Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide, Release 1.4.x

First Published: 2015-12-15

Last Modified: 2017-02-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE 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 LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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: http://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)

CONTENTS

Preface

CHAPTER 1

CHAPTER 2

Preface

Audience

This publication is intended for experienced network administrators who will configure and maintain the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM). This guide is part of a documentation set that is designed to help you install, troubleshoot, and upgrade your Cisco APIC-EM. For a complete list of the Cisco APIC-EM documentation set, see Related Documentation, on page ix.

Note In this guide, the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to as the controller.

Document Conventions

This documentation uses the following conventions:

Convention	Description
^ or **Ctrl**	The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive.

Convention	Description
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.

Convention	Description
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS XE software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Related Documentation

This section lists the Cisco APIC-EM and related documents available on Cisco.com at the following url:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

- Cisco APIC-EM Documentation:
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Supported Platforms*
    - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
    - *Open Source Used In Cisco APIC-EM*
- Cisco Network Visibility Application for the Cisco APIC-EM
    - *Cisco Network Visibility Application for APIC-EM Release Notes*
    - *Cisco Network Visibility Application for APIC-EM Supported Platforms*

    - *Cisco Network Visibility Application for APIC-EM User Guide*

- Cisco Path Trace Application for Cisco APIC-EM
    - *Cisco Path Trace Application for APIC-EM Release Notes*
    - *Cisco Path Trace Application for APIC-EM Supported Platforms*
    - *Cisco Path Trace Application for APIC-EM User Guide*
- Cisco EasyQoS Application for Cisco APIC-EM
    - *Cisco Path Trace Application for APIC-EM Release Notes*
    - *Cisco EasyQoS Application for APIC-EM Supported Platforms*
    - *Cisco EasyQoS Application for APIC-EM User Guide*
- Cisco IWAN Documentation for the Cisco APIC-EM:
    - *Release Notes for Cisco IWAN*
    - *Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)*
    - *Configuration Guide for Cisco IWAN on Cisco APIC-EM*
    - *Software Configuration Guide for Cisco IWAN on APIC-EM*
    - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*
- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
    - *Release Notes for Cisco Network Plug and Play*
    - *Solution Guide for Cisco Network Plug and Play*
    - *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
    - *Cisco Open Plug-n-Play Agent Configuration Guide*
    - *Mobile Application User Guide for Cisco Network Plug and Play*

Note For information about developing your own application that interacts with the controller by means of the northbound REST API, see the developer.cisco.com/site/apic-em Web site.

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/c/en/us/td/docs/general/whatsnew/whatsnew.html.

CHAPTER 1

Getting Started

About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's Software Defined Networking (SDN) Controller for Enterprise Networks (Access, Campus, WAN and Wireless).

The platform hosts multiple applications (SDN apps) that use open northbound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.

The Cisco APIC-EM platform supports both wired and wireless enterprise networks across the Campus, Branch and WAN infrastructures. It offers the following benefits:

- Creates an intelligent, open, programmable network with open APIs
- Saves time, resources, and costs through advanced automation
- Transforms business intent policies into a dynamic network configuration
- Provides a single point for network wide automation and control

The following table describes the features and benefits of the Cisco APIC-EM.

Table 1: Cisco APIC Enterprise Module Features and Benefits

Feature	Description
Network Information Database	The Cisco APIC-EM periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network.

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
EasyQoS application	The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration.
Cisco Network Plug and Play (PnP) application	The Cisco Network PnP application is one of the components in the Cisco Network PnP solution. The Cisco Network PnP solution extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points.
Cisco Intelligent WAN (IWAN) application	The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) or sub-CA to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the embedded PKI service for automatic SSL certificate management.
Path Trace application	The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
High Availability (HA)	HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing.
Back Up and Restore	The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI.
Audit Logs	The audit log captures user and network activity for the Cisco APIC-EM applications.

Logging into the Cisco APIC-EM

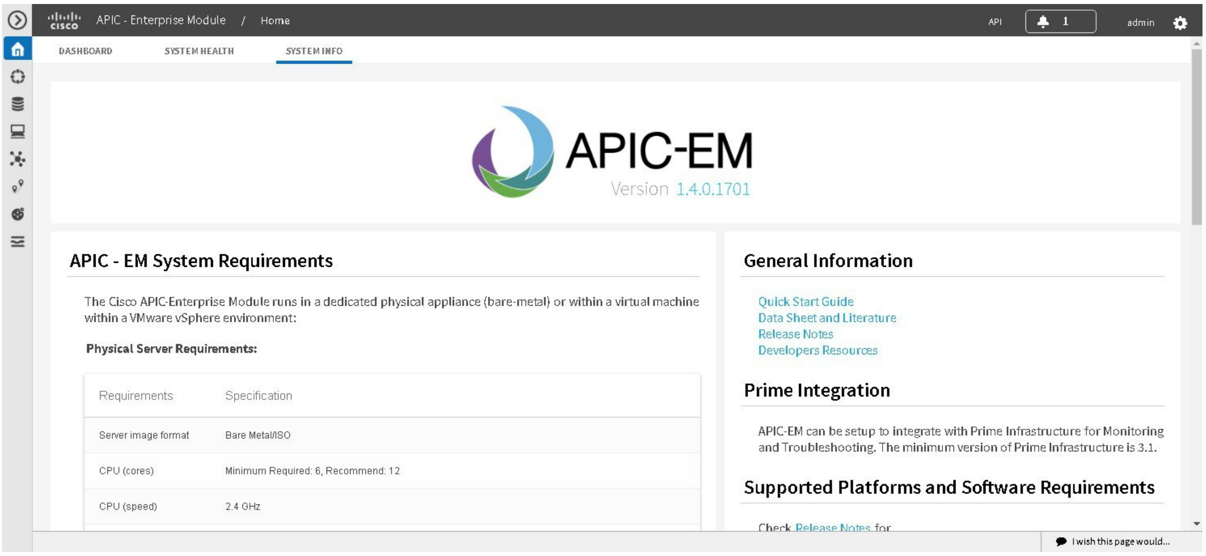
You access the Cisco APIC-EM GUI by entering its network IP address in your browser. The IP address was configured for the Cisco APIC-EM network adapter during the initial setup using the configuration wizard. This IP address connects to the external network.

Step 1 In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:
https://*IP address*

Step 2 On the launch page, enter your username and password that you configured during the deployment procedure.
The **Home** page of the APIC-EM controller appears. The **Home** page consists of the following three tabs:

- **DASHBOARD**
- **SYSTEM HEALTH**
- **SYSTEM INFO**

Figure 1: SYSTEM INFO Tab



APIC - EM System Requirements

The Cisco APIC-Enterprise Module runs in a dedicated physical appliance (bare-metal) or within a virtual machine within a VMware vSphere environment:

Physical Server Requirements:

Requirements	Specification
Server image format	Bare Metal/ISO
CPU (cores)	Minimum Required: 6, Recommend: 12
CPU (speed)	2.4 GHz

General Information

Quick Start Guide
Data Sheet and Literature
Release Notes
Developers Resources

Prime Integration

APIC-EM can be setup to integrate with Prime Infrastructure for Monitoring and Troubleshooting. The minimum version of Prime Infrastructure is 3.1.

Supported Platforms and Software Requirements

Check Release Notes for

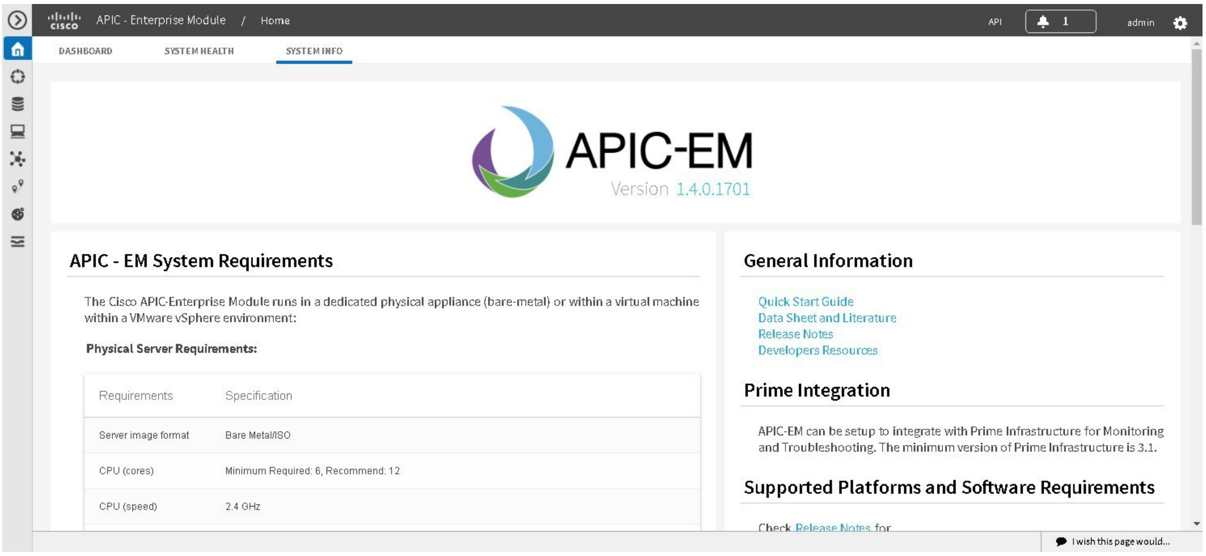
What to Do Next

Click on each tab and review the data provided in the GUI.

Reviewing the SYSTEM INFO Tab

You can use the **SYSTEM INFO** tab to access information at a glance about the controller, its system requirements, supported platforms, and other information. The **SYSTEM INFO** tab is directly accessible from the **Home** page.

Figure 2: SYSTEM INFO Tab



APIC - EM System Requirements

The Cisco APIC-Enterprise Module runs in a dedicated physical appliance (bare-metal) or within a virtual machine within a VMware vSphere environment:

Physical Server Requirements:

Requirements	Specification
Server image format	Bare Metal/ISO
CPU (cores)	Minimum Required: 6, Recommend: 12
CPU (speed)	2.4 GHz

General Information

Quick Start Guide
Data Sheet and Literature
Release Notes
Developers Resources

Prime Integration

APIC-EM can be setup to integrate with Prime Infrastructure for Monitoring and Troubleshooting. The minimum version of Prime Infrastructure is 3.1.

Supported Platforms and Software Requirements

Check Release Notes for

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

All users can access the contents of the **SYSTEM INFO** tab. The **SYSTEM HEALTH** tab access is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All. The **DASHBOARD** tab is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All or ROLE_POLICY_ADMIN privileges and RBAC scope configured to All.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Log into the Cisco APIC-EM **Home** page, as described in the previous procedure.

Step 1 On the **Home** page, click the **SYSTEM INFO** tab to view general information about the controller.
Proceed to perform any or all of the following actions listed in the steps below.

Step 2 Review the information displayed on the GUI page about system requirements.

Step 3 Review the information displayed on the GUI page about supported platforms and software requirements

Step 4 Review the information displayed on the GUI page about Prime Infrastructure support.

Step 5 Click the link to open the **Quick Start Guide**.
The **Quick Start Guide** provides an introduction to the controller and its basic functionality.

What to Do Next

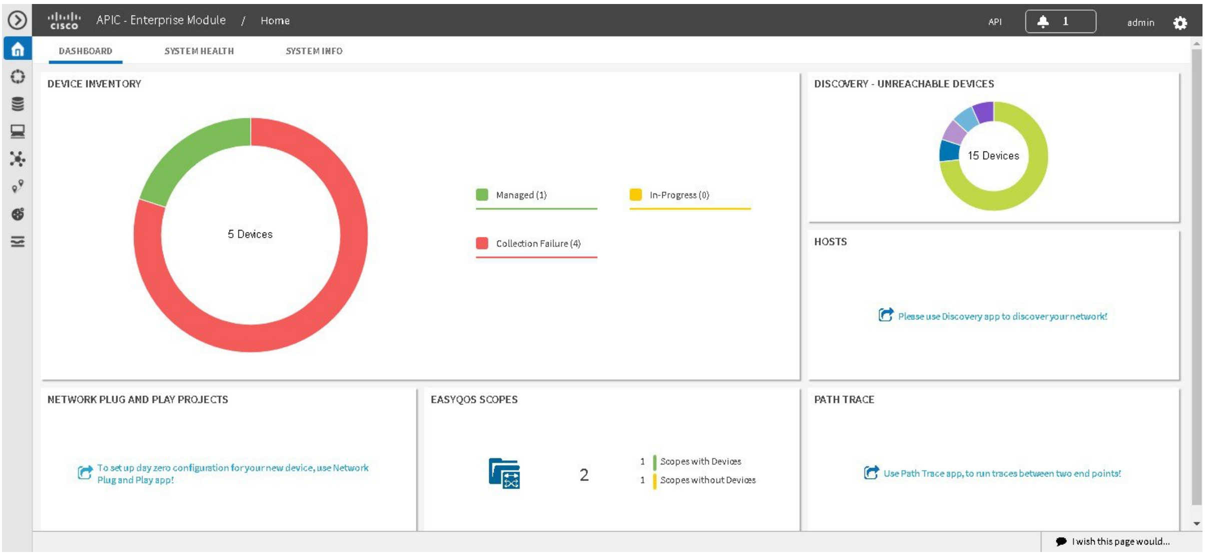
Click the datasheet links or Cisco DevNet links for additional information about the controller and access to Cisco DevNet, respectively.

Click the other tabs to review the controller's dashboard and system health.

Reviewing the DASHBOARD Tab

You can use the **DASHBOARD** tab to quickly view graphical displays of key applications on the controller and their operational status. This information can be used to monitor the controller, the network devices that the controller manages, as well as to assist in troubleshooting any problems. The **DASHBOARD** tab is directly accessible from the **Home** page.

Figure 3: DASHBOARD Tab



Please use Discovery app to discover your network!

To set up day zero configuration for your new device, use Network Plug and Play app!

Use Path Trace app, to run traces between two end points!

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

All users can access the contents of the **SYSTEM INFO** tab. The **SYSTEM HEALTH** tab access is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All. The **DASHBOARD** tab is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All or ROLE_POLICY_ADMIN privileges and RBAC scope configured to All.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Log into the Cisco APIC-EM **Home** page, as described in the previous procedure.

Step 1 On the **Home** page, click the **DASHBOARD** tab to view information about the controller's current activities.
You can view data about the controller's current activities through the dashboard. This data is organized through a set of seven widgets, although only six widgets are displayed at a time.

Note A widget will not appear in the **DASHBOARD** tab if its underlying application has not been installed and enabled.

Unless you have started a discovery and/or a specific controller application, the widgets in the dashboard will be grayed out and inactive. After starting a discovery, data will start to populate and appear in these widgets. Data displayed is updated every few minutes.

Step 2 After performing a successful discovery, review the data displayed in each of the seven widgets.

Device Inventory	Graphical representation of the number of network devices (and percentages of network devices) being actively managed, in progress of being managed, and where there was a failure to connect to and collect device data. Collection failure icons in this widget are clickable and access additional data about the devices where there was a collection failure.
Discovery-Unreachable Devices	Graphical representation of the number of devices reachable and unreachable for a discovery. Clicking the circular icon in this field accesses the **Discovery** window for the specific discovery job.
Branch Sites	Graphical representation of the status of branch sites in your network for the IWAN application. This display includes the following data about branch site status: • Pending • In Progress • Failed • Provisioned **Note** This widget only appears if the IWAN application is installed and enabled.
Hosts	Graphical representation of the hosts in your network. Display includes the number of wired and wireless hosts (and percentages of network hosts as wired or wireless). **Note** This widget only appears if the IWAN application is neither installed or enabled.

Path Trace	Graphical representation of the successful and unsuccessful path traces. Clicking the circular icon in this field accesses the **Path Trace** window.
EasyQoS Scopes	Graphical representation of the policy scopes (EasyQoS) applied to the devices. Displays both number of policies with scopes and without scopes.
PnP Projects	Graphical representation of the status of Plug N Play projects for your network. This display includes the following data about PnP project status: • Provisioned • Pre-Provisioned • In-Progress • Failed Clicking the link in this widget launches the PnP application in the controller.

Each widget in the above table displays data related to an application. If that widget's application is not enabled on the controller, then no data will be visible for that application.

Step 3 Proceed to click within any widget icon to view additional detailed data about its subject matter.
Additionally, by clicking the appropriate link within the widget you can immediately access the underlying application.

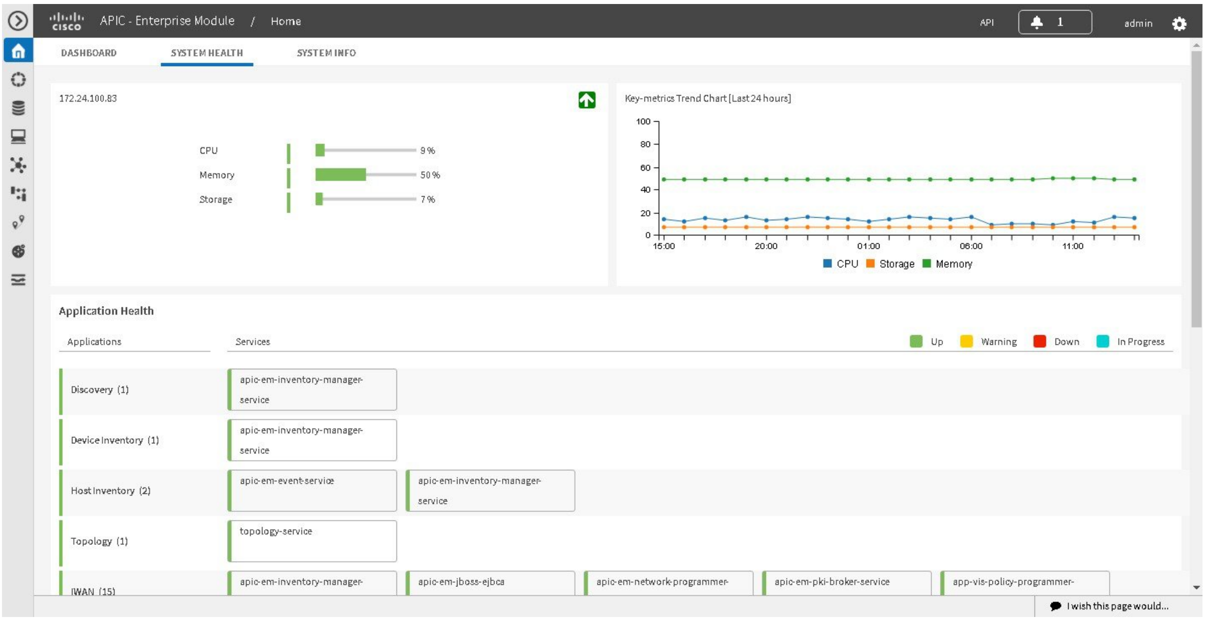
What to Do Next

Click the other tabs to review the controller's system health and system information.

Reviewing the SYSTEM HEALTH Tab

You can use the **SYSTEM HEALTH** tab to quickly view graphical displays of both the basic health of the system and the applications running on the controller. This information can be used to monitor the controller and its applications, as well as to assist in troubleshooting any problems. The **SYSTEM HEALTH** tab is directly accessible from the **Home** page.

Figure 4: SYSTEM HEALTH Tab



Applications	Services				
Discovery (1)	apic-em-inventory-manager-service				
Device Inventory (1)	apic-em-inventory-manager-service				
Host Inventory (2)	apic-em-event-service	apic-em-inventory-manager-service			
Topology (1)	topology-service				
IWAN (15)	apic-em-inventory-manager-	apic-em-jboss-ejbca	apic-em-network-programmer-	apic-em-pki-broker-service	app-vis-policy-programmer-

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

All users can access the contents of the **SYSTEM INFO** tab. The **SYSTEM HEALTH** tab access is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All. The **DASHBOARD** tab is limited to users with ROLE_ADMIN privileges and RBAC scope configured to All or ROLE_POLICY_ADMIN privileges and RBAC scope configured to All.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Log into the Cisco APIC-EM **Home** page, as described in the previous procedure.

Step 1 On the **Home** page, click the **SYSTEM HEALTH** tab to view information about the health of the basic system and the applications running on the controller.
The following information is displayed in the **SYSTEM HEALTH** tab.

System (Host) Health Data	Data displayed include: - Host IP address - CPU—Host CPU usage is displayed in MHZ. Both the currently used and available host CPU is displayed. - Memory—Host memory usage is displayed in GB. Both the currently used and available host memory is displayed. - Storage—Host storage usage is displayed in GB. Both the currently used and available host storage is displayed. **Note** If you have configured a multi-host cluster, then each host's data (CPU, memory, and storage) will be displayed in the UI. Color indicates status for the above host data: - Green—Indicates proper usage and support. - Blue—Indicates usage is approaching improper levels and triggers this warning (color change). - Orange—Indicates a failure based upon the usage exceeding the maximum supported value. Additionally, a graphical representation of the above data over the last 24 hours is displayed in this tab. Moving your cursor or mousing over the graph displays a data summation for specific date and time. **Note** By placing your cursor over (mouse over) a color warning in the window, further information about the warning or failure message appears.

Application Health Data	Displays applications available from the **Navigation** pane, and the services that support each application. For example, the **Topology** application accessible in the GUI is supported by topology-service. Color bars indicate the status for the applications and the supporting service(s): • Green —Indicates that an application instance is starting. An application instance is the aggregation of the service instances. You can configure a minimum or maximum number of service instances, as well as grow and harvest these service instances (spin up or spin down the services). • Yellow—Indicates application instance and its supporting service instance(s) are experiencing issues and triggers this warning (color change). • Red—Indicates a failure of the application instance and its supporting service instance(s). You can harvest a service instance and then regrow it using the GUI. If the service instance does not regrow using the GUI, then you can manually regrow it. When you harvest a service instance, the controller will determine which instance is regrown (load balancing among them). • Blue—Indicates an in-progress state for the application or service instance (growing or harvesting).

Step 2 Place your cursor over a specific service to view additional information about it.
The following additional information is displayed about the service:

- Service name
- Service status (indicated by color code)
- Number of instances of the service currently running
- IP address or addresses of host where service instances are running
- Service version

Step 3 (Optional) Click the green-colored addition icon (+) within the service to grow (start up) an instance of that service for an application.

Caution Growing or harvesting services can be done for troubleshooting a service that is performing erratically. Be sure that you understand the possible effects of growing and harvesting services, because doing so could have unexpected results. For detailed information about growing and harvesting services for troubleshooting purposes, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

Step 4 (Optional) Click the red-colored subtraction icon (-) within the service to harvest (shut down) an instance of the service for an application.

Caution Growing or harvesting services can be done for troubleshooting a service that is performing erratically. Be sure that you understand the possible effects of growing and harvesting the services, because doing so could have unexpected results. For detailed information about growing and harvesting services for troubleshooting purposes, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

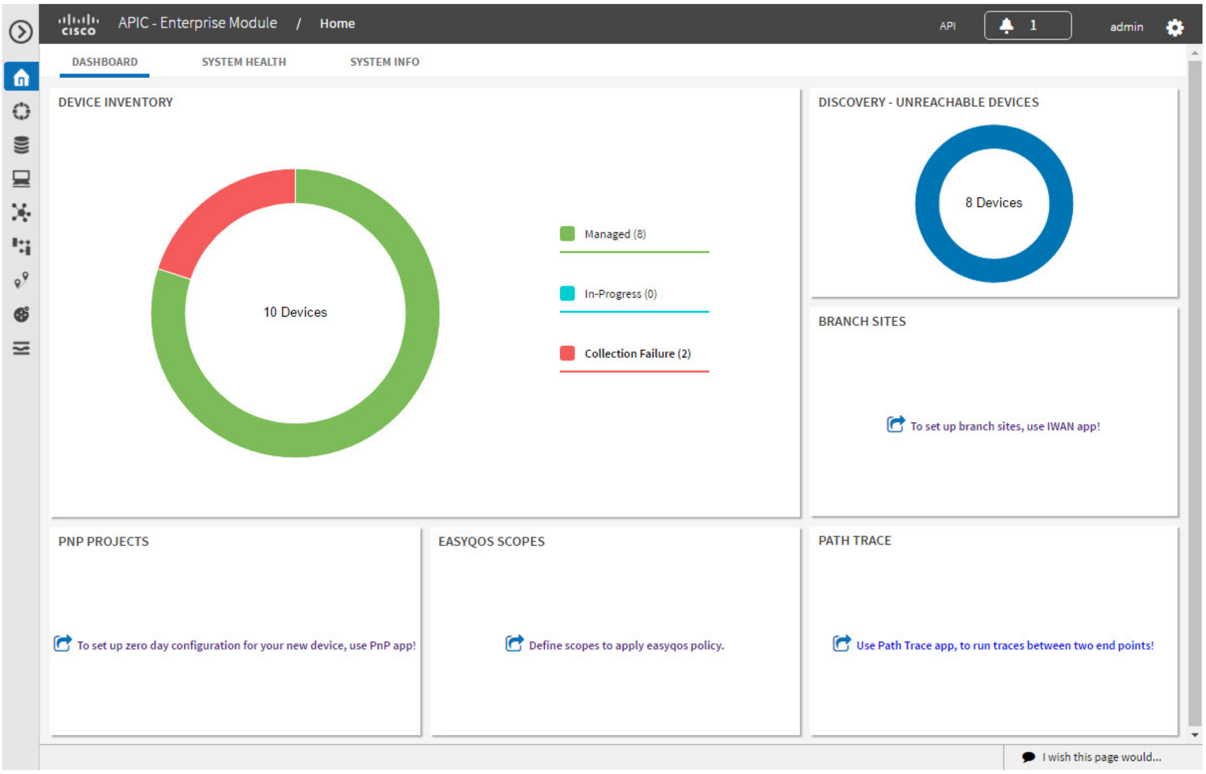
What to Do Next

Click the other tabs to review the controller's dashboard and system information.

Cisco APIC-EM GUI

First GUI Window

When you log into the Cisco APIC-EM, the GUI appears. See the following tables for descriptions of the GUI elements.



To set up branch sites, use IWAN app!

To set up zero day configuration for your new device, use PnP app!

Define scopes to apply easyqos policy.

Use Path Trace app, to run traces between two end points!

Table 2: Cisco APIC-EM GUI Elements

Name	Description
Navigation pane	At the left side of the window, the **Navigation** pane provides access to the Cisco APIC-EM functions and additional applications, such as EasyQoS, Path Trace, IWAN, and Network Plug and Play.
Global toolbar	At the top of the window, the **Global** toolbar provides access to tools, such as API documentation, settings, and notifications. For a full explanation of the icons on the **Global** toolbar, see the Global Toolbar Options table below.
Application or Function Pane	In the main window area, the application or function pane displays the interface of the application or function. When you click an option in the **Navigation** pane or from the **Global** toolbar, the corresponding application or function opens in this pane.
I wish this page would... feedback link	At the bottom of the window, the **I wish this page would...** feedback link opens a preaddressed email in your email application, where you can provide input about your experience using the Cisco APIC-EM and suggestions for improvements.

Navigation Pane Options

The **Navigation** pane provides options to access the major Cisco APIC-EM features and applications.

Table 3: Navigation Pane Options

Icon	Name	Description
ⓥ	**Hide/Unhide Navigation**	Allows you to hide and unhide the **Navigation** pane.
⌂	**Home**	Provides information about the APIC-EM, such as its network status, system health, and system information.
◌	**Discovery**	Allows you to configure discovery options for scanning the devices and hosts in your network.
🛢	**Device Inventory**	Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered devices in your network.
💻	**Host Inventory**	Provides access to the inventory database, where you can display, filter, and sort tabular information about the discovered hosts in your network.

Icon	Name	Description
	Topology	Presents the devices and links that the Cisco APIC-EM discovers as a physical topology map with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
	IWAN	Simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications with preferred paths for hybrid WAN links. Doing so improves the application experience over any connection and saves telecommunication costs by leveraging cheaper WAN links.
	EasyQoS	Enables you to configure quality of service on previously discovered Cisco network devices that support the EasyQoS feature. Using EasyQoS, you can group devices and then define the business relevance of applications that are used in your network. The Cisco APIC-EM takes your QoS selections, translates them into the proper command line interface (CLI) commands, and deploys them onto the selected devices.
	Path Trace	Helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
	Network Plug and Play	Provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points.

