# 

# **Newer Cisco SBA Guides Available**

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.



Cisco Prime LMS Deployment Guide

SMART BUSINESS ARCHITECTURE

BORDERLESS NETWORKS DEPLOYMENT GUIDE

11 11-11

CISCO

SBA

August 2012 Series

# Preface

### **Who Should Read This Guide**

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation
   documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

### **Release Series**

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

#### month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

### **How to Read Commands**

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

configure terminal

Commands that specify a value for a variable appear as follows:

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

class-map [highest class name]

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

#### Router# enable

Long commands that line wrap are underlined. Enter them as one command:

wrr-queue random-detect max-threshold 1 100 100 100 100 100

100 100 100

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

interface Vlan64

ip address 10.5.204.5 255.255.25.0

#### **Comments and Questions**

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

August 2012 Series

# Table of Contents

What's In This SBA Guide	. 1
Cisco SBA Borderless Networks	1
Route to Success	1
About This Guide	1
Introduction	.2
Business Overview	2
Technology Overview	2

Deployment Details7	
Installing and Configuring Cisco Prime LMS7	
Managing the Network	
Appendix A: Product List	
Appendix B: Changes27	

# What's In This SBA Guide

### **Cisco SBA Borderless Networks**

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

### **Route to Success**

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

## **About This Guide**

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



# Introduction

### **Business Overview**

Organizations find it more challenging than ever to enable efficiency and productivity for information technology staff due to data network management complexity. Cisco's Borderless Network can have multiple services running on the infrastructure, and as the network and number of services continue to evolve, data network management becomes even more critical for operational efficiency. IT staff must be able to adapt to an evolving network while ensuring existing operations are monitored, and have the flexibility to quickly isolate and fix network performance issues. These management needs fall into different use cases, such as network configuration, deployment, asset management, and troubleshooting. An IT staff's top concern is to have a unified network management application that can help them address these needs, thus increasing the staff's productivity.

### **Technology Overview**

Cisco Prime LAN Management Solution (Prime LMS) is an integrated approach to network management tools for configuration, deployment, asset management, and troubleshooting. Prime LMS provides an intuitive GUI that can be accessed from anywhere from within the network and gives you a full view of a network use and performance. This guide adds to the example configuration already built in the core Cisco Smart Business Architecture (SBA) guides. This supplemental guide includes:

- Step-by-step procedures for installing and deploying Prime LMS.
- Detailed descriptions of how you can monitor and troubleshoot your network.
- Templates that you can use to deploy global configurations across your networks.

Figure 1 depicts the Cisco SBA architecture overview. With such a network and services on top of it, network management applications like Prime LMS play a critical role in day-to-day network operations. Prime LMS is an integrated suite of management functions that simplify the configuration, administration, monitoring, and troubleshooting of Cisco solutions. Built on top of the latest Web 2.0 standards, Prime LMS allows network administrators to manage Cisco Borderless Networks for customers through a browser-based interface that be accessed from anywhere at any time within the network.



218

The following sections describe the tasks this guide covers.

#### **Installation and Deployment**

Most often, network administrators are unsure of the most efficient method to configure Prime LMS. Prime LMS provides a very important feature: the Getting Started workflow. This guided sequence eliminates configuration guesswork and assists you in performing essential and optional configuration and management tasks. It is a quick and sure way of getting Prime LMS running with minimal human errors.

#### **Configuration and Inventory Management**

As networks grow, network administrators have a tedious job in keeping track of devices being added to or removed from the network. Administrators have to ensure that the devices are running proper software and that configurations are archived, and they must also implement network compliance by enforcing policies across the network. Prime LMS plays an important role in the end-to-end management of business-critical technologies and services. It aligns management functionality with the way that IT staff do their jobs. The following primary functions are included in the workflow and enable IT staff to achieve greater efficiency:

- Inventory Manager—Builds and maintains an up-to-date software and hardware inventory, providing a detailed inventory report, which you can customize, or a predefined inventory.
- Configuration Manager—Maintains an active archive of multiple iterations of configuration files for every managed device and simplifies the deployment of configuration changes. ConfigEditor is a utility to change, compare, and deploy configurations on one device. NetConfig is a similar utility to perform such tasks on multiple devices.
- Software Manager—Simplifies and speeds up software image analysis and deployment. This feature helps in automatic upgrade analysis and helps to select the right image. A network administrator can also use this feature to import images, stage images (local or remote), and then install them on a single device or group of devices.
- Syslog Analysis—Collects and analyzes syslog messages to help isolate network error conditions. A network administrator can filter syslog messages and designate an action based on the messages.
- Audit Service—Continuously monitors incoming data versus stored data to provide comprehensive reports on software image, inventory, and configuration changes. It also tracks the changes made to Prime LMS by the system administrator.

 Compliance Management—Provides a way to enforce certain policies (or configurations) to ensure that the network is compliant per internal or government regulations.

Figure 2 - Inventory Dashboard

My Menu 🔻 Moi	nitor 🔻 Inven	tory 🔻 Configur		.og Out About Sitemap Feedba nin ▼ Work Centers ▼		🗑 🚖 🐥 -
Inventory > Dashboards	s > Inventory					27 Oct 2011, 09:05 F
Hardware Summ	ary		≠摸?」■×	Software Summary		✓ 僖? 二 田 ×
		📕 Cisco In	terfaces and Modules	Software Version		Count
		🔲 Wireless		15.1(4)M2		22
		Unknow	۰	12.2(58)SE2		22
		Switcher	and Hubs	Generic Class		6
		Security		15.1(3)S0a		5
			and VPN	15.0(1)SY		3
		Routers		4.4.1.12		2
		Content	Networking	03.02.00.XO		1
				03.02.01.SG		1
				12.2(55)EX2		1
				8.4(2)		1
Device Change A	udit		✓模? 二田×	15.0(0.0.90)SE1		1
Device Name	User Name	Creation Time	Message			
RS203-2921-2.cisco.l	hmcalath	Oct 27 2011	CONFIG CHANGE	User Tracking Summary		_ / 僖 ? 二 ⊞ ×
K3203-2921-2.CI5C0.I	Diffegiour	08:21:58	CONFIG_CHANGE	Number of End hosts		70
RS203-2921-1.cisco.	bmcgloth	Oct 27 2011 08:17:04	CONFIG_CHANGE	Number of Active End hosts		54
				Number of Connected End Hos		24
A2960S.cisco.local	estg	Oct 27 2011 04:42:30	CONFIG_CHANGE	Number of Dormant hosts in la		g
		Oct 27 2011		Number of New hosts in last 7 Number of Rogue hosts in last		6
A2960S.cisco.local	estg	03:31:35	CONFIG_CHANGE	Number of Rogue nosis in fasi	7 udys	(
	osta	Oct 27 2011 03:21:53	CONFIG_CHANGE	Device Discovery Summa	ary	/存?」田×
A2960S.cisco.local	esig					
A2960S.cisco.local	esuj	03:21:33		Discovery Status	Completed	
		03:21:55	/声? EX	Discovery Status Discovery Start Time	Completed 21 Oct 2011, 11:24 PDT	
Supported Device	e Finder	03:21:53	/存?_ 田 X Submit Paret			
Supported Device		03:21:33	✓ ∯ ? = ⊞ × Submit Reset	Discovery Start Time Discovery End Time Total Devices Discovered	21 Oct 2011, 11:24 PDT	
Supported Device	e Finder	05:21:55		Discovery Start Time Discovery End Time Total Devices Discovered Reachable Devices	21 Oct 2011, 11:24 PDT 21 Oct 2011, 11:24 PDT	
Supported Device	e Finder	03:21:33		Discovery Start Time Discovery End Time Total Devices Discovered	21 Oct 2011, 11:24 PDT 21 Oct 2011, 11:24 PDT 4	

#### Monitoring and Fault Management

A network administrator's most important tasks are to ensure high network availability and to isolate and resolve any network issues before they affect services. Prime LMS provides both monitoring and fault management functionalities, using Simple Network Management Protocol (SNMP) polling and traps. The Prime LMS auto-monitoring feature proactively monitors the network for any indication of device or network fault, enabling quick network repair turnaround time with minimum service degradation.

