer data from the Cisco OnPlus Network Agent and leaves it in a state where it can later be reactivated. See **Performing a Factory Reset on the Cisco OnPlus Network Agent, page 191**.

NOTE After you delete a customer from the portal, you will not be able to access the customer's Cisco OnPlus Network Agent remotely.

STEP 2 On the Overview page of the portal, select the customer to be deleted.

STEP 3 From the Profile menu at the top of the page, choose **Profile**.

STEP 4 Click the **Delete** button at the bottom of the profile.

STEP 5 Click **OK** to confirm the deletion.

Suspending and Resuming a Customer Account

When a customer is suspended, all services are suspended. This includes device discovery, device monitoring, notifications to customer contact targets, firmware upgrades, and configuration backup and restore.

The suspended customer's account profile information is retained on the portal, and the customer can later be resumed without recreating the account.

Suspending a Customer

To suspend a customer on the OnPlus Portal, follow these steps:

STEP 1 On the Overview page of the portal, select the customer to be suspended.

STEP 2 From the Profile menu at the top of the page, choose **Profile**.

STEP 3 Click the **Suspend** button at the bottom of the profile.

The **Overview** page updates to indicate that the account has been suspended. The Network Topology and Device Listing views will not display any devices found, because device discovery is disabled when a customer is suspended.

Resuming a Suspended Customer

To resume a suspended customer on the OnPlus Portal, follow these steps:

STEP 1 On the Overview page of the portal, select the customer account to be resumed.

STEP 2 From the Profile menu at the top of the page, choose **Profile**.

STEP 3 Click the **Unsuspend** button at the bottom of the profile.

The **Profile** page for the customer updates to indicate that the account has been resumed.

Viewing Customer Contact and Location Information

To open or close a drawer with customer contact information and Google map location, select the customer and click the arrow icon  on the tab at the bottom of the highlighted entry.

Editing a Customer Profile or Address

You can edit the customer account profile or address to:

- Change the business name, industry information, or time zone
- Change the customer password
- Add or update a logo image
- Update the customer location information

To edit the customer profile, follow these steps:

STEP 1 On the Overview page of the portal, click the customer that you want to edit.

STEP 2 From the Profile menu at the top of the page, choose **Profile**.

STEP 3 Edit the information as needed, then click **Save**.

To edit the customer address, follow these steps:

STEP 1 On the Overview page of the portal, click the customer that you want to edit.

STEP 2 From the Profile menu at the top of the page, choose **Address**.

STEP 3 Edit the information as needed, then click **Save**.

Updating Your OnPlus Partner Account Information

To update your Cisco OnPlus Partner Account information, choose **Account** from the links on the top right corner of the page.

Update information as needed and click **Save**.

You can update your account information at any time. The contact email address and phone numbers entered here can be used when creating notifications rules for events that are being monitored. See **Using Delivery Rules, page 114**.

Your Partner Account email address can also be used when specifying recipients for scheduled reports. See **Reports, page 169**.

When **Use Light Theme** is checked, lighter background colors are used. Click the **preview** link to the right of the checkbox to see how the theme will look.

You can easily change the **Company Logo** by clicking **Browse** to search for the logo that complies with the upload requirements that appear when you place the cursor in the empty box next to **Browse**.

When you register your account, a default delivery rule for notifications is created. The default delivery rule specifies that notification emails for all events with a severity level of Warning or above will be sent to the work email address for your Partner Account. You can delete this rule or suspend notifications to this email address if needed. See **Deleting Delivery Rules, page 119** and **Enabling or Disabling Notifications to Email or SMS Addresses, page 114**.

4

Using the OnPlus Scanner to Discover Your Network

This chapter provides general information about the Cisco OnPlus Scanner and tips on using it. Also included in this chapter are instructions for customizing the portal features and pages, creating reports, and viewing Cisco device information that is discovered using the OnPlus Scanner.

Cisco OnPlus Scanner Overview

The OnPlus Scanner is available to every Cisco OnPlus Customer. It provides network administrators with an efficient way to manage their network by creating an inventory of Cisco devices and providing important information about the various devices that it discovers.

- Create inventory automatically
- Access lifecycle information about Cisco network devices
- Customize the portal display

- Customize sorting and grouping of data
- Format and schedule reports

Operating System and Browser Recommendations

The OnPlus Scanner is an easy-to-use application that lets you quickly discover devices in your network. Up to 256 devices can be discovered in a single scan, giving you an opportunity to add new devices found in your network to your OnPlus inventory list. Once the devices are in the OnPlus inventory list, you can obtain important lifecycle information including: end-of-life hardware and recommended replacement products, end-of-life software, service contract status, warranty status, product security alerts, and field notices.

Supported Browsers and Operating Systems

The Cisco OnPlus Scanner supports the following operating systems and the current and two prior versions of the following browsers:

	Window XP	Windows 7	MAC	Linux Redhat and Ubuntu
Google Chrome	Supported	Supported	Supported	Not tested
Firefox	Supported	Supported	Supported	Supported
Internet Explorer	Supported	Supported	Not tested	Not tested
Safari	Not tested	Not tested	Supported	Not tested

NOTE We do not recommend using Internet Explorer 6, Internet Explorer 7, and Firefox 3.6 or earlier.

JRE Compatibility

If a 32- or 64-bit operating system running a 32-bit browser is not running the minimum required JRE, the OnPlus Scanner provides a redirection link to download and installs the recommended version.

For a 32-bit browser, you must install 32 bit JRE, and for a 64- bit browser you must install 64-bit JRE. When you manually uninstall JRE, the Java deployment plugin should also be uninstalled. Taking this action will ensure that OnPlus scanner points to the JRE redirection link to allow the download for the installation of the recommended version.

By default, the next-generation Java plug-in is not enabled in Safari on the Mac OS. You must enable the next-generation Java plug-in manually to ensure that the scanner works properly. JRE versions earlier than 1.6 are not recommended

If a 64-bit operating system running a 64-bit browser is not running the minimum required JRE, the OnPlus Scanner will provide instructions to install the recommended version manually.

Google Chrome is not supported on systems running a 64-bit JRE. There is currently no 64-bit version of Google Chrome.

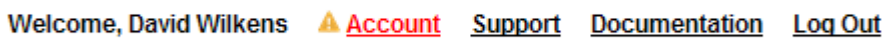
Using the Cisco OnPlus Scanner Dashboard

The Dashboard displays inventory data and provides access to information about the Cisco devices in your network. You can create customized reports that will automatically provide updated information about your network. To take advantage of the features that are part of the OnPlus Scanner Dashboard, read the following information:

- **User Account and Support Tools, page 41**
- **Using Dashboard Navigation, page 43**
- **Using Dashboard Tools, page 43**

User Account and Support Tools

You can set up your account information, find detailed information about Cisco OnPlus Service, and access the OnPlus Support community by using the OnPlus Support Tools found in the upper-right portion of each page. The toolbar contains the following options. The **Account** option appears red, as shown in the illustration, when account information is incomplete. To complete the Account information follow these step:



STEP 1 Click **Account** to access the My Account page.

STEP 2 Choose **Account Type** from the drop-down list if you are changing your account type.

Note: Account Type is only changed when an OnPlus Scanner Customer chooses to become a Cisco Registered Partner.

STEP 3 Fill in your **Identity Information**.

- **First** and **Last Names**
- **Company** affiliation
- Choose **Job Role** and **Job Level (**from the drop-down lists)
- Choose **Timezone** information that most closely matches your location (from the drop-down list)

STEP 4 Fill in **Contact Information.**

STEP 5 Find and apply your company logo using the **Browse** feature on **Global Preferences**.

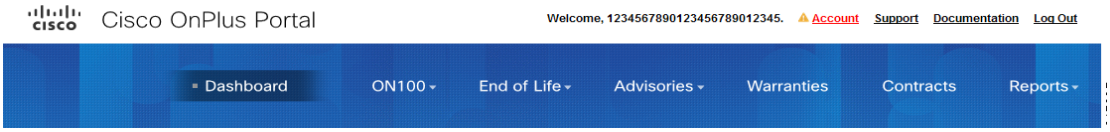
STEP 6 Click **Save**.

Once the account information is complete, the **Account** option will change to black text.

The other support options:

- **Support** — Link to the Support pages where you can join discussions and find information about the Cisco OnPlus Portal.
- **Dogmatization** — Open online help files or download the *Cisco OnPlus Portal User Guide*.
- **Log Out** — Exit the Cisco OnPlus Portal.

Using Dashboard Navigation



Option	Description
Dashboard	Provides a summary view of the information discovered on the network.
ON100	Provides links to information about ON100 functionality, and obtaining and activating an ON100. See **Installing and Activating the Cisco OnPlus Network Agent at the Customer Premises, page 21**.
End of Life	Shows hardware and software end-of-life information, as well as information about replacement devices. You can set periodic reminders. See **Setting the Product Support Expiration Reminder Interval, page 186**
Advisories	Provides product security advisories and field notices.
Warranties	Shows specific start and end dates for warranty support by device. You can set periodic reminders, see **Setting the Product Support Expiration Reminder Interval, page 186**.
Contracts	Lists Cisco devices that are under service contracts. To set periodic reminders, see **Setting the Product Support Expiration Reminder Interval, page 186**.
Reports	Provides available Lifecycle Digest reports or allows you to create new ones. To create a Lifecycle Digest report, see **Creating a Lifecycle Digest Report, page 54**.

Using Dashboard Tools

The Dashboard Tools offer an easy way to help you perform OnPlus functions.

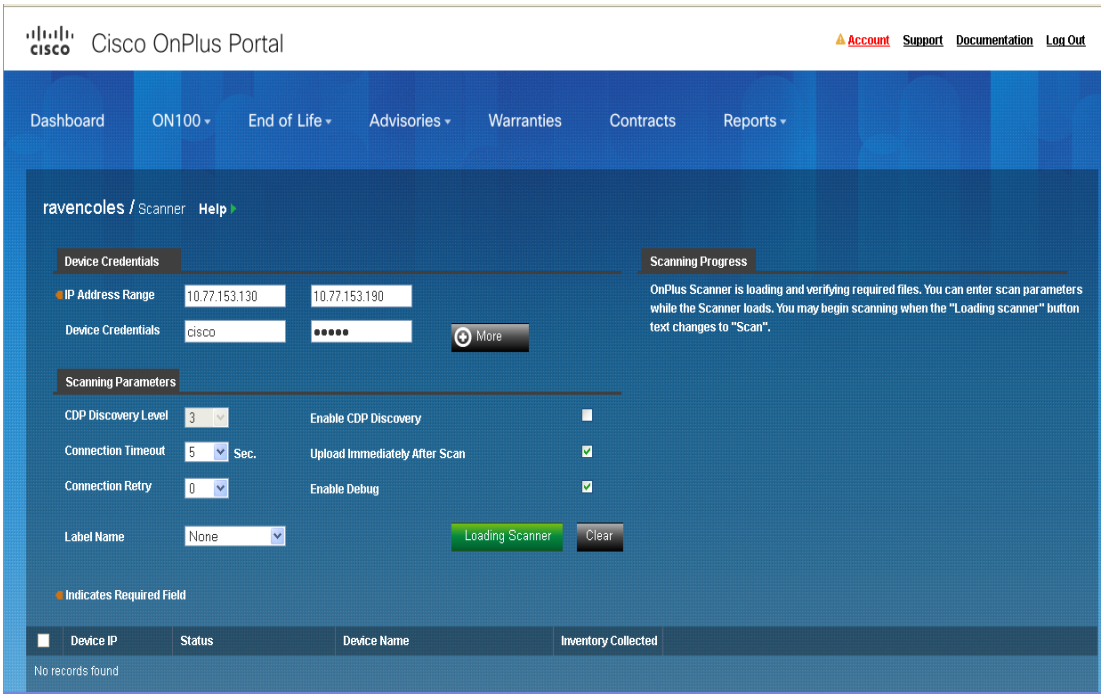
Tool	Device Listing View	Topology View
Legend	Identify the symbols used on the Dashboard page.	Identify the symbols used on the Dashboard page.
Customize	Choose which columns appear on the device listing and how many records display per page.	Choose which columns appear on the device listing and how many records display per page.
Scan My Network	Open the Scanner page.	Open the Scanner page.
Export to CSV	Create an MS Excel spreadsheet using the device information on your Dashboard.	Save the topology view as a PNG image, create an MS Excel spreadsheet, or save the topology as an SVG file to use with MS Visio.
Export to PDF	Create a PDF table that shows all the entries on the Dashboard page in the Device listing.	N/A
Actions 	Delete selected devices or all devices.	Delete all devices.
Settings 	Create labels for a single device or group of devices.	Adjust topology settings, add or delete device categories, and create device labels.
Filter Criteria 	Create precise searches and sorts based on any or all fields in the Dashboard view.	Create precise searches and sorts based on any or all fields in the Topology view.
Full Screen Mode 	Not available for the Device Listing view.	Provides a full screen view of the topology while disabling the ability to enter data.

Tool	Device Listing View	Topology View
Device Listing  **Network Topology**  -	Use the drop-down list to toggle to the Network view you choose.	Use the drop-down list to toggle to the Device Listing view or to change to another topology view.
Zoom 	Not available for the Device Listing view.	Zoom in or out, and zoom to fit to the page.
Info  **or** 	The Info tool appears when a single device is selected. When multiple devices are selected, the info tool icon with + appears. Click the Info tool to open the Device Details window.	The Info tool does not appear in the Dashboard topology view.
Last Scanned 	Informational only. Shows the number of days since the last scan occurred.	Informational only. Shows the number of days since the last scan occurred.

Using the Cisco OnPlus Scanner

After the customer has logged on to the Cisco OnPlus Portal, the Dashboard, Device Listing page displays if data has been scanned previously.

If you are logging in for the first time, the OnPlus Scanner page will open and the scanner will load. There is no saved or scanned data, therefore the Device Listing is blank.



To scan your network using the Cisco OnPlus Scanner, follow these steps:

STEP 1 Returning users, from the Dashboard page, click the green **Scan My Network** button.

Note: First-time user skip Step 1.

The Scanner page will display. As the scanner loads, an informational message will be displayed instructing the user to input parameters while the scanner is loading.

STEP 2 Enter the **IP Address Range** for your network.

Enter a single IP address (IPV4 address) for a single device search or when you are using CDP (Cisco Discovery Protocol) to discover devices in your network.

Enter an IP address range that includes all devices in your search by using the two entry fields.

Subnet masking can be performed by entering the IP Address in the first text box followed by index or subnet mask. For example, use a format similar to this 10.77.153.182/24 or 10.77.153.182/255.255.255.198.

Note: While on the OnPlus Scanner page, you can use the Help button at any time to get help with using OnPlus Scanner features.

STEP 3 Enter **Device Credentials.** Device Credentials can be Telnet, HTTP, HTTPS, or SSH.

a. Click **More** to add more credentials.

b. Enter one or two additional credentials.

Repeat the scan process as many times as needed to discover devices in your network that have different credentials.

Note: Device Credentials will be stored locally for successfully discovered devices. There is no need to re-enter credentials for devices that have been discovered in a previous scan.

STEP 4 Enter the scanning parameters that apply to your search.lease include the details about the credentials that will be stored locally in user system.

STEP 5

CDP Discovery can be used for discovering only devices in your network that are CDP enabled.

a. **CDP Discovery Level** cannot be set until the **Enable CDP Discovery** has been enabled. Set CDP Discovery Level to discover all neighboring devices up to level 5. (Default is 3).

b. If you are using CDP discovery, check the box next to **Enable CDP Discovery.**

c. Set **Connection Timeout** to control the length of your scan and to perform a more thorough scan.

You can adjust the scan in increments of 5 seconds, from 5 to 120 seconds.

d. **Upload Immediately After Scan** allows all devices that successfully scanned to be placed in your OnPlus inventory list. When left unchecked, scanned devices will not automatically transfer to the inventory list. This feature is checked by default.

e. Set **Connection Retry** to increase the number of auto-retries for your OnPlus Scanner to attempt. The maximum number of retries is 3. (Default number of retries is 0.)

f. **Enable Debug** provides log details when checked. This feature is checked by default.

STEP 6 Use the **Label Name** drop-down list to allow you to attach a label to the items that you are scanning. If you have not yet entered any labels, this list displays two options:

- **None** — No label will be attached to the scanned devices. (None is the default.)
- **<New>** — A New Label window will open where you can provide a label for the devices that you are about to scan. The label can be up to 20 characters including spaces. Labels are user-defined words that identify groups of devices to help manage network devices. For example, you may have devices on your network that belong to different cost centers. The labels will associate devices with their cost center.

Note: Labels can be entered and associated with devices after the scanned devices have been transferred to inventory. From the inventory list, you can create and assign labels to associate devices with groups.

STEP 7 Click **Scan**. See **Scanning Progress** to view results of your scan while it is processing.

If you click **Clear**, all the parameters you have entered will be erased.

STEP 8 Once the scan has completed with a Status of Uploaded nn/nn Successfully message, click **Finished.**

Clicking Finished closes the Scanner page and opens the Dashboard page to display the inventory list.

Note: Cancel can be used any time during the scan to the end the scan process. When you click **Cancel**, scanning ends and all the parameters that you had set remain available. You can change any of the parameters at this time, except the IP addresses. Click **Scan** and the scanning process restarts.

Scanning Progress

During the scanning process, messages are displayed that provide information about the scanning progress and success of the scan.

- **Started** provides the date and time that your scan launched.
- **Attempted** gives an actual count of the number of devices being scanned and shows a progressive percent completed.

When the scan in nearing completion, the following message will display when there are devices discovered with a status of Auth failed or Unreachable.

The Status field changes from Uploading to Uploaded nn/nn Successfully when the scan is completed.

Preview List

On the lower portion of the screen is a Preview List that shows you all the devices that have been scanned. The information provided in this list will help you determine when a rescan is necessary. The Preview List provides the following information:

- **Device IP** shows the IP address of the discovered device.
- **Status** shows one of the following scan results: Authentication Failed, Unreachable, or Success.
- **Device Name** appears for discovered devices.
- **Inventory Collected** provides a link to the data collected from the scanned device.

Using the information from the Preview List, you will be able to determine if you need to rescan your network and which type of rescan will be required.

Rescanning Your Network

After the scan has completed, you may need to rescan your network to discover devices that were not found in the initial scanning attempt. You can adjust any of the parameters except the IP address Range in a rescan attempt.

The reasons that rescanning may be necessary are:

- Credentials may have been entered incorrectly causing an Auth Failed status.
- OnPlus may have timed-out causing an Unreachable status.
- The scan attempt failed when using unsupported parameters, for example, attempting CDP discovery when CDP is not enabled on the devices being scanned.

Rescanning for an Auth Failed Status

To rescan when you have received an Auth Failed status, follow these steps:

STEP 1 Change the Device Credentials to match credentials used for devices in your scan.

STEP 2 Choose Auth Failed from the **Rescan Based On** drop-down list.

You can adjust **Connection Timeout** and **Connection Retry** to lengthen your scan.

STEP 3 Click **Rescan**.

Rescanning for an Unreachable Status

To rescan when you have received an Unreachable status, follow these steps:

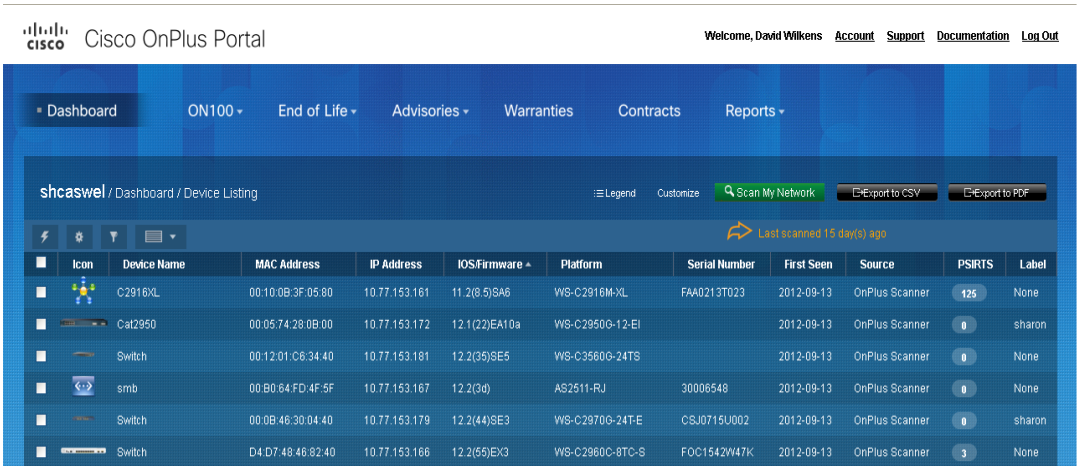
STEP 1 Increase **Connection Timeout**.

STEP 2 Choose Unreachable from the **Rescan Based On** drop-down list.

STEP 3 Click **Rescan**.

Using the Device Listing View

The Device Listing view is the default view for the Dashboard. It provides the following at-a-glance information:



Field Header	Description
Icon	The Icon is the visual representation of the device.
Device Name	A descriptive name that includes the product identifier.

MAC Address	A unique network interface address.
IP Address	A unique identifier that allows the device to communicate using the internet.
IOS/Firmware	The current IOS or firmware on the device.
Platform	The product identifier.
Serial Number	A product based unique identifier.
First Seen	The date that the device was scanned and added to the inventory.
Source	The device discovery method that was used to add the device to the inventory list.
PSIRTS	The product security advisory count.
Label	A user-defined tag used to group devices to meet customer needs.

Obtaining Detailed Device Information

To obtain detailed device information about a specific device in your inventory, follow these steps:

STEP 1 Place your cursor on the device you have chosen and click to open the **Device Information** window.

The fields are informational except for the **Label Name**.

STEP 2 Click the down arrow on **Label Name** to assign a predefined label to the device.

STEP 3 Click **OK** when you are finished.

If you click **OK**, you will close the Device Details window.

STEP 4 Click **Support** to open the **Contract Details** window. From the Contract Details window, you can also choose **Warranty** or **Hardware End of Support**.

Hardware end of life only appears as options when associated data is available for the device.

STEP 5 From the Hardware End of Support window, click the **End-of-support bulletin** URL to open the Product Bulletin for your selected device.

STEP 6 You may close the Product Bulletin window and return to the Device Details window.

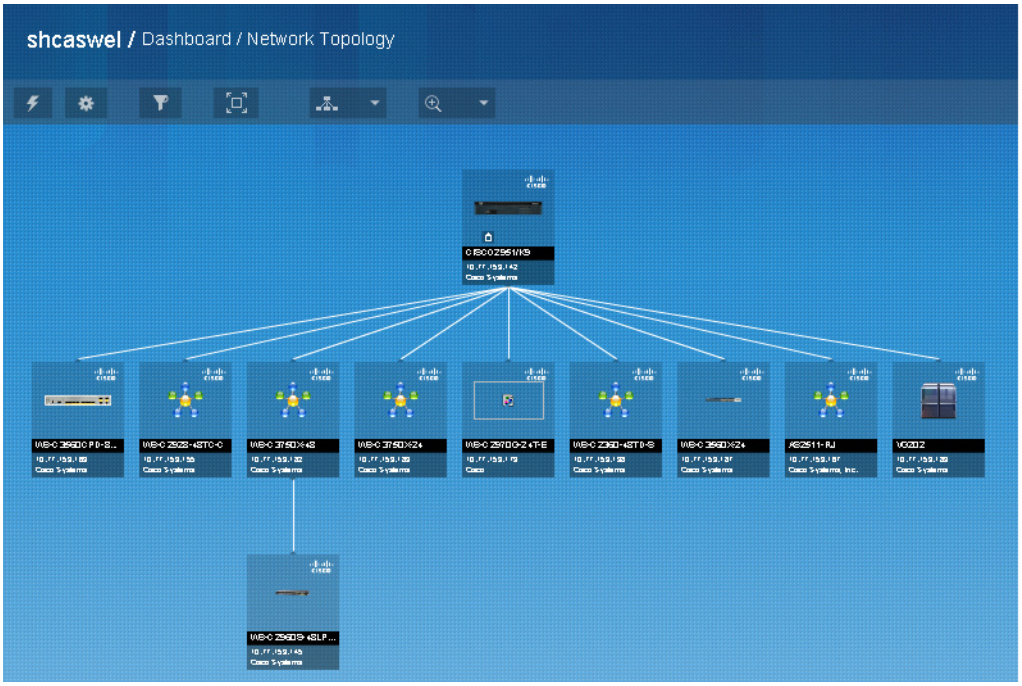
STEP 7 From the Device Details window, click **Info** to obtain detailed information about the device you have selected. Use the scroll bar to scroll through the item list.

STEP 8 Click **OK** to save any changes you have made.

NOTE You can easily switch to the Topology view by clicking the  Device Listing tool.

Using the Network Topology View

The Topology view shows the same devices that appear in the Device Listing view. In the Topology view, the devices display in a relational hierarchy that appears similar to the following illustration.



Device Info Window

To obtain or modify information about the device in the Topology view, follow these steps:

STEP 1 Select a device in the topology. From the menu that appears, click the  **Info** symbol. The Information window for the device will open.

There are five tabs on the Information window: Settings, Support, Info, Events, and Notes.

STEP 2 From the **Settings** tab you can perform the following functions:

- Unlock the **Device Name** to change it manually or allow it to be changed if another name for the device is discovered.
- Add or change the **Device Description**.
- Change the **Icon** by choosing another icon from the drop-down list.
- Change the **Category** by using a selection from the drop-down list.
- Apply a predefined **Label** from the selection in the drop-down list.
- From the **Actions** drop-down list, select an appropriate action.
- View MAC Address and IP Address.

STEP 3 Click **OK** to save your changes and return to the topology view.

STEP 4 From the **Support** tab, you can view **Contract Details, Warranty information**, **Product Security Advisories** and **Field Notices** by clicking the respective options.

Product Security Advisories and Field Notices only appear as options when associated data is available for the device.

STEP 5 Click **Hardware End of Support** to view information about the hardware end-of-support and to link to:

- End-of-support bulletin
- Migration Product URL

STEP 6 Click the **Info** tab to view detailed information about the device you selected.

STEP 7 Click the **Events** tab to view network events.

a. Click the **Show event with severity equal to or higher than** drop-down list to change the severity to view only the events within the severity level in which you are interested.

b. After you have changed the severity level, click **Refresh** to update the list.

STEP 8 Click the **Notes** tab to enter information about the device.

STEP 9 Click **OK**.

Creating a Lifecycle Digest Report

The type of Cisco OnPlus account that you have determines the type of report capability to which you have access. All customers have access to the Lifecycle Digest report.

- Lifecycle Digest is used to send the current device lifecycle status to customers that includes: contract, warranty, end-of-life, and advisories about the devices uploaded to OnPlus.
- Lifecycle Digest reports are sent using email in formatted HTML.
- The email notifications are sent at user-scheduled intervals, always delivered on Monday morning, and can be written in the language you choose.

To create a Lifecycle Digest report, follow these steps:

STEP 1 From the Dashboard page, choose **Reports** > **Lifecycle Digest Settings.**

STEP 2 The **Email Notification** checkbox is **On** by default. By clicking the **Off** checkbox, you will disable the Lifecycle Digest report option.

STEP 3 Fill in the required fields to set the delivery criteria.

- **Preferred Language** — Choose language from the drop-down list options.
- **Report Recipient** — Choose the email address from the drop-down list to which the report will be sent.
- **Frequency** — Choose the option from the drop-down list that best fits your needs. Reports can be delivered weekly, biweekly, or monthly.

STEP 4 From the **Categories** menu, select the options by placing a check in the box next to the option(s) that you want to appear in your Lifecycle Digest report.

STEP 5 Click **Save**.

The report provides links to detailed information for each entry. For example, if you click **View Details** at the end of the line that reports the number of warranties that are expiring, you will open the Cisco Onplus Portal and, after signing in, the Warranty Information page is displayed showing the expired warranties at the top of the warranties list. You can also link directly to the OnPlus Scanner from the report.

The links at the end of the report, **Helpful Link(s)**, let you change the frequency of the Lifecycle Digest report or discontinue the report completely. There is also a link that allows you to comment or offer suggestions about the Lifecycle Digest report.

The illustration shows the content of the Lifecycle Digest report.

Migrating from Cisco OnPlus Scanner to Cisco OnPlus ON100

Customers can migrate from a Cisco OnPlus Scanner account to a Cisco ON100 account, or choose to become a Cisco Registered Partner. As an ON100 Customer or as a Cisco Partner you will be able to take advantage of additional features and functionality that are offered by the Cisco OnPlus Service. To learn about the Cisco ON100 or about becoming a Cisco Registered Partner, from the Dashboard, choose **ON100 > Learn.** When the Cisco OnPlus Service page appears, you will find:

- A detailed video that explains the features of the OnPlus Scanner account and ON100 account
- A topics section called OnPlus for Customer
- A topics section called OnPlus for Partners
- A topics section called Cisco OnPlus Community

The Cisco OnPlus Service page includes more tabs with links to a wide array of information that will help you choose the best Cisco OnPlus options for you and your network.

Cisco OnPlus Scanner Supported Devices

Add the following devices as necessary to the Cisco Device Feature Support section:

- Cisco Catalyst 2000, 3000, 4500 & 6500 series switches and line cards
- Cisco Integrated Services Routers
- Cisco Wireless Access Points

5

Viewing Customer Networks

This chapter explains how to access and use the Dashboard to view details of your network or your customer's network using the Device Listing and Network Topology views.

- **Dashboard Overview and Features**
- **VLAN Discovery**
- **Using the Network Topology View**
- **Using the Device Listing View**
- **Viewing Customer ON100 Status**
- **Installing and Managing OnPlus Apps**

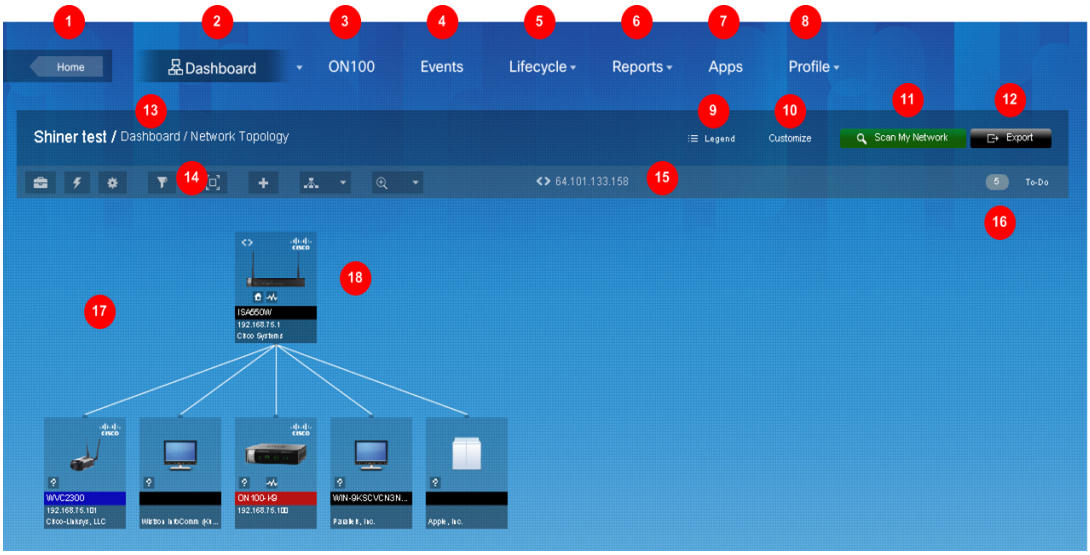
Dashboard Overview and Features

The Dashboard area of the Cisco OnPlus Portal provides the main interface to each customer's network. You can explore and interact with the customer's network using the hierarchical Network Topology view or the tabular Device Listing.

To access a customer's Dashboard from the main Overview page, click a customer in the customer list. By default, the Network Topology view of the customer's network appears.

NOTE If the customer site is still awaiting activation, selecting the customer will open the customer account by activating the OnPlus Scanner. If the customer account is currently suspended, the Dashboard displays a message that states, "This customer has been suspended. Some Dashboard features will not be available for this customer."

The following diagram highlights features and areas of interest on the customer's Dashboard:



1	Click **Home** to return to the main customer list page.
2	When highlighted, indicates that you are viewing the selected customer's network through the Dashboard.
3	Link to information about the Cisco ON100 Network Agent and activate an ON100 in your network.
4	View event history for this customer.
5	View contract, warranty, end-of-life, product advisories and field notices.
6	Create and schedule reports.
7	Install and manage OnPlus applications for this customer. See **Installing and Managing OnPlus Apps, page 81**.
8	View or modify customer profile settings. From the customer profile you can also delete or suspend the customer,
9	View information about what each of the icons, alarm, colors, and action icons represent.
10	Move your mouse over the Customize link to specify dashboard settings that are applied to the Dashboard for all customer networks.
11	Scan the network to discover Cisco devices and add them to the inventory.

12	Export a snapshot of the customer's network to one of the following formats: ▪ Portable Network Graphic (PNG) ▪ Scalable Vector Graphic (SVG) ▪ Comma-separated values (CSV)
13	Name of the currently selected customer.
14	Move your mouse over these toolbar icons to access tools, actions, and settings that are specific to the Topology view. See **Using the Dashboard Toolbar, page 62**.
15	Public IP address of this customer site.
16	Move your mouse over the To-Do list to view available actions and number of devices for which each action is available. See **Using the To-Do List, page 64**.
17	Event and condition notices appear here.
18	Network view area. In the above screenshot, the Network Topology view is shown. If Device Listing is selected, a tabular list of devices is shown here. See **VLAN Discovery, page 65** and **Using the Device Listing View, page 77** for detailed information about using these views.

To learn more about concepts and features that are available in both Dashboard views, read these sections:

- **Device Discovery, page 59**
- **Using the Dashboard Toolbar, page 62**
- **Using the To-Do List, page 64**
- **Filtering Devices in the Dashboard, page 64**
- **VLAN Discovery, page 65**

Device Discovery

The Dashboard views are generated automatically through scanning the network or ON100 device discovery.

Device Discovery Using the OnPlus Scanner

The OnPlus Scanner is used to find and add devices to your OnPlus inventory.

Each time the OnPlus Scanner is used, it creates or updates the inventory list giving the Customer access to a wealth of information about their network devices. For more information about using the OnPlus Scanner, see **Using the OnPlus Scanner to Discover Your Network, page 39**

Device Discovery Using the Cisco ON100

Device discovery begins when you activate the customer's ON100 device, and runs periodically. Depending on the size of the network, it may take several minutes to discover the network when you first activate a site.

The Cisco OnPlus Network Agent uses a combination of standard and proprietary mechanisms such as Bonjour, Cisco Discovery Protocol (CDP), Address Resolution Protocol (ARP), Simple Network Management Protocol (SNMP), Content Addressable Memory (CAM) tables and Universal Plug and Play (UPnP) to implement device discovery.

IMPORTANT Cisco routers (especially Cisco IOS routers) typically ship with discovery protocols disabled by default. For best results, enable discovery protocols such as CDP or Bonjour on the LAN interface to the router.

Discovery is also triggered automatically when new devices are added to the customer site. You can also manually trigger discovery (see **Manually Triggering Device Discovery, page 63**).

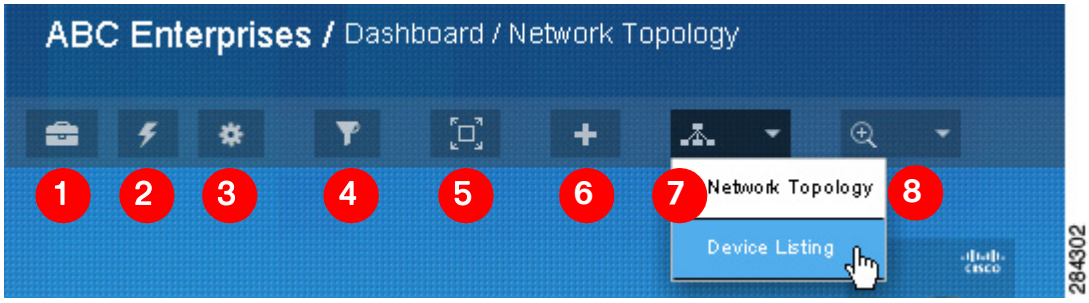
NOTE You may need to provide device access credentials to enable additional devices to be discovered (for example, managed switches, Cisco network devices, wireless access points, and routers). See **Credentials, page 90**.

