Complete First-Time Setup

First-Time Setup Workflow

After you finish configuring all of the Catalyst Center appliances you have installed, perform the tasks described in this chapter to prepare Catalyst Center for production use. Note the following points:

- For the parameter information you need to complete this work, see Required First-Time Setup Information.
- If you plan to deploy high availability (HA) in your production environment, you will need to redistribute services among your cluster nodes to optimize HA operation (see Activate HA). Complete this step after you have configured the SNMP settings for your appliances.

Compatible Browsers

The Catalyst Center GUI is compatible with the following HTTPS-enabled browsers:

- Google Chrome: Version 93 or later.
- Mozilla Firefox: Version 92 or later.

We recommend that the client systems you use to log in to Catalyst Center be equipped with 64-bit operating systems and browsers.

Complete the Quick Start Workflow

After you have installed and configured the Catalyst Center appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Catalyst Center.

When you log in for the first time as the admin superuser (with the username `admin` and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts. Complete this workflow to discover the devices that Catalyst Center will manage and enable the collection of telemetry from those devices.

Before you begin

To log in to Catalyst Center and complete the Quick Start workflow, you will need:

- The *admin* superuser username and password that you specified while completing one of the following procedures:
  - Configure the Primary Node Using the Maglev Wizard
  - Configure the Primary Node Using the Advanced Install Configuration Wizard (32- or 56-core appliance)
  - Configure a Secondary Node Using the Advanced Install Configuration Wizard (80-core appliance)
- The information described in Required First-Time Setup Information.

Step 1 After the Catalyst Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Catalyst Center GUI, using **`HTTPS://`** and the IP address of the Catalyst Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on the browser you are using):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**.

One of the following messages appears:

- Google Chrome:

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted
by your computer's
 operating system. This may be caused by a misconfiguration or an attacker intercepting your
connection.
```

- Mozilla Firefox:

