



Cisco IWAN Application on APIC-EM User Guide, Releases 1.5.0, 1.5.1, 1.5.2

September 12, 2017

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.

© 2017 Cisco Systems, Inc. All rights reserved.



Preface vii

About vii

Audience vii

Organization viii

Conventions viii

Related Documentation x

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

New and Changed Information 1-1

New Features and Changed Information 1-1

CHAPTER 2

Overview 2-1

About the Cisco IWAN Application 2-1

Tutorial Videos 2-2

Workflow for Accessing the Cisco IWAN Application 2-2

Accessing the Cisco IWAN Application 2-2

Cisco IWAN Application Home Page 2-4

CHAPTER 3

Deployment 3-1

Cisco IWAN App on APIC-EM 3-1

Considerations Before Using the IWAN App 3-2

Deploying Cisco APIC-EM 3-2

Installing or Upgrading the Cisco IWAN Application 3-2

CHAPTER 4

Managing Hub Sites 4-1

Setting Up a Hub Site 4-1

Configuring System Settings 4-2

Uploading Certified Cisco IOS Software Images for Branch Devices 4-6

Deleting an Uploaded Cisco IOS Software Image 4-8

Configuring Service Providers 4-9

Configuring IP Address Pools 4-12

 Overview of Address Pool Configuration in the IWAN App 4-12

- Configuring Address Pools 4-14
- Configuring the IWAN Aggregation Site 4-17
- Modifying the Configuration of Hub Sites 4-24
- Understanding the Coexistence of IWAN Sites and Non-IWAN Sites 4-25
- Homogeneous and Heterogeneous Topologies 4-25
 - Homogeneous Topology 4-25
 - Heterogeneous Topology 4-26
- Understanding IP Address Pools 4-27
- Configuring Multi-tunnel Termination (MTT) 4-28
 - Day 0 Multiple WAN Link Configuration: Features, Limitations, Procedure 4-28
 - Day N Multiple WAN Link Configuration: Features, Limitations, Procedure 4-31
- Updating the WAN Bandwidth of a Provisioned Hub Site 4-33
- Modifying the QoS Bandwidth Percentages for a Hub Site 4-34
- Modifying the QoS Bandwidth Percentages for a Service Profile 4-35
- Deleting a User-defined QoS Bandwidth Service Profile 4-36
- Setting the Geographic Location of a Hub Site 4-37
- Collecting Network Data Using LiveAction 4-37
 - Configuring LiveAction 4-38

CHAPTER 5

Managing Branch Sites 5-1

- Overview 5-1
 - IWAN App Operation with NAT 5-2
- Workflow for Managing Branch Sites 5-4
- Bootstrapping Greenfield Devices 5-4
- Adding and Provisioning Greenfield Devices to the Branch Site 5-5
- Adding and Provisioning Brownfield Devices to the Branch Site 5-10
- Viewing Site Status Information 5-22
- Support for 4G/Cellular Technology for WAN Link 5-23
 - Example Scenario 5-23
 - Notes and Limitations 5-25
- 4G-Cellular Support for MPLS Cloud 5-25
- Updating the WAN Bandwidth of a Provisioned Branch Site 5-26
- Updating the WAN IP Parameters of a Provisioned Branch Site 5-27
- Modifying the QoS Bandwidth Percentages for a Branch Site 5-29

CHAPTER 6

Managing Devices 6-1

- Overview 6-1

Custom Configuration of Devices	6-1
Custom Configuration Default Templates	6-2
Enabling Custom Configuration	6-3
Creating and Executing a Custom Configuration	6-3
Viewing Status of Custom Configuration Execution	6-4
Handling Failed Custom Configuration Executions	6-4
Limitations of Custom Configuration	6-5
Replacement of a Hub Device	6-5

CHAPTER 7**Administering Application Policies 7-1**

Understanding the Categorize Applications Tab	7-1
Viewing Applications	7-2
Moving Applications to a Different Category	7-2
Editing Application Information	7-3
Adding a New Application	7-3
Deleting NBAR2 Custom Applications	7-4
Understanding the Define Application Policies Tab	7-5
Operations in the Define Applications Tab	7-6
Moving an Application Category to a Different Business Group	7-7
Modifying the Application Performance	7-7
Understanding the Application Bandwidth Tab	7-8
Viewing the Application Bandwidth	7-8

CHAPTER 8**Monitoring and Troubleshooting Sites 8-1**

Viewing the Complete Cisco IWAN Network	8-1
Monitoring Page, Symbols, and Controls	8-2
Viewing Site Details	8-4
Compliance Reporting: Out-of-Band Configuration Changes	8-6
Compliance Reporting Setup	8-7
Compliance Monitoring	8-7
Service Assurance: Network Connectivity Alarms	8-8
Network Alarm Reporting Setup	8-8
Viewing Network Alarms	8-11

CHAPTER 9**Backup and Restore, Recovery, and Delete 9-1**

Backup and Restore	9-1
Backup and Restore Recommendations	9-1
Backup and Restore Scenarios	9-2

- Recovery 9-4
 - Recovering a Cisco IWAN Site 9-4
 - Post Provisioning Recovery for Hub and Branch Sites 9-4
- Deleting Sites and Devices 9-5
 - Deleting a Hub Site 9-5
 - Deleting a Transit Hub Site 9-5
 - Deleting a Branch Site 9-6
 - Deleting a Hub Device 9-6
- Manually Cleaning Up Devices 9-6
- Adding or Deleting Site Prefixes 9-8

APPENDIX A

- Brownfield Validation Messages A-1**
 - Adding Greenfield and Brownfield Devices to Cisco IWAN A-1
 - Errors A-2
 - Warnings A-3



Preface

This preface includes the following sections:

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

About

The Cisco IWAN application (IWAN app) operates within Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM). Before the 1.3.2 release, the IWAN app was bundled with APIC-EM. Beginning with 1.3.2, it is released separately from APIC-EM and installed manually in APIC-EM. The IWAN app remains an integral part of APIC-EM as in the past.

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	Overview	Introduces Cisco IWAN and describes how to access the Cisco IWAN application.
3	Deployment	Provides information about Cisco IWAN application deployment within Cisco APIC-EM.
4	Managing Hub Sites	Provides information about hub site setup and configuration.
5	Managing Branch Sites	Provides procedures for adding and provisioning branch sites and viewing site status information.
6	Managing Devices	Each site may have one or more associated devices. The IWAN app provides methods for managing the devices individually, including the Custom Configuration feature, which enables executing batch CLI commands on devices in the network.
7	Administering Application Policies	Provides procedures for categorizing and defining application policies based on the application bandwidth.
8	Monitoring and Troubleshooting Sites	Provides procedures for monitoring and troubleshooting sites.
9	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.
A	Brownfield Validation Messages Description	Provides a list of error and warning messages encountered during brownfield device 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.



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



Warning

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

Related Documentation

Documentation	Description
Cisco IWAN Application on APIC-EM User Guide, Releases 1.5.0, 1.5.1, 1.5.2	This document. Provides information about how to deploy, configure, and use the Cisco IWAN application.
Cisco IWAN Application on APIC-EM Release Notes	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 3.1 Documentation	Links to deployment guides and other Cisco Prime Infrastructure documentation.
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 Features and Changed Information, page 1-1](#)

New Features and Changed Information

The following table summarizes new and changed features in the Cisco IWAN app, releases 1.5.0, 1.5.1, 1.5.2.

Table 1-1 *New and Changed Features, IWAN App Releases 1.5.x*

Feature	Description	Reference
Multi-tunnel termination (MTT)	Support for multiple WAN links for a hub device. Multiple links may be added to a device at the time of site provisioning (Day 0) or after provisioning (Day N). The feature is available both for primary and transit hub sites.	Configuring Multi-tunnel Termination (MTT), page 4-28
Global Day N modification of QoS bandwidth at service profile level	Ability to allocate user-defined bandwidth percentages to a QoS class model after provisioning (Day N). Any WAN connection using the class model is updated, whether the connection is at a hub or branch site.	Modifying the QoS Bandwidth Percentages for a Service Profile, page 4-35
4G Support for MPLS Cloud	Support for 4G WAN links on a private MPLS cloud. Before this release, 4G WAN links were supported only on a public INET cloud. <ul style="list-style-type: none"> • All topologies are supported. • Any topology may include one 4G-cellular interface. • The 4G-cellular interface may be used for WAN clouds, not within a LAN. 	4G-Cellular Support for MPLS Cloud, page 5-25
Enhanced IP Pool provisioning options	Ability to configure IP address pools for Service Provider (overlay) and management loopback. Ability to modify Service Provider label, type, and address pool until hub provisioning is complete.	Configuring IP Address Pools, page 4-12

Table 1-1 *New and Changed Features, IWAN App Releases 1.5.x*

Feature	Description	Reference
Improved support for replacing a provisioned hub device (RMA)	Ability to replace a provisioned device (Day N) on a hub site, ensuring that the new router operates exactly like the router that has been replaced.	Replacement of a Hub Device, page 6-5
Additional Cisco ISR 89x routers support	Support added for several Cisco ISR 89x routers for branch sites. See the release notes for details.	Cisco IWAN Application on APIC-EM Release Notes, Release 1.5.1



Overview

This chapter contains the following sections:

- [About the Cisco IWAN Application, page 2-1](#)
- [Tutorial Videos, page 2-2](#)
- [Workflow for Accessing the Cisco IWAN Application, page 2-2](#)
- [Accessing the Cisco IWAN Application, page 2-2](#)
- [Cisco IWAN Application Home Page, page 2-4](#)

About the Cisco IWAN Application

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

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

Cisco IWAN automates deployments with an intuitive browser-based user interface. A new router can be provisioned faster, without requiring the use of router CLI commands.

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.

The application-centric approach offers 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.
- **Reduced 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 rollouts.

Tutorial Videos

Several tutorial videos are available, describing use of the IWAN app.

Table 2-1 *Tutorial Videos*

Tutorial	Description
Deployment Considerations	Issues to review before using the IWAN app, including firewall policy, NAT, controller placement, and so on.
Installation Overview	Installing the APIC-EM controller and IWAN app.
Provisioning the Hub/Transit Sites	Provisioning primary hub and transit hub sites.
Application Policy	Configuring application policies.
Provisioning a Brownfield Branch	Provisioning a brownfield (with pre-existing configurations) branch device.

Workflow for Accessing the Cisco IWAN Application

Table 2-2 *Basic Workflow for Accessing Cisco IWAN*

No.	Action	Reference
1	Deploy Cisco APIC-EM.	Deploying Cisco APIC-EM, page 3-2
2	Install the latest version of the IWAN application.	Installing or Upgrading the Cisco IWAN Application, page 3-2
3	Log into Cisco APIC-EM to access the Cisco IWAN application.	Accessing the Cisco IWAN Application, page 2-2
4	Use the Cisco IWAN application tools.	<ul style="list-style-type: none"> • Managing Hub Sites • Managing Branch Sites • Administering Application Policies • Monitoring and Troubleshooting Sites

Accessing the Cisco IWAN Application

Access the Cisco IWAN application from the Cisco APIC-EM GUI.

Procedure

-
- Step 1** Using Google Chrome or Mozilla Firefox, enter the IP address or the fully qualified domain name (FQDN) for Cisco APIC-EM.
- Step 2** Enter a username and password, and then click **Log In**.
- Step 3** (When logging in for the first time) Review and confirm the Telemetry Disclosure, 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 2-4](#).
-

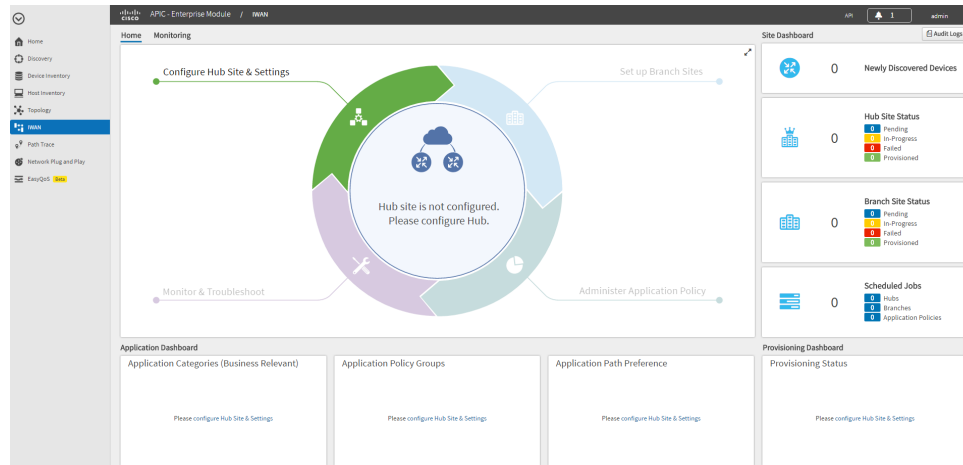
Cisco IWAN Application Home Page

The IWAN App home page shows configuration and monitoring options.

Before Provisioning

At initial setup, the only active configuration option is **Configure Hub Site & Settings**. The IWAN App provides a step-by-step workflow to guide you through the setup and configuration process.

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

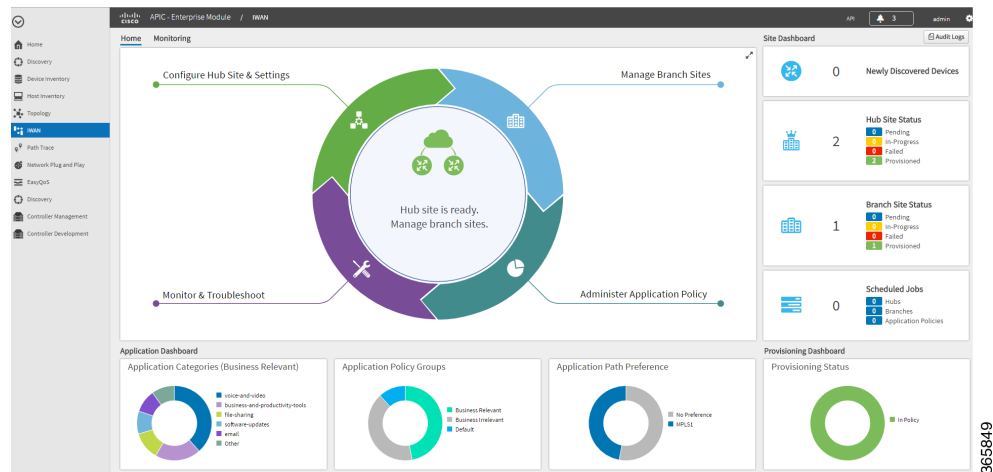


365861

After Provisioning

After you have configured and provisioned Cisco IWAN, the home page provides more information and options. 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 App Home Page—After Provisioning



Task Area	Function	Reference
Configure Hub Site & Settings	Configure and setup the hub site.	Managing Hub Sites, page 4-1
Manage Branch Sites	Add and provision branch sites and view site status information.	Managing Branch Sites, page 5-1
Administer Application Policy	Categorize and define application policies based on the application bandwidth.	Administering Application Policies, page 7-1
Monitor & Troubleshoot	Monitor and troubleshoot sites.	Monitoring and Troubleshooting Sites, page 8-1
Application Dashboard	At-a-glance information about: <ul style="list-style-type: none"> Application Categories Application Policy Groups Application Path Preference 	—
Provisioning Dashboard	Site provisioning status.	—
Site Dashboard	At-a-glance information about: <ul style="list-style-type: none"> Newly Discovered Devices Hub Site Status Branch Site Status Scheduled Jobs 	—



Deployment

This chapter contains the following sections:

- [Cisco IWAN App on APIC-EM, page 3-1](#)
- [Considerations Before Using the IWAN App, page 3-2](#)
- [Deploying Cisco APIC-EM, page 3-2](#)
- [Installing or Upgrading the Cisco IWAN Application, page 3-2](#)

Cisco IWAN App on APIC-EM

As described in the [Overview](#), the Cisco IWAN application (IWAN app) operates through Cisco APIC-EM, as a tool within the APIC-EM browser-based interface.

Separation from APIC-EM Release Schedule

Cisco IWAN app release 1.3.2 introduced a new approach to IWAN app releases. Beginning with this release:

- The IWAN app has been decoupled from the APIC-EM release schedule, and from the APIC-EM installation and upgrade processes.
- IWAN app release numbering is now independent of APIC-EM release numbering.
- Download the IWAN app separately from APIC-EM, then install or upgrade the app using the APIC-EM “App Management” page. See [Installing or Upgrading the Cisco IWAN Application, page 3-2](#).

Integral Part of APIC-EM

While the release schedule and installation are now handled separately from APIC-EM, the IWAN app continues to be an integral part of APIC-EM and continues to appear in the APIC-EM GUI as before.

System Requirements

System requirements for the APIC-EM continue to apply to the IWAN app.

The [release notes](#) describe the software compatible with IWAN app releases, including APIC-EM and Cisco Prime Infrastructure versions.

Considerations Before Using the IWAN App

Tutorial Video

For issues to review before deploying the IWAN app to control Cisco IWAN, see the tutorial video: [IWAN App Deployment Considerations](#)

Deploying Cisco APIC-EM

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

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

Deploy Cisco APIC-EM according to the instructions in the APIC-EM deployment guide, available on the APIC-EM [Install and Upgrade Guides](#) page.

Tutorial Video

[IWAN App Installation Overview](#)

Installing or Upgrading the Cisco IWAN Application

Before Installing or Upgrading the IWAN Application

Do the following before installing the IWAN app:

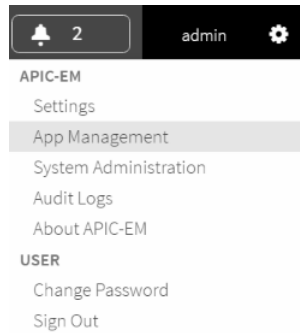
- (If APIC-EM is not already installed) Install Cisco APIC-EM according to the instructions in the APIC-EM deployment guide, available on the APIC-EM [Install and Upgrade Guides](#) page. If necessary, install any necessary patches to upgrade APIC-EM to the desired release.

Some versions of the APIC-EM installation package may include an earlier version of the IWAN app.

- Verify that your Cisco APIC-EM release (release 1.5.0 is required) and the software versions of other elements in the network are compatible with the IWAN app version you are installing. See the [release notes](#) for details.
- **Note:** When upgrading from an earlier release of the IWAN app, the log of operations done by the earlier release will not be preserved after the upgrade.

Recommendations

- Create a backup of the current APIC-EM configuration. See APIC-EM documentation for details about backup and restore. The basic steps are:
 1. In APIC-EM, select: **Settings (gear button) > App Management**.



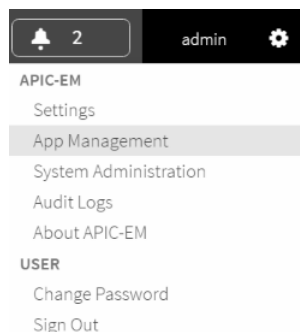
2. Select the **Backup & Restore** tab.
3. Click the **Create New Backup** button.



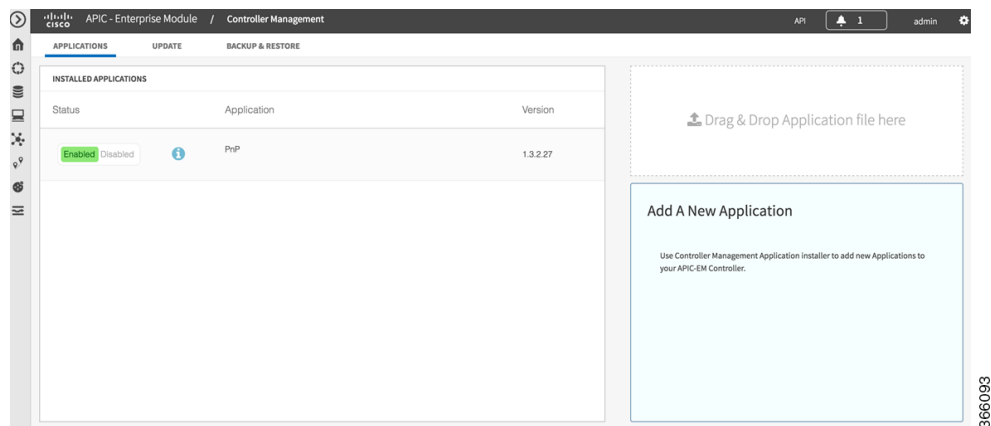
- If upgrading from a previous IWAN app release, perform a backup of the IWAN configuration before upgrading. See [Backup and Restore, Recovery, and Delete](#).

