Release Notes for Cisco Identity Services Engine, Release 2.6

First Published: 2019-02-18
Last Modified: 2019-09-19

Note
Come to the Content Hub at content.cisco.com, where, using the Faceted Search feature, you can accurately zoom in on the content you want; create customized PDF books on the fly for ready reference; and can do so much more...

So, what are you waiting for? Click content.cisco.com now!
And, if you are already experiencing the Content Hub, we'd like to hear from you!
Click the Feedback icon on the page and let your thoughts flow!

Introduction

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, Cisco Wireless Controllers, Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on Secure Network Server appliances with different performance characterizations, and also as software that can be run on a virtual machine (VM). Note that you can add more appliances to a deployment for better performance.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system.

For more information about the features that are supported in this Cisco ISE release, see the Cisco Identity Services Engine Administrator Guide.

System Requirements

For an uninterrupted Cisco ISE configuration, ensure that the following system requirements are fulfilled.

For more details on hardware platforms and installation in this Cisco ISE release, see the Cisco Identity Services Engine Hardware Installation Guide.
Supported Hardware

Cisco ISE, Release 2.6, requires the following platforms.

Note
For Cisco Secure Network Server (SNS) 3600 series appliance support (SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9), you must use only the new ISO file (ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso). Cisco ISE 2.4 Patch 9 or above must be applied after installation. We recommend that you do not use this ISO file for SNS 3500 series appliance, VMware, KVM, or Hyper-V installation.

Table 1: Supported Hardware Platforms and Personas

<table>
<thead>
<tr>
<th>Hardware Platform</th>
<th>Persona</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SNS-3515-K9 (small)</td>
<td>Any</td>
<td>For the appliance hardware specifications, see the &quot;Cisco SNS-3500 and SNS-3600 Series Appliances&quot; chapter in the Cisco Identity Services Engine Hardware Installation Guide 2.6.</td>
</tr>
<tr>
<td>Cisco SNS-3595-K9 (large)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco SNS-3615-K9 (small)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco SNS-3655-K9 (medium)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco SNS-3695-K9 (large)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco ISE-VM-K9 (VMware, Linux KVM, Microsoft Hyper-V)</td>
<td></td>
<td>• For CPU and memory recommendations, see the &quot;VMware Appliance Sizing Recommendations&quot; section in the Cisco Identity Services Engine Hardware Installation Guide 2.6.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For hard disk size recommendations, see the &quot;Disk Space Requirements&quot; section in the Cisco Identity Services Engine Hardware Installation Guide 2.6.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIC—1-GB NIC interface required. You can install up to six NICs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supported Supported Virtual Environments.</td>
</tr>
</tbody>
</table>

After installation, you can configure Cisco ISE with specific component personas such as Administration, Monitoring, and pxGrid on the platforms that are listed in the above table. In addition to these personas, Cisco ISE contains other types of personas within Policy Service, such as Profiling Service, Session Services, Threat-Centric NAC Service, SXP Service for TrustSec, TACACS+ Device Admin Service, and Passive Identity Service.
Note

- Cisco Secured Network Server (SNS) 3400 Series appliances are not supported in Cisco ISE, Release 2.4, and later.
- Memory allocation of less than 16 GB is not supported for VM appliance configurations. In the event of a Cisco ISE behavior issue, all the users will be required to change the allocated memory to at least 16 GB before opening a case with the Cisco Technical Assistance Center.
- Legacy Access Control Server (ACS) and Network Access Control (NAC) appliances (including the Cisco ISE 3300 Series) are not supported in Cisco ISE, Release 2.0, and later.

Federal Information Processing Standard Mode Support


When FIPS mode is enabled on Cisco ISE, consider the following:

- All non-FIPS-compliant cipher suites will be disabled.
- Certificates and private keys must use only FIPS-compliant hash and encryption algorithms.
- RSA Private keys must be of 2048 bits or greater.
- Elliptical Curve Digital Signature Algorithm (ECDSA) Private keys must be of 224 bits or greater.
- Diffie–Hellman Ephemeral (DHE) ciphers work with Diffie–Hellman (DH) parameters of 2048 bits or greater.
- SHA1 is not allowed to generate ISE local server certificates.
- The anonymous PAC provisioning option in EAP-FAST is disabled.
- The Local SSH server operates in FIPS mode.
- The following protocols are not supported in FIPS mode for RADIUS:
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- ESXi 5.x (5.1 U2 and later support RHEL 7), 6.x
• Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
• KVM on RHEL 7.3

**Note**
If you are installing or upgrading Cisco ISE on an ESXi 5.x server to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later.

### Supported Browsers

The supported browsers for the Admin portal include:

- Mozilla Firefox 69 and earlier versions
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 77 and earlier versions

**Note**
If you use Chrome 65.0.3325.189, you may not be able to view guest account details in the print preview section.

- Microsoft Internet Explorer 10.x and 11.x
- Microsoft Edge beta 77 and earlier versions

**Note**
- If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).
- If you use Chrome 65.0.3325.189, you may be unable to view guest account details in the print preview section.
- When self-signed certificates are used, Cisco ISE portal may fail to launch in Microsoft Edge beta 77 browser even if URL redirection is successful. To resolve this issue:
  1. Add both DNS name and IP address in the **Subject Alternative Name (SAN)** field.
  2. After the ISE services are restarted, redirect the portal in a different browser.
  3. Choose **View Certificate > Details** and copy the certificate by selecting the base-64 encoded option.
  4. Install the certificate in Trusted path and relaunch the browser.
- You might see a warning message while downloading an executable (EXE) file in Google Chrome 76 or later. To resolve this issue:
  1. In your browser, click the **Settings** menu at the top-right corner.
  2. At the bottom of the **Settings** window, click **Advanced**.
  3. Under **Downloads**, check the **Ask Where to Save Each File before Downloading** check box.
Support for Microsoft Active Directory


Note

- It is recommended that you upgrade Windows server to a supported version as Microsoft no longer supports Windows server 2003 and 2003 R2.
- Microsoft Active Directory Version 2000 or its functional level is not supported by Cisco ISE.

Cisco ISE supports multidomain forest integration with Active Directory infrastructure to support authentication and attribute collection across large enterprise networks. Cisco ISE supports up to 50 domain join points.

Improved User Identification

Cisco ISE can identify Active Directory users when a username is not unique. Duplicate usernames are common when using short usernames in a multidomain Active Directory environment. You can identify users by Software Asset Management (SAM), Customer Name (CN), or both. Cisco ISE uses the attributes that you provide to uniquely identify a user.

Update the value of the following:

- SAM: Update this value to use only the SAM in the query (the default).
- CN: Update this value to use only CN in the query.
- CNSAM: Update this value to use CN and SAM in the query.

