# Cisco OnPlus for Small Business Wireless Deployments

**Last Revised: May 16, 2012**

This Application Note is intended for use by Cisco OnPlus Partners who want to provide managed wireless services for their customers. The following topics are covered:

- OnPlus Wireless Management application
- Instructions for enabling SNMP on WAP121 and WAP321 Series access points and SNMP access settings OnPlus Portal that are required to enable these features
- OnPlus wireless reports
- Limitations and caveats

## Contents

# Overview

Cisco OnPlus Service complements Cisco's latest Small Business Access Points, WAP121 and WAP321, to provide a comprehensive wireless LAN management solution for VARs that offer, or are expanding to, a managed wireless service practice, and for customers looking for increased visibility and access of their wireless deployments.

**OnPlus Wireless Features**

OnPlus Wireless Management application provides the means for creating, scheduling, and storing wireless reports. Once the OnPlus Wireless Management application is installed, wireless reporting will enable Partners to gain insight into wireless deployments and allow them to collect the necessary background information to provide ongoing guidance to their customers.

Reports can be scheduled daily or monthly, or created instantaneously to track wireless LAN activity in key areas such as: AP Summary, Radio Summary, AP Status, Associated Wireless Clients per AP, Wireless Client Traffic, Wireless Client Type Summary, Top Client Summary,AirMagnet and Top Client Traffic.

The OnPlus AirMagnet Planner for Cisco Small Business enables Partners to leverage offers from Cisco partnerships to take the guesswork out of scoping and planning a wireless deployment. Partners can take advantage of this attractive offer and download the AirMagnet Planner for Cisco Small Business software from the Apps page on the Dashboard menu for any customer account.

When Cisco Small Business WAP121 and WAP321 Series Access Points are present in the network, you can use the OnPlus Service to:

- Discover and view the wireless access points and associated clients in the OnPlus Portal customer network topology and inventory views.
- Get information about access points and the associated clients, including the MAC address, IP address, serial number, firmware version, and device model name.
- Perform basic device and network monitoring on the access points, including monitoring of up/down status with simple alerting via mail or SMS text messages.
- Upload and manage device firmware.
- Back up and restore device configuration.
- Connect to the device's Web-based Configuration utility remotely via the portal.

- View information about Warranty and Service Contracts, PSIRTs, and software/hardware End-of-Life, End-of-Service, and End-of-Support notices.

For more information, see the Cisco OnPlus Portal User Guide. To access the HTML version of the guide from the portal, click the Documentation link at the top of the page. The guide is also available on Cisco.com at the following URL: www.cisco.com/go/onplus-docs.

# Prerequisites

To take advantage of the features described in the **Overview, page 2**, the follow prerequisites must be followed:

- **Installing the OnPlus Wireless Management Application, page 3**
- **Entering Device Login Credentials on the Portal, page 4**
- **Enabling SNMP on WAP121 and WAP321 Series Access Points, page 4**
- **Enabling SNMP Access for a Device on the Portal, page 6**

## Installing the OnPlus Wireless Management Application

Once you have installed a WAP121 or WAP321 in your network, you must install the OnPlus Wireless Management application from the OnPlus AppStore. The OnPlus Wireless Management application allows the Partner to create, view, and manage reports that provide information specific to the access point. To install the OnPlus Wireless Management application, follow these steps:

**STEP 1** From the Overview page, select the Customer for which you will install the OnPlus Wireless Management application.

**STEP 2** From the Dashboard, click **Apps**.

**STEP 3** From the Apps page, select OnPlus Wireless Management and click **FREE**.

**STEP 4** From the + Add App window, click **Add.**

The OnPlus Wireless Management application on the Apps page will display **Installed** below the wireless icon and **Wireless** will appear in the Dashboard main menu bar.

## Entering Device Login Credentials on the Portal

For best results with Cisco OnPlus, be sure to enter access credentials on the OnPlus Portal for each wireless access point at the customer site.

To enter login credentials for a device on the portal, open the Device Information window for the device, select the Credentials tab, choose **Login Access**, and enter the administrative username and password for the access point.

For more information, see the *OnPlus Portal User Guide* or online help.