Procedure

-
- Step 1** Using the Cisco [Download Software](#) tool, navigate to [Policy and Automation Controllers](#), and select APIC-EM, or use this direct link:
<https://software.cisco.com/download/type.html?mdfid=286208072&flowid=77162>
- Step 2** Locate the **IWAN Application Software** option. Download the IWAN application. Note the location of the downloaded file.
- Step 3** Start APIC-EM and open the APIC-EM Applications page.
- a. Select: **Settings (gear button) > App Management**

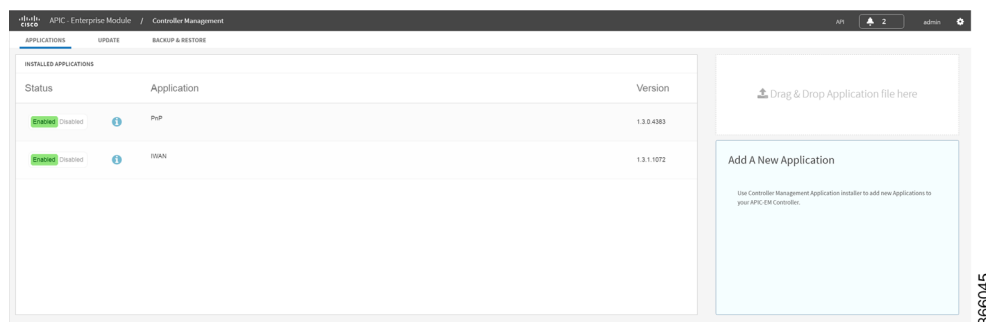


- b. Ensure that the Applications tab is displayed.
(The example below shows a PnP version number used with an earlier release of the IWAN app.)



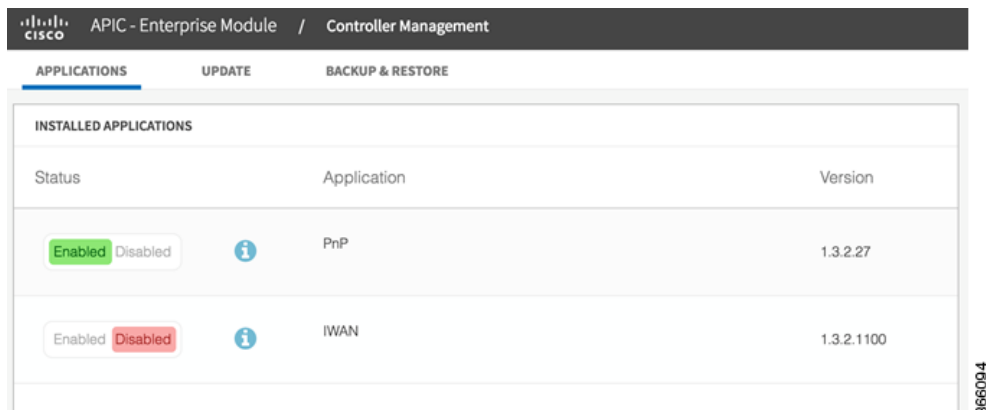
If a version of the IWAN app has been installed previously, it appears in the Installed Applications list.

(The example below shows an earlier release of the IWAN app.)

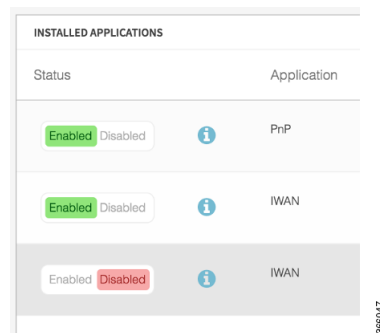


- c. Note the **Drag&Drop Application file here** box at the right side of the APIC-EM Applications page.

Step 4 Drag-and-drop the downloaded IWAN app installation file onto the **Drag&Drop Application file here** box. The new IWAN app appears in the list of applications, and is shown as Disabled. (The example below shows an earlier release of the IWAN app.)



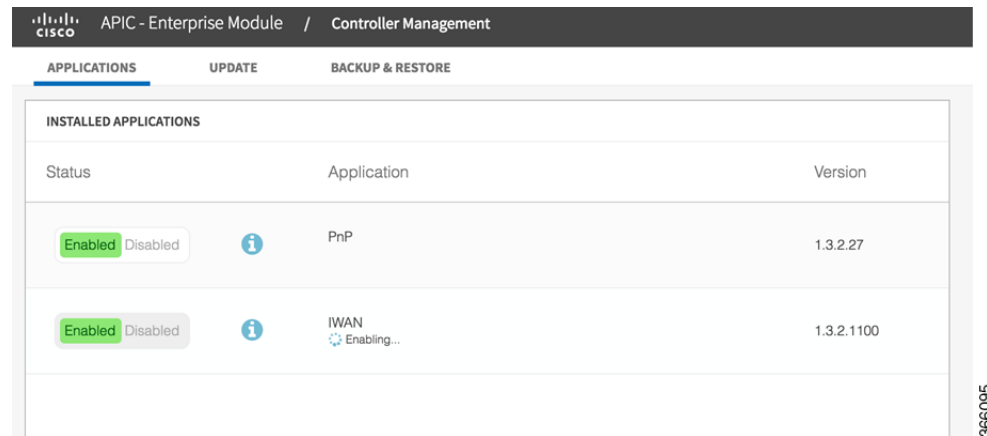
When upgrading from a previous version of the IWAN app, the earlier version of IWAN continues to appear in the list at this point in the installation.



- Step 5** Click **Enabled** for the new IWAN application. APIC-EM enables the new version. When upgrading from a previous version of the IWAN app, APIC-EM preserves the existing IWAN configuration.

The page indicates that the enable process is in progress. Wait for the process to complete. Installation time depends on the cluster size and other factors.

(The example below shows an earlier release of the IWAN app.)



- Step 6** When the installation and enabling are complete, clear the browser cache and refresh the APIC-EM Applications page. The Status column shows that the new IWAN app is enabled, and the Version column shows the new IWAN app version. Any previous version of the IWAN app is removed from the list. (The example below shows an earlier release of the IWAN app.)

The screenshot shows the APIC-EM Controller Management interface. At the top, there are navigation tabs for 'APPLICATIONS', 'UPDATE', and 'BACKUP & RESTORE'. Below these, a section titled 'INSTALLED APPLICATIONS' contains a green notification bar with the message: 'Successfully enabled application=iwan, version=1.3.2.1100'. Underneath, a table displays the installed applications:

Status	Application	Version
Enabled Disabled	PnP	1.3.2.27
Enabled Disabled	IWAN	1.3.2.1100

The 'IWAN' application row is highlighted in green. A vertical ID number '366096' is visible on the right side of the screenshot.



Managing Hub Sites

This chapter contains the following sections:

- [Setting Up a Hub Site, page 4-1](#)
- [Configuring System Settings, page 4-2](#)
- [Uploading Certified Cisco IOS Software Images for Branch Devices, page 4-6](#)
- [Deleting an Uploaded Cisco IOS Software Image, page 4-8](#)
- [Configuring Service Providers, page 4-9](#)
- [Configuring IP Address Pools, page 4-12](#)
- [Configuring the IWAN Aggregation Site, page 4-17](#)
- [Modifying the Configuration of Hub Sites, page 4-24](#)
- [Understanding the Coexistence of IWAN Sites and Non-IWAN Sites, page 4-25](#)
- [Homogeneous and Heterogeneous Topologies, page 4-25](#)
- [Understanding IP Address Pools, page 4-27](#)
- [Configuring Multi-tunnel Termination \(MTT\), page 4-28](#)
- [Updating the WAN Bandwidth of a Provisioned Hub Site, page 4-33](#)
- [Modifying the QoS Bandwidth Percentages for a Hub Site, page 4-34](#)
- [Modifying the QoS Bandwidth Percentages for a Service Profile, page 4-35](#)
- [Deleting a User-defined QoS Bandwidth Service Profile, page 4-36](#)
- [Setting the Geographic Location of a Hub Site, page 4-37](#)
- [Collecting Network Data Using LiveAction, page 4-37](#)
- [Interoperability between APIC-EM and a non-IWAN-enabled Network, page 4-38](#)

Setting Up a Hub Site

From the IWAN App home page, use the **Configure Hub Site & Settings** option to set up a hub site. The Network Wide Settings page opens, with tabs for configuration tasks, as described below.

Tutorial Video

[IWAN App Hub Provisioning](#)

Table 4-1 Network Wide Settings Page—Tasks

Tab	Task	See:
System	Configure system settings, including: <ul style="list-style-type: none"> • Server addresses for NetFlow collector • DNS servers • Syslog server • AAA server • NAT/Proxy addresses • SNMP • DHCP 	Configuring System Settings, page 4-2
Certified IOS Releases	Upload Cisco IOS software images to load onto new greenfield branch devices.	Uploading Certified Cisco IOS Software Images for Branch Devices, page 4-6
Service Providers	Configure service providers: <ul style="list-style-type: none"> • Identifying label for each service provider • Type of connection for each service provider 	Configuring Service Providers, page 4-9
IP Address Pools	Configure IP address pools to allocate IP addresses for: <ul style="list-style-type: none"> • Service providers (overlay) • Loopback • Branch sites 	Configuring IP Address Pools, page 4-12
IWAN Aggregation Site	Configure the IWAN aggregation site(s): <ul style="list-style-type: none"> • Master controller • Hub sites • Hub devices: LAN, WAN, and MC configurations 	Configuring the IWAN Aggregation Site, page 4-17

Configuring System Settings

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

Click **Show More** or **Show Less** to display or hide settings.

Procedure

-
- Step 1** If logging in for the first time, specify the global settings in the CLI Credentials dialog box. Enter a user name and password, 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 4-1 System Settings Tab

APIC - Enterprise Module / IWAN

Network Wide Settings

System Settings

NetFlow Collector

* Netflow Destination IP: 1.1.1.1

* Port Number: 9991

NAT/Proxy IP Address

* APIC-EM behind NAT/Proxy: No Yes

APIC-EM NAT/Proxy IP: _____

DNS

* Domain Name: cisco.com

SNMP

* Version: V2C

* Read Community: *****

To configure additional network settings like DHCP, AAA, Syslog and advance settings in SNMP, DNS, etc. click "Show more" link below:

[Show more](#)

Previous Save & Continue

I wish this page would...

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 **NAT/Proxy IP Address** area, configure the following:

Field	Description
APIC-EM Behind NAT/Proxy	Select Yes if the APIC-EM controller is located behind a NAT router.
APIC-EM NAT/Proxy IP	Public NAT public IP address of the APIC-EM controller.

Step 9 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: 3
Timeout (secs)	Displayed for SNMP V2C only. Timeout period. Default: 10
Trap Destination IP	(Optional) IP address of the SNMP server. Note If you do not enter an IP address, the Cisco IWAN app 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	Select 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. Select 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: 3

Field	Description
Timeout (secs)	Displayed for SNMP V2C only. Timeout period. Default: 10
Trap Destination IP	(Optional) IP address of the SNMP server. Note If you do not enter an IP address, the Cisco IWAN app 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 10 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. To add an additional DHCP server, click the + icon next to the IP address field, and then enter the IP address. Note You can add a maximum of five DHCP servers. To remove a DHCP server, click the - icon next to the IP address field that you want to remove.

Step 11 Click **Save and Continue**.

After updating existing values in the Systems tab, the Network Wide Settings Summary dialog box opens, indicating changes. Do one of the following:

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

Uploading Certified Cisco IOS Software Images for Branch Devices



Note

This step applies to greenfield branch devices only.

You can upload certified Cisco IOS images from your computer into the Cisco IWAN app. 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.

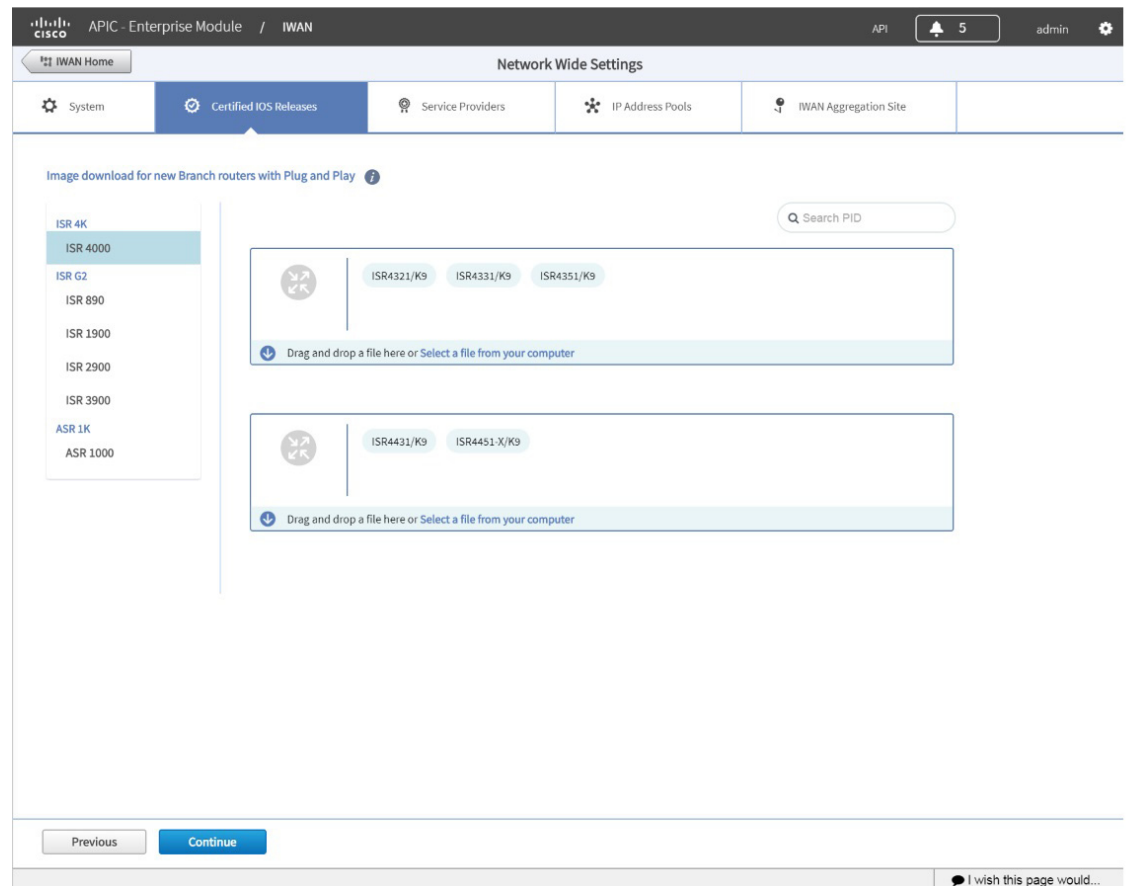
**Note**

If the appropriate software image is already installed on any new greenfield routers, 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 4-2 Certified IOS Releases Tab



Step 2 From the left pane, choose the router type.

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**.

Deleting an Uploaded Cisco IOS Software Image

Before deleting a Cisco IOS software image, it is necessary to disassociate the image from any platform models configured to use the image by default. To delete an image, do the following:

-
- Step 1** Open the “Network Plug and Play” app by clicking its icon in the left panel of APIC-EM.
 - Step 2** Click the “Images” tab at the top of the page to display uploaded images.
 - Step 3** Click an image name of an image to be deleted to open the “Image Info” dialog box.
 - Step 4** In the “Use this Image as Default” column, de-select any selected boxes to disassociate the image from the various platform types. (**Tip:** Click the **All** box two times to clear all boxes in the column.)
 - Step 5** Click the **Save** button in the dialog box.
 - Step 6** Repeat for all the images need to be deleted.
 - Step 7** In the “Images” tab, select the image(s) to delete and click the **Delete** button at the top-left.
-

Configuring Service Providers

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

Procedure

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

Figure 4-3 Service Providers Tab

The screenshot shows the Cisco APIC Enterprise Module interface for configuring service providers. The top navigation bar includes 'APIC - Enterprise Module / IWAN' and user information 'API 5 admin'. The main navigation tabs are 'System', 'Certified IOS Releases', 'Service Providers' (selected), 'IP Address Pools', and 'IWAN Aggregation Site'. The 'Configure Service Providers' section contains a table with the following data:

WAN Label	WAN Type	Metered
INTT	Public	<input type="checkbox"/>
MPLS	Private	<input type="checkbox"/>

Below this is the 'Available QoS models for Service Providers' section, which contains a table with the following data:

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

At the bottom of the page, there are 'Previous' and 'Save & Continue' buttons. A feedback prompt 'I wish this page would...' is visible in the bottom right corner.

- Step 2** In the **Configure Service Providers** area, click the + icon and configure the properties shown in the table below.



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"> • Private • Public
Metered	Select this option if the WAN is metered. <p>Note The Metered option is available 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.</p> <p>Note Only one link can be metered.</p> <p>Note Only one link is permitted on a public cloud.</p>
Available QoS Models for Service Providers	
Profile Name	Lists the names of all available service profiles.
Class Model	Lists the class models that correspond to the respective service profiles: <ul style="list-style-type: none"> • 4 Class • 5 Class • 6 Class • 8 Class

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 4-4 Add Service Profile Dialog Box

Step 4 Enter the following profile information, and 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.
Class Model	Displays the type of class model. Can be one of the following: <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 Bandwidth (%)	Percent bandwidth allocated to the priority class, such as Voice.
Remaining Bandwidth (%)	Percent bandwidth allocated to other classes, such as streaming video, critical class, and so on. <p>Note Enter a value greater than 0. The total value for all the data classes in the Remaining Bandwidth column cannot exceed 100%.</p>



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 [Configuring the IWAN Aggregation Site, page 4-17](#).

Configuring IP Address Pools

Use the IP Address Pools tab to define IP address pools. For general information about IP Address Pools, see [Understanding IP Address Pools, page 4-27](#).



Note When planning IP address pools, consider any future requirements, such as future growth of the IWAN network, and remote sites that might be deployed in the future. After hub site(s) provisioning, the IP address pool settings cannot be changed.



Note Earlier versions of the IWAN App referred to generic IP address pools. Beginning with the 1.5.0 release, the IWAN App refers to Service Provider Address Pool, Global Address Pool, and Site Specific Address Pools.

Overview of Address Pool Configuration in the IWAN App

Generic pool

A generic pool is used to assign IP addresses for DMVPN tunnels, management loopback addresses for Cisco Performance Routing (PfR), and LAN interfaces for greenfield remote sites.

Ensure that the address range allocated for a generic pool is not used elsewhere in the network.

Enter the number of remote sites used in the IWAN network. This corresponds to the number of DMVPN overlays. Click **IP Pool Calculator** to display the subnet mask required for the Generic pool.

Loopback pool

A Loopback pool is used to assign IP addresses for management loopback addresses for Cisco Performance Routing (PfR).

Ensure that the address range allocated for a loopback pool is not used elsewhere in the network.

Enter the number of remote sites used in the IWAN network. This corresponds to the number of DMVPN overlays. Click **IP Pool Calculator** to display the subnet mask required for the Loopback pool.

LAN Greenfield pool

If not allocating addresses for greenfield remote site LANs from the generic pool, there are two options:

1. Create a separate LAN greenfield pool. This will be single IP pool for all remote branches. Calculate the subnet length required for this single IP pool by entering the number of VLANs and number of devices per VLAN by clicking the **IP Pool Calculator** button.

2. To assign specific addresses for the remote site VLAN at every site, use a site-specific pool.

Verify that the address range allocated for the LAN greenfield pool is not used anywhere else in the network.

