# ılıılı cısco

Deployment Guide



# Cisco Prime Infrastructure

Deployment Guide

November 2013

Scope	5
Introduction	5
Installation	6
Prerequisites	7
Server Requirements	7
Client Requirements	8
Server Sizing Matrix	8
Installing the Cisco Prime Infrastructure Virtual Appliance	9
Installing Cisco Prime Infrastructure on a Physical Appliance	9
Starting/Stopping Cisco Prime Infrastructure Services	9
Logging In to Cisco Prime Infrastructure for the First Time	9
Accessing Cisco Prime Infrastructure Through the CLI	10
How to Enable the CLI Root User in the Cisco Prime Infrastructure Server	10
Verifying IOPS for Cisco Prime Infrastructure Virtual Machine	10
<u>Configuring Backup</u>	11
Advanced System Settings	11
Data Retention	11
High Availability	11
HA Setup	12
Licensing	12
Cisco Prime Infrastructure High Availability Setup	12
HA Modes	12
Failover	12
Failback	12
Manual/Automatic Options	13
Automatic Failover	13
Primary Failure Example - Manual Failover	13
Upgrade and Data Migration from Previous Versions	14
Upgrading to Cisco Prime Infrastructure 2.0	14
Migrating from NCS 1.1.1.24 to Cisco Prime Infrastructure 2.0	15
Migrating from WCS 7.x to NCS 1.1.1.24	15
From LMS	15
LMS 2.x	15
LMS 3.x	16
LMS 4.x	16
Exporting Inventory from LMS 4.2.4 and Later	16
Importing into Cisco Prime Infrastructure 2.0.	16
LMS 4.2 Data Migration	17
Cisco Prime Infrastructure Device Packs and Software Updates	18
Application Setup	19
Lifecycle Management	19
Design	19
Deploy	19
Operate	19
Report	19
Administer	20
Creating Groupings and Sites	20
Create Sites	20
Import/Edit Maps from WCS/NCS to Cisco Prime Infrastructure	20

Associate Endpoints to Sites	21
Create Port Groups	21
Users and User Group Management	22
Adding New Users	22
Creating User Groups	23
Image Management Settings	23
Configuration Archive Settings	24
Configuring NTP and DNS for NAMs	25
Connection to Cisco.com	25
<u>Floxy Settings</u>	20
Cisco.com Settings	20
Planning/Preparing the Network	26
Wireless Planning Tool	26
Ports Used	27
Protocol Check	27
Configuring SNMP	28
Enabling SNMP on Wireless Controllers	28
Enabling SNMP on Routers/Switches	28
Enabling Telnet/SSH on Routers/Switches	28
Enabling Telnet/SSH on Wireless Controllers	28
HTTP/HTTPS	28
Preparing the Wireless Network	29
Import Maps from WCS	29
Discovering Your Network	29
Discover Devices	29
Create a New Discovery Profile	30
Configuring Cisco Discovery Protocol/LLDP	31
Filtering	31
Credentials	31
Discover the Network	32
Scheduling Ongoing Discovery	32
Validate Discovery	32
Device Work Center	32
Fixing Credential Errors	33
Importing Devices Manually.	34
Automating Branch Device Deployment	34
Deploying Wireless and Advanced Instrumentation	34
Deploy a WI AN Using a Configuration Template	3/
NetFlow.	35
Check Whether NetFlow Data Are Coming or Not	37
Medianet	37
Enabling Medianet	38
Check Whether Medianet Is Enabled	38
Monitoring(Troubleshooting	30
Basis Manifering	
Basic Monitoring	39
Interface Statistics	
Design Custom Monitoring Templates	<del>4</del> 0 40
Design Custom Monitoring Templates	<del>4</del> 0 11
Deploy Custom womening remplates	4 I
	10
Turning on Advanced Monitoring	42
Turning on Advanced Monitoring	42 42
Turning on Advanced Monitoring <u>NetFlow</u> WAN Optimization - Cisco Wide Area Application Services	42 42 43

Monitor/Troubleshoot a Wireless Network	
RRM/Clean Air	
Build RF Profile	
Apply RF Profiles to AP Groups	
Monitor/Troubleshoot Clients and Users	
Client Visibility	
Wireless Clients	51
Test Analysis Tool (CCXv5 Clients)	
Wired Clients	
Alarms and Events	
Quick Filter	
Creating Advanced Filter	
Trigger Packet Capture from Cisco Prime Infrastructure	
Manual Packet Capture from Cisco Prime Infrastructure	
Automating Packet Capture Using Cisco Prime Infrastructure	
Decoding Packet Capture Using Cisco Prime Infrastructure	
Miscellaneous Multi-NAM Capabilities Within Cisco Prime Infrastructure	57
Remediate Issues	57
Remediate Wireless Issues	57
Remediate Wired Issues	
Optimize	
Use Cisco Prime Infrastructure to Optimize the Operation of Your Converged Network	58
Dashboard Customization	
Customizing the Dashlet Content	60
Advance Configuration Topics	61
Identity Services Engine Integration	61
Automated Deployment	61
Managing Converged Access Using Cisco Prime Infrastructure 2.0	62
Step 1 - Setting Up a New Mobility Hierarchy Using Mobility Work Center	62
Step 2 - Create VLANs and WLANs for the New Mobility Architecture	64
Step 2a - Wizard-Based Guided Workflow for Creating VLANs and WLANs	64
Step 2b - Creating VLANs and WLANs Using Templates (Advance Mode)	
Working with Converged Access Devices in Cisco Prime Infrastructure	
Discovering Templates from Converged Access Devices	72
Monitoring Converged Access Switches	73
References	
Cisco Prime Infrastructure 2.0 Links	
Cisco Product Pages	75
Ordering and Licensing	75
Related Deployment Guides	

# Scope

This document is meant to be used for successfully deploying Cisco Prime<sup>™</sup> Infrastructure. The assumption is that the basic wired and wireless network is already deployed. Cisco Prime Infrastructure will be used to manage, modify, or enhance the existing network. This guide has been updated for Cisco Prime Infrastructure 2.0.

# Introduction

Combining the wireless functionality of Cisco Prime Network Control System (NCS) with Cisco Prime LAN Management Solution (LMS), Cisco Prime Infrastructure simplifies and automates many of the day-to-day tasks associated with deploying, maintaining, and managing the end-to-end network infrastructure from a single pane of glass. The new converged solution delivers many of the existing wireless capabilities for RF management, user access, reporting, and troubleshooting along with wired lifecycle functions such as discovery, inventory, configuration and image management, plug and play, integrated best practices, and reporting.



The image above shows a typical network diagram of a global enterprise that has many sites with varying sizes. You may see traffic coming from one site to another, as well as to and from sites to headquarters. How can we measure which site is consuming most of the WAN bandwidth? Which site has the worst user experience from an application point of view? Which site has more wired clients compared to wireless clients? This is just a partial list of questions that a network engineer could have and that can be easily answered with Cisco Prime Infrastructure.



If you have an Assurance add-on license, you will be able to get an aggregated view from all the data sources in your network as shown in the following figure:

As we can see, Cisco Prime Infrastructure polls some of the devices using Simple Network Management Protocol (SNMP), and collects NetFlow from other data sources directly. In case of Cisco Prime Network Analysis Module (NAM), Cisco Prime Infrastructure collects all the information from the NAM natively. However, the NetFlow Generation Appliance (NGA) sends NetFlow to Cisco Prime Infrastructure. Routers and switches capable of NetFlow and medianet can be enabled and configured by Cisco Prime Infrastructure to get application visibility for the ones that flow through them.

# Installation

The Cisco Prime Infrastructure software runs on either a dedicated Cisco Prime Appliance (PRIME-NCS-APL-K9) or on any server running VMware ESX/ESXi. The Cisco Prime Infrastructure software image does not support the installation of any other packages or applications on this dedicated platform. The Cisco Prime Infrastructure application comes preinstalled on a physical appliance with various performance characteristics.

# Prerequisites

Cisco Prime Infrastructure runs on a 64-bit, Red Hat Linux Enterprise Server 5.4 operating system. You cannot install Cisco Prime Infrastructure on a standalone operating system such as Red Hat Linux, as Cisco Prime Infrastructure is shipped as a physical or virtual appliance that comes preinstalled with a secure and hardened version of Red Hat Linux as its operating system.

#### Server Requirements

Cisco Prime Infrastructure has two deployment options: Virtual appliance in the form of an Open Virtualization Archive (OVA) file, and hardware appliance, also known as the Cisco Prime Appliance. The virtual appliance is an OVA file that can be deployed on ESXi 5.x (ESXi 4.x is not recommended due to file-size limitations). The following table lists the hardware requirements for the virtual appliance based on wired/wireless scale.

Virtual Appliance Size	Virtual CPU (vCPU) <sup>***</sup>	Memory (DRAM)	HDD Size	Throughput (Disk I/O) <sup>**</sup>	Max Concurrent Clients/Users	API Clients
Express	4	12 GB	300 GB	200 MBps	5	2
Custom Express <sup>*</sup>	8	16 GB	600 GB	200 MBps	5	2
Standard	16	16 GB	900 GB	200 MBps	25	5
Pro	16	24 GB	1200 GB	200 MBps	25	5

Custom Express is not a separate OVA. You can take the Express OVA and customize it with the parameters for Custom Express mentioned in the preceding table.

Refer to "Logging In to Cisco Prime Infrastructure for the First Time" for more details on calculating IOPS.

VMware refers to CPU as pCPU and vCPU. pCPU or 'physical' CPU in its simplest terms refers to a physical CPU core i.e. a physical hardware execution context (HEC) if hyper-threading is unavailable or disabled. If hyperthreading has been enabled then a pCPU would constitute a logical CPU. This is because hyperthreading enables a single processor core to act like two processors i.e. logical processors. So for example, if an ESX 8-core server has hyper-threading enabled it would have 16 threads that appear as 16 logical processors and that would constitute 16 pCPUs." So in PI when we say vCPU, we mean Numbers of Threads (assuming Hypter-threading is enabled) that are available for execution to the actual VM. So a 2, quad core, hyper-threading enabled CPUs on the host will give the 16vCPUs to vmware. [2 x 4 (Quad Core) = 8; 8 x 2 (for HT) = 16].

#### **Special Sizing Note:**

- If you have been using a **Medium OVA** from prior versions of Cisco Prime Infrastructure (1.2 or 1.3), and have the same number of devices to manage with Cisco Prime Infrastructure 2.0 without significant change in your usage, you can upgrade to Cisco Prime Infrastructure 2.0. You do not have to increase the resource pool for the OVA in this case.
- Cisco Prime Appliance is equivalent to a standard virtual appliance for sizing purposes. If you are currently
  using the Cisco Prime Appliance to manage more devices than is supported under standard, and have not
  significantly added more devices or turned on new features, you can continue to use the Cisco Prime
  Appliance to manage these devices.

Cisco Prime Appliance comes with the specifications shown in the following table:

Physical Appliance	Physical CPU	Memory (DRAM)	HDD Size	Throughput (Disk I/O)	Max Concurrent Clients/Users	API Clients
Cisco Prime Appliance	8 Cores (16 Threads)	32 GB	900 GB (4x300GB RAID5)	200 MBps	25	5

#### **Client Requirements**

The following table shows all the supported browsers that can be used to access Cisco Prime Infrastructure. Please use the <u>Cisco Prime Infrastructure 2.0 Quick Start Guide</u> for the latest client requirements.

Supported Browser	Browser Version	Additional Notes
Internet Explorer	8.0 or 9.0	Microsoft Internet Explorer 8.0 or 9.0 with <u>Google Chrome Frame plug-in</u> (users logging in to the simplified Lobby Ambassador interface do not need the plug-in).
Mozilla Firefox	Firefox 22 or later	Latest Firefox version may be used, but it may not be tested depending on when it was released.
Mozilla Firefox ESR	ESR 10 or ESR 17	ESR is the more stable version with less frequent updates. <u>Mozilla Firefox ESR</u> 10 or ESR 17 ( <u>ESR 17 is recommended</u> ).
Google Chrome	Chrome 27 or later	Latest Chrome version may be used, but it may not be tested depending on when it was released.

## TIP:

- It is strongly recommended to use a client with at least 4 GB or more. Adding more memory will definitely enhance the end-user experience.
- If you experience any issues with some of the pages not showing up, please try clearing the browser and flash cache as well as installing the latest version of flash available.

#### Server Sizing Matrix

The following table should help users to pick the right OVA size image for Cisco Prime Infrastructure Virtual Appliance. Users with Cisco Prime Appliance (physical) should use the "Standard" column:

Device Type	Express	Custom Express	Standard	Pro
Network Devices				
Max Unified APs	300	2,500	5,000	20,000
Max Wired Devices	300	1,000	6,000	13,000
Max Autonomous APs	300	500	3,000	3,000
Max NAMs	5	5	500	1,000
Clients				
Max Wireless (Roaming) Clients	4,000	30,000	75,000	200,000
Max Changing (Transient) Clients	1,000	5,000	25,000	40,000
Max Wired Clients	6,000	50,000	50,000	50,000
Monitoring				
Max Interfaces	12,000	50,000	250,000	350,000
Max NetFlow Rate (flows/sec)	3,000	3,000	16,000	80,000
Max Events (events/sec)	100	100	300	1,000
Max NAM Data Polling Enabled	5	5	20	40
System				
Max Number of Sites per Campus	200	500	2,500	2,500
Max Virtual Domains	100	500	1,000	1,000
<ul> <li>Max Groups (Total): User-Defined + Out of the Box + Device Groups + Port Groups</li> </ul>	50	100	150	150
Max Concurrent GUI Clients	5	10	25	25
Max Concurrent API Clients	2	2	5	5

<sup>\*</sup> Custom Express is not a separate OVA. You can take the Express OVA and customize it with the parameters for Custom Express mentioned in the preceding table.

Please use the Cisco Prime Infrastructure 2.0 Quick Start Guide for the latest sizing information.

# Installing the Cisco Prime Infrastructure Virtual Appliance

Cisco Prime Infrastructure is delivered as a virtual appliance or <u>OVA</u> file. OVA files allow you to easily deploy a prepackaged virtual machine (VM) - an application along with a database and an operating system. Please follow the link below for detailed instruction on installing Cisco Prime Infrastructure Virtual Application.

- Installing Cisco Prime Infrastructure
- Before You Begin
- Deploying the OVA from the VMware vSphere Client
- Installing the Server

# Installing Cisco Prime Infrastructure on a Physical Appliance

Cisco Prime Infrastructure 2.0 comes preinstalled on the PRIME-NCS-APL-K9 physical appliance. The Cisco Prime Infrastructure 2.0 software image does not support the installation of any other packages or applications on this dedicated platform. If for some reason the appliance comes without any software, the application may be installed from the DVD that comes with it. Once the server boots up, the procedure will be similar to the procedure described for a virtual appliance. More information on installing Cisco Prime Infrastructure on a physical appliance can be found at

http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/install/guide/Cisco\_PI\_Hardware\_Appliance\_I nstallation\_Guide.html.

#### Starting/Stopping Cisco Prime Infrastructure Services

In normal circumstances, you will not have to stop or start NCS services. The services will start automatically once installation is complete, and no manual startup of services is required. If there is a need to restart the services for some reason, the following commands may be executed by the admin user from the command-line interface (CLI):

pi1.cisco.com/admin# **ncs stop** - Stops the Cisco Prime Infrastructure server pi1.cisco.com/admin# **ncs status** - Shows the Cisco Prime Infrastructure server status pi1.cisco.com/admin# **ncs start** - Starts the Cisco Prime Infrastructure server

# Logging In to Cisco Prime Infrastructure for the First Time

Once the Cisco Prime Infrastructure server has been installed and configured, it is now ready to be accessed from the web. The server URL would be https://server\_hostname or https://ip.ad.dr.ess. In Cisco Prime Infrastructure 2.0, log in using the following credential for the very first time:

#### Username: root

Password: <the root password is the one that was entered during the install script>

After the server has been configured, it is advisable to log in with a non-root user to keep the root user for system level configurations as and when needed. More updated information can be found at Cisco Prime Infrastructure 2.0 Quick Start Guide at Logging into the Cisco Prime Infrastructure User Interface.

# Accessing Cisco Prime Infrastructure Through the CLI

In normal circumstances, you may not need to access the CLI, but if there is a need for access to some service requirements, the Cisco Prime Infrastructure server may be accessed through Secure Shell Protocol Version 2 (SSH2) by the admin user. The admin user is provided with a Cisco IOS<sup>®</sup> Software-like shell, which is the preferred shell for carrying out most operational tasks. The password for this admin user is configured during the initial installation and configuration, as mentioned in the "Installing the Cisco Prime Infrastructure OVA" section. Please note that the root password that is prompted in the install script is **only** for web access and not access to the CLI.

#### How to Enable the CLI Root User in the Cisco Prime Infrastructure Server

The root user is **not** enabled by default, but you can enable the root user for the first time using the **root\_enable** command at the admin console. Once the root user is enabled, log out of the admin shell and log in using the **root** user and the previously defined password for root.

#### Verifying IOPS for Cisco Prime Infrastructure Virtual Machine

Until Cisco Prime Infrastructure 1.3, there was no easy way to verify data store IOPS (input/output operations per second) for the virtual infrastructure. With the addition of the following new command, users can now verify the raw performance before proceeding any further. Here is how to use the command (from the root shell):

```
pi20-test5/admin# ncs run test iops
Testing disk write speed ...
8388608+0 records in
8388608+0 records out
8589934592 bytes (8.6 GB) copied, 128.195 seconds, 67.0 MB/s
```

Note that the recommended value for the IOPS is 200 MBps as mentioned in the server requirement section.

# Licensing

Type	Licensed
VUDI	PRIME-NCS-VAPL;pi1:af4ee9e0-ec0d-11e1-82f1-005056857f2f
Product Id	PRIME-NCS-VAPL
Serial Number	pj1:af4ee9e0-ec0d-11e1-82f1-005056857f2f

After you have installed Cisco Prime Infrastructure for the first time you may access the lifecycle and assurance features using the built-in evaluation license that is available by default. The default evaluation license is valid for 60 days for 100 devices. To continue using the system, you will need to purchase the base license and the corresponding feature license before the evaluation license expires. Cisco Prime Infrastructure 2.0 can be ordered through a Cisco partner, distributor, or using the standard Cisco<sup>®</sup> ordering tools at

http://www.cisco.com/go/ordering. More information about getting the license files can be found in the <u>Cisco Prime</u> Infrastructure 2.0 Ordering and Licensing Guide. Cisco Prime Infrastructure licenses are locked to a specific Cisco Prime Infrastructure instance based on a unique device identifier (UDI) for a physical appliance or a virtual unique device identifier (VUDI) for a virtual appliance (figure above). The identifier can be found within the Cisco Prime Infrastructure user interface under Administration > Licenses. Once you have obtained the license file (.lic), you are now ready to apply it. License files can be added to Cisco Prime Infrastructure by going to Administration > Licenses > Files > License Files. The license files should look like the figure on the right. For more information on Cisco Prime Infrastructure licensing you can also refer to the <u>Cisco Prime Infrastructure 2.0 Quick Start Guide</u>.

AURINIZARIOLE & FIGUREZ & LINEZ & FIGURE LINEZ							
	License ID	Feature	Device Limit	Туре			
	tm2	Lifecycle	10000	Permanent			
	tm1	Base	10000	Permanent			
	tm3	Assurance	10000	Permanent			

# **Configuring Backup**

At this point, you do not have any data, but soon you will start accumulating lots of data. It is strongly advisable to configure the backup plan in a more proactive manner. Backup can be configured by navigating to Administration > Background Tasks > Other Background Tasks (Section) > Prime Infrastructure Server Backup. You can either use the default repository, default Repo, or create an external backup repository by clicking the Submit button as shown in the figure (below). Enter FTP credentials and other relevant information to create this new remote backup repository.

Create Backu	p Repository	×
Name	FTPRepo	
Type	🗹 FTP Repository	
FTP Location	192.168.138.135	P
Username	eset	
Password	••••••	
Submit Car	ncel	

#### **Advanced System Settings**

There are some settings in Cisco Prime Infrastructure that need to be looked at closely before you start to manage the network. Optimal settings are already configured, but you may need to tweak the settings based on the network you are managing. You can access the settings by navigating to Administration > System Settings.

#### **Data Retention**

This menu item (Administration > System Settings) allows you to specify how much data is to be stored in Cisco Prime Infrastructure. By default you can store up to 7 days of raw data and 1 year's worth of aggregated data. You can increase these numbers based on the hard drive space that is provided to Cisco Prime Infrastructure. You can find more details on such system settings in <u>Cisco Prime Infrastructure Best Practices</u>.

#### **High Availability**

The Cisco Prime Infrastructure High Availability (HA) implementation allows one primary Cisco Prime Infrastructure server to failover to one secondary (backup) Cisco Prime Infrastructure server. A second server is required that has sufficient resources (CPU, hard drive, network connection) in order to take over Cisco Prime Infrastructure operation in the event that the primary Cisco Prime Infrastructure system fails. In Cisco Prime Infrastructure, the only HA configuration is supported is 1:1 - 1 primary system, 1 secondary system.

The size of the secondary server must be larger than or equal to that of the primary server; for example, if the primary Cisco Prime Infrastructure server is the medium OVA, then the secondary Cisco Prime Infrastructure server must be the medium or large OVA.

#### **HA Setup**

The primary and secondary server can be a mix of a physical and a virtual appliance. For example, if the primary Cisco Prime Infrastructure server is a physical appliance, the secondary server can be either a physical appliance or a large OVA virtual appliance; for example, the server configuration and sizing of large OVA is the same as the physical appliance. Customers must be running the same version of Cisco Prime Infrastructure on both the primary and secondary Cisco Prime Infrastructure servers. The Cisco Prime Infrastructure HA feature is transparent to the wireless controller, that is, there is no software version requirement for the Cisco Wireless LAN Controller (WLC), access points (APs), and the Cisco Mobility Services Engine (MSE).

#### Licensing

A RTU (tight-to-use) license is required to deploy Cisco Prime Infrastructure in an HA implementation. Apart from this, only one Cisco Prime Infrastructure server license needs to be purchased. There is no need to purchase a license for the secondary Cisco Prime Infrastructure server. The secondary server will use the license from the primary when a failover occurs. The secondary node will simulate the UDI information of the primary; thus the secondary server will be able to use the synchronized license from the primary server when the secondary server is active. The same Cisco Prime Infrastructure license file resides on both the primary and secondary Cisco Prime Infrastructure servers. Since the Cisco Prime Infrastructure Java Virtual Machine (JVM) is only running on the primary or secondary (not both), the license file is only active on one system at a given point in time.

#### **Cisco Prime Infrastructure High Availability Setup**

Cisco Prime Infrastructure HA can also be deployed with geographic separation of the primary and secondary servers. This type of deployment is also known as disaster recovery or geographic redundancy.

# **HA Modes**

There are two HA modes: failover and failback. Let's take a look at each of them in detail.

#### Failover

After initial deployment of Cisco Prime Infrastructure, the entire configuration of the primary Cisco Prime Infrastructure server is replicated to the host of the secondary Cisco Prime Infrastructure server. During normal operation (that is, when the primary Cisco Prime Infrastructure server is operational), the database from the primary server is replicated to the secondary Cisco Prime Infrastructure server. In addition to the database replication, application data files are also replicated to the secondary Cisco Prime Infrastructure server. Replication frequency is 11 seconds (for real-time files) and 500 seconds (for batch files).

#### Failback

When the issues on the server that host the primary Cisco Prime Infrastructure server have been resolved, failback can be manually initiated. Once this is done, the screen is displayed on the secondary Cisco Prime Infrastructure server. When you initiate failback, the Cisco Prime Infrastructure database on the secondary Cisco Prime Infrastructure server and any other files that have changed since the secondary Cisco Prime Infrastructure server took over Cisco Prime Infrastructure operation are synchronized between the secondary and the primary Cisco Prime Infrastructure servers. Once database synchronization has been completed, the primary Cisco Prime Infrastructure JVM is started by the primary Health Monitor (HM). When the primary Cisco Prime Infrastructure JVM is running, the preceeding screen is displayed on the secondary HM.

Health M Settings	1onitor Details			
Status	Remote NCS IP Address	State	Failover Type	Actio
8	171.69.217.142	Primary Alone	automatic	None
ogging			Logs	
		Logging	Download Health Monitor Log E	ilos Download

#### Manual/Automatic Options

#### Automatic Failover

Automatic failover is a much simpler process. The configuration steps are the same except that automatic failover is selected. Once automatic failover is configured, the network administrator does not need to interact with the secondary HM in order for the failover operation to take place. Only during failback is human intervention required.

#### Primary Failure Example - Manual Failover

In this example, the secondary Cisco Prime Infrastructure server was configured with manual failover. For example, the network administrator is notified through email that the primary Cisco Prime Infrastructure server has experienced a down condition. The Health Monitor on the secondary Cisco Prime Infrastructure server detects the failure condition of the primary Cisco Prime Infrastructure server. Because manual failover has been configured, the network administrator needs to manually trigger the secondary Cisco Prime Infrastructure server to take over Cisco Prime Infrastructure functionality from the primary Cisco Prime Infrastructure server. This is done if you log in to the secondary HM. Even though the secondary Cisco Prime Infrastructure server is not running, you can connect to the secondary HM using the following syntax: https://<Secondary\_PI\_IP\_Address>:8082/.

The secondary HM displays messages in regard to events that are seen. Because manual failover has been configured, the secondary HM waits for the system administrator to invoke the failover process. Once manual failover has been chosen, the message is displayed as the secondary Cisco Prime Infrastructure server starts. Once the failover process has been completed, which means that the Cisco Prime Infrastructure database replication process is completed and the secondary Cisco Prime Infrastructure JVM process has started, then the secondary Cisco Prime Infrastructure server is the active Cisco Prime Infrastructure server.

Health Monitor on the secondary Cisco Prime Infrastructure server provides status information on both the primary and secondary Cisco Prime Infrastructure servers. Failback can be initiated through the secondary HM once the primary Cisco Prime Infrastructure server has recovered from the failure condition. **The failback process is always initiated manually** so as to avoid a flapping condition that can sometimes occur when there is a network connectivity problem. More details on how to deploy Cisco Prime Infrastructure 2.0 HA can be found at http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/administrator/guide/config\_HA.html.

# **Upgrade and Data Migration from Previous Versions**

Although it may sound trivial to upgrade from Cisco Prime Infrastructure 1.x, there are some instances where we still recommend users to continue using version 1.x. Please note that these recommendations are only specific to Cisco Prime Infrastructure 2.0, and may change once later versions are out in 2.x train.

