

Multiple Cisco DNA Center to Single Cisco ISE

Prescriptive Deployment Guide

November 2021

First Publish: October 2021
Last Update: November 2021



Contents

Hardware and Software Version Summary 3

About This Guide 3

Define..... 5

Design 7

Deploy 13

Process 1: Request Package and Installation 13

Process 2: Integrate Multiple Cisco DNA Center with Single Cisco ISE 15

Operate..... 42

Appendix A: Hardware and Software Versions 49

Appendix B: References Used in this Guide 50

Feedback..... 51

Hardware and Software Version Summary

Table 1. Hardware and Software Version Summary

Item	Part number	Minimum Software version
Cisco® DNA Center Appliance ¹	<ul style="list-style-type: none">DN1-HW-APL (M4-based chassis)DN2-HW-APL (M5-based chassis)DN2-HW-APL-L (M5-based chassis)DN2-HW-APL-XL (M5-based chassis)	1.3.3.5 or higher
SD Access Package ²	<ul style="list-style-type: none">sd-access³	See Cisco DNA Center Release Notes for applicable version
Access Control Application Package ²	<ul style="list-style-type: none">access-control-application³	See Cisco DNA Center Release Notes for applicable version
Multiple Cisco DNA Center Package ²	<ul style="list-style-type: none">multi-dnac-enablement³	See Cisco DNA Center Release Notes for applicable version
Cisco Identity Services Engine	<ul style="list-style-type: none">All supported Cisco Secure Network Server (SNS) AppliancesR-ISE-VMM-K9=	ISE 2.4 Patch 11 or higher ISE 2.6 Patch 3 or higher ISE 2.7 Patch 1 or higher ISE 3.0 – All Patches

¹ Deployments supported:

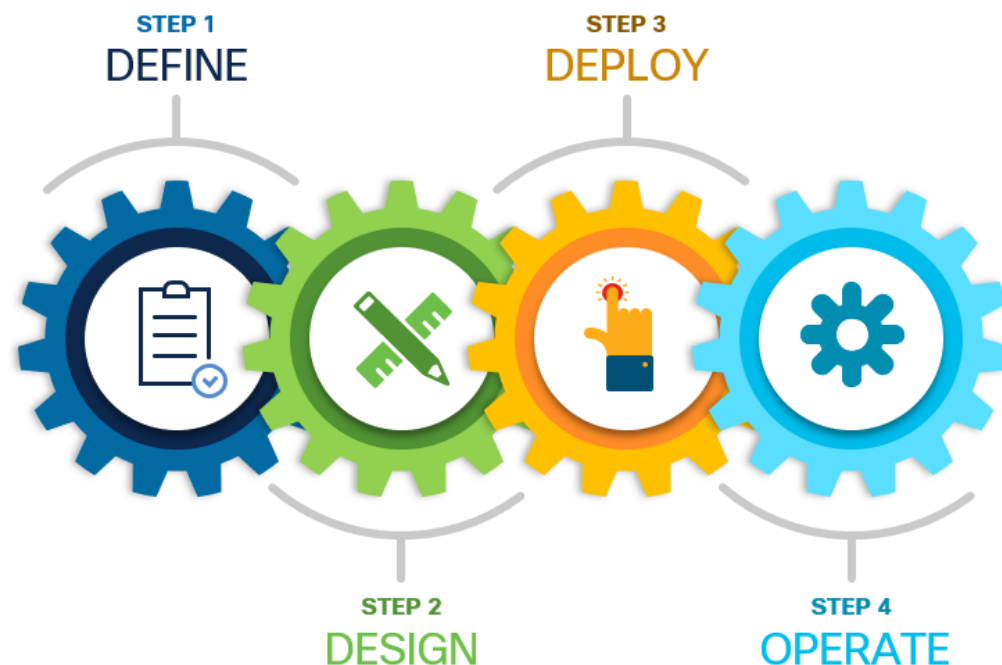
- Single Node Cluster
- Single Node Cluster with Disaster Recovery (DR)
- 3-Node High Availability Cluster
- 3-Node High Availability Cluster with Disaster Recovery

² GUI Display Name

³ CLI Display Name

About This Guide

This guide provides technical guidance to design, deploy and operate the Software-Defined Access Solution using Multiple Cisco DNA Center Clusters with a single Cisco Identity Service Engine (ISE) deployment. It focuses on the steps to integrate these multiple Cisco DNA Center clusters with a single Cisco ISE system.



This guide contains four major sections:

The **DEFINE** section defines the use cases for the Multiple Cisco DNA Center to ISE feature and its benefits in Cisco Software-Defined Access (SD-Access) Fabric.

The **DESIGN** section shows the deployment topology, solution overview, requirements, and considerations with Multiple Cisco DNA Center to ISE solution.

The **DEPLOY** section demonstrates the steps involved to enable Multiple Cisco DNA Center to ISE feature.

The **OPERATE** section demonstrates the Day N procedure and basic troubleshooting tips to be followed on Cisco DNA Center Clusters and Cisco ISE with respect to Multiple Cisco DNA Center Feature.

Define

Cisco DNA Center and Cisco Identity Service Engine integrates to solve multiple use cases such as Micro-Segmentation, secured network access for authorized users, guests, and onboarding IoT devices into a Software Defined Access network. Cisco SD-Access customers with Large or Distributed Enterprise Fabric networks often leverage more than one Cisco DNA Center cluster for management simplicity, multi-regional deployments and even for compliance reasons. At the same time, they leverage a single Cisco ISE cluster for globally consistent Group-based Access Control Policy. The "Multiple Cisco DNA Center" feature centrally manages Virtual Networks, Scalable Groups, Group-based Access Control Policy, Access Contracts and Virtual Networks to Scalable Group associations. It does so by allowing multiple Cisco DNA Center clusters to integrate with a single Cisco ISE system.

What is covered in this Guide?

This guide provides guidance to Cisco Software-Defined Access customers integrating Multiple Cisco DNA Center clusters with Cisco ISE. The process, procedure, and steps listed in this guide are working configurations verified with the Cisco DNA Center, Cisco ISE, and Cisco IOS XE code versions listed in [Appendix A](#).

What is NOT covered in this Guide?

Although this deployment guide is about Cisco DNA Center and Cisco ISE, it does not cover the initial bootstrap and installation of the Cisco DNA Center appliances and Cisco ISE deployment, shared services installation and deployment such as DHCP, DNS, and network connectivity configuration between various infrastructure components such as the routers and switches. Deployment of the SD-Access Fabric and its various features are beyond the scope of this guide as well.

For more information on these items, please see additional references in [Appendix B](#).

About Cisco DNA Center and SD-Access

Cisco DNA Center is the network management and command center for the Cisco Digital Network Architecture (DNA), built on intent-based networking principles. It helps you build the new network and deliver better experiences more securely, so you can focus on your business, and not on your network. It creates a holistic end-to-end platform for your enterprise so you can better manage the business. Cisco DNA Center provides a centralized management dashboard for complete control of this new network. This platform can simplify IT network operations, proactively manage the network, provide consistent wired and wireless policy, and correlate insights with contextual cognitive analytics.

Cisco DNA Center is a hardware appliance powered through a software collection of applications, processes, services, packages, and tools. This software provides full automation capabilities to deploy networks in minutes, to perform device upgrades and patches network-wide with a minimal clicks, and to help ensure configuration consistency and save your team time. It also provides visibility and network assurance through intelligent analytics combined with AI/ML which has more than 30 years of best practices to help optimize your network's performance, reduce troubleshooting time for your team, and lower the cost of network operations.

Cisco® Software-Defined Access (SD-Access) is the industry's first intent-based networking solution for the Enterprise built on the principles of Cisco's Digital Network Architecture (Cisco DNA). Cisco SD-Access provides automated end-to-end segmentation to separate user, device and application traffic without redesigning the network. Cisco SD-Access automates user access policy so organizations can make sure the right policies are established for any user or device with any application across the network. This is accomplished with a single network fabric across LAN and WLAN which creates a consistent user experience anywhere without compromising on security.

Building this next-generation solution involved some key foundational elements including:

Controller-based orchestrator to drive business intent into the orchestration and operation of network elements including day-0 configuration of devices and policies associated with users, devices and endpoints as they connect to a network.

Network fabric leveraging Virtual Network (VN) overlays in order to support mobility, segmentation and programmability at a very large scale.

Programmable switches to build a modern infrastructure for automated device provisioning, open API interfaces, granular visibility using telemetry capabilities along with seamless software upgrades.

Companion Resources

Find the companion guides [Cisco Software-Defined Access Solution Design Guide CVD](#), [Cisco DNA Center & ISE Management Infrastructure Deployment Guide](#), [SD-Access Fabric Provisioning Prescriptive Deployment Guide](#), [SD-Access for Distributed Campus Prescriptive Deployment Guide](#), related deployment guides, design guides, and white papers, at the following pages:

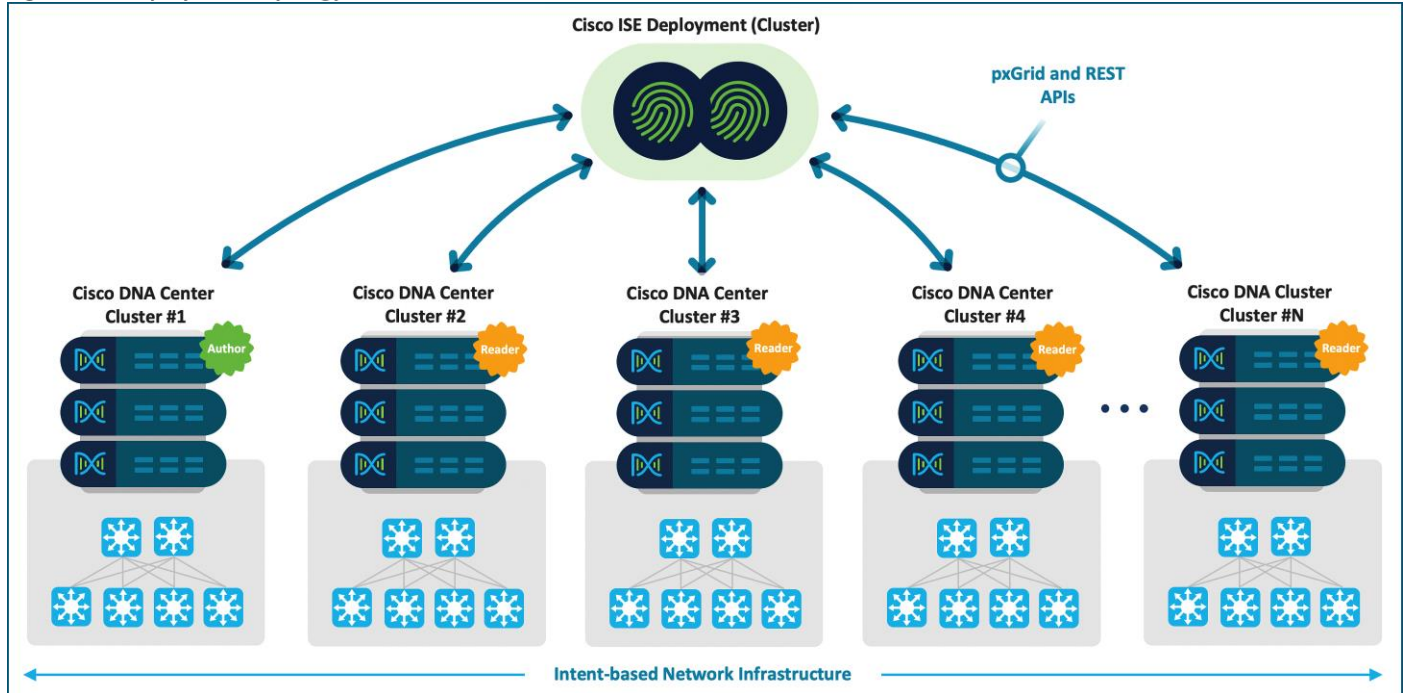
- <https://www.cisco.com/go/designzone>
- <https://cs.co/en-cvds>
- <https://cs.co/sda-resources>

If you didn't download this guide from Cisco Community or Design Zone, you can [check here](#) for the latest version of this guide.

Design

Deployment Topology Overview

Figure 1. Deployment Topology



Solution Overview

Cisco DNA Center provides a mechanism to create a trusted communications link with Cisco ISE to propagate Virtual Networks (VNs), Scalable Group Tags (SGTs), Access Contracts, Group-Based Access Control (GBAC) Policy, and VN-to-SGT Associations. Here, ISE is the consumer of this information. Cisco ISE provides the runtime policy services to the network, which includes Group-Based Access Control Policy downloads to the network devices.

The Multiple Cisco DNA Center feature leverages the existing secure connection with Cisco ISE to replicate VNs, SGTs, Access Contracts, GBAC Policy, and VN-to-SGT Associations from one cluster to another cluster which are integrated with same Cisco ISE deployment. Here, ISE takes this information learned from one cluster (the Author Node as defined below) and propagates it to the other clusters (Reader Nodes).

Multiple Cisco DNA Center feature is supported on all appliance types (44-core, 56-core, and 112-core) deployed in as either a single-node cluster or a three-node cluster with or without Cisco DNA Center Disaster Recover enabled.

Solution Components

The Multiple Cisco DNA Center feature has specific role designations for the clusters:

- Author Node Cluster
- Reader Node Cluster

Author Node Cluster

This is the first cluster that integrates with the ISE deployment. The Author Node cluster is the source of truth for all of Cisco SD-Access policy information. The Author Node cluster manages VNs, SGTs, Access Contracts, GBAC Policy, and VN-to-SGT Associations. Creation, modification, or deletion of policy components can only be performed on the Author Node cluster.

The Author Node cluster pushes VN and policy related information to ISE via ERS/PxGRID REST APIs for Cisco ISE to consume the information and publishes it to all other Cisco DNA Center Clusters in the Reader Node role.

Only **ONE** (1) cluster can be designated as the Author Node supported. It is the only node that can be Brownfield (containing user-defined Virtual Network, Scalable Groups (SGT's), Access Contracts, Group-Based Access Control (GBAC) Policy and VN to SGT Associations) Cisco DNA Center Cluster

Reader Node Cluster

All other Cisco DNA Center clusters are Reader Node cluster. Reader Node clusters have a Read-Only view of VNs, SGTs, Access Contracts, GBAC Policy, and VN-to-SGT Associations. However, these objects are available to use for provisioning operations just as if this were a stand-alone Cisco DNA Center cluster.

A Reader Node cluster does not display Access Contracts or Policies, though has a hyperlink to cross-launch to the Author Node cluster to access that information. Reader Node clusters will consume the same VNs, SGTs, Access Contracts, GBAC Policy, and VN-to-SGT associations that are defined on the Author Node cluster.

VNs can only be created on the Author Node cluster. Once created they are propagated to the Reader Node clusters. To use this VN on the Reader Node clusters, the VN must be added to the fabric site. The Reader Node clusters will configure the associated network attributed such as Virtual Network Identifies (VNID), Route Targets (RT), and Route Distinguishers (RD) which are local to that cluster.

Except for the VN and Policy features listed above, each Reader Node cluster are independent clusters that manage their own network infrastructure.

The Multiple Cisco DNA Center feature enables global policy administration across multiple Cisco DNA Center clusters integrated to a single Cisco ISE. This capability does not change the underlying limitations of managing virtual networks and fabrics on multiple Cisco DNA Center clusters. A virtual network may have the same name across multiple Cisco DNA Center clusters, which allows it to support consistent security group-virtual network associations across multiple clusters. But at the individual cluster level, the actual network attributes to associate with a VN (VRF, route target, route distinguisher, and so on) are not identical across clusters. This is the same as when operating independent Cisco DNA Center clusters.

Before adding a Cisco DNA Center node as a Reader, you must remove all admin-created Cisco SD-Access policy data on the Reader Node cluster for Cisco DNA Center to integrate with Cisco ISE. This includes non-default Virtual Networks (any Virtual Networks other than *DEFAULT_VN* and *INFRA_VN*), Scalable Group to VN mappings, User-defined Access Contracts and Group-Based Access Control Policy.

Tech tip

In Cisco DNA Center Releases 2.2.2.x and earlier, up to **THREE** (3) Reader Node clusters are supported. This is **FOUR** (4) clusters in total including the Author Node cluster.

In Cisco DNA Center Release 2.2.3.x and later up to **FOUR** (4) Reader Node clusters are supported. This is **FIVE** (5) clusters in total including the Author Node cluster.

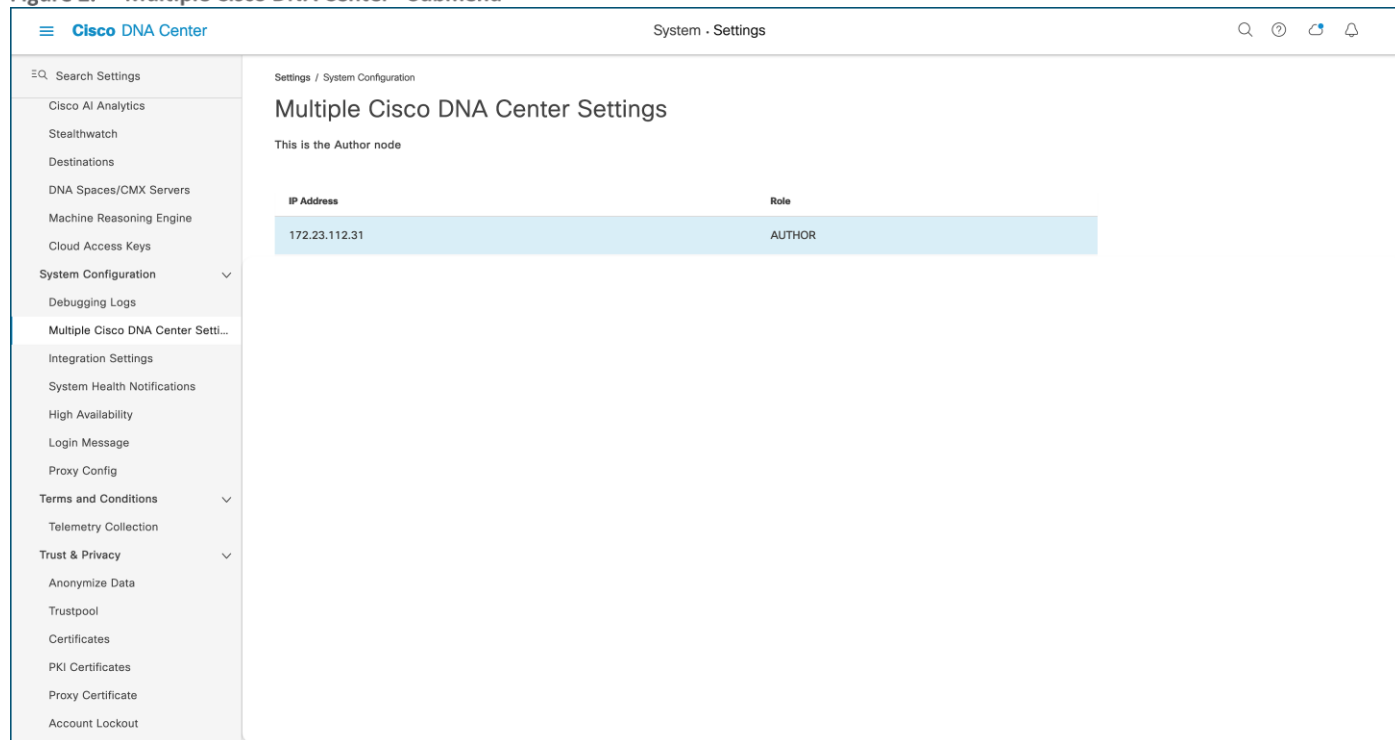
Accessing the Multiple Cisco DNA Center Cluster Software Package

The Multiple Cisco DNA Center functionality is not available as a General Availability feature. A Limited Availability package called *Multiple Cisco DNA Center* is available only to approved customers. To get access to this software package, please reach

out to your Cisco Sales representative or Channel Partner to do a High-Level Design review. Upon design review approval, the software package is released via the Cloud Catalog Server update, and the cluster administrator can download and install the package. For Air-Gapped environment, packages will be released in a separate method for the cluster administrator to download and install the respective package.