My Menu 🔻 Monitor 🔻	Inventory   Cor	nfiguration 🔻 Reports 🔻 A	ldmin ▼ Work C	enters 🔻	· 🗑 ☆ 🕈 •	
Monitor > Dashboards > Monitori	ng				27 Oct 2011, 05	10 P
ault Events Summary		✓ 僖? 二 □ ×	High Severity	Faults	/	_ 8
Events Name	Severity	No. of Devices	Severi Status	Device Name	Event Na Componen Creation 1 Owned E	3y
Unresponsive	Critical	11	Active	10.4.32.241	OutOfRa VOLT-10.4 27-Oct-2( NA	
OperationallyDown	Critical	9	Active	10.4.32.245	OutOfRa VOLT-10.4 27-Oct-2( NA	
OutOfRange	Critical	5	Active	10.4.32.244	OutOfRa VOLT-10.4 27-Oct-2( NA	
InsufficientFreeMemory	Critical	4	-			
			Active	10.4.32.242	OutOfRa VOLT-10.4 27-Oct-2( NA	
Duplicate Device Availability Distribution based on avera	Critical	1 /	Active     Interface Ava	10.255.253.203	OutORA VOLT-10.4 27-Oct-21 NA Unrespo: SNMPAge: 27-Oct-21 NA / 27 27-	1
Duplicate Device Availability Distribution based on avera ast 1 Hour	Critical	1 /	Active     Active     Interface Ava     Distribution bas	10.255.253.203	Unrespoi SNMPAgei 27-Oct-2( NA	3

Prime LMS Fault Monitor is a centralized browser where administrators can read, in a single view, information on faults and events. Fault Monitor collects information about faults from all devices in real time and can display it for single devices or groups. After administrators have acted on a fault, they can clear the alarms, as well.

#### Figure 4 - Fault Monitor Dashboard

●         10.4.63.254         10.4.63.254         Switches and Hubs           ●         10.4.32.245         10.4.32.245         Routers	0 (	V 8	2 Last Update	< _	<del>8</del> 8 8 1
♣         ☑         Device Name         Device IP         Type           ●         10.4.63.254         10.4.63.254         Switches and Hubs           ●         10.4.32.245         10.4.32.245         Routers	0 (		Last Update	-	
●         10.4.63.254         10.4.63.254         Switches and Hubs           ●         10.4.32.245         10.4.32.245         Routers	0 (		Last Update	-	
O O 10.4.32.245 10.4.32.245 Routers	-	0 0			
			27-Oct-2011	L 09:	
O 8 10.4.32.244 10.4.32.244 Routers	1 (	0 0	27-Oct-2011	L 09:	
	5 (	0 0	27-Oct-2011	L 09:	
O O 10.4.32.242 10.4.32.242 Routers	9 (	0 0	27-Oct-2011	L 09:	
O 🔕 10.4.32.241 10.4.32.241 Routers	16 (	0 0	27-Oct-2011	L 09:	
	1 (	0 0	27-Oct-2011	L 08:	
	2 (	0 0	27-Oct-2011	1 08:	
	2 (	0 0	27-Oct-2011	L 08:	
Faults for 10.4.63.254					😽 🖨 🚱 {
🔓 Own It 🛭 🔗 Clear 🔯 Annotate 🖂 Notify 🏢 Event Monitor 🍸 Filter					
🗆 🐥 🖳 🗹 Event Name Component Name		Last	Updated Time 👻	Owned By	

#### **Templates**

Administrators often deploy configurations that are global to the network (switch configurations, permissions, etc.), and they spend a fair amount of time propagating these configurations manually on a device-by-device basis. Prime LMS provides the Template Center feature, which can greatly reduce the configuration deployment time by using predefined or customized templates. These templates can also be imported from machines and then stored as system-defined templates in Prime LMS.

#### Reporting

Prime LMS provides a single launch point for all the reports—including inventory, switch ports, technology, fault and event, performance, and audit reports. Administrators can archive these reports and view them at a later time.

#### Figure 5 - Report Generation and View Layout

Reports  Admin  Work Cent	ers 🔻		문 습
	Switch Port Capacity Ports • Recently Down Reclaim • Summary Utilization History *** Cisco.com Bug Summary Contract Connection Locate Device Compliance and Audit Service Reports • Lifecycle Management Reports • Compliance Reports • Reports Job Browser Change Audit •	Technology     EnergyWise      TrutSic      Meddinet     PoE      VLAN     VRE Lite      System     All Server Analysis     Data Collection Metrics     Device Support     Status      Users      System Audit Reports     System     Device Administration     IPSLA     Performance     Inventory and Config	<ul> <li>Fault and Event         Best Practices          Embedded Event Manager Syslogs             Generic Online Diagnostics Syslogs             History              PSIRT Summary             Syslog              Threshold Volation </li> </ul> <li>Beport Archives             Inventory and Syslog             IPSLA             User Tracking             VRF Lite             Layer2 Services             Report Settings             Report Publish Path         </li>

#### **Work Centers**

The Work Centers feature allows administrators to access more advanced features (such as EnergyWise, Smart Install, Identity, and Auto Smart ports) for day 1 to day N operations.

Figure 6 - Work Center Layout

Work Centers 🔻			물 습
■ TrustSec Dashboard Getting Started Readiness Assessment RADIUS Configuration Identity Configuration ▼ Secured Group Access Configuration ▼ Reports ▼ Jobs Smart Install Getting Started Readiness Assessment Configure ▼ Reports Jobs	<ul> <li>✓ EnergyWise         <ul> <li>Dashboard</li> <li>Getting Started</li> <li>Readiness Assessment</li> <li>Configure →</li> <li>Settings →</li> <li>Reports →</li> <li>Jobs</li> </ul> </li> <li>Medianet         <ul> <li>Dashboard</li> <li>Getting Started</li> <li>Readiness Assessment</li> <li>Configure</li> <li>Readiness Assessment</li> <li>Configure</li> <li>Reports</li> <li>Jobs</li> </ul> </li> </ul>	Auto Smartports Getting Started Readiness Assessment Manage Templates Configure Reports Jobs	25 Apr 2012, 11:20 PC

#### Notes

# **Deployment Details**

#### Process

Installing and Configuring Cisco Prime LMS

- 1. Obtain a license
- 2. Install Software
- 3. Configure basic settings
- 4. Configure Prime LMS user authentication
- 5. Configure Prime LMS user roles
- 6. Add devices and credentials
- 7. Manage administrator tasks
- 8. Configure syslog collection

#### Procedure 1 Obtain a license

Cisco Prime LMS offers a single software installation that can manage up to 10,000 devices. Software licensing allows you to evaluate the software before deciding how you want to proceed: purchasing the license, piloting a small deployment before rolling it out organization-wide, or growing your network management system along with your network. Licensing allows you to first evaluate the software without requiring that you reinstall the software later.

There are two ways to acquire a license:

• **Physical Media**—Ordering the product DVD that comes with a Product Activation Key (PAK). The PAK is normally printed on the software claim certificate included with product DVD kit. Use the PAK on http://cisco.com/go/license in order to get the license.

 Downloading Cisco Prime LMS evaluation software and ordering a digital PAK—Download an evaluation copy of Prime LMS from http:// cisco.com/go/nmsevals. You will receive a PAK via email. Use this PAK on http://cisco.com/go/license in order to get the license.

#### Procedure 2

Install Software

You can install the Prime LMS soft appliance by using the LMS Open Virtualization Archive (OVA) image from the LMS DVD. Before installing, please note that the following:

- Make sure that your system meets the recommended hardware and software specifications listed in the Prime LMS release notes.
- It takes approximately 30 minutes (deployment in the local system) or 50 minutes (deployment in the network) to install the soft appliance on a virtualized environment.
- Soft appliance OVA software can be installed only in the VMware environment.



You need not install any soft appliance image on the virtual machine (VM) before installing Prime LMS, because the LMS OVA image has an embedded RedHat Enterprise soft appliance.

It is recommended you do the following before installing the Prime LMS soft appliance:

- Configure DNS entries for each network device.
- Enable SNMP and Secure Shell (SSH) Protocol on the devices you are going to import.:

**Step 1:** Install and power on the Prime LMS OVA on the VMware ESX/ESXi server using VMWare vSphere. The Welcome screen appears.

