Release Notes for Cisco Identity Services Engine, Release 2.7

First Published: 2019-11-18

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, Private 5G 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.

Note Cisco ISE cannot be installed on OpenStack.

Supported Hardware

Cisco ISE, Release 2.7, can be installed on the following platforms:

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 Patch 6 and above versions support Cisco SNS 3700 series appliances.
- 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 QEMU 1.5.3-160

Note Cisco ISE cannot be installed on OpenStack.

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 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 2.7?

Auto-Logon of Self-Registered Guest after Sponsor Approval

You can now enable automatic logon for a self-registered guest after sponsor approval.

Business Outcome: The guest user is automatically logged in when the sponsor approves the guest access request. This simplifies the process and improves customer experience.

Cisco Support Diagnostics Connector

The Cisco Support Diagnostics Connector helps Cisco Technical Assistance Center (TAC) and Cisco support engineers to obtain deployment information from the primary administration node.

Business Outcome: TAC can now get support information of any particular node in a deployment through the connector. This data enables quicker and better troubleshooting.

CLI Show Logging Enhancement

When you run the show logging command in the Command Line Interface (CLI), the content is displayed in the Unix less environment. You can see the supported less commands by typing “H”.

Business Outcome: Less is more useful for viewing the content of large files. This saves time when examining log files.

EAP TEAP Support

Cisco ISE 2.7 supports the Tunnel Extensible Authentication Protocol (TEAP). The type-length-value (TLV) objects are used within the tunnel to transport authentication-related data between the EAP peer and the EAP server. You can use EAP-MS-CHAPv2 or EAP-TLS as the inner method. EAP chaining is supported for TEAP. EAP chaining allows Cisco ISE to run both the inner methods for user and machine authentication inside the same TEAP tunnel. This enables Cisco ISE to correlate the authentication results and apply the appropriate authorization policy, using the EAPChainingResult attribute.

Business Outcome: TEAP is a tunnel-based EAP method that enables secure communication between a peer and a server by using the Transport Layer Security (TLS) protocol to establish a tunnel and encrypt further communications.

Endpoint Ownership Enhancement

The Endpoint Ownership information is now stored across all the Policy Service nodes (PSNs) with the help of the Light Session Directory (LSD).

Business Outcome: This avoids endpoint ownership flapping.

Feed Service Update

If you have customized your profiler conditions and do not want the profiler feed to replace those conditions, you can manually download OUI updates without downloading the policy updates.

Business Outcome: Improved profiler accuracy with less overhead.

Grace Access

You can grant 5 to 30 minutes of internet access to self-registered guests who are waiting for sponsor approval to your corporate network.

Business Outcome: The guest users can access the internet while waiting for approval.

Guest Password Recovery

You can now enable the Reset Password option in the Guest portal for self-registered guests. Self-registered guests with valid guest account can use this option when they forget their password. When you click this option, the self-registration page is launched. You can enter your phone number or email address (whichever you are registered with) and enter a new password.

Business Outcome: Improves the customer experience and reduces calls to Customer Support team.

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.

Phone Number as the Guest User Identifier

In addition to email address or username, guest users can now use their phone numbers as their user ID for guest access.

Business Outcome: Guest users can now use their mobile numbers as their user ID. This makes it easier for them to remember their user ID.

Profiler Forwarder Persistence Queue

The Profiler Forwarder Persistence Queue stores incoming events before they are sent to the profiler module for further processing.

Business Outcome: This reduces the loss of events due to a sudden burst of events. This queue uses the ISE Messaging Service, and is enabled by default. It requires port 8671 to be open between all Cisco ISE nodes.

Role Based Access Policy

In the Cisco ISE admin portal, the Policy menu option under **Administration > Admin Access > Authorization** has been renamed to **RBAC Policy**. The **RBAC Policy** window is used to add and configure policies for administrator groups.

Secure SMTP

Guest email notifications can now be sent through a secure SMTP server.

Business Outcome: Improved security for Guest emails in your network.

Secure Unlock Client

The Secure Unlock Client mechanism is used to provide root shell access on Cisco ISE CLI for a certain period of time.

Business Outcome: The Secure Unlock client feature has been implemented using the Consent Token tool, which securely grants privileged access for Cisco products in a trusted manner.

