Monitoring and Troubleshooting Service in ISE-PIC

The Monitoring and troubleshooting service is a comprehensive identity solution for all Cisco ISE-PIC run-time services and uses the following components:

- Monitoring—Provides a real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and affect operational conditions.

- Troubleshooting—Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide a 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 for the Identity, Endpoint ID, and Node fields.

Learn more in this section about how you can manage ISE-PIC with monitoring, troubleshooting and reporting tools.

Live Sessions

The following table describes the fields in the **Live Sessions** window, which displays live sessions. From the main menu bar, choose **Live Sessions**.

Table 1: Live Sessions

Field Name	Description
Initiated	Shows the timestamp when the session was initiated.
Updated	Shows the timestamp when the session was last updated due to any change.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of the endpoint device.
Action	Click the Actions icon to open the **Actions** pop-up window. You can do the following: • Clear a session • Check the session status of current user
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of the endpoint device.
IP Address	Shows the IP address of the endpoint device.
Server	Indicates the PIC 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 the like.
Session Source	Indicates whether it is a RADIUS session or PassiveID session.
User Domain Name	Shows the registered DNS name of the user.
User NetBIOS Name	Shows the NetBIOS name of the user.

Field Name	Description
Provider	Endpoint events are learned from different syslog sources. These syslog sources are referred to as providers.
	• 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
	When two events from different providers are learned from an endpoint session, the providers are displayed as comma-separated values in the live sessions page.
MAC Address	Shows the MAC address of a client.
Endpoint Check Time	Shows the time at which the endpoint was last checked by the endpoint probe.
Endpoint Check Result	Shows the result of an endpoint probe. The possible values are:
	• Unreachable
	• User Logout
	• Active User
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 (TS) Agent.
	A Terminal Server (TS) refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilities 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 TS Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port-user mapping.

Field Name	Description
TS Agent ID	(Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server (TS) 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

Available Reports

The following table lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided.

Report Name	Description	Logging Category
IDC Reports		
AD Connector Operations	The AD Connector Operations report provides log of operations performed by AD Connector such as ISE-PIC Server password refresh, Kerberos tickets management, DNS queries, DC discovery, LDAP, and RPC Connections management, etc. If some AD failures are encountered, you can review the details in this report to identify the possible causes.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select AD Connector.
Administrator Logins	The Administrator Logins report provides information about all GUI-based administrator login events as well as successful CLI login events.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit.
Change Configuration Audit	The Change Configuration Audit report provides details about configuration changes within a specified time period. If you need to troubleshoot a feature, this report can help you determine if a recent configuration change contributed to the problem.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit.

Report Name	Description	Logging Category
Current Active Sessions	The Current Active Sessions report enables you to export a report with details about who was currently on the network within a specified time period. If a user isn't getting network access, you can see whether the session is authenticated or terminated or if there is another problem with the session.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select these logging categories: Accounting and RADIUS Accounting.
Health Summary	The Health Summary report provides details similar to the Dashboard. However, the Dashboard only displays data for the past 24 hours, and you can review more historical data using this report. You can evaluate this data to see consistent patterns in data. For example, you would expect heavier CPU usage when most employees start their work days. If you see inconsistencies in these trends, you can identify potential problems. The CPU Usage table lists the percentage of CPU usage for the different ISE-PIC functions. The output of the **show cpu usage** CLI command is presented in this table and you can correlate these values with the issues in your deployment to identify possible causes.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select these logging categories: Administrative and Operational Audit, System Diagnostics, and System Statistics.
Operations Audit	The Operations Audit report provides details about any operational changes, such as: running backups, registering a ISE-PIC node, or restarting an application.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit.
PassiveID	The Passive ID report enables you to monitor the state of WMI connection to the domain controller and gather statistics related to it (such as amount of notifications received, amount of user login/logouts per second etc.)	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Identity Mapping.

Report Name	Description	Logging Category
pxGrid Administrator Audit	The pxGrid Administrator Audit report provides the details of the pxGrid administration actions such as client registration, client deregistration, client approval, topic creation, topic deletion, publisher-subscriber addition, and publisher-subscriber deletion. Every record has the administrator name who has performed the action on the node. You can filter the pxGrid Administrator Audit report based on the administrator and message criteria.	—
System Diagnostic	The System Diagnostic report provides details about the status of the ISE-PIC nodes. If the ISE-PIC node is unable to register, you can review this report to troubleshoot the issue. This report requires that you first enable several diagnostic logging categories. Collecting these logs can negatively impact ISE-PIC performance. So, these categories are not enabled by default, and you should enable them just long enough to collect the data. Otherwise, they are automatically disabled after 30 minutes.	Choose **Administration** > **Logging** > **Logging Categories** and select these logging categories: Internal Operations Diagnostics, Distributed Management, Administrator Authentication and Authorization.
User Change Password Audit	The User Change Password Audit report displays verification about employee's password changes.	Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit.

Cisco ISE-PIC Alarms

Alarms notify you of conditions on a network and are displayed in the Alarms dashlet. There are three alarm severities: critical, warning and information. They also provide information on system activities, such as data purge events. You can 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 re-occurs, then the same alarms are suppressed for about an hour. During the time that the event re-occurs, depending up on the trigger, it may take about an hour for the alarms to re-appear.

The following table lists all the Cisco ISE-PIC alarms, descriptions and their resolution.

