Department of the Air Force (DAF)

Global Enterprise Modernization Software and Support (GEMSS)

Standard Operating Procedures (SOP)

Version 3.0, April 2026

Table of Contents

Section 1 | Purpose

This document provides the standard operating procedures for the Department of the Air Force (DAF) Global Enterprise Modernization Software and Support (GEMMS) contract. This and many other resources are found at Iron Bow's GEMSS Resource website. For any questions or concerns, please email GEMSS@ironbow.com for a prompt reply.

Section 2 | Contract Summary

2.1 Contract Information

Contract Name:	Cisco GEMSS
Cisco Contract Number:	204246961
Reseller:	Iron Bow Technologies
Period of Performance (PoP):	Base: 24 April 2026 – 23 April 2027

2.2 Contract Overview

In April 2026, the Defense of the Air Force (DAF), signed the Department of the Air Force's Global Enterprise Modernization Software and Support (GEMSS) Cisco enterprise agreement contract. This GEMSS program provides the DAF (Air Force and Space Force) access to SmartNet Total Care for all Cisco devices, which provides 24x7 technical support through online and a toll-free telephone call-in service, provides hardware replacement for defective devices (RMA replacement), and provides device software downloads (iOS, patches, hotfixes). Additionally, the contract provides unlimited Cisco DNA Advantage licenses for Cisco SD-WAN and Catalyst-based routing, switching, IOT, and wireless devices. There are 33,000 Cisco Learning Credits (LC), 12 Cisco Modeling Labs (6 enterprise and 6 educational) available for DAF consumption per Period of Performance year. The prime contract holder, Iron Bow Technologies, is partnered with Cisco to provide all GEMSS program entitlements.

2.3 How to Get Cisco Devices Covered by the GEMSS Program?

The DAF uses many methods to implement programs, which may include Cisco devices to achieve the program's Fully Operational Capability (FOC) status. Some purchased devices may not follow the traditional DAF acquisition methods and funding streams (e.g. 3080, 3400) used by operational units.

How do I know if my devices are covered by the GEMSS program? If the devices are DAF-owned and the devices are processing DAF data, operating on a DAF network (e.g. NIPRNet, SIPRNet), the Cisco devices are covered by the GEMSS program. Government Owned, Contractor Operated (GOCO) are covered by the GEMSS program but may require DAF-ownership verification. Devices that are Contractor Owned, Contractor Operated (COCO) are not covered by the GEMSS program.

If the devices do not appear in the Unit's GEMSS Virtual Account under the DAF Smart Account (NEXTGEN USAF), then the following procedure is used to add the devices to a Virtual Account:

- Unit submits a Hardware Request Form, found on the GEMSS Resource website (https://ironbow.com/gemss-usaf-space-force)
- First Civilian or Military will email the completed form to GEMSS@IronBow.com (requests received from contractor emails require device ownership verification before approval)

For contracted companies that purchase, operate, and or maintain Cisco devices, device verification is required before the devices are covered by the GEMSS program. The device model and serial numbers are verified by the Contractor Officer Representative (COR) or first government official

(civilian or military, non-contractor) with oversight of the mission, then sends an email stating the devices are DAF-owned and verified to GEMSS@IronBow.com. The device information is submitted using a completed Hardware Request form found on the Iron Bow GEMSS program website (https://ironbow.com/gemss-usaf-space-force). An alternative method for verification would be to submit the SF 1449, the contracting document that documents the devices were purchased through a DoD/DAF contracting agency.

2.4 Summary of Coverage

2.4.1 Cisco SmartNet Total Care (SNTC)

- Provides unlimited 24x7x365 Technical Assistance Center (TAC) online through a 1-800 telephone service and an online portal, https://mycase.cloudapps.cisco.com/case
- Case prioritization occurs using one of four severity levels
    - Severity 1 or 2 – the suggestion is to call the 1-800 phone number immediately
    - Severity 3 or 4 – call the 1-800 or use the online portal to submit the issue
- Provides 8x5xNext-Business-Day replacement for all DAF-owned, Cisco-branded, hardware
- Provides unlimited Internetwork Operating System (IOS) updates and patch for Cisco devices
    - Access Download from Cisco Software Central: https://software.cisco.com

2.4.2 Cisco DNA Advantage Licensing

Provides the ability to consume unlimited amount Cisco licensing for the following technologies:

- Cisco DNA Advantage for Routing
- Cisco DNA Advantage for Switching
- Cisco DNA Advantage for IOT
- Cisco DNA Advantage for Wireless
- Cisco SD-WAN virtualized network license
- Catalyst Center Network Management Software— Access to centralized management software for automation, configuration, and monitoring of the Cisco ecosystem

Refer to the Cisco Capability Matrix website for compatible Cisco DNA devices.

