



Cisco IWAN on Cisco APIC-EM Configuration Guide, Release 1.3.x

October 21, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

© 2015–2016 Cisco Systems, Inc. All rights reserved.



Preface vii

Audience vii

Organization vii

Conventions viii

Related Documentation x

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

New and Changed Information 1-1

New and Changed Information 1-1

CHAPTER 2

Cisco IWAN Application Overview 2-1

About the Cisco IWAN Application 2-1

Basic Workflow for Accessing the Cisco IWAN Application 2-2

Deploying Cisco APIC-EM 2-2

Accessing the Cisco IWAN Application 2-2

Cisco IWAN Application Home Page 2-3

CHAPTER 3

Configuring and Setting Up the Hub Site 3-1

Basic Workflow for Configuring and Setting Up the Hub Site 3-1

Wizard Step 1—Configuring System Settings 3-2

Wizard Step 2—Uploading Certified Cisco IOS Software Images 3-5

Wizard Step 3—Configuring IP Address Pools 3-6

Wizard Step 4—Configuring Service Providers 3-10

Wizard Step 5—Configuring the IWAN Aggregation Site 3-12

Modifying the Configuration for the Hub Sites 3-20

Understanding the Coexistence of IWAN Sites and Non-IWAN Sites 3-20

 Example of a Heterogeneous WAN Site 3-20

Understanding IP Address Pools 3-21

CHAPTER 4

Managing Branch Sites 4-1

Basic Workflow for Managing Branch Sites 4-1

Bootstrapping Greenfield Devices 4-2

| | |
|---|------|
| Adding and Provisioning Greenfield Devices to the Branch Site | 4-2 |
| Adding and Provisioning Brownfield Devices to the Branch Site | 4-7 |
| Viewing Site Status Information | 4-18 |

CHAPTER 5

| | |
|--|-----|
| Administering Application Policies | 5-1 |
| Understanding the Categorize Applications Tab | 5-1 |
| Viewing Applications | 5-2 |
| Moving Applications to a Different Category | 5-2 |
| Editing Application Information | 5-3 |
| Adding a New Application | 5-3 |
| Understanding the Define Application Policies Tab | 5-4 |
| Moving an Application Category to a Different Business Group | 5-5 |
| Modifying the Application Performance | 5-5 |
| Understanding the Application Bandwidth Tab | 5-7 |
| Viewing the Application Bandwidth | 5-7 |

CHAPTER 6

| | |
|---|-----|
| Monitoring and Troubleshooting Sites | 6-1 |
| Monitoring and Troubleshooting | 6-1 |

CHAPTER 7

| | |
|---|-----|
| Backup and Restore, Recovery, and Delete | 7-1 |
| Backup and Restore | 7-1 |
| Backup and Restore Recommendations | 7-1 |
| Backup and Restore Scenarios | 7-2 |
| Recovery | 7-4 |
| Recovering a Cisco IWAN Site | 7-4 |
| Post Provisioning Recovery for Hub and Branch Sites | 7-4 |
| Delete | 7-5 |
| Deleting a Hub Site | 7-5 |
| Deleting a Transit Hub | 7-5 |
| Deleting Branch Sites | 7-6 |
| Manually Cleaning Up Devices | 7-6 |
| Adding or Deleting Site Prefixes | 7-8 |

CHAPTER 8

| | |
|---|-----|
| Upgrading the Cisco IWAN Application | 8-1 |
| Upgrading the Cisco IWAN Application | 8-1 |

APPENDIX A

| | |
|---|-----|
| Brownfield Validation Messages | A-1 |
| Error Messages Encountered During Brownfield Validation | A-1 |

| | |
|---|-----|
| Warning Messages Encountered During Brownfield Validation | A-3 |
|---|-----|



Preface

This preface includes the following sections:

- [Audience, page vii](#)
- [Organization, page vii](#)
- [Conventions, page viii](#)
- [Related Documentation, page x](#)
- [Obtaining Documentation and Submitting a Service Request, page x](#)

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Organization

This document includes the following chapters:

| Chapter | Title | Description |
|---------|---|--|
| 1 | New and Changed Information | Summarizes release-specific new and changed features for the Cisco IWAN application that are covered in this document. |
| 2 | Cisco IWAN Application Overview | Introduces Cisco IWAN and provides the basic workflow for accessing the Cisco IWAN application. |
| 3 | Configuring and Setting Up the Hub Site | Provides the wizard steps that allow you to configure and setup the hub site. |
| 4 | Managing Branch Sites | Provides procedures for adding and provisioning branch sites and viewing site status information. |

| Chapter | Title | Description |
|---------|--|--|
| 5 | Administering Application Policies | Provides procedures for categorizing and defining application policies based on the application bandwidth. |
| 6 | Monitoring and Troubleshooting Sites | Provides procedures for monitoring and troubleshooting sites. |
| 7 | Backup and Restore, Recovery, and Delete | Provides information about how to backup and restore, recover Cisco IWAN configuration, and delete hub, transit hub, and branch sites. |
| 8 | Upgrading the Cisco IWAN Application | Provides procedure for upgrading the Cisco IWAN application after the Cisco APIC-EM upgrade. |
| A | Brownfield Validation Messages Description | Provides a list of error and warning messages encountered during Brownfield validation. |

Conventions

This document uses the following conventions:

| Convention | Indication |
|---------------------------|---|
| bold font | Commands and keywords and user-entered text appear in bold font . |
| <i>italic font</i> | Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> . |
| [] | Elements in square brackets are optional. |
| { x y z } | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x y z] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| <code>courier font</code> | Terminal sessions and information the system displays appear in <code>courier font</code> . |
| < > | 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. |



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*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.



Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



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



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.

SAVE THESE INSTRUCTIONS



Statements using this symbol are provided for additional information and to comply with regulatory and customer requirements.

Related Documentation

| Documentation | Description |
|--|--|
| Configuration Guide for Cisco IWAN on Cisco APIC-EM, Release 1.3.x | This document. Provides information about how to configure and use the Cisco IWAN application. |
| Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App) | Provides a list of all release notes for the Cisco APIC-EM product, including Cisco IWAN. |
| Cisco IWAN Technology Design Guides | Design guides that describe Cisco validated designs for Cisco IWAN. |
| Cisco APIC-EM Documentation Roadmap | Provides a list of all Cisco APIC-EM product documentation. This document is designed to help you get the most out of the controller and its applications. You can find links to all of the documentation, including Cisco IWAN at: http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html |
| Cisco Prime Infrastructure Release Notes | Provides a list of all release notes for the Cisco Prime Infrastructure product. |
| Cisco Prime Infrastructure 2.X Deployment Guide | Describes how to deploy the Cisco Prime Infrastructure, assuming that you have already deployed the basic wired and wireless network. |
| LiveAction | Provides LiveAction IWAN training and documentation. |

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



New and Changed Information

This chapter contains the following section:

- [New and Changed Information, page 1-1](#)

New and Changed Information

The following table summarizes release-specific new and changed features for the Cisco IWAN application that are covered in this document.

Table 1-1 *New and Changed Information for Release 1.3.x*

| Feature | Description | Reference |
|---|--|---|
| Harmonization of the Cisco IWAN application and the EasyQoS application | Added support to integrate the Cisco IWAN application and the EasyQoS application in the Cisco APIC-EM infrastructure. Provides a unified user experience for managing the life-cycle of applications and groups of applications. | Wizard Step 4—Configuring Service Providers, page 3-10 |
| Day 0 Support for Brownfield devices for branches | Ability to migrate existing customer branch sites to IWAN deployment. | Adding and Provisioning Brownfield Devices to the Branch Site, page 4-7 |
| Brownfield—Branch site prefix declaration enablement | To have a robust IWAN offering at the cost of user input, branch provisioning workflow has been modified to accept site prefix to accommodate subnets that are on a routed network behind the border router. The site prefixes are statically configured in PFR. | Adding and Provisioning Brownfield Devices to the Branch Site, page 4-7 |
| LAN IP address pool support for Brownfield devices | The LAN Brownfield IP address pool feature provides the ability to reserve a LAN Brownfield IP address pool before provisioning the Brownfield branch site. | Adding and Provisioning Brownfield Devices to the Branch Site, page 4-7 Wizard Step 3—Configuring IP Address Pools, page 3-6 |
| Day N service provider count update | Provides the ability to update the service provider count and the remote site count after initial provisioning. Error message is displayed if the required number of addresses cannot be reserved from the Generic IP address pool. | Wizard Step 4—Configuring Service Providers, page 3-10 |



Cisco IWAN Application Overview

This chapter contains the following sections:

- [About the Cisco IWAN Application, page 2-1](#)
- [Basic Workflow for Accessing the Cisco IWAN Application, page 2-2](#)
- [Deploying Cisco APIC-EM, page 2-2](#)
- [Accessing the Cisco IWAN Application, page 2-2](#)
- [Cisco IWAN Application Home Page, page 2-3](#)

About the Cisco IWAN Application

The Cisco Intelligent WAN (Cisco IWAN) application runs on the Cisco Application Policy Infrastructure Controller - Enterprise Module (Cisco APIC-EM).

Cisco IWAN extends Software Defined Networking (SDN) to the branch sites with an application-centric approach that is based on business policies and application rules. This allows IT, centralized management with distributed enforcement across the network.

Cisco IWAN automates deployments with an intuitive browser-based user interface. A new router can be provisioned faster without any knowledge of the Command Line Interface (CLI). Business priorities are translated into network policies based on Cisco best practices and validated designs. Cisco IWAN reduces the time required for configuring advanced network services such as DMVPN, PKI, AVC, QoS and PfR through the use of automation and simple, predefined workflows.

Cisco IWAN uses an application-centric approach to offer the following benefits:

- **Reduced operational costs**—Cisco IWAN helps IT deliver an unparalleled user experience over any connection while lowering operational costs.
- **Simplified IT operations**—Cisco IWAN uses a software-based controller model, automating and centralizing management tasks to ensure faster, more successful deployments.
- **Eliminates network complexity**—Cisco IWAN leverages Cisco APIC-EM to abstract network devices into one system, eliminating network complexity and providing centralized provisioning of the infrastructure to speed up application and service roll outs.

Basic Workflow for Accessing the Cisco IWAN Application

Table 2-1 Basic Workflow for Accessing Cisco IWAN

| No. | Action | Reference |
|-----|--|--|
| 1 | Deploy Cisco APIC-EM. | Deploying Cisco APIC-EM, page 2-2 |
| 2 | Log into Cisco APIC-EM to access the Cisco IWAN application. | Accessing the Cisco IWAN Application, page 2-2 |
| 3 | Use the Cisco IWAN application. | Chapters 3 - 8 |

Deploying Cisco APIC-EM

You access the Cisco IWAN application from the Cisco APIC-EM graphical user interface (GUI). To use Cisco IWAN, you must first deploy Cisco APIC-EM.

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

For detail instructions about how to deploy Cisco APIC-EM, see the following chapters in the [Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide](#):

- Deploying Cisco APIC-EM
- Preparing Virtual Machines for Cisco APIC-EM

Accessing the Cisco IWAN Application

You access the Cisco IWAN application from the Cisco APIC-EM GUI.

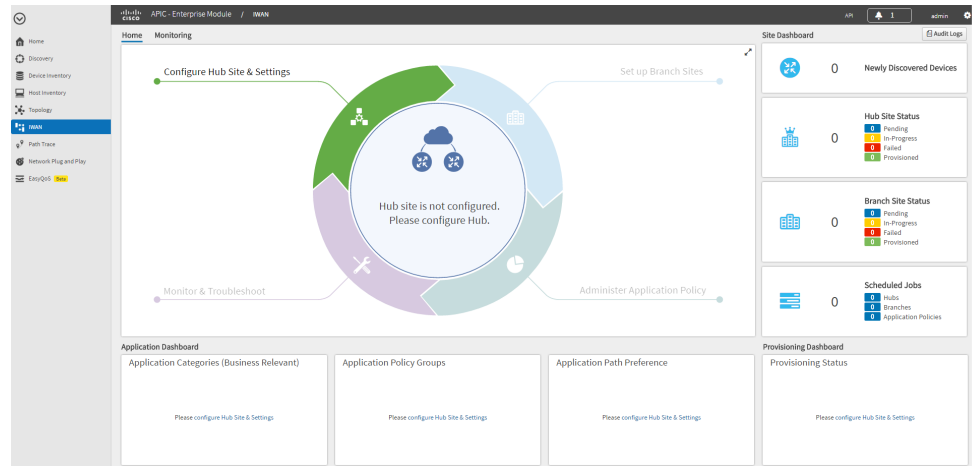
Procedure

-
- | | |
|---------------|---|
| Step 1 | From Google Chrome or Mozilla Firefox, enter the IP address or the fully qualified domain name (FQDN) of the Cisco APIC-EM. |
| Step 2 | Enter your username and password, and then click Log In . |
| Step 3 | Review and confirm the Telemetry Disclosure, which appears only when you log in for the first time, and then click Confirm . The Cisco APIC-EM GUI appears. |
| Step 4 | From the Cisco APIC-EM GUI left navigation pane, click IWAN . The Cisco IWAN application home page opens. See Cisco IWAN Application Home Page, page 2-3 . |
-

Cisco IWAN Application Home Page

If you are a first time user, the Cisco IWAN home page provides an enhanced user experience by allowing you to configure IWAN in a workflow-based model. The wizard steps embedded in the Cisco IWAN application, guide you through the setup and configuration process.

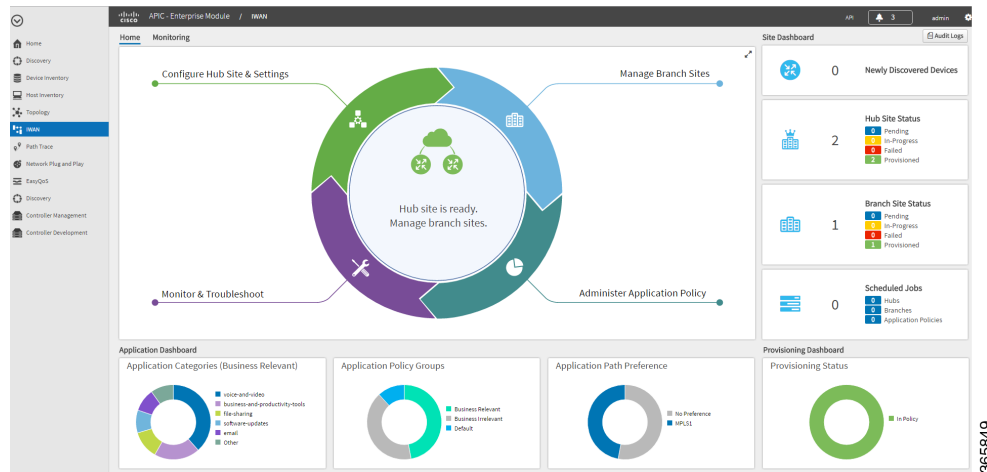
Figure 2-1 Cisco IWAN Application Home Page—New System Initial Login



365861

After you have configured and provisioned Cisco IWAN, the home page provides more information. For example, it displays hub and branch provisioning status, device status, and application status as shown in the following figure.