```
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates.
Firefox does not trust GUI-IP-address because its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate certificates.
```

These messages appear because the controller uses a self-signed certificate. For information on how Catalyst Center uses certificates, see the "Certificate and Private Key Support" section in the *Cisco Catalyst Center Administrator Guide*.

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to** *GUI-IP-address* **(unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Catalyst Center login screen appears.

Step 5 Do one of the following and then click **Log In**:

- If you completed the Maglev configuration wizard and chose the **Start using DNAC pre manufactured cluster** option, enter the admin's username (**admin**) and password (**maglev1@3**).
- If you completed the Maglev configuration wizard and chose the **Start configuration of DNAC in advanced mode** option, enter the admin's username (**admin**) and password that you set when you configured your Catalyst Center appliance.
- If you completed the Install configuration wizard, enter the admin's username (**admin**) and paste the password (**maglev1@3**) that you copied from the wizard's final screen.
- If you completed the Advanced Install configuration wizard, enter the admin's username (**admin**) and password that you set when you configured your Catalyst Center appliance.

In the next screen, you are prompted to specify a new admin password (as a security measure).

Step 6 Do one of the following:

- If you don't want to change the admin password at this time, click **Skip**.
- To set a new admin password:
  a. Enter the same password that you specified in Step 5.
  b. Enter and confirm a new admin password.
  c. Click **Next**.

Step 7 Enter your cisco.com username and password (which are used to register software downloads and receive system communications) and then click **Next**.

Note If you don't want to enter these credentials at this time, click **Skip** instead.

The **Terms & Conditions** screen opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

Step 8 After reviewing these documents, click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Catalyst Center.

Step 9 Complete the Quick Start workflow:

a) Click **Let's Do it**.

b) In the **Discover Devices: Provide IP Ranges** screen, enter the following information and then click **Next**:

- The name for the device discovery job.
- The IP address ranges of the devices you want to discover. Click + to enter additional ranges.
- Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, see the "Preferred Management IP Address" topic in the *Catalyst Center User Guide*.

c) In the **Discover Devices: Provide Credentials** screen, enter the information described in the following table for the type of credentials you want to configure and then click **Next**:

Field	Description
CLI (SSH) Credentials	
Username	Username used to log in to the CLI of the devices in your network.
Password	Password used to log in to the CLI of the devices in your network. The password you enter must be at least eight characters long.
Name/Description	Name or description of the CLI credentials.
Enable Password	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
SNMP Credentials: SNMPv2c Read tab **Note** Catalyst Center does not support SNMPv2c credentials when FIPS mode is enabled. You'll need to enter SNMPv3 credentials instead. For more information regarding FIPS mode, see t_configure_primary_node_mcw_3rdgen.xml.	
Name/Description	Name or description of the SNMPv2c read community string.
Community String	Read-only community string password used only to view SNMP information on the device.
SNMP Credentials: SNMPv2c Write tab	
Name/Description	Name or description of the SNMPv2c write community string.
Community String	Write community string used to make changes to the SNMP information on the device.
SNMP Credentials: SNMPv3	
Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.
Mode	Security level that SNMP messages require: • **No Authentication, No Privacy** (noAuthnoPriv): Does not provide authentication or encryption. • **Authentication, No Privacy** (authNoPriv): Provides authentication, but does not provide encryption. • **Authentication and Privacy** (authPriv): Provides both authentication and encryption. **Note** When FIPS mode is enabled, Catalyst Center only supports **Authentication and Privacy** mode.

Field	Description
Authentication Password	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Authentication Type	Hash-based Message Authentication Code (HMAC) type used when either **Authentication and Privacy** or **Authentication, No Privacy** is set as the authentication mode: • **SHA**: HMAC-SHA authentication. • **MD5**: HMAC-MD5 authentication. **Note** Catalyst Center does not support this authentication type when FIPS mode is enabled.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Choose one of the following privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices. **Note** • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages are exchanged with devices supported with AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
NETCONF	
Port	The NETCONF port that Catalyst Center should use in order to discover wireless controllers that run Cisco IOS-XE.

d) In the **Create Site** screen, group the devices you are going to discover into one site in order to facilitate telemetry and then click **Next**.

You can enter the site's information manually or click the location you want to use in the provided map.

e) In the **Enable Telemetry** screen, check the network components that you want Catalyst Center to collect telemetry for and then click **Next**.

Note If both the **Enable Telemetry** and **Disable Telemetry** options are grayed out, this indicates that either devices are not capable of supporting telemetry or devices are running an OS version that does not support telemetry enablement.

f) In the **Summary** screen, review the settings that you have entered and then do one of the following:

- If you want to make changes, click the appropriate **Edit** link to open the relevant screen.
- If you're happy with the settings, click **Start Discovery and Telemetry**. Catalyst Center validates your settings to ensure that they will not result in any issues. After validation is complete, the screen updates.

  Catalyst Center begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

  A message appears at the top of the homepage to indicate when the Quick Start workflow has completed.

g) Do one of the following:

- Click **View Discovery** to open the **Discovery** page and confirm that the devices in your network have been discovered.
- Click the **Go to Network Settings** link to open the **Device Credentials** page. From here, you can verify that the credentials you entered previously have been configured for your site.
- Click the **View Activity Page** link to open the **Tasks** page and view any tasks (such as a weekly scan of the network for security advisories) that Catalyst Center has already scheduled to run.

- Click the **Workflow Home** link to access guided workflows that will help you set up and maintain your network.

Integrate Cisco ISE with Catalyst Center

Catalyst Center provides a mechanism to create a trusted communications link with Cisco ISE and to share data with Cisco ISE in a secure manner. After Cisco ISE is registered with Catalyst Center, any device that Catalyst Center discovers, along with relevant configuration and other data, is pushed to Cisco ISE. You can use Catalyst Center to discover devices and then apply both Catalyst Center and Cisco ISE functions to them because these devices will be displayed in both the applications. Catalyst Center and Cisco ISE devices are all uniquely identified by their device names.

As soon as the devices are provisioned and assigned to a particular site in the Catalyst Center site hierarchy, Catalyst Center devices are pushed to Cisco ISE. Any updates to a Catalyst Center device (such as changes to IP address, SNMP or CLI credentials, Cisco ISE shared secret, and so on) will be sent to the corresponding device instance on ISE automatically. Note that Catalyst Center devices are pushed to Cisco ISE only when these devices are associated with a particular site where Cisco ISE is configured as its AAA server.

Before you begin

Before attempting to integrate Cisco ISE with Catalyst Center, ensure that you have met the following prerequisites:

- You have deployed one or more Cisco ISE hosts on your network. For information on supported Cisco ISE versions, see the Catalyst Center Compatibility Matrix. For information on installing Cisco ISE, see the Cisco Identity Services Engine Install and Upgrade guides.
- If you have a standalone Cisco ISE deployment, you must integrate Catalyst Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.

Note Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Catalyst Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

- If you have a distributed Cisco ISE deployment:
  - You must integrate Catalyst Center with the primary policy administration node (PAN), and enable ERS on the PAN.

Note We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the PSNs.

  - You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.

- The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and PACs must also be defined in **Work Centers** > **Trustsec** > **Trustsec Servers** > **Trustsec AAA Servers**. For more information, see the *Cisco Identity Services Engine Administrator Guide*.

- Only a user with Super Admin role permissions can integrate Cisco ISE with Catalyst Center.
- Catalyst Center does not support ERS API access if the **Use CSRF Check for Enhanced Security** option is enabled in Cisco ISE.
- You must enable communication between Catalyst Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Catalyst Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- Catalyst Center will check the certificate revocation status if Online Certificate Status Protocol (OCSP) or certificate revocation list (CRL) validation is defined for the certificates used by the Cisco ISE services.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or FQDN in either the certificate subject name or the Subject Alternative Name (SAN).
- Your ability to use an FQDN-only system certificate depends on whether LAN automation is enabled in your Catalyst Center deployment. For more information, see the **alt_names** section bullet in Step 3 of the Catalyst Center Security Best Practices Guide's "Generate a Certificate Request Using Open SSL" topic.

Note For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

This issue does not occur in Cisco ISE 3.0 and later. For more information, see the Cisco ISE Release Notes.

For more information about configuring Cisco ISE for Catalyst Center, see the "Integration with Catalyst Center" topic in the *Cisco Identity Services Engine Administrator Guide*.

Step 1 Enable the pxGrid service and ERS on Cisco ISE:

a) Log in to the primary policy administration node.

b) In the Cisco ISE GUI, click the menu icon and choose **Administration** > **System** > **Deployment**.

The **Deployment Nodes** window appears.

c) Click the hostname of the Cisco ISE node on which you want to enable the pxGrid service. In a distributed deployment, this can be any Cisco ISE node in the deployment.

The **Edit Node** window appears.

d) In the **General Settings** tab, check the **pxGrid** check box, and click **Save**.

e) In the Cisco ISE GUI, click the menu icon and choose **Administration** > **System** > **Settings**.
f) From the left navigation pane, click **ERS Settings** to open the **ERS Settings** window.
g) Click the **Enable ERS for Read/Write** radio button, and then click **OK** in the notification prompt.
h) Click **Save**.

Step 2 Add the Cisco ISE node to Catalyst Center as a AAA server:

a) Log in to the Catalyst Center GUI.
b) From the top-left corner, click the menu icon and choose **System** > **System 360**.