## Enabling SNMP on WAP121 and WAP321 Series Access Points

In order to enable OnPlus features for the WAP 121 and WAP321 Series access points, you must enable and configure SNMP on the access points. If SNMP is not enabled on the access point, wireless reporting, firmware upgrades, and configuration backup and restore via the portal will not work.

You can configure the access point to use either SNMPv2 or SNMPv3.

Make a note of the SNMP settings that you configure on the access point. You will need them later when configuring SNMP access settings on the OnPlus Portal. The SNMP access settings on the portal must match the settings on the access point.

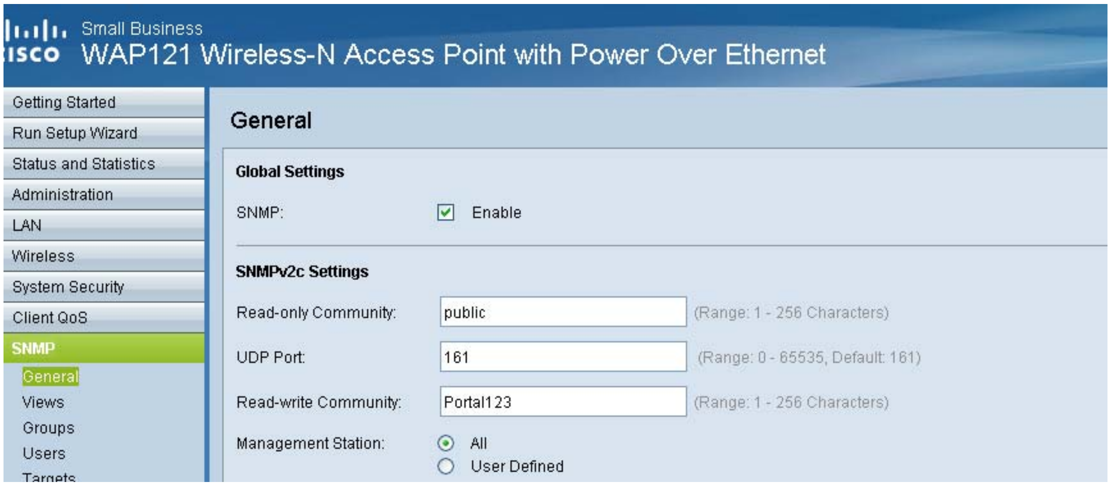
NOTE If needed, you can access the WAP121/321 Series device manager by opening a remote Web connection to the access point via the OnPlus portal. If you encounter problems opening a remote Web connection via the portal, make sure that the Web connection settings on the Connect tab in the Device Information window are configured with port 80 and all other Web connection options are unchecked.

### Configuring SNMPv2 on WAP121/WAP321 Series Access Points

Follow these steps to enable and configure SNMPv2 on the access point using the WAP121/131 Series device manager.

STEP 1 Log in to the WAP121 or WAP321 wireless access point as administrator.

STEP 2 Choose **SNMP** > **General**.



General

Global Settings

SNMP: ☑ Enable

SNMPv2c Settings

| | | |
|---|---|---|
| Read-only Community: | public | (Range: 1 - 256 Characters) |
| UDP Port: | 161 | (Range: 0 - 65535, Default: 161) |
| Read-write Community: | Portal123 | (Range: 1 - 256 Characters) |
| Management Station: | ● All<br>○ User Defined | |

**STEP 3** On the General page, configure these settings:

a. Check the **SNMP** checkbox.

b. **Read-only Community**: Enter a string that contains from 1 to 256 alphanumeric characters.

c. **UDP Port**: Use the default UDP port (161) or enter a custom port number from 0 to 65535.

d. **Read-write Community**: Enter a string that contains 1 to 256 alphanumeric characters.

**STEP 4** Click **Save**.

### Configuring SNMPv3 Settings on WAP121/WAP321 Series Access Points

SNMPv3 offers enhanced security options for authentication and privacy.

Follow these steps to enable and configure SNMPv3 on the WAP121 or WAP321 Series access point using the Web-based device manager.