Global Toolbar Options

The **Global** toolbar provides access to API information, administrative functions, system notifications.

Table 4: Global Toolbar Options

Icon	Option	Description
API	**API**	Displays the automatically generated documentation for the northbound REST APIs.

Icon	Option	Description
	System Notifications	Opens the **System Notifications** dialog box, which provides information about system notifications that have occurred. The icons at the top provide a total of the number of notifications in each of the following categories: • Minor (yellow triangle icon) • Major (orange triangle icon) • Critical (red octagon icon) If notifications have occurred, they are listed below the icons. For example, any notifications about software updates or security certificates updates appear in this window. Click the **Notification History** link to open the **Notifications** window. This window provides information about the notification, such as its severtiy, source, timestamp, and status. You can perform the following actions in this window: • Acknowledge a notification. • Filter notifications by status or security level. • Sort notifications by source, detail, description, timestamp, or status.

Icon	Option	Description
admin ⚙	**Administrative Functions**	Opens a menu of options. From this menu, you can choose the following administrative options: • **Settings—**Allows you to configure controller settings, such user profiles, discovery credentials, network security settings, backup and restore, and other controller settings. • **App Management—**Allows you to individually upload and enable Cisco and third-party applications, backup and restore the controller data, and update the Cisco APIC-EM software. • **System Administration—**Allows you to manage and troubleshoot controller services. **Important** Only advanced users should access the **System Administration** console to attempt to troubleshoot the controller services. • **Audit Logs—**Provides information to help you monitor policy creation and application. • **About APIC-EM—**Displays the installed Cisco APIC-EM software version. You can perform the following user functions: • **Change Password—**Allows you to change your own password. • **Sign Out—**Logs you out of the Cisco APIC-EM.

CHAPTER 2

Securing the Cisco APIC-EM

About Cisco APIC-EM Security

The Cisco APIC-EM requires a multi-layered architecture to support its basic functionality. This multi-layered architecture consists of the following components:

- External network or networks—The external network exists between administrators and applications on one side of the network, and the Grapevine root and clients within an internal network or cloud on the other side. Both administrators and applications access the Grapevine root and clients using this external network.
- Internal network—The internal network consists of both the Grapevine root and clients.
- Device management network—This network consists of the devices that are managed and monitored by the controller. Note that the device management network is essentially the same as the external network described above. This may be physically or logically segmented from the admins or northbound applications.

Important Any inter-communications between the layers and intra-communications within the layers are protected through encryption, authentication, and segmentation.

Note For information about the different services running on the clients within the internal network, see Chapter 4, *Cisco APIC-EM Services*.

PKI and the Cisco APIC-EM

The Cisco APIC-EM relies on Public Key Infrastructure (PKI) to provide secure communications. PKI consists of certificate authorities, digital certificates, and public and private keys.

Certificate authorities (CAs) manage certificate requests and issue digital certificates to participating entities such as hosts, network devices, or users. The CAs provide centralized key management for the participating entities.

Digital signatures, based on public key cryptography, digitally authenticate the hosts, devices and/or individual users. In public key cryptography, such as the RSA encryption system, each entity has a key pair that contains both a private key and a public key. The private key is kept secret and is known only to the owning host, device or user. However, the public key is known to everyone. Anything encrypted with one of the keys can be decrypted with the other. A signature is formed when data is encrypted with a sender's private key. The receiver verifies the signature by decrypting the message with the sender's public key. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates link the digital signature to the sender. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the entity's public key. The CA that signs the certificate is a third party that the receiver explicitly trusts to validate identities and to create digital certificates.

To validate the signature of the CA, the receiver must first know the CA's public key. Typically this process is handled out of band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default.

Cisco APIC-EM PKI Planes

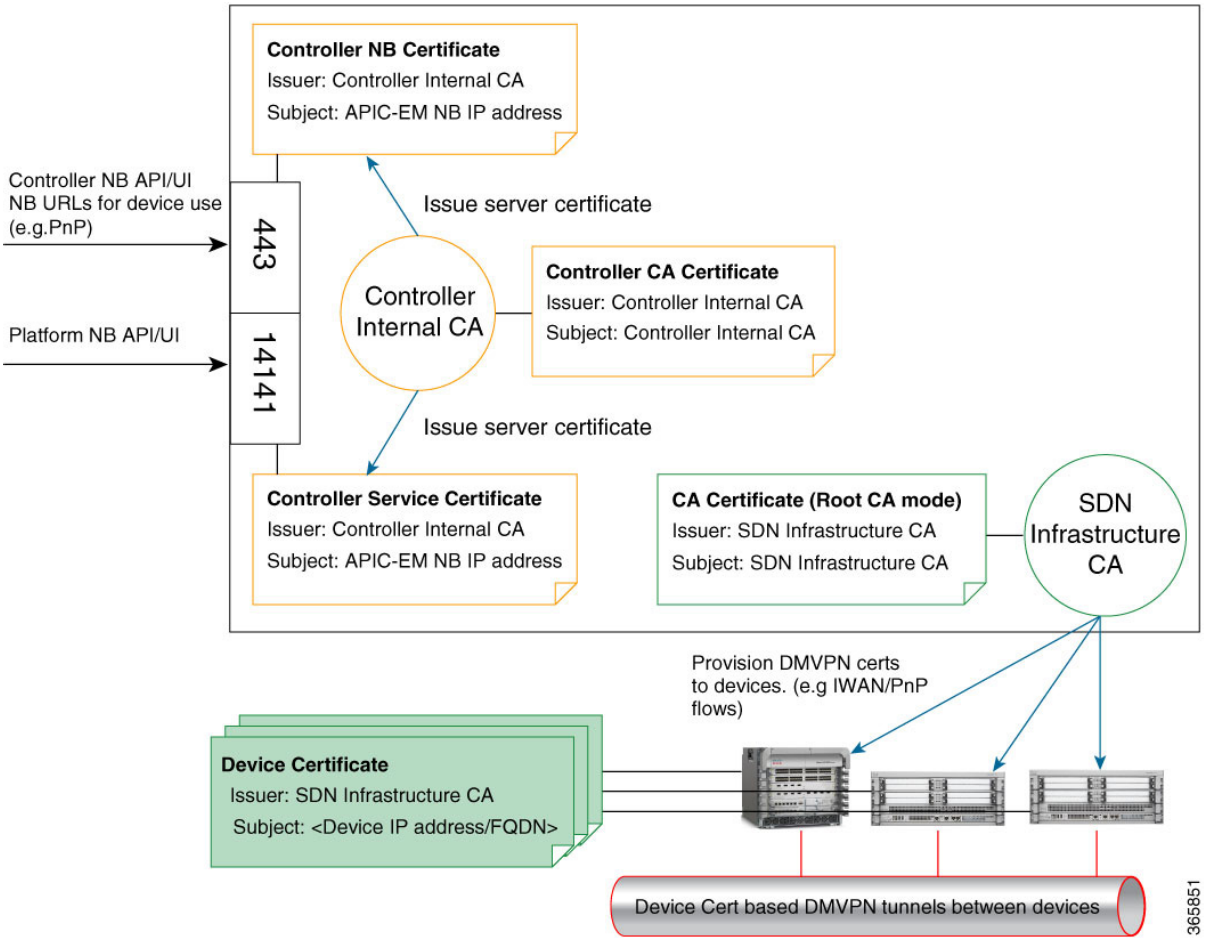
The Cisco APIC-EM provides PKI-based connections in the following distinct PKI planes:

- Controller PKI Plane—HTTPS connections in which the controller is the server in the client-server model, and the controller's server certificate secures the connection. The controller's server certificate can be self-signed (default) or issued by an external CA (recommended.)
- Device PKI Plane—DMVPN connections between devices in the control plane of the network, bilaterally authenticated and secured by the device ID certificates of both devices that participate in the connection. A private CA provided by the Cisco APIC-EM controller (the Device PKI CA) manages these certificates and keys.

- Grapevine Service PKI Plane—The Grapevine root manages this internal PKI plane that secures communications between Grapevine services in a multi-host cluster; the Grapevine Service PKI Plane is not externally accessible, so it is not discussed further here.

The following is a schematic of the Cisco APIC-EM PKI planes, certificate authorities, and certificates. The Controller PKI Plane employs a Controller Internal CA that in response to external requests provides a Controller NB certificate and Controller CA certificate. The Grapevine PKI Plane employs the same Controller Internal CA that in response to internal requests (from controller services) provides a Controller Service Certificate. The Device PKI Plane employs a SDN Infrastructure CA that provides a CA Certificate (Root CA mode in this schematic) for IWAN and PnP devices.

Figure 5: Cisco APIC-EM PKI Planes


Controller NB Certificate
Issuer: Controller Internal CA
Subject: APIC-EM NB IP address
Controller NB API/UI
NB URLs for device use
(e.g.PnP)
443
Issue server certificate
Controller Internal CA
Controller CA Certificate
Issuer: Controller Internal CA
Subject: Controller Internal CA
Platform NB API/UI
14141
Issue server certificate
Controller Service Certificate
Issuer: Controller Internal CA
Subject: APIC-EM NB IP address
CA Certificate (Root CA mode)
Issuer: SDN Infrastructure CA
Subject: SDN Infrastructure CA
SDN Infrastructure CA
Provision DMVPN certs
to devices. (e.g IWAN/PnP
flows)
Device Certificate
Issuer: SDN Infrastructure CA
Subject: <Device IP address/FQDN>
Device Cert based DMVPN tunnels between devices
365851

The Cisco APIC-EM PKI planes support different trust relationships or domains as displayed with the use cases in the following table:

Table 5: PKI Planes in Cisco APIC-EM

	Authentication	Encryption	Use Case
Controller PKI Plane: external caller initiates connection to controller			

	Authentication	Encryption	Use Case
HTTPS	Caller presents username and password or service ticket; Controller presents server certificate.	Yes	REST client, including Cisco Network Plug N Play (PnP) mobile app or Cisco Prime Infrastructure
HTTPS	One-way: controller presents its server certificate.	Yes	Cisco Network Plug N Play (PnP) provisioning workflow
Device PKI Plane: device-to-device connections			
DMVPN	Bilateral authentication via Internet Key Exchange Version 2 (IKEv2) using certificates/keys issued by a private CA within the Cisco APIC-EM controller.	Yes	DMVPN connections between devices

Note The security content and discussion in this deployment guide concerns itself primarily with the Controller PKI Plane. For information about the Device PKI Plane, see the *PKI Planes in Cisco APIC-EM Technote*.

Controller PKI Plane

When an external caller initiates an HTTPS connection to the controller, the controller presents its server certificate. Such connections include the following:

- Logins to the Cisco APIC-EM GUI via HTTPS
- Logins to the Grapevine APIs (port 14141) via HTTPS
- Invocations of the NB REST API via HTTPS

When a NB REST API caller initiates an HTTPS connection to the controller to invoke a NB REST API or to download a file (such as a device image, a configuration, and so on) the controller (server) presents its server certificate to the caller (client) that requested the connection.

Only two NB REST APIs use HTTP instead of HTTPS: the API that downloads the trustpool bundle (GET /ca/trustpool), and the API that downloads the controller's certificate (GET /ca/pem). All other NB REST APIs utilize HTTPS.

Note that controller-initiated connections to devices do NOT take place within the Controller PKI Plane. Even if the connections use SSH or SNMPv3, no CA manages the keys involved, so the connection is not considered to be PKI-based. The controller may initiate connections to devices for purposes that include discovery, managing tags, pushing policy to devices, or interacting with devices on behalf of a REST caller. For compatibility with older devices, discovery can optionally use the TELNET protocol, which is insecure and therefore outside the scope of this PKI discussion.

Device PKI Plane

IWAN-managed control-plane devices form Dynamic Multipoint VPN (DMVPN) connections among themselves. A private Certificate Authority (CA) provided by the Cisco APIC-EM (the Device PKI CA) provisions the certificates and keys that secure these DMVPN connections. The PKI broker service manages these certificates and keys as directed by an admin in the IWAN GUI or as directed by a REST caller that uses the /certificate-authority and /trust-point NB REST APIs.

Note In the default mode, the Device PKI CA in the Cisco APIC-EM cannot be a subordinate/intermediate CA to any external CA. These two PKI planes (one for the controller connections and the other for the device-to-device DMVPN connections) remain completely independent of each another. In the current release, the IWAN devices' mutual interaction certificates are managed only by the Device PKI CA. External CAs cannot manage the IWAN-specific certificates that devices present to each other for DMVPN tunnel-creation and related operations.

Device PKI Plane Modes

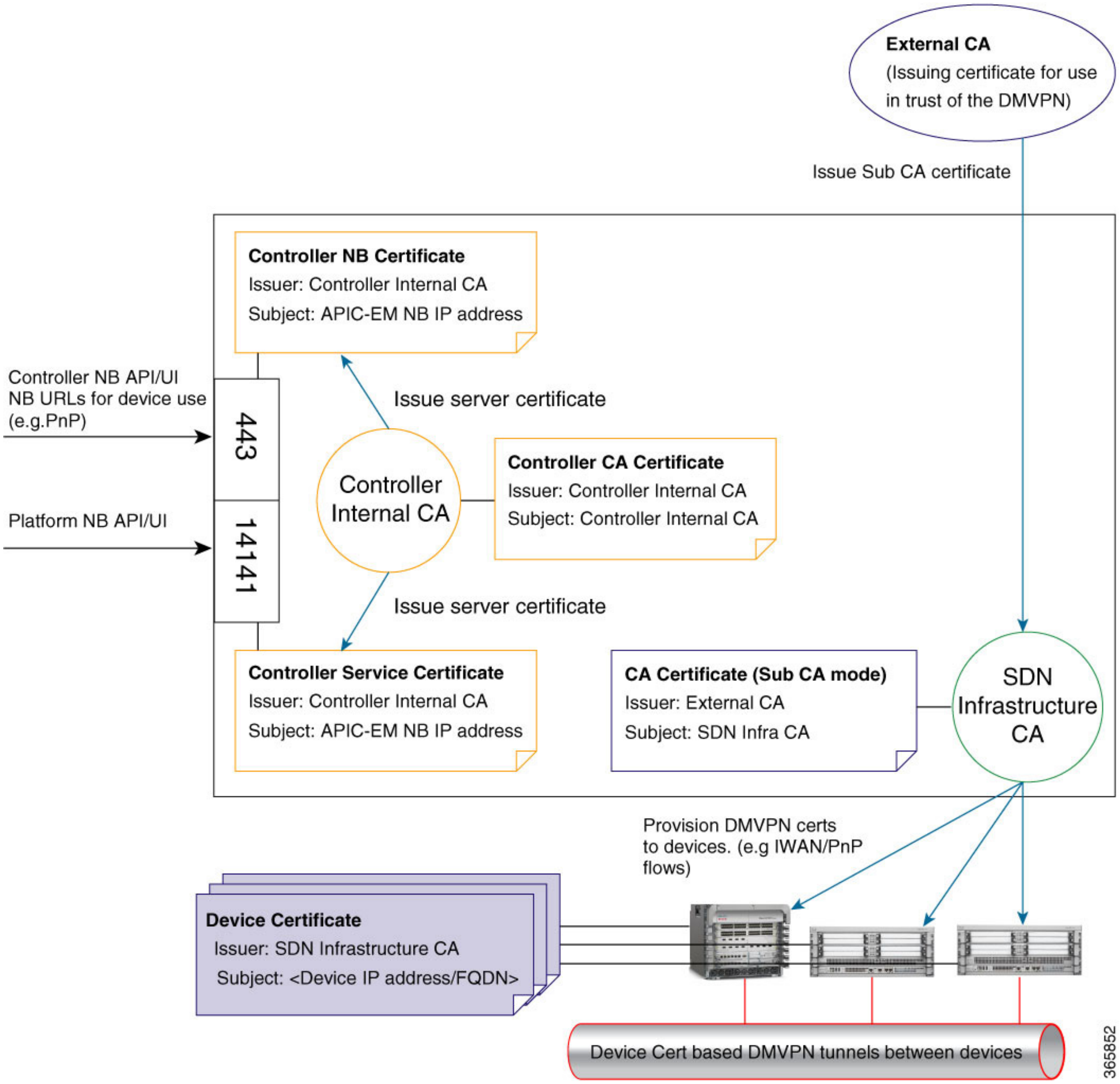
The Device PKI Plane supports two modes:

- Root mode-—The private CA provided by the Cisco APIC-EM controller does not interact with any other CA. This is the default mode for the controller.
- Sub CA mode —In Sub CA mode, the private CA provided by the Cisco APIC-EM controller can be an intermediary CA to an external CA. This means that the private controller CA still manages the certificates and keys that secure device-to-device communications, but it is in a subordinate position to that external CA. This mode must be enabled by an administrator (ROLE_ADMIN).

Changing the PKI mode from root to Sub CA (subordinate CA), changes the hierarchy and subordinates the private controller CA to an external CA. The following is a schematic of the distinct PKI planes, with the Device PKI plane being in Sub CA mode.

The following schematic displays the Sub CA mode for the Device PKI plane. In this schematic the Root CA is external to the controller. See Cisco APIC-EM PKI Planes, on page 18 for a schematic of Root CA mode for the Device PKI plane.

Figure 6: Device PKI Plane—Sub CA Mode


External CA
(Issuing certificate for use
in trust of the DMVPN)
Issue Sub CA certificate
Controller NB Certificate
Issuer: Controller Internal CA
Subject: APIC-EM NB IP address
Controller NB API/UI
NB URLs for device use
(e.g.PnP)
443
Issue server certificate
Controller
Internal CA
Controller CA Certificate
Issuer: Controller Internal CA
Subject: Controller Internal CA
Platform NB API/UI
14141
Issue server certificate
Controller Service Certificate
Issuer: Controller Internal CA
Subject: APIC-EM NB IP address
CA Certificate (Sub CA mode)
Issuer: External CA
Subject: SDN Infra CA
SDN
Infrastructure
CA
Provision DMVPN certs
to devices. (e.g IWAN/PnP
flows)
Device Certificate
Issuer: SDN Infrastructure CA
Subject: <Device IP address/FQDN>
Device Cert based DMVPN tunnels between devices
365852

Related Topics

Changing the Role of the PKI Certificate from Root to Subordinate, on page 46

Configuring the Device Certificate Lifetime, on page 44

Device PKI Notifications

The Cisco APIC-EM provides device PKI notifications to assist the user with both troubleshooting and serviceability.

Important The device PKI notifications described in this section are only activated from device-to-device DMVPN connections and not the controller connections.

The following device PKI notifications are available:

- System Notifications—Notifications indicating that user action is required. These notifications are visible from the **Systems Notifications** view that is accessible from the **Global** toolbar in the GUI.
- Audit Log Notifications—Notifications in system logs that are visible using the controller's **Audit Log** GUI. For information about viewing the audit logs in the controller's GUI, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

The following PKI *System* notification types are supported:

- Information
    - New trust point creation
    - New PKCS12 file creation
    - Successful enrollment of a device certificate
    - Successful renewal of a device certificate
    - Revocation of a device certificate
- Warning
    - Partial revocation—Device unreachable or trust point is in use
    - Enrollment delay after 80 percent of a certificate's lifetime
    - Service launch delay
- Critical
    - Certificate Authority handshake failed
    - Enrollment failed
    - Revocation failed
    - Renew failed

The following *audit log* notifications are available in the system logs:

- Device enrollment
- Certificate push to the device
- Renewal of a device certificate

- Revocation of a device certificate

PKI Certificate Management

The Cisco APIC-EM provides PKI-based connections in the following distinct PKI planes:

- Controller PKI Plane—With this plane, there exists HTTPS connections in which the controller is the server in the client-server model, and the controller's server certificate secures the connection.
- Device PKI Plane—With this plane, there exists DMVPN connections between devices in the control plane of the network, bilaterally authenticated and secured by the device ID certificates of both devices that participate in the connection. These certificates/keys are issued by a private CA that the Cisco APIC-EM controller provides (Device PKI CA).

The following PKI certificate management procedures that are described in this chapter involve only the Device PKI plane:

- Changing the Role of the PKI Certificate from Root to Subordinate, on page 46—This procedure requires that you replace the CA certificate of the private CA with one signed by the external CA.
- Configuring the Device Certificate Lifetime, on page 44—This procedure helps you secure the device-to-device connections between IWAN-managed devices.

Cisco APIC-EM Controller Certificate and Private Key Support

The Cisco APIC-EM supports a PKI certificate management feature (Controller PKI Plane) that is used to authenticate sessions (HTTPS). These sessions use commonly recognized trusted agents called certificate authorities (CAs). The Cisco APIC-EM uses the PKI certificate management feature to import, store, and manage an X.509 certificate from well-known CAs. The imported certificate becomes an identity certificate for the controller itself, and the controller presents this certificate to its clients for authentication. The clients are the NB API applications and network devices.

The Cisco APIC-EM can import the following files (in either PEM or PKCS file format) using the controller's GUI:

- X.509 certificate
- Private key

Note For the private key, Cisco APIC-EM supports the importation of RSA keys. You should not import DSA, DH, ECDH, and ECDSA key types; they are not supported. You should also keep the private key secure in your own key management system.

Prior to import, you must obtain a valid X.509 certificate and private key from a well-known, certificate authority (CA) or create your own self-signed certificate. After import, the security functionality based upon the X.509 certificate and private key is automatically activated. The Cisco APIC-EM presents the certificate to any device or application that requests them. Both the northbound API applications and network devices can use these credentials to establish a trust relationship with the controller.

In an IWAN configuration and for the Network PnP functionality, an additional procedure involving a PKI trustpool is used to ensure trust between devices within the network. See the following *Cisco APIC-EM Trustpool Support* section for information about this procedure.

Note We recommend against using and importing a self-signed certificate into the controller. Importing a valid X.509 certificate from a well-known, certificate authority (CA) is recommended. Additionally, you must replace the self-signed certificate (installed in the Cisco APIC-EM by default) with a certificate that is signed by a well-known certificate authority for the Network PnP functionality to work properly.

The Cisco APIC-EM supports only one imported X.509 certificate and private key at a time. When you import a second certificate and private key, it overwrites the first (existing) imported certificate and private key values.

Note If the external IP address changes for your controller for any reason, then you need to re-import a new certificate with the changed or new IP address.

Related Topics

Importing the Controller's Server Certificate, on page 38

Cisco APIC-EM Controller Certificate Chain Support

The Cisco APIC-EM is able to import certificates and private keys into the controller through its GUI.

If there are subordinate certificates involved in the certificate chain leading to the certificate that is imported into the controller (controller certificate), then both the subordinate certificates as well as the root certificate of these subordinate CAs must be appended together into a single file to be imported. When appending these certificates, you must append them in the same order as the actual chain of certification.

For example, assume that a well-known and trusted CA with a root certificate (CA root) signed an intermediate CA certificate (CA1). Next, assume that this certificate, CA1 signs another intermediate CA certificate (CA2). Finally, assume that the CA certificate (CA2) was the CA that signed the controller certificate (Controller_Certificate). In this example, the PEM file that needs to be created and imported into the controller should have the following order from the top (beginning) of the file to the bottom of the file (end):

1. Controller_Certificate (top of file)
2. CA2 certificate
3. CA1 certificate

The requirement to append the root and subordinate certificates to the controller certificate to create a single file only applies to a PEM file. The requirement for appending a root and intermediate certificates to a root certificate for import is not required for a PKCS file.

Related Topics

Importing the Controller's Server Certificate, on page 38

Obtaining a CA-Signed Certificate for the Cisco APIC-EM Controller

You can perform the following steps to obtain a CA signed certificate to import into and use for the Cisco APIC-EM.

1. Determine the IP address or DNS-resolvable FQDN of your Cisco APIC-EM cluster.
2. Use that IP address or the DNS-resolvable FQDN of your Cisco APIC-EM cluster as the common name in your certificate signing request (CSR).

Note It is preferable for the Subject Alternate Name (SAN) field to also be used, so that both the IP address and the DNS-resolvable FQDN are included in the certificate.

3. Follow the procedure described below to create the CSR.
4. Send the completed CSR to the certificate authority (CA) that you have selected.
5. Receive the signed certificate back from the CA.
6. Install the certificate into the controller using the controller's GUI.

Note This example procedure is performed on the host where the Cisco APIC-EM is installed. You can also perform this procedure to generate a CSR and private key on a Linux OS or Apple Macintosh computer. You do not have to perform this procedure on the host where the Cisco APIC-EM is installed.

Before You Begin

Before you attempt this procedure, you should have knowledge of these topics:

- How to use the OpenSSL application
- Public key infrastructure and digital certificates

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.
The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to create a private key and a CSR.

```
$ openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key

Generating a 2048 bit RSA private key
.......................................................+++
........+++
writing new private key to 'privateKey.key'
-----
You are about to be asked to enter information that will be incorporated
```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Step 4 Respond to the certificate prompts with customer specific information as needed.
For the common name IP address, if this request is for multi-host Cisco APIC-EM deployment, then enter the Virtual IP address planned for the multi-host. If this request is for a single Cisco APIC-EM appliance or VM, then enter the eth0 IP address.

For example:

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:Cloud Unit
Common Name (e.g. server FQDN or YOUR name) []:209.165.201.22
Email Address []:myemail@email.com
```

Step 5 Do not enter values for the extra attributes fields, just press Enter.

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:

An optional company name []:
```

After pressing Enter, two files (CSR and private key) will be generated.

Step 6 Locate the two files (CSR and private key) that were generated on the host.
The two files are: `privateKey.key` and `CSR.csr`.

For example, information about the files is displayed using the following command:

```
$ ls -ltr
total 8

-rw-rw-r-- 1 grapevine grapevine 1708 Apr 18 15:39 privateKey.key
-rw-rw-r-- 1 grapevine grapevine 1054 Apr 18 15:39 CSR.csr
```

Step 7 Secure the privateKey.key file.

Note Never send out the private key. Keep it in a secure location in your network.

Step 8 Copy and paste the CSR content from the CSR.csr file and send it to the CA for signing.

Note The CA will usually be a trustpool CA, unless your company runs its own CA.

In this example, the content in bold below will be the CSR that is copied and sent to the CA for signing and to get the certificate sent back.

```
$ cat CSR.csr

-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAboCAQAwgYwxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTERMA8GA1UE
```

```
MRYwFAYDVQQDDA0xNzIuMjQuMTAwLjU1MSAwHgYJKoZIhvcNAQkBFhFteWVtYWls
QGVtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAONJ7M96
rXjg/kwWcfJUlJJG2agLv7EAIxaB7He84fSdNMVXsJmuYBwZBWuZ9t/h3AKs/n/t
MRYwFAYDVQQDDA0xNzIuMjQuMTAwLjU1MSAwHgYJKoZIhvcNAQkBFhFteWVtYWls
QGVtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAONJ7M96
rXjg/kwWcfJUlJJG2agLv7EAIxaB7He84fSdNMVXsJmuYBwZBWuZ9t/h3AKs/n/t
87nugrgW7SmI4F1wLsVg8KU2X0bmHoke6yCkhCPykQXJR2blMWp/OBc0ASMTIdhH
XRju1y/5
-----END CERTIFICATE REQUEST-----
(grapevine)
```

Important It is likely that instead of a single root CA certificate being sent back to you, that a chain of CA certificates, (including the CA's own public root certificate) will be sent back to you. In this case, follow the rules of appending the CA certificates as described in Cisco APIC-EM Controller Certificate Chain Support, on page 25, before importing them into the controller using its GUI.

Step 9 Once the CA administrator in your organization provides you with the signed certificate (for example, MyCert.pem), drag and drop the **MyCert.pem** and **privateKey.key** into the Cisco APIC-EM GUI certificate page. For information about this procedure, see Importing the Controller's Server Certificate, on page 38

Note The content of MyCert.pem file obtained from the CA administrator should look like the CSR content which is base64 encoded and be in PEM format. Run the **cat** command on the obtained file to view its contents. If the file's contents looks like a binary file in the **cat** command output, then use the converter at this link to convert the file's content into PEM format:

https://www.sslshopper.com/ssl-converter.html.