c) In the Identity Services Engine (ISE) pane, click the **Configure** link.
d) From the **Authentication and Policy Servers** window, click **Add** and choose **ISE** from the drop-down list.
e) Enter the following details in the **Add ISE server** slide-in pane:

- In the **Server IP Address** field, enter the IP address of the Cisco ISE server.
- Enter the **Shared Secret** used to secure communications between your network devices and Cisco ISE.
- In the **Username** and **Password** fields, enter the corresponding Cisco ISE admin credentials.
- Enter the **FQDN** for the Cisco ISE node.
- (Optional) Enter the **virtual IP address** of the load balancer behind which the Cisco ISE PSNs are located. If you have multiple policy service node farms behind different load balancers, you can enter a maximum of six virtual IP addresses.
- **Connect to pxGrid**: Check this check box under **Advanced Settings** to enable pxGrid connection.

  If you want to use the Catalyst Center system certificate as the pxGrid client certificate (sent to ISE to authenticate the Catalyst Center system as a pxGrid client), check the **Use Catalyst Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same Certificate Authority (CA). If this option is disabled, Catalyst Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

  When you enable this option, ensure that:

  - The Catalyst Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise the pxGrid authentication will fail).
  - The Certificate Extended Key Use (EKU) field includes “Client Authentication”.
  - In the **Advanced Settings** area:
    - You can choose the protocol that must be used by checking the check box for **RADIUS** or **TACACS**
    - Enter the required values in the following fields: **Authentication Port**, **Accounting Port**, **Retries**, and **(Timeout seconds)**.

Note This option is available only if third-party certificates are used by Catalyst Center. If Catalyst Center uses the default self-signed system certificate, this option is disabled.

f) Click **Add**.

When the integration with Cisco ISE is initiated, you will see a notification that the certificate from Cisco ISE is not yet trusted. You can view the certificate to see the details.

Click **Accept** to trust the certificate and continue with the integration process, or choose **Decline** if you do not wish to trust the certificate and terminate the integration process.

After the integration completes successfully, a confirmation message is displayed.

If there is any issue in the integration process, an error message is displayed. An option to edit or retry is displayed where applicable.

- If the error message says that the Cisco ISE Admin credentials are invalid, click **Edit** and re-enter the correct information.
- If errors are found with certificates in the integration process, you must delete the Cisco ISE server entry and restart the integration from the beginning after the certificate issue has been resolved.

Step 3 Verify that Catalyst Center is connected to Cisco ISE, and that the Cisco ISE SGT groups and devices are pushed to Catalyst Center:

a) Log in to the Catalyst Center GUI.
b) From the top-left corner, click the menu icon and choose **System** > **System 360**.
c) In the Identity Services Engine (ISE) pane, verify that the status of all listed ISE servers is displayed as **Available** or **Configured**.
d) In the Identity Services Engine (ISE) pane, click the **Update** link.
e) From the **Authentication and Policy Servers** window, verify that the status of the Cisco ISE AAA server is still **Active**.

Step 4 Verify that Cisco ISE is connected to Catalyst Center and that the connection has subscribers:

a) Log in to the Cisco ISE nodes that are shown as pxGrid servers in the **Identity Services Engine (ISE)** pane.
b) Choose **Administration** > **pxGrid Services** and click the **Web Clients** tab.

You should see the pxGrid clients in the list with the IP address of the Catalyst Center server.

Group-Based Access Control: Policy Data Migration and Synchronization

When You Start Using Catalyst Center

In earlier releases of Catalyst Center, the Group-Based Access Control policy function stored some policy Access Contracts and Policies locally in Catalyst Center. Catalyst Center also propagated that data to Cisco ISE. Cisco ISE provides the runtime policy services to the network, which includes group-based access control policy downloads to the network devices. Usually, the policy information in Catalyst Center matches the policy information in Cisco ISE. But it is possible that the data is not in sync; the data may not be consistent. Because of this, after installing or upgrading to Catalyst Center, the following steps are necessary before you can use the Group-Based Access Control capabilities.

- Integrate Cisco ISE with Catalyst Center, if it is not already integrated.
- Upgrade Cisco ISE, if the version is not the minimum required. See the Catalyst Center Release Notes for the required versions of Cisco ISE.
- Perform Policy Migration and Synchronization.

What Is “Migration and Synchronization”?

Catalyst Center reads all the Group-Based Access Control policy data in the integrated Cisco ISE and compares that data with the policy data in Catalyst Center. If you upgraded from an earlier version, existing policy data

is retained. You must synchronize the policies before you can manage Group-Based Access Control Policy in Catalyst Center.

How Does Migration and Synchronization Work?

Usually, the policy data in Cisco ISE and in Catalyst Center is consistent, so no special handling or conversion of data is necessary. Sometimes, when there are minor discrepancies or inconsistencies, only some of the data is converted during the migration. 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. The following list describes the actions taken during migration:

- Security Groups: The Security Group Tag (SGT), which is a numeric value, uniquely identifies a Security Group. Cisco ISE Security Groups are compared to Security Groups in Catalyst Center.