2.4.3 Learning Credits (LC) & Cisco Modeling Labs (CML)

- Cisco Learning Credits provides a means for DAF government personnel access to Cisco University computer-based training, provide Instructor Led Training (online & in-person), request Cisco certification tokens, and access to attending Cisco Live events. To gain access to these training options, a Unit leadership approved Training Request form is submitted to GEMSS@IronBow.com.
- Cisco Modeling Labs provides a means to simulate a network setup to test and configure new and existing network configurations. To gain access to a Modeling Lab complete and email a Training Request form to GEMSS@IronBow.com.
- Training Credits and Modeling Labs access is granted for 12 months from the date the access is granted.

2.4.4 Expert Care – Incident Management (formerly HTOM)

Cisco's single point of contact for all Technical Assistance Center (TAC) support assistance, prioritization, and management. For questions and concerns regarding a TAC case, contact afhtom@cisco.com.

2.4.5 Expert Care – Problem Resolution (formerly HTTS)

- Commonly called, "Classified Support," when speaking with the TAC support team
- Personalized, high-touch support: expedited routing and call handling with limited after hours on-call support
- Ability to transmit and receive classified information via Secret Internet Protocol Router Network (SIPRNet) and Voice over Secured Internet Protocol (VoSIP).

Note: Most technologies are supported from 8:00 a.m. – 8:00 p.m. (Eastern)

2.4.6 Cisco Certified Engineers for Enterprise-wide Solutions

There are five full-time equivalent Cisco-certified engineers that deliver and manage, design and strategically engineer solutions for Headquarters Air Force (HAF). This team works hand-and-glove with HAF and 16 AF on enterprise-wide engineering solutions. If a Unit or Program has an enterprise-wide requirement, the detailed requirement can be routed through SAF/CNS Front Office for prioritization.

Section 3 | Technical Assistance Center (TAC) Support

3.1 What's covered?

The DAF is provided unlimited 24x7 TAC support for all DAF-owned, Cisco-branded, hardware & software, and SWSS-eligible application software (owned as of 21 June 2019).

3.2 How to Open a TAC Case

TAC Cases can be opened by navigating to http://mycase.cloudapps.cisco.com/case (user must login in with their Cisco CCO ID credentials that are associated with a .MIL email address). When a TAC is opened, a severity level is assigned, based on the mission impact, see section 3.3 below for the description of the severity codes.

For Severity Levels 1 and 2 TAC Cases:

1. Call the Technical Assistance Center at 800-553-2447, Option 1
2. Provide TAC the GEMSS contract #204246961
3. Live Customer Hand-off to a Cisco engineer

For Severity Levels 3 and 4 TAC Cases:

Open your service request using the online tool, Support Case Manager (http://mycase.cloudapps.cisco.com/case).

Information Needed to Open a Service Request:

- Your Cisco Connection Online ID (CCO ID) and contact information (full name)
- Severity of your service request (See section 3.3, Severity Level Descriptions.)
- Preferred contact method (email, phone number)
- GEMSS Contract# 204246961 and device serial number
- Description of your issue (symptoms, business impact, technology)
- Site information (for verification purposes)
- Details on troubleshooting steps you have taken.

3.3 Severity Level Descriptions

Severity 1 (S1): The DAF's network or environment is "down" or there is a critical impact to operations. The DAF and Contractor will commit all necessary resources around the clock to resolve this situation.

Severity 2 (S2): Operation of an existing network or environment is severely degraded, or significant aspects of the DAF's operations are negatively affected by inadequate performance of Cisco equipment. The DAF and Contractor will commit full-time resources around the clock to resolve the situation.

Severity 3 (S3): Operational performance of the DAF's network or environment is impaired while most operations remain functional. The DAF and Contractor will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4): The DAF requires information or assistance from the Contractor with Cisco product capabilities, installation, or configuration. There is little or no effect on business operations.

3.4 Case Escalation Procedure

If a case is not progressing adequately or the quality of service is not satisfactory, DAF personnel can escalate the case with the following process:

- During normal business hours 8:00 am – 8:00pm (Eastern): Contact Cisco TAC at 1-800-553-2447 and request the TAC case have its severity level raised. The HTOM Team can also be contacted by emailing afhtom@cisco.com.
- After normal business hours (including weekends/holidays): Contact Cisco TAC at 1-800-553-2447 and request to raise the TAC case's severity level with the on-shift TAC Duty Manager. Outside of 8:00 a.m. – 8:00 p.m. on regular duty days, advanced support is available by engaging the on-call U.S. Public Sector HTOM by email at ggsghtom@epage.cisco.com.

Section 4 | GEMSS Portal

The GEMSS Portal allows DAF personnel to submit requests for Cisco DNA Advantage licenses and gain access to their Unit's DAF GEMSS Virtual Account. Navigating to the GEMSS Portal is accessed at: https://ironbow.servicenowservices.com/gemss. See Appendix A for the steps to create a GEMSS Portal account.

4.1 DAF Smart Account and Virtual Account Overview

There is one Smart Account for the entire DAF, **DAF GEMSS**. Each Unit, Program, or Agency with DAF-owned Cisco devices that process DAF data will have the Cisco devices assigned to a Virtual Account under the DAF Smart Account. **NOTE:** Devices must be assigned under the DAF Smart Account to ensure GEMSS coverage.