All Cisco DNA Center clusters that are integrated with the single Cisco ISE deployment must install this package. Once downloaded, the package installation process automatically restarts the applicable services in the cluster. This installation and service restart may take up to 10 minutes. Once the package is installed, a separate submenu is added under **≡ > System > Settings > System Configuration > Multiple Cisco DNA Center Settings**.

Figure 2. Multiple Cisco DNA Center - Submenu



Cisco Multiple DNA Center Considerations

- In Cisco DNA Center Releases 2.2.2.x and earlier, up to **THREE (3)** Reader Node clusters are supported. This is **FOUR (4)** clusters in total including the Author Node cluster.
- In Cisco DNA Center Release 2.2.3.x and later up to **FOUR (4)** Reader Node clusters are supported. This is **FIVE (5)** clusters in total including the Author Node cluster.
- Before adding Reader Node cluster, you must remove all user-defined Cisco SD-Access policy elements in order to integrate with Cisco ISE. These include any user-defined VNs, SGTs, Access Contracts, and GBAC Policy.
- Once the Multiple Cisco DNA Center Package is installed, the functionality is enabled in the cluster. Uninstalling the package does not disable the functionality nor removes “Establishing Multi DNA Center environment” step with ISE integration process.
- VNs, SGTs, Access Contracts, GBAC Policy, and VN-to-SGT Associations can only be managed on the Author Node cluster. Virtual Networks and SGTs are Read-Only on Reader Node clusters.
- The ability to designate a Virtual Network as a Guest VN is not supported. This limitation is removed if using Cisco DNA Center 2.2.3.x along with Cisco ISE 3.1.

- SGT to VN associations can only be managed on the Author Node cluster. These associations are available as Read-Only on Reader Node clusters.
- When a Cisco DNA Center cluster is upgraded, a new Multiple Cisco DNA Center package may be available. However, this package is not automatically available for download. Use the [earlier process](#) to receive access to newly available packages after upgrade.
- After cluster upgrade, the existing Multiple Cisco DNA Center functionality will continue. If upgrading from 1.3.3.x to 2.x.x.x, ensure that the newer package is installed to avoid seeing potential issues in Multiple Cisco DNA Center settings page. Additional fixes or capabilities are made available through the SD-Access, Access Control Application, and Cisco DNA Center UI packages. The standard cluster upgrade process should automatically download and install these packages. Please consult the [Cisco DNA Center Release Notes](#) for specific package version numbering for a given release.
- The user-defined pxGrid Subscriber name under **≡ > System > Settings > Authentication and Policy Servers** across all FIVE Cisco DNA Center must be unique. This is applicable only if you are running Cisco DNA Center versions 1.3.3.x and below. The Subscriber Name is auto-generated starting with Cisco DNA Center version 2.1.1.x and later.
- The ability to associate a vManage VPN to a Virtual Network is not supported. This limitation is removed if using Cisco DNA Center 2.2.3.x along with Cisco ISE 3.1.
- When promoting a Reader Node cluster to the Author Node role, the application names for specific Access Contracts found under **≡ > Policy > Group-Based Access Control > Access Contracts** are not populated. The application names are displayed as *Advanced*. TCP/UDP port numbers are populated. Please note, the behavior of the network is unchanged since these SGACLs in ISE have not changed. To populate the names, review all the Access Contracts after a promotion operation and edit them selecting the application name.

Multiple Cisco DNA Center to ISE Scale Information

Table 2. Multiple Cisco DNA Center VN and IP Pool Scale

Cisco DNA Center 1.3.3.x	ISE 2.4 Patch 14 and later
	ISE 2.6 Patch 8 and later
	ISE 2.7 Patch 3 and later
	ISE 3.0 Patch 2 and later
300 Virtual Networks	
1250 IP Pools (Total)	
Cisco DNA Center 1.3.3.x	ISE 2.4 Patch 13 and earlier
	ISE 2.6 Patch 7 and earlier
	ISE 2.7 Patch 2 and earlier
	ISE 3.0 Patch 1 and earlier
100 Virtual Networks	
600 IP Pools (Total)	

Table 3. Multiple Cisco DNA Center VN and VLAN Name Scale

Cisco DNA Center 2.1.1.x	ISE 2.4 Patch 14 and later
	ISE 2.6 Patch 8 and later
	ISE 2.7 Patch 3 and later
	ISE 3.0 Patch 2 and later
300 Virtual Networks	
1250 VLAN Names (Total)	

Cisco DNA Center 2.1.1.x	ISE 2.4 Patch 13 and earlier
	ISE 2.6 Patch 7 and earlier
	ISE 2.7 Patch 2 and earlier
	ISE 3.0 Patch 1 and earlier
100 Virtual Networks	
600 VLAN Names (Total)	

Tech tip

A VLAN Name is configured in the Fabric Site – Host Onboarding screen. The configuration allows an administrator to have a single VLAN Name (for use in authorization profiles and authorization policies in Cisco ISE) for multiple IP pools. A common use case is to have a single VLAN Name for a specific virtual network across all sites (where every site has one or more unique IP pools).

Multiple DNA Center Latency Requirements

The latency requirements for this feature are unchanged from the standard latency requirements. Please refer to the [SD-Access requirements](#) section on the Cisco DNA Center datasheet for latency information.

Cisco Multiple DNA Center Policy Management

Cisco DNA Center 1.3.1.x software release introduced the Access Control Application (ACA) package with which Scalable Group, Access Contracts and Group-Based Access Control Policy are available on the Cisco DNA Center user interface. Once Cisco DNA Center was integrated with Cisco ISE and Policy Migration was performed and synchronized, policy authoring privileges are handled within Cisco DNA Center and ISE becomes Read-Only.

Usually, the policy data on Cisco DNA Center and Cisco ISE is consistent, so no special handling or conversion of data is necessary. In case of minor discrepancies or inconsistencies or if there is a conflict, the data in Cisco ISE is given precedence, so as not to introduce changes in policy behavior in the network. For Conflict resolution and actions to take during migration, please see [Group-Based Access Control: Policy Data Migration and Synchronization](#) in the Cisco DNA Center user guide

To retain the policy (Scalable Groups, Access Contracts and Group-Based Access Control Policy) authoring function on Cisco ISE, either:

- Skip the Data migration and Synchronization step under **≡ > Policy > Group-Based Access Control > Policies**.
- Navigate to **≡ > Policy > Group-Based Access Control > Policies > GBAC Configuration**. and select Manage Group-Based Access Control in ISE, GBAC UI in Cisco DNA Center will be inactive and click Save if data migration is complete.

Cisco Multiple DNA Center Upgrade Recommendations

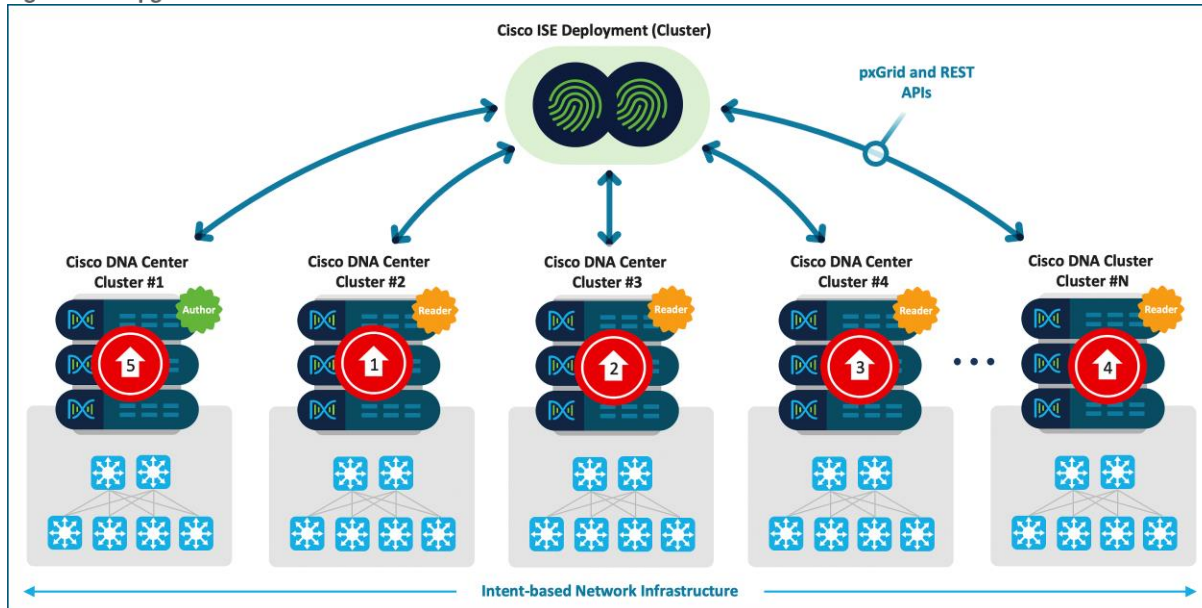
In a Cisco Multiple DNA Center environment, it's strongly recommended to run the **same Cisco DNA Center software version and packages across all Author and Reader Node clusters**. The exception to this is during the process of cluster upgrades.

Tech tip

Basic functionality of the Multiple DNA Center feature does not require the same software version of all the participating Author and Reader Node Cluster. However, using mismatched code versions will result in a difference in fixes, capabilities, and features between the clusters. The same Cisco DNA Center software version and packages is strongly recommended across all Author and Reader Node clusters.

Upgrade all Reader Node clusters first, and then upgrade the Author Node cluster to avoid feature disparity and feature incompatibility across versions. Avoid promotion of a Reader Node cluster to the Author Node role in the middle of an upgrade cycle. All Cisco DNA Center clusters should be upgraded and running the same version software version before promoting a Reader Node Cluster.

Figure 3. Upgrade Recommendations



Deploy

This section focuses on deployment guidelines with various workflows including the Multiple Cisco DNA Center Package installation and Policy Authoring.

There are two implementation options available when it comes for the Multiple Cisco DNA Center to ISE deployment

- A new deployment of multiple Cisco DNA Center clusters that are not currently integrated with ISE.
- An existing Cisco DNA Center cluster that is integrated with ISE and new DNA Center Clusters with or without Cisco ISE Integration.

This prescriptive deployment guide addressed the second option as the majority of customers start with Single Cisco DNA Center and add additional clusters.

Process 1: Request Package and Installation

The multiple Cisco DNA Center cluster functionality isn't currently available in the Cisco DNA Center software release for General Availability. A Limited Availability package (Multiple Cisco DNA Center) is available only to approved customers.

Procedure 1. Download/Install Multiple Cisco DNA Center Package

Step 1. Connect with your Cisco Sales Representative or Channel Partner for:

- High-Level Design review
- Multiple Cisco DNA Center Package release

Packages will be released to the Cisco DNA Center Cluster via Cloud catalog server update. Expect the packages to be available in 1 or 2 days.

Step 2. Navigate to  > **System** > **Software updates** to first download the package and install the package.

Tech tip

The package installation process automatically restarts affected services in Cisco DNA Center, which may take up to 10 minutes.

Step 3. To verify the Package installation, Navigate to  > **System** > **Software Updates** > **Installed Apps**.

Figure 4. Cisco DNA Center Installed Apps

Cisco DNA Center			System - Software Updates
	System Commons	2.1.363.60202	Uninstall
Automation			
	Application Hosting	1.6.0.2104291515	Uninstall
	Application Policy	2.1.363.170112	Uninstall
	Application Registry	2.1.363.170112	Uninstall
	Application Visibility Service	2.1.363.170112	Uninstall
	Cisco Umbrella	2.1.363.590048	Uninstall
	Cloud Device Provisioning Application	2.1.363.60202	Uninstall
	Command Runner	2.1.363.60202	Uninstall
	Device Onboarding	2.1.363.60202	Uninstall
	Image Management	2.1.363.60202	Uninstall
	SD Access	2.1.363.60202	Uninstall
	Stealthwatch Security Analytics	2.1.363.1090038	Uninstall
	Wide Area Bonjour	2.4.363.75002	Uninstall
Assurance			
	AI Network Analytics	2.6.7.436	Uninstall
	Assurance - Base	2.2.2.357	Uninstall
	Assurance - Sensor	2.2.2.346	Uninstall
	Automation - Intelligent Capture	2.1.363.60202	Uninstall
	Automation - Sensor	2.1.363.60202	Uninstall
	Machine Reasoning	2.1.363.210023	Uninstall
	Path Trace	2.1.363.60202	Uninstall
	Rogue And AWIPS	2.2.0.42	Uninstall
Policy Applications			
	Access Control Application	2.1.363.60202	Uninstall
	AI Endpoint Analytics	1.4.329	Uninstall
	Group-Based Policy Analytics	2.2.1.209	Uninstall
	Multiple Cisco DNA Center	2.1.360.60862	Uninstall

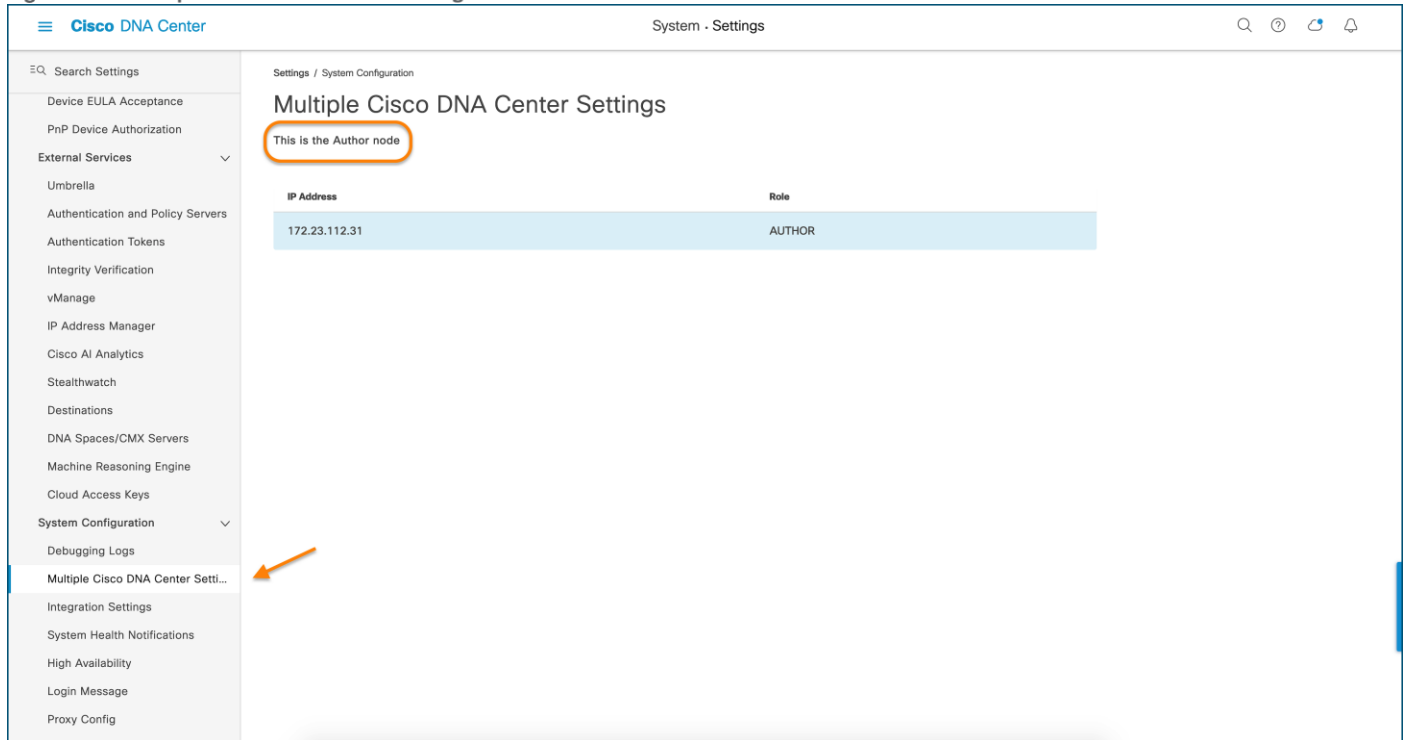
Tech tip

After the required information is provided, Cisco DNA Center retries the Integration process and integration status is shown on the side panel display. Packages highlighted in green are supporting applications required for Multiple Cisco DNAC Center feature to work. All Cisco DNA Center clusters that you intend to integrate into a single Cisco ISE deployment must install this package.

Step 4. Navigate to **System > Settings > System Configuration > Multiple Cisco DNA Center Settings** to verify the default role of the cluster

With the Multiple Cisco DNA Center Package installed, the cluster, by default, is shown as the Author Node cluster as shown in Figure 5 below. Upon integrating (first1st time) or reintegrating (already integrated without package) with Cisco ISE, role negotiation happens, and the first Cisco DNA Cluster will resume the role of Author Node cluster and subsequent Cisco DNA Cluster will become the role of Reader Node clusters.

Figure 5. Multiple Cisco DNA Center Settings



Process 2: Integrate Multiple Cisco DNA Center with Single Cisco ISE

Procedure 1. Integrate / Reintegrate Cisco DNA Center with Cisco ISE

For Greenfield deployments, prerequisites must be met on both Cisco DNA Center and ISE prior to the integration. Please refer to [Cisco DNA Center and Cisco ISE Integration section](#) in the Cisco DNA Center Administrator Guide for more information.

For Brownfield environments wherein Cisco DNA Center is already integrated with ISE, follow the steps below to reintegrate Cisco DNA Center and Cisco ISE using the Multiple Cisco DNA Center Package. This allows Cisco DNA Center to negotiate the Author or Reader Node cluster role based on if it the first cluster or subsequent cluster joining ISE with Multiple Cisco DNA Center Package.

Step 1. In Cisco DNA Center, navigate to **≡ > System > Settings > External Services > Authentication and Policy Servers**

Step 2. Hover over ... under the **Action** column and select **Edit** to reenter the Cisco ISE Super Admin password.

Tech tip

After the required information is provided, Cisco DNA Center retries the Integration process, and the integration status is shown on the side panel display.

Figure 6. Edit Authentication and Policy Servers

The screenshot shows the Cisco DNA Center interface for editing authentication and policy servers. The left sidebar contains a search bar and a list of settings categories. The main content area is titled 'Authentication and Policy Servers' and includes a table of configured servers. An arrow points to the 'Actions' column of the table, which contains 'Edit' and 'Delete' buttons.

IP Address	Protocol	Type	Status	Actions
172.25.73.223	RADIUS_TACACS	ISE	ACTIVE	...

Figure 7. Edit ISE Server Settings

The screenshot shows the 'Edit ISE server' configuration page in Cisco DNA Center. The page displays various fields for configuring the ISE server, including IP address, shared secret, username, password, FQDN, subscriber name, and virtual IP addresses. An arrow points to the 'Password' field, which is currently masked with dots.

