U.S. AIR FORCE | UNITED STATES SPACE FORCE

CISCO

CISCO CATALYST CENTER ADOPTION GUIDE

Enhancing network operations and management across the Department of the Air Force (DAF)

This guide supports the DAF Network Technicians as they plan, deploy, and operate Cisco Catalyst Center.

Turn the page or select a tab to get started.

U.S. AIR FORCE | UNITED STATES SPACE FORCE

Cisco Catalyst Center
ADOPTION GUIDE

Cisco Catalyst Center simplifies complex environments by providing centralized visibility and control across wired and wireless infrastructure. Through automation and AI-driven insights, it empowers teams to reduce manual configuration, identify issues faster, and ensure consistent policy enforcement across the entire network.

About this Guide

This guide provides an overview of Cisco Catalyst Center adoption across Department of the Air Force (DAF) Installations.

Cisco GEMSS Engineering Support

The Cisco Global Enterprise Modernization Software and Support (GEMSS) Engineering Team will assist with planning, implementing, testing, and knowledge transfers.

The DAF GEMSS Enterprise Agreement provides Catalyst Center Advantage Licensing, which:

- Supports Catalyst-based routers, switches, and wireless devices
- Includes Catalyst Center software for monitoring, configuration, backups, and management of the Cisco ecosystem.

Guide Contents

Select a button below or the tabs on the right to navigate to that section.

Select a button to jump to the section.

Modernizing IT infrastructure is not optional; it's a strategic necessity to ensure the DAF is prepared for future conflicts and to provide foundational digital tools for missions.

Dr. Keith Hardiman
Director of IT
DAF CIO Office

Your Catalyst Center Journey Begins Here

Watch this video for a brief welcome message from the Catalyst Center adoption team.

Click to play the video.

U.S. AIR FORCE | UNITED STATES SPACE FORCE

WHAT CATALYST CENTER DELIVERS

Cisco Catalyst Center provides a unified command platform that bridges insight and action. For DAF bases, it's an essential control layer enabling proactive, automated, and scalable network operations.

Below are some capabilities of what Catalyst Center offers. These features directly support tasks already performed day to day.

Key Capabilities

Image Dashboards	Includes health views for network, client, and application performance
Network Services	Visibility and configuration of core services across the fabric
Automation Engine	Streamlined provisioning, compliance enforcement, and config drift control
Software Image Management	Maintain golden images, schedule upgrades, and apply patches safely
Integrated Tooling	Integration available for Identity Services Engine (ISE), Splunk, and other tools for consolidated network management

Feature Highlights

Device 360	Wi-Fi 6 Dashboard	AI Endpoint Analytics	Template Hub
One-click telemetry and config view per device	Deep radio frequency (RF) visibility and performance insights	Detect and classify unknown or misbehaving devices	Rapid config deployment with version tracking

Targeted Features Across Bases

Several bases have begun working with Cisco Catalyst Center in varying capacities. This effort will build on that momentum by establishing a consistent adoption of Catalyst Center capabilities across the DAF. The objective is to ensure that each participating base at a minimum, can utilize the Catalyst Center features outlined below.

Explore the Features

Cisco Catalyst Center offers a wide range of powerful features designed to simplify and automate network management, enhance security, and improve operational efficiency. This guide focuses specifically on four key features:

Inventory Management and Reporting

Manage device inventory and run reports including software version compliance and end of life reports

Software Image Management (SWIM)

Automate software upgrades to efficiently upgrade software base-wide and validate that all devices are running the standard version set for the base

Assurance and Monitoring

Live and historical troubleshooting assistance

Configuration Drift

View history of what changes were made, when those changes were made, and by whom

Select each button to see an example.

U.S. AIR FORCE | UNITED STATES SPACE FORCE

Cisco Catalyst Center IMPLEMENTATION REQUIR

Preparing for a Successful Deployment

Deploying Catalyst Center can seem complex at first glance. The following three areas provide a clear and manageable pathway to a successful deployment.

Environment Requirements

Physical requirements such as power, rack space, upstream switch, and physical cabling requirements

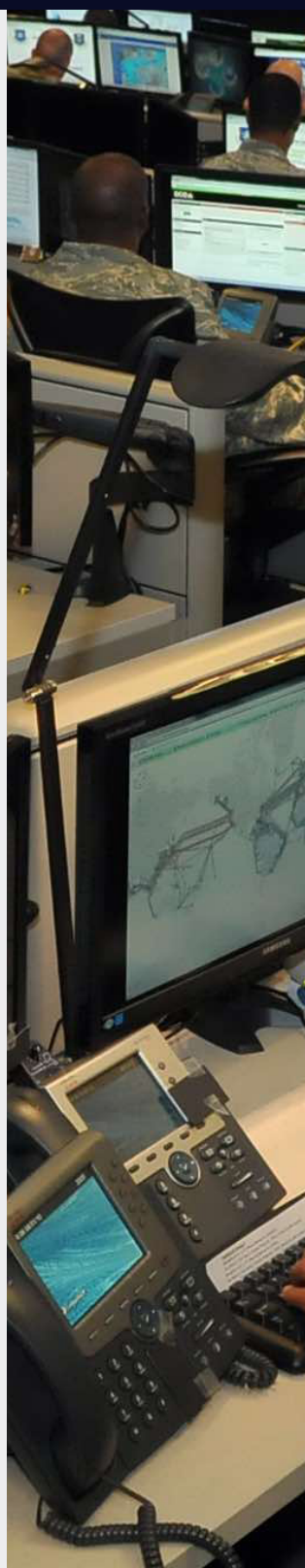
Network Requirements

IP Addresses, hostnames, and other network information such as DNS/NTP

Application Requirements

Developing the hierarchy, starting the process to request Public Key Infrastructure (PKI) signed certificates, and service accounts