LAN Brownfield pool

To create a summary routing entry for all existing LAN subnets across all brownfield sites, use the LAN Brownfield pool option. This will help in advertising only the summary route from the hub representing all of the branch LAN prefixes. Without this entry, the IWAN app uses specific entries for the branch LAN prefixes.



Note

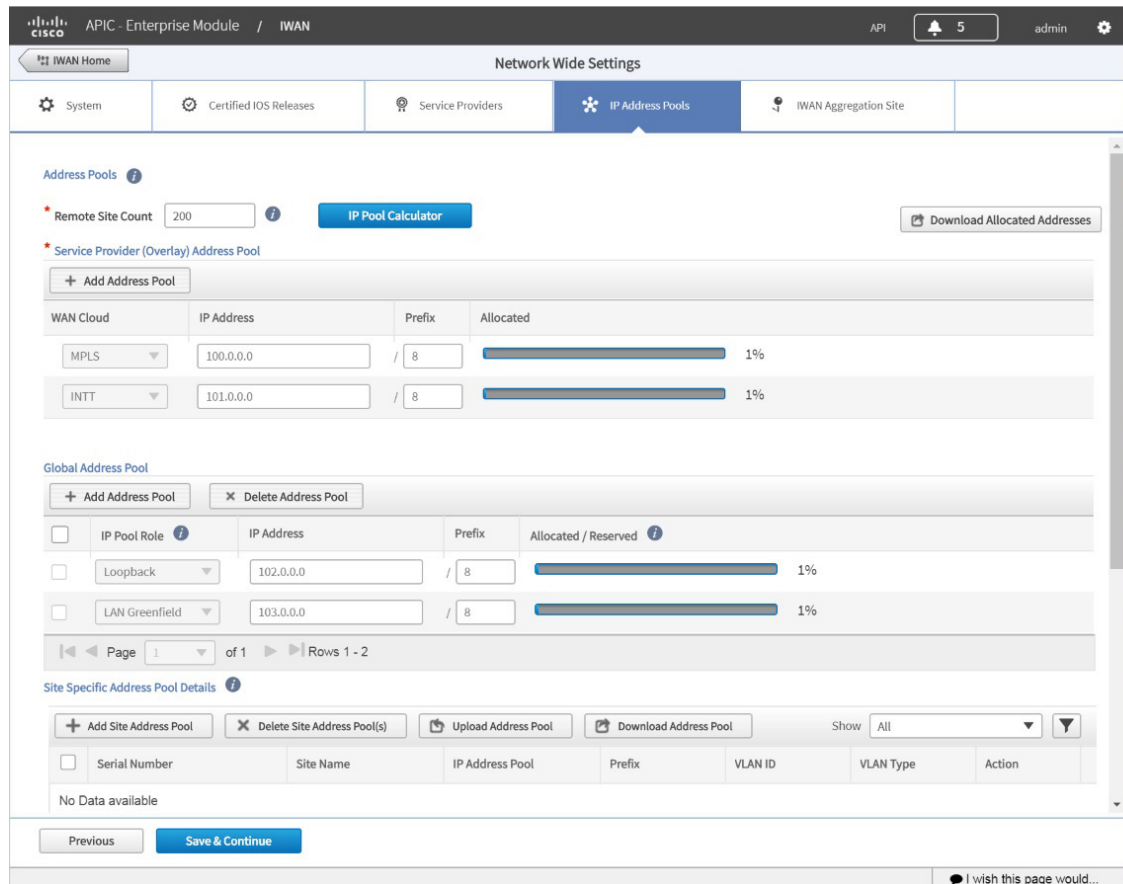
The LAN Greenfield and LAN Brownfield pools are used in defining the enterprise prefix lists in Cisco Performance Routing (PfR).

Configuring Address Pools

Procedure

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

Figure 4-5 IP Address Pools Tab



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 can increase the remote site count by upgrading to Cisco IWAN release 1.3.x. 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 Click the **IP Pool Calculator** button.

The Proposed IP Range dialog box opens, providing:

- Recommended minimum prefix length values for IP pools
- Recommended values for number of IP addresses per VLAN, and number of VLANs.

Step 4 Click **OK** or **Get IP Range**.

- Step 5** To configure a service provider address pool: In the Service Provider (Overlay) Address Pool section, click + **Add Address Pool**.
- Configure a maximum of one service provider address pool per service provider. IP addresses from this pool will be used for overlay IP address needs.

Field	Description
WAN Cloud	Select a service provider name. Note Configuring service provider IP address pools changed in IWAN App releases 1.5.x. If the IWAN App is installed as an upgrade from a release earlier than 1.5.x, to support an existing legacy configuration, IWAN App provides WAN Cloud labels automatically for existing service providers in this step. The WAN label configured for the service provider in the earlier release is used for the WAN Cloud label on this page. Examples: "INET1," "MPLS"
IP Address	IP Address for the IP address pool. This pool is for service provider overlay address needs.
Prefix	CIDR prefix. (The Classless InterDomain Routing (CIDR) prefix notation defines the subnet mask.)
Allocated	Displays the percentage of addresses in the pool that are used.

- Step 6** To configure a global address pool: In the Global Address Pool section, click + **Add Address Pool**.

Field	Description
IP Pool Role	Select a role: <ul style="list-style-type: none"> • Loopback: Used to assign IP address for management loopback addresses for Cisco Performance Routing (PFR). • 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 an existing configuration). You can have any number of LAN brownfield IP address pools. Note To support legacy configurations, the IWAN App provides "Generic" as a role if installed as an upgrade from a previous version of the IWAN App.
IP Address	IP Address for the IP address pool.
Prefix	CIDR prefix. (The Classless InterDomain Routing (CIDR) prefix notation defines the subnet mask.)
Allocated	Displays the percentage of addresses in the pool that are used.

- Step 7** To configure site specific LAN IP address pools:
- Click + **Add Site Address Pool**. The Add Site Address Pool dialog box opens.
 - Enter the properties as shown in the table below, then click **OK**. The newly configured information appears in the table.

By default, greenfield branch site IP addresses assignment is as follows:

- If there is a LAN greenfield IP address pool, greenfield branch sites use this address pool.
- If there is no LAN greenfield IP address pool, greenfield branch sites use the generic IP address pool (applicable only for upgrade deployments—upgraded from an IWAN app release prior to 1.5.0 to releases 1.5.x).

To provision a new greenfield branch site using custom IP address pools for its VLANs, define the VLANs and custom IP address pools before you provision the site. (Doing this prevents the VLANs from using the LAN greenfield IP address pools or generic IP address pools, by default. In this case, the generic IP address pool option applies only to deployments upgraded from an IWAN app release prior to 1.5.0 to releases 1.5.x.)

**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. Plan carefully before provisioning the site.

**Note**

Typically, for greenfield branch sites, the LAN Greenfield pool is required. It is optional only if:

- The greenfield branch site has a site-specific pool defined, and
- It is a single-router branch 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. (The Classless InterDomain Routing (CIDR) prefix notation defines the subnet mask.) Range of values (single serial number): 16 to 30 Range of values (more than one serial number): 16 to 29
VLAN ID	Range of values: 1 to 4094 Note The VLAN ID 99 is reserved for the transit VLAN, therefore you cannot use this ID for other VLANs.
VLAN Type	Enter a VLAN type or select it from the drop-down list. Values: Data, Guest, Voice and Video, Wireless. Note The following restrictions apply when you enter a VLAN type of your choice: <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 8** To upload a large number of site specific address pools:
- In the Site Specific Address Pool Details section, click **Download Address Pool** to download a template CSV file called: `Controller_Profile_DD-MM-YYYY.csv`
 - Create a CSV file containing all of the required information.
 - Click **Upload Address Pool**, and then upload the CSV file.
- Step 9** Click **Save & Continue**.

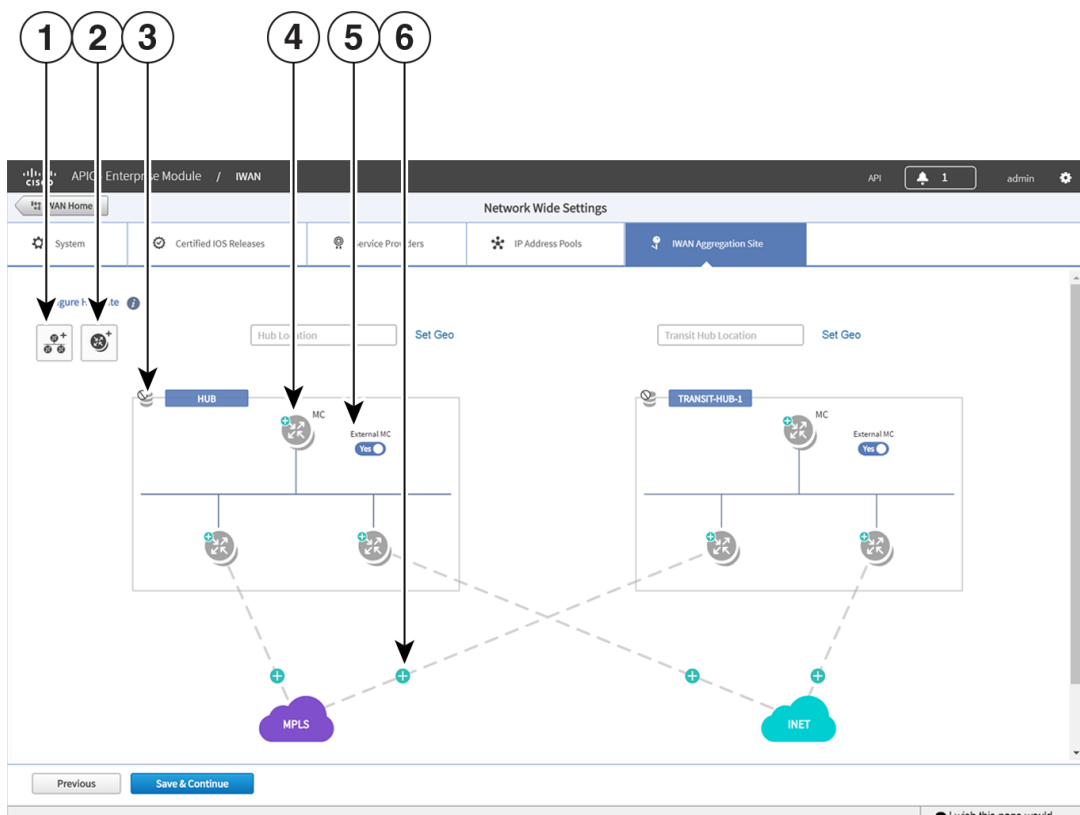
Configuring the IWAN Aggregation Site

Use this procedure to do the following:

- Discover hub devices.
- Configure LANs.
- Configure WANs.
- Configure the external master controller.

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

Figure 4-6 IWAN Aggregation Site Tab



366650

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

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 defined service providers and the respective hub border routers.
- b. Do one of the following:
 - (Recommended) Click the **External MC** button (see # 5 in [Figure 4-6](#)) 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 4-6](#)). 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 4-6](#)) 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.
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

Field	Description
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.

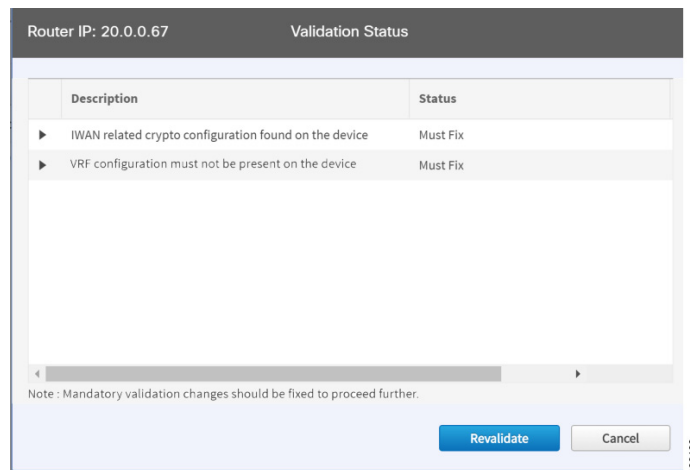
- Click **Add Device**.

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

The Cisco IWAN app accesses the router and checks its configuration to determine if it has any configuration that might conflict with the Cisco IWAN app. 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:



- 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 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, select the appropriate **LAN IP-Interface** check box(es), and 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 4-6](#)). The LAN Routing dialog box opens.

The Routing Protocol, AS Number, and Datacenter prefixes 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 this is not recommended.

Field	Description
Select LAN Protocol for Redistribution	
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	
Available (table)	Automatically populated list of hub site IP addresses.
Selected (table)	IP addresses selected from the Available table.

- b. Select one or more IP addresses from the Available table and click an arrow to move the addresses to the Selected table. Only selected IP addresses (prefixes) will be configured on the hub.
To remove an address from the Selected table, hover over the address and click the red X.
(Optional) Use the Add DCIP/Mask link to filter IP addresses.
- c. Click **Save**.

Step 3 Configure WANs. Do the following:

- a. Click the + icon on the link that connects the router and cloud (see # 6 in [Figure 4-6](#)). The Configure Link dialog box opens.
The dialog boxes that appear depend on the WAN type that you specified while configuring the Service Provider—for example, Private or Public.
- b. For Public WAN, the Configure Link dialog box opens. Enter the following information for each link in the network:

Table 4-2 *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	Public IP address.
Bandwidth (Mbps)	Symmetrical bandwidth for upload and download.
Service Profile	Choose a service profile from the drop-down list. The drop-down list includes default and custom 8 Class service profiles that were configured in the Service Providers tab.

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

Table 4-3 *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.
Use Loopback for DMVPN Tunnel	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 4-25 .

Table 4-3 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	Choose a service profile from the drop-down list. The drop-down list includes all default and custom service profiles (4 Class, 5 Class, 6 Class, and 8 Class) that were 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 4-6](#)). 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 click **Save**.

Modifying the Configuration of Hub Sites

After you have completed all of the configuration 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.

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).

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 app 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.

Homogeneous and Heterogeneous Topologies

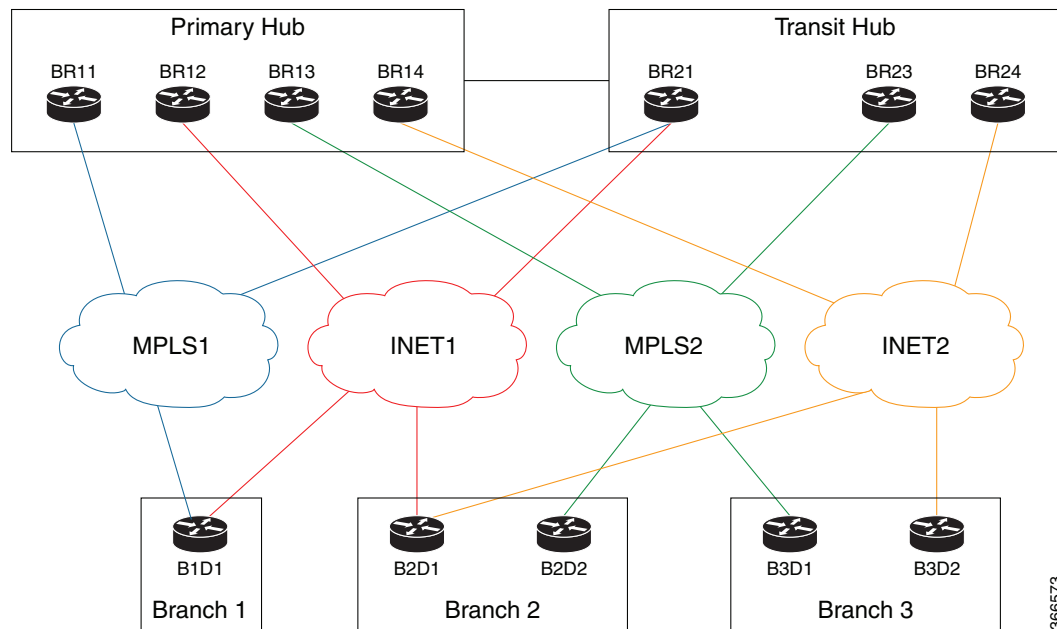
Effective with Cisco IWAN Release 2.0, you can perform the following for a provisioned site:

- 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).

Homogeneous Topology

In a homogeneous topology, a primary hub site and the associated transit hub site have the same total connections to service providers. The sites can have a different number of devices handling the connections, as a single device can have more than one connection. In the example, both hub sites have connectivity to all four service providers.

Figure 4-7 Homogeneous Topology

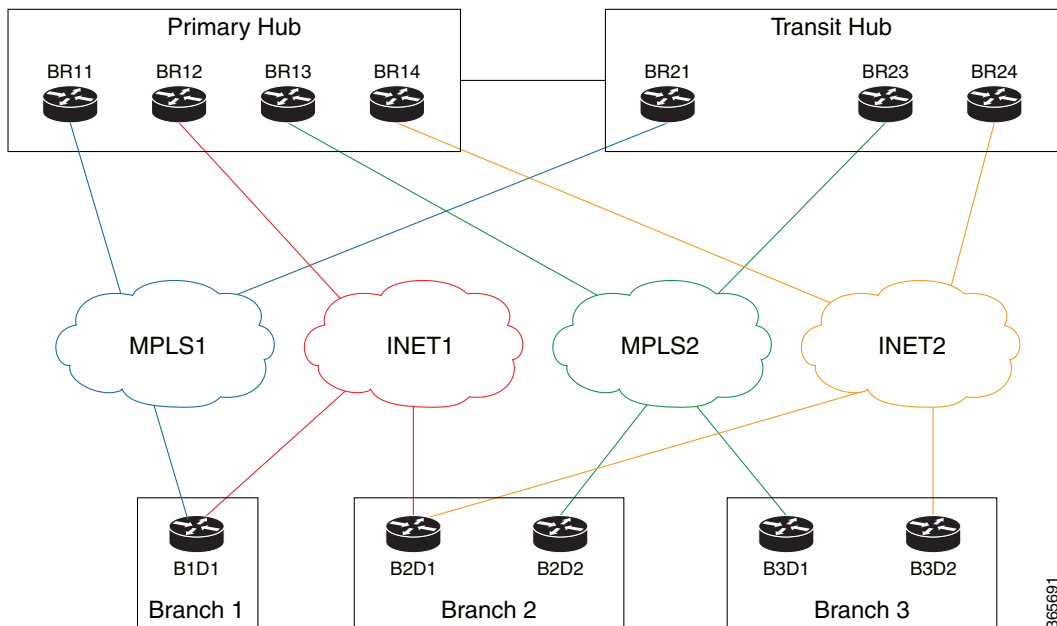


366573

Heterogeneous Topology

In a heterogeneous topology, a primary hub site and the associated transit hub do not have connections to all of the same service providers. In the example, the primary hub is connected to four service providers and the transit hub is connected to only three.

Figure 4-8 Heterogeneous Topology



365691

Understanding IP Address Pools

The IWAN App automatically uses IP addresses from the global enterprise IP address pool space. When provisioning hub and spoke devices, the IWAN App uses IP addresses allocated in the user-configured IP address pools. This includes interface, LAN, VPN overlay, and routing IP addresses.

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 global IP address pool is used.

It is important to define the size of the IP address pools to accommodate the long term needs of the IWAN site. VPN requirements dictate that subnets must be defined and allocated internally before any sites are provisioned. In the current Cisco IWAN release, you can increase the site and service provider counts after initial provisioning, but you cannot change the IP address pool once specified. Therefore, we recommend that you account for any future scale of service providers and site sizes when defining the IP address pools. The service provider IP address pool is used for overlay and loopback addresses.

Optionally, wherever specific IP addresses are required, site-specific LAN and VLAN requirements can be defined and prioritized over the service provider and 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 global 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 app 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.

Configuring Multi-tunnel Termination (MTT)

The IWAN App supports multiple WAN links for a hub device. Multiple links may be added to a device at the time of site provisioning (Day 0) or after provisioning (Day N). The feature is available both for primary hub sites and transit hub sites. (Transit hub sites operate in parallel with primary hub sites, providing load balancing and/or failover support.)

