

# Integrate ISE 3.3 with DNAC

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[ISE Configuration](#)

[Cisco DNA Configuration](#)

### [Verify](#)

### [Troubleshoot](#)

[Section A: Flow of Log Messages on Cisco DNA for a Successful Integration](#)

[Section B: Flow of Log Messages on ISE \(ISE PSC log\)](#)

---

## Introduction

This document describes procedures to integrate ISE 3.3 with Cisco DNA Center (DNAC) using pxGrid connections.

## Prerequisites

- ERS read write access.
- No proxy server between ISE and Catalyst Center.
- PxGrid needs to be enabled on ISE.
- FQDN is required for the integration, not just an ip address (certificate).
- If using Enterprise issued Certificate, need VIP + real ip for Catalyst Center Cluster.
- CLI credentials on ISE no longer used for integration only API-based access is supported.
- Ip reachability is required.

## Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine 3.3
- Cisco DNA

## Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine version 3.3
- Cisco DNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

The SD-Access solution is provided through a combination of Cisco Catalyst Center, the Cisco® Identity Services Engine (ISE), and wired and wireless device platforms that have fabric functionality.

Automation, Analytics, Visibility, and management of the Cisco Catalyst Center is enabled through Cisco Catalyst Center software. SD-Access is part of this software and is used to design, provision, apply policy, and facilitate the creation of an intelligent wired and wireless campus network with assurance.

ISE is an integral component of SD-Access for implementing network access control policy. ISE performs policy implementation, enabling dynamic mapping of users and devices to scalable groups and simplifying end-to-end security policy enforcement. Within ISE, users and devices are shown in a simple and flexible interface. ISE integrates with Cisco Catalyst Center by using Cisco Platform Exchange Grid (pxGrid) and Representational State Transfer (REST) APIs for endpoint event notifications and automation of policy configurations on ISE.

Understanding that Cisco Identity Services Engine (ISE) is a vital part of Cisco DNA Center is essential. It delivers core intent-based services such as:

1. AAA (RADIUS and TACACS+)
2. Network visibility
3. User and device onboarding
4. Security policies
5. Macro and micro segmentation

To utilize these services, Cisco DNA Center must be integrated with ISE to establish a trusted relationship. This guide provides Step-by-Step instructions for completing the integration process.

## Configure

### ISE Configuration

Step 1: Pxgrid must be enabled on ISE .

PxGrid service must be enabled under **System > Deployment > Edit Node > PxGrid**, as shown in the image:

Identity Services Engine Administration / System

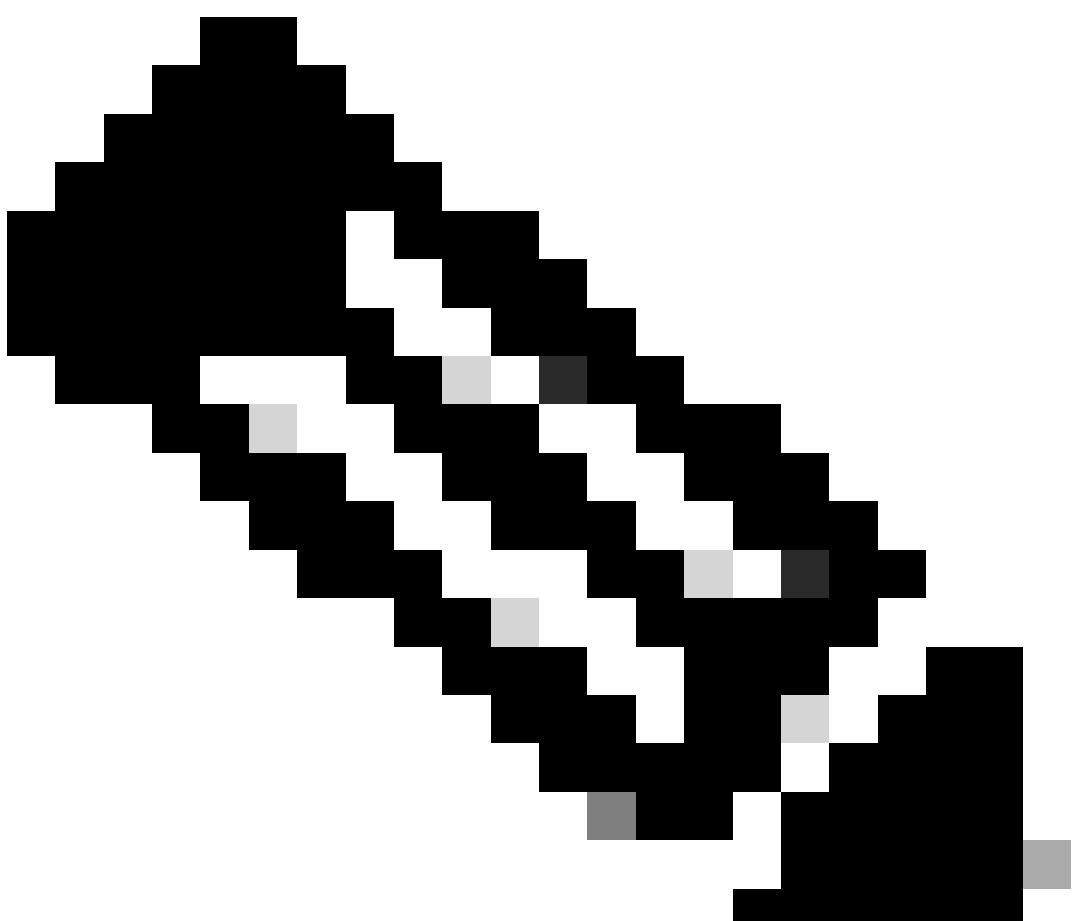
Evaluation Mode 83 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks More

Hostname: ise33seckavin  
FQDN: REDACTED  
IP Address: 10.127.196.72  
Node Type: Identity Services Engine (ISE)  
Role: SECONDARY

Administration  
 Monitoring  
 Policy Service

pxGrid ?



**Note:** In case of a distributed environment, you can have pxgrid persona running on two ISE nodes. The recommendation in a distributed environment is to run pxgrid persona on Non-Admin nodes.

## Step 2: Enable RESTful Services (ERS) Read/Write:

In order to enable Representational State Transfer (REST) and Application Programming Interface (API) services on ISE, ERS Read/Write must be enabled under **Administration > System > Settings > ERS Settings > Enable ERS for Read/Write**, as shown in the image:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar navigation includes Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (which is selected), and Work Centers. Under Administration, there are sub-options like API Settings (which is also selected), Data Connect, Network Success Diagnostics, DHCP & DNS Services, Max Sessions, Light Data Distribution, Endpoint Replication, and Interactive Help. The main content area is titled "API Settings" and has tabs for Overview, API Service Settings (which is selected), and API Gateway Settings. Under "API Service Settings for Primary Administration Node", there are two toggle switches: "ERS (Read/Write)" (which is turned on, indicated by a red box around it) and "Open API (Read/Write)". Under "API Service Setting for All Other Nodes", there are two more toggle switches: "ERS (Read)" (which is turned on) and "Open API (Read)". At the bottom, there is a section titled "CSRF Check (only for ERS Settings)" with two radio button options: "Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)" and "Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)".



