Release Notes for Cisco Global Launchpad 1.9.0

First Published: 2024-05-07

Last Modified: 2024-06-14

Release Notes for Cisco Global Launchpad 1.9.0

This document describes the features, limitations, and bugs for Cisco Global Launchpad, Release 1.9.0.

For information about the features, limitations, and bugs for Cisco DNA Center on Amazon Web Services (AWS), see the Release Notes for Cisco DNA Center, Release 2.3.5.x.

Note

- Cisco DNA Center has been rebranded as Catalyst Center, and Cisco DNA Center VA Launchpad has been rebranded as Cisco Global Launchpad. During the rebranding process, you will see the former and rebranded names used in different collaterals. However, Cisco DNA Center and Catalyst Center refer to the same product, and Cisco DNA Center VA Launchpad and Cisco Global Launchpad refer to the same product.
- With Cisco Global Launchpad, Release 1.9.0, you can deploy Cisco DNA Center 2.3.5.x on AWS.
- For links to all the guides related to this release, see the Cisco DNA Center 2.3.5 on AWS Documentation.

Change History

The following table lists changes to this document since its initial release.

Date	Change	Location
2024-06-14	Added the enhanced login process for hosted Cisco Global Launchpad to the New and Changed Features section.	New and Changed Features, on page 2
2024-04-11	Added CSCwj54137 to the Resolved Bugs list for Cisco Global Launchpad, Release 1.9.	Resolved Bugs, on page 4

Cisco Global Launchpad Overview

Cisco Global Launchpad configures and deploys Cisco DNA Center on AWS. Cisco Global Launchpad provides the most streamlined, supportive installation process of Cisco DNA Center on AWS. Cisco provides two methods for you to use Cisco Global Launchpad. You can download and install Cisco Global Launchpad on a local machine, or you can access Cisco Global Launchpad hosted by Cisco. Regardless of the method, Cisco Global Launchpad provides the tools that you need to install and manage your Cisco DNA Center VA.

For information about the manual methods of deployment for Cisco DNA Center on AWS, see the *Cisco DNA Center 2.3.5 on AWS Deployment Guide*.

New and Changed Features

Feature	Description
Enhanced login process for hosted Cisco Global Launchpad	The process of logging in to the hosted Cisco Global Launchpad has been streamlined. You no longer require a separate Cisco DNA Portal account. Instead, use your Cisco (CCO) account credentials to log in to the Cisco DNA Portal. Additionally, you can bypass the Cisco DNA Portal and go directly to Cisco Global Launchpad using the following URL: **`www.dna.cisco.com/valaunchpad`**
Login status screen	After you log in, a new screen is displayed, showing all configurations and their statuses such as user details, group information, account summary, access tokens, and more.
Improved user interface	Fields that used to be displayed in dialog boxes now appear inline in the main screens. For example, when you add a VA pod or create a Catalyst Center VA, you no longer choose the region from a drop-down list in a dialog box. Instead, you choose the region in the main screen.
Watchdog timer	When creating a new VA pod, creating a new Catalyst Center VA, or deleting VA pod, you no longer need to remain on the displayed screen until the process completes. The implementation of a watchdog timer allows you to exit the screen to any other page in Cisco Global Launchpad while the processes continue in the background. **Important** Do not close the tab or window or refresh the page during these processes. Doing so causes the background processes to pause.
VA pod and Catalyst Center VA timestamps	When creating a new VA pod or Catalyst Center VA, the **Summary** pages now display a timestamp that indicates when the VA pod or Catalyst Center VA was created.
Direct-connect configuration	While creating a new VA pod, you can now select **Direct Connect** as the preferred connectivity option.
Automated NFS backup configuration	The NFS configuration, mount, and directory creation processes are now automated, further simplifying the setup.
Region setup cleanup	A banner offering you the option to delete the region setup is no longer displayed when a region has no VA pods. This information is now displayed in the **Settings** page.
TGW and CGW cleanup	When deleting VA pods, the resources associated with the Transit Gateway (TGW) and Customer Gateway (CGW) are not automatically cleaned up. Cisco Global Launchpad retains these resources so that they can be used by other VA pods. If you no longer need the following resources, you can manually remove them: Transit Gateway (TGW) Transit Gateway Route Table Customer Gateway (CGW) VPN Connection

