Cisco Managed Cellular Activation Configuration Guide

First Published: 2024-05-21

Last Modified: 2024-12-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.

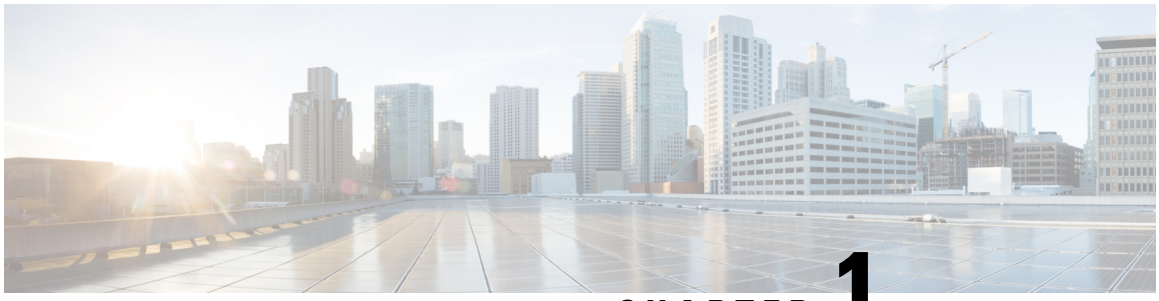
CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **Cisco Managed Cellular Activation** 3

- Managed Cellular Activation 3
- Information About Managed Cellular Activation 4
  - Benefits of Managed Cellular Activation 5
- Supported Devices 6
- Supported Carriers 7
- Prerequisites for the Managed Cellular Activation Solution 7
- Verify Cisco Catalyst SD-WAN Manager's Connectivity to the Cisco IoT Control Center 8
- Restrictions for the Managed Cellular Activation Solution 8
- Configure the Managed Cellular Activation Solution 9
  - Enable the Managed Cellular Activation Functionality in Cisco Catalyst SD-WAN Manager 10
  - Add Account Credentials for a Service Provider 10
  - Configure the Managed Cellular Activation Solution for a Cisco Catalyst Wireless Gateway 11
  - Configure the Managed Cellular Activation Solution for a PIM Using a Configuration Group in Cisco Catalyst SD-WAN Manager 11
  - Deploy a Configuration Group to Devices 12
  - Generate an API Key in Your SIM Management Portal 13
- Monitor the Data Usage of Managed Cellular Activation 13



CHAPTER 1

Read Me First

User Documentation

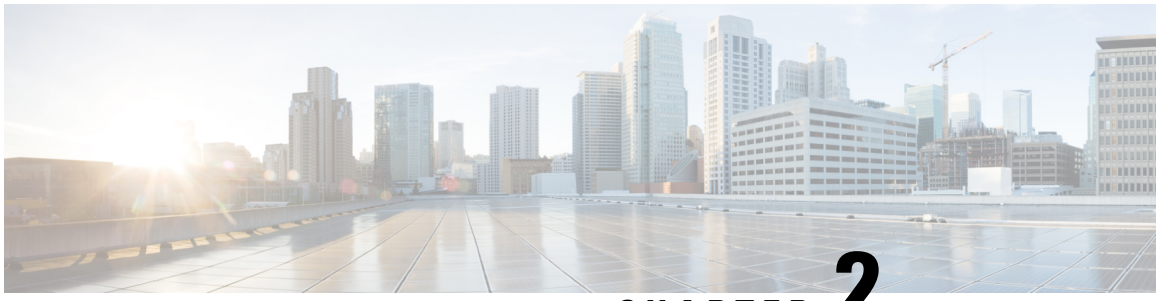
Reference	Description
Cisco Catalyst Wireless Gateway Software Configuration Guide	Configuration of Cisco Catalyst Wireless Gateways
Cellular Pluggable Interface Module Configuration Guide	Configuration of pluggable interface modules

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

Cisco Managed Cellular Activation

- Managed Cellular Activation, on page 3
- Information About Managed Cellular Activation, on page 4
- Supported Devices, on page 6
- Supported Carriers, on page 7
- Prerequisites for the Managed Cellular Activation Solution, on page 7
- Verify Cisco Catalyst SD-WAN Manager's Connectivity to the Cisco IoT Control Center, on page 8
- Restrictions for the Managed Cellular Activation Solution, on page 8
- Configure the Managed Cellular Activation Solution , on page 9
- Monitor the Data Usage of Managed Cellular Activation, on page 13

Managed Cellular Activation

Table 1: Feature History

Feature Name	Release Information	Description
Managed Cellular Activation	Cisco Catalyst SD-WAN Manager Release 20.12.1	The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM. Using Cisco SD-WAN Manager, you can easily configure Managed Cellular Activation for Cisco Catalyst Wireless Gateways, and for pluggable interface modules (PIM) operating in supported routers.
Managed Cellular Activation Support for Cisco Catalyst Rugged Series Routers	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Specific pluggable interface modules of Cisco Catalyst IR1101 Rugged Series Router and Cisco Catalyst IR1800 Rugged Series Router support the Managed Cellular Activation solution.