Select each area to jump to that page



EMENTS

U.S. AIR FORCE | UNITED STATES SPACE FORCE

Cisco Catalyst Center
ENVIRONMENT REQUIREM

Bases need to determine the following:

Physical or virtual appliances?	• If using physical appliances, continue on. • If using VM appliances, please discuss with Cisco engineers.
Are 1 or 3 physical nodes being installed?	• If the part number is DN3-HW-APL or DN3-HW-APL-L, 1 rack unit (RU) is required for each appliance. • If the part number is DN3-HW-APL-XL, 2 RU are required for each appliance. • If using DN2, please refer to product spec sheet for RU requirements.
Consolidated or separate management and enterprise interfaces?	• It is suggested to use one interface for both management (GUI Access) and enterprise (device communication) traffic to/from Catalyst Center. • It is possible to separate management traffic and device management traffic on separate physical interfaces. Only consider this if local security requirements dictate this and separate networks already exist. • If separate interfaces are required, discuss with Cisco engineers to ensure additional requirements are met.
Single or multiple top of rack (TOR) switches?	• It is suggested to use at least two switches (for a single appliance deployment) or three switches (for a cluster of three). • Various combinations of this are possible, it depends on how many racks, appliances, and top of rack switches are available. Please discuss with Cisco engineering to determine what is best.

ENTS

Single or dual Network Interface Cards (NICs)?	• If you have one or two TOR switches, it would be suggested to use dual NICs. If a cluster of 3 is being deployed with three TOR switches, single NIC will be sufficient.
Validate power requirements	• Each appliance has two power supplies; it is strongly recommended that each power supply receives power from a different source. • Please refer to the install guide below for power requirements for each appliance model and validate with your local maintenance team to ensure the proper circuit is provided.
Validate cable requirements	• Ensure proper cables and SFPs are supplied. • Each appliance requires both copper (1 gig for Cisco Integrated Management Controller (CIMC)) and 10 gig fiber. • The total number of cables and upstream switch ports required can vary based on the specific deployment, please ensure that these requirements are satisfied.

Please refer to the Installation Guide that is applicable for your Catalyst Center deployment type and version for more details.

U.S. AIR FORCE | UNITED STATES SPACE FORCE

Cisco Catalyst Center NETWORK REQUIREMENTS

Required IP Address Types

Three groups of IP addresses are required for the Catalyst Center Appliance: Cisco Integrated Management Controller (CIMC), Enterprise IP, and Cluster IP.

CIMC	This is how the physical server itself can be managed remotely. This will also provide the ability to remotely view the Keyboard, Video, Mouse (KVM).
Enterprise IP	The Enterprise IP address is what is used to access the Catalyst Center GUI. It is also the address that is used for communication with devices that are being managed. Four addresses must be provided for this. One is a Virtual IP address (VIP) and the other three are the physical addresses that will be configured on the servers. Four addresses must be allocated whether one or more appliances are being installed. If enterprise and management traffic is being broken out, an additional four addresses will need to be provided for the dedicated management interface. Please discuss this in further detail with Cisco engineering to ensure other requirements are met.
Cluster IP	This needs to be a brand new L2 (non-Switched Virtual Interface (SVI)) VLAN dedicated for Catalyst Center, it should not extend outside of the switches that the Catalyst Center appliances are directly connected to. Just like the Enterprise IP, four addresses must be allocated for this.

Each function on the server (except the CIMC) is capable of using dual NICs to provide redundancy should the upstream switch fail. Please discuss with Cisco engineering to determine if dual NICs are best suited for your scenario.