Feature	Description
Network connectivity	On the **Network Connectivity Check** page, a progress bar and timer now display, indicating how long it has been since you clicked on the **Proceed to network connectivity check** button in the previous screen.
Alerts	An **Alerts** panel has been added on the dashboard to display critical alerts pulled from Amazon CloudWatch.
Button name change	The **+ Add VA pod** button in the dashboard has been updated to **+ Add a VA pod**.
Login error messages	Login error messages provide more details.
Encryption of EBS volumes	EBS volumes are now automatically encrypted. For Cisco Global Launchpad releases earlier than 1.9.0, you must manually encrypt the EBS volumes if it is requirement for your organisation.

Upgrade Cisco Global Launchpad

When upgrading to the latest release of Cisco Global Launchpad, make sure you are familiar with the following:

- You cannot upgrade from a previous release of Cisco Global Launchpad to Cisco Global Launchpad, Release 1.9.x. You need to reinstall Docker Community Edition (CE) and then install Cisco Global Launchpad, Release 1.9.x.
- Cisco Global Launchpad must be running Release 1.2.1 or later before you can install Release 1.9.x and update a region version. For more information, see "Update a Region" in the *Cisco Global Launchpad 1.9 Administrator Guide*.
- To enable access to the new regions added in Release 1.9.x, your admin user needs to log in to Cisco Global Launchpad after the Cisco Global Launchpad, Release 1.9.x has been installed. After the admin user has logged in, access to all regions is enabled for all other users.
- Resources created in the current release of Cisco Global Launchpad aren't supported in earlier releases.

Compatible Browsers

Cisco Global Launchpad is compatible with the following HTTPS-enabled browsers:

- Google Chrome: Version 93 or later.
- Mozilla Firefox: Version 92 or later.
- Apple Safari: Version 16.1 or later.

We recommend that the client systems you use to log in to Cisco Global Launchpad be equipped with 64-bit operating systems and browsers.

Bugs

Open Bugs

This Cisco Global Launchpad release has no open bugs.

Resolved Bugs

Cisco Global Launchpad, Release 1.9

The following table lists the resolved bugs in Cisco Global Launchpad, Release 1.9.

Bug Identifier	Headline
CSCwj54137	Cisco Global Launchpad VA deployment does not present the Direct Connect attachment.

Limitations and Restrictions

Cisco Global Launchpad, Release 1.9.x has the following limitations and restrictions:

Automated Deployment Workflow

- The configuration for the Existing Transit Gateway (TGW) and Existing Customer Gateway (CGW) scenario is not available in the automated deployment method. You must manually configure this routing as discussed in the *Cisco DNA Center 2.3.5 on AWS Deployment Guide*.
- Any manual alterations made to the automated configuration workflow of Catalyst Center on AWS can cause conflict with the automated deployment. We recommend against making manual changes with Cisco Global Launchpad through the AWS console, because it can lead to issues that Cisco Global Launchpad cannot resolve.
- A valid Enterprise DNS is mandatory to deploy Catalyst Center on AWS. For more information, see "Create a New Cisco DNA Center VA" in the *Cisco DNA Center 2.3.5 on AWS Deployment Guide*.
- The DNS server cannot be updated through Cisco Global Launchpad after deploying Catalyst Center on AWS. However, you can update the DNS server using the AWS console. For more information, see "Update the DNS Server on a Cisco DNA Center VA Using the AWS Console" in the *Cisco DNA Center 2.3.5 on AWS Deployment Guide*.
- You can create only one Catalyst Center VA per VA pod.
- When configuring a VA pod, the following VPN vendors are not supported:
  - **Barracuda**
  - **Sophos**
  - **Vyatta**
  - **Zyxel**
- Deleting a VA pod on Cisco Global Launchpad can take approximately 20 to 40 minutes.

The Overview Pane

On the **Dashboard** pane, the **Privacy - Terms** link isn't working.

Hosted Cisco Global Launchpad

When you refresh any pane on hosted Cisco Global Launchpad pane from your browser, such as the **Create/Manage Cisco Catalyst Center(s)** pane, you are redirected to the **Dashboard** pane. During the refresh, the URL loses the query parameters that contain information about the selected region.

