Release Notes for Cisco Identity Services Engine, Release 2.6

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 to Cisco Identity Services Engine

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, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, 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 machines (VMs). 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 detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in 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, can be installed on the following platforms:

Caution 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 Platforms

Hardware Platform	Configuration
Cisco SNS-3515-K9 (small)	For appliance hardware specifications, see the *Cisco Secure Network Server Appliance Hardware Installation Guide*.
Cisco SNS-3595-K9 (large)	
Cisco SNS-3615-K9 (small)	
Cisco SNS-3655-K9 (medium)	
Cisco SNS-3695-K9 (large)	

After installation, you can configure Cisco ISE with specific component personas such as Administration, Monitoring, or 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.

Caution

- Cisco ISE 3.1 and later releases do not support Cisco Secured Network Server (SNS) 3515 appliance.
- Cisco 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 (FIPS) Mode Support

Cisco ISE uses embedded Federal Information Processing Standard (FIPS) 140-2-validated cryptographic module, Cisco FIPS Object Module Version 6.2 (Certificate #2984). For details about the FIPS compliance claims, see Global Government Certifications.

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 2048 bits or greater.
- Elliptical Curve Digital Signature Algorithm (ECDSA) private keys must be 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:

- VMware ESXi 5.x, 6.x, 7.x
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on RHEL 7.1, 7.3, and 7.5

For information about the virtual machine requirements, see the *Cisco Identity Services Engine Installation Guide* for your version of Cisco ISE.

Caution Cisco ISE does not support VMware snapshots for backing up ISE data because a VMware snapshot saves the status of a VM at a given point in time. In a multi-node Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. We recommend that you use the backup functionality included in Cisco ISE for archival and restoration of data.

Using VMware snapshots to back up ISE data results in stopping Cisco ISE services. A reboot is required to bring up the ISE node.

Supported Browsers

The supported browsers for the Admin portal include:

- Mozilla Firefox 96 and earlier versions from version 82
- Mozilla Firefox ESR 91.3 and earlier versions
- Google Chrome 97 and earlier versions from version 86
- Microsoft Internet Explorer 11.x
- Microsoft Edge, the latest version and one version earlier than the latest version

Support for Microsoft Active Directory

Cisco ISE works with Microsoft Active Directory servers 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019 at all functional levels.

Note

- It is recommended that you upgrade Windows server to a supported version as Microsoft no longer supports Window 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.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
```

Supported Antivirus and Antimalware Products

For information about the antivirus and antimalware products supported by the Cisco ISE posture agent, see Cisco AnyConnect ISE Posture Support Charts.

Supported Ciphers

In a clean or fresh install of Cisco ISE, SHA1 ciphers are disabled by default. However, if you upgrade from an existing version of Cisco ISE, the SHA1 ciphers retain 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**).

Note This does not apply to the Admin portal. When running in Federal Information Processing Standard Mode (FIPS), an upgrade does not remove SHA1 ciphers from the Admin portal.

Cisco ISE supports TLS versions 1.0, 1.1, and 1.2.

Cisco ISE supports RSA and ECDSA server certificates. The following elliptic curves are supported:

- secp256r1
- secp384r1
- secp521r1

Note Cisco ISE does not support intermediate certificates having SHA256withECDSA signature algorithm for any of the elliptical curves due to the limitations in the current implementation of OpenJDK 1.8.

The following table lists the supported Cipher Suites:

Cipher Suite	When Cisco ISE is configured as an EAP server When Cisco ISE is configured as a RADIUS DTLS server	When Cisco ISE downloads CRL from HTTPS or a secure LDAP server When Cisco ISE is configured as a secure syslog client or a secure LDAP client When Cisco ISE is configured as a RADIUS DTLS client for CoA

TLS 1.0 support	When TLS 1.0 is allowed (DTLS server supports only DTLS 1.2) Allow TLS 1.0 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.0 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.0, check the Allow TLS 1.0 check box in the **Security Settings** window. To view this window, choose **Administration > System > Settings > Protocols > Security Settings**.	When TLS 1.0 is allowed (DTLS client supports only DTLS 1.2)
TLS 1.1 support	When TLS 1.1 is allowed Allow TLS 1.1 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.1 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.1, check the Allow TLS 1.1 check box in the Security Settings window(Administration > System > Settings > Protocols > Security Settings).	When TLS 1.1 is allowed
ECC DSA ciphers		
ECDHE-ECDSA-AES256-GCM-SHA384	Yes	Yes
ECDHE-ECDSA-AES128-GCM-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA384	Yes	Yes
ECDHE-ECDSA-AES128-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed
ECDHE-ECDSA-AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
ECC RSA ciphers		
ECDHE-RSA-AES256-GCM-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES128-GCM-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed

ECDHE-RSA-AES128-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
ECDHE-RSA-AES128-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
DHE RSA ciphers		
DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	When SHA-1 is allowed
DHE-RSA-AES128-SHA	No	When SHA-1 is allowed
RSA ciphers		
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed
AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
3DES ciphers		
DES-CBC3-SHA	When 3DES/SHA-1 is allowed	When 3DES/DSS and SHA-1 are enabled
DSS ciphers		
DHE-DSS-AES256-SHA	No	When 3DES/DSS and SHA-1 are enabled
DHE-DSS-AES128-SHA	No	When 3DES/DSS and SHA-1 are enabled
EDH-DSS-DES-CBC3-SHA	No	When 3DES/DSS and SHA-1 are enabled
Weak RC4 ciphers		
RC4-SHA	When "Allow weak ciphers" option is enabled in the Allowed Protocols page and when SHA-1 is allowed	No
RC4-MD5	When "Allow weak ciphers" option is enabled in the Allowed Protocols page	No

EAP-FAST anonymous provisioning only: ADH-AES-128-SHA	Yes	No
Peer certificate restrictions		
Validate KeyUsage	Client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Validate ExtendedKeyUsage	Client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	Server certificate should have ExtendedKeyUsage=Server Authentication

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.

Note If you choose to configure IPv6 address, you should also have an IPv4 address configured (in addition to IPv6 address) for the Cisco ISE node communication. Hence, dual stack (combination of both IPv4 and IPv6) is required.

  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: 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. For more information, see https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/.

Cisco ISE, Release 2.6 and later 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 sending MUD URL in DHCP and LLDP packets are on board, using those profiles and policies.

Cisco ISE performs unsigned classification of IoT devices. Cisco 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 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

Cisco ISE 2.6 supports Cisco Secure Network Server 3615, Secure Network Server 3655, and Secure Network Server 3695 appliances.

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

LDAP Server Reconfiguration after Upgrade

Limitation

The primary Hostname or IP is not updated which causes authentication failures. This is because while upgrading the Cisco ISE deployment, the deployment IDs tend to reset.

Condition

When you enable the **Specify server for each ISE node** option in the **Connection** window (**Administration** > **Identity Management** > **External Identity Sources** > **LDAP** > **Add** or choose and an existing server) and then upgrade your Cisco ISE deployment with PSNs, the deployment IDs tend to reset.

Workaround

Reconfigure the LDAP Server settings for each node. For more information, see **LDAP Identity Source Settings** section in the *Administrative Access to Cisco ISE Using an External Identity Store* chapter in the "Cisco Identity Services Engine Administrator Guide, Release 2.4".

Upgrade GUI Notification

Limitation

Upgrade GUI shows that the upgrade progress at 0% for secondary PAN until upgrade is at 100%. The upgrade process continues in background and there’s no impact on upgrade.

Condition

While upgrading from Cisco ISE 2.4 Patch 8 to a higher release.

Workaround

Check the ade.log file for the upgrade process. To display the ade.log file, enter the following command from the Cisco ISE CLI:

