# Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide, Release 1.3.x

**First Published:** 2015-11-02

**Last Modified:** 2016-10-25

**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

# CONTENTS

# Preface



## Audience

This publication is for experienced network administrators who will deploy the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) in their network. Use this guide to deploy, make secure, access, verify, and troubleshoot the Cisco APIC-EM.

For information about using the controller's GUI for the first time, see the *Cisco APIC-EM Quick Start Guide*.

**Note** The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to within this deployment guide as a controller.

## Document Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.) |
| **bold** font | Commands and keywords and user-entered text appear in **bold** font. |
| *Italic* font | Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font. |
| `Courier` font | Terminal sessions and information the system displays appear in `courier` font. |

| Convention | Description |
|---|---|
| **Bold Courier** font | **Bold Courier** font indicates text that the user must enter. |
| [x] | Elements in square brackets are optional. |
| ... | An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| {x \| y} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

### Reader Alert Conventions

This document may use the following conventions for reader alerts:

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip** Means *the following information will help you solve a problem.*

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

**Timesaver** Means *the described action saves time.* You can save time by performing the action described in the paragraph.

**Warning** IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

# 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:
  - *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*
  - *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
  - *Open Source Used In Cisco APIC-EM*
- 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*[1]
    *Cisco IWAN on Cisco APIC-EM Configuration Guide*
  - *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*

[1] This is an updated and renamed version of the previous version of this document (*Cisco IWAN on Cisco APIC-EM Configuration Guide*).

- *Cisco Open Plug-n-Play Agent Configuration Guide*
- *Mobile Application User Guide for Cisco Network Plug and Play*

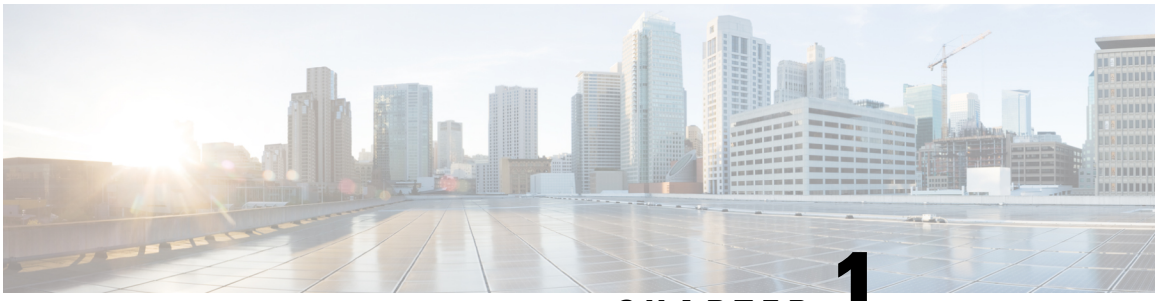
**Note** For information about developing your own application that interacts with the controller by means of the northbound REST API, see the developer.cisco.com/site/apic-em Web site.

# Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

### Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

# New and Changed Information

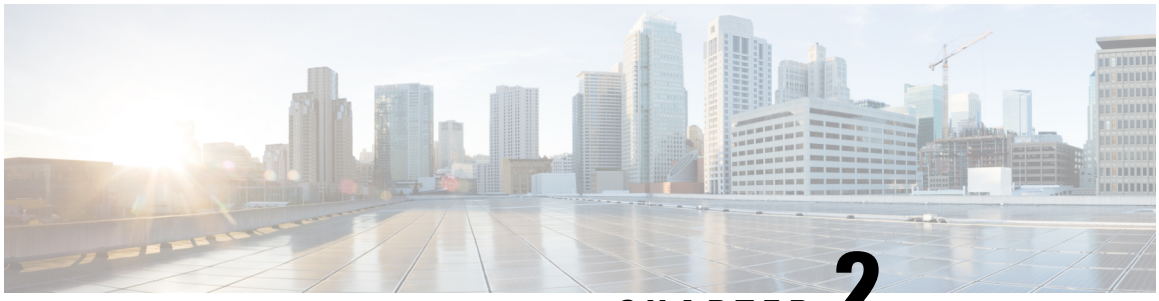


## New and Changed Information

The table below summarizes the new and changed features for the Cisco APIC-EM Release 1.3.0.x that are covered in this guide. For information about all of the new features in the release, see the Release Notes.

| Feature | Description | Where Documented |
|---|---|---|
| New **Dashboard** tab located in **Home** page. | The **Dashboard** tab contains up to six widgets that display data about the controller's applications. | See Chapter 6, Configuring the Cisco APIC-EM Settings, "Reviewing the Dashboard Tab". |
| New **Discovery Credentials** functionality. | You can now create global credentials (CLI and/or SNMP) when configuring a discovery job in the **Discovery** window of the controller's GUI. | See Chapter 6, Configuring the Cisco APIC-EM Settings, "Discovery Credentials". |
| New **Device Controllability** feature support. | You can now enable the controller to configure network devices with SNMP values during the discovery process. | See Chapter 6, Configuring the Cisco APIC-EM Settings, "Enabling Device Controllability". |
| New **Groups** feature support. | You can now create groups (selected network devices) and limit access to these groups through the user's RBAC scope. | See Chapter 6, Configuring the Cisco APIC-EM Settings, "Configuring Groups for User Permissions". |
| New PKI subordinate certificate support. | You can change the Device PKI certificate for the controller from a root certificate to a subordinate certificate using the controller's GUI. | See Chapter 6, Configuring the Cisco APIC-EM Settings, "PKI Certificate Management". |
| New configurable certificate lifetimes for the network devices. | You can change the certificate lifetime of network devices using the controller's GUI. | See Chapter 6, Configuring the Cisco APIC-EM Settings, "PKI Certificate Management". |

| Feature | Description | Where Documented |
|---|---|---|
| New default tunneling configuration for inter-host communications (Internet Protocol Security or IPsec). | The previous default tunneling protocol was Generic Routing Encapsulation (GRE).<br>**Note** For a new, fresh installation, IPSec is configured for inter-host communications. If you are updating the controller from a previous version and are currently using GRE for inter-host communications, then after the update GRE will still be used for inter-host communications. | See Chapter 5, Deploying the Cisco APIC-EM, "Configuring Cisco APIC-EM as a Single Host Using the Wizard". |
| New controller management support for individual applications on the Cisco APIC-EM. | You now have the ability to enable and disable the IWAN and Network PnP applications on the Cisco APIC-EM. | See Chapter 7, Managing the Cisco APIC-EM and Applications. "Cisco APIC-EM Application Separation". |



CHAPTER 2

# Overview



## 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. |
| 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 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.<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |
| 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.<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |

| Feature | Description |
|---|---|
| Cisco Active Advisor application | The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on:<br>• End-of-life milestones for hardware and software<br>• Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices<br>• Warranty and service contract status<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |
| Cisco Integrity Verification application | The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network devices, noting any unexpected or invalid results that may indicate compromise. The objective of the Cisco IV application is early detection of the compromise, so as to reduce its impact. The Cisco IV application operates within the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) as a beta version for this release.<br>**Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*. |
| Cisco Remote Troubleshooter application | The Cisco Remote Troubleshooter application uses the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues with your system. The app uses outbound SSH to create a secure connection to the cluster through this tunnel.<br>As an administrator, you can use the Remote Troubleshooter application to control when a support engineer has access to a particular cluster and for how long (since a support engineer cannot establish a secure tunnel on their own). You will receive indication that a support engineer establishes a remote access session, and you can end a session at any time by disabling the tunnel they are using. |
| 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. |

| Feature | Description |
|---|---|
| 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. |

# Primary Components

The following are the primary components required for a Cisco APIC-EM deployment:

- The Cisco APIC-EM software provided as an ISO image downloaded from the Cisco website
- Supported Cisco routing and switching platforms

The Cisco APIC-EM ISO image consists of the following components:

- Ubuntu 14.04 LTS 64-bit
- Open-VM-Tools
- Cisco APIC-EM services
- Grapevine Elastic Services Platform, consisting of a Grapevine root and client template

**Note** Open-VM-Tools is only installed if the ISO image is installed within a virtual machine running on vSphere. The tools will not be installed if the ISO image is installed on a bare-metal or on a hypervisor from another vendor.

For this release, you can deploy and run the Cisco APIC-EM on the following:

- Server (bare-metal hardware)—This is the recommended platform. The Cisco APIC-EM ISO image is installed directly on a server (bare-metal hardware) rather than within a host operating system (OS).

  **Note** Cisco also offers physical appliances that can be purchased with the Cisco APIC-EM ISO image pre-installed and tested.

- Virtual machine—Cisco APIC-EM ISO image is installed within a virtual machine within a VMware vSphere environment.

The Cisco APIC-EM makes use of the Ubuntu operating system environment and Linux containers (LXC). The Grapevine root runs within the host's operating system. The Grapevine clients run in LXCs within the host. The Cisco APIC-EM services that run on the Grapevine Elastic Services Platform provide the controller with its core functionality. See Chapter 3, *Cisco APIC-EM Services* for additional information about the services.

## IP Connectivity

The Cisco APIC-EM communicates with its supported platforms using the following protocols:

- SNMPv2c or SNMPv3
- Telnet or SSH

**Note** Currently, the Cisco APIC-EM supports IPv4 only. IPv6 support is planned for a future release.

# System Requirements

## System Requirements—Server (Bare-Metal hardware)

The following table lists the minimum system requirements for a successful Cisco APIC-EM server (bare-metal hardware) installation. Review the minimum system requirements for a server installation. The minimum system requirements for each server in a multi-host deployment are the same as in a single host deployment, except that the multi-host deployment requires two or three servers.

**Note** The three server, multi-host deployment provides both software and hardware high availability. The two server, multi-host deployment only provides software high availability and does not provide hardware high availability. For this reason, we strongly recommend that for a multi-host deployment three servers be used. With either two or three servers, all of the servers must reside in the same subnet.

**Caution** You must dedicate the entire server for the Cisco APIC-EM. You cannot use the server for any other software programs, packages, or data. During the Cisco APIC-EM installation, any other software programs, packages or data on the server will be deleted.

***Table 2: Minimum System Requirements—Server***

| **Server Option** | Image Format | Bare metal/ISO |
|---|---|---|

| | | |
|---|---|---|
| **Hardware Specifications** | CPU (cores) | 6 (minimum)<br>**Note** 6 CPUs is the minimum number required for your server. For better performance, we recommend using 12 CPUs. |
| | Memory | 32 GB (minimum single host deployment)<br>**Note** For a multi-host hardware deployment of 2 or 3 hosts (with 3 hosts being the maximum number supported for a multi-host deployment) 32 GB of RAM is required for each host. |
| | Disk Capacity | 500 GB of available/usable storage after hardware RAID |
| | RAID Level | Hardware-based RAID at RAID Level 10 |
| | CPU Speed | 2.4 GHz |
| | Disk I/O Speed | 200 MBps |
| | Network Adapter | 1 |
| **Networking** | Web Access | Required |
| | Browser | The following browsers are supported when viewing and working with the Cisco APIC-EM:<br>• Google Chrome, version 50.0 or later<br>• Mozilla Firefox, version 46.0 or later |

# System Requirements—Virtual Machine

The following table lists the minimum system requirements for a successful Cisco APIC-EM VMware vSphere installation. You must configure at a minimum 32 GB RAM for the virtual machine that contains the Cisco APIC-EM when a single host is being deployed. The single host server that contains the virtual machine must

have this much RAM physically available. For a multi-host deployment (two or three hosts), 32 GB of RAM is required for each of the virtual machines that contains the Cisco APIC-EM.

**Note** The three server, multi-host deployment provides both software and hardware high availability. The two server, multi-host deployment only provides software high availability and does not provide hardware high availability. For this reason, we strongly recommend that for a multi-host deployment three servers be used. With either two or three servers, all of the servers must reside in the same subnet.

***Table 3: Minimum System Requirements—Virtual Machine***

| | | |
|---|---|---|
| **Virtual Machine** | VMware ESXi Version | 5.1/5.5/6.0 |
| | Image Format | ISO |
| | Virtual CPU (vCPU) | 6 (minimum)<br>**Note** 6 vCPUs is the minimum number required for your virtual machine configuration. For better performance, we recommend using 12 vCPUs. |
| | Datastores | We recommend that you do not share a datastore with any defined virtual machines that are not part of the designated Cisco APIC-EM cluster.<br>If the datastore is shared, then disk I/O access contention may occur and cause a significant reduction of disk bandwidth throughput and a significant increase of I/O latency to the cluster. |

| | | |
|---|---|---|
| **Hardware Specifications** | Memory | 32 GB (minimum single host deployment)<br>For specific Cisco APIC-EM scale requirements, see the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.<br>**Note** For a multi-host hardware deployment of 2 or 3 hosts (with 3 hosts being the maximum number supported for a multi-host deployment) 32 GB of RAM is required for each host. |
| | Disk Capacity | 500 GB |
| | CPU Speed | 2.4 GHz |
| | Disk I/O Speed | 200 MBps |
| | Network Adapter | 1 |
| **Networking** | Web Access | Required |
| | Browser | The following browsers are supported when viewing and working with the Cisco APIC-EM:<br>• Google Chrome, version 50.0 or later<br>• Mozilla Firefox, version 46.0 or later |

| | | |
|---|---|---|
| | Network Timing | To avoid conflicting time settings, we recommend that you disable the time synchronization between the guest VM running the Cisco APIC-EM and the ESXi host. Instead, configure the timing of the guest VM to a NTP server.<br>**Important** Ensure that the time settings on the ESXi host are also synchronized to the NTP server. This is especially important when upgrading the Cisco APIC-EM. Failure to ensure synchronization will cause the upgrade to fail. |

**Related Topics**

Configuring Resource Pools Using vSphere Web Client, on page 154
Configuring a Virtual Machine Using vSphere Web Client, on page 157
Preparing a VMware System for Cisco APIC-EM Deployment, on page 151
Virtual Machine Configuration Recommendations

# Supported Multi-Host Configurations

The Cisco APIC-EM supports a single host, two host, or three host cluster configuration. With a single host configuration, 32 GB of RAM is required for that host. With a two or three host cluster configuration, 32 GB of RAM is required for each host in the cluster.

**Note** Cisco APIC-EM does not support a cluster with more than three hosts. For example, a multi-host cluster with five or seven hosts is not currently supported.

The three host cluster provides *both* software and hardware high availability. The single host or two host cluster only provides software high availability; they do not provide hardware high availability. For this reason, we strongly recommend that for a multi-host configuration three hosts be used.

A hardware failure occurs when the physical host itself malfunctions or fails. A software failure occurs when a service on a host fails. Software high availability involves the ability of the services on the host or hosts to be restarted and respun. For example, on a single host, if a service fails then that service is respun on that host. In a two host cluster, if a service fails on one host then that service is re-spun on the remaining host. In a three host cluster, if a service fails on one host, then that service is re-spun on one of the two remaining hosts.

When setting up a two host or three host cluster, you should never set up the hosts to span a LAN across slow links. This may impact the recovery time if a service fails on one of the hosts. Additionally, when configuring either a two host or three host cluster, all of the hosts in that cluster must reside in the same subnet.

For additional detailed information about multi-host clusters, see Multi-Host Support, on page 147.

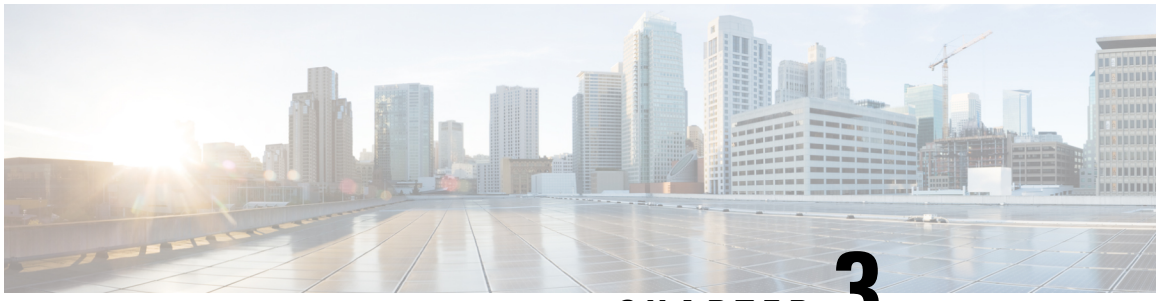
# Supported Cisco Platforms and Software Releases

For information about the supported Cisco platforms and software releases:

- See the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module* for the list of supported platforms and software releases for the base controller applications (Discovery, Inventory, Topology,EasyQoS and Path Trace).
- See the *Release Notes for Cisco IWAN on APIC-EM* for the list of supported platforms and software releases for the IWAN application.
- See the *Release Notes for Cisco Network Plug and Play* for the list of supported platforms and software releases for the Cisco Network Plug and Play application.

# Supported Northbound REST APIs

The Cisco APIC-EM provides northbound REST APIs that you can use to that you can use to issue requests to the controller and exchange data with the controller in a platform-agnostic way. For detailed information about supported northbound REST APIs, see the internal, interactive documentation located within the GUI itself. Click the **API** button at the top right of the GUI to view this documentation.



CHAPTER 3

# Cisco APIC-EM Security



## Information 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*.

# External Network Security

The Cisco APIC-EM provides its service over HTTPS and presents its X.509 server public certificate to client communications arriving at any of the external interfaces (eth0, eth1, eth2, etc.). The external clients (for example, northbound REST API consumer applications, devices performing file downloads from the controller, DMVPN certificate renewal, or certificate revocation list (CRL), etc.) may reach the controller via a NAT, proxy gateway, or directly.

The external X.509 certificate that is presented by the controller is one that has been either dynamically generated and self-signed by the controller itself, or one that has been imported (user's X.509 certificate) with a private key into the controller using the GUI. You have the option to either use the a self-signed X.509 certificate from the controller or to import and use your own X.509 certificate and private key. By default, the self-signed X.509 certificate presented to an API request is signed by Grapevine's internal Certificate Authority (CA). This self-signed X.509 certificate may not be recognized and accepted by your host. To proceed with your API request, you must ignore any warning and trust the certificate to proceed.

**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.

Northbound REST API requests from the external network to the Cisco APIC-EM are made secure using the Transport Layer Security (TLS) protocol. Although the controller supports several TLS versions, the default setting for the controller is TLS, version 1.0. You can restrict TLS support to a later and more secure version using the CLI. For additional information, see Configuring the TLS Version Using the CLI, on page 27 .

**Related Topics**

Configuring the TLS Version Using the CLI, on page 27

# Internal Network Security

Several key intra-Grapevine communications using HTTP are sent over SSL using the internal public key infrastructure (PKI). All the internal Grapevine services, database servers, and the Cisco APIC-EM services themselves listen only on the internal network in order to keep these services segmented and secured.

**Note** This PKI plane exists within the Cisco APIC-EM. This PKI plane is inaccessible to northbound REST API callers, such as third-party applications. For information about the other PKI planes, see Cisco APIC-EM PKI Planes, on page 16.

**Related Topics**

Configuring IPSec Tunneling for Multi-Host Communications, on page 29

# Device Management Network Security

Device management network security involves both controller-initiated communications and device-initiated communications.

For controller-initiated communications (discovery or pushing policy to the devices), the Cisco APIC-EM uses the following protocols to access and program network devices:

- SSH version 2
- SNMP versions 2c and 3
- Telnet (disabled by default)

**Note** If supported by the network devices, we strongly recommend using SNMP version v3c with authentication and privacy enabled. The controller does not connect to devices that are SSH version 1. HTTP and HTTPS are not supported for device discovery by the controller.

For device-initiated communications, network devices can use the following protocols to communicate and interact with the controller:

- HTTP
- HTTPS
- SNMP versions 2c

The use of HTTP or HTTPS is not up to the device itself; it is determined by the NB REST API that the device is calling. HTTP is supported for less sensitive communications.

**Related Topics**

Configuring the TLS Version Using the CLI, on page 27

# Information about PKI

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.

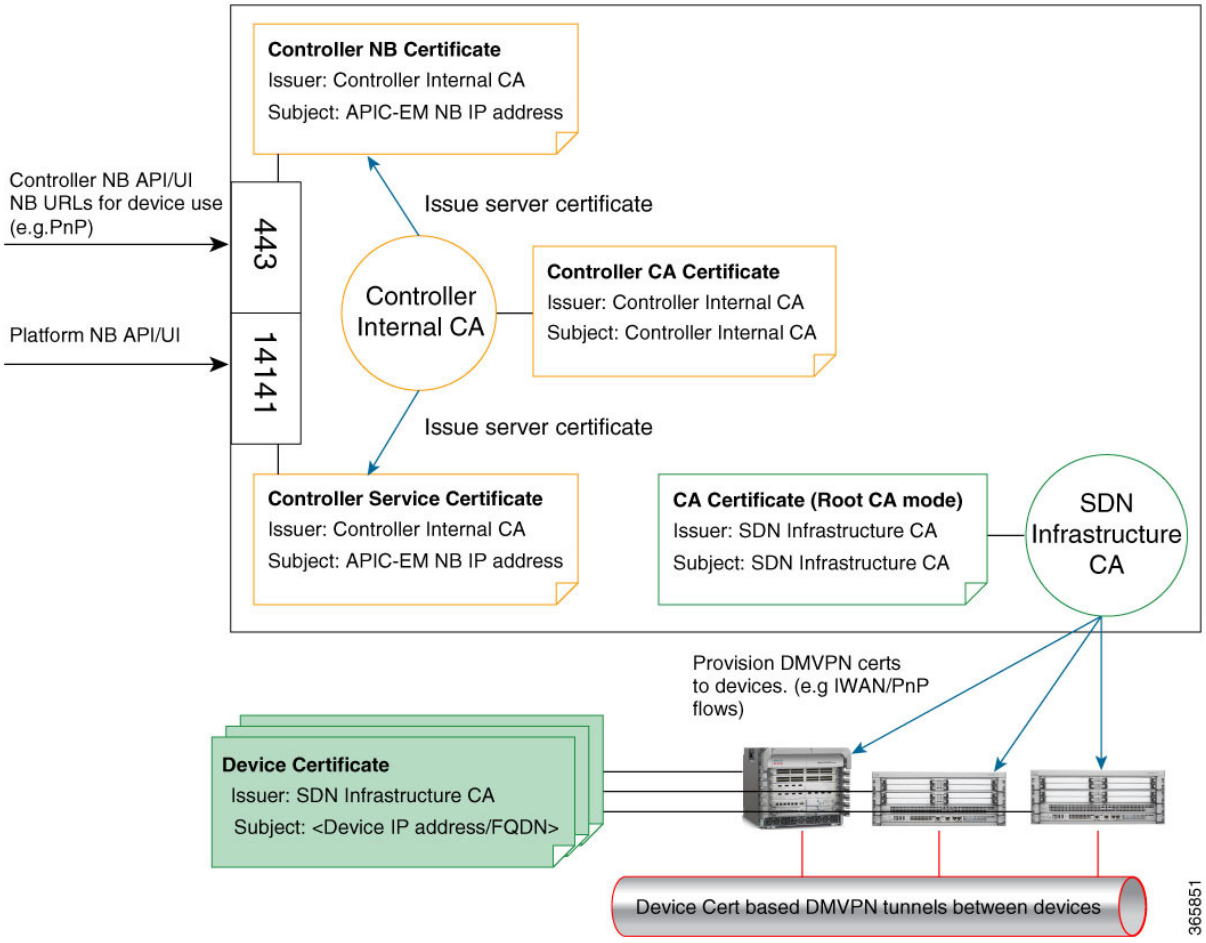
# Cisco APIC-EM PKI Planes

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 1: Cisco APIC-EM PKI Planes*




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

*Table 4: PKI Planes in Cisco APIC-EM*

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

| | Authentication | Encryption | Use Case |
|---|---|---|---|
| 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

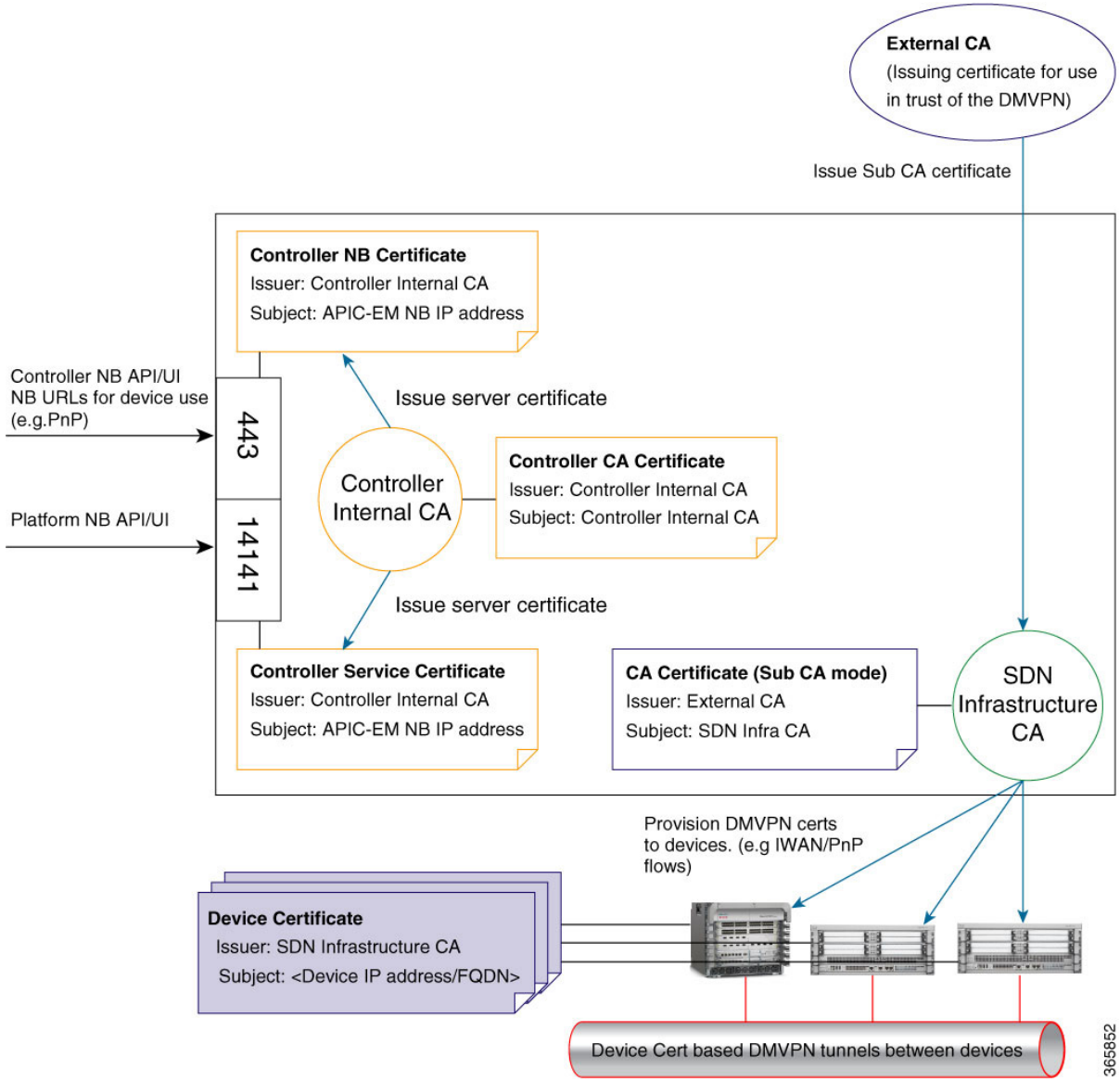
The Device PKI Plane supports two modes:

- 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 16 for a schematic of Root CA mode for the Device PKI plane.

*Figure 2: Device PKI Plane—Sub CA Mode*




### Related Topics

Changing the Role of the PKI Certificate from Root to Subordinate, on page 111
Viewing the Device Certificate Lifetime, on page 115

## 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 Viewing Audit Logs, on page 116.

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

# 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 105

# 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 105

# 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 as the common name in your certificate signing request (CSR).
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 22, 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 105

**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 105

# 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 109.

**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 108

# 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 109

# 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, on page 14
Device Management Network Security , on page 14

# 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 Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard, on page 54.

**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 Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard, on page 54..

**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, on page 14

# 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:

- Eight character minimum length.
- 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 121

# 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 5: 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 |
| 162 | SNMP | UDP |
| 443 [2] | HTTPS | TCP |
| 500 | ISAKMP<br>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 |

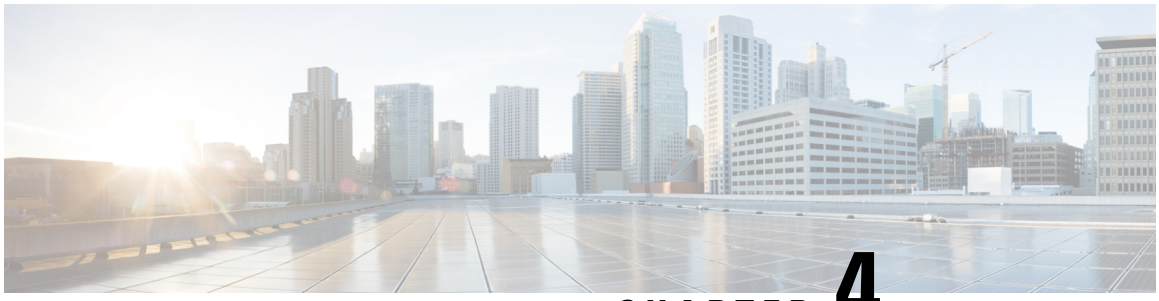
[2] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see Configuring the TLS Version Using the CLI, on page 27

*Table 6: 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 |

| Port Number | Permitted Traffic | Protocol (TCP or UDP) |
|---|---|---|
| 53 | DNS | UDP |
| 80 | Port 80 may be used for an outgoing proxy configuration.<br>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).<br>**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:<br>http://www.cisco.com/security/pki/ | TCP |
| 123 | NTP | UDP |
| 161 | SNMP agent | UDP |
| 443<br>[3] | HTTPS | TCP |
| 500 | ISAKMP<br>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 |

[3] 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 27



CHAPTER 4

# Cisco APIC-EM Services



## About Cisco APIC-EM Services

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network, using Grapevine as an Elastic Services platform to support the controller's infrastructure and services. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

The Cisco APIC-EM controls elasticity at the service level, rather than at the Grapevine client level.

## Service Managers and Monitors

The Cisco APIC-EM services that run on the Grapevine Elastic Services Platform provide the controller with its functionality. The Grapevine Elastic Services Platform consists the following components:

- Grapevine root—Handles all policy management in regards to service updates, as well as the service lifecycle for both itself and the Grapevine client.
- Grapevine client—Location where the supported services run.

