Cisco Catalyst Center 2.3.7.x on ESXi Release Notes

First Published: 2023-12-20

Last Modified: 2024-04-16

Release Notes for Cisco Catalyst Center 2.3.7.x on ESXi

Catalyst Center on ESXi is a new form factor that supports Catalyst Center in a virtual environment. The virtual form factor helps customers rapidly deploy and operate Catalyst Center. For customers who are running Cisco Prime Infrastructure on a virtual machine (VM), Catalyst Center on ESXi provides a migration path to take advantage of Catalyst Center features.

Note Cisco DNA Center has been rebranded as Cisco Catalyst Center. During the rebranding process, you will see the former and rebranded names used in different collaterals. Be assured that Cisco DNA Center and Catalyst Center refer to the same product.

This document describes the features, limitations, and bugs for Catalyst Center on ESXi, Release 2.3.7.4 and 2.3.7.5.

For links to all of the guides in this release, see Related Documentation, on page 8.

Change History

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

Date	Change	Location
2024-04-16	Updated the package versions.	Package Versions, on page 2
2024-04-11	Added CSCwi86275 to the resolved bugs list.	Resolved Bugs, on page 7
2024-04-08	Updated with information about Catalyst Center 2.3.7.5 on ESXi software.	—
2024-03-01	Removed the Validation Tool from the unsupported features list.	Unsupported Features, on page 4
2024-02-21	Corrected the Validation Tool navigation path.	Unsupported Features, on page 4

Date	Change	Location
2024-01-18	Added the link to download the Catalyst Center on ESXi 2.3.7.4 software.	Package Versions, on page 2
	Added CSCwi68000 to the open bugs list.	Open Bugs, on page 6
2023-12-20	Initial release.	—

Package Versions

Package Name	Release 2.3.7.5	Release 2.3.7.4
Release Build Version		
Release Version	2.3.7.5.75367	2.3.7.4.75326
System Updates		
System	2.5.64	2.3.132
System Commons	2.715.65430	2.714.65447
Package Updates		
Access Control Application	2.715.65430	2.714.65447
AI Endpoint Analytics	1.11.919	1.11.726
AI Network Analytics	3.1.39	3.1.30
Application Hosting	2.3.124020205	2.3.123120506
Application Visibility and Policy	2.715.1175429	2.714.1175142
Assurance	2.370.5148	2.370.4191
Automation - Intelligent Capture	2.715.65430	2.714.65422
Catalyst Center API Catalog	6.5.142	—
Catalyst Center Global Search	6.5.14	6.3.8
Catalyst Center Platform	6.5.185	6.3.138
Catalyst Center UI	3.2.350	3.1.69
Cisco Identity Services Engine Bridge	2.715.90505	2.714.90200
Cloud Connectivity	6.3.18	6.1.45
Cloud Connectivity - Contextual Content	6.4.18	6.2.15
Cloud Connectivity - Digestor	6.4.15	6.2.10

Package Name	Release 2.3.7.5	Release 2.3.7.4
Core Platform	0.7.78	0.5.200
DxHub Cloud Connectivity	6.5.16	6.3.14
Identity and Access Management	5.1.21	4.0.33
Identity and Access Management - UI	5.1.12	3.1.11
Multiple Cisco Catalyst Center	2.715.65430	2.714.65422
Network Controller Platform	2.715.65430	2.714.65422
Network Data Platform - Base Analytics	2.370.50207	2.370.40107
Network Data Platform - Caching Infra	6.3.22	6.2.8
Network Data Platform - Core	6.3.513	6.2.34
Network Data Platform - Ingestion Infra	6.3.44	6.2.17
Network Data Platform - Manager	6.3.103	6.2.13
Network Data Platform - Pipeline Infra	6.3.522	6.2.27
Network Data Platform - Storage Management	6.3.51	6.2.54
RCA-Scripts Package	0.2.2	0.1.11
Rogue and aWIPS	2.9.408	2.9.210
SD Access	2.715.65430	2.714.65422
System Management Operations	1.3.51	1.1.1108
System Remediation	1.0.1	—
Telemetry	3.4.14	3.2.18

Features

New and Changed Features

New and Changed Features for Catalyst Center 2.3.7.5 on ESXi

This Catalyst Center on ESXi release has no new features.