```
show logging system ade/ADE.log
```

For more information, see CSCvp78781.

pxGrid Certificate Issue

Limitation

Default self-signed certificate for pxGrid fails.

Condition

While upgrading from Cisco ISE 2.7 Patch 7 to a higher release.

Workaround

Either use a different certificate, or add "SSL Client" to the existing certificate.

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.
   a. On the Work Centers->TrustSec->Settings->ACI Settings, uncheck “TrustSec-ACI Policy Element Exchange”, and save.
   b. Check **TrustSec-ACI Policy Element Exchange**, and save.
   c. 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 reauthenticates 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.

Endpoint Protection Services API

As of Cisco ISE 1.4, ANC replaces Endpoint Protection Services. ANC provides additional classifications, and performance improvements. There are new APIs for ANC in the Cisco ISE SDK. While the ERS APIs might still work, we strongly recommend that you move to ANC.

Server IP update under Trustsec AAA Server list

When the IP of the Cisco ISE instance is changed via CLI, then Cisco ISE will restart the services. Once the services are up, we need to change the IP of Trustsec AAA Server. Choose **Workcenters** > **TrustSec** > **Components** > **Trustsec Servers** > **Trustsec AAA Servers**.

Upgrade Information

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

Note When you upgrade to Cisco ISE 2.6 patch 7, you will see an error message if you were using the RE_AUTHENTICATE in an ANC policy. The existing policies will still work.

Applying patch 2 eliminates the error message. Or you can remove those policies before upgrading.

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.

Note 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.

Cisco ISE runs on the Cisco Application Deployment Engine operating system (ADEOS), which is based on Red Hat Enterprise Linux (RHEL). For Cisco ISE, Release 2.6, ADEOS is based on RHEL 7.5. For more information, see Cisco Identity Services Engine Upgrade Journey.

If you are upgrading Cisco ISE nodes on VMware virtual machines, after upgrade is complete, ensure that you change the Guest Operating System to supported version of Red Hat Enterprise Linux (RHEL). To do this, you must power down the VM, change the Guest Operating System to the supported RHEL version, and power on the VM after the change.

Patch Compatibility

This patch is compatible with the following patch releases:

- 2.2 Patch 15
- 2.3 Patch 7

- 2.4 Patch 10
- 2.6 Patch 2

Upgrade Packages

For information about the upgrade packages and the supported platforms, see 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.

Upgrade Procedure Prerequisites

- Run the Upgrade Readiness Tool (URT) before the upgrade to check whether the configured data can be upgraded to the required Cisco ISE version. Most upgrade failures occur because of data upgrade issues. The URT validates the data before the actual upgrade and reports the issues, if any. 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.

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. Choose **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.

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.

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.

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.

To download offline client provisioning resources:

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:

Procedure

Step 1 Go to https://www.cisco.com/web/secure/spa/posture-offline.html.

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.

Note The **File to Update** field is a mandatory field. You can select only one archive file (.zip) containing the appropriate files. Archive files other than .zip, such as .tar, and .gz are not supported.

Step 8 Click **Update Now**.

Configuration Prerequisites

- The relevant Cisco ISE license fees should be paid.
- The latest patches should be installed.
- Cisco ISE software capabilities should be active.

See the following resources to configure Cisco 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 and licensing 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 Center, see the *Cisco DNA Center documentation*.

For information about Cisco ISE compatibility with Cisco DNA Center, see the *Cisco SD-Access Compatibility Matrix*.

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 https://software.cisco.com/download/home (you will 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 "Install a Software Patch" section 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*.

Note Cisco ISE Release 2.6 Patch 10 and later releases support the licensing feature SSM On-Prem connection method. If you enable this feature and need to roll back to Cisco ISE 2.6 Patch 9 or earlier, you must disable the licensing feature before you uninstall the patch with the licensing feature.

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 the 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.

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 12

The following table lists the resolved caveats in Release 2.6 cumulative patch 12.

Caveat ID Number	Description
CSCwa77161	PLR returned upon 3.0P5 to 3.0P3
CSCwa74844	Application server crashes when System Time page is accessed in 2.6 Patch 11
CSCvz90468	Internal users using External Password Store get disabled if users are created using API flow
CSCvw53772	dom4j before 2.1.3 allows external DTDs and External Entities by default

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 11

The following table lists the resolved caveats in Release 2.6 cumulative patch 11.

Patch 11 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.

Identifier	Headline
CSCvy69539	CIAM: openjdk - multiple versions
CSCvz51536	Cisco ISE Wildcard certificate failing with internal error
CSCvy75191	Cisco ISE XML external entity injection vulnerability
CSCvs96530	Cisco ISE formula injection vulnerability
CSCvz18044	VNs fail to replicate from Author to Reader
CSCwa23393	Cisco ISE 2.7 patches 4,5, and 6 report the error "There is an overlapping IP Address in your device"
CSCwa80547	CIAM: unixodbc 2.3.0
CSCvy63778	REST API for CoA works with any server IP
CSCvz21417	Upgrade Cisco ISE 3.0 and earlier patches with CiscoSSL 1.0.2za

Identifier	Headline
CSCwa60873	Optimize bouncy-castle class to improve performance on PAN
CSCvy33615	Cisco ISE 3.1 BH: Default profiling policies' description displays the space character hex code instead of space
CSCvy71313	CIAM: cpio 2.12
CSCwb14106	CIAM: cyrus-sasl 2.1.27
CSCvy71261	CIAM: nettle 3.4.1
CSCvy84989	enabling cookies for POST /ers/config/internaluser/ causes Identity Group(s) Does Not Exist error
CSCwa80520	CIAM: libpng 1.6.20
CSCvy06719	Manual ActiveSession report is empty
CSCvz60870	High Active Directory latency during high TPS causes HOL blocking on ADRT
CSCwa80553	CIAM: samba 4.8.3
CSCvz13783	The licensing page has zero count after upgrading to patch 13
CSCvy04443	MNT REST API for ReAuth fails when used in a distributed deployment (separate MnT)
CSCvz86020	Live log/session does not display latest data due to "Too Many Files Open" error
CSCvs95495	Reauth issue - Aruba - 3rd party device
CSCvx58520	With PLR, Profiler Online Updates error : Failed to get License file data : null
CSCvy89317	Cisco ISE: DST Root CA X3 Certificate Authority - Expires by 30 Sep 2021 (within 90 days)
CSCvy36968	Unable to retrieve the license details causing features to be disabled
CSCwa06912	High Latency observed for Tacacs+ requests with date time condition in authorization policies
CSCwa80501	CIAM: perl 5.16.3
CSCvs66551	Multiple vulnerabilities in apache log4j
CSCvz80829	Version pre-check fails for 3.2 full upgrade.
CSCwa78479	Cisco ISE assessment of CVE-2021-4034 Polkit
CSCvy48766	Cisco ISE installation fails with "Database Priming Failed" error when an all-numbers subdomain is used
CSCvy34977	Application server stuck on initializing state due to certificate template curve type P-192

Identifier	Headline
CSCvx01272	Generate bulk certificates does not include the Cisco ISE self-signed certificate
CSCvw78289	Auth Passed live logs are not seen when using a profile name with more than 50 characters
CSCwa41166	Unsafe characters in T+ commands stored in hex numeric character references
CSCwb03479	hotpatch.log needs to be included in support-bundle
CSCvx48255	CIAM: screen 4.1.0 CVE-2021-26937
CSCwb29140	Threads are exhuasted after moving to latest patches where NSS RPM is updated (only Release 3.0 Patch 5 and Release 2.7 Patch 7)
CSCvz20851	Cisco ISE sensitive information disclosure vulnerability
CSCvw94603	External MDM server (Microsoft Intune), change in polling interval does not take effect
CSCwa23207	Multiple runtime crashes seen due to memory allocation inconsistency
CSCvz79665	Microsoft Intune Graph URL changed from graph.windows.net/tenant to graph.microsoft.com
CSCwa47133	Cisco ISE Evaluation log4j CVE-2021-44228
CSCwa96229	Cisco ISE allowing user to change admin password without validating current password
CSCvy11976	Cisco ISE privilege escalation vulnerability
CSCvy90691	When duplicated RADIUS vendor ID is present, any network device change can cause PSN to crash.
CSCwa60903	Cisco ISE adds six extra hours to nextUpdate date for CRL
CSCvy71229	CIAM: libx11 1.6.8
CSCwa80679	CIAM: net-snmp 5.7.2
CSCwb11026	Apply code fix based on Red Hat recommendation for "Cisco ISE unable to talk to NTP daemon" error
CSCwa80484	CIAM: nss 3.44.0
CSCwb12022	Terminated sessions are not cleared from Cisco ISE live sessions tab.
CSCwa80530	CIAM: jspdf 1.0.0
CSCvz22331	Authentication is not blocked in policySet with TimeAndDate condition for specific minute in the day
CSCvz77905	Cisco ISE RADIUS service, denial of service vulnerability
CSCvz50255	CIAM: bind 9.11.20

Identifier	Headline
CSCvz55258	Cisco:cisco-av-pair AuthZ conditions stopped working
CSCvy81878	Cisco ISE - Persistent self cross-site scripting vulnerability
CSCvy96905	memory leak on systemd-journal process
CSCvu68240	Daily purge is not happening and hence data to be purged does not get copied to repository
CSCwb01843	DST/TZ update should happen automatically
CSCwa80550	CIAM: quartz - multiple versions
CSCwa80359	CIAM: sqlite 3.7.17
CSCvz65576	Fullupgrade wont work with patch when CLI repo or disk repo is used
CSCvx57545	Cisco ISEdailycron temp1 tracking is causing delay in AWR reports
CSCvz33839	Menu access customization is not working
CSCvy96144	UDI information is missing in the GUI
CSCvz85117	Cisco ISE Health Check I/O bandwidth performance check false alarm
CSCvy14905	CTS-SXP-CONN : ph_tcp_close from device to Cisco ISE SXP connection - Hawkeye
CSCvq26129	libcgroup umask configuration information disclosure vulnerability
CSCvz00258	SessionCache not cleared for TACACS AuthZ failures results in high heap usage and auth latency
CSCvu58732	ntpd in NTP earlier than 4.2.8p14, and 4.3.x earlier than 4.3.100 allows remote attack
CSCvx14400	Multiple vulnerabilities in glibc
CSCvw65181	CIAM found poi vulnerable
CSCvz13747	SystemTest : 2.6P10 : PPAN UI page not opening after PAN failover
CSCwa80532	CIAM: jsoup 1.10.3
CSCvo39514	MnT log processor not running because of collector log permission
CSCvy86528	Cisco ISE sensitive information disclosure vulnerability
CSCvx58736	3.1:Maxscale: Core generated by /opt/CSCOcpm/prrt/diag/bin/diagRunner start
CSCvy42885	Cisco ISE Application server crash/restart due to cancellation of configuration backup
CSCvz71872	CIAM: nss - multiple versions
CSCwa80482	CIAM: libx11 1.6.7

Open Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 11

Caveat ID Number	Description
CSCwa74844	Application server crashes when accessing System Time page in 2.6 Patch 11

New Features in Cisco ISE Release 2.6.0.156 - Cumulative Patch 10

Licensing Method for Air-Gapped Networks

Smart Software Manager (SSM) On-Prem is a connection method in which you configure an SSM On-Prem server that manages smart licensing in your Cisco ISE-enabled network. With this connection method, Cisco ISE does not require a persistent connection to the Internet.

For more information, see the Licensing Chapter in the *Cisco Identity Services Engine Administrator Guide*.

Full Upgrade and Split Upgrade Options Added to Cisco ISE GUI

You can select one of the following options in the **Administration > System > Upgrade> Upgrade Selection** window to upgrade your Cisco ISE deployment:

- **Full Upgrade**: Full upgrade is a multi-step process that enables a complete upgrade of your Cisco ISE deployment sequentially. This method will upgrade all nodes in parallel and in lesser time compared to the split upgrade process. The application services will be down during this upgrade process because all nodes are upgraded parallelly.
- **Split Upgrade**: Split upgrade is a multi-step process that enables the upgrade of your Cisco ISE deployment while allowing services to remain available during the upgrade process. This upgrade method allows you to choose the Cisco ISE nodes to be upgraded on your deployment.

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 10

The following table lists the resolved caveats in Release 2.6 cumulative patch 10.

Patch 10 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.

Caveat ID Number	Description
CSCvi53134	Account used for ISE AD join may become locked after passive-id service is enabled
CSCvn25548	Account is suspended temporarily due to excessive failed authentication
CSCvt52104	Multiple Vulnerabilities in jetty
CSCvt89098	ISE does not reattempt wildcard replication for failed nodes
CSCvt94587	"Plus License is out of compliance and trying generate Internal CA operations" error shown while trying to regenerate ISE Root CA chain
CSCvu13139	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash)

Caveat ID Number	Description
CSCvu16067	Changes in IP table settings causing TCP slowness and TACACS latency
CSCvu19221	Support Information is out of the flow
CSCvu58927	Update "blacklist portal" to "blocked list portal" everywhere in the ISE UI + code
CSCvu58954	Update "blacklist identity group" to "blocked list identity group" everywhere in the ISE UI + code
CSCvu84184	Certificate chain is not sent on the portal
CSCvv07101	PKCS11 key store creating memory leak when having endpoints in ISE
CSCvv83510	ISE 3.0 Upgrade failing at step RuleResultsSGTUpgradeService
CSCvv92638	Cannot configure scheduled config and operational backup with start date same as current day
CSCvw48396	Cisco ADE-OS Local File Inclusion Vulnerability
CSCvw59312	Heap buffer overflow in Freetype CVE-2020-15999, CVE-2018-6942
CSCvw60197	Multiple Vulnerabilities in glibc
CSCvw89326	For PKI based SFTP, exporting GUI key for MnT node is possible only when it is promoted to PAN
CSCvx10186	ISE remains in eval expire state even after registering with Smart Licensing
CSCvx18730	Sudo Privilege Escalation Vulnerability Affecting Cisco Products: January 2021
CSCvx37297	Error 400 while authenticating to Sponsor portal with Single Sign-on/Kerberos User.
CSCvx43825	Receiving acct stop without NAS-IP address keeps session in started state
CSCvx47891	AMP events not mapped correctly for new endpoints
CSCvx49538	CIAM: bind - multiple versions CVE-2020-8625
CSCvx78643	Emails sent for all system alarms even when there is no email address configured