Each virtual account is set up using the nomenclature, Parent Name-Unit or Program Name-[N, S, or T]. The first part of the name will identify what parent organization the Unit or Program reports to (e.g. MAJCOM, FLDCOM, or CCMD). The second part is the Unit or Program's abbreviation. For the 375th Communications Squadron an abbreviation like 375 CS will be used. The last letter denotes the classification, N = Non-Secure (e.g. NIPRNet), S = Secret (e.g. SIPRNet) , T = Top Secret (e.g. JWICS). A complete virtual account may look like *AMC-375 CS-N*. A new virtual account request is submitted through the GEMSS Portal, see Appendix B for the steps. Submit the following information with the request:

- Smart Account Domain: en-ea.us.af.mil
- Reason for Request
- Cisco Connection Online (CCO) IDs that require virtual account access

- DAF Unit or Program Name and Office Symbol
- Name of the Parent CCMD, MAJCOM, or FLDCOM the Unit or Program is assigned

4.2 Maintaining Parent-Level and Unit-Level Virtual Accounts

Each Unit or Program's Virtual Account is assigned to a Parent Virtual Account, which is either a Combatant Commands (CCMD), Major Commands (MAJCOM), or Field Commands (FLDCOM). Each Parent Virtual Account has an assigned Command representative who is an Admin User (e.g. government person on A6 staff). Only the Command representative, the GEMSS Team, and Cisco will have Admin permissions, all others will only be granted User permissions (e.g. personnel accessing Unit's virtual account will only have User access not Admin access). Below is a list of actions the Parent and sub-Virtual Account users will perform annually.

NOTE: Users will only be granted access to an account when their Cisco account is associated with a .MIL, an AFIT.edu, or USAFA.edu email address. Exceptions require the first government person that oversees the contractor, the COR of the contract, or the Command representative to email an exception request with a justification to GEMSS@IronBow.com. Personal email addresses will not be permitted under any circumstances (e.g. Gmail, Yahoo, etc.).

- Parent and sub-Virtual Accounts should be reviewed for proper user access; submit any add or delete for access to GEMSS@IronBow.com when personnel PCS, retire, or are added/removed from a contract
- Devices are removed from CLC when turned into DLA Disposition Services (DRMO); submit a Hardware Request Form from the GEMSS Resource website (https://ironbow.com/gemss-usaf-space-force) or the Unit's verified DPAS inventory to GEMSS@IronBow.com to maintain account accuracy
- Devices listed in CLC are verified accurate to ensure Cisco postures replacement devices in geographically-close warehouses; otherwise, device replacement timelines will be impacted
- Review, at the start of each Fiscal Year, the list of unsupported devices (LDOS status) and integrate into long-range predictive planning (budget execution, POM planning, UFR consideration) to maintain a healthy Cisco ecosystem, see Appendix D for the process to export a list of unsupported devices.

To gain permissions to a Virtual Account, submit a request through DAF GEMSS Portal, see Appendix B for the steps, or email the info to GEMSS@IronBow.com. When submitting the request, include the following information:

- Smart Account Domain: en-ea.us.af.mil
- Reason for Request
- Your CCO ID (CCO IDs must be associated with a .MIL email address)
- Name of CCMD, MAJCOM, or FLDCOM requesting permissions to
- Name of DAF Unit or Program (as applicable)
- Name of Cisco Software Benefit Administrator (SBA)

4.3 Procuring Licenses for Existing Hardware

For existing products that require licenses, users will need to request the licenses via DAF GEMSS Portal, see Appendix D for the steps. Users will need to provide the following information:

- Hardware Product Model
- Name of Unit or Program's Virtual Account and Parent Virtual Account

- Quantity of licenses requested
- For SDWAN routing licenses, include bandwidth tier (15M, 100M, 1GB, 10GB)

Once complete, the GEMSS Team will deposit licenses in the Unit's or Program's Virtual Account. Licenses can be accessed at Cisco Software Central (http://software.Cisco.com). For more information on accessing licenses, refer to Appendix C and Appendix E.

4.4 Procuring Licenses for New Devices

New devices are bundled with software licenses and support. To remove these costs, the purchase must be associated with the DAF GEMSS Smart Account, by providing the Contracting Squadron with the following information:

- Smart Account Name: NEXTGEN USAF
- Smart Account Domain: en-ea.us.af.mil
- Name of Unit or Program's Virtual Account
- List of model and serial number of any LDOS devices being replaced

For more information on accessing licenses, refer to Appendix C and Appendix E.

Section 5 | Device Information and Replacement

The Cisco Software Central (https://software.cisco.com) website is the location where units can access various details about the GEMSS Virtual Account, assigned devices and licenses, and access software downloads. Appendix D provides a process to export a list of unsupported devices, which allows for the long-range planning and replacement of devices. If a device requires replacement now, call TAC support, see section 3.2 for the process to contact TAC support.