To configure the attributes mentioned above for identifying Active Directory users, update the IdentityLookupField parameter in the registry on the server that is running Active Directory:

```
REGISTRY\Software\Microsoft\Windows\CurrentVersion\Lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
```

Supported Antivirus and Antimalware Products

For more information on the antivirus and antimalware products supported by the ISE posture agent, see the Cisco AnyConnect ISE Posture Support Charts at:


Supported Ciphers

In a clean or fresh install of Cisco ISE, SHA1 ciphers are disabled by default. However, in case of an upgrade from an existing version of Cisco ISE, the SHA1 ciphers are preset to the options from the earlier version. You can view and change the SHA1 ciphers settings using the Allow SHA1 Ciphers field (Administration > System > Settings > Security Settings).
What is New in Cisco ISE, Release 2.6?

Base Licensing

The features described below require Cisco ISE base licensing.

**CLI Access by External Identity Store**

ISE supports authentication of CLI administrators by external identity sources, such as Active Directory.

**Business Outcome**

You can manage a single source for passwords without the need to manage multiple password policies and administer internal users within ISE, thereby reducing time and effort.

**IPv6 Support**

In addition to the IPv4 support, Cisco ISE, Release 2.6 extends IPv6 support for the following functions or events:

**ISE Management**

You can access and manage a Cisco ISE node over an IPv6 address, and configure an IPv6 address to Eth0 (Interface) during setup wizard as well as through CLI.

You can also manage Secure Socket Shell (SSH) with IPv6 addresses. Cisco ISE supports multiple IPv6 addresses on any interface and these IPv6 addresses can be configured and managed using CLI.

**Network Time Protocol Support**

You can access, configure, and manage Network Time Protocol (NTP) servers with IPv4, FQDN, IPv6 addresses, or with a mix of these.

Cisco ISE also supports NTP server fallback mechanism and server authentication over an IPv6 address.

**Domain Name System Support**

You can configure a combination of IPv4 and IPv6 Domain Name System (DNS) servers and even manage IPv4 or IPv6-based DNS servers through CLI and GUI. Static hostnames can be mapped with IPv6 addresses.

For further details, see ISE Cisco Identity Services Engine CLI Reference Guide, Release 2.6

**External Repositories**

You can add an external repository in Cisco ISE with an IPv6 address. Communication between a Cisco ISE node and an IPv6 external repository is possible when the node has an IPv6 address configured to Eth0.

For further details, see ISE Cisco Identity Services Engine CLI Reference Guide, Release 2.6

**Audit Logs and Reports**

You can view the reports relating to login and logout activities, password changes, and operational changes made by you while accessing Cisco ISE through an IPv6 address. These events can be viewed in the audit reports available in the Cisco ISE dashboard.
Simple Network Management Protocol

Simple Network Management Protocol (SNMP) traps and MIBs can be communicated through IPv6 addresses. You can configure IPv4-based, IPv6-based SNMP or multiple SNMP (a mix of IPv4 and IPv6) servers.

Access Control Lists And Dynamic Access Control Lists

From Cisco ISE, Release 2.6, you can define Access Control Lists (ACLs), Dynamic Access Control Lists (DACLs) and Cisco Airespace ACLs with IPv6 addresses.

Active Directory

You can connect to the IPv6 Active Directory from Cisco ISE.

External Restful Service Portal

External Restful Service is available on an IPv6 client.

Syslog Client or Logging Targets

You can configure IPv6-based syslog targets.

Posture

You can access RADIUS servers with an IPv6 address.

For more information on Cisco ISE, Release 2.6, IPv6 support, see Cisco Identity Services Engine Administrator Guide, Release 2.6.

Business Outcome for IPv6 Support

You can migrate to an IPv6-based network to complete the events mentioned above.

Japanese or English View of the Administrator Portal

The Administration console currently supports two languages, Japanese and English. You can select either the Japanese view or the English view under Account Settings.

Business Outcome

Suitable for Japanese-speaking and English-speaking administrators to configure and use Cisco ISE.

Policy Service Nodes and the Light Session Directory

The Light Session Directory feature can be used to store user session information and replicate it across the Policy Service Nodes (PSNs) in a deployment, thereby eliminating the need to be totally dependent on the Primary Administration Node (PAN) or the Monitoring and Troubleshooting (MnT) node for user session details. The Light Session Directory feature stores only the session attributes required for Change of Authorization (CoA). To enable the Light Session Directory feature, choose Administration > Settings > Light Session Directory and check the Enable Light Session Directory check box.

Business Outcome

Improved performance and scalability of Cisco ISE node.
REST Support for External Administrators

From Cisco ISE 2.6, External RESTful Services (ERS) users can either be internal users or belong to an external Active Directory. The Active Directory group to which the external users belong should be mapped to either the ERS Admin or the ERS Operator group. With this enhancement, administrators no longer have to create internal user counterparts for external users who need access to ERS services.

**Business Outcome**

The process of enabling external administrators to access RESTful services is simplified.

Support for Manufacturer Usage Descriptor

Manufacturer Usage Descriptor (MUD) is an IETF standard, which defines a way to on-board IoT devices. It provides seamless visibility and segmentation automation of IoT devices. MUD has been approved in IETF process, and released as RFC8520.


Cisco ISE, Release 2.6 supports identification of IoT devices. Cisco ISE automatically creates profiling policies and Endpoint Identity Groups. MUD supports profiling IoT devices, creating profiling policies dynamically, and automating the entire process of creating policies and Endpoint Identity Groups. Administrators can use these profiling policies to create manually Authorization Policies and Profiles. IoT devices emitting MUD URL in DHCP and LLDP packets are on board, using those profiles and policies. Full automation, including enforcement in the system, is expected to be added in a future release.

Cisco ISE performs unsigned classification of IoT devices, and accessed through profiler policies. ISE does not store the MUD attributes; the attributes are only used in the current session. In the **Context and Visibility > Endpoints** window, you can filter IoT devices by the **Endpoint Profile** field.

The following devices support sending MUD data to Cisco ISE:

- Cisco Identity Services Engine 2.6
- Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2
- Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2
- Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2
- Internet of Things (IoT) devices with embedded MUD functionality

Profiler Support

Cisco ISE supports the following profiling protocols and profiling probes:

- LLDP and RADIUS - TLV 127
- DHCP - Option 161

**Business Outcome**

The number of IoT devices that are connected to enterprise networks is increasing. Until now, Cisco ISE could not classify these devices. From Release 2.6, Cisco ISE can classify and display the IoT devices that are connected to your network, using an automated process.
Syslog over ISE Messaging

From Cisco ISE, Release 2.6, Monitoring and Troubleshooting (MnT) WAN Survivability is available for UDP syslog collection. Syslogs are recorded using ISE Messaging Service. The Remote Logging Targets, where the syslogs are collected and stored uses port TCP 8671 and the Secure Advanced Message Queuing Protocols (AMQPs) for sending syslogs to MnT.