CSCvx78796	ISE 2.7 p2 : RADIUS Authentication Troubleshooting report shows incorrect or no data in its result
CSCvx79679	Workaround for False Failed login Event not working on 2.6 patch 8
CSCvx79693	Qualys integration is failing with ISE
CSCvx84402	Not able to retrieve Endpoint Identity Groups via API calls
CSCvx85807	Smart license of de-registration flow is not working in ISE and ISE-PIC
CSCvx93203	ISE configuration backup size mismach when using NFS repository

Caveat ID Number	Description
CSCvx96190	Top Authorization report does not show filter in scheduled reports
CSCvx96915	Vulnerabilities fixed in XStream 1.4.16
CSCvx99151	ISE internal ERS user attepting to authenticate via external ID store causing REST delays
CSCvx99176	ISE 2.7p3: NAD IP definitions using - or * do not perform full IP comparison
CSCvy06417	ISE persistant XSS Admin Group
CSCvy14342	High CPU seen on PSN nodes from ISE 2.6P3 onwards due to PIP query evaluation
CSCvy15172	Cisco Identity Services Engine Self Cross-Site Scripting Issue
CSCvy20277	Special characters allowed previously in Descriptions field for few objects no longer can be used
CSCvy29461	Unable to download Debug Logs from GUI
CSCvy36868	ISE 2.6 does not support "cariage return" <cr> character in command-set
CSCvy41066	Tacacs custom AV pair as condition in policies is not working
CSCvy42972	Full upgrade should throw warning if data size is more than 40GB overall
CSCvy74456	External DNAC authentication via ISE fails with "Invalid login credentials" error
CSCvy76601	Context Visibility Delete 'All' function showing incorrect number of endpoints on confirmation popup
CSCvy79179	Empty RabittMQ password causing Replication issue.
CSCvz01485	ISE 2.7 patch 4 unable to upload .json file for Umbrella security profile
CSCvz05704	Platform check fails for ISE having disk size more than 1TB

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 9

The following table lists the resolved caveats in Release 2.6 cumulative patch 9.

Patch 9 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.

Caveat ID Number	Description
CSCvh04231	Guest remember-me flow radius accounting and access accept is not sending Guest Username.
CSCvn31249	GNU gettext default_add_message Double-Free Vulnerability.
CSCvo04728	MIT Kerberos 5 KDC krbtgt Ticket S4U2Self Request Denial of Service.

Caveat ID Number	Description
CSCvo75129	Runtime prepends "\" to ";" in dhcp-class-identifier in syslog message sent to profiler.
CSCvq12204	ISE 2.4 SNMPv3 user added with wrong hash after reload causing SNMPv3 authentication failure.
CSCvq26124	ISC BIND managed-keys Trust Anchor Denial of Service Vulnerability.
CSCvq58506	Show running-configuration fails to complete.
CSCvr47716	Info-ZIP UnZip File Overlapping Denial of Service Vulnerability CVSS v3.0 Base 7.5
CSCvr55906	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow Vulner CVSS v3.1 Base: 9.8.
CSCvr57375	ISE 2.7 BETA: Username field in Self-Registration Portal Config is not saved.
CSCvr77653	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.
CSCvr77655	GNU patch pch_write_line Function Denial of Service Vulnerability.
CSCvr80914	SSSD Group Policy Objects Implementation Improper Access Control Vulnerability.
CSCvr80921	ISC BIND Dynamically Loadable Zones Unauthorized Access Vulnerability.
CSCvr81463	libssh2 packet.c Integer Overflow Vulnerability CVSS v3.1 Base: 8.1.
CSCvr94153	TPS - update curl lib in prrt.
CSCvr97388	Samba Filename Path Separators Unauthorized Access Vulnerability.
CSCvs29611	ISE 2.4 p5 crashes continuously around midnight, generating core files.
CSCvs39800	gllibc LD_PREFER_MAP_32BIT_EXEC Environment Variable ASLR Bypass Vulnerability.
CSCvs52211	Update CiscoSSL to fix CSCvg56800 - Evaluation of ISE vulnerability nginx Oct 2017.
CSCvs76914	libxml2 xml Parse Balanced Chunk Memory Recover Memory Leak Vulnerability.
CSCvs85273	Multiple Vulnerabilities in libcurl.
CSCvs91984	System button_open Memory Leak Vulnerability.
CSCvt11664	ISE Feed Server fails via 'createLicenseSource' method "FlexlmListException: Error".
CSCvt30558	Multiple Vulnerabilities in python.
CSCvt43844	ISE: runtime-aaa debugs do not print packet details in ascii; breaking Endpoint debugs.

Caveat ID Number	Description
CSCvt44403	SSLDUMP() logs printed on Showtech via Audit logs causing showtech file to grow extensively.
CSCvt50572	Impossible to create whitelist policy via ERS API.
CSCvt51244	Multiple Vulnerabilities in activemq-all.
CSCvt65332	Description using two lines, or <Enter> was used, under Client provisioning resources throws errorA.
CSCvt75739	Heavy delay observed in sxp mappings when 50k acc packets with single SGT and VN send.
CSCvt82384	Rotation of diagnostics.log is not working on ISE.
CSCvu04874	Suspected memory leak in io.netty.buffer.PoolChunk.
CSCvu22058	ISE with DUO as External Radius Proxy drops access-reject.
CSCvu22259	CIAM: batik 1.7.
CSCvu24402	CIAM: cups 1.6.3.
CSCvu30439	CIAM: ksh.
CSCvu31098	CIAM: libssh.
CSCvu33861	ISE 2.4 p6 - REST API MnT query to get device by MAC address taking more than 2 minutes.
CSCvu34433	ISE 2.x, Free space on Undo tablespace not cleared as per isehourlycron.sh cron script.
CSCvu37728	CIAM: perl 5.14.1.
CSCvu37765	CIAM: procps 3.3.10.
CSCvu37775	CIAM: python (version 2.7.5, 2.7.14 & 3.7.1).
CSCvu38141	CIAM: vim 7.4.160.
CSCvu58892	Update "master guest report" to "primary guest report" everywhere in the ISE UI + code.
CSCvu59038	Update "master/slave" terms to "primary/subordinate" in "show interface" command.
CSCvu62938	Posture fails when primary PSN/PAN are unreachable.
CSCvu70683	Alarm Suppression required for ERS queries along with suppression on iselocalstore.log.
CSCvu81838	CIAM: d-bus 1.10.24.
CSCvu84773	Cisco Identity Services Engine Cross-Site Scripting Vulnerability.

Caveat ID Number	Description
CSCvu87758	Guest password policy settings cannot be saved when set to ranges for Alphabets or numbers.
CSCvu90703	CLDAP thread is hung and running infinite.
CSCvu91039	ISE not doing lookup for all mac addresses in mac list causing redirectless Posture to fail.
CSCvu91859	CIAM: libjpeg & libjpeg-turbo.
CSCvv00951	App server crashes while transitioning into stopping state.
CSCvv07078	Context visibility: exception caught on transport layer: Unable to load Context Visibility page.
CSCvv08784	ISE:SEV2: Unable to restore backup of ISE 2.4 patch 12.
CSCvv08885	Cisco Identity Services Engine Privilege Escalation Vulnerability.
CSCvv09910	SYSAUX tablespace full despite fix for CSCvr96003.
CSCvv14390	Max Sessions Limit is not working for Users and Groups.
CSCvv29737	DNA ACA SG Sync Fails with JDBCException:could not prepare statement.
CSCvv35921	Can not start CSV exporting for Selected User in internal ID Store.
CSCvv36189	Radius passed-auth live logs not sent due to invalid IPv6 Address.
CSCvv41935	PSK cisco-av-pair throws an error if the key contains < or > symbols.
CSCvv46034	Device admin service is getting disabled when updating TACACS configuration.
CSCvv46958	TrustSec enabled NADs not showing in trustSec Matrices when NDG column exceeds 255 characters.
CSCvv50721	Can not get the download link of NetworkSetupAssistant.exe using Aruba dynamic URL redirect.
CSCvv53221	ISE_EST_Local_Host RADIUS Shared Secret empty causes ISE application server intializing state.
CSCvv54798	Context Visibility CVS exported from CLI not showing IP Addresses.
CSCvv55663	ISE 2.6/2.7 Repositories get deleted post ISE node reload.
CSCvv58629	Certificate Authority Service initializing EST Service not running after upgrade to ISE 2.7 p2.
CSCvv59233	ISE RADIUS Live Log details missing AD-Group-Names under Other Attributes section.
CSCvv60353	Authentication summary report gets stuck if the total records are more than 5M.

Caveat ID Number	Description
CSCvv62382	proxy bypass settings does not allow upper characters.
CSCvv62729	ISE - Network Device API call throws error 500 if you query an non-existent network device.
CSCvv77007	ISE constantly requesting internal "Super Admin" users against the external RADIUS token server.
CSCvv77530	Unable to retrieve LDAP Groups/Subject Attributes when % character is used twice or more in bind password.
CSCvv77928	Bulk certificate generation failed with 'An unexpected error occurred' message after RMA'd pPAN.
CSCvv85588	Memory Leak : High Allocation in by CAD_ValidateUser during PassiveID stress.
CSCvv91007	Smart Licensing Entitlement Tab gets stuck at "Refreshing" if there is connection failure.
CSCvv91234	ISE 2.6 scheduled reports are not working when primary MNT is down.
CSCvv91684	ISE Collection Filters will not display in GUI.
CSCvv92203	ISE 2.6 P6/Unable to create SGT: NetworkAuthZProfile with entered name already exists.
CSCvv93442	ISE 2.6p3 Adding Double Slash "//" in File Path with SFTP Servers.
CSCvv94791	[CFD] ACA Sync broken - "Error occurs during migration: Waiting for Sync Runtime timed out".
CSCvv99093	ISE nodes intermittently trigger Queue Link alarms : Cause=Timeout.
CSCvw01829	ISE admin/portal Login with Chrome 85/86 could show error Oops. Something went wrong.
CSCvw02887	Memory leak after adding AD Groups for passiv-id flow.
CSCvw06722	USID is found different when user login with Email/Userid when Ldap store is configured.
CSCvw08330	Posture does not work with dynamic redirection on 3rd party NADs.
CSCvw08602	Not Throwing error for ip overlap case.
CSCvw10671	GNU.org bash rbash BASH_CMDS Modification Privilege Escalation Vulnerability.
CSCvw20636	Authorization Profiles showing "No data available" after NAD profile deleted.
CSCvw22228	pxGrid ANC applyEndpointPolicy does not handle all MAC address formats correctly.
CSCvw24268	Cisco Identity Services Engine Untrusted File Upload Vulnerability.
CSCvw25285	Passive ID is not working stable with multi-connect syslog clients.

Caveat ID Number	Description
CSCvw25615	ISE TACACS logging timestamp shows future date.
CSCvw26415	ISE 3.0 not importing certificates with missing CN and SAN into Trusted Certificate Store.
CSCvw28441	NADs shared secrets are visible in the logs while using APIs.
CSCvw29490	Internal User custom attributes are not sent in CoA-Push.
CSCvw33115	ISE MNT Live Session status is not changing to Postured in VPN use case.
CSCvw36743	ISE Service Account Locked and WMI not established due to special characters in password.
CSCvw48697	API IP SGT mapping not returning result for [No Devices].
CSCvw50829	AD security groups cannot have their OU end with dot character on RBAC policies.
CSCvw58824	XStream before version 1.4.15 shows multiple vulnerabilities
CSCvw59855	In js/parts/SvgRenderer.js in Highcharts JS before 6.1.0, the use of backtracking regular expressions permitted an attacker to conduct a denial of service attack against the SVGRenderer component.
CSCvw59920	Multiple Vulnerabilities in c3p0.
CSCvw61589	ISE Policy Evaluation : RADIUS requests dropped after deleting policy sets.
CSCvw64840	CIAM found mariadb vulnerable.
CSCvw68480	ISE incorrect number for the TOTAL field.
CSCvw75563	HotSpot Guest portal displays Error Loading Page when passcode field contains special characters.
CSCvw76847	ISE conditions Library corruption during Pen test.
CSCvw77219	Dot1x authentication failed due to duplicate manager: add=false.
CSCvw78269	CWE-20: Improper Input Validation to Create Node Group.
CSCvw80520	"Radius Authentication Details" Report takes time when IMS(ISE Messaging Service) is disabled
CSCvw81454	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities.
CSCvw82774	ISE 2.6/2.7 Sorting based on username does not work in User Identity Groups.
CSCvw82927	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities.
CSCvw83296	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities.
CSCvw83334	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities.

Caveat ID Number	Description
CSCvw87147	Live session is not showing the correct active session.
CSCvw87173	ISE 2.4 p13 break AD Authorization lookup for MAB authenticated endpoints.
CSCvw87175	MAB authentication via Active Directory passes with AD object disabled.
CSCvw89818	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerabilities.
CSCvw93570	ISE 2.4 patch 8 Unable to edit,.duplicate or delete guest portals.
CSCvw94096	iPod not shown as an option in ISE BYOD portal.
CSCvw95488	ISE 2.6 : Runtime crashes while TACACS+ get_handle is called by a socket stream.
CSCvw95968	Unable to create support bundle if Japanese language is selected in Account Settings.
CSCvx00245	Itune Integration is throwing error while saving though test connection is working fine.
CSCvx15427	Health Checks:DNS Resolvability: False failures with ISE FQDN as CNAME (alias).
CSCvx15448	Health Checks:Disk space: shows insufficient failure information.
CSCvx23205	Add IdenTrust Commercial Root CA 1 Certificate to ISE truststore.
CSCvx36013	ISE Health Check Platform Support should update UI directly with results.
CSCvx37149	SGA value Under-Provisioned for SNS3515 running all personas on same node.
CSCvx46638	In EAP chaining scenario, posture policy failed to retrieve machine AD group membership.
CSCvx48922	Memory leak on TACACS flow.
CSCvx50752	Add IdenTrust Commercial Root CA 1 Certificate for Smart Call Home and Smart Licensing.
CSCvx54213	Network Devices > Default Device page requires PLUS license to allow configuration.
CSCvx70327	Services not running after upgrade to 2.7.
CSCvx77418	Upgrade failed from 2.6+ restore -> P8 to 3.1.0.289.
CSCvx82808	MacOS Big Sur 11.x BYOD Failing EAPtls when using a CA Signed Certificate.
CSCvw08765	Upgrade license check should check ISE DB for smart license registration.
CSCvw51801	ISE Live Session Postured session is moving to Started upon Interim Update.
CSCvw53412	SB should collect Hibernate.log.
CSCvv63548	Memory Leak: PSN rmi GC collection not working properly causing memory leak in passive id flow.

Open Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 9

Caveat ID Number	Description
CSCvy53361	PAN login page times out after entering the credentials
CSCvx35960	TACACS + authentications fails all of a sudden with maximum connection limit reached error
CSCvq43600	Disabled PSN persona but TACACS port 49 still open

Known Limitations in Cisco ISE 2.6 Patch 9

Special Characters Usage Limitations in Name and Description Fields

- The following special characters cannot be used in the **Description** field for TACACS+ profiles and Device Administration Network conditions: [%\<>*^:"|',=/()$.@;&-!#{}.?]. Supported characters are: alphanumeric, underscore(_), and space.
- The following special characters cannot be used in the **Name** and **Description** fields for Authorization Profiles: %\<>*^:\"|',=. Supported characters for the **Name** and **Description** fields are: alphanumeric, hyphen(-), dot(.), underscore(_), and space.
- The following special characters cannot be used in the **Name** and **Description** fields for Time and Date conditions: [%\#$&()~+*@{}!/?;:',=^`]"<>". Supported characters for the **Name** and **Description** fields are: alphanumeric, hyphen(-), dot(.), underscore(_), and space.

Change in SNMP User Password Format and SNMP Hash Minimum Length

After applying Cisco ISE 2.6 Patch 9, SNMP user configuration might be removed due to the change in the SNMP user password format. SNMP user passwords are now displayed in hash format. You must reconfigure the SNMP user settings again.

SNMP hash with less than 80 characters will not work and you will see the below error:

```
snmp-server user FT10 v3 hash fe7c35f09ff1238e369968a0be273f22
fe7c35f09ff1238e369968a0be273f22
          % Error: Decryption Failed. Could not add SNMP User
```

New Features in Cisco ISE Release 2.6.0.156 - Cumulative Patch 8

Health Check

An on-demand health check option is introduced to diagnose all the nodes in your deployment. Running a health check on all the nodes prior to any operation helps identify critical issues, if any, that may cause downtime or blocker. Health Check provides the working status of all the dependent components. On failure of a component, it immediately provides troubleshooting recommendations to resolve the issue for a seamless execution of the operation.

Ensure that you run Health Check before initiating the upgrade process.

Business Outcome: Identify critical issues to avoid downtime or blockers.

DNS Cache

The DNS requests for hosts can be cached, thereby reducing the load on the DNS server.

This feature can be enabled in the configuration mode using the following command:

service cache enable hosts ttl *ttl*

To disable this feature, use the **no** form of this command.

no service cache enable hosts ttl *ttl*

Admin can choose the Time to Live (TTL) value, in seconds, for a host in the cache while enabling the cache. There is no default setting for *ttl*. The valid range is from 1 to 2147483647.

Note TTL value is honored for negative responses. The TTL value set in the DNS server is honored for positive responses. If there is no TTL defined on the DNS server, then the TTL configured from the command is honored. Cache can be invalidated by disabling the feature.

Business Outcome: Load on DNS Server is reduced.

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 8

The following table lists the resolved caveats in Release 2.6 cumulative patch 8.

Patch 8 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.

Caveat ID Number	Description
CSCuo02920	ISE not returning configured Radius AVP 18 in access-reject
CSCvf61114	ERS Update/Create for "Authorization Profile" failing XML Schema Validation
CSCvg50777	nas-update=true accounting attribute will cause session to not be deleted.
CSCvi27454	ISE 2.4 BETA : The status of the pxGrid services should show as active/standby not running/disabled
CSCvi45372	Non-internal-CA signed pxGrid certificate incorrectly replaced upon ISE reload
CSCvi62805	CSCvi62805 ISE ODBC does not convert the mac address as per configured stored procedure
CSCvm62775	ISC BIND krb5-subdomain and ms-subdomain Update Policies Vulnerability
CSCvn64652	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvo14624	Latency observed with high TPS rates, when ISE messaging service is turned ON
CSCvo35516	Device Sensor not able to correctly parse DHCP attributes via RADIUS probe
CSCvo43289	ISE truncates the SGT name after a "-" character and assigning a version id

Caveat ID Number	Description
CSCvo49521	ISE Adds an additional character at the end of OperatingSystemVersion
CSCvo75129	Runtime prepends "\" to ";" in dhcp-class-identifier in syslog message sent to profiler
CSCvp07968	ISE Repository Password is accepted in GUI but not CLI
CSCvp27534	Active endpoints missing from MNT session directory during 2.7 Longevity
CSCvp50171	core files are generated on PSN during 2.7 Longevity
CSCvp55012	GNU Wget Buffer Overflow Vulnerability
CSCvp85813	ISE TACACS livelogs does not have the option to filter using specific NAS ip address.
CSCvp86673	Application server stuck in Initializing due to corrupted indexes
CSCvq02371	High Auth Latency - no info which thread pool is guilty
CSCvq07886	Apache ActiveMQ Corrupt MQTT Frame Out of Memory Denial of Service V ...
CSCvq43600	Disabled PSN persona but TACACS port 49 still open.
CSCvq44063	Incorrect DNS config can lead to TACACS or Radius auth failure
CSCvq48503	ISE False alarm - Health status unavailable
CSCvq54061	System Summary is not available for MNT nodes
CSCvr22065	Import NAD is failing with unsupported error When shared secret key has special character (8o\v|)
CSCvr30644	glibc Multiple Vulnerabilities CVE-2018-11236, CVE-2018-11237, CVE-2018-6485 and CVE-2017-16997
CSCvr32299	Evaluate 32-bit glibc vulnerabilities RHSA-2018:0805
CSCvr33778	FreeType Buffer Over-Read Vulnerabilities
CSCvr80934	Samba Symbolic Link Traversal Vulnerability CVSS v3.1 Base: 5.4
CSCvr81384	Failing Network Devices CSV import, process silently aborting without reason
CSCvr85513	core file generated on PSN
CSCvs03195	Max Session Counter time limit option is not working
CSCvs14743	EgressMatrixCell Allows Duplicate Creation Through ERS Call
CSCvs42441	Service account passwords returned from server in SMS and LDAP page
CSCvs50437	ISE versions use old JDBC version (11.2.0.3) which is not compatible with new Oracle Database
CSCvs62597	Authz Profiles not pulling properly using REST API (Pagination is missing)

Caveat ID Number	Description
CSCvs98602	X.Org libX11 Client Segmentation Fault Denial of Service Vulnerability
CSCvs98604	X.Org libX11 Off-by-One Memory Write Arbitrary Code Execution Vulnerable
CSCvt11179	"AD-Operating-System" attribute is not being fetched when this OS attribute changes on the AD Server
CSCvt15787	TCPDump - Node and Interface field Unavailable
CSCvt46850	Unavailability to edit saved compound conditions using conditions library.
CSCvt53541	SMS over HTTPS is not sending username/password to gateway
CSCvt64739	Application Server takes more time to initialize
CSCvt65853	ISE-2.x || MNT REST API for ReAuth fails when using in distributed deployment
CSCvt68108	ISE Server-side authorization checks insufficient
CSCvt70689	Application server may crash when MAR cache replication is enabled
CSCvt71355	pxGrid unable to delete user in INIT state
CSCvt73953	Mismatched Information between CLI export and Context Visibility
CSCvt80285	Cannot select 45 or more products when creating Anti-Malware Condition for definition
CSCvt81194	CPU spikes are being observed at policy HitCountCollector
CSCvt85836	Session cache getting filled with incomplete sessions
CSCvt93117	ise-psc.log filled up with "check TTConnection is valid" causing relevant logs to roll over
CSCvt96594	ISE 2.6 : Create Guest User using external sponsor users via ERS fails with 401 Unauthorized Error
CSCvu01181	ISE 2.6 : TacacsConnectionManager needs to be enhanced to remove the stale connections
CSCvu04874	suspected memory leak in io.netty.buffer.PoolChunk
CSCvu05164	ISE is not allowing to disable Radius in NAD via API
CSCvu13368	ISE : Oracle process reached limit : causing multiple issues
CSCvu15948	TC-NAC adapter stopped scanning with nexpose (insiteVM)
CSCvu21093	ISE 2.6p6 // Portal background displays incorrectly
CSCvu25625	ISE is returning an incorrect version for the rest API call from DNAC
CSCvu25975	Import option is not working under TACACS command sets

Caveat ID Number	Description
CSCvu26008	portal page customization changes are not reflecting in certificate provisioning portal
CSCvu28305	ISE logging timestamp shows future date
CSCvu30286	ERS SGT create is not permitted after moving from Multiple matrix to Single matrix
CSCvu31176	2.4P11 VPN + Posture : Apex Licenses are not being consumed,
CSCvu31853	NDG added through ERS became associated with all network devices in DB
CSCvu32240	When running ISE ERS API for internaluser update the existing identityGroups value is set to null
CSCvu33416	License out of compliance alarm with a valid license
CSCvu33861	ISE 2.4 p6 - REST API MnT query to get device by MAC address taking more than 2 seconds
CSCvu33884	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvu35506	code for securityGroupAclTopic missing from 2.4 and 2.6, but topic still advertised
CSCvu35802	Shared email for AD users fail to retrieve groups,ISE shows multiple account found in forest
CSCvu39653	Session API for MAC Address returning Char 0x0 out of allowed range
CSCvu41815	[CFD] GBAC sync breaks on deleting VN from SG if AuthZ profile is mapped to the same VN for diff SG
CSCvu45697	Compress messages.x files in the system
CSCvu47395	ISE 2.x, 3.x : Drop_Cache required for systems with High Memory Issues
CSCvu49019	suspected Memory Leak in Elastic search
CSCvu53836	ISE Authorize-Only requests are not assessed against Internal User Groups
CSCvu55557	Radius secret 4 chars min requirement is not checked when REST API used to create NAD
CSCvu58793	ERS REST API returns duplicate values multiple times when use filter by locations
CSCvu59093	SessionDB columns are missing from ISE (>=2.4)
CSCvu59491	ISE creates new site in insiteVM (tc-nac server)
CSCvu63833	Failed Logins to ISE GUI Are Not Seen in Audit Report When AD Is Selected as the Identity Source
CSCvu69478	ISE: REST API PUT query may fail after successful ERS Guest queries
CSCvu70768	Alarms and system summary is not showing up on ISE GUI

Caveat ID Number	Description
CSCvu73387	authentication failure with reason"12308 Client sent Result TLV indicating failure"
CSCvu90107	ISE allows duplicates device ID in ERS flow in all version.
CSCvu90761	ISE Radius Live Sessions Page Showing No Data Found
CSCvu91016	InternalUser Attributes in ATZ policy will fail TACACS+ ASCII Authentication
CSCvu91601	ISE Authentication Status API Call Duration does not work as expected
CSCvu93259	HitCount REFRESH and RESET button is not visible in ISE 26p7,p9
CSCvu94025	ISE should either allow IP only for syslog targets or provide DNS caching
CSCvu97041	Restore of Config backup on ISE 2.6 P7 is causing issues with node registration
CSCvu97657	ISE 2.4 Application server going to Initializing on enabling endpoint debugs
CSCvv00377	Overlap of network devices using subnet and IP range
CSCvv04416	ISE:SEV3:Endpoint data not visible on secondary Admin node .
CSCvv07049	ISE unable to connect with ODBC "Connection failed" with a port number
CSCvv08466	Log Collection Error alarms appear
CSCvv09167	TACACS Aggregate table is not purged properly.
CSCvv10572	Unable to register IND with ISE on 2.4 P13
CSCvv10683	Session Cache for dropped session not getting cleared; causing High CPU on the PSN's
CSCvv14001	ISE : Authz profile not saved with proper attributes when Security Group selected under common tasks
CSCvv23256	ISE Authentication Status API Call does not return all records for the specified time range
CSCvv25102	Modify TCP settings to enhance TACACS+ and TCP on ISE
CSCvv26811	Policy Export Is Not Being Saved Without Encryption After It is Saved With Encryption
CSCvv42857	MAC 11.0 support for ISE is not available
CSCvv43383	NFS Repository is not working from GUI
CSCvv43558	Evaluation of positron for Apache Struts Aug20 vulnerabilities
CSCvv48544	Health check doesn't work when ISE has NIC teaming enabled
CSCvv50563	Filters do not work for ISE Profiler Reports
CSCvv54761	Export of Current active session reports only shows sessions that has been updated since midnight

Caveat ID Number	Description
CSCvv57639	Saving command with parenthesis in TACACS command set gives an error (ISE 2.7 p2)
CSCvv57830	Group lookup failed as empty value to be appended to the context
CSCvv67935	ISE - Security Group values in Authorization Profile disappear shortly after fetching
CSCvv72306	No password audit will be generated after changing ISE internal user password via Switch/Router CLI
CSCvv74373	ISE 3.0 DNS resolvability false Alarm
CSCvv39584	Remove ojdbc8 from 2.6/2.7 patch branch
CSCvv41074	Multiple version of ojdbc in 2.6p7 results in licensing/mnt/deployment issues

New Features in Cisco ISE Release 2.6.0.156 - Cumulative Patch 7

ANC Enhancement

MAC address is not always a unique identifier for an endpoint. USB NIC dongles means that multiple users can have the same MAC address. Plus, some endpoints have the same MAC address. MAC spoofing also shows duplicate MAC addresses.

To better identify an endpoint for the ANC service, Cisco ISE uses the IP address of the switch that the endpoint is connected to. The switch's IP address is the `NAS-IPAddress` attribute.

Endpoint sessions can use the MAC address and `NAS-IPAddress` in an ANC Policy.

MDM vendors can use `NAS-IPAddress` in pxGrid v2 API.

PxGrid v2 is required to use `NAS-IPAddress` in the new API. The existing API still works. But you cannot use both the old and new APIs together.

Upgrading Cisco ISE Consideration

If you upgrade to Cisco ISE 2.6 patch 7, you will see an error message if you were using the RE_AUTHENTICATE in an ANC policy. The existing policies will still work.

Applying Cisco ISE 2.6 patch 2 eliminates the error message. Or you can remove those policies before upgrading.

Enable Probe Data Publisher

The Probe Data Publisher initiates a pxGrid publisher on the Primary Policy Administration Node (PAN). When the primary PAN identifies a change in attributes for a connected endpoint, the updated attribute data is published to the relevant pxGrid Topic in Cisco ISE.

This option, by default, is not enabled. We recommend that this option be enabled only if you have an external data consumer configured.

To enable the Probe Data Publisher, go to **Work Centers** > **Profiler** > **Settings**, and check the **Enable Probe Data Publisher** checkbox.

Telemetry

After installation, when you log in to the Admin portal for the first time, the Cisco ISE Telemetry banner is displayed. Using this feature, Cisco ISE securely collects nonsensitive information about your deployment, network access devices, profiler, and other services that you are using. This data will be used to provide better services and more features in the forthcoming releases. By default, telemetry is enabled. To disable or modify the account information, choose **Administration > Settings > Network Settings Diagnostics > Telemetry**. The account is unique for each deployment. Each admin user need not provide it separately.

Telemetry provides valuable information about the status and capabilities of Cisco ISE. Telemetry is used by Cisco to improve appliance lifecycle management for IT teams who have deployed Cisco ISE. Collecting this data helps the product teams serve customers better. This data and related insights enable Cisco to proactively identify potential issues, improve services and support, facilitate discussions to gather additional value from new and existing features, and assist IT teams with inventory report of license entitlement and upcoming renewals.

It may take up to 24 hours after the Telemetry feature is disabled for Cisco ISE to stop sharing telemetry data. Starting with patch 6, telemetry is disabled immediately.

Interactive Help

The Interactive Help provides tips and step-by-step guidance to complete tasks with ease.

Business Outcome: This helps the end users to easily understand the work flow and complete their tasks with ease.

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 7

The following table lists the resolved caveats in Release 2.6 cumulative patch 7.

Patch 7 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.

Caveat ID Number	Description
CSCvb55884	ISE RBAC Network Device Type/Location View not working
CSCvd38796	No AD domain attributes retrieved for RA-VPN/CWA if AD used for both authC and authZ
CSCvj47301	ISE sends CoA to active-compliant sessions when a node-group member is unreachable
CSCvn12644	ISE Crashes during policy evaluation for AD attributes
CSCvn50531	tcpdump print_prefix Function Stack-Based Buffer Overread Vulnerability
CSCvo15781	Logwatch files are not capped for size
CSCvo28970	AnyConnect displays Cisco NAC agent error when using Cisco temporal agent
CSCvo51415	ISE 2.4 URT fails with cert error
CSCvo68357	ISE restore option should not have <cr> Carriage return without encryption-key
CSCvo73749	'MAR cache distribution is not enabled' even when it has been enabled.

Caveat ID Number	Description
CSCvp16483	Remove older journal log files
CSCvp17458	libssh2 SSH_MSG_CHANNEL_REQUEST Packet Handling Out-of-Bounds Read V ...
CSCvp40398	Cannot configure scheduled config and operational backup with start date same as current day
CSCvq07619	GnuPG Filename Status Message Spoofing Vulnerability
CSCvq13431	ISE PSN node crashing while fetching context attributes during posture plus RADIUS flow
CSCvq19646	Evaluation of positron for TCP_SACK
CSCvq48396	Replication failed alarm generated and ORA-00001 exceptions seen on ise-psc.log
CSCvq61089	My Device Portal does not show a device after BYOD on-boarding with SAML authentication
CSCvq73677	GNU patch OS Shell Command Injection Vulnerability
CSCvq86741	FasterXML jackson-databind logback-core Class Polymorphic Deserializ ...
CSCvq86746	Multiple Vulnerabilities in jquery - guest portals
CSCvr09749	GNU patch do_ed_script OS Shell Command Execution Vulnerability
CSCvr19392	Apache Commons Beanutils PropertyUtilsBean Class Property Suppression Vulnerability
CSCvr39943	Blank Course of Action for Threat events received from CTA cloud to TC-NAC adapter
CSCvr40545	EAP-FAST authentication failed with no shared cipher in case of private key encryption failed.
CSCvr47732	FasterXML jackson-databind Polymorphic Typing Vulnerability CVSS v3.1 Base: 9.8
CSCvr47790	Apache Commons Compress File Name Encoding Algorithm DoS Vulnerability CVSS v3.0 Base: 7.5
CSCvr56785	Localdisk size needs to be increased to accommodate large corefiles
CSCvr77676	libmspack chmd_read_headers Function Denial of Service Vulnerability
CSCvr84753	ISE 2.2 patch 14 AD status shows up as "updating.." indicating the process is hung
CSCvr85363	ISE App crash due to user API
CSCvr87373	ACI mappings are not published to SXP pxGrid topic
CSCvs05260	App server and EST services crash/restart at 1 every morning

Caveat ID Number	Description
CSCvs09981	Add the capability to filter out failed COA due to MAR cache checks among group nodes in ISE
CSCvs19481	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvs23628	Policy engine continues to evaluate all Policy Sets even after rule is matched
CSCvs25569	Invalid root CA certificate accepted
CSCvs36758	Unable to configure CRL URL with 2 parenthesis at ISE 2.6
CSCvs38883	Trustsec matrix pushing stale data
CSCvs39880	Highload on Mnt nodes with Xms value
CSCvs40406	SEC_ERROR_BAD_DATABASE seen in system/app debug logs while removing a trusted CA cert
CSCvs42758	The CRL is expired with specific condition
CSCvs44006	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvs44795	ISE not updating SGT's correctly
CSCvs46399	AuthZ profile advanced profile for url-redirect does not allow custom HTTPS destination
CSCvs46853	ISE 2.6 CA Certificate with the same CN removed from Trusted Store while integrating with DNA-C
CSCvs46998	Condition disappeared from the library but is still in DB
CSCvs47941	Fail to import Internal CA and key on ISE2.6
CSCvs51519	NFS mounting causes crash
CSCvs52031	MACAdress API is not working(API/mnt/Session/MACAddress)
CSCvs55464	Creating a new user in the sponsor portal shows "invalid input"
CSCvs55594	Days to Expiry value, marked as 0 for random authentications
CSCvs58106	NAD CSV imports should allow all supported characters in the TrustSecDeviceID
CSCvs60518	ISE Admin User Unable To Change The Group For Internal Users
CSCvs62081	collector log is dumped with pxgid and dnac messages
CSCvs62586	Tacacsprofile not retrieved properly using REST API
CSCvs65467	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvs65989	After importing network device / groups, unable to add new Location

Caveat ID Number	Description
CSCvs67042	ISE 2.2+ affected with memory leak. Everyday 1-2% increase in native memory due to Inflater()
CSCvs67785	Days duration is not getting updated in portal page customization for self registration portal
CSCvs68914	Errors when SG created using _ underscore sent from DNAC
CSCvs69726	ISE 2.2+ affected with memory leak. Everyday 1-2% increase in native memory by PORT_Alloc_Util()
CSCvs70863	ISE 2.6 - Cannot enable FIPS if Default Device Admin has been modified
CSCvs70997	ISE: 2.4p9 Intermediate CA cert not installed when configuring SCEP RA
CSCvs75274	Unable to do portal customization for "certificate provisioning portal"
CSCvs76257	ISE crashes due to empty string instead of username in RadiusProxyFlow::stripUserName()
CSCvs77182	ISE: Unable to use attribute "url-redirect" with HTTPS, same URL with HTTP works fine.
CSCvs78160	URT fails on a ConditionsData clause from INetworkAuthZCheck
CSCvs83303	API is not retrieving the data when interim-updates are not stored DB
CSCvs84948	Multiple Vulnerabilities in binutils
CSCvs85970	Having string 'TACACS' in AD join-point causes AD joinpoint to not show in AuthZ condition
CSCvs86344	ISE 2.4 Guest ERS Call Get-By-Name fails when guest username contains @ sign (guest@example.com)
CSCvs86686	Multiple Vulnerabilities in patch
CSCvs86690	Multiple Vulnerabilities in python
CSCvs86697	Multiple Vulnerabilities in sudo
CSCvs86775	ISE 2.6 Install: Input Validation- Check IP Domain Name
CSCvs88222	Vulnerability in unzip package - RHEL 7
CSCvs88368	ISE SNMP server crashes when using Hash Password.
CSCvs91808	Importing metadata xml file with special characters results in unsupported tags error
CSCvs96541	ISE 2.4 P11 On OP Backup Restore, EPOCH_TIME column is removed
CSCvs97302	.dmp files not deleted from /opt/oracle/base/admin/cpm10/dpdump even after the reset-config on ISE

Caveat ID Number	Description
CSCvt00283	404 error upon refresh of success page of guest sponsored portal
CSCvt01161	NMAP - MCAFeeEPROOrchestratorClientscan fails to execute on 2.6 version of ISE
CSCvt03094	ISE expired tacacs session not cleared timely from session cache
CSCvt03292	Cert Revoke and CPP not functioning without APEX license.
CSCvt03935	Change "View" Options Wording in TrustSec Policy Matrix--ISE
CSCvt04047	POST getBackupRestoreStatus occures on every ISE page after navigating to Backup/Restore menu
CSCvt04144	No threshold option for High disk Utilization in Alarm Settings
CSCvt05201	Posture with tunnel group policy evaluation is eating away Java Mem
CSCvt07230	ISE shouldn't be allowing ANY in egress policy when imported
CSCvt08143	Time difference in ISE 2.6
CSCvt10214	[ENH] Add the ability to "GET|PUT|DELETE by Name" using the API for network devices
CSCvt12236	IP SGT static mapping import not working correctly with hostnames
CSCvt13198	FasterXML jackson-databind xbean-reflect/JNDI Blocking Vulnerability
CSCvt13707	pxGrid 2.0 WebSocket distributed upstream connect issue
CSCvt13719	pxGrid 2.0 WebSocket ping pong too slow even on idled standalone
CSCvt13746	ISE doesn't display all device admin authz rules when there are more authz policies and exceptions
CSCvt14248	Certificate Authority Service initializing EST Service not running after upgrade to ISE 2.6
CSCvt15256	Authentication goes to process fail when "Guest User" ID Store is used.
CSCvt15893	Radius Errors/Misconfigured supplicants tables do not exist after upgrade to ISE2.6
CSCvt15935	PERMGEN configured instead of metaspace for JDK8
CSCvt16882	When accessing the portal with iPad using Apple CNA and AUP as a link we get 400 Bad Request error.
CSCvt17335	Publishing batch logic in Pxgrid when we use WMI and REST at the same time
CSCvt17783	ISE shouldn't allow ANY SGT or value 65535 to be exposed over SGT import or export
CSCvt19657	ISE ERS API Endpoint update slow when large number of endpoints exist

Caveat ID Number	Description
CSCvt24276	Cannot add/modify allowed values more than 6 attributes to System Use dictionaries
CSCvt35044	EP lookup takes more time causing high latency for guest flow
CSCvt36117	Identity group updates for an internal user in ISE
CSCvt36322	ISE 2.6 MDM flow fails if redirect value is present in the URL
CSCvt36324	Hostname goes missing from CARS configuration
CSCvt37910	[ENH] Add the ability to "GET|PUT|DELETE by Name" using the API for /ers/config/internaluser
CSCvt38308	ISE: If min pwd length is increased then existing shorter pwd fails to login via GUI with no error
CSCvt40534	MNT node election process is not properly designed.
CSCvt49961	Syslog Target configured with FQDN can cause Network Outage
CSCvt57027	Authentication Status API call on ISE 2.6p5 returns blank output
CSCvt57571	App-server crashes if IP-access submitted w/o any entries
CSCvt57805	Intermittent password rule error for REST API Update Operation
CSCvt61181	ISE ERS API - GET call on Network Device is slow while processing SNMP configuration
CSCvt71559	Alarm Dashlet shows 'No Data Found'.
CSCvt85722	No debug log for non working MNT widgets
CSCvt87409	ISE DACL Syntax check not detecting IPv4 format errors
CSCvu10009	PUT verb for /ers/config/internaluser/name/{username}makes id&password&name mandatory in req content
CSCvu14634	EAP TLS authentication is getting failed in 2.6p5 /p6 after backup restore from 2.6p3
CSCvu42244	Machine authentication via EAP-TLS is failing during authorization flow with user not found error

Open Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 7

Caveat ID Number	Description
CSCvv41074	Multiple version of ojdbc in 2.6p7 results in licensing/mnt/deployment issues.

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 6

The following table lists the resolved caveats in Release 2.6 cumulative patch 6.

Patch 6 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.

Caveat ID Number	Description
CSCvi35647	Posture session state need to be shared across PSNs in multi-node deployment
CSCvp05303	Provisioned Certificates are not getting deleted after revocation
CSCvs82557	SXP Bindings are not published to pxGrid 2.0 clients

New Features in Cisco ISE Release 2.6.0.156 - Cumulative Patch 5

Cisco AI Endpoint Analytics Support

Cisco AI Endpoint Analytics is a solution on Cisco DNA Center that improves endpoint profiling fidelity. It provides fine-grained endpoint identification and assigns labels to various endpoints. Information gathered through deep packet inspection, and probes from sources like Cisco ISE, Cisco SD-AVC, and network devices, is analyzed for endpoint profiling.

Cisco AI Endpoint Analytics also uses artificial intelligence and machine learning capabilities to intuitively group endpoints with similar attributes. IT administrators can review such groups and assign labels to them. These endpoint labels are then available in Cisco ISE if your Cisco ISE account is connected to an on-premise Cisco DNA Center.

These endpoint labels from Cisco AI Endpoint Analytics can be used by Cisco ISE administrators to create custom authorization policies. You can provide the right set of access privileges to endpoints or endpoint groups through such authorization policies.

Open Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 5

After you install Cisco ISE 2.6 Patch 5, guest authentications based on SSID may fail due to an issue being tracked by CSCvt36324. In this case, run the command

