Reintegrate Cisco ISE with Cisco Catalyst Center

Reintegrate Cisco ISE with Cisco Catalyst Center

This guide is designed for the following two use cases:

- If you want to replace the Cisco ISE platform from hardware to a virtual network that is integrated with the Catalyst Center, including any IP address change.

- If you want to change the IP address of the existing Cisco ISE while moving the existing Cisco ISE from the current Catalyst Center to the new Catalyst Center.

You can follow the same procedure for both the use cases. You can also use the same procedure if you want to change the IP address of Cisco ISE. You can transition your existing Cisco ISE to a new Cisco ISE without having to make any configuration changes in Catalyst Center.

This procedure is mainly used for moving the Cisco ISE from Catalyst Center, ABC to Catalyst Center, XYZ.

Note If you are viewing this guide on cisco.com, click any of its figures to view a full-sized version.

Prerequisites

Ensure the following:

- Catalyst Center and the existing Cisco ISE pxGrid are functioning and SGT synchronization is working.

- The existing and new Cisco ISE are on the same software version and patch.

- The Smart Registration portal is accessible to mitigate licensing challenges, if any, during the transition.

- You break the new Cisco ISE VM cluster and make each Cisco ISE a standalone node.

- You reset the new Cisco ISE applications to the factory default to avoid issues, if any, during the transition.

- The new Cisco ISE has A and PTR records registered on DNS servers.

- You back up the existing Cisco ISE.

- You open a proactive TAC case to mitigate Cisco ISE technical and licensing issues, if any.

- The licenses should be the same for both the existing and new Cisco ISE nodes.

IP Addresses and Naming Conventions

The following table shows example IP address and naming conventions involved in the migration.

Note The round-trip time between Catalyst Center, XYZ and Catalyst Center, ABC is around 20 to 30 ms during peak hours.

Technology	Name	IP Address	Location
Existing Cisco ISE (3955 hardware) - Primary (PAN + MNT + PSN + Device Admin + PXG)	Existing-ISE-1	10.0.0.1	ABC
Existing Cisco ISE (3955 hardware) - Secondary (SAN + MNT + PSN + Device Admin + PXG)	Existing-ISE-2	10.0.0.2	ABC
New Cisco ISE (3615 VM) - Primary (SAN + MNT) - 600 GB	New-ISE-1	10.0.0.3	XYZ
New Cisco ISE (3615 VM) - Primary (SAN + MNT) - 600 GB	New-ISE-2	10.0.0.4	XYZ
New Cisco ISE (3615 VM) - PXG - 300 GB	New-ISE-3	10.0.0.5	XYZ
New Cisco ISE (3615 VM) - PXG - 300 GB	New-ISE-4	10.0.0.6	XYZ
New Cisco ISE (3615 VM) - PSN - 300GB	New-ISE-5	10.0.0.7	XYZ
New Cisco ISE (3615 VM) - PSN - 300GB	New-ISE-6	10.0.0.8	XYZ
Catalyst Center-1	HQ-SDA-Catalyst-1	10.255.255.250	ABC
Catalyst Center-2	HQ-SDA-Catalyst-2	10.255.255.251	ABC
Catalyst Center-3[1]	HQ-SDA-Catalyst-3	10.255.255.252	ABC
Catalyst Center VIP	HQ-SDA-Catalyst	10.255.255.253	ABC

[1] The example here shows a three-node Catalyst Center cluster. The procedure is independent of whether the Catalyst Center cluster is a standalone cluster, a two-node cluster, or a three-node cluster.

Existing Setup State

The following figure shows an example of the existing setup.
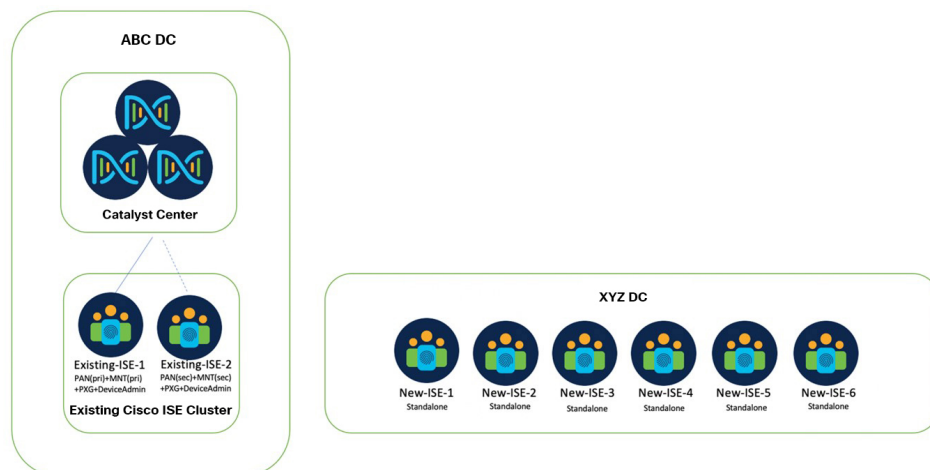
- *Existing-ISE-1* and *Existing-ISE-2* are in one cluster as the primary responsible for device administration.