Table 2: Cisco ISE-PIC Alarms

Alarm Name	Alarm Description	Alarm Resolution
Administrative and Operational Audit Management		
Deployment Upgrade Failure	An upgrade has failed on an ISE PIC node.	Check the 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-PIC node.	Check the ADE.log on the failed node for upgrade failure reason and corrective actions.
Secure LDAP connection reconnect due to CRL found revoked certificate	CRL check result is 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 new certificate and install it on LDAP server.
Secure LDAP connection reconnect due to OCSP found revoked certificate	OCSP check result is 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 new certificate and install it on LDAP server.
Secure syslog connection reconnect due to CRL found revoked certificate	CRL check result is 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 new certificate and install it on syslog server.
Secure syslog connection reconnect due to OCSP found revoked certificate	OCSP check result is 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 new certificate and install it on syslog server.

Alarm Name	Alarm Description	Alarm Resolution
Administrator account Locked/Disabled	Administrator account is locked or disabled due to 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.
ERS identified deprecated URL	ERS identified deprecated URL	The request URL is deprecated and it is recommended to avoid using it.
ERS identified out-dated URL	ERS identified out-dated URL	The requested URL is out-dated and it is recommended to use a newer one. This URL will not be removed in future releases.
ERS request content-type header is out-dated	ERS request content-type header is out-dated.	The request resource version stated in the request content-type header is out-dated. That 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.	Please review your xml input.
Backup Failed	The Cisco ISE-PIC backup operation failed.	Check the network connectivity between Cisco ISE-PIC and the repository. Ensure that: • The credentials used for the repository is 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 to inform the administrator that the CA server is up.

Alarm Name	Alarm Description	Alarm Resolution
Certificate Expiration	This certificate will expire soon. When it expires, Cisco ISE-PIC 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-PIC 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 ISE-PIC flow from the beginning to be provisioned with a new certificate.
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.
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, delete it, and import it in order to re-attempt replication.
Certificate Replication Temporarily Failed	Certificate replication to secondary node temporarily failed	The certificate was not replicated to a secondary node due to a temporary condition such as a network outage. The replication will be retried until it succeeds.
Certificate Expired	This certificate has expired. Cisco ISE-PIC 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-PIC 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 certification request coming in matches with attributes from the sender.

Alarm Name	Alarm Description	Alarm Resolution
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 could occur if the specified CRL is unavailable.	Ensure that the download URL is correct and is available for the service.
DNS Resolution Failure	DNS resolution failed on the node.	Check if the DNS server configured by the command **ip name-server** is reachable. If you get the alarm as 'DNS Resolution failed for CNAME <hostname of the node>', then 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 Technical Assistance Center (TAC) to obtain firmware update
Insufficient Virtual Machine Resources	Virtual Machine (VM) resources such as CPU, RAM, Disk Space, or IOPS are insufficient on this host.	Ensure that a minimum requirements for the VM host, as specified in the Cisco ISE Hardware Installation Guide.
NTP Service Failure	The NTP service is down on this node.	This could be because there is a large time difference between NTP server and Cisco ISE-PIC node (more than 1000s). 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.	Execute **show ntp** command from the CLI for troubleshooting. Ensure that the NTP servers are reachable from Cisco ISE-PIC. 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-PIC configuration backup is scheduled.	Create a schedule for configuration backup.

Alarm Name	Alarm Description	Alarm Resolution
Operations DB Purge Failed	Unable to purge older data from the operations database. This could occur if M&T nodes are busy.	Check the Data Purging Audit report and ensure that the used_space is lesser than the threshold_space. Login to M&T nodes using CLI and perform the purge operation manually.
Replication Failed	The secondary node failed to consume the replicated message.	Login to the Cisco ISE-PIC GUI and perform a manual syncup from the deployment page. De-register and register back the affected Cisco ISE-PIC node.
Restore Failed	Cisco ISE-PIC restore operation failed.	Ensure the network connectivity between Cisco ISE-PIC and the repository. Ensure that the credentials used for the repository is correct. 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.	Re-install the patch process on the server.
Patch Success	A patch process has succeeded on the server.	-
Replication Stopped	ISE-PIC node could not replicate configuration data from the primary node.	Login to the Cisco ISE-PIC GUI to perform a manual syncup from the deployment page or de-register and register back the affected Cisco ISE-PIC node with required field.
Endpoint certificates expired	Endpoint certificates were marked expired by daily scheduled job.	Please re-enroll the endpoint device to get a new endpoint certificate.
Endpoint certificates purged	Expired endpoint certificates were purged by daily scheduled job.	No action needed - this was an administrator-initiated cleanup operation.
Slow Replication Error	Slow or a stuck replication is detected.	Please verify that the node is reachable and part of the deployment.
Slow Replication Info	Slow or a stuck replication is detected.	Please verify that the node is reachable and part of the deployment.
Slow Replication Warning	Slow or a stuck replication is detected .	Please verify that the node is reachable and part of the deployment.

Alarm Name	Alarm Description	Alarm Resolution
EST Service is down	EST Service is down.	Make sure that the CA and EST services are up and running and Certificate services endpoint Sub CA certificate chain is complete.
EST Service is up	EST Service is up.	A notification 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-PIC and Cisco systems.
Telemetry Communication Failure	Telemetry messages were not sent successfully.	Ensure that there is network connectivity between Cisco ISE and Cisco systems.
ISE Services		
AD Connector had to be restarted	AD Connector stopped unexpectedly and had to be restarted.	If this issue persists, contact the Cisco TAC for assistance.
Active Directory forest is unavailable	Active Directory forest GC (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.
ID Map. Authentication Inactivity	No User Authentication events were collected by the Identity Mapping service in the last 15 minutes.	If this is a time when User Authentications are expected (e.g. work hours), then check the connection to Active Directory domain controllers.
Configured nameserver is down	Configured nameserver is down or unavailable.	Check DNS configuration and network connectivity.
AD: Machine TGT refresh failed	ISE-PIC server TGT (Ticket Granting Ticket) refresh has failed; it is used for AD connectivity and services.	Check that the Cisco ISE-PIC machine account exists and is valid. Also, check for possible clock skew, replication, Kerberos configuration and/or network errors.
AD: ISE account password update failed	ISE-PIC server has failed to update it's AD machine account password.	Check that the Cisco ISE-PIC machine account password is not changed and that the machine account is not disabled or restricted. Check the connectivity to KDC.