- If you have been using Cisco Prime Infrastructure 1.x Small OVA, an inline upgrade to Cisco Prime Infrastructure 2.0 is not supported. Recommendation in this case is to migrate instead; that is, back up 1.x after applying the relevant patch and then restore onto a freshly installed Cisco Prime Infrastructure 2.0 Express OVA. You will most likely need to increase CPU/memory based on the new requirement for Cisco Prime Infrastructure 2.0 as mentioned in the preceding Server Sizing Matrix.
- If you are using Cisco Prime Infrastructure 1.3.x managing an AireOS 7.4-based wireless infrastructure, please continue to stay with the Cisco Prime Infrastructure 1.3.x train. Only if you are going to deploy Converged Access infrastructure do you then need to upgrade to Cisco Prime Infrastructure 2.0.
- If you are using Cisco Prime Infrastructure 1.4 managing an AireOS 7.5-based wireless infrastructure (due to 802.11ac support), please continue to stay with Cisco Prime Infrastructure 1.4 until the 1.4.1 train. The next significant release with AireOS 7.5 support would be Cisco Prime Infrastructure 2.1.

#### **Upgrading to Cisco Prime Infrastructure 2.0**

Users can upgrade to Cisco Prime Infrastructure 2.0 only from one of the following supported versions:

- Cisco Prime Infrastructure 1.3.0.20
- Cisco Prime Infrastructure 1.2.1.12

(You must first install available point patches as explained in Installing Point Patches.)

Cisco Prime Network Control System 1.1.1.24

(You must first install available point patches as explained in Installing Point Patches.)

Here is a good flow chart to guide you on the upgrade path:



**Patch Requirements:** If you are using NCS 1.1.1.24, you **MUST** apply the patch before beginning the upgrade process. You can find the more patch details at

http://www.cisco.com/en/US/docs/wireless/prime\_infrastructure/1.3/quickstart/guide/cpi\_qsg130.html#wp69624.

Note: It is strongly recommended best practice is to use "database restore" instead of an "in-line upgrade."

# Migrating from NCS 1.1.1.24 to Cisco Prime Infrastructure 2.0

To migrate to a new Cisco Prime Infrastructure 2.0 system, follow the process as described in the following links. Note that HA must be disabled before taking the backup and should only be enabled after the restore (<u>Restoring</u> <u>Cisco Prime Infrastructure Database in a High Availability Environment</u>) has been completed.

- <u>Taking Application Backups From the Interface</u>
- Installing Cisco Prime Infrastructure
- <u>Restoring From Application Backups</u>

# Migrating from WCS 7.x to NCS 1.1.1.24

Direct migration from WCS 7.x to Cisco Prime Infrastructure 2.0 is **NOT** possible. **We strongly recommend upgrading your WCS to 7.0.230.0 (for data integrity) or higher before attempting to migrate to NCS.** Users will first need to do an intermediary migration to NCS 1.1.1.24, and then do an inline upgrade (or migration) to Cisco Prime Infrastructure 2.0.

- Migrating WCS to NCS 1.1
  - Exporting WCS Data
  - Migrating WCS Data to NCS
  - Nonupgradable Data
  - Migrating WCS User Data to NCS 1.1 (for Multiple WCS Servers)
  - Upgrading Cisco Prime Infrastructure in a High Availability Environment

#### From LMS

Cisco Prime LMS features were reevaluated for usefulness, usability, and value. Some features are redesigned and have transitioned, some are on the road map, others are to be determined by customers, and a few are being deprecated. Also see the <u>Cisco Prime Infrastructure LMS Functional Support Reference</u> for details on which LMS data sets will be migrated or backed up into Cisco Prime Infrastructure 2.0.

# LMS 2.x

LMS 2.x has reached its end of life, and that is why upgrading from LMS 2.x to Cisco Prime Infrastructure 2.0 is not supported (nor is it recommended). Customers could export their device inventory into a comma-separated value (CSV) file for their own records. Alternatively customers can also start using Cisco Prime Infrastructure 2.0 for basic network management type features. Even though data migration is not possible, you should still be able to manage your network in no time starting with discovery from within Cisco Prime Infrastructure 2.0.

# LMS 3.x

LMS 3.x has also reached end of engineering. If you are currently using basic management features such as monitoring, configuration management, inventory management, software image management, and fault management, you should consider upgrading to Cisco Prime Infrastructure 2.0. Even though data migration is not possible, you should still be able to manage your network in no time starting with discovery from within Cisco Prime Infrastructure 2.0.

LMS 3.x customers requiring features like CiscoView, Layer 2 topology, IP service-level agreements (IP SLAs), and VLAN management are recommended to run Cisco Prime Infrastructure 2.0 as a separate server side by side until equivalent features are being migrated into Cisco Prime Infrastructure 2.0.

# LMS 4.x

LMS 4.x customers using basic management features like monitoring, syslogs, configuration management, inventory management, software image management, and fault management should consider migrating to Cisco Prime Infrastructure 2.0.

LMS 4.x customers requiring features like CiscoView, Layer 2 topology, IP SLAs, work centers, and VLAN management are recommended to run Cisco Prime Infrastructure 2.0 as a separate server side by side or to wait until all the features have been migrated into Cisco Prime Infrastructure 2.x.

# Exporting Inventory from LMS 4.2.4 and Later

With LMS 4.2.4 (and later releases), there is an easy way from the web interface to export the device list with credentials, which can then be consumed by Cisco Prime Infrastructure. The device list can be exported from Administration > Export Data to Cisco Prime Infrastructure (under System).

Then select Export Device List and Credentials from the export options as shown in the following figure:



#### Importing into Cisco Prime Infrastructure 2.0

Once you have the exported the device list with credentials from LMS 4.2.4, it can be imported into Cisco Prime Infrastructure 2.0 by navigating to Operation > Device Work Center > Bulk Import as shown in the following figure:

{/	Edit 💥 Delete 🦓 Syno	Groups & Sites 👻 😤 /	Add Device 😰 Bulk Import			Show	All	- 8
ξΠ	Device Name 🔹	Reachability	IP Address	Device Type	Collection Status	Collection Time	Software Version	2
10	3560-DC-1	🔄 Reachable	10.0.252.4	Cisco Catalyst 3560	Managed with Warnings	September 13, 2012	12.2(52)5E	j
(	27E0 DUV 1	Deachable	10.0.252.2	Ciaco 27E0 Chadlabl	Managad	Contombox 14, 2012	10 0/0E/CEE	5

#### LMS 4.2 Data Migration

If you have a need to migrate data from LMS 4.2.x, Cisco Prime Infrastructure 2.0 now allows you to import this successfully. The procedure for this is detailed as follows:

- As mentioned in the section "Exporting Inventory from LMS 4.2.4 and Later" go to Admin > Export data to Cisco Prime Infrastructure (Under System) to prepare LMS Data to be migrated. For migration choose the second option, "Export complete data of LMS". For more details refer to the following URL: <u>http://www.cisco.com/en/US/docs/net\_mgmt/ciscoworks\_lan\_management\_solution/4.2/user/guide/admin</u> /server.html#wp1234250
- Configure the repository on Cisco Prime Infrastructure 2.0. It can be local or remote. The repository indicates where the backup file is located. You may configure a local (as previously mentioned) repository or a remote repository as shown below:

```
ncs-br-n45/admin# config ter
Enter configuration commands, one per line. End with CNTL/Z.
ncs-br-n45/admin(config)# repository test
ncs-br-n45/admin(config-Repository)# url ftp://ipaddress/foldername
ncs-br-n45/admin(config-Repository)# end
ncs-br-n45/admin#
```

3. Once the repository is created, run the following command to see all the backup files:

#### admin# show repository <repository-name>

Import the LMS backup into Cisco Prime Infrastructure using the following command (in admin mode):

#### admin# Lms migrate repository <repository-name>

```
ncs/admin# lms migrate repository repo
Repository name : repo
Initiating LMS data restore . Please wait...
```

- 4. After Importing data from the LMS server to Cisco Prime Infrastructure 2.0, the restored data id categorized into four buckets:
- 1. Network data (mandatory)
  - DCR (Device Credential Repository) import
  - Static group import
  - Dynamic group import
  - · LMS users import
  - SWIM image import
  - User-defined templates
- 2. Settings (mandatory) MIBS Image import
- 3. User objects
- 4. Historic data (optional data)

Currently Cisco Prime Infrastructure 2.0 will only support import items 1 and 2 from the preceding list.

5. You will then be asked to enter the password for the .zip file (as shown below) that was created during export from LMS for security purposes.

```
Initiating LMS data restore . Please wait...
INFO: no staging url defined, using local space.
INFO: Backup Status : SUCCESS
Enter the password to unlock the zip file : **
```

6. You then need to enter Cisco Prime Infrastructure's web username and password to get the session for importing the LMS data.

```
Enter the Cisco Prime Infrastructure Login Username : root
Enter the Cisco Prime Infrastructure Login Password : *********
```

- Once the user has entered this command in the admin console, the system will validate the following conditions:
  - · Zip file validation
  - Check sum validation
  - · Backupcontents.xml it is used to display the buckets details

```
The following data types are available in the given exported data. Choose an option using comma separated values to migrate.
```

```
1 network
2 settings
3 All of the above
Enter an option or comma-separated options :3
```

 To migrate all the available data choose option 3 as shown above and let the system install Cisco Prime LMS 4.2.x data on your Cisco Prime Infrastructure 2.0 server.

#### **Cisco Prime Infrastructure Device Packs and Software Updates**

There was always the framework for allowing users to seamlessly download and install patches for Cisco Prime Infrastructure itself. Starting Cisco Prime Infrastructure 2.0, we will be pushing out patches using this mechanism. In order to check for software updates, navigate to **Administrator** > **Software Update** as shown in the figure (below).



Once you click that link, you will see the page as shown in the following figure. Going forward you will be able to check for software patches as well as device packs.



Simply click Check for Updates to see the availability. If available, select the update and click Install as shown in the preceding figure

# Application Setup

Cisco Prime Infrastructure 1.x introduced a new lifecycle approach to managing your wired and wireless infrastructure. There are five phases in this lifecycle: design, deploy, operate, report, and administer. The details for each of these phases are briefly described in the following section.

# Lifecycle Management

#### Design

In this phase, you can assess, plan, and create configurations required to roll out new network services and technologies. You can create templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation, automating the work required to use Cisco validated designs and best practices.

#### Deploy

In this phase, you can schedule the rollout and implementation of network changes. Changes may include published templates created in the design phase, software image updates, and support for user-initiated ad hoc changes and compliance updates. This accelerates service rollout, minimizes chances for errors, and is highly scalable.

#### Operate

In this phase, you can utilize preconfigured dashboards to provide up-to-date status monitoring on the overall health of the network. Simple one-click workflows and 360-degree views enhance troubleshooting and reduce the time to resolve network issues. Unified alarm displays with detailed forensics provide actionable information and the ability to automatically open service requests with the Cisco Technical Assistance Center (TAC).

#### Report

In this phase, you can provide a wide variety of preconfigured reports for up-to-date information on the network, including detailed inventory, configuration, compliance, audit, capacity, end of sale, security vulnerabilities, and many more. Reports can be scheduled or run immediately, emailed, or saved as PDFs for future viewing purposes.

#### Administer

In this phase, you can provide an easy-to-use set of workflows that help to maintain the health of the application and keep devices, users, and the software up to date, allowing the IT staff to focus on other important activities.

#### **Creating Groupings and Sites**

Cisco Prime Infrastructure provides a very easy way to map each of the devices into its own site. There is also an ability to create groups based on predefined rules or criteria. Let's take a look at how to create sites and groups in Cisco Prime Infrastructure to help visualize applications in an intuitive manner.

#### **Create Sites**

There are two way of creating sites. If your access points follow a very consistent naming convention, you can automatically create a site tree map based on the hostname. The image below shows how a device hostname separated by hyphens can be used as a delimiter to create a site map tree automatically.

Sample AF hame		LON-Oxford-1	-3500 💟
Delimiter		- Create	basic regex based on delimiter
Regular exp	pression	(.*)-(.*)-(.*)-	(.*)
See Exam	ples	Test	
latch the gro	oups of yo	our regular expre	ssion with Campus, Building, and Floo Resulting map name
Group 1	Campu	s 💌	LON
Group 1 Group 2	Campu: Building	s 💌	] LON ] Oxford
Group 1 Group 2 Group 3	Campu: Building Floor/C	s 🔹	] LON ] Oxford ] 1
Group 1 Group 2 Group 3 Group 4	Campus Building Floor/C	s 🔍 🔻	] LON ] Oxford ] 1 ] 3500

To create automatic site hierarchies go **to Design > Automatic Hierarchy Creation**. Enter the AP Hostname and a suitable regular expression (or generate one as mentioned in the tip below). Click **Test** to see how the site is created from the hostname. Change the pull-down to map to the appropriate campus, building, floor, device, and so on.

**TIP:** After entering a sample hostname for an AP, you can click **Create basic regex based on delimiter** to automatically generate the regular expression.

#### Import/Edit Maps from WCS/NCS to Cisco Prime Infrastructure

If you have already created sites for the wireless network in a previous version of WCS or NCS, you can export from those applications and import the information into Cisco Prime Infrastructure as well. You can go to **Design > Site Map Design > Import Maps > Choose File** (as shown in figure below). Once the file has been uploaded, all the sites will be automatically created by Cisco Prime Infrastructure.

Import Ma	ар
Monitor > Map	s > Import Map
Step 2 of 4:	Select a file previously exported from WCS or NCS to Import
Import Map	data with XML Format (File exported from WCS or NCS)
Next Ca	ncel

#### **Associate Endpoints to Sites**

Now that you have created all the sites where your network equipment is staged, it is time to map those sites to their respective subnets, data sources, and VLANs. This allows Cisco Prime Infrastructure to see the traffic flow, especially when it comes to application performance. In order to create an endpoint, you can go to **Design > Endpoint-Site Association.** The image below shows how various sites are mapped to their subnets. In addition to the subnet mask, you can also specify the default data source desired for that site in addition to the VLANs for those sites.

Endpoint-Site Association				
🖌 Edit 🗙 Dolete 🤤 Add Row 👳 Mul	tiple Update		Show	/ All
Site		SubNet	Data Source	VLAN
Amsterdam Branch		192.168.152.0/26		
Boxborough Branch		10.5.0.0/16		
Derver Branch	0	10.9.0.0 /	15	0
🗌 India Branch		10.7.0.0/16	Save Cancel Datasources	×
🗌 London Branch		10.11.0.0/16		
Los Angeles Branch		10.2.0.0/15		
Management Apps		192.166.0.0/16	₩	12.4
Management Apps		171.0.0/8	10.0.109.2-32582	
			10.0.107 2-32630	

#### **Create Port Groups**

The next step in getting started with Cisco Prime Infrastructure is to create groups in addition to the default port groups that come preconfigured. Port groups creation can be accessed from **Design > Port Grouping**. If a custom port group needs to be created, you can hover over **User Defined** and click the plus sign icon to access a pop-up menu for adding a new group as shown in image below.



The WAN Interfaces port group is a special preconfigured port group. The interfaces in this group are your WAN interfaces that need to be actively monitored. In order to add WAN interfaces to this group, select all groups and filter the WAN interfaces based on your interfaces type, IP address, interface description, or any other attributes that are used to denote a WAN interface group. It is highly recommended to populate this group with the WAN interface to get the most out of this application.

# Users and User Group Management Adding New Users

User Groups			
Administration > Users, Roles & AAA > User G	iroups		
Group Name	Members	Audit Trail	Export
Admin	test1 , bkapoor		Task List
Config Managers	bkapoor		Task List
Lobby Ambassador			Task List
Monitor Lite			Task List
North Bound API			Task List
Root	root		Task List
Super Users	test1 , bkapoor		Task List
System Monitoring	bkapoor		Task List
User Assistant			Task List
User Defined 1	prime		Task List
User Defined 2	test	8	Task List

As noted earlier, it is not advisable to use the root user to log in for normal use. New users and groups can be created by navigating to **Administration > Users**, **Roles & AAA** as shown in the preceding figures. It would help to chalk out what are the various levels at which you want to distribute the users, and to create those roles first. It doesn't really matter whether you create users or groups first. New users can be easily added by going to **Administration > Users**, **Roles & AAA > Users > Add Users > Select "Add Users" from the drop-down on the right side**. Once you get into the add user workflow, fill in the username, password, and local authorization for this user as shown in the figure below (right).

A virtual domain can also be assigned to the users when you define their roles by selecting the virtual domain on the left side and moving it to the right side as shown in the image below (left).

General Virtual Domains
Username jfields   New Password ••••••••••••••••••••••••••••••••••••

#### **Creating User Groups**

User groups are synonymous with roles. All the roles except the user-defined roles are preconfigured. Userdefined groups can be modified by going to **Administration > Users**, **Roles & AAA > User Groups > User Defined #.** Other groups and roles cannot be modified, but you can add users to them, see the audit trail, and even export the TACACS+/RADIUS command sets by clicking the task list. User-defined roles can be modified by clicking the User Defined # link in the figure above (left). Once clicked, all the knobs on the user access controls are exposed as shown in the figure (below). You can select the whole category, for example, Network Configuration, or a few of the options within that category to customize the role. Once the group/role is created, multiple users can then be assigned to that group.



#### **Image Management Settings**

There aren't any mandatory settings required for software image management, but a number of knobs can be accessed from **Administration > System Settings > Image Management** as shown in figure (right). These include the team shared Cisco.com username/password, job failure handling options, image and configuration protocol options, and so on. Users are strongly recommended to glance through this page and set it up initially so that preferred preferences are applied when distributing images on managed devices. Images can easily be added to the local repository by choosing **Operate > Software Image Management > Import**. Follow the wizard to import images from Cisco.com directly.

Cisco.com user name 🌵	
Cisco.com password 🕸	
SSH user name 🕸	
SSH password 🏶	
Staging directory 🕸	/opt/Staging
	Continue distribution on failure 🔍
	Collect images along with inventory collection $\oplus$
	Reboot immediately 🕸
	Distribute parallelly 🕸
	TFTP fallback 🕸
	Backup current image 🕕
	Insert boot command @
	Recommend latest maintenance version of each major release
	Recommend Same Image Feature 🕕
	Recommend versions higher than current version ${\mathfrak P}$
	Recommend general deployment images only 🕀
	Include CCO for recommendation @
	Use SCP for image upgrade and import @
	TFTP
	SCP
Image transfer protocol order	

Images can be deployed to devices by going to **Operate > Software Image Management**. Select the image from the list (once it has been added to the repository) and click **Distribute Images**. Once the devices are selected to be upgraded/downgraded, a prerun status is shown, which avoids the job failure in the first place. You can also run Upgrade Analysis from the same place to get a report on this.

Distribute Images						>
Device Name	IP Address	Distribute Image Name	Distribute	Location Status	Status Message	-
FL4-3750S-1	10.15.10.1	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	8	Warning: Required Spa	
3750-PHY-1	10.0.252.3	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	<b>2</b>	Ok	
AMS-3750-SBR	192.168.152.10	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	8	Warning: Required Spa	
LON-3750-SBR	10.11.10.3	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	8	Warning: Required Spa	
LA-3750-SBR	10.2.10.1	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	8	Warning: Required Spa	
SIN-3750-SBR	10.6.10.1	c3750-ipservicesk9-mz.122-58.SE1.b	in flash2	8	Warning: Required Spa	
NY-3750-SBR.cisco.com	10.4.10.1	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	8	Warning: Required Spa	
RTP-3750-SBR	10.1.10.1	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	8	Warning: Required Spa	
SF-3750-SBR	10.3.10.1	c3750-ipservicesk9-mz.122-58.SE1.b	in flash1	<b>O</b>	Ok	-
BXB-3750-SBR	10.5.10.1	c3750-ipservicesk9-mz, 122-58.SE1.b	in flash1	0	Ok	-
<ul> <li>Distribution Options</li> </ul>						-
Insert boot command		Reboot Device	OFF	- P		
🔲 Distribute Parallely		Erase Flash B	efore Distribution			
🗌 Backup Current Image		🗹 Continue on	failure			
TFTP Fall Back		Use SSH				
						1
					Submit Ca	ncel

# **Configuration Archive Settings**

		Date	Created By	Description	Out of band
*	0	September 11, 2012 3:05:21 AM P	Inventory	Archived by inventory	Yes
		Configuration Type		Compare With	
		Running Configuration		Previous   Startup   Other Version   Other Device	
		Startup Configuration		Previous   Other Version   Other Device	

The Configuration Archive will be one of the most used portions from a daily operation point of view. It is highly recommended to go to Administration > System Settings > Configuration Archive. The Basic tab allows users to define protocol order, SNMP timeout, the number of days and the versions to retain, thread pool count, and other such variables. The Advanced tab allows users to define a command exclude list for each of the device family types. Once this is done, users may view and compare configurations by navigating to **Operate > Configuration Archives** (under the Device Work Center). Browse the device and open up the tree to see all the configuration versions that have been archived for this device as shown in the preceeding figure. When you click Compare there, you quickly see the color-coded configuration differences instantly as shown in same preceeding figure.

onfiglets	NY-3750-SBR.cisco.com / Startup Configuration /		NY-3750-SBR.cisco.com / Running Configuration /
a * 🗄 * 🛞	September 11, 2012 3:05:21 AM PD1		September 11, 2012 3:05:21 AM PD1
r Configlets ▶ All	Interface-Interface GigabitEthernet1/0/3 description Voice endpoints Vlan 141 switchport access vlan 12 switchport mode access	*	Interface-Interface GigabitEthernet1/0/3 description Connected to Polycom 6000 in access mode switchport access vian 11
Difference Only	switchport voice vian 11 Interface-Interface GigabitEthernet1/0/4 description Voice endpoints Vian 141 switchport access vian 12 switchport mode access switchport voice vian 13		Interface-Interface GigabitEthernet1/0/4 description connected to ex60 in the rack switchport access vian 11
	Interface-Interface GigabitEthernet1/0/7 switchport access vian 12 switchport mode access	h	Interface-Interface GigabitEthernet1/0/7 switchport access vian 11
	MediaTrace-Mediatrace Global	III	MediaTrace-Mediatrace Global mediatrace session-params EMSAM_PARAMS_1664414584 mediatrace session-params EMSAM_PARAMS_2120357176 mediatrace 1664414584 mediatrace schedule 1664414584 life 14400 start-time nor
	MediaTrace-Mediatrace Path-specifier-mediatrace path-	Ŧ	mediatrace 2120357176 mediatrace schedule 2120357176 life 14400 start-time no MediaTrace-Mediatrace Path-specifier-mediatrace path mediatrace path-specifier EMSAM_PATH_1664414584 des
	< III >		4 III Þ

# **Configuring NTP and DNS for NAMs**

It is extremely important to configure NTP and DNS for all the NAMs in your network. You can now configure those without going to the CLI or logging in to the individual NAM web GUIs. From the Cisco Prime Infrastructure Device Work Center, navigate to Device Group > Device Type > Cisco Interfaces and Modules. Click the name of the NAM on which you want to configure NTP/DNS, and then click **Configure** in the bottom pane. Now click **Feature** on the left (still in the bottom pane), and you will see a link for "system." Click it to see a form for this NAM that allows you to configure all the system-related information for a given NAM including NTP and DNS. The image on the left (above) shows where the NTP and DNS can be configured.

And Moulas Official		i address Ends	1212		~ <b>[</b>	ocietted 1
EDC XUGGES Sync	caurba ereites + 3	E ADD DEMCE	nport		Show [	
Device Name 🔺	Reachability	(P Address	Device Type	Collection Status	Collecton Time	Software Versio
ACC-NAM2204.d.	Ø Unreachable	192.168.136.67	Cisco NAM 2284	Managed with Warn.	September 28, 2	S.1(1)
Campus-NAM3.es	Reachable	192 168 136 129	Cano Catalyst 65.	Managed	Ortober 25, 201	5.1(2)
DC+NAM2220.cite	Reachable	192.168(136.32	Cisco NAM 2220	Managed	Ortober 25, 201.	S.1(2)
Nam	Reachable	192.168.136.123	Cisco SM-SRE Ne	Managed with Warni.	October 25, 201	
RTP-NAM-SRE.CB	🛛 Reachable	192.168,136,131	Cisco SM-SRE Ne.	Managed	October 25, 201.	5.1(2-patch5)
61			m			
onfiguration Archive	Image					
≠ DNS Parameters DNS Parameters	image ame eset-cbco.cr	Im		Namo Servers	172.28.162.114	
VOS Parameters     Dos Parameters     Domain N     SMNP Agent	image ame [eset-cbco.cr	m		Name Servers	172.28.162.114	
V DNS Parameters     DCmah N     SNNP Agent     System Time	image ame [eset-c&co.cl	Im		Nama Servars	172.28.102.114	
DNS Parameters DNS Parameters Domain N SiNNP Agent System Time System System 'WB'	image ame esst.cbco.cl	m		Namo Servars	172.28.152.114	
DNS Parameters     Dons Parameters     Donain N     StNIP Agent     System Time     System Time     With     Pimary NIP Se     Nome/Pi	Image ame eset-cbco.cl Tme	im		Namo Sorvars	172.23.192.114	
DNS Parameters DNS Parameters Donnin N SOMP Agent System Time System Time	Image ame esat-ckco.cl Time  Image Tree  Image I	m		Nama Sarvas	172.28.102.114	

## **Connection to Cisco.com**

Cisco.com connection is required for some of the advanced features such as Smart Interactions (TAC service requests, and support forums), importing software images, contract connection, and many others. It is vital for the Cisco Prime Infrastructure server to be able to connect to Cisco.com to pull the data for those reasons. There are two parts to making this work: proxy settings and Cisco.com user settings.

# **Proxy Settings**

If Cisco Prime Infrastructure requires a proxy to connect to the Internet, you can enter the proxy information by going to **Administration > System Settings > Proxy Settings**. You can enable proxy settings and enter all the proxy information there. Authenticating proxies is also supported in Cisco Prime Infrastructure.

#### Cisco.com Settings

Once the proxy settings are configured, you can enter your Cisco.com credentials at the following places:

- Administration > System Settings > Image Management
- Administration > System Settings > Support Request Settings

Add APs
Name Prefix AP_
Add APs Automatic 💌
AP Type AP 3500i
Enable 11n Support
802.11a/n Antenna Internal-3500i-5GH 💌
802.11b/g/n Internal-3500i-2.40
Protocol 802.11a/n,b/g/n 💌
Throughput 802.11a/n <b>10-1</b>
802.11b/g/n 5 💌
Services: Advanced Options
▼ Data/Coverage
Voice
Location with Monitor Mode APs
Table Courses Area 16 (as forth)
Calculate
Recommended AP Count: 4
Data/Coverage 1
Voice
Location 4
Location with Monitor
Mode APs
Demand
Overrride Coverage Per
Apply to Map Cancel

# Planning/Preparing the Network

# Wireless Planning Tool

The built-in planning tool provides a way for network administrators to determine what is required in the deployment of a wireless network. As part of the planning process, various criteria are input into the planning tool. Complete these steps:

1. Specify the AP prefix and AP placement method (automatic versus manual).

- 2. Choose the AP type and specify the antenna for both the 2.4 GHz and 5 GHz bands.
- 3. Choose the protocol (band) and minimum desired throughput per band that is required for this plan.
- 4. Enable planning mode for advanced options for data, voice, and location. Data and voice provide safety margins for design help. Safety margins help design for certain RSSI thresholds, which is detailed in online help. The location with monitor mode factors in APs that could be deployed to augment location accuracy. The location typically requires a denser deployment than data, and the location check box helps plan for the advertised location accuracy.
- 5. Both the Demand and Override options allow for planning for any special cases where there is a high density of client presence such as conference rooms or lecture halls.

Generated proposal contains these:

- · Floor plan details
- Disclaimer/scope/assumptions
- Proposed AP placement
- Coverage and data rate heat map
- · Coverage analysis

#### **Ports Used**

The following table shows all the ports that are used by Cisco Prime Infrastructure to communicate with devices and with other Cisco Prime Infrastructure servers.

Protocol	Transport	Port Used	Port Usage Description
ICMP		7	Server to endpoints. Endpoint discovery
SSH	TCP	22	SSH to Cisco Prime Infrastructure/Assurance server
SCP	TCP	22	SCP to Cisco Prime Infrastructure/Assurance server
TFTP	UDP	69	Network devices to Cisco Prime Infrastructure/Assurance server
FTP	TCP	2021	FTP to Cisco Prime Infrastructure/Assurance server
SNMP	UDP	161	Cisco Prime Infrastructure/Assurance server to network devices/NAM
SNMP Trap	UDP	162	Network devices to Cisco Prime Infrastructure/Assurance server
Syslog	UDP	514	Network devices to Cisco Prime Infrastructure/Assurance server
JNDI		1099	AAA server to Cisco Prime Infrastructure/Assurance server
RMI		4444	AAA server to Cisco Prime Infrastructure/Assurance server
HTTPS	TCP	443	Browser to Cisco Prime Infrastructure/Assurance server
NetFlow	UDP	9991	Network devices/NAMs to Cisco Prime Infrastructure/Assurance server
JMS		61617	JMS port open for Automated Deployment Gateway
Health Monitor		8082	Cisco Prime Infrastructure Health Monitor Check. System use only

#### **Protocol Check**

For successfully managing a device using Cisco Prime Infrastructure, it is crucial that all the essential protocols be defined in the device credential for a given device. The following matrix shows what protocols are needed for various wired and wireless device types.

Device Family	SNMP RW	Telnet/SSH	нттр
Classic wireless controllers	У		
New mobility-based wireless controllers (Cisco IOS XE)	У	у	

Device Family	SNMP RW	Telnet/SSH	нттр
Access points	У	У	
Routers/switches	У	У	
Medianet-capable routers and switches	У	У	
Network Analysis Module	У	У	У
Third-party devices	У		

These credentials are sufficient to discover wired as well as wireless networks. Let's now focus on how to enable each of these protocols.

#### **Configuring SNMP**

SNMP is one of the protocols that Cisco Prime Infrastructure uses when talking to devices for getting basic information. When discovery is initiated, SNMP is used to query what type of device is it. Cisco Prime Infrastructure supports all versions of SNMP: v1, v2c, and v3 (noAuthNoPriv, authNoPriv, authPriv).

#### **Enabling SNMP on Wireless Controllers**

From the WLC web GUI, navigate to **Management > Communities** (under SNMP). Click **New** to create a new SNMP v1/v2c community. An SNMP v3 community can be configured by going to the SNMP v3 User from the left panel menu.

#### **Enabling SNMP on Routers/Switches**

As the routers and switches may have Cisco IOS Software, Cisco IOS XE Software, or NX-OS running, it may be best to refer to

http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies\_tech\_note09186a0080094aa4,the shtml documentation to configure SNMP on the devices. For configuring SNMP on Cisco Nexus<sup>®</sup> 5000 or similar devices, use

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/sm\_snmp.html. For more devices, the following **sample** syntax should work for SNMP v1/v2c:

- # configure terminal
- # snmp-server community pu6l1c RO (using "public" is not recommended)
- # snmp-server community prlvat3 RW (using "private" is not recommended)

#### Enabling Telnet/SSH on Routers/Switches

Cisco Prime Infrastructure can work with Telnet or SSHv2. If you are able to Telnet/SSH into the device, Cisco Prime Infrastructure should be able to do the same. If you have to enter another password to enable this, be sure to enter that in the device credentials. More on how to edit credentials is discussed in the section "Fixing Credential Errors."

#### **Enabling Telnet/SSH on Wireless Controllers**

From the WLC web GUI, navigate to **Management > Telnet-SSH** to open the Telnet-SSH Configuration page. Allow either the Telnet or SSH sessions.

#### HTTP/HTTPS

The HTTP protocol is mainly used for a selected few devices as mentioned in the protocol matrix above. HTTP is used by NAM for Representational State Transfer (REST) API calls, as well as for enabling/disabling Mediatrace on medianet-capable devices. For medianet-capable devices, the HTTP user must have a privilege level of 15.

# **Preparing the Wireless Network**

There are some tasks that are wireless centered, and do not apply to the wired infrastructure. Let's take a look at those in this section. This document assumes that your wireless infrastructure is up and running. If you need to deploy the wireless network, please refer to the NCS 1.1 Deployment Guide at http://www.cisco.com/en/US/products/ps10315/products\_tech\_note09186a0080bba943.shtml.

# Import Maps from WCS

The map export/import feature is available in WCS 7.0. This feature is detailed in the WCS 7.0

#### Configuration Guide, which is available at

<u>http://www.cisco.com/en/US/docs/wireless/wcs/7.0/configuration/guide/WCS70cg.html</u>. After you export maps from your WCS server, you can import this set of maps in your NCS server. The next step on how to import your maps is covered in the WCS 7.0 Configuration Guide.

**TIP:** It is important that APs from your WCS server be added to your Cisco Prime Infrastructure server prior to importing maps, because APs on your WCS maps are also included during the export process. APs that have not been added to your Cisco Prime Infrastructure system, but are present on exported floor maps, result in errors that are displayed when you import those maps into Cisco Prime Infrastructure.

# **Discovering Your Network**

Cisco Prime Infrastructure uses and enhances the discovery mechanisms that were used in Cisco Prime LMS 4.x. Protocols like ping, SNMP (v1, v2c, and v3), Cisco Discovery Protocol, Link Layer Discovery Protocol (LLDP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF) are used to discover the network. This section will focus on how best to configure the discovery profile once and to automate the discovery going forward.

# **Discover Devices**

It is a very common practice to import the CSV file into the network management application and start managing the devices going forward. This is not a bad idea, but it leaves more chances for human error, especially if the spreadsheet is not updated with newly deployed devices in the network. With discovery, you always get the latest picture of your wired as well as wireless network.

Discovery Settings			×
*Name AMER_Network		Current Discovery Settings	^
Protocol Settings			
PingSweep Module	$\diamond$		
▼ Layer 2 Protocols			
CDP Module	\$		
LLDP Module	4>		
Advanced Brotocols			11
Routing Table	\$		
Address Resolution Protocol	\$		
Border Gateway Protocol	\$		
OSPF	\$		
ilters			
IP Filter	¢		
<ul> <li>Advanced Filters</li> </ul>			
System Location Filter	\$		
System Object ID Filter	\$		
DNS Filter	4		+
4	111	1	

#### **Create a New Discovery Profile**

When we create the discovery profile, we are telling Cisco Prime Infrastructure which protocols we want to use from the ones mentioned above to discover the network. Each of them has its own pros and cons, but it's definitely necessary to have them all available at our discretion. Discovery can be easily accessed from the Getting Started Wizard when you log in for the first time or by navigating to **Operate > Discovery** (under Device Work Center). There are two options here: Quick Discovery and Discovery Settings. Quick Discovery allows you mainly to ping sweep your network followed by SNMP polling to get more details on the devices.

If you are planning to configure the discovery correctly the first time and reuse your configuration, start by clicking **Discovery Settings**. Now click **New** in the discovery settings modal pop-up. A window (as shown above) will pop up, where you can configure all the discovery settings will open. You will observe that the pop-up is broken down into multiple sections: Protocol Settings, Filters, Credential Settings, and Preferred Management IP (only two are shown in the preceding figure). You need to select at least one item from Protocol Settings, SNMP and Telnet/SSH from Credential Settings, and Preferred Management IP.

Start by giving the profile a suitable name. Depending on how many protocols you want to enable, start filling in the relevant information. Click the "+" icon next to the Ping Sweep Module to open up more settings. You can add your subnets manually or use the Import CSV File button to import all your subnets from a simple CSV file. The CSV file needed for the import will have columns that correspond to the GUI, such as IP Address and Subnet Mask. Similarly you can fill in more protocols as well, but remember that the more protocols you add, the more time it will take to converge the discovery.

CDP Module	\$
LLDP Module	0
✓ Enable Link Layer Discove ✓ Enable Cross Router Bou	ery Protocol Indry
🖉 Edit 🗙 Delete 👷 Add	Row Import CSV File 🔶
Seed Device	Hop Count
• 10.1.2.1	
	Save   Cancel

**TIP:** If the majority of your devices are Cisco, or if LLDP is enabled on Cisco/non-Cisco devices, then using Cisco Discovery Protocol/LLDP will converge the discovery faster. If the network has a mixture of multivendor network devices, ping sweep should help. Ping sweep will also help with doing a directed discovery, for example, on a 10.1.1.0/24 network.

**TIP:** If Cisco Discovery Protocol information is desired in the Device Work Center, Cisco Discovery Protocol can be enabled in the discovery. It is not mandatory.

#### **Configuring Cisco Discovery Protocol/LLDP**

Configuring Cisco Discovery Protocol and configuring LLDP are very similar in nature. The first check box enables the use of LLDP in the discovery. The second check box enables jumping the router (or Layer 3) boundaries. Cisco Discovery Protocol is a Layer 2 protocol, and if we want the discovery to continue all the way until there are no neighbors available, we need to use this option. Unlike ping sweep, the seed device for a Cisco Discovery Protocol/LLDP discovery is a single device from which the discovery should initiate. If the hop count is left blank, discovery will continue until the end of the Cisco Discovery Protocol/LLDP neighbor is reached. You can add your subnets manually or use the Import CSV File button to import all of your Cisco Discovery Protocol/LLDP seeds from a simple CSV file. The CSV file needed for the import will have columns that correspond to the GUI, such as Seed Device IP Address and Hop Count.

Other protocols are very similar in nature. Some require the hop counts, while others like Border Gateway Protocol (BGP) and OSFP don't require hop counts.

#### Filtering

If you want to discover all of the subnets but would like to have a way to import information on certain devices based on their IP address, system location, type of device, or DNS, you can use filters to do just that.

**TIP:** If you are running discovery for the first time, pick a smaller range or hop count to begin with. Do not use filters in this discovery. Once the results are what you expect, go back and edit that profile to add filters as needed.

#### Credentials

Credentials are also an important part of the discovery. Please refer to the credential matrix from the Protocol Check section and enter the credentials appropriately. If this is not done, devices in the Device Work Center will error out with "Managing with Credential Errors." You can configure multiple community strings for the same network. This really helps to manage multiple devices without having to worry about which community is configured on what device.



For example, in the figure above, you could add another SNMP string for the 10.1.2.<sup>\*</sup> network in addition to the one already configured.

redential Settings			
SnmpV2 Credential		¢	
Telnet Credential		0	
☑ Enable Telnet Crea	dential		
🖉 Edit 🗙 Delete	Add Row		
IP	User Name	Password	Enable Passw.
• 10.1.2.*	•••••	•••••	•••••
	Sa	ive Cancel	

The last thing to configure before we run discovery is the preferred management IP. Once the devices are discovered and added to the inventory, how do you want to manage them? Do you want to see the device list with DNS, loopback IP, or local hostname configured on the devices (also called sysName)? If DNS is not used on your network devices, go ahead and select sysName. If devices have a specific management VLAN and all the devices have loopback configured for that, it would be a good idea to use that. DNS is the last choice as the device names become very long and it clutters up the device selector.

#### **Discover the Network**

With Cisco Prime Infrastructure, you can now discover the wired and wireless network in just one discovery. When the discovery profile is saved, select the discovery profile and click the Run Now button as shown in the figure on the left. The results will be displayed on the same page as the discovery settings. You can refresh the job and watch the status of the discovery in real time.

Disc	overy	Gettings			
G	Run Now	Schedule	New	🖥 Copy 🗙 Delete 🥖 Edit	
	Name			Date Created	Date Modified
0	Lab1			2012-Aug-21 21:17:07	2012-Aug-21 21:17:07
۲	test1			2012-Sep-04 21:22:14	2012-Sep-05 09:20:04

#### **Scheduling Ongoing Discovery**

In addition to running discovery in real time, you can schedule discovery to run when you want it. Select the discovery profile name and click Schedule instead of Run Now. You will get a modal pop-up that looks like the figure (above). Scheduling is extremely flexible in Cisco Prime Infrastructure. You can run every **x** minutes to y years.



#### Validate Discovery

Now that we have discovered our wired/wireless network, how can we make sure we are archiving the entire inventory, configuration, and other relevant information? We can start with inventory, as that is where we will know whether Cisco Prime Infrastructure was having issues fetching inventory or configuration information.

#### **Device Work Center**

Navigate to **Operate > Device Work Center** to see the entire inventory that has been discovered. The left pane allows you to filter on devices based on the device types or user-defined group that we can create. The top portion of the Device Work Center allows you to see quick information on the device as shown in the figure above. Once you click the device's name, the bottom pane is populated with more detailed information. Tabs in the bottom pane can be changed to quickly access focused, detailed information as seen in the image above.

Device Group	Device Group > Device Type > Close Costaluet 2/7EC C	Switches and Hubs >	Cisco Catalyst 37	50 Series Switches				
(م	Cisco Catalyst 3750 S	eries switches					Se	lected 1   Total 10 🗛 🖄
=• <u>@</u> •	🖉 Edit 💥 Delete 💐 Syna	Groups & Sites 🔻	9 Add Device	Bulk Import			Show All	
Switches and Hubs     Switches and Hubs     Gisco Catalyst 2960 Series	Device Name	Reachability	IP Address	Device Type	Collection Status	Colection Detail	Collection Time	Software Version
ᡖ Gisco Catelyst 3500 Series 🚍	LA-375D-SER	Reachable	10.2.10.1	Cisco 3750 St	Managed	Collection Status : Co	September 12, 2	12.2(58)8E1
👌 Cisco Catalyst 3560 Series 🗐	LON 3750 SER	🔄 Reachable	10.11.10.3	Cisco 3750 St	Managed	Colection Status : Co	September 12, 2	12.2(53)682
Cisco Catalyst 3560-E Serie Gisco Catalyst 3250 Series	NY-3750-SBR.ds	Reachable	10.4.10.1	Ckco 3750 St.,	Managed with War	Collection Status : Fa feature_vlanUnexpe	September 12, 2	12.2(58)5E1
Cisco Catalyst 4500 Saries	RTP-3750-SER	🔄 Reachable	10.1.10.1	Cisco 3750 St	Managed	Collection Status : Co	September 12, 2	12.2(58)6E1
Circle Catrilicet 4000 Casilor	5F-3750-SBR	🛛 Reachable	10.3.10.1	Cisco 3750 St.,	Managed	Collection Status : Co	September 12, 2	12.2(53)652
111 <b>b</b>	SIN-3750-SBR	Reachable	10.5 10.1	CISCO 3750 St.	Managed	Colection Status : Co	September 12, 2.	15.0(1)SE
Device Details Configuration	Configuration Archive	Image						Selected 0   Total 5 🔗
Schedule Rollback 🐻 Schedule Archive	Schedule Overwrite					S	now All	- 8
Date	<ul> <li>Created By</li> </ul>	1	Descrip	ation			Out of band	
August 28, 2012 4 24:53 PM PD	T Syslog		Archive	ed by syslag			Yes	
August 28, 2012 3:29:24 PM PD	T Syslog		Archive	ed by syslog			Yes	
August 28, 2012 3:03:39 PM PD	T Syslog		Archive	ed by syslog			Yes	
August 28, 2012 2:40:55 PM PD	T Sysiog		Archive	ed by syslog			Yes	
August 22, 2012 10:37:39 AM P	DT Inventory		Initial v	rerson				

#### **Fixing Credential Errors**

At times you will encounter a few devices that don't have the SNMP strings or the CLI access that you thought they would have. You can either streamline or change the information on the devices, or if you have another set of credentials for a different subnet, you could add that to the CLI section of the discovery profile and rerun the discovery. If you have a handful of changes, you can click the devices with a status of Managed with Warning and then click the Edit button to modify the credentials.

Device Group > ALL ALL		
Edit Delete 🖓 Sync 🎄 Groups & Sites	Edit Device	* Indicates required fields
Device Name         Reachability         IP Av           3560-DC-1         Image: 10.0         10.0           3750-PHY-1         Image: 10.0         3945-East-1.cisc         192.	oddress/DNS         General Parameters           0.252.4         IP Address           0.252.3         DNS Name           .168.152.1         DNS Name	10.0.252.3
3945-West-1         10.0           7206-Core-1         10.0            10.0           Configuration Archive         Image	0.103.1       0.255.42       Version       * Retries       * Timeout	v2c • 2 5 (secs)
Summary 10.0.252.3 > System > Summary	* Community * Confirm Community	•••••

With Cisco Prime Infrastructure 2.0, there is now an ability to export devices with credentials directly from the GUI. Navigate **to Operate > Device Work Center** and you should be able to see the "Export Device" button as shown in following figure:



At that point in time, you can export the device credentials, change them using a spreadsheet application, and import them back.

TIP: If you need to change the credentials for devices in bulk, this method can be used to do that.

# **Importing Devices Manually**

Bulk Import	×
Operation: Device	a 💌
Select CSV File	Choose File No file chosen
Bulk device add sar Bulk site add sampl	nple template can be downloaded here e template can be downloaded here
	Import Close

If you maintain a spreadsheet that has all the devices and would rather get started with that, you do have this option in Cisco Prime Infrastructure 2.0. If you to go **Operate > Device Work Center > Bulk Import**, you get an import pop-up as shown in the figure at the right.

**TIP:** Export the device template using the first "here" link. Use the exported CSV file to populate the device information. This will make sure your import goes through successfully.

# **Automating Branch Device Deployment**

If you have a need to deploy devices in branches from time to time, automated branch deployment can really ease your Day-0 task, by empowering you with zero-touch deployment. This is another way of automatically adding devices in Cisco Prime Infrastructure. There are some guided workflows as well to onboard newer 3850 switches and 5760 controllers. We will talk about this method in detail in "Advance Configuration Topics."

# Deploying Wireless and Advanced Instrumentation

Cisco Prime Infrastructure can really simplify the dreaded task of deploying advance instrumentation like Application Visibility and Control (AVC), Flexible NetFlow, Next Generation Network Based Application Recognition 2 (NBAR2), and much more. Cisco Prime Infrastructure uses converged configuration templates to achieve this task. This section will focus on instrumentation that will help visualize some of the common challenges in managing application responses within a corporation.

#### **Deploy a WLAN Using a Configuration Template**

General Cor	ntrollers Cou	intry/DCA Tem	plates Apply/Schedule A	Audit Reboot	Report
II Controllers				Group Controlle	rs
IP Address	Name	Config Group	Mobility Group Name	IP Address	Name
92.168.136.48 V	WLC-4400-1	none	eset		
92.168.136.49 S	SJ-WISM2-1	none	mobile-1		
92.168.136.4€ ¥	VLC-2100-1	none	eset		
92.168.152.11 A	MS-2504-WLC	none	AMS	-	
			>>		
			(Add)		
			<<		
			Remove	1	
				č –	

Configuration groups are an easy way to group controllers logically. This feature provides a way to manage controllers with similar configurations. Templates can be extracted from existing controllers to provision new controllers or existing controllers with additional configuration parameters. Configuration groups can also be used to schedule configuration sets from being provisioned. Controller reboots can also be scheduled or cascaded depending on operational requirements. Mobility groups, dynamic channel assignment (DCA), and controller configuration auditing can also be managed using configuration groups.

Configuration groups are used when grouping sites together for easier management (mobility groups, DCA, and regulatory domain settings) and for scheduling remote configuration changes. Configuration groups can be accessed from **Design > Wireless Configuration** (under Configuration) **> Controller Config Groups**.

- Adding controllers: Controllers in WCS are presented and can be moved over to the new configuration group.
- Applying templates: Discovered or already present templates can then be applied to the controller.
- Auditing: Make sure that template-based audit is selected in the audit settings and then audit the controllers in the group to make sure that they comply with policies.

# **NetFlow**

NetFlow is an embedded instrumentation within Cisco IOS Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. NetFlow gives network managers a detailed view of application flows on the network. Cisco Prime Infrastructure supports Traditional NetFlow (TNF) as well as Flexible NetFlow (FNF). A summarized view of what versions of NetFlow exist, their support, and their implied usage in Cisco Prime Infrastructure can be seen in the following two tables.

Flow Record Type	NetFlow Version	Cisco Prime Infrastructure Support	Template to Use	Technologies Used By
Traditional NetFlow (TNF)	Cisco (v5)	Yes	There is no template for this, but one can be created.	Network traffic stats
Flexible NetFlow (FNF)	RFC 3954 (v9)	Yes	Collecting Traffic Statistics under OOTB (Out of the box) Folder	<ul><li>PerfMon</li><li>Performance Agent (PA)</li></ul>
IPFIX	RFC 5101 RFC 5102 (v10)	Yes	AVC Template uses IPFIX	IPFIX is a protocol developed by the IETF working group. The IETF Working group used NetFlow v9 as the basis for IPFIX.

The following table shows further breakdown of NetFlow, and how NetFlow data is used for application visibility.

Features	Description	Export Format Support	Template to Be Used	Suggested Use
TNF	Basic NetFlow records	Version 5	Custom template needs to be created	Old platform that does not support Flexible NetFlow or IPFIX yet.
FNF	Flexible, extensible flow records. Report application from NBAR2.	Version 9 (IPFIX)	Traffic Statistics under OOTB Folder	<ul> <li>For newer platforms such as</li> <li>ISR G2</li> <li>ASR 1000</li> <li>Report application visibility</li> </ul>
PA	Application Response Time (ART)	Version 9 (IPFIX)	Need to develop	<ul> <li>ART</li> <li>Transaction time</li> <li>Per application latency</li> <li>Response time</li> <li>(Available only on ISR G2)</li> </ul>
PerfMon	Media Performance	Version 9 (IPFIX)	PerfMon template under OOTB Folder	<ul><li>Voice/video performance</li><li>Jitter</li><li>Packet loss</li></ul>

Check out the AVC Solution Guide for more detailed use cases on where and how to use AVC. The solution guide can be found at <u>http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/solution\_overview\_c22-</u>728972.html#wp9000608.

#### Using Configuration Templates to Enable NetFlow

Deploying TNF is relatively simple, but FNF can be challenging. Cisco Prime Infrastructure greatly simplifies managing NetFlow end to end. You can follow the design, deploy, operate, report model for NetFlow as well. You can design the NetFlow template by going to **Design > Configuration Templates > My Templates > OOTB > Collecting Traffic Statistics**. This will open the NetFlow v9 templates as shown in the figure above. You can fill in all the metadata at the top of the template and save as a new template.

🔹 🧰 My Templates	▼ Template Detail
CEM  Content  Conten	CLI Content Form View  *Flow Exporter Name  *IP Address  *Flow Exporter Port 9,991  *Flow Monitor Name  *Interface
🐨 Trap Receiver 🐨 stp	Save Save as New Template Cancel UnPublish Deploy

The next step is to publish the template so that it becomes available for other members to deploy the template. Note that the default port for NetFlow for Cisco Prime Infrastructure 2.0 is 9991 and cannot be changed in this release.

-		
<ul> <li>Switches and Hu</li> </ul>	is Switches and Hubs	
] 🔹 🕨 Cisco Catalyst	1500 Series Swi Cisco Catalyst 4500 Series Switches	
] 🔹 🕨 Cisco Catalyst	3500 Series XL 1 Cisco Catalyst 3500 Series XL Switches	
] 🔹 🕨 Cisco Catalyst	i500 Series Swi Cisco Catalyst 6500 Series Switches	
🛛 🔻 Cisco Catalyst	750 Series Swi Cisco Catalyst 3750 Series Switches	
] FL4-3750S-	FL4-3750S-1 Switches and Hubs 10.15.10.1 Cisco	-
<ul> <li>Value Assignment</li> </ul>		
rvices	Feature CLI Preview	
Name	*Flow Exporter Name LONDON-BR	
3750-PHY-1	*IP Address 10.1.2.3	
	*Flow Experter Part To cont	
		=
	"How Monitor Name LON-MONITOR	
	*Interface G1/0	
	Apply	**
	III	•

**TIP:** <u>Samplicator</u> (Not tested nor supported by TAC) may be used to point all devices to send NetFlow to one place. Samplicator can then fork out NetFlow data to multiple Cisco Prime Infrastructure instances as desired. Samplicator can also be used for syslogs and traps in addition to Netflow.

Now that the template is published, the next task is to deploy the template so that we can configure devices to start sending NetFlow data to Cisco Prime Infrastructure. Go to **Deploy > Configuration Templates**, find **Collecting Traffic Statistics** in the list, and click **Deploy**.
You will see the Template Deployment modal pop-up window (see figure above). Select the device or devices, fill in the values, and click **Apply** to accept the changes. You can fill in values for each device or you can use the export to/import from a spreadsheet option for quick data entry. Click the CLI Properties to see the CLI that is generated from the values provided. Finally, schedule your job to enable NetFlow on the devices.

#### **Check Whether NetFlow Data Are Coming or Not**

We have now enabled NetFlow on the devices, but how do we know whether or not Cisco Prime Infrastructure is receiving it? A quick way to tell is to go to Design > Monitor Configuration and see if there are multiple NetFlow instances for each unique NetFlow template. Normally you will see a template (see figure on left) as Flexible\_NetFlow-<FNF\_Type>. Once you click that template, the right pane will show template details. The bottom most portion (see figure above), Exporting Devices, should tell us which device is using/sending the NetFlow for that template. The middle portion of the same template shows all the attributes sent in that template. You may also run a report by choosing **Report > Report Launch Pad > Raw NetFlow Reports** and selecting a netFlow report. Click **New** to generate a new report. Specify all the details and run the report to see if you are really getting any data from this device based on what was configured. All NetFlow-pertinent dashlets will also start populating automatically (after two polling cycles).

,	A	letFlow
		Flexible_Netflow-AVC-1
		Flexible_Netflow-App-Traffic-1
		Flexible_Netflow-Application-1
	<b>a</b>	Flexible_Netflow-Application-2
		Flexible_Netflow-Traffic-Conv-1
	<b></b>	Flexible_Netflow-Traffic-Conv-2
	-	Flexible_Netflow-Traffic-Conv-3
		Flexible_Netflow-Traffic-Conv-4
	<b>a</b>	Flexible_Netflow-Traffic-Host-1
	<b></b>	Flexible_Netflow-Traffic-Host-2
	<b>•</b>	Flexible_Netflow-URL-1
	B-	Flexible_Netflow-Unprocessed-1
	<b>a</b>	Flexible_Netflow-Voice-Video-1
	<b></b>	Flexible_Netflow-Voice-Video-2
	<b>•</b>	Flexible_Netflow-Voice-Video-3
		Netflow-V1
	-	Netflow-V5

#### Medianet

The Cisco architecture for medianet is an end-to-end IP architecture that enables pervasive and quality rich-media experiences. Medianet combines a smarter network to smarter endpoints with medianet technology embedded into network elements and endpoints. Cisco Prime Infrastructure simplifies the whole lifecycle for medianet from enablement to reporting.

#### **Enabling Medianet**

Enabling medianet does require using the CLI to configure some devices that support medianet. Cisco Prime Infrastructure has predefined templates for enabling medianet. Just as we enabled NetFlow, we can do the same thing for medianet. Navigate **to Design > Feature Design > Search for "medianet**", as shown in the figure (below).

Feature Design	Monitor Configuration
Search Results	
media	
All	System Templates - CLI
<₽ • 🔳 • 唥	•
MediaTrace-Re	sponder-Configuration
Medianet - Perf	Mon

The first one is to make a medianet device as medianet responder, while the last one is for enabling medianet PerfMon, which allows you to see the traffic that is flowing through a given interface. The steps for deploying the template remain the same as with any other CLI template. Note that the first two templates for enabling medianet do not have any variables.

**TIP:** Make sure that a user is defined in the device with privilege level 15 for the Web Services Management Agent (WSMA) to work.

# **Check Whether Medianet Is Enabled**

	ate Parameters'				
-			10 A 11	Sho	v _
257	10 ID	10.0	LE IP Address	San Francisco E	kranc
10	Trace Service Analyze on Mu	Path Itiple I	Data Sources		
-	10.4.11.13	2	10.2.11.13	1	
0		<b>\$</b>	10.2.11.13	1	
0	10.4.11.13	-43	a contact a contact		
000	10.4.11.13 10.4.11.13	-4	10.2.11.13	1	

Once medianet is turned on, there are a few commands that can be executed on the CLI to see whether the devices can show the medianet data. Here are a few commands you can use on the devices:

```
show mediatrace session statistics show mediatrace session data
```

Please refer to the <u>Troubleshooting Guide</u> for details on how to make sure medianet is operational. Once medianet is verified to be working, we can see the RTP conversation (see the figure above) details dashlets showing sessions.



For troubleshooting, simply choose **Troubleshoot > Trace Service Path** in the same dashlet. This will launch another window where Mediatrace can be visually seen as in the figure above.

RTP S	Stream	IS								Selected	d O   Tota	
a <sup>ll</sup> Tr	ace Se	ervice Pa	ith 🔞 Analyze I	Path 💠 Sp	pecify Session for	Path Trace						
	Teres		Time		Source		Destination			Jitter	Packet Loss	MOS
		iype	IP Address	Site	User ID	IP Address	Site	User ID	(ms)	%	1405	
•	0	41	10.15.11.10		Unknown	192.168.138	ĸ	Unknown	1.66	0	4.38	
•	0	40	10.3.11.42		Unknown	10.4.11.100		Unknown	846.3	5.53	0	
•	0	40	10.4.11.13		Unknown	10.2.11.13		Unknown	932.3	0	0	
•	0	40	10.3.11.41		Unknown	10.9.11.12		Unknown	0	0	0	
	0	H H	102 168 138		Linknown	102 168 152		ifiolds	2 10	0	r	

To see the active calls navigate to **Operations > Path** Trace under Operational Tools. You can then select the audio or video calls with jitter/packet loss for troubleshooting as shown in the figure above.

# Monitoring/Troubleshooting

#### **Basic Monitoring**

Cisco Prime Infrastructure provides a very easy and flexible model for monitoring your wired/wireless network. Cisco Prime Infrastructure allows you to define or "design" monitoring templates that dictate how and what you want to monitor. You can then turn on monitoring by deploying the monitoring template. The results are then shown in the form of dashboards, dashlets, and reports.

#### **Basic Device Health**

The Basic Device Health feature is turned on by default for all devices. This includes device monitoring of device availability, CPU, and memory. Basic Device Health is polled every 5 minutes by default, but you can customize this as well.

The template is called Device Health - choose **Design > Monitoring Configuration > Features > Metrics > Device Health.** The parameters can be changed by clicking the polling value for that row as shown in the figure below.

Š□ * Parameter	* Parameter Description	
device availability	Device Availability	5 min 🔹
S cpuUtilization	CPU utilization Save   Cancel	1 min
	Memory Pool Utilization	5 min
bufferMissPercent	Buffer Miss Percentage	15 min 30 min
	Largest Free Buffer Percentage	1 hour
envTemperature	Current Temperature in degrees Celsius	6 hour
		12 hour _ 2

**TIP:** Don't forget to save the template after making the changes. The template will need to be republished and redeployed if changes are made.

## **Interface Statistics**

Interface Statistics are **not** enabled by default, as monitoring interfaces can get very tricky if not done correctly. Some business-critical device interfaces should be polled more often than others, so there is no "one size fits all" when it comes to monitoring interfaces. Interface polling can be very quickly enabled by using a predefined monitoring template. You can navigate to **Design > Monitoring Configuration > Features > Metrics > Interface Health** (shown below). Follow the same methodology to change the polling interval as mentioned for Device Health. You can see how interface availability is changed to every minute.

5	* Parameter	Description		Polling Frequency	
50	Interface Availability	Interface Availability		1 min 👻	
	ifInErrors	ifInErrors	Save   Cancel	5 min	
	ifOutErrors	ifOutErrors		5 min	
	ifInDiscards	ifInDiscards		5 min	

#### **Design Custom Monitoring Templates**

Flexible monitoring templates enable users to customize how they monitor their network. You can create your own templates by navigating to **Design > Custom SNMP Templates** and selecting the MIB and the table as shown in the figure on the left. You can then see all the variables from the table. Select the ones you are interested in, and they will be now available for polling. If the MIB you are interested in is not available in the drop-down list, you can upload a new MIB by clicking Upload MIB on the same page. Once you save the page after selecting the object identifiers (OIDs), you should see a template created as shown in the figure below

Custom SNMP Templates			
Basic Advanced			
Name 64BitQoS	COC MIT	Table's	
CISCO-CLASS-BASED			
cbQosCMPrePolicyByte     cbQosCMPostPolicyByte	cbQosCMPrePolicyByte64     cbQosCMPostPolicyByte64     cbQosCMPostPolicyByte64	cbQosCMPrePolicyBitRate  cbQosCMPostPolicyBitRate	cbQasCMPostPolicyByteOverflow cbQasCMPostPolicyByteOverflow
□ cbQosCMDropPkt ✓ cbQosCMDropByte64	cbQosCMDropPkt64 cbQosCMDropBitRate	cbQosCMDropByteOverflow cbQosCMNoBufDropPktOverflow	cbQosCMDropByte cbQosCMNoBufDropPkt
cbQosCMNoBufDropPkt64			

You can now create a poller from this template. If you now change the metadata and save this template, it will become a deployable monitoring poller and will be visible under My Templates. You are now ready to deploy the template to get monitoring started.

Temp	olates					
	Features       Custom SNMP       Memory Stats       Pre_Post_QoS_64       Etst       Rexible NetFlow       Metrics       Threshold       My Templates       Device - Heathh (defaultion)       Device - Heathh (defaultion)	ime Me ≣ :	Template Basic     * Name     Description     Type     Sub Type     Template Contr     Custom SNMP     Select Polling Fil	Pre_Post_QoS Poil Pre and Po Pr ent Parameters requency : 1 n	_64_Bits st QoS Custom SNMP re_Post_QoS_64 nin	Author Contact Teja
	IH_Swathi Interface Metrics		* Parameter		Description	
	InterfaceTest		cbQosCMDropB	yte64		
	and the second se		the second se	And the second states and the		
	Nam Metrics		cbQosCMPostPo	olicyByte64		

#### **Deploy Custom Monitoring Templates**

In order to deploy the monitoring template just created, you can navigate to **Deploy > Monitoring Deployment > My Templates**. Table view allows users to see how many devices are being polled using the template in question. Now locate your template, select it, and click **Deploy**. You will see a modal pop-up list as shown in the figure at the left. You can either select a device or devices or you can select the Device Groups option to select predefined or user-defined groups or even sites, as shown in the figure at left. Choose the appropriate group, and click **Submit**. Once back in Table view, you can see that devices are now assigned to the poller we chose in the previous step. This means that Cisco Prime Infrastructure will now be polling the devices based on what was designed in the template.

Tem O D Dev	plate Deployment evices • Device Groups rice Groups	
	Name	Description
	Third Party Device	Third Party Device
	Cisco UCS Series	Cisco UCS Series
	Cisco Interfaces and Modules	Cisco Interfaces and Modules
	Third Party Access Point	Third Party Access Point
	▼ Site Groups	Site Groups
	Los Angeles Branch	This is a site group
	System Campus	This is a site group
	San Francisco Branch	This is a site group
	San Jose Data Center	This is a site group
	Amsterdam Branch	This is a site group

### Data Collection from NAM

In order for Cisco Prime Infrastructure to manage Network Analysis Module, it needs to have a minimum software version of 5.1.1 plus the latest patches available.

▼ Device Data Sources				
				Show All
Data Source	Туре	Exporting Device	Status	Last 5 min Flow Record Rate
10.0.111.2-32443	NETFLOW	10.0.111.2	🔽 Up	1861
10.0.101.2-32442	NETFLOW	10.0.101.2	🛃 Up	243
10.0.109.2-32582	NETFLOW	10.0.109.2	🔽 Up	17

We can then make sure that Cisco Prime Infrastructure is enabled to poll the NAM data. You can navigate to **Administration > Data Sources** (Under System Setting SubMenu). The top portion of the same page shows all the devices that are actively sending NetFlow data to Cisco Prime Infrastructure. The bottom pane of the page shows all the NAMs that have been discovered or added to the inventory.

Select the NAM that should be polled by Cisco Prime Infrastructure, and click **Enable** as shown in the figure below.

▼ N	NAM Data Collector							
C	🕞 Enable 🔹 Disable							
		Name		Туре	Host IP Address	Data Usage in System		
•		ACC-NAM2204.cisco.com	<u>ج</u>	Cisco NAM 2204 Appliance	192.168.136.67	Enabled		
•		Campus-NAM3.eset-cisco.com	<b>S</b>	Cisco Catalyst 6500 Series Network Analysis Mod	192.168.136.129	Enabled		
►		DC-NAM2220.cisco.com	S.	Cisco NAM 2220 Appliance	192.168.136.32	Enabled		
•		RTP-NAM-SRE.cisco.com	6	Cisco SM-SRE Network Analysis Module	192.168.136.131	Enabled		

#### **Turning on Advanced Monitoring**

Cisco Prime Infrastructure consumes a lot of information from various different sources. Some of the sources for data include NAM, NetFlow, NBAR, medianet, PerfMon, and Performance Agent. Detailed description of these advance monitoring can also be referenced from AVC Solution Guide

(http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/solution\_overview\_c22-

<u>728972.html#wp9000608</u>) posted on Cisco.com. The following table depicts the sources of the data for the site dashlets as used by Cisco Prime Assurance:

Dashlet Category	Dashlet Name	NAM	Medianet	NetFlow	PA	NBAR2
Site	Application Usage Summary	У	У	У	У	У
	Top N Application Groups	У	У	У	У	У
	Top N Applications	У	У	У	У	У
	Top N Applications with Most Alarms	У	У	У	У	У
	Top N Clients (In and Out)	У	У	У	У	У
	Top N VLANs	У		У	У	
	Worst N RTP Streams by Packet Loss	У	У			
	Worst N Clients by Transaction Time	У			У	

Dashlet Category	Dashlet Name	NAM	Medianet	NetFlow	РА	NBAR2
Application	Application Configuration	у	у	у	у	у
	Application ART Analysis	у			у	
	App Server Performance	у			у	
	Application Traffic Analysis	у	у		у	У
	Top N Clients (In and Out)	у			у	
	Worst N Clients by Transaction Time	У			У	
	Worst N Sites by Transaction Time	У			У	
	KPI Metric Comparison	У	У		У	
	DSCP Classification	У		У		
	Number of Clients Over Time	У		У		
	Top Application Traffic Over Time	У		У		
	Top N Applications	У		У	У	
	Top N Clients (In and Out)	У		У	у	
	Average Packet Loss	у	у			
	Client Conversations	у		у		
	Client Traffic	у		у		
	IP Traffic Classification	У		У		
	Top N Applications	У		У		
	DSCP Classification	у		у		
	RTP Conversations Details	у	у			
	Top N RTP Streams	у	у			
	Voice Call Statistics	у	у			
	Worst N RTP Streams by Jitters	у	у			
	Worst N RTP Streams by MOS	у				
	Worst N Sites by MOS	у				
	Worst N Site to Site Connections by KPI	у	у		у	

The following table shows how the application-specific dashlets get populated in Cisco Prime Assurance:

#### NetFlow

Once we have verified that NetFlow is enabled on devices and directed to Cisco Prime Infrastructure, we are now ready to turn on monitoring for NetFlow. Just as for Device and Interface Health, all it takes is provisioning the appropriate monitoring template and deploying it. You can start out by going to **Design > Monitoring Configuration > Features > Flexible NetFlow**, choosing the templates based on what was discussed in an earlier NetFlow section, filling out the appropriate details, and saving the template. The template will be instantiated with the new name as specified in the header under My Templates. You can then navigate to **Deploy > Monitoring Deployment**. Look for the template you just created. In this case it's called "RTP-Branch-NetFlows". Looking at the figure on the right, templates with an orange ball with a right arrow are already deployed, and the templates with a green ball with a right arrow are the ones that are still not deployed. Once the template is deployed, dashlets should start populating the data after a couple of polling cycles.



#### WAN Optimization - Cisco Wide Area Application Services

Cisco Wide Area Application Services (WAAS) devices and software help you to ensure high-quality WAN enduser experiences across applications at multiple sites. You can refer to the following URL <u>http://wwwin.cisco.com/dss/adbu/waas/collateral/Using%20NAM%20in%20a%20WAAS%20Deployment.pdf</u> for various scenarios for deploying WAAS in your network.

Once you have deployed your WAAS changes at candidate sites, you can navigate to **Operate > WAN Optimization** to validate the return on your optimization investment. Cisco Prime Infrastructure also allows you to monitor WAAS-optimized WAN traffic by navigating to **Operate > WAN Optimization > Multi-Segment Analysis**. Click the **Conversations** tab to see individual client/server sessions, or the **Site to Site** tab to see aggregated site traffic. Some of the key dashlets to help with WAAS monitoring are detailed in the following table:

Dashlet	Description
Transaction Time (Client Experience)	Graphs average client transaction times (in milliseconds) for the past 24 hours, with separate lines for optimized traffic and pass-through traffic (in which optimization is turned off). With optimization enabled, you should see a drop in the optimized traffic time when compared to the pass-through time.
Average Concurrent Connections (Optimized versus Pass-through)	Graphs the average number of concurrent client and pass-through connections over a specified time period.
Traffic Volume and Compression Ratio	Graphs the bandwidth reduction ratio between the number of bytes before compression and the number of bytes after compression.
Multisegment Network Time (Client LAN-WAN - Server LAN)	Graphs the network time between the multiple segments.
Average and Maximum Transaction Time	The time between the client request and the final response packet from the server. Transaction time will vary with client uses and application types, as well as with network latency. Transaction time is a key indicator in monitoring client experiences and detecting application performance problems.
Average Client Network Time	The network time between a client and the local switch or router. In WAAS monitoring, client network time from a Wide Area Application Engine (WAE) client data source represents the network round-trip time (RTT) between the client and its edge WAE, while client network time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
Average WAN Network Time	The time across the WAN segment (between the edge routers at the client and server locations).
Average Server Network Time	The network time between a server and NAM probing point. In WAAS monitoring, server network time from a

Dashlet	Description
	server data source represents the network time between the server and its core WAE.
Average Server Response Time	The average time it takes an application server to respond to a request. This is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application server resources, such as the CPU, memory, disk, or I/O.
Traffic Volume	The volume of bytes per second in each of the client, WAN, and server segments.
Average and Maximum Transaction Time	The time between the client request and the final response packet from the server. Transaction time will vary with client uses and application types, as well as with network latency. Transaction time is a key indicator in monitoring client experiences and detecting application performance problems.

# Monitor/Troubleshoot a Wireless Network RRM/Clean Air

RF profiles and groups are supported in Cisco Prime Infrastructure for both RF profile creation templates and AP group templates. If you use Cisco Prime Infrastructure to create the RF profiles through the creation of templates, this gives the administrator a simple way to create and apply templates consistently to groups of controllers. The process flow is the same as was previously discussed in the controller feature set with some minor but important differences.

The process is the same as previously discussed in that you first create RF profiles, and then you apply the profiles through the AP groups. There are differences in how this is done from Cisco Prime Infrastructure and in the use of templates for deployment across the network.

# **Build RF Profile**

With Cisco Prime Infrastructure there are two ways that you can approach building or managing an RF profile. Choose **Configure > Controllers**, then click the IP address of the controller and choose **802.11 > RF Profiles** in order to access profiles for an individual controller.

Properties	>	RF Profiles : Add From Template
System	>	Contractily NO Translate Fullets for 'NF Durille' to starts from
WLANs	>	currently NO Template Exists for RF Profile to create from.
FlexConnect	>	To create a New Template for 'RF Profile' click here to get redirected to template creation page.
Security	>	
Access Points	>	
802.11	~	
ᡖ 802.11 General		
ᡖ Load Balancing		
ᡖ Band Select		
ᡖ Preferred Call		
ᡖ Media Stream		
💾 RF Profiles		
SIP Snooping	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	ᢣ᠋᠆ᠧᡔᢍᡟᡟᡊᢦᠴᡗᠧᡡᠵᡡᡊ᠇᠆᠆᠐ᡐᠬᠬᡐᠧᡡ᠆᠆᠆ᡔᡧᡐᡐᡗᡐ᠆᠆᠆᠆ᡔᡘ᠔ᢦᡇᡘᠧ᠆᠆ᢣᢦ᠆ᡇᠬ᠆ᡔᠬ

The figure below displays all the RF profiles currently present on the chosen controller and allows you to make changes to profiles or AP group assignments. The same limitation as with the controller GUI is in effect in regard to a profile that is currently applied to an AP group. You have to disable the network or unassign the RF profile from the AP group.

System	>	RF Profiles Contro	ller Templates				г	- Select a command - 💌 🕜
WLANS	>	Configure > Controller Ter	nplate Launch Pad > ou	2.11 > RF Profiles V			L	
FlexConnect	>	Template Name	Profile Name	Description	Radio Type	Applied To Controllers	Applied To Virtual Domains	Last Saved At
Security	>	BldgO-RF-Profile	BldgO-RF-Profile	Default 802.11b/g Template	802.11b/g	0	0	2012-Sep-27, 21:09:22 UTC
802.11	~							
ᡖ Load Balancing								
🏭 Band Select								
ᡖ Preferred Call								
🎳 Media Stream								
H RF Profiles								
🖶 SIP Shooping								

When you create a new profile, Cisco Prime Infrastructure prompts you to choose an existing template. If this is the first time it is being accessed, you are directed to the Template Creation dialogue for an 802.11 controller template.

You may also navigate to **Configure > Controller Template Launch Pad > 802.11 > RF Profiles** (see figure on left) in order to go to the controller template launch pad directly.

Ternolata Nan	88				
Profile Name			=		
Description					
Radio Tuna		902.115			
Radio Type IPC		002.118			
Minimum Pow	er Level Assanment (-10 to 30 dBm)	-10			
Maximum Pow	ver Level Assignment (-10 to 30 dBm)	30			
Power Thresh	nold v1(-80 to -50 dBm)	-70			
Power Thresh	nold v2(-80 to -50 dBm)	-67			
)ata Rates 🕖		hourse and hourse	High Density Configurations		
6 Mbps	Mandatory 💌		Maximum Clients(1 to 200)	200	
9 Mbps	Supported 💌		Multicast Configurations	10	
12 Mbps	Mandatory 💌		Multicast Data Rate (i)	auto	
18 Mbps	Supported 💌		Coverage Hole Detection		(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
24 Mbps	Mandatory 💌		Data RSSI(-90 to -60 dBm)		-80
36 Mbps	Supported 💌		Voice RSSI(-90 to -60 dBm)		-80
48 Mbps	Supported 💌		Coverage Exception(1 to 75)	Clients)	3
54 Mbps	Supported 💌		Coverage Level(0 to 100 %)		25
			Load Balancing		
			Window(O to 20 Clients)	5	
			Denial (1 kg 10)	2	

In both cases, a new RF profile is created in Cisco Prime Infrastructure through the use of a template. This is a preferred method, since it allows the administrator to use the workflow of Cisco Prime Infrastructure and apply templates and configurations to all or select groups of controllers and reduce configuration errors and mismatches.

Complete these steps:

- 1. In order to create an RF profile template, choose **Add Templates** from the pull-down menu at the top right of the screen as shown in the figure at right.
- 2. Configuration of the template/settings is almost identical with the addition of a template name. Make this descriptive for easy recognition in the future. Change settings as needed or required and choose **Save** as seen in the figure below



**Note:** If you choose a threshold value for Transmit Power Control Version 2 (TPCv2) and it is not the chosen TPC algorithm for the RF group, then this value is ignored.

**TIP:** A simple setting to change for validation is the minimum TPC power. The minimum power can be raised if you choose a dBm value that is more than the current power level assigned by Radio Resource Management (RRM). This helps to validate the RF profiles operation.

3. Once you click **Save** the options at the bottom of the screen change as shown in the following figure (below):

Save	Apply to Controllers	Delete	Cancel
------	----------------------	--------	--------

Choose **Apply to Controllers** and the controller dialogue box appears to display the list of controllers managed by this server as shown in the figure below

4. From the figure on the right, Select **Save Config to Flash** box, then select the controller that you wish to have the profile available on, and click **OK**.

Cont Config	Controller Templates > Apply to Controllers Configure > Controller Template Launch Pad > 802.11 > RF Profiles > Controller Templates > Apply to Controllers							
🔲 Sav	ve Config to Flash after apply boot Controller after apply							
	IP Address	Controller Name						
	171.69.217.67	WCS-5508-sim1						
OK	Cancel							

5. You can see the controller template results as shown in the figure below:

Controller Template 'BldgO-RF-Profile' > Template Results Configure > Controller Template Launch Pad > 802.11 > RF Profiles > Controller Template 'BldgO-RF-Profile' > Template Results						
Controller Name	Operation Status	Reason				
171.69.217.67 WCS-5508-sim1 Success -						
	ch Pad > 802.11 > RF Profiles Controller Name WCS-5508-sim1	ch Pad > 802.11 > RF Profiles > Controller Template 'BldgO-RF-Profile       Controller Name     Operation Status       WCS-5508-sim1     Success				

Now when you view the RF profiles screen, you can see the new template created as shown in the figure below.

System	>	RF Profiles Control	ler Templates					Ardd Template
WLANs	>	Coningure > Controller Lem	ipiate Launch Pad > 00.	2.11 > RF Promes V				Select a command
FlexConnect	>	Template Name	Profile Name	Description	Radio Type	Applied To Controllers	Applied To Virtual Domains	Apply Templates Delete Templates
Security	>	BldgO-RF-Profile	BldgO-RF-Profile	Default 802.11a Template	802.11a	0	0	2012-Sep-27, 21:16:57 UTC
802.11	~							
ᡖ Load Balancing								
晶 Band Select								
ᡖ Preferred Call								
🎳 Media Stream								
H RF Profiles								
SIP Spopping	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The previous steps can be repeated in order to create and apply additional templates as required, for example, for 802.11b.

#### Apply RF Profiles to AP Groups

As with the WLC configuration for RF profiles, newly created profiles can be applied to a controller through the use of AP groups they are assigned to. In order to do this, either a previously saved AP group VLANs template or a newly created template can be used.

Choose Configure > Controller Template Launch Pad and choose AP Group as shown in the figure below.

System	Controller Template Launch Pad	Controller Template Launch Pad			
💾 General	Configure > Controller Template Launch Pad				
ᡖ SNMP Community	System	-			
	General 🕖	New			
	SNMP Community 🕖	New			
Toles	Network Time Protocol 🛈	New			
ᡖ AP Username Password	User Roles 🕖	New			
ᡖ AP 802.1X Supplicant Cr	AP Username Password ①	New			
ᡖ Global CDP Configuration	AP 802.1X Supplicant Credentials 🛈	New			
H DHCP	Global CDP Configuration ①	New			
	DHCP 1	New			
Dynamic interface	Dynamic Interface ①	New			
ᡖ Interface Groups	Interface Groups 🕧	New			
ᡖ QoS Profiles	QoS Profiles (1)				
🗄 AP Timers	AP Timers 🛈				
旹 Traffic Stream Metrics QoS	Traffic Stream Metrics QoS $\widehat{\ell}$				
WLANs	> Williams	-			
FlexConnect	> WLAN Configuration ①	New			
Security	> AP Group (i)	New			

In order to create a new template, choose **New** and fill in the required information. See the figure below.