By default, the ISE Messaging Service option is disabled until Cisco ISE, Release 2.6 Patch 1.

From Cisco ISE, Release 2.6 Patch 2 onwards, by default, the ISE Messaging Service option is enabled.

For more information, see the Cisco Identity Services Engine Administrator Guide, Release 2.6

Business Outcome

Operational data will be retained for a finite duration even when the MnT node is unreachable.

Hardening Improvements

The following caveats are fixed to ensure improved hardening of Cisco ISE:

- CSCvj85532- Streamlined security enforcement upon administrators' authentication failures.
- CSCvk46033- Improved security hardening for connections to the Cisco ISE SSH server.
- CSCvk09565- Conformance to RFC 3164 standards.
- CSCvj96345- Improved security for connections to the Cisco ISE Administration application.

TrustSec Deployment Verification Report

You can use this report to verify whether the latest TrustSec policies are deployed on all network devices and whether there are any discrepancies between the policies configured on Cisco ISE and those deployed on the network devices.

Business Outcome

You can easily verify whether the latest TrustSec policies are deployed on the network devices or if there are any discrepancies.

NFS Repository Credentials

When you add a repository and select NFS as the protocol, you can no longer enter credentials to connect to the repository.

Business Outcome

Using credentials to connect to an NFS repository caused problems.

Apex Licensing

The features described below require Cisco ISE apex licensing.

Identify Managed Devices with Dynamic MAC Addresses

AnyConnect 4.7 now provides a Unique Device ID (UDID) to identify a connected user. The UDID value can be mapped with information from Mobile Device Management (MDM) providers to help identify users
who have the same MAC address. MAC address sharing is common in open offices, where more than one person shares a dock or USB dongle.

**Business Outcome**

You can develop a solution that uses the UDID to uniquely identify a user, when device connections are shared.

**Flexible Remediation Notification**

From Cisco ISE, Release 2.6, you can delay the grace period prompt from being displayed to the user until a specific percentage of grace period has elapsed.

For example, if the **Delay Notification** field in the **Policy > Posture > Posture Policy** window is set to 50 percent and the configured grace period is 10 minutes, Cisco ISE checks the posture status after 5 minutes and displays the grace period notification if the endpoint is found to be noncompliant. Grace period notification is not displayed if the endpoint status is compliant. If the notification delay period is set to 0 percent, the user is prompted immediately at the beginning of the grace period to remediate the problem. However, the endpoint is granted access until the grace period expires.

**Business Outcome**

Prevents unnecessary remediation prompts for endpoints waiting for JAMF software or Microsoft System Center Configuration Manager (SCCM) updates.

**Generic or Custom Messaging Through Cisco AnyConnect**

More informative messages can now be displayed by Cisco AnyConnect when it is used in the context of Cisco ISE Posture service. End users can now see messages about posture status and errors. You can modify the content that is displayed in AnyConnect posture profiles. Note that this feature requires Cisco AnyConnect Version 4.7.

**Business Outcome**

Better communication with end users.

**Platform**

**Support for Cisco Secure Network Server 3600 Series Appliance**


For Cisco Secure Network Server (SNS) 3600 series appliance support (SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9), you must use only the new ISO file (ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso). Cisco ISE 2.4 Patch 9 or above must be applied after installation. We recommend that you do not use this ISO file for SNS 3500 series appliance, VMware, KVM, or Hyper-V installation.

**Business Outcome**

Improved performance, scalability, and platform manageability over SNS 35xx series appliances.
Known Limitations and Workarounds

IP-SGT Bindings Are Not Propagated Under Certain Conditions

Under the following conditions, IP-SGT mappings are not propagated to ACI.

On the ISE administrators console, navigate to Work Centers -> TrustSec -> Components:

1. Create a security group, but don't check Propagate to ACI.
2. Create an IP-SGT binding with previously created Security Group. It may be a static, session or SXP binding.
3. On the Security Group, click Propagate to ACI.
4. Click Save.
5. The Security Group synchs to ACI, but not IP-SGT that is mapped to the Security Group.

Workaround

Either:

1. Restart the ACI propagation in ISE and recreate the IP-SGT mappings.
   2. Check TrustSec-ACI Policy Element Exchange, and save.
   3. The connection between Cisco ISE and ACI is reestablished.
2. Delete the old IP-SGT bindings, and recreate them while Propagate to ACI is checked.

Note

The connection between ACI and ISE reauthenticate every 24 hours, which also fixes this problem.

SXP Protocol Security Standards

Limitation: Security Group Exchange Protocol (SXP) transfers unencrypted data and uses weak Hash Algorithm for message integrity checking per draft-smith-kandula-sxp-06.
Workaround: There is no workaround.

For more information, see https://tools.ietf.org/html/draft-smith-kandula-sxp-06.

Patch Build Download Using Chrome Browser

Limitation: Integrity checksum issues occur when you use the Google Chrome browser to download the patch build.
Condition: The Message Digest 5 (MD5) sum values do not match.
Workaround: Download the patch build using the FireFox browser. Verify that the downloaded patch bundle has the correct MD5 checksum.
Radius Logs for Authentication

Details of an authentication event can be viewed in the Details field of the Radius Authentications window. The details of an authentication event are available only for 7 days, after which no data on the authentication event will be visible. All the authentication log data will be removed when a purge is triggered.

Profiler RADIUS Probe

Limitation: Endpoints are not profiled; they are only authenticated and added to the database.
Condition: The RADIUS probe is disabled.
Workaround: Disable the profiling services completely.

NAM TLS 1.2 Incompatibility Warning

Limitation: ISE implementation of EAP-FAST does not support key generation in TLS 1.2.
Condition: If you are using NAM 4.7 to authenticate endpoints using EAP-FAST, remember that only certain versions of ISE support TLC 1.2, which is required for EAP-FAST. If you use an incorrect version of ISE, the authentication fails, and the endpoint does not have access to the network.
Workaround: In order to resolve this issue, upgrade the Cisco ISE software as shown for the following releases:

- Cisco ISE Release 2.4: Patch 5 or later.
- Cisco ISE Releases 2.0, 2.0.1, and 2.1. Install the Struts2-CVE-2018-11776 PSIRT fix, before you apply the hot patch. You can download the Struts2-CVE-2018-11776 PSIRT fix from Cisco software downloads.

Note

In order to obtain hot patches for Cisco ISE releases earlier than Release 2.4, contact the Cisco Technical Assistance Center (TAC). Ensure that the ISE software has the latest patches applied before you apply the hot patch.

For more information, see https://www.cisco.com/c/en/us/support/docs/field-notices/703/fn70357.html.