After installation, service functionality is enabled using the following managers and monitors:

- Grapevine Root
  - Service manager—Starts, stops, and monitors service instances across the Grapevine clients.
  - Capacity manager—Provides on-demand capacity to run the services.
  - Load monitor—Monitors the load and health of services across the Grapevine clients.
  - Service catalog—Repository of service bundles that can be deployed on the Grapevine clients.
- Grapevine Client

- Service manager—Starts, stops, and monitors service instances on the Grapevine client.
- Service instance manager—Deploys the service.

# Service Features

The Cisco APIC-EM provides the following service features:

- Adding capacity on an existing client—When a service load exceeds a specified threshold on a client, the controller can request another service instance to start on a second, preexisting client.
- Adding capacity on a newly instantiated client—When a service load exceeds a specified threshold on a client, the controller can request a new client to be instantiated and then start another service instance on this client.
- Allows automatic scaling of services—As the service load increases, the controller instantiates additional service instances in response. As the service load decreases, the controller tears down the number of instances in response.
- Resiliency for services—When a service fails, the controller starts a replacement instance. The controller then ensures that the service's minimum instance count requirements are maintained.

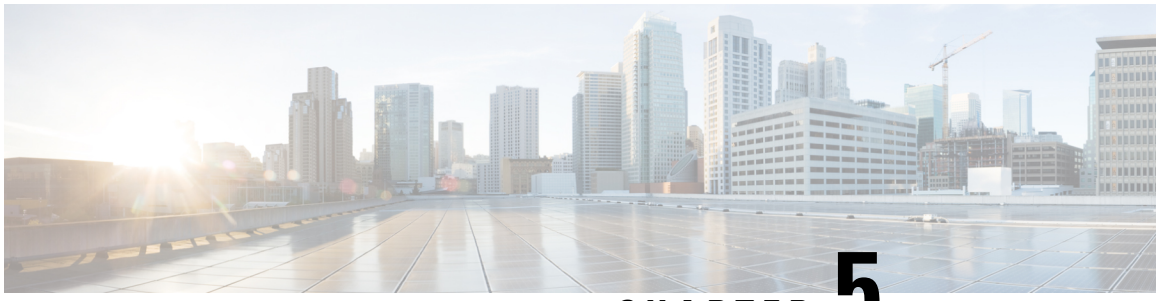
# Services

The following is a list of Cisco APIC-EM services for this release.

**Note** The Cisco APIC-EM services available on the controller is dependent upon the applications installed and enabled on the host. For information about troubleshooting services, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

- 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
- identity-manager-pxgrid-service

- ip-pool-manager-service
- ipgeo-service
- log-aggregator
- nbar-policy-programmer-service
- network-poller-service
- node-ui
- pfr-policy-programmer-service
- pnp-service
- policy-analysis-service
- policy-manager-service
- postgres
- qos-lan-policy-programmer-service
- qos-policy-programmer-service
- rbac-service
- remote-ras
- reverse-proxy
- router
- scheduler-service
- task-service
- telemetry-service
- topology-service
- visibility-service



CHAPTER 5

# Deploying the Cisco APIC-EM



# Information about the Cisco APIC-EM Deployment

You can deploy the Cisco APIC-EM on either a server (bare-metal hardware) or within a virtual machine in a VMware vSphere environment. You can also deploy the Cisco APIC-EM as either a single host or in a multi-host environment.

**Note** We recommend that you deploy the Cisco APIC-EM in a multi-host environment for enhanced scalability and redundancy.

# Pre-Deployment Checklists

## Single Host Checklists

Review the following checklists before beginning your single-host Cisco APIC-EM deployment.

**Note** A host is defined as physical server or virtual machine with instances of a Grapevine root and clients running. The Grapevine root is located in the host OS and the clients are located within Linux containers. The clients run the services within the Linux containers. You can set up either a single host deployment or multi-host deployment (2 or 3 hosts) for your network. For high availability and scale, your multi-host deployment must contain three hosts. All inbound traffic to the controller in a single host deployment is through the host IP address that you configure using the configuration wizard. All inbound traffic to the controller in a multi-host deployment is through a Virtual IP that you configure using the configuration wizard.

**Networking Requirements**

This Cisco APIC-EM deployment requires that the network adapters (NICs) on the host (physical or virtual) are connected to the following networks:

- Internet (network access required for **Make A Wish** requests and telemetry collection)
- Network with NTP server(s)
- Network with devices that are to be managed by the Cisco APIC-EM

**Note** The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment.

**IP Address Requirements**

Ensure that you have available at least one IP address for the network adapter (NIC) on the host.

The IP address is used as follows:

- Direct access to the Grapevine root
- Direct access to the Cisco APIC-EM controller (for GUI access)

**Note** If your host has 2 NICs, then you might want to have two IP addresses available and configure one IP address for each NIC.

# Multi-Host Checklists

Review the following checklist before beginning your multi-host Cisco APIC-EM deployment.

- You must satisfy the requirements for the single host deployment as described in the previous section for each host.
- Additionally, you must establish a network connection between each of the hosts using either a switch or a router. Each host must be routable with the other two hosts.
- You must configure a virtual IP (VIP).

You configure one or more NICs on each host using the configuration wizard. Each NIC that you configure must point to a non-routable network (if all your networks are routable, then you only need one NIC). A VIP is required per non-routable network. For example, if you configure 2 NICs on all 3 hosts in a multi-host cluster and each NIC points to a separate, non-routable network, then you need to configure 2 VIPs. The VIP provides an interface redundancy feature for your multi-host deployment. With a VIP, the IP address can float between the hosts.

When deploying the controller in a multi-host configuration:

- You provide a VIP address when configuring the controller using the wizard.
- On startup, the controller will bring up the VIP on one of the hosts.
- All inbound requests into controller from the external network are made via this VIP (instead of the host IP address), and the requests are routed to the services running on different hosts via the reverse-proxy service.
- If the host on which has the VIP fails, then Grapevine will bring up the VIP on one of the remaining two hosts.
- The VIP must reside in the same subnet as the three hosts.
- If you are planning to obtain a certificate issued for a multi-host environment, then it is important to get the certificate issued against the virtual IP or the host name resolvable to the virtual IP.

## Multi-Host Deployment Virtual IP

A multi-host deployment has three physical IP addresses and one virtual IP that floats across the IP addresses by design in order to provide high availability. This capability to float also means that any SSH client that wants to connect to the virtual IP address will see different host-identity public SSH keys each time the virtual IP moves its residence from one host to another host. Most SSH clients will complain that the new host is not trusted, since an entry already exists (as you might have accepted the key earlier for the older host which owned that virtual IP address before). To prevent this inconvenience, you may want to add the host keys of all the three hosts to your known hosts list as described below.

For example on a Linux or Apple Mac OS client machine, run the **ssh-keyscan** command on each of the three host physical IP addresses as follows:

```
$ ssh-keyscan -t rsa 209.165.200.30
# 209.165.200.30 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.30 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRd
SYnuCHfDiY5Pptt3BmaPgC6OlER4wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVzlwtHHZdhO6G93MyLLGsWq
XSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9oimdv.....


$ ssh-keyscan -t rsa 209.165.200.31
# 209.165.200.31 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.31 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDF57F90z2His86tEj4s75pTc7h0nfzF
2c3QweHCNN2ov474HJJcPrnWTw4DAoPpPCU6zWvR0QLxunURDb+pMeZrIIyd49xn9+OBSmBpzrnety7UB2uP
XzL1RvVxayw8mkXkj779LhFh9vkXR4DtX7XLjg.....


$ ssh-keyscan -t rsa 209.165.200.32
# 209.165.200.32 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.32 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9kwzodGzGkh/UFXVa9fptGe+sa3CBR
6SNerXxpCmfT9AOXH8xuk3/CBX+DDUQgGJVmqw6maCYKOy0RtAhGxdsNdPL6ETTKzxYB5uzw3KhcDJ6D6ob6
```

```
jdzkR6yRuXVFi2OE+u1Aqs7J8GO66FfdavU8.....
```

Next, change the IP address in the SSH key line of each output to the virtual IP address of the following and append all three key lines to the `~/.ssh/known_hosts` file and save it.

Assuming that 209.165.200.33 is the virtual IP address in the above multi-host example, you would add three lines in the `~/.ssh/known_hosts` file of your client machine as follows:

```
209.165.200.33 ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRdSYnuCHfDiY5Pptt3BmaPgC6OlER4
wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVzlwtHHZdhO6G93MyLLGsWqXSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9
oimdvPbrQPua7Zg9oblDxaBPn0Fqj00YDjKqTkp/IkZHEfHbDM996GLEbWlOvoHeCCqeZ1nWgFIqzAF+ty8+X5Z/fh
hmGe+w2tQlMfrs9pcZDaEEmq/w1W+uRohxLKs+OHnHYAbMzC6O+5fLEr2BwaZf8W016eo1WpPsxUVK6StbXBOQZrcH0
bPsUbIjKJkzafpft9Dp73pSd/vwaoB3DrvNec/PiEJYk+R.....
```

After the above change, the client will have no trouble performing uninterrupted SSH into the virtual IP address of the hosts even with the IP address floating.

# Verifying the Cisco ISO Image

Prior to deploying the Cisco APIC-EM, you can verify that the ISO image that you downloaded is a genuine Cisco image.

**Note** If you are deploying the Cisco APIC-EM from an ISO image that you downloaded, then perform this procedure. This procedure is not required, if deploying the controller with the Cisco APIC-EM Controller Appliance (Cisco APIC-EM ISO image pre-installed and tested).

### Before you begin

You must have received notification of the location of the Cisco APIC-EM ISO image or contacted Cisco support for the location of the Cisco APIC-EM ISO image.

**Step 1** Download the ISO image from the location specified by Cisco.

**Step 2** Download the Cisco public key for signature verification from the location specified by Cisco.

The Cisco public key is named:

`cisco_image_verification_key.pub`

**Step 3** Download the secure hash algorithm (SHA512) checksum file for the ISO image from the location specified by Cisco.

**Step 4** Obtain the specific release ISO image's signature file from Cisco support via email or by download from the secure Cisco website (if available).

For example, `apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.sig`.

**Step 5** (Optional) Perform a SHA verification to determine whether the ISO image was corrupted due to a partial download.

For example, run one of the following commands (depending upon your operating system):

- On a system running MAC OS X version:

```
shasum -a 512 apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

- On a Linux system:

```
sha512sum apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

Microsoft Windows does not include a built-in checksum utility, but you can install a utility from Microsoft at this link: http://www.microsoft.com/en-us/download/details.aspx?id=11533

Compare the output of the above command (or Microsoft Windows utility) to the SHA512 checksum file downloaded earlier in step 3. If the command output fails to match, download the ISO image again and run the appropriate command a second time. If the output still fails to match, contact Cisco support.

**Step 6** Verify that the ISO image is genuine and from Cisco by verifying the signature. Run the following command on the ISO image:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.sig apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

If the ISO image is genuine, then running this command should result in a **Verified OK** message. If this message fails to appear, then do not install the ISO image and contact Cisco support.

**Note** The image name and the signature names used here are only examples. Use the exact names of these files that you downloaded from the Cisco website.

This command will work in both MAC and Linux environments. For Windows, you need to download and implement OpenSSL from www.openssl.org, if you have not already done so.

### What to do next

After you verify that the ISO image is genuine and from Cisco, install the Cisco ISO image.

# Installing the Cisco ISO Image

Perform the steps in the following procedure to install the Cisco ISO image on the host (server or virtual machine).

**Note** If you are deploying the Cisco APIC-EM from an ISO image that you downloaded, then perform this procedure. This procedure is not required, if deploying the controller with the Cisco APIC-EM Controller Appliance (Cisco APIC-EM ISO image pre-installed and tested).

### Before you begin

You must review the system requirements before beginning this procedure.

You must review the Cisco APIC-EM pre-deployment checklist before beginning this procedure.

You must have downloaded and verified the Cisco ISO image by performing the tasks in the previous procedure.

For installing the Cisco APIC-EM ISO image into a virtual machine using VMware, you must create an empty virtual machine that you will attach the Cisco APIC-EM ISO image to and then boot up. When creating this virtual machine, do not accept the VMware default settings but configure the settings as per the system requirements previously listed in this guide.

**Note** See the VMware documentation for information about creating and configuring new virtual machines.

Perform one of the following procedures:

- For installing the Cisco APIC-EM ISO image on a server and from local media:
  - Burn the ISO image onto a DVD or a bootable USB flash drive.
  - Insert the DVD into the DVD drive of the physical appliance.

    If your physical appliance does not come with a DVD drive, you can connect an external USB DVD drive to the appliance and insert the disk into that external drive.
  - You can also connect a bootable USB flash drive where you burnt the ISO image to into the appliance.

    **Note** Cisco UCS servers provide an additional method of installing a remote ISO using a Virtual KVM console. See your Cisco UCS server documentation for information about this procedure. Note that installing the ISO image using a Virtual KVM console may take longer than the above methods.

- For installing the Cisco APIC-EM ISO image on a virtual machine:
  - Upload the Cisco APIC-EM ISO image directly to the virtual machine's datastore.
  - Attach the Cisco APIC-EM ISO image as a virtual CD-ROM drive of the virtual machine.

### What to do next

Boot up the host (server or virtual machine) and run the wizard to configure the Cisco APIC-EM.

# Cisco APIC-EM Configuration Wizard Parameters

When the Cisco APIC-EM software configuration begins, an interactive configuration wizard prompts you to enter required parameters to configure the controller.

**Note** Ensure that the DNS and NTP servers are reachable before you run the configuration wizard and whenever a Cisco APIC-EM host reboots in the deployment.

*Table 7: Cisco APIC-EM Configuration Wizard Parameters*

| Configuration Wizard Prompt | Description | Example |
|---|---|---|
| Host IP address | Must be a valid IPv4 address for the host.<br>This IP address is used for the network adapter (eth0) on the host and connects to the external network or networks. For multiple network adapters, have several IP addresses available. | 10.0.0.12 |
| (Optional) Virtual IP address | Must be a valid IPv4 address.<br>This virtual IP address is used for the network adapter (eth0) on the host. You should only configure a virtual IP address, if you are setting up a multi-host deployment. | 10.12.13.14 |
| Netmask IP address | Must be a valid IPv4 netmask. | 255.255.255.0 |
| Default Gateway IP address | Must be a valid IPv4 address for the default gateway. | 10.12.13.1 |
| Primary server | Must be a valid IPv4 address for the primary server. | 10.15.20.25<br>**Note** Enter either a single IP address for a single primary server, or multiple IP addresses separated by spaces for DNS servers. |
| Primary NTP server | Must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server. | 10.12.13.10<br>Enter either a single IP address for a single NTP primary server, or multiple IP addresses separated by spaces for several NTP servers. We recommend that you configure three NTP servers for your deployment. |
| Add/Edit another NTP server | Must be a valid NTP domain. | 10.12.13.11<br>Allows you to configure multiple NTP servers.<br>**Note** We recommend that you configure three NTP servers for your deployment. |

| Configuration Wizard Prompt | Description | Example |
|---|---|---|
| HTTPS proxy server | Must be a valid IPv4 address for the HTTPS proxy with port number. | https://209.165.200.11:3128 |
| Admin Username | Identifies the administrative username used for GUI access to the Cisco APIC-EM controller.<br>We recommend that the username be three to eight characters in length and be composed of valid alphanumeric characters (A–Z, a–z, or 0–9). | admin2780 |
| Admin Password | Identifies the administrative password that is used for GUI access to the Cisco APIC-EM controller. You must create this password because there is no default. The password meet the following requirements:<br>• Eight character minimum length.<br>• Does NOT contain a tab or a line break.<br>• Does contain characters from at least three of the following categories:<br>  • Uppercase alphabet<br>  • Lowercase alphabet<br>  • Numeral<br>  • Special characters (for example, ! or #) | MyIseYPass2 |
| Linux Username | Identifies the Linux (Grapevine) username used for CLI access to the Grapevine root and clients. | The default is 'grapevine' and cannot be changed. |

| Configuration Wizard Prompt | Description | Example |
|---|---|---|
| Linux Password | Identifies the Linux (Grapevine) password that is used for CLI access to the Grapevine roots and clients. You must create this password because there is no default. The password meet the following requirements:<br>• Eight character minimum length.<br>• Does NOT contain a tab or a line break.<br>• Does contain characters from at least three of the following categories:<br>  • Uppercase alphabet<br>  • Lowercase alphabet<br>  • Numeral<br>  • Special characters (for example, ! or #) | MyGVPass01 |

# Configuring Cisco APIC-EM as a Single Host Using the Wizard

Perform the steps in the following procedure to configure Cisco APIC-EM as a single host using the wizard.

### Before you begin

You must have either received the Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a server or virtual machine as described in the previous procedures.

**Step 1** Boot up the host.

**Step 2** Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed.

**Note** You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

**Step 3** Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option to begin.

You are then prompted to enter values for the **NETWORK ADAPTER #1 (eth0)**.

**Step 4** Enter configuration values for the **NETWORK ADAPTER #1 (eth0)** on the host.

The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has three network adapters you are prompted to confirm configuration values for network adapter #1 (eth0), network adapter #2 (eth1), and network adapter #3 (eth2) respectively.

**Note** The primary interface for the controller is eth0 and it is best practice to ensure that this interface is made highly available.

On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

| | |
|---|---|
| **Host IP address** | Enter the host IP address to use for the network adapter. This host IP address (and network adapter) connects to the external network or networks.<br>These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.<br>**Note** The configuration wizard validates the value entered and issues an error message if incorrect. If you receive an error message for the host IP address, then check to ensure that eth0 (ethernet interface) is connected to the correct network adapter. |
| **Virtual IP** | (Optional) Enter a virtual IP address to use for this network adapter. You should only configure a virtual IP address, if you are setting up a multi-host deployment.<br>**Note** For additional information about virtual IP, see Multi-Host Deployment Virtual IP, on page 41 |
| **Netmask** | Enter the netmask for the network adapter's IP address. |
| **Default Gateway IP address** | Enter a default gateway IP address to use for the network adapter.<br>**Note** If no other routes match the traffic, traffic will be routed through this IP address. |
| **DNS Servers** | Enter the DNS server or servers IP addresses (separated by spaces) for the network adapter. |

| | |
|---|---|
| **Static Routes** | If required for your network, enter a space separated list of static routes in this format: <network>/<netmask>/<gateway><br><br>Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes. |

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation and if your host has two network adapters, you are prompted to enter values for **NETWORK ADAPTER #2 (eth1)**. If your host has three network adapters, you are prompted to enter values for **NETWORK ADAPTER #2 (eth1)** and **NETWORK ADAPTER #3 (eth2)**. If you do not have any additional network adapters or if you do not have more than one non-routable network, then proceed directly to the next step.

**Step 5** If the controller is being deployed in your network behind a proxy server and the controller's access to the Internet is through this proxy server, then enter configuration values for the **HTTPS PROXY**.

**Note** If there is no proxy server between the controller and access to the Internet, then this step will not appear. Instead, you will be prompted to enter values for **CLOUD CONNECTIVITY**.

| | |
|---|---|
| **HTTPS Proxy** | Enter the protocol (HTTP or HTTPS), IP address, and port number of the proxy.<br><br>For example, enter **https://209.165.200.11:3128** |
| **HTTPS Proxy Username** | Enter the username, if authentication is required for the proxy. |
| **HTTPS Proxy Password** | Enter the password, if authentication is required for the proxy. |

After configuring the **HTTPS PROXY**, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for **CLOUD CONNECTIVITY**.

**Step 6** Enter configuration values for **CLOUD CONNECTIVITY**.

| | |
|---|---|
| **CCO Username** | Enter a Cisco Connection Online (CCO) username for cloud connectivity. For example, enter the username that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner.<br>**Note** If you do not have a CCO username and password, then enter your company name in the username and company name fields and leave the password field empty for this step. This will permit you to proceed through the config-wizard process. Values entered for this step are used for telemetry collection. For information about telemetry collection, see Telemetry Collection, on page 124. |
| **CCO Password** | Enter a Cisco Connection Online (CCO) password for the CCO *username*. For example, enter the password that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner. |
| **Company Name** | Enter the company or organization's name with which you are affiliated. |

Once satisfied with the cloud connectivity settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values entered. After validation, you are then prompted to enter values for the **LINUX USER SETTINGS**.

**Step 7** Enter configuration values for the **LINUX USER SETTINGS**.

| | |
|---|---|
| **Linux Password** | Enter a Linux password.<br>The Linux password is used to ensure security for both the Grapevine root and clients located on the host (appliance, server, or virtual machine). Access to the Grapevine root and clients by you or the controller requires this password.<br>The default username is grapevine.<br>For information about the requirements for a Linux password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security.<br>**Note** The Linux password is encrypted and hashed in the controller database. |
| **Re-enter Linux Password** | Confirm the Linux password by entering it a second time. |

| | |
|---|---|
| **Seed Phrase Password Generation** | (Optional) Instead of creating and entering your own password in the above **Linux Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase.<br>Enter a seed phrase and then press <**Generate Password**> to generate the password. |
| **Auto Generated Password** | (Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password.<br>**Note** When finished with the password, be sure to save it to a secure location for future reference.<br>Press <**Use Generated Password**> to save the password. |

After configuring the Linux password, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for the **APIC-EM ADMIN USER SETTINGS**.

**Step 8** Enter configuration values for the **APIC-EM ADMIN USER SETTINGS**.

| | |
|---|---|
| **Administrator Username** | Enter an administrator username.<br>Your administrator username and password are used to ensure security for the controller itself. Access to the controller's GUI requires that you enter this username and password. |
| **Administrator Password** | Enter an administrator password.<br>For information about the requirements for an administrator password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security.<br>**Note** The administrator password is encrypted and hashed in the controller database. |
| **Re-enter Administrator Password** | Confirm the administrator password by entering it a second time. |
| **Seed Phrase Password Generation** | (Optional) Instead of creating and entering your own password in the above **Administrator Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase.<br>Enter a seed phrase and then press <**Generate Password**> to generate the password. |

| | |
|---|---|
| **Auto Generated Password** | (Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password.<br>**Note** When finished with the password, be sure to save it to a secure location for future reference.<br>Press <**Use Generated Password**> to save the password. |

After configuring the administrator password, enter **next>>** to proceed.

After entering **next>>**, you are then prompted to enter values for either the **NTP SERVER SETTINGS**.

**Step 9** Enter configuration values for **NTP SERVER SETTINGS**.

| | |
|---|---|
| **NTP servers** | Enter a single NTP server address or a list of NTP servers each separated by a space.<br>The Elastic Services Platform (Grapevine) manages a Network Time Protocol (NTP) server to provide time synchronization for the Grapevine clients. You must configure the NTP server for the clients. The NTP server is external to the cluster.<br>**Note** We recommend that for redundancy purposes, you configure at least three NTP servers for your Cisco APIC-EM deployment. |

**Note** Cisco routers can also be configured as NTP servers.

After configuring the NTP server(s), enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for **INTER-HOST COMMUNICATION**.

**Step 10** Enter configuration values for **INTER-HOST COMMUNICATION**.

| | |
|---|---|
| **Enable IPSec Encryption** | You can configure IPSec tunneling for communications between the hosts in a multi-host cluster. By selecting *yes*, you configure IPSec tunneling.<br>The default is IPSec and the default option is set to *yes*. |

Once satisfied with the inter-host communication setting, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

**Step 11** Enter configuration values for **CONTROLLER CLEAN-UP**.

| | |
|---|---|
| **Harvest All Virtual Disks** | Entering **yes** will delete all Grapevine virtual disks that belong to the controller for this specific deployment.<br>For an initial configuration, enter **no**. |
| **Delete All Clients** | Entering **yes** will delete all Grapevine clients that belong to the controller for this specific deployment.<br>For an initial configuration, enter **no**. |

For an initial configuration, enter **no** for both options.

After configuring the controller clean-up, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values to finish the configuration and begin the configuration wizard installation.

**Step 12** 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.

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

**Step 13** Open your browser and enter the host IP address to access the Cisco APIC-EM GUI.

You can use the displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

**Step 14** After entering the IP address in the browser, a message stating that "Your connection is not private" appears.

Ignore the message and click the **Advanced** link.

**Step 15** After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.

Ignore the message and click the link.

**Note** This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

**Step 16** In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

### What to do next

For a multi-host deployment, perform the following procedure to configure another host and join it with this host to create a cluster.

For a single-host deployment, begin to use the Cisco APIC-EM to manage and configure your network.

**Note** You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens an email. Use this email to send a comment on the current window or to send a request to the Cisco APIC-EM development team.

# Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard

Perform the steps in this procedure to configure Cisco APIC-EM on your host and to join it to another, pre-existing host to create a cluster. Configuring the Cisco APIC-EM on multiple hosts to create a cluster is best practice for both high availability and scale.

**Caution**

- When joining a host to a cluster as described in the procedure below, there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that is being joined to.
- When joining the additional hosts to form a cluster be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- You should also expect some service downtime when the adding or removing hosts to a cluster, since the services are then redistributed across the hosts. Be aware that during the service redistribution, there will be downtime.

### Before you begin

You must have either received a Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a second server or virtual machine.

You must have already configured Cisco APIC-EM on the first host (server or virtual machine) in your planned multi-host cluster following the steps in the previous procedure. This procedure must be run on the second host that you are joining to the cluster. When joining the new host to the cluster, you must specify an existing host in the cluster to connect to.

**Note** The Cisco APIC-EM multi-host configuration supports the following two workflows:

- You first configure a single host running Cisco APIC-EM in your network. After performing this procedure, you then use the wizard to configure and join two additional hosts to form a cluster.
- If you already have several single hosts configured with Cisco APIC-EM, you can use the configuration wizard to join two additional hosts to a single host to form a cluster.

**Step 1** Boot up the host.

**Step 2** Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed with the deployment.

**Note** You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

**Step 3** Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose one of the two displayed options to begin.

- **Create a new APIC-EM cluster**
- **Add this host to an existing APIC-EM cluster**

For the multi-host deployment, click the **Add this host to an existing APIC-EM cluster** option.

**Step 4** Enter configuration values for the **NETWORK ADAPTER #1 (eth0)** on the host.

The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has two network adapters you are prompted to confirm configuration values for network adapter #1 (eth0) and network adapter #2 (eth1).

**Note** On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

| | |
|---|---|
| **Host IP address** | Enter a host IP address to use for the network adapter. This host IP address connects to the external network or networks.<br>**Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI. |
| **Netmask** | Enter the netmask for the network adapter's IP address. |

Later in this procedure, the following information will be discovered and copied from the cluster to the configuration file of this host:

- Default Gateway IP address
- DNS Servers
- Static Routes

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation, you are then prompted to enter values for the **APIC-EM CLUSTER SETTINGS**.

**Step 5** Enter configuration values for the **APIC-EM CLUSTER SETTINGS**.

| | |
|---|---|
| **Remote Host IP** | Enter the eth0 IP address of the pre-configured host that you are now joining to form a cluster.<br>**Note** If a virtual IP address has already been configured on another host for a multi-host cluster, you may also enter that IP address value. This field accepts either the IP address of a pre-configured host to the cluster or the virtual IP address of the cluster. |

| | |
|---|---|
| **Administrator Username** | Enter an administrator username.<br>This is the administrator username on the pre-configured host that you are now joining to form a cluster. |
| **Administrator Password** | Enter an administrator password.<br>This is the administrator password on the pre-configured host that you are now joining to form a cluster. For information about the requirements for an administrator password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security.<br>**Note** The administrator password is encrypted and hashed in the controller database. |

After configuring the administrator cluster settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard then proceeds to prepare the host to join the cluster.

You will receive a message to please wait, while the remote cluster is being queried and data is retrieved.

**Step 6** Enter configuration values for the **Virtual IP**.

**Note** If you are joining the host to a cluster where the virtual IP has already been configured, then you will not be prompted for virtual IP configuration values. If you are joining the host to a cluster where a virtual IP has not yet been configured, then you will be prompted for virtual IP configuration values.

| | |
|---|---|
| **Virtual IP** | Enter the virtual IP address to use for the network that the controller is directed to.<br>**Note** For additional information about virtual IP, see Multi-Host Deployment Virtual IP, on page 41 |

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

**Step 7** (Optional) Enter additional configuration values for the **Virtual IP**.

The configuration wizard proceeds to continue its discovery of any pre-existing configuration values on the hosts in the cluster. Depending upon what the configuration wizard discovers, you may be prompted to enter additional configuration values. For example:

- If eth1 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth1. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth2 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth2. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth3 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for this eth3. You are also prompted for a VIP, if it has not yet been configured for this NIC.

**Note** This configuration wizard discovery process and prompting continues for the number of configured Ethernet ports in the cluster.

| | |
|---|---|
| **Virtual IP** | Enter the virtual IP address to use for the network that the controller is directed to. |
| **IP address** | Enter an IP address to use for this network adapter. This IP address connects to the external network or networks.<br>**Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI. |

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

**Step 8** A final message appears stating that the wizard is now ready to proceed to join the host to the cluster.

The following options are available:

- **[back]**—Review and verify or modify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin the process to join this host to the specified Cisco APIC-EM.

Enter **proceed>>** to proceed. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

At the end of the configuration process, a successful configuration message appears.

**Step 9** Open your browser and enter an IP address to access the Cisco APIC-EM GUI.

You can use the first displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

**Note** The first displayed IP address can be used to access the Cisco APIC-EM GUI. The second displayed IP address accesses the network where the devices reside.

**Step 10** After entering the IP address in the browser, a message stating that "Your connection is not private" appears.

Ignore the message and click the **Advanced** link.

**Step 11** After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.

Ignore the message and click the link.

**Note** This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

**Step 12** In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

### What to do next

Proceed to follow the same procedure described here to join the third and final host to the multi-host cluster.

**Note** You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens an email. Use this email to send a comment on the current window or to send a request to the Cisco APIC-EM development team.

# Powering Down and Powering Up a Single Host or Multi-Host Cluster

Under certain circumstances such as troubleshooting, you might want to gracefully power down and then power up either a single host or a multi-host cluster. This procedure describes how to perform these procedures.

For information about powering down and powering up a single host within a multi-host cluster, see Powering Down and Powering Up a Single Host Within a Multi-Host Cluster, on page 60.

### Before you begin

You should have deployed the Cisco APIC-EM following the procedures in this 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.

### What to do next

Log back into the controller's GUI and begin working with the Cisco APIC-EM to manage and monitor the devices within your network.

# Powering Down and Powering Up a Single Host Within a Multi-Host Cluster

Under certain circumstances such as troubleshooting, you might want to gracefully power down and then power up a single host within a multi-host cluster. For example, to perform maintenance on that host while keeping the Cisco APIC-EM controller running and functional. This procedure describes how to perform this procedure.

