



Monitoring and Troubleshooting Service in Cisco ISE

The Monitoring and Troubleshooting (MnT) service is a comprehensive identity solution for all Cisco ISE run-time services. The **Operations** menu contains the following components, and can be viewed only from the primary Policy Administration Node (PAN). Note that the **Operations** menu does not appear in the primary Monitoring node.

- **Monitoring:** Provides real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and monitor operational conditions.
- **Troubleshooting:** Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide resolution in a timely manner.
- **Reporting:** Provides a catalog of standard reports that you can use to analyze trends and monitor system performance and network activities. You can customize reports in various ways and save them for future use. You can search records using wild cards and multiple values in all the reports for the **Identity**, **Endpoint ID**, and **ISE Node** (except the **Health Summary** report) fields.

ISE Community Resource

For a complete list of troubleshooting TechNotes, see [ISE Troubleshooting TechNotes](#).

- [Network Privilege Framework Event Flow Process](#), on page 2
- [User Roles and Permissions for Monitoring and Troubleshooting Capabilities](#), on page 2
- [Data Stored in the Monitoring Database](#), on page 2
- [Cisco ISE Telemetry](#), on page 3
- [Information that Telemetry Gathers](#), on page 3
- [SNMP Traps to Monitor Cisco ISE](#), on page 6
- [Cisco ISE Alarms](#), on page 9
- [Log Collection](#), on page 29
- [RADIUS Live Logs](#), on page 29
- [TACACS Live Logs](#), on page 32
- [Live Authentications](#), on page 33
- [RADIUS Live Sessions](#), on page 35
- [Export Summary](#), on page 38
- [Authentication Summary Report](#), on page 39
- [Diagnostic Troubleshooting Tools](#), on page 40

- [Session Trace Test Cases](#), on page 42
- [Technical Support Tunnel for Advanced Troubleshooting](#), on page 44
- [TCP Dump Utility to Validate Incoming Traffic](#), on page 45
- [Obtaining Additional Troubleshooting Information](#), on page 48

Network Privilege Framework Event Flow Process

The Network Privilege Framework (NPF) authentication and authorization event flow uses the process described in the following table:

Process Stage	Description
1	Network Access Device (NAD) performs either a normal authorization or a flex authorization.
2	An unknown agentless identity is profiled with web authorization.
3	A RADIUS server authenticates and authorizes the identity.
4	Authorization is provisioned for the identity at the port.
5	Unauthorized endpoint traffic is dropped.

User Roles and Permissions for Monitoring and Troubleshooting Capabilities

Monitoring and troubleshooting capabilities are associated with default user roles. The tasks you are allowed to perform are directly related to your assigned user role.

See [Cisco ISE Administrator Groups](#) for information on the permissions and restrictions set for each user role.

See section "Cisco ISE Administrator Groups" in Chapter "Cisco ISE Admin Guide: Overview" in *Cisco ISE Administrator Guide* for information on the permissions and restrictions set for each user role.



Note Accessing Cisco ISE using the root shell without Cisco TAC supervision is not supported, and Cisco is not responsible for any service disruption that might be caused as a result.

Data Stored in the Monitoring Database

The Cisco ISE monitoring service collects and stores data in a specialized monitoring database. The rate and amount of data utilized to monitor network functions may require a node dedicated solely to monitoring. If your Cisco ISE network collects logging data at a high rate from policy service nodes or network devices, we recommend a Cisco ISE node dedicated to monitoring.

To manage the information stored in the monitoring database, perform full and incremental backups of the database. This includes purging unwanted data and then restoring the database.

Cisco ISE Telemetry

Telemetry monitors your system and the devices in your network to provide feedback to Cisco on how you use the product. Cisco uses this information to improve the product.

Cisco ISE telemetry data communication occurs as HTTPS traffic through Port 443 with <https://connectdna.cisco.com/>.

Telemetry is enabled by default. To disable this feature:

1. Choose **Administration > System > Settings > Network Success Diagnostics > Telemetry**.
2. Uncheck the **Enable Telemetry** check box to disable telemetry.

With Cisco ISE 2.4 Patch 12, telemetry is disabled immediately. Before applying the patch, it may take up to 24 hours after the feature is disabled for Cisco ISE to stop sharing telemetry data.

Telemetry requires Smart Licensing. If you are not already using smart licensing, see Smart Licensing in the Licensing book for your version of Cisco ISE.

- **Cisco Account:** Enter your Cisco account credentials so that you can get emails from Telemetry. We may also use this ID to contact you if Telemetry finds any serious issues that may affect your Cisco ISE deployment..
- **Transport Gateway:** You can use a proxy between your Cisco ISE and the Cisco external telemetry servers for extra security. To do this, check this check box and enter the FQDN of your proxy server. Telemetry does not require a proxy.

Cisco provides software for Transport Gateway. You can download from cisco.com. This software runs on a Linux server. See the [Smart Call Home Deployment Guide](#) for information on how to deploy the Transport Gateway software on an *RHEL server*. If you are using this Cisco software, the URL value is **<FQDN of proxyserver>/Transportgateway/services/DeviceRequestHandler**.

You can use this gateway to connect to the Smart Licensing server, too. From Version 3.5 of the Transport Gateway, you cannot change the port, but you can enter IP address instead of the FQDN.

Information that Telemetry Gathers

Telemetry sends the following information to Cisco.

Nodes:

For each Policy Administration Node (PAN)

- Current number of postured endpoints
- Current number of PxGrid clients
- Current number of endpoints managed by MDM
- Current number of Guest users
- Start and end date of this telemetry record

For each Policy Service Node (PSN)

- Number of profiler probes
- Node service type
- Passive ID used

For All nodes

- Number of CPU cores
- VM available disk space
- System name
- Serial number
- VID and PID
- Uptime
- Last CLI login

MnT node count**pxGrid node count****Licenses**

- Have any licenses expired?
- Number of Apex licenses available, maximum ever used
- Number of Base licenses available, maximum ever used
- Number of Plus licenses available, maximum ever used
- Number of small, medium, and large VM licenses
- Is an evaluation license in use?
- Name of the smart account
- Number of TACACS devices
- Expiration date, remaining days, license term
- Service types, primary and secondary UDI

Posture

- Number of inactive policies
- Last posture feed update
- Number of active policies

Guest Users

- Maximum number of authenticated guests for the day
- Maximum number of active guests for the day

- Maximum number of BYOD users for the day

Network Access Devices (NAD)

- Authorization: Activated ACLs, VLANs, Policy size
- NDG map and NAD hierarchy
- Authentication:
 - Number of RADIUS, RSA ID, LDAP, ODBC, and Active Directory ID stores
 - Number of local (nonadmin) users
 - NDG map and NAD map
 - Number of policy lines

For authorizations, active VLANs, policy count, number of activated ACLs:

- Status, VID, PT
- Average load, memory usage
- Number of PAP, MnT, pxGrid, and PIC nodes
- Name, profile name, profile ID

NAD Profile

For each NAD profile:

- Name and ID
- Cisco device
- TACACS support
- RADIUS support
- Trustsec support
- Default profile

Profiler

- Date of last feed update
- Are automatic updates enabled?
- Endpoints profiled, endpoint type, unknown endpoints, percentage unknown, and total endpoint count
- Number of custom profiles
- Serial number, scope, endpoint types, custom profiles

Mobile Device Management (MDM)

- List of MDM nodes
- For a date range, current MDM endpoint count, current guest user count, current postured users count

- pxGrid client count
- Node count

SNMP Traps to Monitor Cisco ISE

SNMP traps help you to monitor the status of Cisco ISE. If you want to monitor Cisco ISE without accessing the Cisco ISE server, you can configure a MIB browser as an SNMP host in Cisco ISE. You can then monitor the status of Cisco ISE from the MIB browser.

See the [Cisco Identity Services Engine CLI Reference Guide](#) for information on the **snmp-server host** and **snmp-server trap** commands.

Cisco ISE supports SNMPv1, SNMPv2c, and SNMPv3.

Cisco ISE sends the following generic system traps if you configure the SNMP host from the CLI:

- Cold start: When the device reboots.
- Linkup: When Ethernet interface is up.
- Linkdown: When Ethernet interface is down.
- Authentication failure: When the community strings do not match.

The following table lists the generic SNMP traps that are generated by default in Cisco ISE.

OID	Description	Trap Example
.1.3.6.1.4.1.8072.4.0.3 \n NET-SNMP-AGENT-MIB::nsNotifyRestart	Indicates that the agent has been restarted.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET-SNMP-AGENT-MIB::nsNotifyShutdown	Indicates that the agent is in the process of being shut down.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmNotificationPrefix

OID	Description	Trap Example
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	Signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the Down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	Signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the Down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	Signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

Process-Monitoring SNMP Traps in Cisco ISE

Cisco ISE allows you to send hrSWRunName traps for Cisco ISE process statuses to the SNMP manager if you configure an SNMP host from the Cisco ISE CLI. Cisco ISE uses a cron job to trigger these traps. The cron job retrieves the Cisco ISE process status from Monit. After you configure the **SNMP-Server Host** command from the CLI, a cron job runs every five minutes and monitors Cisco ISE.



Note When an ISE process is manually stopped by an admin, Monit for the process also stops and no traps are sent to the SNMP manager. A process-stop SNMP trap is sent to the SNMP manager only when a process accidentally shuts down and is not automatically revived.

The following is a list of process-monitoring SNMP traps in Cisco ISE.

OID	Description	Trap Example
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	A textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. If this software was installed locally, this must be the same string as that used in the corresponding hrSWInstalledName. The services considered are app-server, rsyslog, redis-server, ad-connector, mnt-collector, mnt-processor, ca-server est-server, and elasticsearch.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

Cisco ISE sends traps for the following statuses to the configured SNMP server:

- Process Start (monitored state)
- Process Stop (not monitored state)
- Execution Failed: When the process state changes from Monitored to Execution Failed, a trap is sent.
- Does Not Exist: When the process state changes from Monitored to Does Not Exist, a trap is sent.

A unique object ID (OID) is generated for every object in the SNMP server and a value is assigned to the OID. You can find the object with its OID value in the SNMP server. The OID value for a running trap is *running*, and the OID value for the Not monitored, Does not exist, and Execution failed traps is *stopped*.

Cisco ISE sends traps using the OID of hrSWRunName that belongs to the HOST-RESOURCES MIB, and sets the OID value as < *PROCESS NAME* > - < *PROCESS STATUS* >, for example, runtime - running.

To stop Cisco ISE from sending SNMP traps to the SNMP server, remove the SNMP configuration from the Cisco ISE CLI. This operation stops sending SNMP traps and polling from the SNMP manager.

Disk Utilization SNMP Traps in Cisco ISE

When a Cisco ISE partition reaches its threshold disk utilization limit and the configured amount of free space is reached, the disk utilization trap is sent.



Note Cisco ISE does not have any MIB for process status or disk utilization. Cisco ISE uses OID HOST-RESOURCES-MIB::hrSWRunName for sending SNMP trap. You cannot use SNMP walk or SNMP get command to query the process status or disk utilization.

The following is a list of disk utilization SNMP traps that can be configured in Cisco ISE:

OID	Description	Trap Example
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	Percentage of space used in the disk.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	Path where the disk is mounted. dskPath can send traps for all the mount points in the output of the ISE admin command show disks .	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

Cisco ISE Alarms

Alarms notify you of critical conditions on a network and are displayed in the Alarms dashlet. They also provide information on system activities, such as data purge events. You can either configure how you want to be notified about system activities, or disable them entirely. You can also configure the threshold for certain alarms.

Most alarms do not have an associated schedule and are sent immediately after an event occurs. At any given point in time, only the latest 15,000 alarms are retained.

If the event recurs, the same alarms are suppressed for about an hour. During the time that the event recurs, depending on the trigger, it may take about an hour for the alarms to reappear.

You can filter the alarms you want to view based on alarm name, category, severity, or status. As you select filters, the effects are additive, also referred to as cascading filter, which allows you to drill down to find the particular data you are looking for.

The **Quick Filter** allows you to enter a value for any of the field attributes displayed in the listing page, refreshes the page, and lists only those records that match your filter criteria.

The **Advanced Filter** allows you to filter information based on specified conditions, such as, *Alarm Name contains TrustSec*. You can specify more than one condition.

You can create and save user-specific custom filters that are accessible only to you.

Click **Clear All Filters** to remove all the applied filters.

The following table lists all the Cisco ISE alarms, descriptions, and resolutions.

Table 1: Cisco ISE Alarms

Alarm Name	Alarm Description	Alarm Resolution
Administrative and Operational Audit Management		
Deployment Upgrade Failure	An upgrade has failed on an ISE node.	Check ADE.log on the failed node for upgrade failure reason and corrective actions.
Upgrade Bundle Download failure	An upgrade bundle download has failed on an ISE node.	Check ADE.log on the failed node for upgrade failure reason and corrective actions.
SXP Connection Failure	SXP connection has failed.	Verify that the SXP service is running. Check the peer for compatibility.
Cisco profile applied to all devices	Network device profiles define the capabilities of network access devices, such as MAB, Dot1X, CoA, and Web Redirect.	Consider editing the configuration of non-Cisco network devices to assign the appropriate profile.
Secure LDAP connection reconnect due to CRL found revoked certificate	CRL check result indicates that the certificate used for LDAP connection is revoked.	Check the CRL configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the LDAP server.
Secure LDAP connection reconnect due to OCSP found revoked certificate	OCSP check result indicates that the certificate used for LDAP connection is revoked.	Check the OCSP configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the LDAP server.
Secure syslog connection reconnect due to CRL found revoked certificate	CRL check result indicates that the certificate used for syslog connection is revoked.	Check the CRL configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the syslog server.
Secure syslog connection reconnect due to OCSP found revoked certificate	OCSP check result indicates that the certificate used for syslog connection is revoked.	Check the OCSP configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked, issue a new certificate and install it on the syslog server.
Administrator account Locked/Disabled	Administrator account is locked or disabled because of password expiration or incorrect login attempts. For more details, refer to the administrator password policy.	Administrator password can be reset by another administrator using the GUI or CLI.

Alarm Name	Alarm Description	Alarm Resolution
ERS identified deprecated URL	ERS-identified deprecated URL	The request URL is deprecated and we recommend that you avoid using it.
ERS identified out-dated URL	ERS-identified outdated URL	The requested URL is outdated and we recommend that you use a newer one. The outdated URL will not be removed in future releases.
ERS request content-type header is outdated	ERS request content-type header is outdated.	The request resource version stated in the request content-type header is outdated. This means that the resource schema has been modified. One or more attributes may have been added or removed. To overcome that with the outdated schema, the ERS engine will use default values.
ERS XML input is a suspect for XSS or Injection attack	ERS XML input is a suspect for XSS or injection attack.	Review your XML input.
Backup Failed	The ISE backup operation failed.	Check the network connectivity between Cisco ISE and the repository. Ensure that: <ul style="list-style-type: none"> • The credentials used for the repository are correct. • There is sufficient disk space in the repository. • The repository user has write privileges.
CA Server is down	CA server is down.	Check to make sure that the CA services are up and running on the CA server.
CA Server is Up	CA server is up.	A notification is issued to inform the administrator that the CA server is up.
Certificate Expiration	This certificate will expire soon. When it expires, Cisco ISE may fail to establish secure communication with clients.	Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.
Certificate Revoked	Administrator has revoked the certificate issued to an endpoint by the internal CA.	Go through the BYOD flow again from the start to be provisioned with a new certificate.

Alarm Name	Alarm Description	Alarm Resolution
Certificate Provisioning Initialization Error	Certificate provisioning initialization failed.	More than one certificate found with the same value of CN (CommonName) attribute in the subject. Cannot build certificate chain. Check all the certificates in the system, including those from the SCEP (Simple Certificate Enrollment Protocol) server.
Certificate Replication Failed	Certificate replication to secondary node failed.	The certificate is not valid on the secondary node, or there is some other permanent error condition. Check the secondary node for a pre-existing, conflicting certificate. If found, delete the pre-existing certificate on the secondary node, and export the new certificate on the primary node, delete it, and import it in order to reattempt replication.
Certificate Replication Temporarily Failed	Certificate replication to secondary node temporarily failed.	The certificate was not replicated to a secondary node because of a temporary condition such as a network outage. The replication is retried until it succeeds.
Certificate Expired	This certificate has expired. Cisco ISE may fail to establish secure communication with clients. Node-to-node communication may also be affected.	Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.
Certificate Request Forwarding Failed	Certificate request forwarding failed.	Make sure that the certificate request that is coming in matches the attributes from the sender.
Configuration Changed	Cisco ISE configuration is updated. This alarm is not triggered for any configuration change in users and endpoints.	Check if the configuration change is expected.
CRL Retrieval Failed	Unable to retrieve CRL from the server. This occurs if the specified CRL is unavailable.	Ensure that the download URL is correct and is available for the service.

Alarm Name	Alarm Description	Alarm Resolution
DNS Resolution Failure	DNS resolution failed on the node.	Check if the DNS server configured by the ip name-server command is reachable. If you get the alarm as DNS Resolution failed for CNAME <hostname of the node> , ensure that you create CNAME RR along with the A record for each Cisco ISE node.
Firmware Update Required	A firmware update is required on this host.	Contact Cisco TAC to obtain firmware update.
Insufficient Virtual Machine Resources	Virtual Machine (VM) resources such as CPU, RAM, disk space, or IOPS (Input/output operations per second) are insufficient on this host.	Ensure that the minimum requirements for the VM host, as specified in the <i>Cisco ISE Hardware Installation Guide</i> .
NTP Service Failure	The NTP service is down on this node.	This could be because there is a large time difference between the NTP server and a Cisco ISE node (more than 1000 seconds). Ensure that your NTP server is working properly and use the ntp server <servername> CLI command to restart the NTP service and fix the time gap.
NTP Sync Failure	All the NTP servers configured on this node are unreachable.	Run the show ntp command from the CLI for troubleshooting. Ensure that the NTP servers are reachable from Cisco ISE. If NTP authentication is configured, ensure that the key ID and value matches with that of the server.
No Configuration Backup Scheduled	No Cisco ISE configuration backup is scheduled.	Create a schedule for configuration backup.
Operations DB Purge Failed	Unable to purge older data from the operations database. This occurs if the MnT nodes are busy.	Check the Data Purging Audit report and ensure that the used space is lesser than the threshold space. Log in to the MnT nodes using the CLI and perform the purge operation manually.
Profiler SNMP Request Failure	Either the SNMP request timed out, or the SNMP community or user authentication data is incorrect.	Ensure that SNMP is running on the NAD and verify that SNMP configuration on Cisco ISE matches with NAD.

Alarm Name	Alarm Description	Alarm Resolution
Replication Failed	The secondary node failed to consume the replicated message.	Log in to the Cisco ISE GUI and perform a manual synchronization from the Deployment window. Deregister and register back the affected Cisco ISE node.
Restore Failed	Cisco ISE restore operation failed.	Ensure network connectivity between Cisco ISE and the repository. Ensure that the credentials used for the repository is correct. Also ensure that the backup file is not corrupted. Execute the reset-config command from the CLI and restore the last-known good backup.
Patch Failure	A patch process has failed on the server.	Reinstall the patch process on the server.
Patch Success	A patch process has succeeded on the server.	—
External MDM Server API Version Mismatch	External MDM server API version does not match with what is configured in Cisco ISE.	Ensure that the MDM server API version is the same as what is configured in Cisco ISE. Update the Cisco ISE MDM server configuration, if needed.
External MDM Server Connection Failure	Connection to the external MDM server failed.	Ensure that the MDM server is up and the Cisco ISE-MDM API service is running on the MDM server.
External MDM Server Response Error	External MDM server response error.	Ensure that the Cisco ISE-MDM API service is running properly on the MDM server.
Replication Stopped	ISE node could not replicate configuration data from the PAN.	Log in to the Cisco ISE GUI to perform a manual synchronization from the Deployment window or deregister and register back the affected ISE node with the required field.
MDM Compliance Polling Disabled	Periodic compliance polling received huge non-compliance device information.	Keep the number of non-compliant device requests reaching the MDM server below 20000.
Endpoint certificates expired	Endpoint certificates were marked expired by daily the scheduled job.	Re-enroll the endpoint device to get a new endpoint certificate.
Endpoint certificates purged	Expired endpoint certificates were purged by the daily scheduled job.	No action is needed. This is an administrator-initiated clean-up operation.

Alarm Name	Alarm Description	Alarm Resolution
Endpoints Purge Activities	Purge the activities on endpoints for the past 24 hours. This alarm is triggered at midnight.	Review the purge activities by choosing Operations > Reports > Endpoints and Users > Endpoint Purge Activities .
Slow Replication Error	Slow or a stuck replication is detected.	Verify that the node is reachable and is a part of the deployment.
Slow Replication Info	Slow or stuck replication is detected.	Verify that the node is reachable and is part of the deployment.
Slow Replication Warning	Slow or a stuck replication is detected.	Verify that the node is reachable and part of the deployment.
PAN Auto Failover - Failover Failed	Promotion request to the Secondary Administration Node failed.	See the alarm details for further action.
PAN Auto Failover - Failover Triggered	Successfully triggered the failover of the Secondary Administration Node to Primary role.	Wait for the promotion of secondary PAN to complete, and bring up the old primary PAN.
PAN Auto Failover - Health Check Inactivity	PAN did not receive the health check monitoring request from the designated monitoring node.	Verify if the reported monitoring node is down or out-of-sync, and trigger a manual synchronization, if needed.
PAN Auto Failover - Invalid Health Check	Invalid health check monitoring request received for auto failover.	Verify if the health check monitoring node is out-of-sync, and trigger a manual synchronization if needed.
PAN Auto Failover - Primary Administration Node Down	PAN is down or is not reachable from the monitoring node.	Bring up the PAN, or wait for failover to happen.
PAN Auto Failover - Rejected Failover Attempt	Secondary administration node rejected the promotion request made by the health check monitor node.	See the alarm details for further action.
EST Service is down	EST service is down.	Make sure that the CA and EST services are up and running, and that the certificate services endpoint sub CA certificate chain is complete.
EST Service is up	EST service is up.	A notification is sent to inform the administrator that the EST service is up.
Smart Call Home Communication Failure	Smart Call Home messages were not sent successfully.	Ensure that there is network connectivity between Cisco ISE and Cisco Systems.

Alarm Name	Alarm Description	Alarm Resolution
Telemetry Communication Failure	Telemetry messages were not sent successfully.	Ensure that there is network connectivity between Cisco ISE and Cisco Systems.
Adapter not reachable	Cisco ISE cannot connect to the adapter.	Check the adapter logs for more details about the failure.
Adapter Error	Adapter has encountered an error.	Check the description of the alarm.
Adapter Connection Failed	The adapter cannot connect to the source server.	Ensure that the source server is reachable.
Adapter Stopped Due to Error	The adapter has encountered an error and is not in the desired state.	Ensure that the adapter configuration is correct and the source server is reachable. See the adapter logs for more details about the error.
Service Component Error	The service component has encountered an error.	Check the description of the alarm.
Service Component Info	The service component has sent a notification.	None.
ISE Services		
Excessive TACACS Authentication Attempts	The ISE Policy Service nodes are experiencing higher than expected rate of TACACS authentications.	<ul style="list-style-type: none"> • Check the re-auth timer in the network devices. • Check the network connectivity of the ISE infrastructure.
Excessive TACACS Authentication Failed Attempts	The ISE Policy Service nodes are experiencing higher than expected rate of failed TACACS authentications.	<ul style="list-style-type: none"> • Check the authentication steps to identify the root cause. • Check the ISE or NAD configuration for Identity and Secret mismatch.
MSE Location Server accessible again	MSE Location Server is accessible again.	None.
MSE Location Server not accessible.	MSE Location Server is not accessible, or is down.	Check if the MSE Location Server is up and running and is accessible from the ISE nodes.
AD Connector had to be restarted	AD Connector stopped unexpectedly and had to be restarted.	If this issue persists, contact Cisco TAC for assistance.

Alarm Name	Alarm Description	Alarm Resolution
Active Directory Forest is unavailable	Active Directory forest Global Catalog is unavailable, and cannot be used for authentication, authorization, and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
Authentication domain is unavailable	Authentication domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
ISE Authentication Inactivity	Cisco ISE policy service nodes are not receiving authentication requests from the network devices.	<ul style="list-style-type: none"> • Check the Cisco ISE and NAD configuration. • Check the network connectivity of the Cisco ISE and NAD infrastructure.
ID Map. Authentication Inactivity	No user authentication events were collected by the Identity Mapping Service in the last 15 minutes.	If user authentications are expected during this time, for example, during work hours, check the connection to the Active Directory domain controllers.
CoA Failed	Network device has denied the Change of Authorization (CoA) request issued by the Cisco ISE policy service nodes.	Ensure that the network device is configured to accept CoA from Cisco ISE. Check if CoA is issued on a valid session.
Configured nameserver is down	Configured nameserver is down or unavailable.	Check DNS configuration and network connectivity.
Supplicant Stopped Responding	Cisco ISE sent last message to the client 120 seconds ago, but there is no response from the client.	<ul style="list-style-type: none"> • Verify that the supplicant is configured properly to conduct a full EAP conversation with Cisco ISE. • Verify that NAS is configured properly to transfer EAP messages to and from the supplicant. • Verify that the supplicant or NAS does not have a short timeout for EAP conversation.

Alarm Name	Alarm Description	Alarm Resolution
Excessive Authentication Attempts	Cisco ISE policy service nodes are experiencing higher than expected rate of authentications.	<p>Check the reauthorization timer in the network devices. Check the network connectivity of the Cisco ISE infrastructure.</p> <p>After the threshold is met, the Excessive Authentication Attempts and Excessive Failed Attempts alarms are triggered. The numbers displayed next to the Description column are the total number of authentications that have succeeded or failed against Cisco ISE in the last 15 minutes.</p>
Excessive Failed Attempts	Cisco ISE policy service nodes are experiencing higher than expected rate of failed authentications.	<p>Check the authentication steps to identify the root cause. Check the Cisco ISE or NAD configuration for identity and secret mismatch.</p> <p>After the threshold is met, the Excessive Authentication Attempts and Excessive Failed Attempts alarms are triggered. The numbers displayed next to the Description column are the total number of authentications that have succeeded or failed against Cisco ISE in the last 15 minutes.</p>
AD: Machine TGT refresh failed	ISE server Ticket Granting Ticket (TGT) refresh has failed. The TGT is used for Active Directory connectivity and services.	Check that the ISE machine account exists and is valid. Also check for possible clock skew, replication, Kerberos configuration, or network errors, or all of them.
AD: ISE account password update failed	ISE server has failed to update it's AD machine account password.	Check that the ISE machine account password is not changed and that the machine account is not disabled or restricted. Check the connectivity to KDC.
Joined domain is unavailable	Joined domain is unavailable, and cannot be used for authentication, authorization, and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
Identity Store Unavailable	Cisco ISE policy service nodes are unable to reach the configured identity stores.	Check the network connectivity between Cisco ISE and the identity stores.

Alarm Name	Alarm Description	Alarm Resolution
Misconfigured Network Device Detected	Cisco ISE has detected too many RADIUS accounting information from NAS.	Too much duplicate RADIUS accounting information has been sent to ISE from NAS. Configure NAS with accurate accounting frequency.
Misconfigured Supplicant Detected	Cisco ISE has detected misconfigured supplicant on the network.	Ensure that the configuration on the supplicant is correct.
No Accounting Start	Cisco ISE policy service nodes have authorized a session, but did not receive accounting start from the network device.	Ensure that RADIUS accounting is configured on the network device. Check the network device configuration for local authorization.
Unknown NAD	Cisco ISE policy service nodes are receiving authentication requests from a network device that is not configured in Cisco ISE.	Check if the network device is a genuine request and add it to the configuration. Ensure that the secret matches.
SGACL Drops	Secure Group Access (SGACL) drops occurred. This occurs if a Trustsec-capable device drops packets because of SGACL policy violations.	Run the RBACL drop summary report and review the source causing the SGACL drops. Issue a CoA to the offending source to reauthorize or disconnect the session.
RADIUS Request Dropped	The authentication and accounting request from a NAD is silently discarded. This may occur because of unknown NAD, mismatched shared secrets, or invalid packet content per RFC.	Check that the NAD/AAA client has a valid configuration in Cisco ISE. Check whether the shared secrets on the NAD/AAA client and Cisco ISE match each other. Ensure that the AAA client and the network device, have no hardware problems or problems with RADIUS compatibility. Also, ensure that the network that connects the device to Cisco ISE has no hardware problems.
EAP Session Allocation Failed	A RADIUS request was dropped because EAP sessions limit is reached. This condition can be caused by too many parallel EAP authentication requests.	Wait for a few seconds before invoking another RADIUS request with a new EAP session. If system overload continues to occur, try restarting the ISE server.
RADIUS Context Allocation Failed	A RADIUS request was dropped due to system overload. This condition can be caused by too many parallel authentication requests.	Wait for a few seconds before invoking a new RADIUS request. If system overload continues to occur, try restarting the ISE server.

Alarm Name	Alarm Description	Alarm Resolution
AD: ISE machine account does not have the required privileges to fetch groups	Cisco ISE machine account does not have the required privileges to fetch groups.	Check if the Cisco ISE machine account has rights to fetch user groups in the Active Directory.
Posture Configuration Detection	The posture state synchronization port is not blocked for compliant authorization profiles.	Configure an ACL to block the posture state synchronization probe from reaching Cisco ISE if the client posture status is compliant.
System Health		
High Disk I/O Utilization	Cisco ISE system is experiencing high disk I/O utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.
High Disk Space Utilization	Cisco ISE system is experiencing high disk space utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.

Alarm Name	Alarm Description	Alarm Resolution
High Load Average	Cisco ISE system is experiencing high load average.	<p>Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.</p> <p>Do not use third-party tools to check the load average on a single CPU core because this metric would not reflect the overall system load. We recommend that you use the tech top command in the Cisco ISE CLI for a cumulative view of the system load.</p> <p>If the High Load Average alarm is seen against 2:00 a.m. time stamps for Primary and Secondary MnT nodes, note that CPU usage might be high due to DBMS statistics being run at that hour. CPU usage will be back to normal after the DBMS stats is complete.</p> <p>A High Load Average alarm is triggered at 1:00 a.m. every Sunday by a weekly maintenance task. This maintenance task rebuilds all the indexes that occupy more than 1 GB space. This alarm can be ignored.</p>

Alarm Name	Alarm Description	Alarm Resolution
High Memory Utilization	Cisco ISE system is experiencing high memory utilization.	<p>Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.</p> <p>Do not use third-party tools to check memory utilization. We recommend that you use the show memory command in the Cisco ISE CLI to check memory utilization.</p> <p>In a Cisco ISE node, its operating system manages memory utilization. You must check for the available memory (instead of free memory) metric for a more reliable measure of memory utilization.</p> <p>Note that an operating system segments most of the memory in buffer or cache. If less than 90% of the total memory is displayed as used, and there is no substantial increase in swap memory, Cisco ISE memory utilization can be considered stable.</p>
High Operations DB Usage	Cisco ISE monitoring nodes are experiencing higher volume of syslog data than expected.	Check and reduce the purge configuration window for the operations data.
High Authentication Latency	Cisco ISE system is experiencing high authentication latency.	Check if the system has sufficient resources. Check the actual amount of work on the system, for example, number of authentications, profiler activity, and so on. Add an additional server to distribute the load.
Health Status Unavailable	The monitoring node has not received the health status from the Cisco ISE node.	Ensure that Cisco ISE nodes are up and running, and are able to communicate with the monitoring nodes.
Process Down	One of the Cisco ISE processes is not running.	Restart the Cisco ISE application.
Profiler Queue Size Limit Reached	The ISE Profiler Queue Size Limit has been reached. Events received after reaching the queue size limit will be dropped.	Check if the system has sufficient resources, and ensure that the EndPoint attribute filter is enabled.

Alarm Name	Alarm Description	Alarm Resolution
OCSP Transaction Threshold Reached	The OCSP transaction threshold has been reached. This alarm is triggered when the internal OCSP service transaction has reached its threshold.	Check if the system has sufficient resources.
Licensing		
License About to Expire	License installed on the Cisco ISE nodes are about to expire.	See the Licensing window in Cisco ISE to view the license usage.
License Expired	License installed on the Cisco ISE nodes has expired.	Contact the Cisco Accounts team to purchase new licenses.
License Violation	Cisco ISE nodes have detected that you are exceeding or are about to exceed the allowed license count.	Contact the Cisco Accounts team to purchase additional licenses.
Smart Licensing Authorization Expired	Authorization for Smart Licensing has expired.	See the Cisco ISE License Administration window to manually renew registration for Smart Licensing or check your network connectivity with Cisco Smart Software Manager. Contact your Cisco partner if the issue persists.
Smart Licensing Authorization Renewal Failure	Renewal of authorization with Cisco Smart Software Manager has failed.	See the Cisco ISE License Administration window to manually renew authorization with Cisco Smart Software Manager using the Refresh button in the Licenses table. Contact your Cisco partner if issue persists.
Smart Licensing Authorization Renewal Success	Renewal of authorization with Cisco Smart Software Manager was successful.	Send notification to inform that authorization renewal of Cisco ISE with Cisco Smart Software Manager was successful.
Smart Licensing Communication Failure	Communication of Cisco ISE with Cisco Smart Software Manager has failed.	Check your network connectivity with Cisco Smart Software Manager. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.
Smart Licensing Communication Restored	Communication of Cisco ISE with Cisco Smart Software Manager was restored.	Send notification to inform that your network connectivity with Cisco Smart Software Manager has been restored.
Smart Licensing De-Registration Failure	Deregistration of Cisco ISE with Cisco Smart Software Manager has failed.	See the Cisco ISE License Administration window for additional details. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.

Alarm Name	Alarm Description	Alarm Resolution
Smart Licensing De-Registration Success	Deregistration of Cisco ISE with Cisco Smart Software Manager was successful.	Send notification to inform that deregistration of Cisco ISE with Cisco Smart Software Manager was successful.
Smart Licensing Disabled	Smart Licensing is disabled on Cisco ISE, and traditional licensing is in use.	See the License Administration window to enable Smart Licensing again. See the Cisco ISE Admin Guide or contact your Cisco partner to learn about using Smart Licensing on Cisco ISE.
Smart Licensing Evaluation Period Expired	Evaluation period of Smart Licensing has expired.	See the Cisco ISE License Administration window to register Cisco ISE with Cisco Smart Software Manager.
Smart Licensing HA Role changed	High-availability role change has occurred while using Smart Licensing.	Send notification to inform that the HA role of Cisco ISE has changed.
Smart Licensing Id Certificate Expired	Smart Licensing certificate has expired.	See the Cisco ISE License Administration window to manually renew registration for Smart Licensing. Contact your Cisco partner if the issue persists.
Smart Licensing Id Certificate Renewal Failure	Registration renewal for Smart Licensing with Cisco Smart Software Manager has failed.	See the Cisco ISE License Administration window to manually renew registration for Smart Licensing. Contact your Cisco partner if the issue persists.
Smart Licensing Id Certificate Renewal Success	Registration renewal for Smart Licensing with Cisco Smart Software Manager was successful.	Send notification to inform that registration renewal with Cisco Smart Software Manager was successful.
Smart Licensing Invalid Request	Invalid request was made to Cisco Smart Software Manager.	See the Cisco ISE License Administration window for additional details. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.
Smart Licensing Out of Compliance	Cisco ISE licenses are out of compliance.	See the ISE License Administration window for additional details. Contact your partner or Cisco account team to purchase new licenses.
Smart Licensing Registration Failure	Registration of Cisco ISE with Cisco Smart Software Manager has failed.	See the ISE License Administration window for additional details. Log in to Cisco Smart Software Manager or contact your Cisco partner if issue persists.

Alarm Name	Alarm Description	Alarm Resolution
Smart Licensing Registration Successful	Registration of Cisco ISE with Cisco Smart Software Manager was successful.	Send notification to inform that registration of Cisco ISE with Cisco Smart Software Manager was successful.
System Error		
Log Collection Error	The Cisco ISE monitoring collector process is unable to continue with the audit logs generated from the policy service nodes.	This will not impact the actual functionality of the Policy Service nodes. Contact Cisco TAC for further resolution.
Scheduled Report Export Failure	Unable to copy the exported report (CSV file) to the configured repository.	Verify the configured repository. If it has been deleted, add it back. If it is not available or is not reachable, reconfigure the repository to a valid one.
TrustSec		
Unknown SGT was provisioned	Unknown SGT was provisioned.	ISE provisioned an Unknown SGT as part of the authorization flow. Unknown SGT should not be assigned as part of a known flow.
Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration	Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration.	ISE identified some network devices that have a different IP-SGT mapping sets. Use the IP-SGT Mapping Deploy option to update the devices.
TrustSec SSH connection failed	TrustSec SSH connection failed.	ISE failed to establish SSH connection to a network device. Verify if the network device's SSH credentials in the Network Device window are similar to the credentials configured on the network device. Check the network device-enabled SSH connections from ISE (IP address).
TrustSec identified ISE was set to work with TLS versions other than 1.0	TrustSec-identified ISE was set to work with TLS versions other than 1.0.	TrustSec supports only TLS Version 1.0.
Trustsec PAC validation failed	Trustsec PAC validation failed.	ISE could not validate a PAC that was sent by the network device. Check the Trustsec device credentials in the Network Device window and in the device CLI. Make sure the device uses a valid PAC that was provisioned by the ISE server.

Alarm Name	Alarm Description	Alarm Resolution
Trustsec environment data download failed	Trustsec environment data download has failed.	Cisco ISE has received illegal Environment Data request. Verify the following: <ul style="list-style-type: none"> • PAC exists in the request, and is valid. • All the attributes exist in the request.
TrustSec CoA message ignored	TrustSec CoA message was ignored.	Cisco ISE sent a TrustSec CoA message and did not receive a response. Verify if the network device is CoA capable. Check the network device configuration.
TrustSec default egress policy was modified	TrustSec default egress policy was modified.	Make sure it is aligned with your security policy.



Note Alarms are not triggered when you add users or endpoints to Cisco ISE.

Alarm Settings

The following table describes the fields in the **Alarm Settings** window(**Administration > System > Settings > Alarm Settings > Alarm Configuration > Add**)

Field Name	Description
Alarm Type	Alarm type.
Alarm Name	Name of the alarm.
Description	Description for the alarm.
Suggested Actions	Action to be performed when the alarm is triggered.
Status	Enable or disable the alarm rule.
Severity	Select the severity level for your alarm. Valid options are: <ul style="list-style-type: none"> • Critical: Indicates a critical error condition. • Warning: Indicates a normal but significant condition. This is the default condition. • Info: Indicates an informational message.
Send Syslog Message	Send a syslog message for each system alarm that Cisco ISE generates.

Field Name	Description
Enter multiple e-mails separated with comma	List of e-mail addresses or ISE administrator names or both.
Notes in Email (0 to 4000 characters)	Custom text messages that you want associated with your system alarm.

Add Custom Alarms

Cisco ISE contains 12 default alarm types, such as High Memory Utilization and Configuration Changes. Cisco-defined system alarms are listed in the **Alarms Settings** window (**Administration > System > Settings > Alarm Settings**). You can only edit the system alarms.

In addition to existing system alarms, you can add, edit, or delete custom alarms under the existing alarm types.

For each alarm type, you can create a maximum of five alarms. The total number of alarms is limited to 200.

In the **Alarm Configuration** tab of the **Alarm Settings** window, the **Conditions** column displays details for four alarms: High Authentication Latency, High Disk I/O Utilization, High Disk Space Utilization, and High Memory Utilization. Each of these alarms has a configurable threshold value. However, the **Conditions** column may not display details even after the threshold values are configured. In such a scenario, re-edit the relevant threshold field for the alarm to view the details in the **Conditions** column.

Perform this procedure to add an alarm.

Step 1 Choose **Administration > System > Settings > Alarm Settings**.

Step 2 In the **Alarm Configuration** tab, click **Add**.

Step 3 Enter the required details. See the [Alarm Settings](#) section for more information.

Based on the alarm type (High Memory Utilization, Excessive RADIUS Authentication Attempts, Excessive TACACS Authentication Attempts, and so on), additional attributes are displayed in the **Alarm Configuration** window. For example, **Object Name**, **Object Type**, and **Admin Name** fields are displayed for Configuration Change alarms. You can add multiple instances of the same alarm with different criteria.

Step 4 Click **Submit**.

Cisco ISE Alarm Notifications and Thresholds

You can enable or disable Cisco ISE alarms and configure alarm notification behavior to notify you of critical conditions. For certain alarms, you can configure thresholds such as maximum failed attempts for the Excessive Failed Attempts alarm or maximum disk utilization for the High Disk Utilization alarm.

You can configure the notification settings on a per-alarm basis, and enter the email IDs of the users who have to be notified for each alarm (both system-defined and user-defined alarms).



Note The recipient email address specified at the alarm rule level overrides the global recipient email address setting.

Enable and Configure Alarms

-
- Step 1** Choose **Administration > System > Settings > Alarm Settings > Alarm Configuration**.
 - Step 2** Select an alarm from the list of default alarms by clicking on the radio button and click **Edit**.
 - Step 3** Select **Enable** or **Disable** from the **Status** drop-down list.
 - Step 4** Configure alarm threshold, if applicable.
 - Step 5** Click **Submit**.
-

Cisco ISE Alarms for Monitoring

Cisco ISE provides system alarms that notify you whenever any critical system condition occurs. Alarms that are generated by Cisco ISE are displayed in the Alarm dashlet. These notifications automatically appear in the Alarm dashlet.

The Alarm dashlet displays a list of recent alarms. From this list, you can choose which alarm's details you want to view. You can also receive notifications of alarms through e-mail and syslog messages.

View Monitoring Alarms

-
- Step 1** Go to the Cisco ISE **Dashboard**.
 - Step 2** Click on an alarm in the **Alarms** dashlet. A dialog box opens with the alarm details and a suggested action.
 - Step 3** Click **Refresh** to refresh the alarms.
 - Step 4** Acknowledge alarms to reduce the alarm counters (number of times an alarm is raised) by marking them as read. Select alarms for acknowledgement by checking the check boxes next to the timestamps.

Choose **Acknowledge Selected** from the **Acknowledge** drop-down list to mark as read all the alarms currently displayed in the window. By default, 100 rows are displayed in the window. You can choose a different number of rows to be displayed, by choosing a value from the **Rows/Page** drop-down list.

Choose **Acknowledge All** from the **Acknowledge** drop-down list to mark as read all the alarms in the list, whether or not they are currently displayed in the window.

Note When you check the check box next to the **Time Stamp** in the title row, all the alarms displayed in the window are selected. However, if you then uncheck a check box for one or more of the selected alarms, the select all function lapses. You will see that the check box next to the **Time Stamp** is unchecked at this point.

- Step 5** Click the **Details** link corresponding to the alarm that you select. A dialog box opens with the details corresponding to the selected alarm.

Note The **Details** link corresponding to the alarms that were generated prior to persona change shows no data.

Log Collection

Monitoring services collect log and configuration data, store the data, and then process it to generate reports and alarms. You can view the details of the logs that are collected from any of the servers in your deployment.

Alarm Syslog Collection Location

If you configure monitoring functions to send alarm notifications as syslog messages, you need a syslog target to receive the notification. Alarm syslog targets are the destinations where alarm syslog messages are sent.



Note Cisco ISE monitoring requires that the logging-source interface configuration use the network access server (NAS) IP address. You must configure a switch for Cisco ISE monitoring.

You must also have a system that is configured as a syslog server to be able to receive syslog messages. You can create, edit, and delete alarm syslog targets.

To configure a remote logging target as an alarm target, perform this procedure.

- Step 1** Choose **Administration > System > Logging > Remote Logging Targets**.
- Step 2** Click **Add**.
- Step 3** In the **New Logging Target** window, submit the required details for the logging target, and check the **Include Alarms for this Target** check box.

RADIUS Live Logs

The following table describes the fields in the Live logs window that displays the recent RADIUS authentications. The navigation path for this page is: **Operations > RADIUS > Live Logs**. Note that you can view the RADIUS live logs only in the Primary PAN.

Table 2: RADIUS Live Logs

Field Name	Description
Time	Shows the time at which the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is mandatory and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.

Field Name	Description
Details	<p>Clicking the icon under the Details column opens the Authentication Detail Report in a new browser window. This report offers information about authentication and related attributes, and authentication flow.</p> <p>Clicking the icon under the Details column opens the Accounting Detail report if an accounting event is processed for that session. If the session is in authenticated state, Authentication Detail report is displayed when you click the icon under the Details column.</p> <p>The Response Time in the Authentication Detail report is the total time taken by Cisco ISE to process the authentication flow. For example, if authentication consists of three roundtrip messages that took 300 ms for the initial message, 150 ms for the next message, and 100 ms for the last, Response Time is $300 + 150 + 100 = 550$ ms.</p> <p>Note You cannot view the details for endpoints that are active for more than 48 hours. You will see a window with the following message when you click the Details icon for endpoints that are active for more than 48 hours: No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.</p>
Repeat Count	Shows the number of time the authentication requests were repeated in the last 24 hours, without any change in the context of identity, network devices, and authorization.
Identity	<p>Shows the logged in username that is associated with the authentication.</p> <p>If the username is not present in any ID Store, it is displayed as <code>INVALID</code>. If the authentication fails due to any other reason, it is displayed as <code>USERNAME</code>.</p> <p>Note This is applicable only for users, and not for MAC addresses.</p> <p>To aid in debugging, you can force Cisco ISE to display invalid usernames. Check the Disclose Invalid Usernames check box under Administration > System > Settings > Protocols > RADIUS > Suppression & Reports > Authentication Details. This option is disabled automatically after 30 minutes.</p>
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.
IP Address	Shows the IP address of the endpoint device.

Field Name	Description
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.
MDM Server Name	Shows the name of the MDM server.
Event	Shows the event status.
Failure Reason	Shows the detailed reason for failure, if the authentication failed.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Security Group	Shows the group that is identified by the authentication log.
Session ID	Shows the session ID.



Note In the **RADIUS Live Logs** and **TACACS+ Live Logs** window, a Queried PIP entry appears for the first attribute of each policy authorization rule. If all the attributes within the authorization rule are related to a dictionary that was already queried for previous rules, no additional Queried PIP entry appears.

You can do the following in the **RADIUS Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.



Note All the user customizations are stored as user preferences.

TACACS Live Logs

The following table describes the fields in the TACACS Live Logs window that displays the TACACS+ AAA details. The navigation path for this page is: **Operations > TACACS > Live Logs**. You can view the TACACS live logs only in the Primary PAN.

Table 3: TACACS Live Logs

Field Name	Usage Guidelines
Generated Time	Shows the syslog generation time based on when a particular event was triggered.
Logged Time	Shows the time when the syslog was processed and stored by the Monitoring node. This column is mandatory and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information about the selected authentication scenario. This column is required and cannot be deselected.
Session Key	Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.
Username	Shows the user name of the device administrator. This column is required and cannot be deselected.
Type	Consists of two Types—Authentication and Authorization. Shows names of users who have passed or failed authentication, authorization, or both. This column is mandatory and cannot be deselected.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
ISE Node	Shows the name of the ISE node through which the access request is processed.
Network Device Name	Shows the names of network devices.
Network Device IP	Shows the IP addresses of network devices whose access requests are processed.
Network Device Groups	Shows the name of corresponding network device groups to which a network device belongs.
Device Type	Shows the device type policy that is used to process access requests from different network devices.

Field Name	Usage Guidelines
Location	Shows the location-based policy that is used to process access requests from network devices.
Device Port	Shows the device port number through which the access request is made.
Failure Reason	Shows the reason for rejecting an access request that is made by a network device.
Remote Address	Shows the IP address, MAC address, or any other string that uniquely identifies the end station.
Matched Command Set	Shows the MatchedCommandSet attribute value if it is present, or an empty value if the MatchedCommandSet attribute value is empty or the attribute itself does not exist in the syslog.
Shell Profile	Shows the privileges that were granted to a device administrator for executing commands on the network device.

You can do the following in the **TACACS Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.



Note All the user customizations are stored as user preferences.

Live Authentications

You can monitor recent RADIUS authentications as they occur, from the **Live Authentications** window. The window displays the top ten RADIUS authentications in the last 24 hours. This section explains the functions of the **Live Authentications** window.

The **Live Authentications** window shows the live authentication entries corresponding to the authentication events as they happen. In addition to authentication entries, this window also shows the live session entries corresponding to the events. You can also drill-down a session to view a detailed report corresponding to that session.

The **Live Authentications** window provides a tabular account of recent RADIUS authentications, in the order in which they occur. The last update shown at the bottom of the **Live Authentications** window shows the date of the server, time, and timezone.



Note If the password attribute in an Access-Request packet is empty, an error message is triggered and the access request fails.

When a single endpoint is authenticated successfully, two entries appear in the **Live Authentications** window—one corresponding to the authentication record and another corresponding to the session record (pulled from the session live view). Subsequently, when the device performs another successful authentication, the repeat counter corresponding to the session record is incremented. The Repeat Counter that appears in the **Live Authentications** window shows the number of duplicate RADIUS authentication success messages that are suppressed.

See the Live Authentication data categories that are shown by default. These are described in the Recent RADIUS Authentications section.

You can choose to view all the columns, or only selected data columns. After selecting the columns that you want to be displayed, you can save your selections.

Monitor Live Authentications

- Step 1** Choose **Operations > RADIUS > Live logs**.
- Step 2** From the **Refresh** drop-down list, choose a time interval to change the data refresh rate.
- Step 3** Click the **Refresh** icon to manually update the data.
- Step 4** From the **Show** drop-down list, choose an option to change the number of records that appear.
- Step 5** From the **Within** drop-down list, choose an option to specify a time interval.
- Step 6** Click **Add or Remove Columns** and choose the options from the drop-down list to change the columns that are displayed.
- Step 7** Click **Save** at the bottom of the window to save your modifications.
- Step 8** Click **Show Live Sessions** to view the live RADIUS sessions.

You can use the dynamic Change of Authorization (CoA) feature for the live sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD).

Filter Data in the Live Authentications Page

Using the filters in the **Live Authentications** window, you can filter the information that you need, and troubleshoot network authentication issues quickly. You can filter records in the Authentication **Live Logs** window and view only those records that you are interested in. The authentication logs contain many details, and filtering the authentications by a particular user or location helps you scan the data quickly. You can use several operators that are available in the **Live Authentications** window to filter out records based on your search criteria.:

- 'abc' : Contains 'abc'
- '!abc' : Does not contain 'abc'
- '{}' : Is empty
- '!{}' : Is not empty

- 'abc*' : Starts with 'abc'
- '*abc' : Ends with 'abc'
- '\!', '*', '\{', '\\' : Escape

The Escape option allows you to filter text with special characters (including the special characters used as filters). You must prefix the special character with a backward slash (\). For example, if you want to view the authentication records of users with identity "Employee!", enter "Employee\!" in the **Identity Filter** field. In this example, Cisco ISE considers the exclamation mark (!) as a literal character and not as a special character.

In addition, the **Status** field allows you to filter only passed authentication records, failed authentications, live sessions, and so on. The green check mark filters all the passed authentications that occurred in the past. The red cross mark filters all failed authentications. The blue i icon filters all the live sessions. You can also choose to view a combination of these options.

Step 1 Choose **Operations > RADIUS > Live Logs**.

Step 2 Filter data based on any of the fields in the **Show Live Authentications** window.

You can filter the results based on passed or failed authentications, or live sessions.

RADIUS Live Sessions

The following table describes the fields in the **RADIUS Live Sessions** window, which displays live authentications. The navigation path for this page is: **Operations > RADIUS > Live Sessions**. You can view the RADIUS live sessions only in the Primary PAN.

Table 4: RADIUS Live Sessions

Field Name	Description
Initiated	Shows the timestamp when the session was initiated.
Updated	Shows the timestamp when the session was last updated because of a change.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of an endpoint device.
Action	Click the Actions icon to reauthenticate an active RADIUS session or disconnect an active RADIUS session.
Repeat Count	Shows the number of times a user or endpoint is reauthenticated.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of an endpoint device.
IP Address	Shows the IP address of an endpoint device.

Field Name	Description
Audit Session ID	Shows a unique session identifier.
Account Session ID	Shows a unique ID provided by a network device.
Endpoint Profile	Shows the endpoint profile for a device.
Posture Status	Shows the status of posture validation and details of the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service node from which the log was generated.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows an authorization profile that was used for authentication.
NAS IP Address	Shows the IP address of a network device.
Device Port	Shows the connected port to a network device.
PRA Action	Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.
ANC Status	Adaptive Network Control status of a device as Quarantine , Unquarantine , or Shutdown .
WLC Roam	Shows the boolean (Y/N) used to track if an endpoint has been handed off during roaming, from one Wireless Lan Controller (WLC) to another. It has the value of <code>cisco-av-pair=nas-update=Y</code> or <code>N</code> . Note Cisco ISE relies on the <code>nas-update=true</code> attribute from WLC to identify whether the session is in roaming state. When the original WLC sends an accounting stop attribute with <code>nas-update=true</code> , the session is not deleted in ISE to avoid reauthentication. If roaming fails, ISE clears the session after five days of inactivity.
Packets In	Shows the number of packets received.
Packets Out	Shows the number of packets sent.
Bytes In	Shows the number of bytes received.

Field Name	Description
Bytes Out	Shows the number of bytes sent.
Session Source	Indicates whether it is a RADIUS session or a Passive ID session.
User Domain Name	Shows the registered DNS name of a user.
Host Domain Name	Shows the registered DNS name of a host.
User NetBIOS Name	Shows the NetBIOS name of a user.
Host NetBIOS Name	Shows the NetBIOS name of a host.
License Type	Shows the type of license used, Base, Plus, Apex, or Plus and Apex.
License Details	Shows the license details.
Provider	<p>Endpoint events are learned from different syslog sources. These syslog sources are referred to as providers.</p> <ul style="list-style-type: none"> • Windows Management Instrumentation (WMI): WMI is a Windows service that provides a common interface and object model to access management information about operating system, devices, applications, and services. • Agent: A program that runs on a client on behalf of the client or another program. • Syslog: A logging server to which a client sends event messages. • REST: A client is authenticated through a terminal server. The TS Agent ID, Source Port Start, Source Port End, and Source First Port values are displayed for this syslog source. • Span: Network information is discovered using span probes. • DHCP: DHCP event. • Endpoint <p>Note When two events from different providers are learned or obtained from an endpoint session, the providers are displayed as comma-separated values in the Live Sessions window.</p>
MAC Address	Shows the MAC address of a client.
Endpoint Check Time	Shows the time at which an endpoint was last checked by the endpoint probe.
Endpoint Check Result	<p>Shows the result of an endpoint probe. The possible values are:</p> <ul style="list-style-type: none"> • Unreachable • User Logout • Active User

Field Name	Description
Source Port Start	(Values are displayed only for the REST provider) Shows the first port number in a port range.
Source Port End	(Values are displayed only for the REST provider) Shows the last port number in a port range.
Source First Port	(Values are displayed only for the REST provider) Shows the first port allocated by the Terminal Server Agent. A Terminal Server refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilitates the connection of the multiple endpoints to a LAN network. The multiple endpoints appear to have the same IP address, and therefore, it is difficult to identify the IP address of a specific user. Consequently, to identify a specific user, a Terminal Server Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port user mapping.
TS Agent ID	(Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server Agent that is installed on an endpoint.
AD User Resolved Identities	(Values are displayed only for AD user) Shows the potential accounts that matched.
AD User Resolved DNs	(Values are displayed only for AD user) Shows the Distinguished Name of AD user, for example, CN=chris,CN=Users,DC=R1,DC=com

Export Summary

You can view the details of the reports exported by all the users in the last seven days, along with the status. The export summary includes both the manual and scheduled reports. The **Export Summary** window is automatically refreshed every two minutes. Click the **Refresh** icon to refresh the **Export Summary** window manually.

The super admin can cancel the export that is **In-Progress** or in **Queued** state. Other users are allowed only to cancel the export process that they have initiated.

By default, only three manual export of reports can run at a given point of time; the remaining triggered manual export of reports are queued. There are no such limits for the scheduled export of reports.

The following table describes the fields in the **Export Summary** window. The navigation path for this page is: **Operations > Reports > Export Summary**.

Table 5: Export Summary

Field Name	Description
Report Exported	Displays the name of the report.
Exported By	Shows the role of the user who initiated the export process.
Scheduled	Shows whether the report export is a scheduled one.

Field Name	Description
Triggered On	Shows the time at which the export process has been triggered in the system.
Repository	Displays the name of the repository where the exported data will be stored.
Filter Parameters	Shows the filter parameters selected while exporting the report.
Status	Shows the status of the exported reports. It can be one of the following: <ul style="list-style-type: none"> • Queued • In-progress • Completed • Cancellation-in-progress • Cancelled • Failed • Skipped <p>Note Failed status indicates the reason for failure. Skipped status indicates that the scheduled export of reports is skipped because the primary MnT node is down.</p>

You can do the following in the **Export Summary** window:

- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.

Authentication Summary Report

You can troubleshoot network access for a specific user, device, or search criteria based on the attributes that are related to the authentication requests. You can do this by running an Authentication Summary report.



Note You can generate the Authentication Summary report only for the last 30 days.

Troubleshoot Network Access Issues

- Step 1** Choose **Operations > Reports > Authentication Summary Report**.
- Step 2** Filter the report for the **Failure Reasons**.
- Step 3** Review the data in the **Authentication by Failure Reasons** section of the report to troubleshoot your network access problem.

Note Because the Authentication Summary report collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

Diagnostic Troubleshooting Tools

Diagnostic tools help you diagnose and troubleshoot problems on a Cisco ISE network and provide detailed instructions on how to resolve problems. You can use these tools to troubleshoot authentications and evaluate the configuration of any network device on your network, including TrustSec devices.

The RADIUS Authentication Troubleshooting Tool

This tool allows you to search for and select a RADIUS authentication or an Active Directory-related RADIUS authentication for troubleshooting when there is an unexpected authentication result. Use this tool if you expected an authentication to pass, but it failed, or if you expected a user or machine to have a certain level of privileges, and the user or machine did not have those privileges.

- Searching RADIUS authentications based on Username, Endpoint ID, Network Access Service (NAS) IP address, and reasons for authentication failure for troubleshooting, Cisco ISE displays authentications only for the system (current) date.
- Searching RADIUS authentications based on NAS port for troubleshooting, Cisco ISE displays all the NAS port values since the beginning of the previous month to the current date.



Note When searching for RADIUS authentications based on NAS IP Address and Endpoint ID Fields, a search is first performed in the operational database, and then in the configuration database.

Troubleshoot Unexpected RADIUS Authentication Results

- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > > General Tools > RADIUS Authentication Troubleshooting**.
- Step 2** Specify the search criteria in the fields, as needed.
- Step 3** Click **Search** to display the RADIUS authentications that match your search criteria.
If you are searching for Active Directory-related authentication, and an Active Directory server is not configured in your deployment, a message stating *AD not configured* is displayed.
- Step 4** Select a RADIUS authentication record from the table, and click **Troubleshoot**.
To troubleshoot Active Directory-related authentication, access the Diagnostics Tool under **Administration > Identity Management > External Identity Sources > Active Directory > AD node**.
- Step 5** Click **User Input Required**, modify the fields, as needed, and then click **Submit**.
- Step 6** Click **Done**.

- Step 7** Click **Show Results Summary** after the troubleshooting is complete.
- Step 8** (Optional) To view the diagnosis, the steps taken to resolve the problem, and the troubleshooting summary, click **Done**.
-

The Execute Network Device Command Diagnostic Tool

The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device.


The results that are displayed are the same as what you would see on a console. The tool enables you to identify problems, if any, in a device configuration.

Use this tool to validate the configuration of any network device, or if you are want to know how a network device is configured.

To access the Execute Network Device Command diagnostic tool, choose one of the following navigation paths:

1. Choose **Operations > Troubleshoot > Diagnostic Tools > Execute Network Device Command**. Choose **Work Centers > Profiler > Troubleshoot > Execute Network Device Command**.
2. In the **Execute Network Device Command** window that is displayed, enter the IP address of the network device and the **show** command that you want to run in the corresponding fields.
3. Click **Run**.

Execute Cisco IOS show Commands to Check Configuration

- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Execute Network Device Command**.
- Step 2** In the Cisco ISE GUI, click the **Menu** icon () and choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Execute Network Device Command**.
- Step 3** Enter the information in the appropriate fields.
- Step 4** Click **Run** to execute the command on the specified network device.
- Step 5** Click **User Input Required**, and modify the fields, as necessary.
- Step 6** Click **Submit** to run the command on the network device, and view the output.
-

The Evaluate Configuration Validator Tool

You can use this diagnostic tool to evaluate the configuration of a network device and identify configuration problems, if any. The **Expert Troubleshooter** compares the configuration of the device with the standard configuration.

Troubleshoot Network Device Configuration Issues

- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator**.

- Step 2** Enter the IP address of the network device that you want to evaluate in the **Network Device IP** field.
- Step 3** Check the check boxes and click the radio buttons next to the configuration options you want to compare against the recommended template.
- Step 4** Click **Run**.
- Step 5** In the **Progress Details...** area, click **Click Here to Enter Credentials**.
- Step 6** In the **Credentials Window** dialog box, enter the connection parameters and credentials that are required to establish a connection with the network devices.
- Step 7** Click **Submit**.
- Step 8** (Optional) To cancel the workflow, click **Click Here to Cancel the Running Workflow** in the **Progress Details...** window.
- Step 9** (Optional) Check the check boxes next to the interfaces that you want to analyze, and click **Submit**.
- Step 10** (Optional) Click **Show Results Summary** for details of the configuration evaluation.
-

Troubleshoot Endpoint Posture Failure

- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Posture Troubleshooting**.
- Step 2** Enter the information in the appropriate fields.
- Step 3** Click **Search**.
- Step 4** To find an explanation and determine a resolution for an event, select the event in the list and click **Troubleshoot**.
-

Session Trace Test Cases

This tool allows you to test policy flows in a predictable way to check and verify the way that the policy is configured, without needing to have real traffic originate from a real device.

You can configure the list of attributes and their values to be used in a test case. These details are used to perform interactions with the Policy system to simulate the run-time invocation of the policy.

The attributes can be configured by using dictionaries. All the dictionaries that are applicable to Simple RADIUS authentication are listed in the **Attributes** field.



Note You can configure test cases only for Simple RADIUS authentication.

Configure a Session Trace Test Case

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Session Trace Test Cases**.
- Step 2** Click **Add**.
- Step 3** In the **Test Details** tab, enter a name and description for the test case.
- Step 4** Select one of the predefined test cases or configure the required attributes and their values. The following predefined Test Cases are available:
- Basic Authenticated Access
 - Profiled Cisco Phones
 - Compliant Devices Access
 - Wi-Fi Guest (Redirect)
 - Wi-Fi Guest (Access)
- After you select a predefined test case, Cisco ISE automatically populates the relevant attributes for the test case. You can use the default values of these attributes or select a value from the displayed options. You can also add additional custom attributes to the test case.
- The attributes and the values that you add to the test case are listed in the **Text** field (below the **Custom Attributes** field). When you edit the content in the **Text** field, Cisco ISE checks the validity and syntax of the updated content.
- You can view the summary of all the attributes at the bottom of the **Test Details** window.
- Step 5** Click **Submit** .
- Cisco ISE validates the attributes and their values and indicates errors, if any, before saving the test details.
- Step 6** In the **Test Visualizer** tab, select the node on which you want to run this Test Case.
- Note** Only the nodes with Policy Service persona are displayed in the **ISE Node** drop-down list.
- Click **User Groups/Attributes** to retrieve the groups and attributes for a user from an external identity store.
- Step 7** Click **Execute**.
- Cisco ISE executes the Test Case and displays the step-by-step results of the test case in a tabular format. It displays the policy stages, matching rules, and result objects. Click the green icon to view the details for each step.
- Step 8** (Optional) Click the **Previous Test Executions** tab to view the results of previous test executions. You can also select and compare any two test cases. Cisco ISE displays the comparative view of the attributes for each test case in a tabular format.
- Step 9** You can launch the Session Trace Test Case tool from the **RADIUS Live Logs** window. You can select an entry on the **Live Logs** window and click the **Actions** icon (in the **Details** column) to launch the **Session Trace Test Case** tool. Cisco ISE extracts the relevant attributes and their values from the corresponding log entry. You can modify these attributes and values, if required, and execute the test case.
-

Technical Support Tunnel for Advanced Troubleshooting

Cisco ISE uses the Cisco IronPort Tunnel infrastructure to create a secure tunnel for Cisco technical support engineers to connect to an ISE server and troubleshoot issues with the system. Cisco ISE uses SSH to create the secure connection through the tunnel.

As an administrator, you can control the tunnel access—you can choose when and how long to grant access to a support engineer. Cisco Customer Support cannot establish the tunnel without your intervention. You will receive notifications about the service logins. You can disable the tunnel connection at any point of time. By default, the technical support tunnel remains open for 72 hours. However, we recommend that you or the support engineer close the tunnel after all the troubleshooting work is complete. Note that you can choose to extend the tunnel beyond 72 hours, if needed.

Use the **tech support-tunnel enable** command to initiate a tunnel connection.

The **tech support-tunnel status** command displays the status of the connection. This command provides information on whether the connection is established or not, if there is an authentication failure, or if the servers are unreachable. If the tunnel server is reachable, but ISE is unable to authenticate, ISE tries to authenticate again every five minutes for a period of 30 minutes, after which the tunnel is disabled.

You can disable the tunnel connection using the **tech support-tunnel disable** command. This command disconnects an existing tunnel even if a support engineer is currently logged in.

If you have already established a tunnel connection from an ISE server, the SSH keys that are generated are available on the ISE server. When you try to enable the support tunnel at a later point of time, the system prompts you about reusing the SSH keys generated earlier. You can choose to use the same keys or generate new keys. You can also manually reset the keys using the **tech support-tunnel resetkey** command. If you execute this command when a tunnel connection is enabled, the system prompts you to disable the connection first. If you choose to continue with the existing connection and not disable the connection the keys are reset after the existing connection is disabled. If you choose to disable the connection, the tunnel connection is dropped and the keys are reset immediately.

After you establish a tunnel connection, you can extend it using the **tech support-tunnel extend** command.

See the [Cisco Identity Services Engine CLI Reference Guide](#) for usage guidelines about the **tech support-tunnel** command.

Establish a Technical Support Tunnel

You can establish a secure tunnel through the Cisco ISE CLI.

-
- Step 1** Enter the following command from the Cisco ISE CLI:
- ```
tech support-tunnel enable
```
- The system prompts you for a password and a nickname for the tunnel.
- Step 2** Enter the password.
- Step 3** (Optional) Enter a nickname for the tunnel.
- The system generates an SSH key and displays the password, device serial number, and the SSH key.
- Step 4** Copy the password, device serial number, and SSH key and send it to Cisco Customer Support.

The support engineer can now securely connect to your ISE server. You will receive periodic notifications about service logins.

---

## TCP Dump Utility to Validate Incoming Traffic

The TCP Dump Utility sniffs packets that you can use to verify if the expected packet has reached a node. For example, when there is no incoming authentication or log indicated in the report, you may suspect that there is no incoming traffic, or that the incoming traffic cannot reach Cisco ISE. In such cases, you can run this tool to validate.

You can configure the TCP dump options and then collect data from the network traffic to help you troubleshoot a network issue.



---

**Caution** Starting a TCP Dump automatically deletes a previous dump file. To save a previous dump file, perform the task, as described in the Saving a TCP Dump File section before you begin a new TCP Dump session.

---


## Use TCP Dump to Monitor Network Traffic

### Before you begin

The **Network Interface** drop-down list in the **TCP Dump** window displays only the network interface cards (NICs) that have an IPv4 or IPv6 address configured. By default in VMware, all the NICs are connected, which means that all the NICs have an IPv6 address and are displayed in the **Network Interface** drop-down list.

---

**Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**.

**Step 2** In the Cisco ISE GUI, click the **Menu** icon () and choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**.

**Step 3** From the **Host Name** drop-down list, choose the source for the TCP Dump utility.

**Step 4** From the **Network Interface** drop-down list, choose an interface to monitor.

**Step 5** Click the **Promiscuous Mode** toggle button to On or Off. The default is On.

Promiscuous mode is the default packet sniffing mode in which the network interface passes all the traffic to the system's CPU. We recommend that you leave it On.

**Step 6** In the **Filter** field, enter a boolean expression on which to filter.

The following are supported standard TCP dump filter expressions:

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

- Step 7** Click **Start** to begin monitoring the network.
- Step 8** Click **Stop** after you have collected a sufficient amount of data, or wait for the process to conclude automatically after accumulating the maximum number of packets which is 500,000.



**Note** Cisco ISE does not support frames greater than 1500 MTU (jumbo frames).

## Save a TCP Dump File

### Before you begin


You should have successfully completed the task, as described in [Using TCP Dump to Monitor network Traffic](#) section.



**Note** You can also access TCP Dump through the Cisco ISE CLI. For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.

- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**.
- Step 2** From the **Format** drop-down list, choose an option. **Human Readable** is the default.
- Step 3** Click **Download**, corresponding to the desired location, and then click **Save**.
- Step 4** (Optional) To get rid of the previous dump file without saving it, click **Delete**.

## Compare Unexpected SGACL for an Endpoint or User

- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > TrustSec Tools > Egress (SGACL) Policy**.
- Step 2** In the Cisco ISE GUI, click the **Menu** icon () and choose **Operations > Troubleshoot > Diagnostic Tools > TrustSec Tools > Egress (SGACL) Policy**.
- Step 3** Enter the network device IP address of the TrustSec device whose SGACL policy you want to compare.
- Step 4** Click **Run**.
- Step 5** Click **User Input Required** and modify the fields, as necessary.
- Step 6** Click **Submit**.
- Step 7** Click **Show Results Summary** to view the diagnosis and suggested resolution steps.

## Egress Policy Diagnostic Flow

The Egress Policy diagnostic tool uses the process described in the following table:

| Process Stage | Description                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1             | Connects a the device with the IP address that you provided, and obtains the access control lists (ACLs) for each source and destination SGT pair. |
| 2             | Checks the egress policy that is configured in Cisco ISE and obtains the ACLs for each source and destination SGT pair.                            |
| 3             | Compares the SGACL policy that is obtained from the network device with the SGACL policy that is obtained from Cisco ISE.                          |
| 4             | Displays the source and destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.                |

## Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings

**Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > SXP-IP Mappings** .

**Step 2** Enter the IP address of the network device.

**Step 3** Click **Select**.

**Step 4** Click **Run**.

The Expert Troubleshooter retrieves TrustSec SXP connections from the network device and again prompts you to select the peer SXP devices.

**Step 5** Click **User Input Required**, and enter the necessary information, in that field.

**Step 6** Check the check box of the peer SXP devices for which you want to compare SXP mappings, and enter the common connection parameters.

**Step 7** Click **Submit**.

**Step 8** Click **Show Results Summary** to view the diagnosis and resolution steps.

## Troubleshoot Connectivity Issues in a TrustSec-Enabled Network with IP-SGT Mappings

**Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > TrustSec Tools > IP User SGT**.

**Step 2** Enter the information in the fields, as needed.

**Step 3** Click **Run**.

You are prompted for additional input.

**Step 4** Click **User Input Required** and modify the fields, as necessary.

**Step 5** Click **Submit**.

**Step 6** Click **Show Results Summary** to view the diagnosis and resolution steps.

---

## Device SGT Tool

For devices that are enabled with the TrustSec solution, each network device is assigned an SGT value through RADIUS authentication. The Device SGT diagnostic tool connects to the network device (with the IP address that you provide) and obtains the network device SGT value. It then checks the RADIUS authentication records to determine the SGT value assigned most recently. Finally, it displays the Device-SGT pairs in a tabular format, and identifies whether the SGT values are the same or different.

## Troubleshoot Connectivity Issues in a TrustSec-Enabled Network by Comparing Device SGT Mappings

---

**Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > Device SGT**.

**Step 2** Enter the information in the fields, as needed.

The default port number for Telnet is 23 and SSH is 22.

**Step 3** Click **Run**.

**Step 4** Click **Show Results Summary** to view the results of the device SGT comparison.

---

## Obtaining Additional Troubleshooting Information

Cisco ISE allows you to download support and troubleshooting information from the Admin portal. You can use the support bundles to prepare diagnostic information for the Cisco Technical Assistance Center (TAC) to troubleshoot problems with Cisco ISE.



**Note** The support bundles and debug logs provide advanced troubleshooting information for TAC and are difficult to interpret. You can use the various reports and troubleshooting tools that Cisco ISE provides to diagnose and troubleshoot issues that you are facing in your network.

---

## Cisco ISE Support Bundle

You can configure the logs that you want to be a part of your support bundle. For example, you can configure logs from a particular service to be a part of your debug logs. You can also filter the logs based on dates.

The logs that you can download are categorized as follows:

- Full configuration database: Contains the Cisco ISE configuration database in a human-readable XML format. When you troubleshoot issues, you can import this database configuration into another Cisco ISE node to re-create the scenario.



- Debug logs: Captures bootstrap, application configuration, run-time, deployment, public key infrastructure (PKI) information, and monitoring and reporting.

Debug logs provide troubleshooting information for specific Cisco ISE components. To enable debug logs, see chapter 11 on *Logging*. If you do not enable the debug logs, all the informational messages (INFO) will be included in the support bundle. For more information, see [Cisco ISE Debug Logs, on page 50](#).

- Local logs: Contains syslog messages from the various processes that run on Cisco ISE.
- Core files: Contains critical information that helps identify the cause of a crash. These logs are created when the application crashes, and includes heap dumps.
- Monitoring and reporting logs: Contains information about alerts and reports.
- System logs: Contains Cisco Application Deployment Engine-related (ADE-related) information.
- Policy configuration: Contains policies configured in Cisco ISE in human-readable format.

You can download these logs from the Cisco ISE CLI by using the **backup-logs** command. For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.



---

**Note** For Inline Posture node, you cannot download the support bundle from the Admin portal. You must use the **backup-logs** command from the Cisco ISE CLI.

---

If you choose to download these logs from the Admin portal, you can do the following:

- Download only a subset of logs based on the log type, such as debug logs or system logs.
- Download only the latest *n* number of files for the selected log type. This option allows you to control the size of the support bundle and the time taken for download.

Monitoring logs provide information about the monitoring, reporting, and troubleshooting features. For more information about downloading logs, see [Download Cisco ISE Log Files, on page 49](#).

## Support Bundle

You can download the support bundle to your local computer as a simple tar.gpg file. The support bundle will be named with the date and time stamps in the format `ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar.gpg`. The browser prompts you to save the support bundle to an appropriate location. You can extract the content of the support bundle and view the README.TXT file, which describes the contents of the support bundle, as well as how to import the contents of the ISE database if it is included in the support bundle.

## Download Cisco ISE Log Files

You can download the Cisco ISE log files to look for more information while troubleshooting issues in your network.

You can also download system logs that include ADE-OS and other log files to troubleshoot installation and upgrade issues.

While downloading a support bundle, instead of entering an encryption key manually, you can choose to use a public key for encryption. If you choose this option, Cisco PKI will be used for encryption and decryption of the support bundle. Cisco TAC maintains the public and private keys. Cisco ISE uses the public keys to encrypt the support bundle. Cisco TAC can decrypt the support bundle using the private keys. Use this option if you want to provide the support bundle to Cisco TAC for troubleshooting. Use the shared key encryption if you are going to troubleshoot the issues on premise.

### Before you begin

- You must have Super Admin or System Admin privileges to perform the following task.
- You should have configured the debug logs and debug log levels.

---

**Step 1** Choose **Operations > Troubleshoot > Download Logs > Appliance Node List**.

**Step 2** Click the node from which you want to download the support bundles.

**Step 3** In the **Support Bundle** tab, choose the parameters that you want to be populated in your support bundle.

If you include all the logs, your support bundle will be excessively large and the download will take a long time. To optimize the download process, choose to download only the most recent *n* number of files.

**Step 4** Enter the **From** and **To** dates for which you want to generate the support bundle.

**Step 5** Choose one of the following:

- **Public Key Encryption:** Choose this option if you want to provide the support bundle to Cisco TAC for troubleshooting purposes.
- **Shared Key Encryption:** Choose this option if you want to troubleshoot the issues locally on premise. If you choose this option, you must enter the encryption key for the support bundle.

**Step 6** Enter and re-enter the encryption key for the support bundle.

**Step 7** Click **Create Support Bundle**.

**Step 8** Click **Download** to download the newly-created support bundle.

The support bundle is a tar.gpg file that is downloaded to the client system that is running your application browser.

---

### What to do next

Download debug logs for specific components.

## Cisco ISE Debug Logs

Debug logs provide troubleshooting information for various Cisco ISE components. Debug logs contain critical and warning alarms generated over the last 30 days, and information alarms generated over the last seven days. While reporting problems, you might be asked to enable these debug logs and send them for diagnosis and resolution of your problems.




---

**Note** Enabling debug logs with heavy load (such as monitoring debug logs) will generate alarms about high load.

---

## Obtain Debug Logs

- Step 1** Configure the components for which you want to obtain debug logs. See [Cisco ISE Components and Corresponding Debug Logs](#), on page 51.
- Step 2** [Download Debug Logs](#).

## Cisco ISE Components and Corresponding Debug Logs

*Table 6: Components and Corresponding Debug Logs*

| Component                         | Debug Log       |
|-----------------------------------|-----------------|
| Active Directory                  | ad_agent.log    |
| Cache Tracker                     | tracking.log    |
| Entity Definition Framework (EDF) | edf.log         |
| JMS                               | ise-psc.log     |
| License                           | ise-psc.log     |
| Notification Tracker              | tracking.log    |
| Replication-Deployment            | replication.log |
| Replication-JGroup                | replication.log |
| Replication Tracker               | tracking.log    |
| RuleEngine-Attributes             | ise-psc.log     |
| RuleEngine-Policy-IDGroups        | ise-psc.log     |
| accessfilter                      | ise-psc.log     |
| admin-infra                       | ise-psc.log     |
| boot-strap wizard                 | ise-psc.log     |
| cisco-mnt                         | ise-psc.log     |
| client                            | ise-psc.log     |
| cpm-clustering                    | ise-psc.log     |
| cpm-mnt                           | ise-psc.log     |
| epm-pdp                           | ise-psc.log     |
| epm-pip                           | ise-psc.log     |
| anc                               | ise-psc.log     |
| anc                               | ise-psc.log     |
| ers                               | ise-psc.log     |
| guest                             | ise-psc.log     |

| Component              | Debug Log           |
|------------------------|---------------------|
| Guest Access Admin     | guest.log           |
| Guest Access           | guest.log           |
| MyDevices              | guest.log           |
| Portal                 | guest.log           |
| Portal-Session-Manager | guest.log           |
| Portal-web-action      | guest.log           |
| guestauth              | ise-psc.log         |
| guestportal            | ise-psc.log         |
| identitystore-AD       | ise-psc.log         |
| infrastructure         | ise-psc.log         |
| ipsec-api              | api-service.log     |
| ipsec-ui               | ise-psc.log         |
| mdm                    | ise-psc.log         |
| mdm-pip                | ise-psc.log         |
| mnt-report             | reports.log         |
| mydevices              | ise-psc.log         |
| nsf                    | ise-psc.log         |
| nsf-session            | ise-psc.log         |
| org-apache             | ise-psc.log         |
| org-apache-cxf         | ise-psc.log         |
| org-apache-digester    | ise-psc.log         |
| posture                | ise-psc.log         |
| profiler               | profiler.log        |
| provisioning           | ise-psc.log         |
| policy-engine          | ise-psc.log         |
| prrt-JNI               | prrt-management.log |
| runtime-AAA            | prrt-management.log |
| runtime-config         | prrt-management.log |
| runtime-logging        | prrt-management.log |
| sponsorportal          | ise-psc.log         |
| swiss                  | ise-psc.log         |

# Download Debug Logs

## Before you begin

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose **Operations** > **Troubleshoot** > **Download Logs** > **Appliance Node List**.

**Step 2** From the Appliance node list, click the node for which you want to download the debug logs.

**Step 3** Click the **Debug Logs** tab.

A list of debug log types and debug logs is displayed. This list is based on your debug log configuration.

**Step 4** Click the log file that you want to download and save it to the system that is running your client browser.

You can repeat this process to download other log files as needed. The following are the additional debug logs that you can download from the **Debug Logs** window:

- isebootstrap.log: Provides bootstrapping log messages
  - monit.log: Provides watchdog messages
  - pki.log: Provides third-party crypto library logs
  - iseLocalStore.log: Provides logs about the local store files
  - ad\_agent.log: Provides Microsoft Active Directory third-party library logs
  - catalina.log: Provides third-party logs
-