System	New Controller Tem     Configure > Controller Temp	i <b>plate</b> ilate Launch Pad > WLANs > AP Group > Ne	ew Controller Template	
WLANs	<ul> <li>Name</li> </ul>	PI_HQ_Deploy		
🏭 WLAN Configuration	Description (Ontional)			
旹 AP Group	Coptionally		8	
FlexConnect	> WLAN Profiles	RF Profiles Venue Group		
Security	> Each AP Group can cor	ntain up to 16 WLAN Profiles.		
802.11	>			
802.11a/n	> WLAN Profile	Name	Interface / Interface Group (G)	NAC Override Edit
802.11b/g/n	> IFM Emulation	*	management • virtual •	
Mesh	> Add Remove			
Management				

Choose the RF Profiles tab in order to add RF profiles as shown in the figure (above).

System	>	New Controller Templa Configure > Controller Template	te Launch Pad > WLANs > AP Group > אפע	v Controller Template	
WLANs	~	Name	PI_HQ_Deploy		
ᡖ WLAN Configuration		Description (Optional)			
🗄 AP Group		(optional)			
FlexConnect	>	WLAN Profiles R	F Profiles Venue Group		
Security	>	802 11a Radio		RidaO-RE-Profile	-
802.11	>	802.11b/g Radio		none	-
802.11a/n	>				
802.11b/g/n	>	Create new RF profile.			

System	>	New Controller Template Configure > Controller Template Launch Pad > WLANs > AP Group > New Controller Template
WLANs	~	Name PI_HQ_Deploy
🗄 WLAN Configuration		Description
🗄 AP Group		(uptional)
FlexConnect	>	WLAN Profiles RF Profiles Venue Group
Security	>	▼ Venue Config
802.11	>	Venue Group Business
802.11a/n	>	Venue Type Bank
802.11b/g/n	>	Operator Class
Mesh	>	
Management	>	81 83 84 112 113 115 116 117 118
CLI	>	119         120         121         122         123         124         125         126         127
Location	>	
IРvб	>	▼ Multiple Venue List
PMIP	>	Multiple Venue List
		X Delete 👷 Add Row
		Venue Language Venue Name
		🗹 ENG California

In Cisco Prime Infrastructure 2.0, you can choose the **Venue Group** tab in order to add venue information as well. (See the figure above.)

If you save the template, a warning message may appear. As stated in the previous message, the change of the interface that the assigned WLAN uses disrupts the VLAN mappings for FlexConnect APs applied in this group. Ensure that the interface is the same before you proceed.

Once you choose OK, the dialogue is replaced with more options. Choose the **Apply to Controllers** option as shown in the following figure.

```
Save Apply to Controllers ... Delete Cancel
```

Choose the controllers to which the template needs to be applied as shown in the figure below.

Con Config	troller Template 'Std_AP gure > Controller Template Launch Pa	_Group' > Apply to Control d > WLANs > AP Group > Controller	llers Template 'Std_AP_Group' > Apply to Controlle			
() A О А	pply to controllers in the selecte pply to controllers selected direc	d Config Groups tly				
<ul> <li>Save Config to Flash after apply</li> <li>Reboot Controller after apply</li> <li>Apply AP Group to Access Points link will not be visible if Reboot Controller after apply option is enabled.</li> </ul>						
	IP Address	Controller Name	Config Group Name			
	171.69.217.67	WCS-5508-sim1				

Cisco Prime Infrastructure responds with operational status (see the figure below) on whether the template was successfully applied to the selected controllers.

171.69.217.69 IFM-CONTROLLER2 Success -	

If the template was not pushed successfully, NCS provides a message that states the reason for the failure. In this example, the RF profile that is applied to the group is not present on one of the controllers to which the template was applied.

Apply the RF profile again, specifically to that controller, and then reapply the AP group in order to generate a successful message.

Once the AP group has been deployed with the RF profiles applied (click the **Apply to Access Points** button), only access points attached to the controllers where the AP group was deployed successfully are available to select from.

**Note:** Until this point, no real changes were made to the RF infrastructure, but this changes when APs that contain new RF profiles are moved into the group. When an AP is moved into or out of an AP group, the AP reboots to reflect the new configuration.

Choose the APs you want to add to the AP group and choose OK. A warning message appears. NCS displays the status of the change.

# Monitor/Troubleshoot Clients and Users

# **Client Visibility**

In NCS 1.0, both wired and wireless monitoring and troubleshooting have been integrated with identity services. Integration between wired/wireless network management has been achieved through three network elements:

- Cisco Wireless LAN Controllers
- Cisco Catalyst<sup>®</sup> Switch security features: AAA, RADIUS, 802.1x and MAC authentication, MAC notification traps (nonidentity clients), syslog (identity clients only)
- Cisco Identity Services Engine (ISE)

All clients - wired and wireless - are displayed in the Clients and Users page (Monitor > Clients and Users).

Wired clients display AP name as N/A. Switch port information is provided in interfaces column as shown in the figure below.

S	Troubleshoot 🛛 👗 Test 👻	Disable Rem	nove 🎯 More	• Track Clients	🚋 Identify Unkr	iown Use	rs					
	MAC Address	IP Address	IP Type	AP IP Address	User Name 🔺	Туре	Vendor	Device Name	Location	VLAN	Status	Interface
0	00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	192.168.152.14	jfields		Intel	AMS-2504-WLC	Root Area	13	Associated	vlan 13
0	00:26:b0:94:1b:6c	192.168.152.37	Dual-Stack	192.168.152.14	jfields		Apple	AMS-2504-WLC	Root Area	13	Associated	vlan 13
0	dc:0e:a1:b9:22:58	192.168.152.27	IPv4	N/A	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6

# Wireless Clients

In order to launch the client-troubleshooting tool, click the button to the left of the client list item. Once the client is selected, click the Troubleshoot icon in the toolbar, as shown in the following figure:



The following window is displayed for the client:

Properties			( <u>)</u> ()
General User Name cbala ⊕ IP Address 171.70.241.40 MAC Address 68:bc:c63:df:4c:6a Vendor Apple Endpoint Type Insknown Client Type Regular Media Type Lightweight Mobility Status Local Hostname dhcp-171-70-241-40.cisco.com E2E Not Supported 802.11u Capable No	Session Controller Name sjc14-wi AP Name Sjc14-4 AP IP Address 171.71.1 AP Type Cisco AI AP Base Radio MAC 64:09:8 Anchor Controller Data No 802.11 State Associa Association ID 43 Port 2 Interface corp1 SSID blizzard Profile Name blizzard Profile Name blizzard Profile Name blizzard Profile Name blizzard Profile 0802.11 VLAN ID 260 AP Mode local Data Switching Unknow	-wic2 1B-AP4 33.42 99:42:4c:40 t t Available ted 1(5GHz)	Security Security Policy Type WPA2 EAP Type PEAP On Network Yes 802.11 Authentication Open System Encryption Cipher CCMP (AES) SIMP NAC State Access Radius NAC State Access Radius NAC State RUN AAA Override ACL Name none AAA Override ACL Name none ACL Name none ACL Name none ACL Applied Status N/A FilexConnect Local Authentication No Policy Manager State RUN Authentication ISE Data Not Available Authoriteation Forbile Name Data Not Available Posture Status Unknown TrustSec Security Group Data Not Available Windows AD Domain Data Not Available
oubleshoot	✓ 802.1X Authentication	🛷 IP Address Assignment	Successful Association
Problem No issues found with client connectivity	Recommer No recom • Search • Open or	idation mended actions Cisco Support Community Update a service request	

Log messages can be retrieved from the controller with the use of the Log Analysis tool, as shown in the following figure:

Debug and Analysis	
Click <b>Start</b> to begin capturing log messages from the controller. (It is ne get number of messages have been collected, click <b>Stop</b> .	*
Run Stop Clear Export	<u>A</u>
Status Message	<u></u>
Select LogMessages:	0
802.11 Initialization (0) 802.1x Authentication (0) PEM Messages(0)	<b>X</b>
DHCP Messages (0) AAA Messages(0)	<b>**</b>

Refer to the Policy Enforcement Module (PEM) for more information on the PEM state.

# The Event History tool provides users with event messages from clients and APs, as shown in the following figure:

Event History		
Recent 10 Client Events		
Message	Date / Time	<u></u>
Client 'c8:bc:c8:df:4c:6a (cbala, 171.70.241.40)' is deauthenticated from interface '802.11a/n' of AP 'SJC14-41B-AP5' with reason code '1(Unspecified)'.	2012-Oct-12, 15:05:31 PDT	
Client 'c8:bc:c8:df:4c:6a (cbala, 0.0.0.0)' is deauthenticated from interface '802.11a/n' of AP 'SJC14-41B-AP5' with reason code '1(Unspecified)'.	2012-Oct-12, 14:44:10 PDT	
Client 'c8:bc:c8:df:4c:6a (cbala, 171.70.241.40)' is deauthenticated from interface '802.11a/n' of AP 'SJC14-41B-AP5' with reason code '1(Unspecified)'.	2012-Oct-12, 12:11:29 PDT	
Client 'c8:bc:c8:df:4c:6a (cbala, 0.0.0.0)' is deauthenticated from interface '802.11a/n' of	2012-Oct-12, 09:13:39 PDT	
Recent 10 AP Events		
Message	Date / Time	A
Failed to authorize AP '00:1f:29:c9:85:5c' with certificate type 'Unknown' on controller '171.71.128.78', 'AP Authorization entry does not exist in the Controllers AP Authorization List.'	2012-Oct-12, 15:38:30 PDT	
Failed to authorize AP '00:c0:9f:cd:00:1d' with certificate type 'Unknown' on controller '171.71.128.78', 'AP Authorization entry does not exist in the Controllers AP Authorization List.'	2012-Oct-12, 15:38:17 PDT	
Failed to authorize AP '00:1f:29:c9:85:5c' with certificate type 'Unknown' on controller	2012-Oct-12 15:20:15 PDT	~

# Test Analysis Tool (CCXv5 Clients)

CCXv5 clients are client devices that support Cisco Compatible Extensions version 5 (CCXv5). You can now have troubleshooting capabilities for these clients in the Test Analysis section.

Client Troubleshooting 🛭 < 🔓 ba	ck			
Properties				
Test Analysis				
The following tests are available for clie	ents. Use the checkboxes to select the test(s) you would like t	o perform, then click <b>Start</b> . Click <b>Stop</b> to halt the tests. Wi	nen a test is completed, click on	the test status
to view the results.				
Select Diagnostic Test	Input1	Input2	Status	Results
DHCP			Not initiated	None
IP Connectivity			Not initiated	None
DNS Ping			Not initiated	None
DNS Resolution	Name to resolve:		Not initiated	None
802.11 Association	AP name: AP_ZEST_EC-802.11g	Profile: usdm-8021x	Not initiated	None
802.1x Authentication			Not initiated	None
Profile Redirect	Client Profile Number:		Not initiated	None
Start Stop Frame				2
	L			
Results to require sublable				
sults results available.				

# Wired Clients

Cisco Prime Infrastructure 2.0 provides integrated management of wired and wireless devices/clients. Cisco Prime Infrastructure 2.0 also provides monitoring and troubleshooting for wired and wireless clients. SNMP is used to discover clients and collect client data. ISE is polled periodically to collect client statistics and other attributes to populate related dashboard components and reports.

If ISE is added to the systems and devices are authenticating to it, the Client Details page displays additional details labeled as Security within the Client Troubleshooting, as shown in the following figure:

<ul> <li>Properties</li> </ul>		
General User Name jfields ⊕ IP Address 192.156.152.37 MAC Address 00:26.b0:94:1b:6c Vendor Apple Endpoint Type Apple-Device Client Type Regular Media Type Lightweight Mobility Status Local Hostname Data Not Available E2E Not Supported 802.11u Capable No	Session Controller Name AMS-2504-WLC AP Name NMTG-AP3500-2 AP IP Address 192.166.152.14 AP Type Cisco AP AP Base Radio MAC 04:c5:a4:f2:3f:60 Anchor Controller Data Not Available 802.11 State Associated Association ID 1 Port 1 Interface vian 13 SSID AMS-D011X Profile Name AMS-d011x Profile Name AMS-d011x Protocol 802.11g VLAN ID 13 AP Mode local Data Switching Unknown Authentication Unknown	Security Security Policy Type WPA2 EAP Type PEAP On Network Yes 802.11 Authentication Open System Encryption Cipher COMP (AES) SNMP NAC State RUN AAA Override ACL Name none AAA Override ACL Name none AAA Override ACL Name none ACL Applied Status N/A FlexConnect Local Authentication No Policy Manager State RUN Authentication Profile NameDefault-Corporate-P Posture Status Not Applicable

In order to navigate to **Operation > Clients and Users**, select a client, and click the Troubleshoot icon on the tools menu at the top of the page, as shown in the following figure:

Clients and Users							
	Troubleshoot	🍐 Test 👻	Disable	Remove	More 👻	Track Clients	🚋 Identify Unknown Users

This takes the user to the page shown in the screen shot below. In this example, the client device has link connectivity, but failed IP connectivity.

Troubleshoot	Link Connectivity       Ink Connectivity     Image: Authoritation       Image: Authoritation     Image: Authoritation	*
Problem Client could not complete DHCP interaction	Recommendation         1. Verify that the DHCP server is reachable.         2. Verify that the DHCP server is configured to serve the WLAN.         3. If DHCP bridging mode is enabled and the client is configured to get an address from the DHCP server, verify that the local DHCP server is present.         4. Verify that the client has a static IP address configured and is generating IP traffic.         5. Ensure that the DHCP servers, ensure they are not configured with overlapping scopes.         • Search Cisco Support Community         • Open or Update a service request	

On the right side of the screen, there is a tool bar with these items, all related to troubleshooting:

- Client Troubleshooting Tool
- Log Analysis
- Event History
- Context Aware History

Event History provides messages related to connectivity events for this client. In this example, the client failed to successfully authenticate. Date/time is provided to assist the network administrator in troubleshooting this client.

ISE provides authentication records to NCS through the REST API. Network administrators can choose a time period for retrieving authentication records from ISE. In the example in the following figure, the authentication record indicates that the user was not found in the ISE database.

Stendis Services Engine				Batt
e Las	-			*
D Between Dere STORSTON	Philitiwal	Tene LE x DE x 3E x		£.
Apd Date 12(5)(35/5	Philippini	Tprop 1.7 - 38 - 33 -		-
-Submit-				12
Authentication Records				1
Cene	2004	Falues Research	(m)	
Feb 16, 2011 08:27 49 PM	Authentication Falled.	22050 Subant not found in the job/liceble abortity standor	AO-Ow	

# **Alarms and Events**

Alarms and events provide a single page view of all alarms and events for wired and wireless infrastructure. Persistent alarm summary and alarm browser are displayed at the bottom right of the screen (the figure on the right) regardless of what screen the user is on. Next to it is the Alarm Browser view that shows all the alerts based on severity and device types as shown in the figure below.

		1,0500,001	Anna Summary	N 🖃 🖼
				(8)
	1	10000000		
	critical	Major	Minor	
Alarm Summary	35	0	93	
ΔP	0	0	1	
Application Performance	0	0	0	
Osco Interfaces and Modu	e ()	0	0	
Controler	13	0	0	
Coverage Hole	0	0	0	
Mesh Links	0	0	0	
Mability Service	0	0	0	
Performance	0	0	0	
Roque AP	0	0	78	

#### **Quick Filter**

									Alarm Browser	A 🔲 🕲
								5	elected D   Total 118	ð 🖗 .
0	han	ge Status	SASSIGN Annotation	XDelete	Email Notification	eshoot		Show All		- 8
		Sevenity	Massage	Status	Failure Source	Timestamp	- Owner	Category	Condition	
	۶	🔕 Criti	Port '9' is down on de	Not Advn	If ThirdpartyInterface 1	September 14, 2012		Thrd Part	Thipdparty Contr	-
	۲	🔞 onti,	Port '2' is clown on cle	Not Adkn	If ThirdpartyInterface 1	September 14, 2012		Owner: Sorta	ible cparty contr	1
	۲	🔞 Criti	Port '3' is down on de	Not Advn	IfThirdpartyInterface 1	September 14, 2012		Third Part	Thirdparty Contr	
	•	🔕 onti j	Port '5' is down on de	Not Ackn	If ThirdpartyInterface 1	September 14, 2012		Third Part	Thirdparty Contr	
	٠	😣 Criti	Port '6' is down on de	Not Adm.	If Thirdparty Interface 1	September 14, 2012		Third Part	Thirdparty Contr	
	۲	🔕 oriti	Port '7' is down on de	Not Ackn	If ThirdpartyInterface 1	September 14, 2012		Third Part .	Thirdparty Contr	
	۲	🙁 Criti	Port '6' is down on de	Not Adkn	IfThirdpartyInterface 1	September 14, 2012		Third Part	Thirdparty Contr	
	Þ.	🛕 Mino	Rogue AP '00:1d a1:7	Not Ackn	Rogue AP 00:1d:a1:77	September 14, 2012		Rogue AP	Unclassified Rogu	
	۶	🛕 Mino	Rogue AP '00:1d:a1:7	Not Adkn	Rogue AP.00:1d:a1:77	September 14, 2012		Rogue AP	Undassified Rogu.	-
						😤 Support Cases	Alarm Browse	Alarm Sum	mary 🔕 35 🖁 O	<u>4</u> 83

Almost all of the tables in Cisco Prime Infrastructure have a quick filter widget. This quickly allows users to filter through the table, especially when there are many rows involved. This is very useful with alarms and events or clients and users. The figure (below) shows how quickly correct alarms can be filtered with this.

O Cha	ang	e Status	🔔 Assign 🛛 🔯 Anno	otation 🛛 🔀	Delete 🕞 Email Notificat	ion 🔊	Show	Quick Filter	*	3
	2	Severity	Message	Status	Failure Source	Timestamp -	Owner	Category	Condition	1
		S C	Port '9' is down on	Not Ack	IfThirdpartyInterfa	Last 15 minutes		Third Pa	Thirdparty Co	
		S C	Port '2' is down on	Not Ack	IfThirdpartyInterfa	Last 24 hours		Third Pa	Thirdparty Co	
		8 C	Port '3' is down on	Not Ack	IfThirdpartyInterfa	Last 5 minutes		Third Pa	Thirdparty Co	=
		8 C	Port '5' is down on	Not Ack	IfThirdpartyInterfa	Last 7 days		Third Pa	Thirdparty Co	
		8 C	Port '6' is down on	Not Ack	IfThirdpartyInterfa	Last o nours		Third Pa	Thirdparty Co	
						Last nour				

#### **Creating Advanced Filter**

The Advanced Filter, as the name implies, allows user to filter on the content with complex rules. The following figure shows the Advanced Filter being used with more complex rules. These filters can be saved for one-click use the next time they are needed.

O Cha	ange Status	🔔 Assign 🛛 🔯 Anno	tation 🛛 💥 Delete	Email Notificatio	on » Show	Advanced	l Filter	- 6
Match Filter	the followin Timestamp	g rule:	Is exactly (or equ	uals) 🔹 La:	st hour 🔹 💼	+ Go	Clear Filter	3
	Severity	Message	Status Fai	lure Source	Timestamp	- Own	er Categor	Save #
	🛕 Mi	Interference thres	Not Ack AP	NMTG-AP3500	September 14, 2012 2:18:59 AM PE	T	AP	Radio

# **Trigger Packet Capture from Cisco Prime Infrastructure**

Cisco Prime Infrastructure provides a very flexible solution for capturing packets throughout your network. You can either manually trigger a packet capture or automatically specify the capture based on some advanced parameters, so that it will be triggered once a threshold level is breached. In both of these solutions, packets can be captured locally on the NAM or they can be stitched from multiple NAMs and stored in Cisco Prime Infrastructure.

#### Manual Packet Capture from Cisco Prime Infrastructure

In order to do an ad hoc packet capture, you can navigate to **Operate > Packet Capture** (under Operational Tools) **> Capture Sessions**. If you are coming to this page for the first time, you may not have any capture profiles set up. In order to create a new profile, click **Create** and fill in all the criteria for capturing a particular traffic. If you have a need to capture a particular type of traffic all the time, it may a good idea to proactively create those profiles and test them out before automating them, as will be shown in the next section.

0	Pac	:ket Ca	pture   Capture Sessio	ns				
1	Edit	X	Delete 🜔 Start 🔘 Stop	👩 Create				
			Name	NAM	Start Time 👻	Size (MB)	Packets	State
			SharePoint					
			SharePoint	Campus-NAM3.eset-c	2012-Aug-30 8:58:55 PDT	10	0	Paused

Once the profile is defined, you can test it out by clicking **Start**, as shown in the preceding figure. See if the packets are captured correctly. You can then use these profiles for automatically capturing packets.

#### Automating Packet Capture Using Cisco Prime Infrastructure

Feature (	ategory 17	noloation	1
Tompisto I	Instance A	militation Removes Japa M	j otvor (dofault)
Tempate 1		opication response nine m	letik (deradik)
	Type [4	RTUIDAR *	J.
Matric	Daramotorr		
F	Edit Thresh	old Settings	
Eac	Paramet	ers	Threshold Setting: avoRspTime
CALCULATION OF THE OWNER			
] *F	 	Q.,	Greater Than 1000 Absolute 3 times. 🔶 🛛 ALARM CRITICAL, NAM Sessions SharePoint 🗢
] *F ] nu ] lati	√⊐ + avgRa	pTime	Breater Than 1000 Absolute 3 times.
nu lati	dia ≁   avgRa	pTine	GreaterThan 1000 Absolute 3 times.     ALARM CRITICAL, NAM Sessions SharePoint     Seventy [CRITICAL , ] Packet Capture [SharePoint]
* ⊧   nu   latu   avr	نې خ avgRa	pTine	GreaterThan 1000 Absolute 3 times.      ALAFM CRITICAL, NAM Sessions SharePoint     Seventy CRITICAL     P Packet Capture SharePoint

There are times when you want to capture packets based on a trigger. There is no way to find out ahead of time when the trigger will happen. For example, if you are trying to meet the SLA for AvgRespTime for an application, you may want to start the packet capture if the response time exceeds the predefined time. You can easily achieve this by combining threshold and packet capture in Cisco Prime Infrastructure. Navigate to **Design > Monitoring Configuration > Features > Thresholds**. When you click a threshold template, you can create a new instance from it. Besides the header information, you can select thresholds based on your interest from Traffic Analysis, Application, Voice/Video Signaling, Voice/Video Data, Interface Health, Device Health, and NAM Health. It would be a good idea to explore these options and see what types of trigger points each of them has. Once you select the category for capture, you can then select the subcategory. All the trigger points can then be seen. In order to change any of them, simply select that row and edit the threshold as shown in the image above. You can see (figure above) that we have chosen to alert and start capturing Sharepoint traffic if the AvgRespTime exceeds the default value.