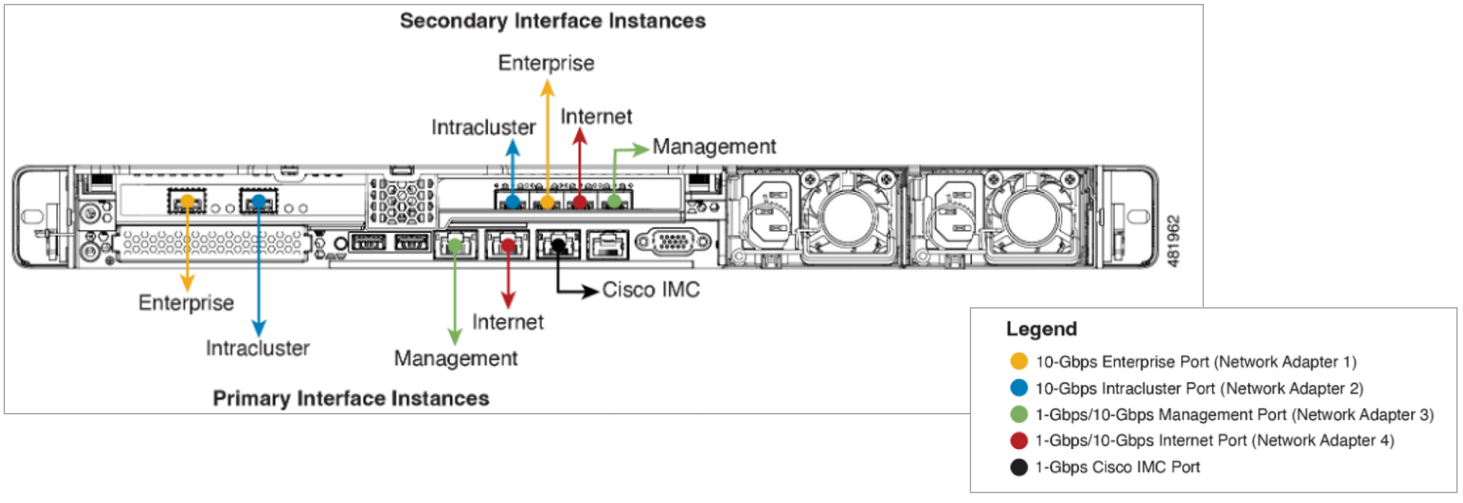
Network Installation Details

This spreadsheet should be filled out to ensure a smooth install and initial setup.

Catalyst Center								
Requirement Type	Description	Hostname	IP Address	Subnet Mask	Default Gateawy	Upstream Switch	Upstream Switch Po	VLAN
Environmental	CIMC Password			N/A	N/A	N/A	N/A	N/A
	Maglev Password			N/A	N/A	N/A	N/A	N/A
	GUI Superuser Password			N/A	N/A	N/A	N/A	N/A
	DNS 1			N/A	N/A	N/A	N/A	N/A
	DNS 2			N/A	N/A	N/A	N/A	N/A
	NTP			N/A	N/A	N/A	N/A	N/A
	NTP			N/A	N/A	N/A	N/A	N/A
Catalyst Center	CIMC (Appliance 1)	CIMC-hostname-1	x.x.x.1	/x	x.x.x.y			w
	CIMC (Appliance 2 - Future)	CIMC-hostname-2	x.x.x.2	/x	x.x.x.y			w
	CIMC (Appliance 3 - Future)	CIMC-hostname-3	x.x.x.3	/x	x.x.x.y			w
	Enterprise IP (VIP)	Enterprise-Hostname	x.x.x.10	/x	x.x.x.y			x
	Enterprise IP (Appliance 1)		x.x.x.1	/x	x.x.x.y			x
	Enterprise IP (Appliance 2)		x.x.x.2	/x	x.x.x.y			x
	Enterprise IP (Appliance 3)		x.x.x.3	/x	x.x.x.y			x
	Cluster IP (VIP)		169.254.6.99	/25	N/A			y
	Cluster IP (Appliance 1)		169.254.6.1	/25	N/A			y
	Cluster IP (Appliance 2 - Future)		169.254.6.2	/25	N/A			y
	Cluster IP (Appliance 3 - Future)		169.254.6.3	/25	N/A			y
	Container Subnet (Internal)			169.254.32.0/20				
	Cluster Subnet (Internal)			169.254.48.0/20				

Download Excel Spreadsheet

The diagram below shows the physical interface locations and roles on the server. Please refer to the installation guide for more details or reach out to Cisco engineers for further clarification on requirements or your specific install.



U.S. AIR FORCE | UNITED STATES SPACE FORCE

Cisco Catalyst Center
APPLICATION REQUIREMEN

Service Accounts

These recommended service accounts for each base will ensure smooth operations during and after installation of Catalyst Center.

Account	Purpose	Key Requirements	Notes
Cisco ID (CCOID)	License and software management	Dedicated account tied to base	Coordinate with Cisco account team for setup
ISE Account	Enable Platform Exchange Grid (PxGrid) Integration	Admin access to ISE and PxGrid permissions	Dedicated account for Catalyst Center
Device Service Account	Allow Catalyst Center to log into network devices	Username/password only, cannot require CAC authentication	May reside on ISE, AD, or on the network device (not recommended)

Determining Network Hierarchy

Catalyst Center has a concept called Network Hierarchy, this is a feature that allows you to categorize and group devices based on the physical location and geographic region. This is how you can segment upgrades and/or manage configuration pushes.

It is key to ensure that a well-considered hierarchy is implemented from the start for device management.

The hierarchy can be imported from a CSV file or configured through the GUI. Please work with your Cisco engineers to determine the best hierarchy for your base and the best way to configure it.

NTS

Catalyst Center Certificates

When it comes to certificates, Catalyst Center has two aspects:

System Certificates

- These are the certificates Catalyst Center will use when users log into Catalyst Center for GUI Management.
- These are also used for PxGrid integration with ISE.
- It is a security vulnerability if this certificate is not PKI signed, it is strongly suggested that this be done.
- Please have the process and contacts engaged so this certificate can be signed when ready.
- Catalyst Center can generate a Certificate Signing Request (CSR) that can be provided to the PKI team for signing and applied when the signed certificate is returned.