Feature Name	Release Information	Description
Managed Cellular Activation Support for Cisco Catalyst Heavy Duty Routers	Cisco Catalyst SD-WAN Manager Release 20.16.1 Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	Specific pluggable interface modules of Cisco Catalyst IR8140 Heavy Duty Routers support the Managed Cellular Activation solution.

Information About Managed Cellular Activation

The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM, which is a physical SIM card that you can configure with a cellular service plan of your choice. For specific Cisco products that support cellular connectivity, you can order the product with an eSIM preinstalled by Cisco. Use Cisco SD-WAN Manager to configure the eSIM with the details of your plan.

Note In this context, eSIM refers to a removable SIM pre-installed by Cisco. In other contexts, eSIM can refer to a non-removable SIM embedded in a cellular-enabled device.

Bootstrap Cellular Plan

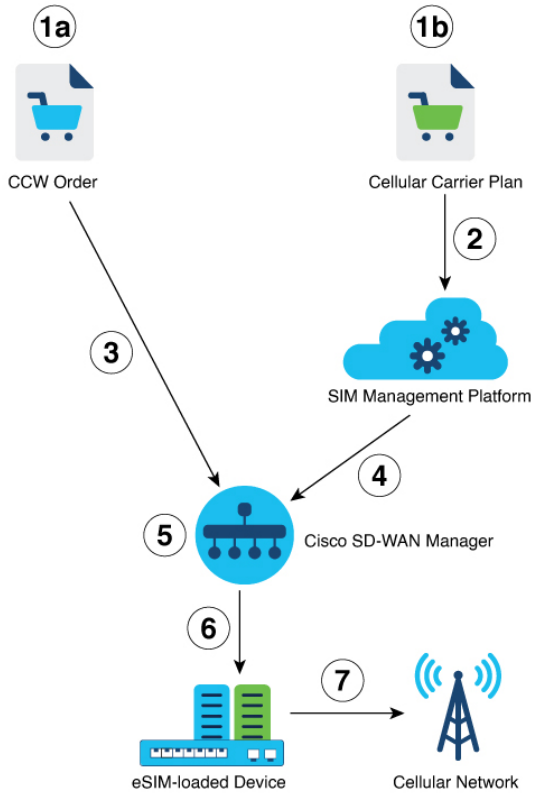
The Managed Cellular Activation solution comes with a bootstrap cellular plan to provide internet connectivity with a limited amount of data intended only for Day 0 onboarding of the device to your cellular plan. Prepare the configuration in Cisco SD-WAN Manager before powering on and onboarding the device, to avoid running out of the limited data in the bootstrap cellular plan.

Managed Cellular Activation Onboarding

Broadly, the solution includes the following steps:

1. Order a product with a preinstalled eSIM card.
2. Set up a plan with a cellular service provider.
3. In Cisco SD-WAN Manager, create a Managed Cellular Activation configuration for your devices that connects the devices that connect to your cellular plan.

Figure 1: Managed Cellular Activation Onboarding Workflow



Steps	Description
1a	Order a device with an eSIM preinstalled for Managed Cellular Activation.
1b	Order a cellular service account with a carrier.
2	The carrier sends your account information to their SIM management platform to prepare to activate a SIM to operate with your account.
3	Onboard the device to Cisco SD-WAN Manager through Plug and Play (PnP).
4	Use account information from the SIM management platform to create a configuration for Managed Cellular Activation.
5	In Cisco SD-WAN Manager, enable and create a configuration for Managed Cellular Activation.
6	Deploy the Managed Cellular Activation configuration to the device.
7	The device loaded with the eSIM connects to the cellular network.

