ScienceLogic

# Monitoring Cisco Wireless LAN Controllers

Cisco: Wireless PowerPack version 105

# Table of Contents


**Introduction** ..... **3**

What are Cisco Wireless LAN Controllers? ..... 3

What Does the Cisco: Wireless PowerPack Monitor? ..... 4

Installing the Cisco: Wireless PowerPack ..... 4

**Configuration and Discovery** ..... **6**

Prerequisites for Monitoring Cisco Wireless LAN Controllers ..... 6

Configuring a Cisco WLC SNMP Credential ..... 7

Configuring a Cisco WLC SNMP Credential in the Skylar One Classic User Interface ..... 9

Discovering Cisco WLC Devices ..... 10

Discovering Cisco WLC Devices in the Skylar One Classic User Interface ..... 12

Verifying Discovery and Dynamic Application Alignment ..... 13

Manually Aligning Dynamic Applications ..... 13

Handling Device Failover ..... 14

Troubleshooting Duplicate Device Issues ..... 15

Viewing Cisco WLC Component Devices ..... 17

**Dashboards** ..... **19**

Device Dashboards ..... 19

Cisco WLC: AP Dashboard ..... 20

Cisco WLC: Interface Dashboard ..... 20

# Chapter 1

# Introduction

## Overview

This manual describes how to monitor Cisco wireless LAN controllers in Skylar One using the "Cisco: Wireless" PowerPack.

This chapter covers the following topics:


*What are Cisco Wireless LAN Controllers?* ..... 3

*What Does the Cisco: Wireless PowerPack Monitor?* ..... 4

*Installing the Cisco: Wireless PowerPack* ..... 4


**NOTE:** ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

## What are Cisco Wireless LAN Controllers?

Cisco wireless LAN controllers (WLC) play a central role in Cisco unified wireless networks. WLCs collect management and data packets from the network's access points (AP) and then switch those packets between wireless clients and the wired portion of the network. The WLC also controls the network

configuration and passes this configuration data to the access points, which act as wireless client interfaces.

# What Does the Cisco: Wireless PowerPack Monitor?

The "Cisco: Wireless" PowerPack enables you to monitor Cisco WLCs and APs using the AIRESPACE-WIRELESS-MIB and CISCO-LWAPP-MIB. The PowerPack includes the following features:

- Dynamic Applications that discover and collect data from all Cisco WLC component devices monitored
- Event policies and corresponding alerts that are triggered when Cisco WLC component devices meet certain status criteria
- Device classes for each of the Cisco WLC component devices monitored
- Device dashboards that display information about Cisco WLC component devices

# Installing the Cisco: Wireless PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "Cisco: Wireless" PowerPack.

**TIP:** By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see the section on *Global Settings*.

**NOTE:** For details on upgrading Skylar One, see the relevant *Skylar One Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page at the ScienceLogic Support Center (Skylar One > PowerPacks, login required).
2. In Skylar One, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

**NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

# Chapter 2

# Configuration and Discovery

## Overview

The following sections describe how to configure and discover Cisco wireless LAN controllers for monitoring by Skylar One using the "Cisco: Wireless" PowerPack:

This chapter covers the following topics:


*Prerequisites for Monitoring Cisco Wireless LAN Controllers* ..... 6

*Configuring a Cisco WLC SNMP Credential* ..... 7

*Discovering Cisco WLC Devices* ..... 10

*Handling Device Failover* ..... 14

*Viewing Cisco WLC Component Devices* ..... 17


## Prerequisites for Monitoring Cisco Wireless LAN Controllers

Before you can monitor Cisco wireless LAN controllers using the "Cisco: Wireless" PowerPack, you must have the following information:

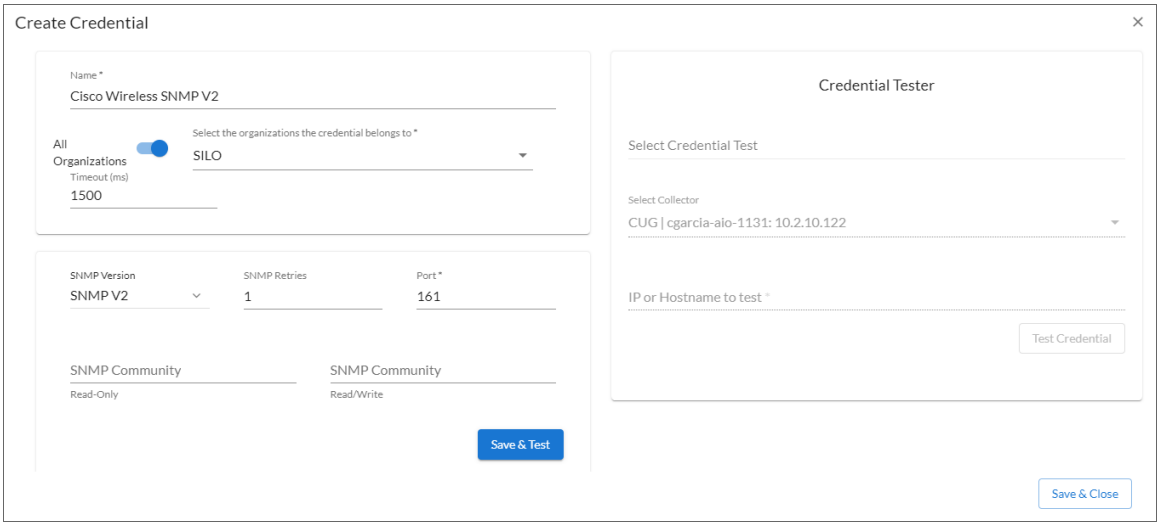
- The IP address of the WLC that you want to monitor with Skylar One
- The settings for an SNMP V2 or SNMP V3 credential that can be used to communicate with the WLC

# Configuring a Cisco WLC SNMP Credential

To configure Skylar One to monitor a Cisco WLC, you must first create a SNMP V2 or SNMP V3 credential. This credential allows the Dynamic Applications in the "Cisco: Wireless" PowerPack to communicate with the WLC.

To create an SNMP credential for monitoring a WLC:

1. Go to the **Credential Manager** page (Manage > Credentials).
2. Click **[Create New]**, and then select *SNMP Credential*. The **Create Credential** page appears:




3. Supply values in the following fields:

- ***Name***. Type a new name for the credential.
- ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
- ***Timeout (ms)***. Time, in milliseconds, after which Skylar One will stop trying to communicate with the device from which you want to retrieve data.
- ***SNMP Version***. Select *SNMP V2* (default) or *SNMP V3* for enhanced security.

**NOTE**: Do not use an SNMP V1 credential for monitoring a WLC. Using an SNMP V1 credential will decrease the performance of the data collection process.

  - If you selected *SNMP V2*, type the community string for the WLC in the ***SNMP Community (Read Only)*** field.

- If you selected *SNMP V3*, supply values in the following fields:
  - ***Security Name***. Type the SNMP username for the WLC.
  - ***Security Passphrase***. Type the passphrase for the SNMP user.
  - ***Authentication Protocol***. If applicable, select the authentication protocol for the SNMP user.
  - ***Security Level***. If applicable, select the security level that is applicable to the SNMP user.
  - ***Engine ID***. If applicable, type the SNMP V3 Engine ID for the SNMP user.
  - ***Context***. If applicable, type the SNMP Context.
  - ***Privacy Protocol***. If applicable, select the privacy protocol for the SNMP user.
  - ***Privacy Protocol Pass Phrase***. If applicable, type the privacy protocol passphrase for the SNMP user.
  - ***Port***. Leave this field by default.
  - ***SNMP Retries***. Leave this field by default.

4. Click **[Save & Close]**.

## Configuring a Cisco WLC SNMP Credential in the Skylar One Classic User Interface

To configure Skylar One to monitor a Cisco WLC, you must first create a SNMP V2 or SNMP V3 credential. This credential allows the Dynamic Applications in the "Cisco: Wireless" PowerPack to communicate with the WLC.

To create an SNMP credential for monitoring a WLC:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]**, and then select *Create SNMP Credential*. The **Credential Editor** page appears.
3. Supply values for the following fields:

- ***Profile Name***. Type a name for the credential.
- ***Timeout (ms)***. Time, in milliseconds, after which Skylar One will stop trying to communicate with the device from which you want to retrieve data.
- ***SNMP Version***. Select *SNMP V2* (default) or *SNMP V3* for enhanced security.

**NOTE**: Do not use an SNMP V1 credential for monitoring a WLC. Using an SNMP V1 credential will decrease the performance of the data collection process.

