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.

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
EasyQoS application	The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration.
Cisco Network Plug and Play (PnP) application	The Cisco Network PnP application is one of the components in the Cisco Network PnP solution. The Cisco Network PnP solution extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points.
Cisco Intelligent WAN (IWAN) application	The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links.
Cisco Active Advisor	The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on: • End-of-life milestones for hardware and software • Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices • Warranty and service contract status
Cisco SD-Bonjour	The Cisco SD-Bonjour application provides controller functions in the network. It enables discovery and distribution of policy-based Cisco SD-Bonjour services, independent of network boundaries.
Cisco Integrity Verification	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.

Feature	Description
Cisco Remote Troubleshooter	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. 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.
Path Trace application	The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
High Availability (HA)	HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing.
Back Up and Restore	The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI.
Audit Logs	The audit log captures user and network activity for the Cisco APIC-EM applications.

Logging into the Cisco APIC-EM

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

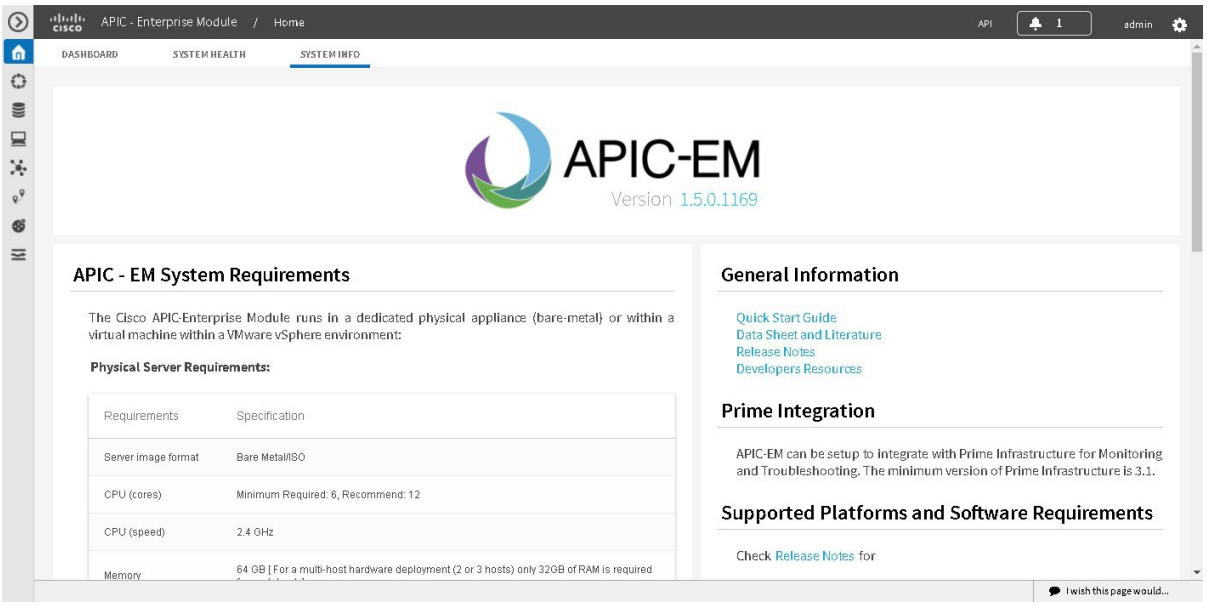
Step 1 In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:
https://*IP address*

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

- **DASHBOARD**

- SYSTEM HEALTH
- SYSTEM INFO

Figure 1: SYSTEM INFO Tab



What to Do Next

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

About Path Trace

With Path Trace, the controller reviews and collects network topology and routing data from discovered devices. Then it uses this data to calculate a path between two hosts or Layer 3 interfaces.

Optionally, you can choose to collect interface, QoS, device, and Performance Monitor statistics for a path. You can use the information gathered through Path Trace to monitor and debug traffic paths that are distributed among the various devices throughout your network.