				đ	Capture Sessio
				Selected 1   Total Top Level Rows 5	) 
🕻 Decode 🔔 Me	rge 🎂 Export 🛛 🚟 Copy To 🗙 Delete 😤 Add Folder 🖉	View Jobs		Show All	• 15
Name	<ul> <li>Size (MB)</li> </ul>	Start Time	End Tin	ne	
ACC-NAM2	204.cisco.com				
Campus-N/	AM3.eset-disco.com				
✓ pktcapm	nr1m1_1.pcap 10.00		2012-A	ug-25 8:27:23 PDT	
SSS1_1.	pcap 10.00		2012-A	ug-25 8:54:47 PDT	
test_1.p	cap 10.00		2012-5	ep-11 2:31:34 PDT	
DC-NAM22	20.cisco.com				
🔲 pi1					
RTP-NAM-S	SRE.disco.com				
oktranov (m) 1	Ethernet II, Src: Cisco_ca:39:c0 (00:16:9c:ca:39:c0), Dst: 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1361	Cisco_54:0c:00 (00:15:c7:54:0c:00)			
0	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Port: telnet (23), Dst Po	0.4.12.12 (10.4.12.12) rt: 62103 (62103), Seq: 910076717, Ack: 367	1490228, Len:		ŀ
0 1 Packet List	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Port: telnet (23), Dst Po <sup>0</sup> [Expert Info (Chat/Sequence): Connection establish admor	).4.12.12 (10.4.12.12) rt: 62103 (62103), Seq: 910076717, Ack: 367 wledge (SYN+ACK): server port telnet]	1490228, Len:		⊛⊛.
0 1 'acket List	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Port: teihet (23), Dst Po (Expert Info (Chat/Sequence): Connection establish advino	).4.12.12 (10.4.12.12) rt: 62103 (62103), Seq: 910076717, Ack: 367 wledge (SYN+ACK): server port telnet]	1490228, Len:		<b>⊗</b> ⊛.
1 Packet List TCP Stream	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Port: telhet (23), Dst Po <sup>0</sup> (Expert Info (Chat/Sequence): Connection establish adviso	)4.12.12 (10.4.12.12) rt: 62103 (62103), Seq: 910076717, Ack: 367 wledge (SYN+ACK): server port telnet] 	1490228, Len:	Info	♦⊛•
1 Packet List TCP Stream	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Port: tehet (23), Dst Po 0 [Expert Info (Chat/Sequence): Connection establish advior 0000 00 15 c7 54 0c 00 00 15 9c ca 39 c0 81 00 0	14.12.12 (10.4.12.12) rt: 62103 (62103), Seq: 910076717, Ack: 367 Wedge (SYN+ACK): server port telnet]  5 61	1490228, Len:	Info Source port: 5247 Destination port: 40575	<ul> <li></li></ul>
CP Stream C Pkt T D 1 2 2 2 2	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Port: tehet (23), Dst Pc © [Expert Info (Chat/Sequence): Connection establish advino 0000 00.15 c? 54 0c 00 00.15 9c ca. 39 c0 01.00 0 0010 00 05 c? 54 0c 00 00 15 9c ca. 39 c0 01.00 0 0010 00 0.5 c? 54 0c 00 00 15 9c ca. 39 c0 01 00 0 0010 00 0.5 c0 00 42 9c 00 00 34 67 cd 70 0020 00 0.10 0.00 00 00 17 6? cd 25 ab x2 dd	<pre>14.12.12 (10.4.12.12) tt: 62103 (62103), Seq: 910076717, Ack: 367 whedge (SYN+ACK): server port telnet] s 51</pre>	1490228, Len:	Info Source port: 5247 Destination port: 40575 Source port: 40575 Destination port: 5247	<ul> <li></li></ul>
I CP Stream O Pkt T D 1 2 2 2 3 2 3 2	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10           Transmission Control Protocol, Src Port: telnet (23), Dst Por           0           (Expert Info (Chat/Sequence): Connection establish addror           0000         00.15 c7 54 0c 00 00 16 9c ca 39 c0 81 00           0010         00.15 c7 54 0c 00 00 16 9c ca 39 c0 81 00           0020         0c 10 0a 40 cc co 00 17 c2 57 35 ca ab 2d           0020         cc 10 0a 40 cc co 00 17 c2 57 35 ca ab 2d	14.12.12 (10.4.12.12) wt: 62103 (62103), Seq: 910076717, Ack: 36/ wkedge (SYN+ACK): server port telnet]  8 61	1490228, Len:	Info Source port: 5247 Destination port: 40575 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247	<ul> <li></li></ul>
	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Part: tehet (23), Dst Part [Expert Info (Chat/Sequence): Connection establish advice 0000 00 15 c7 54 0c 00 00 15 9 ca 39 c0 81 00 0 001 00 00 45 20 00 34 25 A0 00 0 31 c6 7 cd 70 0020 0c 10 50 46 cd 80 00 17 25 7 35 ca 22 dd 0000 00 08 0a 21 0d 02 15 2a 35 41 12	14.12.12 (10.4.12.12) tt: 62103 (62103), Seq: 910076717, Ack: 367 wedge (SYN+ACK): server port telnet]  5 51T90 a 0 6T90 a 0 6	1490228, Len:	Info Source port: 5247 Destination port: 40575 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247 tineta + 5.6120 (SVN, ACK) Seg=01007	<ul> <li>♦ ⊕ .</li> <li>■</li> </ul>
Packet List           Prop Stream         O           Pkt         T           2         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           3         2           5         2	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Part: tehet (23), Dst Pa 0 [Expert Info (Chat/Sequence): Connection establish advinor 0 000 00 15 c7 54 0c 00 00 15 9c ca 39 c0 81 00 0 001 08 00 45 20 00 36 42 Pa 00 00 37 66 7c 47 0 0020 0c 10 0a 040 co 00 17 52 73 65 ea ba 24 4 0030 7e b4 90 12 0b 50 59 st 00 00 0 24 06 56 40 0 06 0a 22 04 02 15 2a 36 41 £2	14.12.12 (10.4.12.12) rtr 62103 (62103), Seq: 910076717, Ack: 367 weedge (SYN+ACK): server port tehnet]  5 51T90 a 05₹90 a 4₹	1490228, Len:	Info Source port: 5247 Destination port: 40575 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247 tainat > 62103 [SVN, ACK] Seq=91007 Source port: 40575 Destination port: 5247	<ul> <li>♦ ⊕ .</li> <li>■</li> </ul>
Product List           Processor           Processor           Processor           Processor           Part           TOP Stream           Pict           T           2           3          2           3          2           3         2           3         2           3         2           4         O           5         2           6         2	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10           Transmission Control Protocol, Src Port: tehnet (23), Dst Por           © [Expert Info (Chat/Sequence): Connection establish advino           0           0000         00.15 c? 54 0c.00 00.15 9c ca. 39 c0.01.00           010         00.05 c? 54 0c.00 00.15 9c ca. 39 c0.01.00           0010         00.05 c0.05 e4 25 ao.00 03 46 9c ad.00           0020         00.10 0a.04 co.00 17 £2 37 35 ab.22 d           0030         7a.14 90 12.06 15 58 9f 00.00 02 04 05 44 0           0040         08 0a.21 04 02 15 2a.36 41 f2           012-08-25 20.05:43.616164         192.168.152.39         11	14.12.12 (10.4.12.12) wt: 62103 (62103), Seq: 910076717, Ack: 36/ wkedge (SYN+ACK): server port teinet]  8 61	1490228, Len:	Info Source port: 5247 Destination port: 40575 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247 tainat - 62103 (SVN, AG, Seq=91007 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247	◆ ⊕ • ■
I           Packet List           ■TCP Stream           ■ TCP Stream           ● TCP Stream	Internet Protocol, Src: 10.15.12.16 (10.15.12.16), Dst: 10 Transmission Control Protocol, Src Part: tehet (23), Dst Pio D [Expert Info (Chat/Sequence): Connection establish advice 0000 00 15 c7 54 0c 00 00 15 9c ca 39 c0 81 00 0 0010 00 00 52 00 34 82 Pio 00 00 37 66 7c 47 0 0000 00 00 15 c7 54 0c 00 00 15 9c ca 39 c0 81 00 0 0010 00 00 05 20 05 48 2 Pio 00 00 37 66 7c 47 0 0000 00 00 a 21 0d 02 15 2a 36 41 f2 012-08-25 20:05:43.616164 192.168.152.39 11 012-08-25 20:05:43.6161747 192.168.152.39 11	14.12.12 (10.4.12.12) tet 62103 (62103), Seq: 910076717, Ack: 367 wedge (SYN+ACK): server port telnet]  5 €1790 a 6690 a 6690 a 70	1490228, Len:	Info Source port: 5247 Destination port: 40575 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247 tinkat > 62103 (\$VN, ACK) Seq='0107 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247 Source port: 40575 Destination port: 5247	<ul> <li>€ ⊕ .</li> <li>I</li> </ul>

#### **Decoding Packet Capture Using Cisco Prime Infrastructure**

Once the packets are captured, there are two options to decode the capture. The easiest way is to select the packet capture session and click Decode from the Packet Capture homepage (**Operate > Packet Capture**). The capture decode is shown in a pop-up window, which makes it extremely easy to evaluate each and every packet as shown in the figure below.

You could also click the Export button and the .pcap file will be downloaded directly on the client PC. This is useful if you need to perform advance troubleshooting on the capture decode. There is a dimmed Merge button between the Decode button and the Export button, which can be used to merge the .pcap files if more than one file is selected.

**TIP:** If the capture file is not very large (that is, not on the order of GB), it makes sense to decode it in Cisco Prime Infrastructure instead of jumping over to the NAM. Otherwise, you should use NAM instead of Cisco Prime Infrastructure for decoding very large capture files.

#### Miscellaneous Multi-NAM Capabilities Within Cisco Prime Infrastructure

Cisco Prime Infrastructure can serve as a central manager of managers (MoM) if multiple NAMs are deployed in the network. Some of the functionality that Cisco Prime Infrastructure can help with includes:

- Centralized monitoring of NAM health
- · Deploying configurations to multiple NAMs using the CLI configuration templates
- Upgrading NAMs using software image management capabilities
- Using one-click packet capture from multiple NAMs based on a capture policy
- · Proactively capturing packets using threshold breaches

All of these allow users to use Cisco Prime Infrastructure to effectively manage the NAMs, thus making it a very good and stable data source for application visibility.

#### **Remediate Issues**

# **Remediate Wireless Issues**

The following tools available within Cisco Prime Infrastructure may be used in order to remediate wireless issues:

- Cisco CleanAir<sup>®</sup>
- Client Troubleshooting
- AP Troubleshooting
- Audit Tool
- · Security Dashboard
- Switchport Tracing (SPT)
- Apart from these key tools, you can find more tools by navigating to Operate > Wireless (under Operational Tools).

🐯 Operatio Path Tra	onal Tools ce	
Packet C	apture 👻	
Media St	reams	
Wireless	•	
	Guest User	
	Voice Audit	
	Voice Diagnostic	
	Location Accuracy Tools	
	Configuration Audit	
	Migration Analysis	
	Unjoined APs	
	Radio Resource Management	
	RFID Tags	
	Chokepoints	
	Interferers	
	Spectrum Experts	
	WIFI TDOA Receivers	

- Contextual device 360-degree views for easy access to assorted tools:
  - Ping
  - TraceRoute
  - Cisco Discovery Protocol Neighbors
  - WLAN and SSID information

• Active AP and client count

# **Remediate Wired Issues**

The following tools within Cisco Prime Infrastructure can be used to remediate wired issues:

- Wired Client Troubleshooting
- Ad Hoc and Automated Packet Capture
- Device Work Center
- Contextual device 360-degree views for easy access to assorted tools:
  - Ping
  - TraceRoute
  - Cisco Discovery Protocol Neighbors
  - Config Diffs
  - Inventory Details
  - Network Audits
  - Support Forums



# Optimize

# Use Cisco Prime Infrastructure to Optimize the Operation of Your Converged Network

There are several tools availabe within Cisco Prime Infrastructure to optimize your network. Some of the tools that help optimize wireless infrastructure would be:

- Wireless Network Performance (RRM)
- Wired Performance (WAN bandwidth)
- Reports

#### **Dashboard Customization**

Cisco Prime Infrastructure uses the latest dashboard, which uses the latest technology of CSS3, HTML5, as well as AJAX with some charts. All of these allow for easy customization and visualization of data. There two main ways of customizing the dashboards:

- Adding your own dashboard in addition to the ones provided
- · Adding/moving dashlets (aka portlets) from one dashboard to another



First navigate to one of the four existing dashboards as show in the figure above.

	P 00.	¢ -
Add New Dashboard	Edit Dashb	oard
Rename Dashboard Add Dashlet(s) Add/Remove Filter(s) Layout Template Manage Dashboards		
Add New Dashboard Rename Dashboard Add Dashlet(s) Add/Remove Filter(s) Add/Remove Filter(s) Add/Remove Filter(s) Add/Remove Filter(s) Add/Remove Filter(s) Add/Remove Filter(s) Add/Remove Filter(s) Add Remove Fi		×
Display Order Network Device Network Interface Service Assurance In_Performance	*	•
Apply Reset	~	×

You can easily add a new dashboard by going to the top right of the screen and clicking the Edit Dashboard

(iv) icon. You should see a new pop-up as shown in the figure at the right. Depending on where you were in the menu when you clicked the gear icon, a new dashboard will be created under that tree. Type in a suitable name for the dashboard and click the Add button to create a new dashboard. A new tab is reflected immediately. If you created a tab by mistake, you can simply go to Manage Dashboards as shown in the figure at the left and delete the newly created dashboard, and then re-create a new one under the appropriate dashboard.

Y Add/Remove Filter(s)	
Carl Application	Remove
💼 Site	Remove
🕗 Time Frame	Remove
👶 Network Aware	Remove

Note that Add/Remove Filter(s) applies only to the default dashboards and not for the custom dashboards. By default all of these filters will be populated for the default dashboards.

The next step is to populate the new dashboard that you created with content. This is done by adding dashlets to it. There are about 50 preconfigured templates that you can use for various dashboards.

A new dashlet can be added by going to the dashboard where you want it to show up and clicking Add Dashlet(s) from the Edit Dashboard menu. Once you see the list of dashlets, you can simply drag and drop the desired dashlet onto the dashboard. You should see a green bar as a confirmation that the dashlet will stay there, as shown in the figure below

		SSID
	<b>O</b> 1	
	Client Protocol Distribution	
Top 5 S	witches by Client Count	
Client	Count	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

#### **Customizing the Dashlet Content**

		Data Sources	
		(*	0
2012 Contomber 10, 15:41:16 DDT			4
2012 September 18, 15:41:16 PD1		All	
Top N Applications 📼 🔿		1.1.1.1-6111382	
		10.0.101.2-32442	=
Dashlet Title	Top N Applications	10.0.102.2-40095	
Refresh Dashlet	1	10.0.103.2-40048	
Refresh Interval	5 minutes 💌	10.0.105.2-32581	
Sort Order	Descending	10.0.107.2-32630	
No. of Rows	15 (Default)	10.0.109.2-32582	
Traffic Type	All Traffic	10.0.111.2-32443	
Data Type	Rate	10.4.10.254-32444	
		192.168.136.129-NDE-10.0.105.2-I	
Time Frame	Past 1 Hour	192.168.136.129-NDE-192.168.136	-
Data Source	All	0	-
DSCP	All	•	

We can not only customize the dashboard but also the content within the dashlets. At times, you may want to know the rates instead of the volume, or you may want information coming from NetFlow instead of NAM or vice versa. You can configure the dashlet to show just that. First, make sure the needed dashlet already exists in the dashboard. If not, you will need to create it as shown in the previous section. Now click Dashlet Options, as shown in the figure (below).



This will expose all of the configurations that can be tweaked for a given dashlet as shown in the figure (right). You may now use the pull-down menu to select and configure as needed. Some key interesting things to note are data type, traffic type, data sources, and differentiated services code point (DSCP). Each dashlet will have its configuration parameters. Once you are done, click Save and Close to return to the default data view.

# Advance Configuration Topics

# **Identity Services Engine Integration**

Cisco ISE is a next-generation identity and policy-based network access platform that helps enable enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. See the figure above. Cisco Prime Infrastructure manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, Cisco Prime Infrastructure collects additional information about these clients from the ISE and provides all relevant client information to Cisco Prime Infrastructure to be visible in a single console.

Identity Services Engines					
Services > Identity Services Engines					Add Identity Services Engine 💽 🗔
}					Select a command
}					Add Identity Services Engine Delete Identity Services Engine(s)
🖇 🔲 Server Address	Port	Retries	Version	Status	Role
192.168.138.151	443		1.1.0.665	Reachable	Stand Alone

Cisco Prime Infrastructure can be integrated with ISE by navigating to **Design > External Management Servers** (under Management Tools) **> ISE Servers**. You can add a new ISE server by selecting Add Identity Services Engine as shown in the figure above. You will then be prompted for some basic ISE connectivity information (see the figure at left above). Once that is entered, the ISE server is then added to the list. Most of the remaining configuration will need to be done on the ISE itself.

Add Identity Services Er	ngine	
Services > Identity Services Engines	> Add Identity Serv	vices Engine
Server Address	10.1.2.3	
Port	443	
Username	admin	
Password	•••••	
Confirm Password	•••••	
HTTP Connection Timeout	30	(secs
Save Cancel		

**TIP:** ISE has a locking mechanism if the password is entered incorrectly three times in a row. It is extremely important to use the correct credentials when integrating within Cisco Prime Infrastructure; otherwise the ISE web interface will be locked out. Users will then need to log in through the ISE CLI to unlock the web interface.

See "<u>Understanding the Cisco ISE Network Deployment</u>" for detailed ISE configuration tasks that are needed to populate the data consumed by Cisco Prime Infrastructure (the steps are the same as with NCS 1.1/ISE 1.x integration).

# **Automated Deployment**

Automated deployment is a feature that started with Cisco Prime Infrastructure 1.2.1 that eases the pain of deploying new branch routers or switches. With Cisco Prime Infrastructure 2.0, the plug and play gateway is now built into the product itself. This method of provisioning is mainly targeted for branch routers. Normally when a device is provisioned in a new branch or remote site, it needs to be prepared for provisioning. Some network engineers prefer to stage the device completely and ship it to the end location, while others prefer to do a partial staging of the device so that it can come online once it's deployed in the end location. Management systems can then be used to push the full configuration. In both cases, a lot of manual configuration is needed, and it amounts to big delays in deploying a new branch or site.

Automated deployment could be used for places where quick and zero-touch deployments are desired. If a nontechnical staff is deploying the device in a remote branch, this feature will definitely prove to be useful.

See the Cisco Plug and Play Solution Guide for detailed steps for using Automated Deployment at <a href="http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/user/guide/Cisco\_Plug-n-Play-Solution-Guide.pdf">http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/user/guide/Cisco\_Plug-n-Play-Solution-Guide.pdf</a>.

# Managing Converged Access Using Cisco Prime Infrastructure 2.0

Converged Access is the convergence of wired and wireless networks into a unified infrastructure. Cisco is also extending wired infrastructure concepts, features, resiliency, and scalability to the wireless infrastructure. Cisco Converged Access is composed of the following core products:

- The new Cisco <u>Catalyst<sup>®</sup> 3850 Series Switch</u> with integrated wired and wireless functionality through builtin Cisco IOS Software wireless LAN controller (WLC), the new Unified Access Data Plane (UADP) application-specific integrated circuit (ASIC), and enhanced hardware and operating system.
- The new Cisco IOS Software-based Cisco 5760 WLC as appliance.
- The Cisco Catalyst 6500 Series <u>Wireless Services Module 2</u> (WiSM2) or Cisco <u>5508 WLC</u> (available through a software patch in the future).

Starting Cisco Prime Infrastructure 2.0, you can now manage converged access architecture in a simplified manner. This section will go into managing the converged access environment using Cisco Prime Infrastructure 2.0.

**TIP:** Before you jump into managing the 3850 switch using Cisco Prime Infrastructure, make sure the following steps are done:

- Make sure the licenses have been accepted from within 3850. More details can be found at <a href="http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps12686/deployment\_guide\_c07-727067.html#wp9000251">http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps12686/deployment\_guide\_c07-727067.html#wp9000251</a>.
- Make sure the Converged Access devices have a minimum of Cisco IOS-XE 3.2.2 or later running on them.

At a high level, following are the tasks that users will need to do in order to deploy converged access architecture using Cisco Prime Infrastructure 2.0:

Step 1. Set up a mobility domain and its hierarchies for the new mobility architecture

Step 2. Create VLANs and WLANs for the new mobility architecture

### Step 1 - Setting Up a New Mobility Hierarchy Using Mobility Work Center

Mobility Work Center is a new feature within Cisco Prime Infrastructure 2.0, which eases management of Unified Access Switches/Controllers. You can navigate to Operate > Mobility Work Center to get started with creating components within new mobility architecture. This screen displays all the mobility devices that are being managed and their role in the Unified Network architecture (MA, MC, and MO). It is beyond the scope of the deployment guide to go into details of the new mobility architecture, but you can refer to the following web page on the topic to understand MA, MC and MO: <a href="http://www.cisco.com/en/US/netsol/ns1187/index.html">http://www.cisco.com/en/US/netsol/ns1187/index.html</a>.

For devices added to Cisco Prime Infrastructure, existing mobility domains and switch peer groups (SPGa) will be automatically populated in this screen.

TIP: Make sure you have atleast Cisco IOS-XE 3.2.2 running on 3850/5760 devices.

	cha	anged to M	O/MC/MA			their role
Mobility Domains	All	Mobility Devices				Selected 0   Total 3 😽 🚔 🖕
(p •	0 S.	Change Role To Mobility Contro	lier 💁 Change Role To Mobility Agent	S Assign Mobility Group		show All
Domain-katana115		Device Name	Management IP	Wireless Interface IP	Mobility Group	Mobility Role
<ul> <li>katana115</li> </ul>		Edison106	172.19.28.106	10.1.1.3	default	Admin - MC, Operational - MA
spg30		MC	172.18.136.161	35.1.1.6	default	Admin - MC, Operational - MC
spgg11 Default-Domain Domain-MC MC campus2-stack1 All Mobility Devices			_			
1	_ Tree hier	rarchy mobility				

To create a new mobility domain, click the "Create Mobility Domain" button.

Home Design      Deploy      Operate      Report      Administration	P 80.
	Que Create Mobility Domain
All Mobility Devices	Selected 0   Total 2 🚸 🚔 🖕
🕵 Change Role To Mobility Controller 🛛 💁 Change Role To Mobility Agent 💁 Assign Mobility Group	Show All

Users will be prompted to provide a mobility domain name and select devices to be members of the mobility domain.

Create Mobility Domain			×
Mobility Domain Name Mobility Oracle None Select Mobility Domain Member	Devices	Selecter	e 0   Totai 1 🚸 🎡 🖕
Device Name	Management IP	Mobility Group	Wireless Int
katana-1	172.23.208.113	default	50.0.0.3

Similarly, new switch peer groups can be created and devices added in Mobility Work Center.

SPGs on the selected Mobility Con	troller		Selected 0   Total 0 😵 🥸 🕳
Create Switch Peer Group	te Switch Peer Group		
Switch Peer Group Name	No. of Mobility Agents		
		No data available	

nea	the Switch Peer Group			×
Sele	ect Mobility Agents		Selected 0	Total 1 😵 🎡 🖕
	Device Name	Management IP	Wireless Interface IP	Mobility Rol
	im-igwc-1	172.23.208.120	40.000.10	Aamin - MA

Once you click on "Create", you can now add a new switch peer group as shown in figure below.

This creates automatic full-mesh mobility peering between controllers.

#### Step 2 - Create VLANs and WLANs for the New Mobility Architecture

There are two way of creating VLANs and WLANs for the new mobility architecture. If you are not familiar with the CLI commands for the new mobility architecture, it would be beneficial to use the wizard-based Guided Workflow GUI. Guided Workflow walks users in a step-by-step manner in configuring the new mobility architecture. It doesn't allow for advance customization, but you should be able to deploy basic mobility on converged access devices using a **zero-touch deployment model**.

#### Step 2a - Wizard-Based Guided Workflow for Creating VLANs and WLANs

Adding these converged access devices into Cisco Prime Infrastructure is the first place to start. While devices can be added or imported manually as mentioned earlier, it is easier to add them using the Plug and Play Setup (Day 0) guided workflow. This allows for managing a device without any need to console into the device (using the DHCP method). Once Cisco Prime Infrastructure knows the devices, we can run the Initial Device Setup (Day 1) guided workflow to add more wired and wireless related configuration. Plug and Play Setup (Day 0) and Initial Device Setup (Day 1) guided workflow (see the figure on right) are two independent workflows, hence devices discovered by any other means (manual, device discovery, import) can be configured by the initial device setup workflow as well.



In order to, add and configure devices using the Plug and Play Setup workflow, select **Workflow > Plug and Play** Setup.

#### TIP:

- TFTP should not be blocked in the network, as it is used by Cisco Prime Infrastructure to upload files to switches.
- Please use lifecycle view (as shown in figure below) for all configuration and template deployment operations for converged access devices, as classic view is not supported.

cisco Infrastructure	🙆 Home	Design 🔻	Deploy 🔻	Operate 🔻	Report *	Administration 🔻	Workflows 🔻	virtual Domain
Workflows: Plug and Play Setup							Plug and P	lay Setup ice Setup
Before you Begin Create Profile	Save Profile							

In the following figure you create a plug and play profile, which will be applied to ALL devices connected to Cisco Prime Infrastructure by this method. Configuration can be changed later.

Create Profile These credentials will be applied to all devices connecting Pre-deploying on Campus Devices Configuration Details Factory Defaults	to Prime Infrastructure. These credents		
These credentials will be applied to all devices connecting Pre-deploying on Campus Devices Configuration Details Factory Defaults	to Prime Infrastructure. These credenti		
Pre-deploying on Campus Devices Configuration Details Factory Defaults		als will be used for initial configur-	ation but may be changed later.
Configuration Details Factory Defaults			
Properties			
Credentials Show Clear Text			
Cano Guidet			
SNMP Helds*	Confirm	[	All fields are required.
Read-Write Contractly String	Confirm	[	These SNMP v2 community settings will be configured on the device and used by Prime Infraction to use for decruisery or process
near nine connents song	comm	L	
SSH Credentials			
		100-270	All fields are required.
Password	Contrm		Teinet is enabled by default. If you prefer SSH ensure that you have the K9 image. The same credentials will be used for both
Enable Password	Contrm	[	Teinet and SSH.
<ul> <li>Plug and Play Gateway Location</li> </ul>			
	All fields are re	equired.	
"PhP Gateway Host Name GudedWorkHow	This is the loc cateway, s p	ation of the Plug and Play Gatew niled as nart of Prime Infrastructu	vay. You may use the default use, or you may specify an external
"PhP Gateway IP Address 172.28.104.55	gateway inste	ead.	and a branch dense and galage

Once the devices are in the Cisco Prime Infrastructure database, they can be configured using the Initial Device Setup (Day 1) guided workflow. This wizard will help configure devices discovered through Plug and Play Setup or other adding device mechanisms as mentioned earlier.

TIP: The wizard currently supports the Catalyst 2000, 3000, and 4000 Series switches, and 5760 controller.

Navigating to **Workflows > Initial Device Setup** will start the guided **Initial Device Setup** (Day 1) workflow wizard (see the following figure).

	<u>a</u> nome Design • Deploy •	Operate • Report •	Administration <b>*</b>	Workflows *	
orkflows: Initial Device Set	up			K Plug and F	Play Setup
0.0				Initial Dev	vice Setup
efore You Begin Assign to Site	Choose Other Devices Configuration Con	firmation			
fore You Begin					
e following features can be configure	ed				
e following features can be configure	Wireless (Qurrently only 3850 and 5760)	w Mara Dataila			
e following features can be configure Vired Management Details	Wireless (Currently only 3850 and 5760) Mobility Domain, Mobility Group and Swit	▼ More Details			
e following features can be configure Wired Management Details Authentication Settings	Wireless (Currently only 3850 and 5760) Mobility Domain, Mobility Group and Swit Mobility Controllers and Mobility Agents	More Details Downlink port configuration	on is done using Cisc	o Auto Smartports.	
e following features can be configure Wired Management Details Authentication Settings /LAN and Switching	Wireless (Currently only 3850 and 5760) Mobility Domain, Mobility Group and Swit Mobility Controllers and Mobility Agents Provision Enterprise Access	More Details  Downlink port configurati All downlink ports on the	on is done using Cisc target device are as:	to Auto Smartports. sumed to be Data	
e following features can be configure Wired Management Details Authentication Settings /LAN and Switching Jplink	Mireless (Currently only 3850 and 5760) Mobility Domain, Mobility Group and Swit Mobility Controllers and Mobility Agents Provision Enterprise Access Provision Guest Access	More Details  Downlink port configurati All downlink ports on the Ports by default. If a Cisc	on is done using Cisc target device are ass o IP Phone or access	to Auto Smartports. sumed to be Data point is discovered	

Devices are assigned to a site as shown in following figure (below).

TIP: Sites must be created ahead of time as mentioned in the earlier section "Creating Groupings and Sites."

lefore Tou Begin Assig	to Ste Choose Other Devic	as Configuration Confirmation					
sign to Site							
a first step is to identify w	which devices to be configured	Begin by choosing a single site and identifying dev	ices to be assigned to that site. If devices nee	ed to be assigned to diffe	rent stes you will		
in the same this substant even	the each site						
e to use this witard once to device much be accord	e for each site.	afa ét de la Sustem Camera					
e to use this witard onor ch device much be assign	e for each site. ed to a site, even if just the de	efault ste is System Campus.					
we to use this wizard once ch device much be assign dd these devices to the sit	e for each site. ed to a site, even if just the de Y System Campus	efault site is System Campus.					
we to use this witard once ch device much be asign dd these devices to the sit evices	e for each site. ed to a site, even if just the de X System Campus	efault site is System Campus.					Selected 0   Total 0 -
e to use this world once th device much be assign id these devices to the sit twices	e for each site, ed to à site, even if just the de en System Campus	elault ste is System Campus.				Show Al	Selected ( Total 0
e to use this worad once th device much be assign id these devices to the sit invices Host Name	e for each ste. ed to a ste, even if just the de system Campus IP Address	efault ste is System Campus.	Readiness	Image Verson	(CDP Neighbors	Show Al	Selected 0   Total 0

Once assigned to a site (see the figure above), both wired and wireless features configuration can be initiated in the next screen (see the figure below).