5.1 Cisco License Central (CLC) Tool

The CLC tool provides access to the Cisco database through the Cisco Software Central website. On the left side of the first row of links is the *Access Cisco License Central* link. Upon clicking this link, you must login using your CCO ID credentials. For awareness, user's CCO IDs must be associated with a .MIL email address. Once logged in, at the top, click on the Devices tab. This will show all devices assigned to the Virtual Accounts. There are many key pieces of information a Unit or Program can extract from this list to provide a better understanding about their network ecosystem. There are standard columns that list the name of the device, model, and serial number, but there is also a key column to watch called *End of Support*, which provides a date when each device will no longer be supported. When a device enters LDOS status Cisco is no longer required to replace or support the device; therefore, is no longer covered by the GEMSS program.

5.2 Device Replacement

Under the GEMSS program, all Cisco devices are covered for defective device replacement. If a Cisco device is no longer functioning and has not entered an unsupported status, submit a TAC case to initiate a replacement, see section 3.2. When a TAC case is entered, the Unit or Program's technician and a Cisco certified technician will work through the issue. If it's determined the device requires replacement, then the TAC Cisco technician will begin the replacement process.

Section 6 | Software Downloads

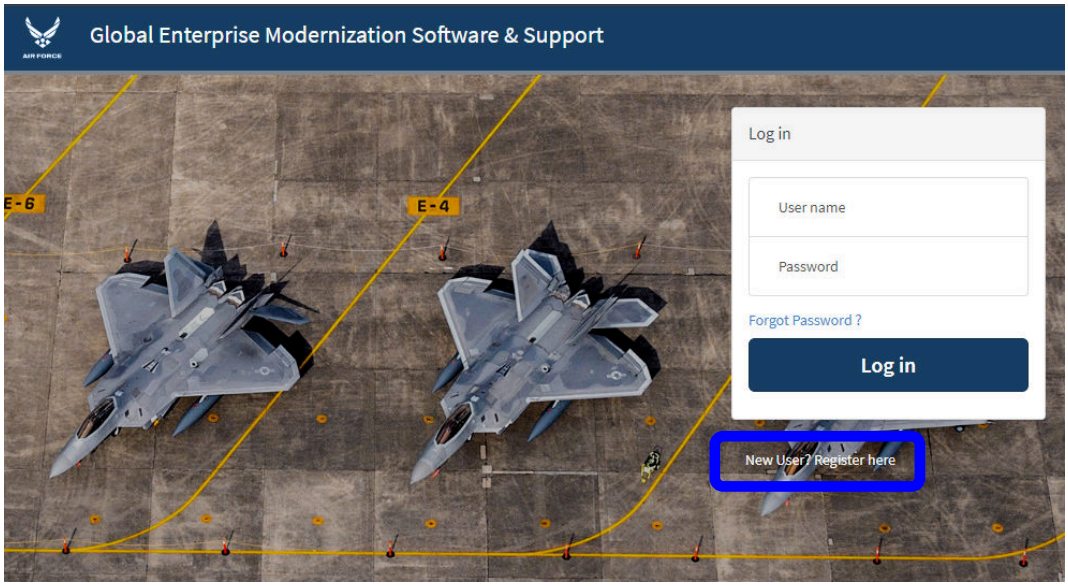
The GEMSS program provides access to device software downloads for all Cisco products (e.g. iOS, bugfixes, hotfixes). To download new updates navigate to the Cisco Software Central (https://software.cisco.com) website. The "Access Downloads" link provides access to a website where current software is found by searching for the model number. The website will also track the user's download history to assist in finding recent downloads.

Network Management Software (Catalyst Center)

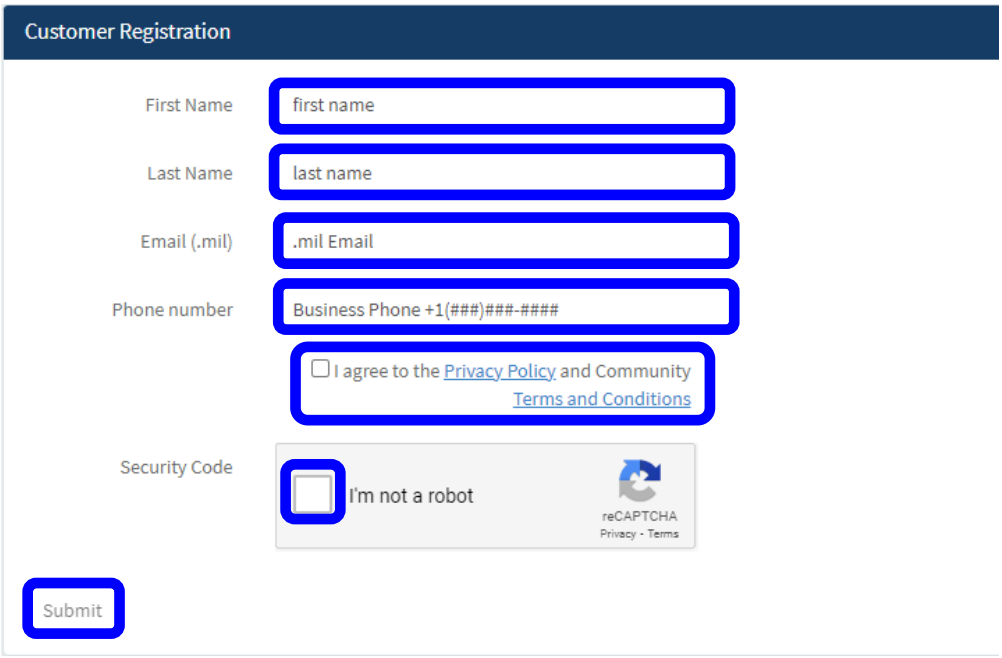
The Cisco Catalyst Center (formerly known as DNA Center) is a GEMSS entitlement and available as a software download virtual image. This network management software provides a way to manage the configuration, management, and monitoring of all Cisco devices on the network. For more details about Catalyst Center and how to use it, see the Catalyst Center website.