**STEP 1** Log in to the WAP121 or WAP321 wireless access point as administrator.

**STEP 2** From the Getting Started page, choose **SNMP** > **Views**.

**STEP 3** In the **View Name** field, enter a name of up to 32 alphanumeric characters to identify the MIB view.

**STEP 4** Choose **SNMP** > **Group**, and configure the following settings:

a. **Authentication type**. For use with the OnPlus Portal, select MD5.

b. **Authentication Pass Phrase**. Enter a phrase that contains from 8 to 32 characters.

c. **Encryption Type**. For use with the OnPlus Portal, select DES.

d. **Encryption Pass Phrase**. Enter a phrase that contains from 8 to 32 characters.

**STEP 5** Click **Add** and then click **Save**.

## Enabling SNMP Access for a Device on the Portal

After enabling and configuring SNMP settings on the access points, you must configure SNMP access settings on the OnPlus Portal for each of the access points at the customer site.

The SNMP access settings configured on the OnPlus Portal must match the settings configured on the access points.

SNMP access settings configured on the portal vary, depending on whether you are using SNMPv2 or SNMPv3.

### Enabling SNMPv2 Access on the OnPlus Portal

To enable SNMPv3 access on the OnPlus Portal, perform these steps on each WAP121/WAP321 access point at the customer site:

**STEP 1** Log in to the portal and navigate to the Topology view for the customer.

**STEP 2** From the Topology view on the Dashboard, select the wireless access point for which you have entered parameters and open the Device Information window.

**STEP 3** From the Device Information window, click the **Credentials** tab and select **SNMP Access**.

**STEP 4** To enable SNMPv2 access, configure the following settings:

a. Check the **SNMPv2** checkbox.

b. **Community String**. Verify that data string displayed here matches the string entered in the Read-only Community field on the access point.

c. Check the **Allow SNMP V2 Access** checkbox.

**STEP 5** Click **OK**.

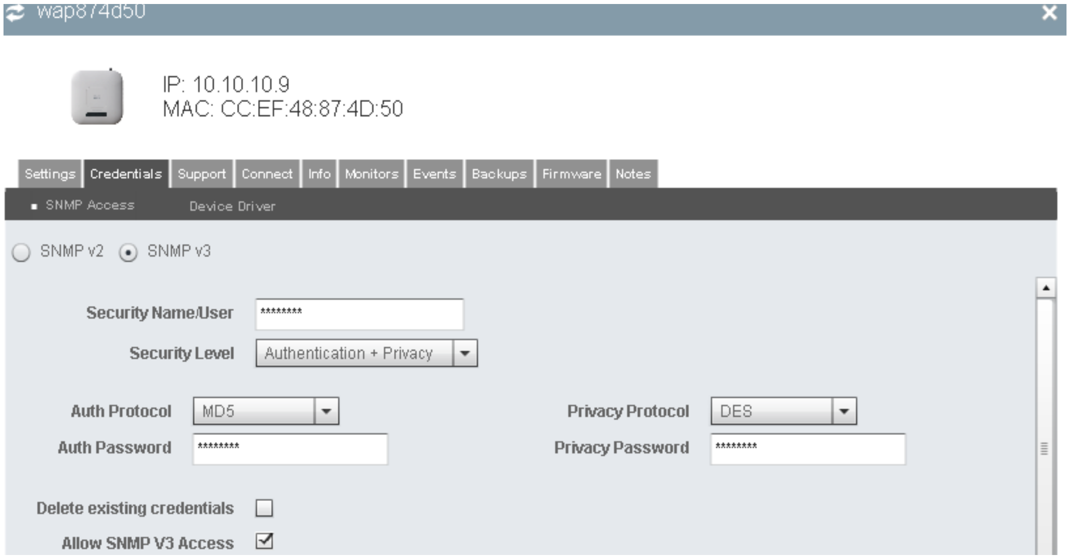
### Enabling SNMPv3 Access on the OnPlus Portal

To enable SNMPv3 access on the OnPlus Portal, perform these steps on each WAP121/WAP321 access point at the customer site:

**STEP 1** Log in to the portal and navigate to the Topology view for the customer.

**STEP 2** From the Topology view on the Dashboard, select the wireless access point for which you have established credentials and open the Device Information window.