- Catalyst Center is integrated with *Existing-ISE-1* as the primary PAN and *Existing-ISE-2* as the secondary PAN with the following discovery learned:

    - *Existing-ISE-1* as primary PAN, PXG, TACACS.

    - *Existing-ISE-2* as secondary PAN, PXG, TACACS.

- *Existing-ISE-1* and *Existing-ISE-2* manage non-SDA network devices for TACACS and RADIUS (device administration).

- *New-ISE* (VMs) are in a separate new cluster that will be refreshed as a standalone with a factory-default reset. The new cluster is responsible for endpoint network access control using dot1x/MAB (RADIUS).

Objective

The objectives of the reintegration are as follows:

- Catalyst Center integrates transparently from the existing Cisco ISE to the new Cisco ISE without changing IP addresses.

- The new Cisco ISE VMs are added to the existing Cisco ISE cluster. The PAN/MNT, pxGrid, and PSN personas are distributed to new nodes as follows:

    - *New-ISE-1* (PAN + MNT) as primary

    - *New-ISE-2* (PAN + MNT) as secondary

    - *New-ISE-3* (PXG1)

    - *New-ISE-4* (PXG2)

    - *New-ISE-5* (RADIUS PSN 1)

    - *New-ISE-6* (RADIUS PSN 2)

    - *Existing-ISE-1* (TACACS PSN 1)

    - *Existing-ISE-2* (TACACS PSN 2)

> **Note**   There is a possible risk to the TACACS functionality of the SDA and non-SDA components during the Cisco ISE transition.

Hardware and Software Versions

The following table lists the hardware and software versions that are used in the existing setup.

Technology	Hardware	Version
Existing Cisco ISE nodes	3955 hardware	2.7 Patch 3
New Cisco ISE nodes	3615 equivalent VM	2.7 Patch 3
Catalyst Center nodes	DN1-HW-APL	1.3.3.9

Reintegration Phases

The reintegration is divided into multiple phases, which are described in the following sections:

1. Add distributed Cisco ISE VM nodes to the existing cluster.

2. Move PAN+MNT personas to the new Cisco ISE nodes.

3. Provision the switches with the new AAA settings.

4. Modify the global authentication template.

Add Distributed Cisco ISE VM Nodes to the Existing Cluster
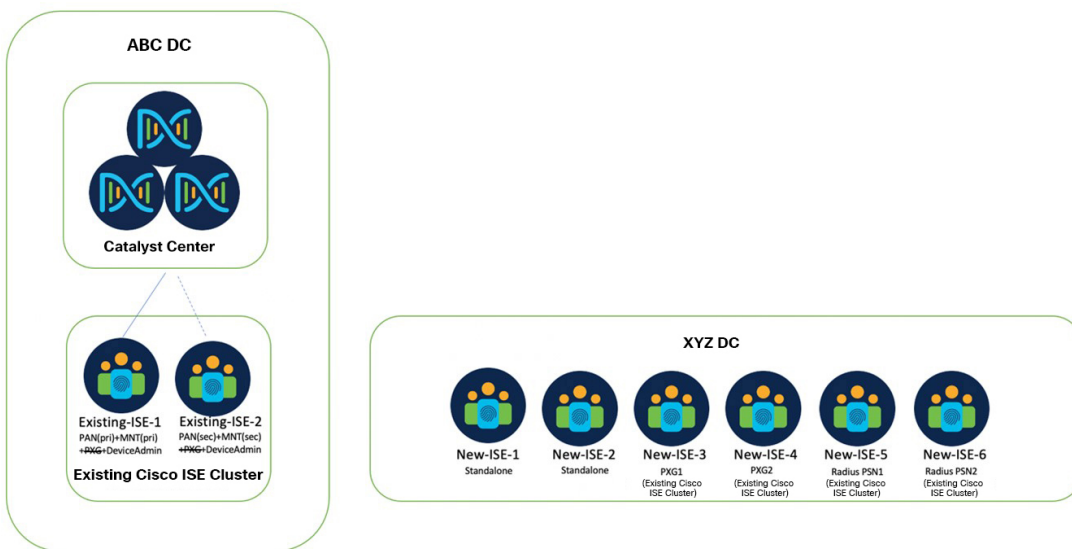
Procedure

|	
Step 1	Log in to *Existing-ISE-1* and choose **System** > **Deployment**. Deselect the PXG2 role from *Existing-ISE-2*.
Step 2	Register the *New-ISE* nodes as follows:

     a) Register *New-ISE-4* (PXG2).
     b) Register *New-ISE-5* (RADIUS PSN 1).
     c) Register *New-ISE-6* (RADIUS PSN 2).
     d) Deselect the PXG1 role from *Existing-ISE-1*.
     e) Register *New-ISE-3* (PXG1).
     f) Verify that all the nodes are synchronized and marked as Green status in Cisco ISE.