```
show running-config
```

to check if hostname is available. If the hostname is not available, contact Cisco TAC to troubleshoot this issue.

Caveat ID Number	Description
CSCvt36324	Redirection not happening as hostname name missing from CARS configuration
CSCvt36452	Expired Evaluation profiler on ISE will cause default radius probe to enable

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 5

The following table lists the resolved caveats in Release 2.6 cumulative patch 5.

Patch 5 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.

Caveat ID Number	Description
CSCux25333	ISE Dashboard allows special characters: <>?"
CSCux25342	Custom filters not working in Session Status column in Live Sessions window
CSCuz18895	CoA REST API is not working for ASA VPN Sessions
CSCvc71503	Endpoints lose static group assignment
CSCve89689	MNT API does not support special character
CSCvf59076	Live sessions show incorrect Authorization profile and Authorization Policy for VPN and Posture scenario
CSCvf94942	TACACS authorization rule fails with no clear explanation when there is no command set defined for the rule if there is a VSA in the shell profile
CSCvh86082	Parsing NMAP smb-os-discovery data should remove
or \x00
CSCvj43999	Self-signed account creation error: "An attempt to text your account information to you has failed"
CSCvj67437	Multiple Vulnerabilities in procps-ng
CSCvj88164	Licensing consumption is incorrect for postured sessions with remote-access VPN
CSCvk48115	ISE 2.3 RSA SecurID authentication fails
CSCvk50684	Not able to delete certificate after hostname change
CSCvm15495	Evaluation of positron for CVE-2018-5391 (FragmentSmack)
CSCvm46997	Multiple Vulnerabilities in openssh
CSCvm56657	Windows 7 device is profiled wrongly post Posture flow, due to anyconnect sending wrong useragent
CSCvn55560	After applying ISE 2.3 patch 5, creation of EOB Guest user does not work
CSCvn73729	Error occurred in publishing threat events with AMP adapters
CSCvo02285	Errors seen in /var/log/secure every 10 seconds for isemntlogproc
CSCvo22887	ISE 2.4 URT does not check if node is on a supported appliance
CSCvo28578	ISE 2.3: Location info and IPSEC info are reversed in Network Device Groups for some NADs

Caveat ID Number	Description
CSCvo47391	Multiple Vulnerabilities in krb5
CSCvo49755	To enable CLI clock timezone command
CSCvo82930	ProfilerCoA:- Exception in getting Policy details Exception seen in Profiler.log
CSCvo87602	Memory leak on ISE node with the openldap rpm running version 2.4.44
CSCvo90281	Patchupload files greater than 1GB don't get deleted while upgrading if upload through WebGUI is interrupted
CSCvo90380	Sponsored Guest account start date is not adjusted when account is extended
CSCvp07591	EAP-GTC Machine Authentication Failure password mismatch due to UTF-8 Validation Check failure
CSCvp12685	Cross-Site Request Forgery (CSRF) [OWASP_CSRFTOKEN bypass]
CSCvp19539	ISE 2.2 Sign On button grey out with Guest portal second factor Radius Token server authentication
CSCvp19738	ISE 2.4 live sessions cannot be filtered based on authentication or authorization policy
CSCvp20910	Cisco Smart Licensing cloud agent in waiting state causes GUI login delay in ISE 2.2
CSCvp24085	ISE 2.4 High CPU utilization on Secondary Admin Node
CSCvp35021	Able to delete CA from trusted page when external CA signs any system certificate
CSCvp40509	Internal User not found in prrt-server intermittently even though PrRTCpmBridge returns user found
CSCvp52008	IETF Dictionary Attribute Ascend-Client-Primary-DNS broken after upgrade
CSCvp70644	Expired guest accounts purge is stuck after daylight time change
CSCvp73335	Radius session detail report is broken if calling-station-id contains CLIENTVPN
CSCvp91987	Wrong job (HOURLY_STATS_JOB) running
CSCvq07756	Network device Import to ISE takes too long when IPV6 address is included
CSCvq30417	MnT Purge with option to export repository not working
CSCvq40899	When binding external CA sign certificate in intermediate CA CSR, certificate chain is broken in CA page
CSCvq49292	ISE TACACS Authentication and Accounting reports older than 30 days missing
CSCvq50182	ISE does not show logging when CTS pac is expired
CSCvq61878	Evaluation of ISE for CVE-2018-20685
CSCvq69138	Change logging level of 90140 INFO PassiveID: Message parsed syslog to DEBUG

Caveat ID Number	Description
CSCvq80132	Trashing IP SGT Static mappings across pages never completes
CSCvq83410	Maximum thread value limit is too low and triggers "Admin thread pool reached threshold value" alarm
CSCvq88821	SNMP traps on access switch connected to Access Points cause incorrect profiling.
CSCvq96801	All SNMP packets are logged to /var/log/messages file
CSCvq97641	ISE 2.4 localhost-<date>.log files growing up to and more than 8 Gb in size
CSCvq98277	No password audit is generated when a user changes ISE internal user enable password via ASA CLI
CSCvq99963	Application Server crash observed in Passive ID dashboard after some time if number of active sessions is more than 200K
CSCvr00348	Posture assessment by condition report is showing empty records
CSCvr06487	ISE Posture Agent Profile does not allow blank remediation timer
CSCvr07263	When creating Purging Rule, Radius directory hangs if there is no plus license
CSCvr07464	ISE 2.6 MUD URL is not parsed correctly if IP address or port is used
CSCvr08988	In external Radius scenario, ISE should replace state attribute before forwarding access challenge to NAD
CSCvr09759	Certificate is not loading from Oracle to NSSDB properly
CSCvr11769	ISE 2.4: Advanced Custom Filter option and export of reports not working as expected
CSCvr12350	"MDM: Failed to connect to MDM server" log entry must include endpoint information
CSCvr13218	Framed-Interface-Id RADIUS attribute not sent in access-accept if IPv6 address is in ::xx format
CSCvr13464	ISE ERS SDK NetworkDeviceGroup PUT does not show ID placement in the API call
CSCvr13481	ISE ERS SDK NetowrkDeviceGroup DELETE does not specify ID location
CSCvr13649	pxGrid XMPP GCL Reconnect failure
CSCvr24458	Network Device POST API allows for characters and spaces in Model name of device but GUI does not
CSCvr25197	After changing password via UCP, "User change password audit" report doesn't have "Identity"
CSCvr29863	When ISE and Cisco DNA Center are integrated, network devices do not appear in ISE when the secret value contains both special characters & and \
CSCvr31312	ISE fails to load network devices page while filtering on IP/Mask

Caveat ID Number	Description
CSCvr32199	Systemd vulnerabilities RHEL 7 RHSA-2019:0049
CSCvr35154	Read-only admin users are able to view TrustSec device configuration credentials
CSCvr35719	Unable to get all tenable adapter repositories
CSCvr36392	Network Devices description issue with Japanese Language
CSCvr38857	Radius Authentication report missing log when custom filter is used
CSCvr40359	ISE not using the device-public-mac attribute in endpoint database
CSCvr40574	Export failed in ISE GUI when private key encryption failed
CSCvr46529	Password lifetime expiration reminder appears for Internal Users with external passwords
CSCvr47215	ACS 5.7 to ISE 2.6 migration doesn't import authorization profiles
CSCvr48043	Multi Shared Secret Field is being populated for exported TACACS devices
CSCvr48101	Unexpected CoAs may be observed with SCCM MDM
CSCvr48729	Unable to access My Devices portal
CSCvr50921	GUI login with AD user failed when similar internal user is disabled
CSCvr51940	ISE not searching machine account properly on AD
CSCvr51959	ISE 2.4: Incorrect sponsor portal presented to user due to incorrect FQDN match
CSCvr53428	ISE services are not coming up after installing patch 2.3 p7
CSCvr57378	DHCP messages are marking endpoints active thereby increasing the active endpoint count
CSCvr60339	Typo in Max Sessions window in Counter Time Limit tab
CSCvr61108	PxGrid ANC API support for Session-ID
CSCvr62517	ISE 2.4 p9: Session directory write failed : String index out of range: -1 alarms seen in the deployment
CSCvr63504	Unable to delete SCEP profile because it is referencing system certificates
CSCvr64067	ISE MnT stops showing Live Logs after 90% Purge
CSCvr67988	ISE sponsor's e-mail gets CCed in guest credential email even when view/print guest' passwords is disabled
CSCvr68971	ISE IP routing precedence issue
CSCvr70581	Called-Station-ID missing in RADIUS Authentication detail report

Caveat ID Number	Description
CSCvr71796	SCCMException seen in SCCM flow and MDMServerReachable value is updated as false in MDMServersCache
CSCvr77321	WSA receives SIDs instead of AD groups from ISE
CSCvr81522	Definition date for few AM product like mcafee and symantec is listed false
CSCvr83696	ISE prefers cached AD OU over new OU after changing the Account OU
CSCvr84125	Config restore from one platform on another platform set incorrect UDI in sec_hostconfig table
CSCvr84143	tzdata needs to be updated in ISE guest OS
CSCvr84978	ISE LDAP bind test does not use the correct server when defined per node
CSCvr86380	Replication alarm when trustsec matrix CSV imported with EMPTY SGACL that is already EMPTY in GUI
CSCvr87936	Valid Base and Plus licenses show out of compliance
CSCvr90773	Live Logs show wrong username in "5436 NOTICE RADIUS: RADIUS packet already in the process" messages
CSCvr95948	ISE fails to re-establish External syslog connection after break in connectivity
CSCvr96003	SYSAUX tablespace is getting filled up with AWR and OPSSTAT data
CSCvr96189	NDG device references not removed from ISE DB thereby preventing NDG deletion
CSCvr98395	No profiling CoA for ip based profile policy
CSCvs01924	ERS Admin account disabled incorrectly due to password expiry
CSCvs01949	ISE Messaging service triggers Queue Link error alarms with reason basic_cancel
CSCvs02166	Different results seen in API calls and GUI
CSCvs03195	Max Session Counter time limit option is not working
CSCvs03810	ISE doesn't display the correct user in RADIUS reports if username is entered differently twice
CSCvs03998	ISE 2.3 p6 LDAP test GUI flow with multiple results does not generate error observed in runtime
CSCvs04047	Authorization Profile created using ERS API does not match with "ASA VPN" field in GUI
CSCvs04433	PSN crashes for TACACS+
CSCvs05104	Set max time frame to 60 mins when EndPoint default interval disabled
CSCvs07344	Reset config on 2.4 patch 9 throws some errors despite finishing successfully

Caveat ID Number	Description
CSCvs12409	ISE Guest creation API validation for Guest Users valid Days doesn't take time into account
CSCvs14297	PassiveID: Configuring WMI with an AD account password that contains $ character throws an error
CSCvs24704	LDAP ID store corruption alarm - Enhancement
CSCvs25258	Improve behavior against brute force password attacks
CSCvs27310	ISE 2.6 and 2.7 - Cannot add character ' in dACL description field
CSCvs36036	ISE 2.6 should allow multiple blank lines in dACL syntax, even if user chooses IPv4 or IPv6