- If you selected *SNMP V2*, type the community string for the WLC in the ***SNMP Community (Read Only)*** field.
- If you selected *SNMP V3*, supply values in the following fields:

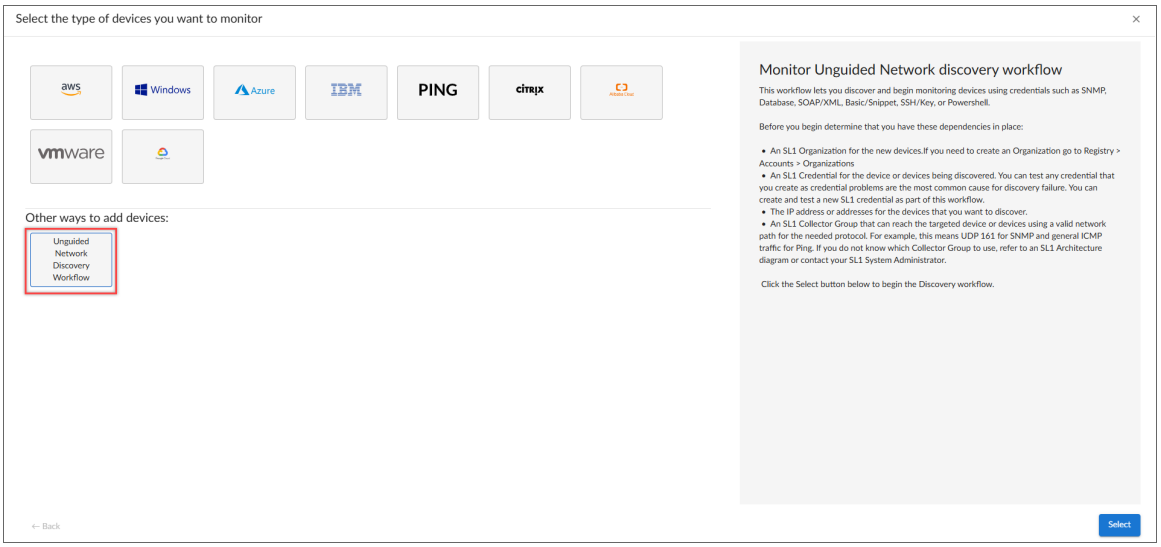
- ***Security Name***. Type the SNMP username for the WLC.
- ***Security Passphrase***. Type the passphrase for the SNMP user.
- ***Authentication Protocol***. If applicable, select the authentication protocol for the SNMP user.
- ***Security Level***. If applicable, select the security level that is applicable to the SNMP user.
- ***SNMP v3 Engine ID***. If applicable, type the SNMP V3 Engine ID for the SNMP user.
- ***Context Name***. If applicable, type the SNMP Context.
- ***Privacy Protocol***. If applicable, select the privacy protocol for the SNMP user.
- ***Privacy Protocol Pass Phrase***. If applicable, type the privacy protocol passphrase for the SNMP user.
- ***Port***. Leave this field by default.
- ***Retries***. Leave this field by default.

4. Click the **[Save]** button.

# Discovering Cisco WLC Devices

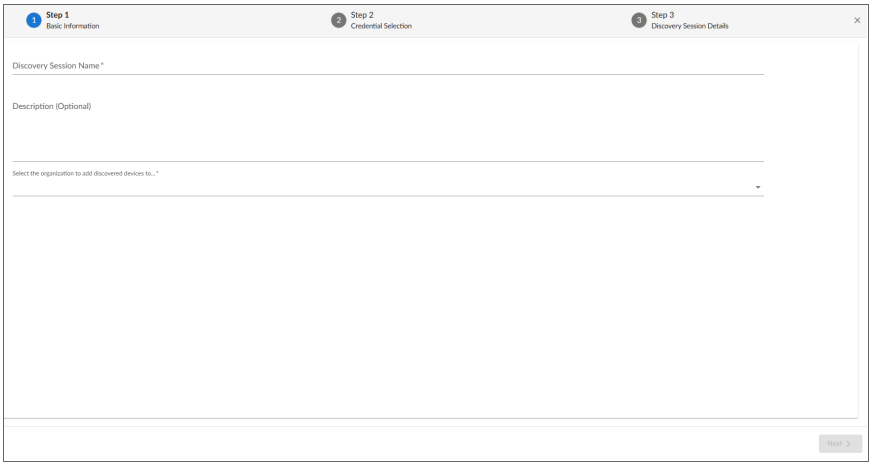
To discover Cisco WLC devices:

1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:




2. Click the **Unguided Network discovery workflow** button. Additional information about the requirements for discovery appear in the General Information pane to the right.