Related Topics

Importing the Controller's Server Certificate, on page 38

Cisco APIC-EM Trustpool Support

The Cisco APIC-EM and Cisco IOS devices support a special PKI certificate store known as the trustpool. The trustpool holds X.509 certificates that identify trusted certificate authorities (CAs). The Cisco APIC-EM and the devices in the network use the trustpool bundle to manage trust relationships with each other and with these CAs. The controller manages this PKI certificate store and an administrator (ROLE_ADMIN) has the ability to update it through the controller's GUI when certificates in the pool are due to expire, are reissued, or must be changed for other reasons.

Note The Cisco APIC-EM also uses the trustpool functionality to determine whether any certificate file that is uploaded via its GUI is a valid trustpool CA-signed certificate or not.

The Cisco APIC-EM contains a pre-installed, default, Cisco-signed trustpool bundle named ios.p7b. This trustpool bundle is trusted by supported Cisco network devices natively, since it is signed with a Cisco digital signing certificate. This trustpool bundle is critical for the Cisco network devices to establish trust with services and applications that are genuine. This Cisco PKI trustpool bundle file is available on the Cisco website (Cisco InfoSec).

The link is located at:http://www.cisco.com/security/pki/

For the controller's Network PnP functionality, the supported Cisco devices that are being managed and monitored by the controller need to import this file. When the supported Cisco devices first boot-up, they contact the controller to import this file.

The Cisco APIC-EM trustpool management feature operates in the following way:

1. You boot-up the Cisco devices within your network that supports the Network PnP functionality.

   Note that **not** all Cisco devices support the Network PnP functionality. See the *Release Notes for Cisco Network Plug and Play* for a list of the supported Cisco devices.

2. As part of initial PnP flow, these supported Cisco devices download a trustpool bundle directly from the Cisco APIC-EM using HTTP.

3. The Cisco devices are now ready to interact with the Cisco APIC-EM to obtain further device configuration and provisioning per the Network PnP traffic flows.

Important If an HTTP proxy gateway exists between the controller and these Cisco devices, then perform an additional procedure to import the proxy gateway certificate into the controller. See Importing a Proxy Gateway Certificate, on page 42.

Note At times, you may need to update this trustpool bundle to a newer version due to certificates in the trustpool expiring, being reissued, or for other reasons. Whenever the trustpool bundle that exists on the controller needs to be updated, you can update it by using the controller's GUI. The controller can access the Cisco cloud (where the Cisco approved trustpool bundles are located) and download the latest trustpool bundle. After download, the controller then overwrites the current, older trustpool bundle file. As a practice, you may want to update the trustpool bundle before a new certificate from a CA is to be imported using the **Certificate** window or the **Proxy Gateway Certificate** window, or whenever the **Update** button is active and not grayed out.

Related Topics

Importing a Trustpool Bundle, on page 41

Security and Cisco Network Plug and Play

With the Cisco Network Plug and Play (PnP) application, the Cisco APIC-EM responds to HTTPS requests from supported Cisco network devices and permits these devices to download and install an image and desired configuration. Before a device can download these files from the controller, the initial interaction between the controller and device involves the establishment of a trust relationship.

In certain Cisco Network Plug and Play scenarios, your network configuration may also have a proxy gateway present between the controller and PnP-enabled devices. For example, in an IWAN deployment a branch router may communicate with the Cisco APIC-EM through a proxy gateway at the DMZ at initial provisioning. Depending upon whether there is a proxy gateway present or not, the trust information provided by the controller at the initial transaction with the devices may correspond to either the proxy gateway's or to the controller’s certificate issuer (if the corresponding server certificates are not valid CA signed). On the other hand, in either proxy or non-proxy cases, if the certificate is a simple self-signed certificate, then that certificate will be downloaded by the device into its trust store.

Note Using a self-signed certificate for either the Cisco APIC-EM or the proxy gateway is strongly discouraged. We strongly recommend using a publicly verifiable CA issued certificate to be installed on the controller, as well as the proxy gateway if one is present.

With a valid CA issued certificate for the controller or the proxy gateway (if present), the PnP-enabled devices can download the trustpool bundle (ios.p7b) containing all the well known CA root certificates. This permits the devices to establish secure connections to the controller or to the proxy gateway for further provisioning and operation of those devices. If such a certificate is not a valid CA issued or self-signed, then the devices will have to download the issuing CA's or self-signed certificate to proceed further with a secure connection to the controller or a proxy gateway in front of the controller. The Cisco APIC-EM facilitates automatic downloads of the relevant trusted certificates on the devices, depending on the nature of the certificate installed on it. However; when a proxy gateway is present, the controller provides a provisioning GUI to facilitate similar pre-provisioning.

Related Topics

Importing a Proxy Gateway Certificate, on page 42

Configuring the TLS Version Using the CLI

Northbound REST API requests from the external network to the Cisco APIC-EM (from northbound REST API based apps, browsers, and network devices connecting to the controller using HTTPS) are made secure using the Transport Layer Security protocol (TLS). The Cisco APIC-EM supports TLS versions 1.0, 1.1, and 1.2.

By default, the minimum TLS version that a client can use to communicate with the controller is version 1.0. If your network device IOS/XE versions can support a higher version than version 1.0, then it is strongly recommended to configure the minimum TLS version of the controller to that higher version, but first ensure that all of your network devices under Cisco APIC-EM control can support the higher version.

Important With the controller TLS version set to 1.2, a client initiating a lower TLS connection version (for example, versions 1.0 or 1.1) will be rejected and any communications from this client will fail. With the controller TLS version set to 1.0, a client initiating a higher TLS connection version (for example, versions 1.1 or 1.2) will be permitted. Any versions lower than TLS 1.0 (such as SSLv3 and SSLv2) are not supported by the Cisco APIC-EM.

You configure the TLS version for the controller by logging into the host (physical or virtual) and using the CLI.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have grapevine SSH access privileges to perform this procedure.

Important This security feature applies to ports 443 and 14141 on the Cisco APIC-EM. Performing this procedure may disable traffic on port 14141 to the controller infrastructure for a few seconds. For this reason, you should configure TLS infrequently and only during off-peak hours or a maintenance time period.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **grape config display** command at the prompt to display the default TLS minimum version.

```
$ grape config display

PROPERTY                         VALUE
----------------------------------------------------------------------
client_grow_timeout              150
client_heartbeat_timeout         120
client_idle_timeout              60
enable_policy                    True
enable_secure_tunnel             True
enable_service_rollback          False
host_cpu_threshold               0.9
host_datastore_threshold         1.0
host_heartbeat_timeout           120
host_memory_threshold            0.00999999977648
https_proxy
https_proxy_password
https_proxy_username
load_multiplier                  1.0
max_spare_capacity               1
policy_startup_delay             120
tls_minimum                      1_0

(grapevine)
```

The above command output indicates that the current TLS minimum version is 1.0.

Step 4 Enter the **grape config update tls_minimum 1_2** command at the prompt to update to TLS version 1.2

```
$ grape config update tls_minimum 1_2
Config updated successfully

(grapevine)
```

To update the TLS version to 1.1, you would enter the **grape config update tls_mimimum 1_1** command.

Step 5 Enter the **grape config display** command at the prompt a second time to view the new TLS minimum version.

```
$ grape config display

PROPERTY                         VALUE
```

```
----------------------------------------------------------------------
client_grow_timeout              150
client_heartbeat_timeout         120
client_idle_timeout              60
enable_policy                    True
enable_secure_tunnel             True
enable_service_rollback          False
host_cpu_threshold               0.9
host_datastore_threshold         1.0
host_heartbeat_timeout           120
host_memory_threshold            0.00999999977648
https_proxy
https_proxy_password
https_proxy_username
load_multiplier                  1.0
max_spare_capacity               1
policy_startup_delay             120
tls_minimum                      1_2

(grapevine)
```

The TLS minimum version should display *1_2*, which indicates the TLS 1.2 version.

Related Topics

External Network Security
Device Management Network Security

Configuring IPSec Tunneling for Multi-Host Communications

The default tunneling protocol used for inter-host communications in a multi-host cluster is Internet Protocol Security (IPsec). The previous default tunneling protocol (in earlier controller release versions) was Generic Routing Encapsulation (GRE). Communications between the hosts in a multi-host cluster can be made more secure using IPSec. If you current tunneling configuration between hosts is GRE, then you can enable secure tunneling with IPSec with the configuration wizard.

Perform the steps described in the following procedure to enhance security for communications between the hosts. The steps are organized as follow:

1. Break up or disassemble your existing multi-host cluster (steps 1-6).
2. Enable IPSec tunneling on the last host that was in your cluster (steps 7-11).
3. Reassemble your multi-host cluster around that host where you enabled IPSec tunneling. (steps 11-21).

Note Do not enable or disable the secure tunnel mode (IPSec tunneling) while the Cisco APIC-EM is in a multi-host cluster. The configuration wizard does not support such a change while in a multi-host cluster.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

The current tunneling protocol is GRE, and not IPSec.

You must have grapevine SSH access privileges to perform this procedure.

Step 1 Using a Secure Shell (SSH) client, log into one of the hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 2 Enter the **grape config display** command to view and confirm your current GRE tunneling configuration.

```
$ grape config display
```

The **enable_secure_tunnel** value will be set to **false** for a GRE configuration.

Step 3 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 4 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 5 A message appears with an option to **[proceed]** and remove this host from the cluster.
Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from the cluster.
At the end of this process, this host is removed from the cluster.

Step 6 Repeat the above steps (steps 1-4) on the second host in your cluster. This will break up your multi-host cluster.

Important Make a note of the final host in the cluster that you have just broken up or disassembled. You must perform the next steps (enabling IPSec tunneling) on that final host. For example, with 3 hosts in a cluster (A, B, and C) and you first remove host A, then remove host B, then you must enable IPSec on host C.

Step 7 Using a Secure Shell (SSH) client, log into the last host in your cluster and run the **config_wizard** command.

```
$ config_wizard
```

Step 8 Review the current configuration values in the configuration wizard and click **next>>**, until you access the **INTER-HOST COMMUNICATION** screen.

Step 9 Configure IPSec tunneling for communications between the hosts in a multi-host cluster by selecting *yes*.
By entering 'yes', you are configuring IPSec tunneling with this step.

Step 10 Click **next>>** until the last step of the configuration wizard process is reached.

Step 11 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM deployment.
At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Next, proceed to log into the other hosts previously in your multi-host cluster and use the configuration wizard to reassemble the cluster (with IPSec tunneling configured between the hosts).

Step 12 Using a Secure Shell (SSH) client, log into one of the other hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 13 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 14 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option.

Note Joining this other (second) host to the host with the enabled IPSec tunneling, automatically configures IPSec tunneling on this other (second) host.

Step 15 Proceed to recreate the cluster using the configuration wizard.
For additional information about this step and process, see .

Step 16 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

Step 17 Using a Secure Shell (SSH) client, log into the third host and use the configuration wizard to join the new multi-host cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 18 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 19 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Add this host to an existing APIC-EM cluster** option.

Note Adding this host to the new multi-host cluster with the enabled IPSec tunneling, automatically configures IPSec tunneling on this host.

Step 20 Proceed to add this host to the cluster using the configuration wizard.
For additional information about this step and process, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 21 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

At the end of this step, you have updated your cluster and configured IPSec tunneling.

Related Topics

Internal Network Security

Password Requirements

The Cisco APIC-EM password policy governs password values in logins to the controller GUI, SSH logins to the Grapevine root, northbound API requests, and logins to the Grapevine console for troubleshooting. The

Cisco APIC-EM rejects a password that does not conform to the password policy. If a password is rejected, the controller provides an error message that describes the reason for the rejection.

A new or changed password must meet the following criteria:

- Length of password must be from 8 (minimum) to 127 (maximum) characters.
- Does NOT contain a tab or a line break.
- Does contain characters from at least three of the following categories:
    - Uppercase alphabet
    - Lowercase alphabet
    - Numeral
    - Special characters

      Special characters include the space character or any of the following characters or character combinations:

      ```
      ! @ # $ % ^ & * ( ) - =  + _ { } [ ] \\ | ; : " ' , < . > ? /
      :: #! ./ ;; >> << () **
      ```

For example, `Splunge!` is a valid password because it meets the eight-character minimum length, contains at least one uppercase alphabetic character, contains at least one lowercase alphabetic character, and contains at least one special character (`!`).

Related Topics

Configuring Password Policies, on page 51

Cisco APIC-EM Ports Reference

The following tables list the Cisco APIC-EM ports that permit incoming traffic, as well as the Cisco APIC-EM ports that are used for outgoing traffic. You should ensure that these ports on the controller are open for both incoming and outgoing traffic flows.

Note Ensure that proper protections exist in your network for accessing ports 22 and 14141. For example, you can configure a proxy gateway or secure subnets to access these ports.

Table 6: Cisco APIC-EM Incoming Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH	TCP
67	bootps	UDP
80	HTTP	TCP
123	NTP	UDP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
162	SNMP	UDP
443[1]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP (Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP
14141	Grapevine APIs	TCP
16026	SCEP	TCP

[1] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see Configuring the TLS Version Using the CLI, on page 30

Table 7: Cisco APIC-EM Outgoing Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH (to the network devices)	TCP
23	Telnet (to the network devices)	TCP
53	DNS	UDP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
80	Port 80 may be used for an outgoing proxy configuration. Additionally, other common ports such as 8080 may also be used when a proxy is being configured by the Cisco APIC-EM configuration wizard (if a proxy is already in use for your network). **Note** To access Cisco supported certificates and trust pools, you can configure your network to allow for outgoing IP traffic from the controller to Cisco addresses at the following URL: http://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP agent	UDP
443[2]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP ((Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP

[2] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see Configuring the TLS Version Using the CLI, on page 30

Configuring Security Settings

Importing the Controller's Server Certificate

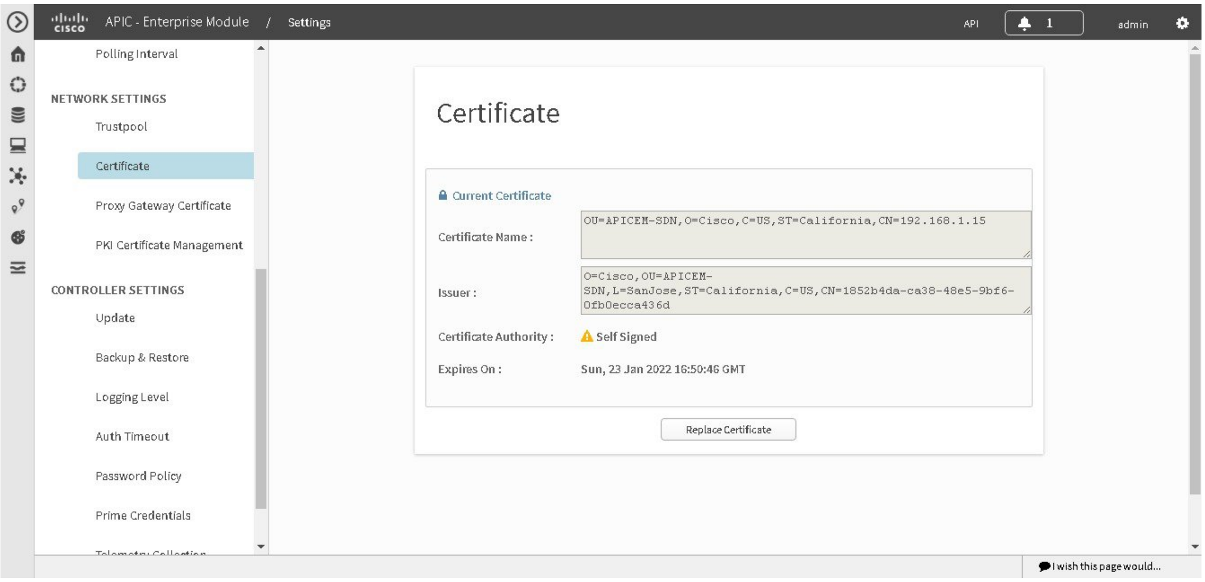
The Cisco APIC-EM supports the import and storing of an X.509 certificate and private key into the controller. After import, the certificate and private key can be used to create a secure and trusted environment between the Cisco APIC-EM, NB API applications, and network devices.

Note If you have a multi-host deployment and you plan to acquire a valid CA-issued certificate for your controller HTTPS server, then use the virtual IP address that you assigned to the multi-hosts as the Common Name for the certificate when you order. If you are using a host name instead, make sure the host name is DNS-resolvable to the virtual IP address of the multi-host deployment.

If you already have a single host Cisco APIC-EM with a previously purchased CA-issued certificate for its external IP address, then it is ideal to use that original physical IP address of the single host as the virtual IP address of the multi-host deployment. This way you can save your investment in the CA-issued certificate and external client applications can continue using the same IP address to access your Cisco APIC-EM services.

You import a certificate and private key using the **Certificate** window in the Cisco APIC-EM GUI.

Figure 7: Certificate Configuration Window



Certificate Name : OU=APICEM-SDN,O=Cisco,C=US,ST=California,CN=192.168.1.15

Issuer : O=Cisco,OU=APICEM-SDN,L=SanJose,ST=California,C=US,CN=1852b4da-ca38-48e5-9bf6-0fb0ecca436d

Certificate Authority : ⚠ Self Signed

Expires On : Sun, 23 Jan 2022 16:50:46 GMT

Important The Cisco APIC-EM itself does NOT interact with any external CA directly; therefore, it does not check any Certificate Revocation Lists and it has no way to learn of revocation of its server certificate by an external CA. Note, also, that the controller does not automatically update its server certificate. Replacement of an expired or revoked server certificate requires explicit action on the part of a ROLE_ADMIN user. Although the controller has no direct means of discovering the revocation of its server certificate by an external CA, it does notify the admin of expiration of its server certificate as well as self-signed key being operational.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have acquired an X.509 certificate and private key from a well-known certificate authority (CA) for the import.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Certificate** to view the **Certificate** window.

Step 4 In the **Certificate** window, view the current certificate data.
When first viewing this window, the current certificate data that is displayed is the controller's self-signed certificate. The self-signed certificate's expiration is set for several years in the future.

Note The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification will appear in the controller's GUI 2 months before the expiration date and time of the certificate.

Additional displayed fields in the **Certificate** window include:

- Certificate Name—The name of the certificate.
- Issuer—The issuer name identifies the entity that has signed and issued the certificate.
- Certificate Authority—Either self-signed or name of the CA.
- Expires On—Expiration date of the certificate.

Step 5 To replace the current certificate, click the **Replace Certificate** button.
The following new fields appear:

- **Certificate—**Fields to enter certificate data
- **Private Key—**Fields to enter private key data

Step 6 In the **Certificate** fields, choose the file format type of the certificate:

- **PEM—**Privacy enhanced mail file format

- **PKCS—**Public-key cryptography standard file format

Choose one of the above file types for the certificate that you are importing into the Cisco APIC-EM.

Step 7 If you choose **PEM**, then perform the following tasks:

- For the **Certificate** field, import the **PEM** file by dragging and dropping this file into the **Drag n' Drop a File Here** field.

  Note For a PEM file, it must have a valid PEM format extension (.pem, .cert, .crt). The maximum file size for the certificate is 10KB

- For the **Private Key** field, import the private key by dragging and dropping this file into the **Drag n' Drop a File Here** field.
  - Choose the encryption option from the **Encrypted** drop-down menu for the private key.
  - If encryption is chosen, enter the passphrase for the private key in the **Passphrase** field.

    Note For the private keys, they must have a valid private key format extension (.pem or .key).

Step 8 If you choose **PKCS**, then perform the following tasks:

- For the **Certificate** field, import the **PKCS** file by dragging and dropping this file into the **Drag n' Drop a File Here** field.

  Note For a PKCS file, it must have a valid PKCS format extension (.pfx, .p12). The maximum file size for the certificate is 10KB

- For the **Certificate** field, enter the passphrase for the certificate using the **Passphrase** field.

  Note For PKCS, the imported certificate also requires a passphrase.

- For the **Private Key** field, choose the encryption option for the private key using the drop-down menu.
- For the **Private Key** field, if encryption is chosen, enter the passphrase for the private key in the **Passphrase** field.

Step 9 Click the **Upload/Activate** button.

Step 10 Return to the **Certificate** window to view the updated certificate data.
The information displayed in the **Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

Related Topics

Cisco APIC-EM Controller Certificate and Private Key Support, on page 24

Cisco APIC-EM Controller Certificate Chain Support, on page 25

Obtaining a CA-Signed Certificate for the Cisco APIC-EM Controller, on page 26

Importing a Trustpool Bundle

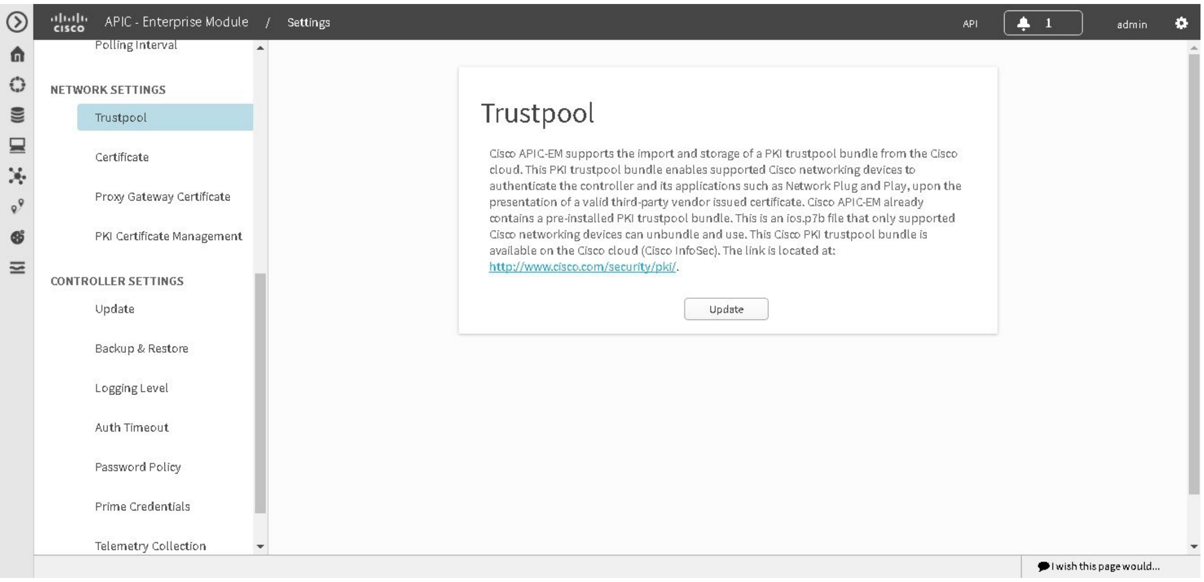
The Cisco APIC-EM contains a pre-installed Cisco trustpool bundle (Cisco Trusted External Root Bundle). The Cisco APIC-EM also supports the import and storage of an updated trustpool bundle from Cisco. The trustpool bundle is used by supported Cisco networking devices to establish a trust relationship with the controller and its applications, such as Network PnP.

Note The Cisco trustpool bundle is an ios.p7b file that only supported Cisco devices can unbundle and use. This ios.p7b file contains root certificates of valid certificate authorities including Cisco itself. This Cisco trustpool bundle is available on the Cisco cloud (Cisco InfoSec). The link is located at: http://www.cisco.com/security/pki/.

The trustpool bundle provides you with a safe and convenient way to use the same CA to manage all your network device certificates, as well as your controller certificate. The trustpool bundle is used by the controller to validate its own certificate as well as a proxy gateway certificate (if any), to determine whether it is valid CA signed certificate or not. Additionally, the trustpool bundle is available to be uploaded to the Network PnP enabled devices at the beginning of their PnP workflow so that they can trust the controller for subsequent HTTPS-based connections.

You import the Cisco trust bundle using the **Trustpool** window in the Cisco APIC-EM GUI.

Figure 8: Trustpool Window



Trustpool

Cisco APIC-EM supports the import and storage of a PKI trustpool bundle from the Cisco cloud. This PKI trustpool bundle enables supported Cisco networking devices to authenticate the controller and its applications such as Network Plug and Play, upon the presentation of a valid third-party vendor issued certificate. Cisco APIC-EM already contains a pre-installed PKI trustpool bundle. This is an ios.p7b file that only supported Cisco networking devices can unbundle and use. This Cisco PKI trustpool bundle is available on the Cisco cloud (Cisco InfoSec). The link is located at: http://www.cisco.com/security/pki/.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Trustpool** to view the **Trustpool** window.

Step 4 In the **Trustpool** window, view the **Update** button.
The **Update** button in the controller's **Trustpool** window becomes active when an updated version of ios.p7b file is available and Internet access is available. The **Update** button remains inactive if there is no Internet access or if there is no updated version of the ios.p7b file.

Step 5 Click the **Update** button to initiate a new download and install of the trustpool bundle.

Note After the new trustpool bundle is downloaded and installed on the controller, the controller then makes this trustpool bundle available to the supported Cisco devices to download.

Related Topics

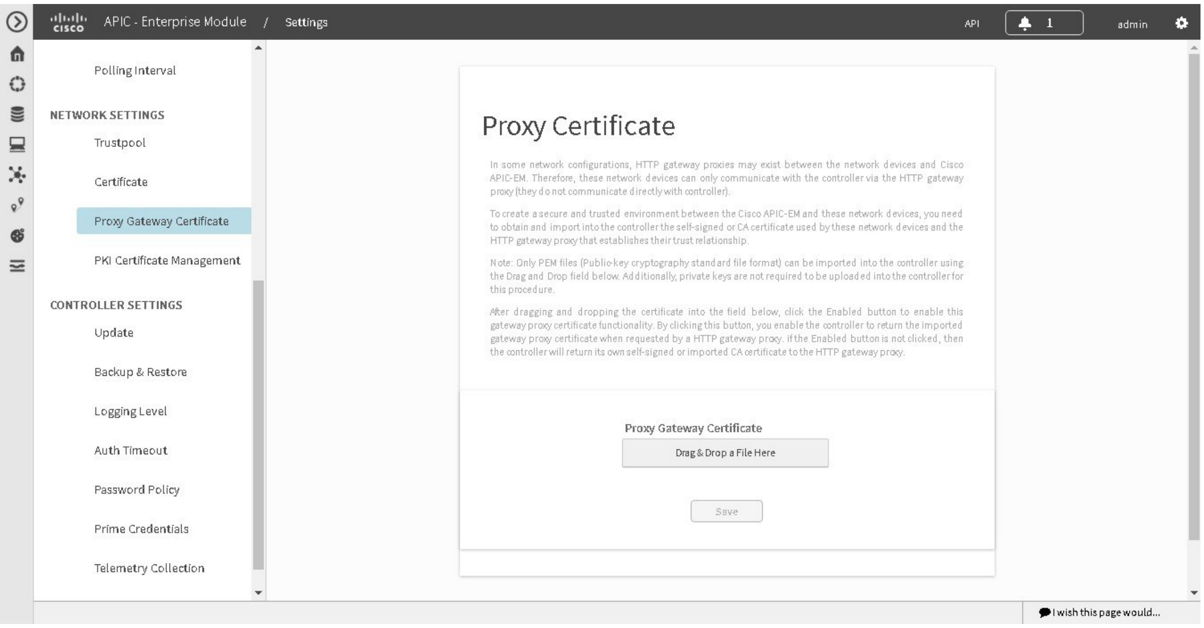
Cisco APIC-EM Trustpool Support, on page 28

Importing a Proxy Gateway Certificate

In some network configurations, proxy gateways may exist between the Cisco APIC-EM and the remote network it manages (containing IWAN and PnP network devices). Common ports such as 80 and 443 pass through the gateway proxy in the DMZ, and for this reason SSL sessions from the network devices meant for the controller terminate at the proxy gateway. Therefore, the network devices located within these remote networks can only communicate with the controller via the proxy gateway. In order for the network devices to establish secure and trusted connections with the controller, or if present, a proxy gateway, then the network devices should have their PKI trust stores appropriately provisioned with the relevant CA root certificates or the server’s own certificate under certain circumstances.