Figure 2-2 Cisco IWAN Application Home Page—After Provisioning



| Task Area | Description | Reference |
|-------------------------------------|---|---|
| Configure Hub Site and Settings tab | Provides the wizard steps that allow you to configure and setup the hub site. | Configuring and Setting Up the Hub Site, page 3-1 |
| Manage Branch Sites tab | Allows you to add and provision branch sites and view site status information. | Managing Branch Sites, page 4-1 |
| Administer Application Policy tab | Allows you to categorize and define application policies based on the application bandwidth. | Administering Application Policies, page 5-1 |
| Monitor and Troubleshoot tab | Allows you to monitor and troubleshoot sites. | Monitoring and Troubleshooting Sites, page 6-1 |
| Application Dashboard | Provides at-a-glance information about: <ul style="list-style-type: none"> Application Categories Application Policy Groups Application Path Preference | — |
| Provisioning Dashboard | Provides site provisioning status. | — |
| Site Dashboard | Provides at-a-glance information about: <ul style="list-style-type: none"> Newly Discovered Devices Hub Site Status Branch Site Status Scheduled Jobs | — |



Configuring and Setting Up the Hub Site

This chapter contains the following sections:

- [Basic Workflow for Configuring and Setting Up the Hub Site, page 3-1](#)
- [Wizard Step 1—Configuring System Settings, page 3-2](#)
- [Wizard Step 2—Uploading Certified Cisco IOS Software Images, page 3-5](#)
- [Wizard Step 3—Configuring IP Address Pools, page 3-6](#)
- [Wizard Step 4—Configuring Service Providers, page 3-10](#)
- [Wizard Step 5—Configuring the IWAN Aggregation Site, page 3-12](#)
- [Modifying the Configuration for the Hub Sites, page 3-20](#)
- [Understanding the Coexistence of IWAN Sites and Non-IWAN Sites, page 3-20](#)
- [Understanding IP Address Pools, page 3-21](#)

Basic Workflow for Configuring and Setting Up the Hub Site

Use the wizard provided with the Cisco IWAN application to configure and set up the hub site.

Table 3-1 *Basic Workflow for Configuring and Setting Up the Hub Site*

| No. | Task | Reference |
|-----|--|---|
| 1 | Configure system settings. | Wizard Step 1—Configuring System Settings, page 3-2 |
| 2 | Upload certified Cisco IOS software images. Note This wizard step is displayed for Greenfield branch devices only. | Wizard Step 2—Uploading Certified Cisco IOS Software Images, page 3-5 |
| 3 | Configure IP address pools. | Wizard Step 3—Configuring IP Address Pools, page 3-6 |
| 4 | Configure service providers. | Wizard Step 4—Configuring Service Providers, page 3-10 |
| 5 | Configure the IWAN aggregation site. | Wizard Step 5—Configuring the IWAN Aggregation Site, page 3-12 |

Wizard Step 1—Configuring System Settings

Use this procedure to configure system settings such as Netflow Collector, DNS, AAA, Syslog, SNMP, and DHCP.

All of the system settings might not be displayed. Click the **Show More** or **Show Less** button as needed to display or hide the settings.

Procedure

- Step 1** If you are logging in for first time, you are directed to specify the global settings in the CLI Credentials dialog box. Enter your user name and password, and then click **Add**.
- Step 2** From the left navigation pane, click **IWAN**. The Cisco IWAN home page opens.
- Step 3** From the Cisco IWAN home page, click **Configure Hub Site & Settings**. The Settings tab opens by default and the System Settings page displays as shown in the following figure:

Figure 3-1 Systems Settings Tab

- Step 4** In the **Netflow Collector** area, enter the following properties:

| Field | Description |
|------------------------|--|
| NetFlow Destination IP | IP address of the NetFlow collector (server). Traffic stats are sent from the network devices to the NetFlow collector. |
| Port Number | Port number of the NetFlow collector (server). |

Step 5 In the **DNS** area, enter the following properties:

| Field | Description |
|------------------|--|
| Domain name | DNS domain name. |
| Primary Server | (Optional) IP address of the primary DNS server. |
| Secondary Server | (Optional) IP address of the secondary DNS server. |

Step 6 In the **Authorization, Authentication, Accounting** area, enter the following properties:

| Field | Description |
|------------|--|
| IP Address | (Optional) IP address of the Authentication, Authorization, and Accounting (AAA) server. TACACS is the only supported centralized AAA service for Cisco IWAN. When a TACACS server is provided, the devices use TACACS for management access to the spoke devices (SSH & HTTPS). Whether or not TACACS is provided, a local AAA user database is created on the spoke device, which is used when the TACACS server is not available. One of the following default values are used for the local AAA user credentials: <ul style="list-style-type: none"> • Cisco APIC-EM global credentials. • Username and password specified in the global device credentials for branch routers. • Username and password entered while provisioning the hub. |
| Key | (Optional) Key for accessing the AAA server. |

Step 7 In the **Syslog** area, enter the following:

| Field | Description |
|-----------|--|
| Server IP | (Optional) Destination IP address of the syslog server. Syslog messages from all routers are sent to this server. |

Step 8 In the **SNMP** area, choose the version number in the Version field. Depending on the SNMP version number you choose, V2C or V3, different properties display.

- For SNMP version V2C, enter the following properties:

| Field | Description |
|-----------------|---|
| Version | SNMP software version. Value: V2C. |
| Read Community | SNMP V2C read community string. |
| Write Community | (Optional) SNMP V2C write community string. |
| Retries | Number of retries. Default is 3. |

| Field | Description |
|---------------------|--|
| Timeout (secs) | Displayed for SNMP V2C only. Timeout period. Default is 10. |
| Trap Destination IP | (Optional) IP address of the SNMP server. Note If you do not enter an IP address, the Cisco IWAN application is used as an SNMP server. The APIC-EM controller can serve as the SNMP manager for managed network devices or a separate SNMP server can be specified to handle SNMP traps. SNMP settings determine the inventory from hub and remote site devices and these values are reflected in the configuration. |

- For SNMP version V3, enter the following properties:

| Field | Description |
|---------------------|---|
| Version | SNMP software version. Value: V3. |
| Mode | Choose the mode from the drop-down list. Options are: <ul style="list-style-type: none"> Authentication and Encryption No Authentication and No Encryption Authentication and No Encryption |
| Auth. Type | Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. Choose the authentication type from the drop-down list. Options are: <ul style="list-style-type: none"> HMAC-SHA HMAC-MDS |
| Username | The authentication username. |
| Auth. Password | Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. The password for the authentication username. |
| Encryption Type | Displayed if you chose Authentication and Encryption in the Mode field. The encryption username. |
| Encryption Password | Displayed if you chose Authentication and Encryption in the Mode field. The password for the encryption username. |
| Retries | Number of retries. Default is 3. |

| Field | Description |
|---------------------|--|
| Timeout (secs) | Displayed for SNMP V2C only. Timeout period. Default is 10. |
| Trap Destination IP | (Optional) IP address of the SNMP server. Note If you do not enter an IP address, the Cisco IWAN application is used as an SNMP server. The APIC-EM controller can serve as the SNMP manager for managed network devices or a separate SNMP server can be specified to handle SNMP traps. SNMP settings determine the inventory from hub and remote site devices and these values are reflected in the configuration. |

Step 9 In the **DHCP** area, enter the following properties:

| Field | Description |
|------------------|---|
| External DHCP IP | (Optional) Destination IP address of the DHCP server. The DHCP server that provides client computers and other TCP/IP-based network devices with valid IP addresses. |

Step 10 Click **Save and Continue**. The Certified IOS Releases tab opens. See [Wizard Step 2—Uploading Certified Cisco IOS Software Images, page 3-5](#).

Wizard Step 2—Uploading Certified Cisco IOS Software Images



Note

This wizard step is displayed for Greenfield branch devices only.

You can upload certified Cisco IOS images from your computer into the Cisco IWAN application. When a Greenfield device comes up, the Plug-n-Play agent interacts with the Plug-n-Play server in Cisco APIC-EM, downloads the appropriate Cisco IOS software image to the device, and reloads the device with that image.



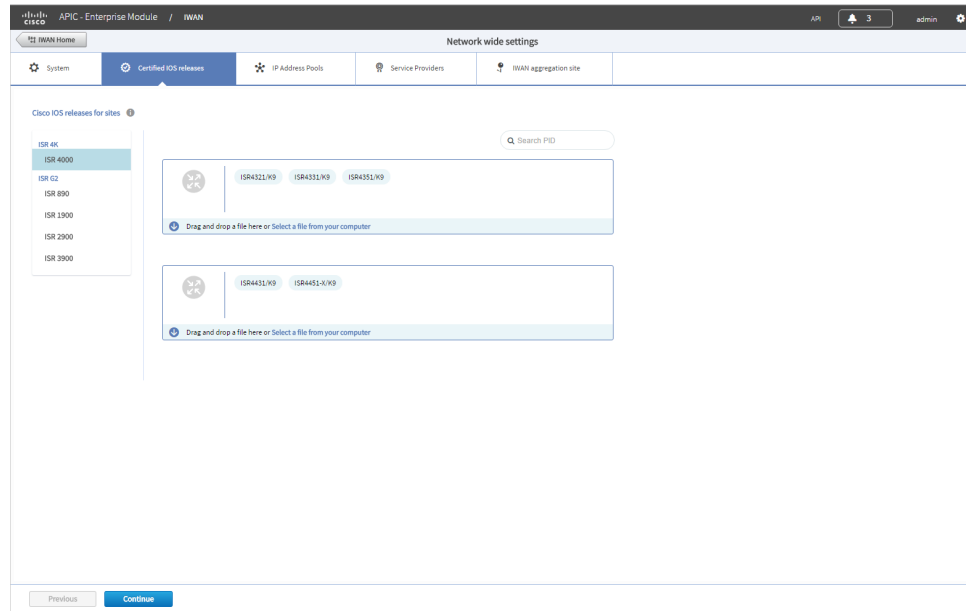
Note

If the appropriate software image is already installed on your router, you can skip this step.

Procedure

- Step 1** Click the **Certified IOS Releases** tab. The Cisco IOS Releases for Sites page opens as shown in the following figure:

Figure 3-2 *Certified IOS Releases Tab*



365855

- Step 2** From the left pane, choose the router type for which you want to upload the Cisco IOS image.
- Step 3** Do one of the following:
- Drag and drop the Cisco IOS software image file from your computer into the GUI.
 - Browse to the location where you have saved the Cisco IOS software image file and upload it into the system.
- Step 4** Click **Continue**. The IP Address Pools page opens. See [Wizard Step 3—Configuring IP Address Pools, page 3-6](#).

Wizard Step 3—Configuring IP Address Pools



Note

The generic IP address pool is used for overlay and loopback addresses. The generic IP address pool is divided according to the number of remote sites and service providers as you specify in the IP Address Pools tab. Plan by understanding your future requirements and specify the maximum number of service providers and remote sites that you might choose to deploy. Once the IP address pool settings are specified, they cannot be changed.

Use the IP Address Pools tab to define IP address pools. For information about IP Address Pools, see [Understanding IP Address Pools, page 3-21](#).

Procedure

- Step 1** Choose the **IP Address Pools** tab. The Address Pools page opens as shown in the following figure:

Figure 3-3 IP Address Pools Tab

The screenshot shows the Cisco IAN IP Address Pools configuration page. The top navigation bar includes 'System', 'Certified IOS releases', 'IP Address Pools' (selected), 'Service Providers', and 'WAN aggregation site'. The main content area has a 'Remote Site Count' field set to 10 and a 'Service Provider Count' field set to 4. A 'Check IP Range' button is visible. Below these fields are buttons for 'Add Address Pool', 'Upload Address Pool', 'Download Address Pool', and 'Download Allocated Addresses'. The 'Site Specific Address Pool Details' section contains a table with the following data:

| Serial Number | Site Name | IP Address Pool | Prefix | VLAN ID | VLAN Type | Action |
|---------------|-----------|-----------------|--------|---------|-----------|--------|
| F0C17475V2C | Dubai | | | | | X + |

At the bottom of the page are 'Previous' and 'Save & Continue' buttons.

- Step 2** In the **Remote Site Count** field, enter the maximum number of remote sites to deploy.
- If you are an existing customer with Cisco IWAN release 1.2.x, you have the ability to increase the remote site count by upgrading to Cisco IWAN release 1.3. Based on the availability of internal IP addresses in pre-reserved subnets (which are created during initial provisioning) you can specify a higher number of remote site count.
- Step 3** In the **Service Provider Count** field, enter the maximum number of service providers that you might require.
- If you are an existing customer with Cisco IWAN release 1.2.x, you have the ability to increase the service provider count by upgrading to Cisco IWAN release 1.3. You can specify a maximum of four service providers.
- Step 4** Click the **Check IP Range** button. The Proposed IP Range page opens.
- Based on the number of remote site and service provider count that you entered, the Proposed IP Range page provides information about the minimum suggested prefix length that you can use for the generic IP address pool, the prefix length for LAN interface pools, the number of IP addresses per VLAN, and the number of VLANs. Click **OK** or **Get IP Range**.

Step 5 Do one of the following:

- To manually enter an IP address, click + **Add Address Pool**. Enter the following properties:

| Field | Description |
|------------|---|
| Role | Can be one of the following: <ul style="list-style-type: none"> Generic—The first range always defaults to the generic IP address pool. LAN Greenfield—Choose this option to define the LAN IP address pool for new Greenfield branch devices. You can have any number of LAN Greenfield IP address pools. LAN Brownfield—Choose this option to define the LAN IP address pool for Brownfield branch devices (devices with existing configuration). You can have any number of LAN Brownfield IP address pools. |
| IP Address | IP Address for the IP address pool. |
| Prefix | CIDR prefix. |
| Allocated | Displays the percentage of addresses in the pool that are used. |

- To upload a large number of IP addresses, click **Upload Address Pool**, and then upload a .csv file from your computer.

For details about the type of information that you must include in the .csv file, click the **Download Address Pool** tab. A Controller_Profile_DD-MM-YYYY.csv file is downloaded to your system, which provides the template details.

Step 6 Click + **Add Site Address Pool** to enter information for the site-specific LAN IP address pool. The Add Site Address Pool dialog box opens. Enter the properties as shown in the table below, and then click **OK**.

By default, Greenfield branch sites use IP addresses from the LAN Greenfield IP address pool (if there is one) or from the generic IP address pool (if there is no LAN Greenfield IP address pool). If you want to provision a new Greenfield branch site using specific IP address pools for its VLANs (for example, if you do not want the VLANs to use IP addresses from LAN Greenfield IP address pools and generic IP address pools), you can define the VLANs and respective IP address pools before you provision the site.



Note After a site is provisioned, you cannot move back-and-forth between site-specific IP address pool with VLANs and site-specific IP address pool without VLANs. Therefore, make sure that you have a clear vision before you start provisioning the site.

| Field | Description |
|-----------------|--|
| Serial Number | Serial number(s) of the site device(s). If a site has more than one device, include all serial numbers separated by a semi-colon. |
| Site Name | Name of the site. |
| IP Address Pool | IP address pool to be used for hosts in this VLAN. |
| Prefix | CIDR prefix. |

| | |
|-----------|---|
| VLAN ID | <p>Range of values: 1–4094.</p> <p>Note The VLAN ID 99 is reserved for the transit VLAN, therefore you cannot use this ID for other VLANs.</p> |
| VLAN Type | <p>Enter a VLAN type or select it from the drop-down list.</p> <p>Values: Data, Guest, Voice and Video, Wireless.</p> <p>Note The following restrictions apply when you enter a VLAN type of your choice:</p> <ul style="list-style-type: none">– The VLAN type value should not be more than 200 characters in length.– The VLAN type should not include the ? character.– For site-specific address pools, you can enter a maximum of 20 entries per site. |

Step 7 Repeat step 6 as required to add additional site address pools.