PKI Certificates

- Catalyst Center uses certificates to securely communicate with network devices.
- By default, Catalyst Center will sign certificates and provide those to devices when they are onboarded into Catalyst Center.
- It is possible to convert Catalyst Center into a subordinate certificate authority (sub CA) to a enterprise PKI, but this is a cumbersome process.
- Please discuss this with the Cisco engineering team to determine the best path forward.

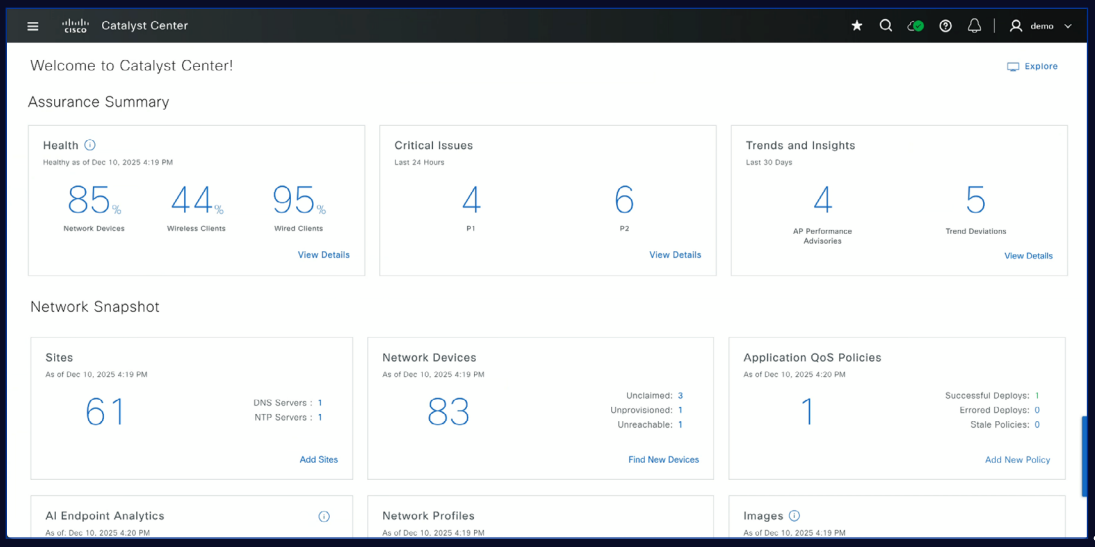
U.S. AIR FORCE | UNITED STATES SPACE FORCE

Cisco Catalyst Center
GUI OVERVIEW

Catalyst Center offers two ways to navigate through the menus. You can use the hamburger menu to navigate through various pages, or you can use the search bar to navigate to a specific page.

Hamburger Menu Navigation

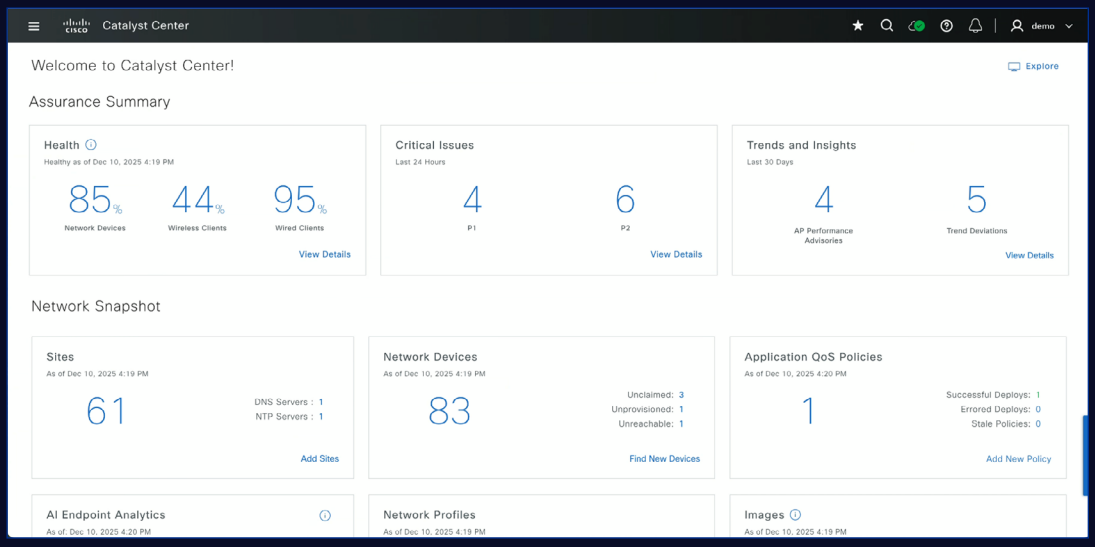
In this example, we use the hamburger menu to navigate to the Inventory page.



Click to zoom

Search Bar Navigation

Here, the search bar is used to navigate to the same Inventory page.



Click to zoom

Hierarchy Configuration

To configure the Hierarchy, navigate to Hierarchy (Hamburger Menu > Design > Network Hierarchy).

