QUICK START GUIDE

Cisco Prime Assurance Manager 1.1

Quick Start Guide

Revised: 5 July, 2012, OL-26374-01

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO PRIME ASSURANCE

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the End User License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the End User License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software.

ADDITIONAL LICENSE RESTRICTIONS:

- Installation and Use. The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use the following Software components:
  - Cisco Prime Assurance Manager: May be installed on a server in Customer's network management environment.

  For each Software license granted, customers may install and run the Software on a single server to manage the number of network devices and codecs specified in the license file provided with the Software, or as specified in the Software License Claim Certificate. Customers whose requirements exceed the network device and codec limits must purchase upgrade licenses or additional copies of the Software. The network device and codec limits are enforced by license registration.
- Reproduction and Distribution. Customers may not reproduce nor distribute the Software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Please refer to the Cisco Systems, Inc. End User License Agreement.

1 About This Guide

This guide explains how to install Cisco Prime Assurance Manager 1.1 (or Prime AM 1.1).

This guide is targeted to administrators who configure, monitor, and maintain Cisco Prime Assurance Manager, and troubleshoot problems that may occur. These administrators must be conversant with VMware OVA applications, and to be familiar with virtualization concepts and virtualized environments.

For detailed information about configuring and managing this product, see the *Cisco Prime Assurance Manager 1.1 User Guide*.

2 Product Overview

Cisco Prime Assurance Manager is a web-based user application for application-aware network service assurance and performance management. It comprises two types of components:

- Data collectors—Collect performance and performance-oriented fault data from devices in the network using protocols and mechanisms such as Cisco NAM, NetFlow, SNMP polling, traps, syslogs, etc. Collected data is aggregated and thresholds are compared against it.
- Cisco Prime Assurance Manager server—With the collected data, Prime AM provides the following functionality to end users:
  - Centralized performance monitoring—Prime AM provides dashboards and reports to view performance data at varying levels of granularity and aggregation, both spatial and time-based.
  - Service Assurance—Prime AM identifies running applications and network services automatically, correlating these services with performance and fault data.
  - Troubleshooting—Performance events can trigger packet capture and decoding that can be used to troubleshoot network performance problems and faults.
  - Traffic Analysis—Data collection from different sources can be used to analyze traffic for the purposes of capacity planning and optimization.

3 Key Features

The following table details the key features of Cisco Prime Assurance Manager.

Table 1 Cisco Prime Assurance Manager Key Features

Feature	Function	Benefit
Performance Monitoring	Centralized performance monitoring for voice, video, and TCP-based applications	Gain visibility into the end-user experience, manage business-critical applications in compliance with service level objectives.
Traffic Analysis	Traffic analysis data collection, on-screen indicators, and reports for WAN optimization and data flow analysis.	Improve application performance by identifying WAN optimization opportunities, detecting abnormal traffic behavior, analyzing network resource usage and throughput, including historical trending
Performance Diagnostics	Problem scoping and isolation	Drill-downs into granular performance data for real-time visibility and troubleshooting
Multi-NAM Management	Automated NAM discovery, central packet capture management, central reporting from multiple NAMs, centralized application classification to ensure consistency across NAMs, central provisioning of WAAS server lists for WAN optimization visibility, contextual cross-launch into NAM UI for more granular analysis, centralized thresholding.	Quickly and easily leverage the power of multiple NAM devices to deliver consistent application experiences across global networks.
Centralized Reporting	Out-of-the-box, flexible, customer-generated, scheduled, exportable, executive-facing reports	Improve productivity and communication using pre-packaged and custom sets of views of performance data
Centralized Performance Data Collection	Performance data access to internal and external management applications, abstract collection management	Allow customers easy access to Cisco embedded intelligent instrumentation and probes, by leveraging the automation of discovery, configuration, collection, and maintenance
Usability	Provides out-of-the-box “zero touch” monitoring using the current NAM, NetFlow, SNMP and other data reported by your network devices.	Leverage discovery and automation to provide meaningful reporting with little to no configuration

For detailed information about Prime AM features, see the *Cisco Prime Assurance Manager 1.1 User Guide*.