Alarm Name	Alarm Description	Alarm Resolution
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-PIC policy service nodes are unable to reach the configured identity stores.	Check the network connectivity between Cisco ISE-PIC and identity store.
AD: ISE machine account does not have the required privileges to fetch groups	Cisco ISE-PIC machine account does not have the required privileges to fetch groups.	Check if the Cisco ISE-PIC machine account has rights to fetch user groups in Active Directory.
System Health		
High Disk I/O Utilization	Cisco ISE-PIC 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 etc. Add additional server to distribute the load.
High Disk Space Utilization	Cisco ISE-PIC 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 etc. Add additional server to distribute the load.
High Load Average	Cisco ISE-PIC system is experiencing high load average.	Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.
High Memory Utilization	Cisco ISE-PIC system is experiencing high memory utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.
High Operations DB Usage	Cisco ISE-PIC monitoring nodes are experiencing higher volume of syslog data than expected.	Check and reduce the purge configuration window for the operations data.
Health Status Unavailable	The monitoring node has not received health status from the Cisco ISE-PIC node.	Ensure that Cisco ISE-PIC nodes are up and running. Ensure that Cisco ISE-PIC nodes are able to communicate with the monitoring nodes.

Alarm Name	Alarm Description	Alarm Resolution
Process Down	One of the Cisco ISE-PIC processes is not running.	Restart the Cisco ISE-PIC application.
OCSP Transaction Threshold Reached	The OCSP transaction threshold has been reached. This alarm is triggered when internal OCSP service reach high volume traffic.	Please check if the system has sufficient resources.
Licensing		
PIC License Expired	License installed on the Cisco ISE-PIC nodes has expired.	Contact Cisco Accounts team to purchase new licenses.
PIC Licence expiring within 30 Days	License installed on the Cisco ISE-PIC nodes will be expiring in 30 days.	Contact Cisco Sales team for extension of the ISE-PIC license.
PIC Licence expiring within 60 Days	License installed on the Cisco ISE-PIC nodes will be expiring in 60 days.	Contact Cisco Sales team for extension of the ISE-PIC license.
PIC Licence expiring within 90 Days	License installed on the Cisco ISE-PIC nodes will be expiring in 90 days.	Contact Cisco Sales team for extension of the ISE-PIC license.
System Error		
Log Collection Error	Cisco ISE-PIC monitoring collector process is unable to persist the audit logs generated from the policy service nodes.	This will not impact the actual functionality of the Policy Service nodes. Contact TAC for further resolution.
Scheduled Report Export Failure	Unable to copy the exported report (CSV file) to configured repository.	Verify the configured repository. If it has been deleted, add it back. If it is not available or not reachable, reconfigure the repository to a valid one.

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

Alarm Settings

The following table describes the fields in the **Alarm Settings** window(**Settings** > **Alarm Settings**).

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.

Field Name	Description
Severity	Select the severity level for your alarm. Valid options are: • 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-PIC generates.
Enter multiple e-mails separated with comma	List of e-mail addresses or ISE-PIC 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-PIC contains 5 default alarm types, such as Configuration Changed, High Disk I/O Utilization, High Disk Space Utilization, High Memory Utilization and ISE Authentication Inactivity. Cisco-defined system alarms are listed in the Alarms Settings page (Settings > Alarms Settings). You can only edit the system alarms.

In addition to the 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 5 alarms and the total number of alarms is limited to 200.

To add an alarm:

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

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

Step 3   Enter the required details. Refer to the Alarm Settings section for more information.

Based on the alarm type, additional attributes are displayed in the Alarm Configuration page. For example, Object Name, Object Type, and Admin Name fields are displayed for Configuration Changed alarms. You can add multiple instances of same alarm with different criteria.

Step 4   Click **Submit**.

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.

Use TCP Dump to Monitor Network Traffic

The TCP Dump window lists TCP dump process files that you create. You can create different files for different purposes, run them as needed, and delete them when you don't need them.

You can control the data that is collected by specifying size, number of files, and how long the process runs. If the process finishes before the time limit, and the file is less than the maximum size, and you enabled more than one file, then the process continues and creates another dump file.

You can run TCP dump on more interfaces, including bonded interfaces.

✎

Note   Human-readable format is no longer an option; the dump file is always in raw format.

We support IPv6 connections to the repository.

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

Step 2   From the **Network Interface** drop-down list, choose an interface to monitor.

Step 3   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 4   Enter a **File Name** for this TCP dump process.

Step 5   From the **Repository** drop-down list, choose a repository to store TCP dump log files in.

Step 6   From the **File Size** drop-down list—Select a maximum file size.

If the dump exceeds this file size, a new file opens to continue the dump. The number of times the dump can continue to a new file is limited by the **Limit to** setting.

Step 7   The **Limit to** option can be used to limit the number of files that the dump can expand into.

Step 8   The **Time Limit** option can be used to configure how long a dump runs before ending.

Step 9   Set **Promiscuous Mode** by clicking **On** or **Off**. The default is **On**.

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

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   Click **Download**, corresponding to the desired location, and then click **Save**.

Step 2   (Optional) To get rid of the previous dump file without saving it, click **Delete**.

TCP Dump Settings

The following table describes the fields on the **tcpdump** utility page, which you use to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear. The navigation path for this page is: **Troubleshoot**.