The Hierarchy Structure is:

Global > Area (Parent) > Area (Child) > Building > Floor (If Desired)

An example of this could be as follows: Global > Sage Airforce Base (Area) > CDN_Region_1 (Area) > Building A (Building) > Floor 1 (Floor)

View Example 

Configuring Device Credentials

Catalyst Center is capable of managing full device configurations, including TACACS and running configurations. However, for this adoption guide, the focus is on enabling core capabilities of managing software on devices, viewing alerts, and assisting with troubleshooting. Templates and configuration management are intended as follow-on efforts.

To configure the minimum settings required for Catalyst Center to begin managing a device, the device credentials and telemetry settings must be configured.

To configure the Device Credentials, click the Hamburger Menu > Design > Network Settings > Device Credentials

Under the Device Credentials tab, click Manage Credentials, select Add, and select the credential type you want to add (CLI and Simple Network Management Protocol (SNMP) are required at minimum, Department of War (DoW) Security Technical Implementation Guide (STIG) requires SNMPv3 vs V2.)

The default Telemetry settings should be sufficient and not require any changes.

View Configuration 

U.S. AIR FORCE | UNITED STATES SPACE FORCE

Catalyst Center Assurance

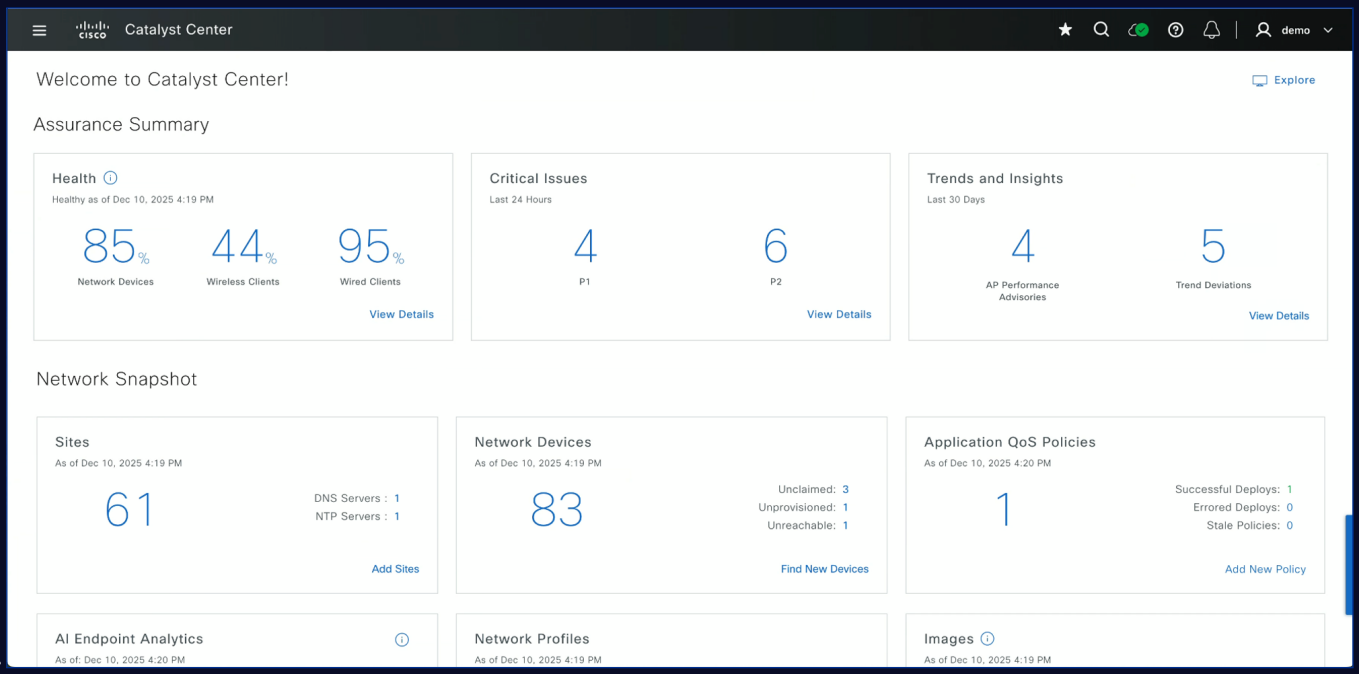
Catalyst Center Assurance provides combination of network health and a view of reported issues and events. This feature can be used for viewing a snapshot of the networks current state as well as assist with troubleshooting issues in real time.

Network and Device Health is a concatenated score determined by various factors based on data gathered from devices. Some of these data points include:

Syslog Reports of Events
Such as interface going up or down

Device Environmental State
Like power supply or temperature information

Device Overall Running State
For example, CPU/memory usage



Click to zoom

Reporting

Catalyst Center features an extensive library of pre-defined reports and empowers users to create custom reports tailored to specific requirements.

Select the example SWIM Report below to view a walkthrough of how to run a report based on a report template.