**Important** This procedure uses the **grape host evacuate** command. The **grape host evacuate** command only works in a 3 host cluster (not a 1 or 2 host cluster). For a 2 host cluster, instead of using **grape host evacuate** command, use the standard host removal process to first remove the host you want to remove from the cluster, then reattach it back into the cluster. For detailed information, see "Troubleshooting Cisco APIC-EM Multi-Host" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

### Before you begin

You should have deployed the Cisco APIC-EM following the procedures in this guide.

All of the hosts in a multi-host cluster need to be functional and running prior to beginning this procedure.

**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 **grape host display** command to review the command output and determine the *host_id* of the host that you want to power off.

**Step 4** Enter the **grape host evacuate** command to harvest (gracefully shut down) the services on the host.

Use the *host_id* for this command that you determined in the previous step.

```
$ grape host evacuate host_id
```

This command harvests all services running on the specified host (*host_id*) using the **grape host evacuate** command. In a multi-host cluster, the services on the specified host are harvested and transferred to the other two hosts in the cluster.

**Important** The **grape host evacuate** command only works in a 3 host cluster (not a 1 or 2 host cluster). For a 2 host cluster, instead of using **grape host evacuate** command, use the standard host removal process to first remove the host you want to remove from the cluster, then reattach it back into the cluster. For detailed information, see "Troubleshooting Cisco APIC-EM Multi-Host" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

**Step 5** Power down the host, by entering the following command:

```
$ sudo shutdown -h now
```

**Note** Enter your password a second time when prompted.

**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 back on.

**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 host enable host_id
```

The host ID to enter for this command must be the same as the host ID used in the **grape host evacuate** command in step 4.

Wait a few minutes for the Cisco APIC-EM services to start up again.

### What to do next

Log back into the controller's GUI and begin working with the Cisco APIC-EM to manage and monitor the devices within your network.

# Uninstalling the Cisco APIC-EM

The following procedure describes how to uninstall the Cisco APIC-EM.

**Note** If you plan to reinstall the Cisco APIC-EM after uninstalling it, then you must follow the procedure described below to avoid any possible problems. You should have also contacted Cisco support for the link to download the latest Cisco APIC-EM ISO image. Be aware that 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 and if you are reinstalling the Cisco APIC-EM, then you will need to access the host and restart it.

**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 appliance to the external network.

**Step 2** Enter the Linux username ('grapevine') and password when prompted.

**Step 3** Enter the **reset_grapevine factory** command at the prompt.

```
$ reset_grapevine factory
```

**Step 4** Enter your Linux grapevine password a second time to start the reset process.