4 About Cisco Prime Assurance Manager Licensing

Cisco Prime Assurance Manager is licensed based on the number of managed network interfaces. To use Prime AM, you must have one of the following licenses:

- Evaluation license—Valid for 60 days and 100 interfaces. You can obtain an evaluation license at https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?DemoKeys=Y
- Base license—Purchased base licenses are available in sizes of 50, 100, 500, 1000, or 5000 interfaces. You must purchase a single base interface count to use Prime AM unless you are purchasing Prime AM as an add-on to an existing NCS (WAN) installation. If you already have NCS (WAN) installed with a base license, you need only purchase add-on licenses to use Prime AM. You can obtain a base license at http://www.cisco.com/go/licensing using the Product Authorization Key (PAK) provided as part of your order and the Virtual Unique Device Identifier (VUDI) obtained from your installed instance of Prime AM.
- Add-On licenses—Purchased add-on licenses are available in sizes of 50, 100, 500, 1000, or 5000 interfaces. You can purchase add-on licenses as your interface count increases. Add-on licenses are available at http://www.cisco.com/go/licensing using your PAK and VUDI.

Prime AM license files are node-locked to the virtual machine based on the Virtual Unique Device Identifier (VUDI), which consists of the product identification and a uniquely generated serial number. You can view this information in the Prime AM web interface by choosing **Administration > Licenses**.

For more information about ordering Prime AM licenses, refer to the license information at http://www.cisco.com/go/primeassurance.

5 Pre-Installation Tasks

Meet the requirements and complete the tasks in the following sections before installing Cisco Prime Assurance Manager.

System Requirements

VMware ESX or ESXi Server 4.1.x (or later) software is required on the server.

Table 2 lists the minimum server requirements for each of the Cisco Prime AM OVA options. In this table, "Flow Records" includes NetFlows and flow records generated by NAM polling.

Table 2 Minimum Server Requirements for Deploying Virtual Appliances

OVA Size	Maximum Flow Records	Maximum NAMs	Minimum Requirements
Small	<1,000 records per second	10 (with polling enabled for 5)	RAM—8 GB Disk Space—200 GB Processors—4 virtual CPUs at 2.93 GHz or faster
Large	<15,000 records per second	80 (with polling enabled for 25)	RAM—16 GB Disk Space—400 GB Processors—8 virtual CPUs at 2.93 GHz or faster
Extra Large	<80,000 records per second	400 (with polling enabled for 40)	RAM—24 GB Disk Space—1.2 TB Processors—8 virtual CPUs at 2.93 GHz or faster

Web Client Requirements

Hardware—A Mac or Windows laptop or desktop compatible with one of the supported browsers:

- Internet Explorer 8.0 with the Flash and Chrome plug-ins
- Mozilla Firefox 7.0

Display Resolution —We recommend that you set the screen resolution to 1024 x 768 or higher.

Adobe Flash Player—Adobe Flash Player version 10.x or later must be installed on the web client for Cisco Prime Assurance Manager features to work properly. We recommend that you download and install it from the Adobe website.

Ports Used

Table 3 lists the ports that Cisco Prime Assurance Manager uses. These ports must be open before installation.