Primary and Transit Hub Sites Require Connectivity to All Links

For topologies that use primary and transit hub sites together, both the primary and transit hubs must have connectivity to the same service providers at Day 0 (at the time of provisioning). This is called a “homogeneous” topology (see [Homogeneous and Heterogeneous Topologies, page 4-25](#)).

Number of Devices at Primary and Transit Hub Sites May be Different

When using a topology that includes a primary hub site and a transit hub site, it is not necessary for the device configuration to be identical at both sites. The sites may have a different number of devices, but those devices must share the same connectivity. This may require configuring multiple links to a single device.

For example, if a primary site has two devices, each with a single link to a service provider, and the associated transit site has only one device, that single device must have two links to provide the same connectivity as the primary site.

Day 0 Multiple WAN Link Configuration: Features, Limitations, Procedure

Features

Table 4-4 Day 0 Multiple WAN Link Features

Feature
Service Providers, Devices, Links
Supported service providers: 2 to 4
Minimum number of devices for a hub site: 1
Maximum number of links per device: 3
Options
Provision a multi-link hub site with any combination of public/private links.
Different devices at a hub site can be provisioned to operate with different sets of links.
Provision multiple hub sites with a different number of devices at each site.

Requirements and Limitations

Table 4-5 Day 0 Multiple WAN Link Requirements and Limitations

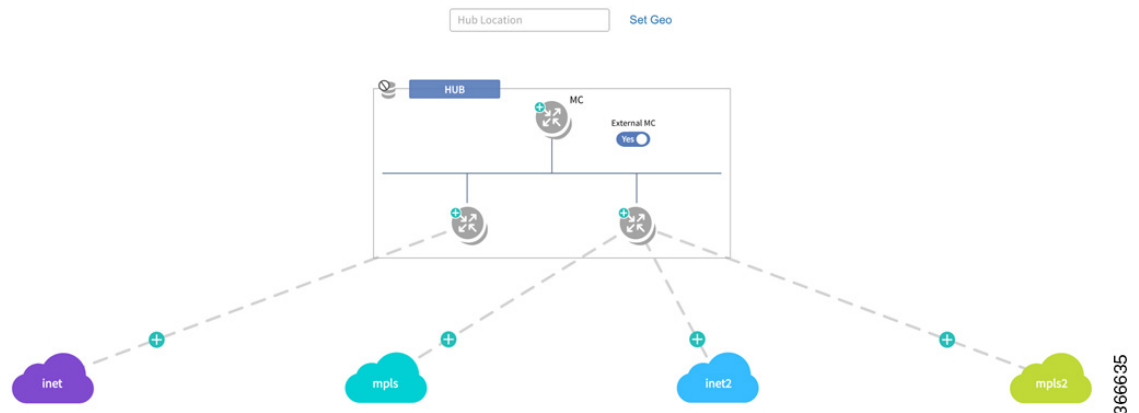
Requirement/Limitation
OS for Participating Devices
Cisco IOS XE 16.3.3
Connectivity
At the time of hub site provisioning (Day 0), each hub site must have connectivity to all service providers.

Adding Multiple Links to a Hub Device at Day 0

Adding a link to a device before provisioning (Day 0) requires drawing a link between a device and a cloud. Use the following procedure.

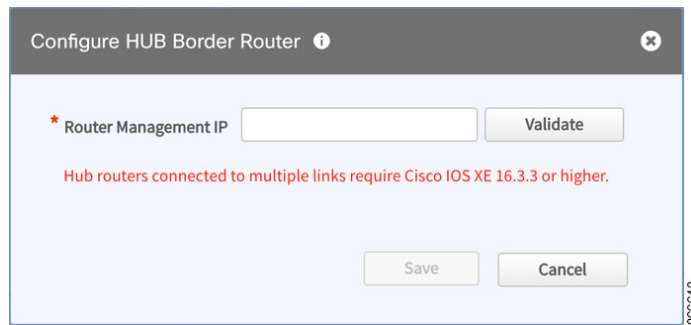
Procedure

- Step 1** Open the Network Wide Settings page > IWAN Aggregation Site tab.
- Step 2** To add a link for a hub device, click and hold over the device, and “draw” a line to the intended cloud icon. If required, draw multiple new links.
- The newly drawn links appear as dotted lines to indicate that they have not yet been configured.



- Step 3** Click the device with a new link (or click one of the devices with a new link if adding links to more than one device).

A dialog box appears, prompting you to enter the router management IP. The dialog also indicates that to perform this operation, the device must be running Cisco IOS XE 16.3.3.



- Step 4** Enter the required information and click the **Save** button to proceed.
- Step 5** In the subsequent dialog boxes, enter the SNMP and SSH/Telnet information as required, and click the **Add Device** button.
- Step 6** In the LAN IP-interface area, select the interface(s) to use, and click the **Save** button.
The IWAN App performs several validations. If any validations fail, a Validation Status dialog box appears, indicating the errors. For example, if the device OS is not compatible with the links that you have drawn for it, a validation error appears.
- Step 7** For each new link, click the plus-sign on the new link to open the Configure Link dialog box.
- Step 8** Enter information for the WAN IP-interface and other required fields.
- Step 9** Click the **Save** button.
The lines indicating links (which were formerly dotted lines) appear solid.
- Step 10** If other devices have newly drawn links, click the devices one-by-one and repeat the preceding steps for each.
- Step 11** At the bottom of the page, click the **Save & Continue** button.
A summary of the configuration appears.
- Step 12** Click the **Continue** button to begin provisioning.

Day N Multiple WAN Link Configuration: Features, Limitations, Procedure

Features

Table 4-6 Day N Multiple WAN Link Features

Feature
Service Providers, Devices, Links
Supported service providers: 2 to 4
Minimum number of devices for a hub site: 1
Maximum number of links per device: 3
Options
Add new links to one or more hub devices (see Adding Links to an Existing Hub Device at Day N, page 4-31).
Different devices at a hub site can be configured to operate with different sets of links.
Delete a transit hub site with multi-linked devices.

Requirements and Limitations

Table 4-7 Day N Multiple WAN Link Requirements and Limitations

Requirement/Limitation
OS for Participating Devices
Cisco IOS XE 16.3.3
Connectivity
After hub site provisioning (Day N), hub sites may have different connectivity to service providers. This arrangement is called “heterogenous” (see Homogeneous and Heterogeneous Topologies, page 4-25).
Limitations
Cannot delete an existing link from a hub router on Day N. If the device has the last link connected to a cloud, can de-provision the branch attached and then delete the hub device. After doing this, can then re-provision the branch site, using the desired links.
Cannot add a new link to a hub "master controller" (MC) device.
Adding a link to a device interrupts routing activity on the device.
When adding a link to the only device providing connectivity to a branch site, connectivity to that site will be lost during this process.

Adding Links to an Existing Hub Device at Day N

The procedure for adding a link to a device after provisioning (Day N) differs from the procedure used before provisioning (Day 0). At Day 0, add links by drawing a link between a device and a cloud. At Day N, use the following procedure.

**Note**

- Adding a link to a device interrupts routing activity on the device.
- If this is the only device providing connectivity to a branch site, connectivity to that site will be lost during this process.

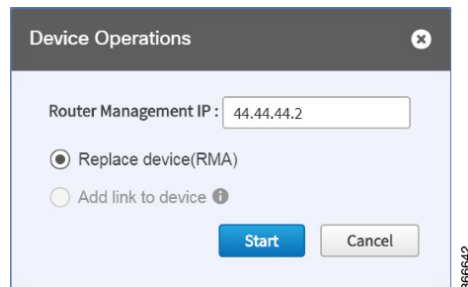
Procedure

Step 1 Create a clean configuration file on the bootflash of the router with the filename: IWAN_RECOVERY.cfg

This is a config file containing the configuration prior to use of the device with the IWAN app. The file must include the current LAN, WAN, and SNMP details, along with the information for the new WAN link being added.

Step 2 Open the Network Wide Settings page > IWAN Aggregation Site tab.

Step 3 Click the device to display the Device Operations dialog box.



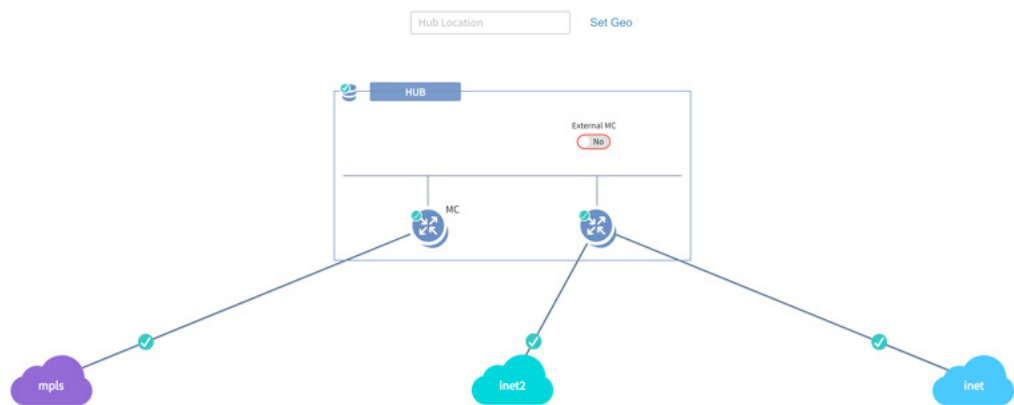
Step 4 In the Device Operations dialog box, select **Add link to device** and click the **Start** button.

The “Add link to device” dialog box appears, displaying important information about adding a link.

Step 5 Select each item in the “Add link to device” dialog box to confirm and proceed.

- Step 6** A series of "Configure Hub Border Router" dialog boxes appear, providing options for adding the link.
- **Automatic method:** If the clean configuration file on the device includes up-to-date LAN IP information and SNMP credentials, the IWAN App auto-populates the fields in the dialog boxes that follow, and closes them automatically, without requiring any user input. **Result:** The IWAN app reverts the device to the configuration defined in the clean configuration file, adds the existing WAN link automatically, and prompts you for the new link information.
 - **Manual method:** If the clean configuration file on the device contains different LAN IP information or different SNMP credentials, the "Configure Hub Border Router" dialog boxes prompt you for that information, assisting you in reprovisioning the device with the existing WAN link and configuring the new link. Enter the information to proceed with adding the new link to the device.

After completing the process, the new link appears as a solid line in the topology.



366644

Updating the WAN Bandwidth of a Provisioned Hub Site

You can change the upload or download WAN bandwidth after a hub site is provisioned ("day N"). Also see [Updating the WAN Bandwidth of a Provisioned Branch Site, page 5-26](#).

Valid bandwidth values depend on the interface type:

- TenGigabit interface: 0.1 to 10000 Mbps
- Gigabit interface: 0.1 to 1000 Mbps
- Cellular interface: 0.1 to 300 Mbps

Use the following procedure to update the bandwidth settings.

Procedure

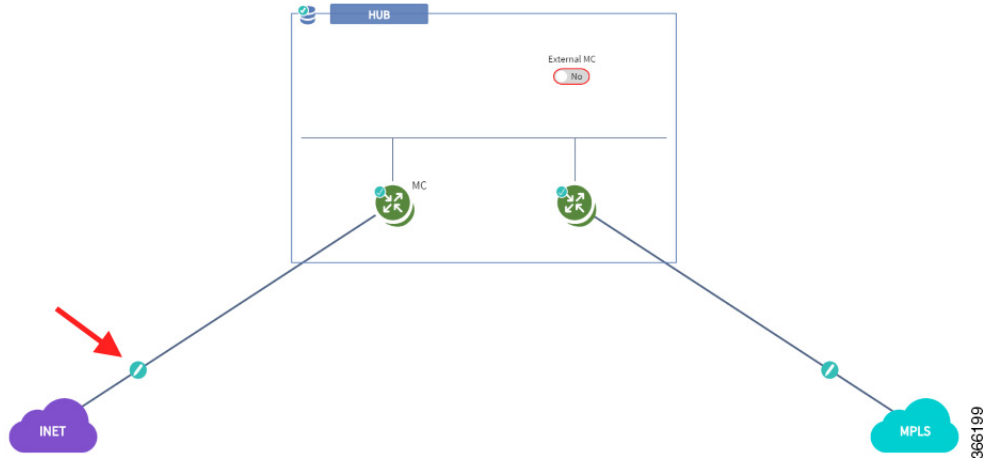
-
- Step 1** From the IWAN app home page, click **Set up Branch Sites**.
- Step 2** Click the **Sites** tab.

Step 3 Click the pencil icon (Edit Site) for a hub site. The IWAN Aggregation Site page opens.



Note You can also reach this page by clicking **Configure Hub Site & Settings** on the IWAN front page, and then clicking the **IWAN Aggregation Site** tab.

Step 4 Click the pencil icon on the WAN link. The Configure Link dialog box opens.



Step 5 In the Bandwidth field, enter a new value.

Step 6 Click **Save** in the dialog box.

Step 7 Click the **Save & Continue** button at the bottom left of the page. The Hub Site summary dialog box appears.

Step 8 Click **Continue** to close the summary.

Modifying the QoS Bandwidth Percentages for a Hub Site

You can modify the QoS bandwidth percentages for a hub site after the site is provisioned (Day N).

Procedure

Step 1 From the IWAN app home page, click **Set up Branch Sites**. The Sites page opens.

Step 2 Click the **Sites** tab.

Step 3 Click the pencil icon (Edit Site) for a hub site.



Note You can also reach this page by clicking **Configure Hub Site & Settings** on the IWAN front page, and then clicking the IWAN Aggregation Site tab.

Step 4 Click the pencil icon on a WAN link (link between router and cloud). The Configure Link dialog box opens.

- Step 5** In the Configure Link dialog box, click the **Edit** (pencil) icon next to the Service Provider field. A dialog box opens, showing information for the specific service profile.
 - Step 6** Modify the QoS bandwidth percentages as needed.
 - Step 7** Click **Update**. The modified bandwidth percentages are applied to the WAN link.
-

Modifying the QoS Bandwidth Percentages for a Service Profile

You can modify the QoS bandwidth percentages globally for a service profile at any time. Any WAN connection using the service profile is updated, whether the connection is for a hub or for a branch site. This operation is available even after sites using the service profile have been provisioned (Day N).

Updating the QoS bandwidth percentages globally for the service profile can save time, compared with updating the percentages individually for each connection. This may be useful when the changes are intended for each WAN connection that uses the specific service profile.

Procedure

- Step 1** From the IWAN app home page, click **Configure Hub Site & Settings**. The Network Wide Settings page opens.
- Step 2** Open the **Service Providers** tab.

- Step 3** The “Available QoS models for Service Providers” section lists existing service profiles, including default and user-created profiles. To edit a service profile, click the pencil icon for the profile. The Edit Service Profile dialog box opens.

Class Name	DSCP	Priority Bandwidth (%)	Remaining Bandwidth (%)
VOICE	EF	20	
CALL-SIGNALING	CS3		4
CRITICAL-DATA	AF21		25
INTERACTIVE-VIDEO	AF41		30
NET-CONTROL-MGMT	CS6		5
SCAVENGER	CS1		1
STREAMING-VIDEO	AF31		10
DEFAULT	0		25
			Total: 100

- Step 4** Modify the QoS bandwidth percentages as needed.
- Step 5** Click the **Update** button. The modified bandwidth percentages are applied to all WAN links using the service profile.

Deleting a User-defined QoS Bandwidth Service Profile

You can delete a user-defined QoS bandwidth service profile that is not in use.

Procedure

- Step 1** From the IWAN app home page, click **Configure Hub Site & Settings**. The Network Wide Settings page opens.
- Step 2** Open the **Service Providers** tab.
- Step 3** The “Available QoS models for Service Providers” section lists existing service profiles, including default and user-created profiles. To delete a user-defined service profile, click the “X” icon for the profile.

If you attempt to delete a service profile that is in use, the IWAN app displays a warning.

Setting the Geographic Location of a Hub Site

Setting the geographic location of a hub site is optional. The location may be set at any time, even after provisioning the site (Day N).

After setting the geographic site location, that information appears on the Sites list page, and in the Site Details page for the site.

Procedure

-
- Step 1** From the IWAN app home page, click **Configure Hub Site & Settings**. The Network Wide Settings page opens.
- Step 2** Open the IWAN Aggregation Site tab.
- Step 3** Above each hub site, do one of the following:
- a. Enter a city name in the field. As you type, city options will appear. Select one.
- or
- b. Click Set Geo to set the location in a map view.
-

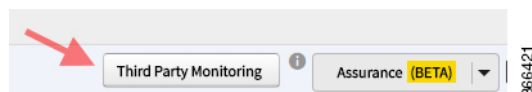
Collecting Network Data Using LiveAction

The IWAN App operates together with a network statistics “collector” to collect network performance data from the IWAN network. Specifically, the collector exports Cisco AVC and Performance Routing (PfR) Netflow records from routers in the network to the IWAN App.

By default, the IWAN App operates with [Cisco Prime Infrastructure](#) to collect network performance data. Optionally, you can configure the IWAN App to use [LiveAction](#) for collecting performance data.

Indication that the IWAN App Is Using LiveAction

When the IWAN App is configured to use LiveAction, the map view provides an indicator of third-party monitoring.



Limitations When Using LiveAction

- When using LiveAction to collect network data, you cannot filter the display of IWAN sites by application status.
- The site details dialog boxes do not display the application status.

Enabling LiveAction Network Monitoring

For information about enabling LiveAction network monitoring, see the LiveAction templates in [Custom Configuration Default Templates, page 6-2](#).

Configuring LiveAction

Procedure

-
- Step 1** From the IWAN app home page, click **Configure Hub Site & Settings**. The Network Wide Settings page opens.
 - Step 2** Open the System tab.
 - Step 3** In the Netflow Collector section:
 - a.** In the Netflow Destination IP field, configure the collector address.
 - b.** In the Port Number field, enter 2055, the port used by Live Action.



Note When using Cisco Prime Infrastructure, set the port number to 9991.

Interoperability between APIC-EM and a non-IWAN-enabled Network

If devices at an IWAN-enabled branch site managed by APIC-EM handle traffic flowing to or from a non-IWAN-enabled network, use the IWAN App to manually configure the non-IWAN-enabled network as an enterprise prefix list for the devices. Without this, the IWAN App may be unable to provision devices at the branch site. There are two ways to add the non-IWAN-enabled network as an enterprise prefix list - create a global address pool as a LAN brownfield pool or add a DC prefix list.

Adding a LAN Brownfield Pool

Procedure

-
- Step 1** From the IWAN app home page, click **Configure Hub Site & Settings**.
 - Step 2** Open the IP Address Pools tab.
 - Step 3** In the Global Address Pool area, click the **Add Address Pool** button. A new line is added to the Global Address Pool table.
 - Step 4** On the new line for defining an address pool, in the IP Pool Role column, select **LAN Brownfield**.
 - Step 5** On the new line, enter the network IP address and mask of the non-IWAN-enabled network.
-

Adding a DC Prefix List

Procedure

- Step 1** From the IWAN app home page, click **Configure Hub Site & Settings**.
 - Step 2** Open the IWAN Aggregation Site tab.
 - Step 3** Click the icon for the hub. The LAN Routing dialog box opens.
 - Step 4** In the LAN Routing dialog box, click **Add DCIP/Mask** and enter the subnet IP and mask and of the non-IWAN-enabled network. Click the plus sign (+) to complete the entry.
 - Step 5** In the LAN Routing dialog box, click **Save**.
-



Managing Branch Sites

This chapter contains the following sections:

- [Overview, page 5-1](#)
- [Workflow for Managing Branch Sites, page 5-4](#)
- [Bootstrapping Greenfield Devices, page 5-4](#)
- [Adding and Provisioning Greenfield Devices to the Branch Site, page 5-5](#)
- [Adding and Provisioning Brownfield Devices to the Branch Site, page 5-10](#)
- [Viewing Site Status Information, page 5-22](#)
- [Support for 4G/Cellular Technology for WAN Link, page 5-23](#)
- [4G-Cellular Support for MPLS Cloud, page 5-25](#)
- [Updating the WAN Bandwidth of a Provisioned Branch Site, page 5-26](#)
- [Updating the WAN IP Parameters of a Provisioned Branch Site, page 5-27](#)
- [Modifying the QoS Bandwidth Percentages for a Branch Site, page 5-29](#)

Overview

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

Greenfield and Brownfield Devices

You can add and provision two types of devices:

- Greenfield Devices
 - Greenfield devices are brand new out-of-the-box routers.
 - Discovered by the Cisco Plug-n-Play (Cisco PnP) application.
 - No pre-existing configurations to synchronize with IWAN-based configuration, no configuration conflicts to address.