```
$ sudo password for grapevine *********
```

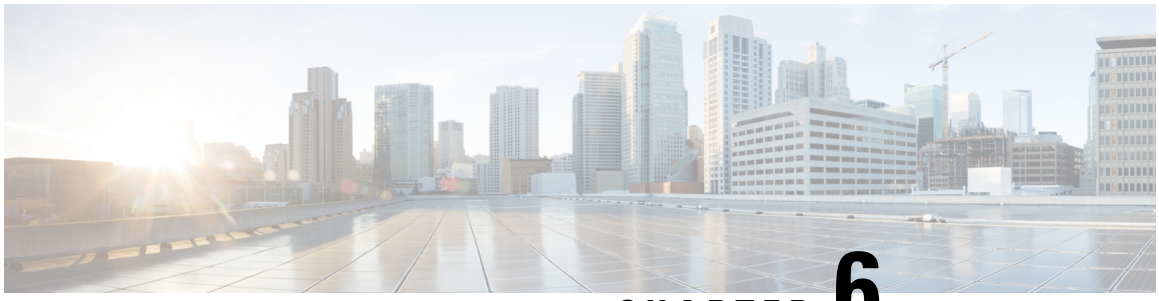
After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

You are then prompted to confirm your intent 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
- Stops and shuts down any Linux containers
- 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)



CHAPTER 6

# Configuring the Cisco APIC-EM Settings



## Logging into the Cisco APIC-EM

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

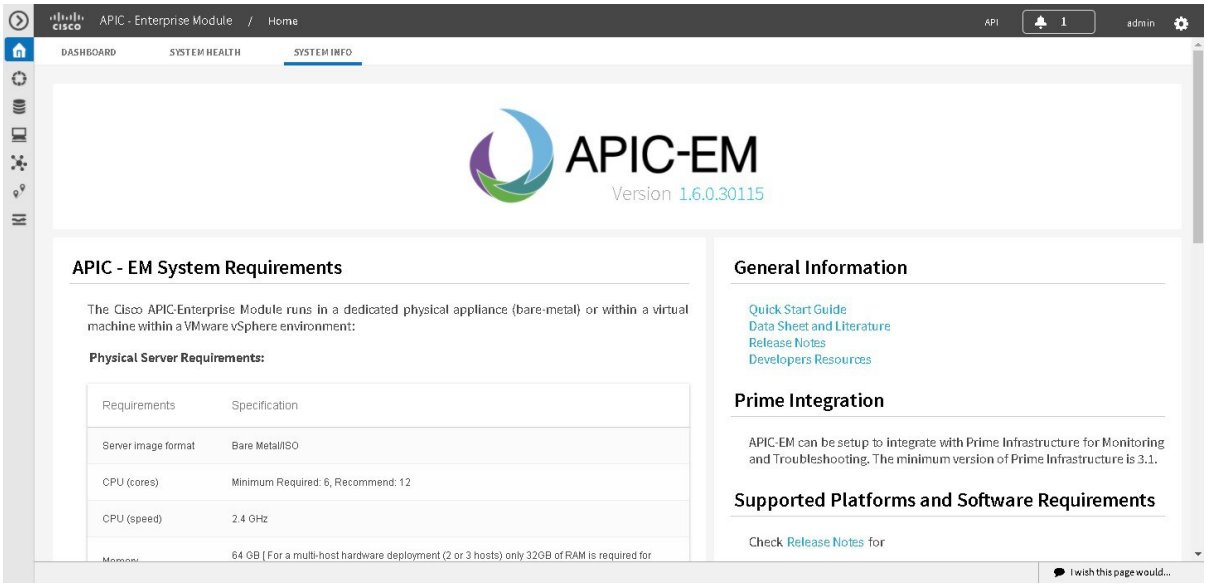
**https://***IP address*

**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**

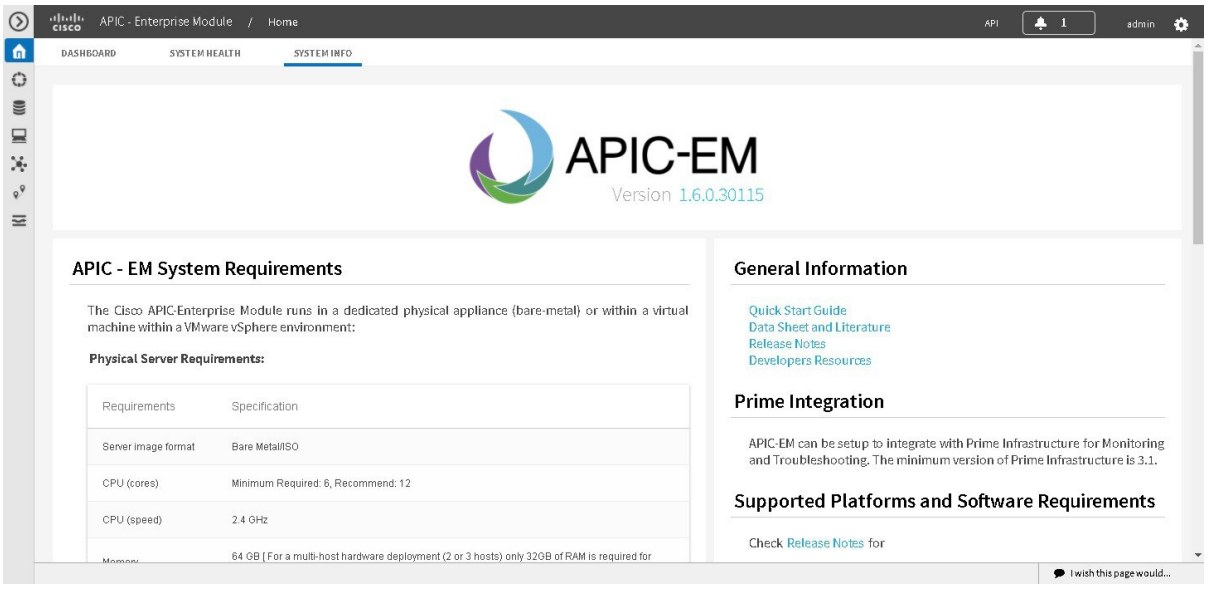
*Figure 3: SYSTEM INFO Tab*




# 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 4: SYSTEM INFO Tab*



### 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 the chapter, "Managing Users".

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

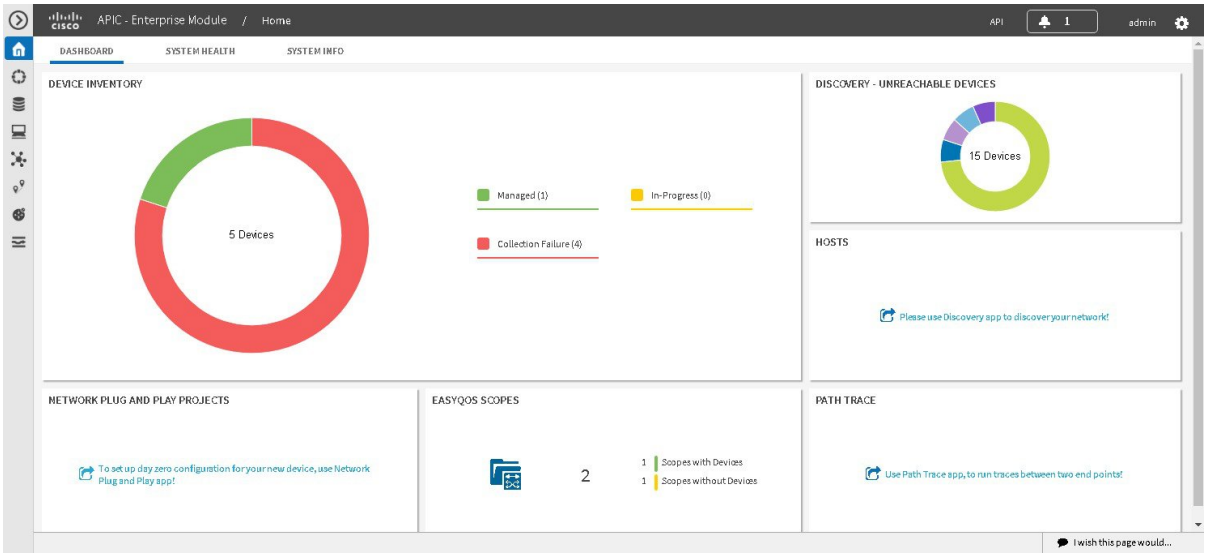
Click the datasheet links or Cisco DevNet links for additional information about the controller and access to Cisco DevNet, respectively.

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 5: DASHBOARD Tab*




### 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 the chapter, "Managing Users".

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.<br>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.<br>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:<br>• Pending<br>• In Progress<br>• Failed<br>• Provisioned<br>**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).<br>**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.<br>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.<br>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:<br>• Provisioned<br>• Pre-Provisioned<br>• In-Progress<br>• Failed<br>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.

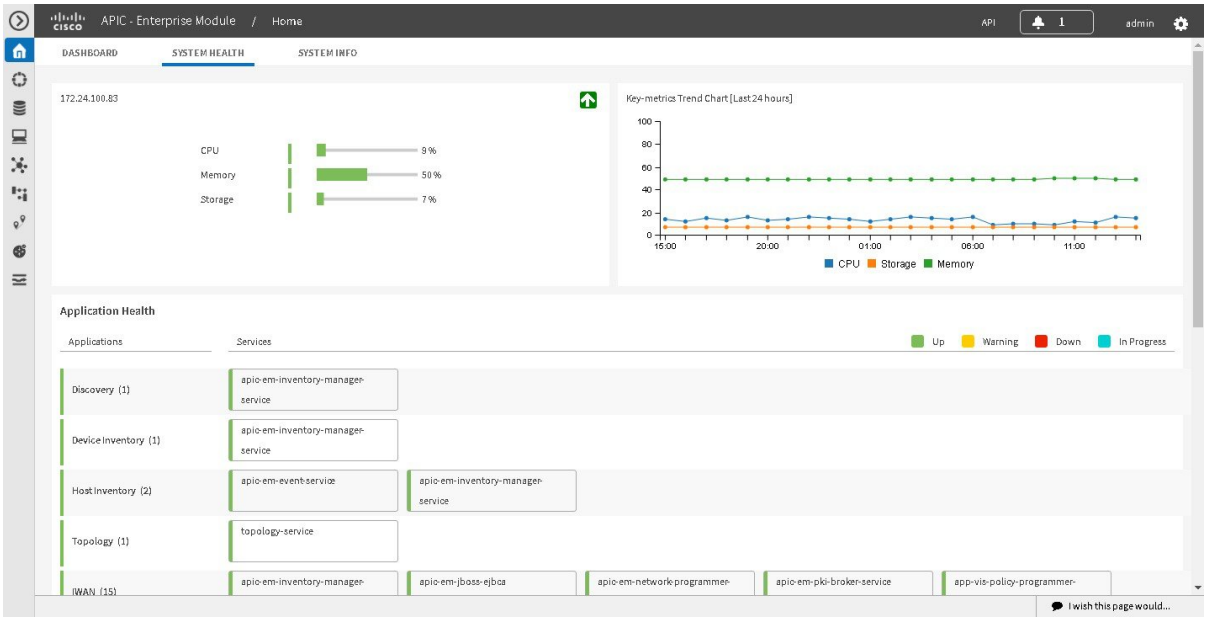
### What to do next

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 6: SYSTEM HEALTH Tab*




### 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 the chapter, "Managing Users".

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:<br>• Host IP address<br>• CPU—Host CPU usage is displayed in MHZ. Both the currently used and available host CPU is displayed.<br>• Memory—Host memory usage is displayed in GB. Both the currently used and available host memory is displayed.<br>• Storage—Host storage usage is displayed in GB. Both the currently used and available host storage is displayed.<br>**Note** If you have configured a multi-host cluster, then each host's data (CPU, memory, and storage) will be displayed in the UI.<br>Color indicates status for the above host data:<br>• Green—Indicates proper usage and support.<br>• Blue—Indicates usage is approaching improper levels and triggers this warning (color change).<br>• Orange—Indicates a failure based upon the usage exceeding the maximum supported value.<br>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.<br>**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.<br><br>Color bars indicate the status for the applications and the supporting service(s):<br><br>• 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).<br><br>• Yellow—Indicates application instance and its supporting service instance(s) are experiencing issues and triggers this warning (color change).<br><br>• 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).<br><br>• 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.

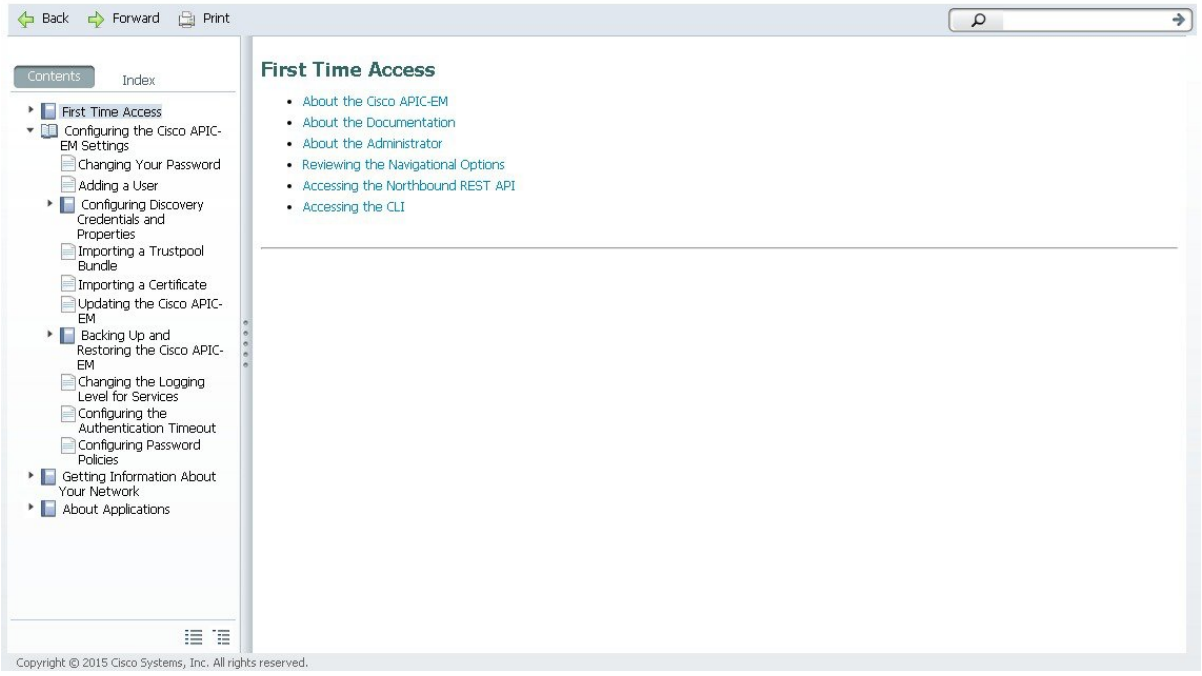
# Quick Tour of the APIC-EM Graphical User Interface (GUI)

For a quick introduction to the Cisco APIC-EM GUI, log into the Cisco APIC-EM controller as an administrator and follow the procedure below.

**Step 1** Click the **Quick Start Guide** link that appears on the Cisco APIC-EM **Home** page.

The *Quick Start Guide* opens in a separate window.

***Figure 7: Quick Start Guide***




**Step 2** Take a few moments to review the contents of the *Quick Start Guide*, which provides a short introduction to the main components of the Cisco APIC-EM graphical user interface and briefly describes how to configure some of the Cisco APIC-EM settings.

### What to do next

If you are using the IWAN application with Cisco Prime Infrastructure for your network, then proceed to configure your Prime credentials. If you are not using the IWAN application with Cisco Prime Infrastructure, then proceed to configure the discovery credentials for your network.

# User Settings

## 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 82. For information about configuring external controller authentication, see Configuring External Authentication, on page 84.

## 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.

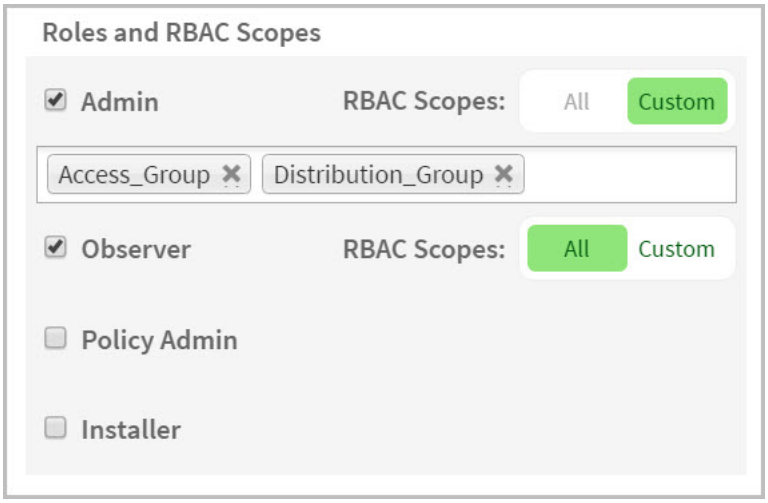
# RBAC Scopes

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 8: Example of RBAC Scope Assignment*




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.

# 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*.

# 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 82.
- 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 Authentication, on page 84.

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 RBAC Scope for Users within your Network

You can use the following workflow to assist in configuring RBAC scope for users and devices within your network.

1. Discover the devices within your network.

   Run a discovery on the devices within your network using the **Discovery** functionality of the controller. For information about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

2. Create a set of groups consisting of network devices for user access.

   For information about this procedure, see Configuring Groups for User Access, on page 79.

3. Assign network devices to their relevant groups.

   For information about this procedure, see Configuring Groups for User Access, on page 79.

4. Create internal users for the controller and assign their roles and RBAC scope.

   For information about this procedure, see Creating Internal Users, on page 82.

5. Configure external authentication and authorization for users from an AAA server.

   For information about this procedure, see Configuring External Authentication, on page 84.

6. View external users that have access to the Cisco APIC-EM using the controller's GUI.

   For information about this procedure, see Viewing External Users, on page 89.

## Configuring Groups for User Access

The Cisco APIC-EM supports the configuration of groups.

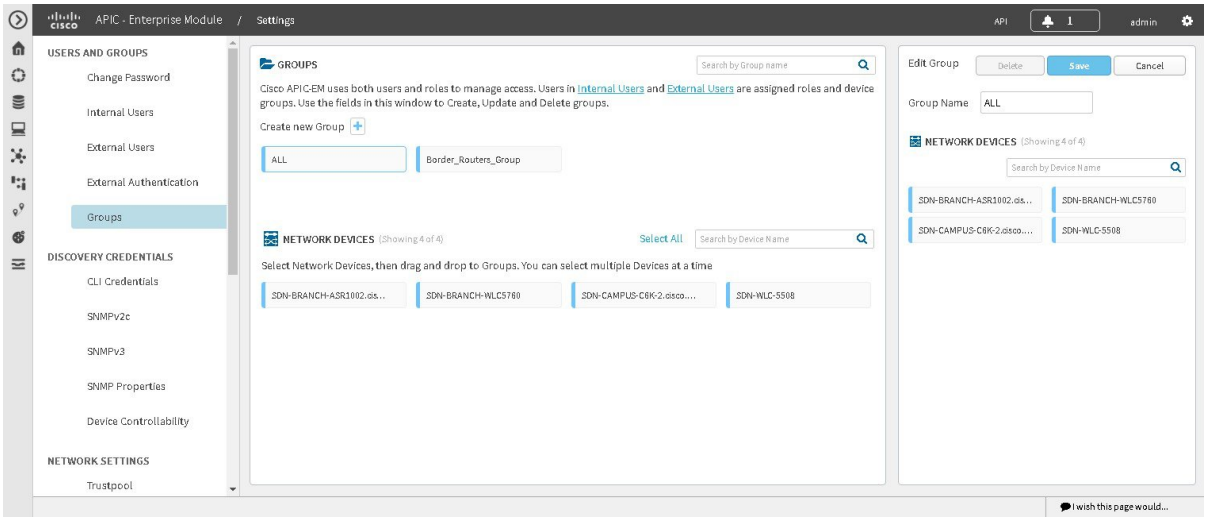
A group is a named entity that represents a specific set of resources for access-control purposes. You assign users to groups using RBAC scope. Assigning a user to a group with RBAC scope enables that user to access the resources in that group; if the user is not assigned to a particular group, the user 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 9: Configuring Groups Window***




**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 the chapter, "Managing Users".

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.<br>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.<br>A **Search by Device name** field permits you to enter a device name to only display that device in this field.<br>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.<br>**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.<br>Clicking on a specific group in the **Groups** field provide options to delete, edit and save, or cancel (exit) the group.<br>A **Search by Device name** field permits you to enter a device name to only display that device in this field.<br>Clicking on a device provides the following information:<br>• Name—Name of the discovered device.<br>• IP address——IP address of the discovered device.<br>• Family—Generic family name, for example "Routers" or "Wireless Controller".<br>• Type—Specific type of device, for example," Cisco 3945 Integrated Services Router G2"<br>• 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.

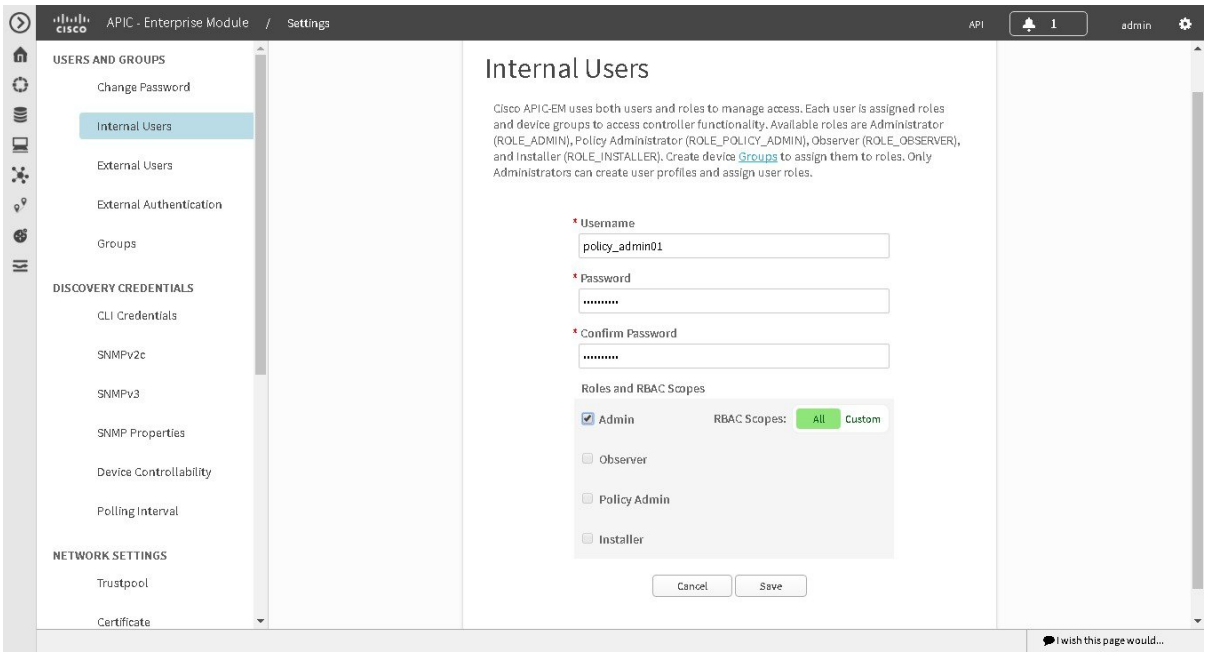
## Creating Internal Users

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 10: Internal Users Window***




### 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.

## Configuring External Authentication

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:

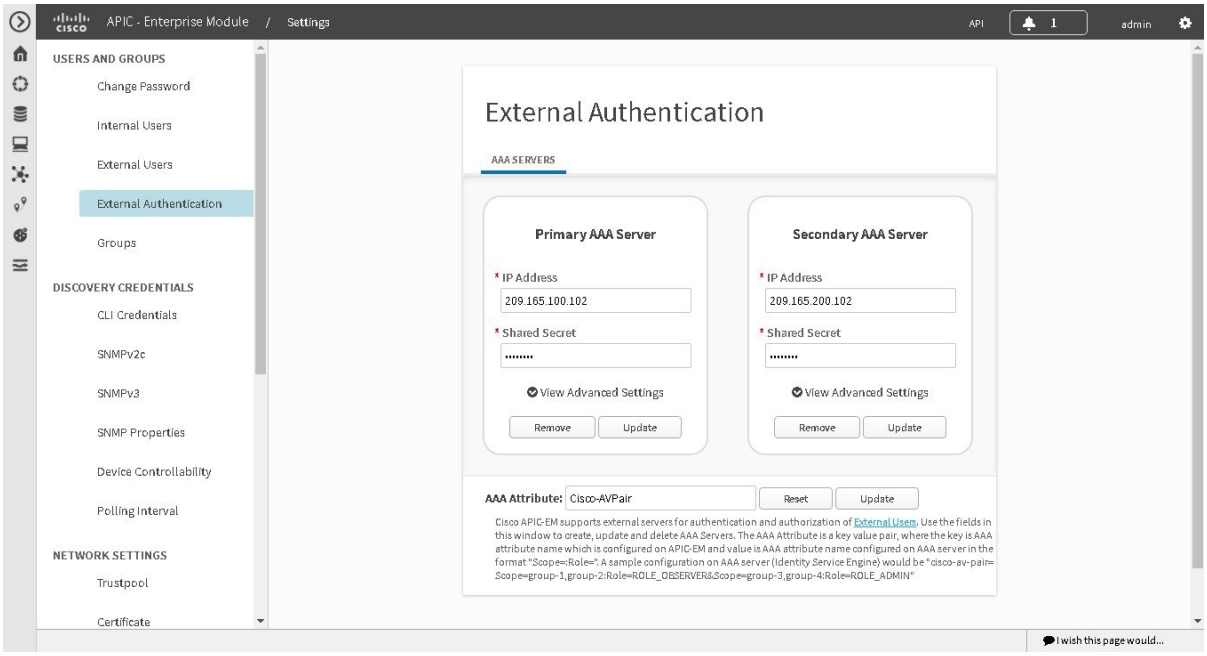
1. Authenticate/authorize with the user's credentials on a primary AAA server.
2. Authenticate/authorize with the user's credentials on a redundant or secondary AAA server.
3. Authenticate/authorize with the user's credentials managed by the Cisco APIC-EM.

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 12: External Authentication Window*




## 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 the chapter, "Managing Users".

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:

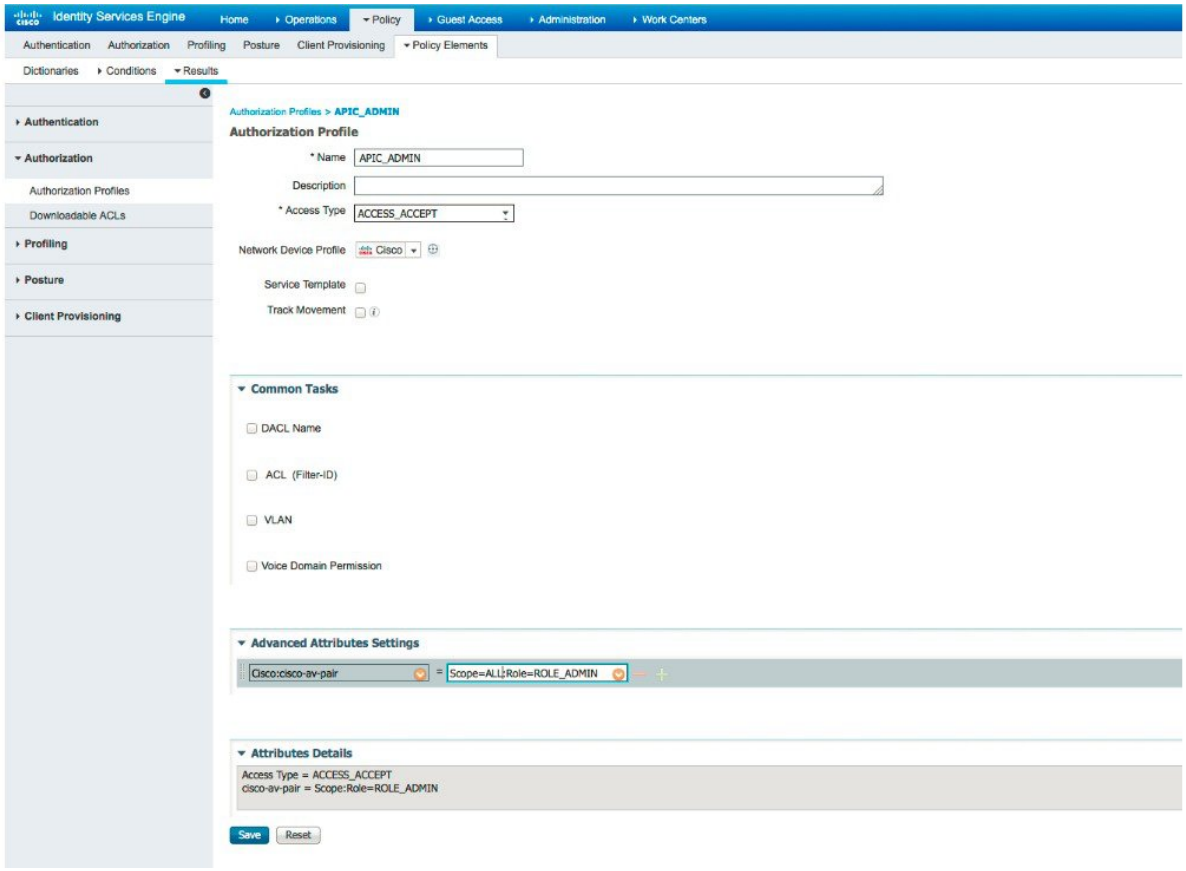
- **Name**: Enter a name for the authorization profile. We recommend that you enter a name similar to the role to be used for the profile. For example, for an admin (ROLE_ADMIN) use a name with "admin" within it, such as "APIC_ADMIN".
- **Description**: Enter a description for the profile
- **Access 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 11: AAA Server Configuration Example (Cisco ISE 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 **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.

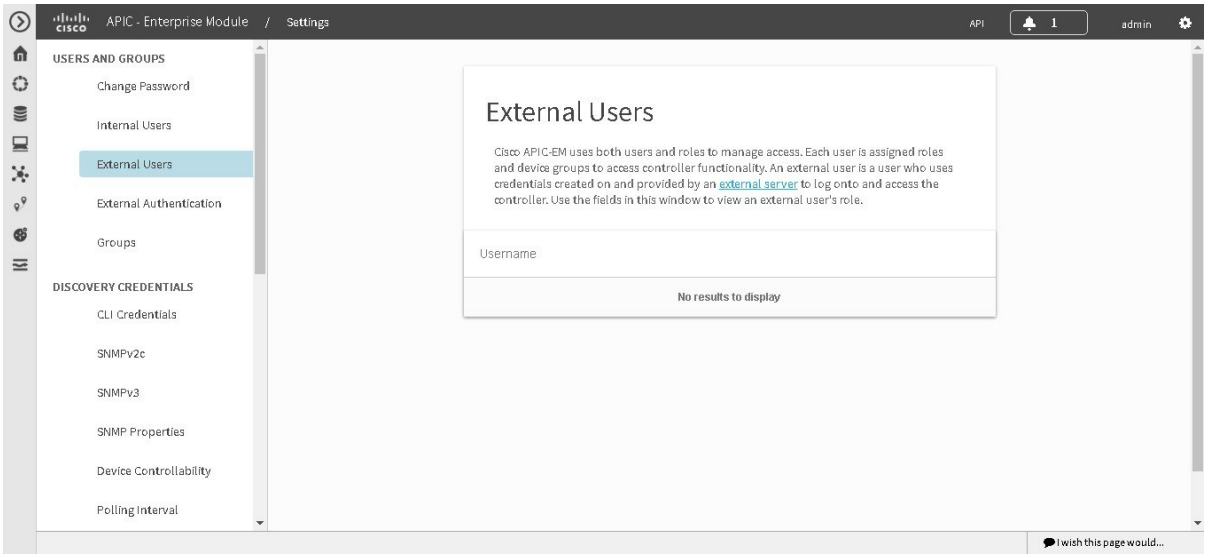
**Note** If the authentication/authorization is successful and access is granted, then the user's external authentication/authorization is saved in the controller's database. All users successfully granted access can be viewed in the **External Users** window.

## 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 Authentication, on page 84.

*Figure 13: External Users Window*




### 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).

# Discovery Credentials

The Cisco APIC-EM supports two different types of discovery credentials: global and job specific (or discovery request-specific). Both types of discovery credentials can consist of CLI or SNMP credentials that are configured using the controller's GUI.

Global credentials can be configured in either the **Discovery** window or the **Discovery Credentials** windows (as described in this chapter). Job specific credentials are only configured in the **Discovery** window.

**Note** For information about the procedure to configure global and/or job specific credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Both CLI and SNMP credentials are required for a successful discovery. The SNMP credentials (either global or job specific) are used for *device* discovery. The CLI credentials (either global or job specific) are used for capturing or applying *device configurations* for the controller's inventory.

You should enter at least one set of SNMP credentials, either SNMPv2c or SNMPv3, for your device discovery. If you are going to configure SNMPv2 settings in your network, then SNMP Read Only (RO) community string values should be entered in the controller to assure a successful discovery and populated inventory. However, if an SNMP RO community string and SNMP Read Writer (RW) community string is not entered into the controller, as a *best effort*, discovery will run with the default SNMP RO community string "public." Additionally, if no SNMP RO community string is entered but a SNMP RW community string is entered, then the SNMP RW community string will be used as SNMP RO community string.

**Note** You can enter values for both SNMP versions (SNMPv2c and SNMPv3) for a single discovery. The controller supports multiple SNMP credential configurations. Altogether, you can enter a maximum of 5 global device credentials (SNMP or CLI) using the **Discovery Credentials** windows as described in this chapter, with an additional credentials set being created in the **Discovery** window. Therefore, for a single discovery scan request, you can configure a total of 6 credential sets of each type (CLI or SNMP).

# Global Credentials

Global credentials are defined as preexisting credentials that are common to the devices in a network. Global credentials (CLI and SNMP) are configured on the devices using the GUI (**Discovery** window or **Discovery Credentials** window) and permit successful login to the devices. Global credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this device credential when performing network discoveries.

You can configure the global CLI credentials in the **CLI Credentials** window. You access this window by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane. You can also configure global CLI credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global CLI credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You configure the global SNMP credentials in the **SNMPv2c** or **SNMPv3** window . You access these windows by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click one of the SNMP window links on the Setting Navigation pane. You can also configure global SNMP credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global SNMP credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

**Note** Multiple credentials can be configured in the **CLI Credentials** window.

# Job Specific Credentials

Job specific credentials (request-specific credentials) are defined as preexisting *device* credentials for a specific network device or set of devices that do not share the global credentials.

You configure job specific credentials in the **Discovery** window prior to performing a discovery that is exclusive for that set of network devices. You access this window by clicking **Discovery** on the Navigation pane.

# Discovery Credentials Example

Assume a network of 200 devices that form a CDP neighborship (neighboring devices discovered using Cisco Discovery Protocol (CDP)). In this network, 190 devices share a global credential (Credential-0) and the 10 remaining devices each have their own unique or job specific credentials (Credential 1- 5)

To properly authenticate and access the devices in this network by the Cisco APIC-EM, you perform the following tasks:

1. Configure the CLI global credentials as Credential-0 for the controller.

   You can configure the global credentials in the **CLI Credentials** window. You access this window, by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane.

2. Configure the SNMP (v2c or v3) global credentials.

   You can configure these global credentials in the two SNMP windows. You access these GUI windows by clicking the **Settings** button at the top right and then clicking **SNMPv2c** or **SNMPv3** on the Setting Navigation pane.

3. Run a **CDP** discovery using one of the 190 device IP addresses (190 devices that share the global credentials) and selecting the global credentials in the GUI. You run a **CDP** discovery in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

4. Run 10 separate **Range** discoveries for each of the remaining 10 devices using the appropriate job specific credentials and SNMP values (for example, Credential-1, Credential-2-5, etc.).

   You configure the job specific credentials in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

5. Review the **Device Inventory** table in the **Device Inventory** window to check the discovery results

# Discovery Credentials Rules

Discovery credentials (global and job specific) operate under the rules as described in the bullet list and table below.