Table 3 Ports Used

Port	Protocol	Direction	Usage
7	ICMP	Server to endpoints.	Endpoint discovery.
22	TCP	Server to endpoints.	To initiate SSH connection to endpoints during troubleshooting processes.
		Client to server.	To connect to the Cisco Prime Assurance Manager server.
25	TCP	Server to SMTP server	SMTP
53	TCP	Server to DNS server	DNS
161	UDP	Server to network devices.	SNMP MIB polling
162	UDP	Endpoints to server.	Trap receiver port.
443	TCP	Server to interfaces.	HTTPS connectivity to interfaces during troubleshooting.
8080	TCP	Client to server	Browser access to Cisco Prime Assurance Manager server (via HTTP).
8443	TCP	Server to call processors	HTTPS connectivity for RTMT and Cisco Unified CM registration.
		Client to server.	Secure browser access to the Cisco Prime Assurance Manager server (via HTTPS).
9991	UDP	Network devices to server	NetFlow data receiver
20514	UDP	Endpoints to server.	Syslog receiver

Supported Data Sources

To monitor your network interfaces and services, Prime AM needs to collect data from them using the exported data sources shown in Table 4. For each source, the table shows the devices that support this form of export, and the minimum version of IOS or other software that must be running on the device in order to export the data.

Use this table to verify that your network devices and their software are compatible with the type of data sources Prime AM uses. If needed, upgrade your hardware or software. Note that each software version given is a *minimum*. Your devices can run any later version of the same software or IOS release train.

You may also need to make changes to ensure that Prime AM can collect this data, as explained in “Configuring Data Sources”.

Table 4 Prime AM Supported Data Sources, Devices and Software Version

Device Data Sources	Supported Devices	Minimum Software Version
Medianet NetFlow	Cisco Catalyst 3750 Series Switches, Cisco Catalyst 3560 Series Switch	IOS 12.2(58)SE
	Cisco Catalyst 6500 and Catalyst 6500-E Series Switches	IOS 15.0(1)SY
	Cisco 880, 890, 1900, 2900 and 3900 Series Integrated Services Routers	IOS 15.1(3)T

Table 4 Prime AM Supported Data Sources, Devices and Software Version (continued) (continued)

Device Data Sources	Supported Devices	Minimum Software Version
NetFlow (NF) and Flexible NetFlow (FNF)	Nearly all Cisco devices	IOS 11.1 (for NF only) or IOS 12.2(31)SB2 (for FNF)
Network Analysis Module (NAM)	Any NAM-compatible product, including the Cisco Catalyst 6500 Series Network Analysis Module (NAM-1/NAM-2/NAM-3), Cisco 7600 Series Network Analysis Module (NAM-1/NAM-2/NAM-3) Cisco NAM 2200 Series Appliances, Cisco Network Analysis Module Software, Cisco Prime NAM for ISR G2 SRE, Cisco Prime NAM for Nexus 1010, and the Cisco Prime NAM for WAAS Virtual Blade (VB).	Cisco Prime Network Analysis Module Software 5.1 (2-patch4)
Performance Agent (PA)	Cisco 880, 890, 1900, 2900, and 3900 Integrated Services Routers (PA is not supported on "E" models and 3925)	IOS 15.1(4)M
Simple Network Management Protocol (SNMP)	All	N/A

Configuring Data Sources

Before installing, you should enable your supported devices to provide Prime AM with fault, application and performance data, and ensure that time and date information are consistent across your network. The following topics provide guidelines on how to do this.

Enabling Medianet NetFlow

To ensure that Cisco Prime Assurance Manager can make use of Medianet data, your network devices must:

- Enable Medianet NetFlow data export for the basic set of statistics supported in Cisco Prime Assurance Manager.
- Export the Medianet NetfFlow data to the Cisco Prime Assurance Manager server and port.