**STEP 3** From the Device Information window, click the **Credentials** tab, then select **SNMP Access**.



IP: 10.10.10.9
MAC: CC:EF:48:87:4D:50

○ SNMP v2 ● SNMP v3

Security Name/User: ********
Security Level: Authentication + Privacy
Auth Protocol: MD5
Auth Password: ********
Privacy Protocol: DES
Privacy Password: ********
Delete existing credentials □
Allow SNMP V3 Access ☑

**STEP 4** Check the **SNMP v3** checkbox and configure the following settings:

a. **Security Name/User**: Enter the View Name exactly as it is configured on the access point.

b. **Security Level**: Select **Authentication + Privacy**.

c. **Auth Protocol**: Select **MD5**.

d. **Privacy Protocol**: Select **DES.**

e. **Auth Password**: Enter the Authentication Pass Phrase exactly as it is configured on the access point.

f. **Privacy Password:** Enter the Encryption Pass Phrase exactly as it is configured on the access point.

g. **Delete existing credentials**: Enabled (box is checked).

h. **Allow SNMP V3 Access**: Enabled (box is checked).

STEP 5 Click **OK**.

## Data Collection on the OnPlus Network Agent

OnPlus collects data from each access point at a fixed 5-minute interval. Data is stored in two time series: the last 24 hours, and the last 31 days.

The resolution of the data in the report is determined by the report period that is selected when the report is created:

- If the Report Start date is the same as the Report End date, the report period is a single day, and the data contained in the report will have an hourly resolution, showing data from the last 24 hours.
- If the report period spans multiple days, the data contained in the report will have a daily resolution, showing data from the last 31 days. The data for any given day is actually an average of the hourly data that is consolidated once at the end of each day.

## Generating Wireless Reports

To generate a Wireless Report, follow these steps:

STEP 1 There are two methods to access the wireless report capability:

**Method 1**

a. From the Overview page, choose the Customer from the customer Name List.

b. From the Dashboard page, click **Wireless.**

c. From the Wireless page, click **+ Create Wireless Report.**

d. Go to **Step 2**.

**Method 2**

a. From the Overview page on the portal, select **Reports** > **Report Listing.**

b. From the Reports page, click **+ Create Report.**

**STEP 2** From the + Create Report window, select **Wireless Access Point Summary** or **Wireless Client Summary** from the Report pull-down menu.

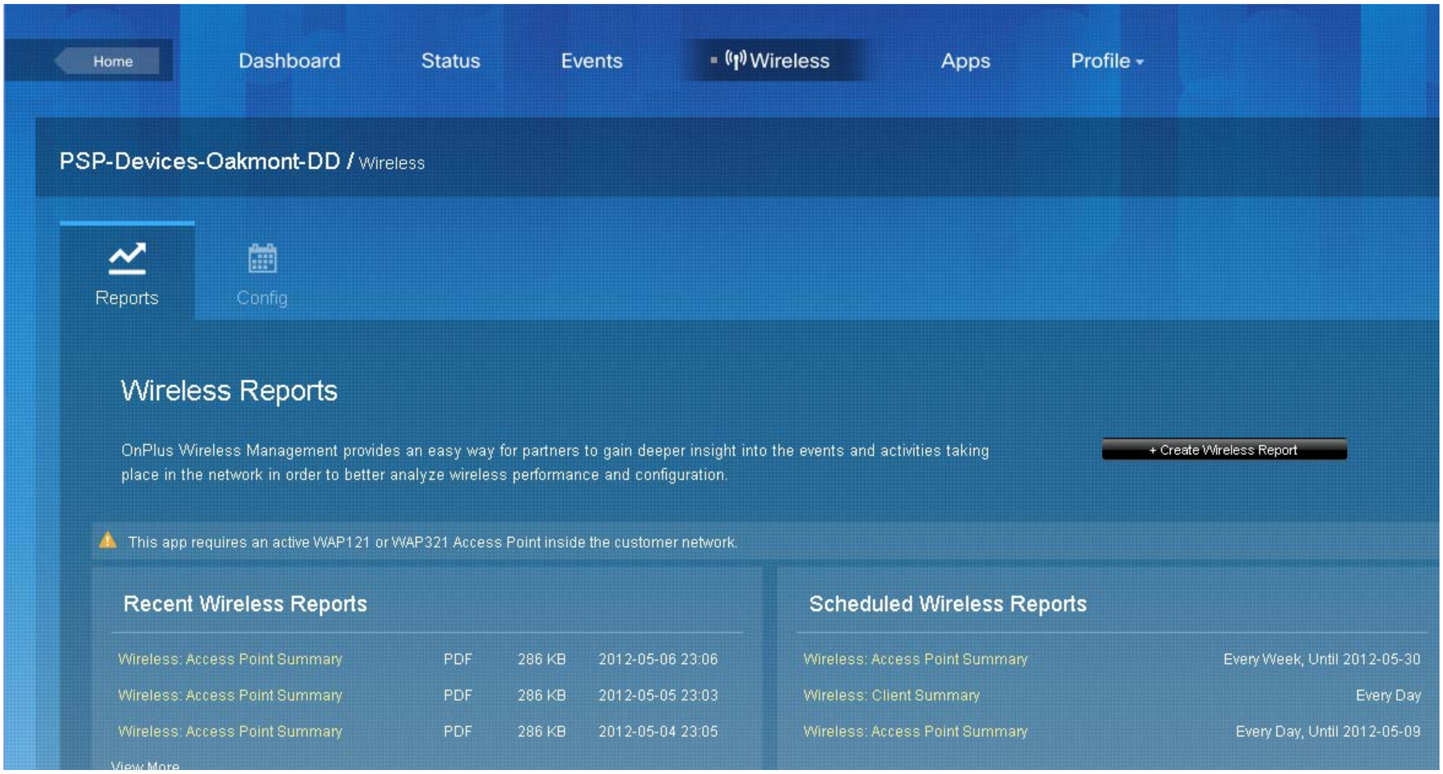
**STEP 3** Configure report settings, choose report sections, and set scheduling options as you would for any other OnPlus report.

**STEP 4** When finished, click **Save**.

## Using the OnPlus Wireless Management Application

The OnPlus Wireless Management application consolidates all wireless reports for viewing, easy access, and management.

From the Wireless page, Partners are able to create new wireless reports, open completed reports to view or save, and access scheduled reports to view details and delete selected reports from the schedule queue.



PSP-Devices-Oakmont-DD / Wireless

Wireless Reports

OnPlus Wireless Management provides an easy way for partners to gain deeper insight into the events and activities taking place in the network in order to better analyze wireless performance and configuration.

This app requires an active WAP121 or WAP321 Access Point inside the customer network.

Recent Wireless Reports

| | | | |
|---|---|---|---|
| Wireless: Access Point Summary | PDF | 286 KB | 2012-05-06 23:06 |
| Wireless: Access Point Summary | PDF | 286 KB | 2012-05-05 23:03 |
| Wireless: Access Point Summary | PDF | 286 KB | 2012-05-04 23:05 |

Scheduled Wireless Reports

| | |
|---|---|
| Wireless: Access Point Summary | Every Week, Until 2012-05-30 |
| Wireless: Client Summary | Every Day |
| Wireless: Access Point Summary | Every Day, Until 2012-05-09 |

# Report Descriptions

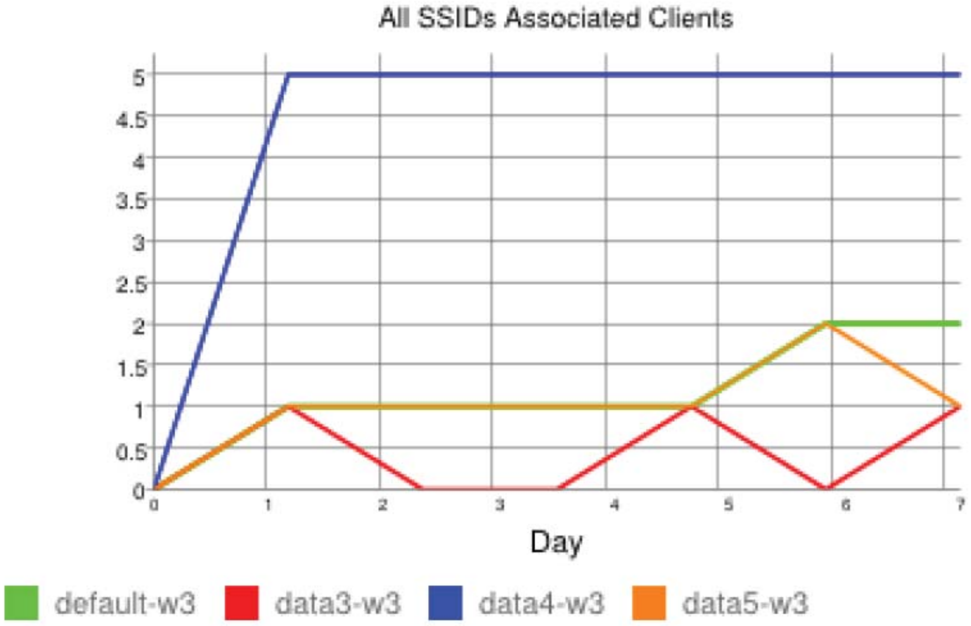
## Wireless AP Summary

This report contains historical data for a period that is customer-specified. The reports includes the following types of information for the access points in the network:

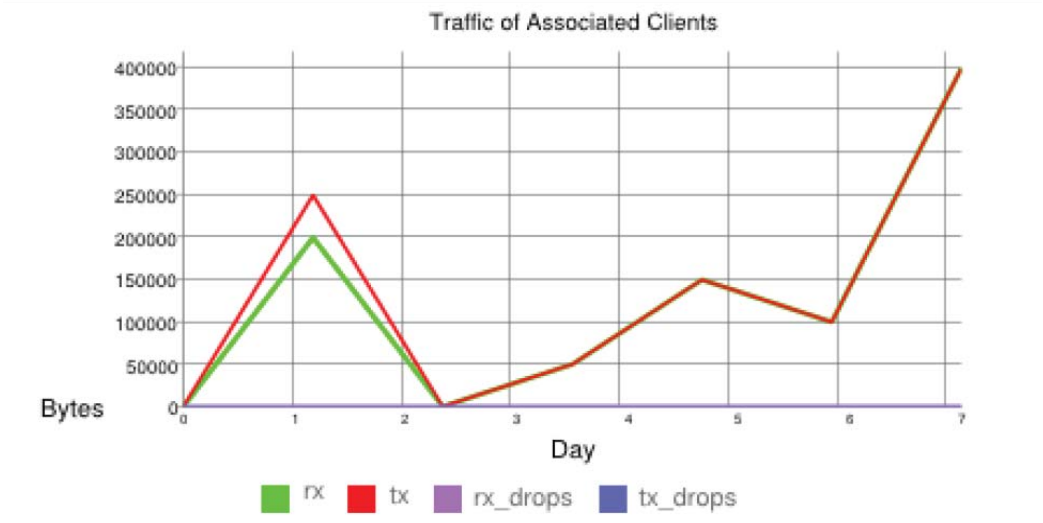
- Access Point Summary
  - Configuration Status - IP Address, Device Name, Radio Status, Firmware Version.
  - Configuration Details -Model, MAC Address, Serial Number, Clustering Status.
  - Radio Details - Status, Name, Radio, MAC Address, Wireless Mode, Radio Channel, Radio Channel Policy, Max Clients, and TX Power.