IP Address	Protocol	Type
172.25.73.223	RADIUS_TACACS	ISE

Fields in the 'Edit ISE server' form:

- Server IP Address: 172.25.73.223
- Shared Secret: [Empty]
- Username: admin
- Password: [Masked]
- FQDN: ISE10-1.demo.local
- Subscriber Name: DNAC10
- Virtual IP Address(es): [Empty]
- Advanced Settings: [Toggle Off]

Figure 8. ISE Server Integration on Cisco DNA Center

The screenshot shows the Cisco DNA Center web interface. The main content area is titled 'Authentication and Policy Servers' and contains a table with the following data:

IP Address	Protocol	Type
172.25.73.223	RADIUS_TACACS	ISE

A side panel titled 'ISE server Integration' is open on the right. It displays a progress list with the following steps:

- Initiating connection...
Connecting to ISE and validating credentials
- Establishing trust...
Reading, validating, and storing trusted certificates
- Discovering nodes...
Discovering ISE primary and secondary admin nodes and pxGrid nodes
- Establishing Multi DNA Center environment...**
Joining Multi DNA Center Environment
- Connecting to pxGrid...
Loading and validating pxGrid certificates, subscribing to pxGrid topics

The fourth step, 'Establishing Multi DNA Center environment...', is highlighted with an orange circle. A success message at the top of the side panel states: 'Integration of Cisco ISE server 172.25.73.223 was successful. Visit System 360 to view health status.'

Tech tip

This is a five-step reintegration process, and the fourth step, which is circled above, is where Cisco DNA Center negotiates the Author/Reader Node role with ISE.

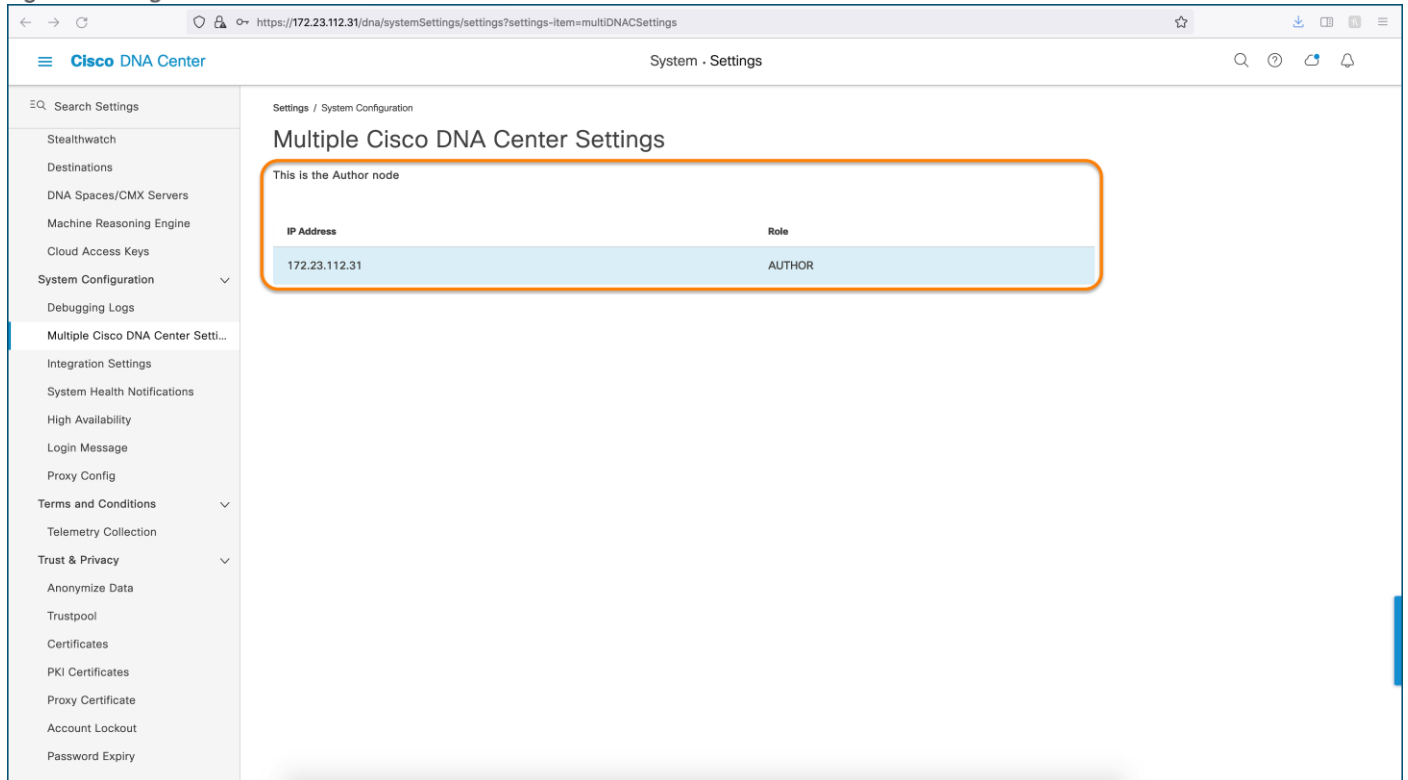
Step 3. Close the side panel and ensure the **Authentication and Policy Server** page shows **Status** as **ACTIVE**.

Tech tip

If the status of the configured Cisco ISE server is "FAILED" due to password change, click Retry, and update the password to resynchronize with ISE.

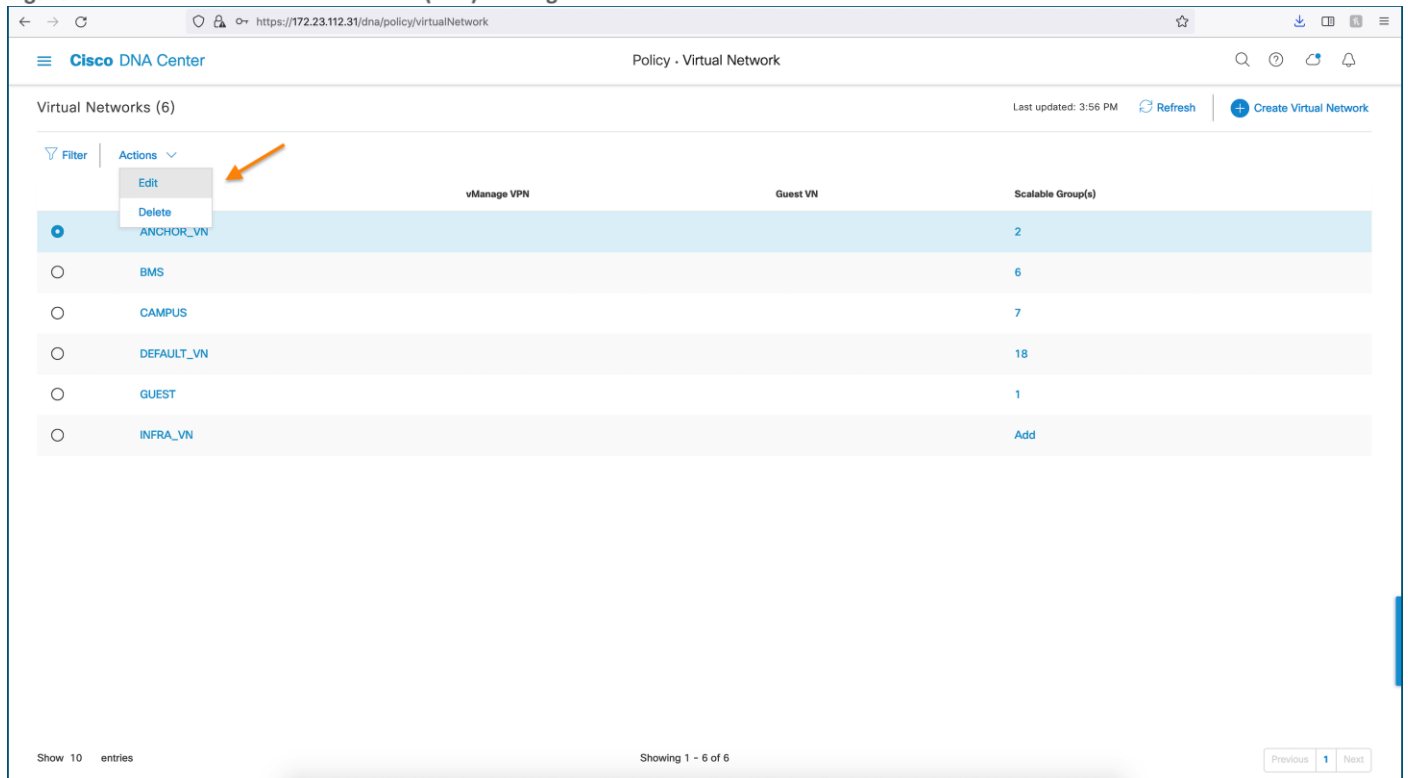
Step 4. Navigate to **≡ > System > Settings > System Configuration > Multiple Cisco DNA Center Settings** to verify the negotiated role of the cluster as Author Node.

Figure 9. Negotiated Author Role on Cisco DNA Center



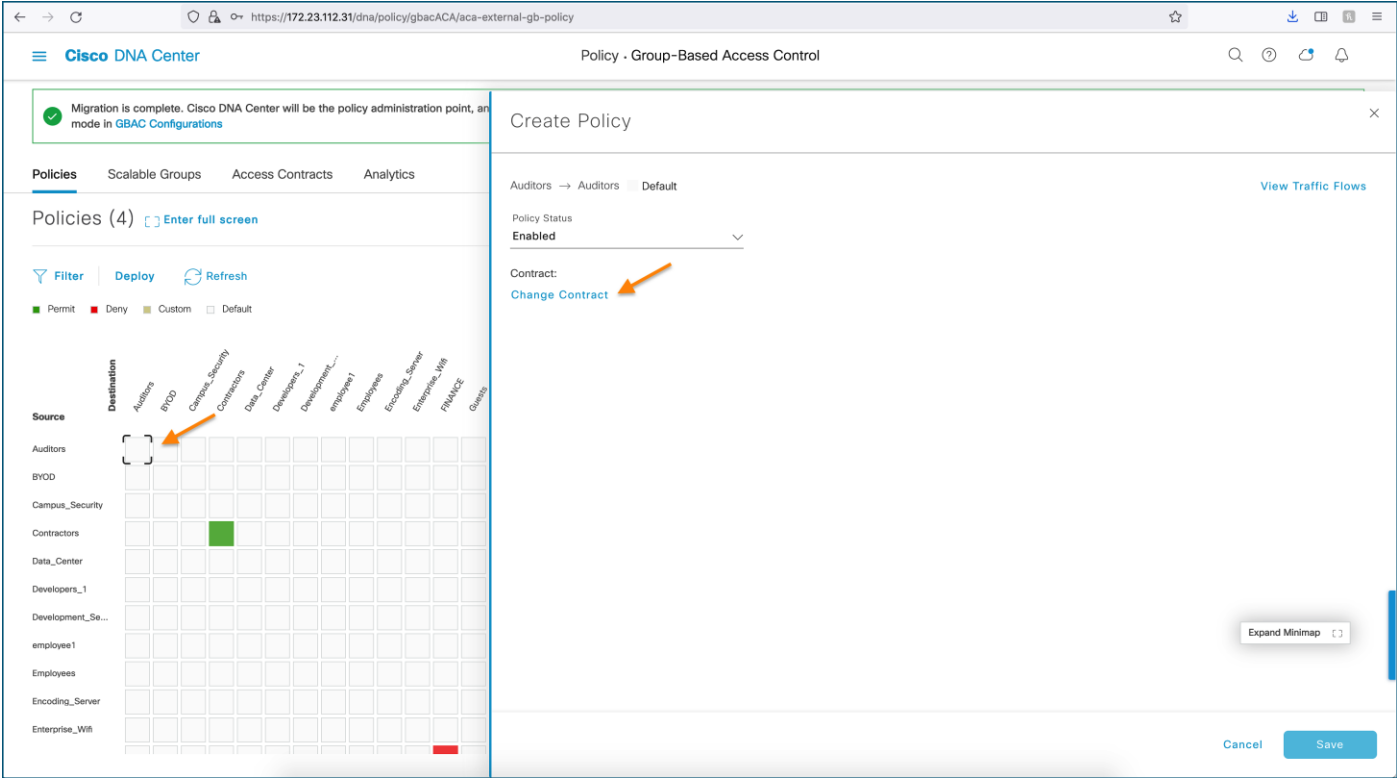
Step 5. Navigate to **Policy > Virtual Network** to confirm Read-Write (edit) privileges for Virtual Network.

Figure 10. Virtual Network Read-Write (Edit) Privileges on Author Node Cluster



Step 6. Navigate to **≡ > Policy > Group-Based Access Control > Policies** to view the Group-Based Access Control Policy Matrix and to confirm Read-Write (edit) privileges of the Matrix.

Figure 11. Group-Based Access Policy Read-Write (Edit) Privileges on Author Node Cluster



Step 7. Navigate to **≡ > Policy > Group-Based Access Control > Scalable Groups** to view the total number of Scalable Groups and to confirm Read-Write (edit) privileges.

Figure 12. Scalable Group Read-Write (Edit) Privileges on Author Node Cluster

The screenshot shows the Cisco DNA Center interface for Group-Based Access Control. A green banner at the top states: "Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations." Below this, the "Scalable Groups" tab is active. A table titled "Scalable Groups (29)" displays the following data:

Name	Tag Value	Description	Created in	Policies	Virtual Networks
Auditors	9/0x9	Auditor Scalable Group		0	DEFAULT_VN
BYOD	15/0xf	BYOD Security Group		0	DEFAULT_VN
Campus_Security	21/0x15	CS Group		0	BMS
Contractors	5/0x5	Contractor Security Group		2	ANCHOR_VN, DEFAULT_VN
Data_Center	27/0x1b			0	ANCHOR_VN, BMS, CAMPUS
Developers_1	8/0x8	Developer Scalable Group		0	DEFAULT_VN
Development_Servers	12/0xc	Development Servers Security Group		0	DEFAULT_VN
employee1	28/0x1c			0	DEFAULT_VN
Employees	4/0x4	Employee Security Group		0	DEFAULT_VN

At the bottom right of the table, there is a "Create Scalable Group" button, which is highlighted by an orange arrow. The interface also shows "0 Selected" and buttons for "Edit", "Delete", and "Deploy".

Procedure 2. Integrating other Cisco DNA Center Clusters with Cisco ISE as Reader Nodes

To integrate subsequent Cisco DNA Center clusters using the Multiple Cisco DNA Center Package to same Cisco ISE, the cluster must be in a Greenfield-state. This means that it cannot have:

- **Non-Default Virtual Networks**—Any Virtual Networks other than *DEFAULT_VN* and *INFRA_VN*.
- **Non-Default Scalable Groups**—Any Security Group other than those with a tag value 0 to 15(0xf)
- **Non default Virtual Network to Scalable Group mappings**— All 15 SGT will be mapped to *DEFAULT_VN*
- **Non-Default Scalable Groups (Security Groups)**

Each user-defined (non-default) constructs described above must be removed or Cisco DNA Center displays a banner, the connection is refused, and the integration does not complete.

Step 1. Verify the Package installation by navigating to **≡ > System > Software Updates > Installed App**

Figure 13. Multiple Cisco DNA Center Package

System - Software Updates			
Device Onboarding	2.1.363.60202	Uninstall	
Image Management	2.1.363.60202	Uninstall	
SD Access	2.1.363.60202	Uninstall	
Stealthwatch Security Analytics	2.1.363.1090038	Uninstall	
Wide Area Bonjour	2.4.363.75002	Uninstall	
Assurance			
AI Network Analytics	2.6.7.436	Uninstall	
Assurance - Base	2.2.2.357	Uninstall	
Assurance - Sensor	2.2.2.346	Uninstall	
Automation - Intelligent Capture	2.1.363.60202	Uninstall	
Automation - Sensor	2.1.363.60202	Uninstall	
Machine Reasoning	2.1.363.210023	Uninstall	
Path Trace	2.1.363.60202	Uninstall	
Rogue And AWIPS	2.2.0.42	Uninstall	
Policy Applications			
Access Control Application	2.1.363.60202	Uninstall	
AI Endpoint Analytics	1.4.329	Uninstall	
Group-Based Policy Analytics	2.2.1.209	Uninstall	
Multiple Cisco DNA Center	2.1.360.60862	Uninstall	
DNA Center Core			
Cisco DNA Center Global Search	1.5.0.362	Uninstall	
Cisco DNA Center UI	1.6.2.349	Uninstall	
Cloud Connectivity - Contextual Content	1.3.1.307	Uninstall	
Network Data Platform - Base Analytics	1.6.1016	Uninstall	
Network Data Platform - Core	1.6.576	Uninstall	
Network Data Platform - Manager	1.6.539	Uninstall	
Programmability And Integrations			

Step 2. Navigate to **Policy > Virtual Network** to verify cluster includes only the default Virtual network.

Figure 14. Default Virtual Network Verification on Reader Node Cluster

Identity Services Engine (ISE) is not integrated or is currently unavailable. All the ISE dependent operations are not available.

Virtual Networks (2) Last updated: 5:29 PM [Refresh](#) [Create Virtual Network](#)

Name	vManage VPN	Guest VN	Scalable Group(s)
DEFAULT_VN			15
INFRA_VN			Add

Showing 1 - 2 of 2

Step 3. Navigate to **Policy > Group-Based Access Control** to verify that there are no user-defined policies.

Figure 15. User-Defined Policy Verification on Reader Node Cluster

Identity Services Engine (ISE) has not been integrated, or is currently not available. Integrate ISE (2.4.0.357 Patch(es) 11 or 2.6.0.156 Patch(es) 3 or 2.7.0.356 Patch(es) 1 or above) to Cisco DNA Center in [Authentication and Policy Servers settings](#). You have to come back and enable synchronization so that Cisco DNA Center could distribute policies in ISE.

Policies (0) [Enter full screen](#) [GBAC Configuration](#) Default: Permit IP [Create Policies](#) [Create View](#)

[Filter](#) [Deploy](#) [Refresh](#)

■ Permit ■ Deny ■ Custom ■ Default

Source	Destination
Auditors	Auditors
BYOD	BYOD
Contractors	Contractors
Developers_1	Developers_1
Development_Se...	Development_Se...
Employees	Employees
Guests	Guests
Network_Services	Network_Services
PCI_Servers	PCI_Servers
Point_of_Sale_S...	Point_of_Sale_S...
Production_Serv...	Production_Serv...

[Expand Minimap](#)

Step 4. Navigate to **Policy > Scalable Groups** to verify non-user-defined Scalable Groups.

Figure 16. Default Scalable Groups on Reader Node Cluster

Identity Services Engine (ISE) has not been integrated, or is currently not available. Integrate ISE (2.4.0.357 Patch(es) 11 or 2.6.0.156 Patch(es) 3 or 2.7.0.356 Patch(es) 1 or above) to Cisco DNA Center in [Authentication and Policy Servers settings](#). You have to come back and enable synchronization so that Cisco DNA Center could distribute policies in ISE.