**Job Specific Credential Rules**

- Job specific credentials can be provided when creating a new network discovery, but only a single set of job specific credentials is allowed per network discovery.
- Job specific credentials take precedence over any configured global credentials.

- If the job specific credentials are provided as part of a network discovery and cause an authentication failure, then discovery is attempted a second time with the configured global credentials (if explicitly selected in the **Discovery** window of the controller's GUI). If discovery fails with the global credentials then the device discovery status will result in an authentication failure.
- When using Cisco APIC-EM APIs for a network discovery and the job specific credentials (both CLI and SNMP) are *not* provided as part of the network discovery, then the global credentials (both CLI and SNMP provided by the user) are used to authenticate devices.

### Global Credential Rules

***Table 8: Global Credential Rules***

| Global Credentials | Job Specific Credentials | Result |
|---|---|---|
| Not configured | Not configured | If the network discovery is run from the controller's GUI, then the default SNMP read community string (public) is used for the discovery scan. A discovery failure will not occur in this case.<br>If the network discovery is run using Cisco APIC-EM APIs, then a discovery failure will occur since both CLI and SNMP credentials must be configured for a successful device discovery using the Cisco APIC-EM APIs. |
| Not configured | Configured | The specified job specific credentials will be used for discovery. |
| Configured | Not configured | All the configured global credentials will be used. |
| Configured but not selected | Configured | Only the job specific credentials will be used. |
| Configured and selected | Not configured | Only selected global credential will be used. |
| Configured and selected | Configured | Both specified credentials (global and job specific) will be used for discovery. |
| Configured, but wrong global credential IDs are mentioned in the discovery POST REST API. | Correct job specific credentials configured | Discovery fails.<br>**Note** This scenario is only possible by API not from the controller GUI. |

| Global Credentials | Job Specific Credentials | Result |
|---|---|---|
| Configured, but wrong global credential IDs are mentioned in the discovery POST REST API. | Not configured | Discovery fails.<br>**Note** This scenario is only possible by API not from the controller GUI. |

# Discovery Credentials Caveats

The following are caveats for the Cisco APIC-EM discovery credentials:

- If a device credential changes in a network device or devices after Cisco APIC-EM discovery is completed for that device or devices, any subsequent polling cycles for that device or devices will fail. To correct this situation, an administrator has following options:
  - Start a new discovery scan with changed job specific credentials that matches the new device credential.
  - Edit the existing discovery by updating or modifying the global credentials, and then rerun the discovery scan.
- If the ongoing discovery fails due to a device authentication failure (for example, the provided discovery credential is not valid for the devices discovered by current discovery), then the administrator has following options:
  - Stop or delete the current discovery. Create one or more new network discovery jobs (either a **CDP** or **Range** discovery type) with a job specific credential that matches the device credential.
  - Create a new global credential and execute a new discovery selecting the correct global credential.
  - Edit an existing global credential and re-run the discovery.
- Deleting a global credential does not affect already discovered devices. These already discovered devices will not report an authentication failure.
- The Cisco APIC-EM provides a REST API which allows the retrieval of the list of managed network devices in the Cisco APIC-EM inventory. The purpose of this API is to allow an external application to synchronize its own managed device inventory with the devices that have been discovered by the Cisco APIC-EM. For example, for Cisco IWAN scenarios, Prime Infrastructure makes use of this API in order to populate its inventory with the IWAN devices contained in the Cisco APIC-EM inventory in order to provide monitoring of the IWAN solution.

**Note** Only the username is provided in clear text. SNMP community strings and passwords are not provided in cleartext for security reasons.

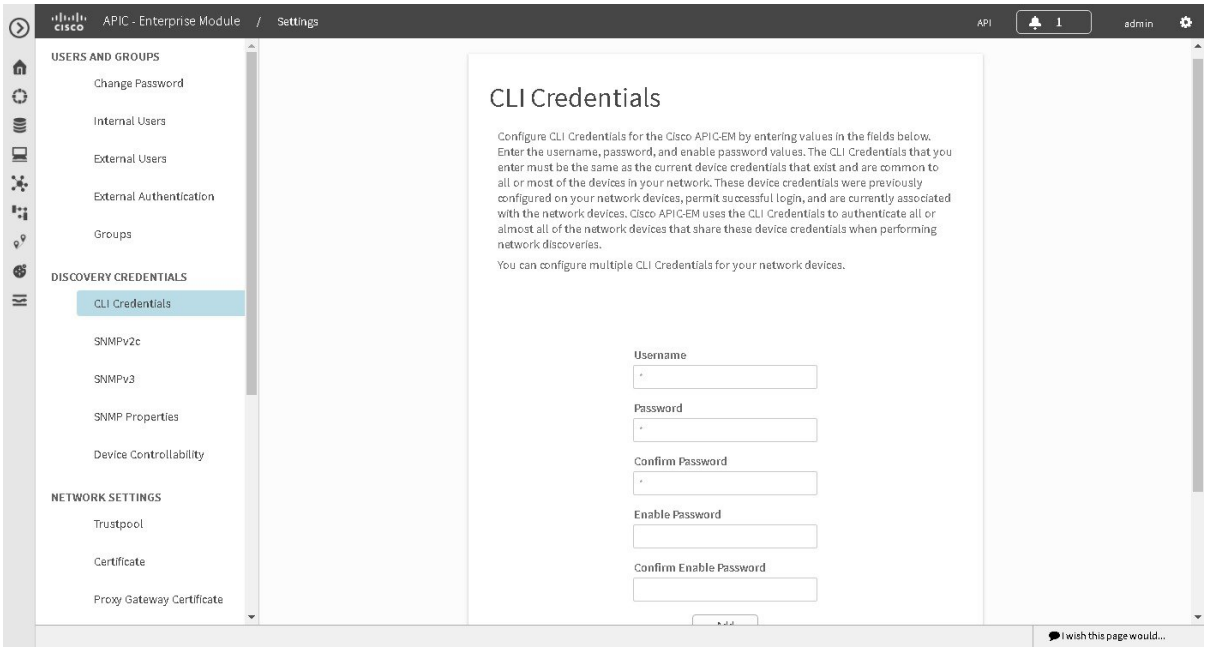
# Configuring CLI Credentials—Global

CLI credentials are defined as preexisting *device* credentials that are common to most of the devices in a network. CLI credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this CLI credential when performing devices discoveries.

You configure the CLI global credentials in the **CLI Credentials** window or the **Discovery** window. This procedure describes how to configure CLI global credentials in the **CLI Credentials** window.

**Note** You can configure up to five CLI credentials.

***Figure 14: CLI Credentials Window***




### 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 the chapter, "Managing Users".

**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 **CLI Credentials** to view the **CLI Credentials** window.

In the **CLI Credentials** window, enter the appropriate CLI global credentials for the devices within your network or networks.

**Step 4** Enter the CLI Credentials username in the **Username** field.

**Step 5** Enter the CLI Credentials password in the **Password** field.

**Step 6** Reenter the CLI Credentials password in the **Confirm Password** field to confirm the value that you just entered.

**Step 7** If your network devices have been configured with an enable password, then enter the CLI Credentials for the enable password in the **Enable Password** field.

**Note** Both the CLI credentials password and enable password are saved in the controller in encrypted form. You cannot view these original passwords after you enter them.

**Step 8** If you entered an enable password in the **Enable Password** field, reenter it in the **Confirm Enable Password** field to confirm the value that you just entered.

**Step 9** In the **CLI Credentials** window, click **Add** to save the credentials to the Cisco APIC-EM database.

### What to do next

Proceed to configure SNMP values for your network device discovery.

For a successful device discovery (with all the device information to be collected), CLI credentials (global and/or job specific) should be configured using the controller. The global credentials for CLI and SNMP (v2c or v3) can be configured in the **Discovery Credentials** windows (as described in this chapter) or the **Discovery** window, and are used in addition to any job specific credentials (for CLI and SNMP) that are also configured in the **Discovery** window.

# Configuring SNMP

You configure SNMP for device discovery using the following **Discovery Credentials** windows in the Cisco APIC-EM GUI:

- **SNMPv2c**
- **SNMPv3**
- **SNMP Properties**

**Note** You can also configure SNMP for device discovery in the **Discovery** window of the controller's GUI. For information about the procedures to configure SNMP for device discovery in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

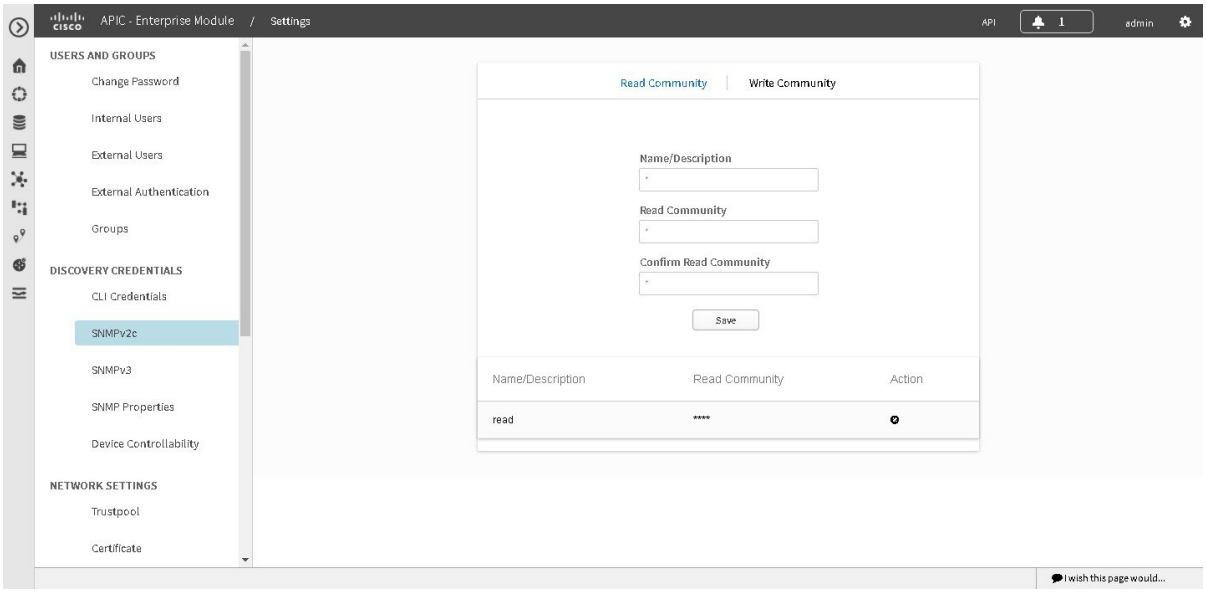
**Important** You can use SNMP and the existing security features in SNMP v3 to secure communications between the controller and the devices in your network. SNMP v3 provides both privacy (encryption) and authentication capabilities for these communications. If possible for your network, we recommend that you use SNMPv3 with both privacy and authentication enabled.

# Configuring SNMPv2c

You configure SNMPv2c for device discovery in the **SNMPv2c** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv2c for the controller must match the SNMPv2c values that have been configured for your network devices.

**Note** You can configure up to five read community strings and five write community strings.

***Figure 15: Configuring SNMPv2c***




SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv2c is the community string-based administrative framework for SNMPv2. Community string is a type of password, which is transmitted in clear text. SNMPv2c does not provide authentication or encryption (noAuthNoPriv level of security).

**Note** In addition to configuring SNMPv2c for device discovery in the controller, a "best effort" Cisco APIC-EM discovery is in place, meaning that devices having SNMP with Read-Only (RO) community string set to "public" will be discovered all the time irrespective of the configured SNMP Read/Write community string.

### Before you begin

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

You must have your network's SNMP information available for this configuration procedure.

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 the chapter, "Managing Users".

**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 **SNMPv2c** to view the **SNMPv2c** window.

**Step 4** In the **SNMPv2c** window, click **Read Community**.

Enter your **Read Community** values:

- **Name/Description**—Description of the Read-Only (RO) community string value and/or the device or devices that are configured with it.
- **Read Community**—Read-Only community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Read Community**—Reenter the Read-Only community string to confirm the value that you just entered.

**Note** If you are configuring SNMPv2c for your discovery, then configuring **Read Community** values is mandatory.

**Step 5** Click **Save** to save your **Read Community** values.

The **Read Community** values will appear in the table below.

**Step 6** (Optional) In the **SNMPv2c** window, click **Write Community**.

Enter your **Write Community** values:

- **Name/Description**—Description of the Write community string value and/or the device or devices that are configured with it.
- **Write Community**—Write community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Write Community**—Reenter the Write community string to confirm the value that you just entered.

**Step 7** (Optional) Click **Save** to save your **Write Community** values.

The **Write Community** values will appear in the table below.

### What to do next

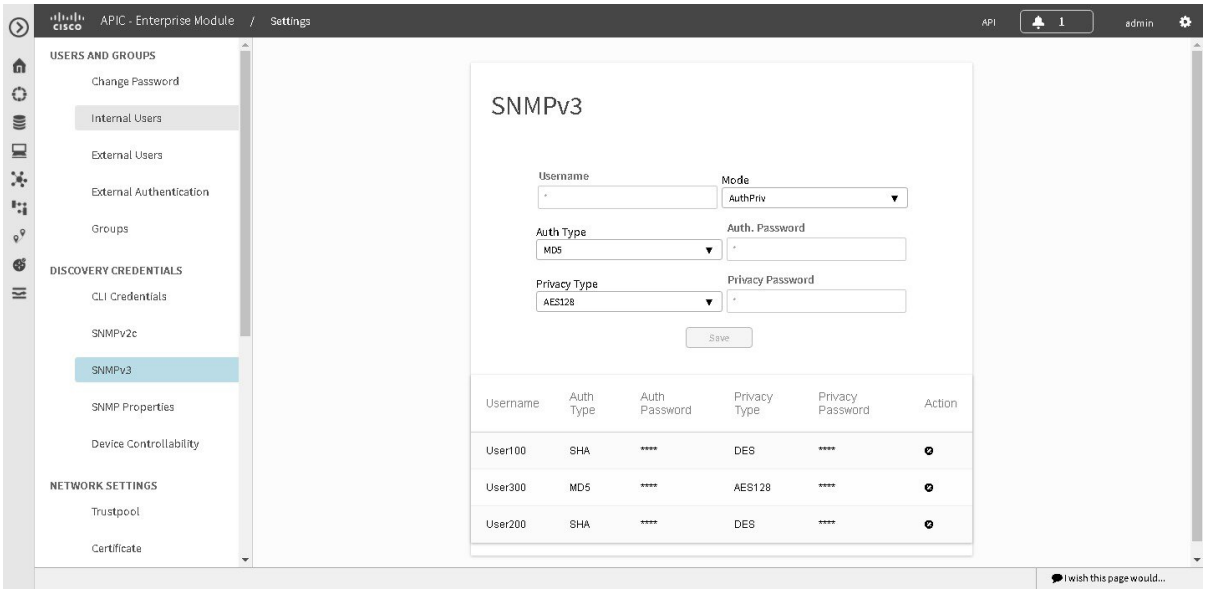
If required for your SNMP configuration, proceed to configure either **SNMPv3** or **SNMP Properties** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

## Configuring SNMPv3

You configure SNMPv3 for device discovery in the **SNMPv3** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv3 for the controller must match the SNMPv3 values that have been configured for your network devices. You can configure up to five SNMPv3 settings.

***Figure 16: Configuring SNMPv3***




SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The following are supported SNMPv3 security models:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption
- AuthNoPriv—Security level that provides authentication but does not provide encryption

- AuthPriv—Security level that provides both authentication and encryption

The following table identifies what the combinations of security models and levels mean:

***Table 9: SNMP Security Models and Levels***

| Model | Level | Authentication | Encryption | What Happens |
|---|---|---|---|---|
| v2c | noAuthNoPriv | Community String | No | Uses a community string match for authentication. |
| v3 | noAuthNoPriv | User Name | No | Uses a username match for authentication. |
| v3 | AuthNoPriv | Either:<br>• HMAC-MD5<br>• HMAC-SHA | No | Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash algorithm (SHA) |
| v3 | AuthPriv | Either:<br>• HMAC-MD5<br>• HMAC-SHA | Either:<br>• CBC-DES<br>• CBC-AES-128 | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.<br>Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption. |

### Before you begin

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

You must have your network's SNMP information available for this configuration procedure.

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 the chapter, "Managing Users".

**Note** With SNMPv3, passwords (or passphrases) must be at least 8 characters in length (minimum). Additionally, for several Cisco Wireless LAN controllers, passwords (or passphrases) must be at least 12 characters in length (minimum). Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, and/or managed by the controller.

**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 **SNMPv3** to view the **SNMPv3** window.

If you use SNMPv3 in your network to monitor and manage devices, then configure the SNMPv3 values for discovery for your network.

**Step 4** In the **SNMPv3** window, enter a **Username** value and choose a **Mode** from the drop down menu.

The following **Mode** options are available:

- **AuthPriv**
- **AuthNoPriv**
- **NoAuthNoPriv**

**Note** Subsequent **SNMPv3** configuration options might or might not be available depending upon your selection for this step.

**Step 5** If you selected **AuthPriv** or **AuthNoPriv** as a **Mode** option, then choose an **Authentication** type from the drop down menu and enter an authentication password.

The following **Authentication** options are available:

- **SHA**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm
- **MD5**—Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm

**Step 6** If you selected **AuthPriv** as a **Mode** option, then choose a **Privacy** type from the drop down menu and enter a SNMPv3 privacy password.

The SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.

The following **Privacy** type options are available:

- **DES**—Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

- **AES128**—Cipher Block Chaining (CBC) mode AES for encryption.

**Step 7** Click **Save** to save your SNMPv3 configuration values.

The **SNMPv3** configured values will appear in the table below.

### What to do next

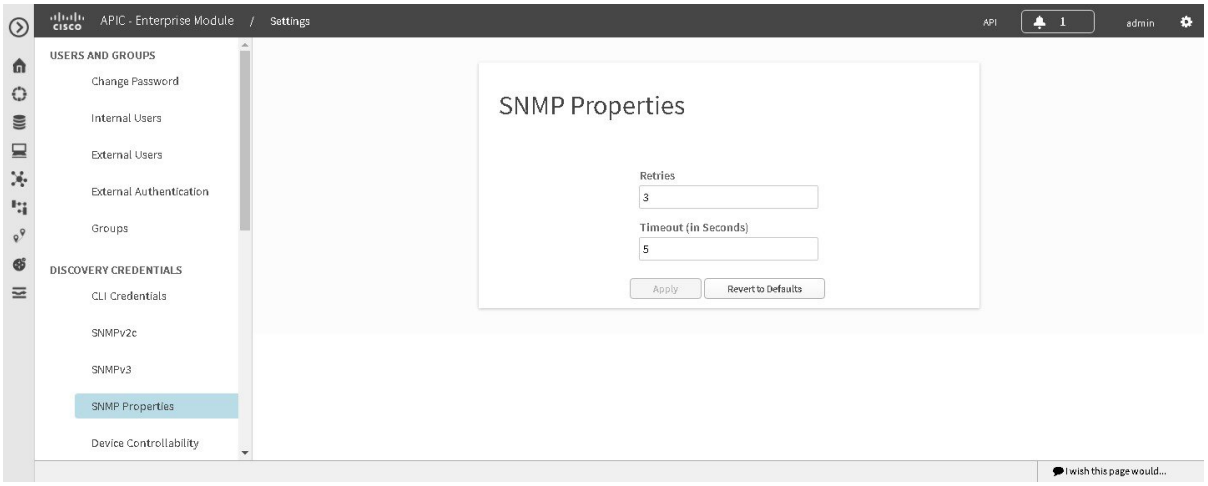
If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMP Properties** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

## Configuring SNMP Properties

You configure SNMP properties for device discovery in the **SNMP Properties** window in the Cisco APIC-EM GUI.

***Figure 17: Configuring SNMP Properties***




### Before you begin

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

You must have your network's SNMP information available for this configuration procedure.

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 the chapter, "Managing Users".

**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 **SNMP Properties** to view the **SNMP Properties** window.

Configure the SNMP property settings for discovery in your network.

**Step 4** In the **SNMP Properties** window, enter a value in the **Retries** field.

The value entered in this field is the number of attempts the controller attempts to use SNMP to communicate with your network devices.

**Step 5** In the **SNMP Properties** window, enter a value in the **Timeout** field.

The value entered in this field is the length of time in seconds the controller attempts to use SNMP to communicate with your network devices.