Step 8 Click **Save and Continue**. The Service Providers tab opens. See [Wizard Step 4—Configuring Service Providers, page 3-10](#).

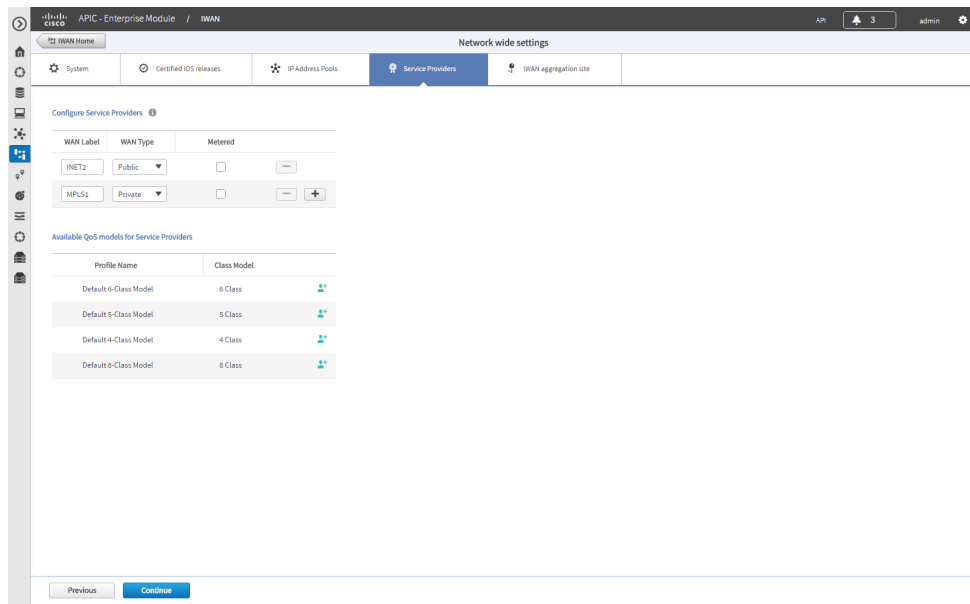
Wizard Step 4—Configuring Service Providers

Use the Service Providers tab to define the type of links and the number of service providers.

Procedure

- Step 1
- Choose the **Service Providers** tab. The Configure Service Providers Page opens as shown in the following figure:

Figure 3-4 Service Providers Tab



365858

- Step 2
- From the **Configure Service Providers** area, click the + icon to define the following properties:

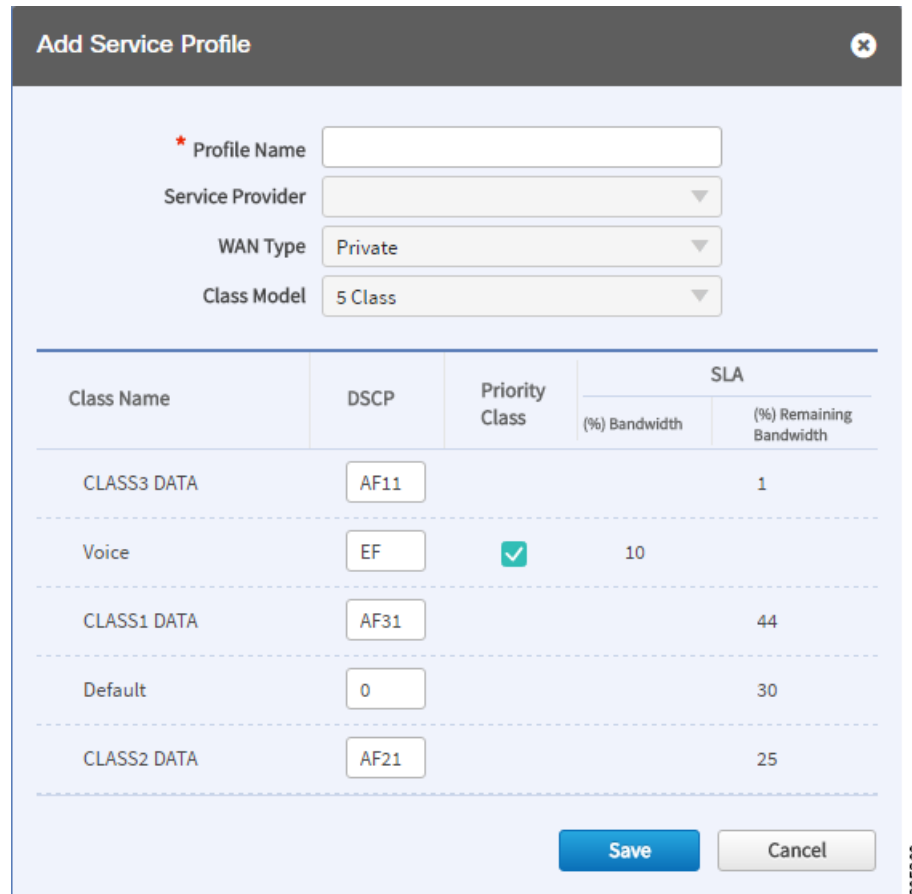


Note You can specify a maximum of four service providers.

| Field | Description |
|-----------|--|
| WAN Label | WAN transport type. Can be a maximum of seven characters. |
| WAN Type | Can be one of the following: <ul style="list-style-type: none">PrivatePublic |
| Metered | Choose this option if the WAN is metered. <div>Note You can choose the Metered option only when the number of service providers is greater than two. You cannot choose one of the link as a metered link if there are only two service providers.</div> <div>Note Only one link can be metered and is permitted on a public cloud.</div> |

- Step 3** (Optional) If you require a custom class model than the default ones that are provided, click the **Available QoS Models for Service Providers** area, and then click the + icon next to the profile that most closely matches the service provider Service Level Agreement (SLA). The Add Service Profile dialog box opens as shown in the following figure:

Figure 3-5 *Add Service Profile Dialog Box*



The dialog box titled "Add Service Profile" contains the following fields and table:

- Profile Name:** A text input field with a red asterisk indicating it is required.
- Service Provider:** A drop-down menu.
- WAN Type:** A drop-down menu with "Private" selected.
- Class Model:** A drop-down menu with "5 Class" selected.

| Class Name | DSCP | Priority Class | SLA | |
|-------------|------|-------------------------------------|---------------|-------------------------|
| | | | (%) Bandwidth | (%) Remaining Bandwidth |
| CLASS3 DATA | AF11 | | | 1 |
| Voice | EF | <input checked="" type="checkbox"/> | 10 | |
| CLASS1 DATA | AF31 | | | 44 |
| Default | 0 | | | 30 |
| CLASS2 DATA | AF21 | | | 25 |

At the bottom right are "Save" and "Cancel" buttons. A small vertical text "365860" is visible on the right edge of the dialog box.

- Step 4** Enter the following profile information, and then click **Save**.



Note For the Private WAN interface, a set of predefined service provider profiles are available. Egress QoS queuing is applied on the WAN Egress to fulfill the service provider SLA.

| Field | Description |
|------------------|---|
| Profile Name | Name of the new service profile. |
| Service Provider | Choose the service provider from the drop-down list. |
| WAN Type | Choose the WAN Type from the drop-down list. Can be one of the following: <ul style="list-style-type: none"> Private Public |

| Field | Description |
|----------------|---|
| Class Model | Choose the service provider class model from the drop-down list. Options are: <ul style="list-style-type: none"> • 4 Class • 5 Class • 6 Class • 8 Class |
| Class Name | Displays the data class name. |
| DSCP | Displays the Differentiated Services Code Point (DSCP) values for each class. Once saved, it appears as a new profile. You cannot edit this value after it is saved. |
| Priority Class | Indicates the class that uses the most bandwidth. |
| SLA | Displays the percentages of used and available bandwidth (based on service level agreement offered by the service provider). |

**Note**

After you add the profile information, the profile details appear in the Available QoS Models for Service Providers area.

- Step 5** Click **Continue**. The IWAN Aggregation Site tab opens. See [Wizard Step 5—Configuring the IWAN Aggregation Site, page 3-12](#).

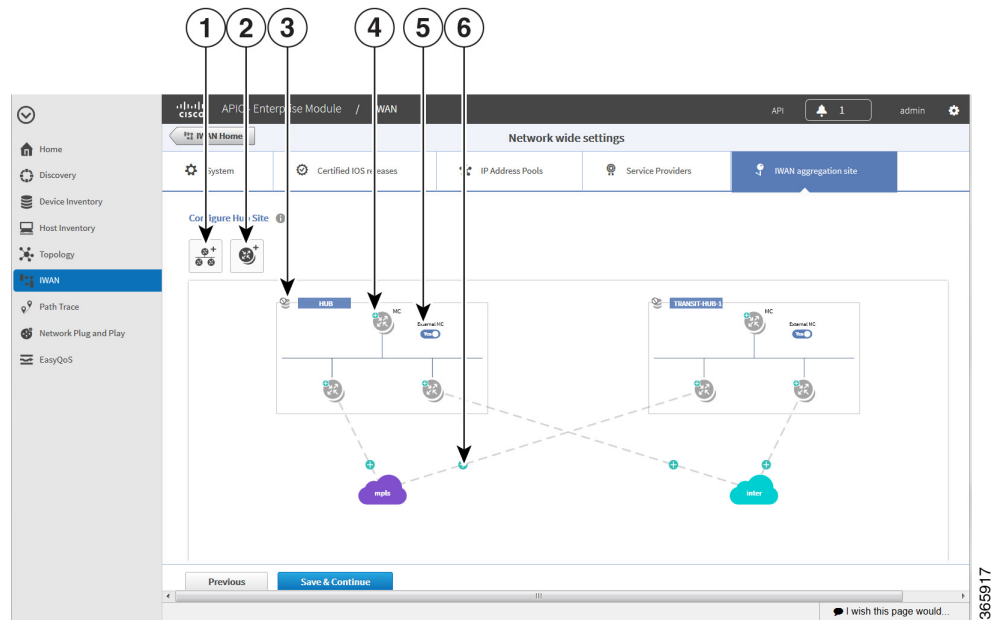
Wizard Step 5—Configuring the IWAN Aggregation Site

Use this procedure to do the following:

1. Discover hub devices.
2. Configure LANs.
3. Configure WANs.
4. Configure the external master controller.

Refer to the following figure to understand the procedure that follows:

Figure 3-6 *IWAN Aggregation Site Tab*



| | | | |
|---|------------------------|---|-------------------------------------|
| 1 | Add POP Icon | 4 | Configure External MC Router + Icon |
| 2 | Add Border Router Icon | 5 | External MC Toggle Button |
| 3 | Configure LAN Icon | 6 | Configure WAN Link + Icon |

Procedure

Step 1 Discover hub devices. Do the following:

- a. Select the **IWAN Aggregation Site** tab. The Configure Hub Site page opens and displays all of the service providers that you defined in wizard step 4 and the respective hub border routers.
- b. Do one of the following:
 - (Recommended) Click the **External MC** button (see # 5 in Figure 3-6) to toggle to **Yes**. A new router is added as a standalone master controller (MC).
 - Click the **External MC** button to toggle to **No**. One of the border routers is designated as an MC.
- c. To add an additional hub, click the **Add POP** icon ((see # 1 in Figure 3-6). A transit hub is added next to the primary hub (see TRANSIT-HUB-1 in the above figure).



Note

You can specify a maximum of two hub sites during provisioning. You can add or delete routers after hub provisioning.

- d. (Optional) To rename the new TRANSIT-HUB-1 to another name, click the name of the hub, and then add a different name.



Note You can only change the name of the hub during initial configuration, before routers are added to it.

- e. To add a border router to a hub, hover over the **Add Border Router** icon (see # 2 in [Figure 3-6](#)) the **Add to POP** options appear. Choose one of the two available hubs. A new border router is added in the appropriate hub.



Note You can have a maximum of four border routers in a hub site.

- f. To configure the newly added border router, click on the + icon on top of the router, the Configure Router dialog box opens.
- g. From the Configure Router dialog box, do the following:
- In the **Router Management IP** field, enter the management IP address of the hub router.
 - Click **Validate**. The Configure Router dialog box opens again with additional fields as shown in the following figure:

| Field | Description |
|---|---|
| Router Management IP | Hub router management IP address. |
| Master Controller | Check this option to choose this device as the Master Controller. |
| SNMP | |
| Version | SNMP version number. Depending on the version number you choose, different properties display. |
| Read Community (Displayed if you chose SNMP V2C.) | SNMP V2C read community string. |
| Write Community (Displayed if you chose SNMP V2C.) | (Optional) SNMP V2C write community string. |

| Field | Description |
|--|---|
| Mode (Displayed if you chose SNMP V3.) | Choose the mode from the drop-down list. Options are: <ul style="list-style-type: none"> • Authentication and Encryption • No Authentication and No Encryption • Authentication and No Encryption |
| Auth. Type (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. Choose the authentication type from the drop-down list. Options are: <ul style="list-style-type: none"> • HMAC-SHA • HMAC-MDS |
| Username (Displayed if you chose SNMP V3.) | Displayed if you chose SNMP V3. The authentication username. |
| Auth. Password (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. The password for the authentication username. |
| Encryption Type (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption in the Mode field. The encryption username. |
| Encryption Password (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption in the Mode field. The password for the encryption username. |
| SNMP Retries and Timeout | |
| Retries | Number of SNMP retries. Default: 3 |
| Timeout (secs) | Number of seconds to wait before the system considers an SNMP request to have timed out. Default: 10 |
| SSH/Telnet | |
| Protocol | Protocol used to communicate to the host (SSH or Telnet). |
| Username | SSH or Telnet username. |
| Password | SSH or Telnet password. |
| Enable Password | Enable password for the username. |
| Timeout (secs) | Number of seconds to wait before the system considers an SSH or Telnet request to have timed out. |

– Enter the properties as shown in the table above.



Note These credentials can be entered only once. The values are automatically populated to the remaining hub devices in the system.

- Click **Add Device**.

The device is verified in the background to determine if the device is suitable for provisioning. The following occurs:

The Cisco IWAN application accesses the router and checks its configuration to determine if it has any configuration that might conflict with the Cisco IWAN application. This is called Brownfield Validation.

If the router does not have conflicting configurations, an orange icon appears on top of the device and the Configure Router Dialog opens.

If the router has conflicting configurations, the Validation Status dialog opens listing all the validation failures, as shown in the following figure:

| Description | Status |
|---|----------|
| ▶ IWAN related crypto configuration found on the device | Must Fix |
| ▶ Device clock is not synchronized. | Must Fix |
| ▶ VRF configuration must not be present on the device | Must Fix |

Note : Mandatory validation changes should be fixed to proceed further.

Revalidate Cancel

- h. The validation status could be either Warning or Must Fix. Do the following:
 - If the validation status is Warning, you can fix it or ignore it.
 - If the validation status is Must Fix, remove the configurations suggested by the description, and then click **Revalidate**.

For information about the messages displayed in the Validation Status dialog box, see [Appendix A, “Brownfield Validation Messages.”](#)

After the router is successfully validated (it does not have any Must Fix errors), the Configure Router dialog box opens.