New and Changed Features for Catalyst Center 2.3.7.4 on ESXi

Feature	Description
Default Single Network Interface Card (NIC)	By default, one NIC is enabled when you install Catalyst Center 2.3.7.4 as a virtual appliance on ESXi. See "Deploy a Virtual Appliance" for setup instructions in the *Cisco Catalyst Center 2.3.7.x on ESXi Deployment Guide*.
Second NIC Installation (Day-N)	As an option, after you install Catalyst Center 2.3.7.4 on ESXi, you can add an additional NIC to your deployment. For information, see "Configure an Additional Network Adapter" in the *Cisco Catalyst Center 2.3.7.x on ESXi Deployment Guide*.
ESXi Launcher App Enhancements	You can configure a virtual appliance using the ESXi Launcher App in interactive mode or silent mode. For information, see the following topics in the *Cisco Catalyst Center 2.3.7.x on ESXi Deployment Guide*. • Configure a Virtual Appliance Using the Interactive ESXi Launcher App • Configure a Virtual Appliance Using the ESXi Launcher App in Silent Mode
Diagnostics Center Validation Tool	The validation tool (**System** > **System 360** > **System Health** > **Tools** > **Validation Tool**) is supported with some limitations.

Unsupported Features

Catalyst Center 2.3.7.x on ESXi supports all of the features that Catalyst Center supports, except for the following features:

- **Automation**: Cisco Wide Area Bonjour application, Cisco DNA Traffic Telemetry Appliance, Cisco Secure Network Analytics.

- **Wireless**: Cisco User-Defined Network (UDN), Cisco Umbrella.

- **Assurance**: Sensor.

- **System Workflows**: Backup and Restore using VMware vSphere Client snapshot function, Backup and Restore from Catalyst Center hardware appliance to Catalyst Center on ESXi virtual appliance.

- **Setting Page**: Authentication API Encryption.

- **Security Policy Access (SPA)**: Security Sensor in Endpoint Analytics, Group-Based Policy Analytics (GBPA).

- **Telemetry**: VM- and host-level telemetry.

VA Requirements

The Catalyst Center on ESXi is intended for enterprise environments, such as manufacturing or education, where a large-scale requirement is present within a single physical environment.

The following requirements must be met in order to successfully deploy a Catalyst Center on ESXi virtual appliance. For performance tips that cover the most performance-critical areas of VMware vSphere, see:

- VMware vSphere Client 7.0: *Performance Best Practices for VMware vSphere 7.0* (PDF)

- VMware vSphere Client 8.0: *Performance Best Practices for VMware vSphere 8.0* (PDF)

Table 1: Virtual Machine Minimum Requirements

Feature	Description
Virtualization platform and hypervisor	VMware vSphere (which includes ESXi and vCenter Server) 7.0.x, including all patches
Processors	Intel 2.1-GHz and above CPU 32 vCPUs with 64-GHz reservation must be dedicated to the VM
Memory	256-GB DRAM with 256-GB reservation must be dedicated to the VM
Storage	3-TB solid-state drive (SSD) If you plan to create backups of your virtual appliance, also reserve additional datastore space. For information, see "Backup Server Requirements" in the *Cisco Catalyst Center on ESXi Administrator Guide*.
IO Bandwidth	180 MB/sec
IOPS	2000-2500
Latency	Catalyst Center on ESXi to network device connectivity: 200 ms

Limitations and Restrictions

Catalyst Center on ESXi has the following limitations and restrictions:

- Unlike the Catalyst Center platform, you cannot connect VMs to create three-node clusters. To achieve high availability, you need to use VMware vSphere. For more information, see the "High Availability" section in the *Cisco Catalyst Center on ESXi Administrator Guide*.

- Catalyst Center on ESXi does not support the following VMware vSphere features:

    - Fault tolerance

    - Suspending and resuming VMs

    - Cloning VMs

    - Snapshot (as backup)

- With Catalyst Center on ESXi, application telemetry is not supported for Cisco Catalyst 9500 Series Switches.

- To configure the Management interface and the Enterprise interface, manually create a virtual machine using the VMware vSphere UI and then configure both interfaces using either the Maglev Configuration wizard or the Install Configuration wizard. For more information, see the "Deploy a Virtual Appliance" section in the *Cisco Catalyst Center on ESXi Deployment Guide*.

Multiple Catalyst Centers—Limited Availability

Multiple Catalyst Center allows you to define a single global set of virtual networks for software-defined access across multiple Catalyst Center clusters integrated with a single Cisco ISE system. This Multiple Catalyst Center functionality is a Limited Availability offering in Catalyst Center on ESXi.

To facilitate global administration of Cisco SD-Access across multiple Catalyst Center clusters with a consistent set of virtual networks, the Multiple Catalyst Center feature leverages the existing secure connection with Cisco ISE to propagate virtual networks, Security Group Tags (SGTs), access contracts, and Group-Based Access Control (GBAC) Policy from one cluster to another cluster, all integrated with the same Cisco ISE deployment. Cisco ISE takes the information learned from one cluster (the Author node) and propagates it to the other clusters (Reader nodes).

