



Software Configuration Guide for Cisco IWAN on APIC-EM

Release 2.0.0
May 25, 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 v

Organization v

Conventions vi

CHAPTER 1

Introduction 1-1

Deploying and Configuring IWAN on APIC-EM 1-1

CHAPTER 2

Deploy Cisco IWAN on APIC-EM 2-1

CHAPTER 3

Log in to APIC-EM to Access Cisco IWAN 3-1

CHAPTER 4

Configure Hub Site and Settings 4-1

System 4-1

Certified IOS Releases 4-4

IP Address Pools 4-4

Service Providers 4-9

IWAN Aggregation Site 4-11

Configure LAN Settings for the Data Center 4-20

Configure Master Controller 4-22

CHAPTER 5

Set Up Branch Sites 5-1

Bootstrap 5-1

Sites 5-1

Devices 5-1

Select Topology 5-2

Edit site name and location 5-3

Configure WAN Clouds 5-3

Configure LAN 5-5

Site Summary 5-6

CHAPTER 6

Administering Application Policy and Monitoring Sites 6-1

Administering Application Policy 6-1

Categorize Applications 6-1

Define Application Policy 6-4

Bandwidth Usage 6-7
 Monitoring Sites 6-7

CHAPTER 7

Backup, Restore, Recovery, and Delete 7-1
 Backup and Restore for IWAN on APIC-EM 7-1
 Recommendations 7-1
 Caveats and Workarounds 7-2
 Recovery for IWAN Devices 7-3
 Recovery Mechanism for Hub and Branch Sites 7-3
 Post Provisioning Recovery Mechanisms for Hub and Branch Sites 7-3
 Deleting Sites 7-4
 Deleting a Hub Site 7-4
 Deleting Transit POPs (Datacenters) 7-4
 Deleting Branch Sites 7-5

CHAPTER 8

Upgrading IWAN App 8-1
 Upgrading IWAN 8-1

APPENDIX A

Brownfield Validation Messages Description A-1
 Error Messages Encountered in Brownfield Validation A-1
 Warning Messages Encountered in Brownfield Validation A-2

APPENDIX B

Related Documentation B-1



Preface

Organization

This guide includes the following sections:

Section	Title	Description
1	Introduction	Introduces Cisco IWAN on APIC-EM and describes the sequence of sections to follow in this guide to complete the hub and branch site provisioning process.
2	Deploying Cisco IWAN on APIC-EM	Describes where to find instructions for deploying Cisco APIC-EM (controller).
3	Log in to APIC-EM to Access Cisco IWAN	Describes initially logging in to Cisco IWAN on APIC-EM application and the top-level menu.
4	Update Hub Site and Settings	Describes provisioning of hub site.
5	Apply Network Wide Settings	Describes manual steps between provisioning of hub site and later branch site provisioning.
6	Set up Branch Sites	Shows the steps for provisioning branch sites.
7	Administer Application Policy	Describes the organization of application policies and categories.
8	Backup, Restore, and Recovery	Describes backup, restore, and recovery mechanisms.
9	Upgrading IWAN	Describes steps to upgrade IWAN.
A	Brownfield Validation Messages Description	Describes the error messages and warning messages encountered in brownfield validation.
B	Related Documentation	Describes documentation for Cisco IWAN on APIC-EM, Cisco APIC-EM and Cisco Plug and Play.

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.



Caution

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



Timesaver

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



Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of

each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS



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



Introduction

Cisco IWAN on APIC-EM extends Software Defined Networking to the branch with an application-centric approach based on business policy and application rules. This provides IT centralized management with distributed enforcement across the network.

Cisco IWAN on APIC-EM automates Cisco IWAN deployments with an intuitive browser-based GUI. A new router can be provisioned in a matter of minutes 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 on APIC-EM 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 on APIC-EM uses an application-centric approach to offer these benefits:

- Lower Operational Costs

Cisco IWAN on APIC-EM helps IT deliver an unparalleled user experience over any connection while lowering operational costs.

- Simplified IT Operations

Cisco IWAN on APIC-EM uses a software-based controller model, automating and centralizing management tasks to ensure faster, more successful deployments.

- Less Complexity

Cisco IWAN on APIC-EM leverages the Cisco Application Centric Infrastructure Controller Enterprise Module (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.

Deploying and Configuring IWAN on APIC-EM

The process for deploying and configuring Cisco IWAN on APIC-EM is summarized below. Before following the below sequence, ensure that the system requirements are as mentioned in the *Release Notes for IWAN on APIC-EM*.

- [Deploy Cisco IWAN on APIC-EM, page 2-1](#)
- [Log in to APIC-EM to Access Cisco IWAN, page 3-1](#)
- [Configure Hub Site and Settings, page 4-1](#)
- [Set Up Branch Sites, page 5-1](#)
- [Administering Application Policy and Monitoring Sites, page 6-1](#)



Deploy Cisco IWAN on APIC-EM

The Cisco IWAN on APIC-EM application is part of the Cisco APIC-EM (controller) software.

To install Cisco APIC-EM, follow the deployment steps in section “*Deploying the Cisco APIC-EM*” in the Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide. (See Related Documentation.) This requires an ISO image file to be loaded onto Cisco UCS hardware.



Note

Please follow the guidelines in Appendix B: Preparing Virtual Machines for Cisco APIC-EM to avoid deployment issues on controller.



Log in to APIC-EM to Access Cisco IWAN

Perform the following steps to login to Cisco IWAN on APIC-EM.

Step 1 Enter the FQDN name of the APIC-EM cluster or the External Network IP address in the Google Chrome browser. As of this release, Google Chrome is the supported browser.

Step 2 When logging in for first time, click **Set up Hub site(s) & Settings**.

You are directed to the specify the global settings in the **CLI Credentials** page before provisioning the hub.

Refer to the Network IP address used in “Deploying the Cisco APIC-EM” section of the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.



Note If a message appears that says the site’s security certificate is not trusted, ignore the message. After Cisco IWAN is deployed, you can replace the selfsigned certificate by selecting Settings and Certificate. The Cisco APIC-EM supports the import and storing of an X.509 certificate and private key into the controller.

Step 3 Enter your username and password at the Login window and click **Log In**.

a. Review and confirm the Telemetry Disclosure, which appears only when you log in for the first time.

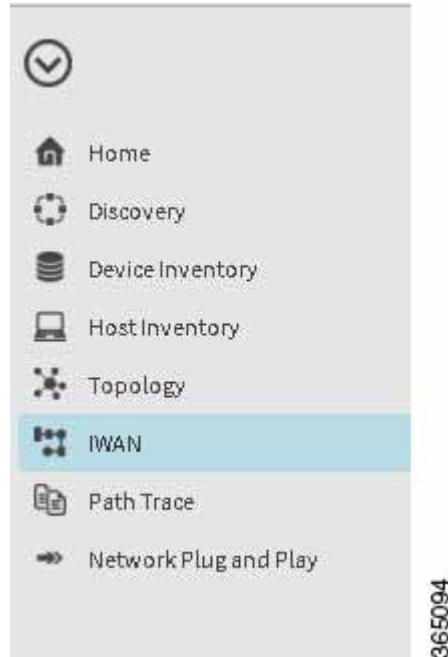
After clicking **Confirm**, the Cisco APIC-EM GUI now appears.

b. Proceed with accessing and using the Cisco APIC-EM for your network.

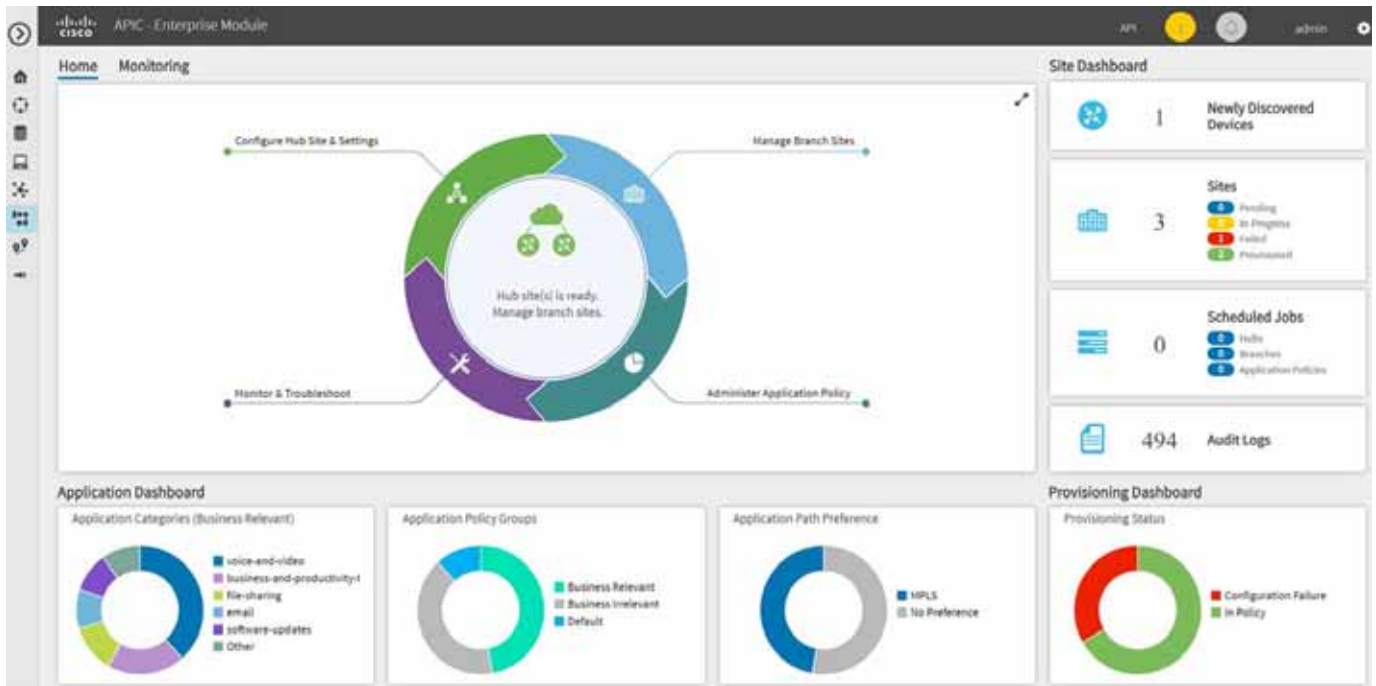
After IWAN Application is loaded, you will see the dashboard UI of Cisco APIC-EM. See the example below.

Example

This example shows the top level menu of Cisco APIC-EM. The left navigation bar shows the IWAN application and other applications such as Network Plug and Play as shown in the following figure.



The frame on the right hand side provides an enhanced user experience by allowing you to configure IWAN in a workflow model, if you are a first time user of IWAN. If you have configured IWAN, this frame provides the configuration status, for example, the hub and branch provisioning status, the device status, and the application status.



Where to Go Next

Go to [Configure Hub Site and Settings](#), page 4-1.



Configure Hub Site and Settings

This section describes setting up the network environment, which provides resources for routers at hub and branch sites. Later, you can provision branch routers using “Setup Branch Sites”.

Select each of the tabs below and complete the configuration tasks:

- [System, page 4-1](#)
- [Certified IOS Releases, page 4-4](#)
- [IP Address Pools, page 4-4](#)
- [Service Providers, page 4-9](#)
- [IWAN Aggregation Site, page 4-11](#)
- [Configure LAN Settings for the Data Center, page 4-20](#)

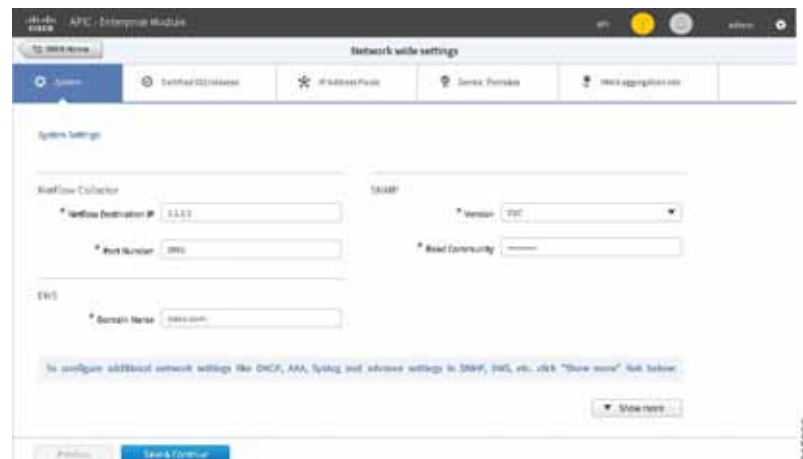


Note

The generic IP pool is used for overlay and loopback addresses. The generic IP pool is divided according to the number of remote sites and service providers as specified in the “IP Address Pools” tab. Please plan by understanding your future requirements by specifying the maximum number of service providers and remote sites they you plan to deploy. The IP address pool settings cannot be changed once specified.

System

Select the “System” tab.



Summary

Enter the global system settings in preparation for enabling both IWAN hubs and spokes.

Select each of the menu options within the “System” menu option to define settings for TACACS, SNMP, DNS, NTP, and Syslog servers.