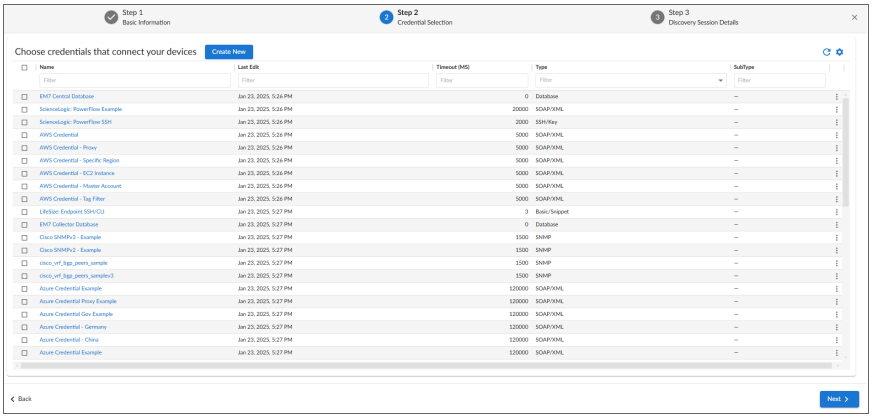
3. Click **[Select]**. The **Add Devices** page appears:



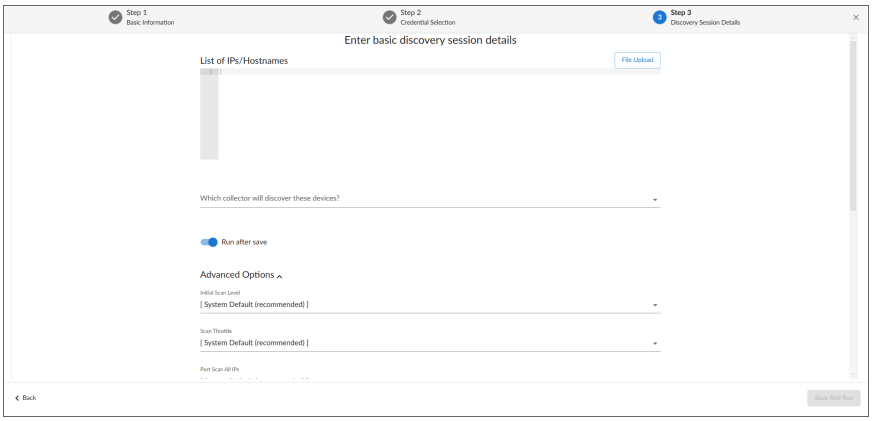

4. Complete the following fields:

- ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
- ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
- ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credentials** page of the **[Add Devices]** wizard appears:




6. On the **Credentials** page, locate and select the **SNMP credential** you created.
7. Click **[Next]**. The **Discovery Session Details** page of the **[Add Devices]** wizard appears:




8. Complete the following fields:
   - ***List of IPs/Hostnames***. Type the IP address for the WLC.
   - ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
   - ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.

     In the **Advanced options** section, click the down arrow icon ( ) to complete the following fields:
     - ***Model Devices***. Enable this setting.
9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Session ) displays the new discovery session.
10. If you selected the Run after save option on this page, the discovery session runs, and the Discovery Logs page displays any relevant log messages. If the discovery session locates and adds any devices, the Discovery Logs page includes a link to the Device Investigator page for the discovered device.

## Discovering Cisco WLC Devices in the Skylar One Classic User Interface

To discover Cisco WLC devices in the classic user interface:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears.
3. Supply values in the following fields:
   - ***Name***. Type a name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Type the IP address for the WLC.
   - ***SNMP Credentials***. Select the SNMP credential you created for the WLC.
4. Optionally, supply values in the other fields in this page. In most cases, you can use the default values for the other fields. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.

5. Click **[Save]**, then close the**Discovery Session Editor** page.
6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon ( ) for the discovery session you created.
7. In the pop-up window that appears, click **[OK]**. The **Discovery Session** page displays the progress of the discovery session.

## Verifying Discovery and Dynamic Application Alignment

To verify that Skylar One has automatically aligned the correct Dynamic Applications during discovery:

1. In the **Discovery Session** page, click the device icon ( ) for the newly discovered Cisco WLC device to view its **Device Properties** page.
2. From the **Device Properties** page for the Cisco WLC device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. The following Dynamic Applications should appear on the **Dynamic Application Collections** page for the WLC device:
    - *Cisco: WLC CPU*
    - *Cisco: WLC CPU and Memory Performance*
    - *Cisco: WLC Memory*
    - *Cisco: WLC System Counts*
    - *Cisco: WLC Configuration*
    - *Cisco: WLC Interface Performance Average*
    - *Cisco: WLC Interface Average*
    - *Cisco: WLC Noise Average*
    - *Cisco: WLC AP Discovery*

**NOTE**: It can take several minutes after discovery for Dynamic Applications to be automatically aligned to the controller device. If the listed Dynamic Applications do not display on this page, try clicking the **[Reset]** button.

## Manually Aligning Dynamic Applications

If the Dynamic Applications have not been automatically aligned, you can align them manually.

**NOTE**: The "Cisco: WLC Rogue AP" Dynamic Application, which can be used to collect information about rogue access points, is not automatically aligned during discovery. To use the "Cisco: WLC Rogue AP" Dynamic Application, follow the instructions in this section.