TrustSec Enhancements

The HTTPS REST API replaces the existing RADUIS protocol to provide all the required TrustSec information to the network devices.

Business Outcome: It enhances the efficiency and ability to download large configurations in a short period of time as compared to the existing RADIUS protocol.

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 upgarding 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 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".

pxGrid Certificate Issue

If you are using the "Netscape Cert Type" for the pxGrid certificate, Cisco ISE may reject that certificate after applying patch 2. Older versions of that certificate specified SSL Server, which now fails, since a client certificate is required. Either use a different certificate, or add "SSL Client" to the existing certificate.

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.

Radius EAP Authentication Performance when Using Default Self-Signed Certificate

In Cisco ISE 2.7, the default self-signed certificate key size is increased to 4096 for enhanced security. Radius EAP authentication performance might be affected, if the default self-signed certificate is used for EAP authentication.

Few TLS Ciphers Cannot be Disabled

The following ciphers cannot be disabled in Cisco ISE:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

The Cisco ISE scenarios that could use these ciphers include:

- Cisco ISE as an EAP or ERS server
- Cisco ISE downloads Certificate Revocation List from an HTTPS or a secure LDAP server
- Cisco ISE as a secure TCP syslog or LDAP client

The Cisco ISE components that could use these ciphers include: Admin UI, all portals, MDM client, pxGrid, and PassiveID Agent.

Security Group Access Control List

When you try to create a Security Group ACL (SGACL), sometimes the following error message is displayed:

```
Failed to create policy, CFS provision failed.
```

This is because creating and updating egress matrix cell flows are not supported for multiple matrixes in Cisco ISE. The following External RESTful Services (ERS) requests are also not supported in the Multiple Matrix mode:

/config/egressmatrixcell/*

/config/sgt/*

/config/sgacl/*

You should, therefore, uncheck the **Allow Multiple SGACL** check box in the TrustSec Matrix Settings (**Work** > **TrustSec** > **Settings** > **TrustSec Matrix Settings**) window. This enables you to create an SGACL, and no error message is displayed.

Valid User-Agent Header

From Cisco ISE Release 2.7, Cisco ISE requires a valid User-Agent header sent along in a web request to a Cisco ISE end-user facing portal, such as a Cisco ISE sponsor portal, to receive successful or redirects responses.

Response Status Lines

From Cisco ISE Release 2.7, Cisco ISE web services and portals return response status lines containing only the HTTP versions and the status codes, but not the corresponding reason phrases.

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 2.7

You can directly upgrade to Release 2.7 from the following Cisco ISE releases:

- 2.2
- 2.3
- 2.4
- 2.6

If you are on a version earlier than Cisco ISE, Release 2.2, you must first upgrade to one of the releases listed above and then upgrade to Release 2.7.

Note We recommend that you upgrade to the latest patch in the existing version before starting the upgrade.

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.

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.

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 1, telemetry is disabled immediately.

Types of data collected include Product Usage Telemetry and Cisco Support Diagnostics.

Cisco Support Diagnostics

The Cisco Support Diagnostics Connector is a new feature that helps Cisco Technical Assistance Center (TAC) and Cisco support engineers to obtain support information on the deployment through the primary administration node. By default, this feature is disabled. See the Cisco Identity Services Engine Administrator Guide for instructions on how to enable this feature.

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/2.7.0.

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 Catalyst Center

Cisco ISE can integrate with Catalyst Center. For information about configuring Cisco ISE to work with Catalyst Center, see the *Cisco Catalyst Center documentation*.

For information about Cisco ISE compatibility with Catalyst 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 the CLI, see the "Patch Install" section in the *Cisco Identity Services Engine CLI Reference Guide*.

Note Cisco ISE Release 2.7 Patch 4 and later releases support the Smart Software Manager (SSM) On-Prem Connection licensing method. After enabling this feature, if you need to roll back to Release 2.7 Patch 3 or earlier, you must disable this feature before uninstalling the patch.

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).

Note The Open Caveats sections list the open caveats that apply to the current release and might apply to releases earlier than Cisco ISE 2.7. A caveat that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 10

The following table lists the resolved caveats in Release 2.7 cumulative patch 10.