       At this stage, *Existing-ISE-1* and *Existing-ISE-2* are still functioning as PAN+MNT+TACACS-PSN.

Step 3	Log in to Catalyst Center and verify the changes.
Step 4	Verify that Catalyst Center and the Cisco ISE pxGrid are functioning, and the SGT/SGT-MATRIX replication works correctly.

Move PAN+MNT Personas to the New Cisco ISE Nodes
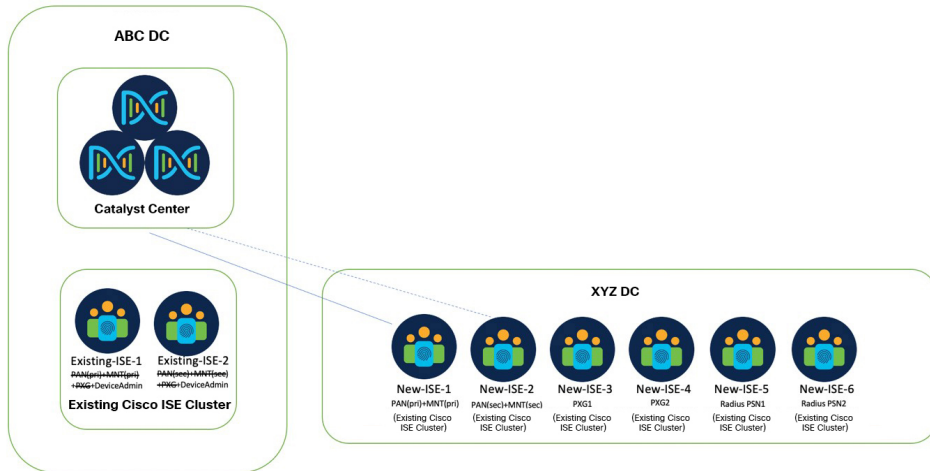
After each step in the following procedure, verify that the node changes are synchronized and marked as Green status in Cisco ISE.

Procedure

Step 1	Log in to *Existing-ISE-1* and choose **System** > **Deployment**. On *Existing-ISE-2*, remove the Secondary PAN and Secondary MNT roles, leaving only the Device Admin role.
Step 2	Log in to Catalyst Center and choose **System** > **System 360**. Confirm that Catalyst Center learns the PAN/MNT changes.
Step 3	Log in to *Existing-ISE-1* and choose **System** > **Deployment**. Register *New-ISE-1* as the secondary PAN and MNT.
Step 4	Log in to Catalyst Center and choose **System** > **System 360**. Verify that Catalyst Center learns the registration of *New-ISE-1* as the secondary PAN.
Step 5	Access the Smart Licensing portal (Cisco SSM), deregister *Existing-ISE-2*, and register *New-ISE-1*.
Step 6	In Cisco ISE, choose **System** > **Licensing** and update the Smart Licensing registration. Verify that no licensing warning message occurs after the reregistration.
Step 7	Log in to *Existing-ISE-1* and choose **System** > **Deployment**. Make *New-ISE-1* the primary and *Existing-ISE-1* the secondary.
Step 8	Log in to *New-ISE-1* and choose **System** > **Deployment**. On *Existing-ISE-1*, remove the Secondary PAN and Secondary MNT roles, leaving only the Device Admin role.
Step 9	Verify that Catalyst Center learns the changes again.
Step 10	Log in to *New-ISE-1* and choose **System** > **Deployment**. Register *New-ISE-2* as the secondary PAN and MNT.
Step 11	Access the Smart Licensing portal (Cisco SSM), deregister *Existing-ISE-1*, and register *New-ISE-2*.
Step 12	In Cisco ISE, choose **System** > **Licensing** and update the Smart Licensing registration. Verify that no licensing warning message occurs after the reregistration.
Step 13	Verify that Catalyst Center shows the PAN primary and secondary nodes correctly.

Provision the Switches with the New AAA Settings

Procedure

Step 1   In Catalyst Center, update the network settings. Choose **Network** > **TACACS** to point to the existing Cisco ISE nodes (10.204.0.20 and 10.204.0.21). Choose **Client** > **RADIUS** to point to the new Cisco ISE PSNs (10.204.2.124 and 10.204.2.125).

Step 2   Provision a sample switch. Verify that TACACS and RADIUS are reflected correctly in the switch configuration.

Step 3   Provision other switches in batches.

Modify the Global Authentication Template

Procedure

Step 1   In the Catalyst Center GUI, click the menu icon and choose **Provision** > **Fabric** and choose the fabric.

Step 2   Choose **Host Onboarding** > **Authentication Template** and change it from **No Authentication** to **Closed Authentication**. This step doesn't modify the configuration on ports that are already statically configured with **No Authentication**.

Step 3   Click **Save**.