High Memory Utilization

Limitation: High memory utilization after installing or upgrading to Cisco ISE Version 1.3 or later.
Condition: Because of the way kernels manage cache memory, Cisco ISE might use more memory, which may trigger high memory usage (80 to 90%) and alarms.
Workaround: There is no workaround.

For more information, see CSCvn07836.

Diffie-Hellman Minimum Key Length

Limitation: Connection to LDAP server fails.
Condition: If the Diffie-Hellman minimum key length that is configured on the LDAP server is less than 1024, connection to the LDAP server fails.
Workaround: Change the Diffie Hellman key size on the LDAP server.

For more information, see CSCvi76985.
ECDSA Certificates

Limitation: Cisco ISE supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates with key lengths of 256 and 384 only.
Condition: ECDSA certificates that are used for EAP authentication are supported only for endpoints with Android Version 6.x and later.

Note
Apple iOS is not supported if you use ECDSA as a system certificate. ECDSA certificates are supported only for Android 6.x and Android 7.x.

Workaround: You can select the key length in the Administration > System > Certificates > Certificate Management > System Certificates window.

Re-create Supplicant Provisioning Wizard References

Limitation: BYOD certificate provisioning flow is broken with both Internal and External Certificates.
Condition: When you upgrade to a new release, or apply a patch, the Supplicant Provisioning Wizard (SPW) is updated.
Workaround: Create new native supplicant profiles and new client-provisioning policies that reference the new SPWs.

Upgrade Information

- Upgrading to Release 2.6
- License Changes
- Upgrade Procedure Prerequisites

Note
If you have installed a hot patch, roll back the hot patch before applying an upgrade patch.

Upgrading to Release 2.6

You can directly upgrade to Release 2.6 from the following Cisco ISE releases:

- 2.1
- 2.2
- 2.3
- 2.4

If you are on a version earlier than Cisco ISE, Release 2.1, you must first upgrade to one of the releases listed above and then upgrade to Release 2.6.
We recommend that you upgrade to the latest patch in the existing version before starting the upgrade.

Cisco ISE, Release 2.6, has parity with 2.0 Patch 7, 2.1 Patch 8, 2.2 Patch 13, 2.3 Patch 5, and 2.4 Patch 5.

**Supported Operating System for Virtual Machines**

You can upgrade to Release 2.6 from either the GUI or the CLI.

Release 2.6 supports Red Hat Enterprise Linux (RHEL) 7.5.

If you are upgrading Cisco ISE nodes on a VMware virtual machine, after you upgrade, ensure that you change the guest operating system to Red Hat Enterprise Linux (RHEL) 7.5. To do this, you must power down the VM, change the guest operating system to RHEL 7.5, and power on the virtual machine after the change.

**Upgrade Packages**

Information about the upgrade packages and the platforms they support, is available at Cisco ISE Software Download.

**License Changes**

**Device Administration Licenses**

There are two types of device administration licenses: cluster and node. A cluster license allows you to use device administration on all policy service nodes in a Cisco ISE cluster. A node license allows you to use device administration on a single policy service node. In a high-availability standalone deployment, a node license permits you to use device administration on a single node in the high availability pair.

The device administration license key is registered against the primary and secondary policy administration nodes. All policy service nodes in the cluster consume device administration licenses, as required, until the license count is reached.

Cluster licenses were introduced with the release of device administration in Cisco ISE 2.0, and is enforced in Cisco ISE 2.0 and later releases. Node licenses were released later, and are only partially enforced in releases 2.0 to 2.3. Starting with Cisco ISE 2.4, node licenses are completely enforced on a per-node basis.

Cluster licenses have been discontinued, and now only node Licenses are available for sale.

However, if you are upgrading to this release with a valid cluster license, you can continue to use your existing license upon upgrade.

The evaluation license allows device administration on one policy service node.

**Licenses for Virtual Machine nodes**

Cisco ISE is also sold as a virtual machine (VM). For this Release, we recommend that you install appropriate VM licenses for the VM nodes in your deployment. Install the VM licenses based on the number of VM nodes and each VM node's resources, such as CPU and memory. Otherwise, you will receive warnings and notifications to procure and install the VM license keys. However, the installation process will not be interrupted. From Cisco ISE, Release 2.4, you can manage your VM licenses from the GUI.

VM licenses are offered under three categories—Small, Medium, and Large. For instance, if you are using a 3595-equivalent VM node with eight cores and 64-GB RAM, you might need a Medium category VM license.
if you want to replicate the same capabilities on the VM. You can install multiple VM licenses based on the number of VMs and their resources as per your deployment requirements.

VM licenses are infrastructure licenses. Therefore, you can install VM licenses irrespective of the endpoint licenses available in your deployment. You can install a VM license even if you have not installed any Evaluation, Base, Plus, or Apex license in your deployment. However, in order to use the features that are enabled by the Base, Plus, or Apex licenses, you must install the appropriate licenses.

VM licenses are perpetual licenses. VM licensing changes are displayed every time you log in to the Cisco ISE GUI, until you check the Do not show this message again check box in the notification pop-up window.

If you have not purchased an ISE VM license earlier, see the Cisco Identity Services Engine Ordering Guide to choose the appropriate VM license to be purchased.

---

Note

If you have purchased ISE VM licenses without a PAK, you can request VM PAKs by emailing licensing@cisco.com. Include the Sales Order numbers that reflect the ISE VM purchase, and your Cisco ID in your email. You will be provided a medium VM license key for each ISE VM purchase you have made.

For details about VM compatibility with your Cisco ISE version, see “Hardware and Virtual Appliance Requirements” chapter in the Cisco Identity Services Engine Installation Guide for the applicable release.

For more information about the licenses, see the "Cisco ISE Licenses" chapter in the Cisco Identity Services Engine Administrator Guide, Release 2.6.

---

**Upgrade Procedure Prerequisites**

- Run the Upgrade Readiness Tool (URT) before an ISE software upgrade in order to check if the configured data can be upgraded to the required ISE version. Most upgrade failures occur because of data upgrade issues; the URT is designed to validate the data before the actual upgrade and reports and tries to fix the issues, wherever possible. The URT can be downloaded from the Cisco ISE Download Software Center.

- We recommend that you install all the relevant patches before beginning the upgrade.

For more information, see the Cisco Identity Services Engine Upgrade Guide.

---

**Telemetry**

After installation, when you log in to the Admin portal for the first time, the Cisco ISE Telemetry banner appears on screen. Using this feature, Cisco ISE securely collects non-sensitive information about your deployment, network access devices, profiler, and other services that you are using. The data that is collected will be used to provide better services and additional features in forthcoming releases. By default, the telemetry feature is enabled. You can choose to disable or modify the account information. To do this, choose Administration > Settings > Smart Call Home. Account information provided is unique to the deployment. Each admin user need not provide it separately.