SWIM Report

Device Name	Device Family	Device Type	Device Role	IP Address	Location	Serial No.	Current Version	Code Upgrade Date	Prior Upgrade Date
CSS-AP9130-A	Unified AP	Cisco Catalyst 9130AXI Unified Access Point	ACCESS	172.16.3.54	Global/United States/Maryland/Fulton/FUL01/Floor 2	FJC27101YNS	17.12.5.41	--	--
CSS-AP9130-B	Unified AP	Cisco Catalyst 9130AXI Unified Access Point	ACCESS	172.16.3.55	Global/United States/Maryland/Fulton/FUL01/Floor 2	FJC27101YNQ	17.12.5.41	--	--
sda-3504-wlc-2	Wireless Controller	Cisco 3504 Wireless LAN Controller	ACCESS	172.16.202.106	Global/United States/Virginia/Herndon/Data Center/Floor 3	FCW2329M0QD	8.10.196.0	--	--
shared-svcs-sw.usps.cisco.com	Switches and Hubs	Cisco Catalyst 38xx stack-able ethernet switch	CORE	172.16.202.254	Global/United States/Virginia/Herndon/Data Center/Floor 3	FOC2004U0KH	16.12.12	Wed, 22 Jan 2025 21:05:17 UTC	--
css-9800-01.usps.cisco.com	Wireless Controller	Cisco Catalyst 9800-CL Wireless Controller for Cloud	ACCESS	172.16.202.107	Global/United States/Virginia/Herndon/Data Center/Floor 3	9EBVRQC5KBA	17.12.5	Mon, 03 Nov 2025 20:38:30 UTC	--
usps-css-fusion-rtr.cisco.com	Routers	Cisco 4451-X Integrated Services Router	BORDER ROUTER	172.16.0.1	Global/United States/Virginia/Herndon/Data Center/Floor 3	FJC2331A007	17.12.4	--	--
sda-3504-wlc-1	Wireless Controller	Cisco 3504 Wireless LAN Controller	ACCESS	172.16.202.105	Global/United States/Virginia/Herndon/Data Center/Floor 3	FCW2329M0N8	8.10.196.0	--	--
EdgeSW2.usps.cisco.com	Switches and Hubs	Cisco Catalyst 9300 Switch	ACCESS	172.16.2.3	Global/United States/Virginia/Herndon/Site 2/Floor 3	FJC2330E0NJ	17.18.1	Wed, 19 Nov 2025 16:25:26 UTC	Wed, 26 Mar 2025 05:31:11 UTC
sda-9300-border2_pod1.usps.cisco.com	Switches and Hubs	Cisco Catalyst 9300 Switch	DISTRIBUTION	172.16.0.3	Global/United States/Virginia/Herndon/Site 2/Floor 3	FJC2330U0TK	17.12.4	--	--
EdgeSW1.cisco.com	Switches and Hubs	Cisco Catalyst 9300 Switch	ACCESS	172.16.2.2	Global/United States/Virginia/Herndon/Site 1/Floor 3	FJC2330S14U	17.16.1	Wed, 02 Jul 2025 01:07:44 UTC	--
shared-svcs-sw.usps.cisco.com	Switches and Hubs	Cisco Catalyst 38xx stack-able ethernet switch	CORE	172.16.202.254	Global/United States/Virginia/Herndon/Data Center/Floor 3	FOC2004U0KH	16.12.12	Wed, 22 Jan 2025 21:05:17 UTC	--
sda-9300-border1_pod1.usps.cisco.com	Switches and Hubs	Cisco Catalyst 9300 Switch	DISTRIBUTION	172.16.0.2	Global/United States/Virginia/Herndon/Site 1/Floor 3	FCW2304L16X	17.12.4	--	--

View Workflow

Commonly Used Report Templates

The most common reports that are run include:

- **Inventory**
- **Software Version Report**
- **Vulnerability**
- **End-of-Life**

Note: Some of these reports may have limited functionality if Catalyst Center is installed in an air-gapped environment without access to the Cisco cloud server over the internet.

U.S. AIR FORCE | UNITED STATES SPACE FORCE

Cisco Catalyst Center
USE CASES

Select each of the four demos in this section to explore a representative use case with a guided walkthrough. These interactions show how the tool is used in practice.

Inventory Management and Reporting

Catalyst Center offers multiple ways to add devices.

Plug and Play (PNP)

An unconfigured device boots up and is provided Catalyst Center details through DHCP and option 43.

Add Device

You can provide the IP address of a single device and/or a CSV file of multiple IP addresses.

Discovery via Subnet

Provide a subnet range of management IP addresses and Catalyst Center will scan through that range looking for devices.

Discovery via CDP/LLDP

Provide a “seed” device that has other devices directly connected. Catalyst Center will use Cisco Discovery Protocol (CDP) to communicate with the connected devices to it for discovery.

If devices are already in production and share a subnet for management IP addresses, Discovery via Subnet will likely be the best way to onboard devices to Catalyst Center.

Discovery via Subnet Demo

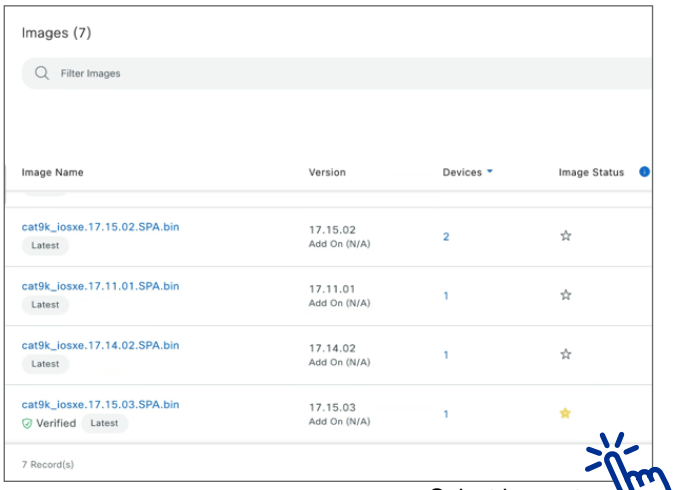
Select the button to launch demo.