Table 3: TCP Dump Settings

Option	Usage Guidelines
Status	• Stopped—the tcpdump utility is not running • Start—Click to start the tcpdump utility monitoring the networ • Stop—Click to stop the tcpdump utility
Host Name	Choose the name of the host to monitor from the drop-down list.
Network Interface	Choose the network interface to monitor from the drop-down list. **Note** You must configure all network interface cards (NICs) or IPv6 address so that they are displayed in the Cisco I portal.

Option	Usage Guidelines
Promiscuous Mode	• On—Click to turn on promiscuous mode (default). • Off—Click to turn off promiscuous mode. Promiscuous mode is the default packet sniffing mode. It is recommende leave it set to On. In this mode the network interface is passing all traffi system's CPU.
Filter	Enter a boolean expression on which to filter. Supported standard tcpdu expressions: ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123
Format	Select a format for the tcpdump file.

Dump File	Displays data on the last dump file, such as the following:
	
	Last created on Wed Apr 27 20:42:38 UTC 2011 by admin
	
	`File size: 3,744 bytes`
	`Format: Raw Packet Data`
	`Host Name: Positron`
	`Network Interface: GigabitEthernet 0`
	`Promiscuous Mode: On`
	
	• Download—Click to download the most recent dump file.
	
	• Delete—Click to delete the most recent dump file.

Logging Mechanism

Cisco ISE-PIC Logging Mechanism

Configure Syslog Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.

Active Directory Troubleshooting

Prerequisites for Integrating Active Directory and Cisco ISE-PIC

This section describes the manual steps required to configure Active Directory for integration with Cisco ISE-PIC. However, in most cases, you can enable Cisco ISE-PIC to automatically configure Active Directory. The following are the prerequisites to integrate Active Directory with Cisco ISE-PIC.

- Ensure you have Active Directory Domain Admin credentials, required to make changes to any of the AD domain configurations.

- Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE-PIC server and Active Directory. You can configure NTP settings from Cisco ISE-PIC CLI.

- You must have at least one global catalog server operational and accessible by Cisco ISE-PIC, in the domain to which you are joining Cisco ISE-PIC.

Active Directory Account Permissions Required to Perform Various Operations

Join Operations	Leave Operations	Cisco ISE-PIC Machine Accounts
The join operation requires the following account permissions: • Search Active Directory (to see if a Cisco ISE-PIC machine account exists) • Create Cisco ISE-PIC machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, CiscoISE-PIC machine account password, SPN, dnsHostname)	The leave operation requires the following account permissions: • Search Active Directory (to see if a Cisco ISE-PIC machine account exists) • Remove the Cisco ISE-PIC machine account from the domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain.	The ISE-PIC machine account that communicates to the Active Directory connection requires the following permissions: • Change password • Read the user and machine objects corresponding to users and machines that are contacted • Query Active Directory to get information (for example, trusted domains, alternative UPN suffixes, and so on) • Read the tokenGroups attribute You can precreate the machine account in Active Directory. If the SAM name matches the Cisco ISE-PIC appliance hostname, it is located during the join operation and re-used. If there are multiple join operations, multiple machine accounts are maintained inside Cisco ISE-PIC, one for each join.

Note	The credentials that are used for the join or leave operation are not stored in Cisco ISE-PIC. Only the newly created Cisco ISE-PIC machine account credentials are stored.

The **Network access: Restrict clients allowed to make remote calls to SAM** security policy in Microsoft Active Directory has been revised. Hence, Cisco ISE might not able to update its machine account password every 15 days. If the machine account password is not updated, Cisco ISE will no longer authenticate users through Microsoft Active Directory. You will receive the **AD: ISE password update failed** alarm on your Cisco ISE dashboard to notify you of this event.

Note	This issue happens in Windows Server 2016 Active Directory or later and Windows 10 version 1607 due to the restriction in them. To overcome this restriction, when you are integrating Windows Server 2016 Active Directory or later or Windows 10 version 1607 with Cisco ISE, you much set the registry value in the following registry from non-zero to blank to give access to all: Registry:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam This allows Cisco ISE to update its machine account password.

The security policy allows users to enumerate users and groups in the local Security Accounts Manager (SAM) database and in Microsoft Active Directory. To ensure Cisco ISE can update its machine account password, check that your configurations in Microsoft Active Directory are accurate. For more information on the Windows operating systems and Windows Server versions affected, what this means for your network, and what changes may be needed, see:

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

Network Ports that Must Be Open for Communication

Protocol	Port (remote-local)	Target	Notes
DNS (TCP/UDP)	Random number greater than or equal to 49152	DNS Servers/AD Domain Controllers	—
MSRPC	445	Domain Controllers	—
Kerberos (TCP/UDP)	88	Domain Controllers	MS AD/KDC
LDAP (TCP/UDP)	389	Domain Controllers	—
LDAP (GC)	3268	Global Catalog Servers	—
NTP	123	NTP Servers/Domain Controllers	—
IPC	80	For the secondary ISE-PIC node	—

Active Directory Requirements to Support ISE-PIC

ISE-PIC uses Active Directory login audit events generated by the Active Directory domain controller to gather user login information. The Active Directory server must be configured properly so the ISE user can connect and fetch the user login information. The following sections show how to configure the Active Directory domain controller (configurations from the Active Directory side) to support ISE-PIC.

To configure Active Directory domain controllers (configurations from the Active Directory side) to support , follow these steps:

✎

Note   You must configure all the domain controllers in all the domains.

---

1. Set up Active Directory join points and domain controllers from ISE-PIC (see Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point).