Troubleshooting Common ON100 Device Discovery Issues

Issue	Possible Causes	Solution
Devices are present on the network but are not shown in the Topology.	Device access credentials are not entered for upstream devices such as routers, switches, or access points.	From the customer's Topology view, locate the upstream router, open the Device window, click the Credentials tab, and enter Login credentials and/or an enable password. See **Credentials, page 90**.
	Devices are located on a different VLAN or subnet from the Cisco OnPlus Network Agent.	If the upstream router is a Cisco router that is supported by the OnPlus Portal and it has visibility over multiple VLANS, additional discovery information can be obtained from the upstream router if device access credentials are provided. From the customer's Topology, locate the upstream router, open the Device window, click the Credentials tab, and enter Login credentials and/or an enable password. See **Credentials, page 90**. Non-Cisco devices and Cisco devices that are not supported, can be added manually to the topology (see **Manually Adding Child Devices, page 74**) or manually re-parented (see **Manually Editing Device Connections (Re-parenting Devices), page 75**.
Device is supported by the portal but are not shown or labeled as an “Unknown Device.”	Device does not advertise any of the supported discovery protocols, or discovery protocols have been disabled on the device for security reasons (or by default).	Enable Bonjour or CDP on the device. For some devices, you may need to provide a driver to enable discovery. From the customer's Topology, locate the affected device, open the Device Information window, click the Credentials tab, choose Driver, and select the appropriate device. See **Device Driver, page 93**.
Non-Cisco or unsupported Cisco device is shown as “Unknown Device.” See **Cisco Device Feature Support, page 241** for a list of Cisco devices supported by OnPlus.	Insufficient information obtained during discovery (the device does not advertise any of the supported discovery protocols, or discovery protocols are disabled for security reasons or by default).	From the customer's Topology, locate the device, open the Device window, click the Settings tab, and edit the device name, category, and description to identify the devices. See **Settings, page 88**.

Using the Dashboard Toolbar

The Dashboard toolbar is available in both the Device Listing and Network Topology views with tools that are available to Customers and Partners. For more details on how Dashboard Toolbar options are used in the Network Topology view, see Customizing Dashboard Settings, page 68.



Callout	Icon	Description
1		**Tools**. Move the mouse over this icon to access Ping Host and Nameserver Lookup tools for testing network connectivity and DNS. The **Cisco Support** option provides access to support tools for Cisco Small Business Support Center agents.
2		**Topology Reset and Site Actions**. Move the mouse over this toolbar icon to access options for resetting the topology and rediscovering the network. You can force closure of an open tunnel connection to a remote device, manually trigger device discovery, re-enable device alarms, or deactivate the entire customer site.
3		**Settings**. Move the mouse over this toolbar icon to access options for adjusting Topology layout and display settings. You can change the Topology layout mode (automatic or manual), set connection line opacity, set snap-to-grid options, and add custom device categories. You can add labels that will be used on individual devices or groups of devices to further define them.
4		**Filter Criteria**. Specify criteria to filter the devices that are shown in the Dashboard view. See Filtering Devices in the Dashboard, page 64.
5		**Full Screen Mode**. Network Topology only. Click here to go into full-screen mode. Press **ESC** to exit full-screen mode. Text input is disabled in full-screen mode.
6		**Add New Device**. Manually add a device to the Network Topology. See Manually Adding Child Devices, page 74.

Callout	Icon	Description
7		**Switch Among Network Topologies and Device Listing Views**. Move the mouse over this icon and choose to display the one of the Network Topologies or tabular Device Listing view.
8		**Zoom.** Network Topology view only. Choose a Zoom percentage for the Topology view or choose **Zoom to Fit**.

Manually Triggering Device Discovery

You can manually trigger device discovery from the Network Topology, the Device Listing view, or the Dashboard Toolbar.

- From the Network Topology view, move the mouse over the Cisco OnPlus Network Agent icon and choose **Device Information**. Click the Settings tab, choose **Trigger Discovery** from the Actions drop-down list, then click **Confirm**.
- From the Device Listing view, right-click the Cisco OnPlus Network Agent icon and choose **View Device Information**. Click the **Settings** tab, choose **Trigger Discovery** from the Actions drop-down list, then click **Confirm**.
- From the Dashboard Toolbar, select the **Topology Reset** and **Site Action** icon, choose **Misc. Actions**, then click **Trigger Discovery**.

Notification messages are displayed on the left side of the page under the Dashboard Toolbar. The initial message will state, Discovery Triggered.

NOTE There will be a delay of 30 to 60 seconds before the next message appears. Do not click Trigger Discovery during this period. The messages will resume, and at the end of the discovery process, a message states Inventory Task is Complete.

The Event Log records every event that occurs during discovery. To view the messages generated by the discovery process, select **Events** from the Dashboard Toolbar. From the Events page, select **Informational** from the Severity drop-down list.

Using the To-Do List

The Dashboard To-Do List feature enables you to quickly locate devices with conditions that may require action such as missing devices, devices that need access credentials, and devices with available firmware upgrades.

Click an item in the To-Do list to filter the view so that only the devices with that condition are displayed.

When you have finished performing actions or viewing device details, click **Show All Devices.**

Filtering Devices in the Dashboard

To access filtering options for the Network Topology and Device Listing views, move the mouse over the Filter icon  located on the Dashboard toolbar.

Specify the filter criteria as described in the following table, then click **Apply Search** to locate matching devices.

Click the **Clear all search criteria** link to clear the currently selected search options, close the Search window, and return to the Dashboard view.

Search Option	Description
Matching	**All of.** Only devices that match all of the search criteria are displayed in the search results. **Any of.** Devices that match one more of the search criteria are displayed in the search results.

Search Option	Description
Search Criteria	Specify one or more of the following criteria: ▪ Text in device names and descriptions. The search is not case-sensitive. ▪ Device class. ▪ Device category. ▪ Icon. Photo icons images are not searched. Only icons for devices that are actually in this customer's inventory are listed. ▪ IP addresses or MAC addresses containing the specified characters. ▪ Serial number, if obtained during discovery. ▪ Devices with serial numbers containing the specified characters. ▪ Devices with one or more monitors configured. ▪ Devices without any monitors configured.

VLAN Discovery

Cisco OnPlus Portal provides VLAN discovery, giving users connectivity across multiple VLANs. VLAN Discovery is established by connecting the ON100 Network Agent to a trunk port, providing connectivity and device discovery across multiple VLANs.

For more information about Cisco OnPlus VLAN discovery and configuration examples, see Cisco OnPlus VLAN Discovery application note, available on the Cisco OnPlus Support Community at the following URL:

https://supportforums.cisco.com/docs/DOC-17447.

Using the Network Topology View

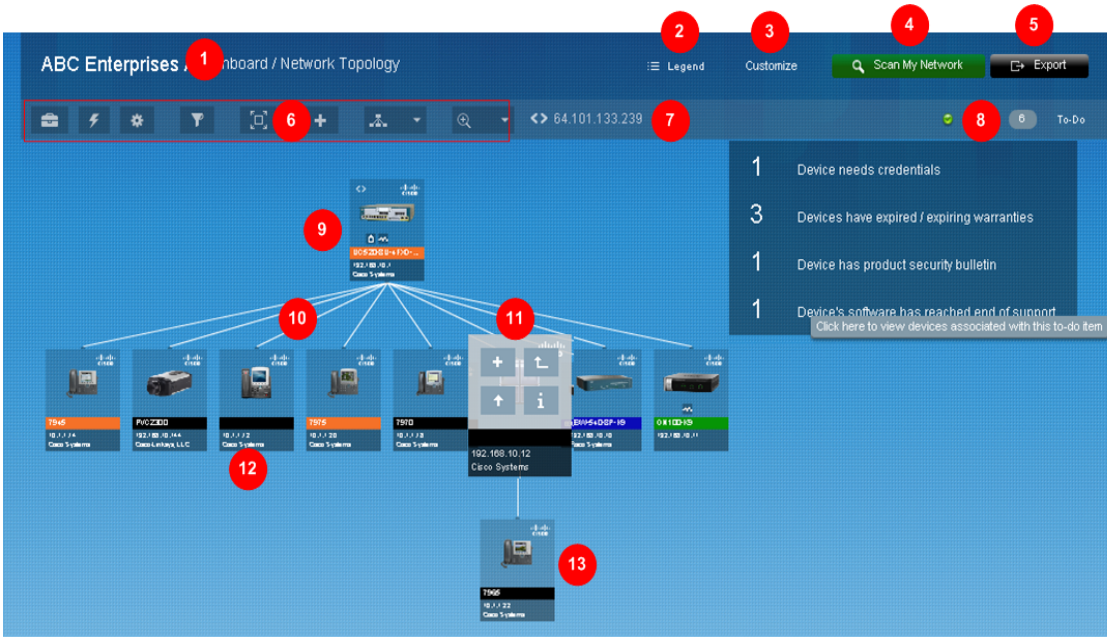
To display the Topology view from the main Overview page, click a customer in the list. By default, the Network Topology view appears, but you can change the default Dashboard view (mouse over the **Customize** link and choose **General Settings** > **Default View**).

To learn more, read these sections:

- **Network Topology Features, page 66**

Network Topology Features

Here is an example of a Topology view for a simple network. The callouts in the example indicate areas of interest in the Topology view.



Callout	Description
1	Name of the currently selected customer.
2	Click the Legend link to view information about what each of the action icons and alarm colors represents.

Callout	Description
3	Move your mouse over the **Customize** link to specify Dashboard settings that are applied to the Network Topology for all customer sites. See **Customizing Dashboard Settings**.
4	Open the OnPlus Scanner page.
5	Click to export a snapshot of the Network Topology view to a .png-format graphic, Scalable Vector Graphic (SVG) file, or Comma Separated Values (.csv) file that you can import into other applications.
6	Dashboard toolbar. See **Using the Dashboard Toolbar, page 62**.
7	WAN IP address. This is the public Internet IP address for the customer network, if it can be determined during device discovery.
8	Dashboard To-Do list. See **Using the To-Do List, page 64**.
9	Root device for the network, indicated by the  icon. See **Making a Device the Root Device for the Network, page 73**.
10	Device connection lines. See **Manually Editing Device Connections (Re-parenting Devices), page 75**.
11	For any device icon, roll the mouse over the icon to access options for adding child devices, making this device the root device on the network, expanding or collapsing subtrees, or opening the Device Information window.  You can also right-click the device icon and choose **View Device Information**.
12	OnPlus Network Agent. The highlight indicates that a firmware upgrade is available. The  icon indicates that monitors are configured for a device.
13	Subtree containing child devices. See **Expanding and Collapsing Subtrees, page 73** and **Manually Adding Child Devices, page 74**.

You can adjust the Topology view to add or modify devices and layout in the Topology view:

- If devices are not detected during discovery, you can still add them manually and edit settings to specify the device category and description

displayed in the Topology view. See Manually Adding Child Devices, page 74.

- If you have added devices manually and need to adjust the connection lines to show the correct relationships, use the **Link/Unlink** feature. See Manually Editing Device Connections (Re-parenting Devices), page 75.
- If discovery does not correctly identify the root device in the Topology (topically the Internet gateway router), choose **Make Root Device** from the Actions menu on the Settings tab in the Device Details popup window. See Making a Device the Root Device for the Network, page 73.
- See Troubleshooting Common ON100 Device Discovery Issues, page 61 for information about how to handle Unknown Devices (?) and devices not discovered.

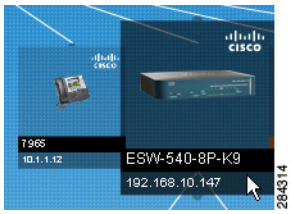
Customizing Dashboard Settings

To customize browser settings that apply to the customer Dashboard, move your mouse over the **Customize** link.

Click a category (for example, Topology Settings) at the top of the flyout menu to access its settings. These are explained in detail in the following table.

Your selections are saved for the device that you are using to access the portal. If you use a different device to access the portal, the default settings will be used, and you will need to re-enter your custom settings. Click **Reset Defaults** to access options for resetting all dashboard settings or settings for a specific category.

Category / Settings	Description
General Settings. These settings apply to both the Network Topology view and the Device Listing view.	
Default View	**Auto Select** determines the view based on the number of devices discovered on the network.(1 to 99 devices are displayed in the Topology view, 100 or more devices are displayed in the Device listing view.). **Topology** displays all devices in the Topology view regardless of the number of devices. **Device Listing** displays all devices in the Device listing view regardless of the number of devices.
Suppress Discovery Update Notices	When this option is enabled, discovery update notices are not displayed on the Dashboard.

Category / Settings	Description
Suppress Credentials Needed Notices	When this option is enabled, device credentials needed notices are not displayed on the Dashboard.
Suppress ALL Notices	When this option is enabled, popup notices are not displayed on the Dashboard.
Topology Settings. These settings are specific to the Network Topology view on the Dashboard.	
Zoom to fit on Startup	When this option is enabled, the Zoom percentage of the Network Topology is adjusted to fit within your browser window when you log in to the portal.
Enable Animation	Enable or disable animations in the Network Topology.
Show IP Address	Enable or disable display of IP addresses in the Network Topology.
Show MAC Address	Enable or disable display of MAC addresses in the Network Topology.
Show NIC Vendor	Enable or disable display of Network Interface Card (NIC) vendor name in the Topology.
Reverse ALT button use on background drag	By default, clicking and dragging with the ALT+LEFT mouse button in the Topology background pans the Topology view, and clicking and dragging with the LEFT mouse button selects multiple devices. When this option is enabled, these mouse button functions are reversed.
Vertical Spacing	Adjust vertical spacing between parent and child devices in the topology. This option can be used to improve the legibility of the topology view for large networks.
Enlarge device on mouse over, at lower zoom level	When this option is enabled, a larger version of the device icon appears when you move the mouse over the icon. This makes it easier to see the icons and text displayed on device icons. 
Hover menu appearance speed	Specify the length of time it takes for the device popup buttons to appear after mousing over a device icon in the Topology view. The range is from 50 ms (Minimum) to 1000 ms (Maximum).

Category / Settings	Description
Device Listing Settings Column visibility settings are specific to the Device Listing.	
Column Visibility	Check or uncheck columns to show or hide them in the Device Listing view.
Reset Defaults Restore default settings for category of Dashboard customization or all settings.	
Reset General Settings	Reset all custom General Settings to the default values.
Reset Topology Settings	Reset all custom Topology settings to their default values.
Reset Device Listing Settings	Reset all custom Device Listing settings to their default values.
Reset All	Reset all custom Dashboard settings to their default values.

Using Dashboard Toolbar Options

To access additional settings and actions that are applied to the Network Topology for specific customers, use the options on the Dashboard toolbar.

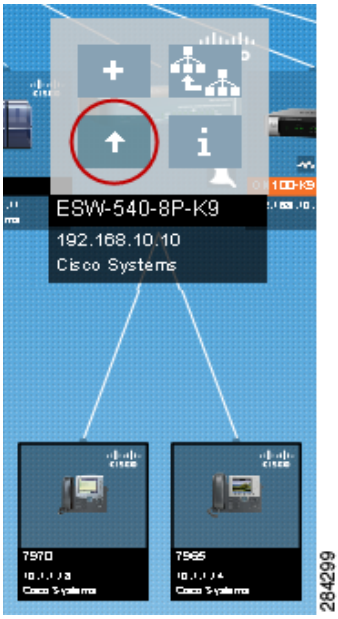
Icon	Category	Settings and Actions
	Tools	**Ping Host**. Enter an IP address or hostname, specify packet size and number of packets, and click **Execute** to test network connectivity.
		Nameserver Lookup. Enter an IP address or host name and click **Execute** to test DNS hostname resolution/server lookup.
		Cisco Support. Cisco Small Business Support Center troubleshooting tool access.

Icon	Category	Settings and Actions
	Site Actions	**Data Reset** **Reset Topology**. Reset the topology to the currently discovered state. Any edits to device connections to re-parent devices are removed. **Rediscover Network**. Remove all custom device settings, manually added devices, and device monitors, then run device discovery. Any edits to device connections to re-parent devices are removed.
		Misc. Actions **Trigger Discovery**. Manually trigger a device discovery update. **Force Disconnect**. Close the open tunnel connection to remote device, if one exists. **Re-enable Alarms**. Re-enable alarms for all devices.
		Deactivate Site. Remove this site and remote all customer data from the Cisco OnPlus Network Agent. The Cisco OnPlus Network Agent cannot be reactivated remotely.

Icon	Category	Settings and Actions
	Layout	**Topology Settings** **Tree Layout Mode**. Choose **Automatic** to use the automated hierarchical tree layout. The Snap-to-Grid option does not apply to Automatic layout mode. Choose **Free Form** if you want to reposition devices in the view and have your changes to the layout saved between sessions. In Free Form layout mode: ▪ No connection lines are drawn. ▪ There are no options for manually editing connections to re-parent devices, collapsing subtrees, or making a device the root device. You can still add child devices to any device. In either mode, you can: ▪ Drag the mouse over multiple devices and left-click to select them and reposition them as a group. ▪ Use SHIFT-click to add or remove devices from the selection. ▪ Selected devices are highlighted. When you change from Free Form to Automatic mode, all Free Form mode layout changes are removed. **Snap to Grid** (Free Form layout mode only). Enable or disable Snap-to-Grid in the Topology view. **Snap Grid Size** (Free Form layout mode only). Choose Small, Medium, or Large. **Connection Opacity**. Set opacity for the connection lines between parent and child devices in the Topology.
	Device Categories	To add a custom device category, click the Plus (+) icon, enter a name for the category, and click **Add**. After the category is added, it will appear in the list of available categories when adding a device manually.
	Filter Criteria	Specify criteria to filter the devices that are shown in the Dashboard view. See **Filtering Devices in the Dashboard, page 64**.
	Full-screen mode	Click this icon to enter full-screen mode. Press ESC to exit full-screen mode. Text input is disabled in full-screen mode.
	Switch views	Click this icon or use the drop-down list to switch between the Network Topology and Device Listing views.
	Zoom	Choose a Zoom percentage or choose Zoom to fit.

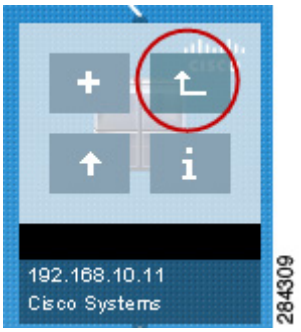
Expanding and Collapsing Subtrees

To expand or collapse subtrees with child devices in the Network Topology hierarchy, move the mouse over the icon for the parent device and click the Up or Down arrow icon to expand or collapse the subtree containing its child devices.



Making a Device the Root Device for the Network

The root device is used to parent other devices for which an accurate topology cannot be determined. If the root device on your network is not currently set to the device that new devices are most often connected to, locate the preferred root device from the Network Topology, click to select the device and click the **Make Root Device** icon.



Manually Adding Child Devices

Devices that are not found during the OnPlus Portal discovery process can be added to the site manually from the Network Topology view. Typically, these are devices that do not broadcast their identity and information using the discovery protocols used by the portal.

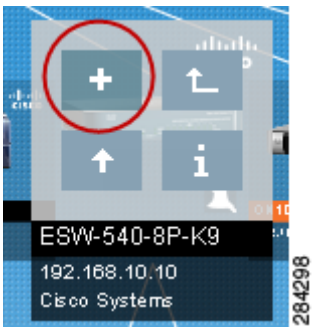
NOTE If devices that are behind a router, switch, or access point do not show up as expected in the Network Topology and Device Listing views, make sure that you have entered device access credentials the parent device before entering them manually.

To manually add a device to the customer site, follow these steps:

STEP 1 Open the Dashboard for the customer's site and display the Network Topology.

STEP 2 From the Network Topology view, locate the parent for the device you want to add.

STEP 3 Move the mouse over the parent device and click the plus sign (+) icon to add the child device. You can also click the Plus sign icon on the Dashboard toolbar.



STEP 4 In the Add New Device dialog box, choose a Category and a Device Type to associate an icon with the device. Complete the rest of the device settings. The parent device is the device to which the device is directly connected.

STEP 5 Click **OK**. The new device appears in the Network Topology under the parent device.

Deleting Manually Added Devices or Missing Devices

You can only delete manually added devices that have not been discovered through the portal's discovery process or devices that are identified as missing from the network. The following notes apply to deleting devices:

- After a device has been discovered, it is no longer marked as manually added and cannot be deleted from the Topology unless it is marked as "Missing" (not present on the network).
- If the deleted device is subsequently rediscovered, it is added to customer site and can be seen in the Network Topology and Device Listing views.
- You cannot delete the root device for the network.

To delete a device, follow these steps:

STEP 1 In the Network Topology view, click the Device Information icon for a manually added device or a device that has been identified as missing to open the Device window.

You can also right-click the device icon and choose **View Device Information**.

A plus sign icon  identifies manually added devices in the Network Topology.

Missing devices have a question mark  icon.

From the Device Listing view, select the device to be deleted in the list, then click the  icon that appears on the Dashboard toolbar.

STEP 2 From the Device window, click the **Settings** tab.

STEP 3 From the Actions menu, choose **Delete device**.

STEP 4 Click **Confirm**.

Manually Editing Device Connections (Re-parenting Devices)

You can manually edit the connections between devices in the Network Topology view.

Here are some tips for manually editing device connections:

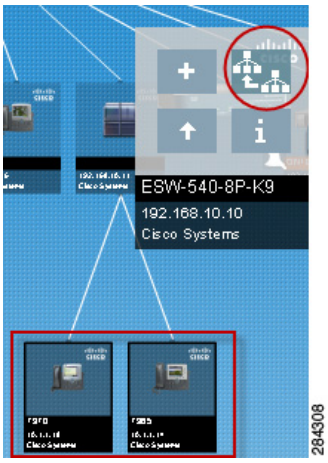
- After you have manually re-parented devices in the Topology view, automatic device discovery updates are not applied to manually re-parented devices.
- To remove manually edited device links and re-enable automatic device discovery updates, click the **Options** button on the Dashboard toolbar and choose **Reset Topology**.
- You cannot completely disconnect a discovered device from the topology. Devices that were added manually, but not discovered can be deleted from the topology, if needed.
- You cannot edit device connections to re-parent devices when the Topology view is being filtered.

To manually edit device connections by re-parenting devices, follow these steps:

STEP 1 In the Network Topology view, locate and select the device or devices that you want to relink. You can drag the mouse in the view, use CTRL-left mouse click or SHIFT-left mouse click to select multiple devices.

The selected devices are highlighted.

STEP 2 With the devices highlighted, move the mouse over the icon in the Topology view for the new parent device and click the  icon (**Make parent of selected devices**).



Reordering Sibling Devices in the Topology View

In Automatic Layout mode, you can reorder devices in the Topology view that are children of the same parent device. You may want to do this if you want to organize the view so that devices of the same type are grouped together.

To reorder devices that are children of the same parent device, select the icons for the device or devices that you want to move, then drag with the mouse to the left or right to reorder them.

NOTE If the devices in the Topology view are currently being filtered, you will have to disable filtering and show all devices in the view before you can reorder them.

Using the Device Listing View

To access the Device Listing view, click the  icon and choose Device Listing (or simply click the icon to switch between the Device Listing and Network Topology views).

From the Device Listing view, you can perform many of the same tasks as in the Network Topology view. Like the Network Topology, the Device Listing is updated automatically as new devices are discovered.

To make the Device Listing the default Dashboard view, click the **Customize** link, choose **General Settings**, and choose **Device Listing** for the **Default View**.

These columns are always displayed in the Device Listing:

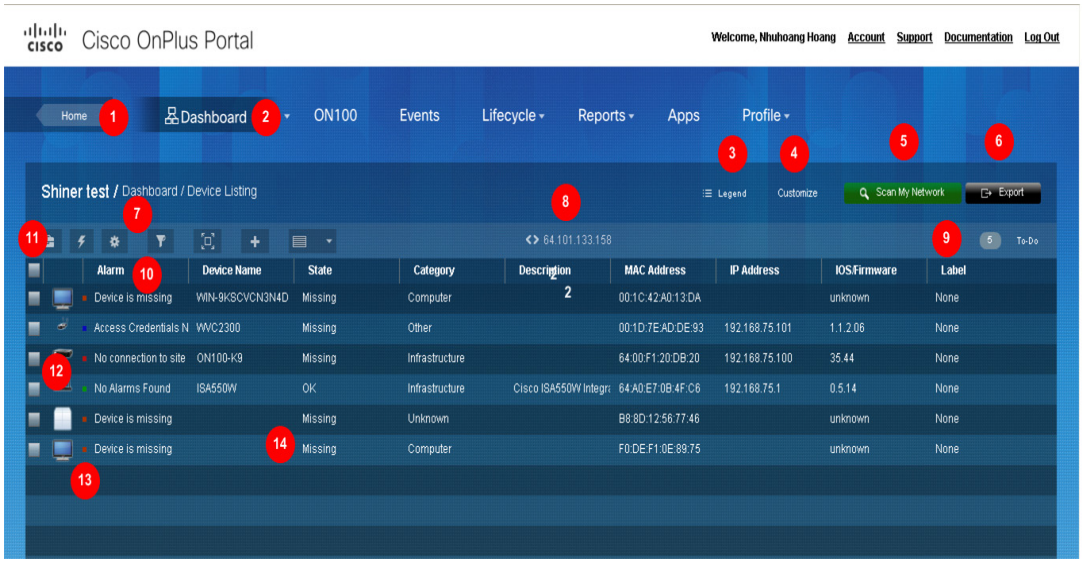
- Device selection checkbox
- Device icon
- **Alarm**. This column indicates the most recent conditions found, such as device credentials needed or firmware upgrade available.
- **Device Name**. This is the device name obtained during discovery or one that was entered manually.

The Device Listing view is covered in more detail in the following sections:

- Device Listing Features, page 78
- Customizing the Device Listing, page 79

Device Listing Features

Here is an example of a Device Listing view that shows available features and areas of interest in the view.



The callouts in the figure are listed and described in the following table.

Callout	Description
1	Click **Home** to return to the Overview page and the main customer list.
2	Indicates that the customer Dashboard is currently selected.
3	Move the mouse over the **Legend** link to see what the icons and alarm colors mean.
4	Move the mouse over the **Customize** link to add or remove columns in the Device Listing. See Customizing the Device Listing, page 79.
5	Scan the network to discover Cisco devices and add them to the inventory.
6	Export the Device Listing to a .csv-format file.

Callout	Description
7	Dashboard toolbar that includes options for using tools, specifying view settings, and filtering devices. See **Using the Dashboard Toolbar, page 62**.
8	WAN IP address (public IP address of this customer site).
9	Dashboard To-Do list. See **Using the To-Do List, page 64**.
10	Click the column headers in the Dashboard view to sort the rows in ascending or descending order.
11	Click the checkbox for a device to select it. When you select one or more devices, the Dashboard toolbar displays an  or  icon that you can click to access the Device window (see **Using Device Information Window Features, page 86**. Click the checkbox at the top of the column to select or deselect all devices. See **Editing and Performing Actions on Multiple Devices, page 103**.
12	Device icons. Right-click a device icon to access options for editing and performing actions on the device or opening a Web, RDP, or VNC connection to the device with the current connection parameters for that device. See **Working with Customer Devices, page 85**.
13	Color coded status indicates the level of alarms for the devices. The Legend (3) provides a description of each code.
14	The highlight indicates the currently selected customer.
15	Labels are user-defined tags that identify individual items or groups of items.

Customizing the Device Listing

To customize the Device Listing view, move the mouse over the **Customize** link on the Dashboard and choose **Device Listing Settings**.

Click the checkboxes to add or remove columns from the view. Click **Select All** or **Select None** to quickly toggle column selection.

Your selections are saved for the device that you are using to access the portal. If you use a different device to access the portal, the default settings will be used, and you will need to re-enter your custom settings. Click **Reset Defaults** to access options for resetting all dashboard settings or settings for a specific category.

Data Column	Description
State	The state can have one of these values: OK (discovery detects that the device is present), MISSING (if the device was previously discovered, but is not currently present), or ADDED (manually added device).
Category	General category for this device (for example, Infrastructure, Telephony, and so on).
Device Class	Device class information obtained during discover (for example, phone, switch, router, or unknown).
Device Type	Model number for this device, obtained during discovery.
Windows Information (WMI)	Information reported by the Windows Management Interface, if WMI access is enabled and the device supports WMI.
Description	User-specified device description.
First Seen	Time and date this device was first discovered on the network.
MAC Address	Unique, 12-character hexadecimal identifier for this device.
IP Address	LAN IP address of this device.
Monitors	Number of currently enabled monitors for this device.
Device Platform	Device platform information obtained during discovery. For some devices this is the same as the Device Type or Device Name.
Backup State	Date of last backup, if applicable. Displays Unsupported if the device does not support configuration backups using the portal.
Connection Settings	Currently configured web (HTTP/HTTPS) connection settings for this device.
Last Seen Via	Discovery protocols that last reported information about a device, for example, CAM, ARP, CDP, DHCP, DDNS, and so on.
Serial Number	Device serial number, if known.

Viewing Customer ON100 Status

To view the current status of the OnPlus Service:

- Check the Status column on the Partner Account Overview page. Mouse over the Status icon to view a description.
- Choose **ON100** from the customer's dashboard. The status can be:
  - **Activate.** The customer has been added, but the Cisco OnPlus Network Agent has not been connected to the customer network and activated with the portal.
  - **Activated, Online**. Normal operation.
  - **Activated, Offline**. Indicates that the ON100 is not communicating with the portal.
  - If the agent is connected to the customer's network, has power, and is not being rebooted or upgraded, but its status is Offline, it could mean that the customer's WAN connection is down. It is also possible that firewall settings on the customer network are blocking outbound traffic on ports that the agent uses to communicate with the portal (see **Port and Protocol Access Requirements, page 23**).

Additional customer status information can be obtained from the Profile page.

- **Account suspended**. The customer's account has been suspended. See **Suspending and Resuming a Customer Account, page 36**.

Installing and Managing OnPlus Apps

To view available Cisco OnPlus applications and install them follow these steps:

STEP 1 For a Customer Account, from the Dashboard page choose **Apps > App Store**

For a Partner Account, select the customer from the list on the Overview page, then from the customer's Dashboard page choose **Apps > App Store**.

Applications for Partner Accounts are added on a per-customer basis.

STEP 2 To begin adding and configuring an application, locate the application from the list. Click **Show All** to display the entire list of available applications.

You can sort the list of applications by name or price using the **Sort by** drop-down list.

Currently, the following services are available:

- **AIRMAGNET Planner for Cisco Small Business**. The OnPlus AIRMAGNET Planner for Cisco Small Business enables Partners to leverage offers from Cisco partnerships for scoping and planning a wireless deployment. To learn more, click the **Watch Video** button.
- **Advanced OnPlus Security.** Install and configure this application to enable enhanced security reporting, alerting, and monitoring that complements Cisco's current security appliances for Small Business.
- **Autotask**. Install and configure this application to integrate the OnPlus Portal with Autotask service ticketing. See **Integrating Autotask Service Ticketing, page 197**.
- **ConnectWise**. Install and configure this application to integrate the OnPlus Portal with ConnectWise service ticketing. See **Integrating ConnectWise Service Ticketing, page 211**.
- **ntop Packet Monitoring**. Install the ntop application on the Cisco OnPlus Network Agent. ntop can be used for packet monitoring using NetFlow or port spanning with output sent to the Cisco OnPlus Network Agent MON port. After the application is installed, you can launch ntop from the OnPlus Portal. See **Enabling ntop Packet Monitoring, page 223**.
- **Kaseya Service Desk**. Install and configure this application to integrate OnPlus Portal events with Kaseya Service Desk ticket management.
- **OnPlus Wireless Management**. Install this application for networks that have wireless access point equipment, such as WAP121 and WAP321, to enhance management and reporting capabilities.

STEP 3 To select the application you want to install, click the button below the application icon.

A message will appear that thanks you for your order, provides an order number, and states that an email has been sent with your order details.

You will receive and email containing the order details and links to Cisco OnPlus Support.

STEP 4 From the Apps page, click **My Account** to display the list of applications that you have ordered as well as other information needed to manage the applications.

STEP 5 To use the applications, you must:

- Configure settings in the application to enable integration with the OnPlus Portal.
- Configure application settings on the OnPlus Portal.

For more information about using the available applications, refer to the following links and resources:

- For Autotask, see **Integrating Autotask Service Ticketing, page 197**
- For ConnectWise, see **Integrating ConnectWise Service Ticketing, page 211**

For Kaseya, you must also set up delivery rules and contacts so that OnPlus Portal event notifications can be delivered to the Autotask or ConnectWise application to create service tickets. More information for using Kaseya is available using the links provided here.

The following application notes are available on Cisco.com at www.cisco.com/go/onplus-docs and also at the Cisco OnPlus Support Community at https://supportforums.cisco.com/docs/DOC-17447:

- *Integrating Autotask Service Desk Ticketing with the Cisco OnPlus Portal*
- *Integrating ConnectWise Service Desk Ticketing with the Cisco OnPlus Portal*
- *Integrating Kaseya Service Desk with the Cisco OnPlus Portal*
- *Cisco OnPlus for Small Business Wireless Deployments*
- *Enabling ntop Packet Monitoring with the Cisco OnPlus Service*
- *OnPlus ON100 VLAN Discovery*
- *Cisco OnPlus Advanced Security Application*

6

Working with Customer Devices

This chapter explains how to monitor and manage devices on customer networks through the OnPlus Portal. See the following sections:

- **Accessing the Device Information Window**
- **Using Device Information Window Features**
- **Windows Management Instrumentation (WMI) Support**
- **Editing and Performing Actions on Multiple Devices**

Accessing the Device Information Window

The Device Information window is the primary interface for interacting with the devices at the customer premises. From this window, you can view and edit device details and monitors, provide device access credentials, and perform actions on devices.

To open the Device Information window, follow these steps:

STEP 1 Open the Dashboard for the desired customer and locate the device that you want to access.

STEP 2 Use one of the following methods to open the window:

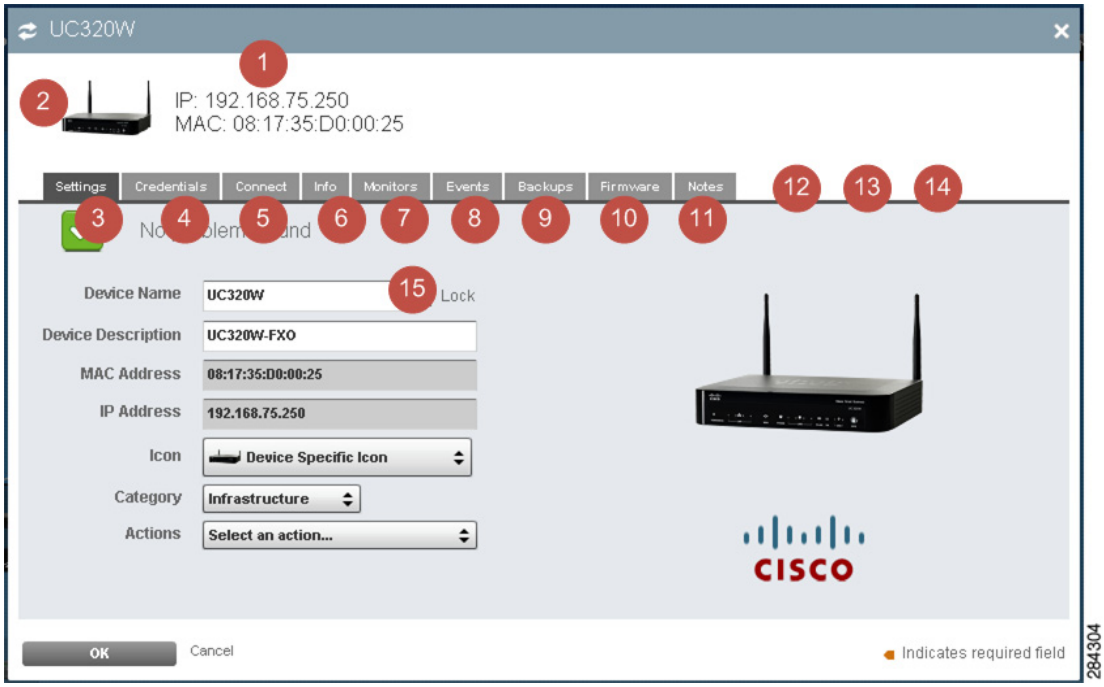
a. From the Network Topology view of the Dashboard, move the mouse over the icon for a device, then click the  icon.

b. From the Device Listing view, click the checkbox to select the device and click the  (Device Information) icon on the Dashboard toolbar.