Step 2: Press Enter in the console window to continue with the next step.

Step 3: Enter the following configuration details of the server:

- Hostname (Example: LMS)
- IP Address (Example: 10.4.48.35)
- IP Netmask (Example: 255.255.255.0)
- Default Gateway (Example: 10.4.48.1)
- · DNS Domain Name (Example: cisco.local)
- Primary Name Server (Example: 10.4.48.10)
- Add/Edit another name server? Y/N (Example: N)
- Primary NTP Server (Example: 10.4.48.17)
- System Time Zone (Example: America/Los\_Angeles)

**Step 4:** Enter the username to access the Prime LMS appliance console. This user will have the privilege to enable the shell access. The default username is *sysadmin*. You cannot use *root* as the username because it is a reserved username. You can use only alphanumeric characters for the username.

**Step 5:** Enter and confirm the sysadmin password. By default, this password is set as the shell password.

**Step 6:** Enter and confirm the password for the admin account to use to log in to Prime LMS using the browser. This password must contain a minimum of five characters and is also used for the System Identity account.

The following message appears:

For security reasons, passwords are not displayed. Do you want to view all the passwords? (Y/N) [N]:

#### Step 7: Enter N.

It takes 15 to 20 minutes to process the database engine, and then the server automatically reboots.

#### **Procedure 3**

**Configure basic settings** 

**Step 1:** On the client machine's web browser, disable any pop-up blockers and ensure that JavaScript is enabled.

To enable JavaScript:

- In Internet Explorer 8 or later, navigate to Tools > Internet Options > Security > Custom level > Settings, and then under Scripting of Java applets, select Enable.
- In Mozilla Firefox 9.x, navigate to Tools > Option > Content, and then select Enable JavaScript.

**Step 2:** Open the Prime LMS portal in your web browser. The browser reaches the Prime LMS portal by appending the port number 1741 to the DNS host name of the server on which you installed Prime LMS. Example: Ims.cisco.local

**Step 3:** Log in using the username **admin** and the password that you provided during installation.



The Getting Started pane shows you the workflow for configuring Prime LMS.

**Tech Tip** 

The configuration process described in this guide does not use every step in the Getting Started workflow.



**Step 4:** Under Getting Started, click **System Settings**, enter values in the **SNTP Server** and **Administrator E-mail ID** field, and then click **Apply**. You will receive automatic email alerts about network issues, job status, report generation, etc.

E-mail Settir	ngs				
SMTP Server	smtp.cisco.local		Administrator E-mail ID	lms@cisco.local	
Enable E-r	nail Attachment	Max. Size Of Att	achment 2 MB 🔻		

Step 5: To configure the Prime LMS portal to support HTTPS connections, navigate to Admin > Trust Management > Local Server > Browser-Server Security Mode Setup.

Current Settings	Browser-Server Security Mode Setup
Browser-Server Security	Current Setting: Enabled
Mode Setup	Change Setting To:      Enable      Disable
Certificate Setup	Apply

Step 6: Select Enable, and then click Apply.

#### **Procedure 4**

**Configure Prime LMS user authentication** 

#### (Optional)

Prime LMS can use its local database, Active Directory, Lightweight Directory Access Protocol (LDAP), TACACS+, and many other modules to authenticate user logins. To enable a common authentication experience for network administrators across network devices and the network management system, this guide describes how to configure Prime LMS to use TACACS+ authentication.

Step 1: Navigate to Admin > System > Authentication Mode Setup.

Step 2: Select TACACS+, and then click Change.

uthen	tication Mode Setup	
Authenti	cation Mode Setup	
Current Log	jin Mode: Local Authentication	
Available	Login Modules	
10	Local Authentication	
2	Local UNIX System	
3	MS Active Directory	
4	RADIUS	
50	TACACS+	

**Step 3:** Set the **Server** (Example: acs.cisco.local) and **Key** (Example: SecretKey), and then click **OK**.

Login Module Options		
Selected Login Module: Description:	TACACS+ CiscoWorks TACACS+ login module	
Server:	acs.cisco.local	]
Port:	49	]
SecondaryServer:		]
SecondaryPort:	49	]
TertiaryServer:		]
TertiaryPort:	49	]
Key:	•••••	
Debug:	🔘 True 🔘 False	
	<ul> <li>Allow all CiscoWorks local users t CiscoWorks Local login.</li> </ul>	to fallback to the
Login fallback options:	<ul> <li>Only allow the following user(s) in CiscoWorks Local login if preceding logic</li> </ul>	
	admin	(comma separated)
	Allow no fallbacks to the CiscoWe	orks Local login.
		OK Cancel

**Step 4:** When the Login Module Change Summary window appears, indicating the changes were updated successfully, click **OK**.

#### Procedure 5

**Configure Prime LMS user roles** 

A role is a collection of privileges that dictates the type of system access the user has. The predefined roles are:

- Help Desk—These users can access network status information only. They cannot perform any action on a device or schedule a job on a network.
- Network Operator—Users can perform all help-desk tasks and tasks related to network data collection. They cannot perform any task that requires write-access on the network.
- Approver—Users can approve all tasks.

- Network Administrator—Users can perform all Network Operator tasks, as well as configuration changes.
- System Administrator—Users can perform all Prime LMS system administration tasks.
- Super Admin—Users can perform all Prime LMS operations, including administration and approval tasks.

When using an authentication module other than the Prime LMS local database, Prime LMS authenticates the user against the external module. After the user is successfully authenticated, Prime LMS assigns the default role to this user unless there is a pre-assigned role for this user.

#### Step 1: Navigate to Admin > System > User Management > Role Management Setup.

Step 2: Select the check box next to the role you want to define as the default role, and then click Set as default.

Choose the role that you will assign to the majority of users in your organization. For example, if the majority of users should be able to use Prime LMS to perform network configuration tasks but not administer the Prime LMS system itself, assign Network Administrator as the default role.

Navigator	Role Ma	nagement Setup		
Local User Policy Setup				Showing 6 record
Local User Setup		Roles	Description	Default Roles
Notify Users	1.	Approver	Approver Role	
Role Management Setup	2. 🥅	Help Desk	Help Desk Role	
	3. 🔽	Network Administrator	Network Administrator Role	V
	4. 🕅	Network Operator	Network Operator Role	
	5. 🕅	Super Admin	Super Admin Role	
	6. 🕅	System Administrator	System Administrator Role	
	Add	Edit Delete Copy I Exp	ort Import I Set as default Clear default	

For any users who require different permissions than those included in the default role, create local user accounts and assign a Prime LMS role to each of the local user accounts you create.

# Step 3: Navigate to Admin > System > User Management > Local User Setup.

Step 4: Click Add. The Add Users window opens.

**Step 5:** Enter the username used in the TACACS+ login, configure a password (it does not have to match the TACACS+ login password and it is not used during authentication), select the **Super Admin** check box, and then click **OK**.

User Login Details Username:	ExampleAdministrat	or
Password:	•••••	Verify Password:
Email:		
Roles Help Desk Help Desk Retwork Operator Retwork Administrator System Administrator Super Admin	. Device Not Ap	uthorization O Enable Device Authorization e level Authorization pplicable
Network Level Login Cred Username:	entials	
	Verify	Password:
Password:		

#### Procedure 6

Add devices and credentials

Before Prime LMS can manage a device, the device must be in the LMS Device Credential Repository (DCR). You can add devices to the DCR in three ways:

- Discover the devices using a discovery protocol
- Add devices manually
- Bulk import of devices

Prime LMS supports Layer 2 and Layer 3 protocols for device discovery. Device discovery using Cisco Discovery Protocol is the preferred protocol used by Prime LMS to discover network devices in the LAN. Both Cisco Discovery Protocol and SNMP must be enabled on devices before using this procedure. If you did not deploy your network by using the Cisco SBA Borderless Networks Deployment Guides, which enable both of these protocols, see http://cisco.com/go/lms for guidance.

The example presented here uses the LMS Prime Discovery feature.