**Note:** In a distributed ISE environment, ensure the Enable ERS for Read is selected, otherwise, the ERS session can come up on primary admin but not on secondary.

Step 3: Make sure both settings are enabled as shown under **Administration > pxGrid Services > Settings**.

Enable **Automatically approve new certificate-based accounts**.

Enable **Allow password based account creation**.

This allows pxGrid clients to be approved automatically.

The screenshot shows the Cisco Identity Services Engine Administration / pxGrid Services interface. The top navigation bar includes 'Evaluation Mode 83 Days', a search icon, and other navigation links. The main menu on the left has sections like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (which is selected), Work Centers, and Interactive Help. The 'Administration' section contains tabs for Summary, Client Management, Diagnostics, and Settings. The 'Settings' tab is active. In the center, there's a 'Settings' section with two checkboxes: 'Automatically approve new certificate-based accounts' and 'Allow password based account creation'. Below these checkboxes are 'Use Default' and 'Save' buttons. A red box highlights the two checked checkboxes.

## Cisco DNA Configuration

Step 1: Log in to Cisco DNAGUI.

Step 2: Navigate to **System Settings > Settings > Authentication and Policy Servers**.

The screenshot shows the Cisco Catalyst Center interface. The left sidebar includes options like Design, Policy, Provision, Assurance, Workflows, Tools, Platform, Activities, Reports, System, and Explore. The main content area is titled 'Policy Servers' and describes its function: 'authenticate Catalyst Center users. Cisco Identity Service Engine (ISE) provides policy and user information.' It shows a table with one row:

| Protocol | Type | Status | Actions |
|----------|------|--------|---------|
| RADIUS   | ISE  | ACTIVE | ...     |

At the bottom right, it says 'As of: Jun 8, 2025 2:54 PM' and has a refresh icon.

Step 3: Click **Add**. From the drop down, select **ISE**:

The screenshot shows the Catalyst Center interface with the following details:

- Left Sidebar:** Device Settings, External Services (selected), Authentication and Policy Servers, Integrity Verification.
- Header:** System / Settings, admin.
- Page Title:** Authentication and Policy Servers
- Description:** Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.
- Buttons:** Add (highlighted with a red box), Export.
- Table Headers:** IP Address, Protocol, Type, Status, Actions.
- Table Data:** One row with IP Address 10.127.196.71, Protocol RADIUS, Type ISE, Status ACTIVE, and Actions (three dots).
- Page Footer:** As of: Jun 8, 2025 2:55 PM.

Step 4: Add all the **details** as shown:

Server ip address: Ip address of ISE Primary Admin node.

Shared secret: This is the Radius shared secret for the switches when they are pushed to the ISE by Cisco DNA as network devices.

Username /Password: ISE admin Credentials.

FQDN: ISE Primary Admin node FQDN.

Subscriber name: This is the name shown under Pxgrid Services on ISE when Cisco DNA initiates a subscription request to ISE Pxgrid.

## Edit ISE server

X

Server IP Address

10.127.196.71

Shared Secret

Username\*

admin

Password\*

FQDN\*

kavinise33ppan.[REDACTED].com

Subscriber Name

pxgrid\_client\_1749316904

Cancel

Save

# ISE server Integration

X



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

Integration of 10.127.196.71 is waiting for user input



Initiating connection...

less than a minute ago

This is the first time Cisco Catalyst Center has seen this certificate from Cisco 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 Cisco ISE primary and secondary admin nodes and pxGrid nodes

Integration of 10.127.196.71 is in progress...



### Initiating connection...

Connecting to Cisco ISE and validating credentials



### Establishing trust...

Reading, validating, and storing trusted certificates



### Discovering nodes...

Discovering Cisco ISE primary and secondary admin nodes and pxGrid nodes



### Connecting to pxGrid...

Loading and validating pxGrid certificates, subscribing to pxGrid topics

## Verify

- Navigate to **System Settings > Settings > Authentication and Policy Servers**.
- ISE integration status would show as **Active**.

The screenshot shows the Catalyst Center web interface. The top navigation bar includes links for Home, System, Settings, Configuration Archive, External Services, Authentication and Policy Servers (which is the active tab), Integrity Verification, SD-Access Compatibility Matrix, IP Address Manager, Cloud Access Login, Cisco AI Analytics, Stealthwatch, Destinations, Cisco Spaces/CMX Servers, Global Manager Integration, and Machine Reasoning Engine. The search bar contains 'Search' and a placeholder 'Search'. The top right corner shows the user 'admin' and a blue profile icon.

The main content area is titled 'Authentication and Policy Servers'. It displays a table with one row of data:

| IP Address    | Protocol | Type | Status | Actions |
|---------------|----------|------|--------|---------|
| 10.127.196.71 | RADIUS   | ISE  | ACTIVE | ...     |

Below the table, a note states: 'Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.' There are 'Add' and 'Export' buttons at the top of the table, and a timestamp 'As of: Jun 4, 2025 9:21 PM' with a refresh icon.

Navigate to **Settings >System 360:**

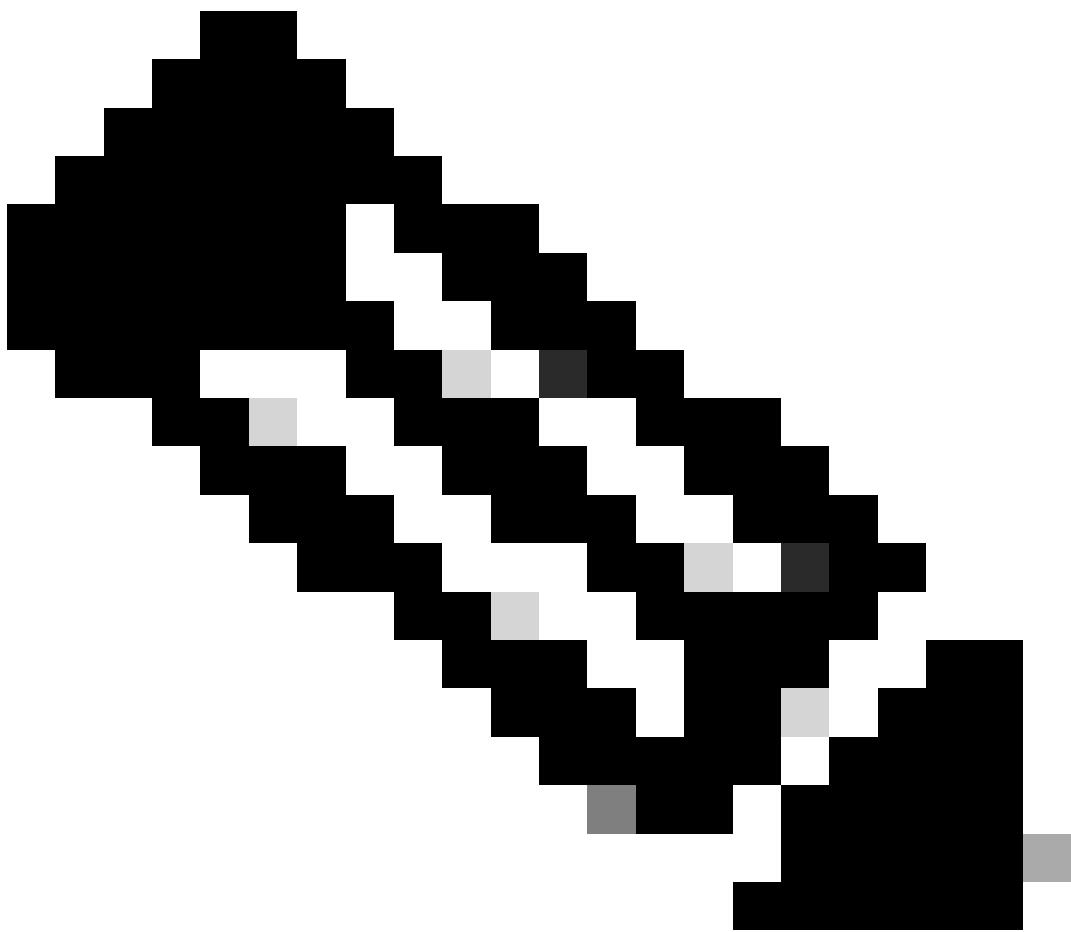
ISE servers show as **Available** under Externally Connected Systems as shown:

The screenshot shows the Catalyst Center System 360 interface. At the top, there are three main sections: Software Management, Backups, and Application Health. In the Software Management section, there is a large blue circular icon. The Backups section shows a message: "No backups server configured" with a "Configure" link. The Application Health section shows two green dots labeled "Automation" and "Assurance". Below these sections, there is a heading "Externally Connected Systems" followed by two tables. The first table, "Identity Services Engine (ISE)", lists four entries: Primary (10.127.196.71), Secondary (10.127.196.73), pxGrid-Active (10.127.196.72), and pxGrid-Standby (10.127.196.74). All entries are marked as "Available" with a green circle icon and have a "Update" link next to them. The second table, "IP Address Manager (IPAM)", shows a message: "No IPAM server configured." with a "Configure" link.

## Troubleshoot

Set these components at debug level in ISE:

- **PxGrid**
- **Infrastructure**
- **Ers**



**Note:** Before you start Cisco DNA-ISE integration, tail the service logs with these commands:

The logs can be checked live on Cisco DNA CLI using these commands:

- **maglev\$ magctl service logs -rf ise-bridge**
- **maglev\$ magctl service logs -rf network-design -c network-design-service**

## Section A: Flow of Log Messages on Cisco DNA for a Successful Integration

Step 1: Fetching ISE Credentials.

```
2025/06/07 17:21:41 [DEBUG] PUT http://network-design-service.fusion.svc.cluster.local:32765/iseIntegrationStatus/Step
```

```
025-06-07 17:21:41,905 | INFO | messageListenerContainer-6 | | c.c.a.c.c.impl.AAARasClientImpl | AAARasClientImpl - create api. RBAC uuid - null | correlationId=1978f306-0857-467d-b974-6444a163f742
```

```
2025-06-07 17:21:41,917 | INFO | messageListenerContainer-6 | | c.c.a.c.s.trust.CiscoISEManager | -----  
----- | correlationId=1978f306-0857-
```

467d-b974-6444a163f742

2025-06-07 17:21:41,917 | INFO | eSSageListenerContainer-6 | | c.c.a.c.s.trust.CiscoISEManager | **Step: Fetching iseUsername, isePassword, iseHostIp, iseHostName, iseSshKey, apicEmIp, apicEmFqdn** | correlationId=1978f306-0857-467d-b974-6444a163f742

2025-06-07 17:21:41,917 | INFO | eSSageListenerContainer-6 | | c.c.a.c.s.trust.CiscoISEManager | -----  
----- | correlationId=1978f306-0857-467d-b974-6444a163f742

2025-06-07 17:21:41,917 | INFO | eSSageListenerContainer-6 | | c.c.a.c.s.trust.CiscoISEManager | Calling GO service for ISE trust CREATE | correlationId=1978f306-0857-467d-b974-6444a163f742

2025-06-07 17:21:41,917 | INFO | eSSageListenerContainer-6 | | c.c.a.c.s.u.GoTrustEstablishmentUtil | Building API payload to call GO service for CREATE request of ISE with ip: 10.127.196.71 and hostname: 1 | correlationId=1978f306-0857-467d-b974-6444a163f742

Step 2: Certificate error awaiting acceptance whether the certificate is self signed and not trusted.

06/07 17:21:42 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:21:42 [DEBUG] GET <https://10.127.196.71/admin/API/PKI/TrustCertificates>

2025/06/07 17:21:44 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/iseIntegrationStatus/Step>

2025-06-07 17:21:44,730 | INFO | qtp480903748-238 | | c.c.a.c.s.c.IseIntegrationStatusController | Update ISE integration status Step for the StepName =**INITIATE\_CONNECTION\_TO\_ISE** | correlationId=831c9c36-d534-415d-86d6-