    - Access Point Status History.

- Up time by hour for Access Point Status, Interface Status, and Radio Status.
- Client Association History Total - history of Average Client Associations across all Access Points.



- Client Association History by AP - history of Average Client Associations per Access point.
- Traffic History Total - the average data transmitted across all Access points.



- Traffic History by AP - the average data transmitted across all Access Points.

## Wireless Client Summary

The Client Summary report provides information on current activity on the network. The report provides the following information:

- Active Connection by AP
  - Shows every active access point in the network.
  - Shows each device currently connected to the access point.
  - Shows continuous connection time per device.
- Active Traffic by AP
  - Shows client traffic on each access point.
  - Shows transmit and receive bytes and dropped bytes.

# Known Issues

The following notes, limitations, and caveats apply to the initial release:

- Wireless reports that were created in OnPlus release 7.1 will remain available in the report list for preview and download. However, going forward, the OnPlus Wireless Management App is required for any new data collection. One must install the OnPlus Wireless Management to resume valid report generation. Since the reports now consist of several new sections and data, it is best that one deletes the existing scheduled rule and create new scheduled reports containing new sections.
- The initial release has been tested with version 1.0.0.3 of the WAP121 and WAP321 Series firmware.
- It is assumed that the SSIDs across all access points per customer site are named the same.
- Wireless report content may not be accurate or the report may be empty when the reporting period includes fractional time periods.

Document No: 78-20777-01