# Step 1: Navigate to Admin > Getting Started > Device Management > Device Addition.

Admin > Getting Started	22 May 2012, 09:16 PDT
Cisco Prime LMS Overview	Getting Started
Cisco Prime LAN Management Solution (LMS) has powerful features that enable you to configure, monitor, troubleshoot	> Introduction
and administer Cisco networks. Cisco Prime Getting Started helps you in setting up LMS and in getting it ready to manage your network infrastructure.	> Data Migration
·	> System Settings
New Features in LMS 4.2 🧮	*Device Management
🔒 Standard Discovery 🔹 Compliance and Audit Management	Device Allocation Settings
	Auto allocate all devices: Enabled
Show more of LMS4.0 and LMS4.1 features	
	😤 Device Addition
Do not show Getting Started wizard at next login	Devices in DCR:
Proceed to Data Migration	> User Management
Skip the rest of the workflow and proceed to Device Status dashboard	> Software and Device Updates

**Step 2:** Click **Credential Sets**. Credential sets allow Prime LMS to apply a default set of credentials to devices after discovery. Prime LMS then uses the credentials in order to manage the device inventory, configuration, and software.

Admin > Getting Star	ted
Device Addition	
	can add devices to Device Credential Repository (DCR), and if required, create credential sets, and configure policies. d directly, using credential sets, or policies.
Adding Devices to	DCR
You can create cre used for accessing	dential sets, and configure policies before adding devices to DCR. The appropriate credential set, based on the policies configured, will be the devices.
Step 1 : Create Cr	redential Sets
You can add, e	dit, or delete credential sets. You can assign these credential sets while adding devices.
Configure Cred	lential Sets
Step 2 : Create Cr	redential Set Policy
You can add, e get accessed.	dit, order, or delete policies for credential sets. While adding devices you can assign the policy and based on the credentials, the devices
Configure Polic	cies for credential sets
Step 3 : Add Devi	Ces
Total number o	f devices in DCR is
Devices can be	added in any one of the following three ways,
Option 1 : Con	figure Device Discovery
You can ad	d devices to DCR through Device Discovery.

Step 3: Click Credential Set Name, and then set the Credential Set Name to SBA-Default.

Default Credentials	Credential Set	
<ul> <li>Credential Sets</li> <li>Credentials Set Name</li> <li>Standard Credentials</li> <li>SMMP Credentials</li> <li>HTTP Credentials</li> <li>Auto Update Server Managed Device Credentials</li> <li>Rx-Boot Mode Credential</li> </ul>	Credential Set : Credential Set Name : * Set Description :	Add New  SBA-Default [a-z, A-Z, 0-9, ., -, _] Default credential set used for devices on import to LMS
		ntial value to add new Credential Set. e can have a maximum of 32 characters.

Step 4: Click Next.

Step 5: In Standard Credentials, enter the Username (Example: Ims), Password, and Enable Password that Prime LMS should use when logging in via SSH, and then click Next.

Default Credentials	Primary Credentia	I		
Credential Sets     ··Credentials Set Name     ··Standard Credentials     ··SNNP Credentials     ··HTTP Credentials     ··Auto Update Server Managed     Device Credentials     ··Rx-Boot Mode Credential	Username: Password: Enable Password:	Ims	Verify:	•••••
	Secondary Credeni Username: Password: Enable Password:		Verify:	
Note: * - Required Field			Back Next Fini	ish Cancel Remove

**Step 6:** In **SNMP Credentials**, configure the **RO Community String** (Example: cisco) and **RW Community String** (Example: cisco123) that Prime LMS should use to poll the network devices, and then click **Next**.

Default Credentials	SNMPv2c/SNMPv1			
✓ Credential Sets ·· Credentials Set Name ·· Standard Credentials ·· SNMP Credentials ·· HTTP Credentials	RO Community String: RW Community String:	•••••	Verify: Verify:	•••••
•• Auto Update Server Managed Device Credentials •• Rx-Boot Mode Credential	SNMPv3 Mode: O	NoAuthNoPriv O AuthNoP	Priv 🔘 Aut	hPriv
	Auth Password:		Verify	:
	Auth Algorithm : Privacy Password:	None 🔻	Verify	:
	Privacy Algorithm :	None 💌		
Note: * - Required Field		Back	Finish	Cancel Remove

**Step 7:** In **HTTP Credentials**, configure the **Username** (Example: Ims) and **Password** that Prime LMS should use when configuring a device via HTTPS.

Step 8: In the Current Mode list, choose HTTPS, and then click Finish.

Default Credential Set - SBA-Defaul	t			
Default Credential Set - SBA-Default Default Credentials * Credential Sets • Credentials Sets Name • Standard Credentials • SNMP Credentials • HTTP Credentials • Auto Update Server Managed Device Credentials • Rx-Boot Mode Credential	Primary HTTP	Ims TP Credential	Verify: Verify:	
	HTTP Port: Current Mode:		PS Port:	
Note: * - Required Field		В	ack Next F	inish Cancel Remove

Step 9: On the Admin > Getting Started page, click Device Management.

The Module Settings pane appears. You use this pane to enable the discovery protocols that Prime LMS will use to discover the devices on the network.

Getting Started	
> Introduction	
> Data Migration	
> System Settings	
<b>~</b> Device Management	
Device Allocation Settings Auto allocate al devices: Enabled	
Device Addition Devices in DCR: 3	
> User Management	

Step 10: Select Device Addition, then scroll down to Edit Custom Discovery Settings.

Standard Discovery Settings		
Seed Device Settings		
Use LMS Server Default Gateway as seed (7)		
Current Default Gateway : 10.4.48.1	Seed Device	0
Use DCR as seed 🍘		
NMP Settings		
Use Policy Configuration Settings (Configured) 🔘 Use Cust	on Policy Configuration Settings	
<u></u>	on roley comparaton actungs	
Edit Policy Configuration		
SNMPv2c to SNMPv1 Fallback SNMPv3 to SNMPv2 Fall	back	
SNMPv2c to SNMPv1 Fallback SNMPv3 to SNMPv2 Fall	back	
Z SNMPv2c to SNMPv1 Fallback SNMPv3 to SNMPv2 Fall	back	
SNMPv2c to SNMPv1 Fallback SNMPv3 to SNMPv2 Fall SNMPv2c to SNMPv1 Fallback	back	
✓ SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
Z SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
Z SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
✓ SNMPv2c to SNMPv1 Failback ☐ SNMPv3 to SNMPv2 Fail		scovery Stop Discovery
Z SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv2 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv2 Fallback ☐ SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3 to SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3 to SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNM		scovery Stop Discovery
Z SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv3 to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3		scovery Stop Discovery
Z SNMPv2c to SNMPv1 Fallback		scovery Stop Discovery
✓ SNMPv2c to SNMPv1Fallback □ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
✓ SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
✓ SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv2c to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fall SNMPv3 to SNMPv1 Fallback ☐ SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMPv3 to SNMPv3 to SNMPv2 Fallback ☐ SNMPv3 to SNMP		scovery Stop Discovery
✓ SNMPv2c to SNMPv1Fallback □ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
✓ SNMPv2c to SNMPv1 Fallback □ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
SNMPv2c to SNMPv1 Fallback SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
✓ SNMPv2c to SNMPv1 Fallback □ SNMPv3 to SNMPv2 Fall		scovery Stop Discovery
SNMPv2c to SNMPv1 Fallback SNMPv3 to SNMPv2 Fall  Fdit Custom Discovery Settings		scovery Stop Discovery

Step 11: Select Cisco Discovery Protocol, and then click Next.

Module Settings
Layer 3 Discovery Protocols
Address Resolution Protocol (ARP)
Border Gateway Protocol (BGP)
Open Shortest Path First Protocol (OSPF)
Routing Table
Layer 2 Discovery Protocols
Cisco Discovery Protocol (CDP)
Link Layer Discovery Protocol (LLDP)
Ping Discovery Option
Ping Sweep on IP Range
Others
Cluster Discovery Module
Hot Standby Router Protocol (HSRP)

The seed device setting page appears. A seed device is the start point from which Prime LMS discovers the network. The seed devices should be the core devices on the network and should reside in DNS. The *Cisco SBA— Borderless Networks LAN Deployment Guide* presents core device options for a range of performance and scale scenarios.