Netflow Collector**Summary**

Enter an IP address for the Netflow collector. This is the IP address of a Netflow collector such as the LiveAction application. Application visibility and performance metrics are sent to the collector.

Field	Description
Netflow Destination IP	IP address of the NetFlow collector (server). Traffic is sent from the network devices to the Netflow collector; for example, Cisco Prime, or LiveAction.
Port Number	Port number of the NetFlow collector (server). Example: 2055.

DNS**Summary**

Enter a domain name and the IP address of a DNS primary server, used by network devices for SSH. The **ip domain-name** command is used to generate RSA keys. A secondary server can be specified for redundancy.

Field	Description
Domain name	The domain name. Example: cisco.com
Primary Server	Primary server IP address. Example: 192.0.2.1
Secondary Server	(Optional) Secondary server IP address. Example: 198.51.100.1

SNMP

Enter SNMP server details. Either the APIC-EM controller can act as an 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.

Click Show more for SNMP Retries and Timeout, to change the values for number of retries and timeout period.

Field	Description
Trap Destination IP	(Optional) IP address of the SNMP server. (If you do not enter an IP address, the Cisco IWAN application is used as an SNMP server.) Example: 10.10.10.10
Version	Software version of SNMP. Values: V2C, V3.
Read Community	SNMP read community. Example: "Public".
Write Community	(Optional) SNMP write community. Example: "Private".
Retries	Number of retries. Default 3.
Timeout (secs)	Timeout period. Default 10.

Syslog

You may enter the IP address of a third party syslog server, to which network devices send syslog messages.

Field	Description
Server IP	(Optional) Syslog server's destination IP address. The router will be configured to send Syslog messages to this server.

Authorization, Authentication, Accounting

Summary

TACACS is the only supported centralized Authentication, Authorization and Accounting (AAA) service for Cisco IWAN. If a TACACS server is provided, spoke devices will utilize TACACS for all management access to the spoke devices (SSH & HTTPS). Whether or not a TACACS service is provided, a local AAA user database is created on the spoke device, which can be used when TACACS is not available.

Cisco APIC-EM global credentials, if present, are used as default values for the local AAA user credentials, else local user credentials default to the username and password specified in global device credentials for branch routers or to the username and password entered while provisioning the hub. The enable password for device configuration mode is cisco123.

Enter an IP address and key for the AAA server.

Field	Description
IP Address	(Optional) IP address of AAA server (TACACS).
Key	(Optional) Key of AAA server.

DHCP

Enter the IP address of a DHCP server that provides client computers and other TCP/IP-based network devices with valid IP addresses.

Field	Description
External DHCP IP	(Optional) Destination IP address of DHCP server.

Where to Go Next

Select the “Service Providers” tab.

Certified IOS Releases

**Note**

If the routers already have the correct image loaded, selecting an image in Certified IOS Releases is optional.

For each of the router types (such as “ISR4431”) displayed in the window, you can specify a Cisco IOS image. To update the image for a router, click on the small “Up” icon of the router. After an image is uploaded it is ready to be pushed to the branch router later.

Where to go Next

Select the “Service Providers” tab.

IP Address Pools

Overview of IP Address Pools

IWAN application will automatically utilize IP addresses carved from the global enterprise IP Pool space. To support this functionality, one generic global IP pool must be defined for the IWAN application. Allocated out of this generic IP pool will be all the IPs required to provision hub and spoke device needs. This includes interface, LAN, VPN overlay and routing needs.

Optionally, one or more LAN IP pools may be defined to further refine the branch LAN side IP address space. These LAN IP pools will be used for LAN needs until exhausted and then if required, generic IP pool is leveraged.

**Note**

It is important to size the generic IP pool correctly for the long term needs of the IWAN site. VPN requirements dictate that subnets must be defined and allocated internally (up front) before any sites are provisioned. Therefore, once the site and service provider sizing is set, it is frozen for the life of the controller. Please plan accordingly for long term IWAN site requirements. For instance, it is best if you specify the service provider, keeping in mind, that you would require in future, depending on your requirements. There have been issues when service providers are added to the network without specifying the appropriate maximum number of service providers.

Optionally, site specific LAN (VLAN) requirements may be defined and prioritized over the generic global IP pools wherever specific IP addresses are required.

Site-Specific Profile

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

Branch Site-Specific Profile

You can preprovision 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 device. Thus, branch sites are available before the devices display in the site provisioning workflow under unclaimed devices. Defining the site and VLAN enables you to easily configure the devices when the 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 can remove or edit any of the global IP address pools at any point until you click **Save & Continue**. However, you cannot modify the IP address pools after you have configured the IP address pools. For dual router branch, you must enter the Site Specific IP address pool for one device. You must specify the serial numbers for each device.



Caution

In Cisco IWAN Release 1.0, the two workflows are not completely integrated. It is up to you to ensure compatibility of site definition. The device and site association must match that in the site provisioning workflow.

Working on the IP Address Pool Tab

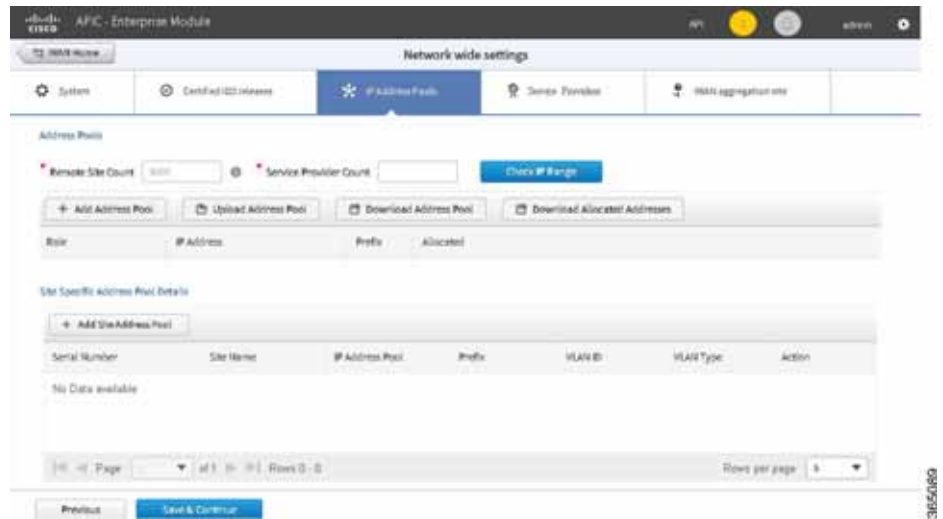


Note

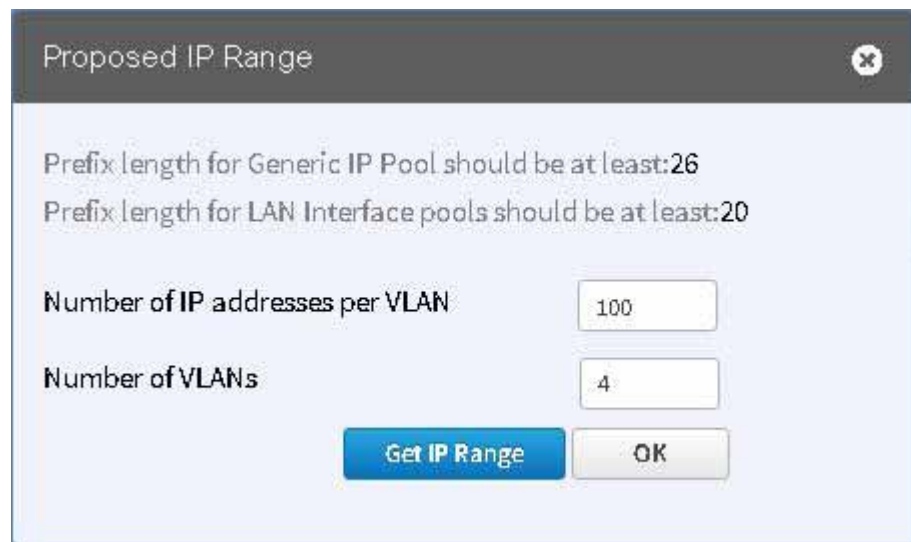
The generic IP pool is used for overlay and loopback addresses. The generic IP pool is divided according to the number of remote sites and service providers as specified in the “IP Address Pools” tab. Please plan by understanding your future requirements by specifying the maximum number of service providers and remote sites they you plan to deploy. The IP address pool settings cannot be changed once specified.

The **IP Address Pools** tab allows you to define the IP pool. Use **Check IP Range** button for suggestion on the minimum prefix needed for generic IP pool and LAN Interface IP pools. For better scalability, you can also export or import IP addresses via .csv file into the application. Upon import, existing targeted network sites are updated with the new VLAN information. If some sites need to utilize specific IP addresses on the VLANs, the IP addresses can either be specified using the options in the **IP Address Pools** tab or import IP addresses via a .csv file.

Step 1 Select the **IP Address Pools** tab.



- Step 2** To help size the global generic IP pools for your network, enter the long term maximum remote sites count and the number of unique service provider paths that you will require and click **Check IP Range**.



The IP prefix identified is the minimum IP pool suggested to support the expected network scale. Optionally, by entering the expected average number of hosts behind each VLAN per site, a prefix for the global LAN IP pools is also suggested. Additionally, this dialog also provides suggestion for the LAN side IP requirements.

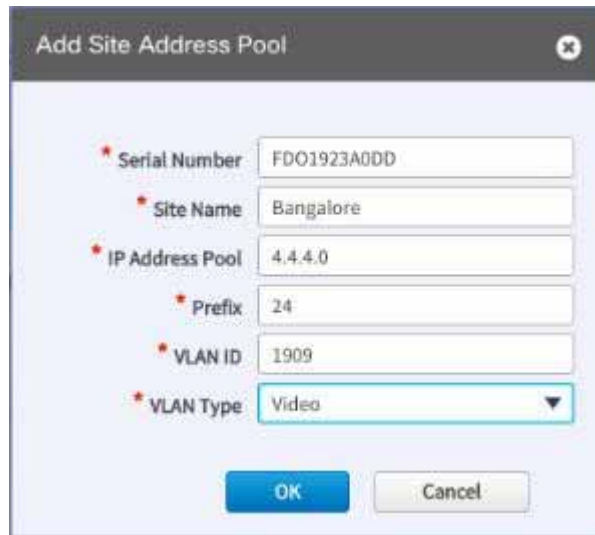
- Step 3** Click **OK**.
- Step 4** Click **Add Address Pool** to enter an IP address along with the suggested or greater prefix. The first range always defaults to the generic IP pool.

Field	Description
IP Address	IP Address for the IP pool. Example: 10.10.10.0

Prefix	CIDR prefix. Example:18
Allocated	Slider bar shows the percentage of the addresses in the pool that has been used by the IWAN application.



Step 5 Click **Site Address Pool** to enter an IP address and prefix based on the suggested sizing for a global LAN IP pool.



Step 6 Repeat this step as required to add additional LAN IP pools.

Field	Description
Serial Number	Serial number. Example: 123456
Site Name	Site name. Example: San Jose.
IP Address Pool	IP addresses for hosts in this VLAN. Example:192.168.99.0/24.
Prefix	Subnet mask for the IP address. Example: 24

VLAN ID	Range of values: 1–4094. Example: 2811. Note You cannot specify 99 as VLAN ID as 99 is assigned to transit VLAN.
VLAN Type	Enter a VLAN type or select a VLAN type from the dropdown menu. Values: Data, Guest, Voice and Video, Wireless.

The following restrictions apply when you enter a VLAN Type of your choice:

- The VLAN type value should not be more than 200 characters in length.
- The VLAN type should not include ? character.
- The allowed number of site-specific address pools is 20 entries per site.



Note

If you do not enter the VLAN details, the configuration information is pushed on the physical interface, which is autopopulated when configuring the LAN during branch provisioning. In such cases, the site is assumed to have no VLANs.

Site Details

Site Address Pool						
Serial No	Site Name	IP	Subnet	VLAN	VLAN Type	Action
123456	San Jose	10.0.0.15	16	123	Data	✗
654321	San Jose	10.0.0.89	16	982	Data	✗

365102

Step 7 Optionally, click **Import CSV** or **Export CSV** to import or export profile based content. Use this step if you want quick processing for large number of site definitions.

The global IP pool, site and VLAN definitions can be imported or updated with **Import CSV** option. The global IP pool, site and VLAN definitions that were previously imported via file or defined via the IP Pool Address tab can be exported using **Export CSV** option. The export workflow provides a template for subsequent import requirements. The content is presented in .csv format and the default exported file name is Controller_Profile_DD-MM-YYYY.csv. These workflows support preprovisioning, scalable site definitions and specific VLAN & IP pool needs.

Step 8 Optionally, click **Export Allocated Addresses** to get a view of the actual usage of IP addresses in the controller on a per site or function basis.

This option provides insight for visibility, DHCP or debugging needs. The content is presented in .csv format and default exported file name is Controller_IP_Allocation_DD-MM-YYYY.csv.

Step 9 Click **Save and Continue** to accept the changes and proceed to the next tab.

Where to Go Next

Select the “Service Providers” tab.