You perform these tasks by running a path trace between two nodes in your network. The two nodes can be a combination of wired or wireless hosts and/or Layer 3 interfaces. In addition, you can specify the protocol for the controller to use to establish the path trace connection, either TCP or UDP.

Note Path traces from the a router's loopback interface or a wireless controler's management interface are not supported.

Note For devices connected to a voice or video endpoint (for example, Cisco IP phones), you need to enable IP Device Tracking (IPDT) for these devices to discover voice/data VLAN information about the endpoints. For information, see IP Device Tracking Configuration.

At every node in the path, the controller reports information about the device and path. For example, if a Layer 2 protocol is used to discover a node, the controller reports that the path is a switched path and labels it as **Switched**. If the controller detects load balancing decisions being made on a discovered device, it reports the path as an ECMP path and labels it as **ECMP**. For a complete list of the protocols and technologies that path trace can identify, see Supported Protocols and Technologies, on page 6.

For unknown devices within a path trace (usually non-Cisco devices), the controller calculates the path between the unknown devices starting from the last known Cisco device (from the **Host Source IP**) to the next, neighboring Cisco device (sometimes the **Destination Source IP**). The collected IP address data about the unknown device is then sent from this neighboring Cisco device to the controller to calculate the trace path. The unknown device is displayed in the controller's GUI as a question mark (?).

Note In certain circumstances, a path trace may flow between one of two (or more) devices. To determine which device actually received the flow for the path trace, the controller reads the NetFlow configurations and records on the devices (if they exist). By reading this data from the devices, the controller can determine the likelihood of the actual path.

Path Trace also supports unknown destinations, where the device is not managed by the Cisco APIC-EM but is reachable.

After the Cisco APIC-EM performs an initial scan, additional on-going network scans are performed at regular intervals every few minutes. Information captured during the on-going scans are displayed in the **Devices** table. Click **Device Inventory** in the navigation pane to view the **Devices** table. Each time the Cisco APIC-EM performs a scan, it also reads and records access control list, quality of service, and SPAN policy configuration information from the network.

Supported Network Environments

Cisco APIC-EM can perform path trace calculations for both campus and WAN networks based on physical connectivity and the protocols used by devices within the path. Specifically, the Cisco APIC-EM supports path traces through the following networking environments:

- Campus/data center to campus/data center
- Campus/data center to branch
- Branch to campus/data center
- Branch to branch

Note If the controller can not complete a path trace for the selected hosts or interfaces, it displays the results of a partial trace.

Supported Protocols and Technologies

The following table describes the device protocols, network connections (physical, wireless, and virtual), and features that Path Trace supports.

Note For detailed information about protocol, wireless connection, and feature support by platform and scenario, see the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

Table 2: Path Trace Supported Device Protocols and Network Connections

Supported Device Protocols and Network Connections	Description
Access Control List (ACL)	Access Control List (ACL) Trace analyzes how a flow is affected by ACLs programmed on the path. After the path is calculated between the source and the destination, the ACL Trace analyzes both ingress and egress interfaces of all devices on the path. Analysis is independent among the ACLs throughout the path. For example, if an ACL has entries that would deny the traffic on an interface along the path, the results of the analysis are reported as if the traffic had reached the destination without being denied by the ACL. However, analysis of entries within an individual ACL is cumulative. That is, if a higher priority ACE is a match, lower-priority ACEs are ignored.
Border Gateway Protocol (BGP)	When BGP is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Dynamic Multipoint VPN (DMVPN)	Path Trace shows DMVPN dynamic tunnels between two spokes by identifying the link information source. For more information, see Understanding DMVPN Path Trace Results.
Enhanced Interior Gateway Routing Protocol (EIGRP)	When EIGRP is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.