To manually align Dynamic Applications:

1. From the **Device Properties** page for the Cisco WLC device, click the **[Collections]** tab.
2. Click the **[Actions]** button and then select *Add Dynamic Applications*. The **Dynamic Application Alignment** page appears.
3. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
4. In the ***Credentials*** field, select the Cisco WLC SNMP credential.
5. Repeat steps 2-4 for the remaining Dynamic Applications you want to align with the device.
6. After aligning the Dynamic Applications, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Application. If collection for the Dynamic Application was successful, the graph icons ( ) for the Dynamic Application are enabled.

# Handling Device Failover

If you want to enable failover support of component devices between root-level Wireless controllers (or re-enable your own previously implemented custom support), you must follow the steps below:

1. Set the GUID (Globally Unique Identifier) for a collection object that is expected to be unique across the component devices. For the “Cisco: WLC AP Discovery” Dynamic Application, this is often the MAC address or Serial Number. For the “Cisco: WLC AP Interface Discovery” Dynamic Application, this is often the Interface Index.

    - Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
    - Type "Cisco: WLC AP Discovery" in the ***Dynamic Application Name*** column.
    - Click the wrench icon ( ) and then select the **[Collections]** tab. The **Collection Objects** page appears.
    - Click the wrench icon ( ) next to the collection object you want to set the GUID for.
    - Under ***Component Identifiers***, select *GUID (%G)*.
    - Click **[Save]**.

> **NOTE:** For failover support, the GUID component identifier must be set for both the “Cisco: WLC AP Discovery" and “Cisco: WLC AP Interface Discovery” Dynamic Applications, if both applications are enabled. If the “Cisco: WLC AP Interface Discovery” Dynamic Application is disabled, you only need to set the component identifier in the “Cisco: WLC AP Discovery" Dynamic Application.

2. Enable collection for the selected collection object. Many of the collection objects for the “Cisco: WLC AP Discovery” Dynamic Application do not collect data by default. To enable collection, the “Cisco: WLC AP Discovery” snippet code must be modified:

> **NOTE:** No additional collections need to be enabled in the "Cisco: WLC AP Discovery" Dynamic Application unless you are using one of those disabled collections as the GUID component identifier described in step 1.

- Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- Type "Cisco: WLC AP Discovery" in the ***Dynamic Application Name*** column.
- Click the wrench icon () and then select the **[Snippets]** tab. The **Snippet Editor & Registry** page appears.
- Click the wrench icon () next to ***Cisco: WLC AP Discovery***.
- Add the final index of the collection object’s SNMP OID to the `COLLECTED_OIDS` list at the top of the snippet. For example, to add the "Serial Number" collection object (which has an SNMP OID of ‘.1.3.6.1.4.1.14179.2.2.1.1.17’, and a final index of ’17’), the “COLLECTED_OIDS” list will go from `* COLLECTED_OIDS = ['6', '16', '3']` to `* COLLECTED_OIDS = ['6', '16', ‘3’, ’17']`
- Click **[Save]**.

> **WARNING:** ScienceLogic does not recommend enabling the "Cisco: WLC AP Interface Discovery" Dynamic Application in order to prevent potentially overloading the collector.

> **NOTE:** These Dynamic Application run every 2 hours by default. As a result, an access point that fails over to another controller may show as unavailable for up to that amount of time before moving to the new controller. This wait time can be reduced by decreasing the polling interval, however, these Dynamic Applications are resource intensive and should only be run at a higher rate if the collector is appropriately sized and has sufficient resources. The WLC controllers should be able to handle the additional SNMP walks as well before making such a change.

## Troubleshooting Duplicate Device Issues

If the Globally Unique Identifier (GUID) Component Identifier is already set to a different collection object (For example, “Serial Number”) in the "Cisco: WLC AP Discovery" Dynamic Application before upgrading to version 105 of the Cisco: Wireless" PowerPack, it will be removed upon upgrading to version 105.

If no GUID is set, components can be duplicated in a failover scenario where the component device moves from one Skylar One root device to another. If the GUID is set, the components should not be duplicated in a failover scenario.

**NOTE:** If duplicate components are created, the original devices may be automatically vanished, depending on the device settings and the global settings in the Skylar One System.

If components are discovered with the GUID component identifier set in a previous version, and the PowerPack is upgraded to 105, duplicate component devices should not be immediately created. However, if the GUID component identifier setting is not restored after the upgrade, you will see duplicate devices created in the event of a failover to another root device. If the GUID setting is restored after the upgrade, no duplicate components should be created upon a failover.

**NOTE:** If a controller and its components are discovered with a GUID component identifier set, and the GUID component identifier is subsequently changed to a different collection object, Skylar One will model the existing devices as new duplicate components using the new GUID value.