In network topologies where there is a proxy gateway present between controller and the remote network it manages, follow the procedure below to import a proxy gateway certificate into the controller.

Figure 9: Proxy Gateway Certificate Window



Proxy Certificate

In some network configurations, HTTP gateway proxies may exist between the network devices and Cisco APIC-EM. Therefore, these network devices can only communicate with the controller via the HTTP gateway proxy (they do not communicate directly with controller).

To create a secure and trusted environment between the Cisco APIC-EM and these network devices, you need to obtain and import into the controller the self-signed or CA certificate used by these network devices and the HTTP gateway proxy that establishes their trust relationship.

Note: Only PEM files (Public-key cryptography standard file format) can be imported into the controller using the Drag and Drop field below. Additionally, private keys are not required to be uploaded into the controller for this procedure.

After dragging and dropping the certificate into the field below, click the Enabled button to enable this gateway proxy certificate functionality. By clicking this button, you enable the controller to return the imported gateway proxy certificate when requested by a HTTP gateway proxy. if the Enabled button is not clicked, then the controller will return its own self-signed or imported CA certificate to the HTTP gateway proxy.

Before You Begin

You have successfully deployed the Cisco APIC-EM and it is operational.

In your network, an HTTP proxy gateway exists between the controller and the remote network it manages (containing IWAN and PnP network devices) . These network devices will use the proxy gateway's IP address to reach the Cisco APIC-EM controller and its services.

You have the certificate file currently being used by the proxy gateway. The certificate file contents can consist any of the following:

- The proxy gateways's certificate in PEM format, with the certificate being self-signed.
- The proxy gateway's certificate in PEM format, with the certificate being issued by a valid, well-known CA.
- The proxy gateway's certificate and its chain in PEM format.

The certificate used by the devices and proxy gateway must be imported into the controller by following this procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Proxy Gateway Certificate** to view the **Proxy Certificate** window.

Step 4 In the **Proxy Gateway Certificate** window, view the current proxy gateway certificate data (if this exists).

Note The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification will appear in the controller's GUI 2 months before the expiration date and time of the certificate.

Step 5 To add a proxy gateway certificate, drag and drop the self-signed or CA certificate to the **Drag n' Drop a File Here** field.

Note Only PEM files (Public-key cryptography standard file format) can be imported into the controller using this field. Additionally, private keys are neither required nor uploaded into the controller for this procedure.

Step 6 Click the **Save** button.

Step 7 Refresh the **Proxy Gateway Certificate** window to view the updated proxy gateway certificate data.
The information displayed in the **Proxy Gateway Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

Related Topics

Security and Cisco Network Plug and Play, on page 29

Managing PKI Certificates

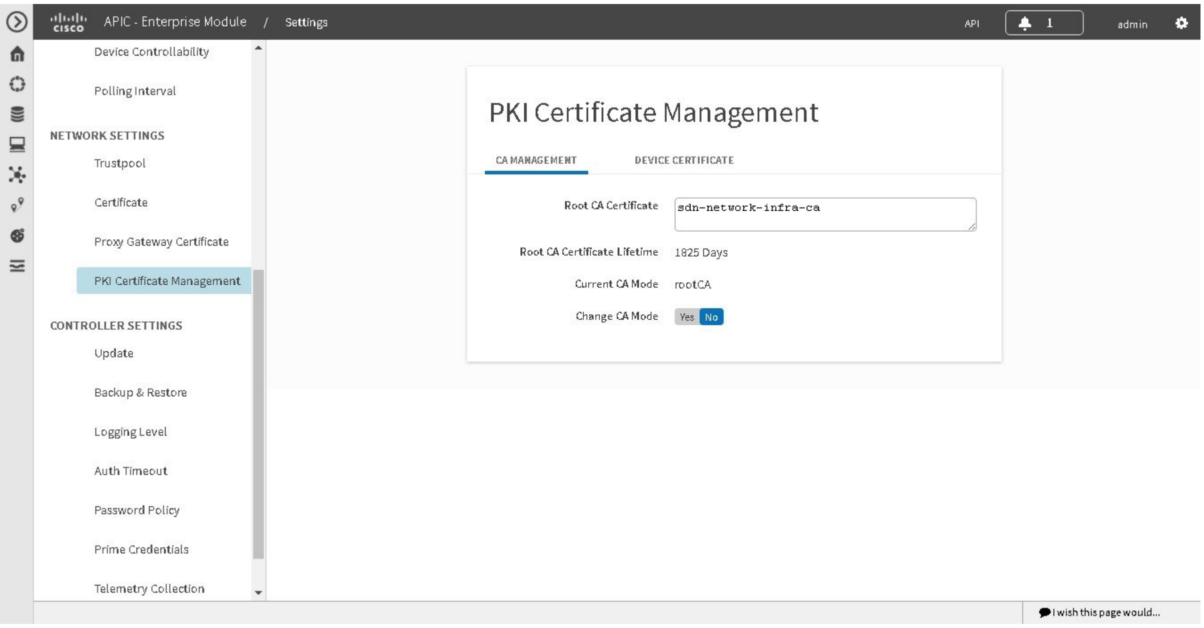
Configuring the Device Certificate Lifetime

The Cisco APIC-EM enables the user to change the certificate lifetime of network devices managed and monitored by the private (internal) controller's CA. The controller's default value for the certificate lifetime is 365 days. After the certificate lifetime value is changed using the controller's GUI, then any network devices subsequently requesting a certificate from the controller are assigned this lifetime value.

Note The device certificate lifetime value cannot exceed the CA certificate lifetime value. Additionally, if the remaining time of CA certificate lifetime is less than configured device's certificate lifetime, then the device will get a certificate lifetime value equal to the remaining CA certificate lifetime.

You change the device certificate lifetime using the **PKI Certificate Managment** window in the Cisco APIC-EM GUI.

Figure 10: PKI Certificate Management Window



PKI Certificate Management

CA MANAGEMENT | DEVICE CERTIFICATE

Root CA Certificate: sdn-network-infra-ca

Root CA Certificate Lifetime: 1825 Days

Current CA Mode: rootCA

Change CA Mode: Yes [✓ No]

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **PKI Certificate Management** to view the **PKI Certificate Management** window.

Step 4 Click the **Device Certificate** tab.

Step 5 Review the device certificate and current device certificate lifetime.

Step 6 In the **Device Certificate Lifetime** field, enter a new value in days.

Step 7 Click the **Apply** button.

What to Do Next

Refresh the **PKI Certificate Management** window to confirm the new device certificate lifetime value.

Related Topics

Device PKI Plane Modes, on page 21

Changing the Role of the PKI Certificate from Root to Subordinate

The Cisco APIC-EM permits the user to change the role of the Device PKI CA from a root CA to a subordinate CA.

When changing the private controller's CA from a root CA to a subordinate CA note the following:

- If you intend to have the controller act as a subordinate CA, then it is assumed that you already have a root CA (for example Microsoft CA) and you are willing to accept the controller as a subordinate CA.
- As long as the subordinate CA is not fully configured, then the controller will continue to operate as an internal root CA.
- You will need to generate a Certificate Signing Request (CSR) file for the controller (as described in this procedure) and manually have it signed by your external root CA.

  Note The controller will continue to run as an internal root CA during this time.

- Once the CSR is signed by the external root CA, then this signed file must be imported back into the controller using the GUI (as described below in this procedure).

  After the import, the controller will initialize itself as the subordinate CA and provide all the existing functionality of a subordinate CA.

- The switch over from internal root CA to subordinate CA is not automatically supported; therefore, it is assumed that no devices have yet been configured with the internal root CA. In case any devices are configured, then it is the responsibility of the network administrator to manually revoke the existing device ID certificates before switching to the subordinate CA.
- Note that there is no rollover provisioning for the subordinate CA, so for this reason we recommend that you choose the longest possible certificate lifetime for subordinate certificate, and not less than 2 years.
- There is no controller warning for expiration of the subordinate CA certificate.
- The subordinate CA certificate lifetime as displayed in the GUI is just read from the certificate itself; it is not computed against the system time. So if you install a certificate with a lifespan of one year today and then look at it in the GUI next July, then the GUI will still show that the certificate has a one year lifetime.
- The subordinate CA certificate should be in PEM format only.
- Due to a Cisco IOS XE crypto PKI import limitation, devices cannot import a PKCS bundle (made up of a device certificate, device key and the subordinate CA certificate) exceeding 4KB size. This problem occurs when the Cisco APIC-EM device PKI CA is changed to SubCA mode with a subordinate CA certificate that has several and/or lengthy X509 attributes defined, thereby increasing the size of the device PKCS bundle beyond 4KB. To circumvent this issue, get the subordinate CA certificate issued with very minimal attributes. For example, do not include CDP distribution and OCSP settings.

The following command output is provided as an example of content from a subordinate CA certificate that can impact the file size, as well as the fields within the certificate where content should be minimized:

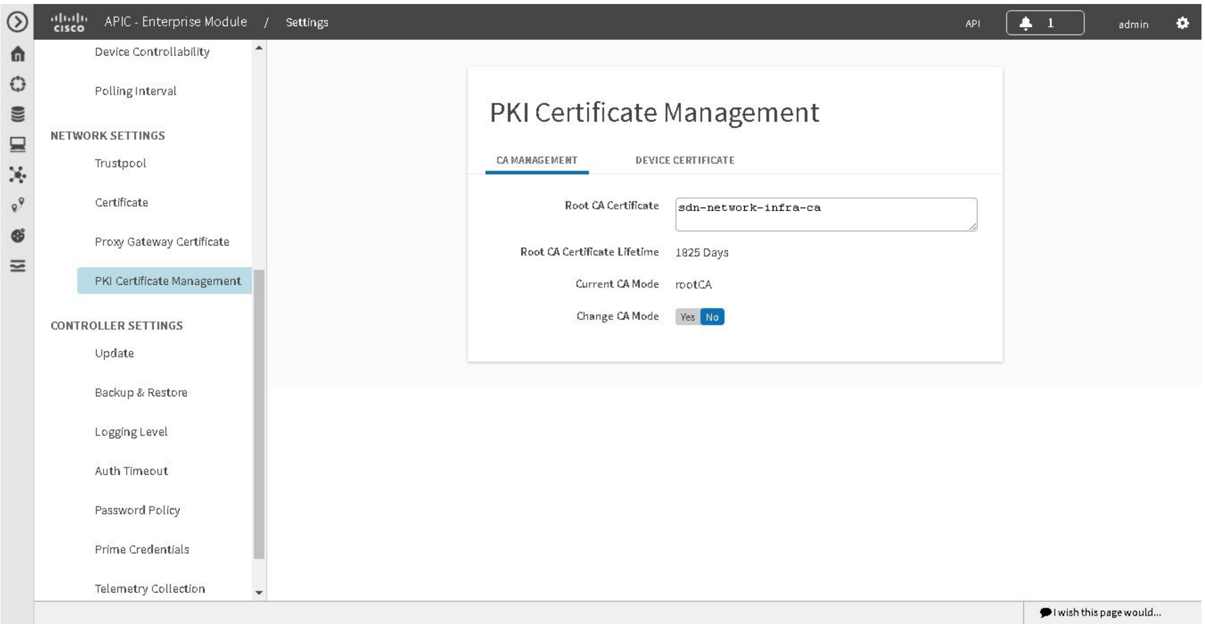
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2e:00:00:00:0e:28:d7:1f:24:a1:1e:ef:70:00:00:00:00:00:0e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=apic-em, CN=apic-em-CA
        Validity
            Not Before: Oct 18 19:56:54 2016 GMT
            Not After : Oct 19 19:56:54 2016 GMT
        Subject: CN=sdn-network-infra-subca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cd:a7:65:a4:c4:64:e6:e0:6b:f2:39:c0:a2:3b:
                    <snip>
                    85:a3:44:d1:a2:b3:b1:f5:ff:28:e4:12:41:d3:5f:
                    bf:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DD:FA:E4:A5:6A:3C:81:29:51:B2:17:ED:82:CE:AA:AD:91:C5:1D
            X509v3 Authority Key Identifier:
                keyid:62:6F:C7:83:42:82:5F:54:51:2B:76:B2:B7:F5:06:2C:76:59:7F:F8