Workflows: Init	Device Setup: Choose Other Devices
Q.	. 🗛 . 👃 . 💷 . 🗎
Before You bog	Assign to See Otopie Other Devices Configuration Confirmation
Choose Other	evices
The devices sel available option	ted in the previous step, plus any ensting divices in the same site will be shown in the table below based on the configuration selected. One feature at a time may be configured and re Wried and Wrieless. This allows you to choose existing devices to be configured as well as the new devices.
I would like to	Select Configuration
	Select Configuration- Add wred features to my device(s)
	Add wreless features to my devoels)

In the **Guided Mode**, wired workflow enables users to configure IP management options, login credentials, VLAN(s), basic services, Cisco Discovery Protocol, Autosmart ports, and uplink(s). Autosmart ports can be enabled in the guided mode. Additional information about autosmart ports can be found in the reference section.

	Choose Other Devices						
Before You Begin to :	Site Choose Other Devices	P Management Options Conferences VLAN and Settleting Aut	cSnart Ports, Uplei	+ Confirmation			
Choose Other Devices							
The devices selected in the pre-	ious step, plus any existing de	vices in the same site will be shown in the table below based on the config.	ration selected. (	One feature at a time m	ay be configured		
rid avalable options are wred a	ind wireless. This allows you to	o choose existing devices to be configured as well as the new devices.					
WOULD BRE TO ACCI WITED TEAT	uses to my device(s) *						
Current Site: Sanjose-Bidg18							
Current Site: Sanjose-Bldg18 Devices						0	Selected 2    Tota
Current Site: Sanjose-Bldg18 Devices						Show All	Selected 2    Tota
Current Site: Sanjose Bidg18 Devices	IP Address	Device Type	Readmess	Image Version	CDP Neighbors	Show All	Selected 2   Tota
Current Site: Sanjose-Bidg18 Devices	IP Address 172.28.104.234	Device Type     Orco Catalyst 3850 24P 10(100)1000 PoE+ Ports Layer 2/Layer 3 E.	Readness Ready	Image Version 03.09.27.51P	CDP Neighbors CL-Core-Switch	Show All Status Ti/A	Selected 2 [ Tota
Current Site: Sanjose Bidg19 Devices Host Name Switch GuestAnchor-5760	IP Address 172.28.104.234 172.28.104.241	Device Type Gisco Catalyst 3550 24P 10/1000 PoE+ Ports Layer 2/Layer 3 E. Gisco Striko Wreles LAN Controller	Readness Ready Ready	Image Version 03.09.27.5NP 03.09.27.5NP	COP Neighbors QCore-Switch TCR_Switch	Show All Status 14/A 14/A	Selected 2    Tota
Current Site: Sanjose Bidg18 Devices Host Name Switch GuestAnchor-5760 3950 A	IP Address 172.28.104.234 172.28.104.241 172.28.104.76	Device Type     Goo Catalyst 3950 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E.     Goo S760 Wreeless LAN Controller     Goo Catalyst 3950 45P 10/100/1000 PoE+ Ports Layer 3/Layer 3 E.	Readness Ready Ready Ready Ready	Image Version 03.09.27.5NP 03.09.27.5NP 03.09.27.5NP	CDP Neighbors CL-Core-Switch TOR_Switch TOR_Switch	Show         All           Status         N/A           N/A         N/A	Selected 2 [Tota
Current Site: Sanjose Bidg18 Devices Host Name Switch GuestAnchor-5760 Ø 3850-A Ø 3850-A	P Address 172-28.104.234 172-28.104.241 172-28.104.76 172-28.104.81	Device Type     Gisco Catalyst 3850 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E     Gisco 5780 Wrieleis LAN Controller     Gisco Catalyst 3850 48P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E  Cinco Catalyst 3850 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E	Readness Ready Ready Ready Ready Ready	Image Version 03.09.27.5NP 03.09.27.5NP 03.09.27.5NP 03.09.27.5NP	CDP Neighbors QCore-Switch TOR_Switch TOR_Switch TOR_Switch	Show         All           Status         N/A           N/A         N/A	Selected 2 [ Tota

Follow through the wizard until the end where you have a chance to see the configuration before pushing it on the wire.

	strage contraining of C						
efore You Segn	adign to Ste Choose	Other Devices P Management Options Credencias VLAN and S	Switching Autos	inart Ports, Upink C			
nfimation							
infirmation ie folowing devices w	li be configured with th	e information shown below.				Show Al	. 8
infirmation ie following devices w Secial Number	If be configured with th	e information shown below. Device Type	Readiness	Image Version	CDP Neighbors	Show Al	. 8
Infirmation le following devices w Serial Number PGC1641V348	II be configured with th IP Address 172.28.104.81	e information shown below. Device Type Occo Catalyst 3850 249 10/100/1000 PoE+ Ports Layer 2/Layer 3 E	Readiness Ready	Image Version 03.09.27.54P	COP Neighbors TOR_Switch	Show [ Al Status N/A	- 8

Wired Advanced Mode workflow is similar to the template configuration (see the figure below).

petere You begin Assign to	Choose Other Devices	Configuration Confirmation					
hoose Other Devices							
The devices selected in the pre- and available options are Wired	vious step, plus any existing de and Wireless. This allows you to	vices in the same ste will be shown in the table below based on the configu o choose existing devices to be configured as well as the new devices.	ration selected.	One feature at a time m	ay be configured		
I would like to Zrid wind fea	h res to my davine(s) .	s (5)					
The sector intervention	on on on this possibility						
e nes sí e suns							
Turrent Site: Sanjose Bidg18							
Turrent Site: Sanjose Bildg18 Devices						\$	elected 1   Total 4
lurrent Site: Sanjose Bildg18 Devices						Show Al	elected 1   Total 4
urrent Site: Sanjose-Bidg18 Devices	IP Address	Device Type	Readness	Image Version	CDP Neighbors	show All Status	elected 1   Total 4
urrent Ste: Sanjose-Bildg18 Devices Host Name Switch	IP Address 172.28.104.234	Device Type     Gicco Gatalyst 3850 249 1/0/1000 PoE+ Ports Layer 2/Layer 3 E	Readness Ready	Image Version 03.09.27.5NP	CDP Neighbors CL-Core-Switch	Show All Status N/A	elected 1   Total 4
urrent Ste: Sanjose-Bildg18 Devices Host Name Switch GuestAnchor 5760	IP Address 172.28.104.234 172.28.104.241	Device Type     Geo Catalyst 3550 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E     Geo ST/50 Wireless LAN Controller	Readness Ready Ready	Image Version 03:09:27:59 P 03:09:27:59 P	CDP Neighbors CL-Corle-Switch TOR_Switch	show Al Status N/A N/A	elected 1   Total 4
Ument Ste: Sanjose-Bildg18 Devices Host Name Switch GuestAnchor 5760 3850-A	IP Address 172.28.104.234 172.28.104.241 172.28.104.241	Device Type     Geco Catalyst 3850 24P 10/100/1000 PoE+ Ports Layer 3/Layer 3 E     Geco 5740 Weekes LWI Controller     Geco Catalyst 3850 45P 10/100/1000 PoE+ Ports Layer 3/Layer 3 E	Readness Ready Ready Ready	Image Version 03.09.27.51P 03.09.27.51P 03.09.27.51P	CCP Neighbors CL:Core Switch TOR_Switch TOR_Switch	Shaw All Status N(A N(A Diployment in Progress	elected 1   Total 4
Current Site: Sanjose-Bildg18 Devices Host Name Switch GuestAnchor/S760 3650-8	P Address 172 28 104 234 172 28 104 234 172 28 104 76 172 28 104 75	Device Type     Gisco Catalyst 3650 24P 10/100/1000 PoE+ Ports Layer 3/Layer 3 E:     Gisco Catalyst 3650 44P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E:     Gisco Catalyst 3650 44P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E:     Gisco Catalyst 3650 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E:	Readness Ready Ready Ready Ready	Image Version 03.09.27.5% 03.09.27.5% 03.09.27.5% 03.09.27.5% 03.09.27.5%	CDP Neighbors CL-Core-Switch TOR_Switch TOR_Switch TOR_Switch	Show Al Status N/A N/A Deployment in Progress Deployment in Progress	elected 1   Total 4
Current Site: Sanjose-Bidg18 Devices Host Name Switch GuestAnchor-5760 3650-A 3650-B	17 Address 172 28 104 234 172 28 104 241 172 28 104 75 172 26 104 81	Device Type     Gicco Catalyst 3850 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E     Gicco Catalyst 3850 45P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E     Gicco Catalyst 3850 45P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E	Readness Ready Ready Ready Ready	Image Version 03.09.27.51P 03.09.27.51P 03.09.27.51P 03.09.27.51P	CCP Neighbors CL-Core Switch TOR, Switch TOR, Switch TOR, Switch	Show Al Status N/A N/A Deployment in Progress Deployment in Progress	elected 1   Total 4
Current Site: Sanjose-Bidg18 Devices Settch GuestAnchor-5760 3850-A 3850-B	17 Address 172 28 104 294 172 28 104 294 172 28 104 291 172 28 104 261 172 28 104 81	Device Type     Gicco Catalyst 3850 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E     Gicco Catalyst 3850 45P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E     Gicco Catalyst 3850 24P 10/100/1000 PoE+ Ports Layer 2/Layer 3 E	Readness Ready Ready Ready Ready	Image Version 03.09-27-51P 03.09-27-51P 03.09-27-51P 03.09-27-51P	CCP Neighbors CL-Core-Switch TOR_Switch TOR_Switch TOR_Switch	Show Al Status N/A N/A Disporment in Progress Disployment in Progress	elected 1   Total 4

Wired **Advanced Mode** workflow enables users to configure system, security, HA, and the interface (see the figure below). It has an option to enter other CLI commands as well.

kflows: Initial Device Setu	p: Configuration	1						
ore You begin 🖌 Assign t	to Site Ora	see Other Denkes	Carlimaton					
ess Switch Configuratio	on : Template '	Mode						
This page allows you much	h greater contri	ol over the configuration settings applied	to your devices - usually using p	veviously defined templates.				
Template Details								
System Security	Layer2	High Availability Other	Interfaces					
This step allows you the of devices as a CSV file, Management Configu	option to manue edit that file an unation	ally assign IP Addresses for previously sele d then import the file to overwrite this to	cted devices. You may also use ble.	previously selected options - and skp this	step. If you have lots of devices you may	y find it easier to edit a spreadshe	et instead of this table	t. To do this, export th Total 1 🔐 🕄
						1	how Al	. 8
Serial Number		Device Type	Host Name	1P Address	Subnet Mask	Gateway		

**TIP:** The uplink configuration is applied only on the identified/dedicated uplink ports on the switch. Downlink ports can't be configured with the uplink configuration.

**Wireless Guided Mode** workflow enables switch peer groups, mobility groups, wireless LAN, and security configurations. See the figure below.

Wireless workflow in Cisco Prime Infrastructure 2.0 supports 3850 switches and 5760 controllers. Following 3 modes are supported:

- Single MC mode with 3850 as the controller
- Single MC mode with 5760 controller
- Multi MC mode with 3850 as the controllers (exceeding 50 APs)

čel	fore You Begin Ass	gn to Site Choose	Coher Devices	arameters v	Wreless LAN Security Confirmat	on			
e	ose Other Devices devices selected in th	e previous step, plus	any existing devices in the same site will be sh	own in the table	below based on the configuration	selected. One feature at a tim	ie may b	e configured	
2	available options are W ould like to Add wire	ired and wireless. Th less features to my de	is allows you to choose existing devices to be ivice(s) *	configured as we	a as the new devices.				
1	ent ste Sanjose-Bld	g18						3	
6	vices						Show	Al	elected 3   Total 3
í	Device Name	IP Address	Device Type	Readiness Sta	tus Image Version	COP Neichbours	4.67		
	GuestAnchor-5760	172.28.104.241	Osco 5760 Wireless LAN Controller	Not Ready	03.09.27.5NP	TOR_Switch			
	3850-8	172.28.104.81	Osco Catalyst 3850 24P 10/100/1000 P	Not Ready	03.09.27.5NP	TOR_Switch			
	3850-A	172.28.104.76	Osco Catalyst 3850 48P 10/100/1000 P	Not Ready	03.09.27.5NP	TOR_Switch			
			17 tue Hills to refer		u uželov zada u tise				
			I would like to configure guest ac	ess as part of m	guestánchor-5760	1			
			<ul> <li>I want to use this device as m</li> </ul>	a set whe	GuestAnchor-5760	1			
	e number of access po	ints I want to deploy	now is 30	) )	00000000	1			

#### Step 2b - Creating VLANs and WLANs Using Templates (Advance Mode)

If you have a custom deployment scenario that cannot be met by a guided workflow, you may need to deploy new mobility architecture using some predefined configuration templates. You can use following two templates to deploy VLANs and WLANs:

### VLANs -

Templates > CLI Templates > System Templates - CLI > Configure VLAN For CUWN-IOS

# WLANs -

Templates > Features and Technologies > Controller > WLANs > WLAN Configuration

Ian     All       All     Image: Configure VLAN For CUWN-IOS       Configure VLAN     Image: Configure VLAN       WLANs     Image: Configure VLAN       Image: Load Balancing       Image: Vlan Group	Search Resul	ts
All	lan	0
Configure VLAN For CUWN-IOS Configure VLAN WLANs Load Balancing Vlan Group	>	All
Configure VLAN For CUWN-IOS Configure VLAN VLANs Load Balancing Vlan Group		🂫 •
Configure VLAN WLANs Load Balancing Vlan Group	Configure VI	AN For CUWN-IOS
WLANs     Dead Balancing     Vian Group	Configure VI	AN
Load Balancing	WLANs	۲
Vian Group	Load Balanc	ing
	I Vlan Group	

You can search for "lan" (see the figure on the left) to see all the applicable templates as mentioned above. You can go into any of the templates and deploy them based on what they do.

These two steps will allow you to deploy converged access devices using Cisco Prime Infrastructure.

# Working with Converged Access Devices in Cisco Prime Infrastructure

TIP:

- In order to refresh complete configuration from converged access devices (3850 and 5760) to Cisco Prime Infrastructure, the recommended method is to use "Sync" from Device Work Center.
- When adding a 3850 and 5760, make sure that the SNMP Timeout value is at least 75 or more.

Wired clients connected through the selected switch/MA (Mobility Agent) can be viewed through **Device > Detailed Details > Clients > Currently Associated Clients** (see the figure below).

										Vitue Do	men ROOT-DOMAIN	D+	
isco Infrastructure		🙆 Home Design 🔻	Deploy *	Operate *	Report <b>*</b> Admi	nistration •							PG
rice Work Center							M Discovery	🔨 🗹 Config	uration Archives	🔄 Software Image Management	Image Dashboar	😳 Automated Deploymen	rt Status 🔝 Networl
evice Group		Device Group > ALL											
	P	ALL											
* E*	÷.											Sei	ected t   Total 2 🔮
ALL		/ Edit X Delete 999	yric Groups & Si	tes * 😐 Add D	evice 😰 Bulk Import	Export Dev	ice 🤞 Verify Creder	tials				Show All	
A Device Type		Device Name	+ React	hability	IP Address		Device Type		Collection Sta	tus Collection Tin	ne Sol	ware Version	Credential Sta
🍰 Site Groups		CL12-ISSU		Reachable	172.28.104	.27	Cisco Catalyst 45	507R płu	Managed	October 16, 2	1012 6:49: 03	03.00.SG	Success
Ser Defined		NGWC-MC-Stack		Reachable	172.28.104	178	Cisco Catalyst 38	50 48P	Managed	October 16, 2	012 6:54: 03.	08.58.EMP6	Not verified
Ace Tettalis Controller Details	Configurat	on Configuration Arc	hive Irra	ige			÷-						
vice Britalis Controller Details. ystem > tterfaces >	Configuration	on Configuration Arc volated Wired Clients lients > Current Associated	hive Ina Wired Clients	ige		(0) (0)	*						
Nice Datable Controller Datable referen > terfaces > liente v	Configurati Current Ass 17228-104-178 > 0	on Configuration Acc ociated Wired Clients lients > Current Associated	hive Ina Wirod Clients	ige			÷.					Salected	0   Total 12 😵 -
vice Datalis controller Details refer terfaces correct	Configurati Current Ass 17238-04-078 > 0 19238-04-078 > 0 19238-04-078 > 0 19238-04-078 > 0 19238-04-078 > 0	on Configuration Act ociated Wired Clients Jierts > Current Associated	hive Ima Wirod Clients IP Addres	uge User Name	Vendor Name	Location	VLAN	Interface	Speed	Association Time	Authentication	Selected	0   Tolai 12 😵
Vice Details Instem >> terfaces >> Insta v Current Associated Wind Clients	Configurati Current Ass 172.28.04.176 > 0 Troublentoo MAC Adde O 00re01ae	on Configuration Arc ociated Wired Clients Intra > Current Associated IP Address. 55:77:40	hive Ima Wirod Clients IP Addres Not Detec	uge User Name Unknown	Vendor Name Cisco	Location Unknown	VLAN 104	Interface Gi1/0/48	Speed 1Gbps	Association Time 2012-0ct-16, 16:49:32 UTC	Authentication N/A	Salected ype On Network Yits	0   Tolai 12 😽 9
vice Datalis ntem > terfaces > Territa ~ Current Associated Wired Clients	Configurat Current Ass 172.28.04.176 > 0 Troublestoo MAC Adde Doubline 70:cesto:	on Configuration Arc ociated Wired Clients liens > Current Associated t ses IP Address 56:77-9b 5:06-60	hive Ima Winod Clients IP Addres Not Detec Not Detec	User Neme Unknown Unknown	Vendor Name Cisco Cisco	Location Unknown Unknown	VLAN 104 104	Interface Ga1/0/48 Gi1/0/48	Speed 1Gbps 1Gbps	Association Time 2012 Oct-16, 18:19:32 UTC	Authentication N/A	Selected ype On Network Yes	0   Tolai 12 😵 §
Vice Details Instem > terfaces > Biortia v Current Associated Wired Clients	Configurati Current Ass 172,28,394,376 > 0 Troublistoo MAC Adde O Doreciter 70,000050 0,0000029	on Configuration Acc belated Wired Clients Inris > Current Associated 1 1985 IP Address 1987716 11:00:00 10:066.dc	hive Ima Wired Clients IP Addres Not Detec Not Detec	User Name Unknown Unknown Unknown	Vendor Name Cisco Cisco Vimvare	Location Linknown Linknown	VLAN 104 104	Interface G1/0/48 G1/0/48 G1/0/48	Speed 1Gbps 1Gbps 1Gbps	Association Time 2012-0ct-16, 18-49-32 UTC 2012-0ct-16, 18-49-32 UTC	Authentication N/A N/A	Solivited ype On Network Yes Yes	0   Tolai 12 😤 Ş
Nee Centroller Details ystem > terfaces > Flenta  v Current Associated Wired Clents	Configurat Current Ass 17228.04.04.04.5 Toublestoo MACAdde 0.00.01.0 0.006.02 0.005.05 0.005.05	on Configuration Act sciated Wired Clients lines > Current Associated 1 1 1 1 1 1 1 1 1 1 1 1 1	hive Ima Wired Clients IP Addres Not Detoc Not Detoc IPv4	ge User Name Unknown Unknown Unknown	Vendor Name Cisco Osco Virnvare Virnvare	Location Loknown Unknown Unknown	VLAN 104 104 104	Interface G1/0/48 G1/0/48 G1/0/48 G1/0/48	Speed IGbps IGbps IGbps IGbps	Association Time 2012-0ct-16, 18:49:32 UTC 2012-0ct-16, 18:49:32 UTC 2012-0ct-16, 18:49:32 UTC 2012-0ct-16, 18:49:32 UTC	Authentication N/A N/A N/A	Swinded Ype On Network Yas Yes Yes Yes	0   Tana 12 😵 Ş
ovice Details Controller Details jystem > refaces > Stents v Current Associated Wired Clients	Configurat Current Ass 172281341345 0 172281341345 0 1702818100 MAC Adde 001061181 00106239 00105055 00105055 0010521	on Configuration Act ociated Wired Clients Into 5 Current Associated 67.716 106603 106603 106003 172.28.104.1.	hive Ima Wired Clients IP Addres Not Detoc Not Detoc Not Detoc	ige User Name Linknown Linknown Linknown Linknown	Vendor Name Cisco Cisco Vimvare Jobel	Location Unknown Unknown Unknown Unknown	VLAN 104 104 104 104	Interface G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48	Speed 1Gbps 1Gbps 1Gbps 1Gbps 1Gbps	Association Time 2012-Oct-16, 18:49:32 UTC 2012-Oct-16, 18:49:32 UTC 2012-Oct-16, 18:49:32 UTC 2012-Oct-16, 18:49:32 UTC	Authentication N/A N/A N/A N/A	Selected ype On Network Yes Yes Yes Yes	8   Talas 12 😵 🖞
NACE Details Controller Details ystem > nterfaces > Simular v Gument Associated Wined Clients	Configurati Current Asso 192.38.09.199 > 0 Troubleshoo MAC Adde 0.00.0128 0.00.05056 0.00.05056 0.00.05056	on Configuration Arc octated Wired Clients Teres > Current Associated BP Address 66.77.4b 1.08:0d 99.006.4c 99.006.4c 172.28.104.1. 274.230 572.28.104.1.	Not Detec Not Detec Not Detec Not Detec Not Detec Not Detec	User Name Unknown Unknown Unknown Unknown Unknown Unknown	Vendor Name Cisco Osco Vimvare Intel Vimvare Vitroare	Location Unknown Unknown Unknown Unknown Unknown	VLAN 104 104 104 104 104	Interface G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48	Speed 1Gbps 1Gbps 1Gbps 1Gbps 1Gbps 1Gbps 1Gbps	Association Time 2012 Oct-16, 18-99-12 UTC 2012-Oct-16, 18-99-12 UTC 2012-Oct-16, 18-99-32 UTC 2012-Oct-16, 18-99-32 UTC 2012-Oct-16, 18-99-32 UTC	Authentication N/A N/A N/A N/A N/A N/A N/A	Selected Ypte On Hetwork Yes Yes Yes Yes Yes Yes	5   Tedai 12 🔗 🗟
ovice Details Controller Details System > Interfaces > Clients * Current Associated Wired Clients	Configurati Current Ass 1224/04/16 × C Troublishoo MAC Addr 0 00:0018 0 00:0018 0 00:0056 0 00:15/21 0 00:17/23	on Configuration Arc Solated Wired Clients Intra > Current Associated P Address 657740 al:Debd 7086.cd 172.28.104.1 ba00.98 172.28.104.1	hive Ima Wired Clients IP Addres Not Detec Not Detec Not Detec Not Detec Not Detec Not Detec	user Næme Unknown Unknown Unknown Unknown Unknown Unknown Unknown	Vendor Name Claco Claco Virrware Intel Virrware Hewlett-packard	Location Unknown Unknown Unknown Unknown Unknown Unknown Unknown	VLAN 104 104 104 104 104 104	Interface Gi1/0/48 Gi1/0/48 Gi1/0/48 Gi1/0/48 Gi1/0/48 Gi1/0/48 Gi1/0/48	Speed 1Gbps 1Gbps 1Gbps 1Gbps 1Gbps 1Gbps 1Gbps	Association Time 2012 Oct-16, 18:49-32 UTC 2012 Oct-16, 18:49-32 UTC	Authentication N/A N/A N/A N/A N/A N/A N/A	Sevinded ype On Network Yes Yes Yes Yes Yes Yes Yes	0   Total 12 😤 🛱
Socie Intella System > Interfaces > Clants ∨ Clants Vined Clants	Configurat Current Ass 1723:194:198 - 0 Troditishoo MAC Add 0 00:01:02 0 00:00:02 0 00:00:00 0 00:00 0	on Configuration Arc ocidated Wined Clients Inters - Current Associated Inters - Current Associated	hive Ima Wired Clients Not Detec Not Detec Not Detec Not Detec Not Detec Not Detec	User Name Unknown Unknown Unknown Unknown Unknown Unknown Unknown	Vendor Name Cisco Cisco Virrware Virrware Istol Virnware Hewrétt-packard Rantan	Location Unknown Unknown Unknown Unknown Unknown Unknown Unknown Unknown	VLAN 104 104 104 104 104 104 104	Interface G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48 G1/0/48	Speed 1Gops 1Gops 1Gops 1Gops 1Gops 1Gops 1Gops 1Gops	Association Time 2012-0ct-16, 18-49-32 UTC 2012-0ct-16, 18-49-32 UTC 2012-0ct-16, 18-49-32 UTC 2012-0ct-16, 18-49-32 UTC 2012-0ct-16, 18-49-32 UTC 2012-0ct-16, 18-49-32 UTC 2012-0ct-16, 18-49-32 UTC	Authentication N/A N/A N/A N/A N/A N/A N/A	Sakuded Ype On Network Yes Yes Yes Yes Yes Yes Yes	0   Tabu 12 😵 🔮

Wireless clients terminating the device can be viewed from the scope of the access point to which they are associated to. To view them, select Controller details and select the access point you want to view (see figure below).

evice Work Center				M Discovery 🔨 Conf	iguration Archives 引 Softwo	are Image Management 🧾 Image Das	shboard 🤤 Automated Deploy	yment Status 🚺 Network Au
Device Group	Device Group > ALL ALL							Selected 1   Total 2 😽 🎯
γ2 · t∷ ·	Edit XDelete	Sync Groups & Sites + 👷 Add D	evice 😰 Bulk Import 📝 Expor	t Device 🤞 Verify Credentials			Show All	- 1
B Device Type	Device Name	<ul> <li>Reachability</li> </ul>	IP Address	Device Type	Collection Status	Collection Time	Software Version	Credential Status
Site Groups	CL12-ISSU	Reachable	172.28.104.27	Osco Catalyst 4507R plu	Managed	October 16, 2012 6:49:	03.03.00.5G	Success
Liser Defined	MGWC-MC-Stat	🛛 Reachable	172.28.104.178	Cisco Catalyst 3850 48P_	Managed	October 16, 2012 6:54:	03.08.58.EMP6	Success
Device Details Controllier Do System Summary Spanning Tree Protocol	Configuration Configuration Summary Nonto > Catologies > 17231(M178 > System Alamo Event, Access Point # 0)	Archive Image n > Summary		00				
Device Details Controllier Do System Summary Spanning Tree Protocol CLI Sessions	Configuration Configuration Summary Montor > Configuration Montor > Configuration Conf	Archive Image	U	nique Device (dentifier (UD1)		-		
Device Details Controller De System System Spannary CLI Sessions DHCP Statistics	Configuration Configuration Summary Motion > Configuration Motion > Configuration Configuration Motion > Configuration Configuration Distribution Configuration Distribution	Archive Image n > Summary 172.28.104	178 N	nique Device (dentifier (UD3)) Jame Switch 1		-		
Device Details Controller Cel System Summary Spanning Tree Protocol CLI Sessions DHCP Statistics WLANS	Configuration Configuration     Summary Motitor > Controlers > 172.81.94.178 > Syst Alarms Alarms P Address Name	Archive Image n > Summary 172.28.104. NGWC-MC-S	178 N tack (	nique Device Identifier (UDI) iame Switch 1 Description UA-3850-48P		-		
Device Details Controller De System System Summary Spanning Tree Protocol Clessions DHCP Statistics WLMs Perts	Configuration Configuration Configuration Summary Montor > Configuration Marms Event Control P Address Name Device Type	Archive Image n > Summary 172.28.104. NGWC-MC-5 3850	178 N 178 I Inck I	nique Device Identifier (UD3) iame Switch 1 Description UA-3850-48P Product ID UA-C1850-48P		-		
Device Details Contruitier Det System System Summary Spanning Tree Protocol Clessions DHCP Statistics WLAtis Ports Security	Configuration C	Archive Image n > Summary 172.28.104. NGWC-MC-5 3850 1 hrs 37 mir	178 N tack I 15 46 secs 1	nique Device Identifier (UD3) Jame Switch 1 Description UA-3850-48P Product ID UA-23550-48P Version ID P6A		-		
Device Details Contruitier Det System System Summary Spanning Tree Protocol CLI Sessions CLI Sessions CLI Sessions CLI Sessions WLAVE Ports Security Mobility	Configuration C	Archive Image n > Summary 172.28.104 NGWC-MC-5 3850 1 hrs 37 mir 110	178 N 178 N 1ack ( 1 15 45 secs 1	nique Device Identifier (UD3) Jame Switch 1 Description UA-C3850-48P Product ID UA-C3850-48P Version ID P6A Setsi Number GOL1617/1VG		-		

Clicking on the Access Point link (see figure above) will take you to an access-point-centrered view. Selecting the access point allows you to view the wireless clients associated with it. (see figure below)

avice Work Center						Configuration Archive	s 👩 Software Image	Naragement 🖉 Inage	o Deshboard 🤤 Au	tomated Deployment Stati	us 🚺 Network Au
Device Group	Device Group > Device T Unified AP	ype > Unified AP									
¢• E• ⊗.	-									Selected 1	Telai t 😌 🏭
ALL .	/ Edit X Delete	Sync Groups & Sites * 🔤 Ad	to Device Bulk	Smport Configure *	Monitor *				Sha	w Al	- 18
Benote Type     Baco Interfaces and Modules     Baco Interfaces and Modules	AP Name	<ul> <li>Ethernet MAC Ad., P c8/9011674/66/37 19</li> </ul>	Address 12.168.152.14	Controller 39 192.168.152.11	AP Model AIR-CAP35021-4-1	Operational Status 9 Registered	Software Version 7.2.110.0	AP Location Amsterdam Branch	Autit Status Identical	Admin Status Enable	АР Түре САРЖАР
Backers     Schleise soft Hole     Schleise soft Hole     Bit Tale Party Access Part     Thick Party Access Part     Thick Party Wirehess Controller     Dirthe Party Wirehess Controller     Dirthe Party     Work out Teleborrus											
Device Details Configuration Access Point Details: нито-игазор-2		-									
Participa Statisticas (MAR Martines	Commit According to	Ciens (Wer Title								Selected 0	
General Interfaces CDP Meghbors											Lunnix 💑 🛱
General Interfaces CCP Neighbors	ar Tuto Uno Mana	Association Time	Entrant Tu	com 1	Interne Concers						11001X 🐥 🕀
General Interfaces CDP Meghbors	ns Type User Name	Association Time	Endpoint Ty	SSID I	lptime (secon Por						1,0013 🦚 63

For devices where the configuration has been modified, Cisco Prime Infrastructure provides a way to view/compare configuration files with a side-by-side view of a running configuration and an archived configuration (for example, startup config). You can obtain this comparison at a device level through Operate > Device Work center > (Selected Device) > Configuration Archive (from the bottom pane).