CSCvs36150	ISE 2.x Network Device stuck loading
CSCvs41571	Self Registered Guest portal unable to save guest type settings
CSCvs42072	Unable to edit static group assignment
CSCvs51296	ISE allows to insert a space before command under Command Sets
CSCvs51537	Backups are not triggering with special characters for encryption key
CSCvs53148	Multiple endpoints profiled every second causing ISE nodes to go out of sync
CSCvs59955	RabbitMQ Container failed to start when port 15672 is in use
CSCvr76574	When an internal user is configured with external passwords, Enable authentication function is broken
CSCvp54240	HSTS is not implemented for root folder
CSCvr70044	"No policy server" error seen in ISE posture module during high load
CSCvt18276	Corrupt Endpoints: Attributes associated to the incorrect Endpoint
CSCvr63698	pxGrid 2.0 authorization profile attribute missing from the session directory

New Features in Cisco ISE Release 2.6.0.156 - Cumulative Patch 3

Multi-DNAC Support

Cisco DNA Center systems cannot scale to more than the range of 25 to 100 thousand endpoints. Cisco ISE can scale to two million endpoints. Currently, you can only integrate one Cisco DNA Center system with one Cisco ISE system. Large Cisco ISE deployments can benefit by integrating multiple DNA Center clusters with a single Cisco ISE. Cisco now supports multiple Cisco DNA center clusters per Cisco ISE deployment, also known as Multi-DNAC.

Business Outcome: This feature for the Access Control app in Cisco DNA Center allows you to integrate up to four Cisco DNA Center clusters with a single Cisco ISE system.

Resolved Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 3

The following table lists the resolved caveats in Release 2.6 cumulative patch 3.

Patch 3 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.

Caveat ID Number	Description
CSCvd16468	Missing NAD info in Alarm "Unknown SGT was provisioned"
CSCvd48081	The software shouldn't allow to delete the pxGrid certificate on a ISE node
CSCvf45991	Pseudo double Auth request on AD
CSCvg60477	ISE 2.3+ does not have authentication condition Network Access:AuthenticationMethod
CSCvg65262	ISE easy wireless setup - SAW secure access wizard not working with wlc code >8.3
CSCvi72862	ISE : Accounting updates tolerance for suppression needs to be more efficient.
CSCvj67166	Supported server ciphers for TLSv1.2 need 2048-bit option
CSCvk52874	ISE does not provide the expected values in the context of EAP chaining
CSCvk53782	ISE ENH : Allow RADIUS Dictionary VSA "Vendor Attribute Size Field Length" of 2 bytes
CSCvm73337	Remove ciphers with Diffie-Hellman moduli size less than or equal to 1024 bits for SSL connections
CSCvm81230	Cisco Identity Services Engine (ISE) Arbitrary Client Certificate Creation Vulnerability
CSCvn21926	Parser error seen with Threat Centric NAC CTA Configuration irrespective of ise version
CSCvn66106	ISE custom attributes not being applied to endpoint when pushed from cloudpost IND
CSCvn70558	MDMServerReachable does not work for SCCM MDM again
CSCvn79043	ISE 2.4 Live Logs Not Filtering
CSCvo04342	Multiple Vulnerabilities in jackson-databind
CSCvo07993	Qualys show connected state once disable/enable tc-nac if added before applying patch.
CSCvo24097	Disclose invalid username by Always show invalid name configuration not working
CSCvo29478	ISE 2.3 P5 ISE doesn't allows to delete SGT tag from GUI although it is not referenced
CSCvo30170	Guest portal client provisioning customization text doesn't save
CSCvo33696	ISE2.4 doesn't reset failedLoginAttempts after successful login of internal users to network device

Caveat ID Number	Description
CSCvo51295	ISE 2.2 Sponsor: Single click approval displays wrong message after clicking on approval link twice
CSCvo64085	The calculation of required space for MNT backup need to be revalidated.
CSCvo94666	ISE 2.4 P5 : Profiling : Netflow probe not working on ISE Bonded Interface
CSCvp00421	ISE Profiler SNMP Request Failure Alarms should show the reason of failure
CSCvp01553	No serialization or batching when large scale(>300) NADs are moved between MatrixA to MatrixB
CSCvp02082	Env data is missing when TrustSec-ACI integration is enabled.
CSCvp03249	ISE: SMTP server sending Email notification gets Exhausted
CSCvp22075	ERS API that requires CSRF token always failing on PUT/POST/DELETE
CSCvp28377	Change in External admin permissions are not getting reflected in other nodes in deployment.
CSCvp33598	ISE deletes all endpoint if mac address is deleted twice at the same time
CSCvp45598	SystemTest : Error when deleting SCEP RA profile
CSCvp46165	Posture redirect fails with error 'unable to determine peer' in AnyConnect_ISEPosture.txt
CSCvp47029	ISE 2.4 With CTA threat, threat endpoints are not detecting
CSCvp51033	GUI Context Visibility report export slowness
CSCvp54424	AD Diagnostic tool shows low level API query failed w/ Response contains no answer. Check DNS config
CSCvp56265	Unable to disable MDM server if configured server is not reachable
CSCvp58616	SQLite FTS3 Query Processing Integer Overflow Vulnerability
CSCvp62113	Enforce NMAP skip host discovery and NMAP scan timeout
CSCvp63038	System Test: Temporal agent installation is failing with internal system error.
CSCvp65586	[pxGrid XMPP Server] TCP/5222 insecure Diffie-Hellman prime p 1024 bits
CSCvp73076	Log Collection Error - Session directory write failed when AD Probe Session is inserted
CSCvp73385	Authentications start failing once AD throws KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
CSCvp74154	Unable to remove an endpoint from the endpoint database due to permission error
CSCvp75207	2.4 P8/P9 Certificate chain does not get imported to Patch 8 and Patch 9

Caveat ID Number	Description
CSCvp77008	ISE LogicalProfile appears under Custom attributes in CV if configure after valid Custom attributes
CSCvp77014	ISE trustsec custom view doesn't sort properly with manual order
CSCvp83214	ISE ERS Create via the API does not use the specified ID
CSCvp88443	ISE CoA is not sent even though new Logical Profile is used under Authz Policy Exceptions
CSCvp88940	Can't use endpoint group description during runtime for authz profile
CSCvp96921	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvp98834	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities
CSCvp98851	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvq04802	ISE fails to handle SAML authentication response token
CSCvq08423	Certificate provisioning portal error with ISE as SubCA and PKCS12 (sinlge file)
CSCvq14925	Renewed self-signed certificate doesn't get updated in trusted store
CSCvq15329	Restore failing for scheduled backup
CSCvq17464	Cannot Update Internal User with External Password ID Store via ERS--ISE
CSCvq19039	ISE fails to save configuration changes for large policy-sets
CSCvq21272	Wrong password being notified after password reset (Only on SMS)
CSCvq24877	Create Failing with ORA-02291 on CEPM.REF_ROLE_MASTER if groupId w/ prepending/trailing spaces
CSCvq27110	Core files on PSN servers causing High Disk Utilization alarms
CSCvq29336	ISE shows "Oops. Something went wrong" if session ID contains "-"
CSCvq33194	Not able to change the language in guest portal with option "Always use"
CSCvq35826	Incorrect audit report while updating Counter Time Limit in Max Session page
CSCvq38085	Posture fails with "Posture failed due to server issues". when Primary PAN is unreachable
CSCvq38610	Certificate trust chain is incomplete for pxGrid on pxGrid alone persona
CSCvq39759	ISE PAN failover inactive days = elapsed days causing incorrect purging of EP's.
CSCvq42847	ISE: "Posture failed due to server issues" error during System scan on MAC OSX
CSCvq45008	ISE doesn't store self-registered EndPoints in configured custom group

Caveat ID Number	Description
CSCvq46232	ISE 2.6 ACI integration Trustesec ACI report doesn't have sent ip-sgt mappings to ACI
CSCvq50088	Export function in Network device groups fails when using RBAC
CSCvq51955	Network Conditions do not work with shorten IPv6
CSCvq52317	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvq52340	'Deleting All' Network Access Users doesn't appear on audit report
CSCvq52402	Cisco Identity Services Engine Information Disclosure Vulnerability
CSCvq54061	System Summary is not available for MNT nodes
CSCvq54153	Cisco Identity Services Engine Policy Set Name Cross Site Scripting Vulnerability
CSCvq54533	Using ECDSA signed certificates with the admin or pxgrid usage breaks pxgrid
CSCvq56241	ISE user import does not fail when username contains invalid characters
CSCvq56281	ISE Guest portal fails to parse http request with two questions marks
CSCvq58785	Static group information is lost from EP in some scenarios
CSCvq62367	PSN generates scheduled reports if no connectivity to MNT
CSCvq63279	Implementation of patch popup
CSCvq65220	ISE 2.6 : Fix for CSCvi89085 breaks detectMACAuthenticationOnPAP flow
CSCvq66846	Move to Mapping Group drop down menu limits SGT Mapping groups to 25
CSCvq69142	PassiveID Agent: No Syslog message is sent to MnT when the agent monitoring DC goes down
CSCvq69228	pxGrid controller contacting terracotta.org
CSCvq71264	Static group assignment losing from guest flow
CSCvq71844	"Cache not properly initialized" message in every Profiler Policy and cannot update Profiler Feed
CSCvq72760	When updating password for administrative user it is possible to bypass entering current password
CSCvq73316	ISE 2.4p9 Grace period is not working with PRA with VPN use case
CSCvq74649	ISE sponsor portal - sorting by creation date doesn't work
CSCvq74995	ISE 2.4 Possible XSS input in Certificate Attributes message when "/" sign is in the name

Caveat ID Number	Description
CSCvq77051	Network devices added via restful API fails authentication with a 'Network Device not located' error
CSCvq78489	ACS to ISE migtool changes the intended results of auth policy
CSCvq79598	IPv6 RADIUS attributes cannot be mapped to any External attribute
CSCvq80211	IP SGT static mapping export fails for entries with no mapping data
CSCvq81381	Internal user using token password will be disabled due to password expired
CSCvq83678	ise.messaging.log not visible on support bundle or gui
CSCvq83700	Remove Unnecessary JQUERY-UI Files from ISE
CSCvq85414	Login page AUP as link does not work with iOS CNA browser
CSCvq86848	Move devices to another group button should be disabled when access has been restricted to NDG
CSCvq97680	ISE 2.6 Patch 2: EAP-TLS auth not matching endpoint groups
CSCvr13444	REST API: Create Network Device with special character ("\") in password field is interpreted as utf
CSCvr27905	ISE fails to parse NMAP Scan information
CSCvr39672	ISE 2.7 BETA: My Devices portal fails to load due to invalid character in Endpoint Description
CSCvr41265	ISE 3695 appliance is having issue with Oracle parameters configured for super MNT
CSCvr43077	Day0: iPad OS 13.1 BYOD flow got failed
CSCvr64000	Hostname change causes ISE Messaging issues - MNT Failover and Queue Link Error-basic_cancel