Appendix A | How to Create a GEMSS Portal Account

1. Begin by navigating to the DAF GEMSS Portal
2. Click the *New User? Register here* hyperlink



3. Complete the Request Form using a ".Mil" email address (e.g., john.doe@spaceforece.mil), click the checkbox to agree to the Policy, click the "I'm Not a Robot" checkbox, then click *Submit*. Once approved you will receive a confirmation email to log into the GEMSS Portal.



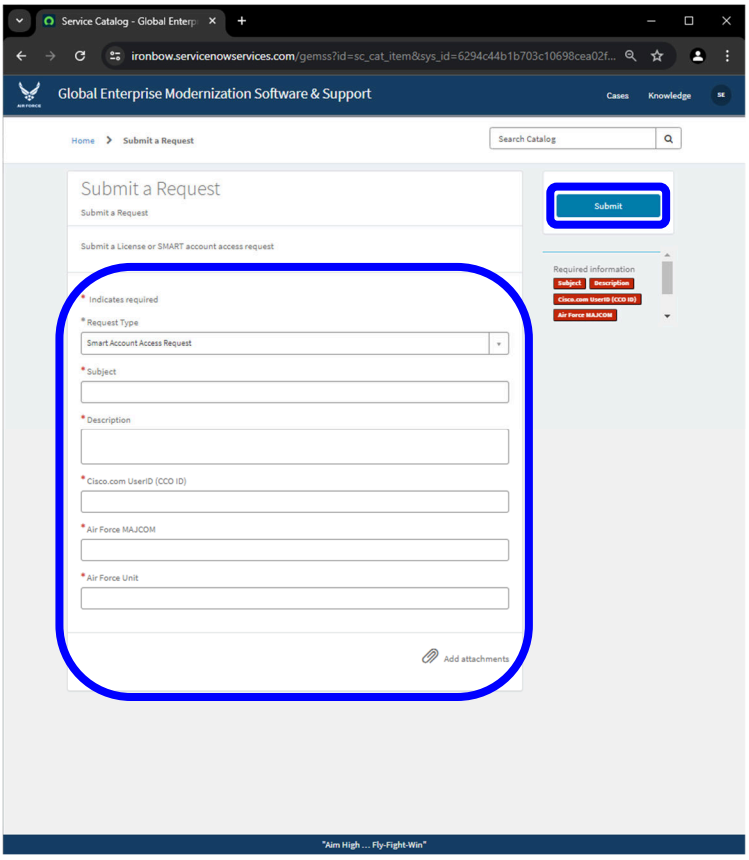
Note: Personal email addresses will not be accepted. For additional assistance, please contact the licensing specialist by email: gemss@ironbow.com

Appendix B | How to Request a New Virtual Account or Access to an Existing Virtual Account