- i. From the Configure Router dialog box, click the appropriate **LAN IP-Interface** check box(es), and then click **Save**.



Note You can choose more than one LAN IP-Interface.

- j. To connect the border router to the cloud, click on the router and drag it to the cloud.
- k. Configure the other border routers using the above steps.

Step 2 Configure LANs. Do the following:

- a. Click the icon on the top-left corner of the primary hub (see # 3 in [Figure 3-6](#)). The Configure LAN dialog box opens with the fields shown in the table below:

The Routing Protocol, AS Number, and Datacenter Prefix are collected from the devices and auto populated for ease of configuration. The common (matching) AS numbers between the devices are displayed for each routing protocol. You can change the AS numbers on the device, but we do not recommend it.

| Field | Description |
|-------------------|---|
| Routing Protocol | Default routing protocol running on the hub routers. Example: EIGRP, OSPF, BGP |
| AS Number | AS number or area number, depending on the routing protocol. Note If the LAN routing protocol is BGP, and there are no matching AS numbers from the other hub device, this field is grayed out. You must manually modify the LAN side routing in the device. Note BGP with different AS numbers is not supported. |
| Datacenter Prefix | IP addresses of the hub site, specified as a prefix. |

- b. Click **Save**.

Step 3 Configure WANs. Do the following:

- a. Click the + icon on the link that connects the router and the cloud (see # 6 in [Figure 3-6](#)). The Configure Link dialog box opens.

The dialog boxes that appear are dependent on the WAN type that you specified while configuring the Service Provider. For example, Private or Public.

- b. For **Private** WAN, the Configure Link dialog box opens. Enter the following information for each link in the network:

Table 3-2 *Configure Link Dialog Box—Private WAN*

| Field | Description |
|-----------------------|--|
| WAN IP-Address | IP address of the WAN interface. |
| Default Gateway | IP address of the default gateway. |
| Enable Non IWAN Sites | Check this option to enable communication between non-IWAN sites and the newly enabled IWAN POP (Hub) and spoke sites for staged migration of the network. See Understanding the Coexistence of IWAN Sites and Non-IWAN Sites , page 3-20. |

Table 3-2 Configure Link Dialog Box—Private WAN

| Field | Description |
|-----------------------|---|
| Loopback IP-Interface | Choose a pre-provisioned loopback IP address from the drop-down list. This enables Cisco IWAN application to form a route between the existing sites and the new IWAN sites. Note The loopback interface must be configured on a private (MPLS) router. The loopback interface is required to support coexistence between the IWAN and non-IWAN sites and must be configured before adding the device to Cisco APIC-EM. It is recommended that you specify a loopback IP address in the same subnet as the WAN interface. |
| Bandwidth (Mbps) | Symmetrical bandwidth for upload and download. |
| Service Profile | Profile name configured in the Service Providers tab. |

- c. For **Public** WAN, the Configure Link dialog box opens. Enter the following information for each link in the network:

Table 3-3 Configure Link Dialog Box—Public WAN

| Field | Description |
|------------------|---|
| WAN IP-Address | IP address of the WAN interface. |
| Default Gateway | IP address of the default gateway. |
| NAT Enabled | Check this option if NAT IP address is used. |
| NAT IP Address | NAT'd IP address. |
| Bandwidth (Mbps) | Symmetrical bandwidth for upload and download. |
| Service Profile | Profile name configured in the Service Providers tab. |

- d. Click **Save**.

Step 4 Configure the external master controller.

During initial hub and router setup, if you clicked the **External MC** button to toggle to **Yes**, a new router was added as a standalone MC. Do the following:

- a. Click the + icon on top of the External MC router (see # 4 in [Figure 3-6](#)). The Configure Router dialog box opens.

For a dedicated master controller, the device must be Greenfield validated. No conflicting configuration with IWAN or dynamic routing protocols are supported for LAN and WAN.
- b. In the **Router Management IP** field, enter the management IP address of the hub router.
- c. Click **Validate**. The Configure Router dialog box opens.
- d. Enter the Router Management IP address, SNMP, SSH or Telnet protocol information, and then click **Save**.

Modifying the Configuration for the Hub Sites

After you have completed all of the wizard steps in the Hub Site and Settings area, you can go back and modify the properties at a later time. Fields that are grayed out, cannot be modified.

Understanding the Coexistence of IWAN Sites and Non-IWAN Sites

The coexistence of IWAN and non-IWAN sites feature allows communication between the newly enabled IWAN POP (Hub) and spoke sites and the non-IWAN sites for staged migration of the network. The benefit of this feature is:

- You can deploy Cisco IWAN on a few sites prior to full scale deployment.
- Non-IWAN sites can continue to communicate with the hub and spoke routers that are IWAN enabled and vice-versa

Prerequisites for Enabling Support of Non-IWAN Sites Along With IWAN Solution

The following configurations must be completed before starting the Cisco IWAN application on APIC-EM workflows:

- Define the Cisco IWAN hub private (MPLS) border router.
- On the hub router:
 - A loopback interface must be enabled on the border router. It is recommended that you specify a loopback IP address in the same subnet as the WAN interface.
 - A static route must be added with the existing MPLS-CE as the default gateway (before provisioning the hub with Cisco IWAN application workflows).
- On the existing MPLS-CE router:
 - The loopback IP address on the IWAN MPLS border router must be advertised through BGP (or another routing protocol used for peering with MPLS provider) on the MPLS-CE router. The loopback IP must be reachable from all remote sites.

Effective with Cisco IWAN Release 1.1.0, you can have two hubs, two clouds and add more devices to the cloud, thereby enabling a multilink network. In other words, a multilink network can have two datacenters and each datacenter can have four devices with four links.

Example of a Heterogeneous WAN Site

Effective with Cisco IWAN Release 2.0, you can perform the following for a provisioned site:

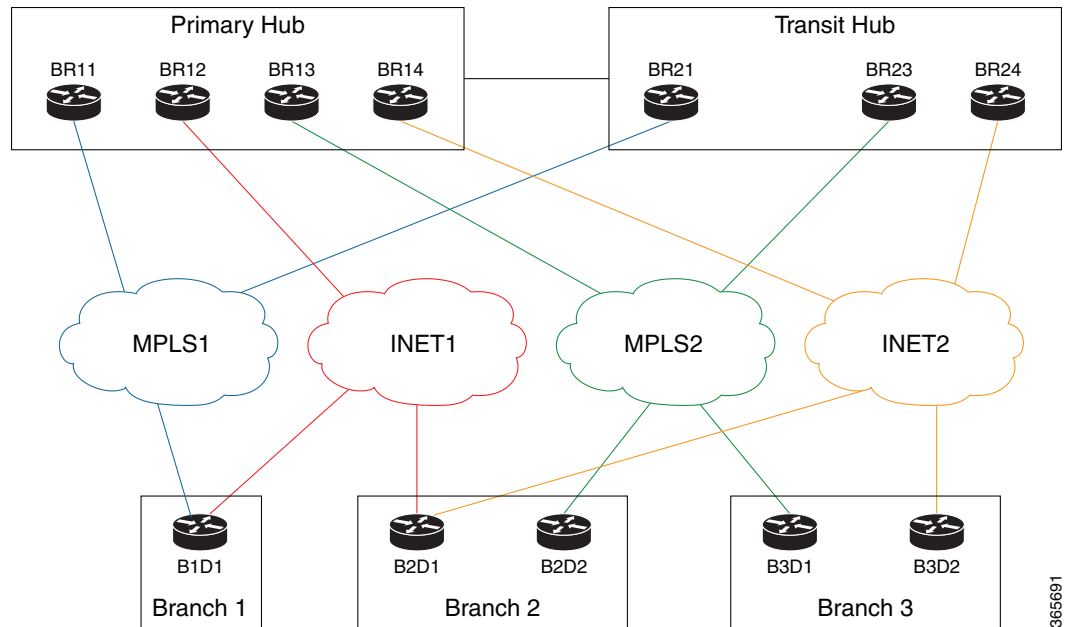
- Add WAN clouds and service providers.
- Add a maximum of two links of any type (Private or Public). The new links do not affect the existing device priority nor do they change the path preference.
- Connect different hub sites to different service providers (the maximum number of service providers is four).

**Note**

You cannot perform the above changes during site provisioning.

See the following figure for an example of heterogeneous topology where the primary hub is connected to four service providers and the transit hub is connected to three service providers. This example shows that both hub sites do not need to have exactly the same number of service providers.

Figure 3-7 *Transit Hub Connected to MPLS Link*



365691

Understanding IP Address Pools

The Cisco IWAN application automatically uses the IP addresses carved from the global enterprise IP address pool space. To support this functionality, one generic global IP address pool must be defined for the Cisco IWAN application. IP addresses are allocated from the generic IP address pool to provision the hub and spoke devices, which include interface, LAN, VPN overlay, and routing IP addresses.

Optionally, one or more LAN Greenfield IP address pools can be defined to further refine the branch LAN side IP address space. If all LAN Greenfield IP address pools are exhausted, the generic IP address pool is used.

It is important to define the size of the generic IP address pool to cater to the long term needs of the IWAN site. VPN requirements dictate that subnets must be defined and allocated internally before any sites are provisioned. At Cisco IWAN release 1.3, you can increase the site and service provider counts after initial provisioning, but you cannot change the generic IP address pool once specified. Therefore, we recommend that you define the generic IP address pool keeping in mind the future scale of service provider and site sizes. The generic IP address pool is used for overlay and loopback addresses. The generic IP address pool is divided according to the number of remote sites and service providers as specified in the IP Address Pools tab.

Optionally, wherever specific IP addresses are required, site-specific LAN and VLAN requirements can be defined and prioritized over the generic global IP address pools.

Site-Specific Profile

Site-specific profile is optional and is required only for pre-provisioning LAN IP addresses on each site. Pre-provisioning allows you to define a site using the site name and device combination before devices are added to the unclaimed device list. This is accomplished by matching the device serial number with the site name. VLAN definition for each site allows you to specify IP address pool ranges, otherwise, the LAN Greenfield IP address pools or the generic IP address pool provides the required LAN IP addresses.

Branch Site-Specific Profile

You can pre-provision specifications for the branch sites. A single or dual router site can be defined using device serial numbers and site name along with VLANs for the site.

For a single router branch, you must specify the serial number of the device. For a dual router branch, you must specify the serial number of both the devices separated by a semi-colon. The Cisco IWAN application automatically matches the site name and device serial numbers and uses the previously defined VLANs and IP address pools. Thus, branch sites are available before the devices are displayed in the site provisioning workflow under unclaimed devices.

Defining the site and VLAN enables you to easily configure the devices when devices are provisioned in the site provisioning workflow. When the devices are claimed and provisioned, the site provisioning workflow does not conflict with the existing site configuration and site name.

You cannot modify the IP address pools after you have saved them.

LAN Brownfield IP Address Pool

In the Cisco IWAN release 1.3, the LAN Brownfield role was introduced to define LAN IP addresses for Brownfield branch devices.

When a Brownfield branch is provisioned, its VLAN subnets are reserved.

If the VLAN subnets are subnets of a LAN Brownfield IP address pool, they are reserved from a LAN Brownfield IP address pool.

If there are no LAN Brownfield subnets for the VLAN subnets, they are reserved as site-specific IP address pools.

The add, delete, and update operations are not allowed on Brownfield site-specific IP address pools.



Managing Branch Sites

After you have configured and setup the hub site, you can add devices to Cisco IWAN and provision them to the sites.

You can add and provision the following two types of devices:

- Greenfield Devices—Discovered by the Cisco Plug-n-Play (Cisco PnP) application. Greenfield devices are brand new out-of-the-box routers.
- Brownfield Devices—Discovered by the Cisco APIC-EM application. Brownfield devices belong to existing sites that are added to Cisco IWAN.

This chapter contains the following sections:

- [Basic Workflow for Managing Branch Sites, page 4-1](#)
- [Bootstrapping Greenfield Devices, page 4-2](#)
- [Adding and Provisioning Greenfield Devices to the Branch Site, page 4-2](#)
- [Adding and Provisioning Brownfield Devices to the Branch Site, page 4-7](#)
- [Viewing Site Status Information, page 4-18](#)

Basic Workflow for Managing Branch Sites

Table 4-1 *Basic Workflow for Managing Branch Sites*

| No. | Task | Reference |
|-----|---|--|
| 1 | Bootstrap devices discovered by the Cisco PnP application. | Bootstrapping Greenfield Devices, page 4-2 |
| 2 | Add devices to Cisco IWAN and then provision them to the sites. | Adding and Provisioning Greenfield Devices to the Branch Site, page 4-2 Adding and Provisioning Brownfield Devices to the Branch Site, page 4-7 |
| 3 | View the site status. | Viewing Site Status Information, page 4-18 |

Bootstrapping Greenfield Devices

You can bootstrap devices discovered by the Cisco PnP application. These devices are called Greenfield devices.

Use this procedure to download a bootstrap file.

Procedure

-
- Step 1** From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.
 - Step 2** Click the **Bootstrap** tab. The bootstrap files that are available for download are displayed.
 - Step 3** From the Download column, click the download bootstrap icon to download the bootstrap file to a local directory on your computer. You can use this file as a template for PnP call home.

After the Greenfield devices are provisioned to a site, the appropriate bootstrap file is automatically uploaded on to the device.

For details, see the *Cisco Open Plug-n-Play Agent Configuration Guide* at:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pnp/configuration/xr-3e/pnp-xr-3e-book.html>.

Adding and Provisioning Greenfield Devices to the Branch Site

Use this procedure to add Greenfield devices that are discovered by the Cisco PnP application and provision them to the branch site.



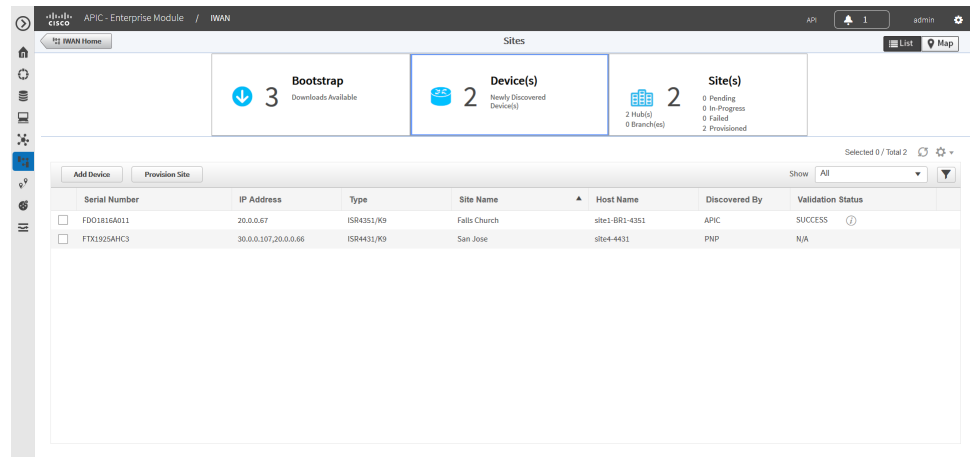
Note

-
- Before you use the devices to provision the site, we recommend that you save the running configuration in flash or bootflash in the IWAN_RECOVERY.cfg file so that you can restore the configuration if needed.
 - There must be at least 16 VTY lines configured.
-

Procedure

Step 1 From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.