2. Perform the following steps from Active Directory:

   • Configure Active Directory for Passive Identity service, on page 21

3. (Optional) Troubleshoot automatic configurations performed by ISE on Active Directory with these steps:

   • Set Permissions when Microsoft Active Directory Users are in Domain Admin Group, on page 24

   • Permissions for Microsoft Active Directory Users Not in Domain Admin Group, on page 25

   • Permissions to Use DCOM on the Domain Controller, on page 26

Configure Active Directory for Passive Identity service

ISE-PIC Active Directory login audit events generated by the Active Directory domain controller to gather user login information. ISE-PIC connects to Active Directory and fetches the user login information.

The following steps should be performed from the Active Directory domain controller:

Step 1   Make sure relevant Microsoft patches are installed on the Active Directory domain controllers.

Step 2   Make sure the Active Directory logs the user login events in the Windows Security Log.

Verify that the Audit Policy settings (part of the Group Policy Management settings) allows successful logons to generate the necessary events in the Windows Security Log (this is the default Windows setting, but you must explicitly ensure that this setting is correct).

Step 3   You must have an Active Directory user with sufficient permissions for ISE-PIC to connect to the Active Directory. The following instructions show how to define permissions either for admin domain group user or none admin domain group user:

   • Permissions Required when an Active Directory User is a Member of the Domain Admin Group

   • Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group

Step 4   The Active Directory user used by ISE-PIC can be authenticated either by NT Lan Manager (NTLM) v1 or v2. You need to verify that the Active Directory NTLM settings are aligned with ISE-PIC NTLM settings to ensure successful authenticated connection between ISE-PIC and the Active Directory Domain Controller. The following table shows all

Microsoft NTLM options, and which ISE-PIC NTLM actions are supported. If ISE-PIC is set to NTLMv2, all six options described in are supported. If ISE-PIC is set to support NTLMv1, only the first five options are supported.

Table 4: Supported Authentication Types Based on ISE-PIC and AD NTLM Version Settings

ISE-PIC NTLM Setting Options / Active Directory (AD) NTLM Setting Options NTLMv1 NTLMv2	NTLMv1	NTLMv2
Send LM & NTLM responses connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLM response only connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only. Refuse LM connection is allowed connection is allowed	Connection is allowed	Connection is allowed
Send NTLMv2 response only. Refuse LM & NTLM connection is refused connection is allowed	Connection is refused	Connection is allowed

Figure 1: MS NTLM Authentication Type Options
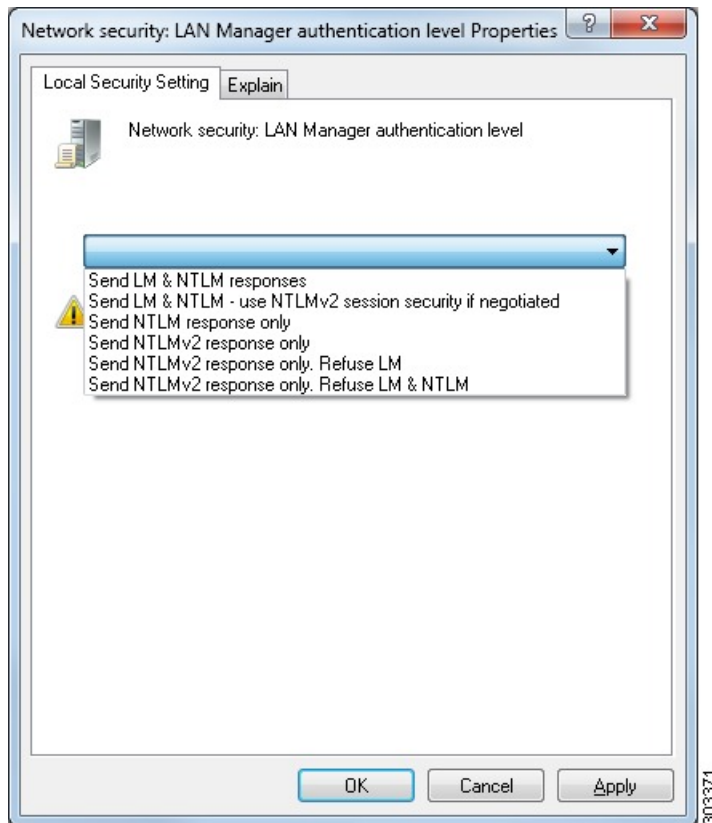
Step 5 Make sure that you have created a firewall rule to allow traffic to `dllhost.exe` on Active Directory domain controllers.

You can either turn the firewall off, or allow access on a specific IP (ISE-PIC IP address) to the following ports:

- TCP 135: General RPC Port. When doing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.

- UDP 137: Netbios Name Resolution

- UDP 138: Netbios Datagram Service

- TCP 139: Netbios Session Service

- TCP 445: SMB

Higher ports are assigned dynamically or you can configure them manually. We recommend that you add %SystemRoot%\System32\dllhost.exe as a target. This program manages ports dynamically.

All firewall rules can be assigned to specific IP (ISE-PIC IP).

Set the Windows Audit Policy

Ensure that the **Audit Policy** (part of the **Group Policy Management** settings) allows successful logons. This is required to generate the necessary events in the Windows Security Log of the AD domain controller machine. This is the default Windows setting, but you must verify that this setting is correct.

Step 1   Choose **Start** > **Programs** > **Administrative Tools** > **Group Policy Management**.

Step 2   Navigate under Domains to the relevant domain and expand the navigation tree.

Step 3   Choose **Default Domain Controller Policy**, right click and choose **Edit**.

The Group Policy Management Editor appears.

Step 4   Choose **Default Domain Controllers Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**.