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....#...I......^...Q...._...S..d...
    Signature Algorithm: sha256WithRSAEncryption
         18:ce:5b:90:6b:1d:5b:b4:df:fa:d3:8e:80:51:6f:46:0d:19:
```

- The subordinate CA does not interact with the higher CAs, so it will not be aware of any revocation of the certificates at a higher level. Due to this fact, any information about certificate revocation will also not be communicated from the subordinate CA to the network devices. Since the subordinate CA does not have this information, all the network devices will only use the subordinate CA as the CDP source.

You change the role of the private (internal) controller's CA from a root CA to a subordinate CA using the **PKI Certificate Managment** window in the Cisco APIC-EM GUI.

Figure 11: PKI Certificate Management Window



PKI Certificate Management

CA MANAGEMENT | DEVICE CERTIFICATE

Root CA Certificate: sdn-network-infra-ca

Root CA Certificate Lifetime: 1825 Days

Current CA Mode: rootCA

Change CA Mode: Yes [✓ No]

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

You must have a copy of the root CA certificate to which you will subordinate the private (internal) controller's PKI certificate.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **PKI Certificate Management** to view the **PKI Certificate Management** window.

Step 4 Click the **CA Management** tab.

Step 5 Review the existing root or subordinate CA certificate configuration information from the GUI.

Root CA Certificate	Displays current root CA certificate (either external or internal root CA certificate).

Root CA Certificate Lifetime	Displays the current lifetime value of the current root CA certificate in days.
Current CA Mode	Displays the current CA mode: root CA or subordinate CA.
Change to Sub CA mode	Button used to change from a root CA to subordinate CA.

Step 6 In the **CA Management** tab, for **Change to Sub CA mode** click **Yes**.

Step 7 In the **CA Management** tab, click **Next**.

Step 8 Review the **Root CA to Sub CA** warnings that appears:

- Changing from root CA to subordinate CA is a process that cannot be reversed.
- You must ensure that no network devices have been enrolled or issued a certificate in root CA mode. Any network devices accidently enrolled in root CA mode must be revoked before changing from root CA to subordinate CA.
- Network devices must come online only after this subordinate CA configuration process is finished.

Step 9 Click **OK** to proceed.
The **PKI Certificate Management** window changes and displays an **Import External Root CA Certificate** field.

Step 10 Drag and drop your root CA certificate into the **Import External Root CA Certificate** field and click **Upload**.
The root CA certificate will then be uploaded into the controller and used to generate a Certificate Signing Request (CSR).

When the upload process is finished a **Certificate Uploaded Successfully message** appears.

Step 11 After the upload process is finished and the success message appears, click **Next** to proceed.
The controller will then generate and display the CSR.

Step 12 View the controller generated Certificate Signing Request (CSR) in the GUI and perform one of the following actions:

- Click the **Download** link to download a local copy of the CSR file.

  You can then attach this CSR file to an email to send to your root CA.

- Click the **Copy to the Clipboard** link to copy the CSR file's content.

  You can then paste this CSR content to an email or attachment to an email and send to your root CA.

Step 13 Send the CSR file to your root CA.
You must send the CSR file to your root CA. Your root CA will then return to you a subordinate CA file that you must import back into the controller.

Step 14 After receiving the subordinate CA file from your root CA, access the controller's GUI again and return to the **PKI Certificate Management** window.

Step 15 Click the **CA Management** tab.

Step 16 Click **Yes** for the **Change CA mode** button in the **CA Management** tab.
After clicking **Yes**, the GUI view with the CSR is displayed.

Step 17 Click **Next** in the GUI view with the CSR being displayed.
The **PKI Certificate Management** window changes and displays an **Import Sub CA Certificate** field.

Step 18 Drag and drop your subordinate CA certificate into the **Import Sub CA Certificate** field and click **Apply**.
The subordinate CA certificate will then be uploaded into the controller.

After the upload finishes, the GUI window changes to display the subordinate CA mode in the **CA Management** tab.

Step 19 Review the fields in the **CA Management** tab.

Sub CA Certificate	Displays current subordinate CA certificate.
External Root CA Certificate	Displays Root CA certificate.
Sub CA Certificate Lifetime	Displays the lifetime value of the subordinate CA certificate in days.
Current CA Mode	Displays SubCA mode.

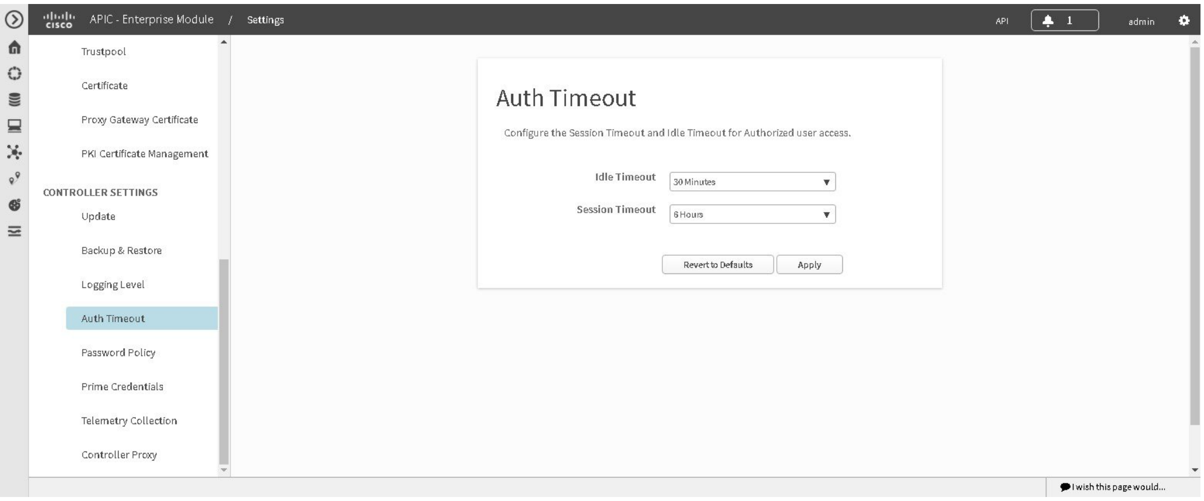
Related Topics

Device PKI Plane Modes, on page 21

Configuring the Authentication Timeout

You can configure authentication timeouts that require the user to log back into the controller with their credentials (username and password) using the **Authentication Timeout** window in the Cisco APIC-EM GUI.

Figure 12: Authentication Timeout Window



Auth Timeout

Configure the Session Timeout and Idle Timeout for Authorized user access.

Idle Timeout: 30 Minutes

Session Timeout: 6 Hours

The following authentication timeout values can be configured:

- Idle timeout—Time interval that you can configure before the controller requires re-authentication (logging back in with appropriate credentials) due to Cisco APIC-EM inactivity. Idle timeouts are API-based, meaning that idle timeout is the time the controller is idle between API usages and not GUI mouse clicks or drags.
- Session timeout—Time interval that you can configure before the controller requires re-authentication (logging back in with appropriate credentials). This is a forced re-authentication.

Note Approximately 2-3 minutes before your session is about to idle timeout, a pop-up warning appears in the GUI stating that your session is about to idle timeout and asking if you wish to continue with the current session. Click **Cancel** to ignore the warning and idle timeout of the session within approximately 2-3 minutes. Click **OK** to continue the session for another 30 minutes.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Authentication Timeout** to view the **Authentication Timeout** window.

Step 4 (Optional) Configure the idle timeout value using the **Idle Timeout** drop-down menu.
You can configure the idle timeout value in increments of 5 minutes, up to an hour. The default value is 30 minutes.

Step 5 (Optional) Configure the session timeout value using the **Session Timeout** drop-down menu.
You can configure the session timeout value in increments of 30 minutes, up to 24 hours. The default value is six hours.

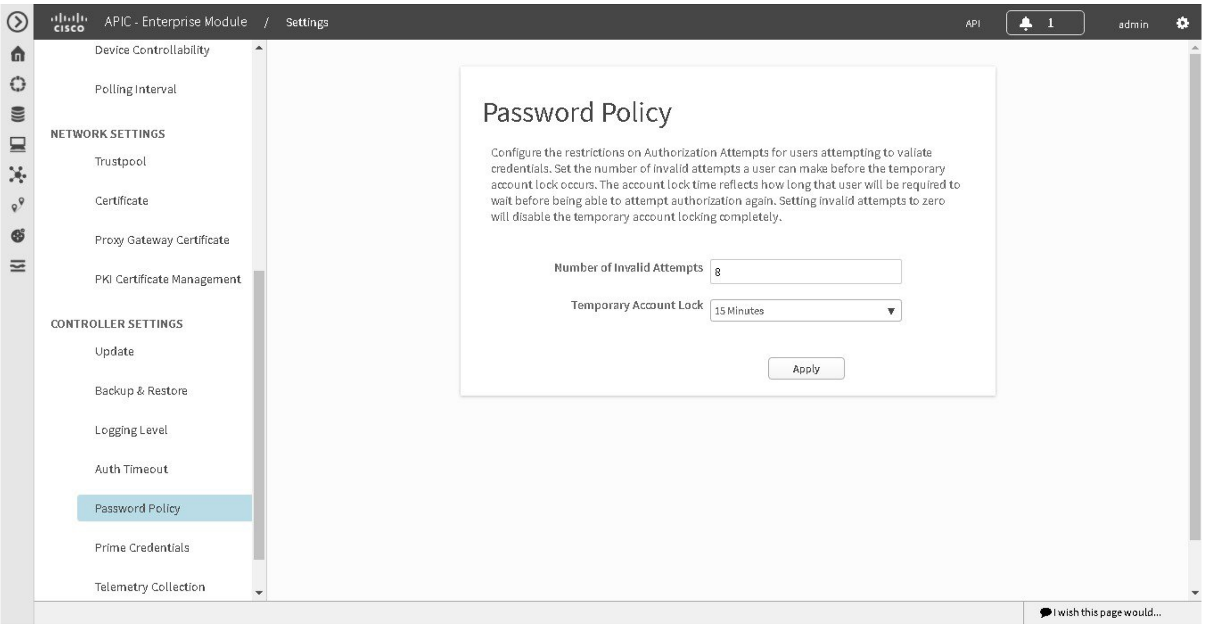
Step 6 Click the **Apply** button to apply your configuration to the controller.
To restore the authentication timeout defaults to the controller, click the **Revert to Defaults** button.

Configuring Password Policies

As an administrator, you can control the number of consecutive, invalid user login attempts to the Cisco APIC-EM. Once a user crosses the threshold set by you as administrator, the user's account is locked and access is refused. Additionally, as an administrator, you can also configure the length of time that the user account is locked. The user account will remain locked until the configured time period expires.

You configure these controller access parameters for the Cisco APIC-EM using the **Password Policy** window.

Figure 13: Password Policy Window



Password Policy

Configure the restrictions on Authorization Attempts for users attempting to valiate credentials. Set the number of invalid attempts a user can make before the temporary account lock occurs. The account lock time reflects how long that user will be required to wait before being able to attempt authorization again. Setting invalid attempts to zero will disable the temporary account locking completely.

Number of Invalid Attempts: 8

Temporary Account Lock: 15 Minutes

The following password policy functionality is supported:

- As an administrator, you can set the number of consecutive, invalid user login attempts to the controller. These consecutive, invalid user login attempts can be set from 0 to 10 attempts, with 8 attempts being the default value. Setting invalid attempts to 0 will disable the feature of locking a user with invalid password attempts.
- As an administrator, you can set the length of time a user account is locked. Permitted lock time intervals for a user account range from 1-3600 seconds, with 900 seconds being the default value.
- When a user account is locked due to the number of consecutive, invalid login attempts, entering correct credentials will still result in a login failure until the expiration of the configured lock out time period.
- An administrator can unlock the user account at any time.

  We recommend that you create at least two administrator accounts for your deployment. With two administrator accounts, if one account is locked for whatever reason then the other account can be used to unlock that locked account.

  Note For information about how to unlock a user account, see the Chapter 4, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

- A locked user account is unlocked when the configured lock out time period expires.
- A user account can never be permanently locked, but to deny access permanently, an administrator can delete the account.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Password Policy** to view the **Password Policy** window.

Step 4 (Optional) Configure the number of permitted consecutive, invalid password attempts by choosing from the **Number of Invalid Attempts** drop-down menu.

Step 5 (Optional) Configure the time interval for locking a user account by choosing from the **Temporary Account Lock** drop-down menu.

Step 6 Click the **Apply** button to apply your configuration to the controller.

Related Topics

Password Requirements, on page 34

CHAPTER 3

Managing Users

About Role Based Access Control

Cisco APIC-EM allows you to define a user profile by role and Role-Based Access Control (RBAC) scope. The role defines the actions that a user may perform, and the RBAC scope defines the resources that a user may access. Currently, devices are the only resources that can be assigned to an RBAC scope.

A user who is assigned a role (for example, ROLE_ADMIN) and scope ALL permissions may perform the full range of actions of the role to the entire scope. However, if this same user is limited to only a subset of devices, the range of actions change, depending on the application (Discovery, EasyQoS, Path Trace, etc.). For detailed application behavior based on limited RBAC scope, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

User Profiles

A user profile defines a user's login, password, role (permissions) and RBAC scope (resource access).

User profiles can exist on the Cisco APIC-EM controller or on an external AAA server. Both of the following types of profiles can coexist for any user:

- Internal user profile: resides on the Cisco APIC-EM controller.
- External user profile: resides on an external AAA server.

The default user profile that is created when the Cisco APIC-EM is deployed has administrator role (ROLE_ADMIN) permissions and access to all resources (RBAC scope ALL). In turn, this user can create other user profiles with various roles and RBAC scopes, including user profiles with ROLE_ADMIN and RBAC scope ALL permissions (a user with global RBAC scope) or with ROLE_ADMIN and RBAC scope set to a specific group (user with partial RBAC scope).

You can view external user profiles which includes a username and their authorization on the controller. You view external user profiles and their roles in the **External Users** window. The authorization for the user consists of an RBAC scope and role in that RBAC scope.

For information about configuring internal users, see Creating Internal Users, on page 73. For information about configuring external controller authentication, see Configuring External AuthenticationConfiguring External User Profiles, on page 79.

About User Roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- Administrator (ROLE_ADMIN)
- Policy Administrator (ROLE_POLICY_ADMIN)
- Observer (ROLE_OBSERVER)
- Installer (ROLE_INSTALLER)

When you deploy the Cisco APIC-EM for the first time, the configuration wizard prompts for a username and password. This first-time user is given full administrative (read and write) permissions for the controller and access to all resources. This user is able to create user profiles for other users.

Note Only users with the administrative role (ROLE_ADMIN) can create users profiles. These users can have RBAC scope set to ALL (user with global RBAC scope) or set to a specific group (user with partial RBAC scope).

Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges and SCOPE: ALL. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

Administrator Role

A user's access to Cisco APIC-EM functionality is determined both by its role and the RBAC scope that it is assigned. In general, the administrator role has full read/write access to all of the Cisco APIC-EM functions:

- User and group settings

  Note For security reasons, passwords are not displayed to any user, not even those with administrator privileges.

Note Although an administrator cannot directly change another user's password in the GUI, an administrator can delete and then re-create the user with a new password using the GUI.

- Discovery credentials and Discovery

Note Only users with access to all resources (RBAC scope set to ALL) can define discovery credentials and perform discovery.)

- Inventory
- Topology
- Path Trace
- EasyQoS (create, modify, and deploy QoS policies to devices)
- System-wide controller-administration functions, such as Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Prime Credentials, Telemetry Collection and Controller Proxy)
- App Management
- System Administration
- Audit Logs
- APIs

Depending on the user's RBAC scope, the administrator's role is impacted as follows:

- With access to all resources (RBAC scope set to ALL), the user can perform all of the administrator functions listed above to all resources.
- With access to a subset of resources (RBAC scope set to **Custom** with resource groups assigned), the user can perform all of the administrator functions listed above, but only to the resources assigned in the RBAC scope, with the following exceptions:
    - Users cannot define discovery credentials or perform discovery.
    - Users can create new users and assign RBAC scopes to them, but they can only assign the RBAC scopes for which they have administrative roles. They can delete only the users that they have created.

Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges and SCOPE: ALL. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

Policy Administrator Role

A user's access to Cisco APIC-EM functionality is determined both by its role and the RBAC scope that it is assigned. In general, the policy administrator role has full read/write access to the following functions:

- Change Password
- Discovery Credentials and Discovery

> **Note** Only users with access to all resources (RBAC scope set to ALL) can define discovery credentials and perform discovery.)

- Inventory
- Topology
- Path Trace
- EasyQoS (create, modify, and deploy QoS policies to devices)
- Prime Credentials
- Policy administration APIs

Depending on the user's RBAC scope, the policy administrator's role is impacted as follows:

- With access to all resources (RBAC scope set to ALL), the user can perform all of the policy administrator functions listed above for all resources.
- With access to a subset of resources (RBAC scope set to **Custom** with resource groups assigned), the user can perform all of the functions listed above (except define discovery credentials and perform discovery), but only for the resources assigned in the RBAC scope.

This role cannot access system-wide controller-administration functions, such as Users and Groups (except to change its own password), Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Telemetry Collection and Controller Proxy.)

Observer Role

A user's access to Cisco APIC-EM functionality is determined both by its role and the RBAC scope that it is assigned. With the exception of being able to change their own password, users with the observer role have read-only access (ability to view but not make any changes) to the following functions:

- Discovery Results
- Inventory
- Topology
- Path Trace
- EasyQoS

- System-wide controller-administration functions, such as Network Settings (Trustpool, Controller Certificate, Proxy Certificate) and Controller Settings (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Prime Credentials, Telemetry Collection and Controller Proxy)
- App Management
- System Administration
- Audit Logs
- APIs

Depending on the user's RBAC scope, the observer's role is impacted as follows:

- With access to all resources (RBAC scope set to ALL), the user can view all of the functions listed above for all resources.
- With access to a subset of resources (RBAC scope set to **Custom** with resource groups assigned), the user can view all of the functions listed above (except discovery credentials and discoveries), but only for the resources assigned in the RBAC scope.

Installer Role

Users who are assigned the installer role (ROLE_INSTALLER) can use the Cisco Plug and Play Mobile application to access the Cisco APIC-EM remotely to perform the following functions:

- View device status.
- Trigger device deployments.

Installers cannot access the Cisco APIC-EM GUI. As such, they are not bound by an RBAC scope.

Note For security reasons, passwords are not displayed to any user, not even those with administrator privileges.

Resource Groups

In Cisco APIC-EM, you create groups to contain related resources. Then, you assign the groups to users to provide them access to the resources in the group. You may only create groups that contain the resources (or a subset of resources) to which you have access. Currently, devices are the only resources that can be assigned to a group.

Keep the following guidelines in mind when creating resource groups:

- Only users with ROLE_ADMIN can define resource groups. A user with ROLE_ADMIN and access to all resources (RBAC scope set to ALL) can create resource groups that contain any or all of the available resources. A user with ROLE_ADMIN and access to only certain resources can create resource groups that only contain the same devices that the user has access to. Users cannot create resource groups that contain resources that they do not have access to.
- A resource group cannot contain another resource group.

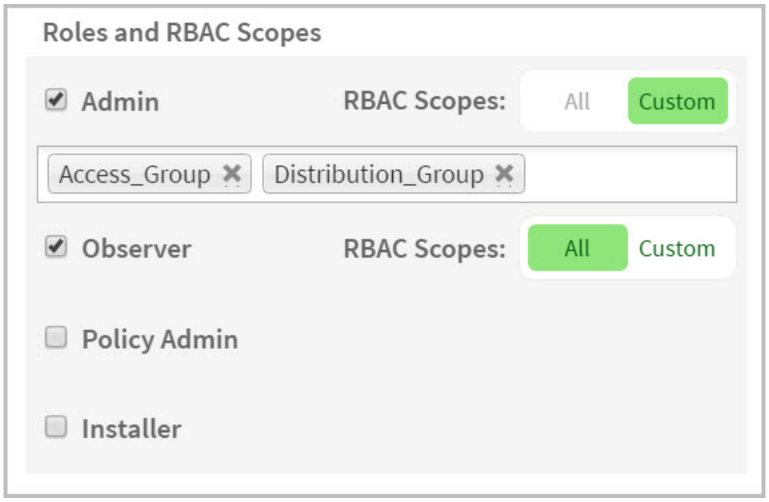
RBAC Scopes

The RBAC scope defines the resources that a user may access. Currently, devices are the only type of resource that can be assigned to an RBAC scope.

When you create a user profile, you can configure one or more user roles for the user. Each user role that you define is assigned a corresponding RBAC scope. The RBAC scope can be all of the resources (RBAC scope set to ALL) or it can be a limited set of resources (RBAC scope set to Custom). When you define a custom RBAC scope, you then need to assign resource groups to it.

For example, in the following figure, the Admin role has been assigned a custom RBAC scope, and the RBAC scope consists of two groups: Access_Group and Distribution_Group. This means that the user can perform all administrative functions to the devices in the Access_Group and Distribution_Group. The Observer role has been assigned the RBAC scope of ALL. This means that the user can view all of the devices in the Cisco APIC-EM.

Figure 14: Example of RBAC Scope Assignment



Roles and RBAC Scopes

☑ Admin RBAC Scopes: All [✓ Custom]

Access_Group ✕ Distribution_Group ✕

☑ Observer RBAC Scopes: [✓ All] Custom

☐ Policy Admin

☐ Installer

Keep the following guidelines in mind when defining RBAC scopes for users:

- A user can have only one role in a given RBAC scope.
- If a user is assigned a role for one RBAC scope and a different role for another RBAC scope, and the RBAC scopes have some resource groups in common, the user is given the higher privileged access to the common devices. For example, a user is assigned ROLE_ADMIN for group G1 and ROLE_OBSERVER for group G2. Groups G1 and G2 have device D1 in common. (The device is in both groups.) This situation results in the user being given ROLE_ADMIN privileges for device D1.
- Users who are working with the Cisco IWAN and Cisco Network PnP applications to monitor and manage devices and hosts must have their **RBAC Scopes** values set to **All**. The Cisco IWAN and Cisco Network PnP applications do not support **Custom** RBAC scopes.

Application Behavior Based on Role and RBAC Scope

A user who is assigned a role (for example, ROLE_ADMIN) and an RBAC scope set to ALL may perform the full range of the role's functions to all of the resources. However, if this same user is assigned a limited RBAC scope, the range of functions change, depending on the application. See the following table for a list of applications and the impact of a user's role and RBAC scope on the functions that they can perform.

For detailed application behavior based on limited RBAC scope, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Table 8: Application Behavior Based on Role and RBAC Scope

Function	Role	Full RBAC Scope	Limited RBAC Scope
Settings (Gear icon) menu			
Settings (Gear icon): • Settings • App Management • System Administration • Audit Logs • Change Password	Admin	Users can perform all of these functions.	Users can only change their own password.
	Policy Admin	Users have access to only these functions: Settings, Audit Logs, and Change Password. See **Discovery Credentials** and **Controller Settings** in this table for details about the functions that a policy admin can perform.	Users have access to only these functions: Settings, Audit Logs, and Change Password. See **Users and Groups** in this table for details about the functions that a policy admin with a limited RBAC scope can perform.
	Observer	Users have access to only these functions: Audit Logs, and Change Password.	Users have access to only these functions: Audit Logs, and Change Password.
Settings			
Users and Groups: • Change Password • Internal Users • External Users • External Authentication • Groups	Admin	Users can perform all of these functions	Users can create and edit internal users, external users, and groups, but they cannot configure external authentication.
	Policy Admin Observer	Users do not have permission to perform these functions.	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Discovery Credentials: • CLI Credentials • SNMPv2c • SNMPv3 • SNMP Properties • Device Controllability	Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Policy Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.
Network Settings: • Trustpool • Certificate • Proxy Gateway Certificate • PKI Certificate Management	Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Policy Admin	Users do not have permission to perform these functions.	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.
Controller Settings: • Update • Backup and Restore • Logging Level • Auth Timeout • Password Policy • Prime Credentials • Telemetry Collection • Controller Proxy	Admin	Users can perform all of these functions	Users do not have permission to perform these functions.
	Policy Admin	Users can configure only the logging level, prime credentials, and telemetry collection.	Users do not have permission to perform these functions.
	Observer	Users do not have permission to view these functions.	Users do not have permission to view these functions.
Discovery			

Function	Role	Full RBAC Scope	Limited RBAC Scope
Discovery Credentials Discovery Jobs Discovery Results	Admin Policy Admin	Users can define discovery credentials and create discovery jobs. **Note** Once saved, discovery credentials are not visible to any user. Users can also view discovery results.	Only users with access to all resources (RBAC scope set to ALL) can define discovery credentials, perform discovery and view discovery results. **Note** Once saved, discovery credentials are not visible to any user.
	Observer	Users can view discovery results.	Users cannot view discovery results. Only users with access to all resources (RBAC scope set to ALL) can view discovery results.
Device and Host Inventory			
Device Roles	Admin Policy Admin	Users can change device roles for all devices.	Users can change device roles, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's scope are not displayed.
	Observer	Users can view device roles for all devices but cannot make any changes.	Users can view device roles, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are not displayed.
Device Tags Policy Tags Location Tags and Markers	Admin Policy Admin	Users can create and change device tags, policy tags, and location tags and markers for all devices.	Users can create and change device tags, policy tags, and location tags and markers, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's scope are not displayed.
	Observer	Users can view device and policy tags for all devices but cannot make any changes.	Users can view device and policy tags, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are not displayed.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Config Display	Admin Policy Admin Observer	Users can view configuration files for all devices and hosts.	Users can view configuration files, however only for the devices defined in their custom RBAC scope. Resources that are not in the user's scope are not displayed.
Topology			
Topology Map Topology Map Layout Saving Topology Map Layout	Admin Policy Admin	Users can view all devices on the topology map, and they can change and save the topology map layout.	Users can view the topology map, and they can change and save the topology map layout. The full network topology is shown. However, resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed.
	Observer	Users can view all of the devices on the topology map but cannot save a changed topology map layout.	Users can view all of the devices on the topology map, but details are displayed only for the resources defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed. Users cannot save a changed topology map layout.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Device Roles Device Tags Policy Tags	Admin Policy Admin	Users can view and change device roles, device tags, and policy tags for all devices.	Users can view and change device roles, device tags, and policy tags, however only on the resources defined in their custom RBAC scope. The full network topology is shown. However, resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed.
	Observer	Users can view all of the devices on the topology map but cannot change the topology map layout.	Users can view all of the devices on the topology map but cannot change the topology map layout. However, details are displayed only for the resources defined in their custom RBAC scope. Resources that are not in the user's RBAC scope are dimmed and labeled as unauthorized. No information or only basic information about the dimmed resources is displayed.
EasyQoS			

Function	Role	Full RBAC Scope	Limited RBAC Scope
Policy Scopes	Admin Policy Admin	Users can view and create policy scopes. When displaying policy scopes, users can view all devices in policy scopes.	Users can create policy scopes, however they can only contain devices that are in their custom RBAC scope. When displaying policy scopes, users can view only the resources defined in their RBAC scope. Resources that are not in the user's RBAC scope are dimmed and shown as locked.
	Observer	Users can view all of the policy scopes. When displaying policy scopes, users can view all devices in policy scopes.	Users can view EasyQoS information, however only for the resources defined in their custom RBAC scope. Users can view information about only the devices defined in their RBAC scope. Devices that are not in the user's RBAC scope are locked and labeled as unauthorized.
Application Registry	Admin Policy Admin	Users have the full application registry functionality. Users can view the applications in the registry, including details about each application, and they can sort the display of applications. They can mark applications as favorites, create custom applications, and edit both custom and NBAR (default) applications.	Users can view the applications in the registry, including details about each application, and they can sort the display of applications. They cannot mark applications as favorites or create custom applications. They cannot edit custom or NBAR (default) applications.
	Observer	Users can view the applications in the registry, including details about each application, and they can sort the display of applications.	Same as an observer with full RBAC scope.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Policies (create, abort, restore, preview, reset, apply, clone, show history for, and delete)	Admin Policy Admin	Users can perform all of the policy-related functions.	Users can perform all of the policy-related functions, but only on policies whose policy scopes contain devices defined in the user's custom RBAC scope. If a policy's policy scope contains any devices that are not in the user's custom RBAC scope, the user will not be allowed to perform any functions on that policy. The policy will be locked and will indicate that the user does not have permission to perform any functions to the policy. A user can view policies whether or not they contain devices in the user's RBAC scope. If a policy contains devices that are not in the user's RBAC scope, the devices details are not displayed. The device is locked and labled as an unauthorized device.
	Observer		Same behavior as an observer with full RBAC scope.

Function	Role	Full RBAC Scope	Limited RBAC Scope
		Users can view all of the policy-related functions, but only on policies whose policy scopes contain devices defined in their custom RBAC scope. If a policy's policy scope contains any devices that are not in the user's custom RBAC scope, the user will not be allowed to perform any functions on that policy. The policy will be locked and will indicate that the user does not have permission to modify the policy. A user can view policies whether or not they contain devices in the user's RBAC scope, but the devices details are not displayed. The device is locked and labeled as an unauthorized device.	
Bandwidth Profile	Admin Policy Admin	Users can create, edit, and delete custom bandwidth profiles for all resources.	Users can only view custom bandwidth profiles.
	Observer	Users can only view custom bandwidth profiles.	Users can only view custom bandwidth profiles.
SP Profile	Admin Policy Admin	Users can create custom SP profiles and edit existing SP profiles for all resources.	Users can view the existing NBAR and custom SP profiles for resources that are in their custom scope, but cannot edit them.
	Observer	Users can view the existing NBAR and custom SP profiles for all resources, but cannot edit them.	Users can view the existing NBAR and custom SP profiles for all resources, but cannot edit them.

Function	Role	Full RBAC Scope	Limited RBAC Scope
Dynamic QoS	Admin Policy Admin	Users can enable and disable dynamic QoS and view dynamic QoS troubleshooting information about all devices.	Users can enable and disable dynamic QoS and view dynamic QoS troubleshooting information about all devices.
	Observer	Users cannot enable or disable dynamic QoS. However, they can view dynamic QoS information about all devices.	Users cannot enable or disable dynamic QoS. However, they can view dynamic QoS information about all devices.
Path Trace			
Basic Path Trace ACL Path Trace Path Trace with QoS, interface, device, and performance monitor statistics	Admin Policy Admin	Users can perform all types of path traces on all resources.	Users can perform ACL traces and traces that gather QoS, interface, device and performance monitor statistics, however, only for the resources defined in their RBAC scope. When the results of a path trace are displayed, the resources that are not in the user's RBAC scope are locked and labeled as unauthorized.
	Observer	Users can perform ACL traces and traces that gather QoS, interface, and device statistics. However, they are unable to perform path traces that gather Performance Monitor statistics. Performance Monitor traces require performance monitoring to be enabled for all flows on all network devices in the path, and an observer does not have permission to make changes on devices.	Users can perform ACL traces and traces that gather QoS, interface, and device statistics. However, they are unable to perform path traces that gather Performance Monitor statistics. Performance Monitor traces require performance monitoring to be enabled for all flows on all network devices in the path, and observers do not have permission to make changes or to access all devices. When the results of a path trace are displayed, the resources that are not in the user's RBAC scope are locked and labeled as unauthorized.
Cisco IWAN			

Function	Role	Full RBAC Scope	Limited RBAC Scope
All Cisco IWAN functions	Admin	Users can perform the full range of functions for all devices.	Not applicable.
	Policy Admin Observer	Not applicable.	Not applicable.
Cisco Network PnP			
All Cisco Network PnP functions	Admin	Users can perform the full range of functions for all devices.	Not applicable.
	Policy Admin Observer	Not applicable.	Not applicable.

About Authentication and Authorization

Users and their roles are subject to an authentication and authorization process.

Note Currently, Cisco APIC-EM supports authentication and authorization. Accounting is not yet supported.

With the Cisco APIC-EM, each resource for the controller is mapped to an action and each action is mapped to a required permission for a user. All REST APIs are therefore protected by the controller authentication process.

You can configure the following types of authentication for user access to the Cisco APIC-EM:

- Internal—Local controller authentication based upon the usernames and passwords created using the controllers's own GUI. For information about configuring internal users, see Creating Internal Users, on page 73.
- External—External controller authentication based upon the usernames and passwords that exist on other AAA servers. For information about configuring external controller authentication, see Configuring External AuthenticationConfiguring External User Profiles, on page 79.

When performing user authentication, the controller attempts to authenticate the user in the following order:

1. Authenticate with AAA server directory credentials using the RADIUS protocol (number of times attempted per user configuration using the GUI or APIs)
2. Authenticate with the user credentials that are configured locally on the controller (number of times attempted per user configuration using the controller GUI)

If the user credentials are authenticated in any of the above steps, then controller access is immediately granted.

Configuring Internal User Profiles

Configuring Groups for User Access

The Cisco APIC-EM supports the configuration of groups.

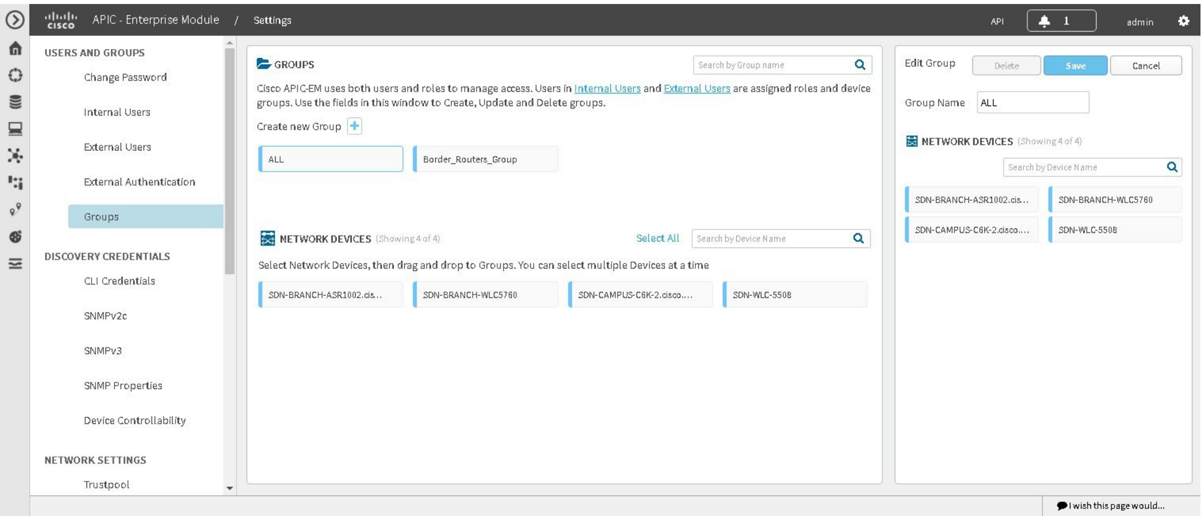
A group is a named entity that represents a specific set of resources for access-control purposes. You assign users to groups using RBAC scope. Assigning a user to a group with RBAC scope enables that user to access the resources in that group; if the user is not assigned to a particular group, the user cannot access the resources in that group. In the current release, groups can contain network devices only; hosts or other resources cannot belong to groups.

Note Hosts and wireless access points (only Cisco Unified access points) cannot be added to a specific group using the GUI. They are added to a group automatically when linked to a wireless LAN controller (WLC) or switch that is added to a group using the GUI.

You can configure groups using the **Groups** window in the Cisco APIC-EM GUI.

Note Hosts and wireless access points (Unified access points only) cannot be added to a group. Instead, they are automatically added to a group when the switch or wireless LAN controller to which the host or wireless access point is connected is added to the group.

Figure 15: Configuring Groups Window



Cisco APIC-EM uses both users and roles to manage access. Users in Internal Users and External Users are assigned roles and device groups. Use the fields in this window to Create, Update and Delete groups.

ALL | Border_Routers_Group

Select Network Devices, then drag and drop to Groups. You can select multiple Devices at a time

SDN-BRANCH-ASR1002.cis... | SDN-BRANCH-WLC5760 | SDN-CAMPUS-C6K-2.cisco.... | SDN-WLC-5508

Group Name: ALL

NETWORK DEVICES (Showing 4 of 4)

SDN-BRANCH-ASR1002.cis... | SDN-BRANCH-WLC5760
SDN-CAMPUS-C6K-2.cisco.... | SDN-WLC-5508

Important Both internal and external users can be configured for group access using RBAC scope. You configure RBAC scope for internal users with the controller's GUI using the **Internal Users** page. You configure RBAC scope for external users on the AAA server itself.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

You must have successfully performed a discovery, with the resulting discovered devices appearing in the controller's **Inventory** window.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Groups** to view the **Groups** window.
The **Groups** window is divided into three fields.

Groups	Provides an addition icon where you can begin to create a group. After creating a group, it appears in this **Groups** field. A **Search by Group name** field permits you to enter a Group name and only display that group in this field.
Network Devices	Displays the discovered devices from your network. A **Search by Device name** field permits you to enter a device name to only display that device in this field. You add devices to a group by dragging and dropping a device from the **Network Devices** field directly onto a group in the **Groups** field. **Note** There are two possible controller GUI views for **Network Devices** based upon the user's role and scope (ADMIN with Scope ALL access or ADMIN with non-global scope access). An ADMIN with Scope ALL access is able to view the total number of devices, including any unassigned devices. An ADMIN with non-global scope access is only able to view the assigned devices.

Groups Overview	Displays total number of groups, discovered devices assigned to groups, and devices not assigned to groups. Clicking on a specific group in the **Groups** field provide options to delete, edit and save, or cancel (exit) the group. A **Search by Device name** field permits you to enter a device name to only display that device in this field. Clicking on a device provides the following information: • Name—Name of the discovered device. • IP address——IP address of the discovered device. • Family—Generic family name, for example "Routers" or "Wireless Controller". • Type—Specific type of device, for example," Cisco 3945 Integrated Services Router G2" • Device Tags—Tags applied to the device in the **Inventory** or **Topology** windows.

Step 4 Click the addition icon in the **Groups** field.

Step 5 Enter a name for the new group in the **Group Name** field that appears.

Step 6 Click the green checkmark to create and save the new group.

Step 7 Drag and drop any network device icons from the **Network Devices** field to the new group icon in the **Groups** field. Dragging and dropping the network device icon to the new group icon will add that device to the new group.

You can also click on several network device icons in the **Network Devices** field to first form a selection of devices, and then drag and drop the entire selection of devices to the group icon to form the new group.

Note When creating an RBAC scope, the hosts and wireless access points that are associated with the selected network devices are also added to that RBAC scope.

Step 8 Continue creating groups and adding devices for your network.

What to Do Next

After configuring groups containing the appropriate devices for your network, access the **Internal Users** window. In this window, you assign group access permissions with the **RBAC Scope** field.

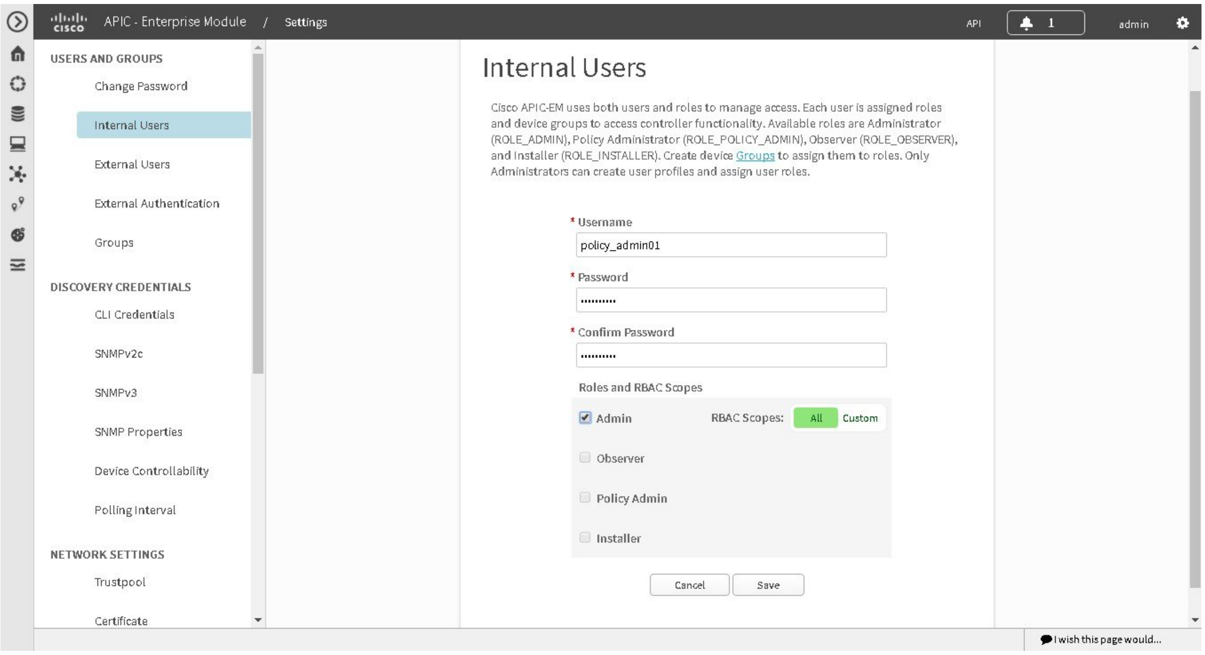
Creating Internal Users

You can create an internal user for the Cisco APIC-EM.

Note User information (credentials) is stored in a local database on the controller.

Note We highly recommend that you configure at least two users with administrator (ROLE_ADMIN) privileges and SCOPE: ALL. In the unlikely event that one user is locked out or forgets his or her password, you have another user with administrative privileges who can help you to recover from this situation.

Figure 16: Internal Users Window



Internal Users

Cisco APIC-EM uses both users and roles to manage access. Each user is assigned roles and device groups to access controller functionality. Available roles are Administrator (ROLE_ADMIN), Policy Administrator (ROLE_POLICY_ADMIN), Observer (ROLE_OBSERVER), and Installer (ROLE_INSTALLER). Create device Groups to assign them to roles. Only Administrators can create user profiles and assign user roles.

* Username: policy_admin01

* Password: ....

* Confirm Password: ....

Roles and RBAC Scopes

☑ Admin RBAC Scopes: [✓ All] Custom

☐ Observer

☐ Policy Admin

☐ Installer

Cancel Save

Before You Begin

You must have administrator (ROLE_ADMIN) permissions, as well as RBAC scope configured to all groups (global RBAC scope) or a specific subset of groups (non-global RBAC scope).

You must have configured the appropriate groups for the network devices using the **Groups** window in the controller's GUI.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Internal Users** to view the **Internal Users** window.

Step 4 Click **Create User**.

Step 5 In the **Create User** fields that now appear, you need to enter the username, password (twice), and role and group of the new user.

Step 6 Enter the username.

Step 7 Enter the password twice.

Step 8 Click the appropriate role for the user.

Step 9 Click the appropriate **RBAC Scope** for the user (either **All** or click and then select a **Custom** RBAC Scope).

The **ALL** option in the **RBAC Scopes** field contains all devices discovered by the controller.

Prior to configuring an internal user, set up RBAC scopes using **Groups** in the controller's GUI.

Step 10 Click **Save** to save the user configuration.
The **Users** window is displayed with the following information about the users:

- **Username—**Username assigned to the user.
- **Actions—**Icons that allow you to edit user information or delete a user.

What to Do Next

Proceed to configure any other internal users for your network devices. If necessary, configure external authentication for any external users for your network devices using the **External Authentication** window in the controllers' GUI.

Deleting a User

A user with the administrator role (ROLE_ADMIN) can delete a user from the Cisco APIC-EM.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information about the users:

- **Username—**Username assigned to the user.
- **Role—**Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope—**Domain or tenancy that the user is allowed to access. In this release, the scope is set to ALL and cannot be changed.
- **Actions—**Icons that allow you to edit user information or delete a user.

Step 3 Locate the user that you want to delete and, in the **Actions** column, click the **Delete** icon.
The user is deleted from the Cisco APIC-EM database and is unable to access the controller.

Note You cannot delete the default administrative user. The Cisco APIC-EM requires at least one administrative user who can log into the controller.

Viewing and Editing User Information

You can view and change user information.

Note User information (credentials) is stored in a local database on the controller.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information about the uses:

- **Username—**Username assigned to the user.
- **Role—**Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope—**Resources that the user is allowed to access.
- **Actions—**Icons that allow you to edit user information or delete a user.

Step 3 If you want to edit a user's information, from the **Actions** column, click the **Edit** icon.
The username and scope are configured by default so you cannot change their settings. However, you can change the role setting. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.

Step 4 When you are finished editing the user information, click **Update**.

Changing Your Password

You can change only your own Cisco APIC-EM password, unless you have administrator privileges (ROLE_ADMIN). With administrative privileges, you can change another user's password by deleting and then recreating the user profile with a new password.

You can use the password generator provided in the **Change Password** window or the following guidelines to create a secure password.

Create a password of at least 8 characters and one that contains characters from at least three of the following four classes:

- Uppercase alphabet
- Lowercase alphabet
- Numerical digits

- Special characters—include the space character or any of the following characters or character combinations:

  ! @ # $ % ^ & * ( ) - = + _ { } [ ] \\ | ; : " ' , < . > ? / :: #! ./ ;; >> << () **

In addition to a complex password, you should also ensure that user names do not create security vulnerabilities. To avoid user names that can create security vulnerabilities, the following rules should be followed:

- All users should have unique user names and passwords.
- Do not allow users to use the admin login and password

To avoid creating security vulnerabilities, we recommend that you follow the Cisco APIC-EM password policies when creating a password. For information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 1 From the **Global** toolbar, click the **Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Change Password**.

Step 3 In the **Change Password** window, enter the appropriate values in the following fields:

- **Username—**Your user name appears in this field by default.
- **Current Password—**Your current password.
- **New Password—**Your new password. Create your own or, to create a stronger password, click **Generate**, enter a seed phrase, and click **Generate**. You can apply the generated password by clicking **Apply Password**, or you can copy and paste it or any part of it before or after your new password entry.

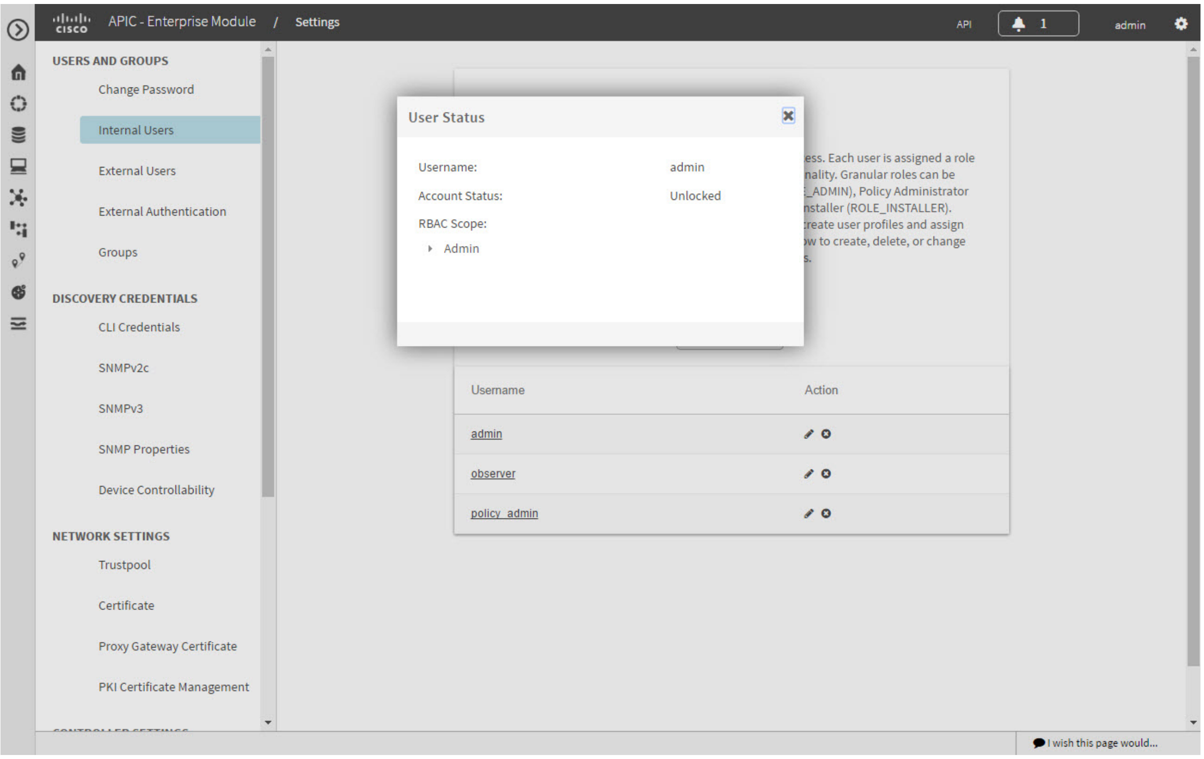
  Note We highly recommend that you use the password generator to create a stronger password.

- **Confirm New Password—**Your new password entered a second time as confirmation.

Step 4 When you are finished, click **Update** to update and save the new password.
Click **Cancel** to cancel the password change.

Viewing User Access Status

As an administrator, you can display the access status of a Cisco APIC-EM user.



User Status

Username: admin

Account Status: Unlocked

RBAC Scope:

- Admin

Username	Action
admin	✎ ⊗
observer	✎ ⊗
policy_admin	✎ ⊗

Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 From the **Global** toolbar, click the**Administrative Functions** (Gear) icon > **Settings**.

Step 2 From the navigation pane in the **Settings** window, click **Users**.
The **Users** window is displayed with the following information about the users:

- **Username—**Username assigned to the user.
- **Role—**Role that defines the user's privileges within the APIC-EM. Valid roles are ROLE_ADMIN, ROLE_POLICY_ADMIN, ROLE_OBSERVER, or ROLE_INSTALLER.
- **Scope—**Resources that the user is allowed to access.
- **Actions—**Icons that allow you to edit user information or delete a user.

Step 3 Click the individual username (link) to view the user's current access status.
The **User Status** dialog box opens, displaying the following information:

- Username
- Account status—Locked or unlocked
- Account Locked Expiration—Time until user account is unlocked

If you are an administrator, you can unlock the user account by clicking **Unlock**.

Note See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for information about configuring a password policy for user access to the controller.

Step 4 When you are finished viewing or editing the user information, click **Close**.

Configuring External Users

Configuring External AuthenticationConfiguring External User Profiles

The Cisco APIC-EM supports external authentication and authorization for users from an AAA server. The external authentication and authorization is based upon usernames, passwords, and attributes that already exist on a pre-configured AAA server. With external authentication and authorization, you can log into the controller with credentials that already exist on the AAA server. The RADIUS protocol is used to connect the controller to the AAA server.

The controller attempts to authenticate and authorize the user in the following order:

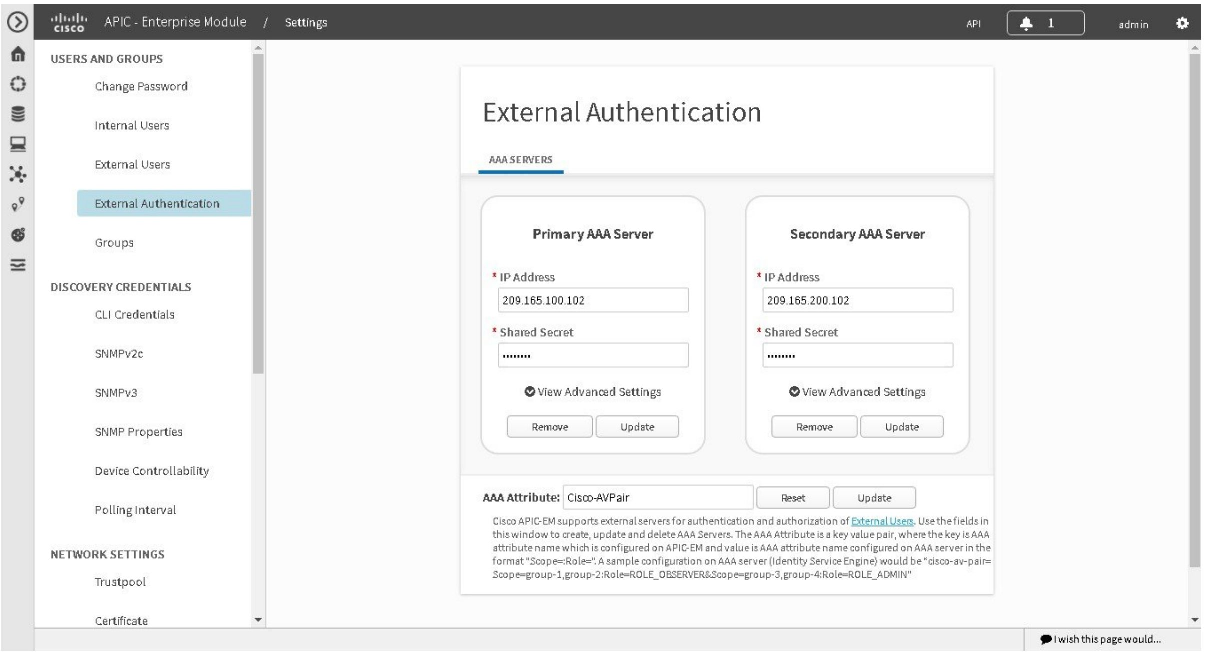
1. Authenticate/authorize with the user's credentials on a primary AAA server.
2. Authenticate/authorize with the user's credentials on a redundant or secondary AAA server.
3. Authenticate/authorize with the user's credentials managed by the Cisco APIC-EM.

A user is granted access to the controller only if both authentication and authorization is successful. When authentication/authorization is attempted using an AAA server, the response from that AAA server may be either a timeout or rejection:

- A timeout occurs when there is no response received from the AAA server within a specific period of time. If the AAA server times out for the authentication/authorization request on the first configured AAA server, then there is a failover to the secondary AAA server. If the secondary AAA server also times out for the authentication/authorization request, then a fall back to local authentication/authorization occurs.
- A rejection is an explicit denial of credentials. If the AAA server rejects an authentication/authorization attempt made from the controller, then there is a fall back to local authentication/authorization.

You configure parameters for the controller to connect to and communicate with an external AAA server, using the **External Authentication** window in the Cisco APIC-EM GUI.

Figure 18: External Authentication Window



Primary AAA Server: * IP Address 209.165.100.102; * Shared Secret ••••••••

Secondary AAA Server: * IP Address 209.165.200.102; * Shared Secret ••••••••

AAA Attribute: Cisco-AVPair

Cisco APIC-EM supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute is a key value pair, where the key is AAA attribute name which is configured on APIC-EM and value is AAA attribute name configured on AAA server in the format "Scope=:Role=". A sample configuration on AAA server (Identity Service Engine) would be "cisco-av-pair= Scope=group-1,group-2:Role=ROLE_OBSERVER&Scope=group-3,group-4:Role=ROLE_ADMIN"

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

You must have the AAA server already preconfigured, set up, and running. You must also configure the AAA server to interact with the Cisco APIC-EM. When configuring the AAA server to interact with the Cisco APIC- EM, perform the following additional steps:

- Register the Cisco APIC-EM with the AAA server.

  Note This could also involve configuring a shared-secret on both the AAA server and Cisco APIC-EM controller.

- Configure an attribute name with a value on the AAA server (the attribute name must match on both the AAA server and controller, see step 10 in the following procedure).

- For a Cisco APIC-EM multi-host configuration, configure all individual host IP addresses and the Virtual IP address for the multi-host cluster on the AAA server.

As an example of using the Cisco Identity Services Engine (ISE) GUI to configure values on an AAA server, you select **Authorization Profiles** in the Cisco ISE GUI navigation pane and proceed to configure an authorization profile. When configuring an authorization profile, you enter the following values:

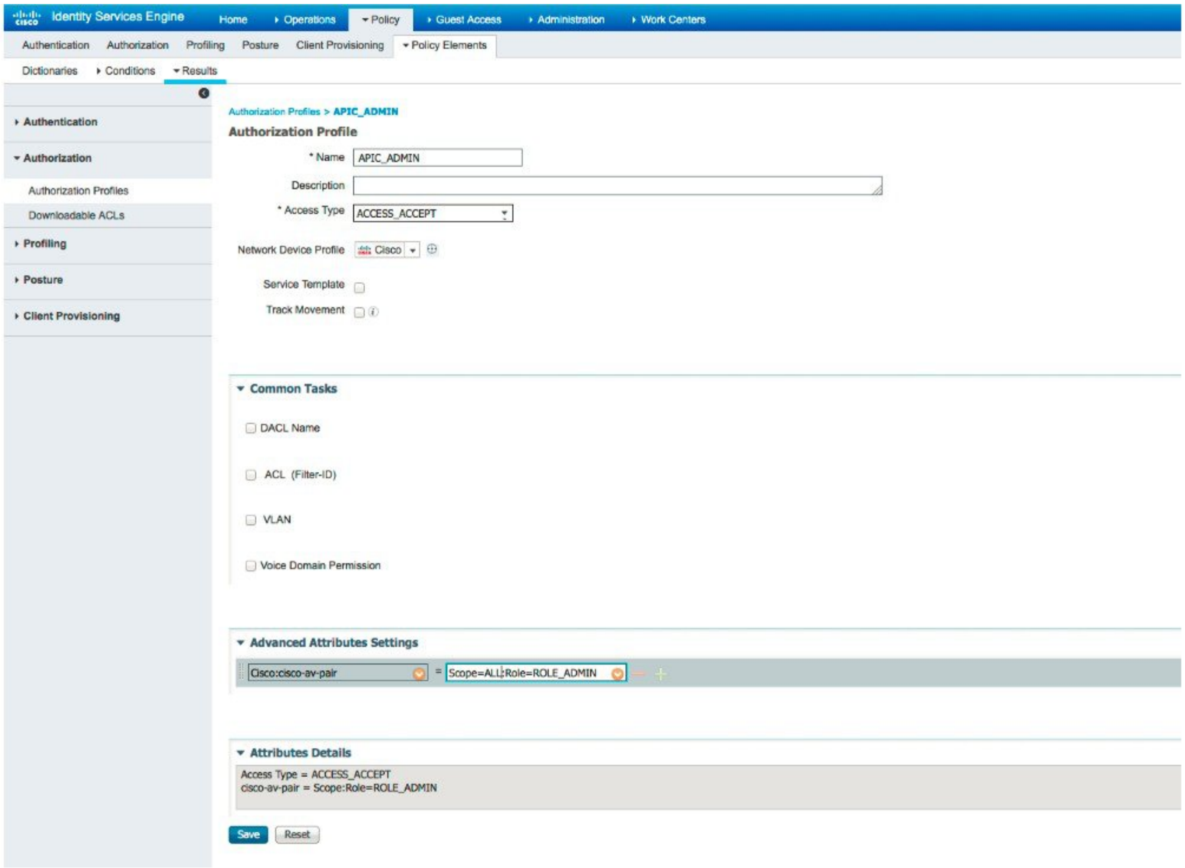
- **Name**: Enter a name for the authorization profile. We recommend that you enter a name similar to the role to be used for the profile. For example, for an admin (ROLE_ADMIN) use a name with "admin" within it, such as "APIC_ADMIN".
- **Description**: Enter a description for the profile
- **Access Type**: ACCESS_ACCEPT
- **Network Device Profile**: Cisco
- **Advance Attribute Settings**:
    - **Attribute Name**: cisco-av-pair (default value)
    - **Scope**: Scope=ALL:Role=ROLE_ADMIN

Note The above **Scope** value is used when setting up external users with administrator permissions (ROLE_ADMIN) and RBAC scope set to ALL. If you have users with different roles and different RBAC scopes, then use the following format for the **Scope** value:

Scope=grp1,grp2,grp5:Role=ROLE_ADMIN&Scope=grp3,grp4:Role=ROLE_OBSERVER

With this **Scope** value format the colon (:) separates the scope(s) from the role. Commas separate the different groups within the scope. The ampersand (&) separates the different roles.

Figure 17: AAA Server Configuration Example (Cisco ISE GUI)



* Name: APIC_ADMIN

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

□ DACL Name

□ ACL (Filter-ID)

□ VLAN

□ Voice Domain Permission

Cisco:cisco-av-pair = Scope=ALL:Role=ROLE_ADMIN

Access Type = ACCESS_ACCEPT
cisco-av-pair = Scope:Role=ROLE_ADMIN

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **External Authentication** to view the **External Authentication** window.

Step 4 Click the **AAA Server** tab to configure the controller with AAA server credential authentication values.

Step 5 Configure access to the AAA server for the controller by entering the following *required* information:

- **IP address—**Enter the IP address of your AAA server
- **Shared Secret—**Enter the AAA server's shared secret.

Click either **View Advanced Settings** to enter additional information for the configuration or **Apply** to save and apply your configuration.

Step 6 (Optional) Configure access to the AAA server for the controller by entering the following information:

- **Protocol—**RADIUS

  The Protocol field is grayed out, since RADIUS is the default protocol.

- **Authentication Port—**The default value for this field is 1812. Enter a different value if you do not use this common value for your AAA server.

- **Account Port—**The default value for this field is 1813. Enter a different value if you do not use this common value for your AAA server.

  Note Accounting is not supported in this controller release.

- **Retries—**Enter the number of times for the controller to attempt authentication, or accept the default value of 1.

- **Timeout (seconds)—**Enter the time interval for the controller to attempt authentication, or accept the default value of 2 seconds.

Click **Apply** to save and apply your configuration.

Step 7 Click the **Add AAA Server** tab to configure a *secondary* AAA server for the controller.
The *secondary* AAA server is the backup AAA server that is used for high availability.

Step 8 Configure access to the *secondary* AAA server for the controller by entering the following *required* information:

- **IP address—**Enter the IP address of your second AAA server

- **Shared Secret—**Enter the second AAA server's shared secret.

Important We recommend that the secondary AAA server has the same configuration as the primary AAA server, otherwise results are unpredictable.

Click either **View Advanced Settings** to enter additional information for the configuration or **Apply** to save and apply your configuration.

Step 9 (Optional) Configure access to the *secondary* AAA server for the controller by entering the following information:

- **Protocol—**RADIUS

  The Protocol field is grayed out, since RADIUS is the default protocol.

- **Authentication Port—**The default value for this field is 1812. Enter a different value if you do not use this common value for your AAA server.

- **Account Port—**The default value for this field is 1813. Enter a different value if you do not use this common value for your AAA server.

- **Retries—**Enter the number of times for the controller to attempt authentication, or accept the default value of 1.

- **Timeout (seconds)—**Enter the time interval for the controller to attempt authentication, or accept the default value of 2 seconds.

Click **Apply** to save and apply your configuration.

Step 10 Enter the **AAA Attribute**.
As part of the required, earlier AAA server configuration, you must have already configured an AAA attribute on the AAA server. The AAA attribute is a key value pair that consists of both a key and its value. The key is the AAA attribute name. On the Cisco APIC-EM, you register this AAA attribute name in the controller's GUI in this field. By doing so,

you are instructing the controller to search for this key (AAA attribute name) in the AAA server response, after logging in with your AAA credentials.

Important The default AAA attribute name on the controller is Cisco-AVPair.

On the AAA server, you configure *both* the key (AAA attribute name) and its value. The key must be the same as that being configured on the Cisco APIC-EM. The value (which is only configured on the AAA server) supports the following format: Scope=*scope_value*:Role=*role_value*

For example: Scope=ALL:Role=ROLE_ADMIN

Note that if you have several users with different roles and scopes, then you use a different format:

For example: Scope=grp1,grp2:Role=ROLE_ADMIN&Scope=grp3,grp4:Role=ROLE_OBSERVER

This format used for multiple users, roles, and scopes is mandatory. The colon (:) separates the scope(s) from the roles in this format. Commas separate the groups within the scopes. The ampersand (&) separates the different role types.

You can only list the role once using this format. So, in the above example if you need to add an admin for a group 5 (grp5), you would need to rewrite using the following format:

Scope=grp1,grp2,grp5:Role=ROLE_ADMIN&Scope=grp3,grp4:Role=ROLE_OBSERVER

Once finished, click **Update** to save the **AAA Attribute** name.

What to Do Next

Log out of the Cisco APIC-EM.

Using your AAA server credentials, log back into the Cisco APIC-EM.

Access the **External Users** window on the controller's GUI to view the AAA server users, roles, and scope.

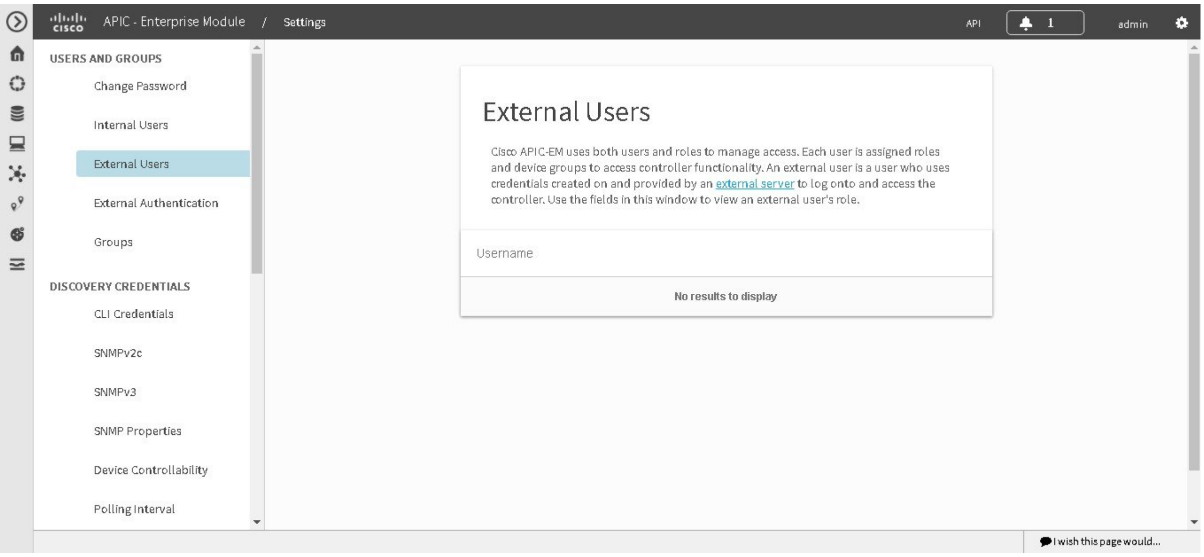
Note If the authentication/authorization is successful and access is granted, then the user's external authentication/authorization is saved in the controller's database. All users successfully granted access can be viewed in the **External Users** window.

Viewing External Users

You can view external users that have access to the Cisco APIC-EM using the controller's GUI. An external user is a user with credentials created on and provided by an external server to log onto and access the controller.

Use the fields in the **External Users** window to view an external user's role and the groups they belong to. For information about configuring external controller authentication, see Configuring External AuthenticationConfiguring External User Profiles, on page 79.

Figure 19: External Users Window



External Users

Cisco APIC-EM uses both users and roles to manage access. Each user is assigned roles and device groups to access controller functionality. An external user is a user who uses credentials created on and provided by an external server to log onto and access the controller. Use the fields in this window to view an external user's role.

Username
No results to display

Before You Begin

You must have administrator (ROLE_ADMIN) permissions, as well as RBAC scope configured to all groups (global RBAC scope) or a specific subset of groups (non-global RBAC scope).

You have already configured external authentication for the controller with an AAA server.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **External Users** to view the **External Users** window.

Step 4 Proceed to view any external users displayed in this window.

Note External users that were authenticated by the controller appear in this window. For example, if you configured an external user on an AAA server (with the name "user_grp01") and this user was authenticated by the controller, then user_grp01 will appear in this window as an active link. Click on the link to view additional user account status (Locked or Unlocked) and authorization (role: list of scopes).

CHAPTER 4

Enabling Applications on the Cisco APIC-EM

Cisco APIC-EM Application Separation

The Cisco APIC-EM treats individual applications as separate from the core infrastructure. Specifically, individual applications can enabled to run on the controller or disabled using either the GUI or the CLI. The following applications are supported for this release:

- **PnP—**Application that provides Network PnP services and functionality on the controller.
- **IWAN—**Application that provides IWAN services and functionality on the controller.

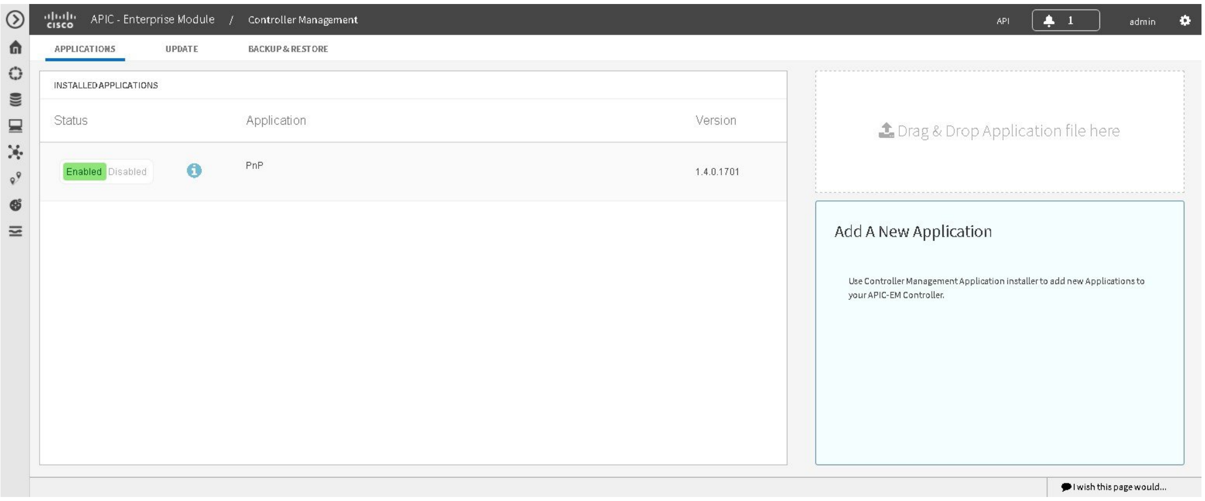
Note Each Cisco APIC-EM application bundle consists of service bundles, meta data files, and scripts; however for this specific release, application bundles are only provided as part of the ISO image.

Enabling and Disabling Applications

With this release, the Cisco APIC-EM treats individual applications as separate from the core infrastructure. Specifically, individual applications can now be enabled to run on the controller or disabled. For this release, Cisco APIC-EM only supports enabling or disabling the IWAN and PnP applications. Future releases will support additional applications with this functionality.

You can perform the application management procedures from the **Applications** tab in the Cisco APIC-EM GUI.

Figure 20: Applications Window


APIC - Enterprise Module / Controller Management
API
1
admin
APPLICATIONS
UPDATE
BACKUP & RESTORE
Drag & Drop Application file here
Add A New Application
I wish this page would...

INSTALLED APPLICATIONS

Status	Application	Version
Enabled Disabled	PnP	1.4.0.1701

Use Controller Management Application installer to add new Applications to your APIC-EM Controller.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Important Enabling and disabling applications for the Cisco APIC-EM may involve controller downtime for a period of time. For this reason, we recommend that you schedule performing these procedures during your network off-peak hours or a maintenance time period.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **App Management** link from the drop-down menu.

Step 3 Review the **Applications** tab that now appears.
The **Applications** tab consists of the following fields:

- **Installed Applications**—Field that displays current applications installed on the controller, status (enabled or disabled), and version.
- **Drag & Drop**—Field where you can drop in an application file to download and install it.

Step 4 In the **Installed Applications** field, review the applications currently installed on the controller, status (enabled or disabled) and versions.
Click on the information icon ("i" symbol within a blue circle) for additional application information.

General information	Provides general information about the application including a definition, its version, whether it can be enabled by default, and whether or not it can be disabled for this release.
Requires	Displays the other applications that it is dependent upon. Proper operation of the application is contingent upon those other applications being installed, enabled, and running.
Services Provided	Provides a list of services and the service version that the application will install.

Step 5 Drag and drop your updated application to the **Drag & Drop** field on the controller GUI.

Important For this specific controller release, application bundles are only provided as part of the ISO image. For this reason, this step in the procedure is not currently available.

Step 6 Review the status bar for the application upload.
The time required for the application upload will vary depending upon the size of the file. After the upload, the new application appears in the **Installed Applications** field.

Note A warning message will appear if the following conditions are not met:

- A prerequisite application bundle is not enabled on the controller.
- The system requirements of memory, CPU, and/or storage are not met.

Important For this specific controller release, the application bundles are only provided as part of the ISO image. For this reason, this step in the procedure is not currently available.

Step 7 Enable the new application by clicking its **Enable** button.
When prompted to confirm, click **Ok**.

Note A warning message will appear if the following conditions are not met:

- A prerequisite application bundle is not enabled on the controller.
- The system requirements of memory, CPU, and/or storage are not met

What to Do Next

Check the **Installed Applications** field. When the status for the application changes to **Enable**, then proceed to access and work with the application in the controller.

CHAPTER 5

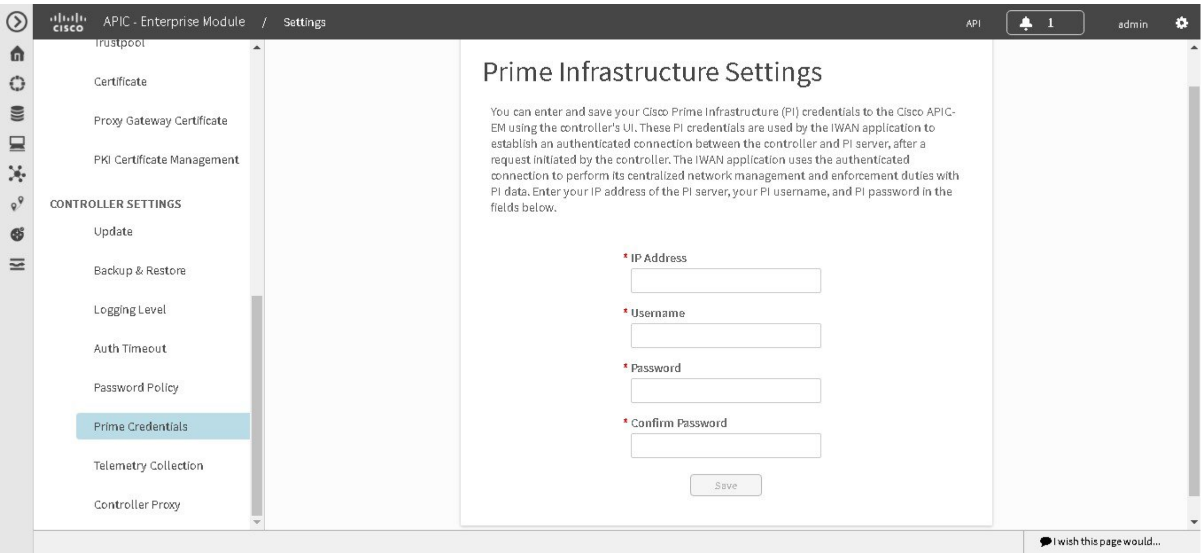
Configuring IWAN-Specific Settings

Configuring the Prime Infrastructure Settings

You can enter and save your Cisco Prime Infrastructure (PI) settings to the Cisco APIC-EM using the controller's UI. These PI settings are used by the IWAN application to establish an authenticated connection between the controller and PI server, after a request initiated by the controller. The IWAN application uses the authenticated connection to perform its centralized network management and enforcement duties with PI data.

You can configure the PI settings using the **Prime Infrastructure Settings** window in the Cisco APIC-EM GUI.

Figure 21: Prime Infrastructure Settings Window



Prime Infrastructure Settings

You can enter and save your Cisco Prime Infrastructure (PI) credentials to the Cisco APIC-EM using the controller's UI. These PI credentials are used by the IWAN application to establish an authenticated connection between the controller and PI server, after a request initiated by the controller. The IWAN application uses the authenticated connection to perform its centralized network management and enforcement duties with PI data. Enter your IP address of the PI server, your PI username, and PI password in the fields below.

* IP Address

* Username

* Password

* Confirm Password

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Prime Credentials** to view the **Prime Infrastructure Settings** window.

Step 4 Enter either the IP address of the PI server or the DNS domain name of the PI server.

Step 5 Enter the PI credentials username.

Step 6 Enter the PI credentials password.

Step 7 Click the **Save** button to save the PI credentials to the Cisco APIC-EM database.

What to Do Next

Proceed to configure the discovery credentials for your network.

CHAPTER 6

Configuring Telemetry

Telemetry Collection

The Cisco APIC-EM uses telemetry to collect information about the user experience with the controller. This information is collected for the following reasons:

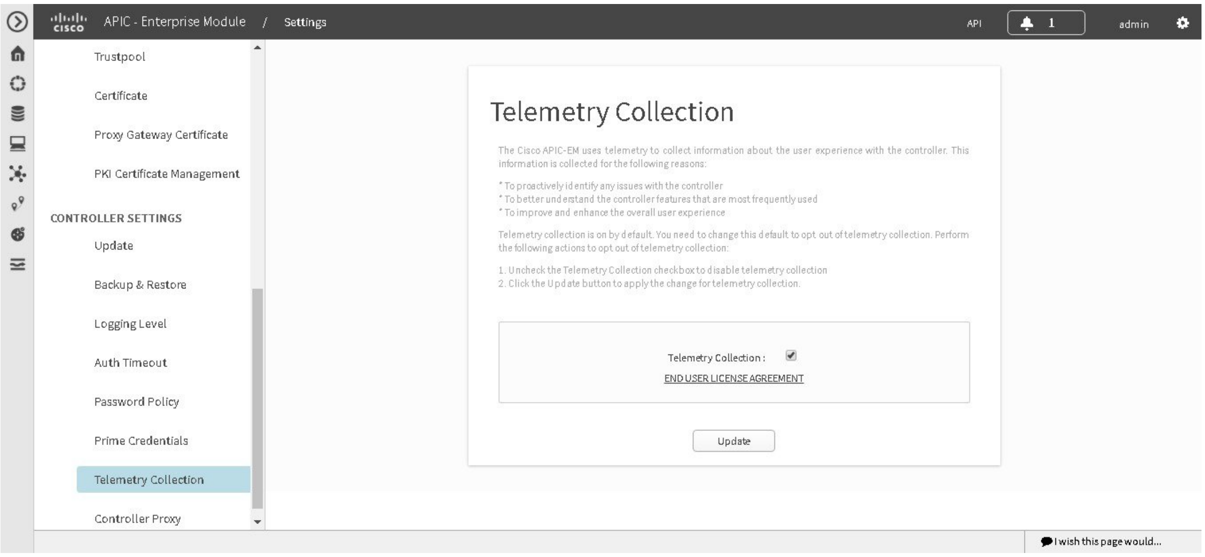
- To proactively identify any issues with the controller
- To better understand the controller features that are most frequently used
- To improve and enhance the overall user experience

You are able to view some of the collected telemetry data by viewing the logs using the Cisco APIC-EM GUI. For information about this method, see *Searching the Services Logs* in Chapter 6, Configuring the Cisco APIC-EM Settings.

Telemetry is enabled with a telemetry service that collects data from the many other controller services. The telemetry service supports Data Access Service (DAS). The telemetry service uploads data to the Cisco Clean Access Agent (CAA) infrastructure on the Cisco cloud using HTTPS.

Telemetry collection is on by default. If you wish to opt out of telemetry collection, then perform the steps in the following procedure.

Figure 22: Telemetry Collection Window



Telemetry Collection

The Cisco APIC-EM uses telemetry to collect information about the user experience with the controller. This information is collected for the following reasons:

* To proactively identify any issues with the controller
* To better understand the controller features that are most frequently used
* To improve and enhance the overall user experience

Telemetry collection is on by default. You need to change this default to opt out of telemetry collection. Perform the following actions to opt out of telemetry collection:

1. Uncheck the Telemetry Collection checkbox to disable telemetry collection
2. Click the Update button to apply the change for telemetry collection.

Telemetry Collection : ☑

END USER LICENSE AGREEMENT

Update

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Telemetry Collection** to view the **Telemetry Collection** window.
When accessing the **Telemetry Collection** window for the first time, the GUI displays a blue box with a check that indicates that telemetry collection is enabled.

Step 4 (Optional) Click the **End User License Agreement** to review the agreement for telemetry collection.

Step 5 (Optional) Uncheck the **Telemetry Collection** blue box to disable telemetry collection.

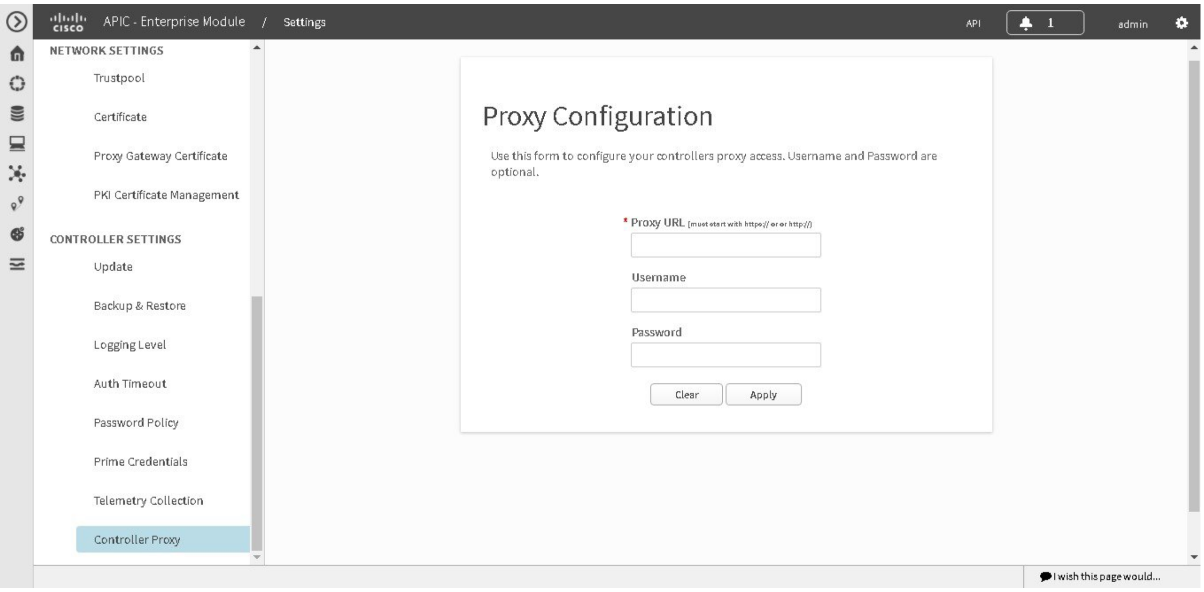
Step 6 (Optional) Click the **Update** button to apply the change for telemetry collection.

Configuring the Proxy

If the Cisco APIC-EM is unable to communicate directly with the telemetry server in the Cisco cloud, then a message will appear in the controller GUI (for an admin user) requesting that you configure access to the proxy. This message will contain a direct link to the **Proxy Configuration** window where you can configure this access. To configure access, enter the appropriate settings for the proxy server that exists between the controller and the telemetry server.

You configure these settings using the **Proxy Configuration** window in the Cisco APIC-EM GUI.

Figure 23: Proxy Configuration Window



Proxy Configuration

Use this form to configure your controllers proxy access. Username and Password are optional.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Controller Proxy** to view the **Proxy Configuration** window.

Step 4 Enter the proxy server's URL address.

Step 5 (Optional) If the proxy server requires authentication, then enter the username for access to the proxy server.

Step 6 (Optional) If the proxy server requires authentication, then enter the password that is required for access to the proxy server.

Step 7 Click the **Apply** button to apply your proxy configuration settings to the controller.

CHAPTER 7

Backing Up and Restoring the Cisco APIC-EM

About Backup and Restore

The back up and restore procedure for the Cisco APIC-EM can be used for the following purposes:

- To create a single backup file to support disaster recovery on the controller
- To create a single backup file on one controller to restore to a different controller (if required for your network configuration)

When you perform a back up using the controller's GUI, you copy and export the controller's database and files as a single file to a specific location on the controller. When you perform a restore, you copy over the existing database and files on the controller using this single backup file.

Note The Cisco APIC-EM uses PostgreSQL as the preferred database engine for all network data. PostgreSQL is an open source object-relational database system.

The following files and data are copied and restored when performing a back up and restore:

- Cisco APIC-EM database
- Cisco APIC-EM file system and files
- X.509 certificates and trustpools
- Usernames and passwords
- Any user uploaded files (for example, any Network Plug and Play image files)

The database and files are compressed into a single *.backup* file when performing the back up and restore. The maximum size of the *.backup* file is 30GB. This number consists of a permitted 20GB maximum size for a file service back up and a 10GB permitted maximum size for the database back up.

Note The .backup file should not be modified by the user.

Only a single back up can be performed at a time. Performing multiple back ups at once are not permitted. Additionally, only a full back up is supported. Other types of back ups (for example, incremental back ups) are not supported.

Note After saving the backup file, you can also download it to another location in your network. You can restore the backup file from its default location in the controller or drag and drop the backup file from its location in your network to restore.

When performing a backup and restore, we recommend the following:

- Perform a back up everyday to maintain a current version of your database and files.
- Perform a back up and restore after making any changes to your configuration. For example, when changing or creating a new policy on a device.
- Only perform a back up and restore during a low impact or maintenance time period.

When a back up is being performed, you will be unable to delete any files that have been uploaded to the file service and any changes you make to any files may not be captured by the back up process. When a restore is being performed, the controller is unavailable.

Note You cannot schedule nor automate a back up and restore at this time. Additionally, once started you cannot manually cancel either the back up or restore process.

Multi-Host Cluster Back Up and Restore

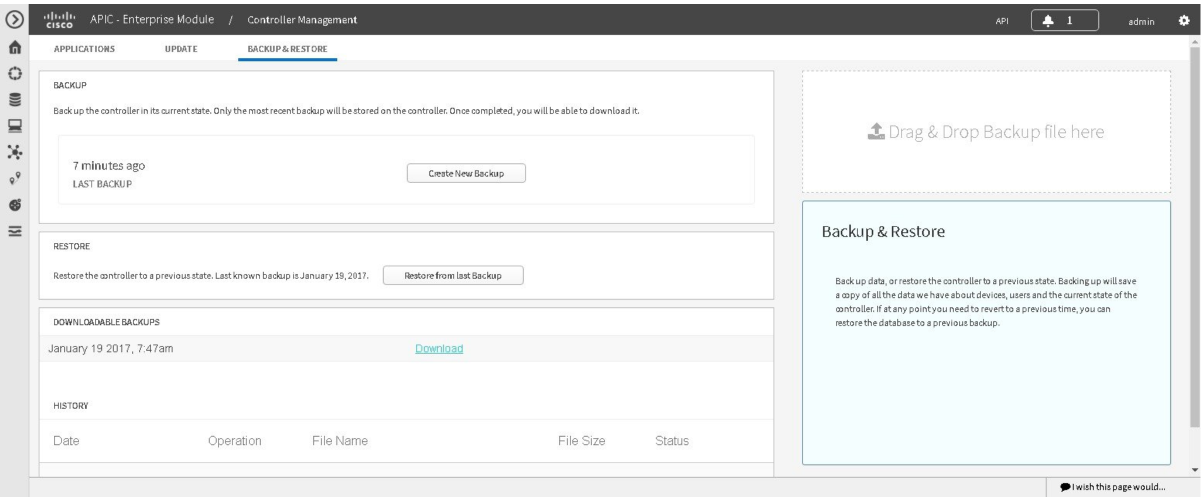
In a multi-host cluster, the database and files are replicated and shared across three hosts. When backing up and restoring in a multi-host cluster, you need to first back up on one of the three hosts in the cluster. You can then use that backup file to restore all three hosts in the cluster. However, you need not perform the restore operation on each of the hosts. You simply restore one of the hosts in the cluster. The controller replicates the restored data to the other hosts automatically.

Note The back up and restore process in a multi-host cluster requires that the Cisco APIC-EM software and version must be the same for all three hosts.

Backing Up the Cisco APIC-EM

You can back up your controller using the **Backup & Restore** window.

Figure 24: Backup & Restore Window



Back up the controller in its current state. Only the most recent backup will be stored on the controller. Once completed, you will be able to download it.

Restore the controller to a previous state. Last known backup is January 19, 2017.

January 19 2017, 7:47am

Date	Operation	File Name	File Size	Status

Back up data, or restore the controller to a previous state. Backing up will save a copy of all the data we have about devices, users and the current state of the controller. If at any point you need to revert to a previous time, you can restore the database to a previous backup.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **App Management** link from the drop-down menu.

Note In previous versions of the controller software, the **Backup and Restore** functionality was directly accessible from the **Settings** navigation pane. Although, the **Backup and Restore** option is still visible from the **Settings** navigation pane, with this release you cannot access this functionality from that GUI location.

Step 3 Click the **Backup and Restore** tab at the top of the window.

Step 4 In the **Backup & Restore** window, create a backup file by clicking on the **Create New Backup** button.
After clicking the **Create New Backup** button, a **Backup in Progress** window appears in the GUI.

During this process, the Cisco APIC-EM creates a compressed *.backup* file of the controller database and files. This backup file is also given a time and date stamp that is reflected in its file name. The following file naming convention is used: *yyyy-mm-dd-hh-min-seconds* (year-month-day-hour-seconds).

For example:

backup_2015_08_14-08-35-10

Note If necessary, you can rename the backup file instead of using the default time and date stamp naming convention.

This backup file is then saved to a default location within the controller. You will receive a **Backup Done!** notification, once the back up process is finished. Only a single backup file at a time is stored within the controller.

Note If the back up process fails for any reason, there is no impact to the controller and its database. Additionally, you will receive an error message stating the cause of the back up failure. The most common reason for a failed back up is insufficient disk space. If your back up process fails, you should check to ensure that there is sufficient disk space on the controller and attempt another back up.

Step 5 (Optional) Create a copy of the backup file to another location.
After a successful back up, a **Download** link appears in the GUI. Click the link to download and save a copy of the backup file to a location on your laptop or network.

What to Do Next

When necessary and at an appropriate time, proceed to restore the backup file to the Cisco APIC-EM.

Restoring the Cisco APIC-EM

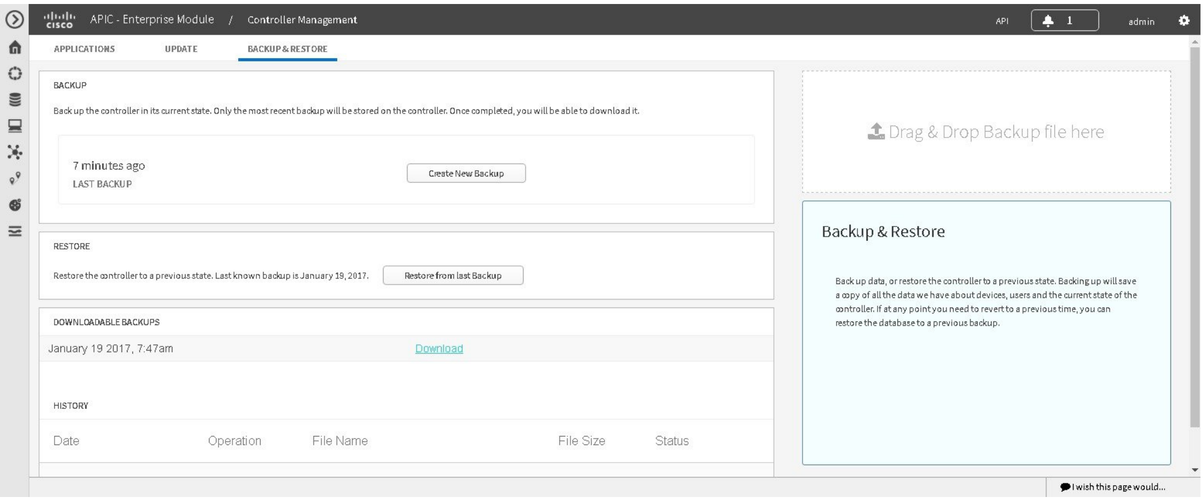
You can restore your controller using the **Backup & Restore** window.

The following restore options are available:

- You can restore from the last know backup file on the controller.
- You can also restore from an archived backup file that was saved and moved to another location on your network.

Caution The Cisco APIC-EM restore process restores the controller's database and files. The restore process does not restore your network state and any changes made by the controller since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates/trustpool bundles.

Figure 25: Backup & Restore Window



Back up the controller in its current state. Only the most recent backup will be stored on the controller. Once completed, you will be able to download it.

7 minutes ago
LAST BACKUP

Restore the controller to a previous state. Last known backup is January 19, 2017.

January 19 2017, 7:47am

Date	Operation	File Name	File Size	Status

Back up data, or restore the controller to a previous state. Backing up will save a copy of all the data we have about devices, users and the current state of the controller. If at any point you need to revert to a previous time, you can restore the database to a previous backup.

Note You can only restore a backup from a controller that is the same software version as the controller where the backup was originally taken from.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

You must have successfully performed a back up of the Cisco APIC-EM database and files following the steps in the previous procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **App Management** link from the drop-down menu.

Note In previous versions of the controller software, the **Backup and Restore** functionaliy was directly accessible from the **Settings** navigation pane. Although, the **Backup and Restore** option is still visible from the **Settings** navigation pane, with this release you cannot access this functionality from that GUI location.

Step 3 Click the **Backup and Restore** tab at the top of the window.

Step 4 To restore the backup file, click on the **Restore from last Backup** button.
You can also drag and drop the backup file from its location in your network onto the **Drag and Drop a backup file** field in this window.

During a restore, the backup file copies over the current database.

Note When a restore is in progress, you are not be able to open and access any windows in the GUI.

Step 5 After the restore process completes, log back into the controller's GUI.
If the restore process was successful, you will be logged out of the controller and its GUI. You will need to log back in.

Note The Cisco APIC-EM restore process restores the controller's database and files. The restore process does not restore your network state and any changes made by the controller since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates/trustpool bundles.

To check whether the restore process was successful, you can either review the **Backup History** field of the **Backup & Restore** window or access the Grapevine root and to run the **grape backup display** command.

Caution

If the restore process was unsuccessful, you will receive an unsuccessful restore notification. Since the database may be in an inconsistent state, we recommend that you do not use the database and contact technical support for additional actions to take.

Step 6 (Optional) Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 7 (Optional) When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 8 (Optional) Enter the **grape backup display** command at the prompt to confirm that the restore process was completed and successful.