Use a configuration like the example below to ensure that Cisco Prime Assurance Manager gets the Medianet data it needs:

```
flow record type performance-monitor PerfMonRecord
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match transport rtp ssrc
  collect application media bytes counter
  collect application media bytes rate
  collect application media packets counter
  collect application media packets rate
  collect application media event
  collect interface input
  collect interface output
  collect counter bytes
  collect counter packets
  collect routing forwarding-status
  collect transport packets expected counter
  collect transport packets lost counter
  collect transport packets lost rate
  collect transport round-trip-time
  collect transport event packet-loss counter
  collect transport rtp jitter mean
  collect transport rtp jitter minimum
  collect transport rtp jitter maximum
  collect timestamp interval
```

```
  collect ipv4 dscp
  collect ipv4 ttl
  collect ipv4 source mask
  collect ipv4 destination mask
  collect monitor event
flow monitor type performance-monitor PerfMon
  record PerfMonRecord
  exporter PerfMonExporter
flow exporter PerfMonExporter
  destination PAMIP
  source Loopback0
  transport udp PAMPort
policy-map type performance-monitor PerfMonPolicy
  class class-default
! Enter flow monitor configuration mode.
  flow monitor PerfMon
! Enter RTP monitor metric configuration mode.
  monitor metric rtp
!Specifies the minimum number of sequental packets required to identify a stream as being an RTP flow.
  min-sequential 2
! Specifies the maximum number of dropouts allowed when sampling RTP video-monitoring metrics.
  max-dropout 2
! Specifies the maximum number of reorders allowed when sampling RTP video-monitoring metrics.
  max-reorder 4
! Enter IP-CBR monitor metric configuration mode
  monitor metric ip-cbr
! Rate for monitoring the metrics (1 packet per sec)
  rate layer3 packet 1
interface interfacename
  service-policy type performance-monitor input PerfMonPolicy
  service-policy type performance-monitor output PerfMonPolicy
```

In this example configuration:

- *PAMIP* is the IP address of the Prime AM server.
- *PAMPort* is the UDP port on which the Prime AMserver is listening for Medianet data (the default is 9991).
- *interfaceName* is the name of the interface (such as “GigabitEthernet0/0” or “fastethernet 0/1”) sending Medianet NetFlow data to the specified *PAMIP*,

For more information on Medianet configuration, see the *Medianet Reference Guide*.

Enabling NetFlow and Flexible NetFlow

To ensure that Prime AM can make use of NetFlow data, your network devices must:

- Have NetFlow enabled on the interfaces you want to monitor.
- Export the NetFlow data to the Prime AM server and port.

Use the commands below to enable NetFlow on Cisco IOS devices:

```
interface interfaceName
ip route-cache flow
```

where *interfaceName* is the name of the interface (such as “fastethernet” or “fastethernet0/1”) on which you want to enable NetFlow,

Note that you must enable NetFlow on each *physical* interface for which you want Prime AM to collect data. These will normally be Ethernet or WAN interfaces. This applies to physical interfaces only. You do not need to enable NetFlow on VLANs and Tunnels, as they are included automatically whenever you enable NetFlow on a physical interface.

Use the following commands to see NetFlow working on the device:

```
show ip flow export
show ip cache flow
show ip cache verbose flow
```

Once NetFlow is enabled, you can configure the device to export NetFlow data to Prime AM using these IOS configuration-mode commands:

```
ip flow-export version 5
ip flow-export destination PAMIP PAMPort
ip flow-export source interfaceName
```

where:

- *PAMIP* is the IP address of the Prime AM server
- *PAMPort* is the UDP port on which the Prime AM server is listening for NetFlow data (the default is 9991)
- *interfaceName* is the name of the interface sending NetFlow data to the specified *PAMIP*. This will cause the source interface's IP address to be sent to Cisco Prime Assurance Manager as part of NetFlow export datagrams.

For more information on NetFlow configuration, see:

- *Cisco IOS Switching Services Configuration Guide, Release 12.1*
- *Flexible NetFlow Configuration Guide, Cisco IOS Release 15.1M&T*
- *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*
- *Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting*

Deploying Network Analysis Modules (NAMs)

Ensure that your NAMs are placed appropriately in the network. For more information, see:

- *Cisco Network Analysis Module Software 5.1 User Guide*—Includes deployment scenarios and covers a variety of topics, including deploying NAMs in the branch, and deploying NAMs for WAN optimization.
- *Cisco Network Analysis Module Deployment Guide*—See the topic "Places in the Network Where NAMs Are Deployed".