Additionally, if a GUID Component Identifier was set on the "Cisco: WLC AP Discovery" Dynamic Application before upgrading to version 105, the upgrade will also trigger Skylar One to re-model all Administration Portal component devices. During this device re-modeling, any SNMP credentials on Administration Portal child devices will be removed. This will cause the "Cisco: WLC Interference Average" Dynamic Application to fail with "Cache not found" errors.

To work around this issue, after upgrading to version 105, run the following SQL commands to restore the credentials on the affected Administration Portal child devices.

First, verify the affected rows by determining which credentials have been reset to zero:

```
SELECT mda.did, ld.device, mda.app_id, da.name, mda.cred_id

FROM master.map_dynamic_app_device_cred mda

JOIN master_dev.legend_device ld ON (ld.id = mda.did)

JOIN master.dynamic_app da ON (da.aid = mda.app_id)

WHERE mda.cred_id = 0

AND mda.did IN (

  SELECT component_did FROM master_dev.component_dev_map

  WHERE parent_did = <WLC_DEVICE_ID>

);
```

Next, apply the workaround:

```
UPDATE master.map_dynamic_app_device_cred

SET cred_id = <YOUR_CREDENTIAL_ID>
```

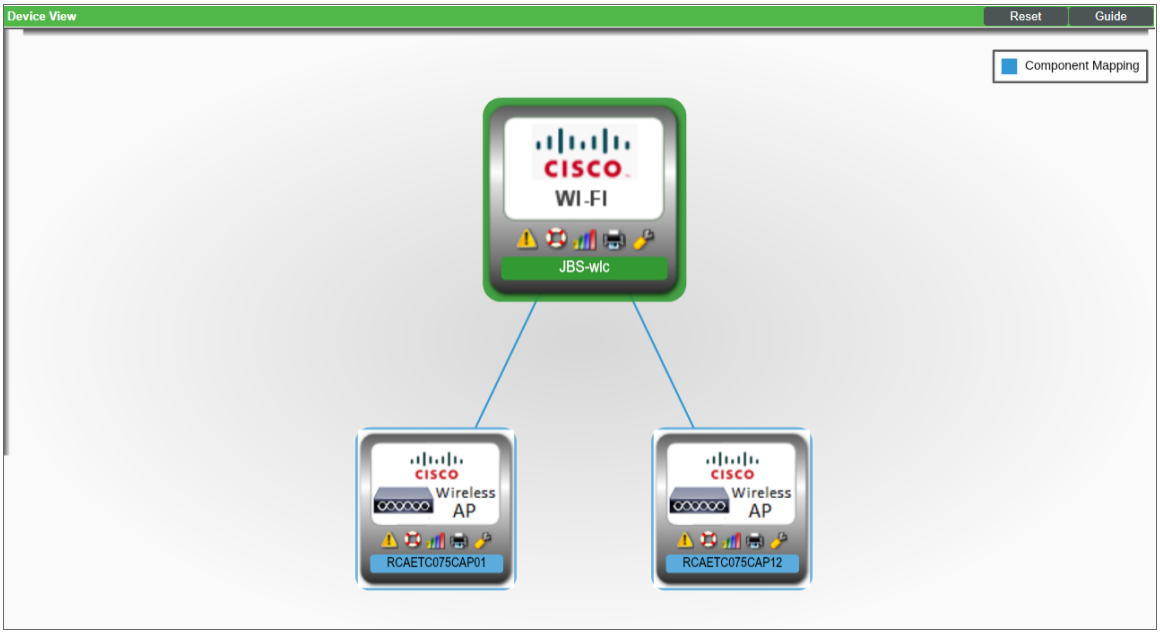
```
WHERE cred_id = 0

AND did IN (

  SELECT component_did FROM master_dev.component_dev_map

  WHERE parent_did = <WLC_DEVICE_ID>

);
```

After applying this fix, wait two to three polling cycles before verifying the Dynamic Application collection is working properly.