Identifier	Headline
CSCwd30039	Cisco Identity Services Engine Command Injection Vulnerability
CSCwe17954	Cisco Identity Services Engine Information Disclosure Vulnerability
CSCwe92624	Africa/Cairo timezone is not adjusted automatically for Daylight Saving Time
CSCvg66764	Session stitching support with ISE PIC Agent
CSCwe92177	Mexico timezone incorrectly changing to Daylight Saving
CSCwd38137	Cisco Identity Services Engine XML External Entity Injection Vulnerability
CSCwd77062	Cisco Identity Services Engine Device Credential Information Disclosure Vulnerability
CSCwe63320	Cisco ISE Releases 3.0, 3.1, and 3.2 display mismatched information on the "Get All Endpoints" report.
CSCwd93719	Cisco Identity Services Engine XML External Entity Injection Vulnerability

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 9

The following table lists the resolved caveats in Release 2.7 cumulative patch 9.

Caveat ID Number	Description
CSCwc98833	Cross-Site scripting vulnerability
CSCwc31482	NetworkSetupAssistance.exe digital signature certificate expires in BYOD flow using Windows SPW
CSCvz65945	"Invalid Length" TACACS auth failures within Live Logs for non-TACACS traffic
CSCwc98828	Interface feature insufficient access control vulnerability
CSCwe08264	Patch install from 2.7P1 or P2 to 2.7P8 is stuck on timezone file

New Features in Cisco ISE Release 2.7.0.356 - Cumulative Patch 8

Support for Cisco Secure Client

Cisco ISE 2.7 Patch 8 supports both AnyConnect and Cisco Secure Client for Windows, macOS, and Linux operating systems. The following Cisco Secure Client versions are supported for these operating systems:

- Windows: Cisco Secure Client version 5.00529 and later
- macOS: Cisco Secure Client version 5.00556 and later
- Linux: Cisco Secure Client version 5.00556 and later

You can configure both AnyConnect and Cisco Secure Client for your endpoints on these operating systems but only one policy will be considered at run time for an endpoint.

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 8

The following table lists the resolved caveats in Release 2.7 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.

Before installing Patch 8 on Cisco ISE 2.7 Patch 7, uninstall the hotpatch to fix CSCwa47133 from Patch 7.

Identifier	Headline
CSCwc74531	ise hourly cron should cleanup the cached buffers instead of the 95% memory usage
CSCwa80359	CIAM: sqlite 3.7.17
CSCwa80547	CIAM: unixodbc 2.3.0
CSCwb07442	SystemTest : Pxgrid connectivity is not coming up post PAN Failover
CSCwa80679	CIAM: net-snmp 5.7.2
CSCwd35608	ISE is sending old Audit Session ID in reath CoA after previously successful port-bounce CoA
CSCwa96229	ISE allowing user to change admin password without validating current password
CSCvv54351	Device Administration using Radius does not consume base license
CSCwb29140	Threads getting exhaust post moving to latest patches were nss rpm is updated(Only 3.0p5&2.7p7,3.1P1
CSCwa84447	Restoring ISE 2.2 Backup in ISE 2.7 Patch 3 will cause the Health Check start button to disappear.
CSCwa35293	ISE 2.7:Authentication success settings shows success/success url
CSCwb33727	ISE 3.1 : Special character in attributes not supported
CSCwb24002	ISE ERS SDK the authenticationSettings are not disabled via API call
CSCwb55232	Create a nested endpoint group using ERS API
CSCvv87286	Fail to import Internal CA and key from ISE 2.7P2 to 3.0
CSCwc93253	ISE - Network device captcha only prompting when filter matches only 1 Network device
CSCwa55996	new objects doesnt exist in condition studio
CSCwb14106	CIAM: cyrus-sasl 2.1.27
CSCwb19256	Pingnode call causing App server to crash (OOM exception) during CRL validation
CSCvx58736	3.1:Maxscale: Core generated by /opt/CSCOcpm/prrt/diag/bin/diagRunner start