Scalable Groups (15) [Create Scalable Group](#)

[Search Table](#)

0 Selected [Edit](#) [Delete](#) [Deploy](#)

<input type="checkbox"/>	Name	Tag Value	Description	Created in	Policies	Virtual Networks
<input type="checkbox"/>	Auditors	9/0x9	Auditor Scalable Group		0	DEFAULT_VN
<input type="checkbox"/>	BYOD	15/0xf	BYOD Security Group		0	DEFAULT_VN
<input type="checkbox"/>	Contractors	5/0x5	Contractor Security Group		0	DEFAULT_VN
<input type="checkbox"/>	Development_Servers	12/0xc	Development Servers Security Group		0	DEFAULT_VN
<input type="checkbox"/>	Employees	4/0x4	Employee Security Group		0	DEFAULT_VN
<input type="checkbox"/>	Guests	6/0x6	Guest Security Group		0	DEFAULT_VN
<input type="checkbox"/>	Network_Services	3/0x3	Network Services Scalable Group		0	DEFAULT_VN
<input type="checkbox"/>	PCI_Servers	14/0xe	PCI Servers Scalable Group		0	DEFAULT_VN
<input type="checkbox"/>	Point_of_Sale_Systems	10/0xa	Point of Sale Scalable Group		0	DEFAULT_VN

15 Records Show Records: 10 1 - 10 < 1 2 >

Step 5. In the Cisco DNAC Center GUI, Click the Menu icon **≡ > System > Settings> External Services> Authentication and Policy Servers**,

Step 6. Click **Add**.

Step 7. Select **ISE**.

Step 8. Configure the Primary AAA Server by providing the following information:

- **Server IP address:** Primary PAN IP Address
- **Shared Secret:** Key for device authentications
- **Username:** Name that is used to login to the Cisco ISE CLI/GUI (Must be Super Admin)
- **Password:** Password for the Cisco ISE CLI/GUI username
- **FQDN:** Fully qualified domain name (FQDN) of the Cisco ISE Server
- **Virtual IP Address**[optional]: Virtual IP address of the load balancer
- **Toggle Advanced Settings button and configure Protocol: TACACS and RADIUS**

Step 9. Click **Add**.

Figure 17. Cisco ISE Integration on Reader Node Cluster

The screenshot displays the 'Add ISE server' configuration window in the Cisco DNA Center. The window is titled 'Add ISE server' and has a close button (X) in the top right corner. The main content area contains the following fields and options:

- Server IP Address***: 172.25.73.223
- Shared Secret***: A text field with a 'SHOW' button to the right.
- Username***: admin
- Password***: A text field with a 'SHOW' button to the right.
- FQDN***: ISE10-1.demo.local
- Virtual IP Address(es)**: A text field with a dropdown arrow and an 'Info' link.
- Advanced Settings**: A toggle switch that is currently turned off.
- Connect to pxGrid**: A checkbox that is currently checked.
- Protocol**: Two radio buttons, 'RADIUS' and 'TACACS', both of which are selected.
- Buttons**: 'Cancel' and 'Add' buttons at the bottom right. The 'Add' button is highlighted with an orange box.

The background shows the 'Authentication and Policy Servers' section of the Cisco DNA Center settings, with a table that currently displays 'No data to display'.

Step 10. In the side panel, due to first-time Integration, click on the **ACCEPT** button for Cisco DNA Center to accept the Certificate pushed by Cisco ISE.

Figure 18. Certificate Acceptance for ISE Server Integration

The screenshot shows the Cisco DNA Center interface. On the left is a sidebar with a search bar and a list of settings categories. The main content area is titled 'System - Settings' and 'Authentication and Policy Servers'. It includes a table with one entry for IP Address 172.25.73.223, Protocol RADIUS_TACACS, and Type ISE. On the right, a modal dialog titled 'ISE server Integration' is open. It contains a warning message about certificate trust and a list of integration steps: Initiating connection..., Establishing trust..., Discovering nodes..., Establishing Multi DNA Center environment..., and Connecting to pxGrid... The 'Initiating connection...' step is highlighted with an orange box, showing a certificate acceptance prompt with 'Accept' and 'Decline' buttons.

Search Settings

SSM Connection Mode

Device Settings

Device Controllability

Network Resync Interval

SNMP

ICMP Ping

Image Distribution Servers

Device EULA Acceptance

PnP Device Authorization

External Services

Umbrella

Authentication and Policy Servers

Authentication Tokens

Integrity Verification

vManage

IP Address Manager

Cisco AI Analytics

Stealthwatch

Destinations

DNA Spaces/CMX Servers

Machine Reasoning Engine

Cloud Access Keys

System Configuration

Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

IP Address	Protocol	Type
172.25.73.223	RADIUS_TACACS	ISE

ISE server Integration

This is the first time DNAC has seen this certificate from ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?

Integration of 172.25.73.223 is waiting for user input

Initiating connection...
a few seconds ago

This is the first time DNAC has seen this certificate from ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?
[View certificate](#)

[Accept](#) [Decline](#)

Establishing trust...
Reading, validating, and storing trusted certificates

Discovering nodes...
Discovering ISE primary and secondary admin nodes and pxGrid nodes

Establishing Multi DNA Center environment...
Joining Multi DNA Center Environment

Connecting to pxGrid...
Loading and validating pxGrid certificates, subscribing to pxGrid topics

[Close](#)

Tech tip

To automatically approve pxGrid client within ISE:

- Navigate to **Administration > pxGrid Services > Settings**.
- Click the checkbox next to ☒ Automatically approve new certificate-based accounts.
- Click **Save**.

To manually approve a pxGrid Client within ISE:

- Navigate to **Administration > pxGrid Services > All Clients**.
- Click **Total Pending Approval(x)**.
- Click **Approve All**.

Figure 19. ISE Server Integration - Five Step Process

← → ↻

https://172.23.112.41/dna/systemSettings/settings?settings-item=authenticationPolicy

☆

⬇

📄

☰

Cisco DNA Center

System · Settings

🔍 Search Settings

Cisco Accounts

▼

PnP Connect

Cisco.com Credentials

Smart Account

Smart Licensing

SSM Connection Mode

Device Settings

▼

Device Controllability

Network Resync Interval

SNMP

ICMP Ping

Image Distribution Servers

Device EULA Acceptance

PnP Device Authorization

External Services

▼

Umbrella

Authentication and Policy Servers

Authentication Tokens

Integrity Verification

vManage

IP Address Manager

Cisco AI Analytics

Stealthwatch

Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

⊕ Add ▼

📄 Export

IP Address	Protocol	Type
172.25.73.223	RADIUS_TACACS	ISE

ISE server Integration

⚠️ Joining existing Multiple Cisco DNA Center environment as Reader node.

✅ Integration of Cisco ISE server 172.25.73.223 was successful. Visit [System 360](#) to view health status.

✅ Initiating connection...
Connecting to ISE and validating credentials

✅ Establishing trust...
Reading, validating, and storing trusted certificates

✅ Discovering nodes...
Discovering ISE primary and secondary admin nodes and pxGrid nodes

✅ Establishing Multi DNA Center environment...
Joining Multi DNA Center Environment

✅ Connecting to pxGrid...
Loading and validating pxGrid certificates, subscribing to pxGrid topics

Close

Tech tip

This is a five-step reintegration process, and the fourth step, which is circled above, is where Cisco DNA Center negotiates the Author/Reader Node role with ISE.

Step 11. Close the Side Panel window and make sure the **Authentication and Policy Server** page shows **Status** as **ACTIVE**.

Figure 20. ISE Server Integration Status on Reader Node Cluster

The screenshot shows the Cisco DNA Center interface. The left sidebar contains a search bar and a list of settings categories. The main content area is titled 'Authentication and Policy Servers' and includes a table of configured servers. An orange arrow points to the 'ACTIVE' status of the first server entry.

IP Address	Protocol	Type	Status	Actions
172.25.73.223	RADIUS_TACACS	ISE	ACTIVE	...

Step 12. Navigate to **System > Settings > System Configuration > Multiple Cisco DNA Center Settings** to verify the Reader & Author Role.

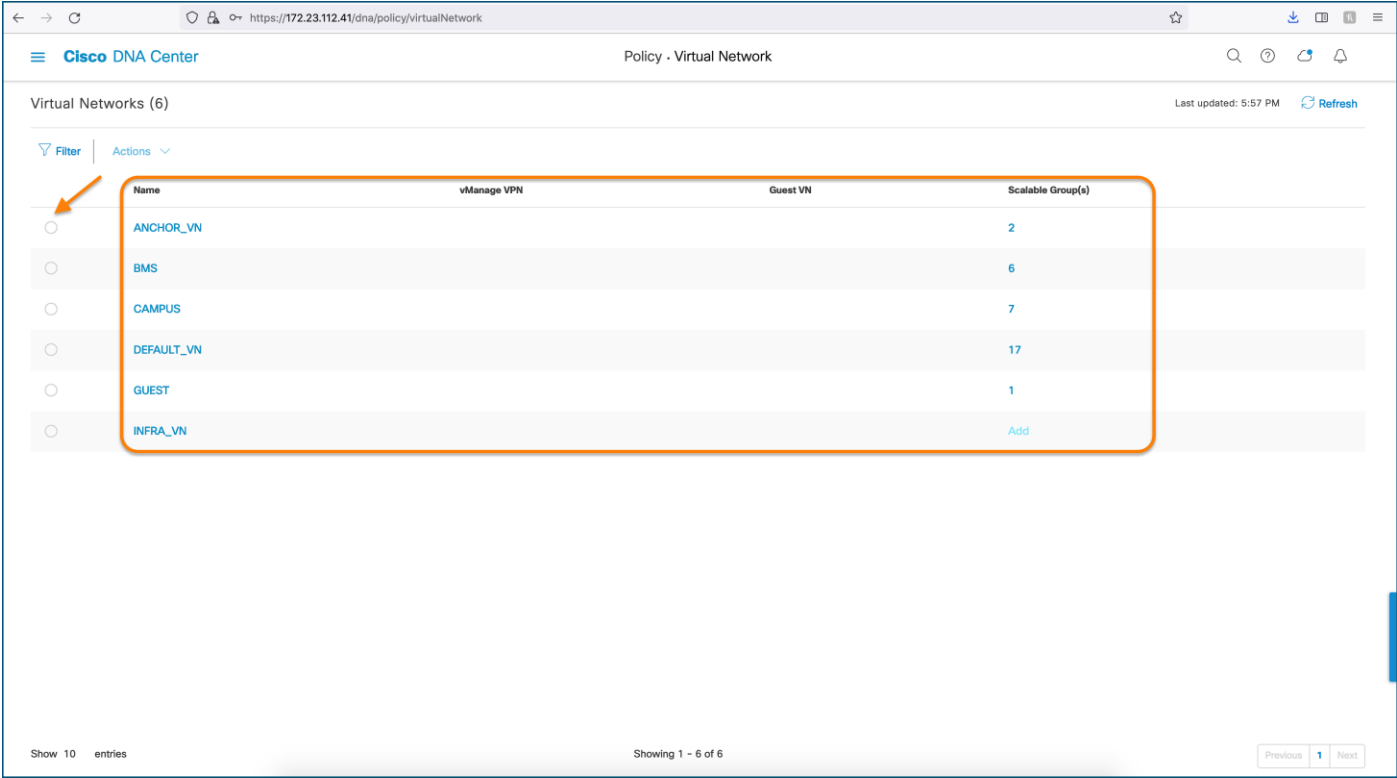
Figure 21. Multiple Cisco DNA Center Setting page on Reader Node Cluster

The screenshot shows the Cisco DNA Center interface for the 'Multiple Cisco DNA Center Settings' page. The left sidebar contains a search bar and a list of settings categories. The main content area is titled 'Multiple Cisco DNA Center Settings' and includes a table of configured nodes. An orange arrow points to the 'Promote to Author' button.

IP Address	Role
172.23.112.41	READER
172.23.112.31	AUTHOR

Step 13. Navigate to **Policy > Virtual Network** to confirm Virtual Networks have been synchronized from Author Node cluster and that privileges are Read-Only. This is shown in the figure below by the grey-out option to select the Virtual Network.

Figure 22. Virtual Network Read-Only privileges on Reader Node Cluster



Virtual Networks (6) Last updated: 5:57 PM [Refresh](#)

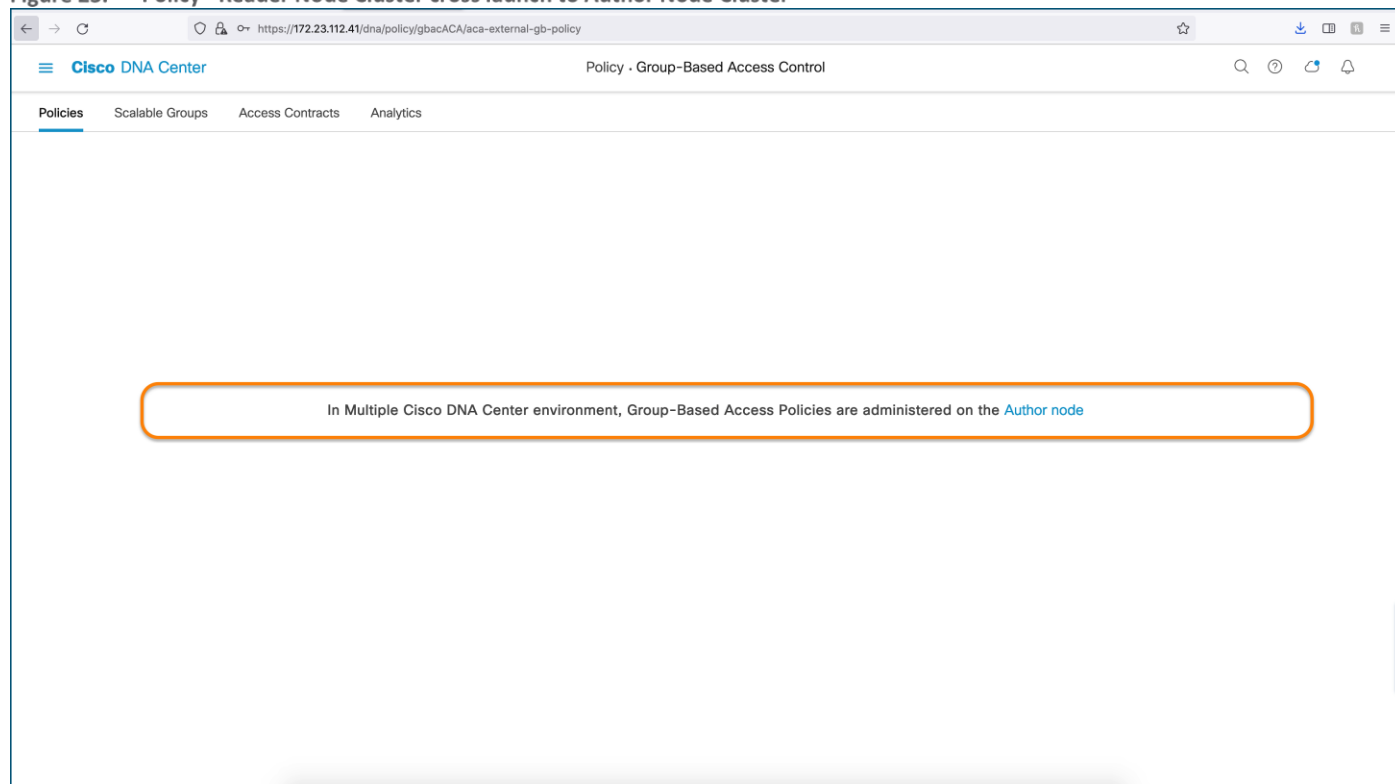
[Filter](#) [Actions](#)

	Name	vManage VPN	Guest VN	Scalable Group(s)
<input type="radio"/>	ANCHOR_VN			2
<input type="radio"/>	BMS			6
<input type="radio"/>	CAMPUS			7
<input type="radio"/>	DEFAULT_VN			17
<input type="radio"/>	GUEST			1
<input type="radio"/>	INFRA_VN			Add

Show 10 entries Showing 1 - 6 of 6 Previous 1 Next

Step 14. Navigate to **Policy > Group-Based Access Control > Policies** to confirm the Reader Node cluster has a hyperlink to cross-launch to the Author Node cluster for Policy-Information authoring as shown in Figure 23.

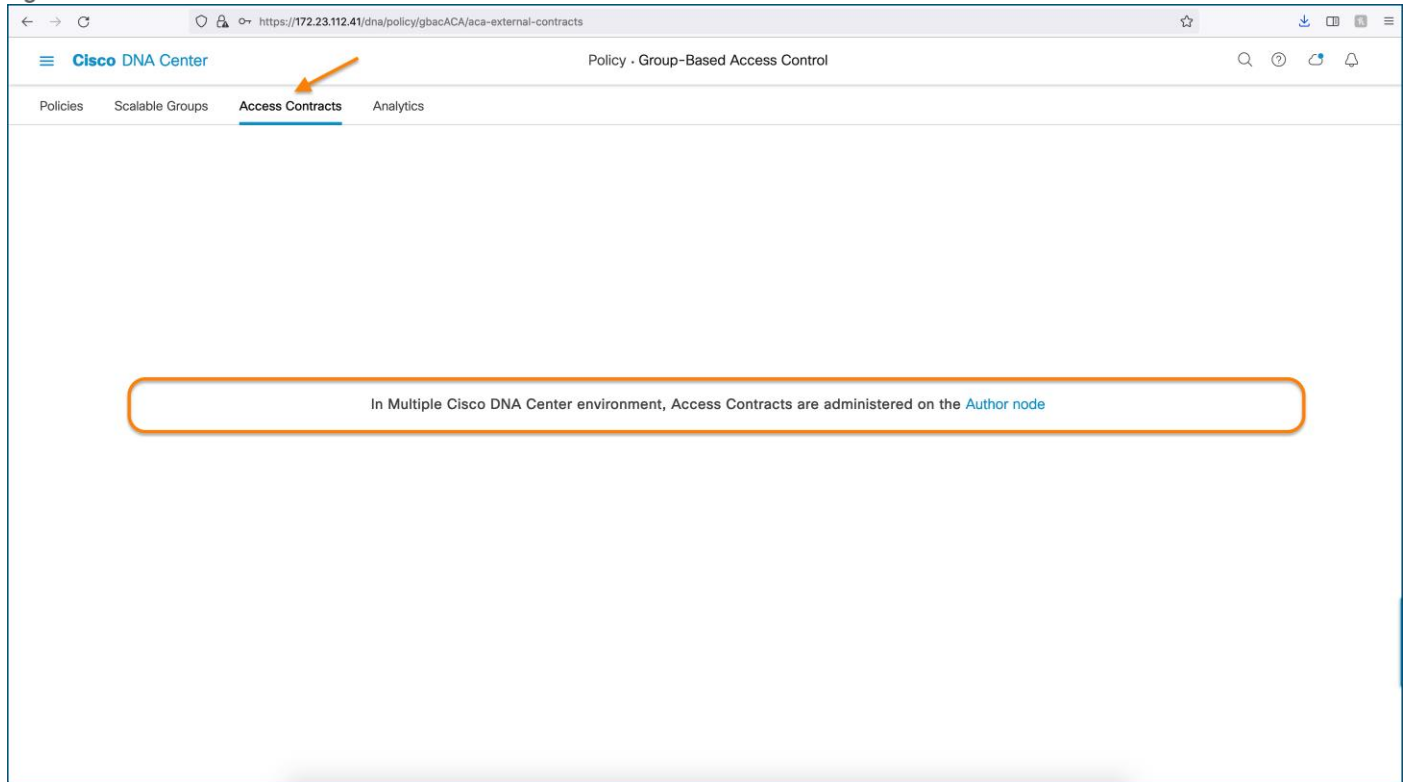
Figure 23. Policy - Reader Node Cluster cross launch to Author Node Cluster



Step 15. Navigate to **Policy > Group-Based Access Control > Scalable Groups** to confirm Scalable Groups synchronized from the Author Node cluster and that privileges are Read-Only.