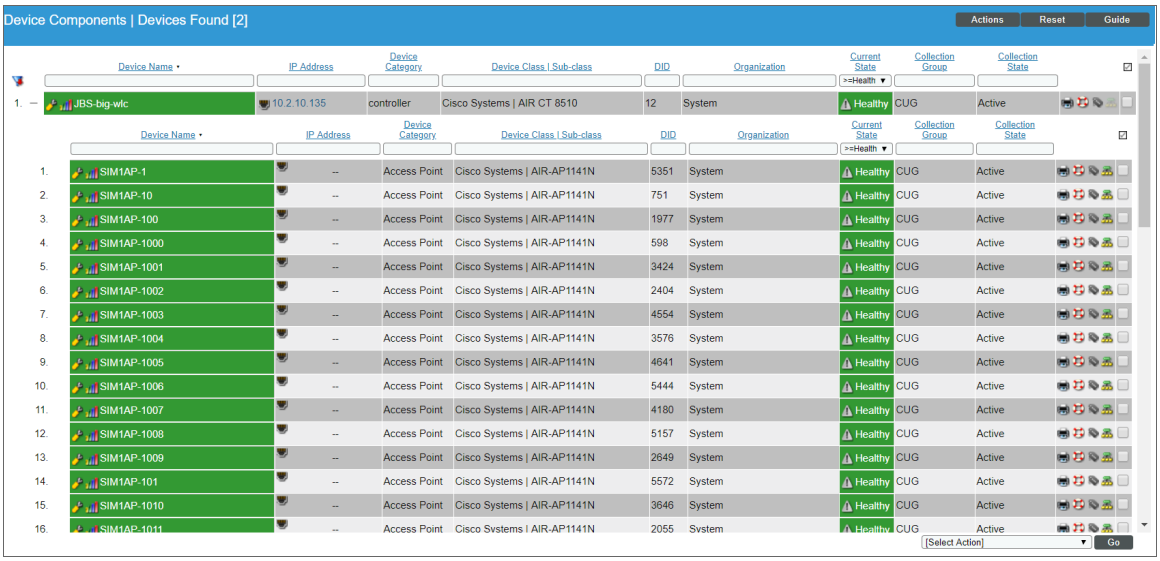
## Viewing Cisco WLC Component Devices

In addition to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), you can view the Cisco WLC device and all associated component devices in the following places in the user interface:

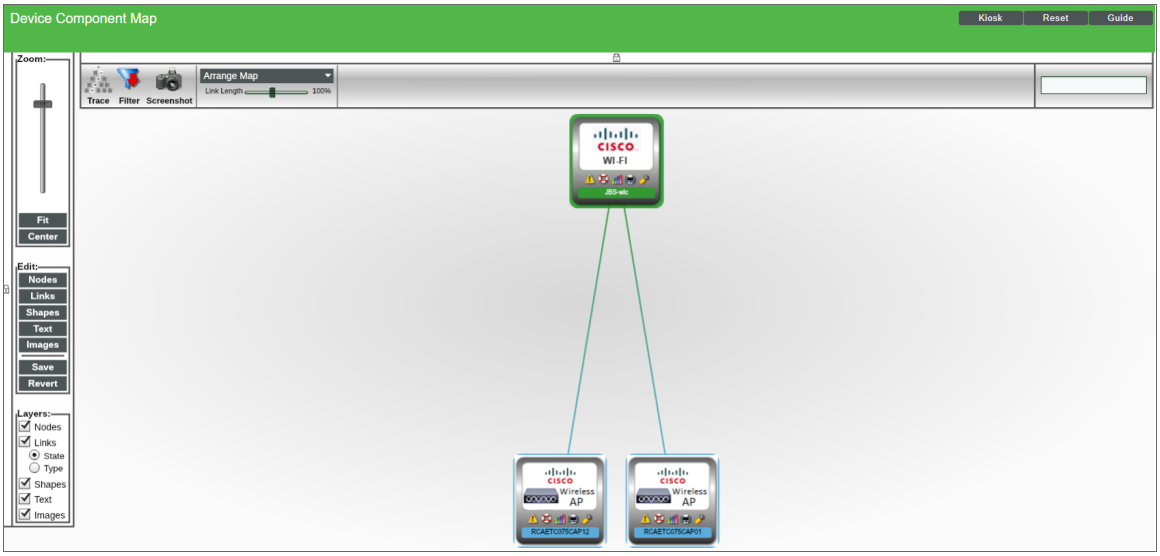
- The **Device View** page displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by Skylar One in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a Cisco WLC, click its plus icon (**+**):




- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. Skylar One automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a Cisco WLC, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



# Chapter 3

# Dashboards

## Overview

The following sections describe the device dashboards that are included in the "Cisco: Wireless" PowerPack:

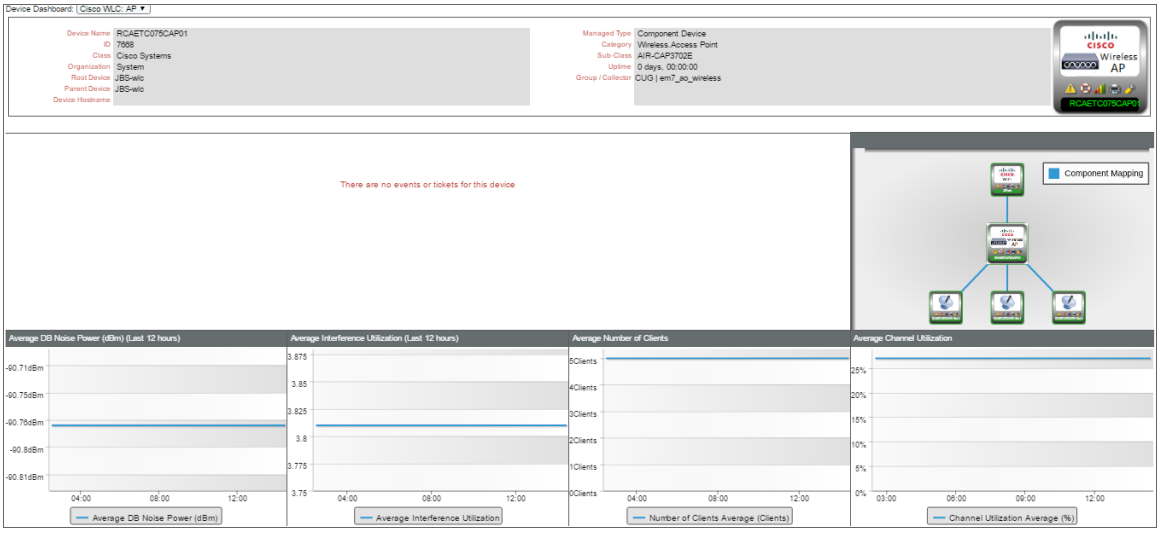
This chapter covers the following topics:

*Device Dashboards* ..... *19*

## Device Dashboards

The "Cisco: Wireless" PowerPack includes device dashboards that provide summary information for Cisco WLC component devices. Each of the device dashboards in the "Cisco: Wireless" PowerPack is set as the default device dashboard for the equivalent device class.

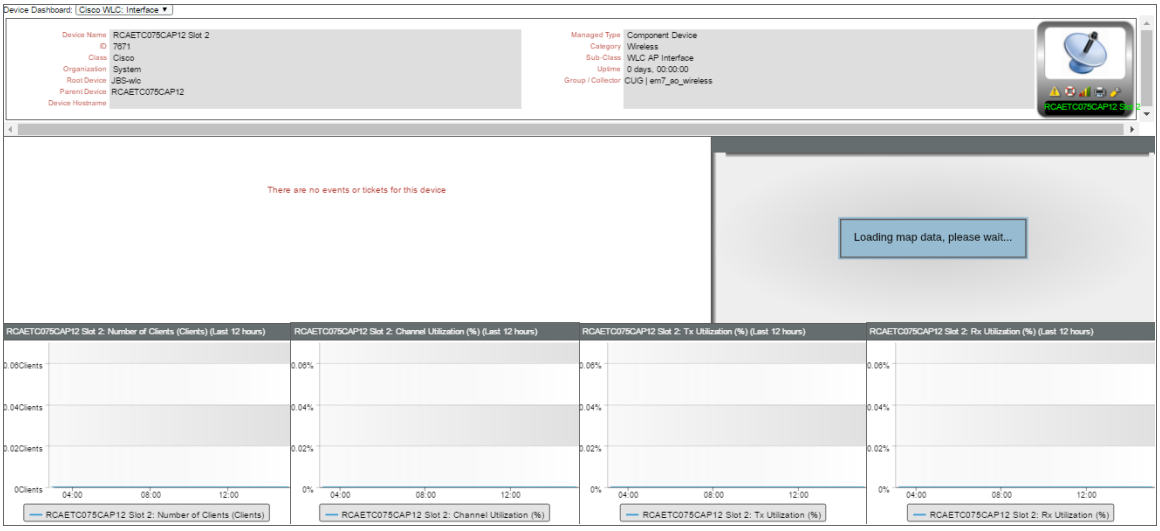
## Cisco WLC: AP Dashboard




The Cisco WLC: AP device dashboard displays the following information about Cisco wireless access points:

- Events and tickets on the device
- A component map
- Average decibel (dB) noise over the past 12 hours
- Average interface utilization over the past 12 hours
- Average number of clients across all interfaces on the access point for the most recent poll
- Average channel utilization across all interfaces on the access point for the most recent poll

## Cisco WLC: Interface Dashboard



The Cisco WLC: Interface dashboard displays the following information about Cisco wireless access point interfaces:

- Events and tickets on the device
- A component map
- Number of clients over the past 12 hours
- Channel utilization over the past 12 hours
- Tx utilization over the past 12 hours
- Rx utilization over the past 12 hours

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information herein, the information provided in this document may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described herein at any time without notice.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010