Step 12: Click CDP, click Add, and then configure the first seed device as the LAN core switch (Example: C6509-1.cisco.local). Enter the maximum number of hops under Hop Count for the first device.

Step 13: Click Add again, configure the second seed device as the other core switch (Example: C6509-2.cisco.local), enter the maximum number of hops under Hop Count for the second device, and then click Next.

**Tech Tip** 

Ensure hostnames have been added to the DNS, or use the device's loopback IP address when adding a device as a seed device.

Seed Devices Module Specific CDP	CDP		
* Global	File to be Imported	Browse Use DCR as Seed Li Jump Router Bound Showing 2 records	
	Seed Devices		
	1. 🕅 C6509-1.cisco.k	ocal 10	
	2. 🔲 C6509-2.cisco.le	ocal 10	
		Delete I Add	

**Step 14:** On the **SNMP settings configuration** page, click **Add**. A new window pops up.

**Step 15:** Enter the target value (\*.\*.\*), which tells Prime LMS to use this SNMP community string for all devices during discovery.

**Step 16:** Enter the read-only SNMP community string configured on your network devices (Example: cisco), and then click **OK**.

۲								
	SNMPv2c to SNMPv1 Fallback SNMPv2 Showing 1-1 of 1 reco							
	1.	SNMP Version	Target *.*.*.*	Read Community	Timeout 3	Retries	Comments	
	1. v2c *.*.* ******* 3 1							

**Step 17:** Click **Next** for **Global Settings**, and under Preferred DCR Display Name, select **Host Name**.

Step 18: Select Update DCR Display Name.

Step 19: In the Default Credential Set list, choose SBA-Default.

Step 20: Under Preferred Management IP, select Use LoopBack Address, check Prefer IPv4 over IPv6 Address, and then click Finish.

Mode: ADDING	Global Settings	
Mode: ADDING # 1. Module Settings # 2. Seed Device Settings # 3. SNMP Settings # 4. Filter Settings 5. Global Settings 6. Summary	Global Settings  Preferred DCR Device Name Sysname DNS Resolvable Host Name Append Domain Name to device name Yes NoTE: If multiple options are selected, the falback order will be Sysname, DNS resolvable hostname, and IP address.  DCR Administration Settings Update DCR Device Name Select a Default Credential Set: SBA-default E-mail:	Preferred Management IP Use LoopBack Address Prefer IPv4 over IPv6 Address Resolve by Name Resolve by SysName None Add Discovered Devices to a Group None Al Devices Devices newly discovered during last rur Group Name: Select
		Delete Devices from Group NOTE: If you select the option "Devices newly discovered during last run" and enter/select an existing Group Name, the group rule will be overwritten.

**Step 21:** In the message that informs you that discovery settings are successfully configured, click **OK**.



**Step 22:** Near the bottom of the Adding Devices to DCR page, click **Start Discovery**.

Device Addition	Getting Started	
Using this page you can add devices to Device Credential Repository (DCR), and if required, create credential sets, and configure policies. Devices can be added directly, using credential sets, or policies.	> Introduction > Data Migration	
Adding Devices to DCR		
You can create credential sets, and configure policies before adding devices to DCR. The appropriate credential set, based on the policies configured, will be used for accessing the devices.	> System Settings	
Step 1: Create Credential Sets	~Device Management	
You can add, edit, or delete credential sets. You can assign these credential sets while adding devices.	Device Allocation Settings	
Configure Credential Sets	Auto allocate all devices: Enabled	
Step 2: Create Credential Set Policy		
You can add, edit, order, or delete policies for credential sets. While adding devices you can assign the policy and based on the credentials, the devices get accessed.	Service Addition	
Configure Policies for credental sets	Devices in DCR: 48	
Step 3: Add Devices		
Total number of devices in DCR is 48	> User Management	
Devices can be added in any one of the following three ways,	Software and Device Updates	
Option 1: Configure Device Discovery		
You can add devices to DCR through Device Discovery.		
Backdo Bacowry         Samary           Standard Discovery Settings         Seed Prove Settings           Seed Prove Settings         (7) Uoc UIG Server Default Gateway as seed ()		
Current Default Gateway : 10.4.48.1 Seed Device		
Use DCR as seed 💿		
SIII4P Settings		
Use Policy Configuration Settings (Configured)     Use Custom Policy Configuration Settings		
Edit Policy Configuration		
SNMP-V2: to SNMP-V1 Falback 📃 SNMP-V3 to SNMP-V2 Falback		
Save Cancel Start Discovery Stop Discovery		

Prime LMS starts discovering the devices on the network. The amount of time this discovery process takes depends on the number of devices on the network. The Discovery window is refreshed every 5 seconds and updates the number of devices being discovered.

**Step 23:** If you want to view the discovery progress, click the discovery **Summary** tab. The data automatically updates. If you want to instantly update the in-progress results, click the blue refresh icon.

Standard Discovery Summary	
Discovery Summary	0
Discovery status	Running
Discovery Type	Custom
Discovery start time	Thu Apr 26 14:56:36 PDT 2012
Discovery end time	
Total devices discovered	25
Reachable devices	13
Unreachable devices	12
Devices newly added to DCR	0
Devices updated in DCR	13
Start Custom Discovery	

After the process is completed, the status changes from running to complete.

Admin > Getting Started	
Device Addition	
Using this page you can add devices to Devic Devices can be added directly, using credent	e Credential Repository (DCR), and if required, create credential sets, and configure policies. ial sets, or policies.
Adding Devices to DCR	
You can create credential sets, and configu	re policies before adding devices to DCR. The appropriate credential set, based on the policies configured, will be used for accessing the devices.
Step 1 : Create Credential Sets	
You can add, edit, or delete credential :	sets. You can assign these credential sets while adding devices.
Configure Credential Sets	
Step 2 : Create Credential Set Policy	
You can add, edit, order, or delete polic	cies for credential sets. While adding devices you can assign the policy and based on the credentials, the devices get accessed.
Configure Policies for credential sets	
Step 3 : Add Devices	
Total number of devices in DCR is 48	
Devices can be added in any one of the	following three ways,
Option 1 : Configure Device Discove	ery
You can add devices to DCR throug	h Device Discovery.
Standard Discovery Sum	imary
Discovery Summary	@
Discover	y status Completed
	ery Type Custom
Discovery s	tart time Thu Apr 26 14:56:36 PDT 2012
Discovery	end time Thu Apr 26 15:00:56 PDT 2012
Total devices dis	scovered 40
	devices 26
Unreachable	
Devices newly added	
Devices update	ainuuk 21
Start Custom Discovery	

Devices on the network have been discovered and are ready for other management tasks such as asset, configuration, and software image management.

#### Procedure 7

Manage administrator tasks

Device configuration can occur on an as-needed or scheduled basis.

Step 1: Navigate to Admin > Collection Settings > Config.

**Step 2:** Click **Config Collection Settings**, and then under Period Polling, select **Enable**.

Periodic	Polling	
Status:	Enable     Disable	
Job ID:	Not Available	
Schedule:	Not Available	Schedu
		Apply Cance
Periodic	Collection	
Status:	Enable O Disable	
Job ID:	Not Available	
Schedule:	Not Available	Schedul
		Apply Cance
VI AN Cor	fig Collection	

Step 3: Click Schedule.

**Step 4:** In the window that appears, set the time to a non-peak time on the network, and then click **OK**.

Schedule	
Scheduling	9
Run Type:	Daily 💌
Date:	26 Oct 2011 🗰 🔻 at 23 💌 30 💌
Job Inform Job Descript E-mail:	nation tion: System Config Polling Job
	OK Cancel

Step 5: Click Apply.