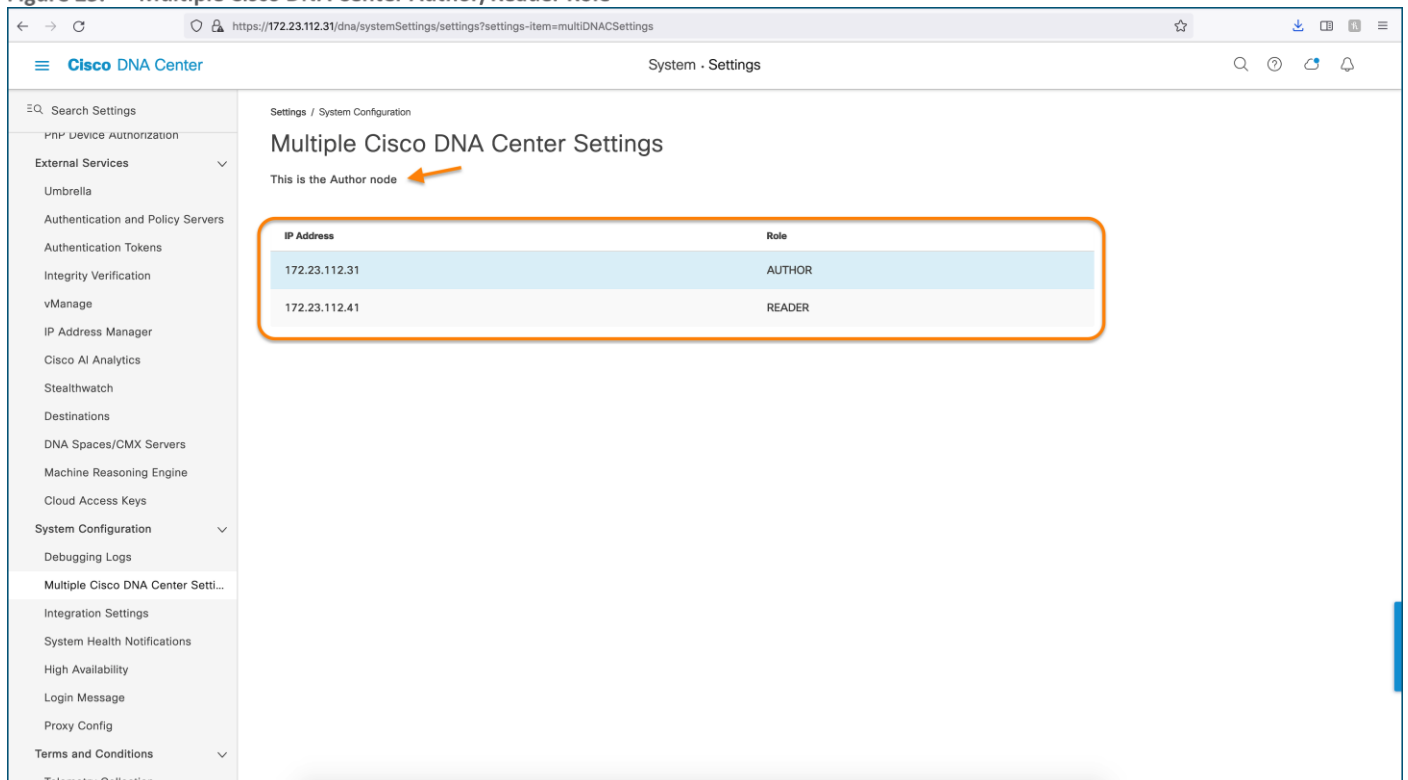
Step 16. Navigate to **Policy > Group-Based Access Control > Access Contracts** to confirm the Reader Node cluster has a hyperlink to cross-launch to the Author Node cluster for Access-Contract authoring as shown in Figure 24.

Figure 24. Access Contract - Reader Node Cluster cross launch to Author Node Cluster



Step 17. On the Author Node cluster, navigate to **System > Settings > System Configuration > Multiple Cisco DNA Center Settings** to verify the Author Node and Reader Node roles.

Figure 25. Multiple Cisco DNA Center Author/Reader Role



Procedure 3. Configuring Virtual Networks

Configuring, modifying, or deleting Scalable Groups, Access Contracts, Group-Based Access Control Policies, and Virtual Networks is only possible on the Author Node cluster.

Perform the below steps to first create Virtual Network

Step 1. In the Cisco DNA Center GUI, navigate to **Policy > Virtual Network**.

Step 2. Click **Create Virtual Network**, and the *Create Virtual Network* slide-in pane appears.

Step 3. In the **Name** field, enter the name of the Virtual Network.

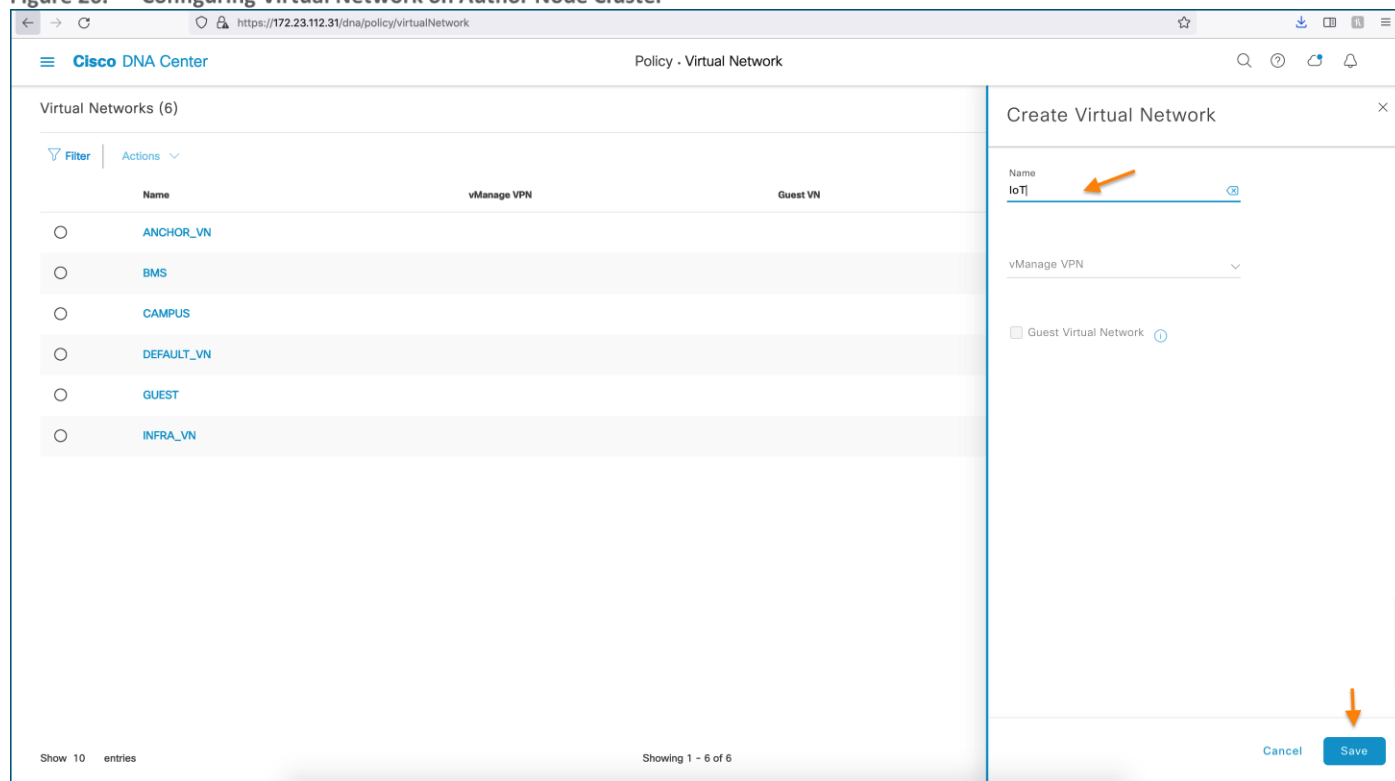
Step 4. [Optional] Select the ☒ Guest Virtual Network check box to configure the virtual network as a guest network.

Tech tip

If using Cisco DNA Center release 2.2.3.x along with ISE 3.1, the Guest Virtual Network attribute, which is enabled by selecting the ☒ Guest Virtual Network, is shared to Reader Node clusters. In any other combination of Cisco DNA Center release along with ISE release, the ability to designate a Virtual Network as a Guest VN is not supported.

Step 5. Click **Save**.

Figure 26. Configuring Virtual Network on Author Node Cluster



Step 6. On the Author Node clusters, navigate to **Policy > Virtual Network** to verify the Virtual Network creation and Read-Write privileges as show in Figure 27 below. Note that the radio buttons are **not** greyed out.

Figure 27. Virtual Network on Author Node Cluster with Read-Write Privileges

The screenshot shows the Cisco DNA Center interface for managing Virtual Networks. The page title is "Policy - Virtual Network". It displays a list of 7 Virtual Networks. The "IoT" row is highlighted with an orange border. The interface includes a "Filter" button, an "Actions" dropdown, and a "Create Virtual Network" button. The table has columns for Name, vManage VPN, Guest VN, and Scalable Group(s).

	Name	vManage VPN	Guest VN	Scalable Group(s)
<input type="radio"/>	ANCHOR_VN			2
<input type="radio"/>	BMS			6
<input type="radio"/>	CAMPUS			7
<input type="radio"/>	DEFAULT_VN			18
<input type="radio"/>	GUEST			1
<input type="radio"/>	INFRA_VN			Add
<input type="radio"/>	IoT			Add

Virtual Networks (7) Last updated: 4:06 PM Refresh Create Virtual Network

Filter Actions

Show 10 entries Showing 1 - 7 of 7 Previous 1 Next

Step 7. On the Reader Node clusters, navigate to **Policy > Virtual Network** to verify the Virtual Network creation and Read-Only privileges as show in Figure 28 below. Note that the radio buttons are greyed out.

Figure 28. Virtual Network on Reader Node Cluster with Read-Only Privileges

The screenshot shows the Cisco DNA Center interface for managing Virtual Networks with Read-Only privileges. The page title is "Policy - Virtual Network". It displays a list of 7 Virtual Networks. The "IoT" row is highlighted with an orange border. The interface includes a "Filter" button, an "Actions" dropdown, and a "Refresh" button. The table has columns for Name, vManage VPN, Guest VN, and Scalable Group(s).

	Name	vManage VPN	Guest VN	Scalable Group(s)
<input type="radio"/>	ANCHOR_VN			2
<input type="radio"/>	BMS			6
<input type="radio"/>	CAMPUS			7
<input type="radio"/>	DEFAULT_VN			17
<input type="radio"/>	GUEST			1
<input type="radio"/>	INFRA_VN			Add
<input type="radio"/>	IoT			Add

Virtual Networks (7) Last updated: 8:57 AM Refresh

Filter Actions

Show 10 entries Showing 1 - 7 of 7 Previous 1 Next

Procedure 4. Deleting a Virtual Network

Deleting a Virtual Network (VN) on the Author Node cluster requires prerequisite actions as the Author Node cluster is not aware of the VN usage on Reader Node clusters.


- All references to a VN on all the Reader Node clusters must be removed before attempting to delete that VN on the Author Node cluster.
- If a VN is deleted on the Author Node cluster, the VN is deleted on the Author Node cluster and the Reader Node clusters no longer have a reference to it.
- If a Reader Node cluster is using that VN, that VN displays as **out of sync with Author**.

In this occurs, perform the steps below to synchronize the Reader Node cluster with the Author Node cluster.

Step 1. Remove all the references of Virtual Network on the Reader Node cluster.

Step 2. Perform one of the actions below to resync:

On Author Node, navigate to  > **Policy > Group-Based Access Control > Policies > GBAC Configuration** and click **Re-sync policy data now**.

On the Reader Node cluster, navigate to  > **System > Settings > External Services > Authentication and Policy Servers** and re-enter the ISE Super Admin Password to perform a resynchronization with ISE.

Procedure 5. Configure Scalable Groups and associate a Scalable Group to Virtual Network

Perform the below steps to create Scalable Groups and associate a Scalable Group to Virtual Network on the **Author Node** cluster.

Step 1. In the Cisco DNA Center, navigate to  > **Policy > Group-Based Access Control > Scalable Groups**

Step 2. Click **Create Scalable Group**, the **Create Scalable Group** slide-in pane appears.

Step 3. In the Create Scalable Group slide-in panel, enter a name and description for the Scalable Group.

Step 4. Remove the DEFAULT_VN Virtual Network by clicking the **X** symbol next to the name.

Step 5. From the drop-down, select the respective Virtual Network (e.g., IoT).

Figure 29. Scalable Group creation and SGT-VN Mapping

The screenshot displays the Cisco DNA Center interface for creating a Scalable Group. The main window shows a table of existing Scalable Groups with columns for Name, Tag Value, Description, and Created In. A modal dialog titled 'Create Scalable Group' is open on the right. The dialog contains the following fields and options:

- Name***: Mobile_Robot (indicated by an orange arrow)
- Tag Value (decimal)***: 29
- Description (optional)**: Empty text box
- Virtual Networks***: IoT (indicated by an orange arrow)
- Propagate to ACI**: Unchecked checkbox
- Buttons**: Cancel and Save (indicated by an orange arrow)

The background table lists the following Scalable Groups:

Name	Tag Value	Description	Created In
Auditors	9/0x9	Auditor Scalable Group	0
BYOD	15/0xf	BYOD Security Group	0
Campus_Security	21/0x15	CS Group	0
Contractors	5/0x5	Contractor Security Group	2
Data_Center	27/0x1b		0
Developers_1	8/0x8	Developer Scalable Group	0
Development_Servers	12/0xc	Development Servers Security Group	0
employee1	28/0x1c		0
Employees	4/0x4	Employee Security Group	0

Step 6. Click **Save**.

The Scalable Groups window displays the Scalable Group name, tag value, assigned Virtual Networks and associated policies.

Step 7. At the bottom right of the page, choose (**Show Records**) to show 25, 50, or 100 records per page to view all records.

An orange triangle icon is displayed next to the Scalable Group if synchronization with Cisco ISE is incomplete.

Step 8. To manually sync, Locate the name of Scalable Group as entered in [Step 3](#) and select the Scalable Group by checking the checkbox next to the name of the Scalable Group

Step 9. Click **Deploy** for Cisco DNA Center pushes the information to Cisco ISE via Rest API.

Tech tip

Once Deployed, the *Sync not started / Sync in progress* triangle will be removed.

Figure 30. Scalable Group Synchronization with ISE

The screenshot shows the Cisco DNA Center interface for Group-Based Access Control. A notification at the top states: "Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations".

The main section is titled "Scalable Groups (30)". It includes a search bar and a table of Scalable Groups. The table has columns: Name, Tag Value, Description, Created in, Policies, and Virtual Networks. The table lists 10 groups, including HVAC, Information_Technology, Lighting_Control, Mobile_Robot, Network_Services, PCI_Servers, Phone, Point_of_Sale_Systems, and Printer. An orange arrow points to the "Deploy" button above the table. Another orange arrow points to the "Show Records: 100" dropdown at the bottom right of the table.

Name	Tag Value	Description	Created in	Policies	Virtual Networks
HVAC	22/0x16	HV Group		0	BMS
Information_Technology	16/0x10	IT Group		0	DEFAULT_VN
Lighting_Control	23/0x17	LC Group		0	BMS
Mobile_Robot	29/0x1d			0	IoT
Network_Services	3/0x3	Network Services Scalable Group		1	DEFAULT_VN
PCI_Servers	14/0xe	PCI Servers Scalable Group		0	DEFAULT_VN
Phone	19/0x13			0	CAMPUS
Point_of_Sale_Systems	10/0xa	Point of Sale Scalable Group		0	DEFAULT_VN
Printer	17/0x11	Printer Group		0	CAMPUS

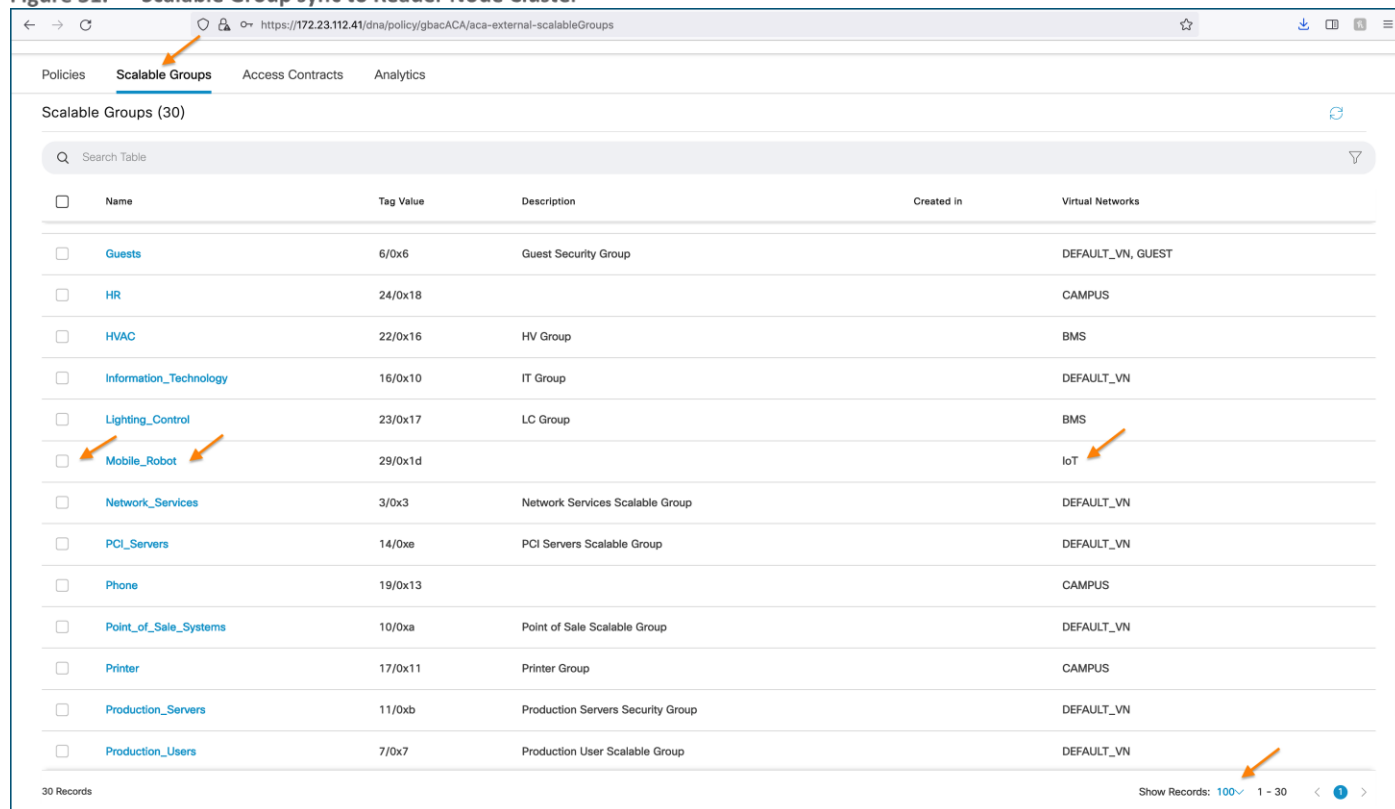
30 Records

Show Records: 100 1 - 30

Step 10. On a Reader Node cluster, navigate to **Policy > Group-Based Access Control > Scalable Groups** to verify the Scalable Group creation and association of a Scalable Group to Virtual Network.