```
$ grape backup display
```

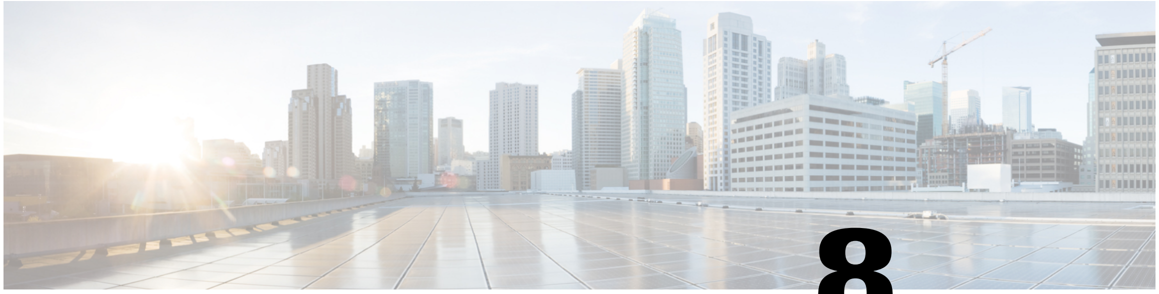
Check the command output to ensure that the restore process was completed and successful. Look for the property operation marked "restore" in the command output, with the latest start_time and ensure that the status is marked as a "success".

Step 9 (Optional) Using the Secure Shell (SSH) client, log out of the appliance.

Step 10 Return to the controller's GUI and review the **Backup History** field of the **Backup & Restore** window.
After the restore, information about it appears in the **Backup History** field of the **Backup & Restore** window. The following update data is displayed in this field:

- **Date—**Local date and time of the restore
- **ID—**Controller generated identification number of the backup file
- **Operation—**Type of operation, either backup or restore
- **Update Status—**Success or failure status of the operation.

Note If you place your cursor over (mouseover) a failure status in this field, then additional details about the failure is displayed.



CHAPTER 8

Managing the Cisco APIC-EM

Adding Static Routes to the Controller

You can troubleshoot the Cisco APIC-EM installation by running the configuration wizard a second time and updating any earlier configuration entries, including the static routes used by the controller. The configuration wizard saves and displays your previous configuration settings, so you do not have to reenter them.

Note When performing this procedure, controller downtime occurs. For this reason, we recommend that you perform this procedure during a maintenance time period. For information about changing settings for a multi-host configuration, see Changing the Settings in a Multi-Host Cluster.

Before You Begin

You have installed Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Restart the configuration wizard using the following command.