If your NAMs are deployed properly, then no other pre-installation work is required. When you conduct discovery using Cisco Prime AM, you will need to enter HTTP access credentials for each of your NAMs.

Note Prime AM uses a more efficient REST interface to query NAMs. For this reason, it does not support the direct export of NetFlow data from NAMs. Any device exporting NetFlow data must export that NetFlow data directly to Prime AM, not via a NAM. Exporting NetFlow data from any NAM to Cisco Prime Assurance Manager will result in data duplication.

Enabling Performance Agent

To ensure that Prime AM can collect application performance data, use the IOS *mace* (for Measurement, Aggregation and Correlation Engine) keyword to configure Performance Agent (PA) data flow sources on your branch-office and data center routers.

For example, use the following commands in IOS global configuration mode to configure a PA flow exporter on a router:

```
flow exporter mace-export
destination 172.30.104.128
transport udp 9991
```

Use commands like the following to configure flow records for applications with flows across the router:

```
flow record type mace mace-record
collect application name
collect art all
```

where *application name* is the name of the application whose flow data you want to collect.

To configure the PA flow monitor type:

```
flow monitor type mace mace-monitor
record mace-record
exporter mace-export
```

To collect traffic of interest, use commands like the following:

```
access-list 100 permit tcp any host 10.0.0.1 eq 80
class-map match-any mace-traffic
match access-group 100
```

To configure a PA policy map and forward the PA traffic to the correct monitor:

```
policy-map type mace mace_global
class mace-traffic
flow monitor mace-monitor
!
```

Finally, enable PA on the WAN interface:

```
interface Serial0/0/0
mace enable
```

For more information on configuring Performance Agent, see the *Cisco Performance Agent Deployment Guide*.

Configuring SNMP

To ensure that Cisco Prime Assurance Manager can query SNMP devices and receive traps and notifications from them, you must:

- Set SNMP credentials (community strings) on each device you want to manage using Cisco Prime Assurance Manager.
- Configure these same devices to send SNMP notifications to the Cisco Prime Assurance Manager server.

Use the following IOS configuration commands to set read/write and read-only community strings on an SNMP device:

```
snmp-server community private RW
snmp-server community public RO
```

where *private* and *public* are the community strings you want to set.

Once you have set the community strings, you can specify that device notifications should be sent as traps to the Cisco Prime Assurance Manager server, using the following IOS global configuration command on each SNMP device:

```
snmp-server host PAMHost traps version community notification-type
```

where:

- *PAMHost* is the IP address of the Cisco Prime Assurance Manager server.
- *version* is the version of SNMP that is used to send the traps.
- *community* is the community string sent to the server with the notification operation.
- *notification-type* is the type of trap to send. You may need to control bandwidth usage and the amount of trap information being sent to Cisco Prime Assurance Manager server using this parameter.

You may need to control bandwidth usage and the amount of trap information being sent to Cisco Prime Assurance Manager server using additional commands.

Note that the kind of SNMP information you can make use of in Prime AM depends on the MIBs installed on your devices. For example, if you want Prime AM to monitor the environmentTemperature variable on a device or group of devices, you must ensure that CISCO-ENVMON-MIB AND CISCO-ENTITY-SENSOR-MIB are installed on these devices.

For more information on configuring SNMP, see the snmp-server community and snmp-server host sections of the *Cisco IOS Network Management Command Reference*. Also see the "Configuring SNMP Notifications" section of the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*, and the list of notification-type values.

Configuring NTP

Network Time Protocol synchronization must be configured on all devices and NAMs in your network, as well as on the Prime AM server. You are given a chance to specify the NTP server when you deploy the Prime AM OVA. You can also change the NTP server later, in the installed product, by selecting. Coordinating time stamps on your NAMs and other devices is a matter for your organization's network designers. Failure to organize time synchronization across your network can result in anomalous results in Prime AM.