- For Windows Server 2003 or Windows Server 2008 (non-R2), choose **Local Policies** > **Audit Policy**. For the two Policy items, **Audit Account Logon Events** and **Audit Logon Events**, ensure that the corresponding **Policy Setting** either directly or indirectly includes the **Success** condition. To include the Success condition indirectly, the **Policy Setting** must be set to **Not Defined**, indicating that the effective value will be inherited from a higher level domain, and the **Policy Setting** for that higher level domain must be configured to explicitly include the **Success** condition.

- For Windows Server 2008 R2 and Windows 2012, choose **Advanced Audit Policy Configuration** > **Audit Policies** > **Account Logon**. For the two Policy items, **Audit Kerberos Authentication Service** and **Audit Kerberos Service Ticket Operations**, ensure that the corresponding Policy Setting either directly or indirectly includes the Success condition, as described above.

Note   Cisco ISE uses RC4 cipher in Kerberos protocol while communicating with Active Directory, unless this encryption type is disabled in Active Directory Domain Controller configuration. You can use the **Network Security: Configure Encryption Types Allowed for Kerberos** option in Active Directory to configure the allowed encryption types for Kerberos protocol.

Step 5   If any Audit Policy item settings have been changed, you should then run `gpupdate /force` to force the new settings to take effect.

Set Permissions when Microsoft Active Directory Users are in Domain Admin Group

For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the Domain Admin group does not have full control of certain registry keys in the Windows operating system by default. The Microsoft Active Directory administrator must give the Microsoft Active Directory user full control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following Microsoft Active Directory versions require no registry changes:

- Windows 2003

- Windows 2003R2

- Windows 2008

To grant full control, the Microsoft Active Directory admin must first take ownership of the key:

Step 1 Right-click the key icon and choose the **Owner** tab.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Permissions for Microsoft Active Directory Users Not in Domain Admin Group

For Windows Server 2012 R2, give the Microsoft AD user full control permissions on the following registry keys:

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Use the following commands in Windows PowerShell to check if full permission is given to the registry keys:

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```

- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

The following permissions are required when a Microsoft AD user is not in the Domain Admin group, but is in the Domain Users group:

- Add registry keys to allow ISE-PIC to connect to the domain controller.

-

-

These permissions are only required for the following Microsoft AD versions:

- Windows 2003

- Windows 2003R2

- Windows 2008

- Windows 2008 R2

- Windows 2012

- Windows 2012 R2

- Windows 2016

Add Registry Keys to Allow ISE-PIC to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow ISE-PIC to connect as a domain user, and retrieve login authentication events. An agent is not required on the domain controllers or on any machines in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

```

Make sure that you include two spaces in the value of the DllSurrogate key. If the registry is manually updated, you must include only the two spaces and do not include the quotes. While updating the registry manually, ensure that quotes are not included for AppID, DllSurrogate, and its values.

Retain the empty lines as shown in the preceding script, including the empty line at the end of the file.

Use the following commands in the Windows command prompt to confirm if the registry keys are created and have the correct values:

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`

- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

Permissions to Use DCOM on the Domain Controller

The Microsoft Active Directory user who is used for ISE-PIC Passive Identity service must have the permissions to use DCOM on the domain controller server. Configure permissions with the **dcomcnfg** command line tool.

Step 1 Run the **dcomcnfg** tool from the command line.

Step 2 Expand `Component Services`.

Step 3 Expand **Computers** > **My Computer**.

Step 4 Choose **Action** from the menu bar, click **Properties**, and click **COM Security**.

Step 5 The account that Cisco ISE uses for both access and launch must have Allow permissions. Add the Microsoft Active Directory user to all the four options, **Edit Limits** and **Edit Default** for both **Access Permissions** and **Launch and Activation Permissions**.

Step 6 Allow all local and remote accesses for both **Access Permissions** and **Launch and Activation Permissions**.

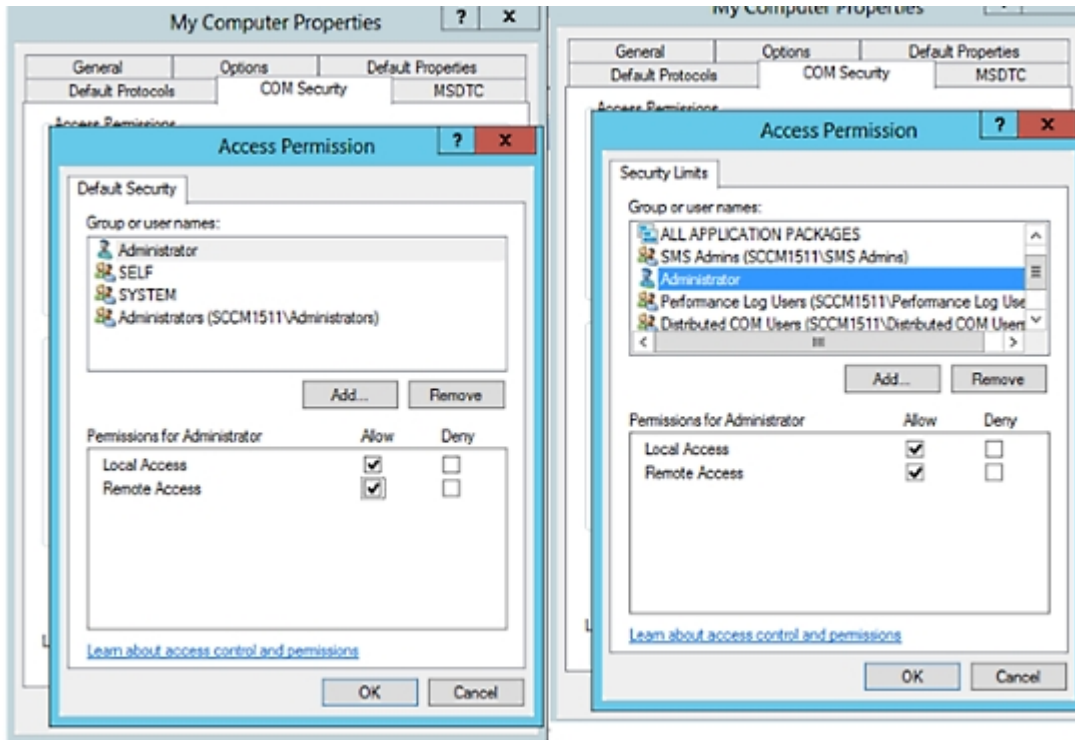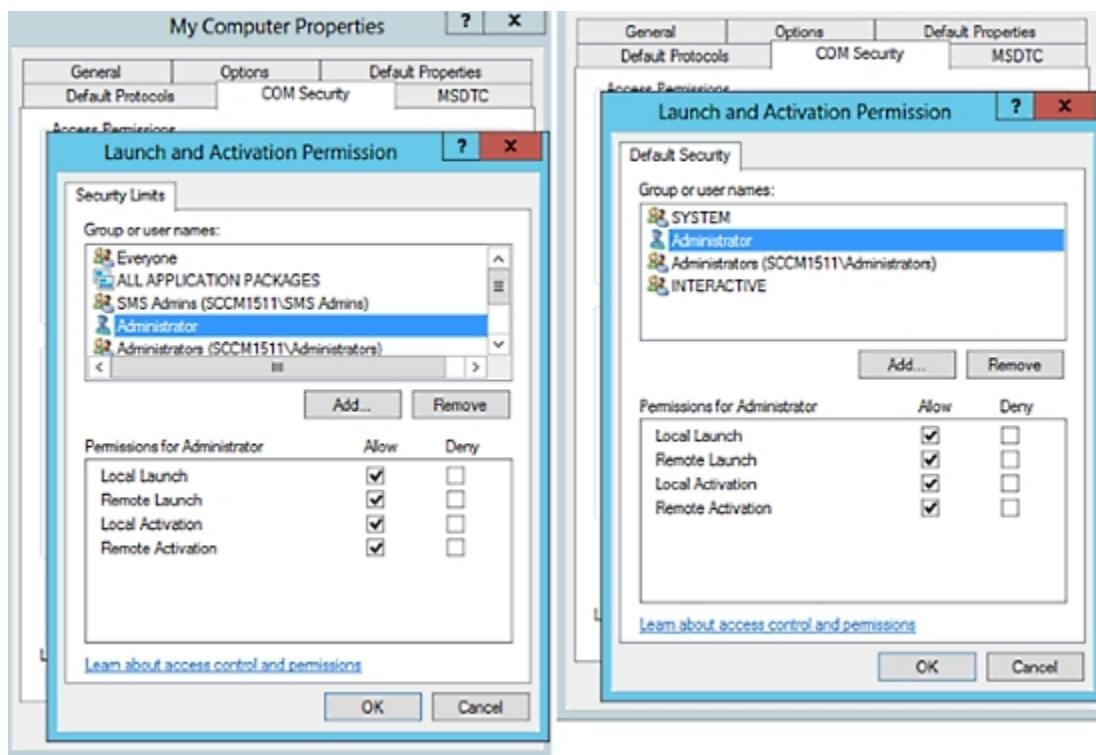*Figure 2: Local and Remote Accesses for Access Permissions*

Figure 3: Local and Remote Accesses for Launch and Activation Permissions

Set Permissions for Access to WMI Root and CIMv2 Namespace

By default, Microsoft Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmimgmt.msc MMC console.

Step 1   Choose **Start** > **Run** and enter `wmimgmt.msc`.

Step 2   Right-click **WMI Control** and click **Properties**.

Step 3   Under the **Security** tab, expand **Root** and choose **CIMV2**.

Step 4   Click **Security**.

Step 5   Add the Microsoft Active Directory user, and configure the required permissions as shown in the following image.
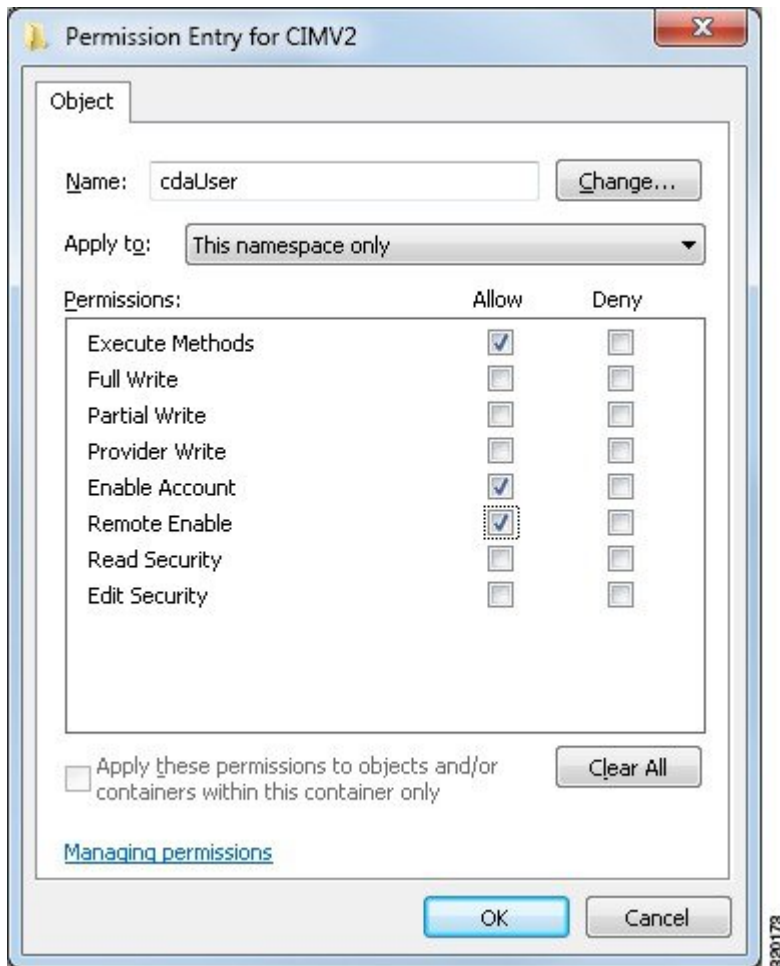
Grant Access to the Security Event Log in the AD Domain Controller

On Windows 2008 and later, you can grant access to the AD Domain controller logs by adding the ISE-PIC ID Mapping user to a group called Event Log Readers.

On all older versions of Windows, you must edit a registry key, as shown below.

Step 1 To delegate access to the Security event logs, find the SID for the account .
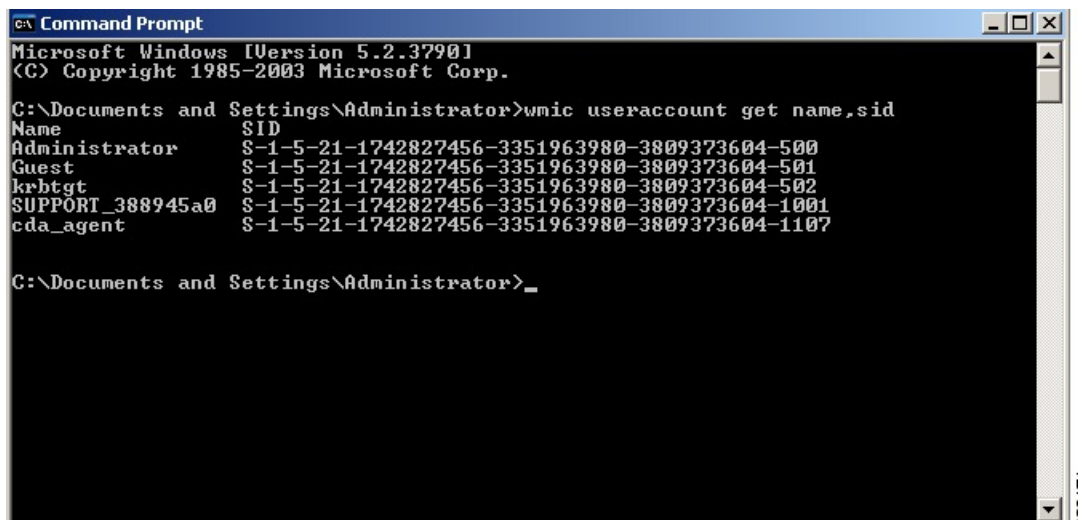
Step 2 Use the following command from the command line, also shown in the diagram below, to list all the SID accounts.