---

**Cisco ISE Live Update Portals**

Cisco ISE Live Update portals help you to automatically download the Supplicant Provisioning wizard, AV/AS support (Compliance Module), and agent installer packages that support client provisioning and
posture policy services. These live update portals are configured in Cisco ISE during the initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the corresponding device using Cisco ISE.

If the default Update portal URL is not reachable and your network requires a proxy server, configure the proxy settings by choosing Administration > System > Settings > Proxy before you access the Live Update portals. If proxy settings allow access to the profiler, posture, and client-provisioning feeds, access to a Mobile Device Management (MDM) server is blocked because Cisco ISE cannot bypass the proxy services for MDM communication. To resolve this, you can configure the proxy services to allow communication to the MDM servers. For more information on proxy settings, see the "Specify Proxy Settings in Cisco ISE" section in the Cisco Identity Services Engine Administrator Guide, Release 2.6.

**Client Provisioning and Posture Live Update Portals**

You can download Client Provisioning resources from:

**Work Centers > Posture > Settings > Software Updates > Client Provisioning.**

The following software elements are available at this URL:
- Supplicant Provisioning wizards for Windows and Mac OS X native supplicants
- Windows versions of the latest Cisco ISE persistent and temporal agents
- Mac OS X versions of the latest Cisco ISE persistent agents
- ActiveX and Java Applet installer helpers
- AV/AS compliance module files

For more information on automatically downloading the software packages that are available at the Client Provisioning Update portal to Cisco ISE, see the “Download Client Provisioning Resources Automatically” section in the "Configure Client Provisioning” chapter in the Cisco Identity Services Engine Administrator Guide, Release 2.6.

You can download Posture updates from:

**Work Centers > Posture > Settings > Software Updates > Posture Updates**

The following software elements are available at this URL:
- Cisco-predefined checks and rules
- Windows and Mac OS X AV/AS support charts
- Cisco ISE operating system support

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically” section in the Cisco Identity Services Engine Administrator Guide, Release 2.6.

If you do not want to enable the automatic download capabilities, you can choose to download updates offline.

### Cisco ISE Offline Updates

This offline update option allows you to download client provisioning and posture updates, when direct internet access to Cisco.com from a device using Cisco ISE is not available or is not permitted by a security policy.
Offline updates are also available for Profiler Feed Service. For more information, see the Configure Profiler Feed Services Offline.

To download offline client provisioning resources, perform the following procedure:

### Procedure

**Step 1**
Go to: https://software.cisco.com/download/home/283801620/type/283802505/release/2.6.0.

**Step 2**
Provide your login credentials.

**Step 3**
Navigate to the Cisco Identity Services Engine download window, and select the release.

The following Offline Installation Packages are available for download:

- win_spw-<version>-isebundle.zip — Offline SPW Installation Package for Windows
- mac-spw-<version>.zip — Offline SPW Installation Package for Mac OS X
- compliancemodule-<version>-isebundle.zip — Offline Compliance Module Installation Package
- macagent-<version>-isebundle.zip — Offline Mac Agent Installation Package
- webagent-<version>-isebundle.zip — Offline Web Agent Installation Package

**Step 4**
Click either Download or Add to Cart.

For more information on adding the downloaded installation packages to Cisco ISE, see the "Add Client Provisioning Resources from a Local Machine" section in the Cisco Identity Services Engine Administrator Guide.

You can update the checks, operating system information, and antivirus and antispyware support charts for Windows and Mac operating systems offline from an archive in your local system, using posture updates.

For offline updates, ensure that the versions of the archive files match the versions in the configuration file. Use offline posture updates after you configure Cisco ISE and want to enable dynamic updates for the posture policy service.

To download offline posture updates, perform the following procedure:

### Procedure

**Step 1**

**Step 2**
Save the posture-offline.zip file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Mac operating systems.

**Step 3**
Launch the Cisco ISE administrator user interface and choose Administration > System > Settings > Posture.

**Step 4**
Click the arrow to view the settings for posture.

**Step 5**
Click Updates. The Posture Updates window is displayed.

**Step 6**
Click the Offline option.

**Step 7**
Click Browse to locate the archive file (posture-offline.zip) from the local folder in your system.
**Configuration Prerequisites**

- The relevant Cisco ISE license fees should be provided.
- The latest patches should be installed.
- Cisco ISE software capabilities should be active.
- Read the Release Notes document for the corresponding release of Cisco Identity Services Engine.

See the following resources to get started with configuring ISE:

- [Getting started with Cisco ISE](#)
- [Videos on the Cisco ISE Channel on YouTube](#)
- [Cisco ISE Design and Integration Guides](#)
- [Cisco Identity Services Engine Administrator Guide](#)

**Monitoring and Troubleshooting**

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the [Cisco Identity Services Engine Administrator Guide](#).

**Ordering Information**

For detailed Cisco ISE ordering information, see the [Cisco Identity Services Engine Ordering Guide](#).

**Cisco ISE Integration with Cisco Digital Network Architecture Center**

Cisco ISE can integrate with Cisco DNA Center. For information about configuring Cisco ISE to work with Cisco DNA, see the Cisco DNA Center documentation [here](https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/tsd-products-support-series-home.html).

For information about which versions of Cisco ISE are compatible with which versions of Cisco DNA Center, see [here](https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html?wcmmode=disabled).
Download and Install a New Patch

To obtain the patch file that is necessary to apply a patch to Cisco ISE, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software, and save a copy of the patch file to your local machine.

For instructions on how to apply the patch to your system, see the section "Install a Software Patch" in the Cisco Identity Services Engine Administrator Guide.

For instructions on how to install a patch using CLI, see the "Patch Install" section in the Cisco Identity Services Engine CLI Reference Guide, Release .

Note

When installing 2.4 Patch 4 and later, CLI services will be temporary unavailable during kernel upgrade. If the CLI is accessed during this time, the CLI displays the "Stub Library could not be opened" error message. However, after patch installation is complete, CLI services will be available again.

Caveats

The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat, use the Cisco Bug Search Tool (BST). The bug IDs are sorted alphanumerically.

Note

The Open Caveats sections lists the open caveats that apply to the current release and might apply to releases earlier than Cisco ISE 2.6. A caveat that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

The BST, which is the online successor to the Bug Toolkit, is designed to improve effectiveness of network risk management and device troubleshooting. You can search for bugs based on product, release, or keyword, and aggregate key data such as bug details, product, and version. For more details on the tool, see the Help page located at http://www.cisco.com/web/applicat/cbsshelp/help.html.