**Step 6** Click **Apply** to save your SNMP configuration values.

You can also click **Revert to Defaults** to revert to the SNMP property default values. The following are the SNMP property default values:

- **Retries**—3
- **Timeout**—5

### What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMPv3** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

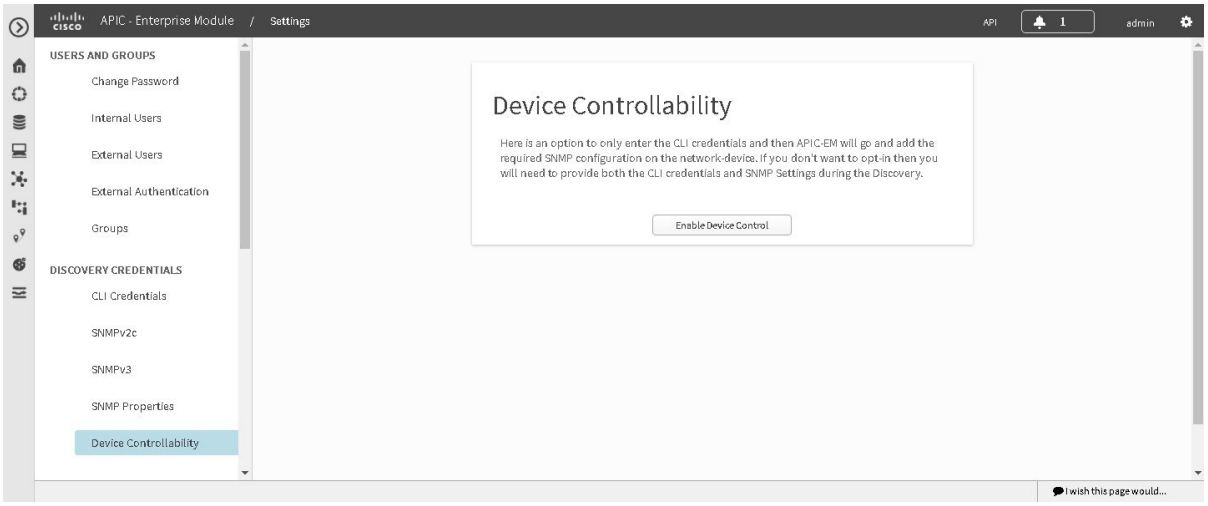
# Enabling Device Controllability

You can enable device controllability using the Cisco APIC-EM GUI. When you enable device controllability, the controller automatically configures (applies) the SNMP credentials that you entered using the controller's GUI on any network devices without SNMP credentials or without matching SNMP credentials.

**Note** The device controllability functionality depends upon whether the CLI credentials provided by the user permits the controller to log into the device in enable mode (privilege level 15 for Cisco IOS devices).

You can enable device controllability for device discovery in the **Device Controllability** window in the Cisco APIC-EM GUI

*Figure 18: Enabling Device Controllability*




### 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 the chapter, "Managing Users".

**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 **Device Controllability** to view the **Device Controllability** window.

**Step 4** Click **Enable Device Control** to enable this feature.

### What to do next

If you have not already done so, configure SNMP in either the **Discovery** window or the appropriate **CLI Credentials** window for SNMP in **Settings**.

# Network Settings

## Importing the Controller's Server Certificate

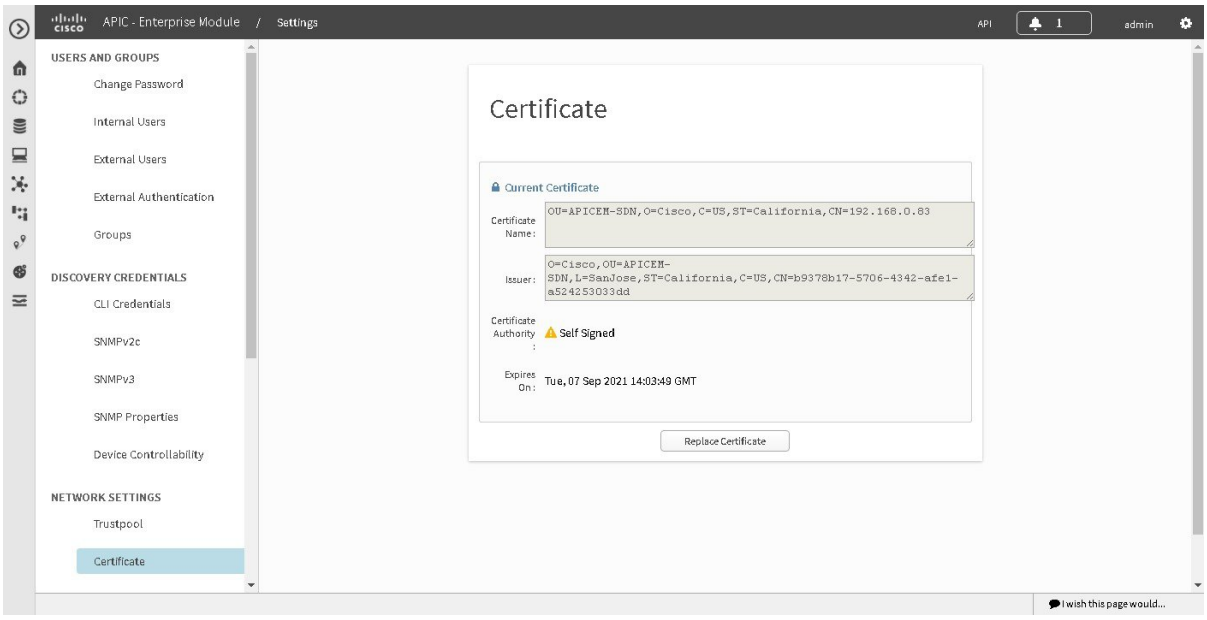
The Cisco APIC-EM supports the import and storing of an X.509 certificate and private key into the controller. After import, the certificate and private key can be used to create a secure and trusted environment between the Cisco APIC-EM, NB API applications, and network devices.

**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 19: Certificate Configuration Window***



**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 the chapter, "Managing Users".

**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 21
Cisco APIC-EM Controller Certificate Chain Support, on page 22
Obtaining a CA-Signed Certificate for the Cisco APIC-EM Controller, on page 23

# Importing a Trustpool Bundle

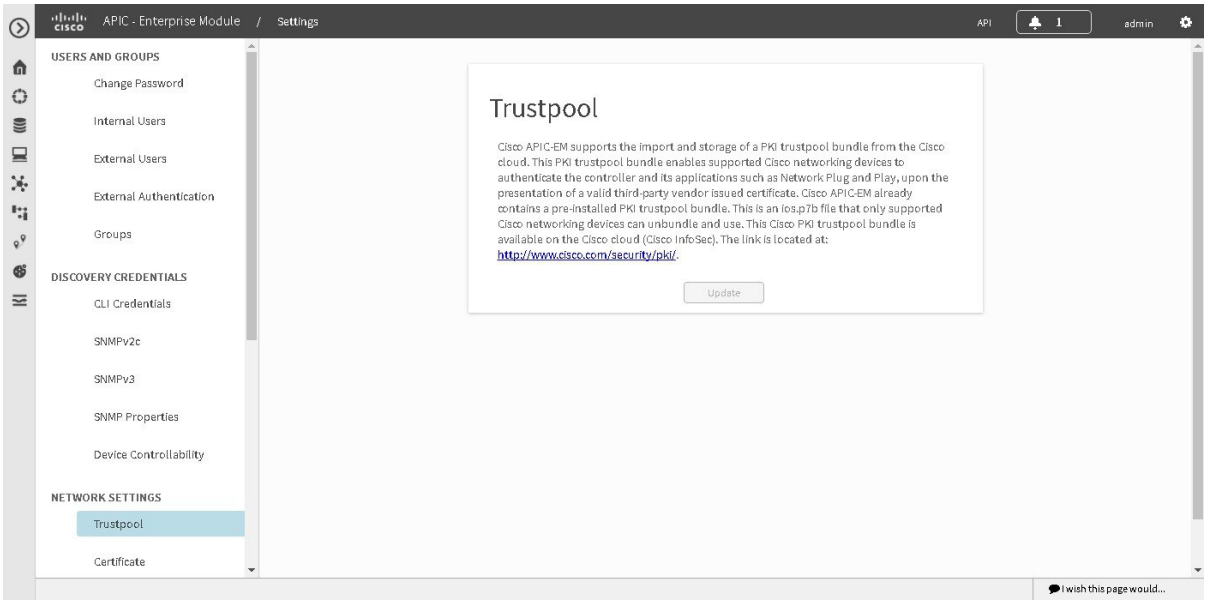
The Cisco APIC-EM contains a pre-installed Cisco trustpool bundle (Cisco Trusted External Root Bundle). The Cisco APIC-EM also supports the import and storage of an updated trustpool bundle from Cisco. The trustpool bundle is used by supported Cisco networking devices to establish a trust relationship 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 20: Trustpool Window***




### 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 the chapter, "Managing Users".

**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**

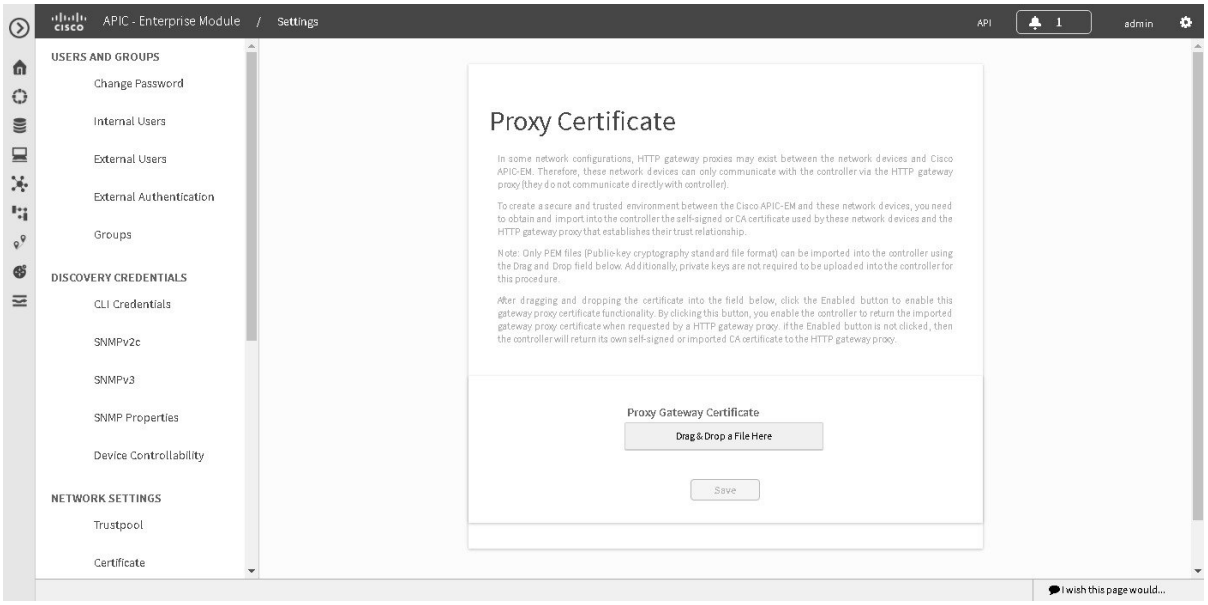
Cisco APIC-EM Trustpool Support, on page 25

# 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 21: Proxy Gateway Certificate Window*




### 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 27

# 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 PKI certificate management procedures described in this section only involves the Device PKI plane and include:

- Changing the private CA from a root CA to a subordinate CA. This procedure requires that you replace the CA certificate of the private CA with one signed by the external CA.
- Changing the lifetime of the device ID certificates that secure device-to-device connections between IWAN-managed devices.

## 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 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:

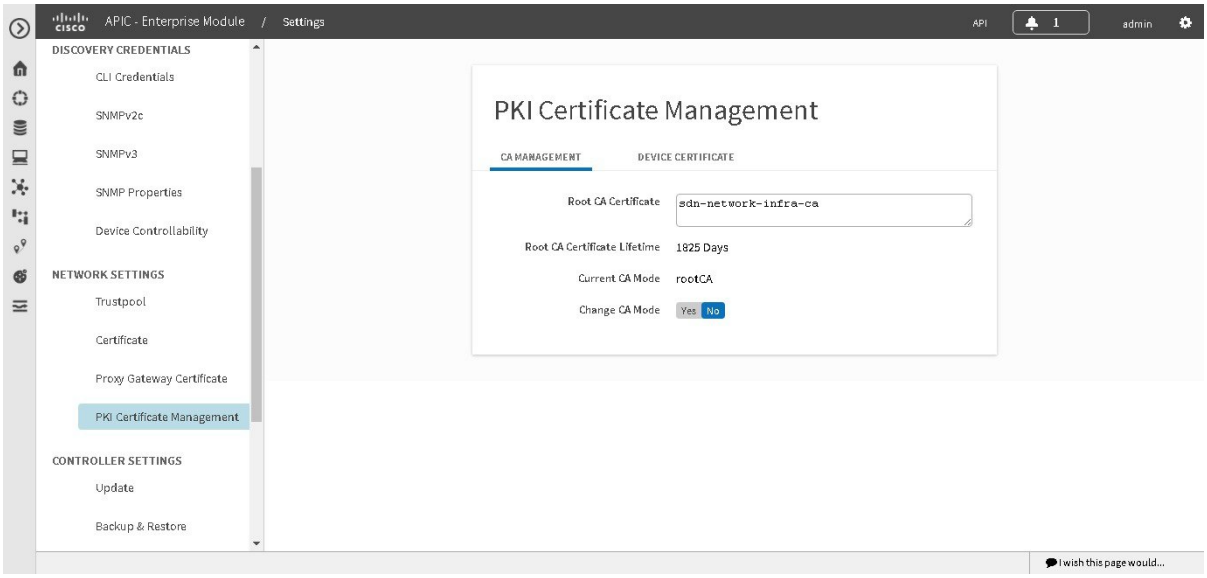
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2e:00:00:00:0e:28:d7:1f:24:a1:1e:ef:70:00:00:00:00:00:0e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=apic-em, CN=apic-em-CA
        Validity
            Not Before: Oct 18 19:56:54 2016 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 22: PKI Certificate Management Window***




### 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 the chapter, "Managing Users".

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 19

## Viewing the Device Certificate Lifetime

The Cisco APIC-EM enables the user to view 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.

**Note** You cannot change the certificate lifetime default value.

**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 the chapter, "Managing Users".

**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** From here, you can review the device certificate and current device certificate lifetime.

**Related Topics**

Device PKI Plane Modes, on page 19

# Logs and Logging

The Cisco APIC-EM generates the following log types that are accessible through the GUI:

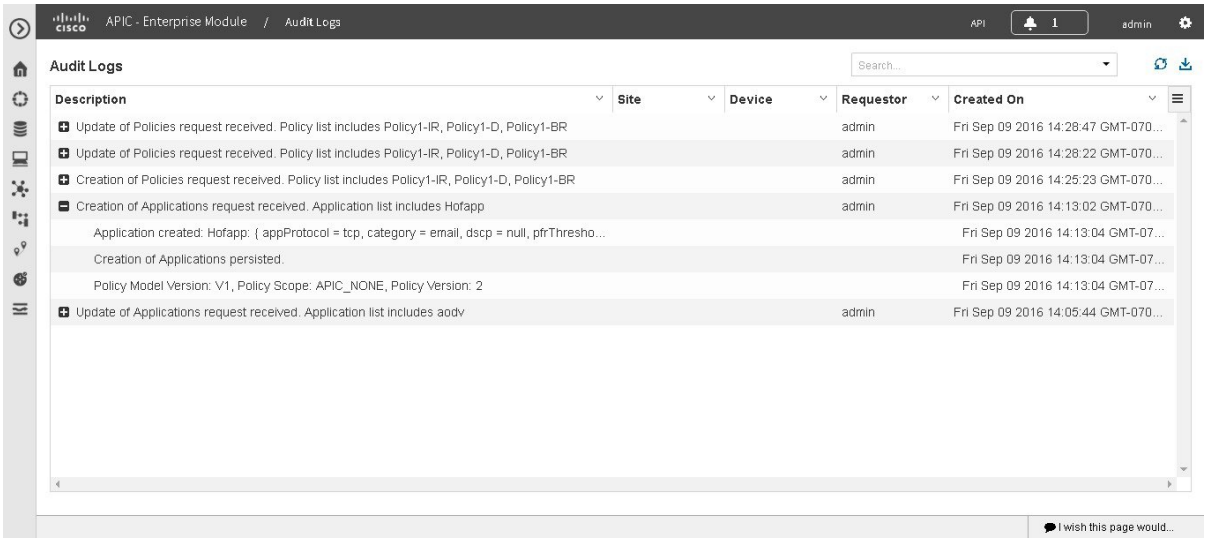
- Audit Logs—Logs used primarily to monitor policy creation and application.
- Service Logs—Logs used to monitor the controller services.

# Viewing Audit Logs

Audit logs capture information about the various ; applications (EasyQoS, PnP and IWAN). Additionally, the audit logs also capture information about device PKI notifications. The information in these audit logs can be used to assist in troubleshooting any issues involving the applications or device PKI certificates.

You can view audit logs using the **Audit Logs** window in the Cisco APIC-EM GUI. The Cisco APIC-EM also supports the ability to export the audit logs to a local system.

***Figure 23: Audit Logs Window***




### Before you begin

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

You must have either administrator (ROLE_ADMIN), policy administrator (ROLE_POLICY_ADMIN), or Observer (ROLE_OBSERVER) permissions and the appropriate resource scope to perform 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 **Audit Logs** link from the drop-down menu.

The **Audit Logs** window appears. In the **Audit Logs** window, you can view logs about the current policies in your network. These policies were applied to network devices by either the IWAN or EasyQoS applications.

The following information is displayed for each policy in the window:

- **Description**—Application or policy audit log description
- **Site**—Name of site for the specific audit log
- **Device**—Device or devices for the audit log
- **Requestor**—User requesting audit log
- **Created On**—Date application or policy audit log was created.

**Step 3** Click on the addition icon (+) next to an audit log to view the children audit logs in the **Audit Logs** window.

Each audit log can be a parent to several child audit logs. By clicking on this icon, you can view a series of additional children audit logs.

**Note** An audit log captures data about a task performed by the controller. Children audit logs are sub-tasks to that one task performed by the controller.

**Step 4** Perform a search of the audit logs by clicking on the **Search** field in the **Audit Logs** window, entering a specific parameter, and then clicking the **Submit** button.

You can search for a specific audit log by the following parameters:

- Description
- Requestor
- Device
- Site
- Start Date
- End Date

**Step 5** Click on the dual arrow icon to refresh the data displayed in the window.

The data displayed in the window is refreshed with the latest audit log data.

**Step 6** Click on the down arrow icon to download a local copy of the audit log in .csv file format.

A .csv file containing audit log data is downloaded locally to your system. You can use the .csv file for additional review of the audit log or archive it as a record of activity on the controller.

### What to do next

Proceed to review any additional log files using the controller's GUI, or download individual audit logs as .csv files for further review or archiving purposes.

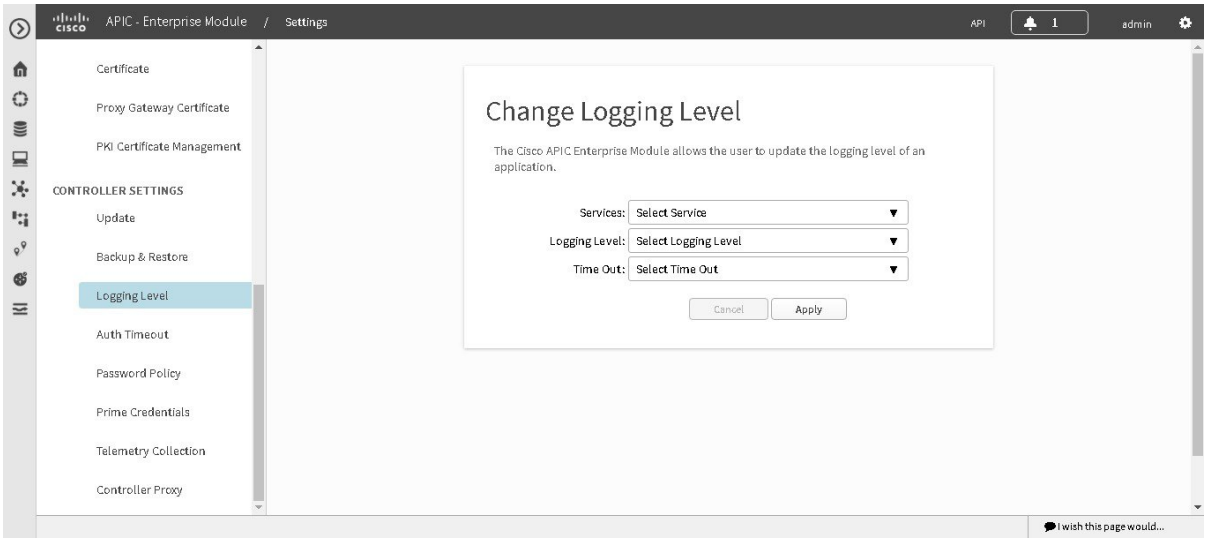
# Changing the Logging Level for Services

You can change the logging level for the Cisco APIC-EM services by using the **Changing the Logging Level** window in the Cisco APIC-EM GUI.

A logging level determines the amount of data that is captured to the controller's log files. Each logging level is cumulative, that is, each level contains all the data generated by the specified level and any higher levels. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs.

You may want to adjust the logging level to assist in troubleshooting any issues by capturing more data. For example, by adjusting the logging level you can capture more data to review in a root cause analysis or rca support file.

***Figure 24: Service Logging Level Window***




The default logging level for services in the controller is informational (**Info**). You can change the logging level with the GUI to set it to debug or trace to capture more information.

**Caution** Any logs collected at the **Debug** level or higher should be handled with restricted access.

**Note** The log files are created and stored in a centralized location on your controller. From this location, the controller can query and display them in the GUI. The total compressed size of the log files is 2GB. If log files created are in excess of 2GB, then the pre-existing log files are overwritten with the newer log files.

**Note** The log files are created and stored in a centralized location on your controller. From this location, the controller can query and display them in the GUI The total compressed size of the log files is 2GB. If log files created are in excess of 2GB, then the pre-existing log files are overwritten with the newer log files.

### Before you begin

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

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

**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 **Changing the Logging Level** to view the **Changing Logging Level** window.

The **Logging Level** table appears with the following fields:

- **Services**
- **Logging Level**
- **Timeout**

**Step 4** In the **Changing Logging Level** window, choose a service from the **Services** field to adjust its logging level.

**Note** The **Services** field displays any services that are currently configured and running on the controller.

**Step 5** In the **Changing Logging Level** window, choose the new logging level for the service from the **Logging Level** field.

The following logging levels are supported on the controller:

- **Trace**—Trace messages
- **Debug**—Debugging messages
- **Info**—Normal but significant condition messages
- **Warn**—Warning condition messages
- **Error**—Error condition messages

**Step 6** In the **Changing Logging Level** window, choose the time period for the logging level from the **Timeout** field for the logging level adjustment.

You configure logging level time periods in increments of 15 minutes up to an unlimited time period.

**Step 7** Review your selection and click the **Apply** button.

To cancel your selection click the **Cancel** button.

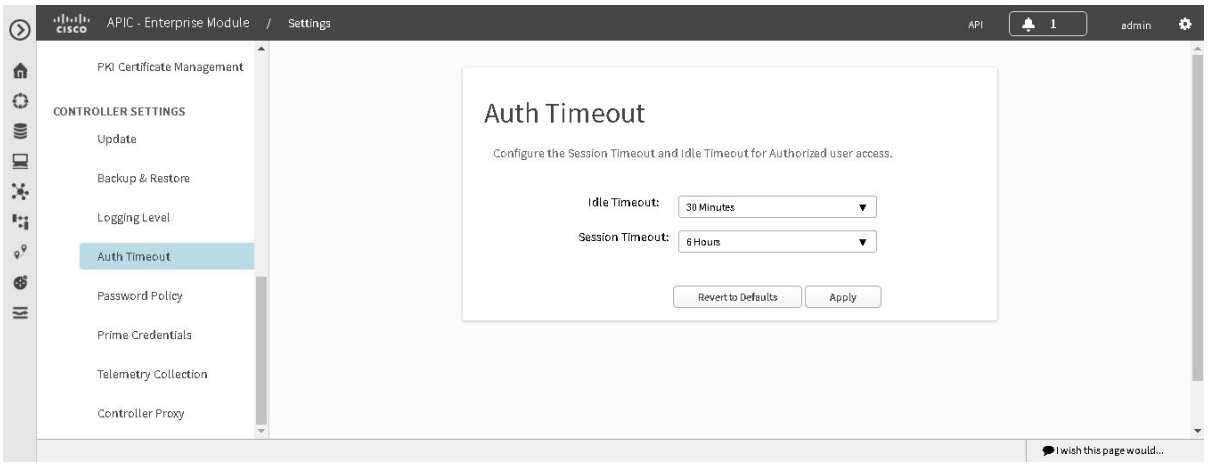
The logging level for the specified service is set.

# Controller Settings

## 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 25: Authentication Timeout Window***




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 the chapter, "Managing Users".

**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.

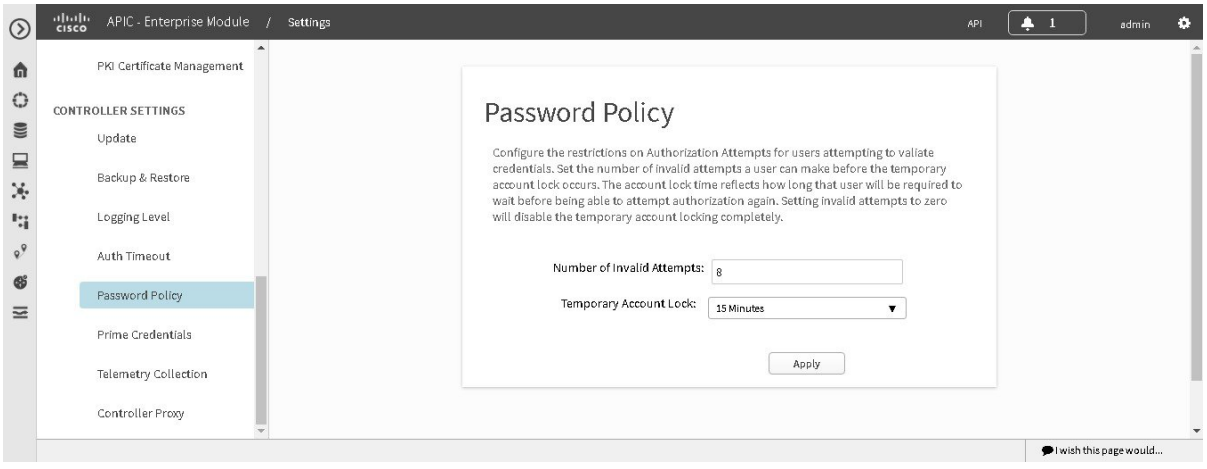
To restore the authentication timeout defaults to the controller, click the **Revert to Defaults** button.

# 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 26: Password Policy Window***




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 the chapter, "Managing Users".

**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

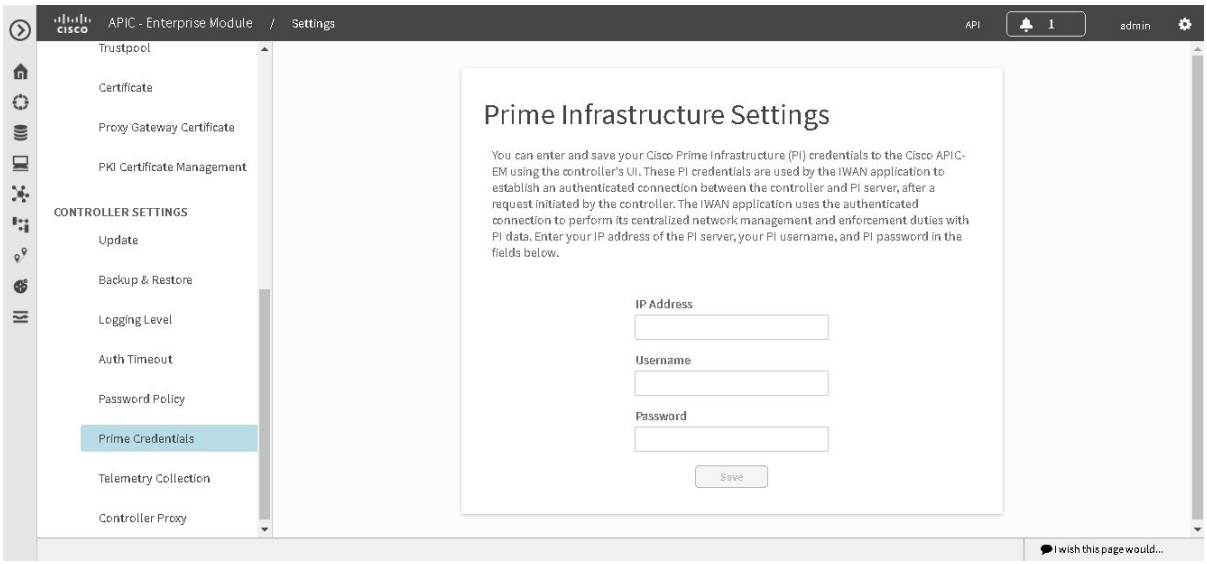
Password Requirements, on page 32

# 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 27: Prime Infrastructure Settings Window***




### 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 the chapter, "Managing Users".

**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.

# 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:

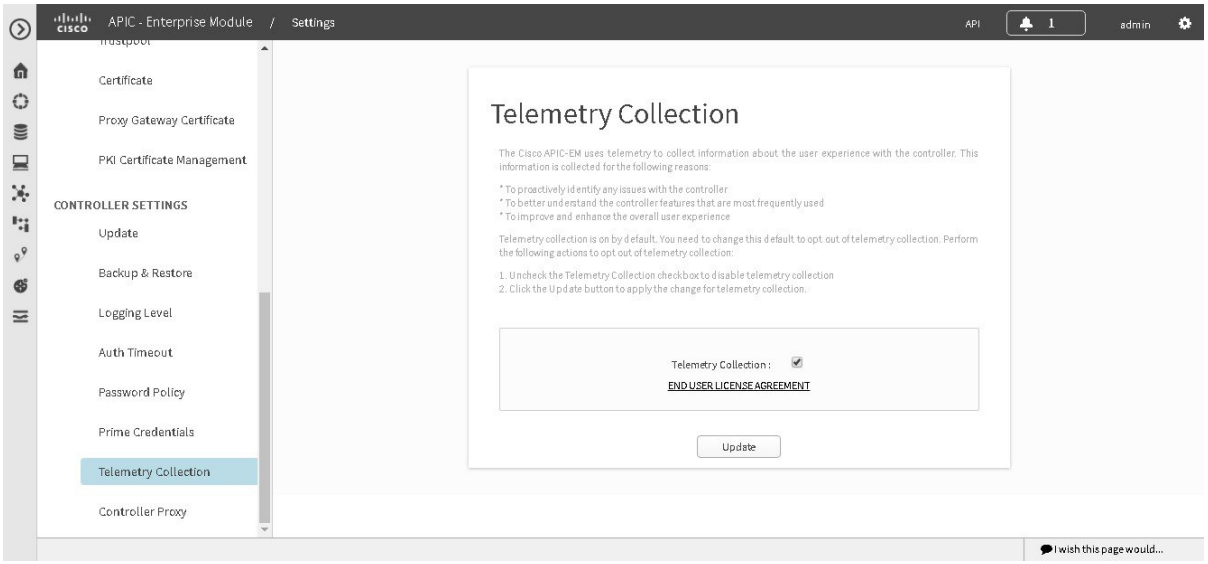
- To proactively identify any issues with the controller
- To better understand the controller features that are most frequently used
- To improve and enhance the overall user experience

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 28: Telemetry Collection Window***




### 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 the chapter, "Managing Users".

**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.

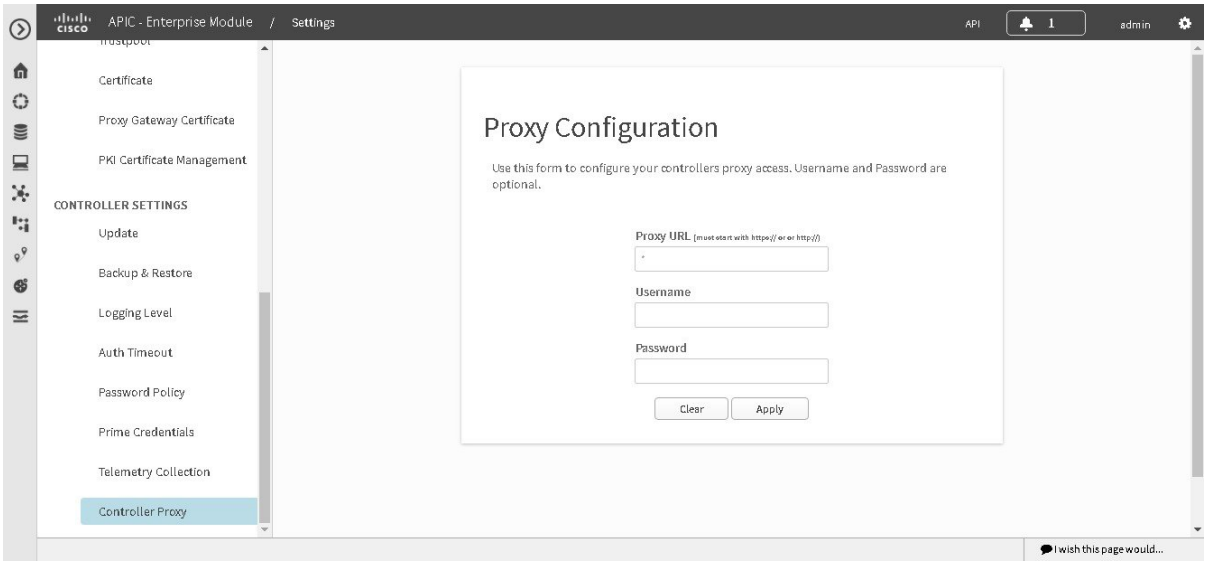
**Step 6** (Optional) Click the **Update** button to apply the change for telemetry collection.

# 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 29: Proxy Configuration Window***




### 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 the chapter, "Managing Users".

**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.

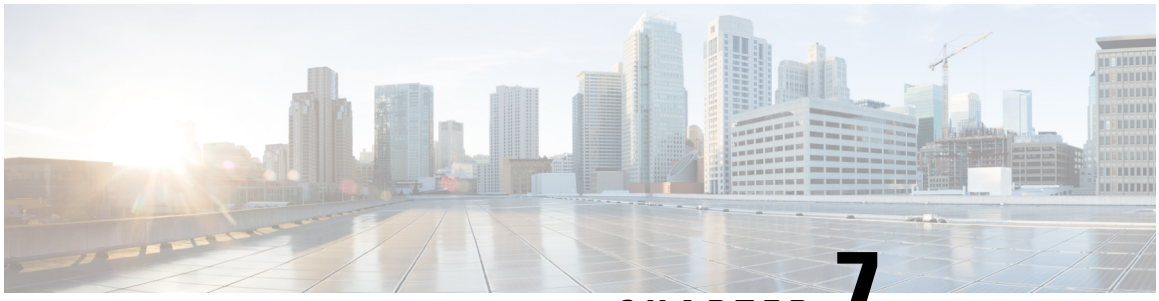
**Step 3** In the **Settings** navigation pane, click **Controller Proxy** to view the **Proxy Configuration** window.

**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

# Managing the Cisco APIC-EM and Applications



## Managing Cisco APIC-EM Using the GUI

You can manage the Cisco APIC-EM using its GUI. The following controller management functions are available using the GUI:

- Application separation (enable and disable supported applications on the controller)
- Backup and restore
- Software update

## Cisco APIC-EM Application Separation

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 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 consists of service bundles, meta data files, and scripts; although for this specific release, application bundles are only provided as part of the ISO image.

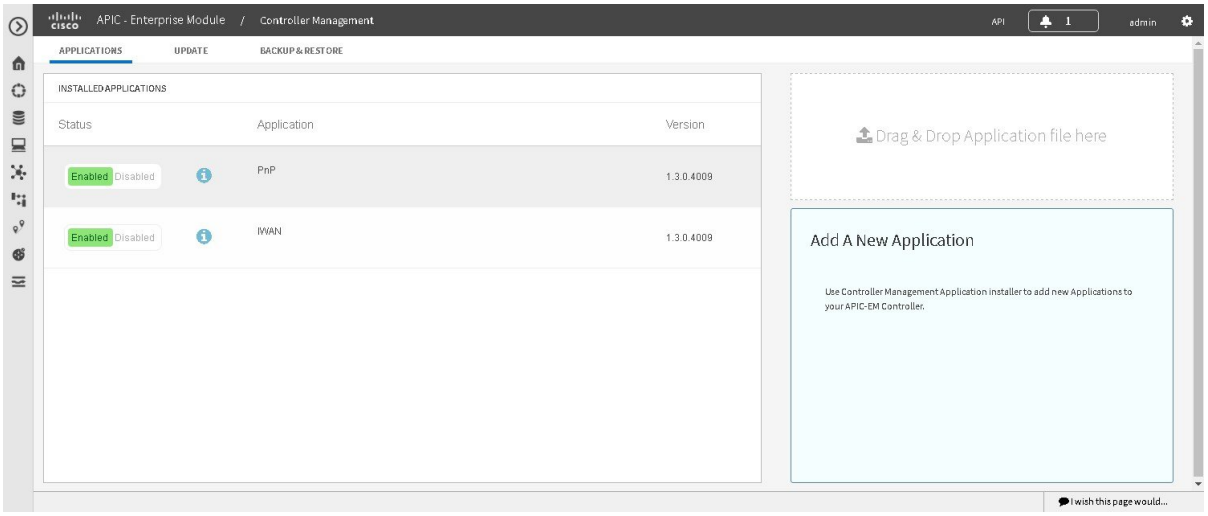
### Enabling and Disabling Applications

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 30: Applications Window***




### 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 the chapter, "Managing Users".

**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.

# Information about Backing Up and Restoring the Cisco APIC-EM

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

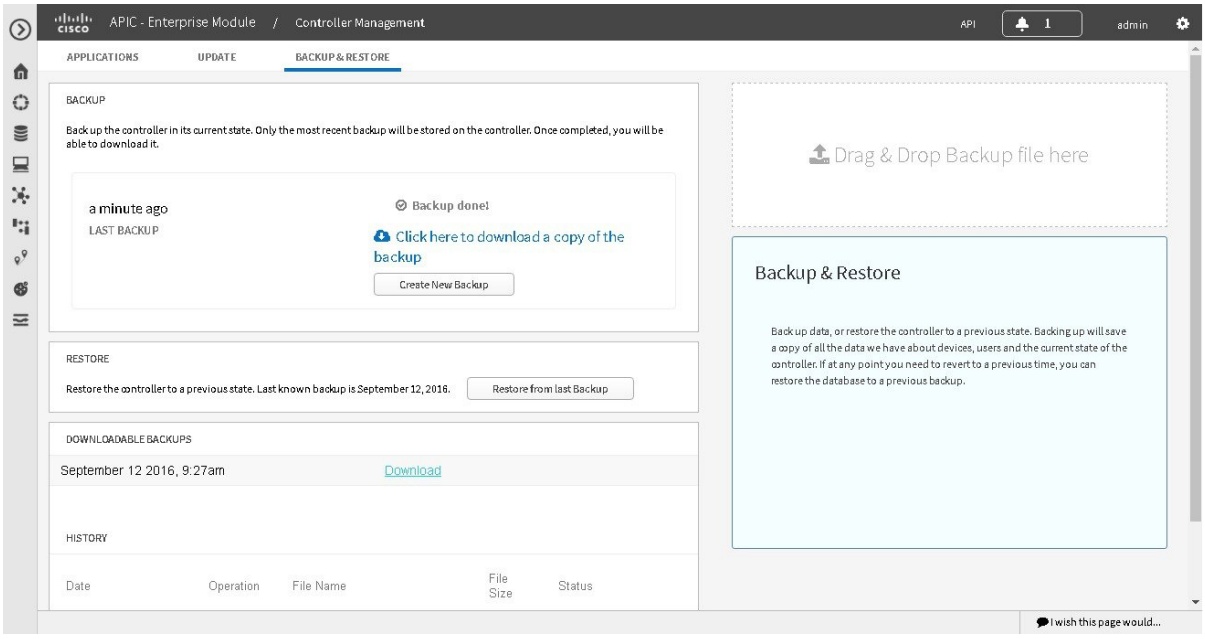
In a multi-host cluster, the database and files are replicated and shared across three hosts. When backing up and restoring in a multi-host cluster, you need to first back up on one of the three hosts in the cluster. You can then use that backup file to restore all three hosts in the cluster. However, 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 31: Backup & Restore Window***



### 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 the chapter, "Managing Users".

**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

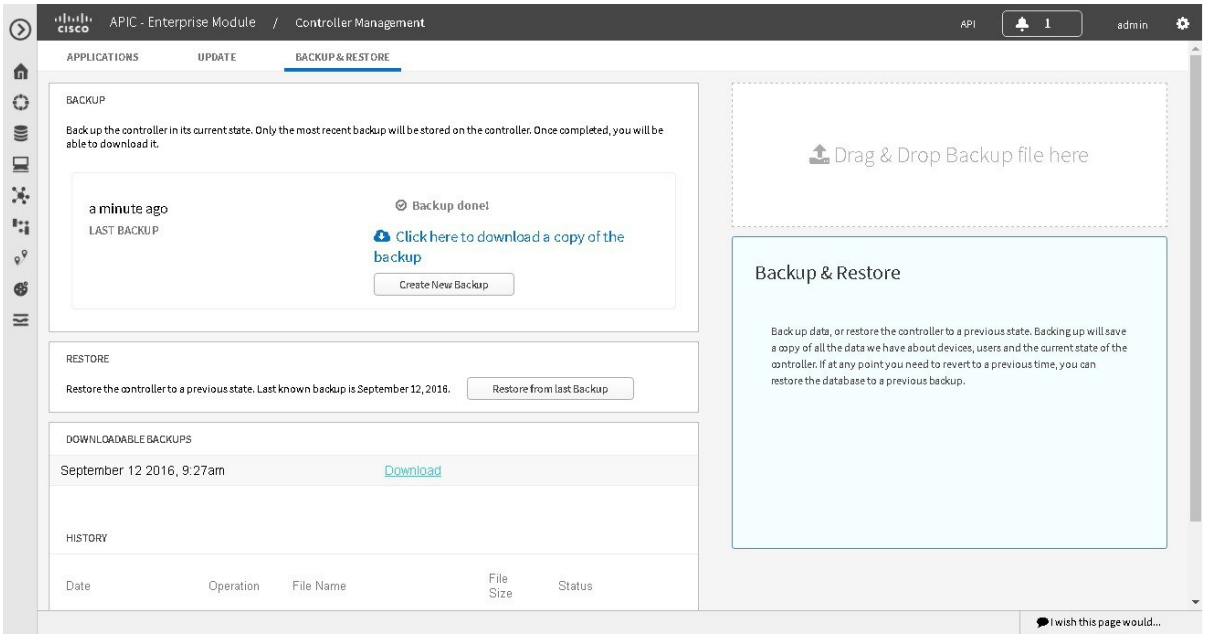
You can restore your controller using the **Backup & Restore** window.

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 32: Backup & Restore Window***




**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 the chapter, "Managing Users".

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.

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.

# Updating the Cisco APIC-EM Software

You can update the Cisco APIC-EM to the latest version using the controller's software update procedure. This procedure requires that you perform the following tasks:

1. Download the release upgrade pack from the secure Cisco cloud.
2. Run a checksum against the release upgrade pack.
3. Upload the release upgrade pack to the controller using the GUI.
4. Update the controller's software with the release upgrade pack.

**Important** This procedure should be read in conjunction with the latest version of the Cisco APIC-EM release notes, as there may be specific additional requirements for that release's upgrade. You should first review the *Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*, before beginning this procedure.

**Note** In a multi-host cluster, you only need to update a single host. After updating that single host, the other two hosts are automatically updated with the release upgrade pack.

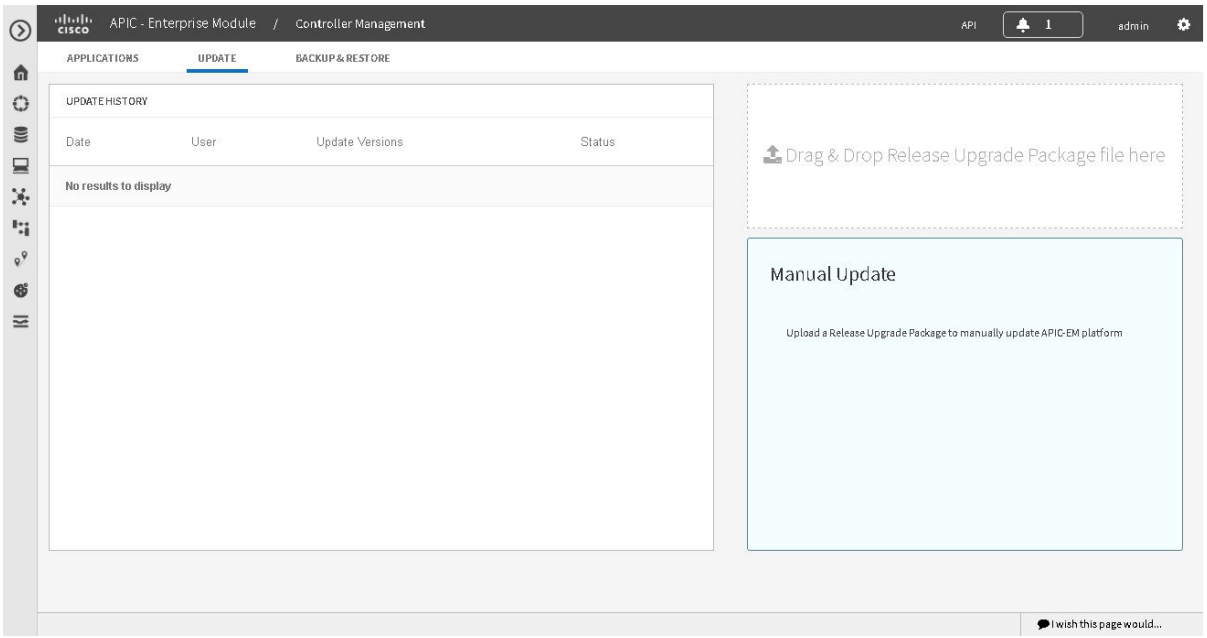
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

**Note** Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

You perform the upload and update procedure using the **Update** window in the Cisco APIC-EM GUI.

***Figure 33: Update Window***




**Note** After a successful upload and software update, you are not permitted to rollback to an earlier Cisco APIC-EM version.

### 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 the chapter, "Managing Users".

**Note** When updating or upgrading the Cisco APIC-EM in a virtual machine within a VMware vSphere environment, you must ensure that the time settings on the ESXi host are also synchronized to the NTP server. Failure to ensure synchronization will cause the upgrade to fail.

You must have received notification from Cisco that the Cisco APIC-EM software update is available for you to download from the secure Cisco website.

You can be notified about the availability of a Cisco APIC-EM software update in the following ways:

- Email notification from Cisco support and/or updated release notes.
- System notification through the controller GUI.

**Note** Notification about available release upgrade packs can be viewed by clicking the **System Notifications** icon on the menu bar.

**Step 1** Review the information in the Cisco notification about the Cisco APIC-EM update file and checksum.

The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

**Note** The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific update. The release upgrade pack can be as large as several Gigabits.

**Step 2** Download the release upgrade pack from the secure Cisco website to your laptop or to a location within your network.

**Step 3** Run a checksum against the release upgrade pack using your own checksum verification tool or utility (either MD5 or SHA512).

**Step 4** Review the displayed checksum verification value from your checksum verification tool or utility.

If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

**Step 5** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

**Step 6** Click the **App Management** link from the drop-down menu.

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

**Step 7** Click the **Update** tab at the top of the window.

**Step 8** If the release upgrade pack is acceptable to use for updating the controller (checksum value match in step 4), then drag and drop the release upgrade pack from the download location on your laptop or in your network onto the **Manual Update** field in the **Update** window.

After dropping the release upgrade pack onto the **Manual Update** field, the upload process begins.

The upload process may take several minutes depending upon the size of the release upgrade pack and your network connection. During the upload process, you can continue to work with the controller. Once the upload process ends and the update process begins, you will not be able to work with the controller.

**Note** If you close the **Update** window for any reason, then the upload process stops. To start the upload process again, open the **Update** window and drag and drop the release upgrade pack onto the **Manual Update** field again. The upload process starts where it previously stopped. To avoid any interruptions to the upload process while working with the controller, open additional windows in the GUI for any other tasks. Keep the **Update** window open during the upload process.

**Step 9** Once the upload process finishes, the update process automatically begins. A message appears in the GUI stating that the update process has started and is in progress.

You should refrain from working with the controller during the update process. During the update process, the controller may shut down and restart. The shut down process may last for several minutes.

**Note** At the beginning of the update process, the controller performs a second verification test on the release upgrade pack. The release upgrade pack itself contains an encrypted security value (signature) that will be decrypted and reviewed by the controller. This second verification test ensures that the release upgrade pack that has been uploaded is from Cisco. The release upgrade pack must pass this second verification test before the update process can continue.

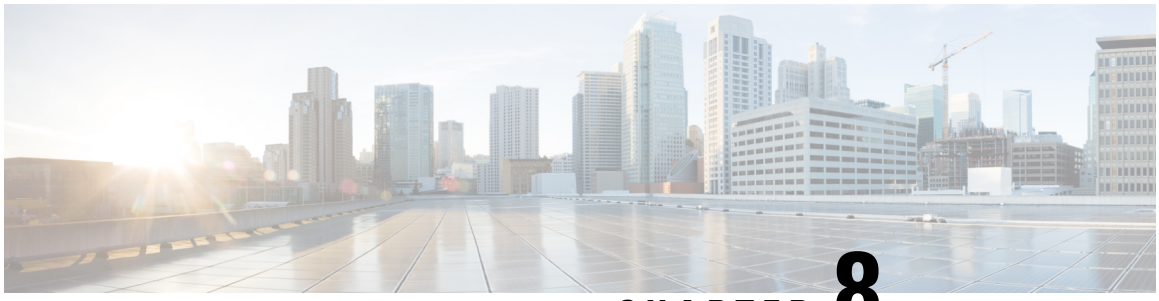
**Step 10** Once the update process finishes, you will receive a success or failure notification.

If the update was successful, you will receive a successful update notification and can then proceed working with the controller. If the update was unsuccessful, you will receive an unsuccessful update notification with suggested remedial actions to take.

After the update (or attempted update), information about it will also appear in the **Update History** field of the **Update** window. The following update data is displayed in this field:

- **Date**—Local date and time of the update
- **User**—Username of the person initiating the update
- **Update Version**—Update path of release upgrade pack version represented with an arrow.
- **Update Status**—Success or failure status of the update.

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



CHAPTER 8

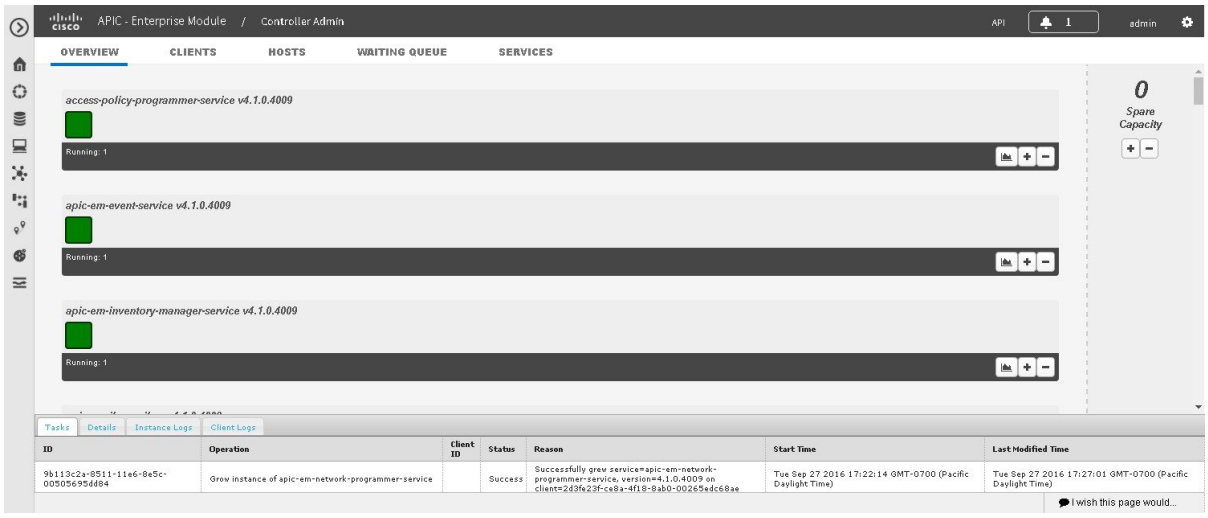
# System Administration Using the GUI



## 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 34: Controller Admin Console***



**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.

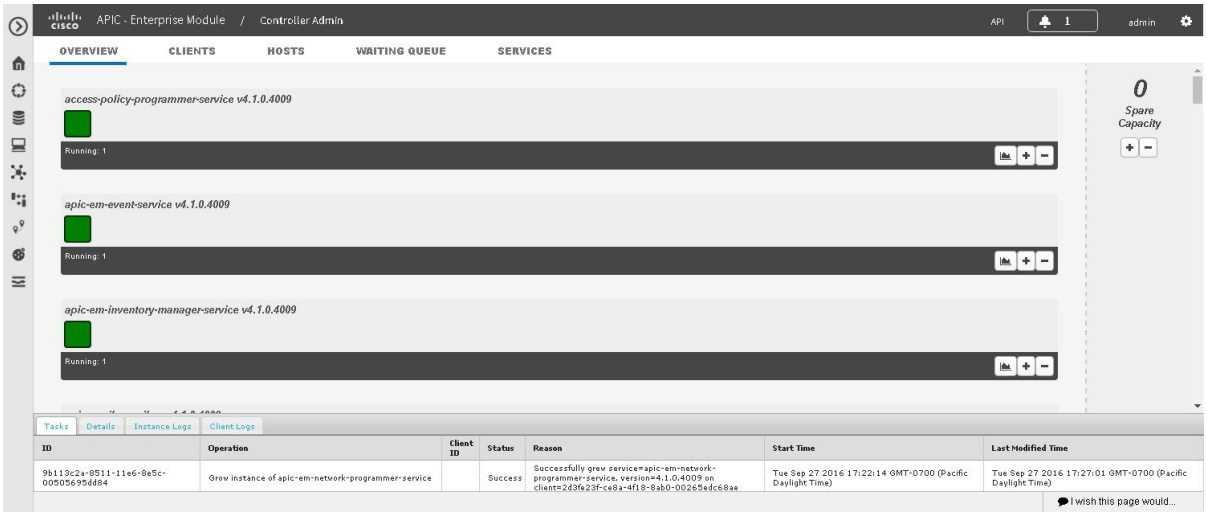
# Reviewing the Service's Version, Status, and Logs

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 35: Controller Admin Console*




### 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** 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 |

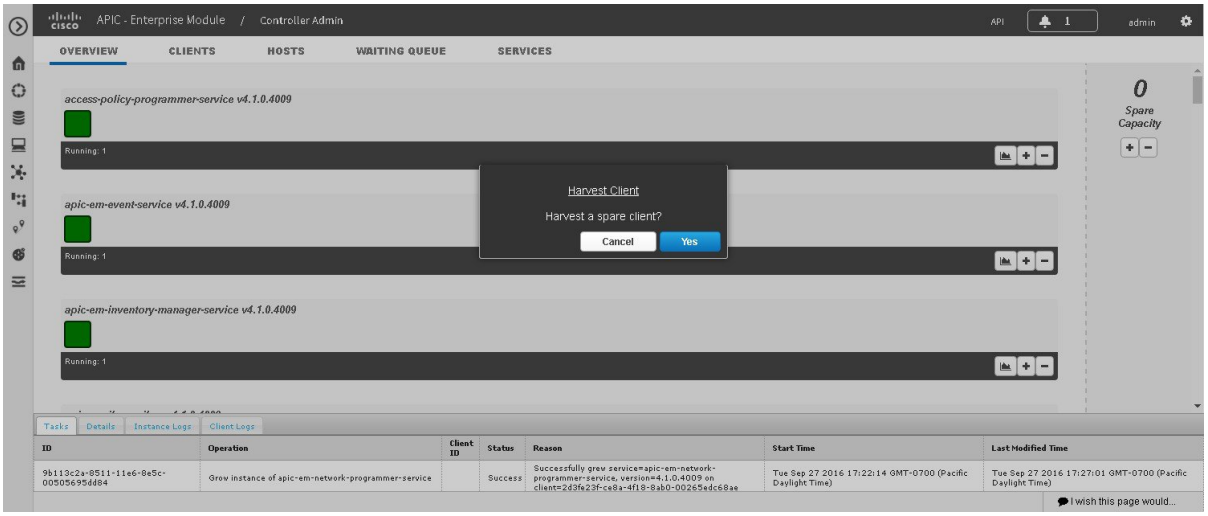
| | |
|---|---|
| **Operation** | Type of task, for example, growing a service |
| **Client ID** | Client identification number |
| **Status** | Status of the task, for example **Success** or **Failed**. |
| **Reason** | Reason given for either a successful or failed task. |
| **Start Time** | Time task 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 36: Removing (Harvesting) a Service Instance***




### 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** 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

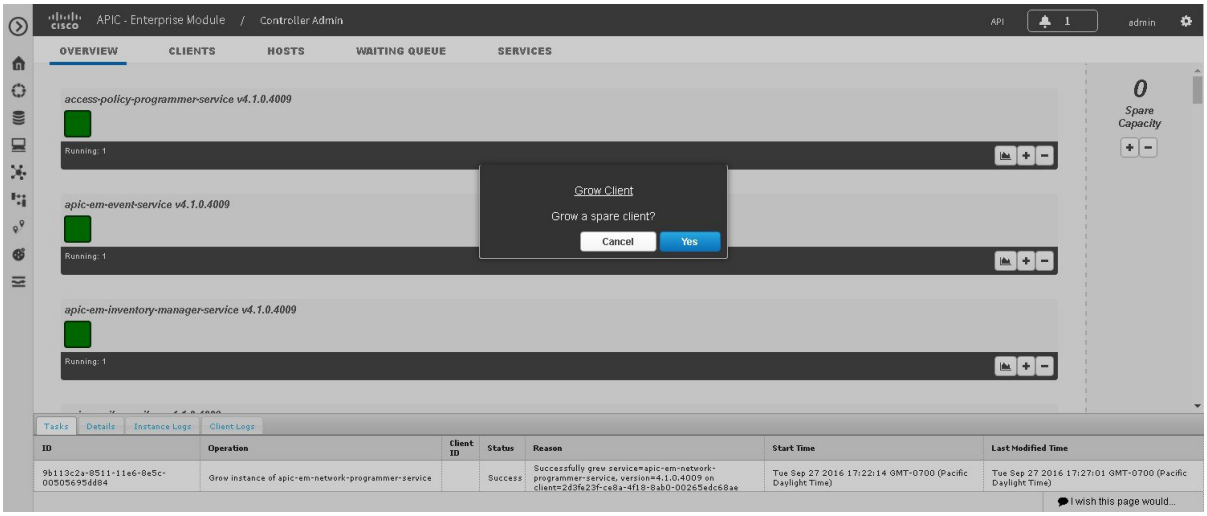
Manage your services by growing additional instances or removing (harvesting) instances from the services. When finished with the **Controller Admin** console, click another icon on the **Navigation** pane to exit the console.

# 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 37: Creating (Growing) a Service Instance*




### 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** 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.

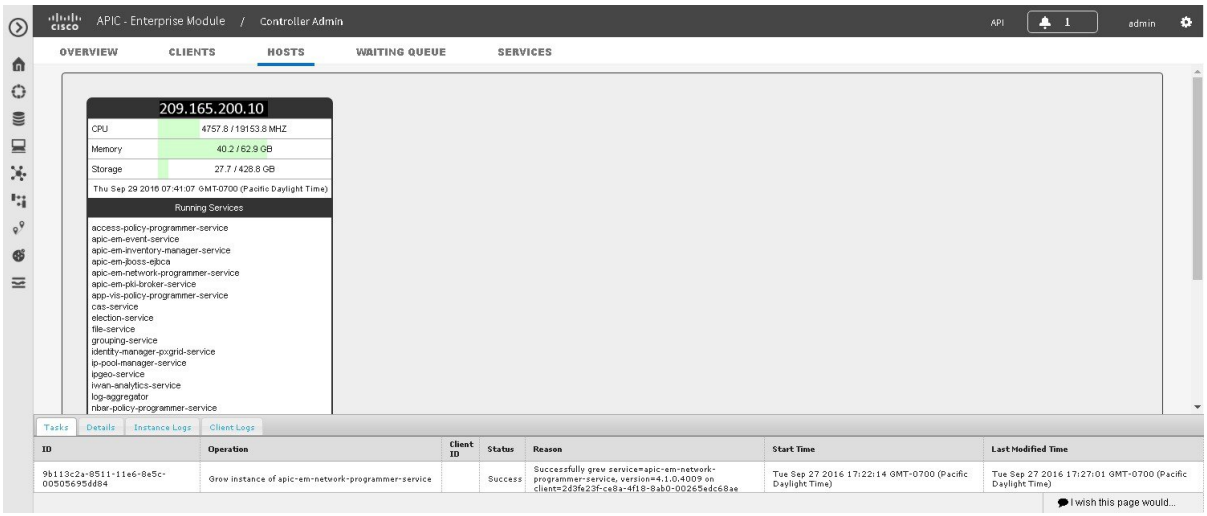
The controller then takes a client from the **Spare Capacity Pool** and spins up an instance of the service.

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 38: Host Data Displayed in the Controller Admin Console***




### 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.

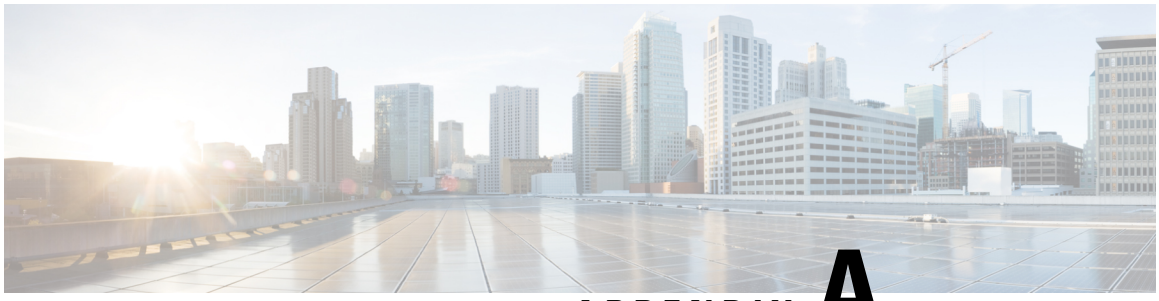
**Step 2** Click the **System Administration** link from the drop-down menu.

**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. |



APPENDIX A

# Cisco APIC-EM Multi-Host Support



## Multi-Host Support

A host is defined as an appliance, physical server, or virtual machine with Linux containers running instances of the Grapevine clients. The Grapevine root itself runs directly on the host's operating system and not in the Linux containers. You can set up either a single host or multi-host deployment. A multi-host deployment with three hosts is best practice for both high availability and scale. Each Grapevine root in a multi-host configuration maintains an Active/Active status with the other Grapevine roots and is therefore able to coordinate with the other Grapevine roots the overall management of the cluster.

**Note** Active/Active is defined as all Grapevine roots being operational and active.

Each host must be running the same controller software in the multi-host configuration. You are able to mix and match physical and virtual appliances in the multi-host configuration.

The multi-host configuration has the following requirements and features:

- Each host in a multi-host configuration requires a minimum of 32 GB of memory.
- A multi-host cluster comprised of 3 hosts is able to tolerate the loss of one of the hosts and supports a single fail-over (although with only two hosts, there is only software high availability, but no hardware high availability).

  **Note** If a second host also fails in the three host cluster, the remaining host in the cluster will become inoperable and the cluster will go down. Therefore, in the event of the loss of one of the hosts, we recommend that you remove this host from the cluster using the configuration wizard and then either repair and rejoin this host to the cluster or join a new host to the cluster.

- As each host is configured with 32 GB of memory, if a host failure occurs then the remaining hosts would have a total 64 GB of memory which is sufficient to run the controller.
- All three hosts must reside in the same subnet.

# Clustering and Database Replication

The clustering feature of the Cisco APIC-EM provides a mechanism for distributing processing and database replication among multiple hosts that run the exact same version of the controller. Clustering provides both a sharing of resources and features, and enables system high availability and scalability.

# Security Replication

In a multi-host environment, the security features of a single host are replicated among the other two hosts, including any X.509 certificates or trustpools. Once you join a host to another host or to a cluster, the Cisco APIC-EM credentials are shared and become the same as that of the host you are joining or the pre-existing cluster. The Cisco APIC-EM credentials are cluster-wide (across hosts) and not per-host.

**Note** We strongly suggest that any multi-host cluster that you set up be located within a secure network environment. For this release, privacy is not enabled for all of the communications between the hosts.

# Service Redundancy

The Cisco APIC-EM provides high availability support using service redundancy. A Cisco APIC-EM cluster can be set up across multiple Linux containers within multiple hosts. On each host, the Grapevine root is an application running on the host and the Grapevine clients are created and reside in the containers. Both the Cisco APIC-EM services and database are then instantiated across the clients within the Linux containers:

- Cisco APIC-EM Services:
  - For service high availability, if a service fails then Grapevine (the Elastics Service Platform) spins up a new instance to replace it. If Grapevine is unable to spin up the new instance on the same container after a sole instance fails, then it spins up a new container and then spins up the new instance on this container.
  - Cisco APIC-EM supports a replacement service instance model. For example, assume that one of the roots on a single host spins up an instance. If that host and its root goes down, then another host on another root spins up an instance to ensure continuity of that service.
- Cisco APIC-EM Database:
  - The Cisco APIC-EM services use a PostgreSQL database management system. PostgreSQL has a built-in master-slave model for synchronizing data across replicated databases to respond to any failover situation.
  - The master and slave postgres instances are grown across different Linux containers and across different hosts. The data of these postgresSql instances are synchronized using PostgresSQL's built-in data streaming replication mechanism. With three hosts, there is one master (with a master postgres instances) and two slaves (each with a slave postgres instance).
  - If the master fails, then the slave seamlessly takes over.
  - In the event of a failure by the master, an election process occurs among the remaining hosts to determine which becomes the new master. This election process can also be triggered by resetting the controller using the CLI or rebooting the host.

**Caution** To protect against any hardware failure, you must deploy the Cisco APIC-EM on a cluster with three hosts.

# Multi-Host Synchronization

Whenever there is a configuration change on one of the hosts, Grapevine synchronizes the change with the other two hosts. The supported types of synchronization include:

- Database—Synchronization includes any database updates related to the configuration, performance, and monitoring data.
- File—Synchronization includes any changes to the configuration files.

# Multi-Host Monitor Process

Grapevine is the main component that manages high availability operations in a cluster. To ensure proper cluster high availability operation, Grapevine uses both health checks and heart beats.

Health checks are used to monitor processes that are low performing and not running properly. Services that run on Grapevine have health checks that are periodically invoked. If there is any indication of an unhealthy service, Grapevine will harvest and regrow that service.

In addition to the health checks, Grapevine also uses heart beats between the services, clients, and roots to monitor the status of the cluster. Grapevine monitors these heart beats for any processes that may have failed. If there is no heart beat, then this indicates that a process has failed and to correct for this situation, Grapevine regrows the service.

Grapevine also uses a heart beat to monitor for adequate memory and storage capability for the cluster. If a heart beat indicates that the cluster's memory or storage fails below an appropriate level necessary for successful operations, then Grapevine will not grow any new services.

# Split Brain and Network Partition

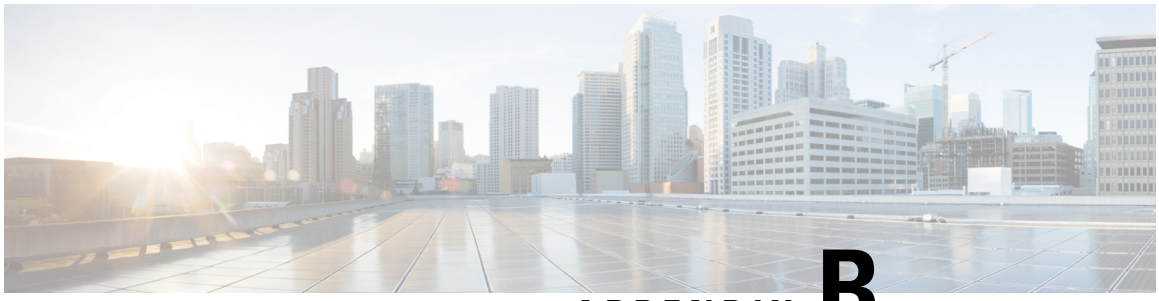
When Cisco APIC-EM is configured as a multi-host cluster, a private network connection is set up between the hosts. This private network connection is used by each host to monitor the health and status of the other cluster hosts. A split brain occurs when there is a temporary failure of the network connection between the hosts, for example, due to any of the following occurrences:

- Physical disconnection of the network connection from a host
- Loss of power to one or more hosts
- Cisco APIC-EM appliance failure

During a split brain occurrence, situations can arise where each separate host is sending commands to a given network device without any coordination with the other hosts, and the results can be problematic.