Step 2 Click the **Device(s)** tab. A list of unclaimed devices are displayed as shown in the following figure:



| Field | Description |
|-------------------|---|
| Checkbox | Choose this checkbox to choose the unclaimed device for provisioning. |
| Serial Number | Serial number of the device. |
| IP Address | IP address of the device. |
| Type | Type of device. |
| Site Name | Name of the site to which the device belongs. To edit the site name, double-click it, and then add the new name. |
| Host Name | Device host name. |
| Discovered By | Can be one of the following: <ul style="list-style-type: none"> PNP—Discovered by the Cisco PnP application. This is a Greenfield device. APIC—Discovered by the Cisco APIC-EM application. This is a Brownfield device. |
| Validation Status | Displays the following for Greenfield devices: <ul style="list-style-type: none"> N/A—Devices discovered by the Cisco PnP application. Can be one of the following for Brownfield devices: <ul style="list-style-type: none"> Success—Devices successfully validated and ready for provisioning to the branch site. These devices are either discovered by the Cisco APIC-EM application or are manually added by clicking the Add Device tab. Failure—Devices that have must-fix errors. These devices are either discovered by the Cisco APIC-EM application or are manually added by clicking the Add Device tab. Warning—You can choose to ignore these errors or fix them. These devices are either discovered by the Cisco APIC-EM application or are manually added by clicking the Add Device tab. |

- Step 3** Check the checkbox next to the Greenfield device(s) that you want to use, and then click the **Provision Site** tab. The Select Topology tab opens and displays the available topologies.



Note To determine if the device is Brownfield or Greenfield, look at the **Discovered By** column in the Add Devices page. PNP indicates that it is a Greenfield device. APIC indicates that it is a Brownfield device.



Note You can choose a maximum of two devices.



Note Greenfield and Brownfield devices cannot be part of the same site.

- Step 4** Click the topology that is appropriate for your network. The L2/L3 options display.



Note The topology options that display are dependent on the number of devices you selected in Step 3.

- Step 5** Click the **L2** option. The Configure Topology page displays.



Note L3 is not supported on Greenfield devices.

- Step 6** From the Configure Topology page, specify the following properties:

| Field | Description |
|----------------|---|
| Site Name | Site name, which you can change if needed. |
| Site Location | Click Set Geo to specify the site location on a map. A map opens. Click on the site, the Site Location field is populated. Click anywhere outside the map to exit the map. |
| POP to Connect | Choose the preferred hub site for this branch site from the drop-down list. |
| Select WAN | Choose the WAN from the drop-down list. |

Step 7 Configure WAN settings for the branch device. Do the following:

- a. Click the + icon next to the WAN cloud. The Configure WAN Cloud dialog box opens. Depending on the WAN type you chose in Step 6, the fields that display in the Configure WAN Cloud dialog box change.
- b. For an Public WAN, the Configure WAN Cloud dialog box displays the following fields. Enter the required properties, and then click **Save**.

| Field | Description |
|-----------------|--|
| WAN Type | Public |
| Interface Type | Type of interface. Values: T1, E1, or Ethernet. |
| Interface | Choose the interface that connects to the WAN cloud from the drop-down list. |
| Connect to WAN | Connection method. |
| Enable | Choose one of the two radio buttons as appropriate: <ul style="list-style-type: none"> Static IP—When selected, the following additional fields display: WAN IP Address, WAN IP Mask, and WAN Gateway IP Address. DHCP |
| Upload (Mbps) | Upload bandwidth (in Mbps). |
| Download (Mbps) | Choose the download bandwidth from the drop-down list. |
| Service Profile | Profile name configured in the Service Providers tab. |

- c. For a Private WAN, the Configure WAN Cloud dialog box displays the following fields. Enter the required properties, and then click **Save**.

| Field | Description |
|-----------------|---|
| WAN Type | Private |
| Interface Type | Type of interface. Values: T1, E1, or Ethernet. |
| Interface | Choose an interface from the drop-down list. |
| Connect to WAN | Connection method. |
| CE IP Address | Customer Edge Server IP Address. This field is auto-populated if the interface has a static IP address already configured. <p>Note Depending on the number of links that you created when setting up the hub sites in the IWAN Aggregation Site, you might need to specify additional IP addresses for CE devices.</p> |
| CE IP Mask | The mask of the CE IP address. |
| PE IP Address | Provider Edge Server IP Address. This field is auto-populated if the interface has an IP address and default gateway. |
| Download (Mbps) | Choose the download bandwidth from the drop-down list. |
| Service Profile | Profile name configured in the Service Providers tab. |

Step 8 Configure LAN settings. Do the following:

Displays the following for Greenfield devices:



Note You can either create the LAN Greenfield IP address pool during hub provisioning; or you can add it after hub provisioning for Greenfield deployments. When the LAN Greenfield IP address pool is not present, the system automatically uses the generic pool IP address.

- a. Click the **+** icon next to the LAN. If site specific IP address pools are configured for the site, the Configure VLAN dialog box opens.
- b. Enter the following properties, and then click **Save**:

| Field | Description |
|----------------------|---|
| LAN Interface | |
| Site Interface | Enter or choose the LAN interface from the drop-down list. |
| VLAN | |
| VLAN Type | Enter or choose a VLAN type from the drop-down list. Default Values: Data, Guest, Voice & Video, or Wireless. To create a custom VLAN, click the + icon in the last VLAN, and then enter the name of the VLAN. |
| VLAN ID | Numeric value within the following ranges: 1 - 98; 100 - 1001; 1006 - 4094. You cannot duplicate a VLAN ID. |
| Total IPs | Number of hosts in the VLAN. |

Step 9 From the Provisioning Sites page, click **Apply Changes**. The Provisioning Site Summary dialog box opens with a summary of the configuration.

Step 10 Review the information, and then do one of the following:

- Click the **Apply Now** radio button, and then click **Submit**.
- Click the **Schedule** radio button, specify a date and time to apply the site provisioning, and then click **Submit**.



Note The **Apply Now** option does not check for validations in conflict with future scheduled workflows. You must reevaluate scheduled jobs based on the changes and update the jobs as required. If there is a conflict when the scheduled job is activated, it might fail to provision the site.

Adding and Provisioning Brownfield Devices to the Branch Site

Use this procedure to add Brownfield devices that are discovered by the Cisco APIC-EM application and provision them to the branch site.

Brownfield devices are not automatically displayed on the Devices tab. You must first add them to Cisco IWAN, and then provision them to the branch site.



Note

- Before you use the devices to provision the site, we recommend that you save the running configuration in bootflash in the IWAN_RECOVERY.cfg file so that you can restore the configuration if needed.
- There must be at least 16 VTY lines configured.
- Devices that are configured with SNMP version 2 or version 3 can be used as branch devices.

Procedure

Step 1 From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.

Step 2 Click the **Device(s)** tab. The following page displays.

| Serial Number | IP Address | Type | Site Name | Host Name | Discovered By | Validation Status |
|---------------------------------------|-----------------------|------------|--------------|----------------|---------------|-------------------|
| <input type="checkbox"/> F201816A011 | 20.0.0.67 | ISR4351/K9 | Falls Church | site1-BR1-4351 | APIC | SUCCESS |
| <input type="checkbox"/> FTX1925AHJC3 | 30.0.0.107, 20.0.0.66 | ISR4431/K9 | San Jose | site4-4431 | PNP | N/A |

365868

Step 3 To add a Brownfield device, click the **Add Device** tab. The Add Device dialog box opens and displays a list of devices discovered by the Cisco APIC-EM application as shown in the following figure:



Note Alternatively, you can add devices using the Cisco APIC EM discovery feature.

Device can be claimed either by selecting from the below inventory list or By [adding New Device](#)

Devices Discovered by APIC-EM

| | Host Name | IP Address |
|-----------------------|----------------|------------|
| <input type="radio"/> | site1-BR2-4351 | 30.0.0.108 |

Claim Device Cancel

Step 4 Do one of the following:

- Choose an existing Cisco APIC-EM discovered device—From the Devices Discovered by APIC-EM area, click the radio button next to the device you want to add to Cisco IWAN, and then click **Claim Device** (see above figure). The claimed device is added to the Devices page and is available for provisioning.
- Add a new device—Click **Adding New Device** (see figure above). The Add Device dialog box opens where you specify the IP address for the new device and additional properties as shown in the following figure and the table that follows, and then click **Add Device**:

Add Device

Router Management

IP

SNMP

Version

V2C

Read Community

Write Community

SNMP Retries and Timeout

Retries

3

Timeout (secs)

10

SSH/Telnet

Protocol

ssh2

Username

Password

Enable Password

Timeout (secs)

300

Add Device

Cancel

| Field | Description |
|--|---|
| Router Management IP | IP address for the new device. |
| SNMP | |
| Version | SNMP version number. Depending on the version number you choose, different properties display. |
| Read Community (Displayed if you chose SNMP V2C.) | SNMP V2C read community string. |

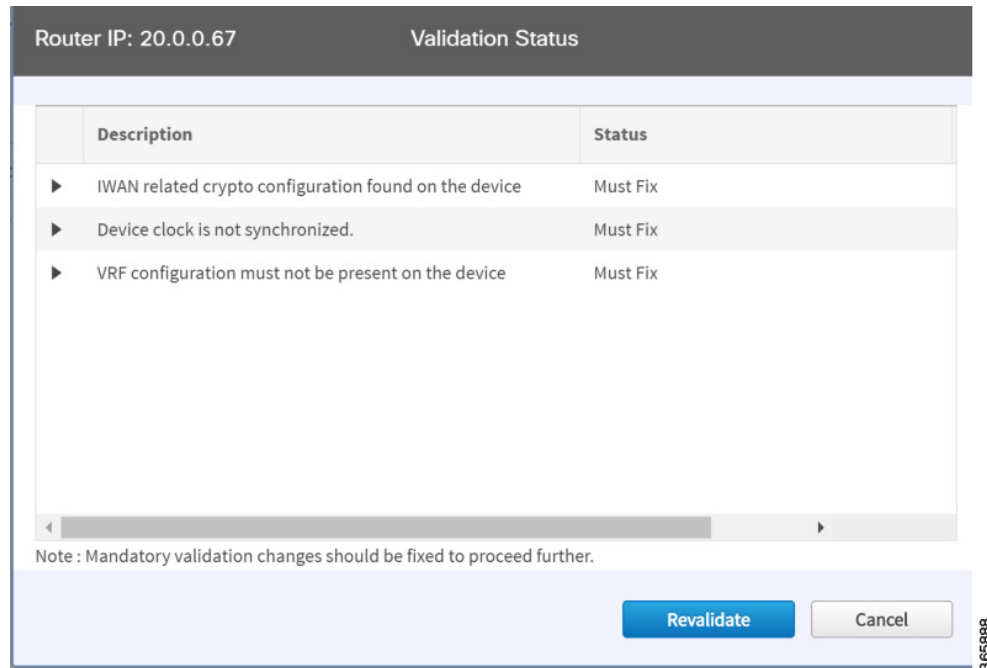
| Field | Description |
|--|---|
| Write Community (Displayed if you chose SNMP V2C.) | (Optional) SNMP V2C write community string. |
| Mode (Displayed if you chose SNMP V3.) | Choose the mode from the drop-down list. Options are: <ul style="list-style-type: none"> • Authentication and Encryption • No Authentication and No Encryption • Authentication and No Encryption |
| Auth. Type (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. Choose the authentication type from the drop-down list. Options are: <ul style="list-style-type: none"> • HMAC-SHA • HMAC-MDS |
| Username (Displayed if you chose SNMP V3.) | Displayed if you chose SNMP V3. The authentication username. |
| Auth. Password (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. The password for the authentication username. |
| Encryption Type (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption in the Mode field. The encryption username. |
| Encryption Password (Displayed if you chose SNMP V3.) | Displayed if you chose Authentication and Encryption in the Mode field. The password for the encryption username. |
| SNMP Retries and Timeout | |
| Retries | Number of SNMP retries. Default: 3 |
| Timeout (secs) | Number of seconds to wait before the system considers an SNMP request to have timed out. Default: 10 |
| SSH/Telnet | |
| Protocol | Protocol used to communicate to the host (SSH or Telnet). |
| Username | SSH or Telnet username. |
| Password | SSH or Telnet password. |
| Enable Password | Enable password for the username. |
| Timeout (secs) | Number of seconds to wait before the system considers an SSH or Telnet request to have timed out. |

The device is verified in the background to determine if the device is suitable for provisioning. The following occurs:

The Cisco IWAN application accesses the router and checks its configuration to determine if it has any configuration that might conflict with the Cisco IWAN application. This is called Brownfield Validation.

If the router does not have conflicting configurations, an orange icon appears on top of the device and the Configure Router Dialog opens.

If the router has conflicting configurations, the Validation Status dialog opens listing all the validation failures, as shown in the following figure:



- c. The validation status could be either Warning or Must Fix. Do the following:
 - If the validation status is Warning, you can fix it or ignore it.
 - If the validation status is Must Fix, remove the configurations suggested by the description, and then click **Revalidate**.

For information about the messages displayed in the Validation Status dialog box, see [Appendix A, “Brownfield Validation Messages.”](#)

Step 5 From the Devices page, check the checkbox next to the Brownfield device(s) that you want to provision for a site, and then click the **Provision Site** tab. The Select Topology tab opens and displays the available topologies.



Note To determine if the device is Brownfield or Greenfield, look at the **Discovered By** column in the Add Devices page. PNP indicates that it is a Greenfield device. APIC indicates that it is a Brownfield device.



Note You can choose a maximum of two devices.

Step 6 Click the topology that is appropriate for your network. The L2/L3 options display.



Note The topology options that display are dependent on the number of devices you selected in Step 5.

Step 7 Depending on the LAN site configuration, click the appropriate **L2/L3** option. The Configure Topology page displays.



Note If the VLAN on branch devices are on the same subnet, choose L2. If the VLAN on the branch devices are on different subnets, choose L3.

Step 8 From the Configure Topology page, specify the following properties:

| Field | Description |
|----------------|---|
| Site Name | Site name, which you can change if needed. |
| Site Location | Click Set Geo to specify the site location on a map. A map opens. Click on the site, the Site Location field is populated. Click anywhere outside the map to exit the map. |
| POP to Connect | Choose the hub that you specified in the IWAN Aggregation Site from the drop-down list. |
| Select WAN | Choose the WAN from the drop-down list. |

Step 9 Configure WAN settings for the branch device. Do the following:

- a. Click the + icon next to the WAN cloud. The Configure WAN Cloud dialog box opens. Depending on the WAN type you chose in Step 8, the fields that display in the Configure WAN Cloud dialog box change.
- b. For a Public WAN, the Configure WAN Cloud dialog box displays the following fields. Enter the required properties, and then click **Save**.

| Field | Description |
|-----------------|--|
| WAN Type | Public |
| Interface Type | Type of interface. Values: T1, E1, or Ethernet. |
| Interface | Choose an interface that connects to the WAN cloud from the drop-down list. |
| Connect to WAN | Connection method. |
| Enable | Choose one of the two radio buttons as appropriate: <ul style="list-style-type: none"> Static IP—When selected, the following additional fields display: WAN IP Address, WAN IP Mask, and WAN Gateway IP Address. DHCP |
| Upload (Mbps) | Upload bandwidth (in Mbps). |
| Download (Mbps) | Choose the download bandwidth from the drop-down list. |
| Service Profile | Profile name configured in the Service Providers tab. |

- c. For a Private WAN, the Configure WAN Cloud dialog box displays the following fields. Enter the required properties, and then click **Save**.

| Field | Description |
|-----------------|---|
| WAN Type | Private |
| Interface Type | Type of interface. Values: T1, E1, or Ethernet. |
| Interface | Choose an interface from the drop-down list. |
| Connect to WAN | Connection method. |
| CE IP Address | Customer Edge Server IP Address. This field is auto-populated if the interface has a static IP address already configured. Note Depending on the number of links that you created when setting up the hub sites in the IWAN Aggregation Site, you might need to specify additional IP addresses for CE devices. |
| CE IP Mask | The mask of the CE IP address. |
| PE IP Address | Provider Edge Server IP Address. This field is auto-populated if the interface has an IP address and default gateway. |
| Download (Mbps) | Choose the download bandwidth from the drop-down list. |
| Service Profile | Profile name configured in the Service Providers tab. |

Step 10 Configure LAN settings. Do the following:

Click the + icon next to the LAN. If you selected L2 topology and the LAN interface is a physical interface or a switchport interface, the Configure VLAN dialog box opens (see below). Choose the LAN interface from the drop-down list, and then click **Save**.