New Features in Cisco ISE Release 2.6.0.156 - Cumulative Patch 2

Syslog over ISE Messaging Service

The UDP sylogs (built-in UDP syslog targets - LogCollector and LogCollector2) will be delivered to the monitoring nodes using the existing ISE Messaging service infrastructure, which is by default enabled now. This enhances WAN survivability of syslog messages. Please ensure to open the TCP port 8671 on firewalls (if any) between all nodes for this feature to work.

You can disable this option to deliver the UDP Syslogs via UDP Ports. To do so, navigate to Administration > System > Logging > Log Settings page in the Cisco ISE GUI and uncheck the Use ISE messaging Service for UDP syslog delivery to MnT option.
Support for Elevated System Administrator Role

For more information, see the Cisco Identity Services Engine Administrator Guide, Release 2.6

Business Outcome
Operational data will be retained for a finite duration even when the monitoring nodes are unreachable.

Support for Elevated System Administrator Role

The Elevated System Administrator role is similar to the existing System Administrator role. Additionally with this role you can create, delete and update admin users except super admin users.

For more information, see the Cisco Identity Services Engine Administrator Guide, Release 2.6.

Business Outcome
Elevated System Admin has the ability to manage admin users.

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 2

The following table lists the resolved caveats in Release 2.6 cumulative patch 2.

Patch 2 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.1.53 or later.

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuw55841</td>
<td>Custom admin unable to create other restricted admin users</td>
</tr>
<tr>
<td>CSCvb56579</td>
<td>SXP Devices page - can't show all the name after 14 chars</td>
</tr>
<tr>
<td>CSCvc77960</td>
<td>Friendly info message has to be displayed instead of blank page for unauthorized access</td>
</tr>
<tr>
<td>CSCvg03526</td>
<td>Patch installation might generate alarm Application patch installation failed</td>
</tr>
<tr>
<td>CSCvh22907</td>
<td>Sponsor Portal Page takes more than 10 seconds to load</td>
</tr>
<tr>
<td>CSCvh64185</td>
<td>Session notification can emit bad values in ADNormalizedUsername,</td>
</tr>
<tr>
<td></td>
<td>ADUserResolvedIdentities fields</td>
</tr>
<tr>
<td>CSCvi51291</td>
<td>ISE CoA doesn't work 2 days after initial auth</td>
</tr>
<tr>
<td>CSCvk76680</td>
<td>ISE-PIC Self signed certificate delete operation fails due to Secure Syslog Server reference error</td>
</tr>
<tr>
<td>CSCvm00481</td>
<td>CA Service still running on command line after Disabling internal certificate authority in Web UI</td>
</tr>
<tr>
<td>CSCvn15748</td>
<td>ISE guest flow max session limit does not send CoA Disconnect with third party NAD</td>
</tr>
<tr>
<td>CSCvn44171</td>
<td>Network access user with external password cannot be used as ISE admin</td>
</tr>
<tr>
<td>CSCvn51282</td>
<td>ISE replaces &quot;ip:&quot; to it's hostname in &quot;ip:inacl&quot; Cisco AV-Pair</td>
</tr>
<tr>
<td>CSCvn60787</td>
<td>Emails are not sent for alarm specific email configuration</td>
</tr>
<tr>
<td>Caveat ID Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCvn73740</td>
<td>EAP-TLS authentications with Endpoint profile set to not unknown fails in second authorization.</td>
</tr>
<tr>
<td>CSCvn79569</td>
<td>App status for ISE is in initialisation state</td>
</tr>
<tr>
<td>CSCvn92246</td>
<td>ISE: admin users unable to delete or modify groups if a tacacs user is saved without any group</td>
</tr>
<tr>
<td>CSCvn92528</td>
<td>ISE 2.4 : Misconfigured supplicant query is one of the reasons for high CPU on both MNT nodes</td>
</tr>
<tr>
<td>CSCvo14624</td>
<td>Latency observed with high TPS rates, when ISE messaging service is turned ON</td>
</tr>
<tr>
<td>CSCvo17704</td>
<td>ISE 2.4 - CLI password will not accept 3 $</td>
</tr>
<tr>
<td>CSCvo28092</td>
<td>ISE Custom Endpoint Attributes - Will not save or delete</td>
</tr>
<tr>
<td>CSCvo45582</td>
<td>Internal Administrator Summary report not allowing to select specific columns</td>
</tr>
<tr>
<td>CSCvo45768</td>
<td>Adding config to support PrA in PSN failover case</td>
</tr>
<tr>
<td>CSCvo50638</td>
<td>TCNAC adapter cannot be configured post upgrade from 2.2 to 2.6</td>
</tr>
<tr>
<td>CSCvo59928</td>