Regions and Availability Zones

- Cisco Global Launchpad must be running Release 1.2.1 or later before you can install Release 1.9.x and update a region version.
- Because the sa-east-1 region is not supported, VA pods and resources created in this region need to be removed manually through the AWS console.
- Cisco Global Launchpad does not support local zones and wavelength zones. It supports only AWS availability zones for regions.
- You cannot create a VA pod in the following availability zones because the minimum instance size (r5a.8xlarge) is not supported in these zones:
  - The us-east-1e availability zone in the us-east-1 region
  - The ap-northeast-2b and ap-northeast-2d availability zones in the ap-northeast-2 region
  - The ca-central-1d availability zone in the ca-central-1 region

Root Cause Analysis

Due to an update to the root cause analysis (RCA) folder structure for Amazon S3 Lifecycle, an RCA triggered in Cisco Global Launchpad, Release 1.2.x and earlier can't be displayed in Cisco Global Launchpad, Release 1.3.0 and later.

Amazon Email Subscription, Logs, and Alarms

- Multiple users should not update their email IDs concurrently. If this occurs, the latest updated email ID is used for email notification.
- The Amazon CloudWatch alarms for lambda functions remain in the insufficient data state unless a failure occurs in the corresponding lambda function execution. When a lambda function fails, Amazon CloudWatch gathers the metrics and triggers the alarm. The threshold for all lambda alarms is one, so Amazon CloudWatch can capture alerts if there are any failures.
- For some alarms, like S3, the metrics are only reported once per day at midnight in Greenwich Mean Time (GMT) or 00:00 UTC. So, it can take 24 to 48 hours for the dashboard metrics to be updated, which is an expected behavior.
- Amazon S3 buckets are automatically created to store objects, such as logs and data. When an object is marked for expiration, the Amazon S3 Lifecycle Policy automatically deletes it from the bucket. However, because the Amazon S3 Lifecycle Policy operates asynchronously, the deletion might take some time. It's important to note that when an object is marked for expiration, you aren't billed for this object anymore even though it might still be visible in the bucket. Because this is an Amazon function and policy, refer to the following Amazon AWS website for the latest information: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

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

Related Documentation

We recommend that you read the following documents relating to Cisco Global Launchpad.

For This Type of Information...	See This Document...
List of release-specific documentation related to Cisco DNA Center 2.3.5 on AWS.	*Documentation for Cisco DNA Center 2.3.5 on AWS*
Deployment and configuration on Cisco DNA Center on AWS.	*Cisco DNA Center 2.3.5 on AWS Deployment Guide*
Management of regions, VA pods, Cisco DNA Center VAs, user activity, and Amazon tools that are used to monitor resources.	*Cisco Global Launchpad 1.9 Administrator Guide*
List of supported regions with links to each region's Cost Calculator for Catalyst Center on the AWS website.	*Cost Calculators for Cisco Catalyst Center on AWS*
Use of the Cisco DNA Center GUI and its applications.	*Cisco DNA Center User Guide*
Configuration of user accounts, security certificates, authentication and password policies, and backup and restore.	*Cisco DNA Center Administrator Guide*
Cisco DNA Center release information, including new features, deployment, and bugs.	*Cisco DNA Center Release Notes*
Security features, hardening, and best practices to ensure a secure deployment.	*Cisco DNA Center Security Best Practices Guide*
Supported devices, such as routers, switches, wireless APs, and software releases.	*Cisco DNA Center Compatibility Matrix*

For This Type of Information...	See This Document...
Hardware and software support for Cisco SD-Access.	*Cisco SD-Access Compatibility Matrix*
Use of the Cisco DNA Assurance GUI.	*Cisco DNA Assurance User Guide*
Use of the Cisco DNA Center platform GUI and its applications.	*Cisco DNA Center Platform User Guide*
Use of the Cisco Wide Area Bonjour Application GUI.	*Cisco Wide Area Bonjour Application User Guide*
Use of the Stealthwatch Security Analytics Service on Cisco DNA Center.	*Cisco Stealthwatch Analytics Service User Guide*
Use of Rogue and aWIPS functionality to monitor threats in Cisco DNA Center.	*Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide*