Troubleshoot Secure Network Analytics (SNA) - Identity Services Engine (ISE) Integration "Connection Failed - Service Cannot Be Found On This ISE Cluster"

Contents

Introduction

This document describes how to validate ISE integration issues for SMC version 7.3.2 onwards. SNA introduces PxGrid v2.0 for the ISE integration component with release 7.3.2. This article focuses on some specific error messages that you can come across when you configure your Cisco ISE Integration on releases 7.3.2 and onward.

For more details about PxGrid v2.0 and it's functionality, please visit - [PxGrid v2.0](#)

Cisco ISE Integration

When SMC integrates with ISE, it makes a request to subscribe to the appropriate service based on the checkboxes selected in the configuration UI -

Integration options ⓘ

Integrated Product ⓘ

◉ Cisco ISE

◎ Cisco ISE PIC (Passive Identity Connector)

☑ Adaptive Network Control ⓘ

☑ Static SGT Classifications ⓘ

☑ Sessions ⓘ

  ☐ Track sessions derived from machine authentications ⓘ

ISE Services

Based on the checkboxes selected, SMC can request -

Service: com.cisco.ise.config.anc

Service: com.cisco.ise.trustsec

**Service**: com.cisco.ise.session

Service: com.cisco.ise.pubsub

In turn for these services, SMC communicates with an ISE node to subscribe to the service. When SMC makes a request to the ISE node for a service, it expects to know what ISE nodes can serve that topic or service.

Potential Failure Reasons

- "Connection Status:Failed Service com.cisco.ise.pubsub cannot be found on this ISE Cluster"
- "Connection Status:Failed Service com.cisco.ise.anc cannot be found on this ISE cluster."
- "Connection Status:Failed Service com.cisco.ise.session cannot be found on this ISE cluster."
- "Connection Status:Failed Service com.cisco.ise.trustsec cannot be found on this ISE cluster."
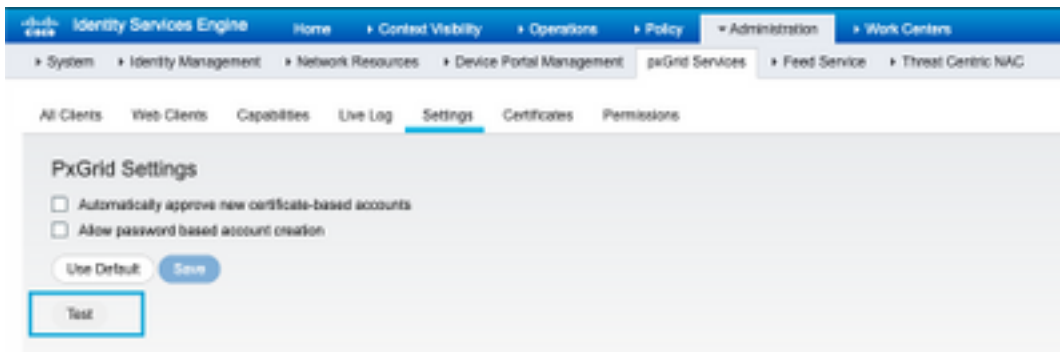
Verification and Troubleshooting

Navigate to **Administration > PxGrid Services > Diagnostics > Tests** and Run the Health Monitoring Test Tool (ISE 3.0 and onward)
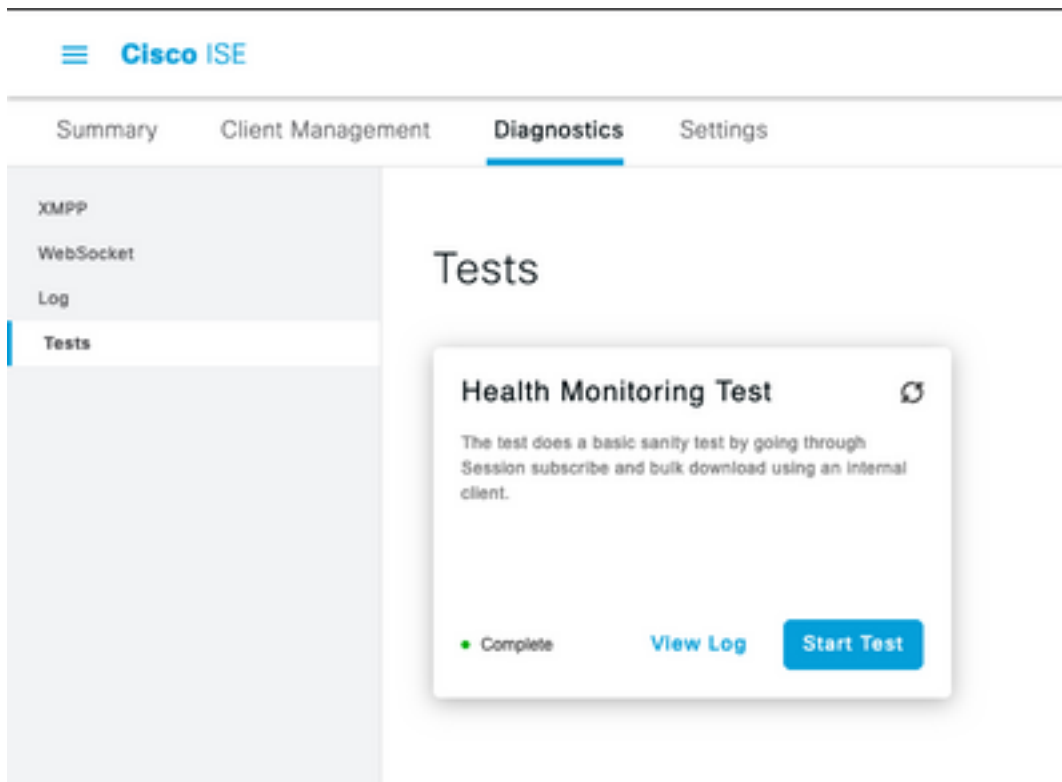
Health Monitoring Test Tool

For ISE 2.4, 2.6 and 2.7:

 Health Monitoring Test
Tool

The results of the test is available to view in the CLI of the PXGrid node indicated in the footer of the page noting Connected via XMPP <hostname>.

Run the command "**show logging application pxgrid/pxgrid-test.log**"

The output when connected and successful indicates:

asc-ise24p12-347/admin# **show logging application pxgrid/pxgrid-test.log**
2021-10-29 01:46:32 INFO TestGridConnection:55 - Starting pxgrid test conenction.........
2021-10-29 01:46:33 INFO TestGridConnectionHelper:307 - SUMMARY>
Subscribe=CONNECTING,session-cnt=0; BulkDownload=NOT STARTED,bd-session-cnt=0
2021-10-29 01:46:33 INFO Configuration:313 - Connecting to host asc-ise24p12-347.rtpaaa.net
2021-10-29 01:46:33 INFO Configuration:318 - **Connected OK** to host asc-ise24p12-347.rtpaaa.net
2021-10-29 01:46:33 INFO Configuration:343 - Client Login to host asc-ise24p12-347.rtpaaa.net
2021-10-29 01:46:34 INFO Configuration:345 - **Client Login OK** to host asc-ise24p12-347.rtpaaa.net
2021-10-29 01:46:35 INFO NotificationHandlerSmack:70 - done refreshing connection state.
2021-10-29 01:46:35 INFO TestGridConnectionHelper:312 - SUMMARY>
Subscribe=CONNECTED,session-cnt=0; BulkDownload=NOT STARTED,bd-session-cnt=0
2021-10-29 01:50:36 INFO TestGridConnection:164 - SUMMARY>
Subscribe=CONNECTED,session-cnt=0;**BulkDownload=SUCCESS**,bd-session-cnt=0
2021-10-29 01:50:36 INFO NotificationHandlerSmack:81 - cleared connection state...
2021-10-29 01:50:36 INFO TestGridConnectionHelper:322 - Client disconnected
2021-10-29 01:50:36 INFO TestGridConnection:75 - SUMMARY>
Subscribe=DISCONNECTED,session-cnt=0;BulkDownload=DISCONNECTED,bd-session-cnt=0

Verify if the account used to connect SMC to ISE is enabled:

Verify that the client is approved and if it is pending, approve the client
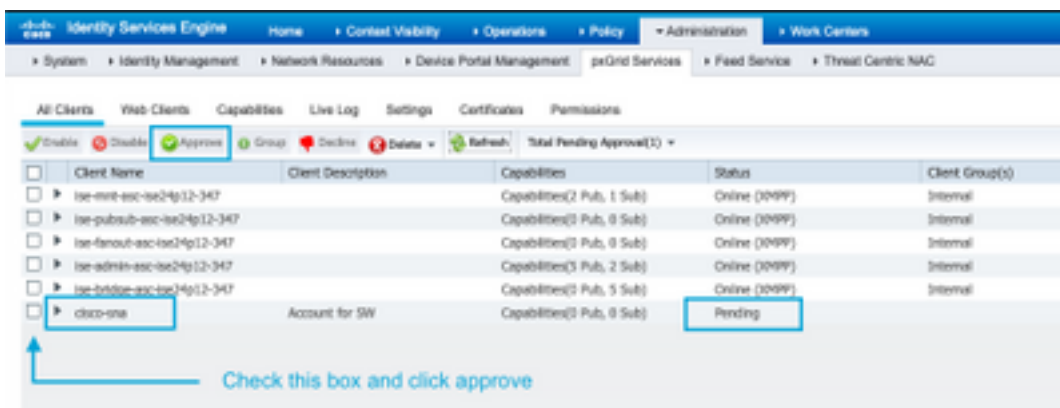
ISE 3.0 and onward:

Administration > PxGrid Services > Client Management > Clients:
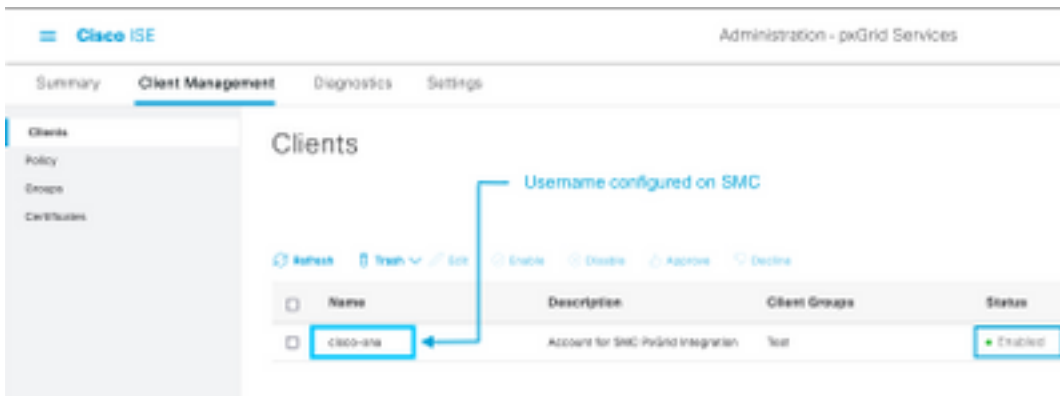
ISE 2.4, 2.6 and 2.7:

Administration > PxGrid Services > All Clients

To check the connection status of the SMC PxGrid client and which ISE node it is connected to, Navigate to **Administration > PxGrid Services > Diagnostics > WebSocket**

Known Causes

- Nodes with PxGrid Persona enabled facing replication issues within the ISE deployment
- PxGrid Certificate Trust issues

Replication issues on ISE deployment

Replication is critical to maintaining up to date information on all member nodes in a deployment. If a node running the PxGrid persona is reporting replication issues, it is possible it does not have up to date information about the topics and services it can serve for PxGrid clients.

If the node is reporting replication failure alarms or slow replication:

Replication Failed

OR

Slow Replication Error

This is a potential cause for the integration failure.

To take corrective action -

Verify IP connectivity with the ISE node, log in via SSH and verify that services are running by issuing:

> # show application status ise

Eg.

asc-ise30p2-353/admin# **show application status ise**

ISE PROCESS NAME STATE PROCESS ID

Database Listener running 24872
Database Server running 114 PROCESSES
Application Server running **40137**
Profiler Database running 35916
ISE Indexing Engine disabled
AD Connector running 40746
M&T Session Database disabled
M&T Log Processor disabled
Certificate Authority Service running 40609
EST Service running 77903
SXP Engine Service disabled
Docker Daemon running 28517
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 29277

ISE API Gateway Database Service running 32173
ISE API Gateway Service running 38161
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled

Perform manual sync of the affected node under **Administration > System > Deployment**

Select the node reporting issues and click **Syncup**
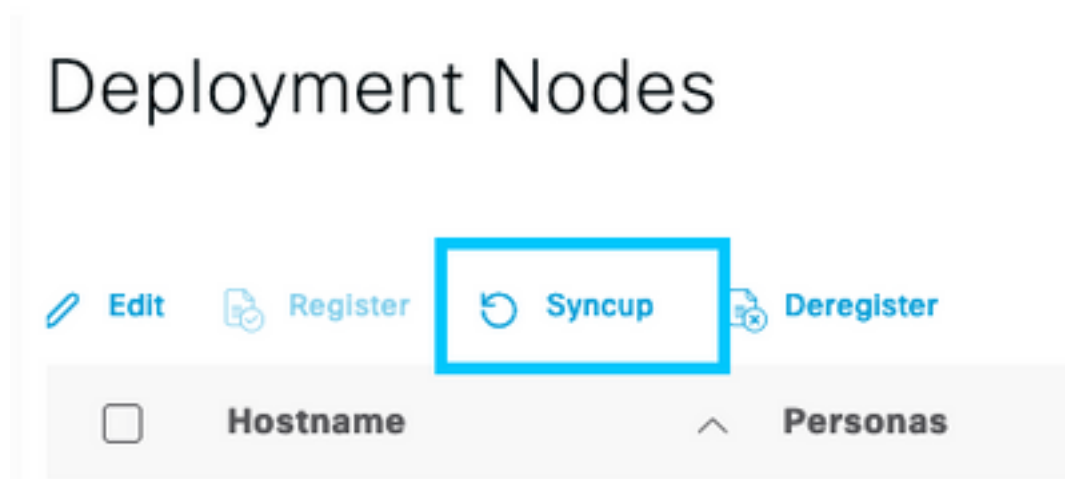
Note: This results in a restart of services on the node being synced and could render the node out of service for 30 min. This activity is recommended to be be performed in a controlled change window.

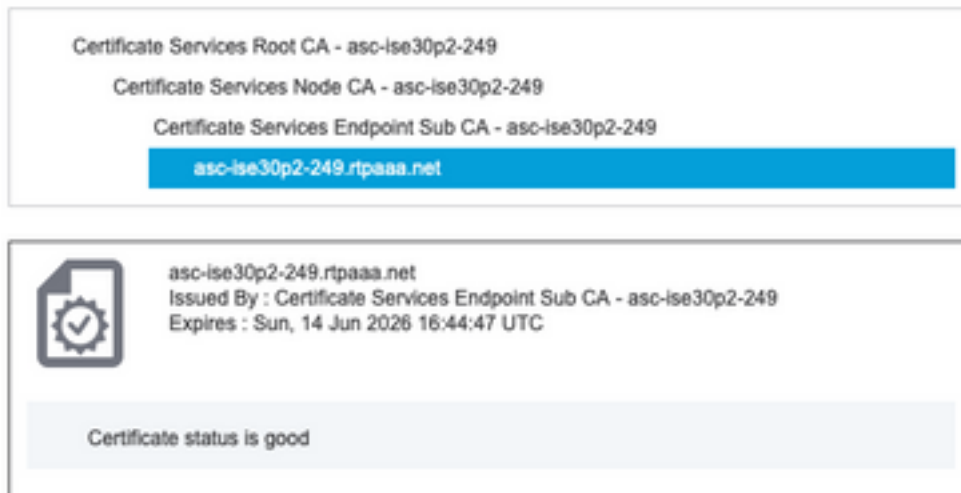## Verify ISE PxGrid Certificate chain

Navigate to **Administration > System > Certificates** on the ISE GUI

Each node with the PxGrid Persona enabled has a certificate with the PxGrid role associated with it.

These certificates can be signed by a 3rd party CA or the ISE internal CA. Check the box next to the certificate and hit view - this must list the certificate details and the certificate chain. There is also a status indicator in the certificate details indicating if the certificate is good or if the chain is incomplete.

If the certificate is signed by the ISE internal CA:

Certificate Hierarchy


```
Certificate Services Root CA - asc-ise30p2-249
    Certificate Services Node CA - asc-ise30p2-249
        Certificate Services Endpoint Sub CA - asc-ise30p2-249
            asc-ise30p2-249.rtpaaa.net
```

asc-ise30p2-249.rtpaaa.net
Issued By : Certificate Services Endpoint Sub CA - asc-ise30p2-249
Expires : Sun, 14 Jun 2026 16:44:47 UTC

Certificate status is good

There are 4 levels, starting from the top:

1. ISE Root CA - This is the CA certificate and each deployment has only 1 ISE Root CA which is the Primary Admin node.

2. ISE Node CA - This is an intermediate CA whose certificate is issued by the ISE Root CA and is also the Primary Admin node

3. ISE Endpoint Sub CA - This is the 3rd level and the issuer of the PxGrid identity certificate. Each node in the deployment has their own ISE Endpoint Sub CA issued by the ISE Node CA (Primary Admin node)

4. PxGrid identity certificate - This is the certificate that the ISE node presents to a PxGrid client i.e SMC during integration and communication

If you have a certificate signed by your organization's CA independent of ISE and/or a 3rd party well known CA:

Verify that the Root CA and any intermediate CAs that signed the PxGrid certificate are installed in the Trusted Security Certificate store on ISE under **Administration > System > Certificates > Certificate Management > Trusted Certificates**

In both cases, when you view the certificate, the UI must indicate **"Certificate Status is good".**

Error condition:

❌ Certificate trust chain is incomplete
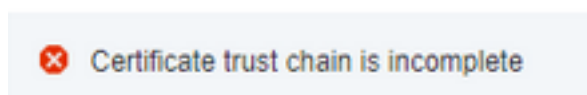
PxGrid Certificate Trust issues

If the certificate trust chain is incomplete when the ISE internal CA is in use, it is required to regenerate the ISE Root CA which then regenerates your ISE PxGrid certificates as part of the process. Update the trust store of your SMC with the newly generated ISE Root CA and ISE Node CA from the Primary Admin and the ISE Endpoint Sub CA certificate from each PxGrid node.

To replace ISE Root CA Chain, navigate to **Administration > System > Certificates > Certificate Management > Certificate Signing Requests** and Select **Generate Certificate Signing Request** which presents this UI:
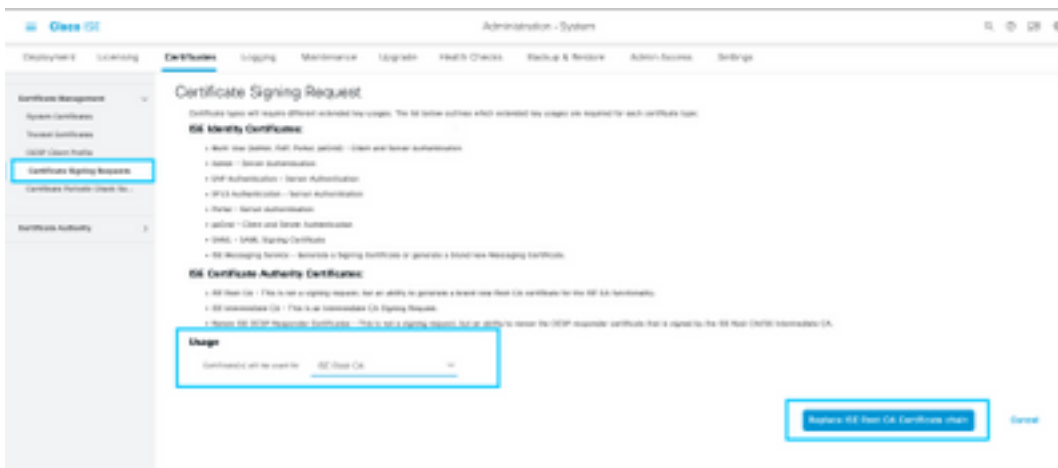
In the dropdown, select **ISE Root CA** and select **Replace ISE Root CA Certificate Chain**

If the certificate trust chain is incomplete when an external CA is in use, add the missing certificates to the ISE trust store under **Administration > System > Certificates > Certificate Management > Trusted Certificates** and restart services on the node by issuing "application stop ise" followed by "application start ise" on the ISE CLI. The CA certificates are added by accessing the GUI of the ISE deployment on the Primary admin node but the services need to be restarted via CLI on the node which displayed the certificate status error.

Note: Restart of services takes the node offline for 15-20 mins.

If issues persist after taking these corrective steps, please engage support for assistance.