Step 11. To show more than 10 records per page, click **Show Records** and select 10, 25, 50, or 100 to see the selected number of Scalable Groups per page as shown in Figure 31.

Figure 31. Scalable Group sync to Reader Node Cluster



Scalable Groups (30)

Name	Tag Value	Description	Created in	Virtual Networks
Guests	6/0x6	Guest Security Group		DEFAULT_VN, GUEST
HR	24/0x18			CAMPUS
HVAC	22/0x16	HV Group		BMS
Information_Technology	16/0x10	IT Group		DEFAULT_VN
Lighting_Control	23/0x17	LC Group		BMS
Mobile_Robot	29/0x1d			IoT
Network_Services	3/0x3	Network Services Scalable Group		DEFAULT_VN
PCI_Servers	14/0xe	PCI Servers Scalable Group		DEFAULT_VN
Phone	19/0x13			CAMPUS
Point_of_Sale_Systems	10/0xa	Point of Sale Scalable Group		DEFAULT_VN
Printer	17/0x11	Printer Group		CAMPUS
Production_Servers	11/0xb	Production Servers Security Group		DEFAULT_VN
Production_Users	7/0x7	Production User Scalable Group		DEFAULT_VN

30 Records

Show Records: 100 1 - 30

Procedure 6. Deleting a Scalable Group

Deleting a Scalable Group on the Author Node cluster requires prerequisite actions. The Author Node cluster is not aware of Scalable Group usage on a Reader Node cluster. You must remove all references to the security group on all the Reader Node clusters before attempting to delete that security group on the Author Node cluster. If you delete a security group on the Author Node cluster, that security group is deleted on the Author Node cluster, Cisco ISE and on the Reader Node cluster if there are no references to it. If one of the Reader Node clusters is using that Security Group, that security group displays as *out of sync with Author*.

Figure 32. Scalable Group Out of Sync with Author Node Cluster

Name	Tag Value	Description	Created in	Virtual Networks
PCI_Servers	14/0xe	PCI Servers Scalable Group		DEFAULT_VN
Phone	19/0x13			CAMPUS
Point_of_Sale_Systems	10/0xa	Point of Sale Scalable Group		DEFAULT_VN
Printer	17/0x11	Printer Group		CAMPUS
Production_Servers	11/0xb	Production Servers Security Group		DEFAULT_VN
Production_Users	7/0x7	Production User Scalable Group		DEFAULT_VN
Quarantined_Systems	255/0xff	Quarantine Security Group		CAMPUS
Out of sync with author...	20/0x14	SL Group		BMS
Smart_Plug	30/0x1e			null
Test_Servers	13/0xd	Test Servers Scalable Group		DEFAULT_VN
TrustSec_Devices	2/0x2	TrustSec Devices Security Group		DEFAULT_VN
Unknown	0/0x0	Unknown Security Group		DEFAULT_VN

Perform the steps below to stay in sync with the Author Node cluster.

Step 1. Remove all the references of Scalable Group on the Reader Node cluster.

Step 2. Navigate to **System > Settings > External Services > Authentication and Policy Servers** and re-enter the Cisco ISE Super Admin Password to perform a resynchronization with ISE.

Procedure 7. Creating Access Contracts

An Access Contract is a set of rules that control the type of network traffic that is allowed to pass between the source and destination Scalable Group. Security Group Access Control Lists (SGACLs) in ISE are called Access Contracts in Cisco DNA Center. Access Contracts define the actions (permit or deny) performed when the traffic matches a network application, protocol, and port.

The steps to manage Access Contract is the same process on standalone Cisco DNA Center cluster or cluster participating in the Multiple Cisco DNA Center feature. The distinction is that creating, editing, and deleting Access Contracts is permitted only on the Author Node cluster, and Access Contracts are not visible on the Reader Node clusters. A hyperlink is displayed to cross-launch to the Author Node cluster's Access Contracts page.

Please refer to **Create Access Contracts** section in the [Cisco DNA Center User Guide](#) for Access Contract creation and conflict and resolution in case of mismatch between Cisco DNA Center and Cisco ISE.

Figure 33. Access Contract creation on Author Node Cluster

The screenshot shows the Cisco DNA Center interface for Policy - Group-Based Access Control. A success message at the top states: "Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations". The "Access Contracts" tab is selected in the navigation bar. A "Create Access Contract" button is highlighted with an orange arrow. Below the tab, a table lists 7 access contracts:

Name	Description	Rules Count	Policies
Deny_HTTP		3	0
Deny IP	Deny IP SGACL		3
Deny_IP_Log	Deny IP with logging		0
FIN_CON		1	0
ICMP_DENY		1	0
Permit IP	Permit IP SGACL		1
Permit_IP_Log	Permit IP with logging		0

At the bottom, it shows "Showing 1 - 7 of 7" entries.

Figure 34. Access Contract – Reader Node Cluster

The screenshot shows the Cisco DNA Center interface for Policy - Group-Based Access Control. The "Access Contracts" tab is selected in the navigation bar, highlighted with an orange arrow. A large message box in the center states: "In Multiple Cisco DNA Center environment, Access Contracts are administered on the Author node".

Procedure 8. Create Group-Based Access Control Policy

Scalable Groups and Access Contracts are the basic building blocks of an Access-Control Policy. While creating an Access-Control Policy, Scalable Groups and Contracts that have created before can be used or new Scalable Group and Contracts can be created.

If you want to specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source group and single or multiple destination groups or you can create an access control policy with a single destination and multiple source groups.

Creating an Access Control policy is the exact same process on Standalone Cisco DNA Center or Multiple Cisco DNAC Center Cluster. Managing(creating/editing/deleting) Access Control policy is permitted only on the Author Node cluster and Access Control policy are not even visible on the Reader Cisco DNAC Cluster node, rather a hyperlink is displayed to cross-launch to Author Node cluster's Access Control Policy page.

Perform the below steps to create Group-based Control policy on the **Author Node**

Step 1. On the Author Node Cluster, navigate to  > **Policy > Group-Based Access Control > Policies.**

Step 2. Click **Create Policies.**

Step 3. To create an Access-Control Policy with a single source and single destination group, select **Source to Destination(s)** from the drop-down.

Step 4. Click on the radio button next to source Scalable Group (for example: Mobile_Robot).

Step 5. Click **Next**

Step 6. Choose the destination Scalable Group (for example: Smart_Plug).

Step 7. Click **Next**

Step 8. Click the radio button next to desired Access Contract.

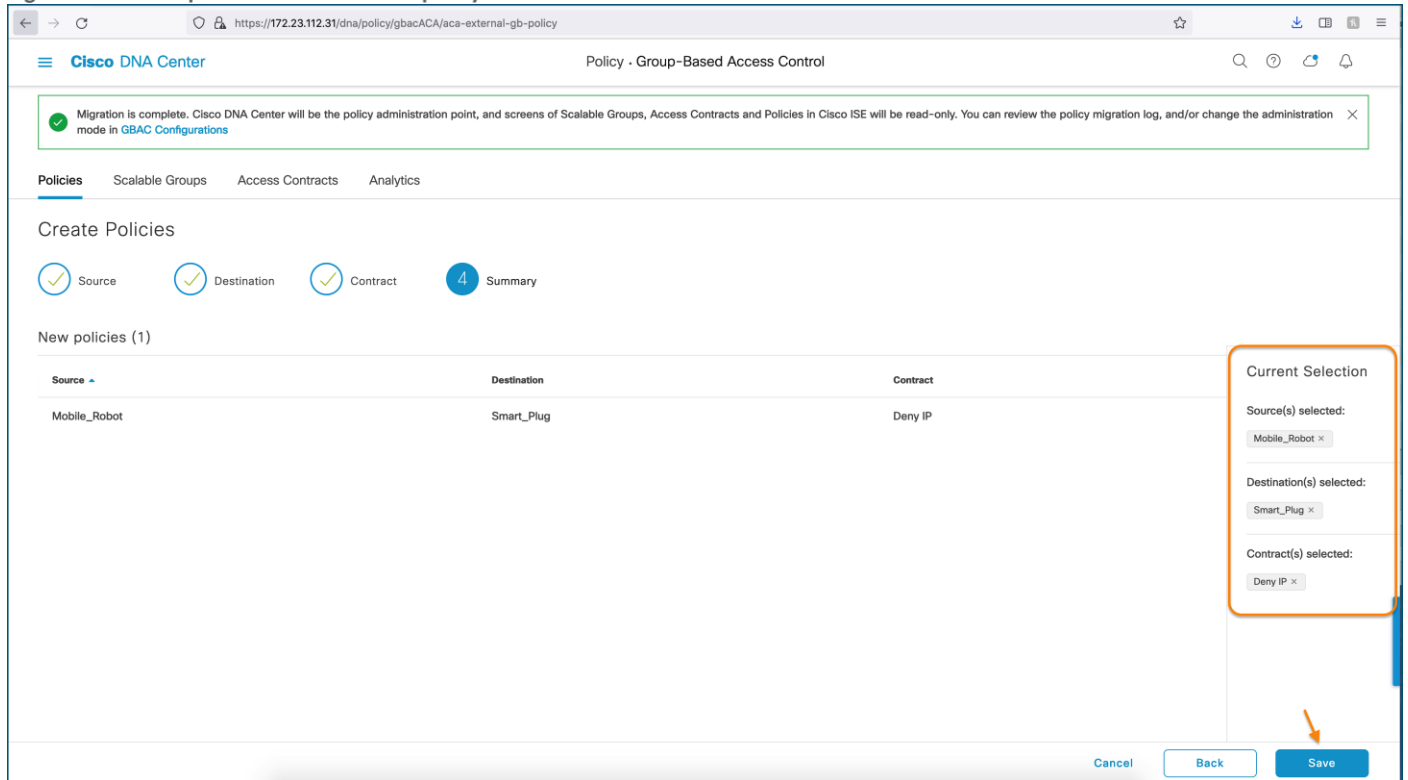
Step 9. Click **Next**

The Summary window lists the policy that you created based on the selected Scalable Groups and contracts.

Step 10. Click **Save.**

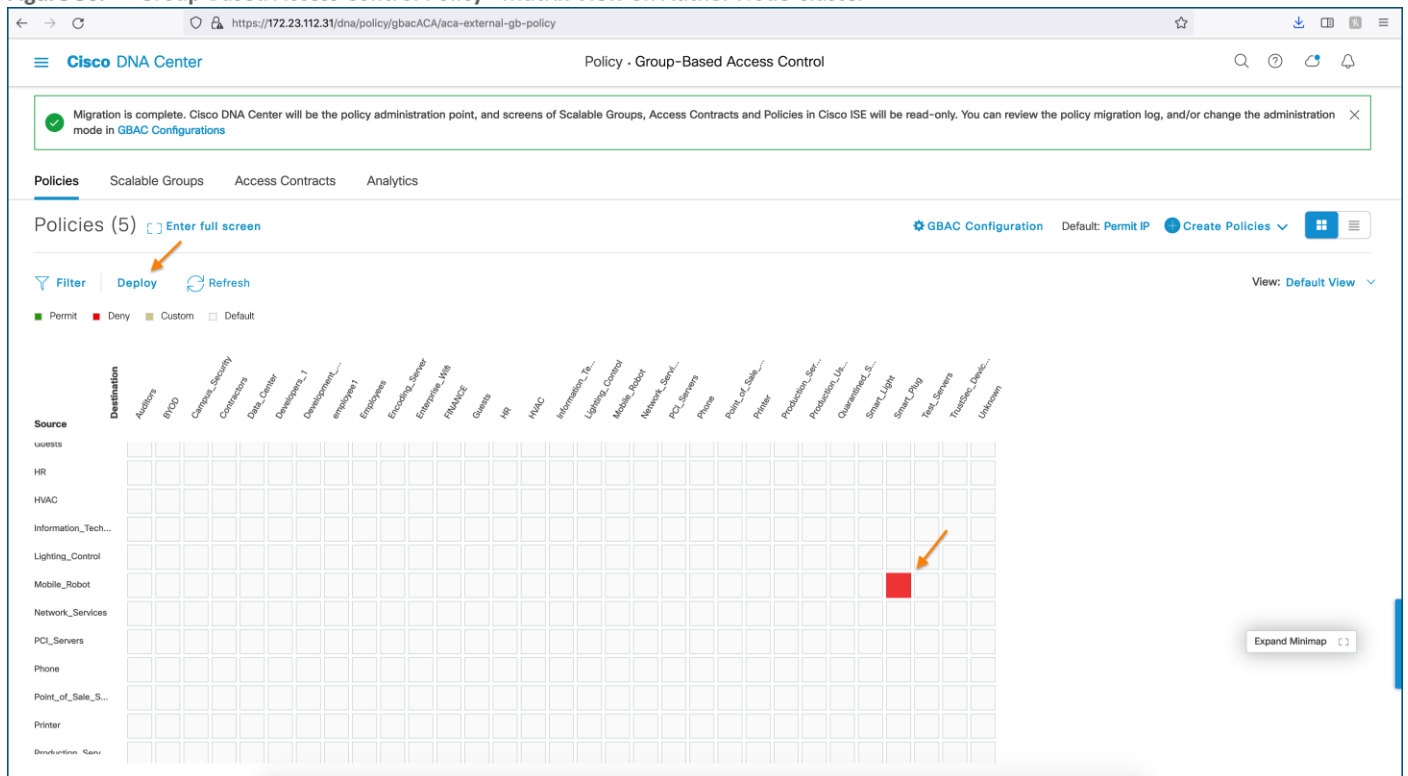
Step 11. Click **Deploy** for Cisco DNA Center pushes the Policy information to ISE.

Figure 35. Group-Based Access control policy creation on Author Node Cluster



Step 12. To verify to policy creation in Cisco DNA Center, map the Cell intersecting the Source and Destination Scalable Group for the policy that was configured previously in [Step 2](#) as shown in Figure 36.

Figure 36. Group-Based Access Control Policy - Matrix View on Author Node Cluster



Step 13. On Cisco ISE, Navigate to **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix** to verify the policy push from Cisco DNA Center.

Tech tip

The *Edit*, *Add*, *Clear*, and *Deploy* buttons are greyed out on Cisco ISE because Cisco DNA center is managing TrustSec Policy. Therefore, these items are Read-Only on ISE.

Figure 37. TrustSec Policy Matrix on Cisco ISE – Read-Only View

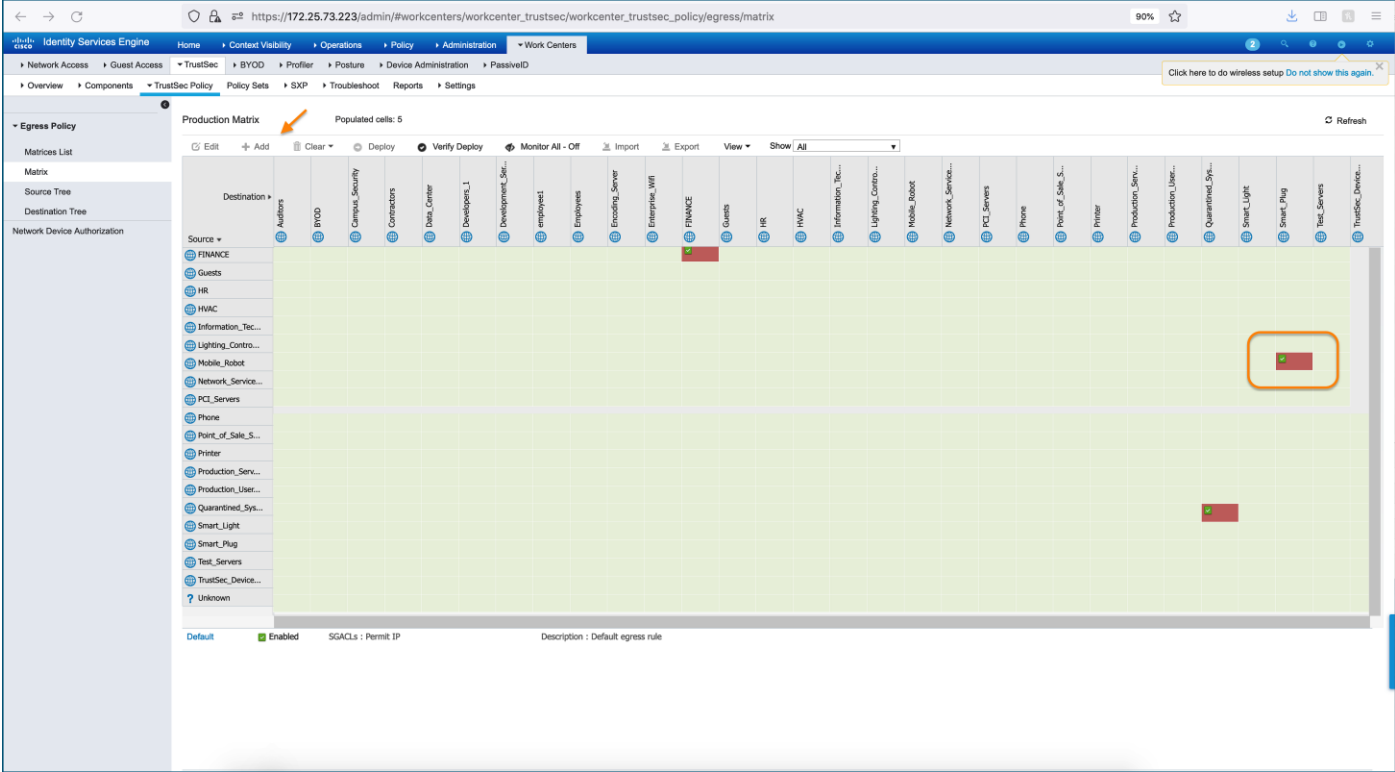


Figure 38. TrustSec Read-Only Privileges on Cisco ISE

TrustSec Overview

Cisco DNA Center is managing TrustSec Security Groups, SGACL's and Egress Policy, those screens are Read Only.

- 1 Prepare**
 - Plan Security Groups**
Identify resources that require different levels of protection
 - Classify the users or clients that will access those resources
 - Objective is to identify the minimum required number of Security Groups, as this will simplify management of the matrix
 - Preliminary Setup**
Set up the [TrustSec AAA server](#).
 - Set up TrustSec [network devices](#).
 - Check default TrustSec [settings](#) to make sure they are acceptable.
 - If relevant, set up [TrustSec-ACI](#) policy group exchange to enable consistent policy across your network.
 - Consider activating the [workflow process](#) to prepare staging policy with an approval process.
- 2 Define**
 - Create Components**
Create [security groups](#) for resources, user groups and Network Devices as defined in the preparation phase. Also, examine if default SGTs can be used to match the roles defined.
 - Define the [network device authorization policy](#) by assigning SGTs to network devices.
 - Policy**
Define [SGACLs](#) to specify egress policy.
 - Assign SGACLs to cells within the [matrix](#) to enforce security.
 - Exchange Policy**
Configure [SXP](#) to allow distribution of IP to SGT mappings directly to TrustSec enforcement devices.
- 3 Go Live & Monitor**
 - Push Policy**
Push the [matrix](#) policy live.
 - Push the [SGTs](#), [SGACLs](#) and the [matrix](#) to the network devices ⓘ
 - Real-time Monitoring**
Check [dashboards](#) to monitor current access.
 - Auditing**
Examine [reports](#) to check access and authorization is as intended.

Operate

Operate section begins with a discussion around promoting Reader Node cluster to Author Node cluster and circumstances when to promote and best practices to follow before this promotion. The later part of the section will focus on the basic high-level troubleshooting steps

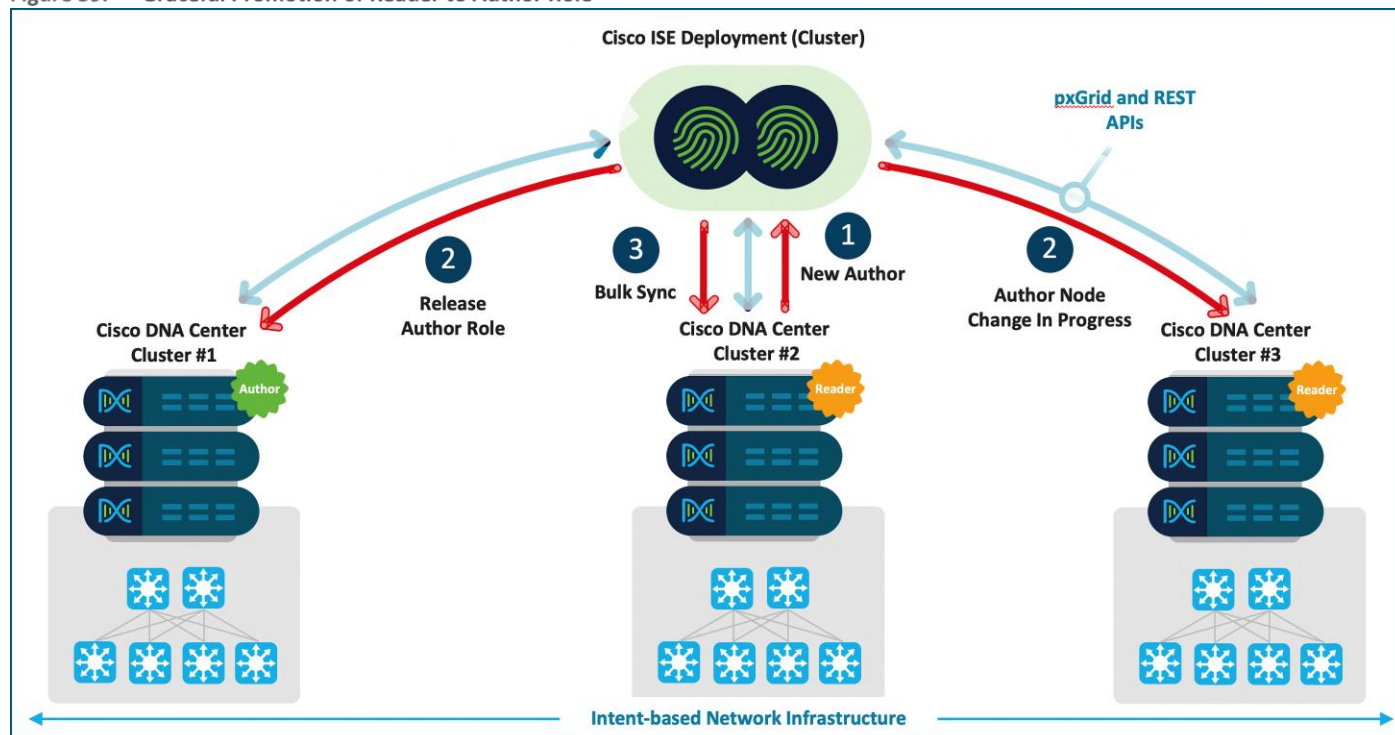
As part of the Multiple Cisco DNA Center solution architecture where we have multiple Cisco DNA Center Clusters and only one has a special role for being policy Author. There may be instances where the Administrator needs to promote a Reader Node cluster to take over the role of Author Node cluster. This promotion should not be done unless:

- The Author Node cluster is taken out of service or is otherwise unavailable for an extended period.
- The Author Node cluster is permanently unavailable or unresponsive for an extended period, and Policy changes are required.

Procedure 1. Graceful Promotion of Reader to Author role

Multiple Cisco DNA Center architecture supports a manual process to promote Reader Cisco DNA Cluster to Author Role if the administrator plans to take the Author Node cluster out of service. All Reader Node clusters, by default, have a [Promote to Author](#) button. You can start promoting a Reader Node cluster to an Author Node while your current Author Node cluster is still in operation. Do not start the promotion operation while the existing Author Node cluster is busy. For example, while synchronizing policies with ISE. If the Author Node cluster is busy, the promotion operation is staggered until the Author node completes current processing.

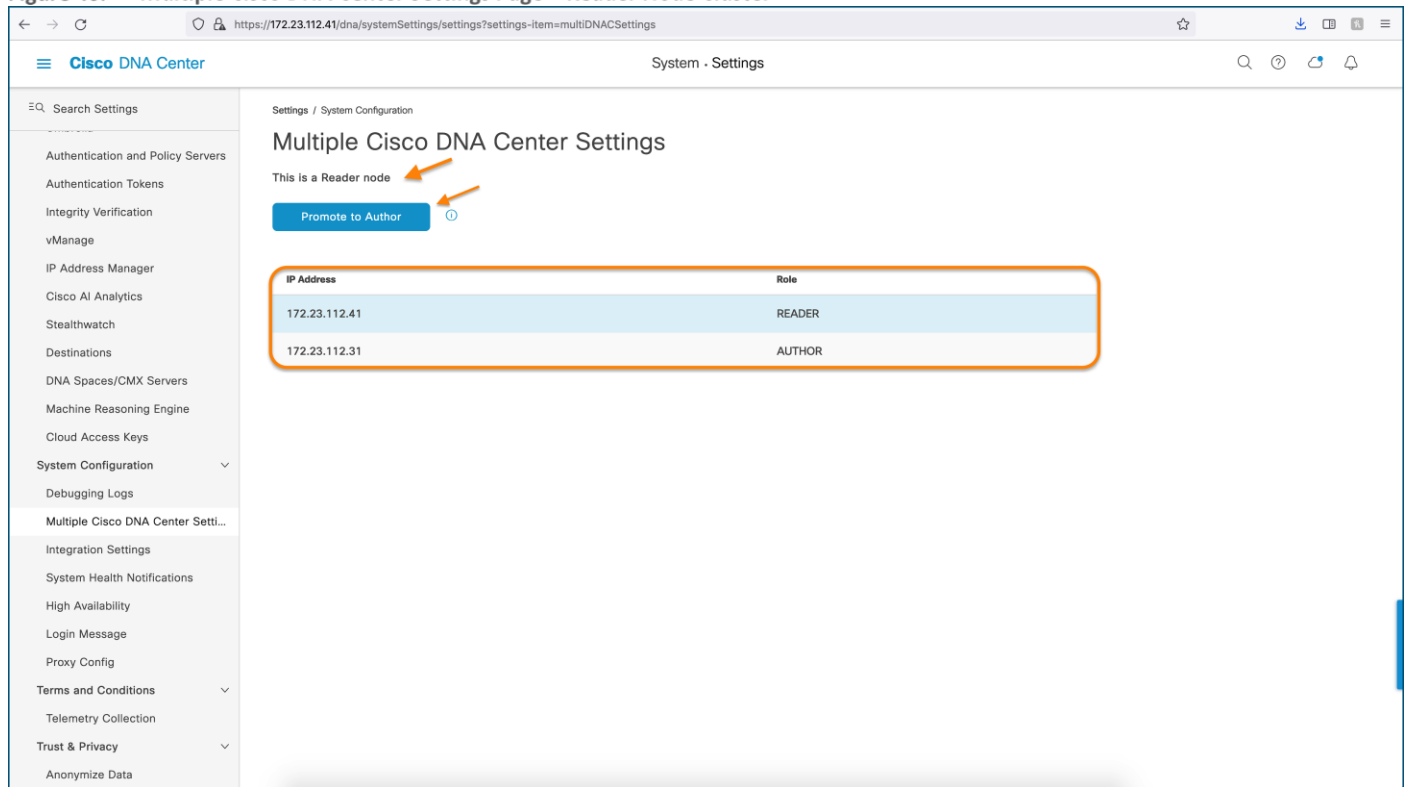
Figure 39. Graceful Promotion of Reader to Author Role



- 1) Upon Graceful promotion of a Reader Node cluster (Cluster #2), Access Control Application on the Reader Node cluster initiates an API call to Cisco ISE for Role change (Reader -> Author).
- 2) Cisco ISE upon receiving a role change will request the current Author to release the role of Author. Current Author (Cluster #1) releases the role of Author (if no sync in progress, else wait until the sync complete) and takes over the role of Reader Node cluster.

- 3) Current Reader (Cluster #2) up for promotion resumes the role of Author Node cluster. Upon the Author and Reader role change, Cisco ISE updates other Reader Node clusters about the New Author via configuration update. Next, the new Author Node cluster (Cluster #2) initiates the data migration from Cisco ISE and disables Promote to Author option in the UI.

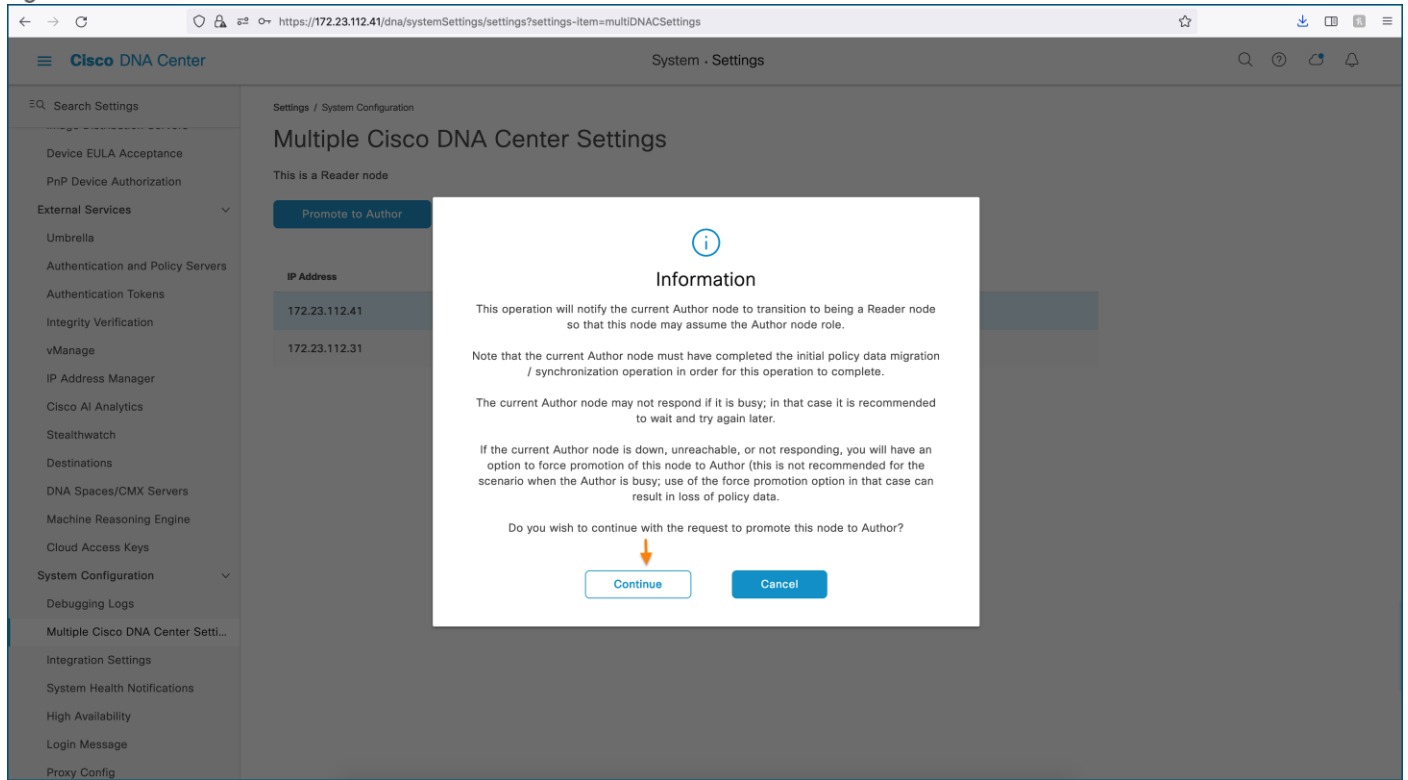
Figure 40. Multiple Cisco DNA Center Settings Page – Reader Node Cluster



Step 1. On the Reader Node cluster, navigate to **System > Settings > System Configuration > Multiple Cisco DNA Center Settings** and verify the Author and Reader Node roles.

Step 2. Click on **Promote to Author** button and upon clicking, below warning messages appears.

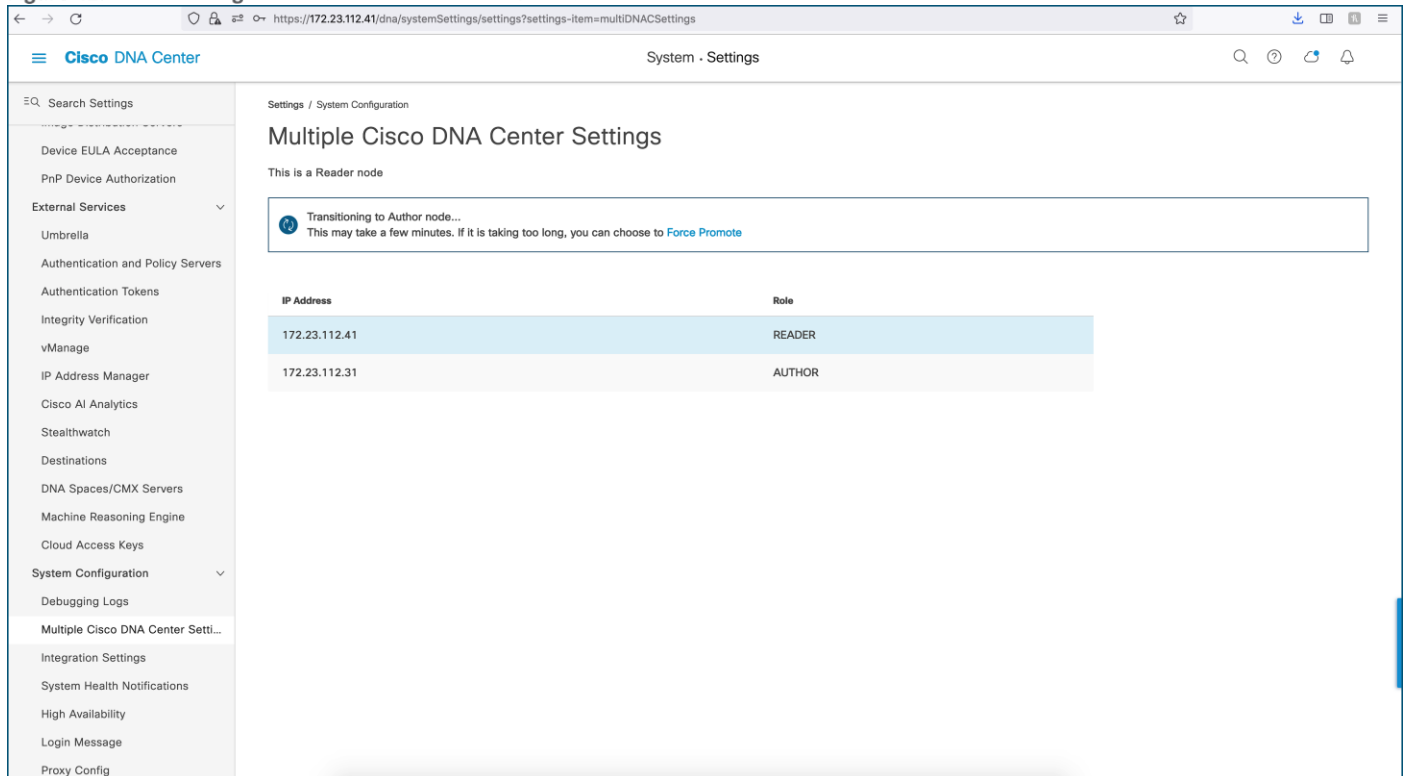
Figure 41. Promote to Author Info Banner – Reader Node Cluster



Step 3. Click **Continue** to promote the node to Author role.

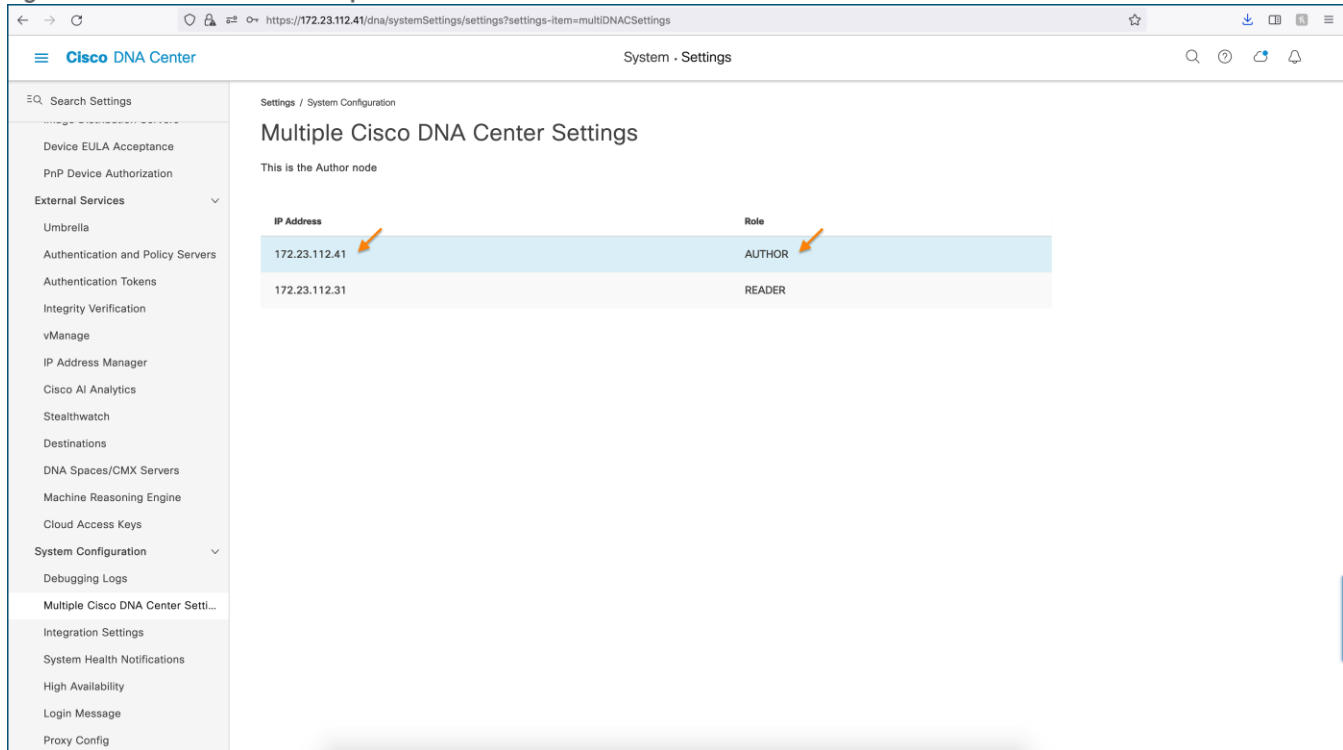
The transition process may take several minutes.

