# Understand ISE Services, Purpose and Troubleshooting

## Contents

# Introduction

This document describes ISE services, purpose and troubleshooting.

# Prerequisites

## Requirements

Cisco recommends that you have knowledge on Cisco Identity Services Engine.

## Components Used

The document is not restricted to any specific software and hardware versions of Cisco Identity Services Engine.

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

Cisco Identity Services Engine (ISE) is a comprehensive solution designed to provide advanced network security through centralized policy management, authentication, authorization, and accounting (AAA). It enables organizations to manage network access for users, devices, and applications while ensuring security, compliance, and seamless user experiences.

To achieve these goals, Cisco ISE utilizes a range of services, each responsible for specific tasks that enable the system to function efficiently. These services work together to ensure secure network access, robust policy enforcement, detailed logging, seamless integrations with external systems, and efficient device profiling.

Each service in ISE plays a vital role in maintaining the integrity and availability of the solution. Some services handle core functions, such as database management and authentication, while others enable advanced features like device profiling, certificate management, and monitoring.

This article provides an overview of the various services in Cisco ISE, explaining their purpose, importance, and potential troubleshooting steps if they experience issues. Whether you are an administrator or a network security professional, understanding these services helps you ensure your ISE deployment runs smoothly and securely.

# Understanding and Troubleshooting ISE services

The services mentioned in the screenshot are utilized by ISE to support its functionality. Verify the status or services available in ISE by using **show application status ise** command via CLI of ISE node. Here is a sample output that shows the status or available services on the ISE.

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4101512
Database Server                        running          107 PROCESSES
Application Server                     running          4118209
Profiler Database                      running          4108739
ISE Indexing Engine                    running          4119606
AD Connector                           running          4121671
M&T Session Database                   running          4114154
M&T Log Processor                      running          4118388
Certificate Authority Service          running          4121560
EST Service                            running          61939
SXP Engine Service                     disabled
TC-NAC Service                         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          4105571
ISE API Gateway Database Service       running          4107770
ISE API Gateway Service                running          4113275
ISE pxGrid Direct Service              running          36228
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          4122893
ISE Prometheus Service                 running          4124896
ISE Grafana Service                    running          4128455
ISE MNT LogAnalytics Elasticsearch     running          4130784
ISE Logstash Service                   running          4135868
ISE Kibana Service                     running          4137540
ISE Native IPSec Service               running          4142286
MFC Profiler                           running          52667
```

*Services available in ISE.*

Now, take a closer look at each service in detail.

**Database Listener**

Database Listener service is a critical component that helps in managing the communication between ISE and the database server. It listens for and processes requests related to the database, ensuring that the ISE system can read from and write to its underlying database.

**Key Points about the Database Listener Service in ISE**

1. **Communication Interface**: It acts as the communication bridge between ISE and the database server, allowing the system to retrieve and store data like user credentials, session information, network policies, and more.

2. **External Database Support**: ISE can be configured to use an external database (such as Oracle or Microsoft SQL Server) for user authentication and policy storage. The Database Listener Service ensures that ISE can connect to and interact with this external database securely and efficiently.

3. **Data Handling**: The service listens for database queries from the ISE system and then translates them into the appropriate actions on the external database. It can handle requests such as inserting, updating, or deleting records, as well as retrieving information from the database.

4. **Database Health Monitoring**: In addition to providing the communication channel, it also helps ensure that the connection to the external database is stable and operational. If the connection fails, ISE falls back to local storage or enter a degraded mode depending on configuration.

**Database Server**

Database Server service is responsible for managing the storage and retrieval of data used by the system. It handles the interaction with the underlying database that ISE uses to store configuration, policy information, user data, authentication logs, device profiles, and other necessary information.

**Key Points about the Database Server Service in ISE**

**1. Internal Data Storage**: The Database Server Service primarily manages the internal embedded database that ISE uses to store operational data locally. This includes data like Authentication and authorization records, User profiles, Network access policies, Device and endpoint information, Session information.

**2. Embedded Database**: In most Cisco ISE deployments, the system uses an embedded PostgreSQL database for local storage. The Database Server Service ensures that this database operates smoothly and handles all queries, updates, and management tasks related to the data stored within it.

**3. Database Integrity**: The service ensures that all transactions are processed properly and that the integrity of the database is maintained. It handles tasks like locking records, managing database connections, and executing database queries.

**Verify and Troubleshoot that Database Listener and Database Server Services are Initializing or not Running**

The Database Listener and Database Server are essential services that must run together for all other services to function properly. If these services are not running or are stuck during initialization, these troublesshooting steps help in recovery.

1. Restart the ISE services by using the **application stop ise** and **application start ise** commands.

2. If this is a VM node, restarting of the node from VM must help recovery of services.

3. If the node is a physical node, restarting / reloading the node from CIMC must help in recovery of services.

4. If the Database is corrupted, contact Cisco TAC for further troubleshooting.

The Database Listener and Database Server typically go down or fail to start when there is a discrepancy in the database or when the database is unable to initialize properly. In those cases, performing application reset by using the command **application reset-config ise** must help in recovery and fresh initiation of the database. Running the **application reset-config ise** command removes configurations and certificates, but IP address and domain name details are retained. It is recommended to contact Cisco TAC for further information and to understand the potential impact before applying this command on any node in the deployment.

**Application Server**

Application Server is a key component responsible for running and managing the core functionality and services of the ISE platform. It hosts the business logic, user interfaces, and services that allow ISE to perform its role in network access control, authentication, authorization, accounting, and policy management.

**Key Points about the Application Server Service in ISE**

**1. User Interface (UI):** The Application Server Service is responsible for rendering the web-based user interface (UI) for ISE. This allows administrators to configure and manage policies, view logs and reports, and interact with other features of ISE.

**2. Service Management**: It is responsible for handling the different services that ISE provides, including policy management, administrative tasks, and communication with other ISE nodes in a distributed deployment.

**3. Centralized Processing**: The Application Server Service plays a central role in ISE architecture, providing the logic that makes sense of policies, authentication requests, and data from network devices, directories, and external services.

**Verification for Application Server is Initializing or Not Running**

Application server depends on few Web applications like Certificates, resources, deployment, licensing. When any of the Web applications failed to initialize, application server stays stuck in the initializing state. Application server takes around 15 to 35 minutes to go from **Not running → Initializing → Running** state depending on the configuration data on the node.

1. Ensure that Admin certificate of ISE is valid and active in the deployment for all the nodes.
2. Ensure all the nodes in the deployment are in sync with Primary Admin node.
3. If the node is a VM, ensure that recommended resources are allocated to the node.

Verify the status of application server by using **show application status ise** command from CLI of the ISE node. Most of the logs related to the application server are available under the

**Catalina.Out and Localhost.log** files.

If the mentioned conditions are satisfied and application server remains stuck in initializing state, secure the support

bundle from CLI / GUI of ISE. Recover / restart the services by using the **application stop ise** and **application start ise** commands.

**Profiler Database**

Profiler Database is a specialized database used to store information about network devices, endpoints, and device profiles discovered by the Profiler service. The Profiler is a critical component of ISE that automatically identifies and classifies network devices (such as computers, smartphones, printers, IoT devices and so on ) based on network characteristics and behaviors.

**Key Points about the Profiler Database Service in ISE**

**1. Device Profiling**: The main function of the Profiler Database Service is to support the profiling process. ISE uses this service to store the information it gathers during profiling, such as:

- Device type (For example: smartphone, laptop, printer, IoT device)
- Device operating system (For example: Windows®, macOS®, Cisco IOS®, Android®)
- Device manufacturer
- Network behaviors or patterns that help to classify devices

**2. Profiler Information**: It stores profiler attributes like the device hardware and software profiles, which are used to match devices to predefined policies. This information is also used to dynamically assign devices to the correct network access policies or VLANs based on their profile.

**3. Profiling Process**: The profiling process is typically based on:

- **Active Profiling**: ISE actively queries devices on the network for information.
- **Passive Profiling**: ISE passively gathers data from network traffic, such as DHCP requests, RADIUS attributes, HTTP headers, and other network protocols, to determine the device type.

**Verify and Troubleshoot ISE Profiling Services**

1. From ISE CLI, run **show application status ise** command to verify profiler database service is running.

2. From GUI of the Primary admin node, navigate to **Administration > Deployment > select the node**. Click **Edit** and verify **session services** and **profiling services** are enabled.

3. Now, navigate to **Administration > Deployment > Select the node**. Move to **Profiler configuration** and verify if required probes are enabled for securing the endpoints data.

4. Navigate to **Administration > System > Profiling** and verify profiler settings configured for CoA.

5. From **Context visibility > Endpoints** > Select the endpoints and verify the attributes collected by different probes for endpoints.

Useful debugs for troubleshooting profiling Issues:

- **profiler (profiler.log)**
- **runtime-AAA (prrt-server.log)**
- **nsf (ise-psc.log)**
- **nsf-session (ise.psc.log)**

**ISE Indexing Engine**

Indexing Engine is a service responsible for efficiently searching, indexing, and retrieving data stored in the ISE database. It enhances the performance and scalability of ISE, particularly when it comes to handling large volumes of data and providing quick access to information needed for authentication, authorization, monitoring, and reporting tasks.

**Key Points about the ISE Indexing Engine in ISE**

**1. Data Indexing**: The ISE Indexing Engine creates indexes for various types of data stored in ISE, such as authentication logs, session logs, policy hits, profiling data, and network access records. Indexing helps in organizing this data in a way that makes searching and querying more efficient.

**2. Log Management and Reporting**: This service plays a critical role in log management by improving the performance of reporting and log queries. For example, when searching for specific authentication events, the indexing engine enables quicker retrieval of the desired records, which is crucial for security monitoring and compliance reporting.

**3.Data Retrieval**: The indexing engine is also responsible for ensuring that ISE can efficiently retrieve indexed data from its underlying database when needed. This allows ISE to provide fast responses to queries from the user interface, external tools, or APIs.

**Verify that ISE Indexing Engine is not Running or Initializing**

1. Verify forward and reverse DNS lookups are working or all the nodes in the cluster via CLI by using the **nslookup <FQDN / IP address of the ISE node >** command.
2. Verify ISE Admin Certificates are valid and active for all the nodes in the cluster.
3. Verify NTP is working and in sync with the ISE nodes via CLI by using **show ntp** command.

Indexing engine is used by Context Visibility and Indexing engine needs to be up and running for Context visibility to work. Useful logs which could help with Indexing Engine troubleshooting are **ADE.log** files which could be secured from the support bundle or tailed through CLI by using **show logging system ade/ADE.log tail** command during the issue.

**AD Connector**

AD Connector (Active Directory Connector) is a service that allows ISE to integrate with Microsoft Active Directory (AD), enabling ISE to authenticate, authorize, and manage users based on their AD credentials and group memberships. The AD Connector serves as a bridge between ISE and Active Directory, allowing ISE to leverage AD for network access control (NAC) and policy enforcement.

**Key Functions of the AD Connector Service in ISE**

**1. Integration with Active Directory**: The AD Connector Service acts as a bridge between ISE and Active Directory. It allows ISE to securely connect to AD, making it possible for ISE to utilize AD as a centralized identity store for user authentication and policy enforcement.

**2. Synchronization**: The AD Connector Service supports synchronizing user and group data from Active Directory to ISE. This ensures that ISE has up-to-date information about users and groups, which is crucial for accurate policy enforcement.

**3. Secure Communication**: The AD Connector Service establishes secure communication channels between ISE and Active Directory, typically using protocols like LDAP over SSL (LDAPS) to ensure data privacy and integrity during authentication and query processes.

**4. Multiple Active Directory Domain Support**: The service can support connections to multiple Active Directory domains. This is particularly useful in large or multi-domain environments, where ISE needs to

authenticate users from different AD forests or domains.

**5. User and Group Lookup**: It enables ISE to query AD for user and group information. This can include details like usernames, group memberships, and other user attributes that can be used to enforce network access policies. For example, network access policies can be applied based on a user AD group membership (For example: granting different access levels to users in different groups).

1. Verify if NTP is in sync with the nodes and the time difference between AD and ISE must be less than 5 minutes.

2. Verify if DNS server can resolve the FQDNs and domains related to the AD.

3. Navigate to **Operations > Reports > Reports > Diagnostics > AD connector Operations**, verify the events or reports related to AD.

Useful logs for troubleshooting are **ad_agent.log** with debug logs for **runtime** component.

### M&T Session Database

M&T Session Database (Monitoring and Troubleshooting Session Database) plays a critical role in storing and managing session-related data for network access events. The M&T Session Database holds information about active sessions, including user authentications, device connections, and network access events, which is essential for monitoring, troubleshooting, and analyzing network activity.

### Key Functions of the M&T Session Database Service in ISE

**1. Session Data Storage**: The M&T Session Database service is responsible for storing and indexing data about user and device sessions on the network. This includes session start and end times, authentication results, the user or device identity, and the associated policies (such as role assignments or VLAN assignments). The data also includes RADIUS accounting information that details the session lifecycle, including initial authentication and any accounting messages that track session events.

**2. Real-time and Historical Data**: The service provides access to real-time session data (active sessions) and historical session data (past sessions). This enables administrators to not only monitor ongoing user access but also look back at past session logs to investigate issues or validate access events. Real-time session monitoring can help ensure that no unauthorized devices are currently on the network.

**3. Enhanced Monitoring**: Provides insights into user and device activity, including the policies applied to their sessions, helping to detect potential security concerns or unauthorized access.

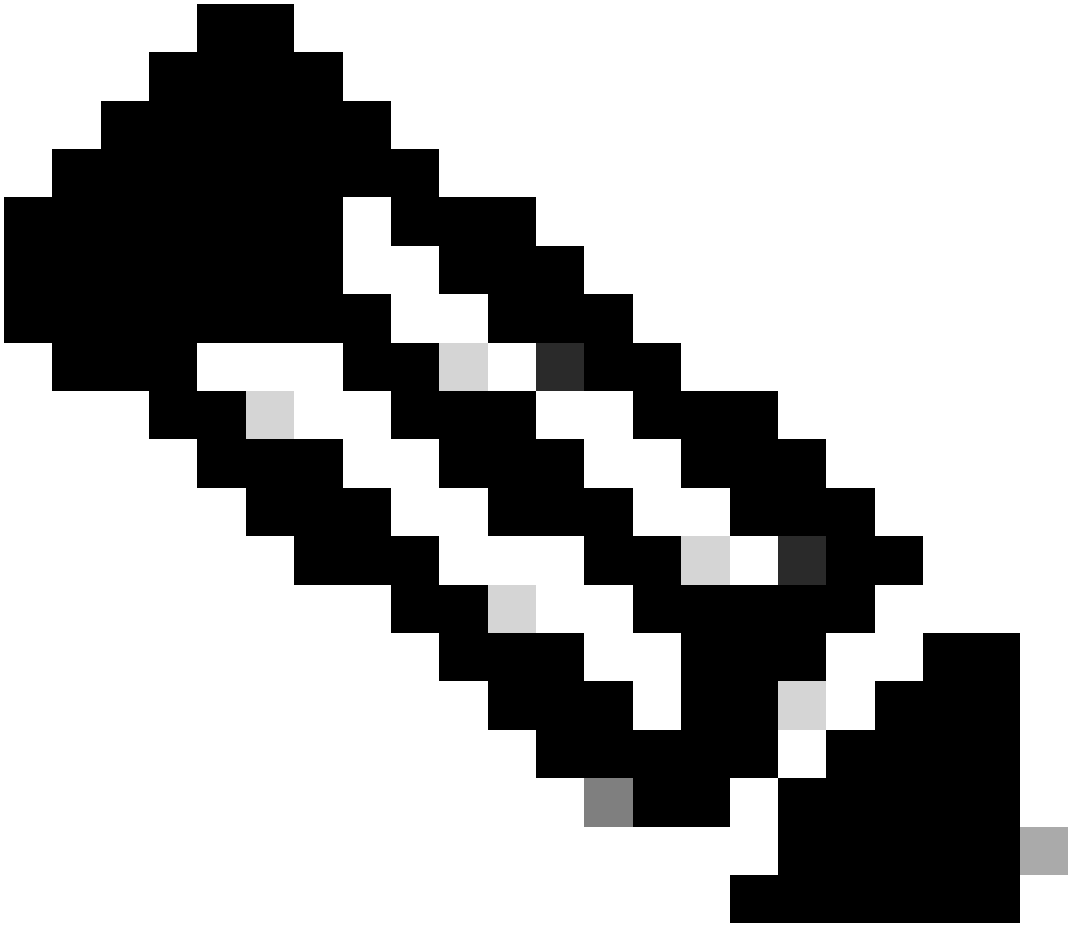
**4. Auditing and Reporting**: Facilitates compliance auditing and reporting by storing a history of network access events and providing data for regulatory reporting.

#### Verify and Troubleshoot for M&T Session Database in ISE

1. Verify if the node is allocated with recommended resources.

2. Secure **show tech-support f**rom ISE CLI for further verification of the issue.

3. Reset M&T session Database by running the **application configure ise** command in via ISE CLI and select option **1**.



**Note**: Reset M&T database must be done only after verifying the potential impact in the deployment. Contact Cisco TAC for further verification.

---

Known defects

Cisco bug ID ·32364

**M&T Log Processor**

M&T Log Processor (Monitoring and Troubleshooting Log Processor) is a component responsible for collecting, processing, and managing log data generated by various services within ISE. It is a key part of the Monitoring and Troubleshooting (M&T**)** framework, which helps administrators to monitor and troubleshoot network access events, authentication attempts, policy enforcement, and other activities within the ISE system. The M&T Log Processor specifically handles the processing of log entries, ensuring that ISE can store, analyze, and present the necessary information for reporting, auditing, and troubleshooting.

**Key Functions of the M&T Log Processor Service in ISE**

**1. Log Collection and Processing**: The M&T Log Processor Service collects and processes logs generated

by various ISE components, such as authentication requests, authorization decisions, accounting messages, and policy enforcement activities. These logs include detailed information about users, devices, and network access attempts, such as timestamps, user IDs, device types, applied policies, success or failure of access requests, and reasons for failures.

**2. Reporting and Compliance**: Logs processed by this service are crucial for compliance reporting. Many regulations require organizations to retain logs of user access and security events. The M&T Log Processor Service ensures that all relevant logs are processed and available for regulatory compliance audits. It helps in generating detailed reports based on log data, such as user access logs, authentication success/failure rates, or policy enforcement logs.

### Verify and Troubleshoot M&T Log Processor Service in ISE

1. Ensure that the ISE node is deployed with recommended resources as per Cisco Installation Guide.

2. To verify the issue, run **show logging system ade/ADE.log tail** command via ISE CLIfor relevant exceptions / errors.

Known defects

Cisco bug ID ·15130

### Certificate Authority Service

Certificate Authority (CA) Service is a critical component that helps manage digital certificates for securing communications and authenticating devices, users, and network services. Digital certificates are essential in establishing trusted connections and ensuring secure communication between clients (computers, smartphones, network devices.) and network infrastructure components (switches, wireless access points, VPN gateways). The CA Service in Cisco ISE works in tandem with X.509 certificates, which are used for several purposes in network security, including 802.1X authentication, VPN access, secure communication, and SSL/TLS encryption.

### Key Functions of the Certificate Authority Service in ISE

**1. Certificate Management**: The Certificate Authority Service is responsible for handling the creation, issuance, management, and renewal of digital certificates within ISE. These certificates are used for various authentication protocols and encryption purposes across the network. It can either act as the internal certificate authority or integrate with an external CA (For example: Microsoft AD CS, Public CAs like VeriSign or DigiCert) to issue certificates.

**2. Issuing Certificates**: For environments that require EAP-TLS or similar certificate-based authentication methods, ISE can issue certificates for Network Access Devices (NADs), users, or endpoints. ISE can automatically generate and deploy certificates for authenticating devices and users, or it can request certificates from an external CA.

**3. Certificate Enrollment**: The CA Service supports certificate enrollment for endpoints, such as laptops, phones, and other network devices, which need to authenticate to the network using certificates. ISE uses protocols such as SCEP (Simple Certificate Enrollment Protocol) or ACME (Automated Certificate Management Environment) to facilitate certificate enrollment for devices.

**4. Certificate Renewal**: The service automates the renewal of expiring certificates for both devices and users. It ensures that certificates are always valid and up to date, preventing service interruptions caused by expired certificates.

**5. Integration with External Certificate Authorities:** While ISE can act as its own CA, it is more common to integrate with an external CA (For example: Microsoft Active Directory Certificate Services). The CA Service can manage the interaction between ISE and the external CA, requesting certificates for users, devices, and network resources as needed.

**EST Service**

Enrolment over Secure Transport (EST) Service is a protocol used for securely issuing digital certificates to network devices and users in a certificate-based authentication environment. EST is a certificate enrolment protocol that allows devices to request certificates from a Certificate Authority (CA) in a secure and automated way. EST Service is particularly useful for device authentication, such as in 802.1X environments, VPN connections, or BYOD (Bring Your Own Device) scenarios, where devices need to authenticate to the network using certificates.

**Key Functions of the EST Service in ISE**

**1.Certificate Enrollment**: The EST Service is responsible for enabling secure certificate enrollment for devices (such as switches, access points, or endpoints) that require certificates for authentication purposes. The enrollment is done over a secure transport (typically HTTPS), ensuring that the process is encrypted and protected from unauthorized access.

**2. Certificate Revocation and Renewal**: Once certificates are enrolled, the EST Service also plays a role in managing certificate revocation or renewal. For example, devices need to request a new certificate when the current one expires, and EST can help automate this process.

**3. Improved Network Access Control**: By enabling devices to authenticate using certificates, the EST Service strengthens the security posture of the network, especially in environments using 802.1X authentication.

**Verify that Certificate Authority and EST service is not Running / Initializing**

1. Navigate to **Administration > System > Certificates > Certificate Authority > Internal CA settings.** Ensure that CA, EST and OCSP Responder Status is Sorted and Enabled.
2. Useful debugs which could help in troubleshooting are est , provisioning , ca-service , and ca-service-cert. Refer to **ise-psc.log , catalina.out , caservice.log** , and **error.log** files.
3. Verify ISE Root CA and ISE Messaging Certificates are valid in the deployment. If renewal of ISE Root CA is required, navigate to **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Request,** select usage as **ISE Root CA.** Click renew **ISE Root CA**.

**SXP Engine Service**

SXP Engine Service is responsible for managing and facilitating the communication between ISE and network devices using the Security Group Tag (SGT) and Security Group Exchange Protocol (SXP). It plays a critical role in supporting TrustSec policies, which are used to enforce network access control based on the Security Group of the device rather than just IP addresses or MAC addresses. The SXP Engine in ISE is primarily used for the exchange of security group information, which helps in enforcing policies based on user or device identity, application, and location. It enables devices to share Security Group Tags (SGTs), which are used to enforce security policies across network devices, such as routers and switches.

**Key Functions of the SXP Engine Service in ISE**

**1.Integration with TrustSec**: SXP is commonly deployed in environments that leverage Cisco TrustSec, a solution that enforces consistent security policies across both wired and wireless networks. The SXP Engine

facilitates the communication of SGTs between devices, allowing for dynamic policy enforcement based on the security context of a device or user.

**2. Security Group Tags (SGTs)**: The core of TrustSec's policy enforcement revolves around SGTs. These tags are used to classify network traffic, and the SXP protocol helps share the mapping of these tags to specific users or devices. This allows for granular, policy-driven control over network access and traffic flow.

**Verification and Troubleshooting for SXP Engine Service in ISE**

1.By default, the SXP Engine service is disabled in ISE. To enable it, go to the **ISE GUI > Administration > Deployment, select the node.** Check **Enable SXP Service** box, and choose the interface. Then, verify the status of the SXP Engine service from the ISE CLI using **show application status ise** command**.**

2.If there are network communication issues, verify the interface assigned to the SXP engine has a valid IP address by using **show interface** command in the CLI, and ensure that the IP subnet is permitted in the network.

3.Check the RADIUS live logs to verify the SXP connection events on ISE.

4.Enable the **SXP** component on the ISE nodes to debug and capture relevant logs and exceptions related to SXP.

**TC-NAC Service**

TC-NAC Service ( TrustSec Network Access Control ) is a component that facilitates the enforcement of TrustSec policies on network devices, ensuring that access control is based on Security Group Tags (SGTs) rather than traditional IP or MAC addresses.

TrustSec, in turn, is a framework developed by Cisco that enables security policy enforcement across the network based on device roles, users, or contexts, rather than using legacy mechanisms like VLANs or IP addresses. It provides more granular and dynamic network access control by grouping devices into different Security Groups and tagging them with SGTs**.**

**Key Functions of the TC-NAC Service in ISE**

**1. Integration with Third-Party NAC Systems**: The TC-NAC Service enables ISE to communicate and interact with third-party Network Access Control solutions. This can be useful for organizations that have existing NAC infrastructure in place but want to integrate it with Cisco ISE to improve functionality, leverage additional security policies, or take advantage of other network security features of Cisco.

**2. Providing Seamless Policy Enforcement**: When integrated with third-party NAC solutions, ISE can take over certain aspects of policy enforcement and decision-making. This allows for a more unified policy framework, ensuring that policies applied by both Cisco and non-Cisco NAC systems are consistent across the network.

**3. Support for Legacy NAC Systems**: The TC-NAC Service helps organizations that have legacy NAC systems in place, allowing them to continue using those systems while adopting Cisco ISE for its enhanced security features. ISE can integrate with older NAC solutions and extend their lifecycle, providing access control, security, and compliance enforcement in tandem.

**4. Facilitating Third-Party NAC Vendor Communication**: This service allows ISE to facilitate communication with third-party NAC solutions that uses proprietary protocols or standards. ISE can interact with the third-party NAC systems via industry-standard protocols (like RADIUS, TACACS+, or SNMP) or

customized APIs, depending on the specific NAC solution being used.

**Verify and Troubleshoot TC-NAC service in ISE**

1. Verify Threat Centric NAC is enabled by navigating to **Administration > Deployment > PSN node > Enable Threat Centric NAC**.

2. If the issue is with SourceFire FireAMP adapter, verify if **port 443** is allowed in your network.

3. Verify endpoint session details from **Operations > Threat-Centric NAC Live Logs.**

Alarms triggered by Threat Centric NAC:

- Adapter not reachable (syslog ID: 91002): Indicates that the adapter cannot be reached.
- Adapter Connection Failed (syslog ID: 91018): Indicates that the adapter is reachable but the connection between the adapter and source server is down.
- Adapter Stopped Due to Error (syslog ID: 91006): This alarm is triggered if the adapter is not in the desired state. If this alarm is displayed, check the adapter configuration and server connectivity. Refer to the adapter logs for more details.
- Adapter Error (syslog ID: 91009): Indicates that the Qualys adapter is unable to establish a connection with or download information from the Qualys site.

Useful debugs to troubleshoot the TC-NAC issues:

- **va-runtime (varuntime.log)**
- **va-service (varuntime.log and vaaggregation.log)**
- **TC-NAC (ise-psc.log)**
- **anc (ise-psc.log)**

**PassiveID WMI Service**

The PassiveID WMI Service is a service that allows ISE to perform device profiling using Windows Management Instrumentation (WMI) as a passive mechanism for identifying and profiling endpoints in the network. It plays a crucial role in device profiling, particularly in environments where devices running Windows OS need to be accurately identified for network access control and policy enforcement.

**Key Functions of the PassiveID WMI service in ISE**

**1. Device Identity Collection**: The PassiveID WMI service allows ISE to passively collect identity information from Windows devices using Windows Management Instrumentation (WMI). It gathers system details such as the hostname of the device, OS version, and other relevant attributes without requiring the device to actively participate.

**2. Integration with ISE Policy**: The information gathered by the PassiveID WMI service is integrated into the ISE policy framework. It helps in the dynamic application of policies based on device attributes such as type, OS, and compliance with security standards.

**Verify and Troubleshoot PassiveID WMI Service**

A highly secure and precise source, as well as the most common, from which to receive user information. As

a probe, AD works with WMI technology to deliver authenticated user identities.In addition, AD itself, rather than the probe, functions as a source system (a provider) from which other probes retrieve user data as well.

Useful debugs and information required for troubleshooting purpose. Set these attributes to debug level for PassiveID WMI issues:

- **PassiveID (passiveid*)**
- **runtime-logging (prrt-server.log)**
- **Active Directory (ad)_agent.log) - Trace level**
- **collector (collector.log) (on PassiveID,MnT nodes and on active pxGrid node if sessions are published)**
- **pxGrid (pxgrid/) (on secondary MnT and active pxGrid node if the sessions are published)**

Information required for troubleshooting PassiveID WMI:

1. Whether it was working before? Any changes done recently. (Like upgrade, patch install on ISE/ upgrade on DC)
2. Is Test connection works fine (Before integration, check for Test connection)
3. Details on username used to Join AD and username used for WMI. (whether admin or non admin account)
4. Check whether for the events (4768, 4770) in DC is logged. (Event viewer log from DC)
5. Capture logs: Set debug level for passive id and runtime-logging then do config wmi for that DC, AD – trace level with timestamp.

**PassiveID Syslog Service**

The PassiveID Syslog Service is a service that enables the PassiveID profiling feature to collect and process syslog messages from network devices in the environment. These syslog messages contain important information about the endpoints connected to the network, and ISE uses them to profile these devices for network access control and policy enforcement.

**Key Functions of the Passive ID Syslog Service**

**1. Passive Authentication:** The Passive ID Syslog service allows Cisco ISE to authenticate users and devices passively by collecting syslog messages from network devices (like switches or routers) that indicate user and device activity. This is useful in situations where traditional active methods of authentication, like 802.1X, is not suitable or feasible.

**2. Event Logging**: The Passive ID Syslog service relies on the syslog protocol to receive logs from network devices that track user access and behavior on the network. The information contained in these logs can include things like device log in attempts, access points, and interface details, which help ISE passively identify the device or user.

**PassiveID API Service**

The PassiveID API Service is a service that enables integration with systems that require information about the identity of devices or users that are connected to the network. It is typically used in environments where network administrators want to perform identity-based policies and actions without requiring active network authentication protocols like 802.1X for every device.

**Key Functions of the Passive ID API Service**

**1. Integration with External Systems:** The Passive ID API allows ISE to receive identity information from third-party systems or network devices (such as switches, routers, firewalls, or any system that can generate identity-related events). These external systems can send information like syslog messages, authentication logs, or other relevant data that can help ISE passively identify a user or device.

**2. Passive Authentication**: The Passive ID API service is used to authenticate users and devices passively by gathering identity data without requiring active authentication (For example: no need for 802.1X, MAB, or web authentication). For instance, it can capture information from network devices, Active Directory logs, or security appliances and use it to identify the user or device.

**3. Mapping Identity Information**: The Passive ID API can be used to map identity data to specific security policies. This information is used to dynamically assign Security Group Tags (SGTs) or roles to users and devices, which then influences the enforcement of network access controls (like segmentation and firewall policies).

**PassiveID Agent Service**

The PassiveID Agent Service is a service that enables device profiling through the use of PassiveID Agents installed on endpoints (such as computers, laptops, mobile devices and so on). The PassiveID Agent allows ISE to gather profiling information about devices on the network by listening to traffic from endpoints, without requiring active scans or direct interactions with the devices.

**Key Functions of the Passive ID Agent Service**

**1. Passive User and Device Identification:** The Passive ID Agent service is responsible for gathering identity-related information passively, typically from network devices or endpoints, and sending this data to ISE. This service allows ISE to authenticate and identify users and devices based on their activities or characteristics, without needing active authentication from the device (For example: without 802.1X credentials being provided).

**2. Integration with Other Cisco Components**: The Passive ID Agent works closely with Cisco network devices, like switches, wireless controllers, and access points, to gather identity-related information from network traffic, syslog logs, or other management systems. It can also integrate with Cisco TrustSec and Cisco Identity Services to map this data to specific Security Group Tags (SGTs) or other identity-based policies.

**3. Contextual Network Access Control**: The Passive ID Agent sends this information to Cisco ISE, which then applies the appropriate access control policies based on the identity and context of the user or device. This can include:

- Role-based access control.
- Dynamic VLAN assignment.
- Network segmentation.
- Enforcing security policies based on the user role or device security posture.

**PassiveID Endpoint Service**

The PassiveID Endpoint Service is a service that is responsible for the identification and profiling of endpoints (devices) on the network based on PassiveID technology. This service helps ISE collect, process, and classify information about devices connecting to the network, without requiring active interaction with the endpoints themselves. The PassiveID Endpoint Service plays a critical role in profiling, network access control, and security policy enforcement.

**Key Functions of the PassiveID Endpoint Service**

**1. Passive User and Device Identification:** The PassiveID Endpoint Service allows Cisco ISE to identify and authenticate devices on the network passively, by leveraging information from network activity or system logs. This includes identifying users and devices based on their network behavior or characteristics, such as MAC address, IP address, or log in information from an external identity store like Active Directory (AD).

**2. Data Collection from Endpoints**: The Endpoint Service collects various types of endpoint-specific data from different sources:

- **User log in information** from external identity stores like Active Directory or other directories.
- **Device characteristics** such as IP addresses, MAC addresses, and device type (For example: whether the device is a Windows PC, mobile phone, or IoT device).
- **Endpoint network activity** such as DHCP requests, ARP requests, and other network-layer communications.

**PassiveID SPAN Service**

The PassiveID SPAN Service is a service that leverages SPAN (Switched Port Analyzer) port mirroring on network devices to capture and analyze network traffic for endpoint profiling purposes. This service helps ISE passively gather information about endpoints (devices) on the network by analyzing their network communication patterns without requiring active probes or agents installed on the devices themselves.

**Key Functions of the PassiveID SPAN Service**

**1. Passive Identity Collection from SPAN Traffic**: The PassiveID SPAN Service allows ISE to collect identity data based on network traffic that is mirrored or copied through a SPAN port on a switch. A SPAN port is typically used for network monitoring by mirroring network traffic from other ports or VLANs. By capturing this traffic, ISE can passively gather identity information such as:

- MAC addresses of devices.
- IP addresses associated with devices.
- DHCP requests or other identity-related information from the captured traffic.
- Authentication logs from network devices, such as switches or wireless controllers.

**2. Capture of User and Device Identity Information**: The SPAN service essentially listens to the traffic that passes through the network and identifies key identity information from the network packets without needing to interact directly with the devices. This can include data such as:

- User identities when they authenticate via protocols like EAP (Extensible Authentication Protocol).
- Device identities based on MAC addresses and IP addresses.
- Device roles and behaviors based on the observed traffic patterns and events.

**Verification and Troubleshooting for PassiveID stack ( PassiveID SPAN service, PassiveID Syslog service, PassiveID Endpoint service, PassiveID Agent, PassiveID API service)**

1. PassiveID stack is a list of providers and all the services in PassiveID stack are disabled by default. Navigate to **ISE GUI > Administration > Deployment > Select the node**, **Enable Passive Identity Service**, click Save. To verify the PassiveID stack service status, log in to the CLI of ISE node and run **show application status ise** command**.**

2. If there are issues with the Passive ID Agent, check if the FQDN of the agent is resolvable from the ISE

node. To perform this, log in to the ISE CLI and run **nslookup < FQDN of Agent configured >** command**.**

3. Ensure ISE Indexing engine is active and both reverse and forward DNS lookups are being resolved by the DNS or name server configured in ISE.

4. To ensure seamless communication with the syslog providers, check **UDP port 40514 and TCP port 11468** are open in your network.

5. To configure SPAN Provider on a node, ensure that the ISE Passive Identity Service is enabled. Verify the interface you want to configure on the SPAN provider is available in ISE by using **show interface** command from ISE CLI.

To check the logs, based on the Passive ID provider, you need to review **passiveid-syslog.log, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log**. The mentioned logs can be secured from the support bundle of ISE node.

**DHCP Server (dhcpd)**

The DHCP Server (dhcpd) Service is a service that provides Dynamic Host Configuration Protocol (DHCP) functionality to network devices. It is used primarily to assign IP addresses to devices (endpoints) that are trying to connect to the network. In ISE, the DHCP server plays a crucial role in providing IP addresses to endpoints that request them when they connect to the network. The service can also provide additional configuration information, such as DNS servers, default gateway, and other network settings.

**Key Functions of the DHCP Server (dhcpd) Service in ISE**

**1. Dynamic IP Address Allocation:** The dhcpd service in ISE functions as a DHCP server, which provides IP address allocation for devices that request an IP address when they connect to the network. This is important in scenarios where devices join the network dynamically, such as in BYOD (Bring Your Own Device) environments or when devices are configured to obtain their IP addresses automatically.

**2. Profile-Based DHCP**: The dhcpd service can allocate IP addresses based on the profile of the device. If ISE has profiled the device (For example: determining it is a smartphone, laptop, IoT device), it can assign an appropriate IP address or apply other settings based on the type of device or role.

**3. Support for DHCP Relay:** ISE can function as a DHCP relay agent, forwarding DHCP requests from devices to an external DHCP server if ISE is not handling the actual IP address assignment. In this case, the dhcpd service can forward requests from devices to a central DHCP server, while ISE continues to apply network policies and access controls.

**Verify and Troubleshoot DHCP Server (dhcpd)**

1. Contact Cisco TAC to verify if the DHCP server package is installed on the ISE.

2. Log in to the root of **ISE > rpm -qi dhcp**.

**DNS Server (Named)**

The DNS Server (named) Service is a service that allows ISE to function as a DNS (Domain Name System) server or DNS resolver. It is primarily responsible for resolving domain names into IP addresses and vice versa, facilitating the communication between devices in the network.

**Key Functions of the DNS Server (Named) Service in ISE**

**1. DNS Resolution for ISE Communication**: The named service in ISE helps to resolve domain names to IP addresses. This is especially important when ISE needs to connect to other network devices or external services (such as Radius servers, Active Directory, or external NTP servers) using domain names rather than IP addresses.

- For example, when ISE needs to reach a Radius server or an external directory service (like Active Directory), it need to resolve the domain name of that server to an IP address.
- ISE queries the DNS server configured on the system to resolve these domain names, ensuring smooth communication.

**2. DNS Resolution for External Services**: The DNS service enables ISE to connect to external services that require domain names. For instance, ISE needs to resolve the names of external services like:

- Cloud-based services.
- NTP (Network Time Protocol) servers.
- Certificate Authorities (CAs) or LDAP servers.

**3. Multi-Domain and Redundant DNS Servers**: ISE can be configured to use multiple DNS servers for redundancy. In the event that one DNS server becomes unavailable, ISE can fall back on another DNS server to ensure continuous operation and DNS resolution.

**Verify and Troubleshoot for DNS Server (Named)**

1. From CLI of ISE node, verify the reachability to name server or DNS server of the deployment by using **ping <IP of DNS server / name server>** command.

2. Verify the DNS resolvance of ISE FQDNs by using the **nslookup <FQDN / IP address of ISE nodes>** command via ISE CLI.

**ISE Messaging Service**

The ISE Messaging Service is a component that facilitates asynchronous communication between various services and components within the ISE system. It plays a crucial role in the overall system architecture of ISE, enabling different parts of the platform to send and receive messages, manage tasks, and synchronize activities.

**Key Functions of the ISE Messaging Service**

**1. Inter-Process Communication (IPC):** The ISE Messaging Service plays a key role in enabling inter-process communication (IPC) between various ISE services. It ensures that different ISE modules and services, such as authentication, authorization, and policy enforcement, can exchange data and instructions in a coordinated manner.

**2. Distributed Environment Support**: In larger or distributed ISE deployments (such as in multi-node or high-availability configurations), the Messaging Service helps facilitate communication between the various ISE nodes. This ensures that data, such as authentication requests, user sessions, and policy updates, are correctly synchronized across different nodes within the ISE system.

**3. Policy and Configuration Sync**: The Messaging Service is involved in synchronizing configurations and policies between ISE nodes. When configuration changes are made to a primary node, the service ensures these changes are propagated to secondary or backup nodes in the system. This is essential in maintaining consistency and ensuring that the network access policies applied across different locations or distributed ISE nodes remain synchronized.

## Verify that ISE Messaging Service is not Running or Initializing

1. Verify that port **TCP 8671** is not blocked in firewall, as this port is used for Inter-node communication between ISE devices.

2. Verify for queue link error and if there are any, renew the ISE messaging and ISE Root CA certificates as queue link errors would usually occur because of the internal certificate corruption issues. To resolve queue link errors, renew ISE Messaging and ISE Root CA certificate by referring to the article : ISE- Queue Link Error

3. From **GUI -> Administration -> Certificates -> Select ISE Messaging Certificate.** Click View to verify the status of the certificate.

Useful logs to troubleshoot ISE Messaging Service is **ade.log** which is available in the support bundle or can be tailed via CLI by using **show logging system ade/ADE.log tail** command during the issue**.**

4. If the ADE.log log showup **rabbitmq: connection refused** errors, contact Cisco TAC to remove the lock for Rabbitmq module from ISE Root.

## ISE API Gateway Database Service

The ISE API Gateway Database Service is a component responsible for managing and processing data related to API requests and responses within the ISE system. It acts as an intermediary that connects the ISE API Gateway with the ISE database, ensuring Custom applications can also update or modify data within ISE. (for example, adjusting access policies or adding/removing users) through API calls managed by the service.

## Key Functions of the ISE API Gateway Database Service

**1. API Access to ISE Data**: The ISE API Gateway Database Service acts as a bridge, allowing external applications to interact with the ISE database via the ISE RESTful APIs. These APIs can be used to retrieve or modify data stored in the ISE database, such as:

- User authentication logs.
- Network access policies.
- Device profiling information.
- System configuration and settings.

**2. Enabling External System Integrations**: This service plays a crucial role in integrating ISE with external systems like:

- External authentication servers (LDAP, Active Directory, RADIUS).
- Network Management Systems (NMS).
- Security Information and Event Management (SIEM) solutions.
- Custom applications or services that need to interact with ISE data.

By providing API access, the API Gateway Database Service allows these external systems to query ISE data, send updates to ISE, or trigger specific actions within ISE in response to external events.

**3. Supporting RESTful API Communication**: ISE exposes RESTful APIs that are designed to work over HTTP/HTTPS. The API Gateway Database Service is responsible for managing the flow of API requests and responses, ensuring that requests are authenticated, processed, and that appropriate data from the ISE database is returned in response.

## ISE API Gateway Service

The ISE API Gateway Service  is a crucial component that provides RESTful API access to ISE services, data, and functionalities. It acts as a bridge between ISE and external systems, allowing these systems to interact programmatically with ISE network access control, policy enforcement, authentication, and other services. The API Gateway enables third-party applications, network management systems, and custom applications to interact with Cisco ISE without the need for manual intervention or direct access to the ISE user interface.

**Key Functions of the ISE API Gateway Service**

**1. Enabling API Access to ISE:** The ISE API Gateway Service enables external systems to securely access and interact with Cisco ISE data and policies using RESTful APIs. This provides programmatic access to ISE functionalities, such as authentication, policy enforcement, session management, and more.

**2. Providing Programmatic Control**: The API Gateway Service allows for programmatic control over ISE functions. Administrators and developers can use APIs to:

- Retrieve or modify network policies.
- Query or manage user sessions and authentication logs.
- Create and manage network access control rules.
- Access or update device profiles.

This control can be leveraged for automation or custom workflow orchestration, such as dynamically adjusting network access policies based on real-time data or integrating ISE into a broader security automation platform.

**3. Monitoring and Reporting**: The API Gateway Service allows external systems to collect data from operational ISE logs, session history, and policy enforcement details. This is important for:

- Compliance reporting.
- Security monitoring.
- Incident response.

API calls can be used to pull logs, audit information, and events, allowing security teams to monitor ISE activities from a centralized dashboard or reporting tool.

**Verify and Troubleshoot ISE API Gateway Service and ISE API Gateway Database Service**

1. Verify if the Admin Certificate of the ISE node is active and valid. Navigate to **Administration > Certificates > Select the node > Select Admin Certificate.** Click View to verify the status of the Admin Certificate of the ISE node.

2. Set **ise-api-gateway, api-gateway, apiservice** components to debug and the logs can be tailed by using these commands:

- **show logging application ise-psc.log tail**
- **show logging application api-gateway.log tail**

**ISE pxGrid Direct Service**

The ISE pxGrid Direct Service is a critical component that supports pxGrid (Platform Exchange Grid) functionality in ISE. pxGrid is a Cisco technology that facilitates secure, standardized, and scalable data sharing and integration between Cisco network security solutions and third-party applications, services, and devices. The ISE pxGrid Direct Service enables direct communication between ISE and other pxGrid-compatible systems without the need for intermediary devices or services.

**Key Functions of the ISE pxGrid Direct Service**

**1. Direct Integration with Third-Party Systems**: The ISE pxGrid Direct Service allows ISE to integrate directly with third-party network security systems, such as firewalls, routers, NAC solutions, SIEM platforms, and other security appliances. It allows these systems to exchange information regarding network access events, security incidents, and contextual network data.

**2. Context Sharing**: One of the primary functions of pxGrid is the sharing of contextual information (like device identities, user roles, security posture, and network access information). With the pxGrid Direct Service, ISE can directly share this context with other devices or applications without relying on traditional methods such as RADIUS or TACACS+.

**3. Simplified Communication**: By using pxGrid, ISE can communicate and exchange information with third-party solutions using a standardized protocol. This simplifies the process of integration, as systems do not need to have custom integrations for each individual third-party solution.

**4. Enhanced Security and Compliance**: The pxGrid Direct Service also improves security posture and compliance by ensuring that all systems in the network ecosystem have access to the same real-time, contextual data about users, devices, and security policies. This ensures more coordinated enforcement of network security policies across the entire environment.

**Verify and Troubleshoot ISEPxgrid Direct Service**

1. Contact Cisco TAC to verify if **edda*.lock*** is present in the /tmp folder. If yes, Cisco TAC removes the lock and restart the Pxgrid Direct service from root.

2. Set **PxGrid Direct** component to debug in ISE node for troubleshooting. The logs can be secured via ISE support bundle or ISE CLI by using these commands:

**show logging application pxgriddirect-service.log**

**show logging application pxgriddirect-connector.log**

The logs mentioned provide information on the endpoint data fetched and received by Cisco ISE along with the connectivity status of Pxgrid Connector.

**Segmentation Policy Service**

The Segmentation Policy Service is a key component responsible for enforcing network segmentation policies based on user identity, device posture, or other contextual information. It helps control the access of users and devices to specific network segments, ensuring that only authorized users or compliant devices can access certain parts of the network. Network segmentation is essential for reducing the attack surface of the network, preventing lateral movement of threats, and ensuring compliance with regulations. The Segmentation Policy Service in ISE is used to enforce these network segmentation rules dynamically and flexibly across the network.

**Key Functions of the Segmentation Policy Service**

**1. Defining Network Segments**: The Segmentation Policy Service in ISE allows administrators to define various network segments (subnets or VLANs) based on the characteristics of users or devices. For example:

- Devices with different security postures can be assigned to different segments (For example: trusted

devices in one VLAN and untrusted devices in another).
- Users from different departments or roles can be assigned to different network segments to enforce least privilege and restrict access to sensitive resources.

**2. Dynamic Segmentation**: This service enables dynamic network segmentation, meaning the network segments or VLANs can change based on real-time conditions. For example:

- A user can be assigned to a specific VLAN based on their role or device health status.
- A device that is deemed non-compliant or is running an outdated operating system can be moved to a quarantine or guest VLAN until it is remediated.

**3. Policy-Based Enforcement**: The Segmentation Policy Service uses policies to make decisions about which segment a device or user must be placed into. These policies can take into account various factors, such as:

- **User Identity**: Based on the user role or attributes.
- **Device Posture**: The health or compliance status of the device (For example: is it running the latest antivirus software?).
- **Location**: The physical location of the user or device in the network (For example: office, guest area, remote access).
- **Time of Access**: The time of day or day of the week when the access request is made.

**4. Enforcement of Security Policies**: The Segmentation Policy Service ensures that security policies are consistently enforced across network devices (like switches, routers, firewalls) by leveraging industry standards like RADIUS and VLAN assignment. This allows Cisco ISE to communicate with network infrastructure devices to enforce the required segmentation policies.

#### Verify and Troubleshoot Segmentation Policy Service

1. Verify if the segmentation is properly configured by navigating to **Work Centres** > **TrustSec** > **Overview** > **Dashboard**.

2. **Work Centres** > **TrustSec** > **Reports**, select TrustSec reports to verify the segmentation policy service status and reports.

### REST Auth Service

The REST Auth Service is a service that provides authentication capabilities using RESTful APIs. It enables external applications and systems to authenticate users or devices by interacting with ISE over HTTP(S) using standard REST protocols. This service allows for seamless integration of Cisco ISE authentication functionality with third-party applications or systems that need to authenticate users or devices but cannot use the traditional methods (like RADIUS or TACACS+).

### Key Functions of the REST Auth Service

**1. RESTful Authentication**: The REST Auth Service enables authentication requests over the REST API protocol. This allows external systems (For example: applications, third-party network devices, or services) to authenticate users or devices using ISE as the authentication server, but through RESTful web service calls rather than traditional authentication protocols like RADIUS or TACACS+.

**2. Integration with External Applications**: This service is designed for external applications that need to authenticate users or devices but do not use traditional authentication methods (like RADIUS or TACACS+). Instead, they can interact with ISE via REST APIs, making it simpler to integrate ISE authentication into web-based or cloud-native applications.

**3. Flexible and Scalable Authentication**: The REST Auth Service provides a scalable method of authentication that is not limited to just network devices or on-premises solutions. It can be used by cloud services, mobile applications, and other web-based platforms that need to authenticate users or devices by querying ISE for credentials and policies.

**4. Easy to Apply**: The REST API offers a standardized interface, which is easier to apply and integrate with modern software and applications compared to traditional methods. It provides JSON formatted responses and uses HTTP methods like GET, POST, PUT, and DELETE, making it more accessible for web developers and systems integrating ISE for authentication.

### Verification and Troubleshooting for Rest Auth

1. To troubleshoot Open API-related issues, set **apiservice** component to debug.

2. To troubleshoot ERS API related issues, set **ers** component to debug.

If the API service GUI page: **https://*{iseip}*:*{port}*/api/swagger-ui/index.html or https://*{iseip}*:9060/ers/sdk** is accessible, it concludes that API service is working as expected.

Refer API Documentation for more information on API.

## SSE Connector

The SSE Connector (Secure Software-Defined Edge Connector) is a service that integrates ISE with the Cisco Secure Software-Defined Access (SD-Access) solution. The SSE Connector allows ISE to securely communicate with the Cisco DNA Center, enabling automated network policies, segmentation, and edge security management in an SD-Access environment.

### Key Functions of the SSE Connector

**1. Integration with Third-Party Security Systems:** The SSE Connector facilitates the integration of Cisco ISE with third-party security systems like firewalls, Intrusion Prevention Systems (IPS), Network Access Control (NAC) solutions, and Security Information and Event Management (SIEM) systems. It allows these external systems to send or receive data from ISE in a secure manner, which can be used for more dynamic policy enforcement.

**2. Real-Time Threat Intelligence**: By connecting ISE with other security systems, the SSE Connector enables the exchange of real-time threat intelligence. This information can include suspicious activity, compromised endpoints, or malicious behaviors detected by other security systems, allowing ISE to dynamically adjust access policies based on current threat levels or device status.

**3. Automated Remediation**: The integration enabled by the SSE Connector can support automated remediation workflows. For example, if a system is flagged as compromised by an external security appliance, ISE can automatically enforce policies that block network access or redirect the endpoint to a remediation network segment for further investigation.

### Verify and Troubleshoot SSE Connector

1. SSE connector is enabled only when PassiveID service is enabled in ISE.

2. **sse-connector ( connector.log )** component in debug provides more information on SSE Connector related messages.

**Hermes (pxGrid Cloud Agent)**

Hermes (pxGrid Cloud Agent) is a component that facilitates the integration between ISE and the pxGrid (Platform Exchange Grid) ecosystem in a cloud environment. Hermes is the cloud-based agent used to enable communication between ISE and cloud-based services or platforms, supporting the pxGrid framework for sharing contextual information across different network and security systems.

**Key Features and Functions of Hermes (pxGrid Cloud Agent)**

**1. Cloud-to-On-Premises Integration:** Hermes (pxGrid Cloud Agent) is designed to facilitate seamless integration between cloud-based services and the on-premises ISE infrastructure. It extends the power of pxGrid beyond traditional on-prem network environments, enabling secure data exchange and policy enforcement across cloud-based applications and services.

**2. pxGrid Ecosystem Support**: pxGrid is a Cisco platform for securely sharing context and information across network security solutions. Hermes acts as the cloud agent for pxGrid, enabling secure, real-time communication between ISE and various cloud-based services. This integration allows network security policies to be consistent across both on-prem and cloud environments, making it easier to manage and enforce security.

**3. Cloud-Based Endpoint Visibility**: One of the core advantages of Hermes is that it provides visibility into cloud-based endpoints, similar to how ISE provides visibility into on-prem endpoints. It can gather data about devices and users in the cloud, such as their compliance posture, security status, and identity information. This allows ISE to enforce network access policies on cloud endpoints just as it would for on-premises devices.

**4. Seamless Extension of ISE to Cloud Environments**: One of the key benefits of Hermes is that it provides a seamless bridge between the ISE on-premises environment and the growing number of cloud-native applications. This makes it easier to extend ISE security policies, authentication methods, and access controls to cloud services without requiring a complete overhaul of the existing infrastructure.

**Verifiy and Troubleshoot Hermes (Pxgrid Cloud Agent)**

1. By default, Hermes service is disabled, connecting ISE with the Cisco PxGrid cloud enables Hermes service. Hence, if the Hermes service is disabled in ISE, verify if Pxgrid Cloud option is enabled from **ISE GUI > Administration > Deployment, select ISE node**. Edit , **enable Pxgrid Cloud.**

2. Useful debugs for troubleshooting issues related to the Pxgrid cloud are **hermes.log** and **pxcloud.log**. These debugs are available on only Pxgrid node where Pxgrid Cloud is enabled.

**McTrust (Meraki Sync Service)**

McTrust (Meraki Sync Service) is a service that enables integration between Cisco ISE and Cisco Meraki systems, specifically for syncing and managing network devices and access policies. The McTrust service acts as a connector that synchronizes user and device information between Meraki's cloud-managed network infrastructure and ISE on-premises identity and policy management systems.

**Key Features and Functions of McTrust (Meraki Sync Service)**

**1. Seamless Integration with Meraki Devices:** McTrust enables ISE to synchronize and integrate with Meraki's cloud-managed devices. This includes devices such as Meraki access points, switches, and security appliances that are part of Meraki's portfolio. It allows ISE to communicate directly with Meraki's

infrastructure, making it easier to apply network access control policies to Meraki-managed devices.

**2. Automated Device Synchronization**: The Meraki Sync Service automatically synchronizes ISE policies with Meraki network devices. This means that any changes made to the network access control policies in ISE are automatically reflected in Meraki devices, without requiring manual intervention. This makes it easier for administrators to manage network access across both Meraki and ISE platforms.

**3. Policy Enforcement for Meraki-Managed Devices**: McTrust allows ISE to enforce network access policies on Meraki devices based on authentication and device posture. It can dynamically assign policies to Meraki network elements, such as adjusting VLAN assignments, applying Access Control Lists (ACLs), or restricting access to certain network resources, depending on the security posture of the device or user requesting access.

**4. Meraki Dashboard Integration**: McTrust integrates ISE directly with the Meraki Dashboard, providing a unified management interface. Through this integration, administrators can view and manage network policies and access control rules for both Meraki devices and ISE-managed resources, all from within the Meraki cloud-managed interface.

### Verify and Troubleshoot McTrust (Meraki Sync Service)

1. Log in to **ISE GUI -> Work Centers -> TrustSec -> Integrations** -> **Sync status**. Verify any issues / errors observed.

2. Ensure that all the admin cerfiicates of ISE nodes are active & valid.

Useful debug for troubleshooting Meraki Sync Service is **meraki-connector.log**.

### ISE Node Exporter

The ISE Node Exporter service is a component used for monitoring and collecting performance metrics from the ISE system, specifically from the ISE nodes (whether they are administration nodes, monitoring nodes, or policy service nodes).

### Key Features and Functions of ISE Node Exporter

**1.Metrics Export**: The ISE Node Exporter provides a variety of performance-related metrics, such as CPU usage, Memory usage, Disk utilization, Network statistics, System load, and Other operating system-level metrics. These metrics are then used for monitoring the health and performance of the ISE node and can be visualized in a monitoring dashboard like Grafana.

**2. System Health Monitoring**: By exporting the performance data to Prometheus, the ISE Node Exporter allows for continuous monitoring of the health and operational status of the ISE node. Administrators can create alerts based on predefined thresholds to notify them of performance degradation or system issues.

**3. Prometheus Integration**: The ISE Node Exporter is typically used in conjunction with Prometheus, an open-source monitoring and alerting toolkit designed for reliability and scalability. The Node Exporter exposes system-level metrics that can be scraped by Prometheus to collect and store time-series data.

### ISE Prometheus Service

The ISE Prometheus Service is a service that integrates Prometheus with ISE to enable monitoring and collecting performance metrics from the ISE system. Prometheus is an open-source monitoring and alerting toolkit used to collect, store, and analyze time-series data, and the ISE Prometheus Service allows ISE to

expose its internal metrics to Prometheus for monitoring purposes.

**Key Features and Functions of ISE Prometheus Service**

**1. Metrics Collection for Monitoring**: The ISE Prometheus Service is designed to export various operational and performance metrics related to the ISE system. These metrics typically include, but are not limited to CPU utilization and system load, Memory usage, Disk usage and I/O performance, Network statistics, Authentication request statistics, Policy enforcement statistic, System health and uptime data

**2. Prometheus Integration**: The **Prometheus Service** allows ISE to expose data in a format that is compatible with **Prometheus**, which scrapes this data at regular intervals. Prometheus then stores the data in a time-series database, making it possible to track trends and historical performance of the ISE system.

**3. Visualization and Reporting with Grafana**: The **Prometheus Service** in ISE integrates seamlessly with **Grafana**, a popular open-source visualization tool. After exporting the metrics to Prometheus, administrators can use **Grafana dashboards** to visualize the data in real-time. This enables easy identification of performance bottlenecks, system trends, and potential issues in the ISE deployment.

**ISE Grafana Service**

The ISE Grafana Service is a service that provides visualization of system performance metrics using Grafana, an open-source platform for monitoring and data visualization. It integrates with Prometheus to display real-time and historical data collected from ISE, allowing administrators to create interactive dashboards that provide insights into the health, performance, and usage of the ISE system.

**Key Features and Functions of ISE Grafana Service**

**1. Customizable Dashboards**: Grafana is highly customizable, allowing administrators to create and modify dashboards according to their specific monitoring needs. Custom queries can be created to extract specific data points from Prometheus, and those queries can be visualized in various formats like graphs, tables, heatmaps, and more.

**2. Centralized Monitoring for Distributed ISE Deployments**: For distributed ISE deployments, where multiple ISE nodes are deployed across different locations, Grafana provides a centralized view of all the system metrics collected from each node. This allows administrators to monitor the performance of the entire ISE deployment from a single location.

**3. Historical Data and Trend Analysis**: With the data stored in Prometheus, Grafana enables historical analysis of system metrics, allowing administrators to track trends over time. For example, they can monitor how CPU usage has changed over the past month or how authentication success rates have fluctuated. This historical data is valuable for capacity planning, trend analysis, and identifying long-term issues.

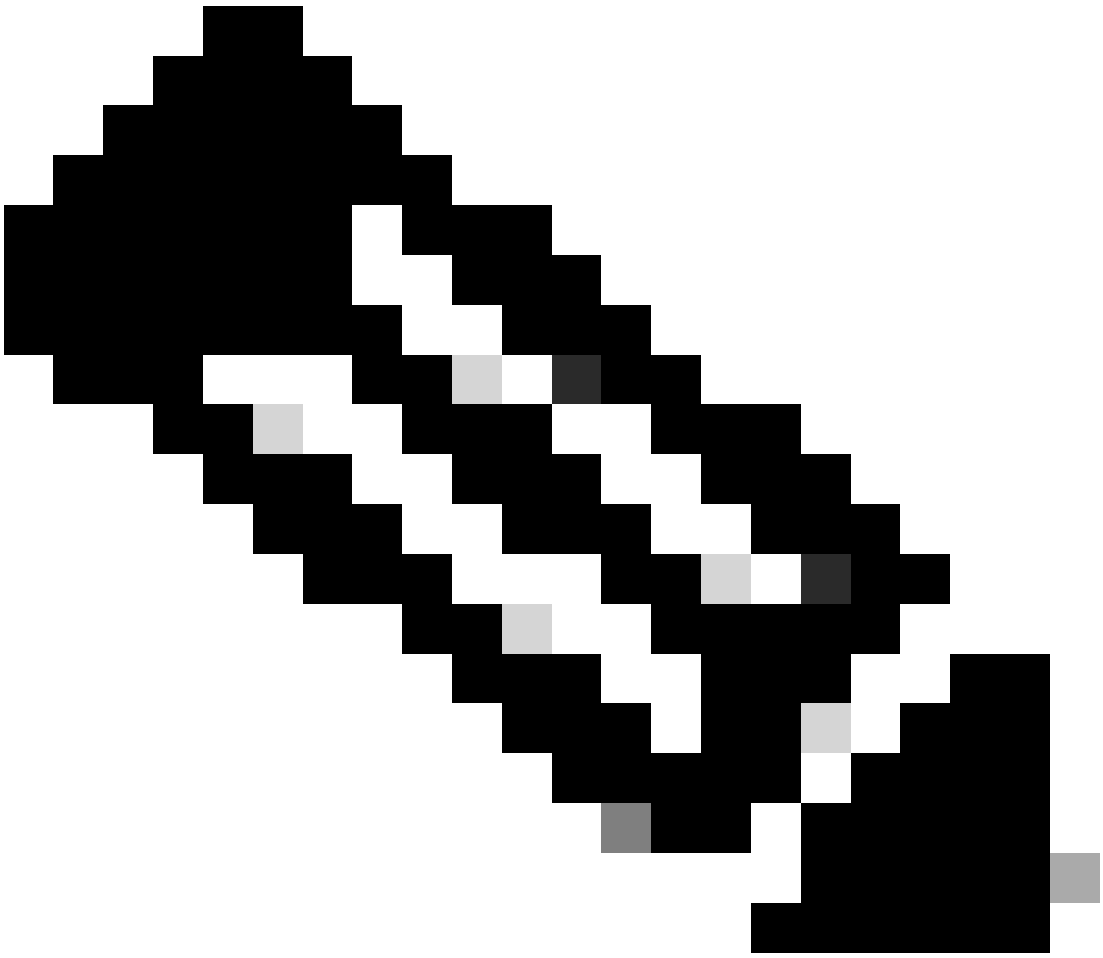
#### Verify and Troubleshoot ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter

1. ISE Grafana Service, ISE Prometheus Service and ISE Node Exporter service work together and are called as Grafana Stack Services. There are no specific debugs to enable for troubleshooting these services. However, these commands help in troubleshooting.

**show logging application ise-prometheus/prometheus.log**

**show logging application ise-node-exporter/node-exporter.log**

**show logging application ise-grafana/grafana.log**



**Note**: When Monitoring is enabled, ISE Node Exporter, ISE Prometheus Service, and ISE Grafana Service must be running and disruption of any of these services cause issues during data collection.

**ISE MNT LogAnalytics Elasticsearch**

The ISE MNT LogAnalytics Elasticsearch is a component that integrates Elasticsearch with ISE Monitoring and Troubleshooting (MNT) capabilities. It is used for log aggregation, search, and analytics related to ISE logs and events. Elasticsearch is a widely-used, distributed search and analytics engine, and when integrated with ISE, it enhances the ability of the system to store, analyze, and visualize log data generated by ISE components.

**Key Features and Functions of ISE MNT LogAnalytics Elasticsearch**

**1. Log Storage and Indexing:** The Elasticsearch service in ISE is responsible for storing and indexing the log data generated by ISE. Elasticsearch is a distributed search and analytics engine, and it allows ISE logs to be stored in a way that enables fast searching, querying, and retrieving specific events, errors, or system activities.

**2. Integration with Log Analytics:** ISE MNT LogAnalytics Elasticsearch works in conjunction with Log Analytics to provide a comprehensive logging solution. It enables ISE to collect log data related to

authentication, policy enforcement, system operations, and other activities. This data is stored in Elasticsearch, making it easier to perform detailed analysis and gain insights into ISE behavior.

**3. Centralized Logging**: By integrating with Elasticsearch, ISE provides a centralized logging solution, which is crucial for environments that require distributed log collection. This allows administrators to view and analyze logs from multiple ISE nodes in a single, unified interface, making it easier to troubleshoot and monitor ISE performance.

**4. Log Analysis and Troubleshooting**: The ISE MNT LogAnalytics Elasticsearch service helps administrators analyze system behavior and troubleshoot issues by making log data easily accessible. For example, if there is a sudden spike in authentication failures or an unexpected system outage, Elasticsearch allows for quick querying of log data to identify the root cause.

#### Verify and Troubleshoot ISE M&T LogAnalytics Elasticsearch

1. Disabling and re-enabling of the Log analytics service in ISE must help. Navigate to **Operations > System 360 > Settings > Log analytics ( disable and enable by using toggle option)**.

2. Restarting of the M&T LogAnalytics from ISE Root resolves the issue. Contact Cisco TAC for performing this action.

Known defects

Cisco bug ID ·66198

### ISE Logstash Service

ISE Logstash Service is a component that integrates Logstash, an open-source data processing pipeline, with ISE for log collection, transformation, and forwarding. Logstash acts as a log collector and log forwarder, allowing ISE logs to be processed and sent to other systems for analysis, storage, and monitoring. Logstash is a powerful, open-source tool that collects, parses, and forwards logs or other data from different sources to a central location for storage, analysis, and visualization. In the context of ISE, the ISE Logstash Service is used to process and forward logs in a structured format to a centralized logging system, where they can be further analyzed, monitored, and visualized.

### Key Features and Functions of the ISE Logstash Service

**1. Log Collection and Forwarding:** The primary function of the ISE Logstash Service is to collect log data from various ISE components (such as authentication logs, system logs, policy enforcement logs and so on.) and forward it to a central location (typically Elasticsearch or another log management system) for storage and analysis.

**2. Log Parsing**: **Logstash** can parse the collected logs into structured formats. It processes raw log data and extracts meaningful information from it, transforming the log entries into a format that is easier to query and analyze. This can involve filtering, parsing, and enriching the data before forwarding it to Elasticsearch or other systems.

#### Verify and Troubleshoot ISE Logstash Service

1. No specific debugs to be enabled. However, **show logging application ise-logstash/logstash.log** provide insights on the status of the service.

2. Disabling and re-enabling of the Log analytics service in ISE must help. Navigate to **Operations > System 360 > Settings > Log analytics** ( disable and enable by using toggle option).

Known defects related to Logstash service

Cisco bug ID ·74832

Cisco bug ID ·58596

**ISE Kibana Service**

ISE Kibana Service is a component that integrates Kibana, an open-source data visualization tool, with ISE logging and monitoring infrastructure. Kibana works in tandem with Elasticsearch (which stores and indexes log data) to provide a powerful platform for visualizing, searching, and analyzing ISE logs and performance metrics**.**

**Key Features and Functions of the ISE Kibana Service**

**1. Data Visualization**: The ISE Kibana Service allows administrators to create visual representations of the log data collected from ISE. This can include:

- Charts, graphs, and tables for trends in authentication, policy enforcement, user activity, and system health.
- Pie charts, line graphs, and bar charts to track specific metrics such as the number of failed log in, session duration, or errors over time.

**Verify and Troublehsoot ISE Kibana Service**

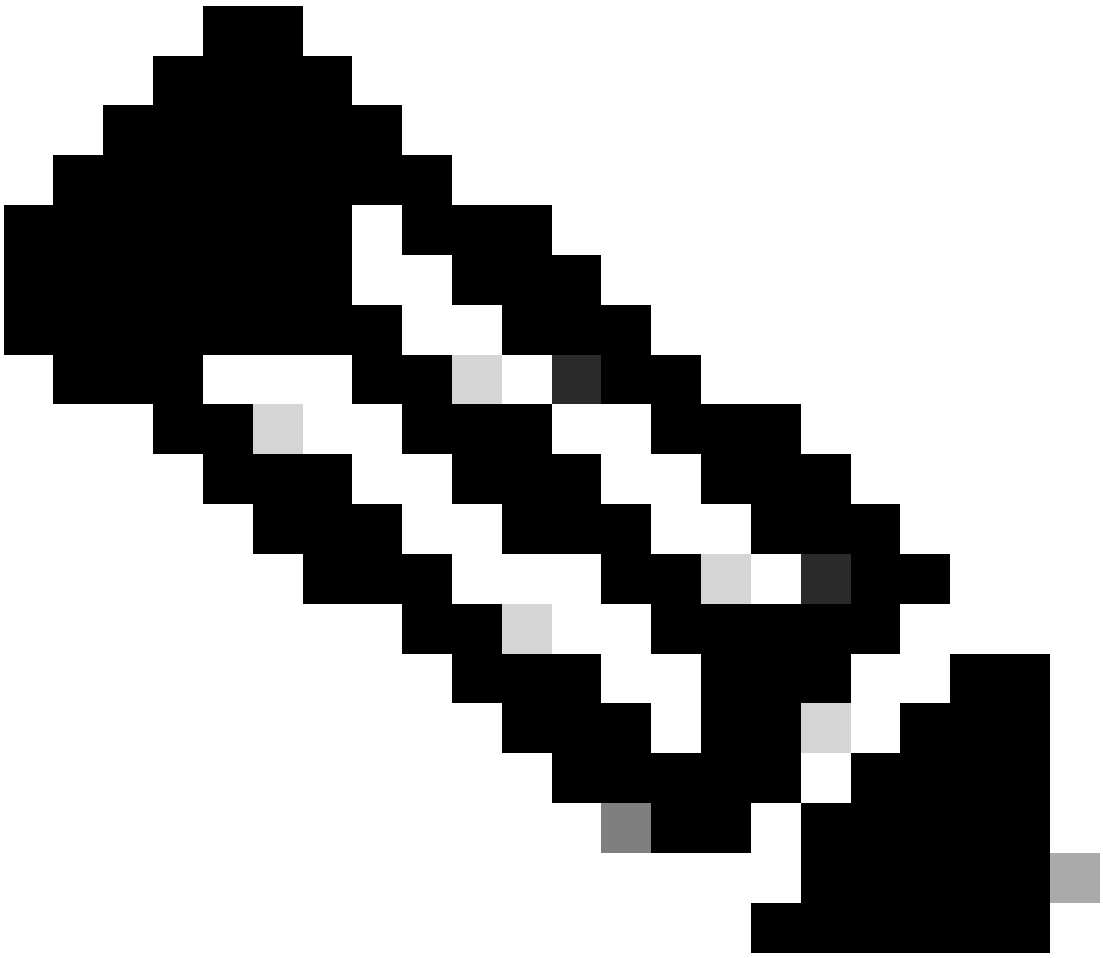
1. If ISE kibana service is not running, disable and Re-enable log analytics in ISE, navigate to **Operations** > **System 360** > **Settings, Log analytics** ( disable and enable by using toggle option).

2. In many scenarios, there can be a duplicate entry in **/etc/hosts** folder which must be causing an issue. Contact TAC to remove the duplicate entry.

Known defects related to the Kibana Issue

Cisco bug ID ·78050

Cisco bug ID ·59848



**Note**: When Log Analytics is enabled, ISE MNT LogAnalytics Elasticsearch, ISE Logstash Service, ISE Kibana Service must be running and disruption of any of these services create issues during the data collection.

**ISE Native IPSec Service**

The ISE Native IPSec Service refers to the built-in support for IPSec (Internet Protocol Security), which provides secure communication between ISE nodes or between ISE and other network devices. IPSec is a suite of protocols used to secure network communications by authenticating and encrypting each IP packet in a communication session.the Native IPSec Service is part of the broader security and network access management framework. It provides capabilities to handle and manage IPsec VPN connections, ensuring that the data transmitted between the ISE system and remote endpoints is secure. This could involve interactions with client devices, network access devices (such as routers or firewalls), or even other ISE nodes, where IPsec encryption and tunneling are necessary for securing sensitive information.

**Key Features and Functions of the ISE Native IPSec Service**

**1. Secure Communication via IPsec:** The primary function of the ISE Native IPSec Service is to establish and maintain secure communication channels using IPsec. This involves the use of encryption and authentication mechanisms to ensure that the data transmitted between ISE and other devices is protected

from interception, tampering, and unauthorized access.

**2. IPsec VPN Connectivity**: The ISE Native IPSec Service helps facilitate VPN connections that use the IPsec protocol to provide a secure, encrypted tunnel for data transmission. This is especially useful for remote workers, branch offices, or other locations needing to securely access the ISE environment over untrusted networks (such as the internet).

**3. Support for Remote Access VPN**: The Native IPSec Service can be involved in remote access VPN configurations, where users or devices located offsite (such as remote employees or branch offices) securely connect to the ISE system via IPsec tunnels. This service ensures that all remote access traffic is encrypted and authenticated before reaching the ISE environment.

4.**IPsec VPN Client Compatibility**: ISE Native IPSec Service ensures compatibility with IPsec VPN clients. It supports common client configurations, enabling devices to securely connect to the network without exposing sensitive data to risks.

### Verifiy and Troubleshoot Native IPSec Service

1. There are no specific debugs to enabled for Native IPSec service. Verify the logs using **show logging application strongswan/charon.log tail** comand via ISE CLI.

2. If any issue is observed for tunnel, verify the status of the tunnel establishment via **GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec**.

## MFC Profiler

The MFC Profiler is a specialized component used for profiling network devices and endpoints. Profiling is a key part of network access control, as it allows ISE to identify devices on the network, classify them, and apply appropriate network policies based on the type of device and behavior.

## Key Features and Functions of the MFC Profiler Service in ISE

**1. Traffic Profiling:** The MFC Profiler service in ISE is responsible for collecting and profiling the traffic data. It monitors how endpoints behave on the network, including the types of applications being used, the services accessed, and the traffic patterns exhibited by devices. This data helps build a profile for each endpoint.

**2. Endpoint Profiling**: The MFC Profiler service allows ISE to identify and categorize endpoints based on their behavior. For example, it detects if an endpoint is a printer, computer, or mobile device based on traffic patterns. This can help enforce more specific policies for different types of devices, improving security and operational efficiency.

### Verifiy and Troubleshoot MFC profiler Service

1. Navigate to **ISE GUI -> Administration -> Profiling -> MFC profiling and AI rules**, verify if the service is enabled.

2. If the service is enabled but showing as disabled / not running via **show application status ise** command in ISE CLI. Disable and re-enable MFC profiling service in ISE by referring to Step1.

Useful debugs for troubleshooting : **MFC profiler** component in debug. The logs could be verified from support bundle or tail the logs by using **show logging application ise-pi-profiler.log tail** command via ISE CLI.

Known defect for MFC profiler showing up not running instead of disabled state:

Cisco bug ID ·72853

**Key Points**

1. To recover the services, restart the services by using **application stop ise** and **application start ise** commands via ISE CLI.

2. When there is a issue, ensure that there is a support bundle being capture from the ISE GUI / ISE CLI for further verification of the issue. Reference link for creation of ISE support bundle via GUI and CLI : Collect Support Bundle on the Identity Services Engine

3. If the Issues are related to resources, load average, disk utilization and so on, it is mandatory to collect thread dump and heap dump for analysis.

4. Before performing reload of the node, contact Cisco TAC and provide secured logs for further analysis.

# Standard Concerns in ISE

Apart from the issues with ISE services, these are some of the concerns found in ISE nodes along with basic troubleshooting steps required.

**Verification for High load Average, Resource Utilization Issues ( CPU / MEMORY / DISK ), Insufficient Resources**

1. Verify that Cisco recommended resources are allocated to the node by using **show inventory** command via ISE CLI.

2. From the CLI of ISE node, run **tech top** command to verify resource utilization of ISE.

3. Verify disk utilization by using **show disk** command via ISE CLI.

4. Purge the inactive endpoints, clear the local disk of node and perform upgrade cleanups.

If the issue persists, Contact Cisco TAC and provide the secured support bundle, Heap dump and Thread dump from the node which is experiencing the issue.

To secure the heap dump, log in to the CLI of ISE node, run the **application configure ise** command. Select **option 22.**

To secure the thread dump, log in to the CLI of ISE node, run the **application configure ise** command, select **option 23.** Thread dump is included in the support bundle or can be tailed via ISE CLI using **show logging application appserver/catalina.out** command.

## Verify and Troubleshoot Monitoring Issues

Monitoring and Troubleshooting(MnT) function of ISE is one of the major block of ISE architecture which provides monitoring, reporting and alerting capabilities.

ISE displays monitoring information in many places, including:

- Cisco ISE Home page
- Context Visibility views
- RADIUS Live Logs and Live Sessions

- Global search
- Threat-Centric NAC Live Logs
- TACACS Live Logs

General issues observed in the Monitoring and Troubleshooting Category:

1. Radius/ TACACS Live logs not available
2. Live sessions not available
3. Health Summary not available
4. Performance (high CPU/Memory) issues seen on the MnT nodes)

Debugs to be enabled on the MnT nodes to narrow down the issue:

1. Cisco-mnt
2. Collector
3. Cpm-mnt
4. runtime-logging

In addition to the mentioned components in debug, this information can help for troubleshooting:

1. Are live sessions also affected or only live logs?
2. Are Radius or TACACS logs affected or both?
3. Do you see high CPU utilization or high swap space usage on MnT nodes?
4. How many buffer files do you see on the MnT nodes. Buffer files can be found under: /opt/CSCOcpm/mnt/data/collector.
5. Is memory and CPU reservations enabled, if not please enable it.
6. Was MnT/config/session DB reset performed in recent past?
7. Are you seeing syslogs being sent from PSN's to MnT nodes?

If you are using Syslog services for MnT, this information is required for troubleshooting purpose:

1. Are you using secure syslog target, if not please disable it as it is known to cause deadlocks in threads causing collector to stop functioning?
2. Are you using secure syslog target, ensure cert mapping is properly set under **Administration->Logging->Remote logging Targets->Secure Syslog collector 1 and 2**
3. Verify if logging categories are appropriately (recommended to remove unused/unwanted logging categories- this reduces the load on MnT nodes) set and logging targets are set correctly configured.
4. Check the **awrrep*.html** files from the support bundle to understand and get a hint of what component is sending more frequent syslogs for instance if TACACS tables are being seen with insert or update queries, we can check the collector logs to correlate to understand what syslogs are being sent more frequently

If the issue is related to the performance on the MnT node, we need this information:

1. **tech top** output from the ISE CLI of the MnT node.

2. If CPU is high, do you also see high memory or high swap space utilization?

3. Support bundle with heap dump and thread dump secured.

# Reference

- Cisco Identity Services Engine Administrator Guide, Release 3.3
- Troubleshoot and Enable Debugs on ISE