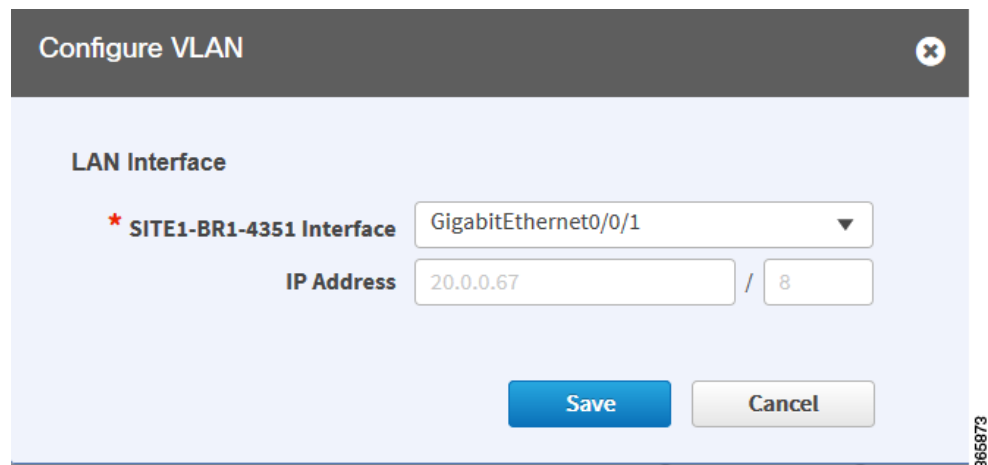
**Note**

- If you selected a dual router topology, the common VLANs between devices are displayed.
- Make sure there are no site-specific IP address pools configured for Brownfield sites.
- The VLAN information seen on the Configure VLAN dialog box is auto populated based on the LAN interface that you selected on the router.
- You cannot edit the auto populated information from the Configure VLAN interface dialog box.
- You can either create the LAN Brownfield IP address pool during hub provisioning; or you can add it after hub provisioning for brownfield deployments. When the LAN Brownfield IP address pool is not present, the system automatically creates site-specific pools for the Brownfield devices.

| VLAN | | |
|---------|------------|---------|
| VLAN ID | IP Address | IP Mask |
| 35 | 35.1.1.0 | 24 |
| 10 | 25.1.1.0 | 24 |

If you selected L3 topology, the following Configure VLAN dialog box opens as shown in the following figure. Do the following:

- Choose the LAN interface from the drop-down list. The IP address is automatically populated.

A screenshot of a 'Configure VLAN' dialog box. The dialog has a dark gray header with the title 'Configure VLAN' and a close button (X icon). The main area is light blue and contains the following fields: 'LAN Interface' with a dropdown menu showing 'GigabitEthernet0/0/1', 'IP Address' with a text field containing '20.0.0.67' and a subnet mask field containing '8'. There are 'Save' and 'Cancel' buttons at the bottom right. A small red star icon is next to the text '* SITE1-BR1-4351 Interface'. A vertical text '365873' is visible on the right side of the dialog box.

Configure VLAN

LAN Interface

* SITE1-BR1-4351 Interface GigabitEthernet0/0/1

IP Address 20.0.0.67 / 8

Save Cancel

365873

- b. Click **Save**.
- c. If you have dual routers, choose the LAN interface for that device, and then click **Save**.
- d. Click the + icon above Routing Configuration. The LAN Routing Configuration dialog box opens as shown in the following figure. Enter the properties and then click **Save**.



Note VLANs are displayed per device.

I

LAN Routing Configuration

Site Prefix ⓘ

/

Add Prefix

Discovered

| <input type="checkbox"/> | Subnet IP | Mask |
|--------------------------|-----------|------|
| <input type="checkbox"/> | 25.1.1.0 | 24 |
| <input type="checkbox"/> | 35.1.1.0 | 24 |

* Selected

| <input type="checkbox"/> | Subnet IP | Mask |
|--------------------------|-----------|------|
| <input type="checkbox"/> | 45.1.1.0 | 24 |
| <input type="checkbox"/> | 55.1.1.0 | 24 |

→

←

LAN Routing Protocol

* Routing Protocol

EIGRP

* AS Number

300

Save

Cancel

365920

| Field | Description |
|-----------------------------|---|
| Site Prefix | Network prefixes auto-learned for the site. |
| Add Prefix button | Click this button to manually add additional site prefix. |
| Discovered Pane | Prefixes automatically discovered by Cisco IWAN. |
| Arrows | Click on the --> arrow to move the prefix from the Discovered pane into the Selected pane. Click on the <-- arrow to move the prefix from the Selected pane into the Discovered pane. |
| Selected Pane | List of selected prefixes. |
| LAN Routing Protocol | |
| Routing Protocol | Default routing protocol running on the devices. Can be: EIGRP or OSPF Note EIGRP and OSPF are supported routing protocols, which means that LAN-WAN redistribution is performed by Cisco IWAN. Cisco IWAN does not perform LAN-WAN redistribution for BGP protocol. |
| Area Number/AS Number | Depending on the routing protocol, enter the following: <ul style="list-style-type: none"> Area number for OSPF. AS number for EIGRP. Note For a dual router site, make sure that the area numbers for OSPF and the AS numbers for EIGRP are the same across both devices. |

Step 11 From the Provisioning Sites page, click **Apply Changes**. The Provisioning Site Summary dialog box opens with a summary of the configuration.

Step 12 Review the information and then do one of the following:

- Click the **Apply Now** radio button, and then click **Submit**.
- Click the **Schedule** radio button, specify the date and time to apply the site provisioning, and then click **Submit**.



Note The **Apply Now** option does not check for validations in conflict with future scheduled workflows. You must reevaluate scheduled jobs based on the changes and update the jobs as required. If there is a conflict when the scheduled job is activated, it might fail to provision the site.

Viewing Site Status Information

Use this procedure to view the information about the site and determine its overall status.

Procedure

- Step 1** From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.
- Step 2** Click the **Site(s)** tab. The following properties appear:

| Field | Description |
|------------|---|
| Health | Health of the hub and health of the site. |
| App Health | Application health for the hub. Prime credentials must be configured to view this information. |
| Site | Click the hub name or site name as appropriate to display the following details: <ul style="list-style-type: none"> • Site status—Whether the site is provisioned. • Application status—Status of the application. • Alarms tab—If there are issues with the site, this tab provides information about the problem. In addition, the system also provides suggestions to troubleshoot and fix the problem. • Hub Topology or Site Topology tab—Topology of the site, including the site name, site location, and preferred POP. Hover on the devices and WAN clouds in the topology to get more details. • IP Address Allocation tab—List of devices, including the subnet mask and the IP address pool to which the device is allocated. • Application tab—Application usage on the site in a graphical format. The graph displays the following: <ul style="list-style-type: none"> – Various applications configured for the site. – Bandwidth usage for each application. – Statistical trend for each application. |
| Location | Location of the site. |
| Status | Whether the site is provisioned. |
| Action | Can be one of the following: <ul style="list-style-type: none"> • Delete icon—Click to delete the site that has issues. See Deleting a Hub Site, page 7-5, Deleting a Transit Hub, page 7-5, or Deleting Branch Sites, page 7-6. • Recovery icon—Option available if recovery for this site is possible. See Recovering a Cisco IWAN Site, page 7-4. • Update Site Prefix (pen) icon—Click to add or delete site prefixes after hub provisioning. This option is only available for L3 Brownfield sites. See Adding or Deleting Site Prefixes, page 7-8. |



Administering Application Policies

This chapter contains the following sections:

- [Understanding the Categorize Applications Tab, page 5-1](#)
- [Understanding the Define Application Policies Tab, page 5-4](#)
- [Understanding the Application Bandwidth Tab, page 5-7](#)

Understanding the Categorize Applications Tab

The Cisco IWAN Application comes with pre-defined applications grouped into categories. Use the **Categorize Applications** tab to view, edit, move, and add custom applications as shown in the following table:

Table 5-1 Categorize Applications Tab

| No. | Task | Reference |
|-----|---|---|
| 1 | View all of the installed applications in an alphabetized list or view the applications by category. View a summary of all applications. Search for a specific application. | Viewing Applications, page 5-2 |
| 2 | Move applications into different categories. | Moving Applications to a Different Category, page 5-2 |
| 3 | Edit application information. | Editing Application Information, page 5-3 |
| 4 | Add new custom application to an existing category. | Adding a New Application, page 5-3 |



Note

For a quick tutorial about what you can do in the Categorize Applications page, click **Teach Me** in the instructional text.

Viewing Applications

Use this procedure to view applications by list, by category, or view a summary of all installed applications.

Procedure

-
- | | |
|---------------|---|
| Step 1 | From the Cisco IWAN on APIC-EM home page, click Administer Application Policy . The Application Policy page opens. |
| Step 2 | Click the Categorize Applications tab. All of the installed applications are displayed in an alphabetized list. |
| Step 3 | To view the applications by category, click the By Applications drop-down list (located under the Add Application tab), and then choose By Category . Not all categories are shown by default, to view all categories click Show available in the instructional text. |
| Step 4 | To view all of the applications in a particular category, click the down arrow by a category. |
| Step 5 | To view a summary of the total number of applications, popular applications, and custom applications, look at the Applications Summary area. |
| Step 6 | To search for a specific application, enter one of the following parameters in the Search field: application short name, long description, ports, and traffic class. |
-

Moving Applications to a Different Category

To share bandwidth, you can choose to move the application into a different category.

Procedure

-
- | | |
|---------------|---|
| Step 1 | From the Cisco IWAN on APIC-EM home page, click Administer Application Policy . The Application Policy page opens. |
| Step 2 | Click the Categorize Applications tab. All of the installed applications are displayed in an alphabetized list. |
| Step 3 | To view all of the applications in a particular category, click the down arrow by a category. |
| Step 4 | To move an application into a different category, drag-and-drop it into the appropriate category, and then click Apply Changes . |
-

Editing Application Information

Use this procedure to edit application information.

Procedure

-
- | | |
|---------------|---|
| Step 1 | From the Cisco IWAN on APIC-EM home page, click Administer Application Policy . The Application Policy page opens. |
| Step 2 | Click the Categorize Applications tab. All of the installed applications are displayed in an alphabetized list. |
| Step 3 | To view all of the applications in a particular category, click the down arrow by a category. |
| Step 4 | To edit application information, click on the pencil icon next to the application. Information about the application appears. |
| Step 5 | Click Edit . The Edit Application dialog box opens. |
| Step 6 | Make your changes, and then click Save . |
-

Adding a New Application

Use this procedure to add a new custom application.

Procedure

-
- | | |
|---------------|---|
| Step 1 | From the Cisco IWAN on APIC-EM home page, click Administer Application Policy . The Application Policy page opens. |
| Step 2 | Click the Categorize Applications tab. All of the installed applications are displayed in an alphabetized list. |
| Step 3 | To add a new custom application, click the Add Application tab. The Add Application dialog box opens. |
| Step 4 | Enter the following properties, and then click Add : |

| Field | Description |
|-------------------|--|
| Name | Name of the application. |
| Type radio button | Choose one of the following: <ul style="list-style-type: none"> • URL—Click the radio button, and then enter the application url in the URL field. • Server IP/Port—Click the radio button, and then enter the IP, port, and protocol for the application to use. • DSCP—Differentiated services code point (DSCP). Click the radio button, and then choose a value from the drop-down list. |
| Similar to | Click the field to display a list of available similar applications, and then choose an application. |
| Category | Choose a category from the drop-down list for the new application to reside. |
| Jitter | (Optional) Specify a different value or keep the default value. |
| Packet loss | (Optional) Specify a different value or keep the default value. |
| Delay | (Optional) Specify a different value or keep the default value. |

Understanding the Define Application Policies Tab

Use the **Define Application Policy** tab to define policies according to their relevance to the business. The application policies are categorized into the following three business groups:

- **Business Relevant**—Applications such as email, voice-and-video, file-sharing, backup-and-storage that are critical to the business.
- **Default**—Applications such as epayment.
- **Business Irrelevant**—Applications that are not relevant to the business such as social media and gaming applications.

Use the **Define Application Policy** tab to do the following:

Table 5-2 *Define Applications Tab*

| No. | Task | Reference |
|-----|---|--|
| 1 | Move an application category to a different business group. | Understanding the Application Bandwidth Tab, page 5-7. |
| 2 | Modify application performance. | Modifying the Application Performance, page 5-5 |

Moving an Application Category to a Different Business Group

Use this procedure to move an application category to a different business group.

Procedure

-
- | | |
|---------------|---|
| Step 1 | From the Cisco IWAN on APIC-EM home page, click Administer Application Policy . The Application Policy page opens. |
| Step 2 | Click the Define Application Policy tab. All of the applications are displayed in three categories: Business Relevant, Default, and Business Irrelevant. |
| Step 3 | To move an application from one business group to another, use the drag-and-drop feature. For example, you can drag the epayment application from the Default group and drop it into the Business Irrelevant group. |
-

Modifying the Application Performance

Use this procedure to modify the application performance parameters.

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the Cisco IWAN on APIC-EM home page, click Administer Application Policy . The Application Policy page opens. |
| Step 2 | Click the Define Application Policy tab. All of the applications are displayed in three categories: Business Relevant, Default, and Business Irrelevant. |
| Step 3 | To modify the application performance, click the down arrow next to an application. The Application Performance dialog box opens as shown in the following figure. |

Step 4 Do the following:

- a. Click the **Application Performance** button to enable or disable it.
- b. Choose the appropriate path preference radio button.
- c. Choose primary and secondary path from the drop-down list. The secondary path can be Drop.

Step 5 Select a path preference, with Path 1 being the preferred path for traffic in this category. For example, Int (Internet).

Step 6 After updating the path preference, click **Save**.

Note The **Save** option does not check for validations in conflict with future scheduled workflows. Please reevaluate scheduled jobs based on these changes and update scheduled jobs as required. If there is a conflict when the scheduled job is activated, it may fail at that time.

Understanding the Application Bandwidth Tab

Use the Application Bandwidth tab to view the bandwidth used across various applications. Based on this information you can choose to move applications into different categories. See [Moving Applications to a Different Category, page 5-2](#).

Viewing the Application Bandwidth

Use this procedure to view the bandwidth used across different applications in a graphical format.