Benefits of Managed Cellular Activation

The Managed Cellular Activation solution simplifies the process of activating a cellular plan on each cellular WAN device, providing the following benefits:

- Easy, fast, and secure deployment
  - Zero Touch Provisioning
  - Remote setup
  - No technical expertise required
- Seamless provisioning
  - Ease of switching carriers
  - No downtime during switchover
- Management simplicity
  - Cisco SD-WAN Manager integration
  - Reduced operational complexity

Supported Devices

Table 2: Platform and Module Support

Platform	First Supported Release	Modules
Cisco Catalyst Wireless Gateway CG113-4GW6	17.12.1a	N/A
Catalyst 8200 Series	17.12.1a	P-5GS6-GL
	17.13.1a	P-5GS6-R16SA-GL, P-LTEAP18-GL, P-LTEA-EA, P-LTEA7-NA
Catalyst 8300 Series	17.12.1a	P-5GS6-GL
	17.13.1a	P-5GS6-R16SA-GL, P-LTEAP18-GL, P-LTEA-EA, P-LTEA7-NA
ISR 1000 Series	17.12.2	P-5GS6-GL
	17.13.1a	P-5GS6-R16SA-GL, P-LTEAP18-GL, P-LTEA-EA, P-LTEA7-NA
Rugged Router IR1101 Series	17.15.1a	P-5GS6-R16SA-GL, P-LTEAP18-GL, P-LTEA-EA, P-LTEA7-NA, P-LTE-MNA, P-5GS6-GL

Platform	First Supported Release	Modules
Rugged Router IR1800 Series	17.15.1a	P-5GS6-R16SA-GL, P-LTEAP18-GL, P-LTEA-EA, P-LTEA7-NA, P-LTEA7-EAL, P-LTE-MNA
Cisco Catalyst IR8140 Heavy Duty Router	17.16.1a	IRMH-LTE7-NA-900

Supported Carriers

AT&T (North America)

Prerequisites for the Managed Cellular Activation Solution

- Ensure Cisco SD-WAN Manager has connectivity to the Cisco IoT Control Center. To verify Cisco SD-WAN Manager connectivity to the Cisco IoT Control Center, see Verify Cisco Catalyst SD-WAN Manager's Connectivity to the Cisco IoT Control Center, on page 8.

Note If the Cisco SD-WAN Manager is hosted in a private cloud or on-premises, configure the local firewall to allow outbound communication from Cisco SD-WAN Manager (interface VPN 0) on port 443 to Cisco IoT Control Center.

- Ensure access to the SIM management platform (for example, Cisco IoT Control Center) account for your cellular plan.

  In the Add Account Credentials for a Service Provider , on page 10 procedure, you need the following information from your account:

  - **Account ID**
  - **Username**
  - **Communication plan**
  - **Rate plan**
  - **Access point name**
  - **Package data network type**
  - **API key**

Note For information about retrieving this information from Cisco IoT Control Center, see Generate an API Key in Your SIM Management Portal, on page 13.

- Complete Cisco Smart Account and Virtual Account for Plug and Play onboarding.
- Synchronize Smart Account and Cisco SD-WAN Manager:

  For devices in a Smart Account to appear in the device list in Cisco SD-WAN Manager, synchronize Cisco SD-WAN Manager with the Smart Account.

Verify Cisco Catalyst SD-WAN Manager's Connectivity to the Cisco IoT Control Center

Before You Begin

- Ensure that Cisco SD-WAN Manager has connectivity to the internet through VPN 0.
- In a multitenant scenario, only the provider has access to Cisco SD-WAN Manager. In this scenario, the provider performs this procedure.

Verify Cisco Catalyst SD-WAN Manager Connectivity to the Cisco IoT Control Center

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.
2. In the **Summary** area, click **Manager**. A dialog box opens and displays the Cisco SD-WAN Manager instances.
3. For each Cisco SD-WAN Manager instance, perform the following steps:
   a. Click **…** and choose **SSH Terminal**.
   b. Log in using your Cisco SD-WAN Manager credentials.
   c. Use the **nslookup** command to verify connectivity to a domain over VPN 0. Here, verify Cisco SD-WAN Manager's connectivity to the domain sdo.jasper.com.

      If the output shows external IP addresses, it confirms that Cisco SD-WAN Manager has connectivity to the domain. If the output indicates that the command cannot resolve the domain, it indicates that Cisco SD-WAN Manager does not have connectivity to the domain.