Supported Device Protocols and Network Connections	Description
Equal Cost Multipath/Trace Route (ECMP/TR)	When ECMP/TR is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained on demand by polling the device. When performing a path trace on ECMP, Cisco Express Forwarding (CEF) lookup is performed on the device on demand for requested tuples. When a path trace detects a number of unknown or unmanaged devices in the path, the path trace is executed on demand from the last known or managed Cisco device and the path calculation is restarted from the first known or managed Cisco device in the trace route result. The unknown or unmanaged hops discovered using path trace are added to the path as unknown devices along with their IP addresses.
Equal Cost Multi Path (ECMP)	When an ECMP routing strategy is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made. **Note** The controller's GUI will display when ECMP is used between devices in a path trace segment.
Hot Standby Router Protocol (HSRP)	When HSRP is used in a network, the controller automatically looks up the HSRP active router for a given segment and calculates the path appropriately for a path trace. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Intermediate System-to-Intermediate System (IS-IS) Protocol	When IS-IS is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Layer 3 Forwarding Interface	The controller can perform path traces between two Layer 3 forwarding interfaces or between a Layer 3 forwarding interface and a host.

Supported Device Protocols and Network Connections	Description
Layer 3 Recursive Lookup	When Layer 3 Recursive Lookup is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. Up to three recursive lookups are supported. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
MPLS-VPN (WAN)	The controller provides path trace support for a branch-to-branch connected and provider-managed MPLS-VPN service. Supported devices for this type of path trace include: • Cisco ASR 1000 Series Aggregation Services Router • Cisco ASR 9000 Series Aggregation Services Router • Cisco Integrated Services Routers (ISR) G2 All customer edge (CE) routers should have NetFlow enabled with traffic running between the hosts and routers. **Note** The above supported devices will be tagged as **Border Routers** for their **Device Role** in the **Device Inventory**. You must keep the above supported devices tagged as **Border Routers** when performing a path trace. The data used for this path trace calculation is obtained through an on-demand query made through the network device at the time the path calculation request is made.
Netflow	When Netflow is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. When we have multiple border routers in the destination island, the Netflow cache from the devices are used to find the actual ingress border router. The Netflow record is matched from these devices on demand for a given tuple. It is essential to configure Netflow on the border routers. If Netflow is not configured, trace route is used to find the ingress interfaces, which might not be accurate.
Next Hop Resolution Protocol (NHRP)	Path Trace shows DMVPN dynamic tunnels between two spokes by identifying the LinkInformationSource as NHRP.

Supported Device Protocols and Network Connections	Description
Open Shortest Path First Protocol (OSPF)	When OSPF is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Physical connectivity (Ethernet, Serial and Packet over SONET (PoS))	The path trace for a given application flow can be displayed over Ethernet, Serial over SONET, and Packet over SONET. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Spanning Tree Protocol (STP)	The controller provides Layer 2 support for Spanning Tree Protocol (STP). The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Static Routing	When static routing is used in a network, the path trace for a given application flow can be displayed through the controller's GUI. The user is able to determine the exact path a particular application is taking. The data used for this path trace calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.
Sub interfaces	When sub interfaces are used within a network, the path trace for a given application flow is displayed. The path trace between the two sub interfaces is displayed, so that the user can visualize an end-to-end path for an application.
Virtual connectivity—Layer 2 Port Channel	When virtual connectivity (Layer 2 port channel) is used within a network, the path trace for a given application flow is displayed. The path trace over virtual interfaces (port channels) is displayed, so that the user can visualize an end-to-end path for an application.
Virtual connectivity—VLAN/SVI	When virtual connectivity (VLAN/SVI) is used within a network, the path trace for a given application flow is displayed. The path trace is displayed, so that the user can visualize an end-to-end path for an application. The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.

Supported Device Protocols and Network Connections	Description
Virtual Routing and Forwarding (VRF)	Path trace supports VRF Lite and VRF route leaking. For information, see Understanding VRF Path Trace Results.
Wireless	The controller provides path trace support for Control and Provisioning of Wireless Access Points (CAPWAP), 802.11, and mobility. When wireless network elements are used, the path trace for a given application flow is displayed. The user knows the exact path a particular application is taking. **Note** The controller's GUI will display CAPWAP and mobility tunneling (for roaming) when either is discovered during a path trace. The data used for this path calculation is obtained during the discovery process and stored in the controller's database where it is kept up to date.