Service Providers

Select the “Service Providers” tab to the type of links and the number of service providers. You can specify up to four links and four service providers. Of the four links, one link can be metered and public. You specify the gateway, interface details for the link in the **IWAN Aggregation Site** tab. After the hub and branches are configured, each link can be associated with a path preference when defining the application policies. For more information, see [“Define Application Policy” section on page 6-4](#).

Field	Description
WAN Label	WAN transport type. This should not be more than seven characters. Example: MPLS.
WAN Type	Two values: Private (MPLS) or Public (Internet).
Metered	Check this option for metered WAN. Leave unchecked for nonmetered WAN. Note One link can only be metered and the metered link is permitted on a public cloud.

Configure Service Providers

WAN Label	WAN Type	Metered	
INET	Public ▼	<input type="checkbox"/>	–
MPLS	Private ▼	<input type="checkbox"/>	–
INET2	Public ▼	<input type="checkbox"/>	– +

Available QoS models for Service Providers

Profile Name	Class Model	
Default 8-Class Model	8 Class	+ +
Default 6-Class Model	6 Class	+ +
Default 5-Class Model	5 Class	+ +
Default 4-Class Model	4 Class	+ +

365519

For MPLS facing WAN interface, a set of predefined Service Provider (SP) profiles are available. Select the profile that most closely matches the SP Service Level Agreement (SLA) for the branch sites. Egress QoS queuing will be applied on the WAN egress to fulfill the SP SLA.

Field	Description
Profile Name	Service provider profile or QoS model. Available service provider profiles/QoS models: Default 4-Class Model Default 5-Class Model Default 6-Class Model Default 8-Class Model
Class Model	Service provider's class model. Example: 4 Class

After you select a profile, the profile details appear in the right hand side of the window.

Example

In this example, for the 8 Class Model, 20% of the bandwidth is assigned to the Voice class, with the remaining bandwidth allocated as shown for the remaining classes.

8 Class Model				
Class Name	DSCP	Priority Class	SLA	
			(%) Bandwidth	(%) Remaining Bandwidth
VOICE	EF	<input checked="" type="checkbox"/>	20	
STREAMING-VIDEO	AF31			10
NET CTRL-MGMT	CS6			5
CALL-SIGNALING	AF41			4
SCAVENGER	CS1			1
INTERACTIVE-VIDEO	AF41			30
DEFAULT	0			25
CRITICAL-DATA	AF21			25

[Hide advanced](#)

365097

The following fields are shown for each class of data within a profile.

Field	Description
Class Name	Data class. Example: VOICE, CLASS1 DATA.
SLA	Service level agreement offered by a service provider for a class within this class model, expressed as a bandwidth value. Shows two parameters: “% Bandwidth” or “% Remaining Bandwidth

Click **Show Advanced**—shows the DSCP values for each class, and which of the classes is a priority class.

To add a new service profile, based on an existing service provider profile, click on the icon next to a class name. The Add Service Profile dialog box appears.

For the new service profile enter a value for Profile Name and click **Save**.

Click **Save and Continue** to proceed to the next tab.

Where to go Next

Select the “IWAN Aggregation Site” tab. See [IWAN Aggregation Site, page 4-11](#).

IWAN Aggregation Site

Select the “IWAN Aggregation Site” tab to configure the hub routers with their respective WAN clouds. A default hub aggregation side with two datacenters, routers and service providers is provided. You can add datacenters, routers, and service providers as required for your network. You can create a link by clicking on a router and dragging to a cloud or vice versa. You can also delete the datacenters, routers, service providers, and links if they are not required by hovering on the network, router or link and clicking “X.”

You can add up to two datacenters and add or delete a device or a link after the hub is provisioned. You can only modify the datacenter settings and devices before you click Apply Changes for the new datacenter that was added.

Coexistence of IWAN Sites and Non-IWAN Sites

This feature allows communication between non-IWAN sites with the newly enabled IWAN POP (Hub) and spoke sites for staged migration of network. The advantages of this feature are as follows:

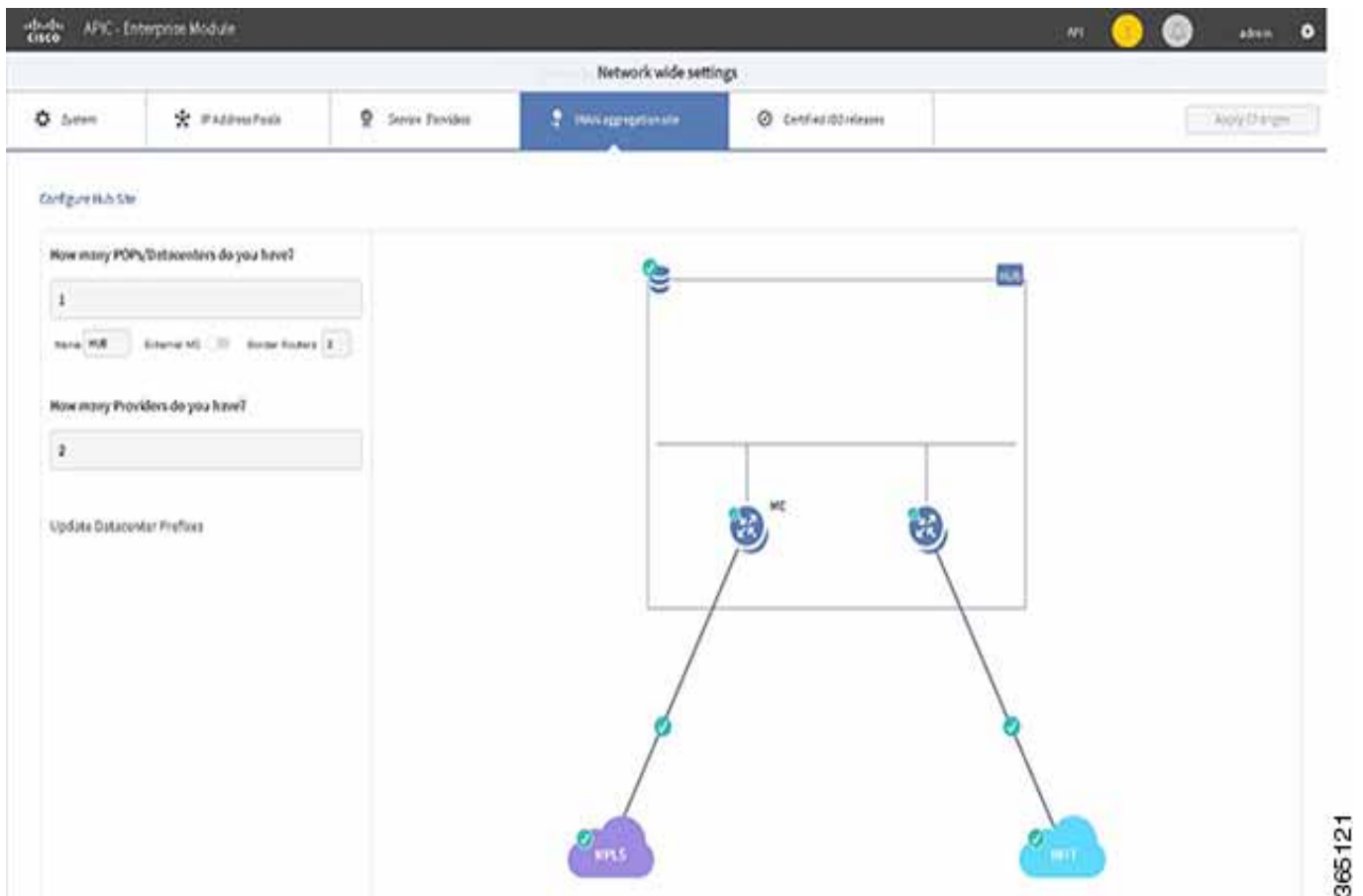
- Deploy IWAN on a few sites prior to full scale deployment
- Non-IWAN sites continue to communicate with hub and spoke routers that are IWAN enabled and vice-versa

Prerequisites for Enabling Support of Non IWAN Sites side-by-side with IWAN solution

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

- Define Cisco IWAN hub 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 App workflows).
- On the existing MPLS-CE router:
 - The loopback IP on the IWAN MPLS border router must be advertised via 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, the multilink network can have two datacenters and each datacenter can have up to four devices with four links.

Heterogeneous WAN Sites

Effective with Cisco IWAN Release 2.0.0, you can perform the following for a provisioned site:

- Add WAN clouds and service providers in any order

- Add up to two MPLS or Internet links. The new links will not affect the existing device priority nor change the path preference.
- Connect hub devices to different service providers. Each device will be connected to only one service provider. Some branches can have a different set of paths than other branches.

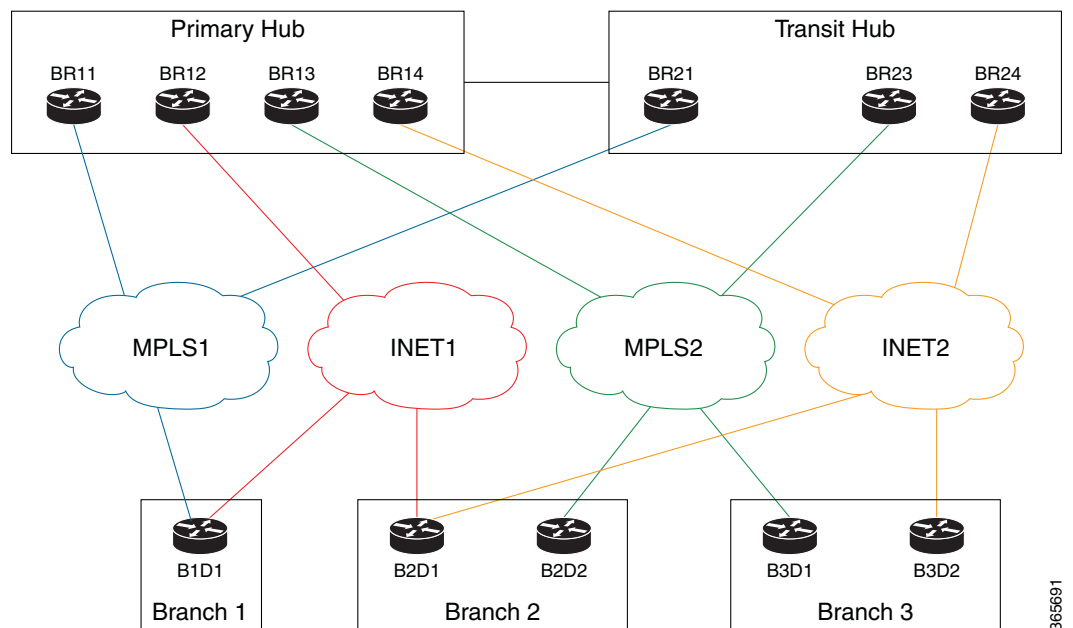


Note

The above changes cannot be performed when provisioning the site.

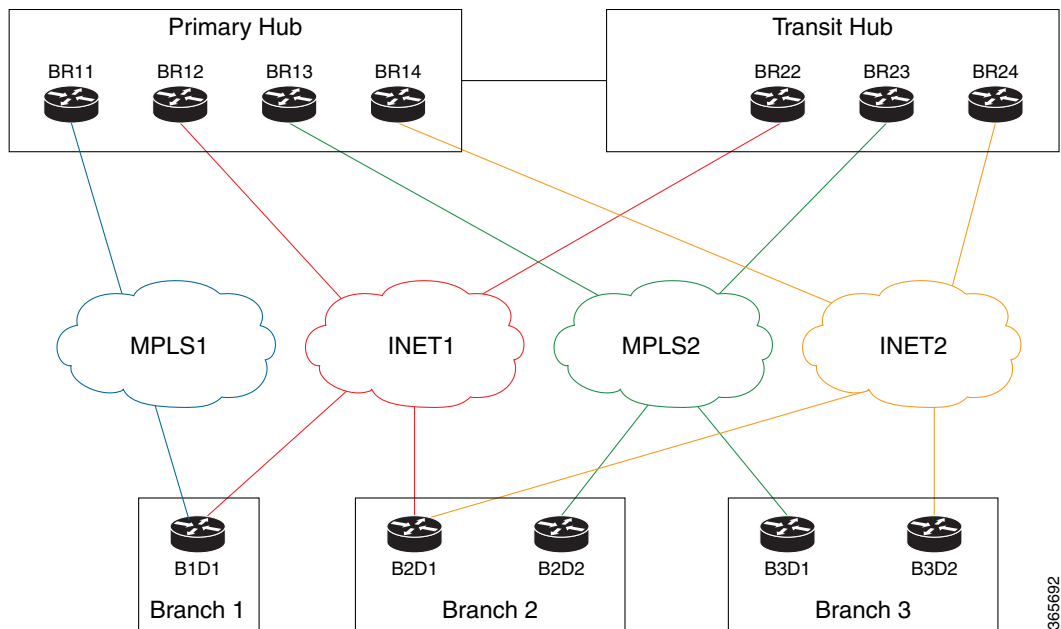
The following figure provides an example of heterogeneous topology with a primary hub, transit hub and different type of links (MPLS and Internet) to connect to the branch routers between the primary and transit hubs. In this topology, the transit hub is not connected to the primary hub.