Logon to the DAF GEMSS Portal using your GEMSS Account username and password

1. Click the *Submit a Request* button.

2. Complete the form with *Required Information*.



3. Click the *Submit* button.

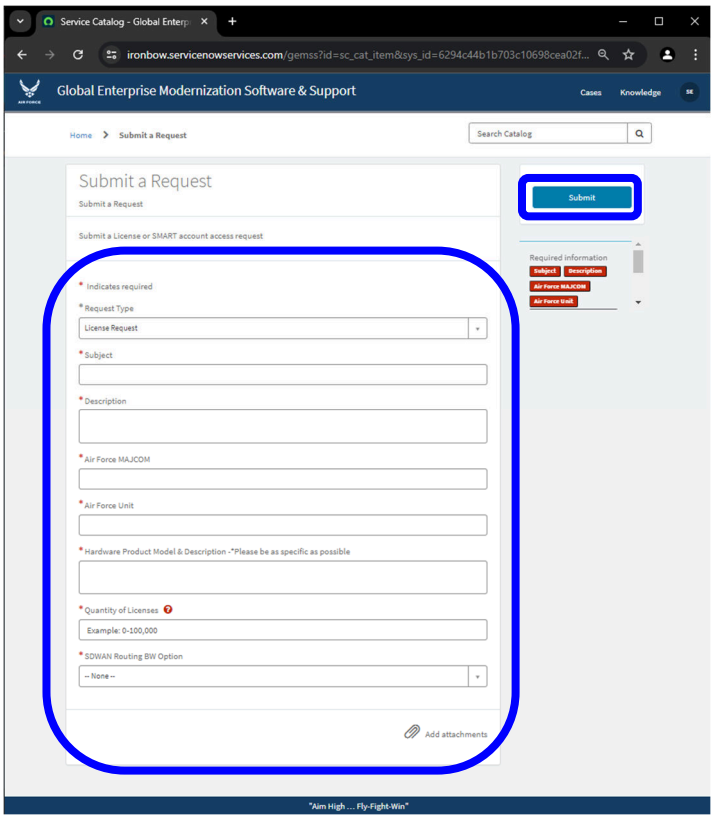
Note: Once the request is completed, an email confirmation is sent to the user. Additionally, the status of any request can be checked under “My Open Cases.”

Appendix C | How to Request Licenses for Existing Devices

Begin by navigating to the DAF GEMSS Portal and log in using your username and password for your GEMSS account:

1. Click the *Submit a Request* button.

2. Complete the form with *Required Information*.



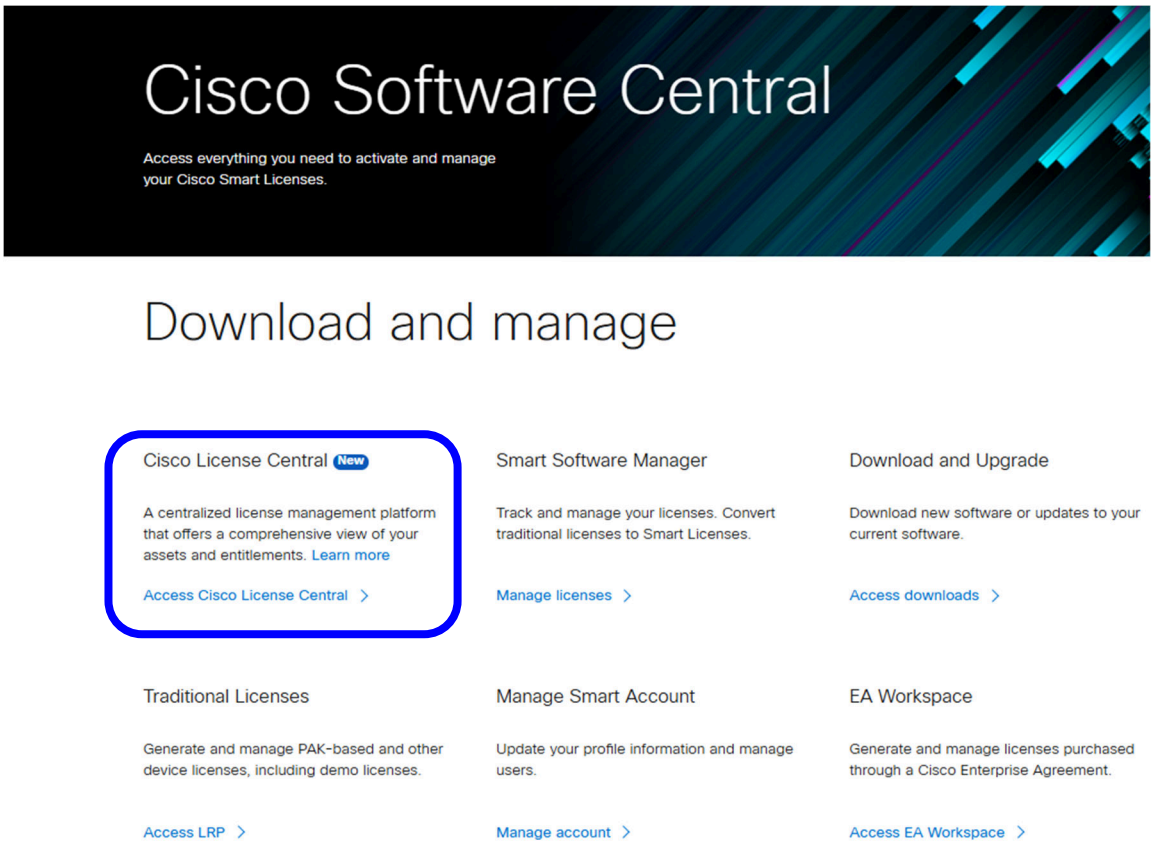
3. Click *Submit*.

Note: Once the request is completed, an email confirmation is sent to the user. Additionally, the status of any request can be checked under “My Open Cases.”