6 Installing Cisco Prime Assurance Manager

Before You Begin

Complete the preparation requirements described in Pre-Installation Tasks, page 4.

Before installing Cisco Prime Assurance Manager in a virtual host, you must also ensure that:

- VMware ESX or ESXi is installed and configured on the machine you plan to use as the Cisco Prime Assurance Manager server host. See the VMware documentation for information on setting up and configuring the host machine.
- The installed VMware ESX or ESXi host is reachable over the network.
- The VMware vSphere Client is installed on the same host. After the virtual host is available on the network, you can browse to its IP address to display a web-based interface from which you can install the VMware vSphere Client.

  Note The VMware vSphere Client is Windows-based. You must download and install the client from a Windows PC.

  After you install the VMware vSphere Client, you can run it and log into the virtual host, using the host name or IP address of the virtual host, the root login ID, and the password you configured. You can add the host to a vCenter if you want to manage it through vCenter. See the VMware vSphere documentation for details.
- The Prime AM OVA is saved to the same machine where your vSphere Client is installed. Depending on your arrangement with Cisco, you may download the OVA file from Cisco.com or take it from your Cisco-supplied installation media.

Deploying the OVA

Make sure that all of the system requirements are met before you deploy the OVA. Please review the sections System Requirements, page 4, and Before You Begin, page 10.

Step 1 Launch your VMware vSphere client.

Step 2 Choose **File > Deploy OVF Template**.

The Deploy OVF Template window appears.

Step 3 Click the **Deploy from file** radio button.

Step 4 Click **Browse** to access the location where you have saved the OVA file.

Step 5 Click **Next**.

The OVF template details are displayed in the OVF Template Details window.

Step 6 Verify the details about the OVA file, including the product name, version, and the size, then click **Next**.

The Name and Location window appears.

Step 7 Specify a name and location for the template that you are deploying. The name must be unique within the inventory folder, and can contain up to 80 characters.

Step 8 Click **Next**.

The Ready to Complete window appears. It displays the details of the OVA file, the name of the virtual appliance, size, host, and storage details.

Step 9 After you verify the options, click **Finish** to start the deployment.

This may take a few minutes to complete. Check the progress bar in the Deploying Virtual Application window to monitor the task status.

After the deployment task has successfully completed, a confirmation window appears.

Step 10 Click **Close**.

The virtual appliance that you deployed is listed under the host, in the left pane of the vSphere client.

Installing the Server

After you deploy the Cisco Prime Assurance Manager OVA, you must configure the virtual application in order to install and start Cisco Prime AM.

Step 1 In the VMware vSphere client, right-click the deployed virtual appliance and choose **Power > Power On**.

Step 2 Click the **Console** tab. At the localhost login prompt, enter **setup**.

Step 3 The console prompts you for the following parameters:

- IP Address—The IP address of the virtual appliance.
- IP default netmask—The default subnet mask for the IP address.
- IP default gateway—The IP address of the default gateway.
- Default DNS domain—The default Domain Name.
- Primary nameserver—The primary name server. You may add or edit this nameserver. To configure multiple name servers or NTP servers, enter **y**.
- Primary NTP server. The default is time.nist.gov.
- Username—The name of the first administrative user. You can accept the default, which is admin.
- Password—Enter your password and confirm it. The default is **admin**. We recommend that you note down the password you enter, as the password cannot be retrieved or reset.

Step 4 When you are done entering these values, the vSphere Client tests the network configuration parameters you entered. If the tests are successful, it begins installing Cisco Prime Assurance Manager. When the installation is complete, the virtual appliance reboots and the system is initialized. When initialization is complete, the system displays a login prompt (please be patient; there will be little or no console activity during initialization).

Step 5 Log in to the virtual appliance using the administrative username and password you specified.