To correct for a split brain event, when the private network connection fails between one of the hosts, the other two hosts create a quorum and establish a network partition between themselves and the failed host with the following results:

- The split brain or network partition scenarios are be handled by ensuring quorum (majority reads and rights) to the controller database.
- The side of the partition with the "minority" stops operating, since it is be unable to perform quorum (majority reads and rights) to the controller database.
- The side of the partition with the "majority" continues to operate, since they are *able* to perform quorum (majority reads and rights) to the controller database.



APPENDIX B

# Preparing Virtual Machines for Cisco APIC-EM



## Preparing a VMware System for Cisco APIC-EM Deployment

To ensure that the Cisco APIC-EM works well within a virtual environment, configure the virtual machine with recommended resource pool values. A resource pool is a logical abstraction for the virtual machines that can be used to manage resources. Resource pools can be grouped into hierarchies and then used to partition CPU and memory resources.

You can configure and prepare the virtual machine using either the VMware vSphere Client or Web Client. We recommend that you use the VMware vSphere Web Client, since the **Latency Sensitivity** setting for resource pools must be configured as **High**. The **Latency Sensitivity** setting can only be configured using the VMware vSphere Web Client.

**Note** When deploying the Cisco APIC-EM in a virtual environment, you must first configure the VMware system before installing Cisco APIC-EM. To install Cisco APIC-EM, you need to download the ISO image containing the controller from Cisco.com and then map the ISO image to the VMware system and boot from it.

### Related Topics


Configuring Resource Pools Using vSphere Web Client, on page 154

Configuring a Virtual Machine Using vSphere Web Client, on page 157

System Requirements—Virtual Machine, on page 8


## Virtual Machine Configuration Recommendations

The following table lists the recommended configuration settings for a successful Cisco APIC-EM VMware vSphere installation, including resource pools. When installing Cisco APIC-EM on a supported virtual machine, we recommend that the following configuration settings are used.

**Note** When preparing the virtual machine for the Cisco APIC-EM, the configuration settings terminology may differ depending upon the VMware application and GUI that your are using.

***Table 10: Virtual Machine Configuration Recommendations (Including Resource Pools)***

| | |
|---|---|
| Datastores | We recommend that you do not share a datastore with any defined virtual machines that are not part of the designated Cisco APIC-EM cluster.<br>If the datastore is shared, then disk I/O access contention may occur and cause a significant reduction of disk bandwidth throughput and a significant increase of I/O latency to the cluster.<br>**Note** When configuring the virtual machine, you can select any of the VMware virtual machine provisioning polices for the virtual disk file (Thick Provision Lazy Zeroed, Thick Provision Eager Zeroed, or Thin Provision). |
| Resource Pool: CPU Resources | • Shares—Normal<br>• Reservation—14400 MHz is minimum configuration setting for this value<br>• Reservation Type—Check box for Expandable<br>• Limit—Unlimited |
| Resource Pool: Memory Resources | • Shares—Normal<br>• Reservation—Refer to the *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes* for detailed information about RAM requirements.<br>• Reservation Type—Check box for Expandable<br>• Limit—Unlimited |
| VMware ESXi Version | 5.1/5.5/6.0 |
| Guest OS: Family and Version | • Guest OS Family—Linux<br>• Guest OS Version—Ubuntu Linux (64-bit) |

| | |
|---|---|
| Virtual Hardware: CPU | • CPU— 6 cores (minimum)<br>• Reservation—14400 MHz is minimum configuration setting for this value<br>• Limit—Unlimited<br>• Shares—Normal<br>**Note** 6 CPUs is the minimum number required for your virtual machine configuration. For better performance, we recommend using 12 CPUs. Additionally, the number of sockets used when setting up CPUs to a virtual machine in VMware does not impact the controller's performance. |
| Virtual Hardware: Memory | • Memory—Refer to the *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes* for detailed information about RAM requirements.<br>• Reserve all memory—Check box to Enable. |
| Virtual Hardware: New Hard disk | 500 GB (minimum) |
| Virtual Hardware: New SCSI controller | VMware Paravirtual |
| Virtual Hardware: New network | • New network value—Enter the network IP address that the controller will connect to for this value.<br>• Status—Check box to enable Connect at Power On<br>• Adapter type—VMXNET3 |
| Virtual Hardware: New CD/DVD Drive | Select Datastore ISO file from the drop down and the configure the location of the ISO file in the File window |
| VM Options: Advanced | Choose High for Latency Sensitivity<br>**Note** You can configure and prepare the virtual machine using either the VMware vSphere Client or Web Client. We recommend that you use the VMware vSphere Web Client, since the Latency Sensitivity setting for resource pools must be configured as High. The Latency Sensitivity setting can only be configured using the VMware vSphere Web Client. |

# Configuring Resource Pools Using vSphere Web Client

To ensure that the Cisco APIC-EM works well within a virtual environment, you should configure resource pools with the recommended values. A resource pool is a logical abstraction for the virtual machines that can be used to manage resources. Resource pools can be grouped into hierarchies and then used to partition CPU and memory resources.

**Note** You should first create a new resource pool with the recommended configuration values as described in this procedure, and then subsequently create a virtual machine (where the Cisco APIC-EM will be installed) on that resource pool.

### Before you begin

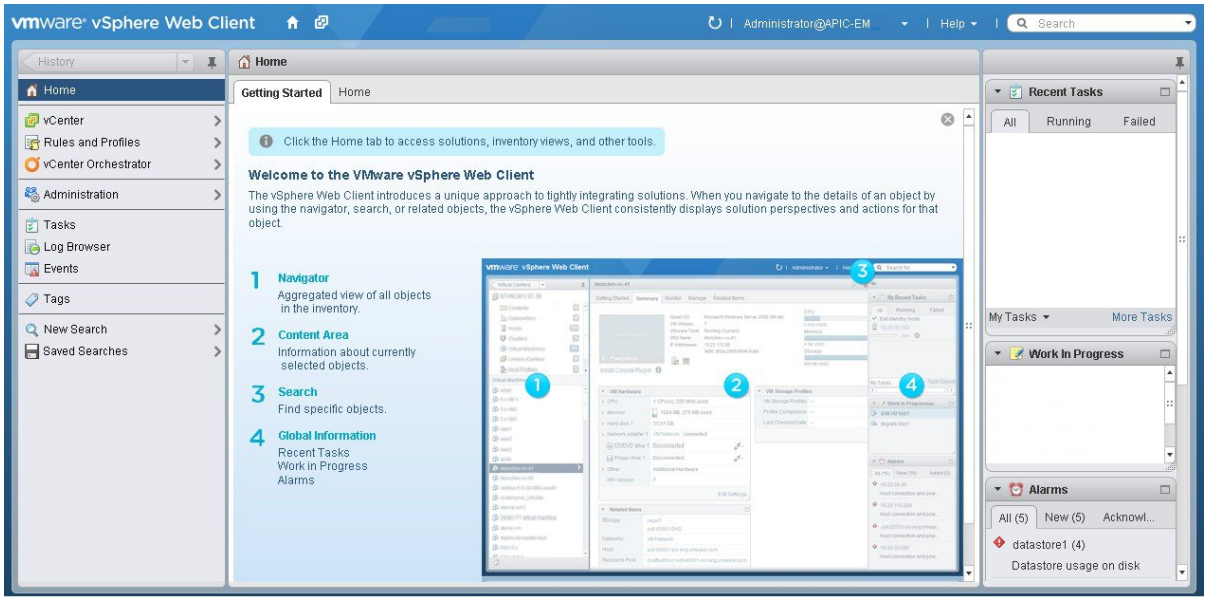
You have reviewed your VMware documentation concerning resource pools and their configuration.

You are familiar with the VMware vSphere Web Client and have a basic knowledge of how to create, manage and troubleshoot virtual machines using it.

You have your host and virtual datastores already set up and accessible in vSphere Web Client for this procedure.

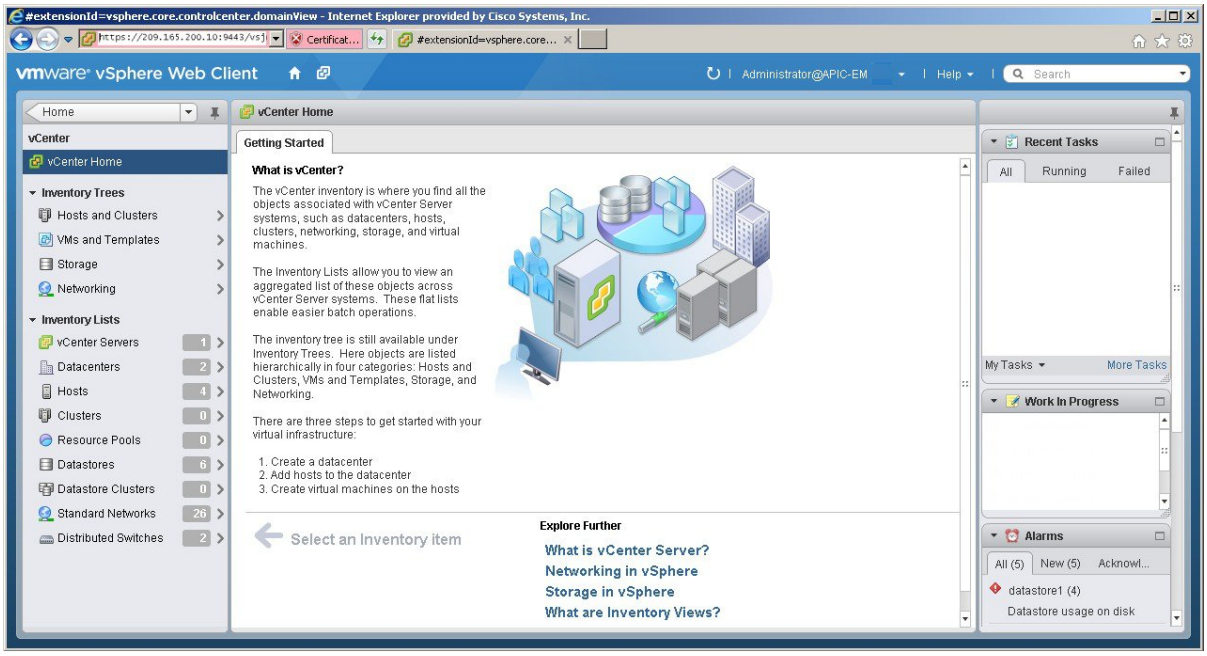
**Step 1** Open the VMware vSphere Web Client to perform the procedure.

***Figure 39: VMware vSphere Web Client***



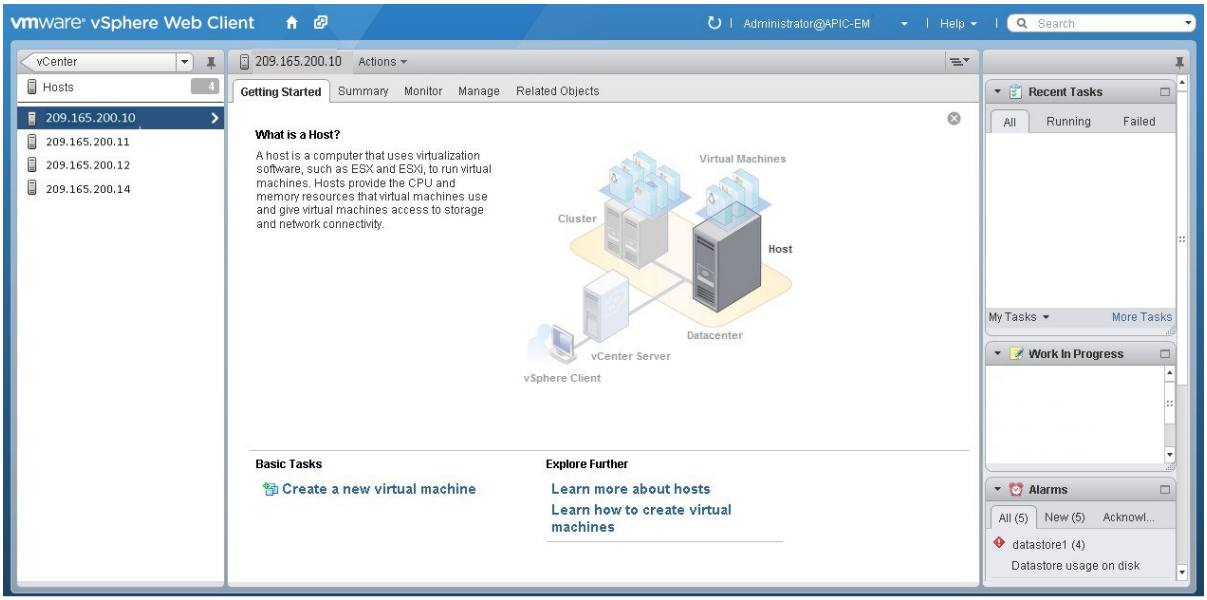

**Step 2** Click **vCenter** in the **Navigator**.

*Figure 40: vCenter Home*




**Step 3** Click on **Hosts**.

*Figure 41: Hosts*

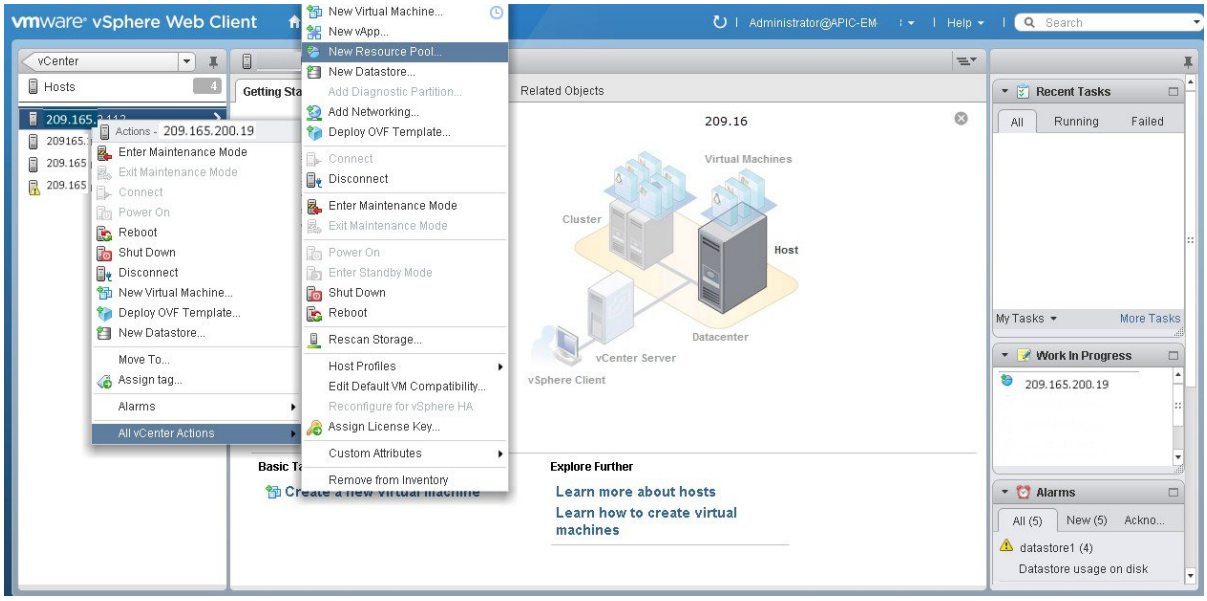



Choose a host where you will create the resource pool.

**Step 4** Right-click on the selected host and click **All vCenter Actions** | **New Resource Pool**.

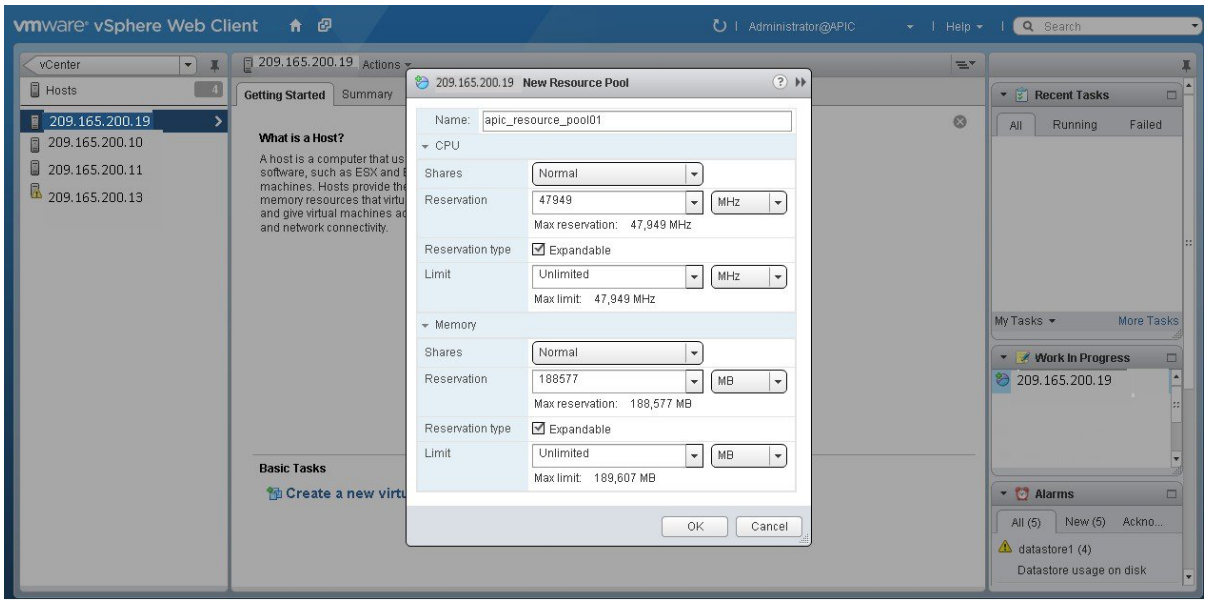
Preparing Virtual Machines for Cisco APIC-EM

*Figure 42: New Resource Pool*




**Step 5** Enter a name and specify values for the resource pool in the **New Resource Pool** dialog box.

*Figure 43: New Resource Pool*




We recommend entering the following resource pool values in this dialog box:

- **CPU Resources**
  - **Shares**—Choose **Normal** from the drop-down menu
  - **Reservation**—14400 MHz is minimum configuration setting for this value
  - **Reservation Type**—Check box for Expandable

- **Limit**—Set to Maximum Limit

- **Memory Resources**
  - **Shares**—Choose **Normal** from the drop-down menu
  - **Reservation**—32 GB or 64 GB is the minimum configuration setting for this value, depending upon your hardware.
  - **Reservation Type**—Check box for Expandable
  - **Limit**—Set to Maximum Limit

**Step 6** Click **OK** to save the configured resource pool values.

### What to do next

Proceed to create a new virtual machine on this resource pool. For assistance with this procedure, see the following procedure, Configuring a VMware Server Using vSphere Web Client.

### Related Topics

Preparing a VMware System for Cisco APIC-EM Deployment, on page 151
Virtual Machine Configuration Recommendations
System Requirements—Virtual Machine, on page 8

# Configuring a Virtual Machine Using vSphere Web Client

To ensure that the Cisco APIC-EM properly functions in a virtual environment, create the virtual machine(s) following the procedure described below with the recommended settings.

**Note** You must create this virtual machine on the resource pool that you earlier configured, as described in the previous procedure.

### Before you begin

You have reviewed the minimum system requirements for a successful Cisco APIC-EM VMware vSphere installation, as previously described in this guide.

You are familiar with the VMware vSphere Web Client and have a basic knowledge of how to create, manage and troubleshoot virtual machines using the Web Client.

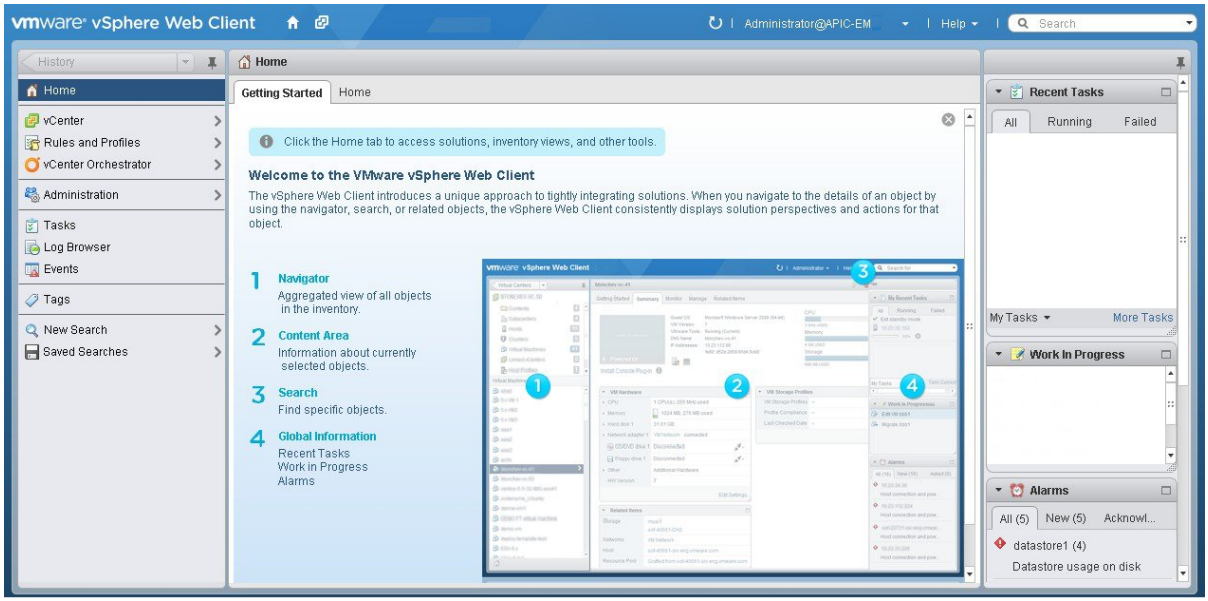
You have your host and virtual datastores already set up and accessible in vSphere Web Client for this procedure.

You have already created a resource pool on the host, following the steps described in the previous procedure, Configuring Resource Pools Using vSphere Web Client.

**Step 1** Open the VMware vSphere Web Client to perform the procedure.

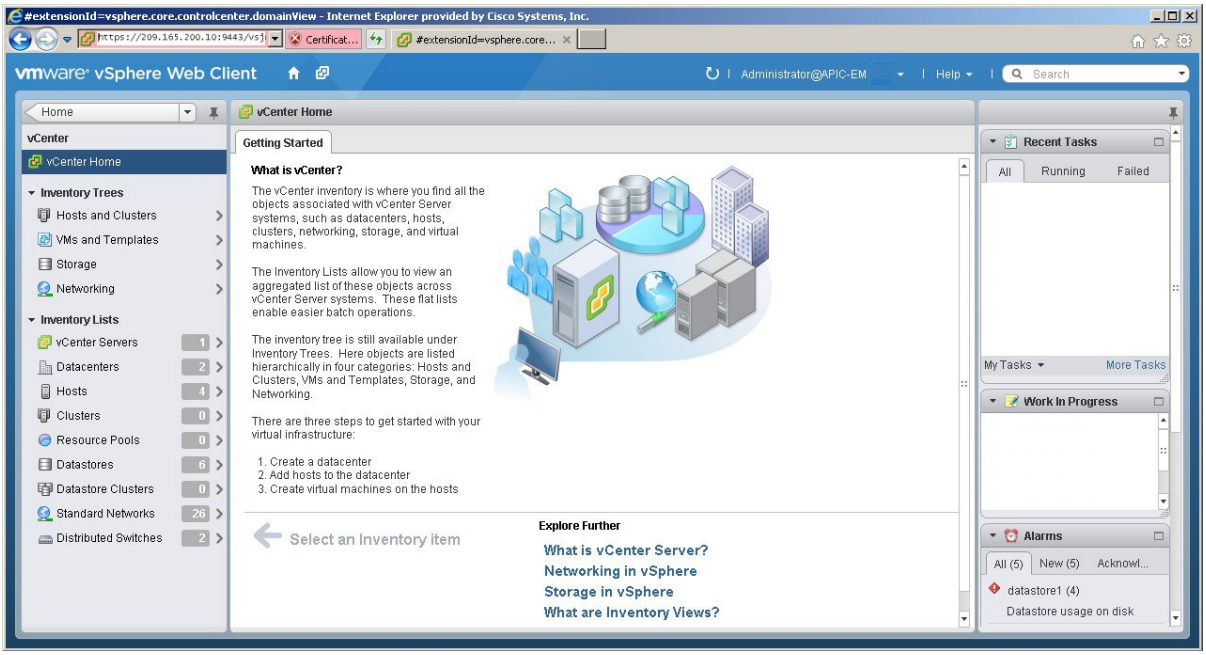
Preparing Virtual Machines for Cisco APIC-EM

*Figure 44: VMware vSphere Web Client*




**Step 2** Click **vCenter** in the **Navigator**.

*Figure 45: vCenter*

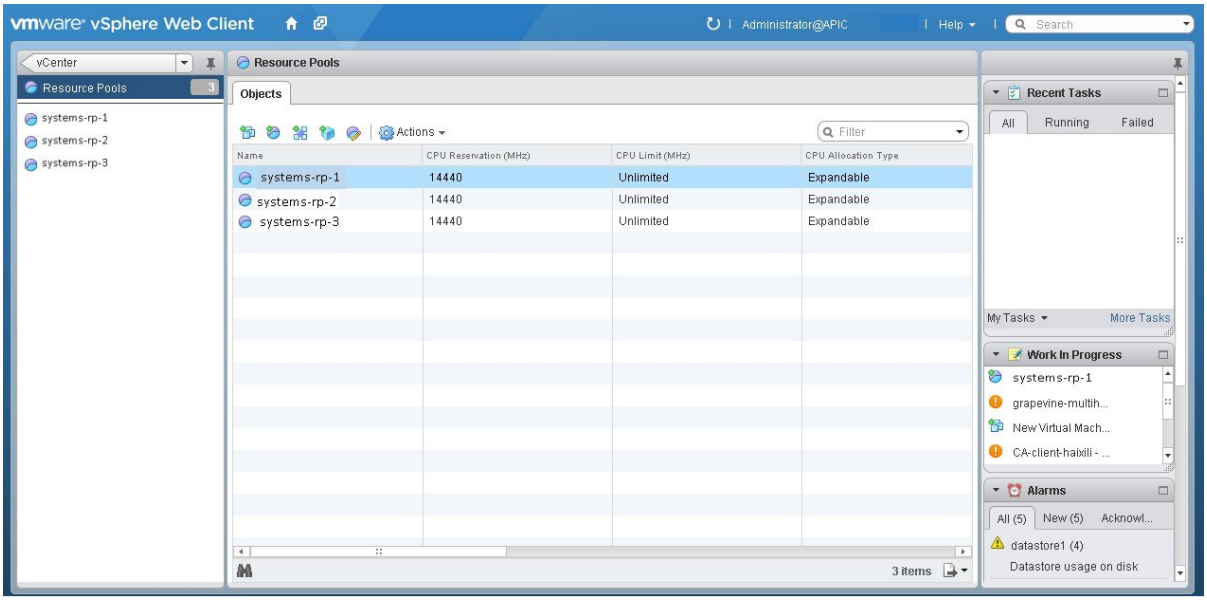



**Step 3** Click **Resource Pools** in the **Inventory Lists** in **vCenter**.

**Step 4** Choose the resource pool where you will install the virtual machine from the list.

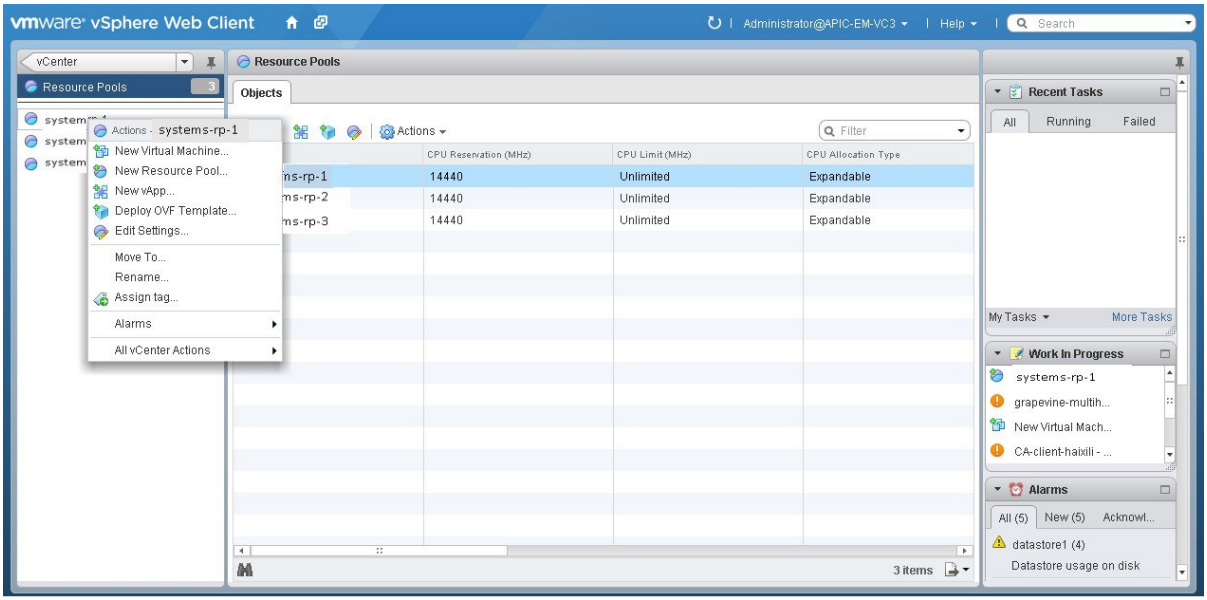
Preparing Virtual Machines for Cisco APIC-EM

*Figure 46: Resource Pools*




**Step 5** Right click on the resource pool and select **New Virtual Machine** from the menu.

*Figure 47: New Virtual Machine*

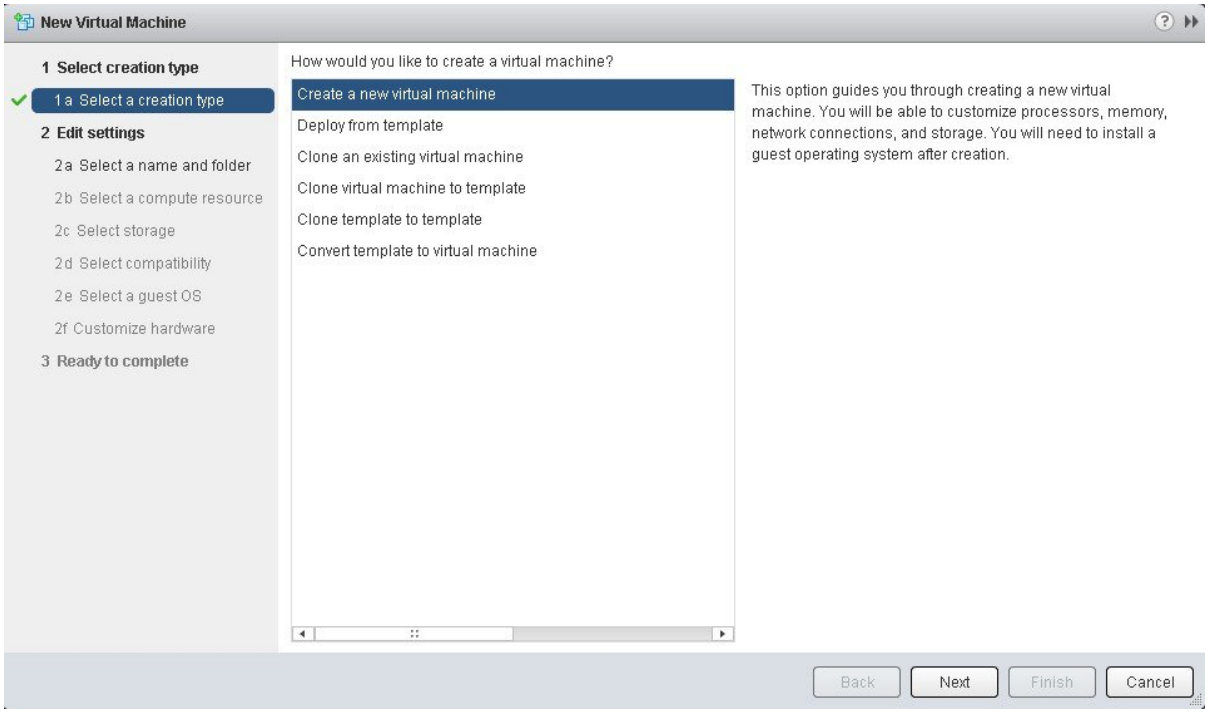



**Note** We strongly recommend that only a single virtual machine be created under the resource pool.

**Step 6** Click **Create a new virtual machine** in the **New Virtual Machine** dialog box under **1a Select creation type**.

Preparing Virtual Machines for Cisco APIC-EM

*Figure 48: Select Creation Type*

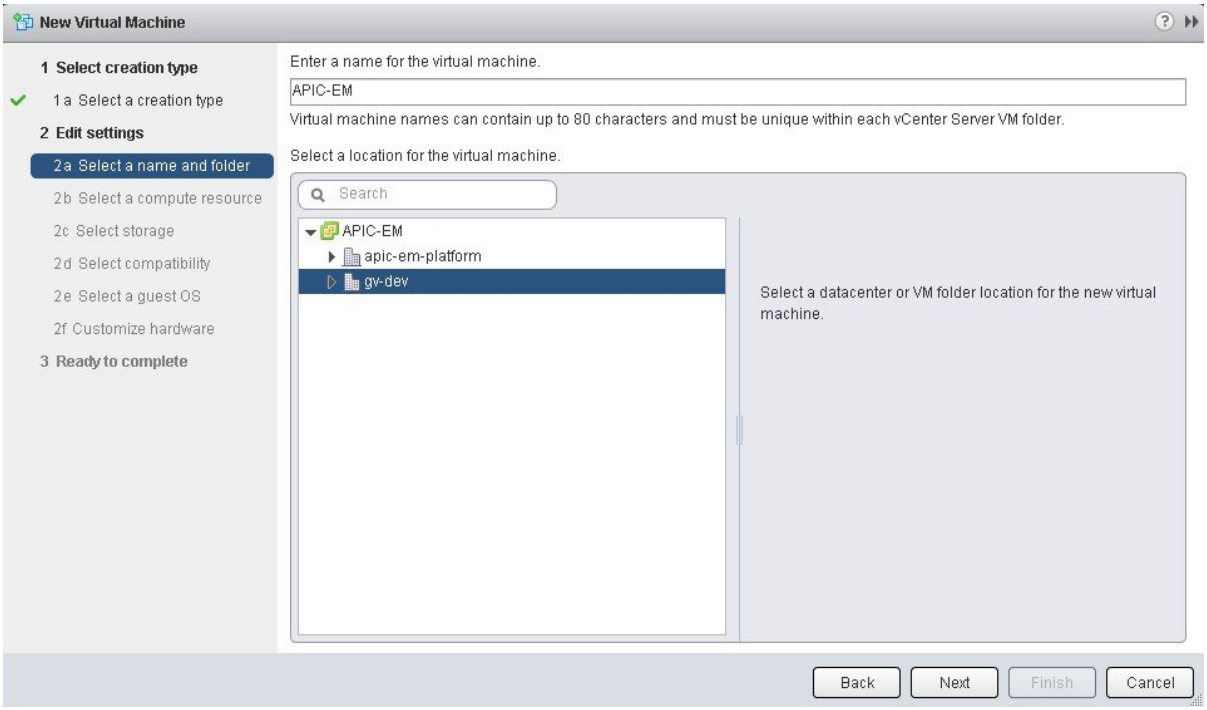



Click **Next** to proceed to the next step.

**Step 7** In the **New Virtual Machine** dialog box under **2 Edit Settings**, click **2a Select a name and folder**.

Enter a name for the virtual machine and a location for the virtual machine.

*Figure 49: Select Name and Folder*



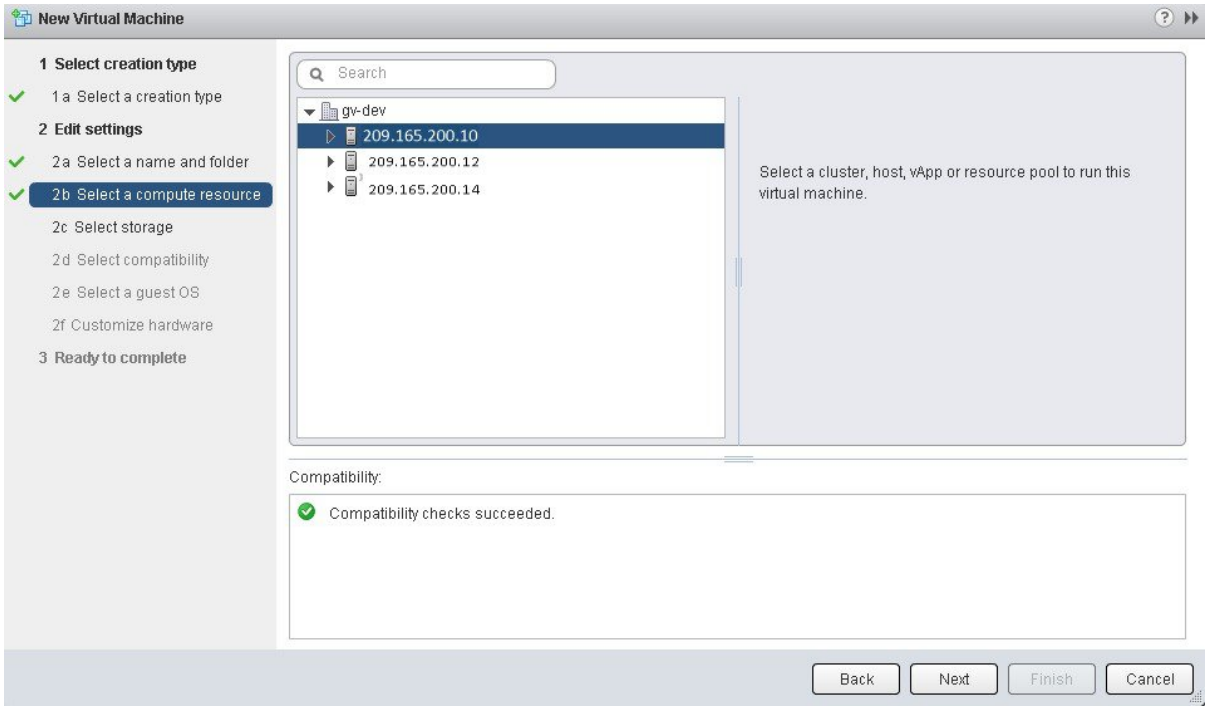

Click **Next** to proceed to the next step.

**Step 8** Click **2b Select a computer resource**.

Select the resource pool that was created in the previous procedure.

Preparing Virtual Machines for Cisco APIC-EM

*Figure 50: Select Computer Resource*

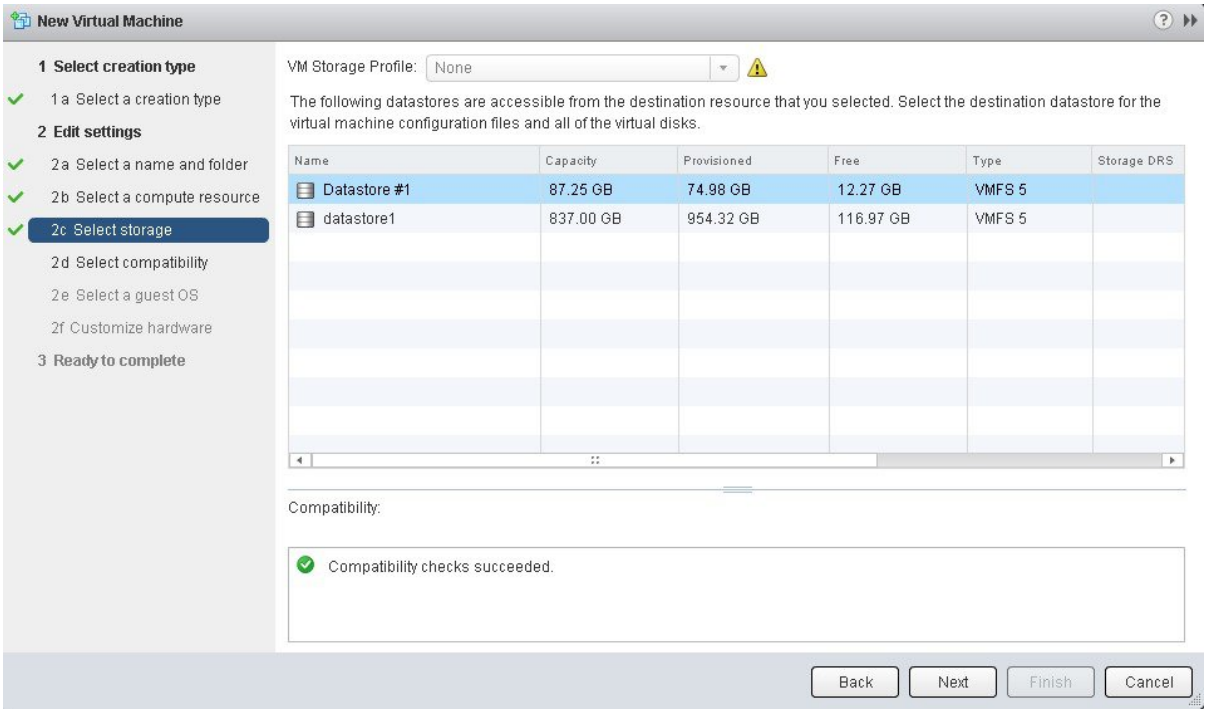



Click **Next** to proceed to the next step.

**Step 9** Click **2c Select storage**.

Select a datastore for your virtual machine.

*Figure 51: Select Storage*



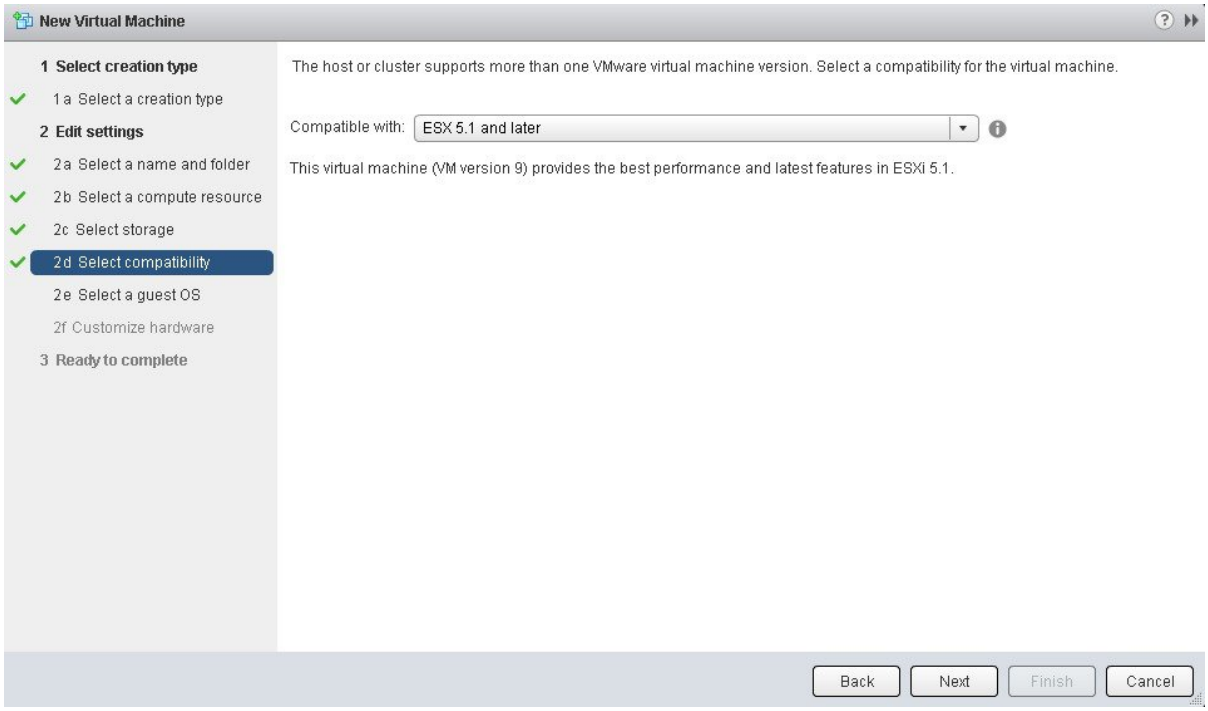

Click **Next** to proceed to the next step.

**Step 10** Click **2d Select compatibility**.

Select **ESX 5.1 and later** from the drop down menu.

Preparing Virtual Machines for Cisco APIC-EM

*Figure 52: Select Compatibility*



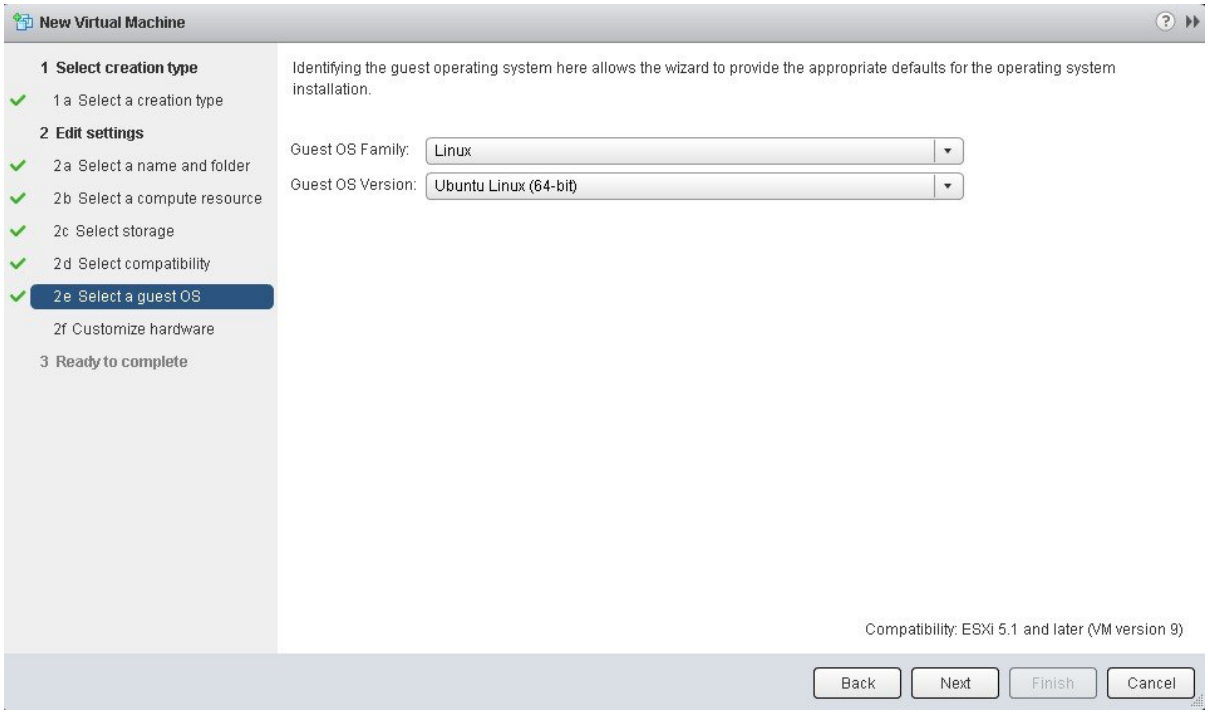

Click **Next** to proceed to the next step.

**Step 11** Click **2e Select a guest OS**.

Select the following values from the drop down menus:

- **Guest OS Family**: Linux
- **Guest OS Version**: Ubuntu Linux (64-bit)

*Figure 53: Select Guest OS*

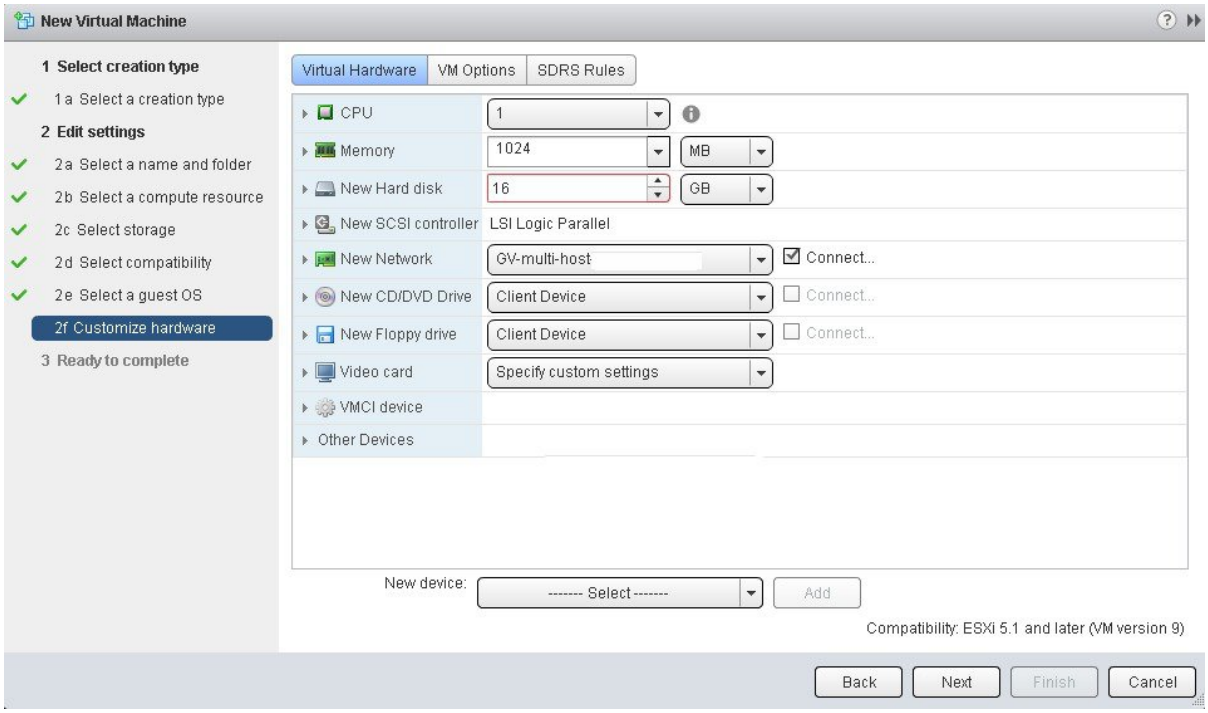



Click **Next** to proceed to the next step.

**Step 12** Click **2f Customize hardware**.

Preparing Virtual Machines for Cisco APIC-EM

*Figure 54: Customize Hardware*




**Step 13** In the **Virtual Hardware** tab, ensure that the following **CPU** values are selected.

| | |
|---|---|
| **CPU** | Enter a value of 6 cores.<br>**Note** 6 cores is the minimum number to enter for your virtual machine configuration. For better performance, we recommend entering and using 12 cores. |
| **Reservation** | Enter a minimum value of at least 14400 MHz. |
| **Limit** | Select **Unlimited** from the drop down menu |
| **Shares** | Select **Normal** from the drop down menu. |

**Note** The above dedicated CPU resources for the host are required for the Cisco APIC-EM.

**Step 14** In the **Virtual Hardware** tab, ensure that the following **Memory** values are selected.

| | |
|---|---|
| **Memory** | Enter a minimum value of 32 GB or 64 GB, depending on your hardware. |
| **Reserve all guest memory (all locked)** | Check this box. |

**Note** The above dedicated memory resources for the host are required for the Cisco APIC-EM.

**Step 15** In the **Virtual Hardware** tab, ensure that the following **New Hard disk** value is entered.

| | |
|---|---|
| **New Hard disk** | Increase to at least 500 GB minimum. |

**Step 16** In the **Virtual Hardware** tab, ensure that the following **New SCSI controller** value is entered.

| | |
|---|---|
| **New SCSI controller** | Select **VMware Paravirtual** from the drop down menu. |

**Step 17** In the **Virtual Hardware** tab, ensure that the following **New Network** values are entered.

| | |
|---|---|
| **New network value** | Enter the network that the controller will connect to for this value. |
| **Status** | Check the box for **Connect at Power On**. |
| **Adapter type** | Select **VMXNET3** from the drop down menu. |

**Step 18** In the **Virtual Hardware** tab, ensure that the following **New CD/DVD Drive** value is entered.

| | |
|---|---|
| **New CD/DVD Drive** | Select **Datastore ISO file** from the drop down and configure the location of the ISO file in the **File** window. |
| **Status** | Check the box for **Connect at Power On**. |

**Step 19** Click the **VM Options** tab to open it and ensure that the following values are entered.

| | |
|---|---|
| **Advanced** | Choose **High for Latency sensitivity** from the drop down menu. |

Click **Ok** to save your configuration and to proceed to the next step.

**Step 20** Click **3 Ready to complete**.

Click **Finish** to finish the virtual machine configuration.

**Step 21** In the virtual machine, map the Cisco APIC-EM ISO image onto the local drive (CD/DVD).

**Step 22** Boot up the virtual machine and choose the **CD-ROM** option from the **Boot Menu**.

**Step 23** Choose **Install Grapevine Appliance** from the **Ubuntu** window that appears in the virtual machine.

### What to do next

Proceed to configure the controller by following the configuration wizard prompts.

For information about the configuration process, see following sections:

- Configuring Cisco APIC-EM as a Single Host Using the Wizard, on page 47
- Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard, on page 54

### Related Topics

Preparing a VMware System for Cisco APIC-EM Deployment, on page 151
Virtual Machine Configuration Recommendations
System Requirements—Virtual Machine, on page 8

Preparing Virtual Machines for Cisco APIC-EM

# INDEX

## Q



## R



## S



## T



## U



## V