```
$ config_wizard
```

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

Step 4 Review the current configuration values in the configuration wizard and click **next>>**, until you access the specific step where you wish to update your previous configuration entry.
For example, if you need to enter a new static route address, click **next >>** until you get to the **NETWORK ADAPTER #1 (eth0)** screen.

Step 5 Update the value that was previously entered in the configuration wizard and is currently displayed.
For static routes, you need to enter a list of space separated static routes in the following format:

Network IP address/Netmask IP address/[Gateway IP address]

Step 6 Click **next>>** until the last step of the configuration wizard process.

Step 7 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM installation.

Changing the Controller's IP Address

You can troubleshoot the Cisco APIC-EM installation by running the configuration wizard a second time and updating any earlier configuration entries, including the IP address (host or virtual) of the controller. The configuration wizard saves and displays your previous configuration settings, so you do not have to reenter them.

Note When performing this procedure, controller downtime occurs. For this reason, we recommend that you perform this procedure during a maintenance time period. For information about changing settings for a multi-host configuration, see Changing the Settings in a Multi-Host Cluster.

Before You Begin

You have installed Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Restart the configuration wizard using the following command.

```
$ config_wizard
```

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

Step 4 Review the current configuration values in the configuration wizard and click **next>>**, until you access the specific step where you wish to update your previous configuration entry.
For example, if you need to enter a new host IP address, click **next >>** until you get to the **NETWORK ADAPTER #1 (eth0)** screen.

Step 5 Update the value that was previously entered in the configuration wizard and is currently displayed.
For example, you can update the host IP setting by entering a new IP address.

Step 6 Click **next>>** until the last step of the configuration wizard process.

Step 7 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM installation.

Changing the Controller Settings in a Multi-Host Cluster

To troubleshoot an issue with a multi-host cluster, you may need to change its configuration settings. This procedure describes how to change the Cisco APIC-EM external network settings, NTP server address, and/or password for the Linux grapevine user in a multi-host cluster. The external network settings that can be changed include:

- Host IP address
- Virtual IP address
- DNS server
- Default gateway
- Static routes

Note In order to change the external network settings, NTP server address, and/or the Linux grapevine user password in a multi-host deployment, you need to first break up the multi-host cluster. As a result, controller downtime occurs. For this reason, we recommend that you perform this procedure during a maintenance time period.

Before You Begin

You must have successfully configured the Cisco APIC-EM as a multi-host cluster using the configuration wizard, as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into one of the hosts in your cluster.
Log in using the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Note The **config_wizard** command is in the PATH of the 'grapevine' user, and not the "root" user. Either run the command as the "grapevine" user, or fully qualify the command as the "root" user. For example: **/home/grapevine/bin/config_wizard**

Step 4 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 5 A message appears with the following options:

- **[cancel]—**Exit the configuration wizard.
- **[proceed]—**Begin the process to remove this host from its cluster.

Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from its cluster.
At the end of this process, this host is removed from the cluster.

Step 6 Repeat the above steps (steps 1-5) on a second host in the cluster.

Note You must repeat the above steps on each host in your cluster, until you only have a single host remaining. You must make your configuration changes on this final remaining host.

Step 7 Using a Secure Shell (SSH) client, log into that final host in your cluster and run the configuration wizard.