- **Brownfield Devices**
 - Brownfield devices belong to existing sites that are being added to Cisco IWAN.
 - Discovered by the Cisco APIC-EM application.
 - May have pre-existing configurations to synchronize with IWAN-based configuration.
 - While provisioning a brownfield device, the IWAN app performs a validation step to determine whether any configuration conflicts exist. If an error or warning is reported, correct the issue on the device and perform the validation again. See [Brownfield Validation Messages](#).

Deployment Requirements

- For both greenfield and brownfield devices, ensure that the device is added to the system using the WAN interface only.
- For successful deployment, the controller must be able to reach the device WAN interface before the deployment.

IWAN App Operation with NAT

Spoke Behind NAT

Use of network address translation (NAT) is supported for WAN links connected to public Internet clouds for all topologies—both for greenfield devices (using PnP discovery) and brownfield branch devices (discovered through APIC-EM).

For greenfield devices, the PnP application automatically adds the NAT router into Cisco APIC-EM using the public NAT IP address.

For brownfield devices, discover the device using the external or public IP address.

To enable connections from Cisco APIC-EM to the NAT router during provisioning, use the following standard ports:

- SSH—port 22
- Telnet—port 23
- SNMP—port 161

After the provisioning is complete and the branch devices are managed by Cisco APIC-EM using the loopback interface, you can optionally remove these configurations.



Note

The NAT router is not managed by Cisco IWAN. Configure the NAT router manually.

APIC-EM Behind NAT

The IWAN app supports network topologies in which the APIC-EM controller communicates with spoke (branch) sites through network address translation (NAT).

When setting up an APIC-EM-behind-NAT network, configure the NAT public IP address of the APIC-EM controller before provisioning any spoke sites. Configure the address in the following location:

IWAN app home page > **Configure Hub Site & Settings** > **System** tab > **NAT/Proxy IP Address** section

NAT/Proxy IP Address ⓘ

* APIC-EM behind NAT/Proxy No Yes

APIC-EM NAT/Proxy IP

366196

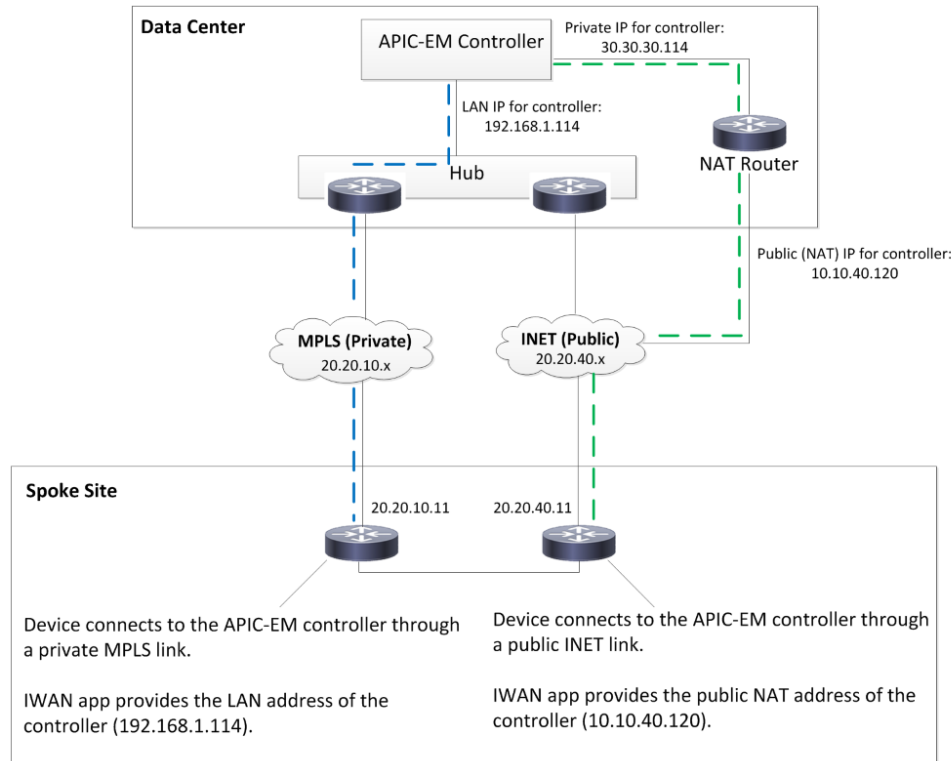
This is a “day 0” (before provisioning any spoke sites) requirement. It is not a “day N” (after spoke sites have been provisioned) option.

IWAN App Provides the NAT Public IP Address to Spoke Devices

Spoke devices that connect to the APIC-EM controller through a public link (such as INET) require the NAT public address of the controller.

- **Greenfield sites:** The PnP application automatically acquires the APIC-EM public NAT IP address. During provisioning, the IWAN app provides this address to the spoke devices that connect by public link.
- **Brownfield sites:** During provisioning, the IWAN app provides the manually configured NAT public IP address of the APIC-EM controller to the spoke devices that connect by public link.

Note: During provisioning, add a brownfield spoke site using its public link interface IP address, or its NAT public IP address (in the case of spoke-behind-NAT).



Limitations

The APIC-EM NAT IP can be changed at Day N only if no spoke sites are configured. If it is necessary to change the APIC-EM NAT IP and spoke sites have been configured, delete the spoke sites, then change the APIC-EM NAT IP.

Workflow for Managing Branch Sites

Table 5-1 Basic Workflow for Managing Branch Sites

No.	Task	Reference
1	Bootstrap devices discovered by the Cisco PnP application.	Bootstrapping Greenfield Devices, page 5-4
2	Add devices to Cisco IWAN and then provision them to the sites.	Adding and Provisioning Greenfield Devices to the Branch Site, page 5-5 Adding and Provisioning Brownfield Devices to the Branch Site, page 5-10
3	View the site status.	Viewing Site Status Information, page 5-22

Bootstrapping Greenfield Devices

You can bootstrap devices discovered by the Cisco PnP application. These are 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. If required, you can use this file as a template to manually copy to the device so that PnP can call-home.

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/xe-3e/pnp-xe-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

- Saving the configuration

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.

- VTY lines

There must be at least 16 VTY lines configured.

- Support for 4G/cellular interface

The IWAN app now supports configuration of a 4G/cellular interface for Cisco ISR4000 Series routers at branch sites.

Supported Connection Types

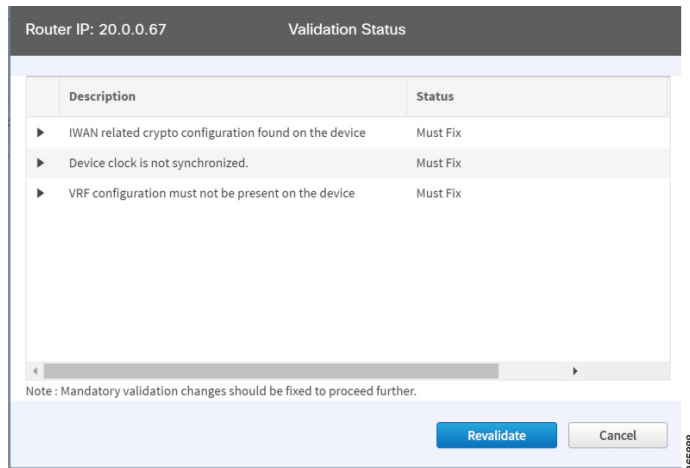
The IWAN app supports many types of routing and switching devices at branch sites, but support for some features is limited to specific types of devices. The following table describes supported connection types.

WAN connection type	Devices that support the connection type
Internet (including T1, E1, Ethernet)	All
MPLS	All
4G/cellular interface	Cisco ISR 4000 Series routers on MPLS link only

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 is displayed as shown in the following figure:



Field	Description
Checkbox	Click this checkbox to choose the unclaimed device for provisioning.
Serial Number	Serial number of the device.
IP Address	IP address of the device. Note If a NAT router is present, then the NAT IP address appears in this column.
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 indicates a greenfield device. • APIC—Discovered by the Cisco APIC-EM application. This indicates 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 Select 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.

The available topology options depend on the network settings configured for the hub site on the IWAN app “Network wide settings” page. See the configuration of service provider count in [Configuring IP Address Pools, page 4-12](#) and the topology in [Configuring Service Providers, page 4-9](#).

Topology options may include:

- 1-link option: Requires hub router connected to one (1) WAN cloud
- 2-link option: Requires hub router connected to two (2) WAN clouds
- 3-link option: Requires hub router connected to three (3) WAN clouds



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. The WAN type selected in the previous step determines the fields that appear in the Configure WAN Cloud dialog box. (These fields differ, depending on the WAN type, such as T1, E1, Ethernet, or Cellular.)
- b. Enter the required properties, and click **Save**. The + icon next to the WAN cloud changes to a checkmark icon.
 - For a Public WAN, the Configure WAN Cloud dialog box displays the following fields.

Field	Description
WAN Type	Public
Interface Type	Type of interface. Values: T1, E1, Ethernet, Cellular
Interface	Choose the interface that connects to the WAN cloud from the drop-down list.
Connect to WAN	Connection method.
NAT Enabled	Check this option if NAT IP address is used.
NAT IP Address	Public IP address.
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 <p>Note This option is not shown if interface type is Cellular.</p>
Upload (Mbps)	Upload bandwidth (in Mbps).
Download (Mbps)	E1 interface—Preset bandwidth value of 3. T1 interface—Preset bandwidth value of 1.5. GigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 1000 TenGigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 9000 For interfaces of types other than E1, T1, GigabitEthernet, or TenGigabitEthernet, the default range will be: 0.1 to 9000 Mbps
Service Provider	Choose a service profile from the drop-down list. The drop-down list includes default and custom 8 Class service profiles that were configured in the Service Providers tab.

- For a Private non-MPLS WAN, the Configure WAN Cloud dialog box displays the following fields.

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)	E1 interface—Preset bandwidth value of 3. T1 interface—Preset bandwidth value of 1.5. GigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 1000 TenGigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 9000 For interfaces of types other than E1, T1, GigabitEthernet, or TenGigabitEthernet, the default range will be: 0.1 to 9000 Mbps
Service Provider	Choose a service profile from the drop-down list. The drop-down list includes all default and custom service profiles (4 Class, 5 Class, 6 Class, and 8 Class) that were configured in the Service Providers tab.

- For an MPLS cloud, the Configure WAN Cloud dialog box displays the following fields.

Field	Description
WAN Type	Private
Interface	Choose an interface from the drop-down list.
Connect to WAN	MPLS
Upload (Mbps)	Upload bandwidth (Mbps)
Download (Mbps)	Download bandwidth (Mbps)
Service Provider	Choose a service profile from the drop-down list. The drop-down list includes all default and custom service profiles (4 Class, 5 Class, 6 Class, and 8 Class) that were 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.

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

Field	Description
LAN Interface	
<i>Site</i> 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.

Tutorial Video

[IWAN App Brownfield Branch Provisioning](#)

**Note**

- Saving the configuration

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.

- VTY lines

There must be at least 16 VTY lines configured.

- SNMP

Devices that are configured with SNMP version 2 or version 3 can be used as branch devices.

- Support for 4G/cellular

The IWAN app now supports configuration of a 4G/cellular interface for Cisco ISR4000 Series routers at branch sites.

The IWAN app supports many types of routing and switching devices at branch sites, but support for some features is limited to specific types of devices. The following table describes supported connection types.

WAN connection type	Devices that support the connection type
Internet (including T1, E1, Ethernet)	All
MPLS	All
4G/cellular	Cisco ISR 4000 Series routers

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.

The screenshot shows the Cisco IWAN Sites page. At the top, there are three summary cards: 'Bootstrap' with 3 Downloads Available, 'Device(s)' with 2 Newly Discovered Device(s), and 'Site(s)' with 2 Hubs(s) and 0 Branch(es). Below these cards is a table with columns: Serial Number, IP Address, Type, Site Name, Host Name, Discovered By, and Validation Status. The table contains two rows of data.

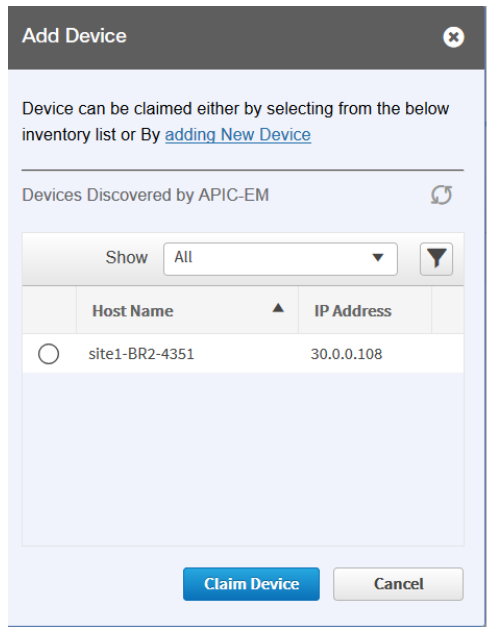
Serial Number	IP Address	Type	Site Name	Host Name	Discovered By	Validation Status
F001816A011	20.0.0.67	ISR4351/K9	Falls Church	site1-BR1-4351	APIC	SUCCESS
FTX1925AHC3	30.0.0.107,20.0.0.66	ISR4431/K9	San Jose	site4-4431	PNP	N/A

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.



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 figure above). 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**.

Field	Description
Router Management IP	IP address for the new device. If you have a spoke device behind a NAT router and you want that NAT router to be the management router, enter the IP address of the NAT router in this field.
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.

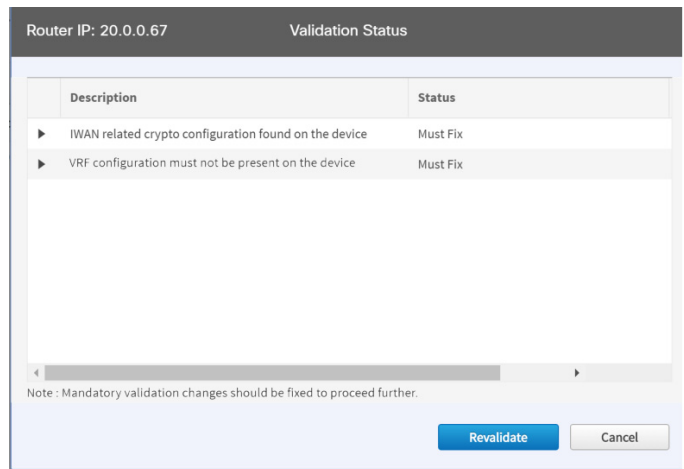
Field	Description
Mode (Displayed if you chose SNMP V3.)	Choose the mode from the drop-down list. Options are: <ul style="list-style-type: none"> • Authentication and Encryption • No Authentication and No Encryption • Authentication and No Encryption
Auth. Type (Displayed if you chose SNMP V3.)	Displayed 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.

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

The Cisco IWAN app accesses the router and checks its configuration to determine if it has any configuration that might conflict with the Cisco IWAN app. 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, select 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.

The available topology options depend on the network settings configured for the hub site on the IWAN app “Network wide settings” page. See the configuration of service provider count in [Configuring IP Address Pools, page 4-12](#) and the topology in [Configuring Service Providers, page 4-9](#).

Topology options may include:

- 1-link option: Requires hub router connected to one (1) WAN cloud
- 2-link option: Requires hub router connected to two (2) WAN clouds
- 3-link option: Requires hub router connected to three (3) WAN clouds



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. Enter the required properties, and click **Save**. The + icon next to the WAN cloud changes to a checkmark icon.
 - For a Public WAN, the Configure WAN Cloud dialog box displays the following fields.

Field	Description
WAN Type	Public
Interface Type	Type of interface. Values: T1, E1, Ethernet, Cellular
Interface	Choose the interface that connects to the WAN cloud from the drop-down list.
Connect to WAN	Connection method.
NAT Enabled	Check this option if NAT IP address is used.
NAT IP Address	Public IP address.

Enable	<p>Choose one of the two radio buttons as appropriate:</p> <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 <p>Note This option is not shown if interface type is Cellular.</p>
Upload (Mbps)	Upload bandwidth (in Mbps).
Download (Mbps)	<p>E1 interface—Preset bandwidth value of 3.</p> <p>T1 interface—Preset bandwidth value of 1.5.</p> <p>GigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 1000</p> <p>TenGigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 10000</p> <p>For interfaces of types other than E1, T1, GigabitEthernet, or TenGigabitEthernet, the default range will be: 0.1 to 10000 Mbps</p>
Service Provider	<p>Choose a service profile from the drop-down list.</p> <p>The drop-down list includes default and custom 8 Class service profiles that were configured in the Service Providers tab.</p>

- For a Private WAN, the Configure WAN Cloud dialog box displays the following fields.

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	<p>Customer Edge Server IP Address. This field is auto-populated if the interface has a static IP address already configured.</p> <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)	E1 interface—Preset bandwidth value of 3. T1 interface—Preset bandwidth value of 1.5. GigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 1000 TenGigabitEthernet interface—Select a bandwidth from the drop-down list or enter a value in the range: 0.1 to 10000 For interfaces of types other than E1, T1, GigabitEthernet, or TenGigabitEthernet, the default range will be: 0.1 to 10000 Mbps
Service Provider	Choose a service profile from the drop-down list. The drop-down list includes all default and custom service profiles (4 Class, 5 Class, 6 Class, and 8 Class) that were configured in the Service Providers tab.

- For an MPLS cloud, the Configure WAN Cloud dialog box displays the following fields.

Field	Description
WAN Type	Private
Interface	Choose an interface from the drop-down list.
Connect to WAN	MPLS
Upload (Mbps)	Upload bandwidth (Mbps)
Download (Mbps)	Download bandwidth (Mbps)
Service Provider	Choose a service profile from the drop-down list. The drop-down list includes all default and custom service profiles (4 Class, 5 Class, 6 Class, and 8 Class) that were 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 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.

Configure VLAN

LAN Interface

* BR1-ISR.EXAMPLE.COM Interface GigabitEthernet0/0/2

* BR2-ISR Interface GigabitEthernet0/0/1

VLAN

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

Save Cancel

365885

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.

Configure VLAN

LAN Interface

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

IP Address 20.0.0.67 / 8

Save Cancel

365873

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



Note VLANs are displayed per device.

LAN Routing Configuration

Site 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

* AS Number

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	<p>Can be one of the following:</p> <ul style="list-style-type: none"> • Delete icon—Click to delete the site that has issues. See Deleting a Hub Site, page 9-5, Deleting a Transit Hub Site, page 9-5, or Deleting a Branch Site, page 9-6. • Recovery icon—Option available if recovery for this site is possible. See Recovering a Cisco IWAN Site, page 9-4. • Edit (pen) icon—Click to do the following: <ul style="list-style-type: none"> – Add or delete site prefixes after hub provisioning. This option is only available for L3 brownfield sites. See Adding or Deleting Site Prefixes, page 9-8. – Modify the QoS bandwidth percentage for a selected branch site. Modifying the QoS Bandwidth Percentages for a Branch Site, page 5-29.