Logging in to Cisco Prime Assurance Manager

Follow these steps to log into the Cisco Prime Assurance Manager user interface through a web browser:

Step 1 Launch one of the Supported Browsers (see System Requirements, page 4) on a different computer from the one on which you installed and started Prime AM.

Step 2 In the browser's address line, enter **https://***IPaddress*, where *IPaddress* is the IP address of the server on which you installed Prime AM. The Prime AM user interface displays the Login window.

Note When you access Cisco Prime Assurance Manager for the first time, some browsers will display a warning that the site is untrusted. If this happens, follow the prompts to add a security exception and download the self-signed certificate from the server. After you complete this procedure, the browser will accept the server as a trusted site in all future login attempts.

Step 3 Enter the default administrator username and password, which are *root* and *Public123*, respectively.

If any licensing problems occur when you first login, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted to any expired licenses. You have the option to go directly to the **Administration > Licenses** page to address these problems.

Step 4 Click **Login** to log into Cisco Prime Assurance Manager. The Prime AM home page appears.

To ensure system security, select **Administration > Users, Roles & AAA > Change Password** to change the password for the *root* administrator.

To exit the user interface, close the browser page or click **Logout** under your username in the upper right corner of the page. Exiting a user interface session does not shut down Prime AM on the server.

If a system administrator stops the Prime AM server during your session, your session ends and the browser displays this message: "The page cannot be displayed." Your session does not reassociate when the server restarts; you must exit the session and start a new session.

7 Getting Started

After you install Cisco Prime Assurance Manager, you must perform additional tasks to begin managing your network. These tasks are all listed in the Getting Started section of the *Cisco Prime Assurance Manager 1.1 User Guide*. After you complete these tasks, you are ready to monitor end-to-end application performance, troubleshoot problems, optimize WAN performance, and assure consistent network service delivery.

8 Navigation and Documentation Reference

This section provides information about navigational paths to access Prime AM features, and the details of the sections where the features are covered in Prime AM documentation.

Table 5 Navigation and Documentation Reference

Task	Navigation in Cisco Prime Assurance Manager	Section in Cisco Prime Assurance Manager User Guide
Discovering your network	**Operate > Discovery**	Setting Up
Setting up site profiles	Operate > Site Profiles & Maps Operate > Device Workcenter	
Setting up port monitoring	**Operate > Port Grouping**	
Setting up virtual domains	Administration > Virtual Domains	

Table 5 Navigation and Documentation Reference (continued)

Task	Navigation in Cisco Prime Assurance Manager	Section in Cisco Prime Assurance Manager User Guide
Using monitoring dashboards	**Operate > Monitoring Dashboards**	Operating the Network
Using templates for configuring and monitoring	**Design > Templates**	
Viewing alarms	**Operate > Alarms & Events**	Monitoring Alarms
Finding and comparing device configurations	**Operate > Configuration Archive**	Working with Device Configurations
Maintaining device configurations	**Operate > Configuration Archive**	Maintaining Device Configuration Inventory
Managing Users	**Administration > Users, Roles & AAA**	Controlling User Access

9 Uninstalling Cisco Prime Assurance Manager

To uninstall Cisco Prime Assurance Manager, including the data collector on the local server:

Step 1 Right-click the Cisco Prime Assurance Manager virtual appliance.

Step 2 Choose **Remove from Disk**.

10 Related Documentation

You can access the following additional Cisco Prime Assurance Manager guides on the Cisco Prime Assurance Manager page on Cisco.com:

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

- *Cisco Prime Assurance Manager 1.1 Quick Start Guide* (this document)
- *Cisco Prime Assurance Manager 1.1 User Guide*
- *Open Source Used in Cisco Prime Assurance Manager 1.1*
- *Cisco Prime Assurance 1.1 Release Notes*

11 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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**.

Printed in the USA on recycled paper containing 10% postconsumer waste.

OL-26374-01