Open Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 3

Caveat ID Number	Description
CSCvs04092	SGT Notification is missing on PxGrid V2 Client

New Features in Cisco ISE Release 2.6.0.156 - Cumulative Patch 2

Syslog over ISE Messaging Service

The UDP syslogs (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.

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.

Caveat ID Number	Description
CSCuw55841	Custom admin unable to create other restricted admin users
CSCvb56579	SXP Devices page - can't show all the name after 14 chars
CSCvc77960	Friendly info message has to be displayed instead of blank page for unauthorized access
CSCvg03526	Patch installation might generate alarm Application patch installation failed
CSCvh22907	Sponsor Portal Page takes more than 10 seconds to load
CSCvh64185	Session notification can emit bad values in ADNormalizedUsername, ADUserResolvedIdentities fields
CSCvi51291	ISE CoA doesn't work 2 days after initial auth
CSCvk76680	ISE-PIC Self signed certificate delete operation fails due to Secure Syslog Server reference error
CSCvm00481	CA Service still running on command line after Disabling internal certificate authority in Web UI
CSCvn15748	ISE guest flow max session limit does not send CoA Disconnect with third party NAD
CSCvn44171	Network access user with external password cannot be used as ISE admin

Caveat ID Number	Description
CSCvn51282	ISE replaces "ip:" to it's hostname in "ip:inacl" Cisco AV-Pair
CSCvn60787	Emails are not sent for alarm specific email configuration
CSCvn73740	EAP-TLS authentications with Endpoint profile set to not unknown fails in second authorization.
CSCvn79569	App status for ISE is in initialization state
CSCvn92246	ISE: admin users unable to delete or modify groups if a tacacs user is saved without any group
CSCvn92528	ISE 2.4 : Misconfigured supplicant query is one of the reasons for high CPU on both MNT nodes
CSCvo14624	Latency observed with high TPS rates, when ISE messaging service is turned ON
CSCvo17704	ISE 2.4 - CLI password will not accept 3 $
CSCvo28092	ISE Custom Endpoint Attributes - Will not save or delete
CSCvo45582	Internal Administrator Summary report not allowing to select specific columns
CSCvo45768	Adding config to support PrA in PSN failover case
CSCvo50638	TCNAC adapter cannot be configured post upgrade from 2.2 to 2.6
CSCvo59928	ISE 2.6 ANC policy is applied with error "microservice_unavailable" on SMC
CSCvo77219	Sponsor guest portal rate limit time not honored
CSCvo78051	Allowed Protocols - Error creating an inline Allowed Protocol in Policy sets page
CSCvp07591	EAP-GTC Machine Authentication Failure Password Mismatch due to failing the UTF-8 Validation Checks
CSCvp12131	ISE 2.4 Patch 6 reload breaks backups
CSCvp13378	PassiveID flow should send User's SamAccountName and ExplicitUPN
CSCvp14725	ADNormalizedUserName Field Missing From Half of sessions
CSCvp16734	Plus Licenses Consumed without Plus Features
CSCvp18692	AD_User_Fetch information's are not in UI as well as Redis
CSCvp28382	Unable to delete multiple admin groups with multi select
CSCvp29197	ISE 2.4p3 Radius livelogs not showing due to invalid NAD ip address
CSCvp29413	Modifying Radius attributes to send in the request to External RADIUS Server is not working on ISE
CSCvp29572	Enable Pxgrid Profiling Probe Saves but will not enable

Caveat ID Number	Description
CSCvp30958	ISE dropping requests due to descriptor allocation exhaustion under external server latency scenario
CSCvp33593	ISE fails to match authz policy with endpoint ID group "unknown"
CSCvp33862	Custom Attribute (advanced filter in CV) not able to filter on risk score (integer value)
CSCvp37101	The AD connectivity issue occurred and the corefile was generated the same day
CSCvp37238	TACACS/AAA live log report not showing configuration change made from ACI
CSCvp39842	ISE 2.6 SFTP repository access fails
CSCvp43302	Deleting guest type throws error & not able to create new guest type with same name
CSCvp45528	Queue Link Error alarm generated after signing of ISE CA certificate by external Root CA
CSCvp50450	ise-elasticsearch.log files not purged in ISE 2.4 and 2.6
CSCvp52201	ISE 2.4 : Replication: Cluster information table has old FQDN
CSCvp54773	ISE 2.4 p6 400 error on sponsor portal after timeout.
CSCvp54949	BYOD flow is broken in IOS 12.2
CSCvp58945	Import of network device template throws error Failed illegal value for Encryption key
CSCvp59286	Multiple Vulnerabilities in struts2-core
CSCvp60359	Upgraded ISE Node Shows LDAP Identity Store Password in Plain
CSCvp61880	Authorization profile fails to import with no warnings or errors to user
CSCvp65699	CSCvp63136: US399914: 2.6 P2 - View third-party licenses and notices - Link Update
CSCvp65711	ISE 2.4 P8 posture scan running when switch to wired network not configured with dot1x
CSCvp65816	"Cisco Modified" Profiles are overwritten by the Profiler Feed Service
CSCvp68285	AUP guest portal error 400 when return from contact support link (iphone captive portal)
CSCvp72966	Email not received to guest if view/print guest password disabled
CSCvp75101	ISE MNT exception when receiving cisco-av-pair=addrv6=0x7f8c0d588608
CSCvp76617	ISE customer endpoint attribute type string doesn't allow certain numbers
CSCvp76911	ISE if using multiple matrices deploy button is missing
CSCvp77941	License usage for Plus either shows 0 or incorrect value

Caveat ID Number	Description
CSCvp83006	Export from Context Visibility-Endpoints does not contain Custom Attr for most of Endpoints
CSCvp86406	Unable to add network device with combination of any digit followed by () in software version field
CSCvp88242	[400] Bad Request error when refreshing the Mydevice portal
CSCvp93901	pxGrid to publish ADUser.. and ADHost..: SamAccountName and QualifiedName
CSCvq13341	ISE 2.6 patch 1 - AD User Test is returning 0 groups

Open Caveats in Cisco ISE Release 2.6.0.156 - Cumulative Patch 2

Caveat ID Number	Description
CSCvq54061	System Summary is not available for MNT nodes
CSCvq69343	IP-SGT maps are not propagated to ACI in specific scenario
CSCwc83059	Post full upgrade VCS information is missing

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.

Caveat ID Number	Description
CSCvg70813	ISE dmp files are not deleted from /opt/oracle/base/admin/cpm10/dpdump for failed backup attempts
CSCvh19430	ISE 2.x : Guest account activation time discrepancy for imported accounts
CSCvi80094	ERS API that requires CSRF token returns HTTP 404 instead of 403
CSCvj05563	Cannot delete security groups having virtual network mapping
CSCvj31598	Import two CA certs with same subject name
CSCvj83747	ISE Secure Access Wizard Easy Wireless null AD groups for BYOD, Secure Access, Sponsored guest flow
CSCvm01627	ISE 2.4 ERS API - PUT and GET Internal User "User Custom Attributes"
CSCvm05840	NAD CSV imports should allow all supported characters
CSCvm90478	"No Data Available" when attempting to add endpoints to Identity Group with RBAC User

Caveat ID Number	Description
CSCvn40822	Guest creation fails ISE 2.3 after patch 5
CSCvn55640	Manage ACC calling infinite time when sponsoruser configured with permissions ALL&GROUP sponsor grps
CSCvn58964	ISE 2.4 slow database response with 500 authorization policies
CSCvn76567	ISE 2.4 - IP-SGT bindings disappear from SXP for user session
CSCvn85484	Removing SCEP RA Profile causes the associated CA chain to be silently removed from Trusted Store
CSCvn92778	Removal of unused logical profile may cause a wrong authorization result
CSCvn98932	Non-existed DACL is not verified by the ISE
CSCvo05269	[ISE 2.4]Unable to use created profiling policy in authorization condition
CSCvo09945	Backups from SFTP repository may show incorrect year in Modified time
CSCvo11090	Able to delete ACI IEPG in ISE.
CSCvo13269	ISE does not allow to add an SGT
CSCvo15770	address shows as HTML code in context visibility
CSCvo18247	ISE: failed to skip duplicate framed-pool attribute during migration
CSCvo19076	ISE endpoint purge ACTIVEDIRECTORY dictionary is not loading
CSCvo24593	pagination is not working in "All SXP mappings" page in ISE.
CSCvo41052	ISE deleting the newly created IP-SGT mapping
CSCvo43289	ISE truncates the SGT name after a "-" character and assigning a version id
CSCvo61900	System Scan throws internal error for MAC built-in FW remediation using ISE 2.4 Patch 7
CSCvo74441	RabbitMQ docker container is not coming up if port 15672 was already in use
CSCvo78171	ISE 2.4 Patch 6 installation breaks FQDN of Sponsor and MyDevices Portal
CSCvo84948	Failed to migrate dACLs from ACS 5.8 to ISE 2.6
CSCvo90393	CoA failure in Radius+PassiveID flow
CSCvp07364	After upgrading from ISE 2.0.1 Patch 4 to 2.4 Patch 6, CoA is not issued from ISE
CSCvp23869	ISE TLS 1.0 and 1.1 security settings are not applied for PxGrid, causing WSA to fail integration
CSCvp48710	Unable to add AD group if it contains "/." or "/.." in the AD group name

Caveat ID Number	Description
CSCvo31313	Change password for few of the internal users not working after upgrade to 2.6
CSCvo32279	APIC logs not seeing in sxp.log when SXP logging set to 'DEBUG'.
CSCvo35144	Delay in clearing of SXP mappings in ISE
CSCvo36769	EAP-TTLS settings page is not saved in ISE 2.6
CSCvo36837	Admin group cannot get access to "Users" at "Device Administration" tab after install patch 5
CSCvo42165	Default python change password script returns CRUD operation exception
CSCvo45606	ISE:WMI-Passed values may compromise the security of ISE. Please remove malicious scripting terms
CSCvo48352	CSV file of RADIUS authentications report may have duplicate records
CSCvo48975	ISE downloads unneeded RA certificate for BYOD
CSCvo61888	Device Administration Current Active Sessions report not available from 2.4 Patch 6
CSCvo74766	ISE DACL syntax checking validation failing on wildcard notation
CSCvo75129	Runtime prepends "\" to ";" in dhcp-class-identifier in syslog message sent to profiler
CSCvo75376	pxGrid node name limit too short for FMC
CSCvo80291	pxGrid startup order causing profiler code to fail init
CSCvo80516	ISE 2.6 LiveLogs not seen and false Health Status is Unavailable alarm
CSCvo82021	ISE : Memory usage discrepancy in GUI and show tech
CSCvo98554	After Importing ISE PB to ISE , Login page are not loaded
CSCvn35142	ISE 2.3 : Posture report for endpoint by condition not working as expected
CSCvo13626	ISE : Improve Posture Assessment by Condition Report export rate for higher records (millions)
CSCvp17444	Admin Access Blank page when using valid RSA/RADIUS Token credentials but is not in ISE Admin DB
CSCvp40082	ISE 2.3/2.4 upgrade to the latest patch may break dynamic redirection for 3rd party NADs
CSCvo08406	[ENH] Change field Active Directory in External DataSource condition to mention Join Point
CSCvo19377	Successful Authentication Entries not shown in the RADIUS Report due to exceeding the CSV limit
CSCvo33474	Fix "Server not reachable" autologout

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.