Step 6: Repeat Step 2 through Step 6 for Periodic Collection.

onfig Colle	ection Settings	
Periodic	Polling	
Status:	Enable Disable	
Job ID:	1143	
Schedule:	Apr 26 2012 05:15:00	Schedul
		Apply Cance
Periodic	C <mark>ollection</mark>	
Status:	Enable Disable	
Job ID:	1142	
Schedule:	Apr 28 2012 04:20:00	Schedul
		Apply Cance
VLAN Cor	ifig Collection	

Step 7: Navigate to Admin > Network > Software Image Management > View / Edit Preferences, select the Use SSH for software image upgrade and software image import through CLI (with fallback to TELNET) check box, and then click Apply.

iew/Edit Preferences				
Repository				
Image Location *:	/var/adm/CSCOpx/fil	es/rme/repository/		
Distribution				
Script Location				
Script Location			Brov	Clear
Script Timeout	90	seconds		
	Available Protoc	cols	Selected Protoco	l Order
	RCP TFTP SCP HTTP	Add	RCP TFTP SCP HTTP	Up
Image Transfer Protocol O	rder	<< Rem		Down
Use SSH for software in Recommendation	nage upgrade and sof	tware image import through	L CLI(with fallback to TELNET).	
Include Cisco.com imag     Include General deploy     Include latest mainten     Include images higher     Include same image fe	ment images. ance release (of each i than running image.	major release).		
Password Policy Enable Job-based Pass User Configurable	vord			

Step 8: Navigate to Admin > Collection Settings > Config > Config Transport Settings.

**Step 9:** For each application in the **Application Name** list, adjust the selected protocol order to be **SSH**, **HTTPS**, **TFTP**, and then click **Apply**.

Application Name:	Archive Mgmt			
	Available Protocols		Selected Protocol Order	
Config Fetch :	SSH HTTPS TETP TELNET RCP SCP	Add >> << Remove	SSH HTTPS TFTP	Up Down
	Available Protocols SSH HTTPS		Selected Protocol Order SSH HTTPS	]
Config Deploy :	TFTP TELNET RCP SCP	Add >> << Remove	TFTP	Up Down

Procedure 8

Step 1: Navigate to Monitor > Fault Settings > Syslog > Configure Syslog on Device. The screen Devices and Tasks appears.





Step 2: Under Device Selector, expand Device Type Groups.

Step 3: Select Routers.

Step 4: Select Switches and Hubs, and then click Next.

Step 5: Click Add Instance.

**Step 6:** Set the **Logging Host Action** to **Add** and set **Hosts** to the Prime LMS server (10.4.48.35).

Step 7: Set the Logging On Action to Enable.

**Step 8:** Set the **Logging Facility Action** to **Enable** and the **Parameter** to **local7**.

Step 9: Set the Trap Action to Enable and the Conditions to errors.

Step 10: Click Save.

Syslog	Configuration	L
Comm	non Parameter	\$
Loggi	ng Host	
Action:	Add 🗖	Hosts (comma separated): 10.4.48.35
IOS Pa	arameters	
Loggi	ng On	
Action:	Enable -	
Loggi	ng Facility	
Action:	Enable 🔹	Parameter: local7 -
Loggi	ng Level	
Buffer	ed	
Action:	No Change 🔻	Conditions: Default
Conse	ole	
Action:	No Change 🔻	Conditions: Default
Monit	or	
Action:	No Change 🔻	Conditions: Default
Trap		
Action:	Enable 🔻	Conditions: errors -

Step 11: Click Next.

**Step 12:** Enter **Job Description** (Example: Configure Syslog Destination of Devices), and then click **Next**.



Step 13: At the Job Work Order screen, click Finish.

Step 14: Click Monitor. You can now view the syslog messages.



Using the Inventory Dashboard, you can view all information regarding hardware, software, user tracking, device audit changes, device discovery, and support devices.

Inventory > Dashboar	ds > Inventory					27 Oct 2011, 07:33 P
Hardware Sumr	nary		/ 存? _ □ ×	Software Summary		/捺?」Ⅲ×
		Cisco I	nterfaces and Modules	Software Version		Count
		Wireles	s	15.1(4)M2		22
		Unknov	10	12.2(58)SE2		22
			s and Hubs	Generic Class		6
				15.1(3)50a		5
		Security		15.0(1)SY		3
		Routers		4.4.1.12		2
		Conten	t Networking	03.02.00.XO		1
				03.02.01.SG		1
				12.2(55)EX2		1
				8.4(2)		1
				15.0(0.0.90)SE1		1
Device Change	1		/ 僖 ? _ 田 ×	ADIO(OIDI)OJOLA		
Device Name	User Name	Creation Time	Message	User Tracking Summary		Z 存 ? □ ⊞ ×
A2960S.cisco.local	estg	Oct 27 2011 04:42:30	CONFIG_CHANGE	Number of End hosts		70
		Oct 27 2011		Number of Active End hosts		54
A2960S.cisco.local	estg	03:31:35	CONFIG_CHANGE	Number of Connected End Ho	sts	24
		Oct 27 2011	CONFIG_CHANGE	Number of Dormant hosts in last 7 days		9
A29003.clsco.local	esty	03:21:53	CONFIG_CHANGE	Number of New hosts in last 7	' days	0
A2960S.cisco.local	estg	Oct 27 2011 03:16:29	CONFIG_CHANGE	Number of Rogue hosts in last	: 7 days	0
A2960S.cisco.local	estg	Oct 27 2011 03:05:05	CONFIG_CHANGE	Device Discovery Summ	агу	✓ − − − ×
				Discovery Status	Completed	
Supported Devi	ce Finder		/存?」回×	Discovery Start Time	21 Oct 2011, 11:24 PDT	
Display Name	•		Submit Reset	Discovery End Time	21 Oct 2011, 11:24 PDT	
Display Name			Jubinit	Total Devices Discovered	4	
				Reachable Devices	3	
				Unreachable Devices	1	
				Devices Newly Added to DCR	0	
				Devices Updated to DCR	3	

#### Procedure 1 Distribute software images

Software Image Management is a feature that enables you to push new images periodically to managed devices. This feature compares a managed device's existing image version with those in the Prime LMS local software image repository or on cisco.com. Available upgrade options are shown, and Prime LMS allows you to upgrade a managed device to an image through the GUI.

You can add software images to the repository (from cisco.com or a device, file system, or URL).

#### Step 1: Navigate to Configuration > Tools > Software Image Management > Software Repository.



#### Step 2: Click Add.

**Step 3:** Choose the source (Example: cisco.com) from which to you want to acquire the image, and then click **Next**.

Image Source	
Cisco.com	
C Device	
File System	
C URL	
Network	
Use generated Out-of-sync Report	

Next you must select device(s) for software upgrade.

Step 4: In the Prime LMS inventory, select a device, and then click Next.

	h Input>>	⇒,¢			
All	Search Results	Selection			
±⊽⊑				*	
	Device Type Grou				
	Content Netwo	orking			
	Routers			H	
E	l 🗐 🖬 Cis co 3900	Series Integrate	d Services		
E	Cis co ASR	1000 Series Ag	gregation S		
	🗄 🔽 🗂 Cis co A				
	E Cisco A				
ŧ.	] 🗐 Switches and	Hubs			
± [		Hubs ice Type		+	
± [	Switches and	Hubs ice Type	•	Ŧ	

Step 5: In the Device/Platforms pane, click the device name.

Step 6: In the Version pane, select the Software Version.

Step 7: In the Feature/Subset pane, select the Software Feature Set.

#### Step 8: Click Next.

Devices/Platforms:		Version:		Feature/Subset:
atalyst 2820 Series atalyst 2820 L2/L3 Series atalyst 2950 L2/L3 Series atalyst 2950 Series atalyst 2955 Series atalyst 4000 Series atalyst 4000 Series atalyst 4000 Series atalyst 6000 Series atalyst 6000 Series atalyst 8510/08515c Series atalyst 8510/08515m Series atalyst 8540c Series atalyst 8540c Series atalyst 8540c Series atalyst 8540c Series	* III +	6000-Supervisor720 8.7(3) 8.7(2a) 8.7(2) 8.7(1) 8.6(6a) 8.6(6) 8.6(5) 8.6(4) 8.6(3) 8.6(2) 8.6(2) 8.6(1) 8.5(9) 8.5(8)	•	6000-Supervisor720 Catalyst 6000 Supervisor 720 Flash Code Catalyst 6000 Supervisor 720 Flash with SSH support
		Images to be Added		
Devi	ces/Platfor	ms Version	Subset	
1 Catal	st 6000 Se	ries 8.7(2a) Catalyst 6000 Superv	isor 720 Flash	with SSH support

**Step 9:** Ensure that the check box in the Download column is selected, and then click **Next**.

Device/Platform	Selected Version and Subset	Image Requirements	Download
Catalyst 6000 Series	8.7(2a) 6000-Supervisor720 Catalyst 6000 Supervisor 720 Flash with SSH support	N/A	2

Step 10: Enter a Job Description, and then click Next.