Software Image Management (SWIM)

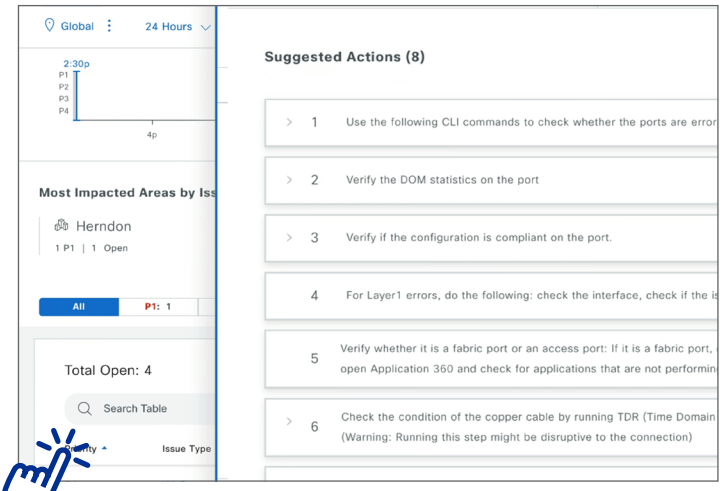
SWIM is the utility in Catalyst Center for managing software versions on Devices.

You can set what is called a “golden image” as a standard version that should be running on certain device models across the network. When a golden image is set, upgrades can be scheduled for devices that are on a different version (higher or lower than the golden image).

Upgrades can be staged where Catalyst Center will copy the files to the devices and perform the software version change later.



Select image to launch demo.



Select image to launch demo.

Guided Troubleshooting

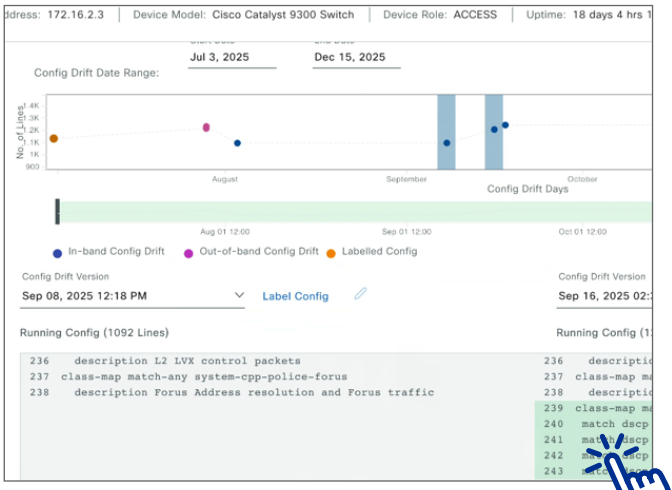
Catalyst Center Assurance allows you to see the health of a device and any alarms that have been raised, as seen on page 16. Catalyst Center also offers guided troubleshooting. As Catalyst Center receives syslog messages from devices, it can not only detect and report the issue, it can provide common steps to assist with troubleshooting and/or resolving the issue.

Config Drift

Catalyst Manager will keep track of changes made to devices. Changes are marked as in band or out of band.

- **In band** means that Catalyst Center made the change using templates and/or telemetry settings.
- **Out of band** means that someone logged into the device directly and made a configuration change.
- NOTE: Unless templates are being used to manage all of the device’s configuration, most changes will show as out of band. This is okay in the early stages of adopting Catalyst Center.

By default, Catalyst Center will retain the last 15 changes, but that can be increased up to 50 changes.



Select image to launch demo.

U.S. AIR FORCE | UNITED STATES SPACE FORCE

MAINTAINING APPLIANCE HEALTH

Credential Management

Catalyst Center requires four accounts and access areas that support software management, device connectivity, and server administration.

CCO Account

- Catalyst Center requires a Cisco Connection Online (CCO) account to be added and stored.
- The CCO account is used to download IOS images and Catalyst Center updates.
- The CCO account must be tied to the contract that includes the licenses for the base.

CIMC Credentials

- The Cisco Integrated Management Controller (CIMC) interface manages the physical aspects of the server remotely.
- CIMC credentials do not integrate with network devices or TACACS.
- Store CIMC credentials securely to avoid password recovery procedures.

Group Mailbox

- Create the CCO account using a group mailbox rather than an individual user.
- A group mailbox allows the account to continue functioning if personnel changes.

Service Account

- Catalyst Center uses a service account to log into network devices.
- The service account must be set to not expire.
- Credentials must remain synchronized between the service account and Catalyst Center.
- Incorrect credentials can cause repeated login attempts and result in device lockouts.

These accounts and credentials enable Catalyst Center to interact with Cisco services, network devices, and the underlying server infrastructure. Clear ownership and proper management of each access type help maintain system availability and prevent avoidable access or authentication issues.

Disaster Recovery

There are two backups used by Catalyst Center, the system backup with configuration information and the assurance data backup with details about what has happened on the network. Both require their own directory on the backup server.