    - When the Name and SGT value are the same, nothing is changed. The information in Catalyst Center is consistent with Cisco ISE and does not need to be changed.
    - When a Cisco ISE Security Group SGT value does not exist in Catalyst Center, a new Security Group is created in Catalyst Center. The new Security Group is given the default association of "Default_VN."
    - When a Cisco ISE Security Group SGT value exists in Catalyst Center, but the names do not match, the name from Cisco ISE Security Group replaces the name of that Security Group in Catalyst Center.
    - When the Cisco ISE Security Group Name is the same, but the SGT value is different, the Security Group from Cisco ISE is migrated. It retains the name and tag value, and the Catalyst Center Security Group is renamed. A suffix of "_DNA" is added.

Contracts

All the SGACLs in Cisco ISE that are referenced by policies are compared to Contracts in Catalyst Center.

- When the SGACL and Contract have the same name and content, there is no need for further action. The information in Catalyst Center is consistent with Cisco ISE and does not need to be changed.
    - When the SGACL and Contract have the same name, but the content is different, the SGACL content from Cisco ISE is migrated. The previous Contract content in Catalyst Center is discarded.

When the SGACL name does not exist in Catalyst Center, a new Contract with that name is created, and the SGACL content from Cisco ISE is migrated.

Note When creating new Access Contracts based on Cisco ISE SGACL content, Catalyst Center parses the text command lines, and, where possible, renders these SGACL commands as a modeled Access Contract. Each ACE line renders as an "Advanced" application line. If a Cisco ISE SGACL contains text that cannot be parsed successfully, the text content of the SGACL is not converted into modeled format. It is stored as raw command line text. These SGACL text contracts may be edited, but no parsing or syntax checking of the text content is performed during migration.

Policies

A Policy is uniquely identified by a source group-destination group pair. All Cisco ISE TrustSec Egress Policy Matrix policies are compared to the policies in Catalyst Center.

- When a policy for a source group-destination group references the same SGACL/Contract name in Cisco ISE, no changes are made.
- When a policy for a source group-destination group references a different SGACL/Contract name in Cisco ISE, the Cisco ISE Contract name is referenced in the policy. This overwrites the previous Contract reference in Catalyst Center.
- The Cisco ISE default policy is checked and migrated to Catalyst Center.

Note Catalyst Center supports a single contract in access policies. Cisco ISE has an option to use multiple SGACLs in access policies, but this option is not enabled by default in Cisco ISE, and in general is not widely used. Existing SDA customers who have been using the previous release of Catalyst Center to manage Group-Based Access Control policy did not use this option.

If you enabled the option to allow multiple SGACLs on Cisco ISE and used this when creating policies, those policies cannot be migrated to Catalyst Center in this release. The specific policy features that make use of the “multiple SGACL” option and cannot be migrated are:

- Multiple SGACLs in a policy.
- Policy Level catch-all rules set to “Permit” or “Deny.” Only the value of “None” is currently supported for migration to Catalyst Center.
- Default Policy set to use a customer-created SGACL, but only the standard values of “Permit IP,” “Permit_IP_Log,” “Deny IP,” and “Deny_IP_Log” are currently supported for migration to Catalyst Center.

If any of the preceding SGACLs are detected during the policy migration and synchronization operation, a notification is generated, and you must choose between the following options to continue:

- **Manage Group-Based Access Control policy in Catalyst Center**: If this option is selected, all management of Group-Based Access Control Policy is done in Catalyst Center. The user interface screens in Cisco ISE for management of Cisco ISE Security Groups, SGACLs, and Egress Policies are available in Read-Only mode. If there were any issues migrating policies (due to use of multiple SGACLs in Cisco ISE), those policies have no contract selected in Catalyst Center. The policy uses the default policy, and you can select a new contract for those policies after completing the migration. If there was an problem migrating the default policy, the default policy is set to "Permit."
- **Manage Group-Based Access Control Policy in Cisco ISE**: If this option is selected, Catalyst Center Group-Based Access Control policy management is inactive. No changes are made to Cisco ISE and there is no effect on policy enforcement in the network. Group-Based Access Control policy is managed in Cisco ISE at the TrustSec workcenter.
- **Manage Group-Based Access Control policy in both Catalyst Center and Cisco ISE**: This option is not recommended for general use, because policy changes made in Cisco ISE are not synchronized with Catalyst Center. The two systems cannot be kept in sync. This option is intended as a short-term or interim option, and should only be considered when you enabled the “Allow Multiple SGACLs” option in Cisco ISE. Use this option if you need more time and flexibility updating Cisco ISE.

Configure Authentication and Policy Servers

Catalyst Center uses AAA servers for user authentication and Cisco ISE for both user authentication and access control. Use this procedure to configure AAA servers, including Cisco ISE.

Before you begin

- If you are using Cisco ISE to perform both policy and AAA functions, make sure that Catalyst Center and Cisco ISE are integrated.
- If FIPS mode is enabled for Catalyst Center, ensure that you enable KeyWrap when integrating Catalyst Center and Cisco ISE. See Step 2e in Integrate Cisco ISE with Catalyst Center.

Note You cannot enable KeyWrap if Catalyst Center and Cisco ISE have already been integrated. To enable this feature, you need to delete Cisco ISE and then reintegrate it with Catalyst Center.

- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:
  - Register Catalyst Center with the AAA server, including defining the shared secret on both the AAA server and Catalyst Center.
  - Define an attribute name for Catalyst Center on the AAA server.
  - For a Catalyst Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.
- Before you configure Cisco ISE, confirm that:
  - You have deployed Cisco ISE on your network. For information on supported Cisco ISE versions, see the Catalyst Center Compatibility Matrix. For information on installing Cisco ISE, see the Cisco Identity Services Engine Install and Upgrade guides.
  - If you have a standalone ISE deployment, you must integrate Catalyst Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.

Note Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Catalyst Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

  - If you have a distributed Cisco ISE deployment:
    - You must integrate Catalyst Center with the primary policy administration node (PAN), and enable ERS on the PAN.

Note We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the PSNs.

- You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.
- The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and PACs must also be defined in **Work Centers** > **Trustsec** > **Trustsec Servers** > **Trustsec AAA Servers**. For more information, see the *Cisco Identity Services Engine Administrator Guide*.

- You must enable communication between Catalyst Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Catalyst Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or FQDN in either the certificate subject name or the Subject Alternative Name (SAN).
- The Catalyst Center system certificate must list both the Catalyst Center appliance IP address and FQDN in the SAN field.

Note For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

This issue does not occur in Cisco ISE 3.0 and later. For more information, see the Cisco ISE Release Notes.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

Step 2 From the **Add** drop-down list, choose **AAA** or **ISE**.

Step 3 To configure the primary AAA server, enter the following information:

- **Server IP Address**: IP address of the AAA server.
- **Shared Secret**: Key for device authentications. The shared secret can contain up to 100 characters.

Step 4 To configure a Cisco ISE server, enter the following details:

- **Server IP Address**: IP address of the ISE server.
- **Shared Secret**: Key for device authentications.
- **Username**: Username that is used to log in to the Cisco ISE CLI.

  Note This user must be a Super Admin.

- **Password**: Password for the Cisco ISE CLI username.

- **FQDN**: Fully qualified domain name (FQDN) of the Cisco ISE server.

  Note
  - We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration** > **Deployment** > **Deployment Nodes** > **List**) and paste it directly into this field.
  - The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative Name (SAN) defined in the Cisco ISE certificate.

  The FQDN consists of two parts, a hostname and the domain name, in the following format:

  hostname.domainname.com

  For example, the FQDN for a Cisco ISE server can be ise.cisco.com.

- **Virtual IP Address(es)**: Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

Step 5 Click **Advanced Settings** and configure the settings:

- **Connect to pxGrid**: Check this check box to enable a pxGrid connection.

  If you want to use the Catalyst Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Catalyst Center system as a pxGrid client), check the **Use Catalyst Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same CA. If this option is disabled, Catalyst Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

  When you enable this option, ensure that:

  - The Catalyst Center certificate is generated by the same Certificate Authority (CA) as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
  - The Certificate Extended Key Use (EKU) field includes "Client Authentication."

- **Protocol**: **TACACS** and **RADIUS** (the default). You can select both protocols.

  Attention If you do not enable TACAS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design** > **Network Settings** > **Network** when configuring a AAA server for network device authentication.

- **Authentication Port**: Port used to relay authentication messages to the AAA server. The default UDP port is 1812.
- **Accounting Port**: Port used to relay important events to the AAA server. The default UDP port is 1813.
- **Port**: The default TACACS port is 49.
- **Retries**: Number of times that Catalyst Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Note After the required information is provided, Cisco ISE is integrated with Catalyst Center in two phases. It takes several minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** window and **System 360** window:

Cisco ISE server registration phase:

- **Authentication and Policy Servers** window: "In Progress"
- **System 360** window: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** window: "Active"
- **System 360** window: "Primary Available" and "pxGrid Available"

If the status of the configured Cisco ISE server is shown as "FAILED" due to a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.

Step 6 Click **Add**.

Step 7 To add a secondary server, repeat the preceding steps.

Configure SNMP Properties

You can configure the retry and timeout values for SNMP.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see the *Cisco Catalyst Center Administrator Guide*.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Device Settings** > **SNMP**.

Step 2 Configure the following fields:

- **Retries**: Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.
- **Timeout (in Seconds)**: Number of seconds Catalyst Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds, in intervals of 5 seconds. The default is 5 seconds.

Step 3 Click **Save**.

Note To return to the default settings, click **Reset and Save**.