				🕅 Discovery 🐖 Confi	iguration Archives 🕣 Softwa	are Image Management 🚟 Image Das	hiboard 🤤 Automated Deploy	ment Status 🔛 Network A
Device Group	Device Group > ALL ALL							Selected 1   Tetal 2 🤞 🎡
All.	/ Edit 🗙 Delete 🦓 Syna	Groups & Sites * 🚊 Add De	vice BulkImport Poport	Device 🤞 Verify Credentials			Show All	- 5
P Sa Device Type	Device Name	<ul> <li>Reachability</li> </ul>	JP Address	Device Type	Collection Status	Collection Time	Software Version	Credential Status
Bite Groups	CL12-ISSU	Reachable	172.28.104.27	Cisco Catalyst 4507R plu	Managed	October 16, 2012 6:49:	03.03.00.SG	Success
Se User Defined	NGWC-MC-Stack	Reachable	172.28.104.178	Cisco Catalyst 3850 48P	Managed	October 16, 2012 6:54:	03.08.58.EMP6	Success
Device Details Controller Details Config	unation Comfiguration Archiv	Image		00				
Device Details Controller Details Config Startup/Running Mismatch: Yes	Configuration Archiv	mage Image		<del></del>				Selected 1   Total 1 👲
Device Details Controller Details Config Startus/Running Mismatch: Yes @Schedue Rattack (2)Schedule Arthue (5)Schedule	uration Configuration Archiv	image Sit Tag		-007			Show All	Selected 1   Total 1 🚸
Device Details Controller Details Config Startup/Running Mismatch: Yes Schedule Ralback Blockde Archive & Schedule	uration Comfiguration Archit Derwrite © Schedule Deploy © 6 • Created By	st Tag Tag		Description		Out of	Show All	Salicted 1   Total 1 👲

**TIP:** You can alternatively access the information from **Operate > Configuration archives**.

You can see a modal pop-up window showing the two configurations side-by-side. When you look at this initially, understand the significance of what each color means. See the following figure for a quick legend snapshot:





# **Discovering Templates from Converged Access Devices**

For devices that have an existing configuration, templates can be discovered from the devices.

Template discovery from a device is initiated from the **Device Work Center** page using the following steps (see the figures below):

(م	Device Work Center			H co	covery 🖪 Configur	ation Antimes 🗇	Software Image H	lanagement 🗐 In	age Dashboard 💟 Ad	unated Deployment Status	D. Netwo
TE: *      *     *     Features and Technologies     Security	Device Group	Device Group > Device Wireless Control	lype > Windows Contro Ider	le .							
Application Visibility	4.5.	te dan Manual	Store Course & Store	-	and least in	Frank Parise and	March, Condensation	Andread in Charles	3	Delected 1 [1	form 8 🥵
Controller	ALL Desize Tune	Deers from a	Beerhalding	IF Address	Dealor Tone	Date:	AP Discours	Software likes	Income Line of	Save Config to Flash	
Network Analysis Module	1 Switches and Hubs	C) 8014-42a-ed_	Reachable	10.34.148.5	Clace Catelyst	Managed with	Completed	0.DEV-0	2012-0:0-1		the first state
Interfaces	United AP	C stringtheast	D Reachable	10.34.148.4	Care Catalon	Planaged with	Concisted	GROW MR PARTS	2012-04-04	Coccerer remplotes sole	n compone
(11 Template	Sto Groups		E Reactable	10.54.150.45	Care E State Ma	Hanaged with	Company of		2012-02-11 05-01-0	Audit Now Update Cedermais	
My Tant	🎒 User Defreed	2 Colorest	Restation 1	10.25 10.26 102	Case Chill Mi	Warnings	Compresso	TRACK SHAPPY	2012-00-11, 09-013	di come	2010-0
Composite Templates		La bitern	Peachable	172.19.26.193	Cisco Catalyst	Hanapid	Completed	03.08.58.0494	2012-042-12, 02:04-4	IS UTC	lidents
My Templates											
Property Townshipson					1000						

1. Select the **Device Group**. (See figure on left).

2. Select the device from the list view. (See figure above on right).

3. Click the double arrow from the menu bar. This will result in the **Configure** menu being displayed. (see figure at right)

• ≫ Sh	All 🔹 🚺
Configure	Save Config to Flash Refresh Config from Controller Discover Templates from Controller Templates Applied to Controller Audit Now Update Credentials
4. Select **Discover Templates from Controller** from the drop-down menu.

Discovered templates will be listed under **My Templates** by navigating to **Design > Feature Design**. If you are trying to deploy template to one of the supported converged access devices, you need to select device type as "CUWN-IOS and UA" or "All" (wherever applicable) as shown in the figure on the left. If a template has the Device Type selection option "All" available and it is chosen, the same template can be deployed on both classical controllers (WLC) and supported converged access devices.

*Device Type	CUWN-IOS and UA	<ul> <li>?</li> </ul>	
		Device Type	×
mplate Detail		↓ E. •	101.
*Community Name		CUWN (default)	
firm Community Name		CUWN-IOS and UA	
Access Mode	Read Only \$	All(CUWN,CUWN-IOS and	UA)

# **Monitoring Converged Access Switches**

Converged access switches can also be monitored through the Device Work Center. The user experience is very similar. The device details tab (see the following figure) has however been augmented with switch specific information as well.

evice Work Center					Discove	ry 🖭 Config	puration Archives 🕃 Softwa	re Image Management. 🔠 Image Dat	shboard 🤤 Automated Deploy	ment Status 🔛 Network A
Device Group	P) Devi	ce Group > ALL								Selocad 1   Totar 7 🛞 👸
General Contraction of the second sec	9. 1	🧨 Edit 🗙 Delete 🖓 Sync. Groups & Sites 🔹 👷 Add Device 👔 Bulk Import 🔐 Export Device 📢 Verify Credentialis						Show All	- 1	
<ul> <li>Re Device Type</li> </ul>	0	Device Name	<ul> <li>Reachability</li> </ul>	IP Address	Device Type		Collection Status	Collection Time	Software Version	Credential Statur
Ba Site Groups	0	0.12-ISSU	Reachable	172.28.104.27	Cisco Catalyst	4507R plu	Managed	October 16, 2012 6:49:	03.03.00.5G	Success
Su User Defined	. 2	NGWC-MC-Stack	Reachable	172.28.104.178	Eisco Catalyst	3850 48P	Managed	October 16, 2012 6:54:	03.08.58.EMP6	Success
Device Datatis Controller De System	tails Configuration Summary U2.28.104.178 > System > General	Configuration Archi	ve ûmage			Unique D	evice (dentifier (UDI)			
A Memory Ponis	IP Address	172.28.104.178				Name	Swit	ch 1		
a Environment	Device Name	Cisco Catalest 38	0 48P 10/100/1000 PoF+ P	orts Lawer 2/Lawer 3 Etherne	t Stackable Switch	Description	00 995	0.00-401		
Hodules	Lip Time	2 hrs 5 mins 12 se	C5	and a few stands, a spacing		Version I	p			
H- VLANS	System Time	2012-Oct-16, 19:	14:22 UTC			Serial Nu	mber FOC:	617V1VG		
A VTP	Reachability Status	Reachable								
H- Physical Ports	Location					Inventory	0			
A Second	Contact					Software 1	Version 03.0	8.58.EMP6		
A Spanning Tree	Cisco Identity Capabl	e No				Model No	ua-1	3850-48P		
M. shanned use	Location Canable	No				1000				

The controller details tab (see the following figure) provides information about the wireless capabilities of the converged switch.

					👬 Discovery 🤨 Conf	figuration Archives 🔂 Software	Image Management 🧾 Image Das	hboard 👽 Automated Deploy	ment Status 🔝 Network Au
Device Group	(م ھ	Device Group > ALL ALL							Solected 1   Tokai 2 😤 🎡
B All	32.4	/ Edit X Delete Syr	nc Groups & Sites 👻 🐏 Add De	vice 💼 Bulk Import 📝 Exp	xort Device 🐗 Verify Credentials			Show All	. 8
Ba Device Type		Device Name	<ul> <li>Reachability</li> </ul>	IP Address	Device Type	Collection Status	Collection Time	Software Version	Credential Status
Bite Groups		CL12-ISSU	Reachable	172.28.104.27	Cisco Catalyst 4507R plu	. Managed	October 16, 2012 6:49:	03.03.00.SG	Success
a User Defined		NGWC-MC-Stack	Reachable	172.28.104.178	Cisco Catalyst 3850 48P	Managed	October 16, 2012 6:54:	03.08.58.EMP6	Success
Device Details Controller De System Commany Spanning Tree Protocol	Summary Henitor > Control Alarma Sents	cn Configuration Arch lens > 172.28.104.178 > System > 5 Access Point # 0	ive Image Summary		University Takates Takatelliker (1)(71)				
Device Details Controller Det System Controller Det Spanning Tree Protocol CLI Sessions	tais Configuration	on Configuration Arch Ins > 172.28.104.175 > System > 5 Access Point # 0	ive Inage Summary	į	Unique Device Identifier (UDI)				
Device Details Controller Der System Sammary Sammary Sanning Tree Protocol CLI Sessions CLI Sessions DHCP Statistics	Summary Nenter > Configuration Alarma Events General IP Address	en Configuration Arch en > 172.28.104.7% > System > 1 Access Point: # 0	ive brage Summary 172.28.104.1	178	Unique Device Identifier (UDI) Name Switch 1				
Device Details Contribute Det System Summary. Spanning The Protocol Classifications Classifications Def Statistics WLANS	Summary Hanter > Configurati Summary Hanter > Control Alarms: Events General IP Address Name	on Configuration Arch Int > 1728LIDK274 > Rystem > 4 Access Point # 0	iva Image Summary 172.28.104.3 NGWC-MC-St	178 ack	Unique Device Identifier (UDS) Name Switch 1 Description UA-3850-48P				
Device Details Controller Det System  Sommary  Sommary  Call Sessions  Call Sessions  DHOP Statistics  Parts  Call Sessions  Call Sessions	Summary Nonter > Configuration Nonter > Control Alarms: Eventoria Ceneral P Address Name > Device Type	on Configuration Arch Int 20208 104.378 > System > 1 Access Point # 0	ive Image Bummary 172.28.104.1 NGWC-MC-56 3850	178 sck	Unique Device Identifier (UDI) Name Switch 1 Description UA-2850-48P Product ID UA-2850-48P				
Device Details Control of Order System Control of Order Spanning Tree Protocol CLI Sessions CLI Sessions DHCP Statistics DHCP Statistics Ports Security	Configuration	on Configuration Arch Int > 1/2.28: 104, 178 > System > 1 Access Point # 0	ive Image Bummary 172.28.104.1 NGWC-MC-St 2850 2 hrs 8 mins	178 ack 26 secs	Unique Device Identifier (UDI) Name Switch 1 Description UA-3850-48P Version ID P6A Serol Number SprC1512/1165				
Device Details Control of our System Sammary Sammary Sammary CLI Sessions UNAs Ports Security Mobility	Configuration     Configuration     Control of the second of the se	on Configuration Arch Ins > 172.88.104.178 > System > 1 Access Point # 0	ive Image Burnmary 172.28.104.1 NGWC-HC-5 3850 2 hrs 8 mins 31C	178 Social Ző soca	Unque Device Identifier (UDI) Name Switch 1 Description UA-3850-48P Product ID UA-2850-48P Version ID P6A Serial Number FOC1637V1VG				
Device Details Contribute Det System Summary Spanning Tree Protocol Control Sessions DefCP Statistics WILANs Ports Security Mobility 802.11a/n	Configuration Configuration Nonites - Control Alarma - Events General P Address Amane P Address P Address P Address P Address P Address P Address System Time P Location	on Configuration Arch Ins > 172.38.104.178 > Rystem > 1 Access Point # 0	ive Image Bummary 172.28.104.1 NGWC-HC-St 2850 2 hrs 8 mins 31C	178 ack 26 secs	Unique Device Identifier (UDS) Name Switch 1 Description UA-3850-48P Product ID UA-C3850-48P Version ID PAA Senal Number FOC1617V1VG Utilization Utilization	ter i be i Conton i Vion Hil			

When monitoring a Catalyst 3850 switch, a list of APs that are joined to the switch can be displayed by clicking Access Point link from the controller detail page (see the following figure).

levice Work Center		H	Discovery 🛃 Configuration Archi	ves 🚳 Software Image	Management 🔠 Image Dat
Device Group	Device Group > Device Type Switches and Hubs	e > Switches and Hubs			
	/Edit XDelete 🝕	Sync 🔒 Groups & Sites 🔹	e: Add Device Bulk Import	Export Device	
Boylice Type     Boylice     Bo	Device Name     PAR.3650-1	<ul> <li>Reachability IP Addr</li> <li>30.12.1</li> </ul>	ss/DNS Device Type 0.2 Cisco Catalyst 3850	Admin Status Managed	Inventory Collection S Completied
Device Details     Configuration	Configuration Archive	Image	18995		
System 👻	Summary 10.12.10.2 > System > Summ	ary			
User Defined Field Memory Pools					
Environment     Modules     Physical Ports	Alarms Event Access Po	ent # 0		Unique Device	Identifier (UDI)
A Santar	TD Address/DUS Name	10 12 10 2		Nama	Switch 1

The converged access switch also provides 360-degree views. Launching the Device 360 View involves the same actions of clicking the bubble after the IP address (see the following figure).

					H Discovery 🖽 Config	puration Archives 👌 Software Image Mar	agement. 🧮 Image Dashboard 😍 Automated De	iployment Status 🔝 Network A
Device Group	(م	Device Group > ALL ALL						automa e l'Anna a 🔊
2• 臣•	- 	A Edd M Palate State	President & Chara an Inc. Addd	An Jos III Bully Tenand III Engent Parcel	. Really Conducting		These All	ateria ( 1 con a 🖉 🖓
ALL .		The Areas Sales	and a store - 12 Mater	when an and a second second	Device 360° Views		#×	
Page Device Type			Reachabelty	173 38 104 37	0	NGWC-MC-Stack	<b>NO BOBO</b>	Credential Status
R User Defined		17 NOWCAR-Stark	Rearbable	122.28.104.128	2			Surrent
		The second second			E	up for 2 top 16 mms 36 secs	tayit 3850 46P 10/100/1000 P0E+ P0R	- provident
					<i>w</i>	OS Type IOS OS Version 03.08.58.1 Last Config Change October 14 Last Inventory Collection October 14	EMP6 5, 2012 6:57:33 PM UTC 5, 2012 6:54:19 PM UTC	
					19.00	Utilization 19/6 8.00%	Memory Utilization 55.00% 0.00%	
		II. Vite associated and a	e Terme	-=+0	4 Low	High Average	Low High Average	
Device Details Controller Det	Configuration	on Configuration Archiv	a tuaña		36 7006 10	17900	55 MM 14 MM 55 MM	
Device Details Controller Dei System	Configuration WLANs	on Configuration Archiv	a traga		36.00% 59	10% 1730%	95.00% 56.00% S5.20% Instance: JOS Process stack	
Device Details Controller Der System	WLANs Monitor > Control	on Configuration Archiv ers > 172.28.104.176 > System > W	u unugu		36.096 19	00% 12.89%	55.00% 56.00% 55.20% instance: 105 Process stack	
Device Details Controller De System Summary Spanning Tree Protocol	WLANs Monitor > Controls WLAN ID	on Configuration Archiv ers > 172.28.104.175 > System > W Profile Name	LANS SSID	Security Policies	35.00% 12	100% 17.80%	55.00% 56.00% 55.20% Instance: JOS Process stack	o. of Cients
Device Details Controller De System Summary Spanning Tree Protocol CLI Sessions	Configuration WLANs Monitor > Control WLAN ID 1	on Configuration Archiv es > 172.28.101.176 > System > W Profile Name gumkha	ssib gumkha	Security Policies	35.00% 19 4 Alarms M	00% 1230% Odules Interfaces Neighbr	55.00% 56.00% S5.20% Instance: JOS Process stack 275 W I 0	io. of Clients
Device Details Controller De System Summary Sammary CLI Sessions CLI Sessions	Configuratia WLANs Monitor > Control WLAN ID 1 2	on Configuration Archiv ers > 172.28.104.175 > System > W Profile Name gumkha gumka	ssiD gumkha gumka	Security Policies None [WPA2] [Auth( 802.1X)]	4 Alema M	odules Interfaces Neighb Timestamp - Mess No data available	55.00%         55.20%           instance: 105 Process stack           arrs:         W. I           sogge         Category           0	io. of Clients
Device Details Controller D System System Sommany Spanning Tree Protocol CLI Sessons CLI Sessons CHCP Statistics WLANs	Configuration	on Configuration Archiv ers > 17228.101.19 > System > W Profile Name gumkha gumka	e intege LANs SSID gumka gumka	Security Policies None (WPA2] [Auth( 802.1X)]	4 Alerna M Status	loos 17.80%	SS00% SS.20% Instance: 105 Process stack ars: W. F soge Category 0	io. of Cients
Device Datais Controller De System Summary Spanning Tree Protocol CLI Sessions DHCP Statistics WLANs Ports	Configurati     WLANs     Monitor > Control     ULAN ID     1     2	on Configuration Archiv ers > 172.28.104.176 > System > W Profile Name gumidia gumica	s ssib gumkha gumka	Security Policies None [WPA2] [Auth( 802.1X)]	4 Alarma M	100 17.80%	SECON SECON SEADN Instruct: 305 Process Back JIS W b N Galege Category 0	io, of Qients
Device Details Controlling De Syndam Syndam Spanning Tree Protocol CLI Seasons CLI Seasons CLI Seasons CLI Anks Perts Security	Configurati WLANs Monitor > Control ULAN ID 1 2 3 3	on Configuration Archiv ers × 172.28 JDR J38 × System × W Profile Name gumidha gumidha gumida	state	Security Policies None [WPA2] [Auth( 802.1X())	4 Aluma M	123294 Indules Interfaces Neighbo Timestamp - Mess No data available	Stations Solow Station Instruct: 205 Proceed stack ars W. P. N. Solow Station ars Category 0	io, of Clients
Desice Details Charter De System System System Sommary Sommary Sommary Sommary CLI Sessions CLI Sessions CLI Sessions CLI Sessions Security Nobitity	Configurati WLANS Monitor > Control ULAN ID 1 2 3 3 3	on Configuration Archiv ers > 172.281.396.195 + System > W Profile Name gumtia gumtia	s anaya LANs SSID Qumidha gumidha	Security Policies None (WPA2] (Auth( 802.1X))	4 Alarma M Status	100 12205 Iodules Interfaces Neighbo Timestamp ~ Mess No data available	SISCIPS 6500% SS32% Instance: JOS Process asck ars: W > Rage Category 0	io. of Clients
Device Datalis Controller De System System System Sosaning Tele Protocol Cul Sessions Cul Sessions WUANS Pers Security Mobility Mobility	Configuration WLANS Manifer > Cannols WLAN ID 1 2 3 3 3 3	on Configuration Archiv ers > 172,281,391,378 > System > W Profile Name gumbha gumbha gumba	e anaye LANe SSID gumka gumka	Security Policies None (WPA2] (Auth( 802.1X))	4 Alarma M Sadus	100 12205 Indules Interfaces Neighbo Timestamp - Mess No data available	SISCIPS 6500% SS.20% Instance: JOS Process Back ors W  Category	io, of Clients

## References

#### **Cisco Prime Infrastructure 2.0 Links**

- Cisco Prime Infrastructure 2.0 Release Notes: http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/release/notes/cpi\_rn.html.
- Cisco Prime Infrastructure 2.0 Quick Start Guide
   <u>http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/quickstart/guide/cpi\_gsg.html</u>.
- Cisco Prime Infrastructure 2.0 Administrator Guide
   <u>http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/administrator/guide/PIAdminBook.html</u>
- Supported Devices in 2.0
   <u>http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/supported/devices/pi20-supported\_devices\_list.xlsx.</u>

## **Cisco Product Pages**

- Cisco Prime Infrastructure <a href="http://www.cisco.com/go/primeinfrastructure">http://www.cisco.com/go/primeinfrastructure</a>.
- Cisco Identity Security Engine (ISE) <u>http://www.cisco.com/go/ise</u>.
- Cisco Prime Network Analysis Module (NAM) http://www.cisco.com/go/nam.
- Cisco Application Visibility and Control <a href="http://www.cisco.com/go/avc">http://www.cisco.com/go/avc</a>.
- Cisco Plug and Play Solution Guide
   <u>http://www.cisco.com/en/US/docs/net\_mgmt/prime/infrastructure/2.0/user/guide/Cisco\_Plug-n-Play-Solution-Guide.pdf</u>.
- Product Downloads <a href="http://www.cisco.com/cisco/web/support/index.html#~shp\_download">http://www.cisco.com/cisco/web/support/index.html#~shp\_download</a>.

# **Ordering and Licensing**

- Cisco Ordering Tools <u>http://www.cisco.com/go/ordering</u>.
- Product Evaluation <u>http://www.cisco.com/go/nmsevals</u>.
- Ordering and Licensing Guide Cisco Prime Infrastructure 2.0 Ordering and Licensing Guide.

#### **Related Deployment Guides**

- Cisco Prime Infrastructure Best Practices
   <u>http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/white\_paper\_c11-728875.html</u>.
- ISE Deployment Guide http://www.cisco.com/en/US/docs/security/ise/1.0/install\_guide/ise10\_deploy.pdf.
- MSE Deployment Guide <u>http://www.cisco.com/en/US/products/ps9742/products\_tech\_note09186a00809d1529.shtml.</u>
- AVC Deployment Guide (Wireless)
   <a href="http://www.cisco.com/en/US/products/ps10315/products\_tech\_note09186a0080bed910.shtml">http://www.cisco.com/en/US/products/ps10315/products\_tech\_note09186a0080bed910.shtml</a>
- AVC Solution Guide with Cisco Prime Infrastructure <u>http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/solution\_overview\_c22-</u> <u>728972.html</u>.
- Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices, Release 2.0 http://www.cisco.com/en/US/docs/wireless/prime\_infrastructure/2.0/configuration/guide/pi\_20\_cg.html.
- Cisco Wireless Solutions Software Compatibility Matrix
   <u>https://www.cisco.com/en/US/docs/wireless/controller/5500/tech\_notes/Wireless\_Software\_Compatibility\_Matrix.html</u>.
- Cisco Catalyst 3850 Switch Deployment Guide
   <u>http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps12686/deployment\_guide\_c07-727067.html</u>.
- Transitioning from Cisco Prime LMS to Cisco Prime Infrastructure <u>http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/app\_note\_c27-716266.html</u>.
- Cisco Prime Infrastructure LMS Functional Support Reference http://www.cisco.com/en/US/products/ps12239/prod\_white\_papers\_list.html.



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

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

Printed in USA