Figure 4-1 Transit Hub Connected to MPLS Link365591



The following figure provides an example of heterogeneous topology with a primary hub, transit hub and different type of links (MPLS and Internet) to connect to the branch routers between the primary and transit hubs. In this topology, the transit hub is not connected to the primary hub.

Figure 4-2 Transit Hub Connected to Internet Link



Perform the following steps in the **IWAN Aggregation Site**:

-
- Step 1** Select the **IWAN Aggregation site** tab.
 - Step 2** Review the default topology. If you would like to enhance the topology by adding additional datacenters and links.
 - Step 3** Click **Add POP** to add an additional datacenter. A transit hub is added.



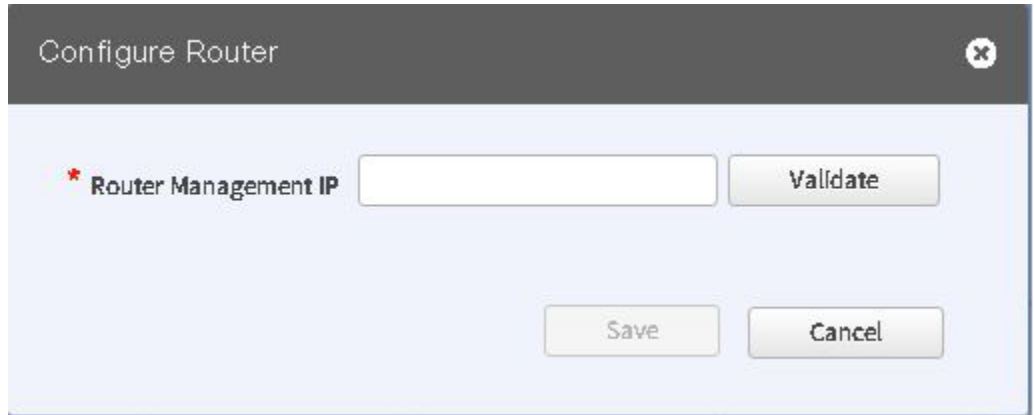
Note You can specify two datacenters (hub sites) only during provisioning. You can add or delete datacenters after hub provisioning. Therefore, if you choose one datacenter when configuring the hub, you can add another datacenter later. Similarly, if you added two datacenters when configuring the hub, you can delete the datacenter.

- Step 4** Optionally, you can rename the datacenter to name of your choice by selecting on the default datacenter name (TRANSIT-HUB-1).
- Step 5** Click **Add Border Router** to add border routers. You can also choose to add the border router to the hubs displayed on the page.

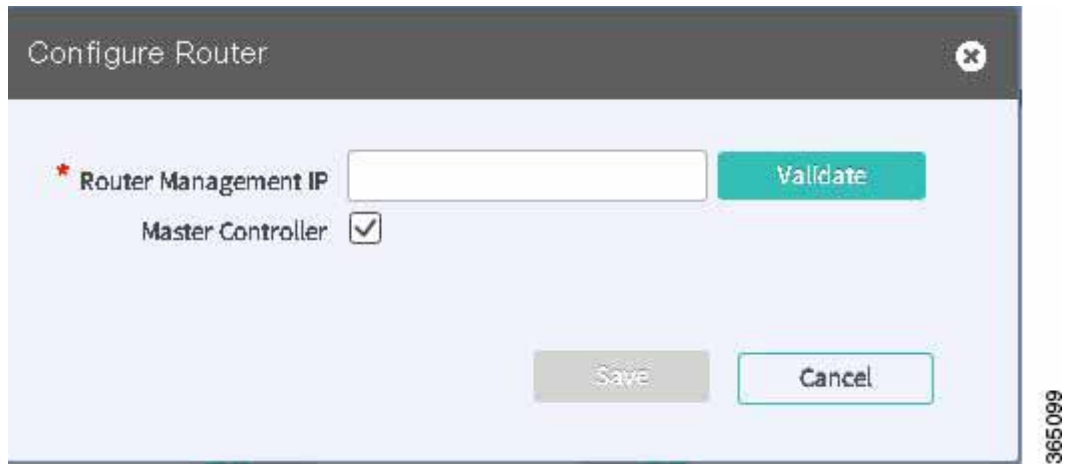


Note The Multilink feature allows you to add up to four border routers and connect the border routers via four links to the different service providers. You can also delete devices either from this page when provisioning the hub via the “IWAN Aggregation Site” tab or when provisioning the branch via the “Select Topology” tab.

- Step 6** Optionally, you can toggle **Yes** or **No** to assign the hub as an External MC.
- Step 7** Click “+” on the hub router. The **Configure Router** dialog box appears.
If you selected **Yes** for **External MC**, the following dialog appears.



If you selected **No** for **External MC**, the following dialog appears.



Field	Description
Router Management IP	Specify the management IP Address for the hub router. Example: 10.0.0.10
Default Gateway	Specify the default gateway. Example: 10.0.0.100
Master Controller	Designates the hub router as the master controller Note This field appears only if External MC is toggled No.

Step 8 Click **Validate**. The **Configure Router** dialog appears.



Note If the hub is not present in the inventory, proceed further, else proceed to step 12.

Configure Router ✕

* Router Management IP

Master Controller

▼ SNMP

* Version

* Read Community

Write Community

▶ SNMP Retries and Timeout

▼ SSH/Telnet

* Protocol

* Username

* Password

* Enable Password

* Timeout (secs)

365087

Field	Description
Router Management IP	IP address selected in step 1 above.
Master Controller	The check box checked in step 2 above, if this hub router is the master controller.
SNMP	
Version	Example: V2C.
Read Community	Example: Public.
Write Community	Example: Private.
SNMP Retries and Timeout	
Retries	Default: 3.
Timeout (secs)	Default: 10.
SSH Telnet	
Protocol	Example: ssh2.
Username	Example: admin.
Password	Example: pwordstrong.
Enable Password	Example: cisco.
Timeout (secs)	Example: 10.

The above credentials need to be entered only one time. The values are populated for the remaining hub devices in the system.

If you choose to populate values for the SSH Telnet, you must configure the following commands on the device:

ip domain name *name*

crypto key generate rsa modulus *modulus-size*. The modulus range is from 360 to 4096.

ip ssh version 2

You must retrieve the generated RSA key pair by using the **show crypto key mypubkey rsa** command to run the **ip ssh rsa keypair-name** *keypair-name* command with the retrieved key pair name. This forces SSH to use the generated RSA keypair for SSH.

Step 9 Click Add Device.

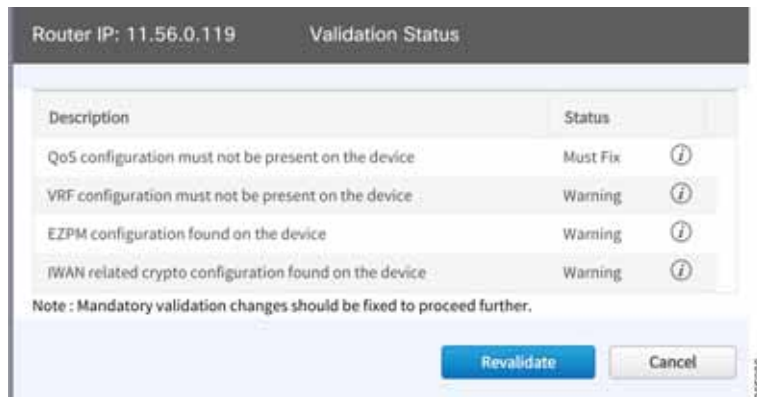
The device is verified in the background if the device is suitable for provisioning, and if there are errors or warnings, the **Validation Status** dialog appears displaying the validation errors or warnings. When the device is validated and ready for configuration, an orange icon with dotted lines appears.



This step is called Brownfield Validation, which indicates validation issues and the Validation Status dialog appears.

Step 10 Do one of the following:

- If the validation messages are warnings, you can choose **Ignore** or fix them.

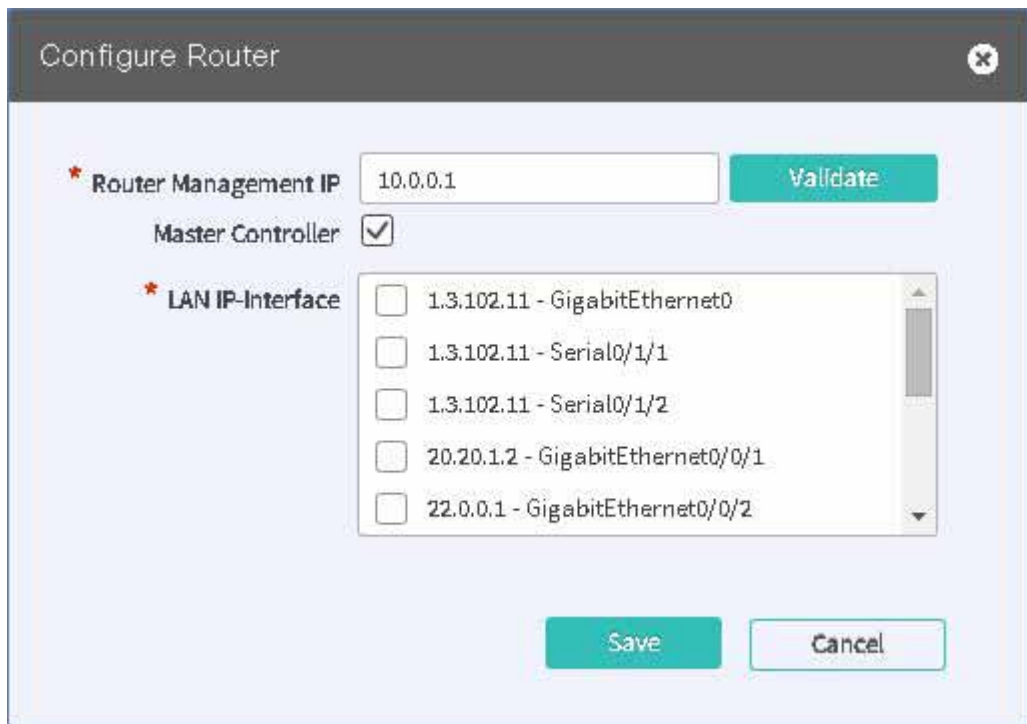


- If the messages are errors, select **Cancel**.

You must fix them via command line interface navigating to the router before proceeding further and follow from steps 5 to 7 and select **Revalidate**. For explanation about messages displayed in the Validation Status dialog, see [Appendix A, “Brownfield Validation Messages Description.”](#)

Step 11 The hub router is added to the inventory and the **Configure Router** dialog appears.

Step 12 Choose the LAN IP-Interface.



Step 13 Configure the other hub routers in a similar method.

Step 14 Click on the link to configure and specify the link in the **Configure Link** dialog box.

The following and the subsequent dialog appear depending on the WAN type that you specified while configuring the type in the **Service Provider** tab for a public and private link respectively.



Note Effective with Cisco IWAN Release 1.1, you can specify static IP addresses for DHCP links.

Perform this step for each link in the network.

Step 15 Select **Enable Non IWAN Sites** to enable communication between IWAN and non-IWAN sites to leverage the coexistence feature, as part of the MPLS configure link..

Step 16 Choose the loopback IP address in the **Loopback IP-Interface** drop down list.

Select the preprovisioned loopback interface from the dropdown list. This enables Cisco IWAN App to form a route of existing sites with new IWAN sites

**Note**

The loopback interface must already be configured on the MPLS router. The loopback interface is required to support co-existence between IWAN and non-IWAN sites and the loopback interface must be configured before adding the device to APIC-EM. It is recommended that you specify a loopback IP address in the same subnet as the WAN interface.

- Step 17** Click **Save**.
- Step 18** Click on the cloud, in this case, MPLS or Internet (Inet), to configure the WAN clouds via the **Configure Provider** dialog box.

The screenshot shows the 'Configure Provider' dialog box with the following configuration:

- WAN Type:** Private
- WAN Label:** MPLS
- Service Profile:** Default 8-Class Model

Buttons: Save, Cancel

365124

- Step 19** Click **Save** to add the device.

Where to go Next

Configure the LAN settings for the data center. See [Configure LAN Settings for the Data Center, page 4-20](#).

Configure LAN Settings for the Data Center

Perform this step to populate WAN subnets in LAN routing.

- Step 1** To configure LAN settings for a data center, click “+” next to “Configure LAN Settings, Datacenter”. The **Configure LAN** dialog appears.

The values for the fields (mentioned in the table below) **Routing Protocol**, **AS Number**, and **Datacenter Prefix** are collected from the devices and autopopulated 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 device, but it is not recommended that you do so. If your LAN routing protocol is BGP, and there are no matching AS numbers, the AS number field is grayed out and you must manually modify the LAN side routing in the device. This release does not support BGP with different AS numbers.

Step 2 Click **Save**.

Field	Description
Routing Protocol	This is the default routing protocol running on the hub routers. Example: EIGRP, OSPF, BGP
AS Number	AS Number or area number, depending on the routing protocol. Example: 5
Datacenter Prefix	IP address range for the data center, addresses behind the hub, specified as a prefix. Example: 10.3.0.3 / 8

If you select BGP as your routing protocol, you must select Advanced Setting to specify the IP addresses. This is not required if your routing protocol is EIGRP or OSPF.

Where to go Next

After specifying the DC LAN and WAN settings, click **Save & Continue** or select the “Certified IOS Releases” tab.

Configure Master Controller

To configure management controller settings, click “+” next to “Configure External Master Controller”. This is required if your topology uses external master controller.

**Note**

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.

In the **Router Management IP** textbox, enter the management IP address of the hub router and click **Validate**.

Enter values in the following fields and click **Save**.

Field	Description
Router Management IP	IP address selected above.
<i>SNMP</i>	
Version	Example: V2C.
Read Community	Example: Public.
Write Community	Example: Private.
<i>SNMP Retries and Timeout</i>	
Retries	Default: 3.
Timeout (secs)	Default: 10.
<i>SSH Telnet</i>	
Protocol	Example: ssh2.
Username	Example: admin.
Password	Example: pwordstrong.
Enable Password	Example: cisco.
Timeout (secs)	Example: 10.



Set Up Branch Sites

After specifying the settings in previous sections [Configure Hub Site and Settings, page 4-1](#), select “Set up Branch Sites” to provision the branch sites.

The Provisioning Site window appears.

- [Bootstrap, page 5-1](#)
- [Sites, page 5-1](#)
- [Devices, page 5-1](#)

Bootstrap

Select a bootstrap file to download. You can use this bootstrap file on each branch router for the MPLS interface WAN. Also see “PnP Bootstrapping” in the Release Notes for IWAN on APIC-EM (See Related Documentation).

Sites

The site host names determine the nearest city to the router and uses this as the basis for the name as well as additional information such as the router model and a suffix number. For example, “San Jose_4431_1”. To change the site name, see [Edit site name and location, page 5-3](#).

Devices

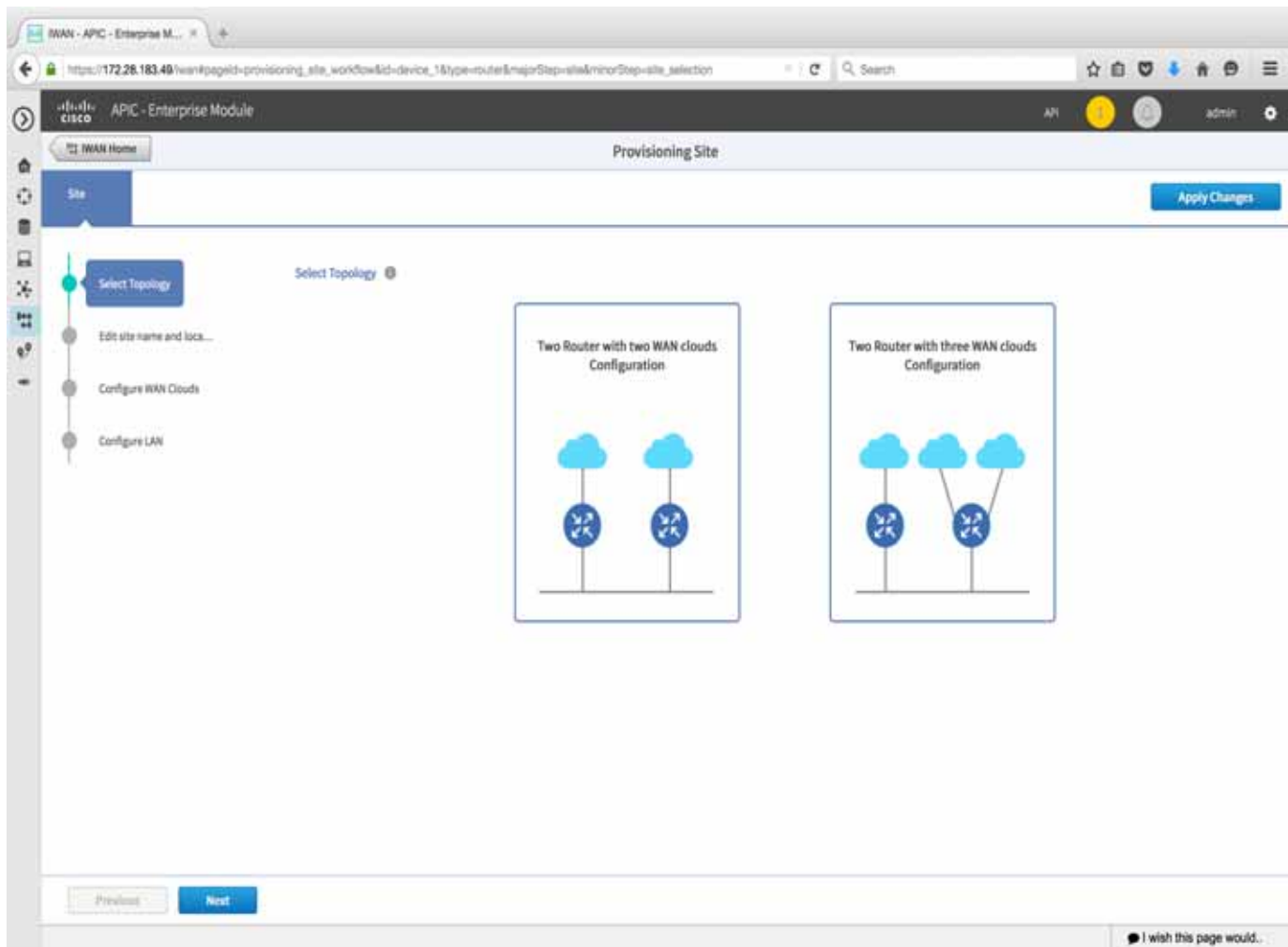
1. Select **Devices** to show a list of devices with serial number, type (e.g Cisco ISR 4451), site name (e.g San Jose).
2. Select devices that you want to provision for a site. (these could include the unclaimed devices)
Note If two devices are selected, they must be from the same site.
3. Click **Provision Site**.

Next, to provision the site, follow the tasks shown on the left side of the window, starting with “Select Topology” and ending with “Site Summary”.

- [Select Topology, page 5-2](#)
- [Edit site name and location, page 5-3](#)

- [Configure WAN Clouds, page 5-3](#)
- [Configure LAN, page 5-5](#)
- [Site Summary, page 5-6](#)

Select Topology



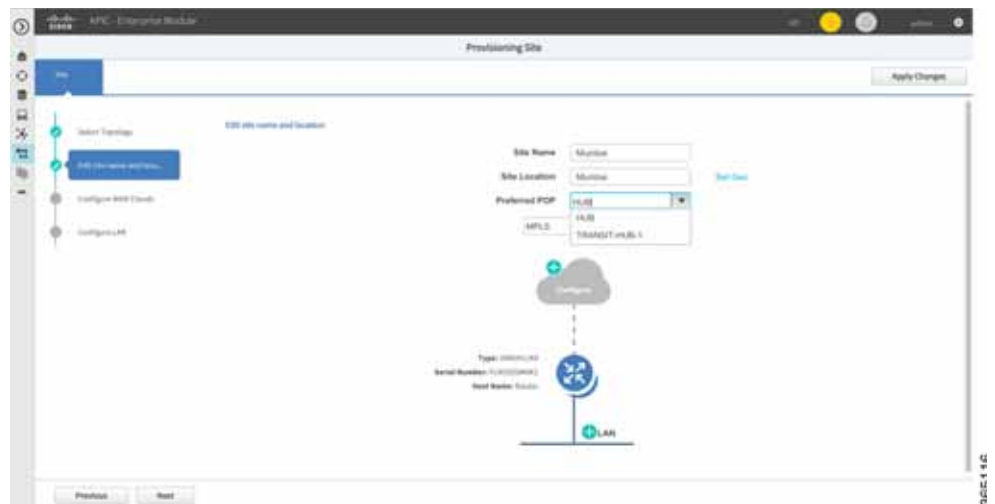
Select one of the WAN topologies that are shown in the window.



Note

The Two Router Configuration option only appears if two devices were selected previously—see [Devices, page 5-1](#) above.

Edit site name and location



Field	Description
Site Name	Preset site name. Change the name if required.
Site Location	Preset location. Click Set Geo to specify the site location on a map.
Preferred POP	Select the preferred datacenter specified in the IWAN Aggregation Site .

Click “+” next to the WAN cloud of a router and select the WAN links defined for provisioning the hub.

Click **Next** or “Configure WAN Clouds” tab.

See [Configure WAN Clouds, page 5-3](#).

Configure WAN Clouds

To configure the settings of a WAN network, click “+” of a router next to a cloud.

Configure each WAN cloud shown in the topology diagram.

1. In the text box on the left hand side, select either “inet”(Internet) or “mpls”.
2. Click “+” adjacent to the WAN cloud.

The Configure WAN Cloud dialog box appears. The fields in the dialog box are different depending on whether the WAN uses an internet or MPLS link.

- [Configure Internet WAN Cloud, page 5-4](#)
- [Configure MPLS WAN Cloud, page 5-4](#)

After entering fields for either Internet or MPLS WAN cloud, click **Next** or “Configure Lan” tab.

See [Configure LAN, page 5-5](#).

Configure Internet WAN Cloud

For an Internet WAN cloud, a dialog box opens with the following fields.

The values for WAN Label and WAN Type fields are populated as specified in **Service Provider** tab when configuring the hub.

Field	Description
WAN Type	“Public” or “Private” appears depending on the option selected while configuring Service Providers in the Service Providers, page 4-9 task.
Interface Type	Type of interface. Values: T1, E1 or Ethernet.
Interface	Select an interface from the drop-down menu. Example: FastEthernet0/0/0
Connect to WAN	Connection method.
Upload (Mbps)	Upload bandwidth (in Mbps). Example: 25.
Download (Mbps)	Select a download bandwidth (in Mbps) from the drop-down menu. Example: 300.

Configure MPLS WAN Cloud

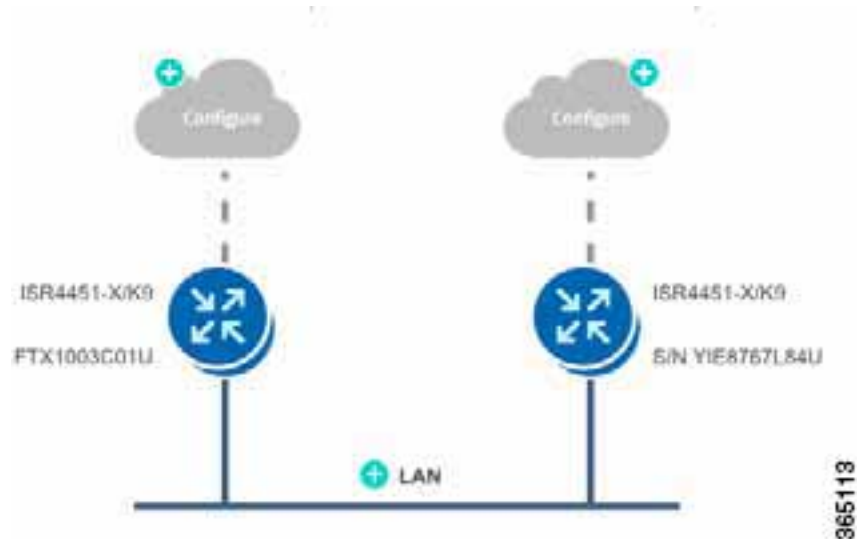
For an MPLS WAN cloud, a dialog box opens with the following fields.

The values for WAN Label and WAN Type fields are populated as specified in **Service Provider** tab when configuring the hub.

Field	Description
WAN Type	“Public” or “Private” appears depending on the option selected while configuring Service Providers in the Service Providers, page 4-9 task.
Interface Type	Type of interface. Values: T1, E1 or Ethernet.
Interface	Select an interface from the drop-down menu. The information in this field is autopopulated from the interface selected while configuring the hub. Example: FastEthernet0/0/0
Connect to WAN	Connection method.
CE IP Address	Customer Edge Server IP Address. The value for this field is autopopulated with IP if you specified static IP addresses while configuring the hub. Note You may need to specify additional IP addresses for the CE devices, depending on the number of links that you created when setting up the hub sites in the IWAN Aggregation Site, page 4-11 task.
PE IP Address	Provider Edge Server IP Address. The value for this field is autopopulated with IP if you specified static IP addresses while configuring the hub.

Download and Upload (Mbps)	Select a bandwidth for upload and download (in Mbps) from the drop-down menu. Example: 100.
Service Provider	Select a Service Provider Model or QoS Model from the drop-down menu. Example: Default 6-Class Model

Configure LAN



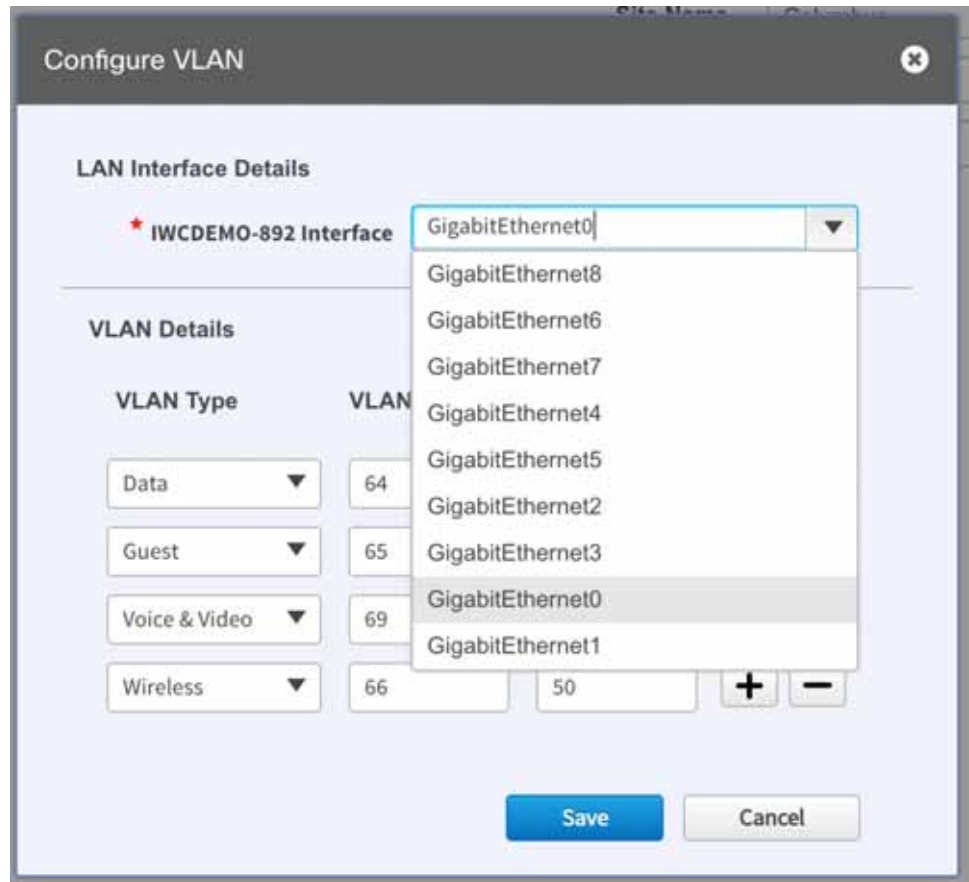
Next to the LAN, under the router, click “+” to specify the LAN attributes. If site specific IP pools are configured for this site, the **Configure VLAN** dialog displays the predefined VLANs for confirmation purposes only. You cannot edit or modify the fields in the dialog.

Cisco IWAN App provides the flexibility to bring up the IWAN on available interfaces thereby adapting to existing customer networks without any changes. You can choose any interface available on the spoke devices as the LAN interface. The available interfaces are fetched from the device and autopopulated in **Configure LAN** dialog and you can select a LAN interface when configuring the branches. You can choose any kind of interface available on your network.



Note

If a switchport interface is chosen as a LAN interface, the interface will be configured as trunk and VLANs and interface VLANs will be created.



Field	Description
VLAN Type	Enter a VLAN type or select a VLAN type from the dropdown menu. Values: Data, Guest, Voice and Video, Wireless.
VLAN ID	Range of values: 1–4094. Example: 2811.
Total IPs	Number of chosen IP addresses for hosts in this VLAN. Example: 120.

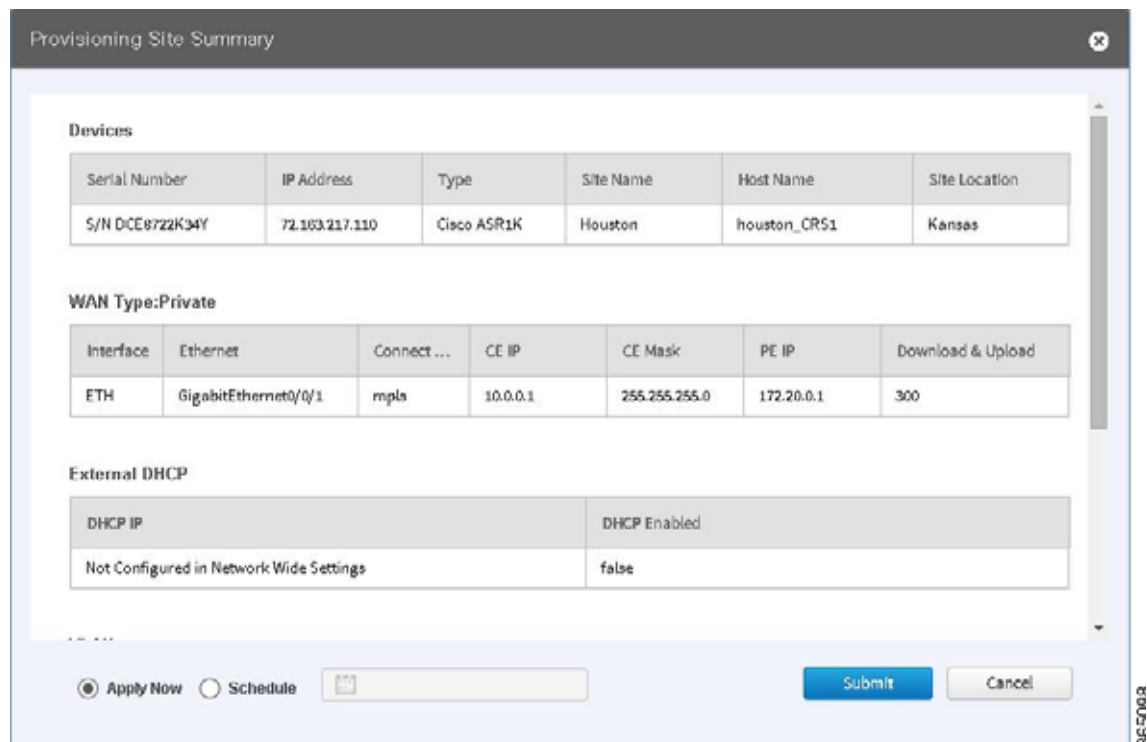
Click “+” of the lowest VLAN to add another VLAN entry in the list. After all VLANs are configured, click **Save**.

Site Summary

A site summary such as the one shown in the following example, appears.



Click **Apply Changes** to complete provisioning of the site. The Provisioning Site Summary dialog appears.



You can either select **Apply Now** or **Schedule** to specify a date and time to apply the site provisioning by clicking **Submit**.



Note

The **Apply Now** 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.



Administering Application Policy and Monitoring Sites

This chapter provides information about administering applications for a site and monitoring the sites.

- [Administering Application Policy, page 6-1](#)
- [Monitoring Sites, page 6-7](#)

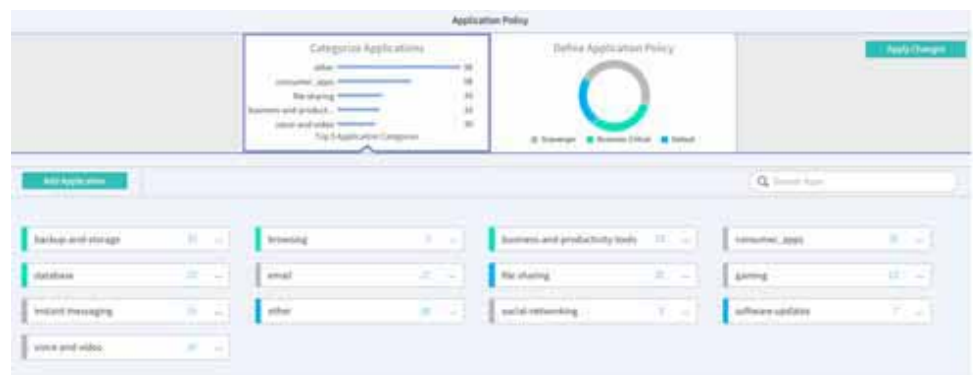
Administering Application Policy

Use the Administer Application Policy menu option to place applications in categories, view and, if required, change the available bandwidth to share bandwidth between applications.

- [Categorize Applications, page 6-1](#)
- [Define Application Policy, page 6-4](#)
- [Bandwidth Usage, page 6-7](#)

Categorize Applications

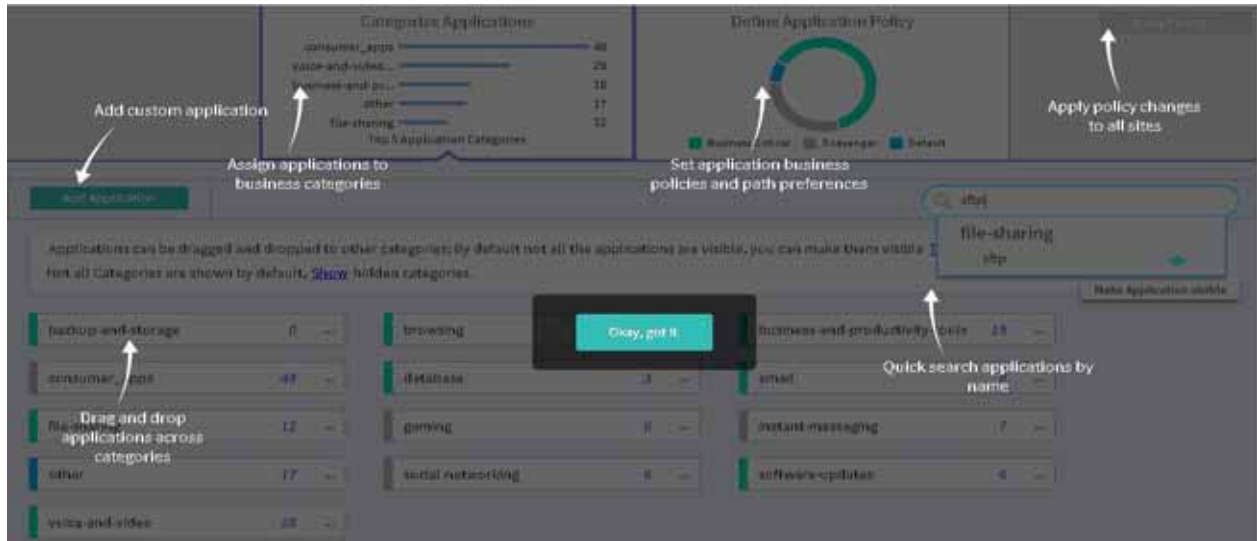
The Categorize Applications window shows application policies and categories to which the applications are assigned. You can use options to change the bandwidth used by applications in the network.



Applications are grouped into categories. To find the category to which an application belongs, enter the application name in the search textbox to the right of the window.

Click a category (for example, backup-and-storage), to see the applications assigned to the category in a drop-down box. The attributes of an application can be edited by clicking the pencil symbol next to the application name in the drop-down box.

You can keep track of application bandwidth usage at each category and move applications between application categories. Categories are grouped into Business Critical, Scavenger and Default groups. The Business Critical group is given the most bandwidth.



Add Application

Click “Add Application” to provide details of a new application and assign it to a category.

Enter values in the following fields:

Field	Description
Name	Name of the application. Example values: Data, Guest, Voice and Video, Wireless.
Type	Application Type. Values: URL, Server IP/Port and DSCP.
Protocol	Protocol used by application. Values: TCP, UDP.
Value	DSCP value if type is DSCP. URL if type is URL. IP address and port if type is Server IP/Port.
Similar to App	Select an application the Jitter, Packet loss and Delay values can be used for this application.
Category	Category where the application will be created.
Jitter	(Optional) Specify a different value or leave the default value as is.
Packet loss	(Optional) Specify a different value or leave the default value as is.
Delay	(Optional) Specify a different value or leave the default value as is.

To define the application policy groups, click “Define Application Policy.”