Job Cont Scheduling Run Type: Immediate 💌	rol Information		
Date: 25 Apr 2012 Job Info Job Description:* Downl E-mail: Comments:	at 16 V 30		
		.4	

**Step 11:** On the **Image Import Work Order**, view the software image job summary, and then click **Next**.

	Image Import Work Order
Work Or	der: Job Summary
	Job Description: Download Software E-mail to: Scheduled at: 30 Aug 2012 16:30 Approval: Disabled Approver List: None Job Based Password: Disabled The following images will be copied to the image repository.
	File Name :cat6000-sup720k9.8-7-2a.bin Size :19462024 Device Name/Platform :Catalyst 6000 Series
	۲ III I

Step 12: Click Finish.

**Step 13:** Click the name of the software image that was added in the previous step and make sure that the device requirements are set correctly.

**Step 14:** Set the **Minimum Ram** and **Minimum Flash** to the correct values if they are incorrect, and then click **Update**.

File Name : e2			z SPA 151-4 M4 bin
Image Name : C			
		ROALN	(3-1V)
Image Version : 15	1.1		
Image Family : C3	3900		
Image Type : S'	YSTEM_SV	V	
File Size : 66	3546432		
Image Check Sum : 85	50e4a16del	od51e51	1da47f0366af205f
Creator :			
Updated At : Ap	pr 26 2012	13:49:40	0
Location : /vi	ar/adm/CS0	Opx/file	es/rme/repository/swim/SYSTEM_SW
Comments : Ad	dded as par	t of Job-	-1148
Minimum RAM (MB):	1024	•	
Minimum Flash (MB):		•	
Feature:	IPISLAIIPV	BIIS-ISIF	FIREWALL PLUS QoS HA NAT MPLS VPN L DLS 3DES SSH APPN IPSEC
Minimum Boot ROM Version:	UNKNOV	VN	
			OK Update

Step 15: Navigate to Configuration > Tools > Software Image Management > Software Distribution.

**Step 16:** Click **Software Distribution**, select **By devices [Basic]**, and then click **Go**.

Distribution Method	
By devices [Basic]	
By devices [Advanced]	
By image	
Use remote staging	

**Step 17:** Choose the device or devices for software image distribution, and then click **Next**.



**Step 18:** On the page that appears, enter your cisco.com credentials, and then click **OK**.

Prime LMS shows the images available in the software repository for the selected device or devices.

Distribute by Device:	5			
			Sł	View Details nowing 2 records
Device Information	Module Information	Image Options	Storage Options	Errors
1. RS200-3945-1.cisco.local	SYSTEM_SW	c3900-universalk9-mz.SPA.151-4.M2.bin(63.78 MB) 💌	flash0:1(3860.38 MB/3992.55 MB 🕶	]
2. RS200-3945-2.cisco.local	SYSTEM_SW	c3900-universalk9-mz.SPA.151-4.M2.bin(63.78 MB) 💌	flash0:1(843.61 MB/976.11 MB) 🔻	]
	<sup>2</sup> )Running Image fo	r RFF device (^)Image in Cisco.com (*)Recomme	nded Option	

**Step 19:** Select the image to which you would like to upgrade the device, and then click **Next**.

**Step 20:** In the Notifications window, click any failures or warnings for the software distribution, and then click **Next**.

**Step 21:** If you want to select options based on your organization's scheduling policy, you can do so on the Job Schedule and Options page, and then click **Next.** 

ob Schedule and Options			
Scheduling Run Type: Immediate  Date: 27 Oct 2011		Dob Options     Reboot immediately after downloa     Do not insert new boot command     Use current running image.     On error, stop processing subsequ	s into configura P fallback imag
Job Description:* Software Upgrad	e	Enable Job Password	
E-mail:		User Name:	
Comments:		Password:	
		Enable Password:	
		Execution: Parallel Sequential	Execution Or
		Reboot : Parallel Sequential	Poot Ordor

A new page shows the work order that was just created.

Step 22: Click Finish. This completes the work order.

#### Procedure 2

**Customize monitoring** 

Monitoring plays a big role in any network management process, and the Monitoring Dashboard provides a unified view of all the activities being monitored by an administrator. Prime LMS has a comprehensive list of monitoring portlets from a device level to the network level—such as device and interface availability; high severity alerts; memory, CPU, and interface use; performance threshold; fault summary; IPSLA violation reports; and syslog information.

You can customize these activities based on your network needs. This procedure describes one such activity, CPU utilization.

# **Step 1:** Access the Monitoring Dashboard by navigating to **Monitor** > **Dashboards** > **Monitoring**.

By default, you can view a list of devices with the top CPU utilization on the dashboard.

			Time I	interval: 1 H
Device Name	CPU Instances		Average %	Graph
A3750X.cisco.local		1	23.08	
RS200-A3750X.cisco.local		1	21.08	
RS212-A2960S.cisco.local		1	19.33	- 🔍
WAN-D3750X.cisco.local		1	11	. 🔍
RS202-A3560X.cisco.local		1	10	
0 - 10 10 - 30	30 - 80		80 - 100	

**Step 2:** Click the **Graph** icon. This displays the details of the CPU utilization for a specific device.

7.50 5.00 2.50 0.00	13:15	13:20	13:25	13:30	13:35	13:40	13:45	13:50	13:55	14:00	14:05	14:
------------------------------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-----

#### **Procedure 3**

#### **Generate and view reports**

Prime LMS provides you a single launch point for all reports that you can generate and view. The Reports menu provides the following options:

- Inventory Report—Contains reports pertaining to devices, hardware, and end-of-sale and end-of-life information
- Switch Port—Contains reports on switch capacity, switch port summary, and utilization history
- Technology—Contains reports for technologies like EnergyWise, Identity, Power over Ethernet, and VRF Lite
- Fault and Event—Contains information about threshold violation, device fault, syslog, and PSIRT
- Performance—Contains information about CPU and interface utilization, interface error, and IPSLA
- **System**—Contains information about the number of users logged in, collection detail, configuration file changes, and 24-hour change
- System Audit—Contains audit reports for software image distribution and download history
- Report Designer—Generates custom reports, especially for syslog and inventory
- cisco.com—Allows you to check contract information and bug status by using the bug toolkit
- **Compliance and Audit**—Reports status of all services on the network, lifecycle management, and regulatory compliance such as HIPAA, SOX, etc.
- View Report Archives—Creates a report from a scheduled report and stores it in the report archive



In this example, you generate an inventory report.

Step 1: Navigate to Reports > Inventory > Hardware > Detailed Hardware.

#### Step 2: Select All Devices, and then click Finish.

Navigator	Inventory Hardware Report
Inventory	
Detailed Device	Device Selector     Group Selector
Device Attributes	Device Selector
24-hour Inventory Change	< <search input="">&gt; → 💭 Run Type: Immediate 💌</search>
<ul> <li>Hardware</li> </ul>	All Search Results Selection Date: 25 Apr 2012
Chassis Slot Details	B All Devices
Chassis Slot Summary	Device Type Groups
Chassis Summary Graph	B Job Description*:
Detailed Hardware	E-mail:     E-mail:
Device Statistics	CSV     Attachment Option: Report type : PDF CSV
Hardware Component Summary	Report Publish Path*:
Hardware Summary Graph	48 device(s) selected
Multi Service Port	Finish
EoS/EoL Hardware	

Prime LMS generates a detailed hardware report, providing information about the device, including system description, RAM, image running, etc.