```
wmic useraccount get name,sid
```

You can also use the following command for a specific username and domain:

```
wmic useraccount where name="iseUser" get domain,name,sid
```

Figure 4: List All the SID Accounts

Step 3   Find the SID, open the Registry Editor, and browse to the following location:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog

Step 4   Click on **Security**, and double click **CustomSD**.

For example, to allow read access to the ise_agent account (SID - S-1-5-21-1742827456-3351963980-3809373604-1107), enter (A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107).

Figure 5: Edit CustomSD String
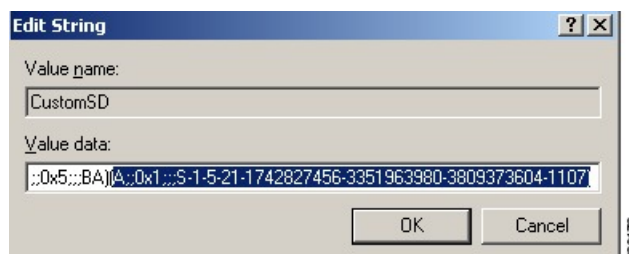
Step 5   Restart the WMI service on the Domain Controller. You can restart the WMI services in the following two ways:

a)   Run the following commands from the CLI:

   net stop winmgmt

   net start winmgmt

b)   Run Services.msc, which opens the Windows Services Management tool. In the Windows Services Management window, locate the **Windows Management Instrumentation** service, right click, and select **Restart**.

Obtaining Additional Troubleshooting Information

Cisco ISE-PIC 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-PIC.

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-PIC provides to diagnose and troubleshoot issues that you are facing in your network.

Cisco ISE-PIC 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-PIC 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-PIC Debug Logs, on page 33.

- 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*.

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-PIC Log Files, on page 32.

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-PIC Log Files

You can download the Cisco ISE-PIC 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.

Before you begin

- You should have configured the debug logs and debug log levels.

Step 1   Choose **Administration** > **Logging** > **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   Click **Create Support Bundle**.

Step 7   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-PIC Debug Logs

Debug logs provide troubleshooting information for various Cisco ISE-PIC 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-PIC Components and Corresponding Debug Logs, on page 33.

Step 2   Download Debug Logs.

Cisco ISE-PIC Components and Corresponding Debug Logs

Note   The list below is a complete list of components available in Cisco ISE. Some of the components listed in the table may not be relevant for ISE-PIC

Table 5: 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
cellular-config	ise-psc.log

Component	Debug Log
cellular-config-api	api-service.log
cellular-config-ui	ise-psc.log
cellular-mnt	collector.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
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

Component	Debug 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
telemetry	sch.log

Download Debug Logs

Step 1   Choose **Administration** > **Logging** > **Download Logs**.

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

Additional References

The following link contains additional resources that you can use when working with Cisco ISE:
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.