      The following is an example indicating connectivity to a domain:

```
Device# nslookup vpn 0 sdo.jasper.com
nslookup in VPN 0:
Server:    10.1.0.1
Address 1: 10.1.0.1 dns.google

Name:      sdo.jasper.com
Address 1: 10.1.0.2 apmx-prod1-vip.jasper.com
```

Restrictions for the Managed Cellular Activation Solution

- Managed Cellular Activation supports only SIM 0.

For more information about Cisco Catalyst Wireless Gateway, see *Cisco Catalyst Wireless Gateway Software Configuration Guide*.

For more information about 5G PIM, see *Cellular Pluggable Interface Module Configuration Guide*.

- The Cisco bootstrap account comes with an eSIM assist feature for a device bring up and contains a predefined data limit. This account is designed to facilitate the initial bring up process with a restricted data quota.
- The Cisco SD-WAN Manager supports only one Cisco IoT Control Center account per user.
- After you configure the eSIM to use your service provider account, you cannot change to a different SP account.
- Managed Cellular Activation supports only IPv4 addressing.

Note If you are using the devices ISR1K C1126/C1127 with VDSL controller built-in, you need to use CLI add-on template to manually add the line 'controller VDSL 0/3/0' to the configuration before deploying it. Otherwise, your device generates errors and the deployment configuration group fails.

Configure the Managed Cellular Activation Solution

Arif: Checking connectivity to sdo.jasper.com. From my experience, that is no sufficient. User should confirm the Rate Plan information can be shown unider vMaage -> Admin->Integration Management

The following workflow describes the process of ordering a cellular-enabled device with an eSIM and activating the Managed Cellular Activation solution.

1. In the Cisco Commerce Workspace, order a cellular-enabled device with a preinstalled eSIM card.
2. Set up an enterprise account contract with a service provider.
3. In Cisco SD-WAN Manager, enable configuration of Managed Cellular Activation.

   See Enable the Managed Cellular Activation Functionality in Cisco Catalyst SD-WAN Manager, on page 10.
4. In Cisco SD-WAN Manager, integrate the account details of your cellular account.

   See Add Account Credentials for a Service Provider , on page 10.
5. In Cisco SD-WAN Manager, create a configuration group for the devices that use the Managed Cellular Activation solution. See the following:

   - Configure the Managed Cellular Activation Solution for a Cisco Catalyst Wireless Gateway, on page 11
   - Configure the Managed Cellular Activation Solution for a PIM Using a Configuration Group in Cisco Catalyst SD-WAN Manager, on page 11
6. Deploy the configuration group to devices.

   See the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x*.
7. Power on the router (or Cisco Catalyst Cellular Wireless Gateway) and initiate WAN connectivity.

8. The device connects to Cisco SD-WAN Manager and the cellular network.

Enable the Managed Cellular Activation Functionality in Cisco Catalyst SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **External Services**, click **Managed Cellular Activation—eSIM**.
3. Toggle **Enable Managed Cellular Activation—eSIM**.
4. Click **Save**.
5. When you are redirected to a single sign-on page for authentication, enter the login credentials of your virtual account.

This enables integration between the SIM management platform, such as Cisco IoT Control Center, and Cisco SD-WAN Manager for Managed Cellular Activation.

Add Account Credentials for a Service Provider

Before You Begin

This procedure creates a set of account credentials for a specific carrier. You can create one or more sets of account credentials. Use the account credentials when configuring Managed Cellular Activation to use a specific carrier.

Prerequisites:

- Set up an account with a cellular carrier.
- In Cisco IoT Control Center, configure a carrier account and generate an API key specific to the carrier account. For more information on generating API key, see Generate an API Key in Your SIM Management Portal, on page 13

Add Account Credentials

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Integration Management**.
2. Click the **Managed Cellular Activation—eSIM Service Provider** tab.
3. Click **Add Service Provider Account Credentials**.
4. To add a service provider account, enter the following details:
   - **Carrier Name**
   - **Account ID**
   - **Username**
   - **API Key**
5. Check the **Accept the Terms and Conditions** check box.

6. Click **Save**
7. Adjacent to an account, click **…** in the **Action** column and choose **Edit**.
8. (Optional) To configure defaults to autopopulate parameters, check the **Make as default** check box.
9. Based on your selected plan with a carrier, choose **Communication Plan**, **Rate Plan** , **Access Point Name**, **Package Data Network Type**, and **Authentication Method** from the drop-down lists.
10. Click **Save**.