Support for 4G/Cellular Technology for WAN Link

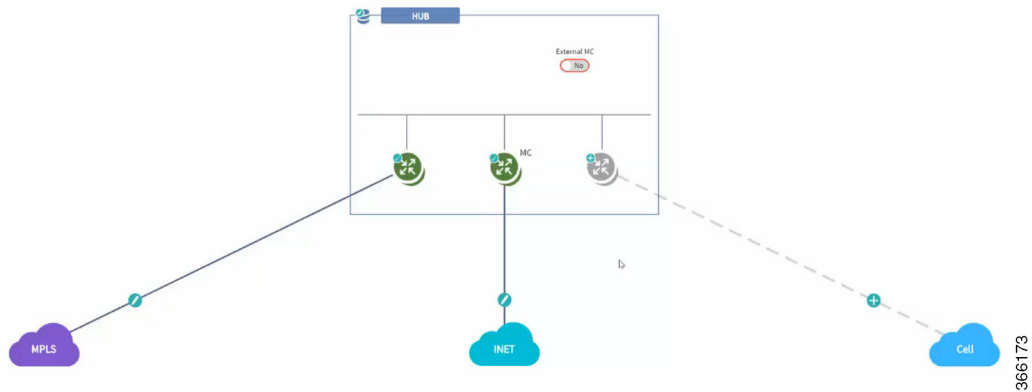
The IWAN app supports use of a 4G cellular connection by Cisco ISR 4000 Series routers at branch sites, as a WAN connection option.

Example Scenario

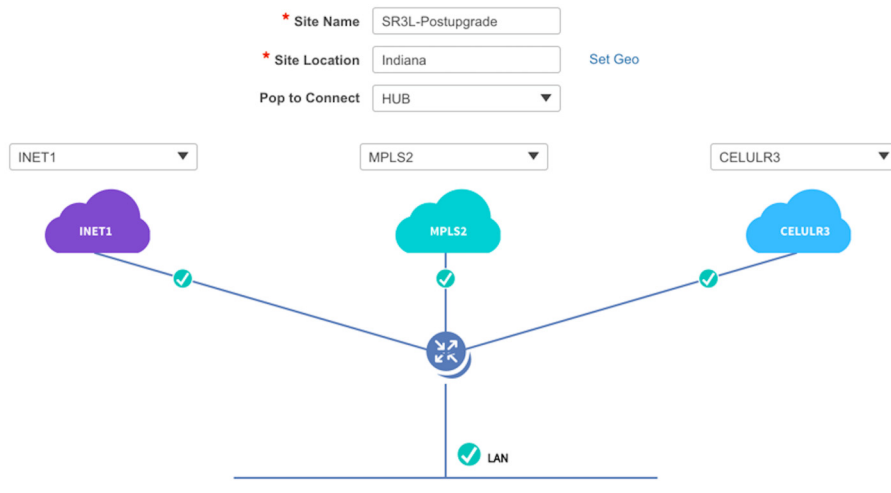
The full instructions for provisioning appear in the [Adding and Provisioning Greenfield Devices to the Branch Site, page 5-5](#) and [Adding and Provisioning Brownfield Devices to the Branch Site, page 5-10](#) sections. The following is a brief description of the provisioning steps for an example scenario using 4G connection for a WAN link:

Procedure

-
- Step 1** In **Configure Hub Site & Settings > Service Providers** tab, configure a services provider with a 4G cellular connection. Note that cellular connections must be configured with a WAN Type value of Public.
- Step 2** In the **Configure Hub Site & Settings > IWAN aggregation site** tab, connect a hub site device to the 4G cellular WAN in the graphical display of the topology.



- Step 3** On a branch site that includes a Cisco ISR 4000 Series device, connect the device to the 4G cellular WAN.
- On the Sites page, select the Device(s) tab. Select an unclaimed Cisco ISR 4000 Series device. This displays the Provisioning Site page.
 - At the Select Topology step, select a topology and click **Next**.
 - At the Select L2/L3 step, select an option and click **Next**.
 - At the Configure Topology step, click the plus-sign on the link between the device and one of the WAN "cloud" options. A Configure WAN Cloud pop-up opens. For each interface on the device, configure any necessary details and click **Save** to proceed to the next interface on the device. When the "Connect to WAN" field in the pop-up displays the name of the 4G cellular WAN, ensure that the Interface field is configured to "Cellular". Click **Save** to complete configuration of the WAN connections for the device. The Configure VLAN pop-up opens.
 - Configure the LAN or verify the existing settings and click Save. The Provisioning Site page appears, showing that the WAN connections for the branch device, including the 4G cellular WAN link. The WAN connections of the device appear as solid lines with a check icon on the line, indicating a valid configuration.



- Click **Apply Changes** to apply the configuration to the device. A Provisioning Site Summary page appears. The cellular WAN link appears in the summary.

Notes and Limitations

Greenfield devices

Supported topologies

- L2 greenfield single router two links
- L2 greenfield Single router three links
- L2 greenfield field dual router three links
- L2 greenfield Dual router dual link
- L2 greenfield Single router single link

Using cellular link for management interface

To use 4G cellular as a management interface on the IWAN app, ensure that the cellular interface is reachable from the APIC-EM controller.

Brownfield devices

Supported topologies

- Brownfield L2/L3 Single router single link
- Brownfield L2/L3 Single router dual link
- Brownfield L2/L3 Single router 3 link
- Brownfield L2/L3 Dual router single link
- Brownfield L2/L3 Dual router three link

Using cellular link for management interface: Supported

To use 4G cellular as a management interface on the IWAN app, ensure that the cellular interface is reachable from the APIC-EM controller.

Hub WAN address connected to cellular cloud must be reachable

The hub WAN address connected to the cellular cloud must be reachable from the cellular branch device before provisioning.

4G-Cellular Support for MPLS Cloud

The IWAN App supports use of 4G-cellular WAN links on a private MPLS cloud.

- All topologies are supported.
- Any topology may include one 4G-cellular interface.

Day 0:

- [Adding and Provisioning Greenfield Devices to the Branch Site, page 5-5, step 7.](#)
- [Adding and Provisioning Brownfield Devices to the Branch Site, page 5-10, step 9.](#)

Day N:

- [Updating the WAN Bandwidth of a Provisioned Branch Site, page 5-26](#)

Limitations

- The 4G-cellular interface may be used for WAN clouds, not within a LAN.

Updating the WAN Bandwidth of a Provisioned Branch Site

You can change the upload or download WAN bandwidth after a branch site is provisioned ("day N"). Also see [Updating the WAN Bandwidth of a Provisioned Hub Site, page 4-33](#).



Note

Beginning with the IWAN App 1.5.0 release, a 4G interface can support an MPLS cloud.

Valid bandwidth values depend on the interface type:

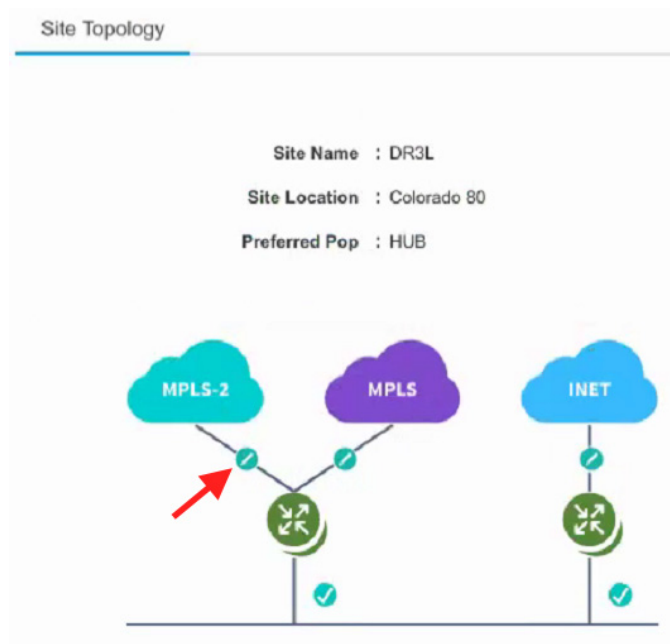
- TenGigabit interface: 0.1 to 10000 Mbps
- Gigabit interface: 0.1 to 1000 Mbps
- Cellular interface: 0.1 to 300 Mbps

Use the following procedure to update the bandwidth settings.

Procedure

- Step 1** From the IWAN app home page, click **Set up Branch Sites**.
- Step 2** Click the **Sites** tab.
- Step 3** Click the pencil icon (Edit Site) for a spoke (branch) site. The Update Site dialog box opens.

- Step 4** In the Site Topology area, click the pencil icon on a WAN link. The Configure WAN Cloud parameters are displayed in the dialog box.



- Step 5** In the Upload or Download fields, enter new bandwidth values.
- Step 6** Click the **Update** button.

Updating the WAN IP Parameters of a Provisioned Branch Site

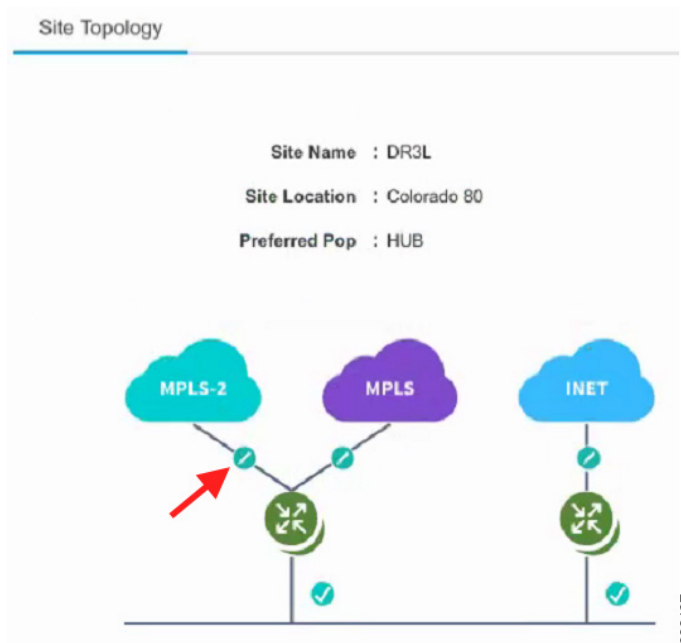
You can change the WAN IP, mask, or next hop settings for a spoke site even after it has been provisioned ("day N").

Use the following procedure to change the IP settings.

Procedure

- Step 1** From the IWAN app home page, click **Set up Branch Sites**.
- Step 2** Click the **Sites** tab.
- Step 3** Click the pencil icon (Edit Site) for a spoke (branch) site. The Update Site dialog box opens.

Step 4 In the Site Topology area, click the pencil icon on a WAN link.



The link settings appear in the dialog box. The available options depend on the type of WAN link.

Step 5 Edit the IP address in or more of the following fields:

- CE IP Address: “Customer edge” IP address. This is the WAN IP address of the branch WAN link.
- CE IP Mask: “Customer edge” IP mask.
- PE IP Address: “Provider edge” IP. This is the gateway of the next hop for the WAN link.

Step 6 Click the **Update** button.



Note To discard changes, click the **Reset** button.

If you enter a value for CE or PE IP address that is not reachable, the operation will succeed, but connectivity between the APIC-EM controller and the site will be lost. If this occurs, restore connectivity. The method for restoring connectivity depends on the specific network. Possible remedies include:

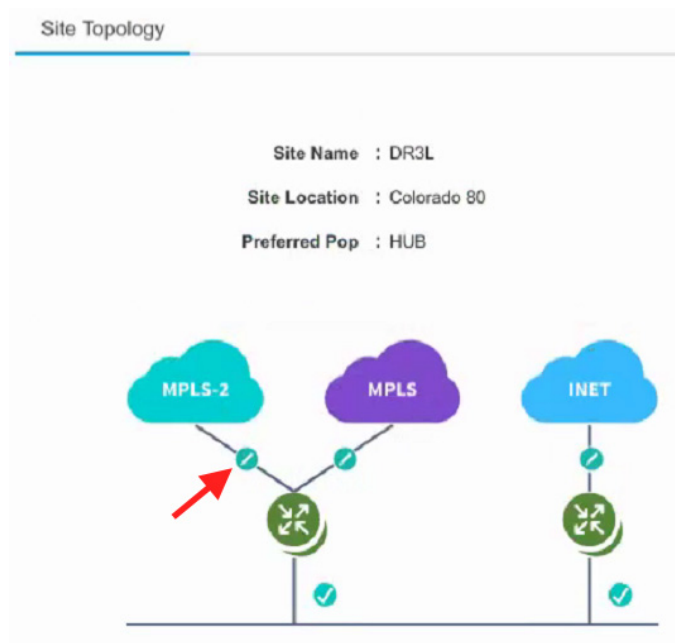
- If the site specified by the new IP address is not active, activate the site to enable connectivity.
- If a new IP address was specified in error, restore the previous IP address. This requires configuring the IP address value directly on the device (not through the IWAN app). Once complete, update the IWAN app with the new valid IP using the “Updating the WAN IP Parameters of a Provisioned Branch Site” procedure described in this section.

Modifying the QoS Bandwidth Percentages for a Branch Site

You can modify the QoS bandwidth percentages for a branch site after the site is provisioned (Day N).

Procedure

- Step 1** From the IWAN app home page, click **Set up Branch Sites**. The Sites page opens.
- Step 2** Click the **Sites** tab.
- Step 3** Click the pencil icon (Edit Site) for a branch site. The Update Site dialog box opens.
- Step 4** In the Site Topology area, click the pencil icon on a WAN link (link between router and cloud).



The Configure Link dialog box opens.

- Step 5** In the Configure Link dialog box, click the **Edit** (pencil) icon next to the Service Provider field. A dialog box opens, showing information for the specific service profile.
- Step 6** Modify the QoS bandwidth percentages as needed.
- Step 7** Click **Update**. The modified bandwidth percentages are applied to the WAN link.



Managing Devices

This chapter contains the following sections:

- [Overview, page 6-1](#)
- [Custom Configuration of Devices, page 6-1](#)
- [Replacement of a Hub Device, page 6-5](#)

Overview

Each hub site or branch site may have one or more associated devices. The IWAN app provides methods for managing the devices individually, including the Custom Configuration feature, which enables executing batch CLI commands on devices in the network.

Custom Configuration of Devices

Custom Configuration is a mechanism for executing CLI configuration commands on devices within the IWAN network. The feature works similarly to executing a batch file of commands, but operates remotely from the IWAN app. Enter a set of commands (and optionally save them for later use), and select the devices on which to execute the configuration commands. The IWAN app sends the commands to each selected device and then indicates whether execution was successful or not.

Rollback Mechanism in Case of Command Failure

If the command execution is not successful, the feature provides a mechanism for rollback—executing a set of commands to reverse any failed configuration operations.

Per-device Parameters

Custom Configuration provides a “parameter” feature that prompts you at run-time to enter parameter values specific to each device on which the commands are being executed. When you execute the configuration, the system prompts you to enter values one-by-one for each selected target device. Parameters appear as a dollar sign (\$) followed by a parameter name. Example: \$interface.

A maximum of 10 parameters may be used.

Custom Configuration Default Templates

The IWAN App includes default configuration templates that provide CLI-level support for various network features. Each template consists of a set of CLI commands to perform a pre-defined function. The templates may include “per-device parameters”—when you execute the configuration, the system prompts you to enter values for the parameters, one-by-one for each selected target device.

The following table summarizes the configuration templates included by default.

Table 6-1 Custom Configuration Default Templates

Template	Description
Liveaction-flow	<p>Enables LiveAction network monitoring.</p> <p>Configures a NetFlow monitor compatible with LiveAction and configures the monitor to export to the LiveAction Server.</p> <p>Choose one of the following templates:</p> <ul style="list-style-type: none"> • LiveAction-SR1L –Single router with 1 WAN link • LiveAction SR2L – Single router with 2 WAN links • LiveAction SR3L – Single router with 3 WAN links <p>The following input is required when executing the template:</p> <ul style="list-style-type: none"> • LIVEACTION_IP- IP: Address of the LiveAction server. Example: 10.1.0.10 • TUN_INTERFACE: Name of the DMVPN tunnel interface. Example: Tunnel10
Direct Internet Access	<p>Configures Direct Internet Access (DIA).</p> <p>Configures NAT, zone-based policy firewall (ZFW) and Policy-Based Routing (PBR) for Direct Internet Access from a branch. The template also configures tracking of the Internet Gateway IP and failover to Tunnel Overlay if the Internet Gateway is not reachable.</p> <p>Note DIA configuration templates are applicable only for Cisco ISR 4000 series routers.</p> <p>The following input is required when executing the template:</p> <ul style="list-style-type: none"> • LAN_SUBNET: Subnet address for LAN with wildcard mask. Example: 10.1.0.0 0.0.255.255 • INET_WAN_INTERFACE_NAME: Internet WAN interface name. Example: GigabitEthernet 0/0/0 • INET_VRF_NAME: Name of the FVRF applied on the WAN interface. Example: IWAN-TRANSPORT-2 • INET_GW_IP: IP address of the internet gateway. Example: 70.70.70.2 • LAN_INTERFACE_NAME: LAN Interface name. Example: GigabitEthernet0/0/2

Table 6-1 Custom Configuration Default Templates

Template	Description
Guest Internet Access	<p>Enables guest internet access on an IWAN branch router.</p> <p>Creates a guest VLAN interface on the router with NAT and zone-based policy firewall (ZFW). The guest VLAN is assigned to a separate VRF called IWAN-GUEST.</p> <hr/> <p>The following input is required when executing the template:</p> <ul style="list-style-type: none"> • INET_WAN_INTERFACE_NAME: Internet WAN interface name. Example: GigabitEthernet 0/0/0 • INET_GW_IP: IP address of the internet gateway. Example: 70.70.70.2 • GUEST_SUBNET: Subnet address of the Guest VLAN with wildcard mask. Example: 10.2.10.0 0.0.0.255 • GUEST_INTERFACE_NAME: Sub-interface name used for Guest VLAN. Example: GigabitEthernet 0/0/0.66 • GUEST_VLAN_ID: VLAN ID number for Guest VLAN. Example: 66 • GUEST_INTERFACE_IP: IP address for the Guest VLAN interface with mask. Example: 10.1.10.1 255.255.255.0 • GUEST_MASK: Subnet mask used for the Guest VLAN interface. Example: 255.255.255.0

Enabling Custom Configuration

Use the following procedure to enable execution of CLI configuration commands using the Custom Configuration feature.


Procedure

-
- Step 1** On the site list page, display the Custom Config Status column by clicking the gear icon above the table and selecting **Custom Config Status**. The column is displayed and the **Custom Config** button appears above the table.
-

Creating and Executing a Custom Configuration

Use the following procedure to open the Custom Configuration window to create a Custom Configuration CLI batch file, or to execute an existing Custom Configuration, called a template.

Procedure

-
- Step 1** On the site list page, click the **Custom Config** button above the table. If the button is not displayed, see [Enabling Custom Configuration, page 6-3](#). The Custom Config page appears.
- Step 2** Select an existing custom configuration or click the plus-sign icon () to create a new one.

- Step 3** In the Actual pane, enter the CLI commands to execute, similarly to a batch CLI command file. The commands will be executed in configuration mode on the device.



Note The IWAN app does not perform any validation of the entered commands.

- Step 4** (Optional) The full set of commands will be executed on all selected devices. To individually enter parameters specific to each device on which the configuration commands are being executed, use a "parameter" value in the CLI command: a dollar sign (\$) followed by a parameter name. Example: \$interface.

When you execute the custom configuration, you will be prompted to enter values for this "parameter" one-by-one for each selected target device. A maximum of 10 parameters may be used.

- Step 5** In the Rollback pane, enter the commands to execute in case one or more of the configuration commands in the Actual pane fail to execute correctly. For information about handling failed executions of custom configuration commands, see [Handling Failed Custom Configuration Executions, page 6-4](#).
- Step 6** In the Devices pane, select the devices on which to execute the CLI configuration commands.
- Step 7** Click **Save** to save the configuration without executing. Click **Deploy** to execute the configuration on the specified devices. The site list page opens automatically, enabling you to view the **Success** or **Failure** status of execution of the configuration commands.
-

Viewing Status of Custom Configuration Execution

On the site list page, the Custom Config Status column shows the Success or Failure status of execution of the configuration commands per site.

If execution fails for any device within a site, the Custom Config Status column for the site displays **Failure**. If a failure occurs, click the **Failure** link in the Custom Config Status column to display the status of each device within the site. For information about handling failed executions of custom configurations, see [Handling Failed Custom Configuration Executions, page 6-4](#).