Figure 42. Promoting Reader Node Cluster to Author Node Role



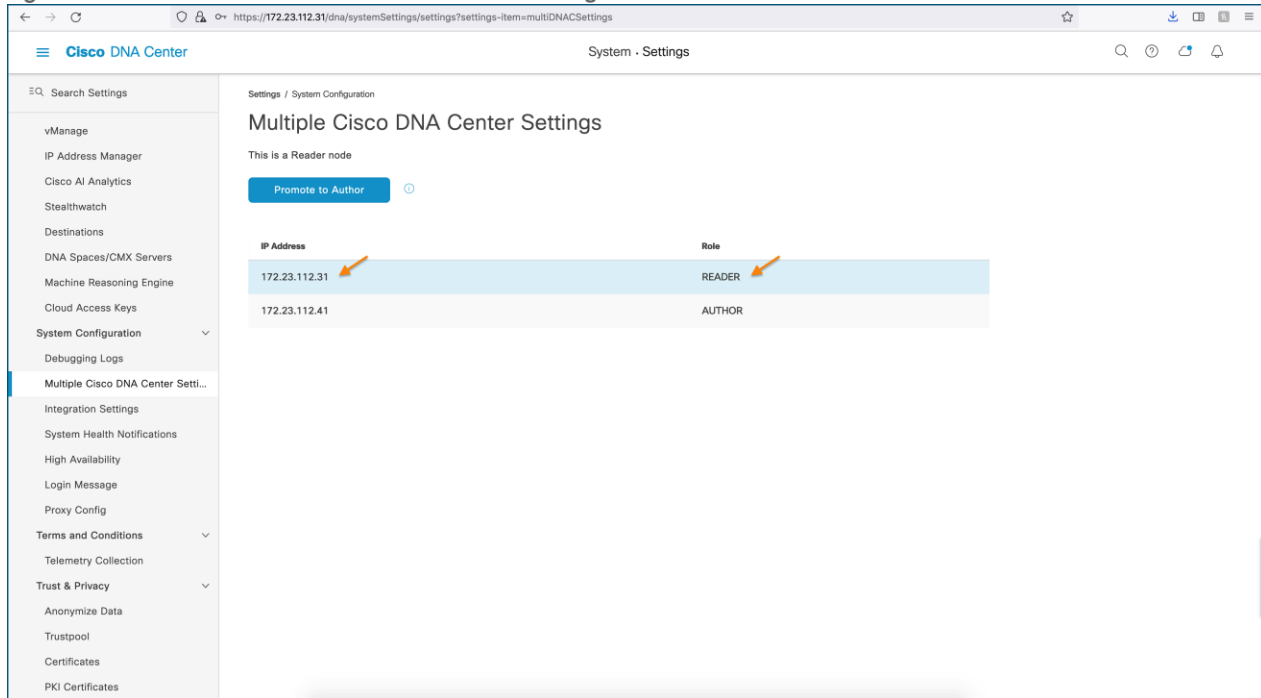
Step 4. Verify that the Cluster this was promoted changes to the Author Role as show in Figure 43.

Figure 43. Reader Node Cluster promoted to Author Role



Step 5. Verify that the previous Author Node cluster is now in the Reader Node role as show in Figure 44.

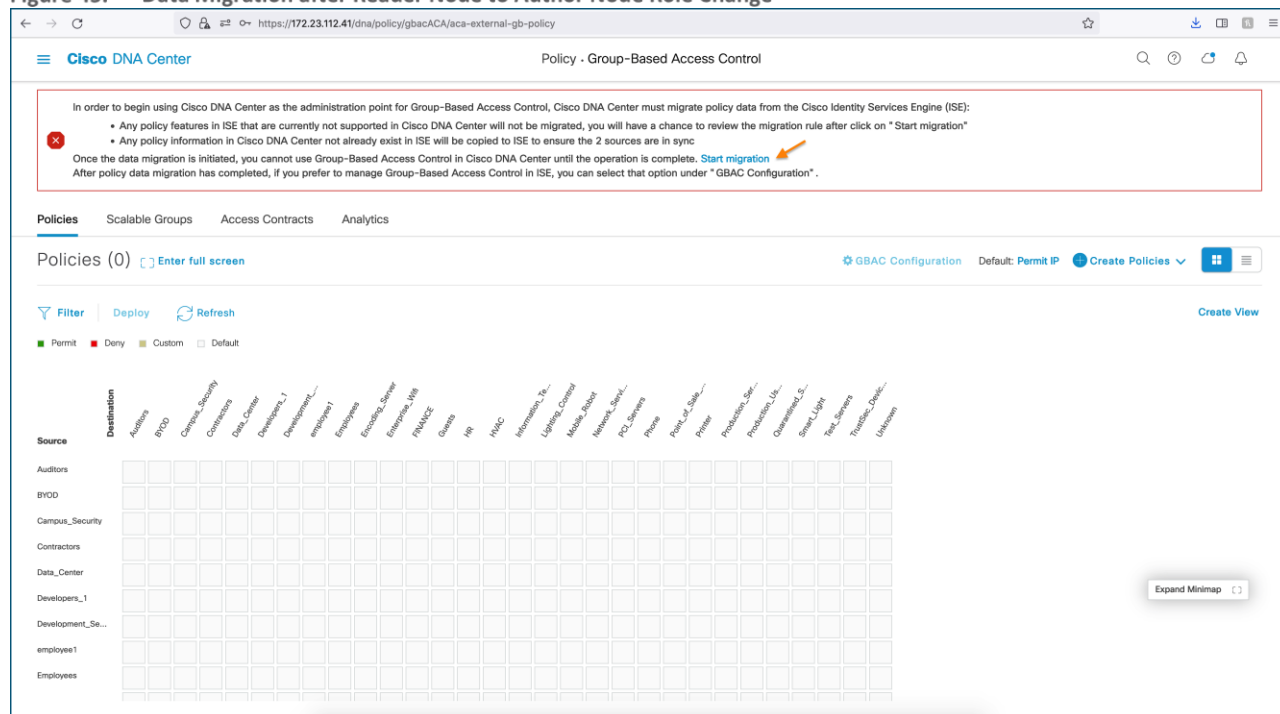
Figure 44. Author Node Role to Reader Node Role Change after Promotion



Step 6. Once the promotion operation is successful, start the migration operation on the Author Node cluster to initiate policy migration from ISE.

Depending on the amount of Policy data, this process may take up to an hour.

Figure 45. Data Migration after Reader Node to Author Node Role Change



Procedure 2. Force Promotion of Reader Role to Author Role

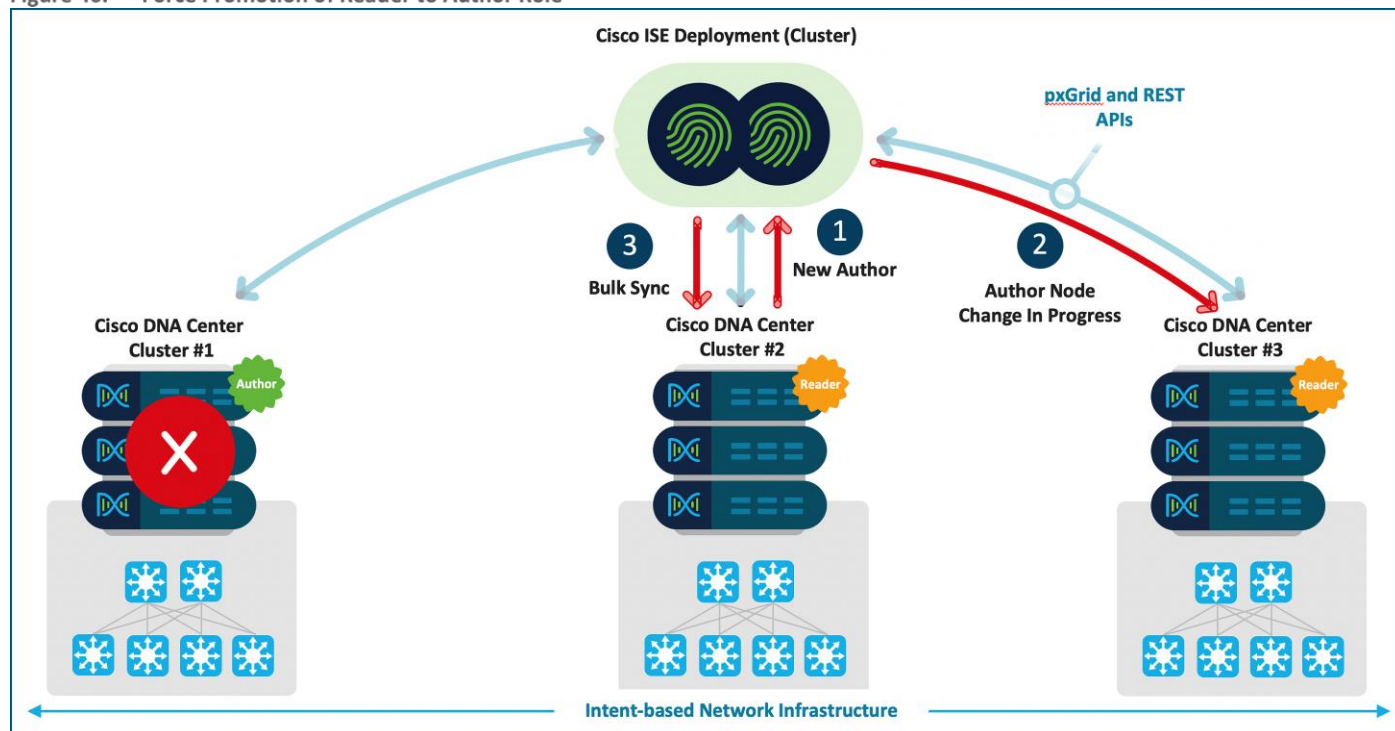
Force Promotion is a form of manual promotion that is intended to promote the current Reader Node cluster. The *Force Promote* option only appears during the [Graceful Promotion](#) process. *Force Promotion* should only be used in the following situations:

- The current Author Node cluster is out of service
- The current Author Node cluster is unresponsive
- The Reader-Node-to-Author-Node graceful promotion is taking more than five minutes

Do not use the *Force Promotion* option while the existing Author Node cluster is in service, as this may result in data loss and the Author Node cluster getting out of sync with ISE. It is **strongly recommended** that *Force Promotion* is used only if service must be restored immediately, and any data loss is acceptable.

After the *Forced Promotion* operation, the promoted Reader Node cluster becomes the new Author Node cluster for the deployment. When a former Author Node cluster becomes available, it will transition to the Reader Node role and download the latest configuration data from ISE.

Figure 46. Force Promotion of Reader to Author Role

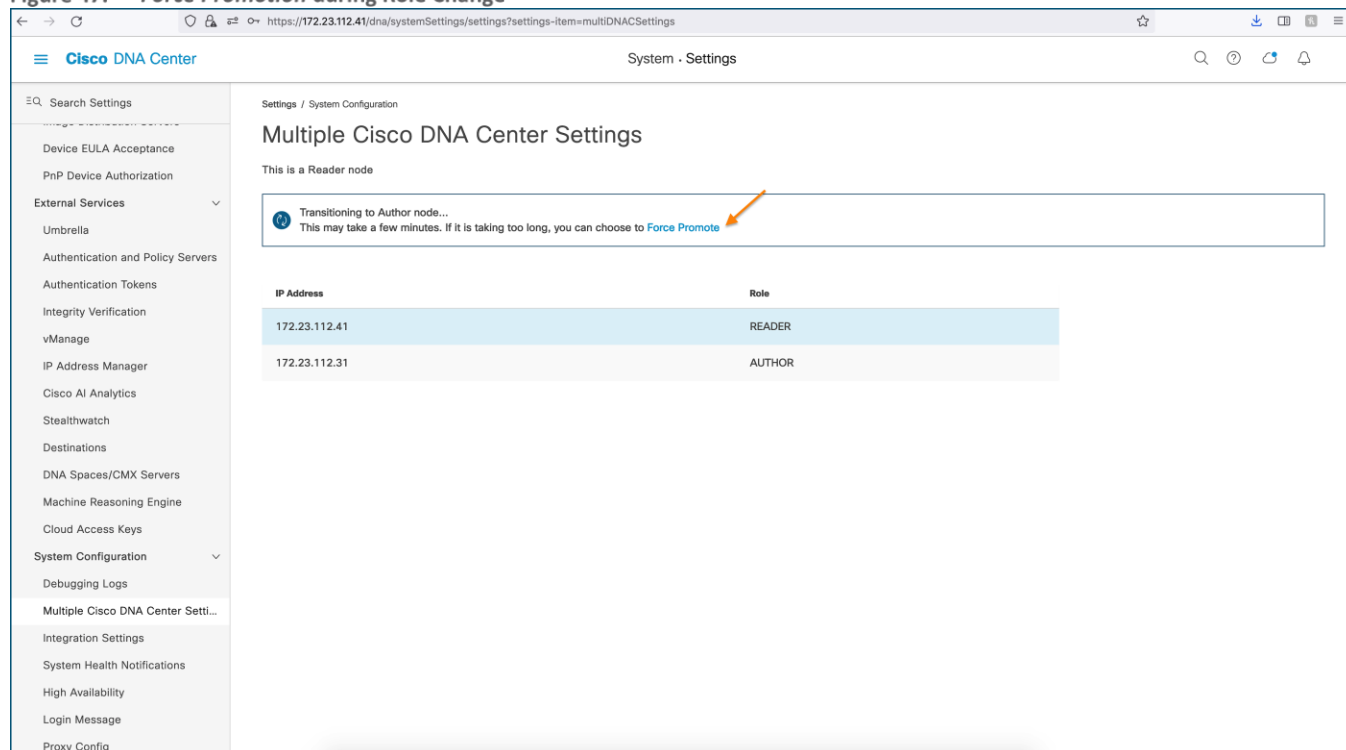


Upon initiating the promotion of a Reader Node cluster (Cluster #2), Access Control Application on the Reader Node cluster initiates an API call to Cisco ISE for Role change (Reader -> Author). Upon receiving a role change, Cisco ISE will request the current Author to release the role of Author. If the current Author (Cluster #1) is unresponsive and if the administrator selects Force Promotion, Reader Node cluster ACA package initiates API call with FORCE FLAG and this would change the Reader Node cluster to Author and Author to Reader role immediately in Cisco ISE. The Configuration update message is sent to all nodes. Next, the new Author Node cluster (Cluster #2) initiates the data migration from Cisco ISE and disables Promote to Author Option in the UI.

The steps to *Force Promote* a Reader Node cluster to Author Node cluster are the same as called out in the [Graceful Promotion](#) section, except an additional step after Step 4 to initiate the *Force Promotion*. A summary of these steps without screen shots are below:

- Step 1.** On the Reader Node cluster, navigate to **≡ > System > Settings > System Configuration > Multiple Cisco DNA Center Settings** and verify the Author and Reader Node roles.
- Step 2.** Click on **Promote to Author** button and upon clicking, below warning messages appears.
- Step 3.** Click **Continue** to promote the node to Author role.
The transition process may take several minutes.
- Step 4.** Click the **Force Promote** button shown in Figure 47.

Figure 47. Force Promotion during Role Change



Procedure 3. Multiple Cisco DNA Center Troubleshooting

Troubleshooting the Multiple Cisco DNA Center to ISE feature can be completed using logs from Cisco DNA Center and ISE. Compilation, Interpretation, and correlation of these logs should be performed with assistance from the Cisco Technical Assistance Center (TAC).

Cisco DNA Center Logs

Cisco DNA Center logs are accessed from the appliance (maglev) CLI. These should only be accessed with assistance from the Cisco TAC.

- **Network-design-service**—Events corresponding to Cisco ISE Connectivity
- **Identity-manager-pxGrid-service**—pxGrid related subscription, registration, and bulk download

Aca-controller-service—Migration, runtime sync, promotion, registration, and entity specific events such as Scalable Groups, Access Contracts, Policy, Scalable-Group-to-VN association.

Cisco ISE Logs

Cisco ISE logs are accessed from the ISE GUI. In ISE:

- Navigate to **Operations > Troubleshoot > Download Logs > Select Node > Debug Logs > Ise-psc.log**
- Navigate to **Administration > System > Logging > Debug log configuration** and set PxGrid, Infrastructure, and ERS logs to **debug**.
- Navigate to **Operations > Troubleshoot > Download Logs > Select PxGrid Node > Debug Logs > Pxgird-server.log**

Appendix A: Hardware and Software Versions

The following products and software versions were included as part of validation in this deployment guide, and this validated set is not inclusive of all possibilities. Additional hardware options are listed in the associated [Software-Defined Access Solution Design Guide](#), the [SD-Access Compatibility Matrix](#), and the [Cisco DNA Center data sheets](#) that may have guidance beyond what was tested as part of this guide. Updated Cisco DNA Center package files are regularly released and available within the packages and updated listings.

Table 4. Cisco DNA Center

Product	Part number	Software Version
Cisco DNA Center Appliance	DN2-HW-APL & DN2-HW-APL-L	2.2.2.3

All packages running on the Cisco DNA Center during validation are listed—not all packages are included as part of the testing for SD-Access validation.

Table 5. Cisco DNA Center Package Versions

Package Name – CLI	Package Name – GUI	Software Version
sd-access	SD Access	2.1.363.60202
access-control-application	Access Control Application	2.1.363.60202
group-based-policy-analytics	Group-Based Policy Analytics	2.2.1.209
multi-dnac-enablement	Multiple Cisco DNA Center	2.1.360.60878

Table 6. Device Platform, Model, and Software Version

Platform	Model (PID)	Software Code Version
Cisco DNA Center	DN2-HW-APL and DN2-HW-APL-L	Cisco DNA Center 2.2.2.3
Identity Services Engine	R-ISE-VMS-K9	ISE 2.6 Patch 7
Catalyst 9000 Series Switches	C9300-48U	17.3.2a

Appendix B: References Used in this Guide

Cisco DNA Center Second-Generation Appliance Installation Guide, Release 2.2.2:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-2/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_2_2_2ndGen.html

Cisco DNA Center Security Best Practices Guide: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html

Cisco Identity Services Engine Installation Guide, Release 2.6: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/install_guide/b_ise_InstallationGuide26.html

Cisco DNA Center SD-Access LAN Automation Deployment Guide: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/b_dnac_sda_lan_automation_deployment.html

Cisco SD-Access Macro-Segmentation Deployment Guide: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-macro-segmentation-deploy-guide.html>

Cisco DNA Center Group-Based Policy Deployment Guide: <https://community.cisco.com/t5/networking-documents/group-based-policy-analytics-deployment-guide/ta-p/4096076>

Cisco DNA Center & ISE Management Infrastructure Deployment Guide: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-dnac-ise-deploy-guide.html>

Feedback

For comments and suggestions about this guide and related guides, join the discussion on [Cisco Community](https://cs.co/en-cvds) at <https://cs.co/en-cvds>.

Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://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/go/trademarks>. 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. (1110R)