<td>ISE 2.6 ANC policy is applied with error &quot;microservice_unavailable&quot; on SMC</td>
</tr>
<tr>
<td>CSCvo77219</td>
<td>Sponsor guest portal rate limit time not honored</td>
</tr>
<tr>
<td>CSCvo78051</td>
<td>Allowed Protocols - Error creating an inline Allowed Protocol in Policy sets page</td>
</tr>
<tr>
<td>CSCvp07591</td>
<td>EAP-GTC Machine Authentication Failure Password Mismatch due to failing the UTF-8 Validation Checks</td>
</tr>
<tr>
<td>CSCvp12131</td>
<td>ISE 2.4 Patch 6 reload breaks backups</td>
</tr>
<tr>
<td>CSCvp13378</td>
<td>PassiveID flow should send User's SamAccountName and ExplicitUPN</td>
</tr>
<tr>
<td>CSCvp14725</td>
<td>ADNormalizedUserName Field Missing From Half of sessions</td>
</tr>
<tr>
<td>CSCvp16734</td>
<td>Plus Licenses Consumed without Plus Features</td>
</tr>
<tr>
<td>CSCvp18692</td>
<td>AD_User_Fetch information's are not in UI as well as Redis</td>
</tr>
<tr>
<td>CSCvp28382</td>
<td>Unable to delete multiple admin groups with multi select</td>
</tr>
<tr>
<td>CSCvp29197</td>
<td>ISE 2.4p3 Radius livelogs not showing due to invalid NAD ip address</td>
</tr>
<tr>
<td>CSCvp29413</td>
<td>Modifying Radius attributes to send in the request to External RADIUS Server is not working on ISE</td>
</tr>
<tr>
<td>CSCvp29572</td>
<td>Enable Pxgrid Profiling Probe Saves but will not enable</td>
</tr>
<tr>
<td>CSCvp30958</td>
<td>ISE dropping requests due to descriptor allocation exhaustion under external server latency scenario</td>
</tr>
<tr>
<td>Caveat ID Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCvp33593</td>
<td>ISE fails to match authz policy with endpoint ID group &quot;unknown&quot;</td>
</tr>
<tr>
<td>CSCvp33862</td>
<td>Custom Attribute (advanced filter in CV) not able to filter on risk score (integer value)</td>
</tr>
<tr>
<td>CSCvp37101</td>
<td>The AD connectivity issue occurred and the corefile was generated the same day</td>
</tr>
<tr>
<td>CSCvp37238</td>
<td>TACACS/AAA live log report not showing configuration change made from ACI</td>
</tr>
<tr>
<td>CSCvp39842</td>
<td>ISE 2.6 SFTP repository access fails</td>
</tr>
<tr>
<td>CSCvp43302</td>
<td>Deleting guest type throws error &amp; not able to create new guest type with same name</td>
</tr>
<tr>
<td>CSCvp45528</td>
<td>Queue Link Error alarm generated after signing of ISE CA certificate by external Root CA</td>
</tr>
<tr>
<td>CSCvp50450</td>
<td>ise-elasticsearch.log files not purged in ISE 2.4 and 2.6</td>
</tr>
<tr>
<td>CSCvp52201</td>
<td>ISE 2.4 : Replication: Cluster information table has old FQDNN</td>
</tr>
<tr>
<td>CSCvp54773</td>
<td>ISE 2.4 p6 400 error on sponsor portal after timeout.</td>
</tr>
<tr>
<td>CSCvp54949</td>
<td>BYOD flow is broken in IOS 12.2</td>
</tr>
<tr>
<td>CSCvp58945</td>
<td>Import of network device template throws error Failed illegal value for Encryption key</td>
</tr>
<tr>
<td>CSCvp59286</td>
<td>Multiple Vulnerabilities in struts2-core</td>
</tr>
<tr>
<td>CSCvp60359</td>
<td>Upgraded ISE Node Shows LDAP Identity Store Password in Plain</td>
</tr>
<tr>
<td>CSCvp61880</td>
<td>Authorization profile fails to import with no warnings or errors to user</td>
</tr>
<tr>
<td>CSCvp65699</td>
<td>CSCvp63136: US399914: 2.6 P2 - View third-party licenses and notices - Link Update</td>
</tr>
<tr>
<td>CSCvp65711</td>
<td>ISE 2.4 P8 posture scan running when switch to wired network not configured with dot1x</td>
</tr>
<tr>
<td>CSCvp65816</td>
<td>&quot;Cisco Modified&quot; Profiles are overwritten by the Profiler Feed Service</td>
</tr>
<tr>
<td>CSCvp68285</td>
<td>AUP guest portal error 400 when retrun from contact support link (iphone captive portal)</td>
</tr>
<tr>
<td>CSCvp72966</td>
<td>Email not received to guest if view/print guest password disabled</td>
</tr>
<tr>
<td>CSCvp75101</td>
<td>ISE MNT exception when receiving cisco-av-pair=addrv6=0x7f8c0d588608</td>
</tr>
<tr>
<td>CSCvp76617</td>
<td>ISE customer endpoint attribute type string doesn't allow certain numbers</td>
</tr>
<tr>
<td>CSCvp76911</td>
<td>ISE if using multiple matrices deploy button is missing</td>
</tr>
<tr>
<td>CSCvp77941</td>
<td>License usage for Plus either shows 0 or incorrect value</td>
</tr>
<tr>
<td>CSCvp83006</td>
<td>Export from Context Visibility-Endpoints does not contain Custom Attr for most of Endpoints</td>
</tr>
</tbody>
</table>
### Open Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 2