Using Device Information Window Features

The following diagram illustrates the main features in the Device Information window.

If the device does not support a particular feature, the tab for that feature is not displayed.



Item	Description
1	The Device Information window titlebar displays the Device Name.
2	The device icon, IP address, and MAC address are displayed at the top of the window.
3	**Settings**. Perform actions on the selected device and view or modify settings to help you identify the device and its category.
4	**Credentials**. Provide device access credentials to enable features that require access to the device such as firmware upgrades, device scanning during discovery, or configuration backup and restore.
5	**Connect**. Manage remote connection settings and establish a remote connection to the selected device through the OnPlus Portal.

Item	Description
6	**Info**. View unformatted device information obtained for the selected device during discovery.
7	**Monitors**. View, add, and manage device monitors for the selected device.
8	**Events**. View event history for the selected device.
9	**Backups**. Back up, restore, download, or upload device configuration for supported Cisco devices.
10	**Firmware**. View, upload, download, or install firmware for supported Cisco devices.
11	**Notes**. Enter notes for the selected device.
12	**Support** (not shown). For supported Cisco devices, you can view warranty, serial number, field notices, service contract information, product security advisories, and end-of-life, end-of-service, or end-of-sale announcements. Service contract and warranty information may not be available for all Clsco devices.
13	**WAN Stats (WAN Network Performance Data)** (not shown). View WAN network performance data monitored using the Cisco OnPlus Network Agent and the device that provides the WAN link.
14	**Status area** (Settings tab only). Any alarms have been detected or actions that can be performed on the device are displayed here. Mouse over the status area to view more information. You can also enable and disable display of alarms.
15	**Device Name.** Displays information about the specific device.

See the following sections for detailed information on using the options on each of the tabs in the Device Information window:

- **Settings**
- **Credentials**
- **Connect**
- **Info**
- **Monitors**
- **Events**
- **Firmware**
- **Device Options**
- **Notes**
- **Backups**

- **WAN Stats (WAN Network Performance Data)**
- **Support**

Settings

These settings and action menus are available on the Settings tab:

- **Status area**. View status to see if any alarms have been detected or if there are actions that can be performed on the device.

  If multiple messages are present, roll the mouse over the status area to view them. To enable or disable the display of these alarms in the Device Information window, click the X icon to the right of each alarm.

- **Device Name**, **Device Description**. Enter a display name and description for the device. Alphanumeric characters, spaces, dashes (-), underscores (_), and colons (:) are allowed.

- Enable the **Lock** option to the right of the Device Name field to prevent the Device Name from being updated as device discovery runs.

- **MAC Address**, **IP Address**. View the MAC address and IP address discovered for the device. If the device was added manually and the MAC address or IP address could not be discovered, you can manually enter values in these fields.

  After the MAC address or IP address has been discovered, these fields become read-only.

- **Icon**. Choose a different icon to display for the device in the Dashboard view. This option does not apply to the Cisco OnPlus Network Agent. When **Device-specific icon** is selected, the icon reported during discovery is shown.

- **Category**. Choose a device category. Device categories are can be used for filtering devices in the Network Topology or Device Listing views.

  To add your own custom device categories so that they are displayed in this category list, mouse over the  icon on the Dashboard toolbar and choose **Device Categories**.

- **Actions**. Perform actions on the device. Click **Confirm** to perform the selected action.

Available actions vary, depending on the device you are viewing.

Action	Applies to	Description
Backup device configuration	Cisco devices that support configuration backup and restore using the OnPlus Portal	Request a configuration backup for this device. Make sure that you have provided valid access credentials for the device. If the device configuration has not changed since the last backup, no backup is created and a notice is displayed. See **Backups, page 97**.
Connect to device using the web	Any device	Open a web connection to this device using HTTP/HTTPS, using the current settings for the device. These settings are located on the Connect tab, under web in the Device Information window. For detailed procedures and information, see **Chapter 8, "Connecting to Devices from the Portal."**
Deactivate this entire site	Cisco OnPlus Network Agent only	Remove all associations and disable all communication between the Cisco OnPlus Network Agent and the portal. This option can be used in the case of a lost, stolen, or defective Cisco OnPlus Network Agent or when you want to reactivate the device, either with the current customer or with a different customer.
Delete this device	Missing or manually added devices that have not been discovered	Delete the selected device from the Topology. The device cannot be deleted if it will cause other devices in the Topology view to become disconnected from the rest of the hierarchy. This option applies only to devices that are missing from the network or have been manually added and never discovered.
Make this device "Root"	Any device	Make the selected device the root device for this customer's network.
Reboot device	Cisco OnPlus Network Agent only	Reboot the Cisco OnPlus Network Agent.
Trigger discovery	Cisco OnPlus Network Agent only	Manually initiate device discovery for the site.

Action	Applies to	Description
Upgrade firmware	OnPlus Network Agent only	Upgrade firmware on this device. The device is restarted after the upgrade. This option is only displayed when a firmware upgrade is available. The OnPlus Network Agent must be present in the network with an **Online, OK** status.

Credentials

The Credentials tab is active for most devices.

Several types of access credentials can be managed from this tab. To learn more, read these sections:

- **Login Access, page 90**
- **Enable Access (Cisco IOS Devices), page 91**
- **SNMP Access, page 92**
- **WMI Access, page 93**
- **Device Driver, page 93**

Login Access

Login access credentials are used for:

- Device scanning during discovery and topology updates
- Access to devices to perform maintenance functions such configuration backup and firmware upgrades

Login access options allow you to:

- **Enter login credentials to enable access to the device.** Additional network devices can be discovered (for example, phones or other devices behind a managed switch or router) and actions such as firmware upgrades or configuration backups can be performed. Device access credentials are also required for obtaining Cisco service contract and warranty information.

  TIP You must click **OK** after entering credentials in order to send them to the portal. It takes at least one discovery cycle for credentials to be validated. Wait a few minutes, then check the credentials tab to verify that they are valid.

- **Enable or disable login access for a device**. When **Allow Login Access** is unchecked (disabled), the Username and Password fields are disabled, device discovery does not attempt to go behind the device (topology scanning is disabled), and automated daily maintenance tasks are not run on the device.
- **Delete existing credentials for a device**. To remove credentials for a device, check the **Delete existing credentials** option, then click **OK** and close the window. The next time you access the tab, the credentials fields will be empty and you can add new credentials.

If the Username and Password fields are outlined in a glowing Blue color, it indicates that the Cisco OnPlus Network Agent could not access the device. the portal To-Do list will also indicate that credentials are needed.

To enable access, enter the username and password for the device and click **OK**. If the credentials are valid, the Connect tab updates to indicate that the device is accessible. Additional devices discovered are then displayed in the Network Topology and Device Listing views.

If the username and password are later changed and the device cannot be accessed by the Cisco OnPlus Network Agent, an **X** and the message **Credentials were invalid when last tried** in the credentials status area. The credentials fields will also be highlighted in Blue.

Enable Access (Cisco IOS Devices)

For Cisco IOS devices, the administrator can specify a separate password that users must enter to access `enable` mode (the default), or a specific privilege level.

You must enter the enable password to be able to back up or restore configuration or upgrade firmware on these devices.

SNMP Access

From the SNMP (Simple Network Management Protocol) Access tab, you can enable or disable SNMPv2 or SNMPv3 management access by entering SNMP credentials. SNMP management access currently is used only to enable firmware upgrades and configuration backup and restore on Cisco SF300 and SG300 devices and to obtain additional discovery information for generic managed switches.

IMPORTANT Before enabling SNMP management access through the portal, you must configure and enable SNMP on the device. Refer to the documentation for the device for information about which versions of SNMP (v2 or v3) are supported on the device.

Limitations. The following limitations apply to SNMP management access through the OnPlus Portal:

- After you enable SNMP management access for a device using the portal, the portal always uses the SNMP access credentials for authentication. To change this, you must remove the SNMP access credentials and disable the SNMP service.
- SNMP authentication access uses passphrases only; keys are not supported.
- The default Engine ID is always used.

OnPlus-supported Cisco devices.The only OnPlus-supported Cisco devices that support both SNMP v2 and SNMP v3 are the SG300 Series and SF300 Series switches. See **SF300 or SG300 (v1.1 Firmware), page 266** and **SF300 or SG300 (v1.1 Firmware), page 266** for information about steps needed to configure SNMP management access using the portal on these devices.

Generic Managed Switches or Generic Managed Routers (non-OnPlus-supported Cisco devices and non-Cisco devices). These devices show up as Unknown Devices in the Topology (discovery for unsupported devices is not guaranteed). To identify these devices, enable and configure SNMP settings on the device, open the Device Information window on the portal and click the **Credentials** > **Device Driver** tab, choose **Generic Managed Switch, SNMPv2/3** or **Generic Managed Router, SNMPv2/3**, and click **OK**. Finally, go to the **SNMP Access** tab, enter SNMP credentials, and click **OK**. After the next discovery cycle completes, any additional information that is discovered will be displayed, and the device icon will show “SNMP.”

WMI Access

WMI Access credentials are used to provide additional discovery information for Microsoft Windows PCs.

When WMI access is enabled for a Windows PC, the following WMI information is collected and displayed on the Information tab in the Device Information window:

- Service Pack, major version
- Service Pack, minor version
- Total visible memory size, in kbytes (for example, a value of 2061856 is approximately 2 GB)
- Name (actual Windows name of this PC)
- Description (Windows description for this PC)
- Platform (Windows operating system platform, for example, Microsoft Windows XP Professional)
- Operating System (same as the platform). For example: Microsoft Windows XP Professional
- Serial number for the Windows OS installed on the PC

For information about enabling WMI access on your customer's PCs, entering credentials, and adding WMI monitors to devices, see **Windows Management Instrumentation (WMI) Support, page 100**.

Device Driver

For Cisco devices that have been automatically discovered, the message "A driver has been discovered for this device, and is in use" is displayed.

Some Cisco devices do not support any form of identifiable discovery or may be configured so that discovery protocols are disabled (for example, for security reasons). As a result, these devices may appear as Unknown Devices in the customer's Network Topology or Device Listing view, and the message "Unable to automatically identify the appropriate driver for this device" is displayed.

For information about selecting generic drivers for Cisco IOS devices and non-Cisco devices, see Generic IOS Router and Generic IOS Switch Device Drivers, page 94 and Generic SNMP Device Drivers, page 94.

To obtain discovery information for these devices, follow these steps:

STEP 1 On the Credentials tab, click **Login Access** and enter login credentials for the device. See Login Access, page 90.

STEP 2 If needed, click **Enable Access** on the Access tab and enter the enable password for the device. See Enable Access (Cisco IOS Devices), page 91.

STEP 3 If you are selecting one of the SNMP device drivers, make sure that you have enabled SNMP on the device and entered SNMP access credentials. See SNMP Access, page 92.

STEP 4 On the Credentials tab, click **Device Driver**.

STEP 5 Choose the appropriate device from the pull-down list of supported Cisco devices.

STEP 6 Click **OK**.

Generic IOS Router and Generic IOS Switch Device Drivers

To improve discovery for Cisco IOS devices that are not currently supported by the OnPlus Portal, select **Generic IOS Router** or **Generic IOS Switch** as the device driver.

Before selecting the Generic IOS Router or Generic IOS Switch device driver, you must:

- Enable CDP and CDP Neighbor on the device.
- Provide Login and Enable Access credentials on the OnPlus Portal. See Login Access, page 90 and Enable Access (Cisco IOS Devices), page 91.

The generic Cisco IOS device drivers provide discovery and cross-launch capability using the portal. Device configuration backup and restore and firmware upgrades, using the portal are not supported.

Generic SNMP Device Drivers

To improve discovery for non-Cisco devices, use the Generic SNMP device driver.

Before selecting the Generic SNMP device driver for a device, you must:

- Enable SNMP on the device.
- Enter SNMP access credentials on the portal.

The Generic SNMP drivers use a MIB called QBRIDGE to get CAM table information. If the device supports QBRIDGE, the CAM table information includes VLAN information, in addition to the MAC address and port. This indirectly provides information about all VLANs in use, as long as they can be seen on the switch. Some additional topology could also be discovered if QBRIDGE is supported. If the device does not support QBRIDGE, the BRIDGE MIB is used, which does not include VLAN information.

The generic SNMP device driver provides discovery and cross-launch capability using the portal. Device configuration backup and restore and firmware upgrades using the portal are not supported.

Connect

From the Connect tab, you can connect to a device remotely from the portal to access its management utility.

The options that you specify depend on the type of remote connection that you select. web (HTTP/HTTPS), Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and generic tunnel connections to a single TCP port are supported.

For important limitations and guidelines on the use of this feature, troubleshooting tips, advanced options, and recommended connection settings for Cisco devices, see **Chapter 8, "Connecting to Devices from the Portal."**

Info

The Info tab displays read-only information about each device that is gathered during device discovery. The information varies, depending on the type of device, and can include the SKU (platform), MAC address, firmware version, IP address, management protocol, management port, capabilities, model, and serial number.

Refer to the Description column for each field for more information about what the data represents.

If WMI access is enabled for a Windows PC, additional information is displayed. See **Windows Management Instrumentation (WMI) Support, page 100**.

Monitors

From the Monitors tab, you can add, delete, or pause event monitors for a device. Depending on the type of device that you are monitoring, different event monitors are available.

For devices other than the Cisco OnPlus Network Agent and the device that provides the WAN link, this tab will be blank when you first access it because event monitors have not yet been added.

NOTE Event monitors on the Cisco OnPlus Network Agent (Network Performance, CPU Load, Duplicate IP, DHCP Server, DNS Service, and Memory) are enabled by default. The monitors on the Cisco OnPlus Network Agent and cannot be deleted, but they can be disabled. You can set severity levels and edit settings for these monitors.

For more information, see **Adding and Managing Device Monitors, page 119**.

Events

For devices with monitoring enabled, this tab shows the event history for this device. Events in the list are color-coded by severity. The currently selected event is highlighted in Blue.

To learn more about event types, see **Event Types, page 130**.

For instructions on how to monitor events and how to set up delivery rules and contacts for receiving event notifications, see **Monitoring and Notifications, page 107**.

Device Options

The Device Options tab offers you the option of entering SMB credentials, which can be used to authenticate with Windows servers. This tab provides enhanced discovery while eliminating Windows Security Event Log entries that might otherwise be generated. SMB discovery is enabled by default; you can disable SMB discovery by unchecking the SMB Discovery Enabled checkbox.

Firmware

From the Firmware tab, you can view, install, upload, or download previously uploaded firmware for Cisco devices. This tab is not displayed for non-Cisco devices and Cisco devices that do not support firmware upgrades through the portal.

For more information, see **Uploading Device Firmware to the Portal, page 153** and **Installing Device Firmware, page 154**.

Notes

Use the Notes tab to record textual information about a remote device at a customer site. Add, modify, or delete your text and click **OK**.

Backups

Once every 24 hours, during the maintenance period for the customer site, the configuration for each supported device is backed up if it has changed. The five most recent backup operations are displayed on the Backups tab in the Device Information window.

This tab is only displayed for Cisco devices that support configuration backup and restore through the OnPlus Portal.

For selected Cisco devices, you can back up, restore, or upload device configuration using the options on the **Backups** tab.

- Valid access credentials are required for backup and restore operations. Some Cisco devices may require an enable password, in addition to login credentials. See **Credentials, page 90**.
- Up to five configuration backups can be archived for each device. The **Origin** column indicates whether the backup was generated directly from the device or uploaded to the device.
- Optional comments that were entered for a configuration backup file are also displayed here. Select the backup file and open the details drawer to edit or add comments.
- You can restore a previous device configuration from one of the stored backups or you can upload a configuration file to restore.

For more information, see:

- Requesting a Device Configuration Backup
- Uploading a Device Configuration File
- Downloading, Deleting, and Restoring Device Configuration Files

Requesting a Device Configuration Backup

Click **Backup Now** to request an immediate device configuration backup. When you click **Backup Now**, the portal displays a notice that the backup has been requested. If the portal detects that the configuration is unchanged, you are notified and a backup is not created.

Uploading a Device Configuration File

Click **Upload File** to upload a device configuration file to the OnPlus Portal. This enables you to distribute known working configurations to target devices.

IMPORTANT Since devices vary in how configuration files are interpreted, you are responsible for the completeness, format, structure, and integrity of the configuration file being sent to the device. For example, some devices can accept and apply partial configuration files; other devices may require that you replace the entire configuration.

The Cisco OnPlus Portal does not validate or perform any checking on the format or content of the uploaded file.

Downloading, Deleting, and Restoring Device Configuration Files

To access options for adding comments, downloading, deleting, and restoring device configuration files, move the mouse over the desired backup file and click the highlighted entry to open the details drawer.

- In the **Comments** field, add or modify comments for the selected backup.
- Click **Restore** to restore a configuration by reapplying a previously saved configuration file to a device, making that the current configuration.

  When you click **Restore** to choose a backup to be restored, a message appears that a restore has been requested and you are prompted to confirm the operation. The device is restarted after the restore operation completes.
- Click **Download** to download the backed up device configuration file to your local machine.
- Click **Delete** to remove the backup file stored on the portal.

WAN Stats (WAN Network Performance Data)

The WAN Stats tab is active only on the Cisco OnPlus Network Agent. From this tab you can view WAN network performance data collected by the agent. The data is displayed as graphs of jitter, latency, and packet loss.

WAN statistics that are available in reports include:

- **Latency.** Latency is the average round-trip time between the Cisco OnPlus Network Agent and the OnPlus Portal measured over 50 packets separated by 100 milliseconds. One sequence is run every 5 minutes. In general, spikes in latency may indicate network congestion between these two points in either direction.
- **Jitter**. Per-packet jitter is the deviation from the average latency as measured over the last 10 packets. Jitter is the average of the per-packet jitter, which is measured over 40 samples.
- **Packet loss**. Packet loss is the percentage of total packets sent that did not return.

When you first click this tab, the following message appears:

“Data is not currently available for graphing.
A request has been sent to retrieve bandwidth data from your appliance. It may take several minutes to appear. You may return later if you wish.

Click **OK** to close the window. You can also leave it up until the graph appears.

After several minutes, the graph updates to display the default graph, which shows Jitter/Latency over time. Jitter is graphed in Blue; latency is graphed in Brown. Roll the mouse over bars in the graph to view details.

You can adjust graph parameters for the time period, graph data (jitter and latency or packet loss), and interpolation type (curve, linear, stepped).

Support

For Cisco devices, if device access credentials are provided and the Cisco product serial number and Product ID are obtained during discovery, Cisco product information is displayed here.

If the device is not a Cisco device or if product support information is not available for the device, the Support tab does not appear.

For more information, see **Viewing Cisco Product Support Information, page 181**.

Windows Management Instrumentation (WMI) Support

When you enable WMI access for Windows PCs, the portal uses the Windows Management Instrumentation interface to obtain device information and set up device monitors.

IMPORTANT The information provided here for enabling WMI access on Windows PCs is not intended to be comprehensive and may not cover all issues related to enabling WMI and configuring remote WMI access.

- Before attempting to enable WMI access through the OnPlus Portal, make sure that remote WMI access is successfully configured and working on your customer's PCs.
- For more information, consult the Microsoft documentation for the version of the operating system running on the Windows PC or the Microsoft support knowledge base.

For details, see these sections;

- **Enabling WMI Access, page 100**
- **Adding WMI Device Monitors, page 102**
- **Disabling WMI Access and Removing Access Credentials, page 103**

Enabling WMI Access

To enable WMI access on the WIndows PC and enter WMI access credentials in the portal, follow these steps:

STEP 1 On the Windows PC, perform the following steps to enable WMI access:

a. If the PC is running Windows Vista or Windows 7, disable User Account Control (UAC).

b. If the PC is running Windows XP, make sure that Simple File Sharing is disabled. To do this, choose **Start > Control Panel > Folder Options**. In the Folder Options dialog box, select the View tab and scroll down to the bottom. Verify that **Use Simple File Sharing** is unchecked. You should not have to restart the PC after changing this option.

c. Enable WMI and DCOM services in Windows. To do this, go to Start > Run, type services.msc, then press Enter.

d. Start the **Windows Management Instrumentation** and **DCOM** (Distributed Common Object Model) services if they are not already running and verify that the Startup Type is set to **Automatic**.

e. Enable remote WMI requests.

You may need to restart the PC after changing these options to enable remote WMI requests.

The following Microsoft support page provides help and troubleshooting information for computers that are members of Windows domains that may have group policies configured that could interfere with remote WMI over DCOM:

http://support.microsoft.com/kb/875605

STEP 2 From the Overview page, click a customer to display the Dashboard for that customer.

STEP 3 From the Network Topology or Device Listing view for the customer, locate a Windows PC with WMI access enabled and click the Device Information (i) icon to open that Device Information window.

STEP 4 From the Device Information window, select the **Credentials** tab and click **WMI Access**.

STEP 5 Enter the following information:

- **Username and Password** — Windows account username and password. You can give any account the ability to read WMI information. For example, you can create an account that is only used for WMI access.
- **Domain (optional)** — If the computer is a member of a domain, you can specify it. The domain field is required only if the account is a domain account. If you enter a domain, but the account is not a member of a domain, the information is ignored.

STEP 6 Check the option to **Allow WMI Access** to enable this feature.

STEP 7 Click **Confirm**.

For related information, see **Adding WMI Device Monitors, page 102** and **Disabling WMI Access and Removing Access Credentials, page 103**.

Adding WMI Device Monitors

You can add one or more WMI monitors to a Windows PC to monitor the amount of free disk space, memory usage, and whether or not a specific process is running on the PC being monitored.

You can add as many WMI monitors as you need.

These guidelines and notes apply to WMI monitoring:

- Before you monitor events through WMI, you must enter WMI access credentials and make sure that the WMI access is enabled for the Windows PC. For instructions on how to do this, see **Enabling WMI Access, page 100**.
- WMI monitors should only be set on Windows devices that support WMI.
- When WMI monitoring thresholds for disk space and memory usage are exceeded, a Monitor: WMI event is generated. When the values being monitored drop below the thresholds, a Monitor: WMI event is generated.
- For a Process Exists WMI monitor, an event is generated if the process name is ever detected as not currently running on the machine. An event is generated when the monitor detects that the process is running again.

The parameters listed here can be set for these monitors.

Monitor	Parameters
Disk Drive Status	▪ Warning states: Degraded, Pred Fail, Stressed, Unknown ▪ Critical states: Error, Service, NonRecover, No Contact, Lost Comm
Disk Free Space	▪ Volume label (for example, C:) ▪ % Free space Warning threshold. The default is 10%. ▪ % Free space Critical threshold. The default is 5%.
Memory Free	▪ % Free Memory Warning threshold. The default is 5%. ▪ % Free Memory Critical threshold. The default is 2%.
Process Exists	▪ One or more process names (for example, winlogon.exe). Use commas to separate multiple items in the list.

Disabling WMI Access and Removing Access Credentials

You can temporarily disable WMI access without removing previously entered credentials or you can completely remove existing WMI credentials.

When WMI access is disabled on a device, any WMI monitors on that device do not generate further events until WMI access is re-enabled. The monitors are not disabled, and they are automatically resumed when WMI access is allowed again. If you do not want the WMI monitoring to resume automatically after access is re-enabled, disable the WMI monitors.

If any WMI monitors are added to a device and WMI credentials are not supplied in the Credentials tab (or existing credentials are deleted), the device icon on the Network Topology is highlighted immediately. When you access the device for editing, the Credentials tab is automatically selected.

To edit WMI access settings, follow these steps:

STEP 1 Open the Dashboard for the customer and locate the Windows PC with WMI access enabled.

STEP 2 From the Network Topology or Device Listing, open the Device Information window, select the Credentials tab, and click **WMI Access.**

STEP 3 To temporarily disable WMI access but retain existing WMI access credentials, uncheck the **Allow WMI Access** option, then click **OK**.

STEP 4 To remove existing credentials and disable WMI access, uncheck the **Delete existing credentials** option, then click **OK**.

Editing and Performing Actions on Multiple Devices

You can select and open multiple devices for editing or perform selected actions from either the Topology view or the Dashboard view.

The following limitations apply to editing multiple devices:

- You cannot open multiple, simultaneous connections from the portal to multiple devices. Only one remote connection (web, RDP, VNC, or generic tunnel) at a time can be opened.

- Actions that you can perform on multiple selected devices include the following (assuming that the action is supported on all of the selected devices):
  - Back up device configuration
  - Reboot device
  - Delete missing or manually added devices
  - Re-parent devices
- When editing Monitors for multiple devices, all existing monitors are deleted (except network monitors on the Cisco OnPlus Network Agent, which cannot be deleted) and replaced with the new monitors.

  You are prompted to confirm the Monitor reset action before continuing.

To select and edit settings or perform actions on multiple devices, follow these steps:

STEP 1 On the Overview page, click the entry for the customer whose devices you want to edit.

STEP 2 To select the devices:

- In the Network Topology view, hold down the SHIFT key or CTRL key and left-click with the mouse at the bottom of device icons to select the devices to be edited. Selected devices will highlight.

  You can also left-click and drag with the mouse to select a group of devices and use Shift-click to add and remove devices from the selection.

  With the devices selected, move the mouse over any one of the selected device icons, then click the  icon.
- In the Device Listing view, click the checkboxes for the devices that you want to select.

  With the devices selected, click the  icon at on the Dashboard toolbar.

Tabs, settings, and actions that are valid for any of the selected device types are available for editing. Settings that are currently configured with different values for the selected devices are also identified.

STEP 3 Choose a setting to edit or an action to perform.

If you are applying an action, such as a device reboot or configuration backup, the window updates to list the devices to which the action will be applied.

STEP 4 Click **OK** to apply settings, click **Confirm** to perform the selected action, or click **Cancel**.

7

Monitoring and Notifications

This chapter explains how to use the Cisco OnPlus Portal device monitoring and event notification delivery features. These topics are covered:

- **Overview**
- **Default Delivery Rule and Contact**
- **Adding and Managing Delivery Contacts**
- **Using Delivery Rules**
- **Adding and Managing Device Monitors**
- **Viewing Events**

Overview

The monitoring and notifications feature of the OnPlus Portal enables you to receive email or SMS text message notifications when monitored events occur. This section covers:

- **Types of Events That Can Be Monitored**
- **Event Notifications**
- **Process for Setting Up Monitors and Notifications**
- **Step-by-Step Example for Monitoring and Notifications**

Types of Events That Can Be Monitored

Through the Cisco OnPlus Portal and Cisco OnPlus Network Agent, you can monitor:

- **Network performance**. A set of default network monitors on the Cisco OnPlus Network Agent are enabled. These monitors generate events when

the specified thresholds are exceeded or conditions are met for the following items:

- WAN network performance (jitter, latency, bandwidth)
- Duplicate IP addresses
- DHCP service availability
- DNS service
- Cisco OnPlus Network Agent connectivity, CPU load, and memory usage

- **Actions on the Portal**. Other events are generated by monitoring portal activities such as firmware upgrades, device restarts, configuration backup or restore, device discovery, and so on. Most of these generate events with a severity level of notice.
- **Cisco Support information notices**. Support events include product end-of-life, end-of-support or end-of-sale notices, service contract expiration, product security advisories, and warranty expiration.
- **Customer devices**. See **Device Monitor Descriptions, page 123** for detailed information about the types of events you can monitor on your customer's devices.

Event Notifications

To receive event notifications using email or SMS message, you must create *delivery contacts* and *delivery rules*:

- Delivery contacts are used to specify the recipient of the notification and the delivery methods that can be used (email or SMS text message).
- Delivery rules allow you to specify criteria for delivering event notifications. The contact and delivery method specified in the rule determine how and to whom the message is delivered.
- Only one contact can be associated with a delivery rule.

A default delivery rule and contact are automatically created for you when you create your account on the portal. See **Default Delivery Rule and Contact, page 111**.

To take advantage of advanced monitoring and notification features, set up additional device monitors and notification delivery rules.

To learn more, read these sections:

- **Process for Setting Up Monitors and Notifications, page 109**
- **Step-by-Step Example for Monitoring and Notifications, page 109**

Process for Setting Up Monitors and Notifications

To set up custom monitoring and notifications, follow these basic steps:

1. Determine the conditions and devices or severity levels that you want to monitor and who should be notified when these monitors trigger events.
2. Enable and configure the appropriate monitors these devices.
   By default only monitors on the Cisco OnPlus Network Agent are enabled.
   See **Adding and Managing Device Monitors, page 119**.
3. Create a delivery contact for the recipient of the event notifications. See **Adding and Managing Delivery Contacts, page 112**.

   IMPORTANT We recommend that you always create the delivery contact before creating the delivery rule because you will be associating the contact and their email or SMS address information when the rule is created.
4. Create a notification delivery rule. When creating the delivery rule, you will use this contact's information for the delivery method. **Using Delivery Rules, page 114**.
5. Test the device monitor and enable the option to generate a real event based on the result. See **Testing a Device Monitor, page 122**.

Step-by-Step Example for Monitoring and Notifications

The following example illustrates the basic process for monitoring and notifications.

Scenario

One of your OnPlus Portal customers, ABC Enterprises, has a server that runs critical business applications. You would like your technician, Mark Anderson, to be notified with an SMS text message to his mobile phone when that server goes down or up.

STEP 1 From the Overview page, click the customer entry for ABC Enterprises to view their Dashboard.

STEP 2 Enable a Host Up/Down monitor on the server.

a. From the Network Topology or Device Listing view, open the Device Information window for the server you want to monitor.

b. Select the **Monitors** tab.

c. Click the **+** icon to list the available monitors and choose Host Up/Down State. There are no other settings to configure for this monitor.

   Host Up/Down state is monitored using an IPv4 ICMP echo-request. It generates a Critical event when a host becomes unreachable. When that host becomes reachable again, a Warning event is generated.

d. Click **OK**.

e. Click **Home** to return to the Partner Account Overview page.

STEP 3 Create a delivery contact for your technician, Mark Anderson.

a. On the Overview page, choose **Notifications** > **Delivery Contacts**.

b. Click **+ Add Delivery Contact**.

c. Enter Mark's contact information and SMS email address. Make sure that the SMS email address is enabled for notifications.

d. In the **Customer** field, select **None**, as Mark is a global contact that is not associated with a specific customer.

e. In the **Preferred Language** field, select the language for the contact from the menu.

f. Click **Save**.

STEP 4 Create a delivery rule that sends a SMS text message notification to Mark Anderson when a Host Up/Down State critical event occurs for the ABC Enterprises customer.

a. On the Overview page, choose **Notifications** > **Delivery Rules**.

b. Click **+ Add Delivery Rule**.

c. In the customer field, choose **ABC Enterprises**.

d. Click the **Specify Event** checkbox.

e. From the **Event Type** list menu, choose **Monitor: Host UP/DOWN State (ICMP)** for the event type.

f. From the **Contact** list, select Mark Anderson.

g. From the **Delivery Method** list, select Mark's SMS email address.

h. Click **Save**.

STEP 5 Test the monitor and delivery rule.

a. From the Network Topology or Device Listing view, open the Device window for the server that you want to monitor.

b. Select the **Monitor** tab.

c. Click the **Host Up/Down** monitor.

d. Click **Test Monitor**.

e. Check the **Generate an event** option when the test runs.

f. Click **Run**. The test output and results are displayed.

g. Click **OK** to close the Device Information window.

h. Click **Home** to return to the Partner Account Overview page.

a. Choose **Notifications** > **Delivery Rule**.

b. Select the delivery rule you created in step 4.

c. Click the **Notifications Sent** number for the selected rule.

d. Verify that the notification generated by the Host Up/Down monitor test is listed.

e. Verify that the SMS text message was delivered to Mark's phone.

Default Delivery Rule and Contact

When you create a Partner Account and complete the portal registration, a default delivery rule is created so that notifications for all events with a severity level of Warning or higher for all customers are delivered to the Partner Account contact email address that was specified when the account was created.

You can disable delivery of notifications to your Partner Account email address, edit or delete this default delivery rule, and manage delivery contacts. See **Using Delivery Rules, page 114** and **Adding and Managing Delivery Contacts, page 112**.

Adding and Managing Delivery Contacts

To enable email or SMS (Simple Message Service) delivery of event and report notifications, you must create delivery contacts and make sure that notifications are enabled for the email and SMS email addresses specified for delivery contacts.

IMPORTANT We recommend that you create the delivery contact before creating the delivery rule, since you will be associating the contact and their email or SMS address when the rule is created.

When you add a customer, you also have the option to create a contact for that customer. This contact is automatically added to the Delivery Contacts list as a Customer contact.

When you create a customer contact, the **Customer** field indicates whether it is a global contact or a customer-specific contact:

- Set the **Customer** field to **None** to create a global contact. Global contacts can receive notifications of events and reports generated for any customer or all customers.
- Select a customer from the list in the **Customer** field to associate the contact with a customer. A contact associated with a specific customer can only receive notification of events or reports generated for that customer.

For instructions, see these topics:

- **Adding a Delivery Contact, page 113**
- **Editing a Delivery Contact, page 113**
- **Deleting a Delivery Contact, page 113**
- **Enabling or Disabling Notifications to Email or SMS Addresses, page 114**

Adding a Delivery Contact

To add a delivery contact for notifications, follow these steps:

STEP 1 From the Overview page on the portal, choose **Notifications** > **Delivery Contacts**.

STEP 2 Click **+ Add Delivery Contact**.

STEP 3 Enter the required information.

The email addresses entered here can be selected as delivery methods when creating notification delivery rules.

The SMS Email and Alt SMS Email addresses are used for delivering text messages to smartphones and should be entered using the address format required by the phone service provider. For example: 9995551212@txt.serviceprovider.net.

STEP 4 If you want to associate this delivery contact with a customer, choose a customer from the drop-down **Customer** menu. Otherwise, choose **None** to create a global contact.

STEP 5 Choose the language for this contact from the **Preferred Language** field menu.

STEP 6 Click **Save**.

Editing a Delivery Contact

To edit a delivery contact, follow these steps:

STEP 1 From the Overview page on the portal, choose **Notifications** > **Delivery Contacts**.

STEP 2 Click a contact in the list to open the actions drawer.

STEP 3 Click **Edit**.

STEP 4 When you are finished making changes, click **Save**.

Deleting a Delivery Contact

When you delete a delivery contact that is associated with a delivery rule, the delivery rule is also deleted.

To delete a delivery contact, follow these steps:

STEP 1 From the Overview page on the portal, choose **Notifications** > **Delivery Contacts**.

STEP 2 Click a contact in the list to access the actions drawer.

STEP 3 Click **Delete**.

STEP 4 Click **OK** to confirm the deletion.

Enabling or Disabling Notifications to Email or SMS Addresses

Notification emails and messages delivered to email and SMS addresses contain a link that allows the recipient to disable notifications.

You can enable or disable notifications to email or SMS addresses from the Cisco OnPlus Portal, by following these steps:

STEP 1 From the Overview page on the portal, choose **Notifications** > **Delivery Contacts**.

STEP 2 Click a contact in the list to open the details drawer.

STEP 3 Click the  and  controls to enable or disable the desired email and SMS addresses. The changes are applied immediately.

Using Delivery Rules

Delivery rules allow you to specify criteria for delivering event notifications.

A default delivery rule is created for you at registration. When you register with the portal and create your account profile, a default delivery rule is created for you, using your name and work email address. The default rule triggers notifications for all events with a severity level of Warning and higher for all customers. You can remove or edit this default rule at any time.

IMPORTANT Before you can create additional delivery rules, you must first set up delivery contacts and make sure that valid email and SMS addresses for text messages are set up for the contacts that will receive notifications.

- To edit your Partner Account information, see **Updating Your OnPlus Partner Account Information, page 37**.
- To create or edit delivery contacts, see **Adding and Managing Delivery Contacts, page 112**.

To add device monitors, see **Adding and Managing Device Monitors, page 119**.

These topics provide important information and procedures for creating and managing delivery rules:

Important Guidelines for Using Delivery Rules

Follow the guidelines in this section when creating delivery rules for notifications.

- **Examine the Event History for the selected criteria or event monitors to estimate the volume of messages that will be generated before creating the rule.**

  Before creating delivery rules, select different severity levels or select an event type and look at the volume and recent history of notifications that have been generated. Doing this will give you a feel for how the event system works and how to determine which monitor events are most useful to you.

  The Event History at the bottom of the Add Delivery Rule dialog box lists the total number of events generated that match the selected criteria. The Event History can be used to estimate how frequently the delivery rule triggers a notification. If a rule would trigger a large number of notifications in a short period of time, adjust your selection criteria before clicking **+ Add Delivery Rule**.