```
$ config_wizard
```

After logging into the host, begin the configuration process.

Step 8 Make any necessary changes to the configuration values for the external network settings, NTP server address, and/or password for the Linux grapevine user using the wizard.
After making your configuration change(s), continue through the configuration process to the final message.

Step 9 At the end of the configuration process, a final message appears stating that the wizard is now ready to proceed with applying the configuration.
The following options are available:

- **[back]—**Review and verify your configuration settings.

- **[cancel]—**Discard your configuration settings and exit the configuration wizard.
- **[save & exit]—**Save your configuration settings and exit the configuration wizard.
- **[proceed]—**Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

Note

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Step 10 Log into the other hosts in your multi-host cluster and use the configuration wizard to recreate the cluster.
Refer to *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide* for information about this specific procedure.

Restoring the Controller to the Factory Default

In certain situations, you may want to restore the Cisco APIC-EM to its original factory default settings. For example, if your controller appliance is being replaced or simply has an undesirable configuration that needs to be completely removed. Under these circumstances, you can restore the controller to its factory defaults and then proceed to reconfigure it as a new controller.

This procedure describes how to a restore the factory defaults to the controller.

Caution This procedure shuts down both the Cisco APIC-EM and the host (physical or virtual) on which it resides. At the end of this procedure, you will need to access the host and restart it.

Before You Begin

You have already installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

You have access to the Cisco APIC-EM using either a physical console or a Telnet connection.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **reset_grapevine factory** command at the prompt.

```
$ reset_grapevine factory
```

Important The **reset_grapevine factory** command will terminate if the SSH connection is disconnected for any reason. To avoid this, we recommend that you use tmux (terminal multiplexer) which is already installed on the controller to run the **reset_grapevine factory** command in the session. You can use the following commands for tmux:

tmux new -s *session_name* **'reset_grapevine factory'**	Command to create a new session using tmux for reset-grapevine factory. Note that 'reset-grapevine factory' in this command is a string value and therefore must be entered within single quotation marks. For example, you can enter the following command: **tmux new -s** *session100* **'reset_grapevine factory'**
tmux ls	Command to view a the list of tmux sessions.
tmux attach -t *session_name* **'reset_grapevine factory'**	Command to attach to a tmux session. Note that 'reset-grapevine factory' in this command is a string value and therefore must be within single quotation marks. For example, you can enter the following command: **tmux attach -t** *session200* **'reset_grapevine factory'** To get more information about tmux, you can run the **man tmux** command.

Step 4 Enter your Linux grapevine password a second time to start the reset process.

```
$ sudo password for grapevine *********
```

After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

You are then prompted to confirm your desire to run the **reset_grapevine factory** command.

Step 5 Enter **Yes** to confirm that you want to run the **reset_grapevine factory** command.
The controller then performs the following tasks:

- Stops all running clients and services
- Deletes all cluster data
- Deletes all user data
- Deletes the configuration files including secrets and private keys
- Shuts down the controller
- Shuts down the host (physical or virtual)

What to Do Next

Perform the following tasks:

- Start up the host (physical or virtual).
- After start up, the configuration wizard appears and prompts you to re-deploy the Cisco APIC-EM.
- Proceed to re-deploy the Cisco APIC-EM using the configuration wizard.

Shutting Down and Restarting the Controller

Under certain circumstances, such as when troubleshooting, you might need to gracefully shutdown and then restart either a single host or a multi-host cluster.

For information about shutting down and restarting a single host within a multi-host cluster, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

Before You Begin

You should have installed the Cisco APIC-EM following the procedures in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **harvest_all_clients** command to harvest (gracefully shut down) all services on a single host or on multiple hosts within a multi-host cluster.

```
$ sudo /home/grapevine/bin/harvest_all_clients
```

Important For a multi-host cluster, you only need to enter this command on one of the hosts to harvest (gracefully shut down) all services on all of hosts in the cluster.

Step 4 Review the command output and subsequent directions.

```
$ sudo /home/grapevine/bin/harvest_all_clients

Disabled Grapevine policy
Harvesting client 1f481f49-fabc-44f9-af5a-0481bd823165...
Harvesting client 6dac3f56-fb05-4fd0-be06-d5c6869e23cd...
Harvesting client c800924c-7603-4092-b1f8-0c19f5141acc...
Waiting on task 05b9192c-9484-11e6-bdc2-0050569f3bee...
Task '05b9192c-9484-11e6-bdc2-0050569f3bee' completed successfully
Waiting on task 05da80da-9484-11e6-bdc2-0050569f3bee...
Task '05da80da-9484-11e6-bdc2-0050569f3bee' completed successfully

Successfully harvested all clients

PLEASE NOTE:
```

```
Grapevine policy has been DISABLED so that services and clients can be harvested.
To start all services again, run the following command:

   grape config update enable_policy true
```

Step 5 Power down the host, by entering the following command:

```
$ sudo shutdown -h now
```

Enter your password a second time when prompted.

For a multi-host cluster, you will need to enter this command on each of the hosts in the multi-host cluster to shut them all down.

Important You need to ensure that the last host that was shutdown in a multi-host cluster is the very first host that is then restarted. Be sure to track the order in which the hosts are shutdown in a multi-host cluster.

Step 6 Review the command output as the host shuts down.

Note The **sudo shutdown** command also powers off the host.

Step 7 Power up the Grapevine root process by turning the host or hosts (in a multi-host cluster) back on.

Important For a multi-host cluster, be sure to restart the host that was shutdown last in the multi-host cluster. This must be the first host restarted.

Step 8 Using a Secure Shell (SSH) client, log back into the host with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

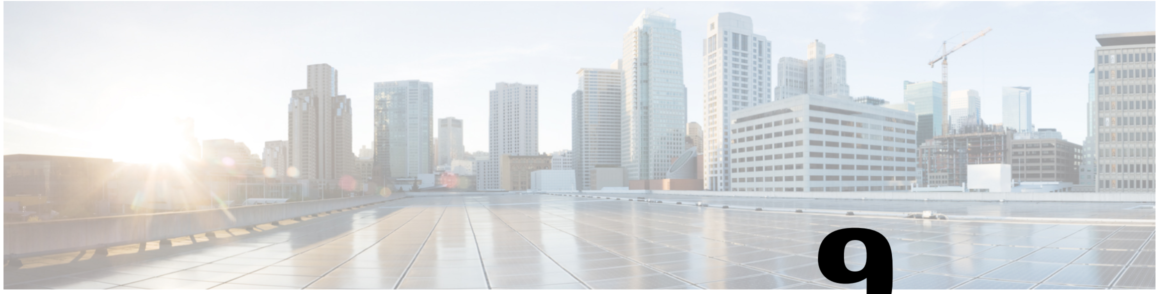
Step 9 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 10 Enable Grapevine, by entering the following command on the Grapevine root:

```
$ grape config update enable_policy true
```

Wait a few minutes for the Cisco APIC-EM services to start up again.

Important For a multi-host cluster, you only need to enter this command on one of the hosts after all of the hosts have been successfully powered on.



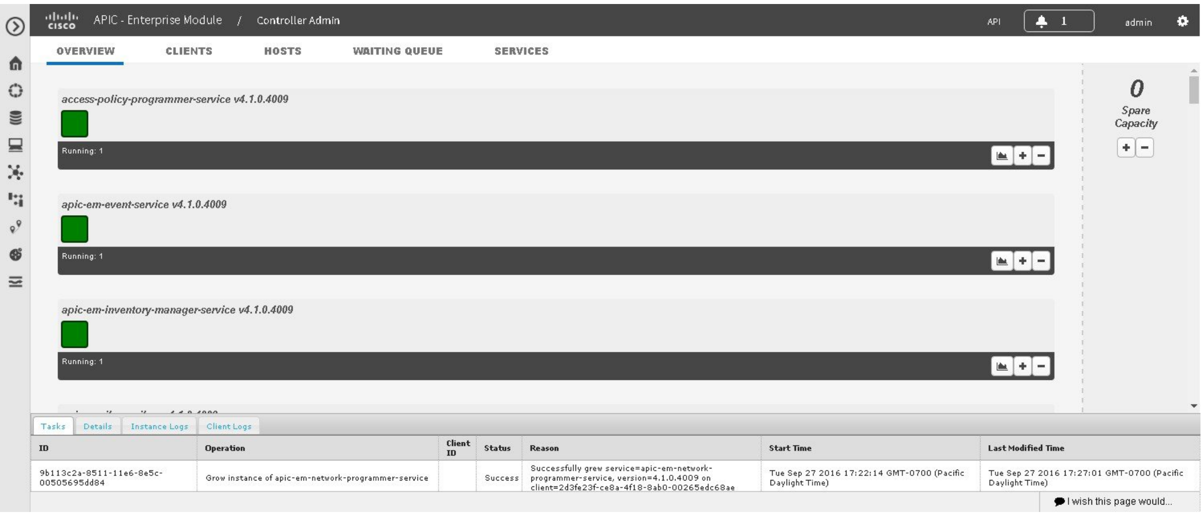
CHAPTER 9

Monitoring the Cisco APIC-EM Services

Controller Admin Console

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when increasing loads occur on a client within the network. You use the **Controller Admin** console to manage and troubleshoot these services. The **Controller Admin** console and its tools were bundled with the deployment files and installed when you first deployed the Cisco APIC-EM.

Figure 26: Controller Admin Console



access-policy-programmer-service v4.1.0.4009

Running: 1

apic-em-event-service v4.1.0.4009

Running: 1

apic-em-inventory-manager-service v4.1.0.4009

Running: 1

ID	Operation	Client ID	Status	Reason	Start Time	Last Modified Time
9b113c2a-8511-11e6-8e5c-00505695dd84	Grow instance of apic-em-network-programmer-service		Success	Successfully grew service=apic-em-network-programmer-service, version=4.1.0.4009 on client=2d3fe23f-ce8a-4f18-8ab0-00265edc68ae	Tue Sep 27 2016 17:22:14 GMT-0700 (Pacific Daylight Time)	Tue Sep 27 2016 17:27:01 GMT-0700 (Pacific Daylight Time)

Note For a multi-host cluster, you do not have to log into each host to view the **Controller Admin** console. In a multi-host cluster, you get a single, consolidated view of all of the services running on all three hosts.

The **Controller Admin** console is directly accessible from the controller's GUI. To access this console, click on **Settings** (gear) icon in the menu bar at the top of the controller's GUI, then click on the **System Administration** link in the drop down menu.

The **Controller Admin** console provides the following windows and functionality:

- **Overview—**Provides a list of services with information about their version and status. You can add or remove services in this window.
- **Clients—**Provides detailed client information in this window.
- **Hosts—**Provides detailed host information in this window.
- **Waiting Queue—**Provides information about the waiting queue.
- **Services—**Provides detailed service information. You can add or remove services in this window.
- **Logs—**Provides detailed task, instance, and client logs.

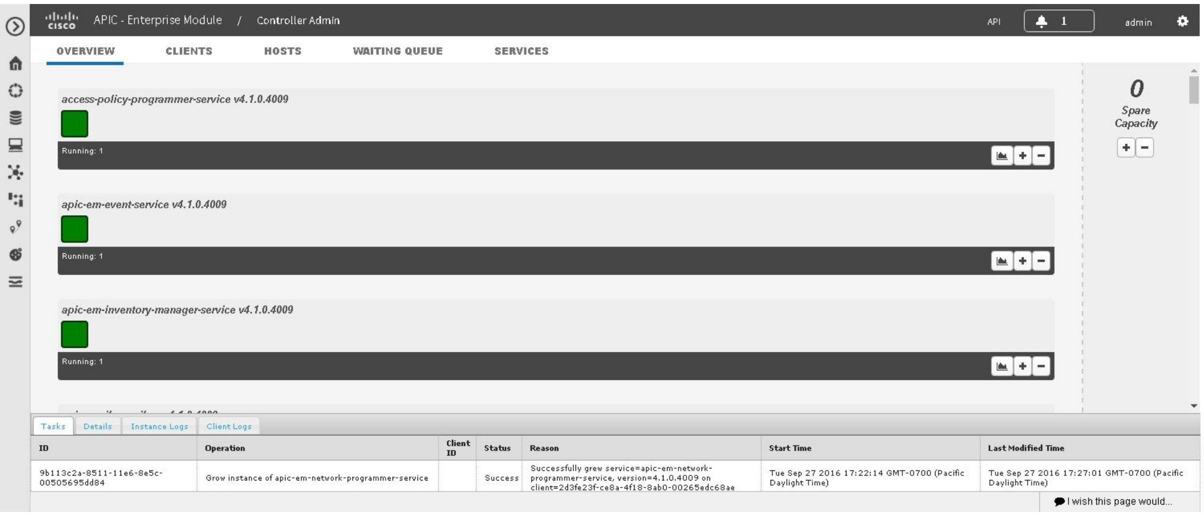
Reviewing the Service's Version, Status, and Logs

You are able to perform the following tasks using the **Controller Admin** console:

- Review the status of each service
- Review the version of each service
- Review the logs of each service

Caution Only advanced users should access the **Controller Admin** console to perform the tasks described in this procedure or attempt to troubleshoot the services.

Figure 27: Controller Admin Console


APIC - Enterprise Module / Controller Admin
API
1
admin
OVERVIEW
CLIENTS
HOSTS
WAITING QUEUE
SERVICES
access-policy-programmer-service v4.1.0.4009
Running: 1
apic-em-event-service v4.1.0.4009
Running: 1
apic-em-inventory-manager-service v4.1.0.4009
Running: 1
0
Spare Capacity
Tasks
Details
Instance Logs
Client Logs
I wish this page would...

ID	Operation	Client ID	Status	Reason	Start Time	Last Modified Time
9b113c2a-8511-11e6-8e5c-00505695dd84	Grow instance of apic-em-network-programmer-service		Success	Successfully grew service=apic-em-network-programmer-service, version=4.1.0.4009 on client=2d3fe23f-ce8a-4f18-8ab0-00265edc68ae	Tue Sep 27 2016 17:22:14 GMT-0700 (Pacific Daylight Time)	Tue Sep 27 2016 17:27:01 GMT-0700 (Pacific Daylight Time)

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **System Administration** link from the drop-down menu.

Step 3 Review the status of each service listed in the **Overview** window in the console.
Each service is represented by a square. A green colored square represents an active instance of the service, and a red colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

In a multi-host environment, a service may be represented by two green colored squares, indicating that the service is running on two different hosts within your cluster. Place your cursor over each square to view the host (IP address) that the service is running on.

Step 4 Review the version of each service in the **Overview** window in the console.
The version is located in the header of each listed service.

Step 5 Review the service logs by clicking a specific active instance of a service (green square icon) and then viewing the **Instance** or **Client** logs located at the bottom of the window.

The **Instance** logs detail information about the instance of the service. The **Client** logs detail information about the client where the service is located.

Step 6 Proceed to review the logs under the **Tasks** tab. The following information is available for the service task:

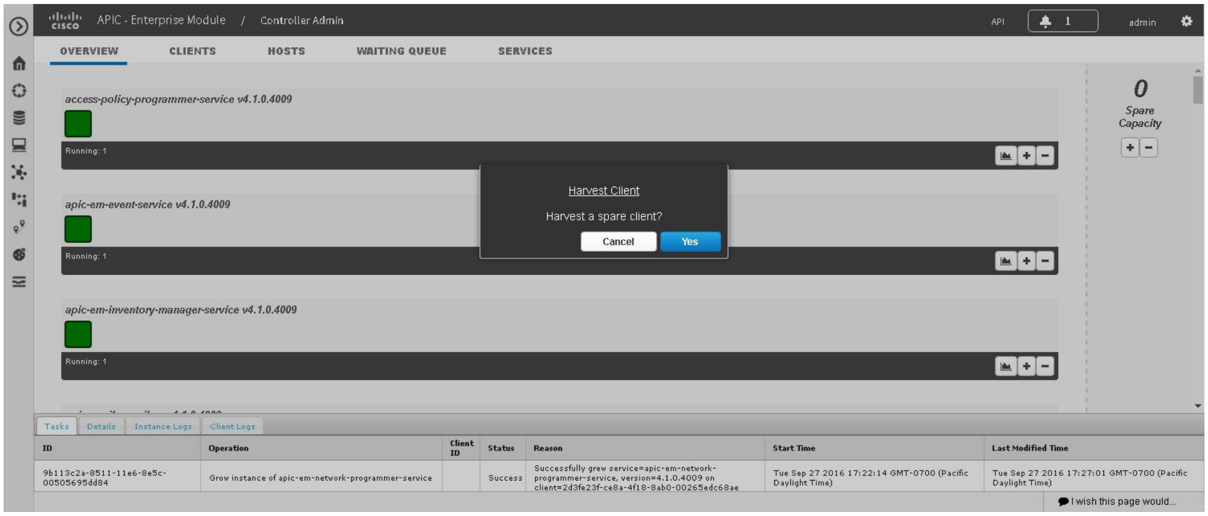
ID	Task identification number
Operation	Type of task, for example, growing a service
Client ID	Client identification number
Status	Status of the task, for example **Success** or **Failed**.
Reason	Reason given for either a successful or failed task.
Start Time	Time task stared.
Last Modified Time	Time service was last modified.

Removing a Service Instance

You are able to remove or harvest a service instance by using the **Controller Admin** console. The **Controller Admin** console tools are bundled within the ISO image and installed when you first deploy the Cisco APIC-EM.

Caution Only advanced users should access the **Controller Admin** console to perform the tasks described in this procedure or attempt to troubleshoot the services.

Figure 28: Removing (Harvesting) a Service Instance


APIC - Enterprise Module / Controller Admin
API
1
admin
OVERVIEW
CLIENTS
HOSTS
WAITING QUEUE
SERVICES
access-policy-programmer-service v4.1.0.4009
Running: 1
apic-em-event-service v4.1.0.4009
Running: 1
apic-em-inventory-manager-service v4.1.0.4009
Running: 1
0
Spare Capacity
Harvest Client
Harvest a spare client?
Cancel
Yes
Tasks
Details
Instance Logs
Client Logs
I wish this page would...

ID	Operation	Client ID	Status	Reason	Start Time	Last Modified Time
9b113c2a-8511-11e6-8e5c-00505695dd84	Grow instance of apic-em-network-programmer-service		Success	Successfully grew service=apic-em-network-programmer-service, version=4.1.0.4009 on client=2d3fe23f-ce8a-4f18-8ab0-00265edc68ae	Tue Sep 27 2016 17:22:14 GMT-0700 (Pacific Daylight Time)	Tue Sep 27 2016 17:27:01 GMT-0700 (Pacific Daylight Time)

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **System Administration** link from the drop-down menu.

Step 3 Review the list of operational services in the **Overview** window in the console.
Each service is represented by a square. A green colored square represents an active instance of the service, and a red colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

Placing your cursor over a square displays the IP address of the client where the service is running.

In a multi-host environment, a service may be represented by two green colored squares, indicating that the service is running on two different hosts within your cluster. Place your cursor over each square to view the host that the service is running on.

Note At the right of the console window are spare clients that are not running any service instances.

Step 4 Locate the service where you want to remove (harvest) an instance of a service and click the subtraction sign (-) at the lower right.
You are then prompted to confirm your action to harvest an instance.

Step 5 Choose **Yes** in the dialog box to confirm that you want to harvest an instance of the service.
The controller then proceeds to spin down the instance of the service.

When the process is finished, the square representing the service instance is removed.

What to Do Next

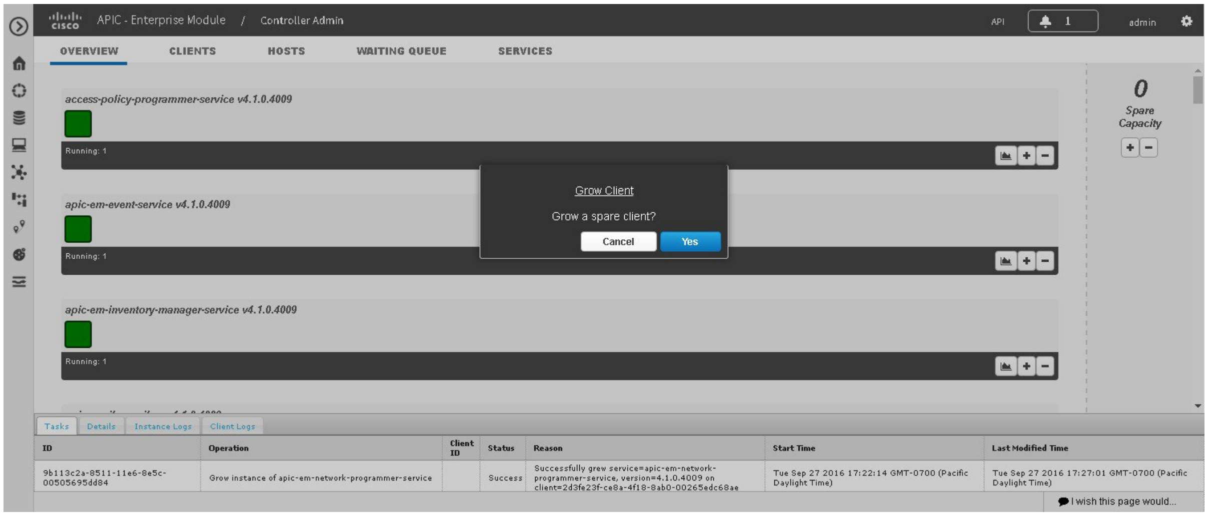
Manage your services by growing additional instances or removing (harvesting) instances from the services. When finished with the **Controller Admin** console, click another icon on the **Navigation** pane to exit the console.

Creating a Service Instance

You can create or grow a service instance using the **Controller Admin** console.

Caution Only advanced users should access the **Controller Admin** console to perform the tasks described in this procedure or attempt to troubleshoot the services.

Figure 29: Creating (Growing) a Service Instance


APIC - Enterprise Module / Controller Admin
API
1
admin
OVERVIEW
CLIENTS
HOSTS
WAITING QUEUE
SERVICES
access-policy-programmer-service v4.1.0.4009
Running: 1
apic-em-event-service v4.1.0.4009
Running: 1
apic-em-inventory-manager-service v4.1.0.4009
Running: 1
0
Spare Capacity
Grow Client
Grow a spare client?
Cancel
Yes
Tasks
Details
Instance Logs
Client Logs
I wish this page would...

ID	Operation	Client ID	Status	Reason	Start Time	Last Modified Time
9b113c2a-8511-11e6-8e5c-00505695dd84	Grow instance of apic-em-network-programmer-service		Success	Successfully grew service=apic-em-network-programmer-service, version=4.1.0.4009 on client=2d3fe23f-ce8a-4f18-8ab0-00265edc68ae	Tue Sep 27 2016 17:22:14 GMT-0700 (Pacific Daylight Time)	Tue Sep 27 2016 17:27:01 GMT-0700 (Pacific Daylight Time)

Before You Begin

You must have successfully installed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **System Administration** link from the drop-down menu.

Step 3 Review the list of operational services in the **Overview** window in the **Controller Admin** console.
Each service is represented by a square. A green colored square represents an active instance of the service, and a red colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

Placing your cursor over a square displays the IP address of the client where the service is running.

In a multi-host environment, a service may be represented by two green colored squares, indicating that the service is running on two different hosts within your cluster. Place your cursor over each square to view the host that the service is running on.

Note At the right of the console window are spare clients that are not running any service instances.

Step 4 Locate the service where you want to manually grow an instance of a service and click the addition sign (+) at the lower right.
You are then prompted to confirm your action to grow an instance.

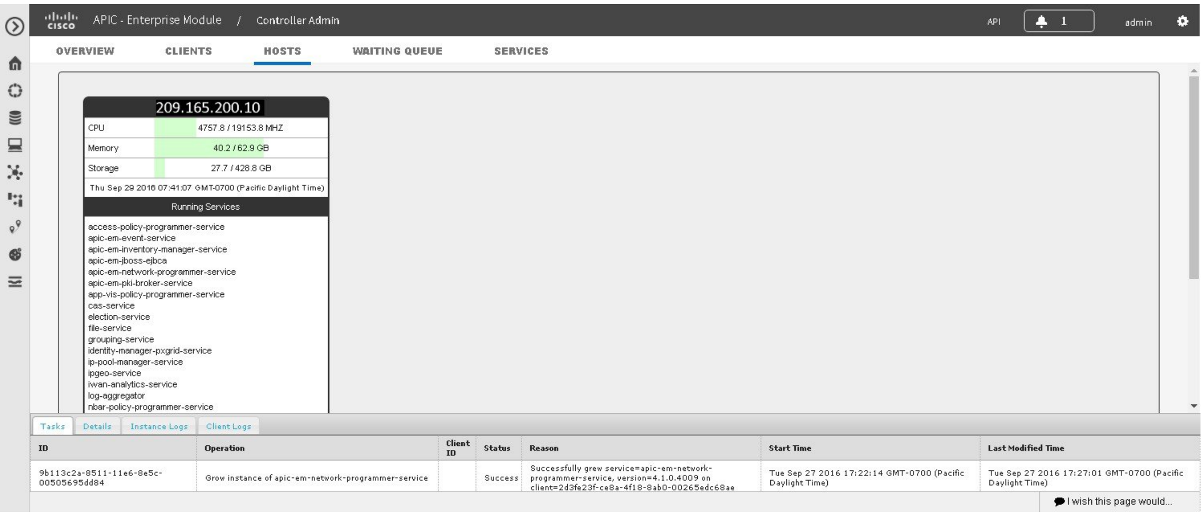
Step 5 Choose **Yes** in the dialog box to confirm that you want to grow an instance of the service.
The controller then takes a client from the **Spare Capacity Pool** and spins up an instance of the service.

When the process is finished, the square that represents the new service instance turns green.

Reviewing the Host Data

You are able to review data about the host or hosts (in a multi-host cluster) where the services are running the using the **Controller Admin** console.

Figure 30: Host Data Displayed in the Controller Admin Console



209.165.200.10

CPU	4757.8 / 19153.8 MHZ
Memory	40.2 / 62.9 GB
Storage	27.7 / 428.8 GB

Thu Sep 29 2016 07:41:07 GMT-0700 (Pacific Daylight Time)

Running Services

access-policy-programmer-service
apic-em-event-service
apic-em-inventory-manager-service
apic-em-jboss-ejbca
apic-em-network-programmer-service
apic-em-pki-broker-service
app-vis-policy-programmer-service
cas-service
election-service
file-service
grouping-service
identity-manager-pxgrid-service
ip-pool-manager-service
ipgeo-service
iwan-analytics-service
log-aggregator
nbar-policy-programmer-service

ID	Operation	Client ID	Status	Reason	Start Time	Last Modified Time
9b113c2a-8511-11e6-8e5c-00505695dd84	Grow instance of apic-em-network-programmer-service		Success	Successfully grew service=apic-em-network-programmer-service, version=4.1.0.4009 on client=2d3fe23f-ce8a-4f18-8ab0-00265edc68ae	Tue Sep 27 2016 17:22:14 GMT-0700 (Pacific Daylight Time)	Tue Sep 27 2016 17:27:01 GMT-0700 (Pacific Daylight Time)

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **System Administration** link from the drop-down menu.

Step 3 Click the **Hosts** tab to view data about the host or hosts where the services are running.
The following data is available in this view.

IP address	Host IP address
Memory	Used and available memory on the host.
Storage	Used and available storage on the host.
Date/Time	Current date and time
Running Services	List of running services on the host.