Because there are significant caveats for the Multiple Catalyst Center functionality, the Cisco SD-Access Design Council reviews the requests and provides guidance for use of the Multiple Catalyst Center to participants in the Limited Availability program.

Contact your account team to submit a request to the Cisco SD-Access Design Council to participate in the Limited Availability program.

Customers who are using Cisco ISE Version 3.1 or earlier must request and install the Limited Availability package before enabling Multiple Catalyst Center.

Note
After this functionality is enabled, it can be disabled only by deleting Cisco ISE. In addition, if this functionality is enabled, because pxGrid is a required component of the solution, pxGrid cannot be disabled subsequently.

Deployment Overview

For information about how to deploy Catalyst Center in a VMware vSphere environment, see the *Cisco Catalyst Center on ESXi Deployment Guide*. The guide also covers configurations we recommend you make before you use the product.

Bugs

Open Bugs

The following table lists the open bugs in Catalyst Center on ESXi for this release.

Bug Identifier	Headline
CSCwh65050	In setups with a large number of APs, the compliance visibility reporting process takes a long time to complete.
CSCwi02622	During the .ova installation, Catalyst Center on ESXi reports, "A required disk image is missing."
CSCwi40135	Config preview for embedded wireless controllers is taking more than one hour to process.

Bug Identifier	Headline
CSCwi47941	An air-gap upgrade fails because the NTP IP subnet is not included in the allowed IP address range.
CSCwi51231	Cisco Wireless AireOS Access Point workflow gets stuck in in-progress state.
CSCwi98870	"Managed Service elasticsearch(ndp) is DEGRADED" event is displayed on system health page even though the service is running fine.

Resolved Bugs

Catalyst Center 2.3.7.5 on ESXi

The following table lists the resolved bugs in Catalyst Center 2.3.7.5 on ESXi.

Bug Identifier	Headline
CSCwf30781	No client data and AP health displayed in the Assurance Custom Dashboard Library.
CSCwh20543	Under scale conditions, the Catalyst Center on ESXi UI is not accessible for several hours while restoring data.
CSCwh29540	When we restore managed service, restore mongo db in the end.
CSCwi01883	Event doesn't trigger an Email notification.
CSCwi21047	PnP failed to onboard an AP.
CSCwi22547	The first time you display the Fabric site table, it displays only 10 sites.
CSCwi33017	Login fallback, although enabled, fails to function when an external TACACS authorization timeout occurs.
CSCwi49349	Email notification for reports includes a link that contains the management IP address instead of the Enterprise IP address.
CSCwi49639	Cisco Wireless AireOS Controller is unable to send Cisco AireOS Network Assurance telemetry due to an unauthorized JSON Web Token (JWT).
CSCwi68000	Import of System Certificate in wrong file format causes IOS-XE-based devices to be reported as not managed in Assurance.
CSCwi86275	When using TACACs for external authentication with a case sensitive username that contains mixed or upper-case letters, authentication succeeds but browser enters a redirect loop between login and home page.

Catalyst Center 2.3.7.4 on ESXi

The following table lists the resolved bugs in Catalyst Center 2.3.7.4 on ESXi.

Bug Identifier	Headline
CSCwi43972	When a user performs an advanced fresh installation with a proxy server for authentication, the installation fails, and the proxy server details are not set in the KVstore yaml in kvstore.config.cluster file.

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 Catalyst Center on ESXi.

For This Type of Information...	See This Document...
Catalyst Center on ESXi release information, including new features, limitations, and open and resolved bugs.	*Cisco Catalyst Center on ESXi Release Notes*
Installation and configuration of Catalyst Center on ESXi, including postinstallation tasks.	*Cisco Catalyst Center on ESXi Deployment Guide*
Configuration of system settings, user accounts, licensing and high availability. Procedures for configuring and performing backup and restore.	*Cisco Catalyst Center on ESXi Administrator Guide*
Use of the Catalyst Center GUI and its applications.	*Cisco Catalyst Center User Guide*
Security features, hardening, and best practices to ensure a secure deployment.	*Cisco Catalyst Center Security Best Practices Guide*
Supported devices, such as routers, switches, wireless access points, and software releases.	*Cisco Catalyst Center Compatibility Matrix*
Hardware and software support for Catalyst Center.	*Cisco SD-Access Compatibility Matrix*

For This Type of Information...	See This Document...
Use of the Cisco Catalyst Assurance GUI.	*Cisco Catalyst Assurance User Guide*
Use of the Catalyst Center Platform GUI and its applications.	*Cisco Catalyst Center Platform User Guide*
Use of Rogue Management functionality as a dashboard within Cisco Catalyst Assurance in the Catalyst Center GUI.	*Cisco Catalyst Center Rogue Management Application Quick Start Guide*

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)