- **Create specific delivery rules to limit the volume of notifications delivered**. Choose higher severity levels or select a specific event type to limit the number to lower the volume of notifications that are generated. For example, selecting All customers and All severity levels generates a very large number of notifications.
- **Verify the customer contact email address**. When gathering contact information from your customers, make sure that the customer email and SMS addresses used for notifications are from valid, approved service providers.
- **Limit the volume of notifications to SMS email addresses (phones)**. If the SMS gateway service provider limits the number of SMS messages to or from an individual or application, the SMS gateway service might not inform the portal of any failed delivery attempts. Carrier fees for SMS messages will apply, so these should not be used with delivery rules that generate a large volume of notifications.

Creating Delivery Rules

To create a delivery rule, follow these steps:

STEP 1 From the Overview page on the portal, choose **Notifications** > **Delivery Rules**.

STEP 2 Click **+ Add Delivery Rule**.

STEP 3 Specify criteria for the delivery rule.

a. **Customer**. Choose **All** to be notified of events that match the selected criteria for all customers or select a specific **Customer**.

When you choose **All**, contacts associated with a specific customer are not listed in the Contact drop-down list.

When you choose **Customer**, the **Contact** drop-down list lists contacts associated with that customer and any contacts that are not associated with a specific customer. A contact is associated with a customer if you specify a customer when creating the delivery contact.

b. **Severity Level** or **Event Type**.

To deliver notifications based on a Severity Level, choose **All** or select a Severity Level from the list.

IMPORTANT Severity levels are cumulative—that is, when you select a severity level, it includes all events of that severity and above. For example, if you choose Error as the severity level, notifications are sent for Error, Critical, Alert, and Emergency events.

To deliver notifications based on a single event type, click the **Specify Event** checkbox and select an event type from the drop-down list. See **Event Types, page 130**.

c. **Contact**. Choose a delivery contact from the list. If no contacts are displayed, you must add at least one delivery contact before continuing. See **Adding and Managing Delivery Contacts, page 112**.

d. **Method**. Choose a delivery method from the list. You must choose a contact before you can set the delivery method.

The delivery methods that appear in the list are the email or SMS addresses defined for this contact. Delivery methods that are disabled are listed, but when the rule is created, the Contact field will indicate that the address is currently disabled.

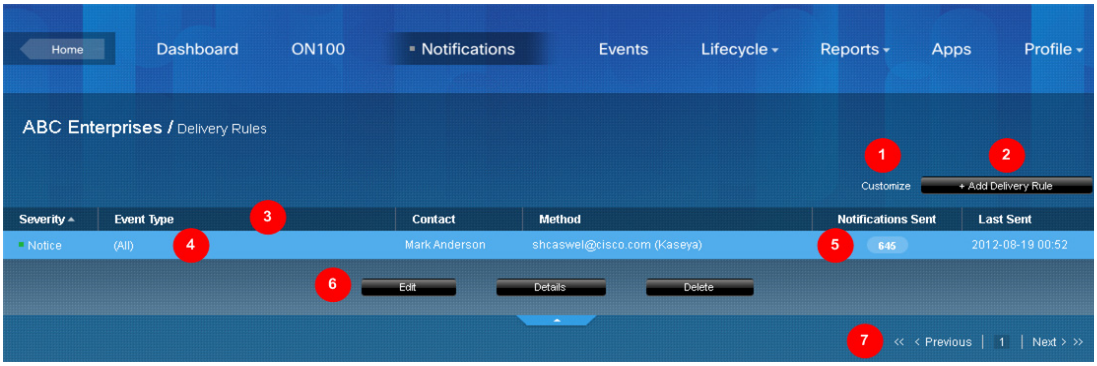
STEP 4 Examine the **Event History** to see how many events were generated in the past two weeks for the selected criteria. As you select different customers and change the severity level or event type, the Event History updates.

STEP 5 When you are satisfied with the rule, click **Save**.

STEP 6 To verify that the rule was created, choose **Notifications** > **Delivery Rules** from the navigation menu. You should see the new rule displayed in the list.

Viewing Delivery Rules

To view a list of delivery rules, access details and actions for a specific rule, or view notification message details, go to the Overview page and choose **Notifications** > **Delivery Rules**.



Callout	Description
1	Move the mouse over the Customize link to specify the number of rules to display per page.
2	Click here to add a new delivery rule.
3	Click a column heading to sort the list in ascending or descending order.
4	Click an entry in the list to select it and open the actions drawer. When the word DISABLED is displayed in the Method field, it indicates that notifications to that email or SMS address have been disabled.
5	Click the Notifications sent count to view message details for notifications sent for this rule.
6	The actions drawer contains options for editing, viewing details, and deleting a rule.
7	Use the paging controls to navigate the list if it is long.

To view notification messages that have been delivered for a rule, click **Notifications Sent** number. Click **Back** to return to the Delivery Rules list.

To view details for a delivery rule, click the rule in the list to open the actions drawer, then click **Details**.

Editing Delivery Rules

To edit a delivery rule, follow these steps:

STEP 1 From the Overview page on the portal, choose **Notifications** > **Delivery Rules**.

STEP 2 Click the delivery rule you want to edit.

STEP 3 Click **Edit** and make the desired changes.

STEP 4 Click **Save**.

Deleting Delivery Rules

To delete a delivery rule, follow these steps:

STEP 1 From the Overview page on the portal, choose **Notifications** > **Delivery Rules**.

STEP 2 Click the delivery rule that you want to delete.

STEP 3 Click **Delete**.

STEP 4 Click **OK** to confirm the deletion.

Adding and Managing Device Monitors

When you add and enable monitors to a device, events are generated according to the criteria specified for the monitors and can be viewed in the Events list for the device.

IMPORTANT If you want to send device monitor event notifications to destinations other than the default, you must add additional delivery contacts and delivery rules. See the sections **Default Delivery Rule and Contact, page 111** and **Using Delivery Rules, page 114**.

See **Step-by-Step Example for Monitoring and Notifications, page 109** for a simple scenario and steps that demonstrate how this feature works.

This section covers the following topics:

- **Default Cisco OnPlus Network Agent Monitors**

Default Cisco OnPlus Network Agent Monitors

When you activate a Cisco OnPlus Network Agent for a customer, a default set of network monitors are created and enabled on the device. The default monitors are listed here:

- WAN network performance
- CPU load
- Duplicate IP address detection
- DHCP service availability
- DNS service availability
- Memory usage

The WAN network performance monitor is also enabled on the device providing the WAN connection. You cannot edit, or delete the default device monitors on the Cisco OnPlus Network Agent, but you can disable them. For more information, see **Using Delivery Rules, page 114**.

Adding and Enabling Device Monitors

To enable monitors on a device, follow these steps:

STEP 1 Use one of the following methods to open the Device window for the device on which you want to add device monitors:

- From the Network Topology View, move the mouse over the icon for a device, then click the  (Device Information) icon.
- From the Device Listing page, click the checkbox to select the device and click the icon on the Dashboard toolbar.

You can also select multiple devices and add the same set of monitors to the selected devices. When you add monitors to multiple devices, any existing monitors on the selected devices are removed and replaced with the new monitors.

STEP 2 Select the **Monitors** tab.

STEP 3 Click the Plus (**+**) icon at the top left corner of the window to display a list of device monitors and choose one.

STEP 4 Fill in the parameters required for the selected event type.

For some types of monitors (for example, Host Performance (ICMP), you can set thresholds for when Warning and Critical events are generated. See **Device Monitor Descriptions, page 123**.

Click the  icon to display information about the currently selected monitor.

See **Device Monitor Descriptions, page 123**.

In the above example, the Host Performance (ICMP) event criteria specifies the following:

- When latency exceeds 250 ms, a Warning event is generated. When Latency exceeds 400 ms, a Critical event is generated.
- When packet loss exceeds 5%, a Warning event is generated. When packet loss exceeds 10%, a Critical event is generated.
- An event is also generated when the host performance monitor detects that the latency or packet loss returns to acceptable levels after a Warning or Critical event.

IMPORTANT When you monitor a device, events are always generated in response. These can be viewed on the Events tab in the Device Information window, or from the Events menu on the dashboard. Notifications are not created or delivered for any of these events unless delivery rules are created with the appropriate severity level or event type and delivery contacts email or SMS addresses are enabled. See **Using Delivery Rules, page 114**.

STEP 5 Repeat the above steps to add more monitors to the selected device or devices.

STEP 6 Click **OK**.

When you return to the Network Topology view, the device you enabled for monitoring now displays a Monitor icon  .

Testing a Device Monitor

To test a device monitor and optionally generate an event for the result, follow these steps:

STEP 1 On the Monitors tab of the Device window, click the Test Monitor icon for the monitor.

STEP 2 Optionally, enable the option to generate an event based on the results of the test.

STEP 3 Click **Run**. The results of the test are displayed.

STEP 4 Click the icon to return to the previous page.

Enabling and Disabling (Pausing) a Device Monitor or All Monitors

To temporarily enable or disable a monitor on a device or all monitors on a device, but retain the device monitor configuration settings, follow these steps:

STEP 1 From the Device window, select the **Monitors** tab.

STEP 2 Click a monitor to select it and display the current settings.

STEP 3 To enable or temporarily disable a monitor, click the **Enable/Disable** control associated with the monitor.

STEP 4 Repeat the previous steps for each monitor on the device you want to enable or disable.

STEP 5 To enable or disable all monitors on a device, click **Enable All** or **Disable All**.

STEP 6 Click **OK**.

Deleting a Monitor from a Device

To delete a monitor from a device, follow these steps:

STEP 1 From the Device window, select the **Monitors** tab.

STEP 2 Click a monitor to select it and display the current settings.

STEP 3 To delete the monitor, click the Minus (-) icon in the upper left corner of the window.

STEP 4 Click **OK**.

Device Monitor Descriptions

You can configure the following device monitors from the Monitors tab in the Device window:

Device Monitor	Devices	Description
CPU Load	Cisco OnPlus Network Agent only	Monitors CPU load on the Cisco OnPlus Network Agent A Warning event is generated if the CPU load exceeds preset thresholds. Intended primarily for Cisco internal use.
DHCP Server	Applicable devices	Monitors the DHCP service to ensure that it is available and serving addresses to devices on the network. When this monitor is added to a device other than the Cisco OnPlus Network Agent, only devices with a DHCP monitor are considered authorized DHCP servers for the network. A Critical event is generated if no DHCP server responds to a DHCP REQUEST packet in the specified amount of time. A Rogue DHCP Server Detection event is generated if a previously unseen or unspecified DHCP server starts answering DHCP requests on the network.
DNS Service	Applicable devices	Monitors the DNS service on this device to ensure that it is responding and able to resolve queries against the specified target DNS hostname. A Warning or Critical event is generated if the latency of the response falls below the specified thresholds. A symptom of slow DNS server response is sluggish web browsing.
Duplicate IP	Cisco OnPlus Network Agent only	Monitors devices to check for duplicate IP addresses. A Duplicate IP Address event is generated when more than one device claims the same address on the network.

Device Monitor	Devices	Description
Host Performance (ICMP)	Any applicable device, except the Cisco OnPlus Network Agent	Monitors host reachability and response time by measuring packet loss and latency performance for the specified host using an IPv4 ICMP echo-request. A Warning or Critical event is generated if the response time for this host falls below the specified latency and packet loss thresholds. A Critical event is generated if the host is completely unresponsive.
Host State	Any applicable device, except the Cisco OnPlus Network Agent	Monitors host reachability using an IPv4 ICMP echo-request. A Critical event is generated if the host becomes unreachable. A Warning event is generated if the host later becomes reachable. Use this monitor for hosts that do not require latency and loss performance measurements.
Incoming Mail Service (IMAP)	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the IMAP mail service response for the specified port on this device. A Warning or Critical event is generated if the response time of the service falls below the specified latency thresholds. A Critical event is generated if the host becomes completely unresponsive to IMAP connections.
Incoming Mail Service (POP3)	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the POP3 mail service response for the specified port on this device. A Warning or Critical event is generated if the response time of the service falls below the specified latency thresholds. A Critical event is generated if the host becomes completely unresponsive to POP3 connections.
Intelligent Platform Management Interface (IPMI)	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the IPMI sensors on this device. A Warning or Critical event is generated if any sensors have readings outside the preset sensor thresholds of the device, depending on which threshold is crossed. A Warning event is generated if the host becomes completely unresponsive to IPMI connections. Typically, IPMI is available on baseboard management controllers (BMCs) of servers such as Cisco Unified Computing System (UCS). OnPlus checks IPMI sensors that have defined thresholds such as voltages, temperatures, and fan RPMs.

Device Monitor	Devices	Description
IP Change	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the IP address of this host to detect changes. A Critical event is generated whenever the IP address changes on this host.
Memory Usage	Cisco OnPlus Network Agent only	Monitors CPU load on the Cisco OnPlus Network Agent. A Warning event is generated when Cisco OnPlus Network Agent memory usage exceeds preset thresholds.
Outgoing Mail Service (SMTP)	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the SMTP mail service response for the specified port on this device. A Warning or Critical event is generated if the response time of the SMTP service falls below the specified latency thresholds. A Critical event is generated if the host becomes completely unresponsive to SMTP connections.
Secure Web Server Monitor	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the secure web service at the specified URL to ensure that it is responding and that it returns the specified text string. A Critical event is generated if the service at the specified URL is unreachable or the response does not contain the specified text string.
SSL Certificate (HTTPS)	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the SSL certificate of the web server on the specified host to ensure that it is valid and has not expired. A Warning event is generated if the certificate expires in less than the specified number of days. A Critical event is generated if a valid certificate cannot be obtained from the host or the certificate is expired.
TCP Service	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the TCP service on the specified port to ensure that it is responding. You can specify a text string to send to the TCP port and an expected return text string. Both of these text strings are optional and independent of each other. The text strings can contain the linefeed (\n), newline (\r), and tab (\t) escape sequences. A Critical event is generated if the target TCP port is not open or if the optional expected text string is not returned.

Device Monitor	Devices	Description
UDP Service	Any applicable device except the Cisco OnPlus Network Agent	Monitors the UDP service on the specified port to ensure that it is responding. You must specify a text string to send to the UDP port and an expected return text string. Both of these text strings are required. The text strings can contain the line feed (\n), newline (\r), and tab (\t) escape sequences. A Critical event is generated if the expected text string is not returned from the UDP service.
WAN Network Performance	Cisco OnPlus Network Agent and the root device for the customer network	Monitors network latency, packet loss, and jitter. Monitor the WAN network performance of this site by measuring jitter, latency, and packet loss against a portal responder service. A Warning or Critical event is generated if the WAN network performance falls below the specified thresholds. A Critical event is generated if there is no response from the portal responder service. **NOTE** A single instance of this monitor is displayed on both the Cisco OnPlus Network Agent and the device that provides the WAN link for the customer network. If you edit WAN Network Performance monitoring thresholds on either of these devices, the changes also appear when the monitor is viewed on the other device.
Web Service	Any applicable device, except the Cisco OnPlus Network Agent	Monitors the web service (HTTP) at the specified URL to ensure that it is responding and that it returns the specified text string. A Critical event is generated if the service at the specified URL is unreachable or the response does not contain the specified text string.

Device Monitor	Devices	Description
Windows Management Interface (WMI)	Windows host with WMI enabled	Monitors status and performance thresholds on a Windows host using WMI. The WMI service must be enabled on the target host and valid credentials must be supplied on the Access tab on the Device window for the device. The following events can be generated, depending on the WMI monitor type: ▪ **Disk Drive Status**: A Warning or Critical event is generated if a disk drive on the host enters one of the specified states. The default states supplied are recommended for typical use. ▪ **Disk Free Space**: A Warning or Critical event is generated if the amount of free disk space on the specified volume falls below the specified thresholds. ▪ **Memory Free**: A Warning or Critical event is generated if the amount of free memory falls below the specified thresholds. ▪ **Process Exists**: A Critical event is generated if the specified process name does not appear in the list of tasks running on the Windows host.

Viewing Events

Events can be generated by:

- Device monitors. These include:
  - Network connectivity and bandwidth thresholds exceeded
  - Host state changes
  - DNS hostname resolution delay or failure
  - IP address changes
  - Device discovery

- Actions such as:
  - Authorized agent logins
  - Firmware upgrades
  - Configuration backup and restore operations
  - Device reboot requests
  - Report completion and delivery
  - Cisco product support events
- Application-specific events
- Services running on the portal

You can view and filter events for a single customer or for a specific device.

To learn more, see these sections:

- **Viewing Events For All Customers, page 128**
- **Viewing Events for a Customer, page 129**
- **Viewing Event History for a Device, page 130**
- **Event Types, page 130**

Viewing Events For All Customers

To view events across all customers, follow these steps:

STEP 1 On the Partner Account Overview page, choose **Notifications** > **Events**.

The Notifications/Events page lists events for all customers. For each event, the customer, date, severity, type, message, and device MAC address (if applicable) are listed. Click column headers to sort the list by customer, date, severity, or type.

STEP 2 If desired, choose an event severity level to see all events of that severity and higher for all customers.

STEP 3 If desired, click a MAC address link in the Device column to open the Device Information window for that device.

STEP 4 Click **Refresh** to update the list.

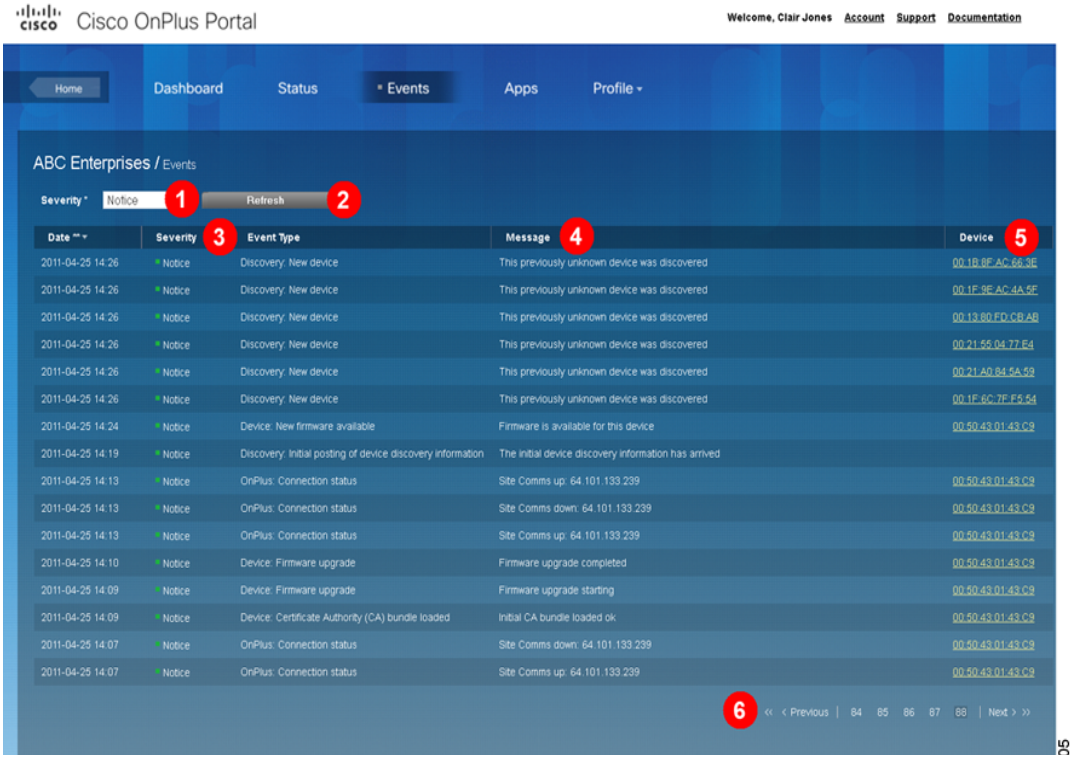
Viewing Events for a Customer

To view events for a customer, follow these steps:

STEP 1 On the Overview page, click the entry for the customer to go to the Dashboard view for that customer.

STEP 2 From the navigation menu, choose **Events**.

Here is an example Events list that shows the features and areas of interest on the Events page for a customer.



Callout	Description
1	Choose one of the options in the Severity drop-down list to filter the event list by Severity. Severity levels are cumulative. The selected Severity level shows all events of that severity and above.
2	Manually refresh the Events list. The list is also refreshed when you revisit the page.

Callout	Description
3	Click column headers to sort events by Date, Severity, or Event Type.
4	Messages are displayed that provide additional information about the event.
5	MAC addresses in the Events list are clickable links. Click a MAC address to view Dashboard details for the device with that address.
6	Use the paging controls at the bottom of the page to navigate the list.

Viewing Event History for a Device

To view event history for a specific customer device, follow these steps:

STEP 1 On the Overview page, click a customer in the list to view their Dashboard.

STEP 2 To open the Device window for a specific customer device, use one of these methods:

- From the Network Topology view, move your mouse over the icon for the device, then click the icon. You can also right-click the device icon and choose **View Device Information**.
- From the Device Listing view, click the checkbox on the left side of the entry to select it and display the icon to the right of the toolbar. Click the icon.

  The Device Information window appears.

STEP 3 In the Device window, select the **Events** tab. You can also choose to filter device events by severity and click column headings to sort the list.

Event Types

This table lists and describes Event Types that can occur on the portal.

Category	Description
Application	Application: Event.

Category	Description
Contact	Message sent to target contact.
Customer Site	Customer Site: Deactivated.
Customer SIte	Customer Site: Installation completed.
Device	Device: Certificate Authority bundle loaded.
Device	Device: Cisco Support Access used.
Device	Device: Configuration backup
Device	Device: Configuration backup requested.
Device	Device: Configuration change.
Device	Device: Configuration restore requested.
Device	Device: Configuration restored
Device	Device: Firmware upgrade completed.
Device	Device: Firmware upgrade requested.
Device	Device: Firmware upgrade.
Device	Device: New firmware available.
Device	Device: Offline. A local monitored device no longer responds on the network.
Device	Device: Reboot request.
Device	Device: Remote tunneled connection (RDP, VNC, TCP) status. Server established remote RDP, VNC, or TCP port remote tunnel connection to a device or closed the connection.
Device Discovery	Discovery: Device discovery change.
Device Discovery	Discovery: Initial posting of device discovery information.
Device Discovery	Discovery: New device. This event is triggered whenever a new device appears in the site. Both this event and the Discovery: Initial posting of discovery event are reset when a Reset All is performed. After a Reset All action, the next device discovery will trigger a Discovery: Initial posting of discovery event, and each device found after that will trigger a Discovery: New Device event.
Monitor	Monitor: Device connectivity (Ping). Latency (ms) and Packet Loss (%) thresholds for monitoring device connectivity (ICMP) have been exceeded.

Category	Description
Contact	Message sent to target contact.
Customer Site	Customer Site: Deactivated.
Customer SIte	Customer Site: Installation completed.
Device	Device: Certificate Authority bundle loaded.
Device	Device: Cisco Support Access used.
Device	Device: Configuration backup
Device	Device: Configuration backup requested.
Device	Device: Configuration change.
Device	Device: Configuration restore requested.
Device	Device: Configuration restored
Device	Device: Firmware upgrade completed.
Device	Device: Firmware upgrade requested.
Device	Device: Firmware upgrade.
Device	Device: New firmware available.
Device	Device: Offline. A local monitored device no longer responds on the network.
Device	Device: Reboot request.
Device	Device: Remote tunneled connection (RDP, VNC, TCP) status. Server established remote RDP, VNC, or TCP port remote tunnel connection to a device or closed the connection.
Device Discovery	Discovery: Device discovery change.
Device Discovery	Discovery: Initial posting of device discovery information.
Device Discovery	Discovery: New device. This event is triggered whenever a new device appears in the site. Both this event and the Discovery: Initial posting of discovery event are reset when a Reset All is performed. After a Reset All action, the next device discovery will trigger a Discovery: Initial posting of discovery event, and each device found after that will trigger a Discovery: New Device event.
Monitor	Monitor: Device connectivity (Ping). Latency (ms) and Packet Loss (%) thresholds for monitoring device connectivity (ICMP) have been exceeded.

Category	Description
Monitor	Monitor: Device hardware problems.
Monitor	Monitor: Device IP address change. The IP address of a device has changed. The check is made whenever device discovery runs. If this is the device that provides the WAN connection, an event is also sent if the WAN IP address changes.
Monitor	Monitor: DHCP server creation.
Monitor	Monitor: DNS hostname resolution. DNS hostname resolution delay, failure, or recovery detected.
Monitor	Monitor: Host state Host down (not reachable) or host up (recovery) events.
Monitor	Monitor: HTTP traffic /web server. Events associated with a monitored web server port. You can specify the HTTP port (default 80), web page name, and text to check that the web server is up and operating normally.
Monitor	Monitor: HTTPS traffic / Secure web server. Events associated with a secure web server monitor. You can specify the HTTPS port (default 443), web page URL, and text to check to ensure that the secure web server is up and operating normally.
Monitor	Monitor: IMAP incoming mail server. Events associated with a monitored IMAP incoming mail server.
Monitor	Monitor: Intelligent Platform Management Interface (IPMI) Events associated with a monitored IPMI-capable device.
Monitor	Monitor: IP address duplication. When a duplicate IP has been detected on the network, a Monitor: Duplicate IP Address event is generated. When the duplicate IP issue is resolved, a second Monitor: Duplicate IP Address event is generated to indicate the recovery.
Monitor	Monitor: Network bandwidth (latency, packet loss, jitter). Network latency, packet loss, and jitter thresholds exceeded or recovery event associated with these thresholds.
Monitor	Monitor: OnPlus CPU load. The CPU load monitor on the Cisco OnPlus Network Agent generates these events when CPU usage thresholds are exceeded or return to normal levels after being exceeded. Intended primarily for Cisco internal use.

Category	Description
Monitor	Monitor: Cisco OnPlus Network Agent memory usage. Monitors memory usage on the Cisco OnPlus Network Agent. This monitor is always enabled. Intended primarily for Cisco internal use.
Monitor	Monitor: POP3 incoming mail server. Events associated with a monitored POP3 incoming mail server port.
Monitor	Monitor: Rogue DHCP server detection.
Monitor	Monitor: SMTP outgoing mail server. Events associated with an SMTP outgoing mail server port monitor.
Monitor	Monitor: SSL certificate.
Monitor	Monitor: TCP traffic. These events are associated with a monitored TCP service on the specified port.
Monitor	Monitor: UDP traffic. These events are associated with a monitored UDP service on the specified port.
Monitor	Monitor: Windows Management Information (WMI).
OnPlus	OnPlus: Connection status. This Cisco OnPlus Network Agent connection status monitor reports the state of the Cisco OnPlus Network Agent. Site Comms Up/Down events are generated with a severity level of Notice for regular operational Up/Down actions such as a user-requested reboot of the Cisco OnPlus Network Agent or an automatic upgrade of firmware on the Cisco OnPlus Network Agent during the daily maintenance window. If there is an unexpected failure of the connection, the corresponding Site Comms Up/Down events are issued with a severity level of Warning.
OnPlus	OnPlus: I/O Error. I/O error occurred during logging; may indicate Cisco OnPlus Network Agent file system is full or corrupted.
OnPlus	OnPlus: Portal-to-Cisco OnPlus Network Agent connection.
OnPlus	OnPlus: Process terminated unexpectedly. A process terminated unexpectedly on the OnPlus device.
OnPlus	OnPlus: Remote tunnel connection status. Server established remote tunnel to the Cisco OnPlus Network Agent.

Category	Description
OnPlus	OnPlus: TCP port 11300 (heartbeat) may be blocked. Site connectivity may be limited. This event, is generated if the CPE can deliver discovery up to the portal, but the heartbeat is not connected at that time. This typically means that the site has restrictive outbound policies in place that prevent outbound traffic on port 11300. See **Port and Protocol Access Requirements, page 23**.
Product	Product: Cisco Security alert (PSIRT)
Product	Product: Cisco service contract alert
Product	Product: End-of-sale, end-of-life, end-of-support alerts.
Product	Product: End-of-sale, end-of-life, end-of-support notice
Product	Product: End-of-warranty alert
Product	Product: End-of-warranty alert.
Product	Product: Security alert (PSIRT).
Report	Reports: Creation completed.
Report	Reports: Creation requested.
Report	Reports: Report sent. Report Delivery events are only generated for scheduled recurring reports with at least one recipient contact email specified. If no recipient is specified a Report Complete event is generated instead.

8

Connecting to Devices from the Portal

This chapter explains how to establish remote connections to devices at the customer site from the Cisco OnPlus Portal. These topics are covered:

- **Overview**
- **Remote Connection Guidelines, Limitations, and Caveats**
- **Opening an RDP, VNC, or Generic Tunnel Connections (SSH, Telnet)**
- **Opening a Web (HTTP/HTTPS) Connection**
- **Manually Closing a Remote Device Connection**
- **Enabling or Disabling Remote Device Connections for a Site**

Overview

Use the Connect to Device feature to open a remote connection to a device at the customer premises using one these connection types: web (HTTP), secure web (HTTPS), Remote Desktop Protocol (RDP), Virtual Network Client (VNC), or generic tunnel (for example, an SSH or Telnet port connection).

Use this feature for remote management access to your customer's devices. The Connect to Device feature enables you to:

- Connect securely to remote devices at the customer premises without having to configure gateway port forwarding to access devices behind the customer's firewall.
- Launch the configuration utility for a device from a remote location.
- Perform minor tasks on customer's CPE such as checking device health or making configuration adjustments.

Support for remote connections to third-party devices and Cisco devices that are fully supported by OnPlus is limited. Cisco cannot test and confirm functionality for all possible combinations of Cisco devices, protocols, and third-party devices.

Remote Connection Guidelines, Limitations, and Caveats

Read this section for important guidelines, caveats, and limitations that apply to remote connections established through the OnPlus Portal.

- **Guidelines for All Connection Types, page 138**
- **RDP, VNC, and Generic Tunnel Connection Guidelines, page 139**
- **Web (HTTP/HTTPS) Connection Guidelines, page 139**

Guidelines for All Connection Types

These guidelines, limitations, and caveats apply to all remote connections established through the OnPlus Portal:

- The Cisco OnPlus Network Agent must be up and operating normally at the site.
- Only one tunnel connection of a given type—Web, RDP, VNC, or Generic Tunnel—can be open at a time *per customer site*. New connections replace older ones.
- If the connection is idle for 20 minutes, it is automatically closed.
- Remote connections must be enabled for the site. For more information, see **Enabling or Disabling Remote Device Connections for a Site, page 149**.
- To ensure correct tunnel operation, the computer and network being used to access the portal must allow outbound TCP connections for ports 11305 and 11700 through 11800. Outbound TCP traffic on these ports is rarely blocked, so this would only be an issue in a restrictive network environment.

RDP, VNC, and Generic Tunnel Connection Guidelines

These guidelines, limitations, and caveats apply to RDP, VNC, and generic tunnel connections established through the OnPlus Portal:

- Tunnel connections made from the OnPlus Portal are intended for user-directed activities such as remote configuration changes or debugging. They are not designed for high-volume data operations or "always-on" services such as automated backups.
- The connection expires after 10 minutes if it is not used (that is, no attempt is made to connect over the tunnel). Tunnel connections are closed after 20 minutes of inactivity.
- A tunneled connection to a device that streams content uses a second connection and a different port will not work. If there is an option to turn off the streaming using the second connection, then you should do so when trying to connect remotely.

  The Cisco PVC2300 IP video camera, which relies on a service that uses NAT Port-Mapping Protocol (NAT-PMP) to stream content to another connection using a different port, is a good example of this type of device.

Web (HTTP/HTTPS) Connection Guidelines

The following guidelines, limitations, and caveats apply to remote web (HTTP/HTTPS) connections established through the OnPlus Portal:

- The Connect tab is not supported for all devices. See **Appendix B, "Cisco Device Feature Support"** for information about Cisco devices that support this feature.
- A reasonable effort is made to support web connections to non-Cisco devices, but these are not guaranteed to work.
- Your web browser must allow cookies and pop-ups for the OnPlus Portal in order to connect remotely to a device over HTTP/HTTPS.
- Remote connections to devices that properly use relative URLs in their content should work.

  However, bugs in web browsers and servers and malformed content output by devices can cause some devices or features to not work correctly (for example, the device might redirect to a local non-routable LAN side address). These types of remote connection failures indicate issues with the device itself.

A simple way to determine if the failure is due to a problem with the device is to use a gateway device and port forward through the firewall to the device with a computer on the outside. If this does not work, then the device is probably causing the problem.

- Different web browsers or versions of the same web browser may exhibit different behavior with the same device.
- If you are connecting to a device that streams content using a second connection and a different port, this type of remote connection will not work. If there is an option to turn off the streaming using the second connection, then you should do so when trying to connect remotely.

  The Cisco PVC2300 IP camera is one example of a device that does this. When connecting to Internet Explorer, it does not use motion JPEG to send content. Instead, it uses a second stream with UPnP port mapping. For the Cisco PVC2300 camera, you can solve this problem by using a browser other than Internet Explorer.

Opening an RDP, VNC, or Generic Tunnel Connections (SSH, Telnet)

The topics in this section provide information about establishing tunneled connections to remote devices through the portal:

- **How Tunneled Connections Work on the Portal, page 140**
- **Creating an RDP, VNC, or Generic Tunnel Connection (SSH, Telnet), page 142**

How Tunneled Connections Work on the Portal

The diagram on the following page provides an overview of the RDP, VNC, and generic tunnel connection implementation on the portal.

As shown in the diagram, a remote tunneled connection made through the OnPlus Portal has three segments:

- The segment between the remote PC and the OnPlus Portal

  For web connections, this segment is secured, since HTTPS is required for connecting to the portal. For RDP, VNC, and Generic Tunnel connections, no additional security is provided.

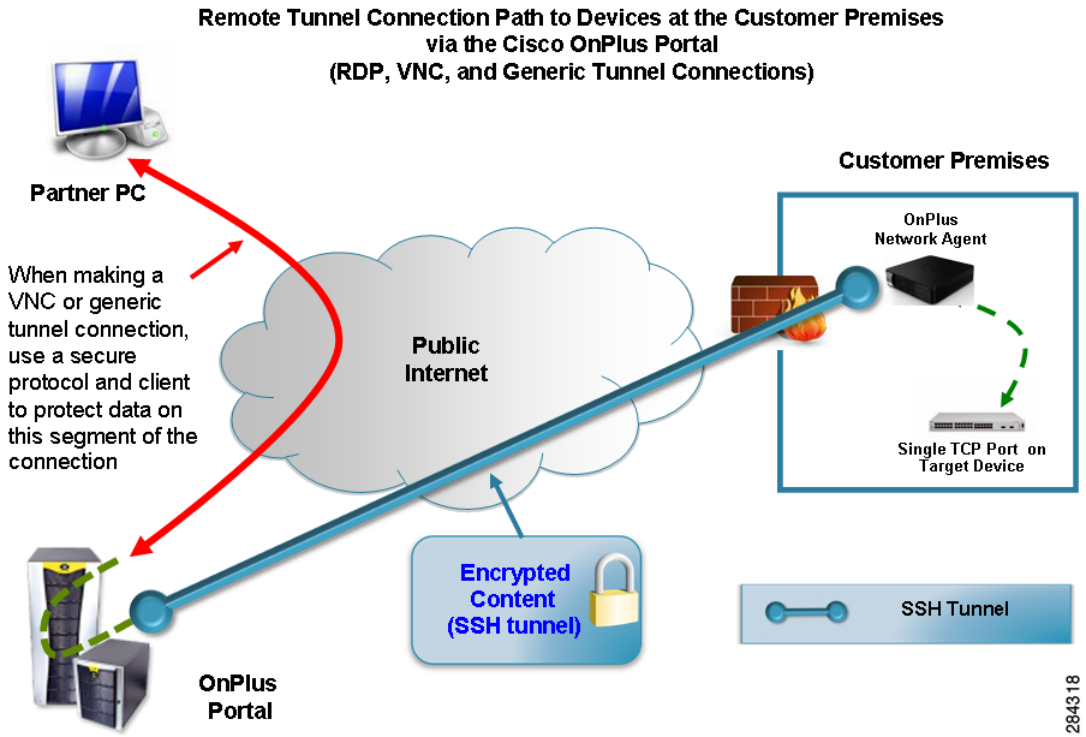
- The segment between the OnPlus Portal and the Cisco OnPlus Network Agent

  This segment of the connection is secured by using an SSL tunnel.

- The segment between the Cisco OnPlus Network Agent and the target device

  This segment of the connection is entirely behind any existing firewall at the customer site. HTTPS connections are encrypted, but HTTP connections are not.

NOTE The following diagram applies only to RDP, VNC, or Generic Tunnel connections. For web proxy connections, a secure HTTPS connection is enforced between the Partner PC and the OnPlus Portal.



The following notes apply to the OnPlus Portal connection implementation:

- The Partner computer has a single port to connect to for the life of the connection. After the connection is made, the tunnel is locked to the source IP address of the partner computer. The port used in this connection is dynamically assigned and should not be bookmarked.

- If the protocol used for the connection supports multiple, simultaneous client connections to a single TCP port on the target device (Telnet and SSH, for example), multiple connections are supported over the same tunnel.
- The Generic Tunnel connection should support any single-port TCP protocol.
- If the target device supports Wake on LAN (WOL), WOL packets are sent during the first 10 seconds of the initial tunnel creation.

  For more information, refer to the hardware and operating system documentation for the target device. You are responsible for configuring WOL for devices and troubleshooting WOL issues.

Creating an RDP, VNC, or Generic Tunnel Connection (SSH, Telnet)

To create an RDP, VNC, or generic tunnel connection (for example, for remote SSH or Telnet access to a device), follow these steps:

STEP 1 Make sure that the device to which you are connecting is configured to allow the connection:

- For all direct-mapped tunnel connections (RDP, VNC, or Generic Tunnel), the firewall on the target device must be configured to permit access to the device.
- For VNC connections, the VNC server on the target device and the VNC client on the PC accessing the device must be properly configured. A secure VNC client and server are recommended.
- For RDP connections, Remote Desktop Sharing must be enabled on the target device. For more information, refer to the Microsoft documentation for RDP.
- For generic tunnel connections, a connection can be made to any single, TCP port. A service must be active on the port at the target device and any firewall must allow connections.

STEP 2 Initiate the connection using one of these methods:

- To try the connection with the default settings, right-click the device icon in the Topology View and choose **Connect to Device using RDP** or **Connect to Device using VNC**.

- To configure connection settings, open the Device Information window from either the Network Topology or Device Listing view, choose the Connect tab, choose a connection type (RDP, VNC, or Generic Tunnel), and configure settings. Click **Connect to Device** to connect using the settings you configured.

  For RDP, VNC, and generic tunnel connections, you only need to specify the correct port number for the desired protocol on the target device.

When the tunnel is successfully created, the Connection Available window appears, with a link to the connection.

If you are creating an RDP connection, you are prompted to save or open the .rdp connection profile file to use with your installed RDP application. Similarly, if you are creating a VNC connection on a Windows PC, you are prompted to save or open the .vnc connection profile file.

For SSH, Telnet, or other generic tunnels, you can cut and paste the address. Or, you can click the **copy to clipboard** icon to copy the address to the clipboard so that you can paste it into a client application (for example, a Telnet or SSH client).

The tunnel is locked to the source IP address of the first device attempts to connect to the tunnel.

STEP 3 Click **OK** to close the Connection Available window.

When the connection is made, the remote connection icon appears on the device icon in the Network Topology view. The Device Information window also indicates that device is connected through a tunnel.

The device icon appears a connection icon  to indicate that the device is connected through a tunnel.

The Device Information window status area also updates to display the message “Tunnel connection established to this device.”

As a shortcut, you can right-click the icon for a device that supports remote connections from the Topology or Customer Dashboard view and choose **Connect to Device through the Web, Connect to Device using RDP, or Connect to Device using VNC**. The currently configured settings are used when making a tunnel connection using this method.

Opening a Web (HTTP/HTTPS) Connection

Refer to the following sections for information about opening a web (HTTP/HTTPS) connection to a remote device through the OnPlus Portal:

- **How Remote Web Connections Work, page 144**
- **Configuring and Opening a Web Connection, page 145**
- **Troubleshooting Web (HTTP/HTTPS) Connection Settings, page 148**
- **Recommended Web Connection Settings for Devices, page 149**

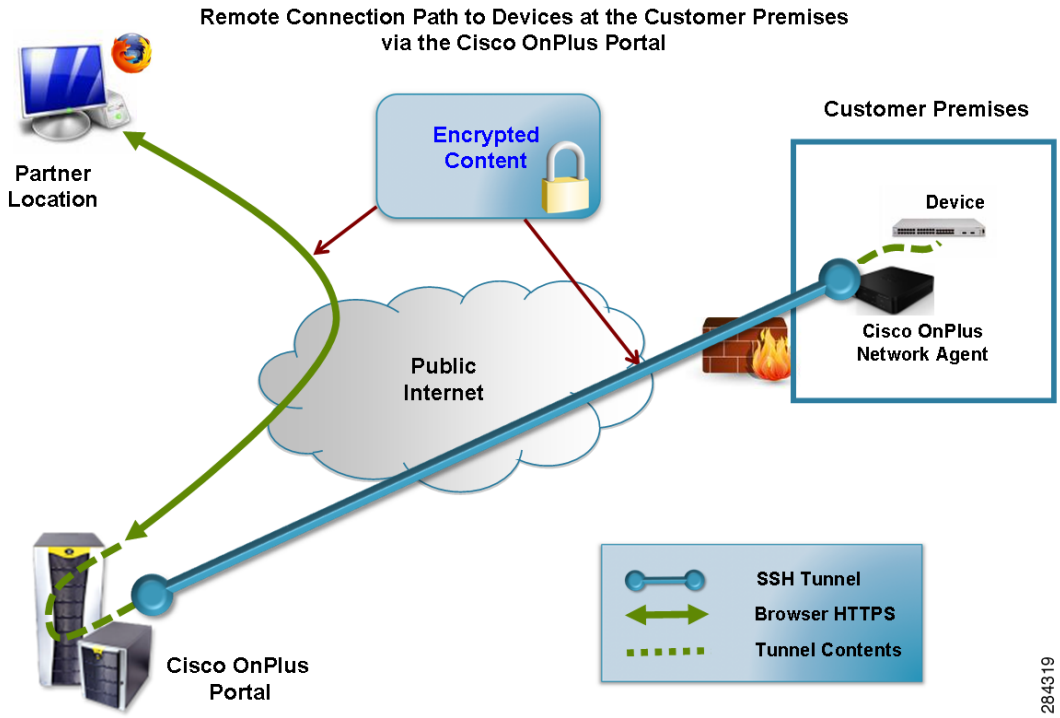
How Remote Web Connections Work

When you connect to devices at the customer premises over the web, all public Internet traffic through the OnPlus Portal is encrypted, even non-encrypted web content.

As shown in the following diagram:

- Traffic to and from the web browser that you use to access the OnPlus Portal is encrypted and is transmitted over an HTTPS connection.
- Traffic to and from the OnPlus Portal and the Cisco OnPlus Network Agent at the customer premises is encrypted and is transmitted over an SSH tunnel.
- The last leg of the connection to CPE at the remote location is accomplished by extending the tunnel from the Cisco OnPlus Network Agent to a port on the device at the customer premises.

  The settings configured on the Connect tab for a device on the portal determine whether or not the local connection between the Cisco OnPlus Network Agent and the device is encrypted.



Configuring and Opening a Web Connection

To configure connection settings and open a connection to a remote device at the customer premises from the OnPlus Portal, follow these steps:

STEP 1 On the Overview page, click a customer from the list and display the Network Topology view for that customer.

STEP 2 Move the mouse over the icon in the Topology view for the device to which you want to connect and click the Device Information icon.

You can also right-click the icon and choose **View Device Information**.

STEP 3 On the Device Information window, click the **Connect** tab.

STEP 4 CLick **Web**.

STEP 5 Edit web connection settings as described in the following table:

Setting	Description
Device Web Port	Enter the port number required for connections to this device. The default management port is port 80, which should work with a large number of devices. You can edit this setting as needed. Refer to the documentation for the device to see if a different port or an HTTPS connection is required.
Secure HTTPS Connection	Check the **Secure HTTP Connection** if the device requires an HTTPS (SSL) connection. When this option is checked, the management port is set to 443, which is the default for HTTPS (SSL) connections. You can edit the port number, if needed. This setting should be used only for devices that require a secure HTTPS/ SSL connection.
Fix Headers	You should only enable the **Fix Headers** option if: ▪ The connection to the device fails, and ▪ Private IP addresses (for example, 192.168.x.x) appear in the URL field of the web browser being used to connect to the device. When **Fix Headers** is enabled, references to private IP addresses are removed from headers and made relative.
Fix URLs	You should only enable the **Fix URLs** option if: ▪ The connection to the device fails, and ▪ Connection timeouts are seen, or ▪ The page on the remote device loads, but links to other content from the page do not work. When **Fix URLs** is enabled, absolute addressing in content URLs is replaced with relative addressing.

Setting	Description
Disable Proxy Behavior	You should only enable the **Disable Proxy Behavior** option if: ▪ The connection to the device fails, or ▪ The page on the remote device loads, but other content from the page, such as Java applets, does not work. When **Disable Proxy Behavior** is enabled, certain web proxy functions of the tunnel are disabled, and a generic tunnel to the Device Web Port is established instead. The Fix Headers and Fix URLs become unavailable. This setting is remembered by the portal, whereas generic tunnel settings are not.

For information about recommended settings for specific devices and troubleshooting tips, see these topics:

- **Troubleshooting Web (HTTP/HTTPS) Connection Settings, page 148**
- **Recommended Web Connection Settings for Devices, page 149**

STEP 6 Click **Connect to Device**.

When the connection is ready, the Connection Available window appears.

STEP 7 In the Connection Available popup window, choose **Click here to connect** to open the connection to the device in a new browser window.

Click **OK** to close the window.

STEP 8 Log in to the device and view or update configuration settings as you normally would.

A remote connection icon appears on the device icon in the Network Topology for the currently connected device.

STEP 9 When you are finished with the connection, reopen the Device Information window, select the Connect tab, and click **Disconnect from device**. Click **Disconnect** when prompted to confirm the action.

After 20 minutes of inactivity, the connection is automatically closed.

As a shortcut, you can right-click the icon for a device that supports remote connections from the Topology or Customer Dashboard view and choose **Connect to Device via Web**. The currently configured settings are used when making a connection using this method.

Troubleshooting Web (HTTP/HTTPS) Connection Settings

When attempting to establish a remote connection to a device through the portal, try connecting to new devices by editing connection settings in the following order:

1. Try the connection with the default settings: Device Web Port set to 80, all other options unchecked.
2. Try using an HTTPS (SSL) connection with the default port; some devices require an HTTPS connection.
3. Try editing the port number if the management application requires a specific port.
4. If you see references to private IP addresses in URLs, try checking the Fix Headers option with Device Web Port set to 80.
5. If you are experiencing connection timeouts or you find that there are links in content pages that are not working, try enabling the Fix URLs option.
6. For some devices, you may need to enable both Fix Headers and Fix URLs.
7. Try the above options using a different web browser.
8. You may encounter problems when attempting to establish a web connection to ESW500 Series switches (for example, a timeout error or blank page). Try the connection over HTTPS on port 443 using Internet Explorer 7 or Safari. Firefox does not work with ESW500 Series switches. Safari does not work with WAP4410N access points.

Recommended Web Connection Settings for Devices

If the device that you are connecting to has a set of connection settings that are known to work with the OnPlus Portal, these recommended default values are automatically populated on the Connect tab for that device.

If the connection settings that you have configured are different from the recommended settings, a message is displayed and you are provided with an option to **Restore Optimal Settings**.

Manually Closing a Remote Device Connection

To manually close an open tunnel connection to a remote device at a customer site, follow these steps:

STEP 1 On the Overview page of the portal, click the customer to open their Dashboard.

STEP 2 On the Dashboard toolbar, click the Site Actions  icon, click **Misc. Actions**, and click **Force Disconnect**.

Enabling or Disabling Remote Device Connections for a Site

Remote connections to devices at customer sites through the OnPlus Portal to a site are enabled by default. If a customer does not want to allow remote connections to devices at their site, you can disable this feature by logging into the customer's Cisco OnPlus Network Agent.

NOTE After remote connections have been disabled, you must be directly connected to the LAN at the customer premises to enable remote connections.

To enable or disable remote connections from the portal to devices at a customer site, follow these steps:

STEP 1 From a PC that is directly connected to the LAN at the customer premises, open a web browser and connect to the Cisco OnPlus Network Agent.

You can do this by entering the IP address of the Cisco OnPlus Network Agent in the URL bar or through Bonjour.

STEP 2 On the Cisco OnPlus Network Agent login page, enter these login credentials:

Username: **admin**
Password: *<Customer_Password>*

TIP The password that you must use is the Customer Password, which is displayed in the **Activation Information** section of the customer Profile page on the portal from the Overview page, click the customer, then choose **Profile** > **Profile**.

STEP 3 Click the **Configuration** link at the top of the page.

STEP 4 To disable remote connections, uncheck the **Allow VAR to remotely connect to devices** option. To re-enable remote connections, check this option.

STEP 5 Click **Update Configuration**.

After you update the configuration, remote connections to devices at the customer site using web (HTTP/HTTPS), RDP, VNC, or generic tunnel are disabled.

9

Cisco Device Management and Maintenance

The topics in this chapter provide information on Cisco device maintenance tasks that can be performed through the Cisco OnPlus Portal:

- **Automated Device Maintenance**
- **Backing Up and Restoring Device Configuration**
- **Managing Firmware for Supported Cisco Devices**
- **Installing Device Firmware**

Automated Device Maintenance

During automated maintenance, the firmware for the Cisco OnPlus Network Agent will be upgraded if new firmware is available. The Cisco OnPlus Network Agent automatically restarts after the upgrade.

For Cisco devices that support automated configuration backup and restore using the OnPlus Portal, a device configuration backup is requested.

- If the device configuration has not been modified, no backup is created.
- Valid login credentials (and enable password, if used) are required for device configuration backups. See **Credentials, page 90**.

Setting the Maintenance Start Time

To set the maintenance start time for a customer site, follow these steps:

STEP 1 From the Overview page on the portal, locate the customer that you want to edit and choose **Profile** > **Maintenance Window** from the navigation menu at the top of the page.

STEP 2 Choose a **Local Start Time**. The time is local to the timezone set on the Cisco OnPlus Network Agent.

STEP 3 Click **Save**.

Backing Up and Restoring Device Configuration

Configuration backups for devices that support this feature can be performed on demand from the **Backups** tab in the Device window. Configuration backup and restore is supported for select Cisco devices.

To perform configuration backup and restore for these devices, access credentials must be provided.

Devices are restarted after configuration is restored.

For more information about backing up and restoring device configuration files, see **Backups, page 97**.

For information about whether configuration backup and restore is supported for a particular device, see the following sections:

- **Device Feature Summary, page 241**
- **Device-Specific Limitations for OnPlus Features, page 243**

Managing Firmware for Supported Cisco Devices

You can upload firmware for selected Cisco devices that you have obtained from Cisco.com to the OnPlus Portal. This enables you to create a library of device firmware images for your customer's devices. The firmware can be used to upgrade devices of that type for your customers. You can upload multiple versions of device firmware and designate a default firmware version for each type of device.

Not all Cisco devices support firmware uploads. If a Cisco device on the network supports firmware uploads, the Firmware tab on the Device window is present.

New firmware for the Cisco OnPlus Network Agent device is made available through the OnPlus Portal and is installed automatically during the daily maintenance window, if needed.

For details, see the following sections:

- **Uploading Device Firmware to the Portal**
- **Viewing Version Information for Uploaded Firmware**
- **Installing Device Firmware**

Uploading Device Firmware to the Portal

To upload firmware for a Cisco device, follow these steps:

STEP 1 Download the firmware for the device from the Cisco.com Software Download area.

STEP 2 Log in to the Cisco OnPlus Portal.

STEP 3 From the **Overview** page, click on a customer that has a device of that type.

STEP 4 From either the Network Topology or Device Listing view on the Customer Dashboard, open the Device Information window.

STEP 5 Click the **Firmware** tab.

If the Firmware tab is not displayed, it means that firmware uploads are not supported for that type of device.

STEP 6 Click **Upload New Firmware** and browse to the location of the firmware that you downloaded from Cisco.com.

STEP 7 In the Upload Firmware dialog box for the device, enter an optional description.

Check the **Default Firmware** option if you want this version of the firmware to be the default firmware for this type of device. A New Firmware Available event is triggered for all devices of that type in your site that are not currently running that version of the firmware.

The **Default Firmware** option is not available if this is the first firmware load that has been uploaded for a device. The first time you upload firmware for a device, that firmware load is marked as the default firmware for the device.

STEP 8 Click **Upload**.

The version of the firmware that you just uploaded will be listed on the **Cisco** > **Firmware** page. See **Viewing Version Information for Uploaded Firmware, page 154**.

Viewing Version Information for Uploaded Firmware

To view a list of device firmware loads that have been uploaded to the portal, go to the main Overview page and choose **Cisco > Firmware** from the top-level navigation menu. The filename, Cisco product ID, and file size is displayed. Default firmware loads are identified with a check in the Default column.

Installing Device Firmware

To install Cisco device firmware that you have previously uploaded to the portal, follow these steps:

NOTE To install firmware, valid access credentials must be provided for the device. See **Credentials, page 90**.

STEP 1 Make sure that you have uploaded the firmware image that you want to install and that it is listed on the **Cisco** > **Firmware** page on the portal. See **Uploading Device Firmware to the Portal, page 153**.

STEP 2 From the Network Topology or Device Listing view, open the Device Information window for the device on which the firmware will be installed.

STEP 3 In the Device Information window, click the **Firmware** tab.

STEP 4 Select the version of the firmware that you want to install and open the actions drawer.

STEP 5 From the **Actions** drawer, choose **Install this firmware**.

The **Install this firmware** option is only displayed in the list if firmware for the device if you have uploaded it to the portal.

STEP 6 Click **Proceed** when prompted to confirm.

After the firmware is installed, the device is usually restarted.

10

Adding and Managing Authorized Agents

This chapter tells you how to invite, approve, and manage Authorized Agents associated with your Cisco OnPlus Partner Account.

Overview

Authorized Agents are other users that you allow to view, edit and delete your Cisco OnPlus Portal content. All information—except for your Partner Account profile, Reports, and Report Schedule—is shared between your account and your Authorized Agents' accounts.

Authorized Agents sign up for the Cisco OnPlus Portal using a special URL that you provide them. After an agent has signed up, you can approve their account. After it is approved, the agent account becomes active and enabled.

Authorized Agents for the Cisco OnPlus Portal must have a Cisco.com login to register with the portal.

- The Cisco.com login must be unique.
- You cannot use the same Cisco.com login for multiple agents or reuse your own Cisco.com login to register an agent.

IMPORTANT Only the user who creates the Cisco OnPlus Portal Partner Account can invite other users to become Authorized Agents. Authorized Agents cannot invite other agents.

To view on-screen instructions and workflow for inviting and managing Authorized Agents, choose **Agents** > **Agent Overview** from the navigation bar at the top of the Overview page.

Inviting Agents

You can invite agents to register using one of two methods:

- **Send an email invite**. On the Overview page, choose **Agents > Invite Agent**, enter one or more email addresses, edit the message, if needed, and click **Send Invite**. Separate multiple email addresses with commas.
- **Copy and paste your unique Cisco OnPlus Sign Up URL into an IM window or email**. From the Overview page, choose **Agents > Agent Overview**. Copy and paste the unique Cisco OnPlus Portal Sign Up URL displayed on that page into an email or IM chat window and send it to the prospective agent.
  - This URL is unique to your account, not to the prospective agent.
  - Use the same URL to invite all of your Authorized Agents.

Agent Registration Process

When the prospective agent receives the portal invitation email, they will follow these steps to register their account on the portal:

STEP 1 Click the sign-up URL link provided in the email to go to the Cisco OnPlus Portal **Register** page.

STEP 2 Complete the fields on the **Register** page. The information to be provided includes:

- Email address to verify registration
- Cisco.com User ID and Password
- Contact information

- Verification code that is displayed in the graphic on the registration page

STEP 3 In the **Privacy Confirmation** section, the agent must click the checkbox to acknowledge that they have read and accepted the Cisco Privacy Statement.

STEP 4 Click **Submit**. Upon successful registration, the **Registration Complete** page appears, and the following message appears:

```
Mary Jones,

Congratulations! You have successfully registered. We will
notify you at the email you provided (email@domain.com) once
the administrator has reviewed and approved your
registration.

To return to the login screen, click here.
```

After the agent has registered, you must go to the Pending Agents page and approve or reject the request. See **Approving or Rejecting Pending Agent Requests, page 159**.

Approving or Rejecting Pending Agent Requests

To approve or reject pending agent requests, follow these steps:

STEP 1 From the Overview page, go to **Agents** > **Pending Agents**.

STEP 2 Locate an agent from the list and click the arrow icon to open the drawer to show the **Approve** or **Reject** options.

STEP 3 Click **Approve** or **Reject**.

- Approved agents receive an email indicating that their account is active and are moved to the **Approved Agents** list on the portal.
- Rejected agents are moved to the **Rejected Agents** list.

To reinvite a prospective agent who was previously rejected, you must first delete them from the Rejected Agents list before sending another invitation.

Deleting an Agent

To delete an approved agent account or remove an agent from the Rejected Agents list, follow these steps:

You can reinvite agents who have been deleted.

STEP 1 From the Overview page, go to **Agents** > **Approved Agents** or **Agents** > **Rejected Agents**.

STEP 2 Locate the agent to be deleted and click the arrow icon to open the drawer to show the **Delete** option.

STEP 3 Click **Delete**.

Logging In as an Agent

When you approve an agent account request, the agent receives an email similar to the following:

:

Mary Jones,

Congratulations! Your Cisco OnPlus Portal account is now active. You may now login at the following URL:

https://www.cisco-onplus.com

Your username: mjones

To log in, the agent clicks on the link in the email, enters the username provided in the email, and uses their Cisco.com account password for authentication.

After the agent is successfully logged in, they must read the **Terms and Conditions** and click the **Accept** button at the bottom of the page.

The Agents menu is not displayed in the navigation bar when the user is logged in as an agent.

What Can Your Authorized Agents See and Do on the Portal

All information—except for your Partner Account profile and any report or report schedules created by you—is shared between your Partner Account and your Authorized Agents' accounts.

This means that all customer sites, customer contacts, events, and notifications can be viewed, edited, and deleted by all of your Authorized Agents. Agents can connect remotely to devices and perform device management actions such as firmware upgrades and device configuration backup and restore.

Authorized Agents cannot invite, approve, reject, delete other agents, and they cannot see the pending, rejected, or approved agent lists.

Authorized agents do not have permission to set product support expiration reminder intervals. These can only be set by the Partner Account holder. For more information, see **Setting the Product Support Expiration Reminder Interval, page 186**.

Only the creator of the Partner Account can invite or manage agents.

11

Giving Your Customer Access to the OnPlus Portal

This chapter describes how to add and manage Customer Logins on the OnPlus Portal. It also includes login instructions for Customers and shows how they can use their authorized access capability.

Overview

Partners and their Authorized Agents can give their Customers a login on the OnPlus Portal to enable them to view their own networks and devices. After the initial activation of a customer login, Partners can modify the Customer's access level or terminate access, as needed.

NOTE Before you can grant access to a Customer, the Customer must first sign up for a Cisco.com account.

After the Customer accepts their invitation and activates their access, they can view, or even modify information about their network, depending on the access that they are given.

There are two levels of access for Customers: read only and full access.

- Read only access lets Customers see their network without being able to change any data or settings.

- Full access allows Customers to view more of their network and allows limited changes to selected data on the portal.

A table has been provided to show the capabilities by access mode. See **OnPlus Features Available to Customers by Access Mode, page 165**.

The process for giving and managing your Customers' access to their network includes:

- Selecting a Customer and sending an OnPlus invitation
- Checking the access status for the Customer to ensure they have activated their access
- Changing the Customer's access mode
- Deleting Customers to terminate network access

Adding a Customer Login

To add a Customer Login, follow these steps:

STEP 1 From the Overview page, choose a Customer for which you want to add a Customer Login.

STEP 2 From the Profile menu at the top of the page, choose **Profile > Customer Logins.**

STEP 3 Click + **Add Customer Login.**

STEP 4 From the Add Customer Login window, enter the required information, ensuring that the correct **Cisco.com User ID** is entered.

STEP 5 Click **Add.** This action adds the Customer to the Customer Logins page with a status of Pending, and forwards an invitation email to the Customer when the **Send Invitation Email** box has been checked.

Customer Login Activation Process

When the Customer receives their OnPlus email invitation they will follow these steps to activate their login:

STEP 1 The Customer clicks on the link provided in the invitation email to go to the Customer Invitation page.

STEP 2 The Customer enters their Cisco.com password and clicks **Activate**.

The page updates to display a message that their invitation has been accepted with a link to the Cisco OnPlus Portal Log In page.

STEP 3 The Customer can click the link to view their network by entering their Cisco.com Username and Password to log in.

After the Customer has successfully logged in, they must read the **Terms and Conditions** and click **Accept** at the bottom of the page.

The Cisco OnPlus Portal opens on the Dashboard page. See **OnPlus Features Available to Customers by Access Mode, page 165** for more information about using Customer Login access.

OnPlus Features Available to Customers by Access Mode

This table shows the access privileges assigned by access mode: Read Only and Full Access.

Feature	Notes	Access Mode	
		Read-Only	Full Access
Customer Dashboard			
Status	View network status	Yes	Yes
Events	View and filter events	Yes	Yes
Profile	View and modify profile information	View Only	Yes (limited)
Ping Host	Test network connectivity	No	Yes
Data Reset Functions	Reset topology or rediscover network	No	Yes
Topology Settings	Change tree layout format	No	Yes
Create Labels	Use the Setting tool to create labels for devices	No	Yes

Feature	Notes	Access Mode	
		Read-Only	Full Access
Filter Criteria	Advanced search settings and capability	Yes	Yes
Full Screen Mode	Change to full screen mode	Yes	Yes
Add Device	Add devices to the network	No	Yes
Network View	Toggle between topology and device listing views	Yes	Yes
Zoom	Zoom in and out on the topology view	Yes	Yes
Legend	Toolbar, icons, alarms, and actions icon table	Yes	Yes
Customize	Create a custom view of the dashboard	Yes	Yes
Scan Network	Use the OnPlus Scanner	No	No
Export	Export the network device listing in PNG, CSV, or SVG formats	Yes	Yes
To-Do	Lists devices that require intervention	Yes	Yes
Devices			
View device information	Customer's own devices only	Yes	Yes
Modify device settings	Customer's own devices only	No	Yes
Modify device access credentials	Customer's own devices only	No	Yes
Connect to device	Customer's own devices only	No	Yes
Add and modify device monitors	Customer's own devices only	No	Yes
View events by device	Customer's own devices only	Yes	Yes
View Cisco support information*	*Excluding Contract Information	Yes	Yes
Configuration backup and restore		No	No
Firmware upgrade		No	No
Change root device	Replace current root device	No	Yes
Collapse/expand sub-tree		No	Yes
Add child device	Add a new child device	No	Yes
Global Partner Account Features	Notifications, Reports, Apps (Some of these functions will not appear on the page and others will appear greyed out.)	No	No

Feature	Notes	Access Mode	
		Read-Only	Full Access
Issue Invitations	Invite Agents or Customers	No	No

Detailed information for using the Dashboard features can be found in **Dashboard Overview and Features, page 57**.

Managing Customer Logins

Activated and Pending Customer Logins are managed from the Customer Logins page.

Editing a Customer Login

STEP 1 From the Customer Name list on the Overview page, select the Customer.

STEP 2 From the Profile menu at the top of the page, choose **Profile > Customer Logins.**

STEP 3 From the Customer Logins page, click once on the entry that you want to edit.

STEP 4 From the actions drawer, choose **Edit**. Edit allows the following functions:

- Enter Comments
- Change the Access Mode.

Deleting a Customer Login

STEP 1 From the **Customer Name** list on the Overview page, select the Customer.

STEP 2 From the Profile menu at the top of the page, choose **Profile > Customer Logins.**

STEP 3 From the Customer Logins page, click once on the entry that you want to delete.

STEP 4 From the actions drawer, choose **Delete**. Delete terminates the Customer's access to the portal.

Resending an Invitation to a Customer Login

STEP 1 From the **Customer Name** list on the Overview page, select the Customer.

STEP 2 From the Profile menu at the top of the page, choose **Profile > Customer Logins.**

STEP 3 From the Customer Logins page, click once on the entry to which you want to resend an invitation.

STEP 4 From the actions drawer, choose **Resend Invite.**

STEP 5 Enter the required information in the email window, and resend the invitation to the Customer.

For information on how the customer activates their access to the portal using the link provided in the invitation, see **Customer Login Activation Process, page 164**

Customer Access Using a Mobile Device

Customers can access their information from a mobile device by logging on through a browser. web browser access provides the same functionality that is available through the OnPlus Portal computer interface. For more information about using Mobile Device Access, see **Chapter 18, "Mobile Device Access to the OnPlus Portal"**.

NOTE Customer access is currently not available through the OnPlus Mobile Application.

12

Reports

This chapter explains how to use Cisco OnPlus Portal reporting features. These topics are covered:

Overview

The type of Cisco OnPlus account that you have determines the type of report capability to which you have access. All customers have access to the Lifecycle Digest report.

Customer Accounts

From the Dashboard page, choose **Reports** and click **Lifecycle Digest Settings**.

- Lifecycle Digest is used to send the current device lifecycle status to customers using email.
- Lifecycle Digest reports are sent using email in formatted HTML.
  - The email consists of the contract, warranty, end-of-life, and advisories about the devices uploaded to OnPlus.

- The email notifications are sent at user-scheduled intervals, always delivered on Monday morning, and can be written in the language you choose.

For more detailed information about the Lifecycle Digest report, see **Lifecycle Digest, page 171**.

Partner Accounts

From the Overview page, choose **Reports** to access these reporting options:

- **Report Listing**. From the Report Listing page, you can create and schedule new reports, view a list of reports, and access options for previewing, downloading, and removing individual reports.
- **Report Schedule**. From the Report Schedule page, you can view information for scheduled reports or remove (cancel) them.

Reports are associated with a specific portal user login:

- You can only view or delete reports that you created.
- You cannot view or delete any reports that were created by your authorized agents.

When you create a report, you can choose to create it immediately or schedule it as a recurring report that is generated daily, weekly, or monthly. You can also specify whether you want to be notified when the report has been created. Reports can be provided in PDF, CSV, and XHTML formats.

For scheduled reports, you can specify a recipient from your delivery contacts and have reports delivered through email. For detailed information about creating and scheduling report, see **Creating a Report, page 174**.

Lifecycle Digest

The type of Cisco OnPlus account that you have, determines the type of report capability to which you have access. All customers have access to the Lifecycle Digest report.

Customer Accounts

From the Dashboard page, choose **Reports** > **Lifecycle Digest Settings**.

- Lifecycle Digest is used to send the current device lifecycle status to customers using email in formatted HTML.
- Lifecycle Digest reports are sent using email in formatted HTML.
- The email consists of the contract, warranty, end-of-life, and advisories about the devices uploaded to OnPlus.
- The email notifications are sent at user-scheduled intervals, always delivered on Monday morning, and can be written in the language you choose.

To create a Lifecycle Digest report, follow these steps:

STEP 1 From the Dashboard view, choose **Reports** > **Lifecycle Digest Settings.**

STEP 2 The **Email Notification** checkbox is **On** by default. By clicking the **Off** checkbox, you will disable the Lifecycle Digest report.

STEP 3 Fill in the required fields to set the delivery criteria.

a. **Preferred Language** - choose language from the drop-down list options.

b. **Report Recipient** - choose the email address from the drop-down list to which the report will be sent.

c. **Frequency** - choose the option from the drop-down list that best fits your needs. Reports can be delivered weekly, biweekly, or monthly.

STEP 4 From the **Categories** menu, select the options by placing a check in the box next to the option(s) you want to appear in your Lifecycle Digest report.

STEP 5 Click **Save**.

The report provides links to detailed information for each entry. For example, if you click **View Details** at the end of the line that reports the number of warranties that are expiring, you will open the Cisco Onplus Portal and, after signing in, the Warranty Information page displays showing the expired warranties at the top of the warranties list. You can also link directly to the OnPlus Scanner from the report.

The link(s) at the end of the report, Helpful Link(s), let you change the frequency of the Lifecycle Digest report or stop it completely. There is also a link that allows you to comment or offer suggestions about the Lifecycle Digest report.

NOTE For customers of Partners, the links to detailed information are not available in the report and the Helpful Link(s) section of the report is not included.

Report Types

The following types of reports can be generated for Partner accounts:

- **Customer Report.** This report lists all of your customers—Online (active), Suspended, and Never Connected (awaiting activation). The report shows customer information (name, address, and contact) and the date of activation, suspension, or creation.
- **Customer Inventory.** This report can be generated for all customers or for a specific customer. The report includes both Cisco devices and non-Cisco

devices. For Cisco devices, the IP address, model, MAC address, and firmware versions are listed. For non-Cisco devices, the IP address, MAC address, model (if known), and vendor (if known) are listed.

- **Event History, filtered by severity.** This report can be generated for all customers or for a specific customer.

  The report includes the total number of events, a graph of event distribution by severity level, and the date, event ID, and message for each event. Events are listed by severity level.

- **Executive Summary.** This report can be generated for a specific customer. The report includes customer information (name, address, timezone), Internet connectivity data (number of times the Internet connection was down), Cisco OnPlus Network Agent device information and status, network topology data, new devices discovered, network event summary data, and product support information (warranties, service contracts, end-of-life and end-of-sale products, field notices, and product security advisories).

- **Notification History.** This report can be generated for all customers or for a specific customer. The report includes the total number of notifications sent for each customer and the date, event type, and delivery target (for example, email address) for each notification.

NOTE The following report options only appear in the Report drop-down list when the OnPlus Wireless Management application is installed, and at least one WAP121 or WAP321 is installed in the network:

- **Wireless Access Point Summary.** This report can be generated for a specific customer, provided that at least one Cisco WAP121 or WAP321 device is installed in a customer's network. The report provides historical data, allowing the user to indicate start and end dates. Sections are user-selectable and include access point, client association, and traffic history data.

- **Wireless Client Summary.** This report can be generated for a specific customer, provided that at least one Cisco WAP121 or WAP321 device is installed in a customer's network. This is an on-demand report that shows all current activity on the network.

- **Top Clients by Connection Time Summary.** This report provides a combined view of up to 100 client networks showing longest connection time to shortest connection time. The report is also broken out by access point showing the client connection time for each access point in the network.

- **Top Clients by Traffic Summary.** This report provides a combined view of up to 100 client networks showing traffic volume from greatest to least. The report is also broken out by access point using the same data to show traffic volume by client for each access point in the network.

The following application note is available on the Cisco Support Community:

- *Cisco OnPlus for Small Business Wireless Deployments*

Creating a Report

To create a report, follow these steps:

STEP 1 Navigate to **Overview >Reports >Report Listing**.

STEP 2 On the Report Listing page, click **+ Create Report**.

STEP 3 Choose the type of report you want to create.

Depending on the type of report that you are creating, choose from these options.

Option	Required?	Description	Applies to These Reports
Format	Yes	Specify a report format. Available formats include Adobe PDF, CSV (comma-separated values), and XHTML - Extensible Hypertext Markup Language.	All reports
Preferred Language	Yes	Specify the language in which the report will be generated. Available options include: French, German, Italian, and Spanish.	All Reports
Customer	Yes	Specify whether the data in the report is provided for all customers or choose a specific customer.	Customer Inventory, Event History, Executive Summary, Notification History
Cover Page Notes	No	Enter notes to display on the title page of the report. You can enter up to 300 characters. This option does not apply to reports created in CSV format.	All reports

Option	Required?	Description	Applies to These Reports
Severity	Yes	Choose a severity level. Events of the chosen severity level and higher are included in the report.	Event History

STEP 4 Click **Next**.

STEP 5 On the **Sections** page, click to select or deselect the sections that you want to include in the report. Available sections listed here vary, depending on the type of report selected.

STEP 6 Click **Next**.

STEP 7 Specify scheduling and notification options for the chosen report type using the following options:

Option	Description
Report Creation	Set the report frequency. Choose **Now** to generate a report immediately. Choose **Every Day**, **Every Week**, or **Every Month** to schedule a recurring report. ▪ Daily reports are run at 00:00:00 (midnight) each day. ▪ Weekly reports are run every 7 days, beginning with the date you set for **First report occurs on**. ▪ Similarly, monthly reports are run every month, beginning with the date you set for **First report occurs on**. ▪ For example, if you set **First report occurs on** to June 15 when scheduling a monthly report, the first report is generated on June 15, and it includes data for the past month. The next monthly report in the series will be generated on July 15.
Report Period Start **Report Period End**	If you chose **Now**, click in these fields, use the Calendar popup to choose start and end dates for the reporting period. This field does not apply to Customer or Inventory reports.

Option	Description
First report occurs on **Last report occurs on**	If you chose **Every Day**, **Weekly**, or **Monthly**, click in each of these fields to open a Calendar popup and specify the reporting period by selecting dates for the first and the last report. You can also choose not to specify an end date by choosing **No end date**. The report schedule is automatically deleted after the last report is run. When you first open the Calendar popup, the current date is selected.
Notify me	This option applies only to scheduled recurring reports. When **Notify me** is checked, a notification is sent to the email address specified in your portal account profile whenever the report is generated.
Report recipient and email address	Choose a customer contact or global contact from the drop-down list. After you choose a recipient, select a delivery method from the drop-down list. Only customer or global contacts with a configured email address target are listed. The report is delivered as an email attachment. For more information about delivery contacts, see **Adding and Managing Delivery Contacts, page 112**. If the contact's email address target is disabled on the Delivery Contacts page, the report is not delivered.
Email message	Optional. If a report recipient and email address are specified, you can enter text to include in the email message that is delivered with the report. You can enter up to 300 characters. Left angle bracket characters (<) and newline characters in the message text are stripped from the email message.

STEP 8 If you are creating the report now, click **Save**. The report will be queued for processing.

To view the status of your report request or preview and download completed reports, choose **Reports** > **Report Listing**. See **Previewing and Downloading Reports, page 177**.

You may need to refresh the Report Listing page to view current report status, especially if you just created the report.

STEP 9 If you are scheduling a series of reports, click **Save** to update the list of scheduled reports.

To view information about scheduled reports, choose **Reports** > **Report Schedule**.

Viewing Report Schedules

NOTE You cannot change a scheduled report after you create it. You must delete and recreate the report and its scheduling information if you need to make changes.

Report schedules are removed from the portal automatically at the start of the next reporting period that occurs after the last report is run.

You can only view report schedules that you created.

To view a scheduled report, follow these steps:

STEP 1 From the Overview page, choose **Reports** > **Report Schedule**.

STEP 2 Click the report schedule that you want to view.

STEP 3 Click **Details** to view additional information and see a list of all reports generated from this rule. Click a specific report to access download and delete actions for the selected report.

STEP 4 Click **Back** to return to the report schedule list.

Previewing and Downloading Reports

On the Report Listing page, you can view report information and processing status, see a list of all reports that have been created, and preview or download completed reports.

To preview or download a report, follow these steps:

STEP 1 From the Overview page, choose **Reports** > **Report Listing**.

Click a column heading to sort the list by Report (type), Notes, State (Queued, Processing, or Error), Format (PDF, CSV, or XHTML), size, or date created.

Use the paging controls on the lower right corner of the page to browse the list, if needed.

STEP 2 Click a report in the list to select it and access the actions drawer.

STEP 3 Choose **Preview** to view a thumbnail version of the completed report. Click the preview graphic on the left to page through sections of the report.

STEP 4 Choose **Download** to download a copy of the completed report to your PC.

When a report is produced in XHTML format, a .zip file is created for you to download. The .zip file contains a root directory with the report (index.html) and all assets (images in .png format and a CSS stylesheet file for formatting). This directory structure allows you to extract reports to a web server "www" directory for easy publishing.

NOTE To view the images, the .zip file must be fully extracted.

STEP 5 Save the report to your computer.

Deleting Reports

You can only access or delete reports that you created.

To delete a single report from the Report Listing page, follow these steps:

STEP 1 From the Partner Account Overview page, choose **Reports** > **Report Listing**.

STEP 2 Click the report that you want to delete.

STEP 3 Click **Delete**.

To delete reports generated from a report schedule rule from the report schedule list, follow these steps:

STEP 1 From the Partner Account Overview page, choose **Reports** > **Report Schedule**.

STEP 2 Click the scheduled report to open the actions drawer.

STEP 3 Click **Details**.

STEP 4 On the report schedule detail page, click **Delete All** to delete all reports that were generated from this scheduling rule. Click **OK** to confirm.

STEP 5 You can also delete a specific report from the history list. To do this, select the report from the Report History list to open the actions drawer, then click **Delete**. Click **OK** to confirm.

Deleting a Report Schedule

You can only delete a report schedule that you created.

To delete a report schedule, follow these steps:

STEP 1 From the Partner Account Overview page, choose **Reports** > **Report Schedule**.

STEP 2 Click the scheduled report to open the options drawer.

STEP 3 Click **Delete**.

STEP 4 Click **OK**.

13

Viewing Cisco Product Support Information

This chapter explains how to view product support information for supported Cisco devices through the OnPlus Portal. These topics are covered:

Overview

Through the OnPlus Portal, you can view the following types of product support information for Cisco devices and software:

- Service Contract (either Smartnet or Small Business Support) and Warranty information (device access credentials required)
- Product Security Advisories (PSIRTs)
- Hardware end-of-life, end-of-support, and end-of-sale notices
- Field notices

IMPORTANT To obtain Service Contract and Warranty information for a Cisco device, you must provide Login and/or Enable access credentials (for instructions, see **Credentials, page 90**). After providing access credentials, the next time that discovery runs on the portal, the Support tab for the device should appear in the Device Information window, and the product support information obtained for the device will be available.

NOTE There can be a delay between the time that the Cisco Support information database is updated and when the updates are available to be displayed on the Cisco OnPlus Portal. Depending on the type of information, the delay can range from a few days to more than a week.

Viewing Product Support Information for All Customers

From the Customer Dashboard, you can view device support information for devices in your network. To access product support information, select options from the Dashboard menu.

Product Support Information Category	Description/Information Included
End of Life (Hardware)	Product Icon, Product ID, and Serial Number Description Announced Date End of Sale Service Renewal End-of-support URl Migration Product ID
End of Life (Software)	Status, Product Icon, Product ID, and Serial Number OS, OS Version Description End of Sale End-of-support URl
Product Security Advisories	Product Icon, Product ID, and Serial Number Type OS and OS Version Advisories
Field Notices	Product Icon, Product ID, and Serial Number Description Date Published Revised URL
Warranties	Product Icon, Product ID and Serial Number Instance IDType Warranty Start Warranty End MAC Address

Product Support Information Category	Description/Information Included
Contracts	Status, Product Icon, Product ID and Serial Number Service Program Service Level Agreement Start Date End Date

From the Partner Account Overview area of the portal, you can view device support information for all of your customers. To access product support information, select options from the Cisco menu.

Product Support Information Category	Description/Information Included
Contract Information	Contract status Customer Product Icon, Product ID, and Serial Number Service Program Service Level Agreement Start date and end date
Warranty Information	Customer Product Icon, Product ID, and Serial Number Warranty Start Date Warranty End Date MAC Address
Hardware End of Life	Status Customer Product Icon, Product ID, and Serial Number Description Announced Date End-of-Sale Date Service Renewal Date End-of-support Date Clickable link to published notice on Cisco.com
Software End of Life (applies mainly to Cisco IOS software versions)	Status Customer Product Icon, Product ID, and Serial Number OS and OS Version Description End-of-support, End-of-life, End-of-sale dates, Clickable link to published notice on Cisco.com

Product Support Information Category	Description/Information Included
Field Notices	Customer Product Icon, Product ID, and Serial Number Description Clickable link to Cisco.com location of full notice Date Published Last Revised Date
Product Security Advisories (PSIRTs) (applies mainly to Cisco IOS software versions)	Customer Product ID and Serial Number Description Type OS and OS Version Service Renewal Date End-of-support date Clickable link to details for each advisory, including Severity, Description, date published, and clickable link to published notice on Cisco.com

Viewing Product Support Information for a Specific Device

To view product support information for a specific device, if you have a Partner account, follow these steps:

STEP 1 From the Partner Account Overview page, click a customer to go to their Dashboard.

STEP 2 From the Topology or Device Listing view on the customer Dashboard, select the device and open the Device Information window.

STEP 3 Click the **Support** tab.

STEP 4 On the **Support** tab, click the category of support information you want to view. Only categories of support information that are available for that device are displayed.

Many of the tabs provide clickable links to additional information.

Product Support Events

Product support events are generated in response to:

- Warranty and service contract expiration
- Product security advisories (PSIRTs)
- Product end-of-sale, end-of-life, and end-of-support announcements
- Field bulletins

These product support events are issued with a severity level of Notice. For information about viewing events, see **Viewing Events, page 127**.

Product support expiration reminders are issued with a severity level of Warning. See **Setting the Product Support Expiration Reminder Interval, page 186**.

Including Product Support Information in Reports

When creating an Executive Summary report, you can choose to include sections that provide a summary of the following product support information for Cisco devices:

- Warranty status
- Contract status
- Product security advisories, grouped by severity
- Field notices

The Device Details section in the Customer Inventory report displays product support information for Cisco devices.

For more information, see **Creating a Report, page 174**.

Setting the Product Support Expiration Reminder Interval

By default, expiration reminders for service contract, product warranty, and hardware or software end-of-life events are generated 60 days prior to the expiration date.

Product support expiration reminders are generated with a severity of Warning, and notifications are delivered to the contact specified in the default delivery rule. If you delete or disable notifications for the default delivery rule without creating another rule for expiration events, you will not receive reminder notifications (see **Creating Delivery Rules for Product Support Notifications, page 187**).

To change the default reminder interval for an product support expiration event to something other than 60 days prior to the expiration date, follow these steps:

IMPORTANT Authorized agents do not have permission to set product support expiration reminder intervals. These can only be set by the Partner Account holder.

STEP 1 From the Partner Account Overview page, choose **Cisco** > **Contract Information**, **Warranty**, **Hardware End-of-Life**, or **Software End-of-Life**.

You can set a different reminder interval for each type of product support expiration event.

STEP 2 Click the **Change** button to the right of the **Reminders** label.

STEP 3 Set the number of days for the reminder.

If you do not want to receive product support expiration reminders, set the number of days before the reminder to **Off**.

STEP 4 Click **Save**.

Creating Delivery Rules for Product Support Notifications

Product support events are generated with a severity level of Notice. To receive notification using email or SMS text messages for these events, we recommend that you create a notification delivery rule, make sure that the **Specify Event** option is enabled and that you specify one of the following Product event types:

- Product: Cisco Security alert (PSIRT)
- Product: Cisco service contract alert
- Product: End-of-sale, end-of-life, end-of-support notice
- Product: End-of-warranty alert

14

Cisco ON100 Maintenance

This section provides instructions for performing manual Cisco OnPlus Network Agent maintenance tasks:

- **Modifying Network Settings after Activation**
- **Resetting a Cisco OnPlus Network Agent**
- **Performing a Factory Reset on the Cisco OnPlus Network Agent**
- **Cisco OnPlus Network Agent Status LEDs**
- **Deactivating a Site to Replace (RMA) the Cisco OnPlus Network Agent**
- **Transferring a Cisco OnPlus Network Agent to a Different Customer**

Modifying Network Settings after Activation

After activation, you can modify network settings on the Cisco OnPlus Network Agent to:

- Assign a static IP address to the Cisco OnPlus Network Agent or use DHCP to obtain an IP address
- Change DNS nameserver settings
- Change NTP server settings

To edit network settings after activation, follow these steps:

STEP 1 From the Network Topology or Device Listing view, open the Device Information window for the device.

STEP 2 From the Actions menu on the Settings tab, choose **Connect to Device**, then click **Confirm**.

NOTE If remote connections to the customer site are disabled, you must connect to the Cisco OnPlus Network Agent from a PC on the LAN by using its IP address or using Bonjour, UPnP, or Cisco FindIT.

STEP 3 Log in to the Cisco OnPlus Network Agent.

a. In the Username field, enter **admin**.

b. In the **Password** field, enter the customer site password (the same one that you entered in the Install site page). By default, this is a 6-digit auto-generated password.

If you do not know the customer password, open the **Profile** page for that customer on the portal and refer to the **Activation Information** section.

Click **Log In**.

STEP 4 Click the **Configuration** link at the top of the page.

STEP 5 Click **Configure additional network settings**.

STEP 6 Edit IP address, DNS nameserver, or NTP settings as needed.

STEP 7 Click **Apply network settings**.

Resetting a Cisco OnPlus Network Agent

When the Cisco OnPlus Network Agent is reset, all processes are safely shut down, the OnPlus Portal is restarted, and the firmware is automatically upgraded, if needed.

This type of reset can be performed to force the Network Agent to check for updated firmware, clear a minor condition, or retry activation. Customer data on the appliance and association with the portal are not affected by this type of reset.

To manually reset the Cisco OnPlus Network Agent from the OnPlus Portal, follow these steps:

STEP 1 From the customer's Network Topology or Device Listing view, open the Device Information window for the Cisco OnPlus Network Agent.

STEP 2 Click the **Settings** tab.

STEP 3 From the **Actions** menu, choose **Reboot device**.

STEP 4 Click **Confirm**.

You can also use the **RESET** button on the back panel of the Cisco OnPlus Network Agent. Press and hold the **RESET** button in for less than 10 seconds.

Performing a Factory Reset on the Cisco OnPlus Network Agent

A factory reset removes all customer data from the Cisco OnPlus Network Agent and all association with the OnPlus Portal. This type of reset is intended to be used in situations where you want to restore the device to factory default state or remove existing customer data so that the agent can be reactivated with another customer.

You can perform a factory reset of the Cisco OnPlus Network Agent by connecting to the device (either remotely from the portal or locally) and using the Cisco OnPlus Network Agent Management Utility.

The Cisco OnPlus Network Agent can also be factory reset using the RESET button on the back panel.

For instructions, refer to the following sections:

- **Performing a Factory Reset Through the OnPlus Portal, page 191**
- **Performing a Factory Reset Using the RESET Button, page 192**

Performing a Factory Reset Through the OnPlus Portal

To perform a factory reset of the Cisco OnPlus Network Agent from the OnPlus Portal, follow these steps:

STEP 1 From the Network Topology or Device Listing view, open the Device window for the device.

STEP 2 From the Actions menu on the Settings tab, choose **Connect to Device**, then click **Confirm**. When the remote connect is established, the Cisco OnPlus Network Agent login page appears.

NOTE If remote connections to the customer site are disabled, you must connect to the Cisco OnPlus Network Agent from a PC on the LAN by using its IP address or using Bonjour, UPnP, or Cisco FindIT.

STEP 3 Log in to the Cisco OnPlus Network Agent.

a. In the Username field, enter **admin**.

b. In the **Password** field, enter the customer site password (the same one that you entered in the Install site page). By default, this is a 6-digit auto-generated password.

If you do not know the customer password, open the **Profile** page for that customer on the portal and refer to the **Activation Information** section.

Click **Log In**.

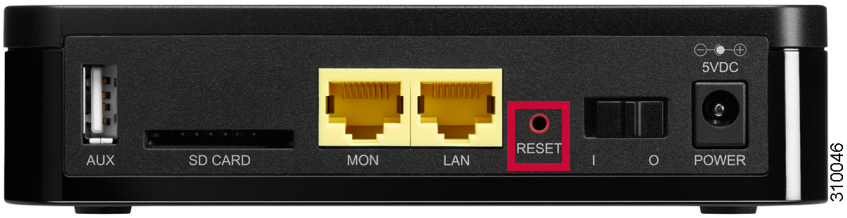
STEP 4 Click the **Maintenance** link at the top of the page.

STEP 5 Click the **Factory Reset** icon.

STEP 6 Click **OK** when prompted to confirm the reset.

Performing a Factory Reset Using the RESET Button

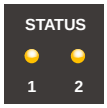
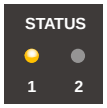
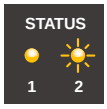
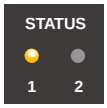
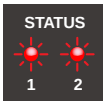
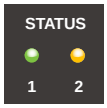
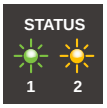
To reset the Cisco OnPlus Network Agent to factory defaults using the RESET button on the back panel of the device, use a paperclip or similar object to press and hold the RESET button for 10 or more seconds.

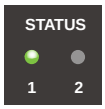
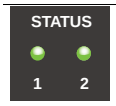


When the STATUS 1 LED is lighted steady green and the Status 2 LED is off, the device is ready to be powered down or reactivated. See **Cisco OnPlus Network Agent Status LEDs, page 193**.

Cisco OnPlus Network Agent Status LEDs

The STATUS 1 and STATUS 2 LEDs on the front panel of the Cisco OnPlus Network Agent indicate the progress of the device during power up, restart, upgrade, and reset operations.

Status LEDs			Description
Power On and Initialization			
	1	Steady Amber	Power-on sequence.
	2	Steady Amber	
	1	Steady Amber	Starting software initialization.
	2	Off	
	1	Steady Amber	Acquiring an IP address. If this pattern appears for more than two minutes, it indicates that the Cisco OnPlus Network Agent has failed to obtain an IP address. If a static IP is configured, this pattern is never displayed for more than 10 seconds.
	2	Blinking Amber	
	1	Steady Amber	Completing software initialization.
	2	Off	
Software Download and Upgrade			
	1	Blinking Red	Downloading and installing the base software image (requires Internet connection). You will only see this pattern prior to activation (during out-of-box installation) or after a factory reset.
	2	Blinking Red	
	1	Steady Green	Upgrading software (requires Internet connection).
	2	Steady Amber	
Restart			
	1	Blinking Green	Restarting the Cisco OnPlus Network Agent. The Cisco OnPlus Network Agent restarts after a normal reset, factory reset, or software upgrade.
	2	Blinking Amber	
Ready for Activation / Device Online, No Connectivity with OnPlus Portal			

Status LEDs			Description
	1	Steady Green	If the Cisco OnPlus Network Agent has not yet been activated, this LED pattern means that the agent software is running and the device is ready for activation. If the Cisco OnPlus Network Agent has already been activated, this LED sequence means that the Cisco OnPlus Network Agent software is running, but the device does not have connectivity to the OnPlus Portal.
	2	Off	
Normal Operation (Activated / Online)			
	1	Steady Green	When both status LEDs are lit Steady Green, it means that the Cisco OnPlus Network Agent is activated, online, and is communicating with the OnPlus Portal. This is the normal mode of operation.
	2	Steady Green	

Deactivating a Site to Replace (RMA) the Cisco OnPlus Network Agent

The site deactivation feature is primarily intended for situations in which you want to replace or RMA a customer's Cisco OnPlus Network Agent and reactivate the customer using the replacement device. This feature can also be used for troubleshooting or demonstration purposes when you want to deactivate a site, then reactivate the customer with the same Cisco OnPlus Network Agent.

When a site is deactivated:

- All customer data is removed from the Cisco OnPlus Network Agent device.
- As long as you do not delete the customer, the customer's information is retained (for example, device credentials and device monitor settings). When the customer is reactivated, these settings will be present.
- The Status page for the deactivated site displays "Activate."
- The Cisco OnPlus Network Agent can no longer be used to communicate with the portal until it is reactivated.

To deactivate a site, follow these steps:

STEP 1 On the Overview page of the portal, click the customer whose site you want to deactivate.

STEP 2 From the Network Topology or Device Listing view, open the Device window for that customer's Cisco OnPlus Network Agent.

STEP 3 Choose the **Settings** tab.

STEP 4 From the **Actions** drop-down list on the Settings tab, choose **Deactivate this entire site**.

STEP 5 Click **Confirm**.

If you are replacing the Cisco OnPlus Network Agent, you can then install the replacement ON100 device and reactivate the customer.

Transferring a Cisco OnPlus Network Agent to a Different Customer

To transfer a Cisco OnPlus Network Agent to a different customer, follow these steps:

STEP 1 Perform a factory reset on the Cisco OnPlus Network Agent associated with the old customer. See **Performing a Factory Reset on the Cisco OnPlus Network Agent, page 191**.

STEP 2 Create an account on the OnPlus Portal for the new customer. See **Adding a Customer, page 34**.

STEP 3 At the new customer site, install and activate the Cisco OnPlus Network Agent using the new customer's activation information. See **Installing and Activating the Cisco OnPlus Network Agent at the Customer Premises, page 21**.

STEP 4 Delete the old customer account to permanently remove all information about that customer from the OnPlus Portal. See **Deleting a Customer, page 35**.

15

Integrating Autotask Service Ticketing

This section provides instructions for configuring Apps settings on the Cisco OnPlus Portal and Autotask. These application settings allow automatic Autotask Service Desk ticket creation, based on events and notifications generated through the portal. In addition, this section provides instructions for Autotask to display the discovered devices.

These topics are covered:

Autotask Version Compatibility

The Cisco OnPlus Portal uses Version 1.5 of the Autotask API.

Autotask supports Internet Explorer 7 or later. If you use another browser, certain parts of the application will be unavailable. For information about web browser compatibility for Autotask, see **Running the Autotask Web Browser Check, page 198**.

Configuring Settings in Autotask

The topics in this section describe settings you must configure in Autotask so that Autotask service desk tickets can be created automatically, based on events that are monitored through the Cisco OnPlus Portal. In addition, this section provides instructions for Autotask to display the discovered devices.

Running the Autotask Web Browser Check

Web browser incompatibilities can result in problems with Autotask setup such as Javascript errors.

To verify that your web browser settings are compatible with Autotask, follow these steps:

STEP 1 Log in to Autotask.

STEP 2 Click **Help** > **Check My Browser Settings**.

STEP 3 Click **Begin Test**.

After the test runs, the results will indicate what must be corrected.

STEP 4 Before continuing, verify that all compatibility checks are Green.

Creating a Service Desk Queue for Service Tickets

In Autotask, you must create a Service Desk queue named OnPlus and add all users (including the creator of the queue) to the OnPlus queue as Resources. This is required so that the OnPlus queue and its tickets appear on the summary page and the navigation tools in Autotask.

IMPORTANT The Autotask Service Desk queue *must* be named OnPlus. If it is not, the integration will not work.

To create a queue in Autotask, follow these steps:

STEP 1 Click the **Admin** icon on the toolbar at the top of the window.

STEP 2 From the Admin menu on the left, choose **Service Desk** > **Queues**.

STEP 3 Click **New** to create a queue.

STEP 4 Name the queue **OnPlus**. The queue must be named OnPlus for the integration to work.

STEP 5 Enter a description, and click **Save**.

Adding an Autotask User

Next, you must add the Autotask user who will be receiving the tickets generated by the OnPlus Portal as a Resource for the OnPlus queue in Autotask. Later, you will associate the same user with the Autotask application configured on the OnPlus Portal.

To add a user as a resource, follow these steps:

STEP 1 Right-click the entry for the OnPlus queue that you just created and choose **Edit Queue Details**.

STEP 2 In the Edit Queue Details dialog box, select the **Resources** tab and click **(+) New** and add the resource.

All service tickets associated with this user's OnPlus Portal account are created using the API and attached to the OnPlus Service Desk queue.

Creating Workflow Rules to Set Ticket Severity Level

In Autotask, you can set the ticket severity level by creating workflow rules using information provided in the Ticket Title or Description fields.

From the Autotask Home page toolbar, select **Help.** From the drop-down list, click **Online Documentation**. In the **Search** textbox, enter Creating and Editing Workflow Rules.

NOTE Ticket Priority categories are fully customizable in Autotask. However, since Autotask does not require a default ticket priority and there is currently an open defect associated with passing ticket priority information through the service integration API, the Cisco OnPlus Portal sets the priority by choosing the Ticket Priority with the highest value.

Modifying the Workflow Policy for Duplicate Ticket Handling

In Autotask, you must also modify the Duplicate Ticket Handling Workflow Policy to only consider a duplicate when the same ticket number is provided.

To access Workflow Policy settings for Duplicate Ticket Handling in Autotask, choose **Admin** > **Service Desk** > **Workflow Policies** and use the [click here to edit] link to the right of the Duplicate Ticket Handling option.

In the **Duplicate Ticket Definition** section of the Duplicate Ticket Handling dialog box, uncheck the **Any ticket with the same alert ID as an existing ticket** setting.

Checking Workflow Policies Settings for Required Fields

If Workflow Policies have been created by your Autotask administrator, you must ensure that additional fields (either standard Autotask fields or custom-created fields) that are marked as required are only required in the application, and not in the web services API. If you do not do this, Autotask service tickets cannot be created through the OnPlus Portal.

To make sure that fields marked as required through Admin Workflow Policies are only required by the application, go to **Admin** > **Service Desk** > **Dashboard** > **Workflow Policies** and verify that any policies for required fields are specified as **Only required in Autotask application**. Here are two examples:

- **Require Issue and Sub-Issue Type fields for service desk tickets** must be set to **Only required in Autotask application**.
- **Require Work Type Name field for service desk tickets** must be set to **Only required in Autotask application**.

Creating a Customer Account in Autotask

Make sure that you have created an account for your customer in Autotask. To create a new account, choose **Directory > Account** and click the **+ New Account** button.

The account name that you enter in Autotask must match the Account Name you enter when adding the Autotask service in the Cisco OnPlus Portal.

Configuring Required API Information to View Discovered Devices

Next, you must configure Autotask with required API information to view discovered devices in the OnPlus Portal Network.

STEP 1 Click the **Admin** icon on the toolbar at the top of the window.

STEP 2 From the Admin menu on the left, choose **Products and Services > Products > Products.**

STEP 3 From the Product Search window, click **+New.**

NOTE The information entered in the fields for Step 4 must be entered exactly as shown.

STEP 4 From the Product window, enter the following information:

- Product Name: OnPlus Discovered Device
- Product Category: Hardware
- Product Description: This product has been discovered by Cisco OnPlus
- Product Code: Select from the drop-down list

Click **Save and Close.**

STEP 5 From the Admin menu, choose **User-Defined Fields.**

STEP 6 From the User-Defined Fields - Products window, click **+New.**

NOTE In Steps 7 through 9, you will be adding three User-Defined Fields. Enter the information exactly as it is presented in these steps.

STEP 7 From the User-Defined Fields window, click **+New** and enter the following information:

- Name*: Device PID
- Description: Device Product ID

- Select Text (Single Line) from the **Field Type** drop-down list, then click **Save & New**.

STEP 8 From the User-Defined Fields window, enter the following information:

- Name*: Device Type
- Select Text (Single Line) from the **Field Type** drop-down list, then click **Save & New**.

STEP 9 From the User-Defined Fields window, enter the following information:

- Name*: MAC Address
- Description: Hardware Address
- Select Text (Single Line) from the **Field Type** drop-down list, then click **Save and Close**.

Viewing the OnPlus Discovered Devices Configuration in Autotask

To view configurations in Autotask, follow these steps:

STEP 1 Log in to Autotask and from the toolbar highlight **Directory** and click **Accounts**.

STEP 2 From the Accounts page, click the Account Name for which you want to view a configuration.

STEP 3 On the Account Summary page, from the Directory Menu, click **Configuration Items** to display the configuration.

NOTE OnPlus discovered devices may take up to three hours to display in the Configuration Items after adding the Autotask App.

Configuring Settings on the Cisco OnPlus Portal

Follow the procedures in this section to configure settings on the Cisco OnPlus Portal to enable integration with Autotask service ticketing:

- **Creating a Delivery Contact for Autotask Ticketing**
- **Adding and Configuring the Autotask Application on the Portal**
- **Creating a Delivery Rule for the Customer on the OnPlus Portal**

Creating a Delivery Contact for Autotask Ticketing

Before you add the Autotask service, you must have a global delivery contact for delivering notifications to Autotask.

- You can use an existing global contact, we recommend that you create a contact to use specifically for Autotask ticketing. The Autotask contact is a global contact that is used for all of your customers that have the Autotask application installed.
- You must create the contact before you add the application and set up notification delivery rules that will use the Autotask contact.

To create a new delivery contact, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page, choose **Notifications > Delivery Contacts**.

For a Partner Account, from the Overview page, choose **Notifications** > **Delivery Contacts**.

STEP 2 Click **+Add Delivery Contact**.

STEP 3 Complete the required fields.

IMPORTANT This applies only to Partner Accounts. When creating a delivery contact for Autotask, make sure that the **Customer** field in the Add Delivery Contact dialog box is set to **None** to make it a global contact.

STEP 4 Click **Save**.

Adding and Configuring the Autotask Application on the Portal

You must add and configure the Autotask application for each customer that you want to be able to generate Autotask Service Desk tickets automatically, based on events and notifications that are generated through the portal.

In this series of steps you will:

- Install the Autotask application to a customer account on the
- Associate the Autotask login credentials of the Resource user for the Autotask OnPlus Queue you just created to the delivery contact you created for Autotask on the portal.
- Enter the unique ID for this customer (Account ID).

To add and configure a customer's Autotask application on the Cisco OnPlus Portal, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page on the portal, choose **Apps.**

For a Partner Account, from the Overview page on the portal, choose a customer for which you want to configure Autotask service desk ticketing, and choose **Apps**.

STEP 2 From the Apps page, click **All**. Locate the **Autotask** application and click **FREE.**

STEP 3 From the **+ Add App** window.

- Specify the Username and Password for the Autotask Resource user associated with the OnPlus Service Queue.
- In the **Associate with a Contact** section, choose the global contact you created for use with the Autotask application.

  IMPORTANT For Partner Accounts, once you set this Global Account Information for one customer, it is used for all your customers that have the Autotask application enabled.

If you have added the Autotask application previously, click the **Make Changes** option to make the fields editable.

STEP 4 Enter the **Account ID** in the field provided, if you know it.

NOTE The Account ID is an internal identifier that is not displayed in the Autotask GUI. You can look up the Account ID by performing a lookup on the Company Name.

STEP 5 If you do not know the Autotask Account ID, click **Lookup**.

STEP 6 In the **Account Name** field, enter the account name exactly as it is specified in Autotask. The name is case-sensitive. The name is used to locate the associated Autotask Account ID that is used by the API.

The **Account Name** field is prepopulated with the Customer Name specified for this customer on the Cisco OnPlus Portal.

The Autotask account name and account ID pairs that match (or start with) the specified Company Name are displayed.

If needed, use the **Lookup** button again to retry the search.

STEP 7 Click the **Add** button at the bottom of the window to apply the configuration.

If the application is added successfully, the Autotask application is moved to the Installed section.

The Autotask user credentials are linked to the contact you specified in **STEP 3** above. An Autotask delivery method is added to the contact's information so that you can enable or disable service ticket generation. When you first associate the contact and add the application, it is enabled.

Creating a Delivery Rule for the Customer on the OnPlus Portal

To begin creating Service Tickets remotely, you must create a notification delivery rule to specify events that will generate an Autotask service ticket and choose the configured Autotask contact as the target for the delivery rule.

Make sure that you have set up device monitors so that events are generated for the type of conditions that you want to use to create service tickets. For example, you may want to monitor and create tickets for Device Offline events or events with a certain severity level.

To create notification rules for Autotask service desk tickets, follow these steps:

STEP 1 Log in to the Cisco OnPlus Portal and choose **Notifications** > **Delivery Rules**.

STEP 2 Click the **+ Add Delivery Rule** button.

STEP 3 For a Partner Account, choose a customer from the drop-down list.

When provisioning a Customer Account, skip Step 3.

STEP 4 You can choose a severity level or specify the type of event that will trigger the creation of an Autotask service ticket.

STEP 5 In the **Contact** field, choose the contact that is associated with the Autotask application. If you need to look up the Contact that is used for Autotask, you can open the Autotask configuration details from the Apps page on the Cisco OnPlus Portal.

STEP 6 Once you choose the Contact, select the Autotask user from the **Method** drop-down list. The Autotask user is identified by the format *<username>* (Autotask) in the list.

If none of the Methods in the list are displayed in this format, it means that you selected the wrong contact.

STEP 7 Click **Save**.

Generating a Test Event, Notification, and Service Ticket

In this procedure, you can:

- Create an example delivery rule.
- Associate that rule with your Autotask delivery contact and method.
- Use the Test Monitor feature to generate an event that matches the criteria for event notifications specified in the delivery rule.
- Verify that the event notification was sent to Autotask.

To generate a test event, notification, and service ticket, follow these steps:

STEP 1 Log in to the Cisco OnPlus Portal, and choose **Notifications** > **Delivery Rules**.

STEP 2 Click the **+ Add Delivery Rule** button.

STEP 3 For a Partner Account, from the **Customer** drop-down list, choose **All** from the drop-down list.

When provisioning a Customer account, skip Step 3.

STEP 4 For the **Severity** level, choose **Warning**.

STEP 5 For the **Contact**, choose the Autotask delivery contact.

STEP 6 For the **Method**, choose the delivery method that you defined for the Autotask delivery contact.

STEP 7 Click **Save**.

STEP 8 From the Overview menu, click one of your Activated, Online customers with the Autotask application installed.

STEP 9 In the Topology view, locate the customer's Cisco OnPlus Network Agent, and open the Device Information window.

STEP 10 In the Device Information window for the Cisco OnPlus Network Agent, click the **Monitors** tab.

The first monitor in the list is the WAN Network Performance monitor.

STEP 11 Click the **Test Monitor** icon to the right of the WAN Network Performance monitor.

STEP 12 Enable the **Generate an event** option.

STEP 13 Click **Run**. The test event will generate a notification because a Warning event is generated by the test (the default severity level of the WAN Network Monitor event is Warning).

STEP 14 After a few minutes, go back to the Overview page and choose **Notifications** > **Delivery Rules**.

STEP 15 Locate the delivery rule that you created for the Autotask test.

- Check the **Notifications Sent** column to see if the count increased.
- Click the number in the **Notifications Sent** column to view event details.
- Verify that the test event appears in the list. Because it was just generated, the test should be near the top of the list. If it is, then the notification was sent to Autotask.

Verifying Service Ticket Creation in Autotask

If the delivery rule and Autotask information are configured correctly for the customer, when the event occurs and the ticket is successfully created, it appears on the Autotask application under **Service Desk > Queues - All Tickets > OnPlus**.

Automated Ticket Resolution (Device Monitor Events Only)

Autotask service desk tickets that are created through notification delivery rules that are based on device monitors are automatically resolved in Autotask when the device monitor generates a subsequent recovery event. This feature applies to all device monitors except IP Change and WAN Network Performance.

For example, if you have created a notification delivery rule that creates a service desk ticket when the device monitor detects that the monitored host is down, a notification is sent to Autotask, and a service desk ticket is created. If the device subsequently comes back up, the Autotask service ticket associated with that event is automatically marked Complete, and the Resolution field displays the device recovery event information.

Suspending Service Ticket Generation for All Customers

To temporarily suspend generation of service tickets through the portal for all customers, follow these steps:

STEP 1 Log on to the Cisco OnPlus Portal, choose **Notifications** > **Delivery Contacts**.

STEP 2 Select the contact associated with Autotask notification delivery.

STEP 3 Click the **Enable** button associated with the Autotask contact to toggle the setting to **Disabled**.

Because the Autotask contact is a global contact for all customers with the application installed, this action suspends Autotask ticketing for all customers with the application.

Updating Global Account Information

To update Autotask Global Account Information (Autotask contact or Autotask username and password), follow these steps:

STEP 1 For a Customer Account, from the Dashboard choose **Apps**.

For a Partner Account, from the Overview page, select a customer that has the Autotask application enabled. From the customer's Dashboard page and choose **Apps**.

STEP 2 Click **Installed** to see the list of installed applications, locate the Autotask application, and click **Edit**.

STEP 3 To change Global Account Information, click the **Make Changes** option to make the fields editable.

STEP 4 Make your changes.

STEP 5 Click **Update**.

The changes are applied to all customers with the Autotask application installed.

Removing the Autotask Application for a Customer

To remove the Autotask application for a specific customer, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page, choose Apps.

For a Partner Account, from the Overview page, select the customer and choose **Apps**.

STEP 2 Click **Installed** for a list of installed applications, locate the Autotask icon and click **Remove**.

STEP 3 Click **OK** to confirm.

Known Issues

The following known issues apply to Autotask integration with the Cisco OnPlus Portal:

- Some changes that can be made using the Autotask GUI (for example, setting a Ticket Priority level as default) cannot be made through the API.

- When querying the account ID using the API with a partial Company Name, if two or more customers match the given string, only one result is returned (instead of the list of matching results). This means that the agent must enter enough characters to ensure a unique match.

16

Integrating ConnectWise Service Ticketing

This section explains how to configure ConnectWise PSA (Professional Service Automation) application settings and Cisco OnPlus Portal settings so that ConnectWise service tickets can be created automatically, based on events that are monitored through the Cisco OnPlus Portal. In addition, this section provides instructions for ConnectWise to display the discovered devices.

These topics are covered:

ConnectWise Version Compatibility

ConnectWise version 2011.2 (10667) has been tested with the Cisco OnPlus Portal. For more information, see www.connectwise.com.

IMPORTANT When setting up ConnectWise integration, if you are using a self-hosted server, your ConnectWise server must have SSL enabled using a signed certificate.

Configuring Settings in ConnectWise

Follow the procedures in this section to configure settings within the ConnectWise application to enable integration with the Cisco OnPlus Portal for service ticketing and to display the discovered devices:

- **Setting Up the Integrator Login in ConnectWise, page 212**
- **Configuring Required API Information to View Discovered Devices, page 213**
- **Setting Up a Company ID in ConnectWise for Each Customer, page 214**
- **Viewing the OnPlus Discovered Devices Configuration in ConnectWise, page 214**

Setting Up the Integrator Login in ConnectWise

ConnectWise PSA administrators can assign permission to integrators. The PSA administrator must set up a master username and password, and enable access to the APIs by an integrator.

Integrators can be allowed access to all objects or just to the objects that they have created themselves.

For ConnectWise, these permissions are set from the Integrator Login setup page in the Setup Tables area.

To allow integrator permissions for Cisco OnPlus, follow these steps:

STEP 1 Log in to ConnectWise and go to **Setup > Setup Tables**.

STEP 2 Filter the list so that it shows the **General** category, then click **Integrator Login**.

STEP 3 Click the **New Item** icon to open the Integrator Login page

STEP 4 Configure the following settings on the Integrator Login page:

- In the **Username and Password** fields, enter the username and password you use to log in to your ConnectWise site.
- Set the **Access Level** to All records.

STEP 5 Under Enable Available APIs, specify these settings:

- Ensure that, at a minimum, the following APIs are enabled:
  - Service Ticket API

- Managed Services API
- Company API
- Product API
- Reporting API
- Configuration API

- Under Service Ticket API, set **Service Board** to Professional Services.
- In the **Ticket Callback URL**, enter https://www.cisco-onplus.com.

STEP 6 Click **Save**.

Configuring Required API Information to View Discovered Devices

To create the OnPlus Discovered Devices setting in ConnectWise, go to **Setup > Setup Tables > Search** and click the **Configuration** table.

STEP 1 From the Configuration Type page, click the **New Item** icon and enter the following text in the **Configuration Type** text box, exactly as shown here:

OnPlus Discovered Device

STEP 2 Click the **Save** icon to save the configuration type and to open a page from which to add items to the configuration type.

NOTE There are four items that must be added to the OnPlus Discovered Device configuration type. These items must be entered exactly as they are presented here. They are MAC Address, Device Type, Device PID, and Serial Number. Repeat Step 3 four times to enter each of these items in the Question field.

STEP 3 Click the **New Item** icon that is located to the left of the Search button and enter the following information:

a. Line Number: (This field is auto-generated)

b. Question: MAC Address

c. Type of field for answer: Text

d. Method of entry: Entry Field

e. Click the **Save** icon.

f. Repeat Step 3 until all four items have been entered in the Question field.

STEP 4 Click the **Go Back** icon to view the list of items you have entered.

Setting Up a Company ID in ConnectWise for Each Customer

To be able to create ConnectWise ticket requests automatically from the OnPlus Portal, you must set up a Company ID in the ConnectWise client for each of your customers on the Cisco OnPlus Portal for which you want to enable this feature.

STEP 1 To create a company in ConnectWise, go to **Contacts > Company** and click the **New Item** icon.

STEP 2 To search for an existing customer, go to **Contacts** > **Company** and click the **Search** button.

Make sure that a Company ID is configured for each of your customers. Refer to the ConnectWise documentation for more information about this setting.

STEP 3 Record the Company ID for each customer, since you must enter it into the ConnectWise service on the Cisco OnPlus Portal.

Viewing the OnPlus Discovered Devices Configuration in ConnectWise

To view configurations in ConnectWise, follow these steps:

STEP 1 Log in to ConnectWise and go to **Contacts > Company** and click **Search.**

STEP 2 From the list of companies, click the Company Name for which you want to view a configuration.

STEP 3 From the company page, click the **Configuration** tab to display the configuration.

NOTE OnPlus discovered devices may take up to three hours to display in the Configuration Items after adding the ConnectWise App.

Configuring Settings on the Cisco OnPlus Portal

Follow the procedures in this section to configure settings on the Cisco OnPlus Portal to enable integration with ConnectWise for service ticketing:

- **Creating a Delivery Contact for ConnectWise Ticketing**
- **Adding and Configuring the ConnectWise Application on the Portal**
- **Creating Workflow Rules to Set Ticket Severity Level**
- **Creating Delivery Rules for ConnectWise Ticketing**

Creating a Delivery Contact for ConnectWise Ticketing

Before you add the ConnectWIse application, you must create a global delivery contact to use for delivering notifications to ConnectWise.

- Although you can use an existing contact, we recommend that you create a contact to use specifically for ConnectWise ticketing. The ConnectWise contact is a global contact that is used for all of your customers that have the ConnectWise application installed.
- You should always create the global contact before you add the application and create notification delivery rules that use the contact.

To create a new global delivery contact, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page, choose **Notifications > Delivery Contacts**.

For a Partner Account, from the Overview page, choose **Notifications** > **Delivery Contacts**.

STEP 2 Click **Add Delivery Contact**.

STEP 3 Complete the required fields.

IMPORTANT This applies only to Partner Accounts. When creating a delivery contact for Autotask, make sure that the **Customer** field in the Add Delivery Contact dialog box is set to **None** to make it a global contact.

STEP 4 Click **Save**.

Adding and Configuring the ConnectWise Application on the Portal

To add and configure ConnectWise integration for a customer, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page on the portal, choose **Apps.**

For a Partner Account, from the Overview page on the portal, choose a customer for which you want to configure ConnectWise service desk ticketing, and choose **Apps.**

STEP 2 From the Apps page, click **All.** Locate the **ConnectWise** application and click **FREE.**

STEP 3 From the **+ Add App** window, in the **Global Account Information** section, enter the following information:

NOTE If you have added the ConnectWise application previously, check the **Make Changes** option to make the fields editable.

- **Site ID**: ConnectWise Site ID (for example, test.connectwise.com). This URL is provided by ConnectWise.
- **Corporate ID**: ConnectWise account login (the value that you enter in the Company ID field when you log in to ConnectWise)
- **Username, Password**: ConnectWise username and password

  This is the same username and password you configured for the Integrator Login within ConnectWise. These are the credentials you use when logging in to your ConnectWise site.
- In the **Associate with a Contact** area, choose a contact to associate with the ConnectWise application on the portal.

Once you have set the **Global Account Information** for one customer for Partner Accounts, it is used for all customers that have the ConnectWise application enabled.

STEP 4 In the **Company ID** field, enter the ConnectWise company ID that you configured in ConnectWise (**Contacts > Company**).

STEP 5 Click **Add**.

If the application is added successfully, the ConnectWise application appears on the list of **Installed** applications.

The ConnectWise user credentials are linked to the contact that you specified in the Add App dialog box.

A ConnectWise delivery method is added to the contact's information so that you can enable or disable service ticket generation. When you first associate the contact and add the application, it is enabled.

Creating Workflow Rules to Set Ticket Severity Level

In ConnectWise, you can set the ticket severity level by creating workflow rules using information provided in the Ticket Title or Description.

From the ConnectWise Home page, click **Help**. From the ConnectWise University home page, enter Workflow Rules Setup Table in the Search window and click **Search**.

Creating Delivery Rules for ConnectWise Ticketing

To begin creating Service Tickets remotely, you must create a notification delivery rule to specify events that will generate a ConnectWise service ticket and choose the configured ConnectWise contact as the target for the delivery rule.

Make sure that you have set up device monitors so that events are generated for the type of conditions that you want to use to create service tickets. By default, only the Cisco OnPlus Network Agent is monitored. For example, you may want to monitor and create tickets for Device Offline events or events of a specific severity level.

To create notification rules for creating ConnectWise service tickets, follow these steps:

STEP 1 Log in to the Cisco OnPlus Portal, and choose **Notifications** > **Delivery Rules**.

STEP 2 Click the **+ Add Delivery Rule** button.

STEP 3 For a Partner Account, choose a customer from the drop-down list.

Note: There is no Customer field for a Customer Account.

STEP 4 Choose a severity level or specify the type of event that will trigger the creation of an ConnectWise service ticket.

STEP 5 In the **Contact** field, choose the contact that is associated with the ConnectWise application. If you need to look up the Contact that is used for ConnectWise, you can open the ConnectWise configuration details from the Apps page on the portal.

STEP 6 Once you choose the Contact, select the ConnectWise user from the **Method** drop-down list. The ConnectWise user is identified by the format <*username*> (ConnectWise) in the list.

If none of the Methods in the list display this information, it means that you selected a contact that is not associated with the ConnectWise user.

STEP 7 Click **Save**.

Generating a Test Event, Notification, and Service Ticket

This procedure enables you to:

- Create an example delivery rule.
- Associate that rule with your ConnectWise delivery contact and method.
- Use the Test Monitor feature to generate an event that matches the criteria for event notifications specified in the delivery rule.
- Verify that the event notification was sent to ConnectWise.

To generate a test event, notification, and service ticket, follow these steps:

STEP 1 Log in to the Cisco OnPlus Portal, and choose **Notifications** > **Delivery Rules**.

STEP 2 Click the **+ Add Delivery Rule** button.

STEP 3 For a Partner Account, from the **Customer** drop-down list, choose **All** from the drop-down list.

Note: There is no Customer field for a Customer Account.

STEP 4 For the **Severity** level, choose **Warning**.

STEP 5 For the **Contact**, choose the ConnectWise delivery contact.

STEP 6 For the **Method**, choose the delivery method that you defined for the ConnectWise delivery contact.

STEP 7 Click **Save**.

STEP 8 From the Overview menu, click one of your Activated, Online customers with the ConnectWise application installed.

STEP 9 In the Topology view, locate the customer's Cisco OnPlus Network Agent, and open the Device Information window.

STEP 10 In the Device Information window for the Cisco OnPlus Network Agent, click the **Monitors** tab.

The first monitor in the list is the WAN Network Performance monitor.

STEP 11 Click the **Test Monitor** icon to the right of the WAN Network Performance monitor.

STEP 12 Enable the **Generate an event** option.

STEP 13 Click **Run**. The test event will generate a notification because a Warning event is generated by the test (the default severity level of the WAN Network Monitor event is Warning).

STEP 14 After a few minutes, go back to the Overview page and choose **Notifications** > **Delivery Rules**.

STEP 15 Locate the delivery rule you created for the ConnectWise test.

- Check the **Notifications Sent** column to see if the count increased as expected.
- Click the number in the **Notifications Sent** column to view event details.
- Verify that the test event appears in the event list. Because it was just generated, the test should be near the top of the list. If it is, then the notification was sent to ConnectWise.

Verifying Service Ticket Creation in ConnectWise

If the delivery rule and ConnectWise information are configured correctly for the customer, when the event occurs and the ticket is successfully created, it appears on the ConnectWise application under **Service Desk** > **Service Board**.

Automated Ticket Resolution (Device Monitor Events Only)

ConnectWise service desk tickets that are created through notification delivery rules that are based on device monitors are automatically resolved in ConnectWise when the device monitor generates a subsequent recovery event. This feature applies to all device monitors except IP Change and WAN Network Performance.

For example, if you have created a notification delivery rule that creates a service desk ticket when the device monitor detects that the monitored host is down, a notification is sent to ConnectWise and a service desk ticket is created. If the device subsequently comes back up, the ConnectWise service ticket associated with that event is automatically marked Complete, and the Resolution field displays the device recovery event information.

Suspending Service Ticket Generation for All Customers

To temporarily suspend generation of service tickets through the portal for all customers, follow these steps:

STEP 1 Log on to the Cisco OnPlus Portal and choose **Notifications > Delivery Contacts.**

STEP 2 Select the contact associated with ConnectWise notification delivery.

STEP 3 Click the **Enable** button associated with the ConnectWise contact to toggle the setting to **Disabled**.

Because the ConnectWise contact is a global contact for all customers with the application installed, ConnectWise ticketing is suspended for all customers with the application.

Updating Global Account Information

To update ConnectWise Global Account Information, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page, choose Apps.

For a Partner Account, from the Overview page, select a customer that has the ConnectWise application enabled and choose **Apps**.

STEP 2 Click **Installed** for a list of installed applications, locate the ConnectWise application and click **Edit**.

STEP 3 To modify Global Account Information, click the **Make Changes** option to make the fields editable.

STEP 4 Make your changes.

STEP 5 Click **Update**. The changes are applied to all customers with the ConnectWise application installed.

Removing the ConnectWise Application for a Customer

To remove the ConnectWise application for a specific customer, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page, choose **Apps**.

For a Partner Account, from the Overview page, select the customer and choose **Apps**.

STEP 2 Click **Installed** for a list of installed applications, locate the ConnectWise application, and click **Remove**.

STEP 3 Click **OK** to confirm.

17

Enabling ntop Packet Monitoring

This section provides instructions for enabling the ntop Packet Monitoring application on the Cisco OnPlus Portal and setting up packet monitoring using either NetFlow or port spanning with output sent to the Cisco OnPlus Network Agent MON port.

NOTE ntop is currently a Beta feature.

These topics are covered:

Overview

ntop is a network traffic probe that shows network usage. For more information, visit www.ntop.org.

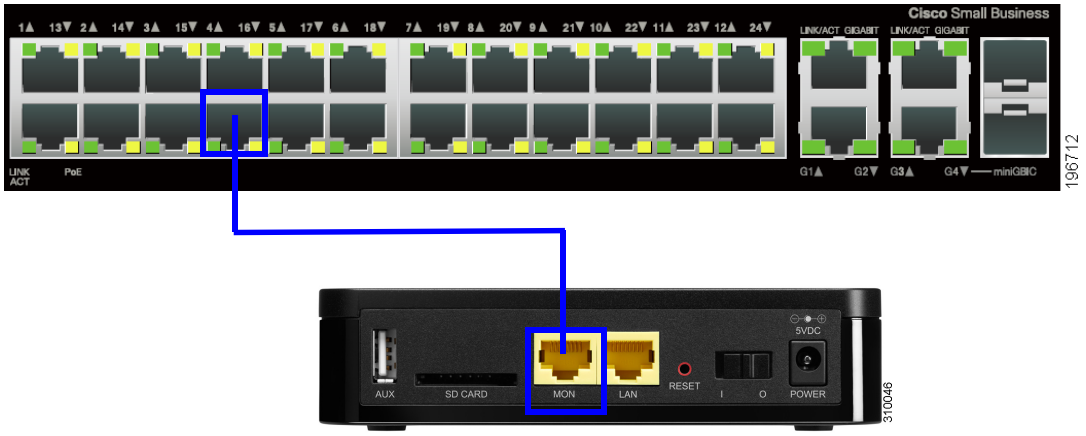
The ntop application is downloaded to the Cisco OnPlus Network Agent and accessed from the portal. You do not need to download the ntop application software.

Two methods are supported for collecting network information to use with ntop:

- **Span**. Using the Cisco OnPlus Network Agent MON port for input, you can use ntop to sniff the traffic you are interested in. When the span traffic is monitored, you must provide the source for the network traffic to be examined. Some switches and routers have the ability to span traffic to a specific port. If you have a network tap or a simple network hub, you can use it to tap the network where you want to look at the traffic.

Refer to the documentation for the device you are using for instructions on how to set up port spanning.

The following diagram shows the connection between a span port on a Cisco Small Business 300 Series Switch and the MON port on the back of the Cisco OnPlus Network Agent.



- **NetFlow (IPFIX)**. Most Cisco IOS routers support the NetFlow protocol. In that case, you can simply enable the protocol in the router and point it at the Cisco OnPlus Network Agent. The NetFlow protocol uses less CPU resources on the Cisco OnPlus Network Agent and does not require you to use the MON port.

  When using NetFlow, we recommend that you assign a static IP address or static DHCP lease to the Cisco OnPlus Network Agent, since the NetFlow configuration uses the IP address of the Cisco OnPlus Network Agent. Also, NetFlow must be activated in ntop, and the port number that it listens on must match the NetFlow configuration on the Cisco IOS router.

  See **Using ntop With NetFlow, page 226**.

Notes, Limitations, and Caveats

These notes, limitations, and caveats apply to using the ntop application with the Cisco OnPlus Network Agent:

- Export of data or writing of data to disk on the Cisco OnPlus Network Agent is not supported.

- A static IP address is recommended for the Cisco OnPlus Network Agent when using NetFlow.
- Cisco OnPlus Portal sets the initial ntop administration username and password to **admin/admin**.
- Some configuration changes in the ntop application (for example, changes to settings that configure reachability) can cause the ntop application to stop functioning or not function correctly.
- If you encounter problems when using the ntop application with the OnPlus Portal, you can try removing the service, then re-adding and enabling it.
- After you remove and re-add the ntop application or after a newer version of ntop is installed on the Cisco OnPlus Network Agent by the OnPlus Portal:
  - All historical data is lost.
  - Any custom configuration of the ntop application is lost.
  - The password is reset to the default (admin/admin).
- The ntop application is automatically restarted when the Cisco OnPlus Network Agent is restarted.
- When you use the **Admin** > **Shutdown** option in the web-based ntop administration tool, ntop is automatically restarted. Remove the ntop service through the OnPlus Portal if you do not want the application to run.

Adding the ntop Application on the Cisco OnPlus Portal

Follow the procedures in this section to configure settings on the Cisco OnPlus Portal to enable the ntop Packet Monitoring App:

- **Installing the ntop Packet Monitoring Application on the Cisco OnPlus Network Agent**
- **Launching the ntop Packet Monitoring Application**

Installing the ntop Packet Monitoring Application on the Cisco OnPlus Network Agent

You must add and configure the ntop application for each customer.

To add and enable ntop packet monitoring for a customer, follow these steps:

STEP 1 From the Overview page on the portal, choose a customer for which you want to enable ntop Packet Monitoring, and choose **Apps.**

STEP 2 Click **All** to locate the **ntop Packet Monitoring** application and click **FREE.**

Launching the ntop Packet Monitoring Application

To launch ntop, follow these steps:

STEP 1 For a Customer Account, from the Dashboard, choose **Apps.**

For a Partner Account, from the Overview page on the portal, choose the customer for which ntop Packet Monitoring was installed. From the customer's Dashboard page, choose **Apps**.

STEP 2 Click **Installed**.

STEP 3 Under **Installed** applications, locate the **ntop Packet Monitoring** application and click **Details**.

If you have just installed the app, you may see a message indicating that the option to launch the ntop portal is not available yet. Close the dialog box and check again in a few minutes.

When the ntop installation finishes, the **Launch ntop Portal** button becomes available.

STEP 4 To open the ntop portal in a new window, click **Launch ntop Portal**.

The network feed that you want to use for the traffic source must be connected (span port) or configured (NetFlow) before useful data can be collected.

If you are using NetFlow, see **Using ntop With NetFlow** for additional configuration steps.

Using ntop With NetFlow

To use ntop with NetFlow configured on a Cisco IOS router, follow the procedures in the following sections:

- **Configuring NetFlow on the Cisco IOS Device**

- Configuring ntop Settings

Configuring NetFlow on the Cisco IOS Device

NetFlow mode uses the Cisco OnPlus Network Agent WAN port with a Cisco router configured to direct NetFlow traffic to the IP address of the Cisco OnPlus Network Agent.

The following sequence of Cisco IOS commands can be used as a model for configuring NetFlow. In the example, the ip flow-export destination IP address is the IP address of the Cisco OnPlus Network Agent.