Before You Begin

Make sure you have done the following:

- Added the Cisco APIC-EM controller IP address on the Prime application.
- Added the Prime credentials in Cisco APIC-EM.

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the Cisco IWAN on APIC-EM home page, click Administer Application Policy . The Application Policy page opens. |
| Step 2 | Click the Application Bandwidth tab. The amount of bandwidth used per application category for each hub is displayed in a graphical format. You can also view the date and time the bandwidth is used the most. |
-



Monitoring and Troubleshooting Sites

This chapter provides contains the following section:

- [Monitoring and Troubleshooting, page 6-1](#)

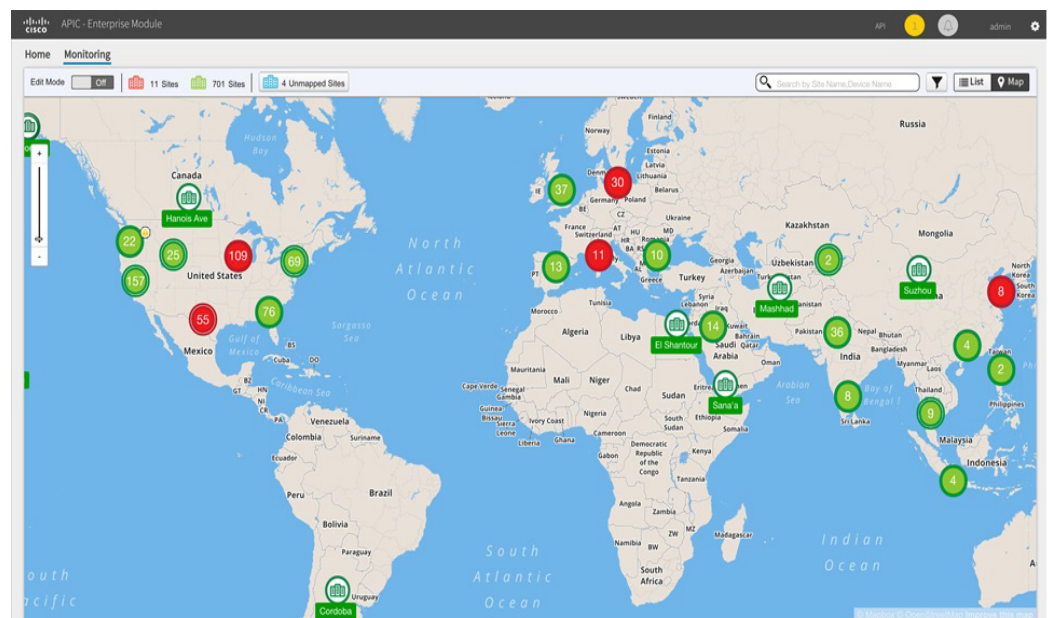
Monitoring and Troubleshooting

Use this procedure to monitor and troubleshoot sites.

Procedure

- Step 1** From the Cisco IWAN home page, click **Monitor and Troubleshoot**. The Monitoring page opens and a map displays with all of the sites highlighted, indicating the number of hubs and branches present across the globe for Cisco IWAN.

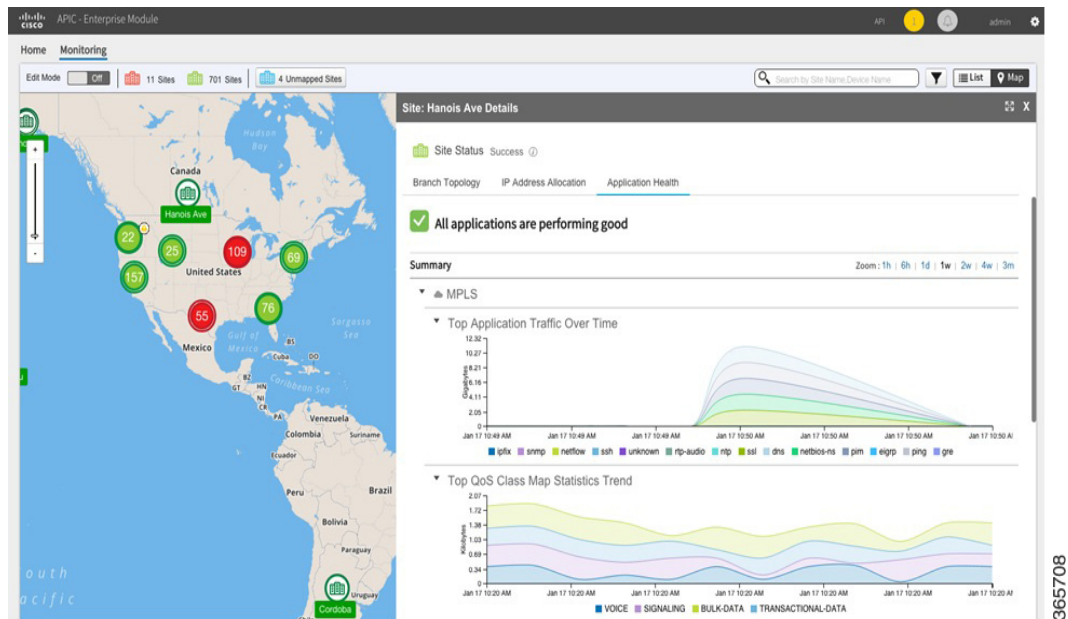
Figure 6-1 *Monitoring Page*



- Step 2** Click a highlighted site. The Site Details page opens with the following information and additional tabs:

- Site status—Whether the site is provisioned.
 - Application status—Status of the application.
- Step 3** Click the **Hub Topology** or **Site Topology** tab, to view the topology of the hub or site as appropriate, including the site name, site location, and preferred POP.
- Step 4** Click the **IP Address Allocation** tab to view a list of devices in the site and the IP addresses to which the devices are allocated.
- Step 5** Click the **Application Health** tab to view the application usage on the site in a graphical format. The graph displays the following:
- Various applications configured for the site.
 - Bandwidth usage for each application.
 - Statistical trend for each application.

Figure 6-2 Application Health Tab



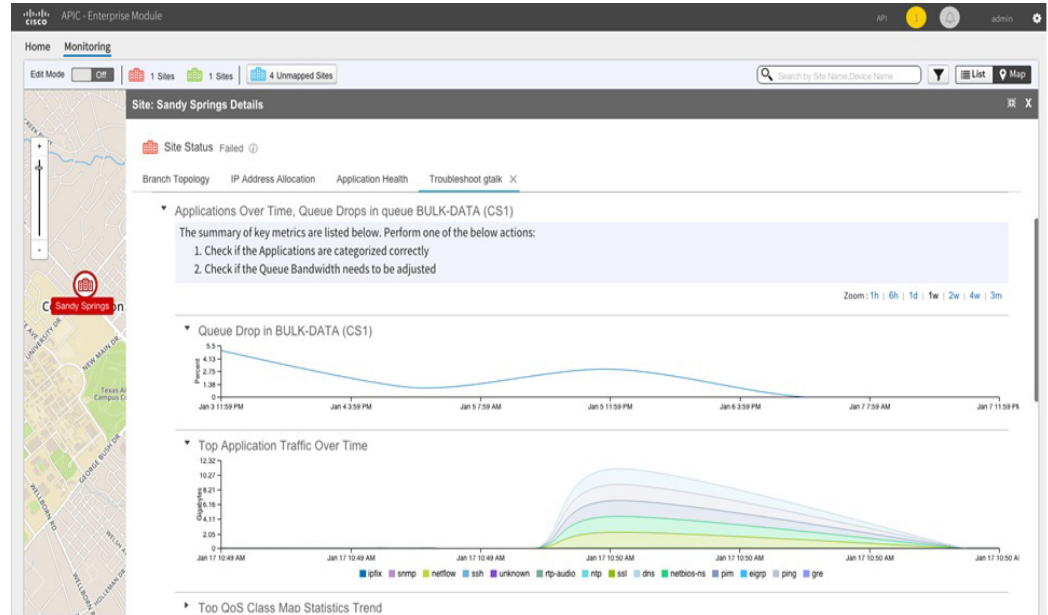
- Step 6** Click the **Alarms** tab to view issues with a site.



Note The Alarms tab appears only when the system suspects that the site has an issue because of an application or due to bandwidth allocation.

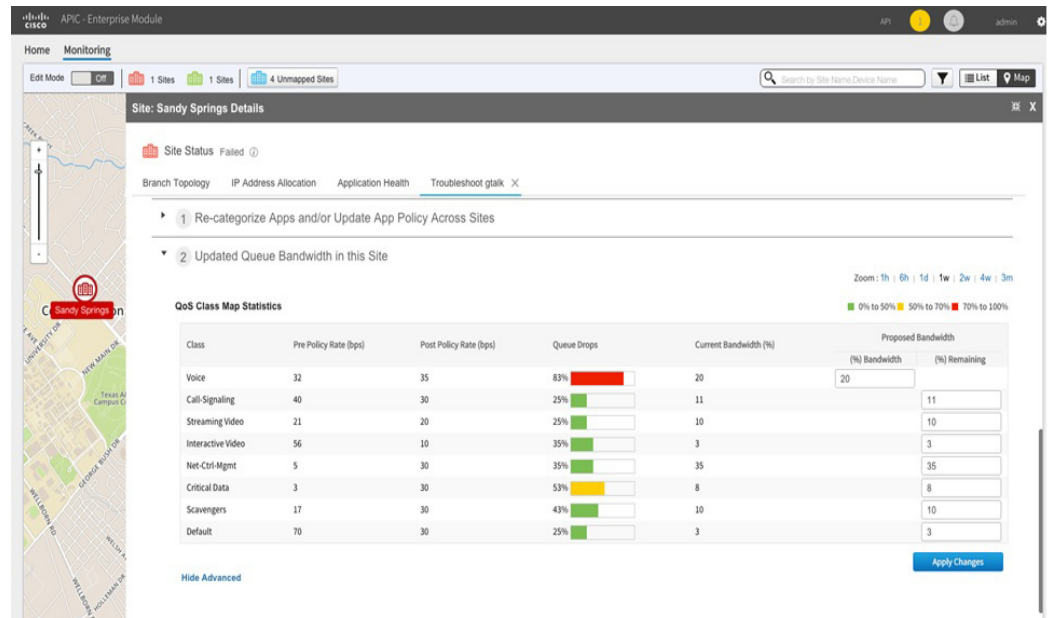
- Step 7** Click the **Troubleshooting** tab to troubleshoot the application when the hub or branch site application health is critical as shown in the following figure.

Figure 6-3 Troubleshooting—Detection



In addition to detecting the application causing the issue, the system also provides suggestions to improve the site. For example, if a site uses more bandwidth the system suggests adjusting the bandwidth among the various applications to provide more bandwidth to the application causing the issue.

Figure 6-4 Troubleshooting—Healing a Site





Backup and Restore, Recovery, and Delete

This chapter contains the following sections:

- [Backup and Restore, page 7-1](#)
- [Recovery, page 7-4](#)
- [Delete, page 7-5](#)
- [Adding or Deleting Site Prefixes, page 7-8](#)

Backup and Restore

Backup and Restore Recommendations

We recommend the following for the proper working of backup and restore:

- Run in multihost mode. This enables active high availability (HA) thereby reducing the backup and recovery windows.
- Before you use the devices to provision the site, we recommend that you save the running configuration in bootflash in the IWAN_RECOVERY.cfg file so that the configuration can be restored if needed.
- If a site is deleted, the routers are reloaded with the configuration that is saved in the IWAN_RECOVERY.cfg file.
- Perform a backup everyday to maintain a current version of your database and files.
- Perform a backup and restore after you initiate changes in the system.
- Do not use backup and restore to undo any intent that you performed earlier. Use workflows supported in the application to accomplish intent.
- Track devices that are added to Cisco IWAN or have their certificates updated.
- Track devices that are deleted from Cisco IWAN or have their certificates revoked.

Backup and Restore Scenarios

Backup and restore *works* in the following scenarios:

- The controller is in a stable state with respect to IWAN application business intent.
- Cisco IWAN application business intent has not been initiated between backup and restore.
- Site status is in success or failure state, with no site recovery in progress.
- No scheduled jobs are active in the same period.

Backup and restore *does not work* in the following scenarios:

- Cisco IWAN is handling application business intent, which includes internal database operations and device policy updates.
- There is a risk in Cisco APIC-EM where the controller and the network is out of sync after a restore and consequentially some or all sites might be out of policy (as displayed on the Site Status screen). Some out of policy situations, such as security related issues might not be detected.
- Workflows performed on the Cisco IWAN application during the backup and restore operation, will be lost and cannot be tracked or retrieved. The following table shows workflow scenarios with possible workarounds:

Table 7-1 Workflow Scenarios Where Backup and Restore Fails With Workaround

| Scenario | Workaround |
|--|---|
| Sites (one or more devices) added to IWAN during the backup and restore operation. | <ol style="list-style-type: none"> 1. Remove the PKI trustpoint and zero out the keys on each device. Use the following commands to clear trustpoints and certificates on each device: <pre>no crypto pki trustpoint sdn-network-infra-iwan crypto key zeroize rsa sdn-network-infra-iwan</pre> 2. Restart the Plug-n-Play workflow. This displays the device as an unclaimed device in the Cisco IWAN application. 3. If the device is already added as a site, copy the startup configuration to the running configuration and reload the router on each affected router. The PnP call home workflow takes over and the device appears as an unclaimed device in the workflow. 4. Reapply site provisioning. 5. Repeat the site creation workflow. |
| Devices that had their certificates renewed during the backup and restore operation. | <ol style="list-style-type: none"> 1. Remove the PKI trustpoint and zero out the keys on each device. 2. Use the following commands to clear trustpoints and certificates on each device: <pre>no crypto pki trustpoint sdn-network-infra-iwan crypto key zeroize rsa sdn-network-infra-iwan</pre> 3. Repeat the site creation workflow for the device or set of devices. <p>When a device is provisioned by the Cisco IWAN application, it is provided with a certificate to prove its identity. This certificate is valid for one year. When eighty percent of the certificate lifetime expires, the device automatically attempts to renew the certificate.</p> <p>If the devices try to renew their certificates between a backup and a restore, the database displays that the certificate has not been renewed.</p> <p>Because it is difficult to track devices and their certificate status, Cisco provides an API to determine the devices whose client ID certificates have expired; and devices whose client ID certificates are going to expire soon.</p> <p>Use the APIs to determine the devices that need to renew certificates or re-provision the expiring or expired client ID certificates respectively. After a device's client ID certificate expires, the only option is to re-provision it.</p> |

Table 7-1 Workflow Scenarios Where Backup and Restore Fails With Workaround

| Scenario | Workaround |
|--|--|
| Sites that are deleted from Cisco IWAN or have their certificates revoked during the backup and restore operation. | <p>Do one of the following:</p> <ul style="list-style-type: none"> Revoke the certificate for each device using the controller's user interface. If the site is part of a network, from the Actions column in the Site Status page, click the X icon to revoke the certificate and clear the application for that site. |
| Configuration or policy updates during the backup and restore operation. | <p>The Cisco IWAN application can detect changes on devices that are in conflict with the controller. If updates are made to a site between a backup and a restore, the site is removed from the policy. We recommend that you reapply the same set of changes that were previously applied. However, the success rate of this approach depends on the nature of the change. If the site is removed from the policy, manual intervention is required. This is because the controller is no longer in charge for removing the policy from the sites unless the manual changes are successful.</p> <p>Note We recommend that use an automated script, which automatically tracks the audit log entries for adding and deleting devices along with the status of their certificates (revoked or created). This script is useful when restoring an unstable system. The audit records are also useful when reapplying the changes lost due to system instability. Run the automated script at regular intervals after backup is complete to prepare the system for restore.</p> |

Recovery

Recovering a Cisco IWAN Site

Use this procedure to recover a site when site provisioning fails.