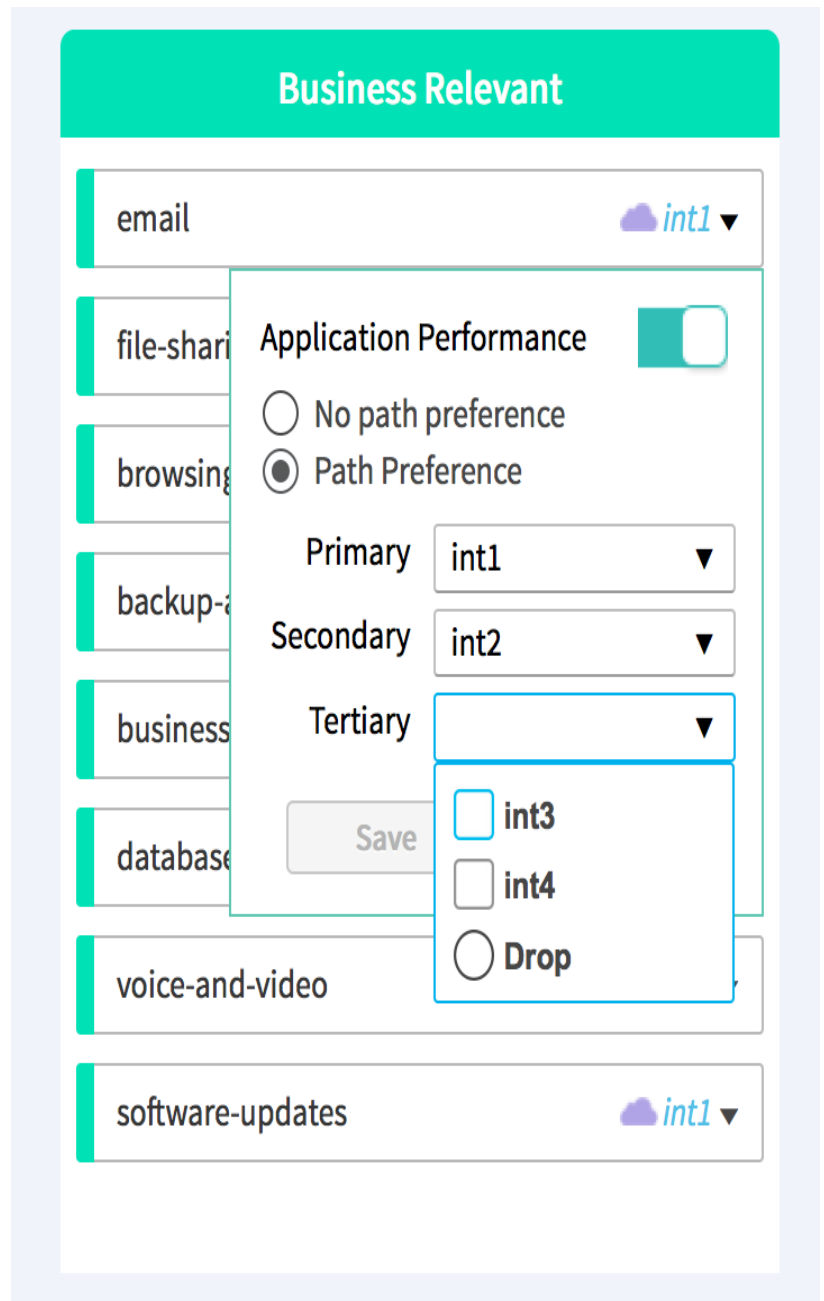
Define Application Policy

Applications are grouped into categories, such as “Voice and Video”. The categories form part of the following business groups: Business Critical, Scavenger and Default.

Change Application Performance

Click on the down arrow next to a category to change the Application Performance in the category to perform the following:

- Enable or disable application performance
- Enable or disable path preference
- Choose primary and secondary path
- Secondary path can be Drop



Select a Path Preference, with Path 1 being the preferred path for traffic in this category. For example, “Int” (Internet).

If you specified metered link as a link type for a service provider, the following dialog appears.

Business Relevant

business-and-prod... MPLS1 ▼

databases

backup-

file-shar

software

email

voice-an

browsing MPLS1 ▼

Application Performance

No path preference
 Path Preference

Primary ▼

Secondary ▼

Tertiary ▼

Last Resort 4G

The metered link is the last resort when the primary, secondary, and tertiary paths are not available. 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.

Move an Application Category

You can drag-and-drop a category from one business group to another; for example, from Default to Scavenger.

Bandwidth Usage

You can view the bandwidth used across various applications in a location by selecting “Bandwidth Usage.” This provides a applications used per location, the bandwidth per Mbps, and the link SLA capacity for each router in a location in pie chart.

Monitoring Sites

In the IWAN Home page, click **Monitoring** to monitor IWAN sites. The sites are displayed on a map, indicating the number of hubs and branches present across the globe for IWAN.

Figure 6-1 Monitoring Sites



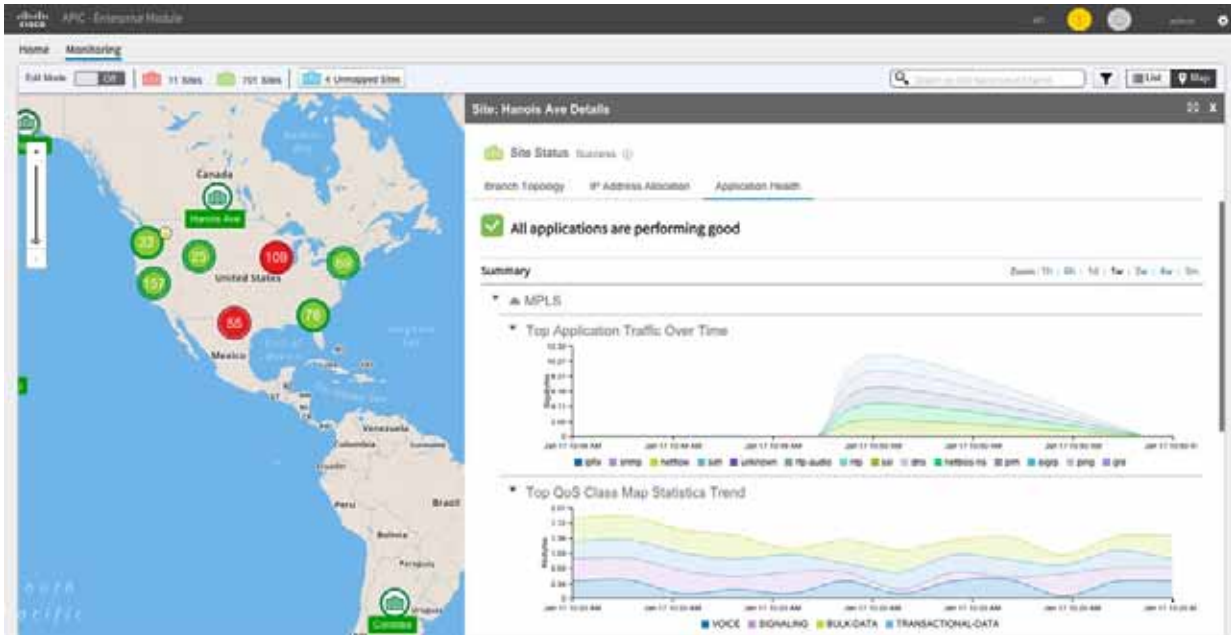
Clicking on a site displays the following (as links):

- Branch Topology
- IP Address Allocation
- Application Health
- Troubleshooting

**Note**

Troubleshooting is displayed on when the system suspects the site to have an issue due to an application or with bandwidth allocation.

Figure 6-2 Application Health

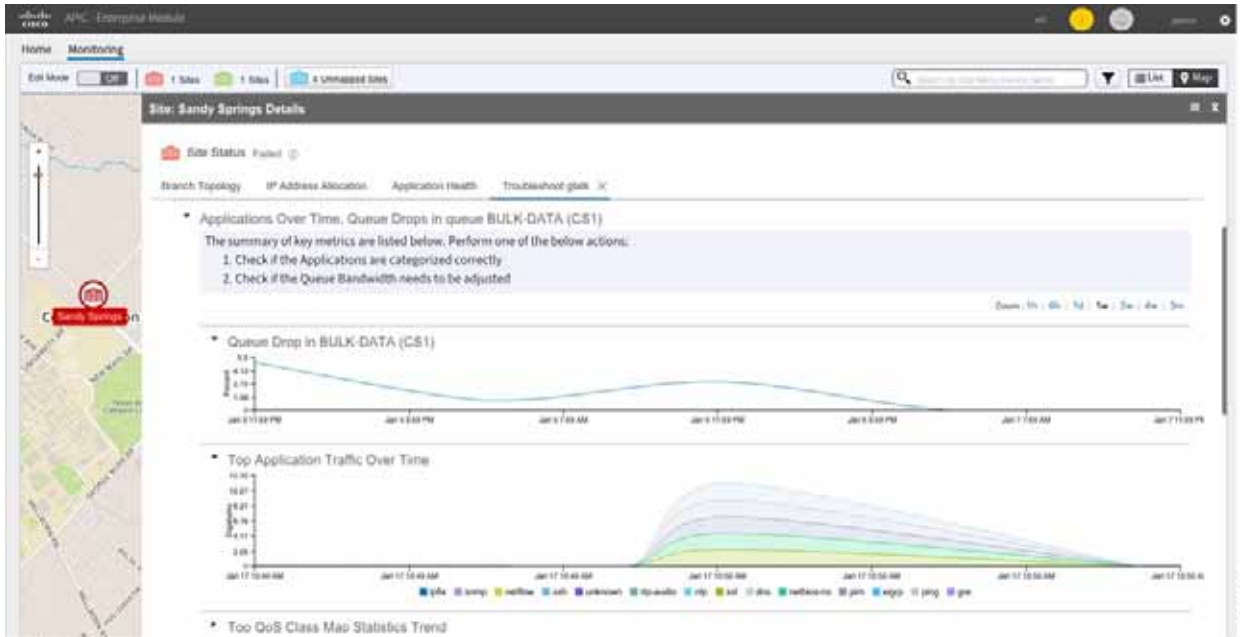


Clicking **Application Health** displays the applications usage on the site in a graphical representation. The graph displays the following:

- Various applications configured for the site
- Bandwidth usage for each application
- Statistical trend for each application

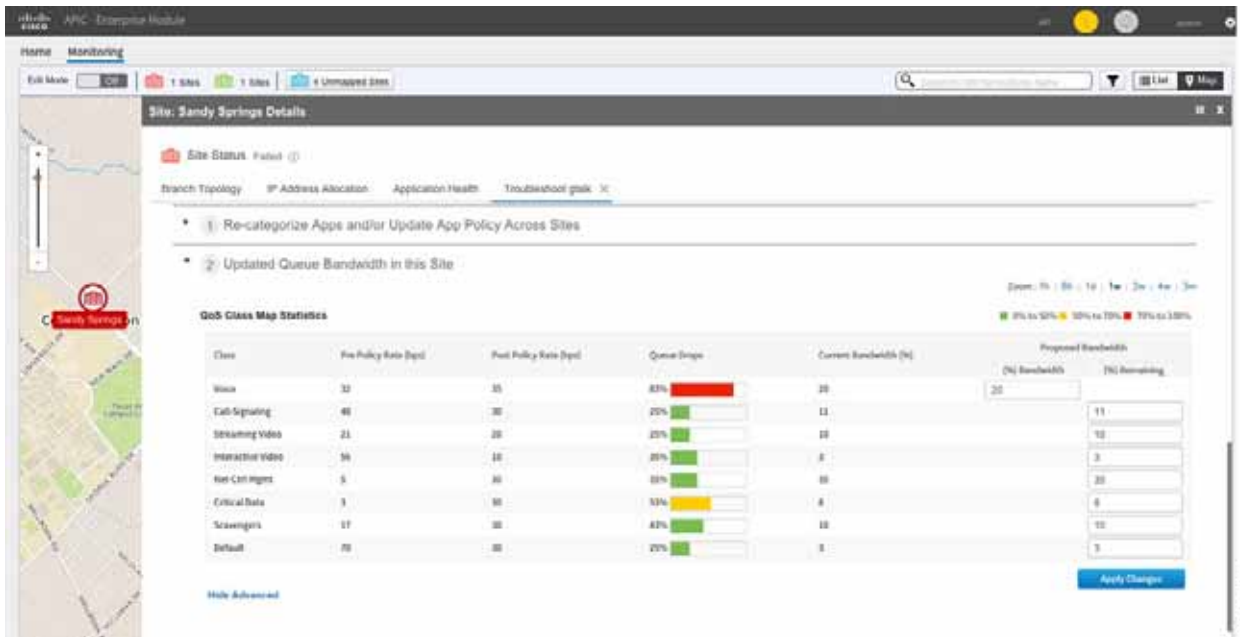
As mentioned, **Troubleshooting** is displayed, when the system detects high usage on a site.

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 provides suggestion in adjusting the bandwidth among the various applications thereby providing more bandwidth to the application causing the issue.

Figure 6-4 Troubleshooting—Healing a site





Backup, Restore, Recovery, and Delete

This chapter provides information about backup, restore, recovery, and delete mechanisms for IWAN on APIC-EM:

- [Backup and Restore for IWAN on APIC-EM, page 7-1](#)
- [Recovery for IWAN Devices, page 7-3](#)
- [Deleting Sites, page 7-4](#)

Backup and Restore for IWAN on APIC-EM

Backup and restore will work in the following scenarios:

- The controller is at stasis with respect to IWAN application business intent. Stasis is the state of the system when IWAN application business intent has succeeded or failed.
- 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 will not work in the following scenarios:

- IWAN application is handling IWAN application business intent, including internal database operations and device policy updates.
- Workflows performed on IWAN application, when backup and restore session is underway, will be lost and cannot be tracked or retrieved later:
 - Sites (one or more devices) are added to IWAN
 - Devices that had their certificates renewed
 - Sites that are deleted from IWAN or have their certificates revoked
 - Configuration or policy updates

Recommendations

Cisco recommends the following for the proper working of backup and restore:

- Run in multi-host mode as far as possible. This enables active HA thereby reducing the backup and recovery windows.
- 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, basically after a stasis period.
- 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 IWAN or have their certificates updated.
- Track devices that are deleted from IWAN or have their certificates revoked.

Caveats and Workarounds

There is a risk in this version of APIC-EM, in which the controller and the network will be out of sync after a restore and consequentially some or all sites may be out of policy (as displayed on the Site Status screen). Some out of policy situations, such as security related issues, may not be detected.