System Backup

- Uses remote sync (RSYNC) over Secure Shell (SSH) for backup of the system files.
- Includes hierarchy, device settings, inventory, templates, etc.

Assurance Backup

- Performs a Network File System (NFS) backup of the assurance data held.
- Receives telemetry from devices in the inventory and evaluates the received data.
- Data is valid from 15-30 days, depending on the data source. Expired data is purged when no longer needed by the system.

These disaster recovery systems support data integrity and service continuity in the event of an outage. Proper configuration ensures Catalyst Center can be restored quickly with minimal impact to network operations.

Planning for access and recovery protects availability.

Shutdown and Power On Procedures

Use proper procedures if restarting or powering down the Catalyst Center appliance. Not following these procedures can result in corruption of the database requiring a re-install of the appliance. Please be sure to follow these steps.

If you want to use SSH in order to halt your appliance or perform a warm restart, complete the following tasks:

Before you begin

You need the following:

- Secure Shell (SSH) client software.
- The IP address that you configured for the 10-Gbps Enterprise port on the appliance that needs reconfiguration. Login to the appliance at this address, on port 2222. To identify the Enterprise port, see the rear-panel figures in the installation guide.
- The Linux username (*maglev*) and the password that is currently configured on the target appliance.

Procedure

Step 1 Using a Secure Shell (SSH) client, login to the IP address of the Enterprise port of the appliance that must be reconfigured, on port 2222:
ssh maglev@*Enterprise-port's-IP-address* **-p 2222**

Step 2 When prompted, enter the Linux password.

Step 3 Enter the command that is appropriate for the task you want to perform:

- To halt the appliance, enter: **sudo shutdown -h now**
- To initiate a warm restart, enter: **sudo shutdown -r now**
- If you are prompted for the Linux password, enter it again.

Step 4 Review the command output that is displayed as the host shuts down.

Step 5 If you halted your appliance, power up the Maglev root process by turning the appliance back on, using the front-panel power button.

Before turning the appliance back on after powering off:

- Validate that the proper power is being supplied to the appliance.
- Validate availability of the management networks in which Catalyst Center participates.
- Ensure network services are online and functioning correctly (NTP/DNS).

Opening a Cisco TAC Case

Cisco Technical Assistance Center (TAC) provides technical support for Cisco products, including Catalyst Center and associated network components. Providing the right details up front can speed troubleshooting with Cisco TAC. Use the guidance below to prepare an effective support case.

- When opening a case with Cisco TAC, be sure to indicate if the issue is with the Catalyst Center itself or something with the network.
- If Catalyst Center guided troubleshooting was used, be sure to include any outputs.
- Ensure a clear problem description is provided. For example, instead of stating “the internet isn’t working,” be more specific by explaining “intermittently throughout the day, users are complaining that they are unable to connect to the internet.”
- Please refer to the GEMSS Quick Reference Guide in Appendix A for details on opening a Cisco TAC case.

Show Tech

The Validation Tool in Catalyst Center System Health allows you to export a file with appliance infrastructure status. You can then share this exported filed with Cisco TAC for more efficient troubleshooting. The video below shows how to export this file.

U.S. AIR FORCE | UNITED STATES SPACE FORCE

Watch this video for a brief overview of the Department of the Air Force (DAF) Global Enterprise Modernization Software and Support (GEMSS) Program.

Click to play the video.

GEMSS FOR U.S. AIR FORCE AND SPACE FORCE

Catalyst Center Engineering Support

The Cisco GEMSS Engineering Team is available to your organization in support of base level enablement.

To request support on Cisco Catalyst Center, contact:
GEMSS-Catalyst-Center-Support@cisco.com

Advanced Service Resources

Five dedicated Cisco certified architect and engineer resources support design, implementation, delivery and management of the Cisco environment.

Helpful Links

DAF Cisco GEMSS Quick Reference Guide

Cisco Catalyst Center Documentation

DAF GEMSS Resource Center

U.S. AIR FORCE | UNITED STATES SPACE FORCE

APPENDIX A

GEMSS Quick Reference Guide

APPENDIX B

Table of Acronyms

CCO	Cisco Connection Online
CDP	Cisco Discovery Protocol
CIMC	Cisco Integrated Management Controller
Cisco TAC	Cisco Technical Assistance Center
CSR	Certificate Signing Request
DAF	Department of the Air Force
DHCP	Dynamic Host Configuration Protocol
DoW	Department of War
GEMSS	Global Enterprise Modernization Software and Support
IPAM	IP Address Management
ISE	Identity Services Engine
KVM	Keyboard, Video, Mouse
LLDP	Link Layer Discovery Protocol
NFS	Network File System
PKI	Public Key Infrastructure
PNP	Plug and Play
PxGrid	Platform Exchange Grid
RF	Radio Frequency
RSYNC	Remote Sync
RU	Rack Unit
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STIG	Security Technical Implementation Guide
Sub CA	Subordinate Certificate Authority
SVI	Switched Virtual Interface
SWIM	Software Image Management
TACACS	Terminal Access Controller Access-Control System
TOR	Top of Rack
VIP	Virtual IP Address
VLAN	Virtual Local Area Network

Created by Skyline-ATS