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvp86406</td>
<td>Unable to add network device with combination of any digit followed by () in software version field</td>
</tr>
<tr>
<td>CSCvp88242</td>
<td>[ 400 ] Bad Request error when refreshing the Mydevice portal</td>
</tr>
<tr>
<td>CSCvp93901</td>
<td>pxGrid to publish ADUser.. and ADHost..: SamAccountName and QualifiedName</td>
</tr>
<tr>
<td>CSCvq13341</td>
<td>ISE 2.6 patch 1 - AD User Test is returning 0 groups</td>
</tr>
</tbody>
</table>

### Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 1

The following table lists the resolved caveats in Release 2.6 cumulative patch 1.

Patch 1 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.1.53 or later.

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvq54061</td>
<td>System Summary is not available for MNT nodes</td>
</tr>
<tr>
<td>CSCvq69343</td>
<td>IP-SGT maps are not propagated to ACI in specific scenario</td>
</tr>
<tr>
<td>CSCvg70813</td>
<td>ISE dmp files are not deleted from /opt/oracle/base/admin/cpm10/dpdump for failed backup attempts</td>
</tr>
<tr>
<td>CSCvh19430</td>
<td>ISE 2.x : Guest account activation time discrepancy for imported accounts</td>
</tr>
<tr>
<td>CSCvi80094</td>
<td>ERS API that requires CSRF token returns HTTP 404 instead of 403</td>
</tr>
<tr>
<td>CSCvj05563</td>
<td>Cannot delete security groups having virtual network mapping</td>
</tr>
<tr>
<td>CSCvj31598</td>
<td>Import two CA certs with same subject name</td>
</tr>
<tr>
<td>CSCvj383747</td>
<td>ISE Secure Access Wizard Easy Wireless null AD groups for BYOD, Secure Access, Sponsored guest flow</td>
</tr>
<tr>
<td>CSCvm01627</td>
<td>ISE 2.4 ERS API - PUT and GET Internal User &quot;User Custom Attributes&quot;</td>
</tr>
<tr>
<td>CSCvm05840</td>
<td>NAD CSV imports should allow all supported characters</td>
</tr>
<tr>
<td>CSCvm90478</td>
<td>&quot;No Data Available&quot; when attempting to add endpoints to Identity Group with RBAC User</td>
</tr>
<tr>
<td>CSCvn40822</td>
<td>Guest creation fails ISE 2.3 after patch 5</td>
</tr>
<tr>
<td>CSCvn55640</td>
<td>Manage ACC calling infinite time when sponsoruser configured with permissions ALL&amp;GROUP sponsor grps</td>
</tr>
<tr>
<td>Caveat ID Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCvn58964</td>
<td>ISE 2.4 slow database response with 500 authorization policies</td>
</tr>
<tr>
<td>CSCvn76567</td>
<td>ISE 2.4 - IP-SGT bindings disappear from SXP for user session</td>
</tr>
<tr>
<td>CSCvn85484</td>
<td>Removing SCEP RA Profile casues the associated CA chain to be silently removed from Trusted Store</td>
</tr>
<tr>
<td>CSCvn92778</td>
<td>Removal of unused logical profile may cause a wrong authorization result</td>
</tr>
<tr>
<td>CSCvn98932</td>
<td>Non-existed DACL is not verifed by the ISE</td>
</tr>
<tr>
<td>CSCvo05269</td>
<td>[ISE 2.4]Unable to use created profiling policy in authorization condition</td>
</tr>
<tr>
<td>CSCvo09945</td>
<td>Backups from SFTP repository may show incorrect year in Modified time</td>
</tr>
<tr>
<td>CSCvo11090</td>
<td>Able to delete ACI IEPG in ISE.</td>
</tr>
<tr>
<td>CSCvo13269</td>
<td>ISE does not allow to add an SGT</td>
</tr>
<tr>
<td>CSCvo15770</td>
<td>address shows as HTML code in context visibility</td>
</tr>
<tr>
<td>CSCvo18247</td>
<td>ISE: failed to skip duplicate framed-pool attribute during migration</td>
</tr>
<tr>
<td>CSCvo19076</td>
<td>ISE endpoint purge ACTIVEDIRECTORY dictionary is not loading</td>
</tr>
<tr>
<td>CSCvo24593</td>
<td>pagination is not working in &quot;All SXP mappings&quot; page in ISE.</td>
</tr>
<tr>
<td>CSCvo41052</td>
<td>ISE deleting the newly created IP-SGT mapping</td>
</tr>
<tr>
<td>CSCvo43289</td>
<td>ISE truncates the SGT name after a &quot;:&quot; character and assigning a version id</td>
</tr>
<tr>
<td>CSCvo61900</td>
<td>System Scan throws internal error for MAC built-in FW remediation using ISE 2.4 Patch 7</td>
</tr>
<tr>
<td>CSCvo74441</td>
<td>RabbitMQ docker container is not coming up if port 15672 was already in use</td>
</tr>
<tr>
<td>CSCvo78171</td>
<td>ISE 2.4 Patch 6 installation breaks FQDN of Sponsor and MyDevices Portal</td>
</tr>
<tr>
<td>CSCvo84948</td>
<td>Failed to migrate dACLs from ACS 5.8 to ISE 2.6</td>
</tr>
<tr>
<td>CSCvo90393</td>
<td>CoA failure in Radius+PassiveID flow</td>
</tr>
<tr>
<td>CSCvp07364</td>
<td>After upgrading from ISE 2.0.1 Patch 4 to 2.4 Patch 6, CoA is not issued from ISE</td>
</tr>
<tr>
<td>CSCvp23869</td>
<td>ISE TLS 1.0 and 1.1 security settings are not applied for PxGrid, causing WSA to fail integration</td>
</tr>
<tr>
<td>CSCvp48710</td>
<td>Unable to add AD group if it contains &quot;/.&quot; or &quot;/../&quot; in the AD group name</td>
</tr>
<tr>
<td>CSCvo31313</td>
<td>Change password for few of the internal users not working after upgrade to 2.6</td>
</tr>
<tr>
<td>CSCvo32279</td>
<td>APIC logs not seeing in spx.log when SXP logging set to 'DEBUG'.</td>
</tr>
<tr>
<td>CSCvo35144</td>
<td>Delay in clearing of SXP mappings in ISE</td>
</tr>
<tr>
<td>Caveat ID Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCvo36769</td>
<td>EAP-TTLS settings page is not saved in ISE 2.6</td>
</tr>
<tr>
<td>CSCvo36837</td>
<td>Admin group cannot get access to &quot;Users&quot; at &quot;Device Administration&quot; tab after install patch 5</td>
</tr>
<tr>
<td>CSCvo42165</td>
<td>Default python change password script returns CRUD operation exception</td>
</tr>
<tr>
<td>CSCvo45606</td>
<td>ISE:WMI-Passed values may compromise the security of ISE. Please remove malicious scripting terms</td>
</tr>
<tr>
<td>CSCvo48352</td>
<td>CSV file of RADIUS authentications report may have duplicate records</td>
</tr>
<tr>
<td>CSCvo48975</td>
<td>ISE downloads unneeded RA certificate for BYOD</td>
</tr>
<tr>
<td>CSCvo61888</td>
<td>Device Administration Current Active Sessions report not available from 2.4 Patch 6</td>
</tr>
<tr>
<td>CSCvo74766</td>
<td>ISE DACL syntax checking validation failing on wildcard notation</td>
</tr>
<tr>
<td>CSCvo75129</td>
<td>Runtime prepends &quot;&quot; to &quot;;&quot; in dhcp-class-identifier in syslog message sent to profiler</td>
</tr>
<tr>
<td>CSCvo75376</td>
<td>pxGrid node name limit too short for FMC</td>
</tr>
<tr>
<td>CSCvo80291</td>
<td>pxGrid startup order causing profiler code to fail init</td>
</tr>
<tr>
<td>CSCvo80516</td>
<td>ISE 2.6 LiveLogs not seen and false Health Status is Unavailable alarm</td>
</tr>
<tr>
<td>CSCvo82021</td>
<td>ISE : Memory usage discrepancy in GUI and show tech</td>
</tr>
<tr>
<td>CSCvo98554</td>
<td>After Importing ISE PB to ISE , Login page are not loaded</td>
</tr>
<tr>
<td>CSCvn35142</td>
<td>ISE 2.3: Posture report for endpoint by condition not working as expected</td>
</tr>
<tr>
<td>CSCvo13626</td>
<td>ISE : Improve Posture Assessment by Condition Report export rate for higher records (millions)</td>
</tr>
<tr>
<td>CSCvp17444</td>
<td>Admin Access Blank page when using valid RSA/RADIUS Token credentials but is not in ISE Admin DB</td>
</tr>
<tr>
<td>CSCvp40082</td>
<td>ISE 2.3/2.4 upgrade to the latest patch may break dynamic redirection for 3rd party NADs</td>
</tr>
<tr>
<td>CSCvo08406</td>
<td>[ENH] Change field Active Directory in External DataSource condition to mention Join Point</td>
</tr>
<tr>
<td>CSCvo19377</td>
<td>Successful Authentication Entries not shown in the RADIUS Report due to exceeding the CSV limit</td>
</tr>
<tr>
<td>CSCvo33474</td>
<td>Fix &quot;Server not reachable&quot; autologout</td>
</tr>
</tbody>
</table>
Resolved Caveats in Cisco ISE Release 2.6.0.156

All Resolved Defects for ISE 2.6
https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283801589&rls=2.6(0.901)&sb=afr&bt=null

Open Caveats in Cisco ISE Release 2.6.0.156

Open Caveats in Cisco ISE, Release 2.6
https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283801589&rls=2.6&sb=afr&sts=open&bt=null

Communications, Services, and Additional Information

• To receive timely and relevant information from Cisco, sign up at Cisco Profile Manager.
• To get the business impact you are looking for with the technologies that matter, visit Cisco Services.
• To submit a service request, visit Cisco Support.
• To discover and browse secure and validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
• To obtain information about general networking, training, and certification titles, visit Cisco Press.
• To find warranty information for a specific product or product family, access Cisco Warranty Finder.