Handling Failed Custom Configuration Executions

Use the following procedure to handle failed Custom Configuration CLI command execution.

Procedure

-
- Step 1** On the site list page, the Custom Config Status column shows the **Success** or **Failure** status of execution of the configuration commands per site. If execution fails for any device within a site, the Custom Config Status column for the site displays **Failure**. If a failure occurs, click the **Failure** link in the Custom Config Status column to open a Site Details pop-up.

- Step 2** The Site Details pop-up displays the status of each device within the site. For each site with **Failure** status, the Rollback option is displayed by default. Do one of the following to resolve the failure status for each device:
- To execute the rollback command(s), click **Deploy**.
 - To change the rollback commands, edit the rollback commands displayed in the window and click **Deploy**. This does not affect the saved version of the custom configuration.
 - To change the custom configuration commands and attempt to execute them again, click **Actual** to display the commands that failed to execute, edit the commands, and click **Deploy** to execute the edited commands. This does not affect the saved version of the custom configuration.
 - To skip any further command execution and remove the **Failure** status for the device, click **Ignore/Reset**.
-

Limitations of Custom Configuration

The Custom Configuration feature has the following limitations:

- Only IWAN provisioned devices are supported.
- Maximum number of characters for a saved Custom Configuration template name: 20
- The commands stored in a single Custom Configuration template ("Actual" commands and "Rollback" commands) must not exceed 9000 characters.
- Maximum number of per-device specified "parameters" (syntax: `$<parameter-name>`): 10
- Maximum number of devices on which to execute a Custom Configuration at once: 20
- Pushing a new set of configuration commands to a device does not automatically synchronize the new configuration back to the database. Consequently, any configuration that conflicts with the configuration that is pushed by the prescriptive IWAN app will be overwritten upon execution of the day N operation from the app.
- After creating a custom configuration, it is not possible to edit the configuration. If changes are necessary, copy the text from the existing configuration, create a new configuration, and paste in the text.

Replacement of a Hub Device

It is possible to replace a provisioned device (Day N) on a hub site. The object is to ensure that the new router operates exactly like the router that has been replaced. This is often called "RMA." This procedure does not apply to devices at branch sites.

Procedure

-
- Step 1** Using a console connection to the existing router (the one being replaced), make a copy of the running configuration (running-config) stored on the router. Save this copied running-config for a later step.
- Step 2** Disconnect the router to be replaced.
- Step 3** Connect the new router exactly as the previous router was installed.

- Step 4** Using a console connection to the newly installed router, paste in the running configuration that was copied (in an earlier step) from the old router.
- Step 5** (If SSH, and not Telnet, is used to discover the device) Enable SSH access to the new router, creating RSA keys and terminal VTY lines.

Use the following steps on the new device, in config mode:

```
ip ssh rsa keypair-name sshkeys

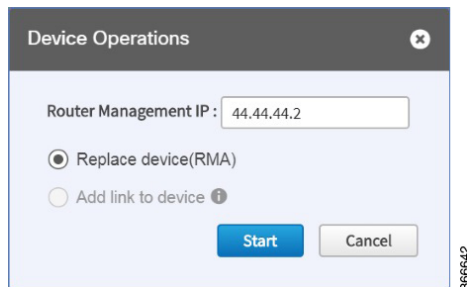
! Enables the SSH server for local and remote authentication on the router.
! For SSH Version 2, the modulus size must be at least 1024 bits.
crypto key generate rsa usage-keys label sshkeys modulus 1024

! Configures SSH control variables on your router.
ip ssh time-out 120

! configure SSH version 2 (will disable SSH version 1)
ip ssh version 2

!--- Enable SSH
line vty 0 15
transport input telnet ssh
```

- Step 6** From the IWAN app home page, click **Configure Hub Site & Settings**.
- Step 7** Click the **IWAN Aggregation Site** tab. The hub topology is displayed.
- Step 8** Click the device (router) to be replaced. The Device Operations dialog box appears.



- Step 9** In the Device Operations dialog box, select Replace Device (RMA) and click the **Start** button.

A dialog box appears, displaying a checklist of actions required before replacing the device. The system then performs an inventory collection, deletes the old trustpoints, and creates new trustpoints.



- Step 10** If the process cannot be completed, a message appears, describing the problem.
- If there is a connectivity issue, repair the connectivity issue and click the **Retry** button.
 - If the procedure fails despite efforts to troubleshoot, click the **Delete Device** button.
- Step 11** (Optional) If the old router had spokes configured and connected to the router, verify that the DMVPN tunnels are operational.
-



Administering Application Policies

This chapter contains the following sections:

- [Understanding the Categorize Applications Tab, page 7-1](#)
- [Understanding the Define Application Policies Tab, page 7-5](#)
- [Understanding the Application Bandwidth Tab, page 7-8](#)

Understanding the Categorize Applications Tab

The IWAN app operates with the Cisco NBAR2 Protocol Pack, which runs on routers within the IWAN network. NBAR2 categorizes network application traffic using the individual protocols in the Protocol Pack, in addition to any user-defined custom protocols. (“Protocols” define how NBAR2 categorizes a specific network application.) The IWAN app shows the applications defined by the NBAR2 Protocol Pack, grouped by application category.

The IWAN app 1.5.x releases operate with Protocol Pack 27.0.0 or 31.0.0. See the [Protocol Pack documentation](#) for details.

Use the **Categorize Applications** tab to view, edit, move, and add custom applications as shown in the following table:

Table 7-1 *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 7-2
2	Move applications into different categories.	Moving Applications to a Different Category, page 7-2
3	Edit application information.	Editing Application Information, page 7-3
4	Add new custom application to an existing category.	Adding a New Application, page 7-3
	Deleting Cisco IWAN custom applications.	Deleting NBAR2 Custom Applications, page 7-4

**Note**

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

Tutorial Video

[IWAN App Application Policy](#)

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 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 Application Category/By Applications** drop-down list, and select **View By Application Category**.
- Not all categories are shown by default. To view all categories, click the **Show** link in the instructional text.
- Step 4** To view all of the applications in a particular category, click the down arrow for a category.
- Step 5** To view a summary of the total number of applications, popular applications, and custom applications, see 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, traffic class.
-

Moving Applications to a Different Category

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

Procedure

-
- Step 1** From the Cisco IWAN 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 click **Apply Changes**.
-

Editing Application Information

Use this procedure to edit application information.

Procedure

-
- Step 1** From the Cisco IWAN 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 for 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 click **Save**.
-

Adding a New Application

Use this procedure to add a new custom application.

Procedure

-
- Step 1** From the Cisco IWAN 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 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.

Deleting NBAR2 Custom Applications

Use this procedure to delete NBAR2 custom applications.

Procedure

- Step 1** From the Cisco IWAN home page, click **Administer Application Policy**. The Application Policy page opens.
- Step 2** Click the **Categorize Applications** tab.
- Step 3** To delete a custom application, do the following:
 - a. In the left window, change the **View By** filter from **Application Category** to **Applications**.
 - b. Click the **Edit** icon next to the application. The Edit Application dialog box opens.
 - c. Click the **Delete** button in the Edit Application dialog box.



Note The Delete button is available only for custom applications (not EasyQoS custom apps or default Protocol Pack applications).

- d. Click **OK** in the confirmation box. The application is removed from the user interface. (The deletion is finalized in a later step with the **Apply Changes** button.)



Note If you change your mind, and do not want to delete the application, refresh the page. The application is restored with all of its configuration.

Step 4 To finalize the application deletion, click **Apply Changes** (top right corner).



Note After you click **Apply Changes**, the application cannot be restored.

Step 5 To delete multiple applications at once, delete them from the user interface, and click **Apply Changes**. The Application Policy Summary page appears, listing all of the applications to be deleted.

Step 6 Review the information in the summary and then do one of the following:

- Click the **Apply Now** radio button, and then click **Continue**.
- Click the **Schedule** radio button, specify a date and time to delete the application, and then click **Continue**.

Understanding the Define Application Policies Tab

Use the **Define Application Policy** tab to define policies according to their relevance to the business.

Application Categories

Application policies are categorized as one of the following:

- **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.

Application Policy

Application policy defines the QoS and PfR policies for each of the application categories.

Cisco IWAN QoS defines how traffic egresses the network. It is critical that the classification, marking, and bandwidth allocations align to the service provider offering to ensure consistent QoS treatment end-to-end.

The IWAN app follows a 12-class model on the ingress to mark all incoming applications, and traffic is marked again on the egress according to the service provider QoS profile attached to the WAN link.



Note You can view the DSCP values and bandwidth allocated for each egress class, and edit the values in the service provider profiles through the **Configure Hub Site and Settings > Service Providers** tab.

To ensure proper QoS treatment, place the application categories in the right column. All categories placed in the Business Relevant column will be marked according to the traffic class for the corresponding applications. To view the traffic class for an application, open the **Categorize Applications** tab, then open the Category for the application, and click the edit button for the application. The following table shows how traffic classes map to specific DSCP values:

Table 7-2 Traffic Classes and DSCP Values

Traffic Class	DSCP Value
BROADCAST_VIDEO	CS5
BULK_DATA	AF11
INTERACTIVE_VIDEO	CS4
MULTIMEDIA_CONFERENCING	AF41
MULTIMEDIA_STREAMING	AF31
NETWORK_CONTROL	CS6
NETWORK_MANAGEMENT	CS2
SCAVENGER	CS1
SIGNALING	CS3
TRANSACTIONAL_DATA	AF21
VOIP_TELEPHONY	EF

All categories placed in **Business Irrelevant** are marked with a DSCP value of CS1, regardless of the traffic class attached to the application. Categories placed in the Default section keep their original incoming marking.

Optionally, set PfR path prioritization by enabling Application Performance for a category and selecting the Path Preference radio button. For each category, the WAN paths configured in the Service Providers tab (on the Configure Hub Site & Settings page) are shown in the category dropdown menu.

Optionally, Drop can be selected from the menu for the secondary path. If this option is selected, and the primary path goes out of policy, the PfR will drop the packets rather than failing over to the secondary path.

Optionally, multiple primary and secondary options can be selected. If the primary path goes out of policy, the SLA threshold for each application is monitored, and applications are dynamically moved to the secondary path.

To view or edit the SLA threshold values for an application, open the Categorize Applications tab, then open the Category for the application, and click the edit button for the application.

Operations in the Define Applications Tab

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

Table 7-3 Define Applications Tab

No.	Task	Reference
1	Move an application category to a different business group.	Understanding the Application Bandwidth Tab, page 7-8.
2	Modify application performance.	Modifying the Application Performance, page 7-7

Moving an Application Category to a Different Business Group

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

Procedure

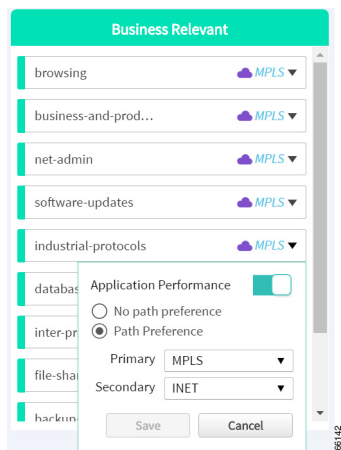
-
- Step 1** From the Cisco IWAN home page, click **Administer Application Policy**. The Application Policy page opens.
 - Step 2** Click the **Define Application Policy** tab. Applications are displayed in three categories: Business Relevant, Default, and Business Irrelevant.
 - Step 3** To move an 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 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 7-2](#).

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 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:

- [Viewing the Complete Cisco IWAN Network, page 8-1](#)
- [Viewing Site Details, page 8-4](#)
- [Compliance Reporting: Out-of-Band Configuration Changes, page 8-6](#)
- [Service Assurance: Network Connectivity Alarms, page 8-8](#)

Viewing the Complete Cisco IWAN Network

Use the Monitoring page to view all sites within your Cisco IWAN network, worldwide, with information about the status of each site. The Monitoring page provides a map showing the geographic locations of each site, and provides an alternative list view that shows sites in a compact table format.

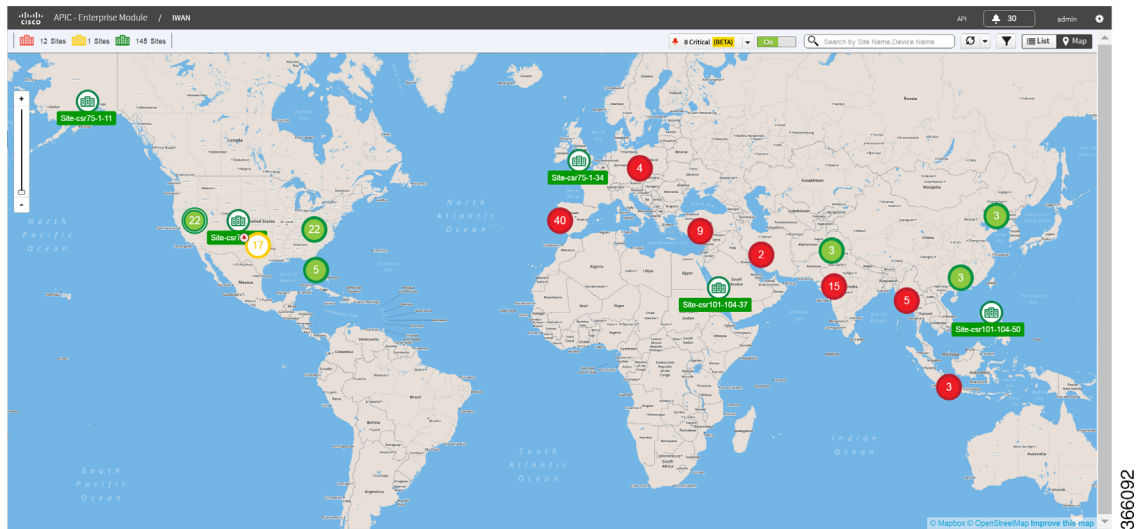
Procedure

-
- Step 1** From the Cisco IWAN app home page, click **Monitor & Troubleshoot**. The Monitoring page opens with a map showing all sites. Site icons indicate a single site at the location. To avoid clutter, where numerous sites are located within a specific area, the map displays a circle with a numeral indicating the total number of sites, including hubs and branches.

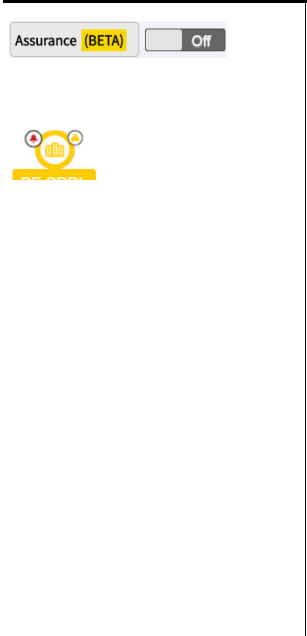



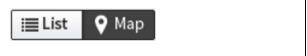
The **Map** and **List** buttons at the top-right switch between the map view and a list view of IWAN sites.

Monitoring Page, Symbols, and Controls

Figure 8-1 Monitoring Page



Map Element	Description
Site Symbols	
	Hub site.
	Branch site.
	Numerous sites in the same area. Zoom in on the map to view the sites separately.
Warnings and Alarms	
	Provisioned site, no warnings or alarms.
	Site with warning of out-of-band changes reported by the Compliance feature. Click to view the Site Details page, then select the Policy Compliance tab to display the site configuration. See Compliance Monitoring, page 8-7 .
	Site with one or more alarms. See Service Assurance: Network Connectivity Alarms, page 8-8 . Click to view the alarm details.
	Site – provisioning failure.
	Green—Number of provisioned sites without network alarms. Yellow—Number of sites with network alarms. The sites with alarms appear yellow on the map. Red—Number of sites with a provisioning failure.

	<p>Controls network alarm reporting, called Service Assurance (beta feature). Service Assurance reports critical network issues affecting sites in the IWAN network. Sites with alarms present appear in yellow. See Service Assurance: Network Connectivity Alarms, page 8-8.</p> <p>Each 30 minutes, the IWAN app requests alarm information from sites in the network, then analyzes the information and updates the display of alarms. If any alarms are present, this control displays the total number of alarms in the network.</p> <p>Optional:</p> <ul style="list-style-type: none"> • If alarms are present, click the Assurance control to display the Alarms page listing all alarms in the system. • Click the down arrow to open a small drop-down window with a Refresh button. Click Refresh to immediately request alarm information from each site in the network without waiting for the next scheduled auto-refresh. While the IWAN app analyzes alarm information, the drop-down window displays the percent progress. When complete, it updates the display. • On the map, hover over a site icon to display information about any alarms affecting the site. Click View Details to display the Site Details page with alarm details. • On the map, click a site icon to display the Site Details page with alarm details.
Additional Features	
	Search for a specific site by site name or device name.
	Updates site information, such as provisioning status, and so on. Refresh does not affect the display of alarms.
	Filters the display of sites according to selected criteria.
	Changes between Map and Site List views.

Viewing Site Details

Each site in the Cisco IWAN network has a Site Details page. The information provided on the page depends on the status of the site, application traffic health, whether alarms are present for the site, and so on.

Procedure

Step 1 Click a site. The Site Details page opens with the following information:

Map Element	Description
Site Status	Indicates whether the site is provisioned.
Hub/Site Topology tab	Graphical display of the site topology, including site name, location, and preferred POP. Hover over elements in the topology to display additional information.
IP Address Allocation	List of devices at the site and the IP addresses to which the devices are allocated.
Application Health tab	Displays information about application traffic. If application traffic performance is good, the tab displays: <ul style="list-style-type: none"> • Application traffic information • Bandwidth usage for each application • Statistical trend for each application If application traffic on the site has experienced problems that impact the application, such as packet loss, excessive delay, or excessive jitter, this tab displays the details. See Figure 8-2 on page 8-5 .
Alarms tab	(Displayed if alarms present) Alarms may be caused by problems with specific applications or by bandwidth allocation issues. The system provides recommended actions for addressing the alarm issues. See Service Assurance: Network Connectivity Alarms, page 8-8 .
Policy Compliance tab	(Displayed if out-of-band configuration detected) See Compliance Reporting: Out-of-Band Configuration Changes, page 8-6 .
Troubleshoot tab	Indicates the application causing a critical alarm, and provides recommended actions for improving the site performance. For example, if an application needs more bandwidth than has been allocated for it, you can adjust the bandwidth settings. See Figure 8-3 on page 8-5 and Figure 8-4 on page 8-6 .