The 2055 in the ip flow-export destination command example corresponds to the Local Collector UDP Port number configured for the NetFlow plugin. The flow export source interface will vary depending on the interface providing the source traffic.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip route-cache flow
router-2621(config-if)#exit
router-2621(config)#ip flow-export destination <OnPlus_Network
Agent_IP_Address> 2055
router-2621(config)#ip flow-export source FastEthernet 0/1
router-2621(config)#ip flow-export version 5
router-2621(config)#ip flow-cache timeout active 1
router-2621(config)#ip flow-cache timeout inactive 15
router-2621(config)#snmp-server ifindex persist
router-2621(config)#^Z
router#write
```

Configuring ntop Settings

If you are using NetFlow, you must perform the following additional configuration steps using the ntop application:

STEP 1 Open the ntop application from the OnPlus Portal:

a. Log in to the Cisco OnPlus Portal and select your customer.

b. Choose **Apps**.

c. Click **Installed** and locate the ntop Packet Monitoring application.

d. Click **Details**.

e. Click **Launch ntop Portal**.

STEP 2 When prompted to authenticate, enter the default administrative username and password.

Username: **admin**
Password: **admin**

NOTE When ntop is installed or upgraded on the Cisco OnPlus Network Agent, the password is always reset to the default.

STEP 3 Activate the NetFlow plugin. To do this, choose **Plugins** > **NetFlow** > **Activate**.

STEP 4 Create a NetFlow device. In the ntop application, choose **Plugins** > **NetFlow** > **Configure** and click **Add NetFlow Device**.

STEP 5 Configure these settings for the NetFlow device:

- **NetFlow Device**. This setting is optional, but useful. Enter a name for the interface and click **Set Device Interface Name**.
- **Local Collector UDP Port**. Enter a port number and click **Set Port**. This port number should correspond to the Port configured for the ip flow-export destination IP_address Port command configured on the router or switch.

STEP 6 In order to see NetFlow content, the NetFlow device must be selected under **Admin** > **Switch NIC**.

If you do not perform this step, you may be examining traffic on the default eth1 port instead of the NetFlow port configured on the Cisco IOS device.

Removing the ntop Packet Monitoring Application

To remove the ntop Packet Monitoring application for a specific customer, follow these steps:

STEP 1 For a Customer Account, from the Dashboard page, choose **Apps**.

STEP 2 For a Partner Account, from the Overview page, select the customer and choose **Apps**.

STEP 3 In the list of installed applications, locate the ntop Packet Monitoring icon and click **Remove**.

STEP 4 Click **OK** to confirm.

When you remove the application, all historical data and custom ntop configuration is lost, and the password is reset to the default (admin/admin).

18

Mobile Device Access to the OnPlus Portal

This chapter provides instructions for accessing the Cisco OnPlus Portal from mobile devices for all users:

Specifically for Cisco OnPlus Partners:

Accessing the OnPlus Portal from a Mobile Device

You can access the OnPlus mobile portal from a web browser running on a mobile device. The web browser on the mobile device must support JavaScript and CSS. Mobile access has been tested with the Safari browser running on iPhone, Android phone and tablet, and Blackberry (RIM) smartphones and the iPad.

To access the OnPlus Portal from a mobile device, follow these steps:

STEP 1 Open a web browser on your mobile device.

STEP 2 Navigate to the portal URL (www.cisco-onplus.com). You are redirected automatically to the mobile portal URL (https://www.cisco-onplus.com/m).

STEP 3 Enter your Cisco.com username and password, and click **Log In**.

If you are a Cisco OnPlus Partner, you can choose a customer or one of your delivery contacts. When you choose a customer, you can view their dashboard or device listing and access details for each device.

To refresh the data for a Cisco OnPlus mobile portal page, refresh the page in the web browser on the mobile device.

To locate options for establishing a remote connection to a device, choose **Device Listing**, then select the device. Types of connections that you can make to the device are listed under **Establish Connection**.

STEP 4 To log out, scroll to the bottom of any mobile portal page and click the **Logout** link.

You can always click the Non-Mobile Site link at the bottom of the page to log in to the portal using the regular web interface.

OnPlus Portal Features Accessible through Mobile Interface

Features Available to all Customers

The mobile interface to the Cisco OnPlus Portal provides access to many of the important portal functions for monitoring and accessing your network. From supported mobile devices, you can:

- Use the touch screen controls to pan and zoom the Topology view or select devices.
- Select devices to view information or perform actions. Available actions vary, depending on the type of device.
  - Establish a web, remote desktop, or VNC connection to a customer device.

    NOTE Before attempting to connect to devices remotely using the mobile portal, you must configure your connection settings on the remote device and the portal on the Connect tab in the Device Information window on the portal. See **Connecting to Devices from the Portal, page 137**.
  - Restart devices.
  - Back up configuration for supported Cisco devices.
- View the global event history and filter it by severity.
- See the last 10 events recorded for any device.

Features Specific to Cisco OnPlus Partners

- View a list of all your customers.
- Select a customer to view their network topology or see a list of devices on the network.
- Activate the customer's Cisco OnPlus Network Agent using the portal. You can only do this if the mobile device is on the same local area network (LAN) as the Cisco OnPlus Network Agent that you are activating.

  See **Activating a Customer from a Mobile Device, page 234**.
- View delivery contacts.

  Click a delivery contact's email or SMS email address to send a message.
- View customer address and location information.

  If you are accessing the mobile portal from an Apple iPhone and have the Google maps application installed, the address is automatically displayed in the Google maps application.

  - On an Google Android phone, you can choose between displaying the map in the Google maps phone application or in your web browser.
  - On a Blackberry smartphone, the location information opens in a Web browser.

Features Not Supported using the Mobile Interface

Cisco OnPlus Portal features that are not supported using the mobile interface include the following:

- Adding, deleting, suspending, or resuming customers
- Using the OnPlus Scanner to scan your network
- Upgrading firmware on devices other than the Cisco OnPlus Network Agent
- Customizing portal pages
- Adding, editing, or removing device access credentials
- Configuring remote connection settings for devices
- Adding, deleting, or modifying device monitors

- Managing Authorized Agents
- Generating, scheduling, or viewing reports
- Editing, deleting, enabling, and disabling delivery contacts
- Viewing or managing notification delivery rules
- Configuring PSA integration Applications (Autotask, ConnectWise) with the OnPlus Portal

Activating a Customer from a Mobile Device

If you are a Cisco OnPlus Partner and your mobile device has a web browser that is connected to the same local area network (LAN) or wireless LAN (WLAN) as the Cisco OnPlus Network Agent, you can use the mobile interface to access the **Activate Now** link on the portal and activate the Cisco OnPlus Network Agent.

STEP 1 Make sure that you have completed all of the steps prior to the Activation step. See **Before You Begin, page 21**.

STEP 2 On the mobile device connected to the same LAN as the Cisco OnPlus Network Agent, log in to the mobile portal.

STEP 3 Select the customer that you want to activate.

STEP 4 Click the **Profile** link to access that customer's profile and activation information.

STEP 5 Scroll to the **Cisco OnPlus Network Agent** section of the page.

STEP 6 Choose **Activate Now** and follow the on-screen instructions.

If you experience problems using the mobile interface to activate the customer, you can always connect to the portal using a web browser on a computer connected to the customer LAN or WLAN and perform the activation as you normally would.

Cisco OnPlus Mobile Application

You can also access the OnPlus Portal from a smartphone or tablet through the OnPlus Portal Mobile Application. Here are just a few of the portal features that are available in the OnPlus Mobile App:

- Customer Overview
- Customer Dashboard
- Customer Inventory, Topology, and Device Listing
- Device Details
- Remote web connection to customer devices

Supported devices include:

- Google Android phone (Android OS version 2.2 and later; 3.0 is not supported)
- Google Android tablet (Android OS version 10.1 and later)
- Apple iPhone 3GS, 4G, 4S, and iPOD Touch (Cisco IOS 4.2 and later)
- Apple iPad and Google Android tablets running the OS versions listed above

Active Cisco OnPlus Customers and Partners can obtain the OnPlus Mobile Application by:

- Searching for “onplus” on the Android Marketplace
- Searching for “onplus” in the Apple iTunes store

For more information about the Cisco OnPlus Mobile Application, visit the Cisco Support Community for the article **Now Available - OnPlus Mobile App** and the **Getting Started Guide**.

19

Feedback and Support

This chapter describes how to access the Cisco OnPlus support community and how to submit feedback for the Cisco OnPlus Portal:

- **Support Community for Cisco OnPlus**
- **Support Access to Cisco OnPlus Network Agent Logs and Customer Sites**
- **Checking OnPlus Service Health Status**
- **Providing Feedback on Cisco OnPlus**

Support Community for Cisco OnPlus

From within the OnPlus Portal, Cisco Partners can access Cisco.com support resources and the OnPlus support community area.

Click the **Support** link at the top of the OnPlus Portal to access the support community. The Cisco.com login page is displayed in the portal.

After you log in to Cisco.com, you are redirected to the OnPlus area of the Cisco Support Community.

Support Access to Cisco OnPlus Network Agent Logs and Customer Sites

Cisco Small Business Support Center (SBSC) agents can collect application logs and runtime output from the Cisco OnPlus Network Agent device. This data is only collected with user approval during active support calls. The collected data is sent to Cisco support personnel as noted during the call. Access to this data is password-protected for Cisco support use only. Cisco support staff must have your explicit authorization to use this feature.

The Cisco Support Tools login is accessed from the Dashboard toolbar.

Click the **Toolbox** icon  , then select the Cisco Support category.

If a tunnel connection to a remote device through the portal is required for Support purposes, the support agent must:

- Ask for permission to share remote desktop during the support call.
- Ask you to create the tunnel connection during the support call.

Checking OnPlus Service Health Status

To check the status of the Cisco OnPlus Service, go to:

www.checkonplus.com

Service health status communications and updates are posted to this page. If you are experiencing problems with the Cisco OnPlus Portal, visit this page to determine if the issue is related to a known service outage.

Providing Feedback on Cisco OnPlus

Use the Cisco OnPlus area of the Cisco Small Business Support to ask questions, initiate discussions, and post comments and suggestions for the Cisco OnPlus Portal. Visit us at https://supportforums.cisco.com/community/netpro/small-business/onplus.

You can also send us comments and suggestions. Click the **Feedback** link at the bottom right of any portal page, choose a category, enter your comments, and click **Send**.

A

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco OnPlus Service.

Community	
Cisco Support Community for the OnPlus Service	https://supportforums.cisco.com/community/netpro/small-business/onplus
OnPlus Training Library videos and podcasts	https://supportforums.cisco.com/docs/DOC-17701
Device Compatibility Matrix	https://supportforums.cisco.com/docs/DOC-17501
Cisco Software Downloads	
Cisco Software Download Center	Downloads for products are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
OnPlus Portal and Documentation	
All Cisco OnPlus Technical Documentation	www.cisco.com/go/onplus
OnPlus Documentation	https://supportforums.cisco.com/docs/DOC-17447
For Partners	
Cisco OnPlus Portal Partner Account Sign-up and Login	www.cisco-onplus.com

A

B

Cisco Device Feature Support

This appendix lists Cisco devices supported by the OnPlus Portal, along with the portal features supported for each device, and any limitations or constraints that apply.

- Device Feature Summary
- Device-Specific Limitations for OnPlus Features
- Remote Access using Generic Tunnel Connection

Device Feature Summary

TIP To view device-specific notes, caveats, and limitations, click the link in the Cisco Device/Model column.

Cisco Device / Model	Device Type	Product Icon	Backup / Restore	F/W Upgrade	Remote Access
AP521	Access Point	Yes	Yes	Yes	Yes
AP541	Access Point	Yes	Yes	Yes	Yes
AP801	Access Point	Yes	Yes	Yes	Yes[1]
AIR-AP1142	Access Point	Yes	Yes	Yes	Yes
WAP121/WAP321	Access Point	Yes	Yes	Yes	Yes
WAP121/WAP321	Access Point	Yes	Yes	Yes	Yes
WAP4410N	IP Camera	Yes	Yes	Yes	Yes
PVC300	IP Camera	Yes			Yes
VC220	IP Camera	Yes			Yes
VC240	IP Camera	Yes			Yes

Cisco Device / Model	Device Type	Product Icon	Backup / Restore	F/W Upgrade	Remote Access
SPA300, SPA500 Series IP Phones	IP Phone	Yes			Yes
Cisco 6900, 7900, 8900, 9900 Series IP Phones	IP Phone	Yes			Yes
NSS300	Storage	Yes	Yes	Yes	Yes
Cisco Integrated Services Router Cisco 870, 1800, 2800 Series ISRs	Router	Yes	Yes	Yes	Yes1.
Cisco BE3000	Router	Yes			Yes1.
Cisco 800 Series ISRsCisco 1800 Series ISRs	Router	Yes	Yes	Yes	Yes1.
IAD2400	Router	Yes	Yes	Yes	Yes
Cisco Integrated Services Router G2 Cisco 866/867VAE, 880, 890, 1900, 2900, 3900 Series ISRs	Router	Yes	Yes	Yes	Yes
RV042/RV082/ RV016 V3	Router	Yes	Yes	Yes	Yes
RV042/RV082/ RV016 V3	Router	Yes	Yes	Yes	Yes
SRP500	Router	Yes	Yes	Yes	Yes
ASA5505	Security Appliance	Yes	Yes	Yes	Yes
SA520	Security Appliance	Yes	Yes	Yes	Yes
NSS300	Storage	Yes	Yes	Yes	Yes
IESW 500 Series	Switch	Yes	Yes	Yes	Yes
SG300 or SF300 (v1.0 Firmware)	Switch	Yes	Yes* (requires SNMP community string)	Yes* (requires SNMP community string)	Yes
SF300 or SG300 (v1.1 Firmware)	Switch	Yes	Yes	Yes	Yes

Cisco Device / Model	Device Type	Product Icon	Backup / Restore	F/W Upgrade	Remote Access
SF500 or SG500	Switch	Yes	Yes	Yes	Yes
WS-C2960	Switch	Yes	Yes	Yes	Yes
Cisco Catalyst 2960, 2960-C, 2960-G, 2960-S, 3750	Switch	Yes	Yes (2960-C/2960-S/3750) No (2960/2960-G)	Yes(2960-C/2960-S/3750) No(2960/2960-G)	Yes1.
Cisco Catalyst 3560, 3560-C, 3560-E, 3560-G, 3560-X, 3560v2	Switch	Yes	Yes No (3560/3560-G)	Yes No (3560/3560-G)	Yes
UC320	Voice System	Yes	Yes	Yes	Yes
SRP500	Voice System	Yes			Yes

1. The normal web connection method is not compatible with CP Express. Use SSH, Telnet, or HTTP through a Generic Tunnel Connection. See Remote Access using Generic Tunnel Connection, page 277.

Device-Specific Limitations for OnPlus Features

Refer to the following sections for important information about limitations and caveats that apply to Cisco OnPlus Portal device feature support:

- AP521
- AP541
- AP801
- AIR-AP1142
- WAP121/WAP321
- WAP121/WAP321
- WAP4410N
- PVC300
- VC220
- VC240
- SPA300, SPA500 Series IP Phones

- Cisco 6900, 7900, 8900, 9900 Series IP Phones
- NSS300
- Cisco Integrated Services Router
- Cisco BE3000
- Cisco 1800 Series ISRs
- IAD2400
- Cisco Integrated Services Router G2
- RV042/RV082/RV016 V3
- RV042/RV082/RV016 V3
- SRP500
- ASA5505
- SA520
- IESW 500 Series
- SG300 or SF300 (v1.0 Firmware)
- SF300 or SG300 (v1.1 Firmware)
- SF500 or SG500
- WS-C2960
- Cisco Catalyst 2960, 2960-C, 2960-G, 2960-S, 3750
- Cisco Catalyst 3560, 3560-C, 3560-E, 3560-G, 3560-X, 3560v2
- UC320
- SRP500

ASA5505

Feature	Constraints/Notes
Discovery	The ASA5505 Series routers do not support CDP, Bonjour, UPnP, or any other supported discovery protocols. Its MAC and IP addresses will be discovered, but it will show up in the Topology as an Unknown Device. In order to properly interface with the device, you must assign a device driver, at which point discovery can proceed. (Device Information > Credentials tab, Device Driver). The command interface to the ASA5505 uses the HTTP interface, which must be enabled on the VLAN that the OnPlus Agent is attached to. The discovery process uses the ARP table on the VLAN that the OnPlus Agent is attached to in order to discover attached devices. Devices that are attached to other VLANs are not discovered. The ASA has no defined WAN port; the canonical configuration creates a VLAN that is used for WAN access and attaches it to one or more switch ports. The remaining ports will normally be attached to another VLAN defined for the LAN side. The OnPlus Agent must be connected to the LAN VLAN.
Firmware Upgrade	ASA5505 Series routers have two significant firmware packages resident on their drive: a system software load and a device manager load. The OnPlus Portal Firmware Upgrade feature supports both of those, with the following constraints: ▪ The only files that will be accepted for upgrade are files that match the two wildcard names: asa*.bin and adsm*.bin. ▪ If a firmware file matches asa*.bin, it is assumed to be a system software load. ▪ If a firmware file matches adsm*.bin, it is assumed to be a device manager load. ▪ System software will not be upgraded if a 'boot image' command is present in the startup-config, since it is likely that the administrator of the router would not want this overridden. ▪ Device manager software will not be upgraded if an 'adsm image' command is present in the startup-config. ▪ Neither package will be upgraded if there is insufficient room on the boot drive to store the upgraded file during the upgrade. ▪ An update of either type of firmware causes a device reboot. ▪ When either type of firmware is updated, the file it replaces will be deleted.

Feature	Constraints/Notes
Remote Access	The ASA5505 device manager can not be run over a tunnel created by the Cisco OnPlus Agent device. Remote ASA management can be performed if SSH access is enabled and a Generic Tunnel connection for SSH is created by the Cisco OnPlus Agent for command line administration. See **Remote Access using Generic Tunnel Connection, page 277**.

UC320

Feature	Constraints/Notes
Discovery	The OnPlus Portal discovery process will log in to the device to probe for network information. To prevent admin users from being forced out of the UC320 admin GUI during discovery, deselect the **Allow login access** option on the Credentials tab in the Device Information window.
Device Configuration Backup/Restore	The backup of a UC300 Series router/voice system consists of retrieving a binary that is a mix of files and settings from the UC300. ▪ Backup and restore operations via the portal require device access credentials for the UC300. ▪ Restoring the configuration requires use of the management GUI on the UC300. ▪ Backup of voice mail and other audio files cannot be accomplished through the portal. This must be set up using the UC300 management GUI through the backup to USB option and daily maintenance window. Restore is a lengthy process. It requires 2 reboots of the device (at 2.5 - 3 minutes per reboot). The device must be rebooted before launching the UC300 management GUI and after the configuration is applied. Other Topology functions are unavailable while this GUI is open.
Firmware Upgrade	Firmware upgrade requires the use of the UC300 management GUI. When a firmware upgrade is requested, a popup dialog box opens that guides the user through the upgrade process. Other Topology functions are unavailable while this dialog box is open.

Cisco Integrated Services Router G2

Cisco 866/867VAE, 880, 890, 1900, 2900, 3900 Series ISR

Cisco 800 Series ISRs

Feature	Constraints/Notes
Discovery	Cisco 800 Series ISRs must have CDP enabled in order to be discovered by the OnPlus Agent device. If you use Cisco CP or Cisco CP Express to configure your router, it is very likely that CDP is disabled, since this is the recommended configuration. If CDP is disabled, the 800 Series router will show up in the Topology as an Unknown Device. Open the Device Information window for the device, select the Credentials tab, click Device Driver, and select the Cisco 800 Series. If CDP is enabled, the device will be discovered properly.

Feature	Constraints/Notes
Access/Device Information	If device access credentials are not provided, the device's MAC address, and IP address are displayed. If the 800 Series ISR has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, additional device information will be displayed, and the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of an 800 Series ISR consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the device is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	If the ISR800 administrator has defined a boot load with the boot system command, firmware upgrades are not performed.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

Cisco 1900 Series ISRs

Feature	Constraints/Notes
Discovery	The Cisco 1900 Series ISRs must have CDP enabled in order to be discovered by the OnPlus Agent device. In addition, the Cisco 1900 Series ISR must be connected to a switch that will provide CDP neighbor information to the OnPlus Agent, as the OnPlus Agent will not generally be connected directly to the ISR. If you use Cisco CP or Cisco CP Express to configure the router, it is very likely that CDP is disabled, since this is the recommended configuration. If CDP is disabled, the 1900 Series router will show up in the Topology as an Unknown Device. Open the Device Information window for the device, select the Credentials tab, click Device Driver, and select the Cisco 1900 Series. If CDP is enabled, the device will be discovered properly.

Feature	Constraints/Notes
Device Configuration Backup and Restore	The backup of an 1900 Series ISR consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the ASA is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	If the administrator of the 1900 Series router has defined a specific boot load with the boot system command, firmware updates are not performed.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**. For HTTP access, open a Generic Tunnel connection on port 80.

Cisco 2900 Series ISRs

Feature	Constraints/Notes
Discovery	The Cisco 2900 Series ISRs must have CDP enabled in order to be discovered by the OnPlus Agent device. In addition, the Cisco 2900 Series ISR must be connected to a switch that will provide CDP neighbor information to the OnPlus Agent, as the OnPlus Agent will not generally be connected directly to the ISR. If you use Cisco CP or Cisco CP Express to configure the router, it is very likely that CDP is disabled, since this is the recommended configuration. If CDP is disabled, the 2900 Series router will show up in the Topology as an Unknown Device. Open the Device Information window for the device, select the Credentials tab, click Device Driver, and select the Cisco 2900 Series. If CDP is enabled, the device will be discovered properly.
Device Configuration Backup and Restore	The backup of a 2900 Series ISR consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the ASA is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	If the administrator of the 2900 Series router has defined a specific boot load with the boot system command, firmware updates are not performed.

Feature	Constraints/Notes
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**. For HTTP access, open a Generic Tunnel connection on port 80.

Cisco 3900 Series ISRs

Feature	Constraints/Notes
Discovery	The Cisco 3900 Series ISRs must have CDP enabled in order to be discovered by the OnPlus Agent device. In addition, the Cisco 3900 Series ISR must be connected to a switch that will provide CDP neighbor information to the OnPlus Agent, as the OnPlus Agent will not generally be connected directly to the ISR. If you use Cisco CP or Cisco CP Express to configure the router, it is very likely that CDP is disabled, since this is the recommended configuration. If CDP is disabled, the 3900 Series router will show up in the Topology as an Unknown Device. Open the Device Information window for the device, select the Credentials tab, click Device Driver, and select the Cisco 3900 Series. If CDP is enabled, the device will be discovered properly.
Device Configuration Backup and Restore	The backup of a 3900 Series ISR consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the ASA is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	If the administrator of the 3900 Series router has defined a specific boot load with the boot system command, firmware updates are not performed.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**. For HTTP access, open a Generic Tunnel connection on port 80.

Cisco Integrated Services Router

Cisco 870, 1800, 2800 Series ISRs

Cisco 800 Series ISRs

Feature	Constraints/Notes
Discovery	Cisco 800 Series ISRs must have CDP enabled in order to be discovered by the OnPlus Network Agent. If you use Cisco CP or Cisco CP Express to configure your router, it is very likely that CDP is disabled, since this is the recommended configuration. If CDP is disabled, the 800 Series router will show up in the Topology as an Unknown Device. Open the Device Information window for the device, select the Credentials tab, click Device Driver, and select the Cisco 800 Series. If CDP is enabled, the device will be discovered properly.
Access/Device Information	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address. If the 800 Series ISR has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected will be displayed, and the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of an 800 Series ISR consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the device is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	If the administrator has defined a boot load with the boot system command, firmware upgrades are not performed. If there is not enough space on the flash to contain the new image and the current load, the firmware on this device cannot be upgraded via the portal. Upgrade the firmware manually.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

Cisco 1800 Series ISRs

Feature	Constraints/Notes
Discovery	Cisco 1800 Series ISRs must have CDP enabled in order to be discovered by the OnPlus Agent device. If you use Cisco CP or Cisco CP Express to configure the router, it is very likely that CDP is disabled, since this is the recommended configuration. If CDP is disabled, the 1800 Series router will show up in the Topology as an Unknown Device. Open the Device Information window for the device, select the Credentials tab, click Device Driver, and select the Cisco 1800 Series. If CDP is enabled, the device will be discovered properly.
Access and Info	If device access credentials are not provided, the device's MAC address, and IP address are displayed. If the 1800 Series ISR has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected be displayed, and the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of an 1800 Series ISR consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the device is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	If the administrator has defined a boot load with the boot system command, firmware upgrades are not performed.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

Cisco 2800 Series ISRs

Feature	Constraints/Notes
Discovery	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address. If the Cisco 2800 Series router has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected will be displayed, and the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of a 2800 Series router consists solely of storing a copy of the startup-config file. To restore the configuration, the saved file is copied to startup-config, and the router is rebooted, loading the new configuration. Configuration backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	To upgrade firmware, make sure that you have entered Level 15 login credentials and password.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

IAD880

Feature	Constraints/Notes
Discovery	The Cisco 800 Series IADs must have CDP enabled in order to be discovered by the OnPlus Agent device. If you use Cisco CP or Cisco CP Express to configure your router, it is very likely that CDP is disabled since this is the recommended configuration. If CDP is disabled, your 800 Series router will show up in the Topology as an unknown device. Open the Device Information window for the device, select the Credentials tab, click Device Driver, and select the Cisco 800 Series. If CDP is enabled, the device will be discovered properly.
Access/Device Information	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address. If the IAD800 series router has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected will be displayed, and the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of an IAD800 Series router consist solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the router device is rebooted, loading the new configuration. Configuration backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	To upgrade firmware, make sure that you have entered Level 15 login credentials and password.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

Cisco BE3000

Feature	Constraints/Notes
Discovery	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address. If the Cisco BE3000 router has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected will be displayed, and the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	Cross launch available.
Upgrade Firmware	Not Supported
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

Cisco Catalyst 2960, 2960-C, 2960-G, 2960-S, 3750

Feature	Constraints/Notes
Discovery	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address. If the Cisco Catalyst 3750 switch has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected will be displayed, and the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of a Cisco 3750 Catalyst switch consists solely of storing a copy of the startup-config file. To restore the configuration, the saved file is copied to startup-config, and the router is rebooted, loading the new configuration. Configuration backup and restore both require device access credentials (login and enable access).

Feature	Constraints/Notes
Upgrade Firmware	To upgrade firmware, make sure that you have entered Level 15 login credentials and password. Device successfully upgrades, but firmware install complete message does not display.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

Cisco Catalyst 3560, 3560-C, 3560-E, 3560-G, 3560-X, 3560v2

Feature	Constraints/Notes
Discovery	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address.
Device Configuration Backup and Restore	To restore the configuration, the saved file is copied to startup-config, and the router is rebooted, loading the new configuration. Configuration backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	To upgrade firmware, make sure that you have entered Level 15 login credentials and password. Device successfully upgrades, but firmware install complete message does not display.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

UC500

Feature	Constraints/Notes
Access/Device Information	You must enter credentials under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal to grant access for the device. After you enter the credentials, the portal can access this such as the CAM table, wireless association table, ARP table, and CDP neighbors as well as determine if a CUE device is installed.
Device Configuration Backup and Restore	UC500 configuration backup and restore is not supported via the OnPlus Portal. Use Cisco Configuration Assistant (CCA) to back up and restore configuration on the UC500 and CUE module.
Software Upgrade	UC500 configuration backup and restore is not supported via the OnPlus Portal. Use Cisco Configuration Assistant (CCA) to manage this device.

Feature	Constraints/Notes
Remote Access	You can access this device remotely via HTTP, SSH, or Telnet. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**. For HTTP access, open a Generic Tunnel connection on port 80.

SRP500

Feature	Constraints/Notes
Discovery	If CDP is enabled, the device will be discovered properly. UPnP discovery is also done, but the device's core firmware reports different version of the firmware in CDP and UPnP discovery. the portal uses the CDP data.
Device Configuration Backup and Restore	The backup of the SRP500 Series router consist solely of storing a copy of the config.xml, status.xml, and strike.xml files. To restore the configuration, the saved files are copied to config.xml and strike.xml, and the router is rebooted if needed by the device, loading the new configuration. The status.xml file is static and does not get restored. This file changes as the configuration changes on the device. Device backup and restore both require device access credentials for the admin user (login and enable access are both required).
Remote Access	Web connectivity to the device will connect you to the HTTP access page for the device.

SA520

Feature	Constraints/Notes
Discovery	This device can be found using CDP and Probe. The user cannot be logged on the page locally. UPnP discovery is not supported.
Access/Device Information	Login access credentials must be provided before any information can be retrieved. If a web browser is logged in with the same credentials that were given to the driver to user the driver will generate an event and not query the device since only one active session per user/password can be active at a time.

Feature	Constraints/Notes
Device Configuration Backup and Restore	You can backup and restore the entire configuration on the device.
Upgrade Firmware	OnPlus Agent takes approximately 5 minutes to come online after firmware reload and reboot.
Remote Access	Remote access is only available through HTTPS (port 443).

IESW 500 Series

Feature	Constraints
Discovery	The ESW can be discovered in three different ways: ▪ If Bonjour advertisements are turned on, and the Cisco Bonjour protocol is enabled, the device will be properly discovered. ▪ If CDP advertisements are turned on, and the OnPlus Agent has access to CDP information, the device will be properly discovered. The OnPlus Agent can either be connected directly to the ESW switch, or it can have access to a device connected to the switch that provides CDP neighbor information. ▪ Finally, the ESW can be selected using a designated driver. Selecting the driver and entering credentials will result in proper discovery. After the ESW has been discovered, it will provide CDP neighbor and CAM information that assists in discovery of additional devices, as well as Topology construction.
Device Access	After discovery, information can be gathered from the ESW using the HTTP management interface. Valid credentials need to be entered. Credentials are entered under **Credentials** > **Login** in the Device Information window on the portal.
Software Upgrade	The ESW may fail to reboot after you upgrade firmware.
Remote Access	For remote web access, use port 80 and enable the Fix Headers option. Additional caveats vary, depending on the web browser you are using: ▪ **Safari.** The Safari browser works fine, but you must ignore the “connection lost” pop-up. ▪ **Firefox**. When you first connect with firefox, you will get an error. The error is different, depending on the version of Firefox you are using. To get it to work, copy the URL and open a new window, then paste the URL into the new window. Ignore the “connection lost” message. ▪ **Internet Explorer.** IE8 works without issues.

WAP121/WAP321

Feature	Constraints/Notes
Discovery	The WAP121 and 321 has an assigned driver and will be discovered by Bonjour and is represented in the topology with a vanity icon.
Constraints	Associated wireless clients will not be listed as AP's children until SNMP is enabled on the AP(s), and after SNMP (v2/v3) credentials are provided to each AP in the portal.
Device Configuration Backup and Restore	You can back up the configuration for the WAP121/321 device by selecting a previously stored configuration file and restore it to the device.
Upgrade Firmware	You can install a firmware image for the Wap121/321 from a previously uploaded image file.
Remote Access	You can access the WAP121/321 from the OnPlus Portal GUI interface.

WAP4410N

Feature	Constraints/Notes
Remote Access	The WAP4410 requires a secure (HTTPS) connection for remote web connection.

PVC2300

Feature	Constraints/Notes
Access/Device Information	The version number may be formatted differently in the Info tab on the portal and on the camera web page. For example, V1.1.2R06 appears in the info tab, and 1.1.2.6 appears on the web page.

AP521

Feature	Constraints/Notes
Discovery	This device will be detected by CDP and CAM tables, so you must plug it into a Cisco OnPlus- supported switch.

Feature	Constraints/Notes
Access/Device Information	You must provide credentials in order to access the device. Credentials are entered under Credentials > Login and Credentials > Enable in the Device Information window on the portal. No information will be read by the portal until you enter valid credentials.
Device Configuration Backup and Restore	You must provide credentials in order to access configuration backup and restore functions.
Upgrade Firmware	As long as you provided credentials, firmware upgrades should function properly. If the device has defined a boot load with the boot system command, firmware updates do not occur, as the administrator has defined a specific load intended for the device.
Remote Access	The normal web access should work correctly with this device. You will be prompted for a username/password and then presented with a configuration web page.

RV042/RV082/RV016 V2

Feature	Constraints/Notes
Discovery	Bonjour must be enabled on these devices.
Access/Device Information	Only HTTP access credentials are supported.
Remote Access	The only supported remote access is via HTTP.

RV042/RV082/RV016 V3

Feature	Constraints/Notes
Discovery	Bonjour must be enabled on these devices.
Access/Device Information	Only HTTP access credentials are supported.
Firmware Upgrade	A known error with RV0xx v3 is that performing a firmware upgrade will always reset the current device configuration to default
Remote Access	The only supported remote access is via HTTP.

IAD2400

Feature	Constraints/Notes
Discovery	Cisco 2400 Series ISRs must have CDP enabled in order to be discovered by the OnPlus Agent device. If you use Cisco CP or Cisco CP Express to configure your router, it is very likely that CDP is disabled, since this is the recommended configuration. If CDP is disabled, the 2400 Series router will show up in the Topology as an Unknown Device. Open the Device Information window for the device, select the Access tab, click Device Driver, and select the Cisco 2400 Series. If CDP is enabled, the device will be discovered properly.
Access/Device Information	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address. If the IAD2400 Series router has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected will be displayed, and the device ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of an IAD2400 Series router consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the router is rebooted, loading the new configuration. Configuration backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	To enable firmware updates, make sure that you have entered Level 15 login credentials and password.

Feature	Constraints/Notes
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

SG300 or SF300 (v1.0 Firmware)

Feature	Constraints/Notes
Discovery	SF300/SG300 Series managed switches with version 1.0 firmware installed can be discovered using one of these methods: ▪ Bonjour. If the device is set to issue Bonjour advertisements, it will be properly discovered and identified. ▪ Designated device driver. If Bonjour discovery is disabled, the device can be discovered by manually designating a driver (Device Information window > Credentials tab, Device Driver), provided valid login credentials are provided. If the switch is using the 1.0 firmware and can be controlled via SNMPv2, discover will be fully supported. The 1.0 firmware does not support CDP.
Access/Device Information	The SF/SG 300 managed switches can be accessed via SNMPv2. **SNMPv2**. To work with SNMPv2, an appropriate view with read/write access must be created for the community that the OnPlus Agent will use. The community string must be entered into the device's SNMP access credentials field. To create SNMPv2 credentials to enable this device to work with the OnPlus Portal, follow these steps: 1. On the SG300/SF300, log in as admin and go to **Security** > **TCP/UDP Services** > **SNMP service enable**. 2. On the SG300/SF300, create the SNMP Community string as read/write. 3. On the OnPlus Portal enter the SNMP Community string in Credentials > SNMP Access in the Device Information window.
Device Configuration Backup and Restore	Backup and restore of SF300/SG300 Series managed switches with version 1.0 firmware installed requires the SNMP service to be enabled on the device and SNMPv2 access to be configured on the portal. When the device has startup-config reloaded, a reboot is issued.

Feature	Constraints/Notes
Upgrade Firmware	Firmware updates are supported on the SF/SG 300 Series of managed switches using SNMPv2 only. SNMPv2 must be enabled on the device and SNMP Access must be configured on the portal. The SF300/SG300 Series switch has space for two images: an active image and a backup image. When a firmware install is requested, the system checks to ensure that the image is not the active or backup image. If it matches either image, the file transfer is cancelled. If this is a new firmware file, it is copied to the device. The switch will copy the new image file on top of the inactive image. The switch has a flag to indicate which image will be active after reboot. This flag is modified to indicate that the newly loaded firmware will be active after a restart. A restart is then sent to the device and the new image loads. The reboot can take 2-3 minutes. While that process is running, the OnPlus Agent continually tries to reconnect. The OnPlus Agent checks to determine if the device acquired a new IP address.
Remote Access	Remote web access via the portal is not supported by the version 1.0 firmware. SNMPv2 access is provided for enabling discovery, configuration backup and restore via the portal, and firmware upgrades via the portal. SNMP control of the device is not available via remote access.

SF300 or SG300 (v1.1 Firmware)

Feature	Constraints/Notes
Discovery	SF/SG 300 Series managed switches with firmware version 1.1 or later can be discovered via one of three methods: ▪ Bonjour. If the device is set to issue Bonjour advertisements, it will be properly discovered and identified. ▪ CDP. If the device is set to issue CDP advertisements, it will be properly discovered and identified. ▪ Designated device driver. In the event that other discovery methods are disabled, the device can be discovered by manually designating a driver (Device Information window > Credentials tab, Device Driver), provided valid login credentials are provided. After the device is discovered and credentials are provided, the switch will perform discovery on other devices found as CDP neighbors, as well as devices in the CAM table. If the switch is using the 1.1 or later firmware, it can be discovered via either SNMP2 or using the HTTP interface.

Feature	Constraints/Notes
Access/Device Information	SF300 and SG300 Series managed switches with version 1.1 firmware installed can be accessed via SNMPv2, SNMPv3, or HTTP. To work with SNMPv2 or v3, an appropriate view with read/write access must be created for the community that the OnPlus Agent will use. The community string must be entered into the device's SNMP access credentials field. **SNMPv2**. To create SNMPv2 credentials to enable this device to work with the OnPlus Portal, follow these steps: 1. On the SG300/SF300, log in as admin and go to **Security** > **TCP/UDP Services** > **SNMP service enable**. 2. On the SG300/SF300, create the SNMP Community string as read/write. 3. On the OnPlus Portal enter the SNMP Community string in Credentials > SNMP Access in the Device Information window. **SNMPv3**. If you create SNMPv3 credentials for the device and set them to be usable, the driver will attempt to use those drivers in preference to any SNMPv2 credentials. The version 1.1 firmware for the SF300/SG 300 switches supports SNMPv3, but there are a few restrictions. ▪ The firmware does not save users that have been defined for SNMPv3. This means that any time the device reboots, you must re-enter the access credentials. ▪ The device does not support the use of passphrases for Privacy. Since the Cisco OnPlus SNMPv3 authentication models only use passphrases (not keys), you cannot use Privacy with this device. ▪ The device does not support AES for a privacy protocol. You must use DES. For an example of how to configure SNMPv3 management access for SF300/SG300 managed switches with the OnPlus Portal, follow these steps: 1. In the device web page go to **SNMP:Engine ID**, select the **Use Default** radio button, and click **Apply**. 2. In the device web page, go to **SNMP:Groups** and add a group. 3. Set the group name to **authnopriv**, select **Security Model SNMPv3**, check the Authentication and No Privacy box, and give the device Read, Write, and Notify privileges as DefaultSuper. 4. Click **Apply**. 5. Under **User SNMP**:Users, add a new user called admin, using the **Local Engine ID**. Set the group name to authnopriv, set the Authentication method to **MD5** password, and set the password to Password01. Click **Apply**. 6. Under **Security:TCP/UDP Services**, enable **SNMP** and click **Apply**. 7. Then save the settings in Admin File management. 8. On the OnPlus Portal, open the Device Information window for the device, select the Credentials tab, choose **SNMP Access**, and click the **SNMPv3** radio button. Specify the corresponding settings and click **OK**. Your credentials should now validate properly with the SF300/SG300 device.

Feature	Constraints/Notes
Device Configuration Backup and Restore	Backup and restore of SF300/SG300 Series managed switch can be performed using either SNMPv2 or the HTTP/XML API. Firmware 1.1 fully supports backup and restore. When the device has startup-config reloaded, a reboot is issued.
Upgrade Firmware	Firmware updates are supported on the SF300/SG300 Series of managed switches using either SNMPv2 or HTTP/XML API. The procedure is fully supported with the 1.1 firmware. The SF300/SG300 Series switch has space for two images: an active image and a backup image. When a firmware install is requested, the system checks to ensure that the image is not the active or backup image. If it matches either image, the file transfer is cancelled. If this is a new firmware file, it is copied to the device. The switch will copy the new image file on top of the inactive image. The switch has a flag to indicate which image will be active after reboot. This flag is modified to indicate that the newly loaded firmware will be active after a restart. A restart is then sent to the device and the new image loads. The reboot can take 2-3 minutes. While that process is running, the OnPlus Agent continually tries to reconnect. The OnPlus Agent checks to determine if the device acquired a new IP address.
Remote Access	The web admin interface to the SF/SG 300 Series managed switch can be accessed remotely using a web connection. SNMPv2/v3 management access is provided for enabling discovery, configuration backup and restore via the portal, and firmware upgrades via portal. SNMP control of the device is not available via remote access.

SF500 or SG500

Feature	Constraints/Notes
Discovery	SX500 Series managed switches can be discovered via one of three methods: ▪ Bonjour. If the device is set to issue Bonjour advertisements, it will be properly discovered and identified. ▪ CDP. If the device is set to issue CDP advertisements, it will be properly discovered and identified. ▪ Designated device driver. In the event that other discovery methods are disabled, the device can be discovered by manually designating a driver (Device Information window > Credentials tab, Device Driver), provided valid login credentials are provided. After the device is discovered and credentials are provided, the switch will perform discovery on other devices found as CDP neighbors, as well as devices in the CAM table.The switch can be discovered via either SNMP2 or using the HTTP interface. If CDP is enabled, the device will be discovered properly. However, when SX500 Series managed switches are stacked, discovery becomes more complex. For CDP discovery to work, the advertisement must come from the master. This means that there should be a connection from the master to either the OnPlus Network Agent or another device that is capable of providing CDP neighbor information to the OnPlus Network Agent. If the CDP advertisements are seen coming from one of the slave switches, the portal cannot associate those with the stack.
Access/Device Information	The SX500 Series managed switches can be accessed via SNMPv2. (Cisco OnPlus Portal supports SNMP v2 and v3, however v3 is not supported for this device in this release.) **SNMPv2**. To work with SNMPv2, an appropriate view with read/write access must be created for the community that the OnPlus Agent will use. The community string must be entered into the device's SNMP access credentials field. To create SNMPv2 credentials to enable this device to work with the OnPlus Portal, follow these steps: 1. On the SX500, log in as admin and go to **Security** > **TCP/UDP Services** > **SNMP service enable**. 2. On the SX500 create the SNMP Community string as read/write. 3. On the OnPlus Portal enter the SNMP Community string in Credentials > SNMP Access in the Device Information window.
Device Configuration Backup and Restore	Backup and restore of SX500 Series managed switches requires the SNMP service to be enabled on the device and SNMPv2 access to be configured on the portal When the device has startup-config reloaded, a reboot is issued.

Feature	Constraints/Notes
Upgrade Firmware	Firmware updates are supported on the SX500 Series managed switches using SNMPv2 only. SNMPv2 must be enabled on the device and SNMP Access must be configured on the portal. The SX500 switch has space for two images: an active image and a backup image. When a firmware install is requested, the system checks to ensure that the image is not the active or backup image. If it matches either image, the file transfer is cancelled. If this is a new firmware file, it is copied to the device. The switch will copy the new image file on top of the inactive image. The switch has a flag to indicate which image will be active after reboot. This flag is modified to indicate that the newly loaded firmware will be active after a restart. A restart is then sent to the device and the new image loads. The reboot can take 2-3 minutes. While that process is running, the OnPlus Agent continually tries to reconnect. The OnPlus Agent checks to determine if the device acquired a new IP address.
Remote Access	Remote web access for the SX500 Series managed switches via the portal UI is supported. SNMPv2 access is provided for enabling discovery, configuration backup and restore via the portal, and firmware upgrades via the portal. SNMP control of the device is not available via remote access.

WS-CE520

Feature	Constraints/Notes
Access/Device Information	CDP must be enabled on this device.
Discovery	The only supported credentials are HTTP login credentials.
Remote Access	The only supported remote access is via HTTP.

WS-C2960

Feature	Constraints/Notes
Discovery	No Catalyst 2900 CatOS devices are supported. Supported devices must be Cisco IOS-based. If CDP is enabled, the device will be discovered properly. However, when 2960 switches are stacked, discovery becomes more complex. For CDP discovery to work, the advertisement must come from the master. This means that there should be a connection from the master to either the OnPlus Network Agent or another device that is capable of providing CDP neighbor information to the OnPlus Network Agent. If the CDP advertisements are seen coming from one of the slave switches, the portal cannot associate those with the stack.
Access/Device Information	Regardless of whether credentials are provided, you will discover the device's MAC address and IP address. If the Cat 2900 Series router has SSH access, and Level 15 credentials are entered under **Credentials** > Login and **Credentials** > Enable in the Device Information window on the portal, the device information collected will be displayed, and the device ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of an Cat 2900 Series router consist solely of storing a copy of the startup-config file. To restore the configuration, the saved file is copied to startup-config, and the router is rebooted, loading the new configuration. Configuration backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	To enable firmware updates, make sure that you have entered Level 15 login credentials and password.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

WS-C4948

Feature	Constraints/Notes
Discovery	No Catalyst 4948 CatOS devices are supported. Supported devices must be Cisco IOS-based. If CDP is enabled, the device will be discovered properly.
Access/Device Information	Regardless of whether your credentials are provided, you will discover the device's MAC address and IP address. If the C4948 Series router has SSH access, and Level 15 credentials are entered under Credentials > Login and Credentials > Enable in the Device Information window on the portal, the device information collected will include Serial Number, PID/VID, device type, model name, and description. In addition, the device's ARP and CAM tables will be used to discover additional devices.
Device Configuration Backup and Restore	The backup of an Cat 4948 series router consist solely of storing a copy of the startup-config file. To restore the configuration, the saved file is copied to startup-config, and the router is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	To upgrade firmware, make sure that you have entered Level 15 login credentials and password.
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

AP541

Feature	Constraints/Notes
Discovery	Since the device is discovered via CDP, it should always have the platform and firmware set. Discovery requires that login username and password be set. Credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal. If you provide credentials, devices connected to this device should show up in the Topology.

Feature	Constraints/Notes
Device Configuration Backup and Restore	Backup and restore requires that login username and password be set. The backup and restore of the device configuration is supported. After a restore, the device is rebooted so the new configuration can take effect. Backups that are done with firmware 1.9.1 are compatible with 1.9.2. Typically, backups are only valid for the firmware load on which they are made.
Upgrade Firmware	Firmware upgrades require that the login username and password be set.

AP801

Feature	Constraints/Notes
Discovery	The AP800 Series access point is discovered through CDP, ARP, DHCP, and CAM table lookup. CDP is the primary discovery method, and the others add more information.
Access/Device Information	Regardless of whether access credentials are provided, the device's MAC address and IP address are discovered. If the AP800 Series access point has SSH access, and Level 15 credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal, the device information collected will include Serial Number, PID/VID, device type, and model name. No description is set.
Device Configuration Backup and Restore	The backup of an AP800 Series access point consists solely of storing a copy of the startup-config file. Other elements, such as users defined in the AAA database, are not backed up. To restore the configuration, the saved file is copied to startup-config, and the access point is rebooted, loading the new configuration. Backup and restore both require device access credentials (login and enable access).
Upgrade Firmware	The AP801 is a Cisco IOS module that shows up as a separate device in the Topology. The firmware image is not a normal Cisco IOS.bin file; it is a tar package that contains the Cisco IOS image and the HTTP access files. During a firmware upgrade, the files are extracted onto the flash in the directory specified in the tar file, the old load directory is removed, and the boot environment variable is set so the access point can boot properly.

Feature	Constraints/Notes
Remote Access	The normal web connection will not work. If you have CP Express loaded on the router, it will try and load that program up and run it. This is a Java program and does not work properly through the HTTP tunnel that is being created. For HTTP access, open a Generic Tunnel connection on port 80. For Cisco IOS command-line administration, enable SSH or Telnet on the device and connect via a Generic Tunnel. See **Remote Access using Generic Tunnel Connection, page 277**.

AIR-AP1142

Feature	Constraints/Notes
Discovery	This device will be detected by CDP and CAM tables, so it must be plugged into a supported switch.
Device Configuration Backup and Restore	You must provide credentials in order for device configuration and backup and restore to function properly. Credentials are entered under **Credentials** > **Login** and **Credentials** > **Enable** in the Device Information window on the portal.
Upgrade Firmware	As long as access credentials are provided this should function properly. If the administrator has defined a specific boot load with the boot system command, firmware updates are not performed.

Cisco 6900, 7900, 8900, 9900 Series IP Phones

Feature	Constraints/Notes
Discovery	Cisco IP Phones are only discovered via CDP and CAM table entries. Since the phones reside on a different VLAN, the OnPlus Agent device is unable to discover them using other methods. If phones are plugged into a router/switch that is not supported by the OnPlus Portal, they will not display in the Topology.
Access/Device Information	A single phone should only be accessed once. The following information will be gathered: Serial number, information to make a PIDVID, and the software version. No other information is read or set. The backup/restore and firmware via the management capabilities item in the Info tab are disabled. After the serial number has been set for a phone, it will not be accessed again. In some cases the phone will be accessed multiple times until the full discovery information is sent to the SN and then back down to the OnPlus Agent in the consumer_sani.xml file. A phone may be accessed multiple times if it has a load from the factory that does not support HTTP access. After the phone has been configured into a PBX system that supports HTTP access and has an upgraded the phone load, it will be accessed to obtain the needed information.

SPA300, SPA500 Series IP Phones

Feature	Constraints/Notes
Discovery	Cisco IP Phones are only discovered via CDP and CAM table entries. Since the phones reside on a different VLAN, the OnPlus Agent device is unable to discover them using other methods. If phones are plugged into a router/switch that is not supported by the OnPlus Portal, they will not display in the Topology.
Access/Device Information	The following information is gathered for these phones during discovery: serial number, product and version ID (PID/VID), and the software version. No other information is read or set. The backup/restore and firmware via the management capabilities item in the Info tab are disabled. After the serial number has been set for a phone, it will not be accessed again. In some cases the phone will be accessed multiple times until the full discovery information is sent to the OnPlus Agent. A phone may be accessed multiple times if it has a load from the factory that does not support HTTP access. After the phone has been configured into a PBX system that supports HTTP access and has an upgraded the phone load, it will be accessed to obtain the needed information. A UC320 behind an SA500 security appliance (existing network installation) will need a route from data network VLAN 1 to voice network VLAN 100 (on this UC320, Networking -> Routing-> static -> Destination = 10.1.1.0 /24 Interface = LAN Gateway = 192.168.75.250).

PVC300

Feature	Constraints/Notes
Remote Access	Remote access will work properly, but this connection should only be used for system configuration and not to view video. In some cases the video may not work depending on the version of browser that is used due to required plug-ins.

VC220

Feature	Constraints/Notes
Remote Access	Remote access will work properly, but this connection should only be used for system configuration and not to view video. In some cases the video may not work depending on the version of browser that is used due to required plug-ins.

VC240

Feature	Constraints/Notes
Remote Access	Remote access will work properly, but this connection should only be used for system configuration and not to view video. In some cases the video may not work depending on the version of browser that is used due to required plug-ins.

NSS300

Feature	Constraints/Implementation Notes
Discovery	Discovery of the NSS300 Series device depends on Bonjour discovery. The NSS300 should have Bonjour advertisements enabled for both web Administration and CSCO-SB.
Device Access and Information	Administration of the NSS300 Series NAS is done via the web interface. Firmware versions 1.1, 1.2, and 1.3 are currently supported. ▪ If available, administration is done using HTTPS on port 443. ▪ If this port is not available, administration is done via HTTP on port 8080. ▪ If neither of these ports are open, the device will not be manageable.

Feature	Constraints/Implementation Notes
Configuration Backup and Restore	Backup and restore of the NSS300 is performed using the backup and restore functions of the web interface, and works exactly as if the user was performing those functions using the conventional administrative interface. A configuration restore requires a reboot, and NAS reboots can vary in time, depending on the amount of storage management that has to take place. ▪ If the reboot time lasts longer than five minutes, the OnPlus Agent may report that it failed to reconnect to the device. ▪ If the device gets a new IP address during reboot, the OnPlus Agent will try to reconnect at the new address, but this process is not completely reliable. Giving managed devices a fixed IP address is recommended.
Firmware Upgrade	Updating firmware on NAS300 is performed using the web interface, and works exactly as if the user was performing those functions using the conventional administrative interface. A firmware update requires a reboot, and NAS reboots can vary in time, depending on the amount of storage management that has to take place. ▪ If the reboot time lasts longer than five minutes, the OnPlus Agent may report that it failed to reconnect to the device. ▪ If the device gets a new IP address during reboot, the OnPlus Agent will try to reconnect at the new address, but this process is not completely reliable. Giving managed devices fixed addresses is recommended.

Remote Access using Generic Tunnel Connection

To connect to a Cisco IOS device using Telnet or SSH for Cisco IOS command-line administration, follow these steps:

STEP 1 Locate the device in the Topology or Device Listing and open the Device Information window.

a. Click the **Connect** tab and choose **Generic Connection**.

b. For SSH, enter **port 22**. For Telnet, enter **port 23**.

c. Click **Connect to device**. The connection URL is displayed in a pop-up window.

d. Copy the link.

STEP 2 Paste the link into your terminal connection software.

For example, if you are using PuTTY:

a. Copy the address into the Host (IP) window.

b. Select SSH or Telnet.

c. Replace the port number displayed in PuTTY (port 22 for SSH; port 23 for Telnet) with the number after the colon (:) in the link address.

d. Choose **Open**.