-
- Step 1** From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.
- Step 2** Click the **Site(s)** tab. From the **Action** column in the Site Status page, click the **Recovery** icon.
- After attempting to recover a site, if the site recovery is a success, the site moves to the Success state, otherwise the **Recovery** icon appears again allowing you to retry recovering the site.
- You can attempt to recover a site multiple times. However, if a site cannot be recovered, the only option is to delete a site.
-

Post Provisioning Recovery for Hub and Branch Sites

The post provisioning recovery feature allows you to reapply the last change to the hub and spoke devices after the sites have been provisioned.

Recovery can be attempted multiple times. To recover a hub or a branch site, click the **Recovery** icon in the **Action** column in the Site Status page.

If recovery fails after multiple attempts, you can choose to delete the site permanently by clicking the delete **X** icon in the **Action** column in the Site Status page.

Delete

Deleting a Hub Site

You can delete a primary hub if the primary hub is in a failed state and no branch sites have been provisioned.

If both the primary hub and transit hub are in failed state, you must delete the transit hub first in order to delete the primary hub. If the delete operation succeeds, both the primary hub and transit hub are reset to the brownfield validation state.

When a hub is deleted after hub provisioning fails, the Cisco IWAN application does the following:

- Revokes the PKI certificate and trustpoint.
- Releases the IP addresses to the IP address pool.
- Deletes the hub from the inventory.

If the delete operation succeeds, the hub is removed from **Sites** page.



Note

The hub site is deleted on a best-effort basis. If the devices are unreachable, they are not restored to the original configuration. In this case, you must manually clean up the configuration on the devices. See [Manually Cleaning Up Devices, page 7-6](#).

You can re-provision the hub from the Configure Hub Site page as part of the hub provisioning (see [Wizard Step 5—Configuring the IWAN Aggregation Site, page 3-12](#)).

Deleting a Transit Hub

You can delete a transit hub irrespective of the state of the transit hub—whether it is provisioned or failed.

When a transit hub is deleted, IWAN performs the following:

- Revokes the PKI certificate and trustpoint from all devices in the transit hub.
- Releases the IP addresses to the IP address pool.
- Deletes the transit hub from inventory.
- Cleans the Network and Wireless Services (NWS) state.

If the delete operation succeeds, the transit hub is removed from the **Sites** page.



Note

The transit-hub site is deleted on a best-effort basis. If the devices are unreachable, they are not restored to the original configuration. In this case, you must manually clean up the configuration on the devices. See [Manually Cleaning Up Devices, page 7-6](#).

Deleting Branch Sites

You can delete branch sites from IWAN irrespective of the branch state—in progress, provisioned, or failed.

Procedure

-
- Step 1** From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.
- Step 2** Click the **Site(s)** tab. From the **Action** column in the Site Status page, click the **X** icon to delete the site.
-



Note

Branch sites are deleted on a best-effort basis. If the devices are unreachable, they are not restored to the bootstrap configuration. In this case, you must manually clean up the configuration on the devices. See [Manually Cleaning Up Devices, page 7-6](#).

When a branch site is deleted, the Cisco IWAN application performs the following:

- Revokes the PKI certificates and trust points.
- Releases the IP addresses from IP address pools.
- Cleans the site information from the database.
- Does the following to try to revert the routers of the deleted site to the bootstrap configuration file: IWAN_RECOVERY.cfg. Does the following:
 - Copies the IWAN_RECOVERY.cfg to the startup configuration.
 - Reloads the device.

See [Backup and Restore, page 7-1](#).

After the site is deleted, the branch devices are removed from the **Devices** tab and are displayed in the unclaimed device list, thereby, allowing you to re-provision the branch site.

Manually Cleaning Up Devices

After a hub site, transit-hub site, or branch site delete operation, the devices in the site are deleted on the best-effort basis. If the devices are unreachable, they are not restored to the original configuration. In this case, you must manually clean up the configuration on the devices.

Use this procedure to manually clean up the configuration on the devices.

Procedure

-
- Step 1** Remove the IWAN PKI trust point. Use the following command:
- no crypto pki trustpoint sdn-network-infra-iwan**
- Step 2** Remove the IWAN RSA key from NVRAM. Use the following commands:
- crypto key zeroize rsa sdn-network-infra-iwan**
- write erase**
- Step 3** Restore the original configuration. Use the following commands:
- config replace bootflash:<original-config-file> force**
- write**
-

Example:

```

RPRE-GA-1-HUB-INET# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RPRE-GA-1-HUB-INET(config)# no crypto pki trustpoint sdn-network-infra-iwan
% Removing an enrolled trustpoint will destroy all certificates
received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
% Be sure to ask the CA administrator to revoke your certificates.

RPRE-GA-1-HUB-INET(config)# crypto key zeroize rsa sdn-network-infra-iwan
Do you really want to remove these keys? [yes/no]: yes
RPRE-GA-1-HUB-INET(config)# end
RPRE-GA-1-HUB-INET# write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
RPRE-GA-1-HUB-INET# config replace bootflash:clean-config force
%EIGRP: Deleting base topology is not allowed.
% Interface GigabitEthernet0/0/4 IPv4 disabled and address(es) removed due to enabling VRF
IWAN-TRANSPORT-2% Profile is applied to Tunnel11-head-0 (head) and possibly other crypto
maps
% No such key-chain% Profile is applied to Tunnel11-head-0 (head) and possibly other
crypto maps% Profile is applied to Tunnel11-head-0 (head) and possibly other crypto maps%
Profile is applied to Tunnel11-head-0 (head) and possibly other crypto maps% Profile is
applied to Tunnel11-head-0 (head) and possibly other crypto maps
The rollback configlet from the last pass is listed below:
*****
!List of Rollback Commands:
no crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-2
end
*****

Rollback aborted after 5 passes
RPRE-GA-1-HUB-INET# write

```

Adding or Deleting Site Prefixes

You can add or delete site prefixes after hub provisioning.



Note

This option is only available for L3 Brownfield sites.

Procedure

- Step 1** From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.
- Step 2** Click the **Site(s)** tab. From the **Action** column in the Site Status page, click the **Update Site Prefix** (pen) icon. The LAN Site Prefix dialog box opens.
- Step 3** To add a site prefix, click the **+** icon.
- Step 4** To delete a site prefix, select the check box next to the prefix that you want to delete, and then click the **X** icon.



Note

You cannot delete all prefixes. You must have at least one prefix per site.

- Step 5** Click **Apply Changes**.



Upgrading the Cisco IWAN Application

This chapter contains the following section:

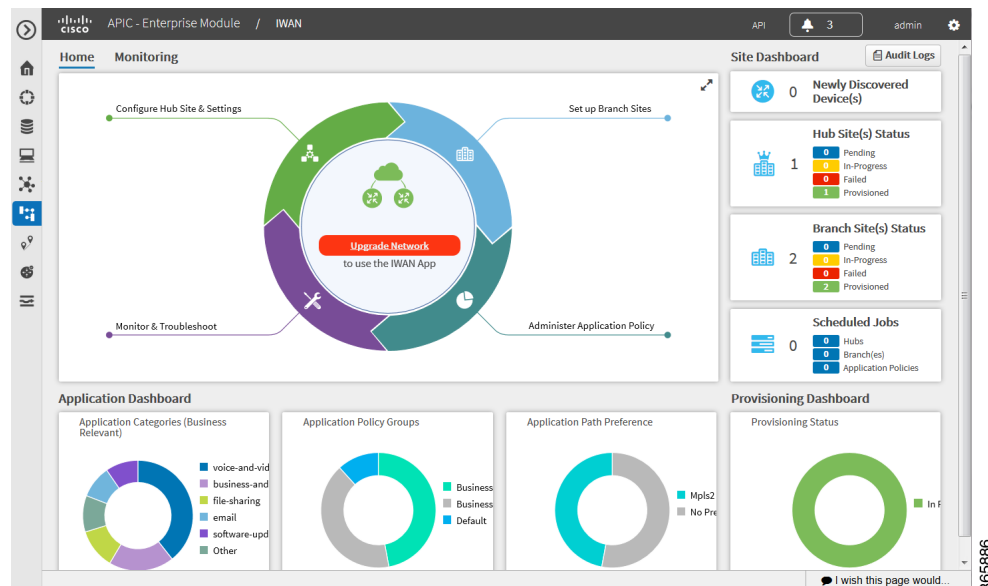
- [Upgrading the Cisco IWAN Application, page 8-1](#)

Upgrading the Cisco IWAN Application

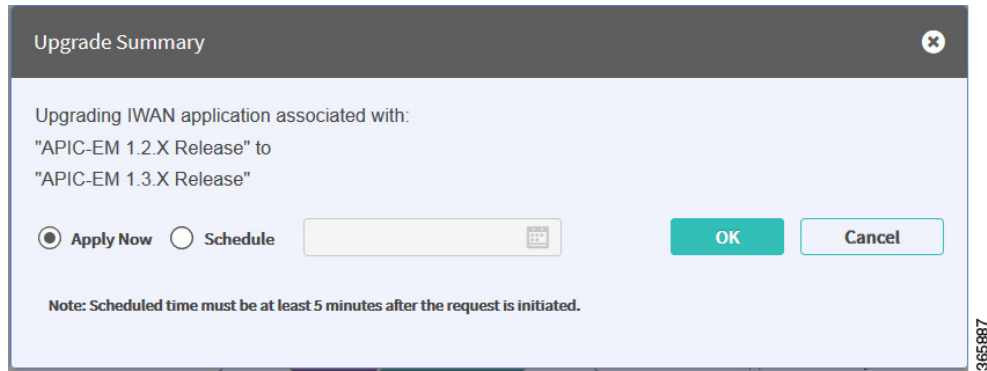
Upgrade the Cisco IWAN application if you want the network to leverage the latest Cisco APIC-EM controller functionality.

Procedure

- Step 1** After the Cisco APIC-EM upgrade process is complete, a red **Upgrade Network** button appears on the Cisco IWAN home page as shown in the following figure:



- Step 2** Clear the browser cache.
- Step 3** Click the red **Upgrade Network** button. The Upgrade Summary dialog box opens as shown in the following figure.



- Step 4** From the Upgrade Summary dialog box, do one of the following:
- To perform the upgrade immediately, click the **Apply Now** radio button, and then click **OK**.
 - To schedule the upgrade later, click the **Schedule** radio button, specify the date and time, and then click **OK**.

After the upgrade is complete, the **Manage Branch Sites > Sites** page opens with the status, **Provisioned**.



Brownfield Validation Messages

This chapter contains the following sections:

- [Error Messages Encountered During Brownfield Validation, page A-1](#)
- [Warning Messages Encountered During Brownfield Validation, page A-3](#)

Error Messages Encountered During Brownfield Validation

The following table provides a description of the error messages encountered during the Brownfield validation process:

Table A-1 Error Messages in Brownfield Validation

| Error Messages | Description |
|--|---|
| Username configuration must have privilege level 15. | <p>Configure a username with privilege level 15 on the device.</p> <p>Example: <code>username username privilege 15 password 0 password</code></p> |
| PfR configuration must not be present on the device. | <p>Ensure that Performance Routing (PfR) configuration is not present on the device.</p> <p>Example: <code>no domain ONE</code></p> |
| QoS configuration must not be present on the device. | <p>Ensure that Quality of Service (QoS) configuration is not present on the device.</p> <p>Example: <code>no class-map match-any nbar-12-clr#VOICE no policy-map nbar-12-clr no policy-map IWAN-INTERFACE-SHAPE-ONLY-INTERNET no service-policy input nbar-12-clr no service-policy output IWAN-INTERFACE-SHAPE-ONLY-INTERNET</code></p> |

| Error Messages | Description |
|---|---|
| Interface loopback 47233 must not be configured on the device. | <p>Remove interface loopback 47233 from the device.</p> <p>Example: <code>no interface loopback47233</code></p> |
| IWAN trustpoint configuration must not be present on device. | <p>Remove Cisco IWAN trustpoint configuration from the device.</p> <p>Example: <code>no crypto pki trustpoint sdn-network-infra-iwan</code></p> |
| VPN routing and forwarding (VRF) configuration must not be present on the device. | <p>Remove the existing VRFs as VRFs as it will interfere with the Cisco IWAN configuration.</p> <p>Make sure that the routers do not have any of the following VRFs:</p> <ul style="list-style-type: none"> • IWAN-TRANSPORT-1 • IWAN-TRANSPORT-2 • IWAN-TRANSPORT-3 • IWAN-TRANSPORT-4 <p>Example: <code>no ip vrf IWAN-TRANSPORT-4</code></p> |

Warning Messages Encountered During Brownfield Validation

The following table provides a d description of the warning messages encountered during the Brownfield validation process:

Table A-2 *Error Messages in Brownfield Validation*

| Warning Messages | Description |
|--|---|
| Please make sure at least two interfaces for WAN and LAN are up and running. | Ensure that the two interfaces for WAN and LAN are up and running. Verify using the show ip interface brief command. |
| IWAN related crypto configuration found on the device. | Remove the crypto configuration because the crypto configuration might interfere with the Cisco IWAN configuration. Example: <code>crypto zeroize mypubkey rsa</code> <code>sdn-network-infra-iwan</code> |
| Device does not have required license. | Required licenses are not enabled on the device. Enable the licenses for the platform in use. For example, AX (Application Experience K9) “appxk9” is required for Cisco 4000 Series Integrated Services Routers; and Advanced Enterprise K9 (adventerprisek9) or Advanced IP Services K9 (advipservicesk9) is required for Cisco ASR 1000 Series Aggregation Services Routers. |
| No routing protocol found on device. | Enable one of the following routing protocols on the device. Example: <code>router ospf AS number</code> <code>router eigrp AS number</code> <code>router bgp AS number</code> |
| EZPM configuration found on the device. | Remove Easy Performance Monitor (EZPM) configuration as EZPM configuration might interfere with the Cisco IWAN configuration. Example: <code>no class-map match-all</code> <code>Business-Critical-and-default-tcp-only</code> <code>no performance monitor context IWAN-Context</code> <code>profile application-experience</code> |

| Warning Messages | Description |
|--|--|
| NBAR configuration found on the device. | <p>Remove the Network Based Application Recognition (NBAR) configuration as NBAR configuration might interfere with the Cisco IWAN configuration.</p> <p>Example:</p> <pre>no ip nbar attribute-map Consumer_App_Prof no ip nbar attribute-map Other_Custom no ip nbar attribute-map Net_Admin_Custom</pre> |
| No device information available for validation. | <p>Revalidate and if problem persists, ensure the following:</p> <ul style="list-style-type: none"> • Device is up and running. • Device connectivity is established. |
| Device does not have valid image version and K9 package. | <p>The Cisco IWAN application does not support the Cisco software image loaded on the device. Boot the device with a 15.5(3) or 15.5(4) image with the K9 feature pack.</p> <p>Example:</p> <pre>asr1000rp1-adventerprisek9.03.16.00.S.155-3.S-ext.bin</pre> |