Figure 8-2 Application Health Tab

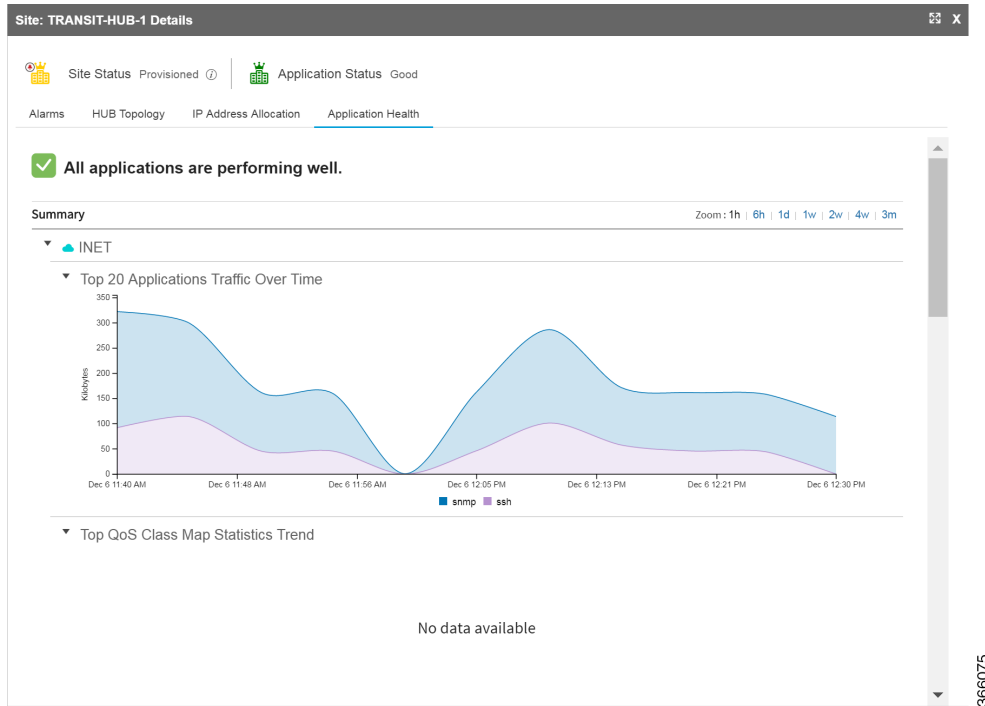


Figure 8-3 Troubleshooting—Detection

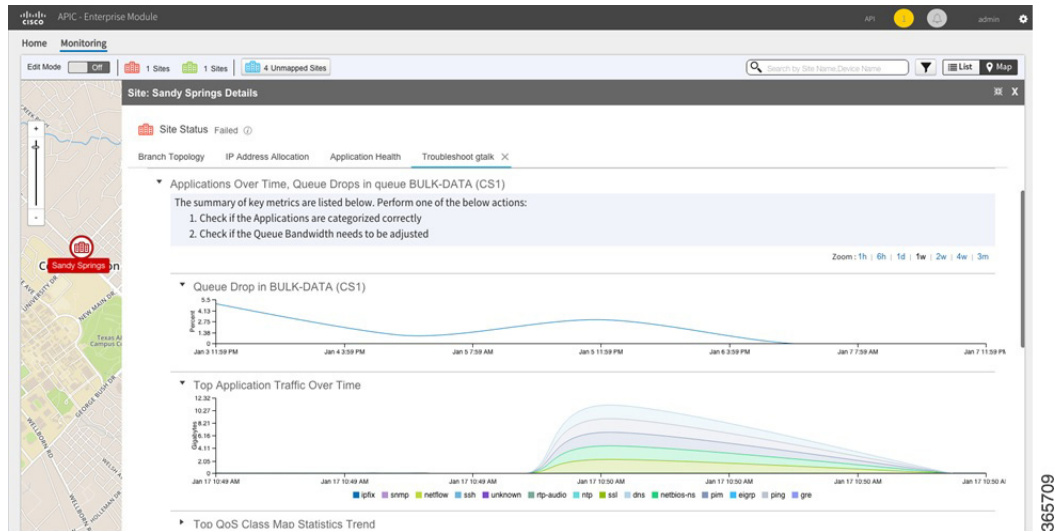
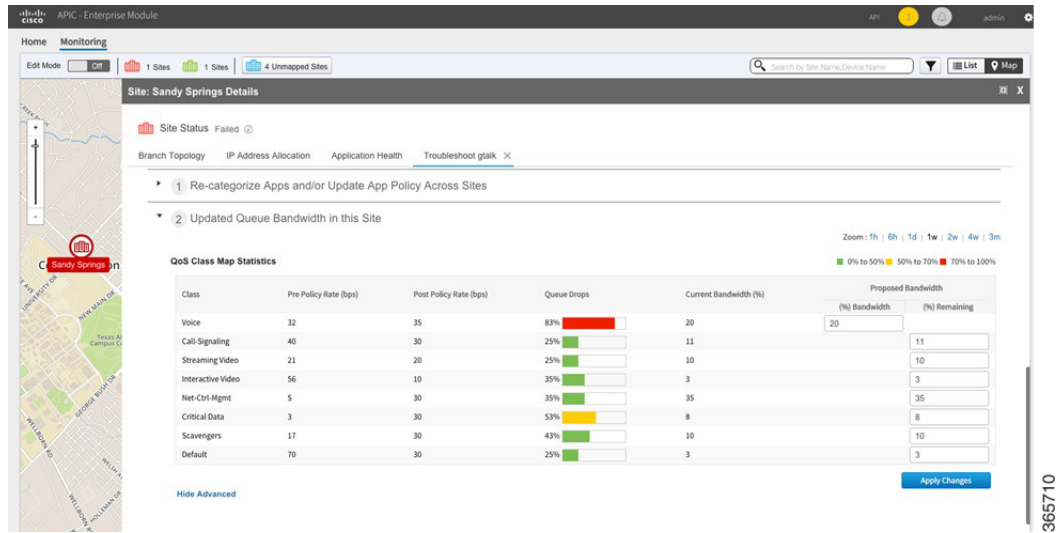


Figure 8-4 Troubleshooting—Adjusting Bandwidth



Compliance Reporting: Out-of-Band Configuration Changes

For sites within a Cisco IWAN network, administrators typically make configuration changes centrally, using the IWAN app. Any configuration changes made locally, directly on a device in the network, and not through the IWAN app, are called out-of-band configuration changes. Sites with local configuration changes are called non-compliant.

The IWAN app can check sites in the network for compliance. The Compliance Reporting mechanism collects configuration information about each site. If it detects a site with out-of-band configuration changes, it flags the site as non-compliant on the IWAN app Monitoring page, displaying a yellow badge on the site in the Map view or a yellow warning symbol in Sites List view.



The Site Details page for a non-compliant site provides details of the changes that have been made locally.

Compliance Reporting Mechanism

Cisco Prime Infrastructure operates with routers in the IWAN network to collect information about router configuration. Prime Infrastructure provides this configuration information to the IWAN app, which then determines the compliance status of each router in the network.

The IWAN app flags a router as non-compliant if:

- The IWAN app detects configuration changes made locally on a router, and not through the IWAN app.
- and
- The configuration discrepancy has exceeded a 5-minute grace period.

Compliance Reporting Setup

To enable the Cisco IWAN app Compliance Reporting feature to report sites that have out-of-band configuration changes, perform the following steps.

- Step 1** On the IWAN app Home page, click **Configure Hub Site & Settings**. The Network wide settings page opens.
- Step 2** Click the **System** tab.
- Step 3** Click the **Show more** button to display additional settings.
- Step 4** In the Syslog section, in the Server IP field, enter the address of the Cisco Prime server. (A network administrator can provide the Prime server address.)



- Step 5** Click the **Save & Continue** button to save the changes. Compliance Reporting is enabled.

Compliance Monitoring

When Compliance Reporting has been activated, the Monitoring page indicates sites that have out-of-band configuration changes, as follows:

- Map view: Yellow warning badge displayed on the site icon.



- Sites List view: Yellow warning icon in the Status column for the site.

Health	App Health	Site	Location	Status	Action
		BR4351	Wyoming	Provisioned	
		DR3L	Wyoming 62721	Provisioned	
		HUB	United Kingdom	Provisioned	
		SR3L4451	Iowa 50508	Provisioned	
		SRDL4431	Wyoming	Provisioned	
		TRANSIT-HUB-1	United Kingdom	Provisioned	

Click a site to view the Site Details page, then select the Policy Compliance tab to display the site configuration details. From the Raw Configuration drop-down menu, select **All** to display the complete details of the site configuration, or select **Difference Only** to display only the out-of-band changes made on the site.

Service Assurance: Network Connectivity Alarms

The IWAN app provides information about critical network issues affecting connectivity throughout the IWAN network. This “Service Assurance” provides important insight into problems that could affect communication between the IWAN app and sites in the network.

Sites throughout the IWAN network report connectivity information to the IWAN app. The application processes the information and presents any critical network issues as alarms on the Monitoring page. A button labeled, “Critical” displays a summary of any alarms present in the network.



The Map view and Sites List view display the alarms for each site, and provide easily accessible details about each alarm.

Alarm Mechanism

At 30-minute intervals, the IWAN app requests information about network functionality from each site in the network. After analyzing the information, the application indicates any critical network issues by displaying alarms on the Monitoring page. Sites affected by the network issues are yellow with a red badge:



To view details of all alarms detected in the network, click the Assurance button at the top of the Monitoring page. For information about alarms affecting a specific site, hover over or click the site icon.



Note

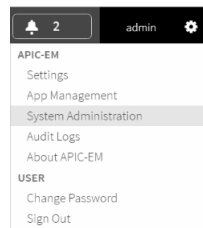
The Service Assurance feature, reporting network alarms, is a “beta” feature in this release. Do not rely on it as the only indicator of network problems.

Network Alarm Reporting Setup

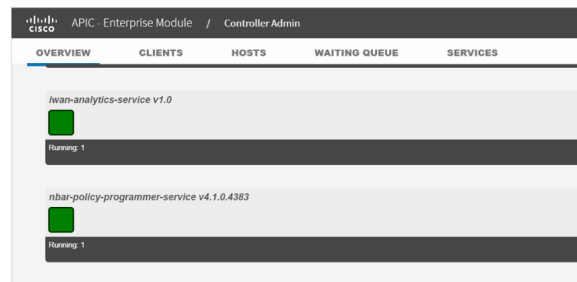
Before Enabling Service Assurance

Before enabling Service Assurance in the IWAN app, verify that the following APIC-EM service is running: **iwana-analytics-service**

To verify this, in APIC-EM, select **Settings (gear button) > System Administration** to view active services.




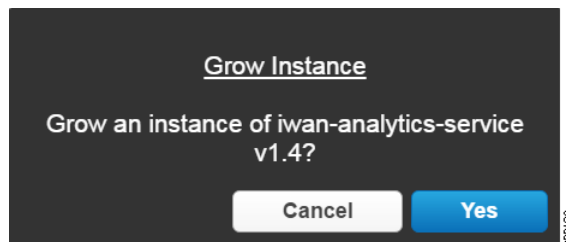
In the Overview tab, verify that **iwana-analytics-service** is running.



If no green square appears under **iwana-analytics-service** in the list of services, then the service is not running. The value of the "Running" label below the service name is 0.



To activate the service, click the plus icon () to the right of the service name. When prompted to grow an instance, click **Yes**.



Starting the service may take several minutes. When complete, a green square appears under the **iwana-analytics-service** name in the list of services.



Procedure

To enable the Service Assurance feature to report network alarms, perform the following steps.

-
- Step 1** On the IWAN app Home page, click **Monitor & Troubleshoot**. The Monitoring page opens.
- Step 2** On the Monitoring page, click the **On/Off** switch next to the **Assurance** button near the top of the page.

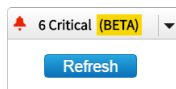


- Step 3** In this beta release of the Service Assurance feature, a window prompts you to select Lab Environment. Click the **Lab Environment** button.



The Service Assurance feature is activated. IWAN begins collecting information about network functionality for all sites in the network, refreshing the information each 30 minutes.

- Step 4** (Optional) On the **Assurance** button, click the down arrow to open a small drop-down window with a **Refresh** button. Click **Refresh** to immediately request alarm information for all sites in the network without waiting for the next scheduled auto-refresh.



While the IWAN app analyzes alarm information, the drop-down window displays the percent progress. When complete, the app updates the display.

Viewing Network Alarms

Do any of the following to view details of network alarms:

- **Map view:** Hover over a site icon to display information about any alarms affecting the site. Click **View Details** to display the Site Details page. The Alarms tab displays the alarm details.



- **Map view or Sites List view:** Click a site icon on the map or site name in the list view to display the Site Details page. The Alarms tab displays the alarm details.



366060



Backup and Restore, Recovery, and Delete

This chapter contains the following sections:

- [Backup and Restore, page 9-1](#)
- [Recovery, page 9-4](#)
- [Deleting Sites and Devices, page 9-5](#)
- [Manually Cleaning Up Devices, page 9-6](#)
- [Adding or Deleting Site Prefixes, page 9-8](#)

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 every day 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 app 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 9-1 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 app. 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>After a device's client ID certificate expires, the only option is to re-provision it.</p>

Table 9-1 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.

Deleting Sites and Devices

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 device was successfully provisioned or is unreachable, it will not be restored to the original configuration. In this case, you must manually clean up the configuration on the devices. See [Manually Cleaning Up Devices, page 9-6](#).

You can re-provision the hub from the Configure Hub Site page as part of the hub provisioning (see [Configuring the IWAN Aggregation Site, page 4-17](#)).

Deleting a Transit Hub Site

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 9-6](#).

Deleting a Branch Site

You can delete branch sites from IWAN regardless 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 9-6](#).

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 9-1](#).

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.

Deleting a Hub Device

If there are more than two hub devices in one POP, you can delete the individual hub devices in the primary or the transit POP until there are two devices left. The hub device should not have branches connected with the only WAN link.

When a previously successfully provisioned hub device is deleted, it is not restored to the original configuration. In this case, you must manually clean up the configuration on the device (see [Manually Cleaning Up Devices, page 9-6](#)) and restore its original configuration.

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.
PRE-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.

PRE-GA-1-HUB-INET(config)# crypto key zeroize rsa sdn-network-infra-iwan
Do you really want to remove these keys? [yes/no]: yes
PRE-GA-1-HUB-INET(config)# end
PRE-GA-1-HUB-INET# write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
PRE-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
PRE-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**.
-



## Brownfield Validation Messages

---

This chapter contains the following sections:

- [Adding Greenfield and Brownfield Devices to Cisco IWAN, page A-1](#)
- [Errors, page A-2](#)
- [Warnings, page A-3](#)

## Adding Greenfield and Brownfield Devices to Cisco IWAN

The Cisco IWAN application (IWAN app) can add “greenfield” or “brownfield” devices to the IWAN network.

“Greenfield” refers to new, unconfigured devices. Because these devices do not have any pre-existing configuration, there are no conflicts when bringing them into the IWAN network and configuring them using the IWAN app.

“Brownfield” refers to devices that belong to existing sites that are being added to an IWAN network. They may have pre-existing configurations to synchronize with IWAN-based configuration, and these existing configurations may cause conflicts.

### Validation

While provisioning a brownfield device, the IWAN app performs a validation to determine whether any configuration conflicts exist. It reports the conflicts in two categories:

- **Errors**—Conflicts that prevent adding the device to the IWAN network.
- **Warnings**—Conflicts that do not prevent the device from being added to the IWAN network. It is recommended to correct the configuration issues that trigger validation warnings.

If the IWAN app detects an error or warning during provisioning, correct the issue on the device and perform the validation again. Refer to the [Errors](#) and [Warnings](#) sections below for details.

# Errors

The following table describes errors that can occur during validation. These errors prevent adding a device to the IWAN network.

**Table A-1 Validation Errors**

| Configuration Conflict                                                            | Recommendation                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username configuration must have privilege level 15.                              | <p>Configure a username with privilege level 15 on the device.</p> <p><b>Example:</b><br/> <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><b>Example:</b><br/> <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><b>Example:</b><br/> <code>no class-map match-any nbar-12-cl1s#VOICE</code><br/> <code>no policy-map nbar-12-cl1s</code><br/> <code>no service-policy input nbar-12-cl1s</code><br/> <code>no service-policy output IWAN-INTERFACE-SHAPE-ONLY-INTERNET</code></p>                                          |
| Interface loopback 47233 must not be configured on the device.                    | <p>Remove interface loopback 47233 from the device.</p> <p><b>Example:</b><br/> <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><b>Example:</b><br/> <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"> <li>• IWAN-TRANSPORT-1</li> <li>• IWAN-TRANSPORT-2</li> <li>• IWAN-TRANSPORT-3</li> <li>• IWAN-TRANSPORT-4</li> </ul> <p><b>Example:</b><br/> <code>no ip vrf IWAN-TRANSPORT-4</code></p> |

Table A-1 Validation Errors

| Configuration Conflict                                                                     | Recommendation                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recovery configuration file unavailable in flash                                           | IWAN recovery configuration file "IWAN_RECOVERY.cfg" is needed to enable recovery of device.<br>Create a recovery file using the CLI command:<br><b>copy running-config flash:IWAN_RECOVERY.cfg</b>                                                           |
| Conflicting EIGRP configuration present on the device                                      | Remove EIGRP configuration using the CLI command:<br><b>no router eigrp IWAN-EIGRP</b>                                                                                                                                                                        |
| Configure Port-Channel in aggregate mode to support QoS policy configuration               | Applicable only to ASR routers. Ensure that port-channel is in aggregate mode when it is used as WAN/LAN interface.<br>Configure port-channel aggregate mode using the CLI command:<br><b>platform qos port-channel-aggregate &lt;port-channel-number&gt;</b> |
| QoS policy configuration is not supported for the targeted type of interface: Port-Channel | Device platform type does not support QoS policy configuration on port-channel interface.<br>Choose other types of LAN/WAN interface.                                                                                                                         |

## Warnings

The following table describes errors that can occur during validation. These warnings do not prevent a device from being added to the IWAN network, but it is recommended to correct the issues that trigger these warnings.

Table A-2 Validation Warnings

| Configuration Conflict                                                       | Recommendation                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br>Verify using the <b>show ip interface brief</b> command.                                                                                                                                                                                              |
| IWAN related crypto configuration found on the device.                       | Remove the crypto configuration because the crypto configuration might interfere with the Cisco IWAN configuration.<br><br><b>Example:</b><br><b>crypto zeroize mypubkey rsa sdn-network-infra-iwan</b>                                                                                                                     |
| No routing protocol found on device.                                         | Enable one of the following routing protocols on the device.<br><br><b>Example:</b><br><b>router ospf AS number</b><br><b>router eigrp AS number</b><br><b>router bgp AS number</b>                                                                                                                                         |
| EZPM configuration found on the device.                                      | Remove Easy Performance Monitor (EZPM) configuration as EZPM configuration might interfere with the Cisco IWAN configuration.<br><br><b>Example:</b><br><b>no class-map match-all Business-Critical-and-default-tcp-only</b><br><b>no performance monitor context IWAN-Context profile</b><br><b>application-experience</b> |

Table A-2 Validation Warnings

| Configuration Conflict                                                           | Recommendation                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NBAR configuration found on the device.                                          | Remove the Network Based Application Recognition (NBAR) configuration as NBAR configuration might interfere with the Cisco IWAN configuration.<br><br><b>Example:</b><br><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.                                  | Revalidate and if problem persists, ensure the following: <ul style="list-style-type: none"> <li>• Device is up and running.</li> <li>• Device connectivity is established.</li> </ul>                                                                                                                                                                                    |
| Device does not have valid image version and K9 package.                         | The Cisco IWAN app 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.<br><br><b>Example:</b><br><pre>asr1000rp1-adventerprisek9.03.16.00.S.155-3.S-ext.bin</pre>                                                                                                                   |
| Insufficient number of VTY lines present on the device                           | A minimum of 16 VTY lines are required to be configured on the device.<br><b>line vty &lt;first-line-number&gt; &lt;last-line-number&gt;</b>                                                                                                                                                                                                                              |
| One of the VTY line exec-timeout is less than 5 mins                             | Ensure VTY line exec timeout are not less than 5 minutes<br><br>Verify using the CLI command:<br><b>show running-config   sec line vty</b>                                                                                                                                                                                                                                |
| Configured Throughput on device does not match with installed license throughput | Applicable only to CSR routers. Remove the <b>platform hardware throughput level</b> CLI to achieve maximum throughput, as follows:<br><b>no platform hardware throughput level MB &lt;configured-value&gt;</b>                                                                                                                                                           |
| No active license found on the device                                            | Applicable only to CSR routers. Either the license has expired or is not supported.<br><br>Verify license issues using CLI command:<br><b>show self-diagnostics</b>                                                                                                                                                                                                       |
| Device does not have required license.                                           | Required licenses are not enabled on the device. Enable the licenses for the platform in use. <ul style="list-style-type: none"> <li>• ASR routers: adventerprisek9 or advipservicesk9 and IPSEC EULA should be accepted</li> <li>• ISR 4000 Series routers: appxk9 and securityk9</li> <li>• ISR G2 routers: datak9 and securityk9</li> <li>• CSR routers: ax</li> </ul> |
| Device clock is not synchronized                                                 | Ensure that the router clock is in sync with controller clock. Verify using the <b>show clock</b> command.<br><br>Recommended to configure NTP server using the CLI command:<br><b>ntp server &lt;controller-ip&gt;</b>                                                                                                                                                   |