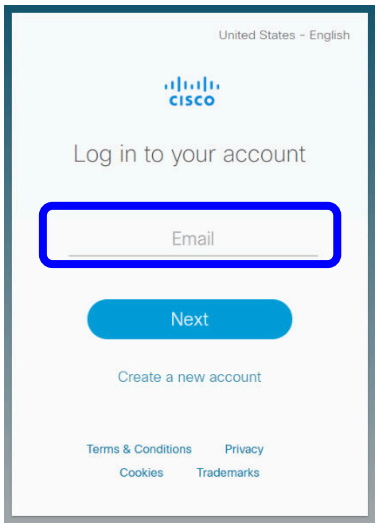
Appendix D | Export a list of Devices that enter Last Day of Support (LDOS)

A list of unsupported devices or LDOS devices assigned to a virtual account identifies what devices are no longer being supported by Cisco. This can support the Program Objective Memorandum (POM) planning process. Here is how to export a list of devices that will reach LDOS by the end of the Fiscal Year.

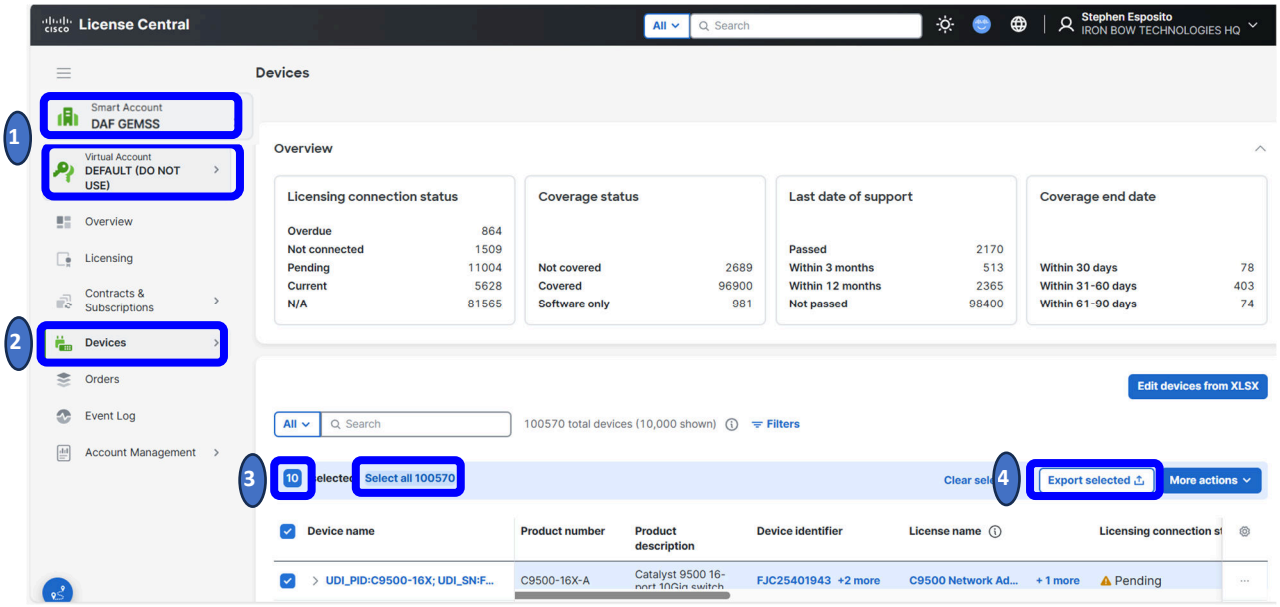
1. Navigate to Cisco Software Central (https://software.cisco.com)
2. Click *Access CLC* link on the left side of the first row of links



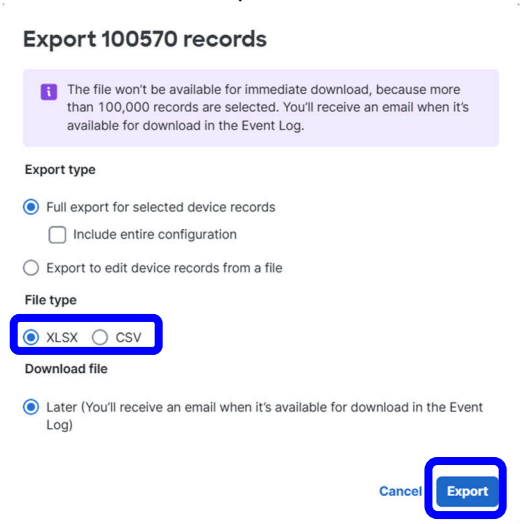
3. Login using CCO ID credentials or use the “Create a new account” link if your CCO ID is not associated with a “.Mil” email address.



4. Verify the proper Virtual Account are selected (top-left side of website), see #1 in picture below. Next, click “Devices”, see #2, then “Device Inventory” from the push out menu. The devices for the chosen accounts are displayed at the center bottom of the website. Click the checkbox, see #3, then click the Select All, next to the checkbox. This will select all the devices for all the chosen accounts.