For workflows mentioned above, the following workarounds is recommended:

Sites (one or more devices) are added to IWAN

Remove the PKI trustpoint and zero-out the keys on each device. Use the following commands to clear trustpoints and certificates on each device:

```
no crypto pki trustpoint sdn-network-infra-iwan
crypto key zeroize rsa sdn-network-infra-iwan
```

Restart the plug and play (PnP) workflow to allow the device to show as an unclaimed device in the IWAN application. If the device is already added as an IWAN site, copy the startup configuration to the running configuration and reload the router on each affected router. Following, this, the PnP call home workflow takes over and the device shows up as an unclaimed device in the IWAN workflow. The IWAN site provisioning must be reapplied. Repeat the IWAN site creation workflow.

Device that had their certificate renewed

Remove the PKI trustpoint and zero-out the keys on each device . Use the following commands to clear trustpoints and certificates on each device:

```
no crypto pki trustpoint sdn-network-infra-iwan
crypto key zeroize rsa sdn-network-infra-iwan
```

Repeat the IWAN site creation workflow for the device or set of devices.



Note

When a device is provisioned by IWAN, 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 will automatically attempt to renew this certificate. As it is difficult to track devices and their certificate status, Cisco will provide an API, to determine devices with expired client ID certificates or devices with client ID certificates that will expire soon. If devices renew certificates between a backup and a restore, the database certificate displays that the device has not been renewed after completion of the restore session. These API's will provide a method to determine the devices that need to renew certificates or reprovision the expiring or expired client ID certificates respectively. After a device's client ID certificate has expired, the only option is to reprovision it.

Sites that are deleted from IWAN or have their certificates revoked

Revoke the certificate for each device via the controller user interface. If the site is a part of the IWAN network, the **Site Delete** button can be used to revoke the certificate and clear the IWAN application for that site.

Configuration or policy updates

Cisco IWAN Application can detect changes on devices that are in conflict with the controller. If updates made to a site between a backup and a restore, the site is removed from the policy. It is recommended 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 policy from the sites unless the manual changes are successful.

**Note**


It is recommended that the audit log entries for adding and deleting devices along with the status of their certificates (revoked or created) be tracked automatically via using an automated script. This script can be useful when restoring a nonstatis system. All audit records are useful in when reapplying the changes lost due to system instability. This automated script must run at regular intervals after backup is complete to prepare the system for restore.

Recovery for IWAN Devices

Use the **Recovery** icon to recover a site after when site provisioning fails. After a attempting to recover a site, if site recovery is a success, the site moves to the Success state, else the **Recovery** icon reappears allowing you to retry recovering the site. An attempt will be made to push the last change that was made.

You can attempt to recover a site multiple times. If site is cannot be recovered the only option is to delete the site.

Recovery Mechanism for Hub and Branch Sites

Step 1 Navigate to the Site Status page and click the **Recovery** icon .

The **Recovery** icon is displayed in the Recovery column.



Health	Site	Devices	Location	Status	Delete Site	Recovery
	HUB	1	Falls Church, United States	SUCCESS	X	

Step 2 If recovery succeeds, you can start provisioning the hub and the **Recover** icon is grayed out until next failure.

Post Provisioning Recovery Mechanisms for Hub and Branch Sites

Post provisioning recovery of the hub and branch sites after the sites have been provisioned allows for the last change set to be reapplied. means retrying the last change set for the hub and spoke devices.

- In case of hub device, recovery can be attempted several times. The **Recovery** button appears on the Main Landing page.
- In case of site device, recovery can be attempted multiple times. The **Recovery** button appears on the Sites Landing page. If recovery fails after multiple attempts, you can choose to delete the site by clicking on the **Delete** icon against the **Site Delete** column to remove site permanently.

Deleting Sites

In addition to recovering hub and branch sites, you can also delete sites in IWAN via the **Delete Site** icon in the Sites Listing page.

Deleting a Hub Site

You can delete a primary hub if the primary hub is in failed state and no branch sites have been provisioned. A primary hub cannot be deleted after branch sites have been provisioned. The **Delete Site** icon is disabled thereby disallowing you to delete the hub. When you delete the primary hub, the transit POP are also deleted. The configuration on the primary hub is reset to brownfield validation state.

When a hub is deleted after hub provisioning fails, IWAN performs the following:

- PKI certificate and trustpoint is revoked
- IP addresses are released to the IP address pool
- Hub is deleted from inventory

If the delete operation succeeds, the primary hub is removed from Site Listings page. You can reprovision the primary hub via the main page as part of the hub provisioning. If the delete operation fails, the following message is displayed and you can reprovision hub again.

```
Unable to revert configuration on devices. Please restore site manually before re-provisioning.
```

Deleting Transit POPs (Datacenters)

You can delete a transit POP (datacenter) irrespective of the datacenter state—provisioned or failed.

When a POP site is deleted, IWAN performs the following:

- Revoke PKI certificate and trustpoint from all devices in pops.
- Release IP addresses to IP address pool.
- Delete POPs from inventory.
- Clean the Network and Wireless Services (NWS) state.

If the delete operation succeeds, the transit pop is removed from IWAN and the devices are cleaned. If the delete operation fails, which might happen when a device is cannot be reached on a network, the following message appears and the states of the pops is deleted. You must reprovision the transit pops.

```
Unable to revert configuration on devices. Please restore site manually before re-provisioning.
```

Deleting Branch Sites

You can delete branch sites from IWAN irrespective of the branch state—provisioned or failed—via the **Delete Site** icon in the Sites Listing page. As a part of the Multilink feature, you can delete branch sites either from the “IWAN Aggregation Site” tab or from the “Select Topology” tab.

**Note**

Deleting branch sites must be performed on a best effort basis when devices cannot be reverted to greenfield validation. After deleting a branch site, the device must be cleaned manually.

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

- The initial configuration is saved to the **bootflash:IWAN_RECOVERY.cfg** file on device.
- The site is recovered to bootstrap configuration by performing the following:
 - Copying the **bootflash:recovery.cfg** file information to startup configuration
 - Reloading the device
- PKI certificate and trustpoint is revoked.
- IP addresses are released to the IP address pool.
- The site information is cleaned in the database.

When the delete operation succeeds, the branch site is removed from the Sites Listing page and is displayed in the unclaimed device list thereby allowing you to reprovision the branch site. If delete fails, the branch site is not added to the unclaimed device list and displays the following message

```
Unable to revert configuration on devices. Please restore site manually before re-provisioning.
```



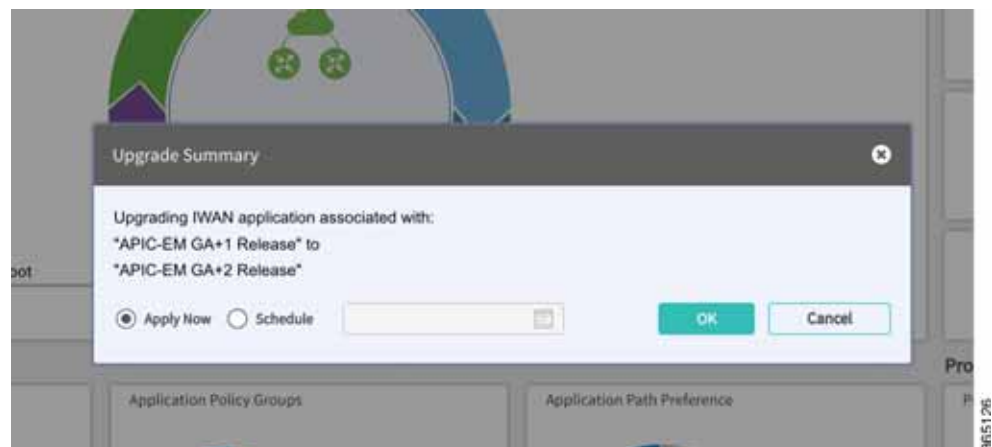

Upgrading IWAN App

This chapter provides information about upgrading IWAN Application:

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

Upgrading IWAN

IWAN application requires an additional network upgrade step when the APIC-EM upgrade process is complete. After the APIC-EM upgrade process is complete—the “reset-grapevine” and the 30-minute wait for inventory resynchronization—the IWAN main landing page will look as shown in the following image.



You need not upgrade IWAN unless you need a new IWAN application workflow or update the network to leverage the new IWAN controller functionality. You can either perform the upgrade immediately or schedule to perform the upgrade in the future, at a convenient time or when the network is down.

To upgrade, click the text **Network upgrade is required to use the IWAN App** in the main landing page. The **Upgrade Summary** window appears.

The upgrade information is sent to all affected sites in the network and will show on the site status screen as a provision in-progress for those sites. Once the upgrade is complete, normal site status will prevail.

After performing the upgrade clear the browser cache. Cisco IWAN App is now ready to accept further input.



Brownfield Validation Messages Description

Error Messages Encountered in Brownfield Validation

The following table provides an explanation of the error messages encountered in Brownfield Validation:

Table A-1 *Error Messages in Brownfield Validation*

Error Messages	Description
Username configuration must have privilege level 15	<p>Configure a user name with privilege 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 neither Performance Routing (PfR) configuration nor PfR related configuration is 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 neither Quality of Service (QoS) configuration nor QoS related configuration is present on the device.</p> <p>Example: <code>no class-map match-any nbar-12-cl#VOICE no policy-map nbar-12-cl# no policy-map IWAN-INTERFACE-SHAPE-ONLY-INTERNET no service-policy input nbar-12-cl# no service-policy output IWAN-INTERFACE-SHAPE-ONLY-INTERNET</code></p>
Interface loopback 47233 must not be configured on the device	<p>Remove loopback 47233 from the device.</p> <p>Example: <code>no interface loopback47233</code></p>

Error Messages	Description
IWAN trustpoint configuration must not be present on device	Remove IWAN trustpoint configuration from the device. Example: <code>no crypto pki trustpoint sdn-network-infra-iwan</code>
VPN routing and forwarding (VRF) configuration must not be present on the device	It is recommended removing existing VRFs as VRFs may interfere with the IWAN configuration. Example: <code>no ip vrf IWAN-TRANSPORT-4</code>

Warning Messages Encountered in Brownfield Validation

The following table provides an explanation of the warning messages encountered in Brownfield Validation:

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 two interfaces are up on the device. Verify using the show ip interface brief command.
IWAN related crypto configuration found on the device	It is recommended removing crypto configuration as crypto configuration might interfere with the IWAN configuration. Example: <code>crypto zeroize mypubkey rsa sdn-network-infra-iwan</code>
Device does not have required license	Required licenses not enabled on 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 for Cisco ASR 1000 Series Aggregation Services Routers.
Device does not have valid image version	Cisco software image available on the device is not the recommended software image for IWAN. Boot the device with software image Cisco IOS Release 15.5(3)S1 or Cisco IOS XE Release 3.16.1 and above.

Warning Messages	Description
No routing protocol found on device	<p>It is recommended enabling one of the following routing protocols on the device.</p> <p>Example:</p> <pre>router ospf AS number router eigrp AS number router bgp AS number</pre> <p>In case of BGP, ensure that there are no conflicting routing protocols are configured on the devices. If no routing protocol is configured, the default IWAN protocol will be configured.</p>
EZPM configuration found on the device	<p>It is recommended to remove Easy Performance Monitor (EZPM) configuration as EZPM configuration may interfere with IWAN configuration.</p> <p>Example:</p> <pre>no class-map match-all Business-Critical-and-default-tcp-only no performance monitor context IWAN-Context profile application-experience</pre>
NBAR configuration found on the device	<p>It is recommended to remove Network Based Application Recognition (NBAR) configuration as NBAR configuration may interfere with 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>Device information for validation failed. Revalidate and if problem persists, ensure the following:</p> <ul style="list-style-type: none"> • Device is up and running. • Device connectivity is be established from the cluster.
Device does not have K9 package in the image	<p>IWAN does not support the Cisco software image loaded on the device. Boot up image with K9 package.</p> <p>Example:</p> <pre>asr1000rp1-adventerprisek9.03.16.00.S.155-3.S-ext.bin</pre>
Device does not have valid image version and K9 package	<p>Boot the device with software image Cisco IOS Release 15.5(3)S1 or Cisco IOS XE Release 3.16.1 and above with K9 package</p>



Related Documentation

See the following documentation related to Cisco IWAN:

Documentation	Description
Cisco IWAN Technology Design Guides	Design guides that describe Cisco Validated Designs for Cisco IWAN. See http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-branch-wan/cvd_ent_wan.html .
Release Notes for Cisco IWAN on APIC-EM	Summary of the features and caveats for Cisco IWAN on APIC-EM.
Release Notes for Cisco IWAN	Summary of the components in the latest release of the Cisco Intelligent Wide Area Network (Cisco IWAN) Solution.
Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module	Description of the features and caveats for the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM).
Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide	Information about the Cisco APIC-EM (rather than the Cisco IWAN application that runs on Cisco APIC-EM). This includes information about deployment, verification, and troubleshooting.
Release Notes for Cisco Prime 3.1	Information about Cisco Prime Infrastructure which can be used to configure Cisco IWAN. Note Cisco IWAN App Release 1.1 supports Cisco Prime Infrastructure Release 3.1 beta version.
Cisco Prime Infrastructure 2.X Deployment Guide	This guide describes how to deploy the Cisco Prime Infrastructure, assuming that the basic wired and wireless network is already deployed.
LiveAction	Documentation on LiveAction software.