Cisco Catalyst 6500	Series Swil	ches											
Device Name	Updated A	System	n Description	Location	n Contact	Serial Number	Chassis Type	Vendor		NVRAM Size (KB)	NVRAM Used (KB)	ROM Version	Total Flash Device Size (MB)
	Apr 24 2012 16:26:46	r 24 2012 Cisco IOS Software, s2154 Software (s2154-IPSERVICESK9-M), Version 15.0(1)5Y1, 26:46 RELEASE SOFTWARE (fol) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Thu 16-Feb-12 21:36 by prod rel team				SMG123	IN257 cevChas	sisCat6509	1024.00	0.00		12.2(50r)5Y53	2 3938.28
	Apr 25 2013 12:02:04	RELEA	OS Software, s2154 Software (s2154-IPSERVICESK9-M), Version 15.0(1) SE SOFTWARE (fc4) Technical Support: http://www.cisco.com/techsu ght (c) 1986-2012 by Cisco Systems, Inc. Compiled Thu 16-Feb-12 21:36 el team	port		5MG123	IN259 cev Chas	sisCat6509	1024.00	0.00		12.2(50r)5Y53	2 1495.96
	Apr 25 2012 12:02:14	RELEA	OS Software, s2154 Software (s2154-IPSERVICESK9-M), Version 15.0(1)5 SE SOFTWARE (fc4) Technical Support: http://www.cisco.com/techsu ght (c) 1986-2012 by Cisco Systems, Inc. Compiled Thu 16-Feb-12 21:38 el team	port		5MG123	IN257 cev Chas	sisCat6509	1024.00	0.00		12.2(50r)5Y53	2 3938-28
Cisco Catalyst 3750	Series Swit	ches											
Device Name	Upd	ated At	System Description		Location	Contact	Serial Number	Chassis V	endor Type	Total RAN Size(MB)	NVRAM Size (KB	) NVRAM Used (KB)	Total Flash Device Size (MB)
HQ-C3750X- PR1.cisco.local	Apr 12:0	:20	Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Vensi RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/ Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Thu 22-Dec-1 prod_rel, team	echsupport			DO1443Z10Y	cevChass	isWsC3750x24	P272.00	512.00	26.35	55.00

**Procedure 4** 

**Deploy templates** 

Another important feature, *templates*, is specifically designed for deploying configurations in managed networks. Typically, a network consists of thousands of devices, and it is an enormous task for administrators to configure each of these devices individually. Ideally, they would like to have a set of templates with standard (or global) configurations that are common to certain devices in the network. Using these templates, administrators can quickly deploy the configuration, thus saving a lot of time as well as avoiding configuration errors that may happen during manual configuration.

Prime LMS provides system-defined or user-defined templates, which are in the form of .xml files. You can customize these templates to accommodate your needs. This procedure focuses on importing and deploying templates that are specific to the Cisco SBA architecture.

Templates based on *Cisco SBA—Borderless Networks LAN Deployment Guide* are included as part of Prime LMS. You can also edit the templates or even create an entirely new template. If you choose to create a customized template, you do it manually by creating it in an .xml file.

**Step 1:** In the Prime LMS portal, navigate to **Configuration > Template Center**. The Deploy screen appears.

**Step 2:** Choose the template that you would like to deploy, and then click **Next**. You can sort how the templates are displayed by clicking the column titles.

Choo	ose	Templates				
Selec	t te	mplates to deploy configuration				
Ter	npla	ite Selector			Selected 1	Total 55 🛞
			Show	All		- 76
		Template Name	-	Features	Туре	Role In
	۶	3750X 3560X Infrastructure Connectivity to Distribution Switch		SBA	Partial	Acces 4
	۲	3750X 3560X Infrastructure Connectivity to WAN Router		SBA	Partial	Acces
	۲	Access Switch Global Configuration		SBA	Partial	Acces
	۲	Cat 2960S Infrastructure Configuration to Distribution Switches		SBA	Partial	Acces
	۲	Cat6500 Connectivity to WAN Routers and LAN Core		SBA	Partial	Distril
	۲	Cat6500 Distribution Layer Connectivity to Access Layer		SBA	Partial	Distril
	۲	Catalyst 2960-S and 3750-X Platform Configuration		SBA	Partial	Acces
	۶	Catalyst 3560-X Platform Configuration		SBA	Partial	Acces
	۲	Catalyst 3750 Distribution Layer Connectivity to Access		SBA	Partial	Distril
	۲	Catalyst 3750 and 3750X Platform Configuration		SBA	Partial	Distril
	۲	Catalyst 3750G Distribution Layer Switch Global Configuration		SBA	Partial	Distril
	۲	Catalyst 4500 Access Switch Global Configuration		SBA	Partial	Acces .
•		III				F.

**Step 3:** In Device Selector, choose the devices to which you want to push these templates, and then click **Next**.



**Step 4:** In the list, choose to which device in the network you want to apply the configuration.

tho	iose Templates							
cho	iose Device Groups							
Cor	ifigure 3750X 35	60X Infrastructure Connectivity	y to Distribution Switch					
		dirite the side	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1					
Inf	rastructure Con	nectivity Configuration to Distri	ibution Switches					
	rustructure com	incentively consignation to blat						
Unk	que Device Level P	arameters						
	Edit 👔 Import							
ŕ	Device	Channel Group Number	Interface Type	Start Interface Number	End Interface Number	Voice Vlan	Data Vlan	Managemen
۲	10.5.0.2							
0	10.5.148.5							
0	10.5.168.2							
	10.5.180.5							
C	10.5.196.5							
	10.5.52.5							
0	10.5.68.5							
C	10.5.7.2							=
	10.5.7.3							
Ö	A3750X- PR1.cisco.local							
0	D3750X.disco.loc	al						
C	IE-D3750X.cisco.	loc						
Ċ	WAN-D3750X.cis	:co.						*
	4			111				

A page appears that requires you to provide the variables for the commands for that particular template. In this example, LAN Switch Universal Template displays the required variables.

Step 5: Fill in the required variables, and then click Save and Edit Next.

s X
▼
Save and Edit Next Cancel

**Step 6:** The Ad Hoc Configuration Commands for Selected Devices page lets you enter configuration commands that will be deployed on the selected devices in addition to the commands in the template.

Deploy	
Choose Templates	A
Choose Device Groups	×
Configure 3750X 3560X Infrastructure Connectivity to Distribution Switch	×
Adhoc Configuration Commands for Selected Devices	
Tou can enter configuration commands here that will be deployed on the selected devices in addition to the commands in the template. The commands that you enter here will not be validated.	Revise Next Freih Canal
Schedule Deployment	

**Step 7:** Enter the desired deployment frequency and date(s), a Job Description, and then click **Finish**. This deploys the template on the selected device based on the scheduled settings. If you choose the email option, Prime LMS sends a confirmation email to the specified administrator.

Deploy		
Choose Templates		4
Choose Device Groups		✓
Configure 3750X 3560X Infrastructure Connectivity to Distribu	ion Switch	V
Adhoc Configuration Commands for Selected Devices		V
Schedule Deployment		
Scheduler Immediate Orac Daily Daily Veesty Orac Sobol Options Config to Struce Oracle Struce Config to Struce Oracle Struce Ora	Job Description*         Deploy Configuration           E-mail	* Indicates required field
Login Username		
Login Password		
Enable Password		
		Preview QL Previous Next Finish Cancel

# Appendix A: Product List

# **Network Management**

Functional Area	Product Description	Part Numbers	Software
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	4.2
	Prime Infrastructure 1.1 Software – 5K Device Base License	R-PI-1.1-5K-K9	
	Prime Infrastructure 1.1 Software – 2.5K Device Base License	R-PI-1.1-2.5K-K9	
	Prime Infrastructure 1.1 Software – 1K Device Base License	R-PI-1.1-1K-K9	
	Prime Infrastructure 1.1 Software – 500 Device Base License	R-PI-1.1-500-K9	
	Prime Infrastructure 1.1 Software – 100 Device Base License	R-PI-1.1-100-K9	
	Prime Infrastructure 1.1 Software – 50 Device Base License	R-PI-1.1-50-K9	

# Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We changed the Cisco Prime LMS Deployment Guide to include a consolidated deployment guide, for 250 to 10,000 connected users.
- We changed the authentication method from either Cisco TACACS+ or Active Directory to using only Cisco TACACS+.



#### Feedback

Click here to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITH-OUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS ON ON TO CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

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

© 2012 Cisco Systems, Inc. All rights reserved.



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.

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