Configure the Managed Cellular Activation Solution for a Cisco Catalyst Wireless Gateway

Before You Begin

Create a configuration group for Cisco Catalyst Wireless Gateways (Teleworker workflow). For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Configure the Managed Cellular Activation Solution for a Cisco Catalyst Wireless Gateway

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Group**.
2. Click **…** adjecent to a configuration group for a Cisco Catalyst Wireless Gateway and choose **Edit**.
3. Click **Add Global Profile Feature**.
4. From the feature drop-down list, choose **Managed Cellular Activation—eSIM**.
5. (Optional) Click **Add Account Credentials** to add new account credentials. See Add Account Credentials for a Service Provider.
6. In the **Select Service Provider Account Credentials** drop-down list, choose an account.
7. If the account that you have chosen is configured to autopopulate default settings, then based on your selected plan with a carrier, those settings appear for the **Communication Plan**, **Rate Plan** , **Access Point Name**, **Package Data Network Type**, and **Authentication Method**. You can update the default settings according to your requirements.
8. Click **Save**.

Configure the Managed Cellular Activation Solution for a PIM Using a Configuration Group in Cisco Catalyst SD-WAN Manager

Before You Begin

Create a configuration group for the Cisco IOS XE Catalyst SD-WAN device. For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Configure the Managed Cellular Activation Solution for a Cisco Catalyst Wireless Gateway

1. From the **Cisco Catalyst SD-WAN Manager** menu, choose **Configuration** > **Configuration Groups**
2. Click **…** adjacent to a configuration group for a Cisco IOS XE Catalyst SD-WAN device and choose **Edit**.
3. Open the **Transport and Management Profile** section and click **Add Feature**.
4. From the feature drop-down list, choose **Managed Cellular Activation Flex Cellular Profile**.
5. Enter the cellular profile name and description.
6. (Optional) Click **Add Account Credentials** to add new account credentials. See Add Account Credentials for a Service Provider , on page 10.
7. In the **Select Account Credentials** drop-down list, choose an account.

   If the account that you have chosen is configured to autopopulate default settings, then based on your selected plan with a carrier, those settings appear for the **Communication Plan**, **Rate Plan**, **Access Point Name**, **Package Data Network Type**, and **Authentication Method**. You can update the default settings according to your requirements.
8. (Optional) To configure parameters for a separate data profile, check the **Set up separate data profile** check box.
9. Click **Add Feature** and from the drop-down list, choose **Managed Cellular Activation Flex Cellular Controller**.
10. Enter a feature name and description for **eSIM Cellular Controller**.
11. Configure the **Cellular ID** based on the slot configuration of your device (for example, Cisco Catalyst 8200 Series, Cisco Catalyst 8300 Series, and ISR1000). Enter the interface slot and port number in which the cellular PIM card is installed. Currently, it can be 0/2/0.

Note For more information on slot configuration, see the Cellular Controller section in *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

12. To associate a cellular profile with this feature, in the **Attach Profile** and **Data Profile** sections, choose a Cisco eSim Flex Cellular Profile.
13. Click **Save**.

Deploy a Configuration Group to Devices

1. For information about deploying configuration groups to devices, see the Using Configuration Group section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x*.
2. After you begin the deployment, to monitor the status, click **View Deployment Status**.

Note It might take several minutes to push configurations to the device and complete the changeover from the bootstrap cellular plan provided by Cisco to your cellular plan, which is called the integrated circuit card identification number (ICCID) swap.

3. In the **Action** column, click the logs icon to view the latest status of the swap.
4. The swap is successful if there are no error messages in the log. You will see a new ICCID in the monitoring page after the swap is successful.

The log is useful for verifying that you have configured a service provider for Managed Cellular Activation. For example, you can verify that Managed Cellular Activation is not using the temporary default cellular plan (bootstrap plan) provided by Cisco.

The log also shows information about the status of deploying a configuration group to its associated devices.

Generate an API Key in Your SIM Management Portal

Before You Begin

Ensure that you have access to the SIM management portal for your carrier—for example, AT&T uses Cisco IoT Control Center as its SIM management portal.

Generate an API Key

1. Log in to your SIM management portal.

   For information about logging in to the portal, refer to your carrier.
2. Within the portal, generate an API key to use when adding the account credentials for your service provider in Cisco SD-WAN Manager.

   For instructions on generating an API key, see the help available within the portal.

Monitor the Data Usage of Managed Cellular Activation

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. To view the health of every deployed device, choose the device and click **Cellular (eSIM)**.
3. In the **Cellular (eSIM)** tab, review the data usage of the current ICCID.