2025-06-07 17:21:44,964 | ERROR | eSSageListenerContainer-6 | | c.c.a.c.s.h.CreateAaaMessageHandler | **Certificate waiting for user acceptance {}** | correlationId=1978f306-0857-467d-b974-6444a163f742

com.cisco.apicem.commonsettings.service.exception.CertificateWaitingUserAcceptanceException:  
{"i18n": {"code": "NCND80015"} }

at  
com.cisco.apicem.commonsettings.service.util.GoTrustEstablishmentUtil.callGoServiceForTrustProcessing(GoTrustProcessing)  
~[classes/:na]

at  
com.cisco.apicem.commonsettings.service.trust.CiscoISEManager.establishTrustWithPAN(CiscoISEManager.java:214)  
~[classes/:na]

at  
com.cisco.apicem.commonsettings.service.trust.CiscoISEManager.establishTrust(CiscoISEManager.java:184)  
~[classes/:na]

at  
com.cisco.apicem.commonsettings.service.handler.CreateAaaMessageHandler.handleRBACInvocation(CreateAaaMessageHandler)  
~[classes/:na]

at  
com.cisco.apicem.commonsettings.service.handler.CreateAaaMessageHandler.handleRBACInvocation(CreateAaaMessageHandler)  
~[classes/:na]

at  
com.cisco.apicem.commonsettings.service.handler.CreateAaaMessageHandler.handleRequest(CreateAaaMessageHandler.java:11)  
~[classes/:na]

at  
com.cisco.grapevine.amqp.impl.GrapevineMessageListener.invokeHandler\_aroundBody0(GrapevineMessageListener.java:11)  
~[message-queue-sdk-7.0.722.60901.jar:7.0.722.60901]

at  
com.cisco.grapevine.amqp.impl.GrapevineMessageListener\$AjcClosure1.run(GrapevineMessageListener.java:1)  
~[message-queue-sdk-7.0.722.60901.jar:7.0.722.60901]

at org.aspectj.runtime.reflect.JoinPointImpl.proceed(JoinPointImpl.java:167) ~[aspectjrt-1.9.6.jar:na]

at  
com.cisco.enc.i18n.localization.aop.EnableI18nOnRequestHandler.getEmptyResponse(EnableI18nOnRequestHandler.java:11)  
~[i18n-7.1.722.60901.jar:7.1.722.60901]

at  
com.cisco.grapevine.amqp.impl.GrapevineMessageListener.invokeHandler(GrapevineMessageListener.java:452)  
~[message-queue-sdk-7.0.722.60901.jar:7.0.722.60901]

at  
com.cisco.grapevine.amqp.impl.GrapevineMessageListener.onMessage(GrapevineMessageListener.java:273)  
~[message-queue-sdk-7.0.722.60901.jar:7.0.722.60901]

at  
org.springframework.amqp.rabbit.listener.AbstractMessageListenerContainer.doInvokeListener(AbstractMessageListenerContainer.java:511)  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.AbstractMessageListenerContainer.invokeListener(AbstractMessageListenerContainer.java:491)  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.SimpleMessageListenerContainer.access\$001(SimpleMessageListenerContainer.java:40)  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.SimpleMessageListenerContainer\$1.invokeListener(SimpleMessageListenerContainer.java:111)  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.SimpleMessageListenerContainer.invokeListener(SimpleMessageListenerContainer.java:101)  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.AbstractMessageListenerContainer.executeListener(AbstractMessageListenerContainer.java:461)  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.SimpleMessageListenerContainer.doReceiveAndExecute(SimpleMessageListenerContainer.java:141)  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at

org.springframework.amqp.rabbit.listener.SimpleMessageListenerContainer.receiveAndExecute(SimpleMessageLister  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.SimpleMessageListenerContainer.access\$1800(SimpleMessageListenerCo  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at  
org.springframework.amqp.rabbit.listener.SimpleMessageListenerContainer\$AsyncMessageProcessingConsumer.ru  
~[spring-rabbit-1.7.15.RELEASE.jar:na]

at java.base/java.lang.Thread.run(Thread.java:834) ~[na:na]

2025-06-07 17:21:46,284 | INFO | qtp480903748-916 | | c.c.a.c.s.util.CommonSettingsUtil | Retrieved  
DB value for MultiCisco DNAConfigurationTable = MultiCisco  
DNAConfigurationTable[clusterUuid=878771ce-8f93-44a5-82c9-3561e14c2d77,createTime=2024-08-23  
14:18:11.381,inMultiCisco DNAMode=false,lastUpdatedTime=2024-08-23 14:18:11.381,multiCisco  
DNAFeatureEnabled=false,instanceUuid=7f606daa-ca05-472b-b45c-  
fe8dfdead1717,instanceId=7007,authEntityId=7007,authEntityClass=1586401731,instanceTenantId=66c88fc4104bfb  
| correlationId=5888c4bb-f407-4771-97e6-e5c9a9e08746

Step 3: Certificate acceptance invoked.

17:22:05,574 | INFO | qtp480903748-909 | | c.c.a.c.s.controller.AAAController | **Incoming Cert  
Accepted by user?: true** | correlationId=8b73524a-a3b1-4ebd-9d3a-b70830d64c83

2025-06-07 17:22:05,581 | INFO | eassengerListenerContainer-9 | | c.c.a.c.s.h.CreateAaaMessageHandler |  
**Entering user cert acknowledgment phase** | correlationId=8b73524a-a3b1-4ebd-9d3a-b70830d64c83

2025-06-07 17:22:05,605 | INFO | eassengerListenerContainer-9 | | c.c.a.c.s.trust.CiscoISEManager | -----  
----- | correlationId=8b73524a-a3b1-  
4ebd-9d3a-b70830d64c83

2025-06-07 17:22:05,605 | INFO | eassengerListenerContainer-9 | | c.c.a.c.s.trust.CiscoISEManager | **Step:  
Fetching iseUsername, isePassword, iseHostIp, iseHostName, iseSshKey, apicEmIp, apicEmFqdn** |  
correlationId=8b73524a-a3b1-4ebd-9d3a-b70830d64c83

2025-06-07 17:22:05,605 | INFO | eassengerListenerContainer-9 | | c.c.a.c.s.trust.CiscoISEManager | -----  
----- | correlationId=8b73524a-a3b1-  
4ebd-9d3a-b70830d64c83

2025-06-07 17:22:05,605 | INFO | eassengerListenerContainer-9 | | c.c.a.c.s.trust.CiscoISEManager | **Calling  
GO service for ISE trust CERT\_ACCEPT** | correlationId=8b73524a-a3b1-4ebd-9d3a-b70830d64c83

2025-06-07 17:22:05,605 | INFO | eassengerListenerContainer-9 | | c.c.a.c.s.u.GoTrustEstablishmentUtil |  
Building API payload to call GO service for **CERT\_ACCEPT request of ISE with ip: 10.127.196.71 and  
hostname:** | correlationId=8b73524a-a3b1-4ebd-9d3a-b70830d64c83

Step 4: Building Trust.

2025-06-07 17:22:06,365 | INFO | qtp480903748-246 | | c.c.a.c.s.c.IseIntegrationStatusController |  
Update ISE integration status Step for the StepName =**INITIATE\_CONNECTION\_TO\_ISE** |  
correlationId=c1bfde32-4cec-4c9f-afab-06291f1bc437

2025-06-07 17:22:06,375 | INFO | qtp480903748-909 | | c.c.a.c.s.c.IseIntegrationStatusController |  
Update ISE integration status Step for the StepName =**ESTABLISHING\_TRUST\_WITH\_ISE** |

correlationId=fbba646c-bdae-4554-8c70-0a5836f4c860

Step 5: Checking ISE ERS config.

2025/06/07 17:22:06 [DEBUG] GET <https://10.127.196.71/admin/API/NetworkAccessConfig/ERS>

```
{"asctime":"2025-06-07T17:22:07.529Z","correlationId":"","level":"info","msg":"Current ERS config on ISE {XMLName:{Space: Local:ersConfig} ID:1 ISCSR: false IsPAP: true IsPSNS: true}","packagename":"ISE Connection Manager"}
```

Step 6: Validating ISE version.

2025/06/07 17:22:07 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:07 [DEBUG] GET <https://10.127.196.71:9060/ers/config/op/systemconfig/iseverSION>

```
{"asctime":"2025-06-07T17:22:09.065Z","correlationId":"","level":"info","msg":"ISE version is Version:3.3 Patch:0 PatchList:0","packagename":"ISE Connection Manager"}
```

Step 7: Fetching telemetry info.

2025/06/07 17:22:09 [DEBUG] GET <https://10.127.196.71:9060/ers/config/telemetryinfo>

```
{"asctime":"2025-06-07T17:22:10.161Z","correlationId":"","level":"info","msg":"Telemetry ID 30d43265-1577-4e02-a10b-6b549099f544","packagename":"Utilities"}
```

```
{"asctime":"2025-06-07T17:22:10.161Z","correlationId":"","level":"info","msg":"Check and enable openAPI on ISE nodes","packagename":"ISE Connection Manager"}
```

Step 8: Fetching API status from ISE.

2025/06/07 17:22:10 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:10 [DEBUG] GET <https://10.127.196.71/admin/API/apiService/get>

```
{"asctime":"2025-06-07T17:22:11.291Z","correlationId":"","level":"info","msg":"OpenAPI is already enabled, {true true}","packagename":"ISE Connection Manager"}
```

Step 9: Trust establishment with ISE completed.

```
{"asctime":"2025-06-07T17:22:11.291Z","correlationId":"","level":"info","msg":"Updating overall status to trusted","packagename":"ISE Connection Manager"}
```

2025/06/07 17:22:11 [DEBUG] GET <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo/b745dd4f-2a22-47d8-a216-6a5a85f3ea69>

```
{"asctime":"2025-06-07T17:22:11.304Z","correlationId":"","level":"info","msg":"Sending node status update to NDS. Payload {\\"aaaServerId\\":\"b745dd4f-2a22-47d8-a216-6a5a85f3ea69\",\\\"ciscoIseList\\\":[{\\\"ciscoIseId\\\":\\\"acc84e0a-cfdb-48a4-2f56eafe5490\\\",\\\"description\\\":\\\"\\\",\\\"failureReason\\\":\\\"\\\",\\\"fqdn\\\":\\\"\\\",\\\"ipAddress\\\":\\\"10.127.196.71\\\",\\\"op
```

2025/06/07 17:22:11 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo>

```
{"asctime":"2025-06-07T17:22:11.319Z","correlationId":"","level":"info","msg":"Node update status to NDS, response code 200 OK","packagename":"ndsutil"}
```

```
{"asctime":"2025-06-07T17:22:11.319Z","correlationId":"","level":"info","msg":"Sending certificates to NDS","packagename":"ISE Connection Manager"}
```

```
{"asctime":"2025-06-07T17:22:11.319Z","correlationId":"","level":"info","msg":"Adding {17487437175958362366089997042 CREATE}","packagename":"ndsutil"}
```

```
{"asctime":"2025-06-07T17:22:11.319Z","correlationId":"","level":"info","msg":"Sending node status update to NDS. Payload [{"\serialNumber": "17487437175958362366089997042", "\issuer": "CN=l", "\operationType": "CREATE"}]},"packagename":"ndsutil"}
```

2025/06/07 17:22:11 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo/iseCerts>

```
{"asctime":"2025-06-07T17:22:11.329Z","correlationId":"","level":"info","msg":"Node update status to NDS, response code 200 OK","packagename":"ndsutil"}
```

```
{"asctime":"2025-06-07T17:22:11.329Z","correlationId":"","level":"info","msg":"Updating ISE Step ESTABLISHING_TRUST_WITH_ISE with status COMPLETE","packagename":"ndsutil"}
```

```
{"asctime":"2025-06-07T17:22:11.329Z","correlationId":"","level":"info","msg":"Sending request to NDS {"StepName": "ESTABLISHING_TRUST_WITH_ISE", "StepStatus": "COMPLETE"}","packagename":"nd
```

2025/06/07 17:22:11 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/iseIntegrationStatus/Step>

Step 10: Discovery of nodes in ISE deployment.

```
{"asctime":"2025-06-07T17:22:11.339Z","correlationId":"","level":"info","msg":"Updating ISE Step DISCOVERING_NODES with status IN_PROGRESS","packagename":"ndsutil"}
```

```
{"asctime":"2025-06-07T17:22:11.339Z","correlationId":"","level":"info","msg":"Sending request to NDS {"StepName": "DISCOVERING_NODES", "StepStatus": "IN_PROGRESS"}","packagename":"ndsutil"}
```

2025/06/07 17:22:11 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/iseIntegrationStatus/Step>

```
{"asctime":"2025-06-07T17:22:11.348Z","correlationId":"","level":"info","msg":"Posted ISE integration Step to NDS, http response code=200","packagename":"ndsutil"}
```

2025/06/07 17:22:11 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:11 [DEBUG] GET <https://10.127.196.71/admin/API/Infra/Node/SimpleList>

```
{"asctime":"2025-06-07T17:22:12.512Z","correlationId":"","level":"info","msg":"66c88fc4104bfb741d052de9:b745dd4f-2a22-47d8-a216-6a5a85f3ea69 Received 4 nodes from ISE","packagename":"ISE Connection Manager"}
```

```
{"asctime":"2025-06-07T17:22:12.512Z","correlationId":"","level":"info","msg":"Adding Primary PAN node localise33ppan/10.127.196.71, role PRIMARY","packagename":"ISE Connection Manager"}
```

de localise33ppan/10.127.196.71, role PRIMARY","packagename":"ISE Connection Manager"}

2025/06/07 17:22:12 [DEBUG] **POST** <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:12 [DEBUG] **GET** <https://10.127.196.71:9060/ers/config/node/name/ise33localspan>

{"asctime":"2025-06-07T17:22:13.612Z","correlationId":"","level":"info","msg":"**Adding Secondary PAN node i**"}

{"asctime":"2025-06-07T17:22:13.612Z","correlationId":"","level":"info","msg":"**Adding MnT primary node**"}

2025/06/07 17:22:13 [DEBUG] **POST** <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:13 [DEBUG] **GET** <https://10.127.196.71:9060/ers/config/node/name/ise33seclocal>

{"asctime":"2025-06-07T17:22:14.737Z","correlationId":"","level":"info","msg":"Adding pxgrid node"

2025/06/07 17:22:14 [DEBUG] **POST** <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:14 [DEBUG] **GET** <https://10.127.196.71:9060/ers/config/node/name/isepxgrid2025>

{"asctime":"2025-06-07T17:22:15.863Z","correlationId":"","level":"info","msg":"Adding PSN node isepxgrid2025.localad.com/10.127.196.74","packagename":"ISE Connection Manager"}

2025/06/07 17:22:15 [DEBUG] **POST** <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:15 [DEBUG] **GET** <https://10.127.196.71:9060/ers/config/node/name/localise33ppan>

{"asctime":"2025-06-07T17:22:17.047Z","correlationId":"","level":"info","msg":"**Adding PSN node I/10.127.196.71**","packagename":"ISE Connection Manager"}

Step 11: Discovery of nodes Completed.

2025/06/07 17:22:17 [DEBUG] **GET** <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo/b745dd4f-2a22-47d8-a216-6a5a85f3ea69>

{"asctime":"2025-06-07T17:22:17.843Z","correlationId":"","level":"info","msg":"Sending node status update to NDS. Payload {"aaaServerId":"b745dd4f-2a22-47d8-a216-6a5a85f3ea69","ciscoIseList":[{"ciscoIseId":"49523ddb-e1d5-c53d-1e20-01f8509a3c28","description":",","failureReason":",","fqdn":",","ipAddress":"10.127.196.73"},{"operationTy

2025/06/07 17:22:17 [DEBUG] **PUT** <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo>

{"asctime":"2025-06-07T17:22:17.860Z","correlationId":"","level":"info","msg":"**Node update status to NDS, response code 200 OK**","packagename":"ndsutil"}

{"asctime":"2025-06-07T17:22:17.860Z","correlationId":"","level":"info","msg":"**Updating ISE Step DISCOVERING\_NODES with status COMPLETE**","packagename":"ndsutil"}

{"asctime":"2025-06-07T17:22:17.860Z","correlationId":"","level":"info","msg":"**Sending request to NDS {"StepName":"DISCOVERING\_NODES","StepStatus":"COMPLETE"} , packagename: "ndsutil"}**"}

Step 12: Fetching of ISE Local certificates.

```
{"asctime":"2025-06-07T17:22:17.871Z","correlationId":"","level":"info","msg":"GetCertChainForISERole , role EAP and node l","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:17.871Z","correlationId":"","level":"info","msg":"Fetching local certificates from ISE 10.127.196.71","packagename":"Certificate Manager"}
```

2025/06/07 17:22:17 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:17 [DEBUG] GET <https://10.127.196.71/admin/API/PKI/LocalCertificates>

```
{"asctime":"2025-06-07T17:22:19.264Z","correlationId":"","level":"info","msg":"Building cert chain for leaf cert. Node=10.127.196.71;cname=","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:19.264Z","correlationId":"","level":"info","msg":"Certificate is self-signed. Subject=CN and Issuer=CN, skip cert chain build","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:19.264Z","correlationId":"","level":"info","msg":"Inserting into iseCerts","packagename":"DAL"}
```

```
{"asctime":"2025-06-07T17:22:19.276Z","correlationId":"","level":"info","msg":"Successfully inserted into iseCerts","packagename":"DAL"}
```

2025/06/07 17:22:19 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

Step 13: Pxgrid connection check.

```
{"asctime":"2025-06-07T17:22:19.336Z","correlationId":"","level":"info","msg":"PxGrid is enabled","packagename":"ISE Connection Manager"}
```

```
{"asctime":"2025-06-07T17:22:19.336Z","correlationId":"","level":"info","msg":"Updating ISE Step PXGRID_CONNECTION with status IN_PROGRESS","packagename":"ndsutil"}
```

```
{"asctime":"2025-06-07T17:22:19.336Z","correlationId":"","level":"info","msg":"Sending request to NDS {\\"StepName\\":\\"PXGRID_CONNECTION\\",\\"StepStatus\\":\\"IN_PROGRESS\\"}","packagename":"ndsutil"}
```

2025/06/07 17:22:19 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/iseIntegrationStatus/Step>

```
{"asctime":"2025-06-07T17:22:19.349Z","correlationId":"","level":"info","msg":"Posted ISE integration Step to NDS, http response code=200","packagename":"ndsutil"}
```

```
{"asctime":"2025-06-07T17:22:19.349Z","correlationId":"","level":"info","msg":"Fetching and building admin certificate chain for node 10.127.196.72","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:19.349Z","correlationId":"","level":"info","msg":"Fetching server certificate for 10.127.196.72","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:20.907Z","correlationId":"","level":"info","msg":"fetched server cert chain for 10.127.196.72, chain length 4","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:20.907Z","correlationId":"","level":"info","msg":"Check if peer has
```

```

provided complete certificate chain, chain length=4","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:20.907Z","correlationId":"","level":"info","msg":"Build/update cert-chain for Node=10.127.196.72;cname=","packagename":"Certificate Manager"}
```

```
{"asctime":"2025-06-07T17:22:20.907Z","correlationId":"","level":"info","msg":"Inserting to ise-bridge certpool. Issuer=CN=Certificate Services Node CA - localise33ppan; Subject=CN=Certificate Services Endpoint Sub CA - ise33seclocal; Serial Number=336164adf99b4663b51c7d8787b671e2","packagename":"Certificate Manager"}
```

2025/06/07 17:22:20 [DEBUG] GET <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo/b745dd4f-2a22-47d8-a216-6a5a85f3ea69>

```
{"asctime":"2025-06-07T17:22:20.920Z","correlationId":"","level":"info","msg":"Sending node status update to NDS. Payload {"aaaServerId":\\"b745dd4f-2a22-47d8-a216-6a5a85f3ea69\\","ciscoIseList": [{"ciscoIseId":\\"dad546ca-fe8f-28d9-a112-56ecade00239\\","description":\\"\\","failureReason":\\"\\","fqdn":\\"\\","ipAddress":\\"10.127.196.72\\","operationT
```

2025/06/07 17:22:20 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo>

```
{"asctime":"2025-06-07T17:22:20.936Z","correlationId":"","level":"info","msg":"Node update status to NDS, response code 200 OK","packagename":"ndsutil"}
```

Step 14: Certificate update.

```
{"asctime":"2025-06-07T17:22:22.585Z","correlationId":"","level":"info","msg":"Fetch endpoint certs from ISE , \u0026{CertTemplateName:pxGrid_Certificate_Template Format:PKCS8_CHAIN Password: CertificateRequest:{San:52:ad:88:67:42:58 Cn:admin_66c88fc4104bfb741d052de9}}","packagename":"PxGridClient"}
```

2025/06/07 17:22:22 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

2025/06/07 17:22:22 [DEBUG] PUT <https://10.127.196.71:9060/ers/config/endpointcert/certRequest>

```
{"asctime":"2025-06-07T17:22:24.071Z","correlationId":"","level":"info","msg":"Inserting into iseCerts","packagename":"DAL"}
```

```
{"asctime":"2025-06-07T17:22:24.072Z","correlationId":"","level":"info","msg":"Successfully inserted into iseCerts","packagename":"DAL"}
```

Step 15: Pxgrid Client activation.

```
{"asctime":"2025-06-07T17:22:24.074Z","correlationId":"","level":"info","msg":"Successfully loaded privateKey from endpoint certs","packagename":"PxGridClient"}
```

```
{"asctime":"2025-06-07T17:22:24.074Z","correlationId":"","level":"info","msg":"Number of cert entries in client cert chain 1","packagename":"PxGridClient"}
```

2025/06/07 17:22:24 [DEBUG] POST <https://10.127.196.72:8910/pxgrid/control/AccountActivate>

```
{"asctime":"2025-06-07T17:22:25.247Z","correlationId":"","level":"info","msg":"Got Response 200 , for URL https://10.127.196.72:8910/pxgrid/control/AccountActivate","packagename":"PxGridClient"}
```

```
{"asctime":"2025-06-07T17:22:25.247Z","correlationId":"","level":"info","msg":"GOT ACCOUNT
```

**ACTIVATE RESPONSE: \u0026{AccountState:ENABLED  
Version:2.0}","packagename":"PxGridClient"}**

2025/06/07 17:22:25 [DEBUG] POST <https://10.127.196.72:8910/pxgrid/control/ServiceLookup>

{"asctime":"2025-06-07T17:22:26.311Z","correlationId":"","level":"info","msg":"**Got Response 200 , for URL https://10.127.196.72:8910/pxgrid/control/ServiceLookup**","packagename":"PxGridClient"}

{"asctime":"2025-06-07T17:22:26.311Z","correlationId":"","level":"info","msg":"Try to connect pubsub service \u0026{Name:com.cisco.ise.pubsub NodeName:~ise-pubsub-ise33seclocal Properties:map[wsUrl:wss://:8910/pxgrid/ise/pubsub]}","packagename":"PxGridClient"}

{"asctime":"2025-06-07T17:22:26.311Z","correlationId":"","level":"info","msg":"**ISE Pubsub Web Service URL: wss://10.127.196.72:8910/pxgrid/ise/pubsub**","packagename":"PxGridClient"}

2025/06/07 17:22:26 [DEBUG] POST <https://10.127.196.72:8910/pxgrid/control/AccessSecret>

{"asctime":"2025-06-07T17:22:27.461Z","correlationId":"","level":"info","msg":"**Got Response 200 , for URL https://10.127.196.72:8910/pxgrid/control/AccessSecret**","packagename":"PxGridClient"}

{"asctime":"2025-06-07T17:22:27.461Z","correlationId":"","level":"info","msg":"Trying to dial to wsurl wss://10.127.196.72:8910/pxgrid/ise/pubsub","packagename":"ws-endpoint"}

{"asctime":"2025-06-07T17:22:28.479Z","correlationId":"","level":"info","msg":"**Connected to wss://10.127.196.72:8910/pxgrid/ise/pubsub successfully**","packagename":"ws-endpoint"}

2025/06/07 17:22:28 [DEBUG] POST <https://credentialmanager.maglev-system.svc.cluster.local:443/api/v1/credentialmanager/decryption>

{"asctime":"2025-06-07T17:22:28.479Z","correlationId":"","level":"info","msg":"**Setting as active pxgrid node**","packagename":"PxGridClient"}

{"asctime":"2025-06-07T17:22:28.533Z","correlationId":"","level":"info","msg":"**Updating ISE Step PXGRID\_CONNECTION with status COMPLETE**","packagename":"ndsutil"}

{"asctime":"2025-06-07T17:22:28.533Z","correlationId":"","level":"info","msg":"Sending request to NDS {\\"StepName\\":\\"PXGRID\_CONNECTION\\",\\"StepStatus\\":\\"COMPLETE\\"}","packagename":"ndsutil"}

2025/06/07 17:22:28 [DEBUG] PUT <http://network-design-service.fusion.svc.cluster.local:32765/iseIntegrationStatus/Step>

2025/06/07 17:22:28 [DEBUG] GET <http://network-design-service.fusion.svc.cluster.local:32765/aaaStatusInfo/b745dd4f-2a22-47d8-a216-6a5a85f3ea69>

Step 16: Trustsec SGT download.

{"asctime":"2025-06-07T17:22:34.370Z","correlationId":"","level":"info","msg":"**BULK DOWNLOADING FOR SERVICE com.cisco.ise.config.trustsec TOPIC securityGroupTopic**","packagename":"PxGridClient"}

{"asctime":"2025-06-07T17:22:34.371Z","correlationId":"","level":"info","msg":"**Bulkdownload URLs: [https://10.127.196.71:8910/pxgrid/ise/config/trustsec]**","packagename":"PxGridClient"}

{"asctime":"2025-06-07T17:22:34.371Z","correlationId":"","level":"info","msg":"**Trying bulk download of com.cisco.ise.config.trustsec using**

<https://10.127.196.71:8910/pxgrid/ise/config/trustsec/getSecurityGroups>","packagename":"PxGridClient"}

2025/06/07 17:22:34 [DEBUG] **POST**

<https://10.127.196.71:8910/pxgrid/ise/config/trustsec/getSecurityGroups>

{"asctime":"2025-06-07T17:22:35.424Z","correlationId":"","level":"info","msg":"Got Response 200 , for URL

<https://10.127.196.71:8910/pxgrid/ise/config/trustsec/getSecurityGroups>","packagename":"PxGridClient"}

{"asctime":"2025-06-07T17:22:35.424Z","correlationId":"","level":"info","msg":"**Reset Security Group Cache.**","packagename":"cache"}

{"asctime":"2025-06-07T17:22:35.424Z","correlationId":"","level":"info","msg":"**Updating Security Group Cache**","packagename":"cache"}

{"asctime":"2025-06-07T17:22:35.424Z","correlationId":"","level":"info","msg":"**SG bulkdownload data, ACA is not registered for it yet, dont push to RMQ**","packagename":"Subscribers"}

{"asctime":"2025-06-07T17:22:35.424Z","correlationId":"","level":"info","msg":"**Done subscribing to all the topics and completed bulk downloads**","packagename":"ISE Connection Manager"}

## Section B: Flow of Log Messages on ISE (ISE PSC log)

Step 1: Fetching node details.

2025-06-07 22:45:22,788 INFO [ers-http-pool15][] cpm.ers.app.web.BasicAndTokenAuthenticator -::::- **Basic authentication successful. User: admin**

2025-06-07 22:45:22,788 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getPathInfo=/node

2025-06-07 22:45:22,788 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getMethod=GET

2025-06-07 22:45:22,788 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> **getRequestURL=https://ise-bridge.ise-bridge.svc.cluster.local:8080/ers/config/node**

2025-06-07 22:45:22,788 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> **getRemoteHost=10.62.113.211**

2025-06-07 22:45:22,788 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> **getLocalPort=9060**

2:45:22,794 DEBUG [ers-http-pool15][] ers.app.impl.handlers.NodeCRUDHandler -::::- DEBUG INFO --- RESULT com.cisco.cpm.ers.app.proxy.HostConfigProxy@2ff9a8ef

2025-06-07 22:45:22,794 DEBUG [ers-http-pool15][] ers.app.impl.handlers.NodeCRUDHandler -::::- DEBUG INFO --- RESULT com.cisco.cpm.ers.app.proxy.HostConfigProxy@39c857df

2025-06-07 22:45:22,794 DEBUG [ers-http-pool15][] ers.app.impl.handlers.NodeCRUDHandler -::::- DEBUG INFO --- RESULT com.cisco.cpm.ers.app.proxy.HostConfigProxy@24e4889c

2025-06-07 22:45:22,794 DEBUG [ers-http-pool15][] ers.app.impl.handlers.NodeCRUDHandler -::::- DEBUG INFO --- RESULT com.cisco.cpm.ers.app.proxy.HostConfigProxy@73eb7edf

2025-06-07 22:45:22,802 INFO [ers-http-pool15][] cisco.cpm.ers.fw.CRUDService -::::- **The GET ALL resources request for resource type 'node' Completed Successfully**

Step 2: Version check on ISE.

2025-06-07 22:48:39,847 INFO [ers-http-pool15][] cpm.ers.app.web.BasicAndTokenAuthenticator -::::- Basic authentication successful. User: admin

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.CertificateAuthenticator -::::- Authentication is password based, skipping certificate-based authentication

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getPathInfo=/op/systemconfig/iseversion

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getMethod=GET

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter -->

**getRequestURL**=<https://10.127.196.71:9060/ers/config/op/systemconfig/iseversion>

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getRemoteHost=10.62.113.211

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getLocalPort=9060

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ## RateLimitFilter Servlet => Continue with the ERS Request, The current bucket count is: 49

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> getPathInfo=/op/systemconfig/iseversion

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> getMethod=GET

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> **getRequestURL**=<https://10.127.196.71:9060/ers/config/op/systemconfig/iseversion>

2025-06-07 22:48:39,848 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> getRemoteHost=10.62.113.211

2025-06-07 22:48:39,849 DEBUG [ers-http-pool15][] cpm.ers.app.web.PAPFilter -::::- ##### PAPFilter.doFilter --> **getPathInfo**=/op/systemconfig/iseversion

2025-06-07 22:48:39,849 DEBUG [ers-http-pool15][] cpm.ers.app.web.PAPFilter -::::- ##### PAPFilter.doFilter --> getMethod=GET

2025-06-07 22:48:39,849 DEBUG [ers-http-pool15][] cpm.ers.app.web.PAPFilter -::::- ##### PAPFilter.doFilter --> **getRequestURL**=<https://10.127.196.71:9060/ers/config/op/systemconfig/iseversion>

2025-06-07 22:48:39,849 DEBUG [ers-http-pool15][] cpm.ers.app.web.PAPFilter -::::- ##### PAPFilter.doFilter --> getRemoteHost=10.62.113.211

Step 3: Fetching telemetry info.

2025-06-07 22:48:41,371 INFO [ers-http-pool15][] cpm.ers.app.web.BasicAndTokenAuthenticator -::::- Basic authentication successful. User: admin

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.CertificateAuthenticator -::::- Authentication is password based, skipping certificate-based authentication

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getPathInfo=/telemetryinfo

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getMethod=GET

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> **getRequestURL**=<https://10.127.196.71:9060/ers/config/telemetryinfo>

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getRemoteHost=10.62.113.211

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getLocalPort=9060

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ## RateLimitFilter Servlet => Continue with the ERS Request, The current bucket count is: 49

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> getPathInfo=/telemetryinfo

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> getMethod=GET

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> **getRequestURL**=<https://10.127.196.71:9060/ers/config/telemetryinfo>

2025-06-07 22:48:41,371 DEBUG [ers-http-pool15][] cpm.ers.app.web.PICFilter -::::- ##### PICFilter.doFilter --> getRemoteHost=10.62.113.211

2025-06-07 22:48:41,372 DEBUG [ers-http-pool15][] cpm.ers.app.web.PAPFilter -::::- ##### PAPFilter.doFilter --> getPathInfo=/telemetryinfo

2025-06-07 22:48:41,374 INFO [ers-http-pool15][] ers.app.impl.handlers.TelemetryInfoCRUDHandler - ::::- Within GET ALL API

2025-06-07 22:48:41,377 INFO [ers-http-pool15][] cisco.cpm.ers.fw.CRUDService -::::- **The GET ALL resources request for resource type 'telemetryinfo' Completed Successfully**

Step 4: REST based requests are used by ISE to fetch information in the integration.

2025-06-07 22:49:00,957 INFO [ers-http-pool18][] cpm.ers.app.web.BasicAndTokenAuthenticator -::::- Basic authentication successful. User: admin

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getPathInfo=/sessionservicenode

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> getMethod=GET

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.MaxThreadsLimiterFilter -::::- ##### MaxThreadsFilter.doFilter --> **getRequestURL**=<https://ise-bridge.ise-bridge.svc.cluster.local:8080/ers/config/sessionservicenode>

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.MaxThreadsLimiterFilter -:::::-  
#### MaxThreadsFilter.doFilter --> getRemoteHost=10.62.113.211

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.MaxThreadsLimiterFilter -:::::-  
#### MaxThreadsFilter.doFilter --> getLocalPort=9060

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.MaxThreadsLimiterFilter -:::::-  
## RateLimitFilter Servlet => Continue with the ERS Request, The current bucket count is: 49

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.PICFilter -::::- ####  
PICFilter.doFilter --> getPathInfo=/sessionservicenode

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.PICFilter -::::- ####  
PICFilter.doFilter --> getMethod=GET

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.PICFilter -::::- ####  
PICFilter.doFilter --> **getRequestURL**=<https://ise-bridge.ise-bridge.svc.cluster.local:8080/ers/config/sessionservicenode>

2025-06-07 22:49:00,957 DEBUG [ers-http-pool18][] cpm.ers.app.web.PICFilter -::::- ####  
PICFilter.doFilter --> getRemoteHost=10.62.113.211