5. To export the list, click on the Export Selected button, see #4 above, then the popup menu below is displayed. Choose the type of file to download. Either an Excel file or a Comma Separated Values (CSV) file, then click the Export button.



6. The file is downloaded immediately. The file can be found in the computer’s Downloads folder.

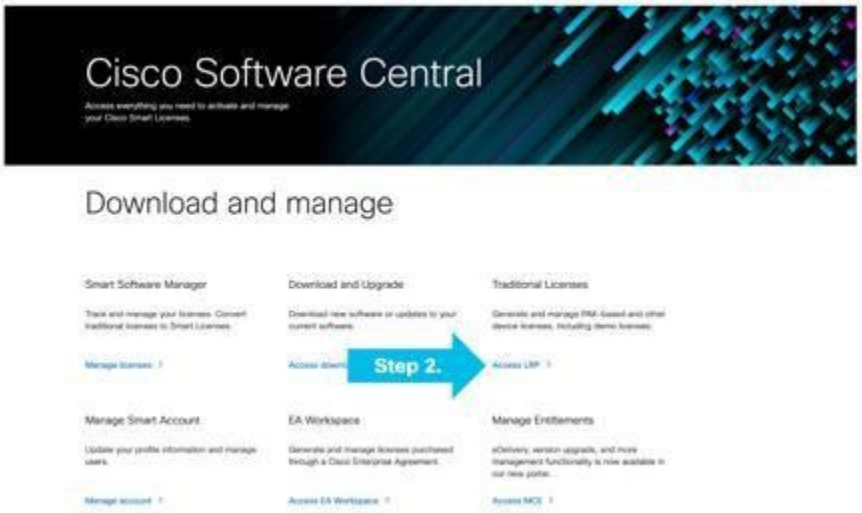
Appendix E | Accessing GEMSS Software Licenses with Cisco Smart Accounts

E.1 Accessing Traditional Licensing

Traditional PAK-based Licenses can be accessed from the License Registration Portal. To access licenses, navigate to Cisco Software Central , then:

1. Log in using your CCO ID, by clicking *User* (CCO IDs must be associated with a .MIL email address)

2. Click on *Access LRP* under Traditional Licenses, where the license files (lic) are available for download.

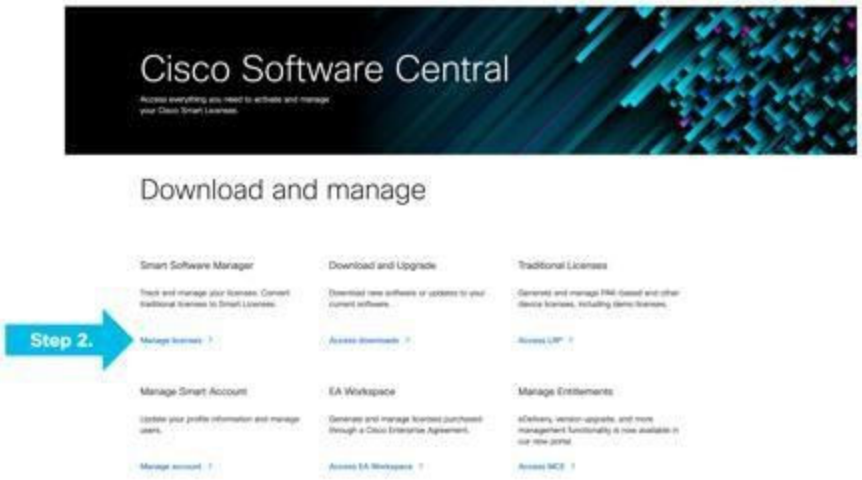


E.2 Accessing Smart Licensing

Smart Licenses can be accessed from Cisco Smart Software Manager. To access licenses, navigate to Cisco Software Central :

1. Log in using your CCO ID, by clicking *User* (CCO IDs must be associated with a .MIL email address)

2. Click on *Manage licenses* under Smart Software Manager, where the license files (lic) are available for download.



Note: For more information on how to configure Smart Licensing on Cisco products, go to Cisco.com and search for Cisco Smart Licensing, or click here.

Appendix F | Abbreviations and Definitions

CCMD	Combatant Command (e.g., TRANSCOM, NORTHCOM)
CCO ID	Cisco Connection Online Identification. The user credentials created at Cisco.com to access device details from the Cisco Software Central website (CCO IDs must be associated with a .MIL email address).
CLC	Cisco License Central A tool in the Cisco Software Central website that provides user access to accounts, devices, and license details assigned to the accounts.
DAF	Department of the Air Force
FLDCOM	Field Command, used by Space Force (e.g. SSC, SpOC, STARCOM)
LDOS	Last Day of Support. Cisco's term that defines a date when a device will no longer be supported, replace, or create software updates for.
MAJCOM	Major Command, used by Air Force (e.g. ACC, AMC, AFMC PACAF, USAFE)
SDWAN	Software Defined Wide Area Network