Identifier	Headline
CSCwc12303	PGA memory used by the instance exceeds PGA_AGGREGATE_LIMIT on MNT node
CSCwa97123	NTP Sync Failure Alarms with more than 2 NTP Servers Configured.
CSCwa40040	Session Directory Write failed, SQLException: String Data right truncation on ISE3.0P4
CSCvs96530	Cisco Identity Services Engine Formula Injection Vulnerability
CSCwa80710	CIAM: jszip 2.5.0
CSCwa06912	High Latency observed for Tacacs+ requests with date time condition in authorization policies
CSCwb75954	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability
CSCwc30019	CIAM: openssl 1.0.2n
CSCwb07504	Sorting internal users based on User Identity Groups doesn't work in Identity Mangement->Identities
CSCwa80520	CIAM: libpng 1.6.20
CSCwc69492	ISE 3.1 | Metaspace exhaustion causes crashes on ISE node
CSCwb75959	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCwb61614	guest users (AD or internal) cant delete/add their own devices on specific node
CSCwc72251	pxgrid publishing changed for accounting stop
CSCvy32277	TLSv1.1 enabled on port 8084
CSCvz85074	Fix for CSCvu35802 breaks AD group retrieval with certificate attribute as identity in EAP-Chaining
CSCwb27857	ISE 3.0 P5: Unable to login into GUI of MnT nodes using RSA 2FA in distribusted deployment.
CSCwd03009	RMQForwarder thread to control based on hardware Appliance in platform.properties on 2.7 p7
CSCwb52396	ISE PRA failover
CSCwa95892	ui_time_left variable showing wrong duration
CSCwa76896	Duplicated culomn "Failure Reasons" in RADIUS Authentications Report
CSCwc06638	3.0P6 : system summary not getting updated post Patch RollBack and Patch Install
CSCwa17925	After fixing failed pre-upgrade check, proceed button still not available
CSCwa25731	Last 7 days filter not working in Reports

Identifier	Headline
CSCwd45843	Auth Step latency for policy evaluation due to GC activity
CSCwb26965	ISE 3.1: Getting error while creating network device groups via REST API.
CSCwc57939	ISE detects large VMs as Unsupported
CSCwb86283	ISE Deployment : All nodes thrown OUT_OF_SYNC as a result of incorrect cert expiry check
CSCwa49859	Attribute value dc-opaque causing issues with Live Logs.
CSCwa80484	CIAM: nss 3.44.0
CSCvz99311	Cisco Identity Services Engine Software Resource Exhaustion Vulnerability
CSCwb26227	CIAM: jackson-databind 2.9.8
CSCwb88360	Disable temp mnt persona on upgraded node fails in split upgrade
CSCwb85456	CIAM: openssl upgrade to 1.0.2ze and 1.1.1o
CSCwb91392	Healthcheck and fullupgrade precheck timesout when 3rd party CA cert is used for admin
CSCwa80501	CIAM: perl 5.16.3
CSCwc65711	MAC - CSC 5.0554 web dployment pkgs are failed to upload to ISE->CP-> resources[100MB]
CSCwa18443	Need to handle Posture expiry when 8 octet MAC is present in endpoint on the deployment node
CSCvv10712	Sec_txnlog_master table should be truncated post 2M record count
CSCvz63643	ISE 2.7: EndpointPersister thread getting stopped
CSCvx49736	containerd.io RPM package openssl 1.0.2r CIAM CVE-2021-23841 + others
CSCwb09861	CIAM: glib 2.56.4
CSCvz43123	CIAM: jspdf 2.3.0
CSCwa90930	Need hard Q cap on RMQ
CSCvz24558	Spring Hibernate TPS upgrade (hibernate 5.5.2, Spring 5.3.8)
CSCwa75348	ODBC Behavior Failover Issues
CSCvz94133	Config backup fails due to "EDF_DB_LOG"
CSCwd31405	Latency observed during query of Session.PostureStatus
CSCwb27894	EAP-TEAP with EAP-TLS unable to match condition that has "CERTIFICATE.Issuer - Common Name"

Identifier	Headline
CSCvz91479	Schema upgrade failed while modifying constraints for 3.1->3.2.0.804 upgrade
CSCwb05532	Location of "Location" and "Device Type" exchanging every time clicking Network Devices > Add
CSCwc23593	LSD is causing high CPU
CSCwc93451	Profiler should ignore non-positive RADIUS syslog messages for forwarding from default RADIUS probe
CSCwb03231	application server stuck initializing after installing p5 or p6 due to missing table
CSCwb41741	ISE - Invalid character error in Admin Groups
CSCwb32466	ISE 3.1: Unable to delete endpoint identity group created via REST API when setting no description.
CSCwa59237	Deployment-RegistrationPoller causing performance issues on PAN node with 200+ internal certificates
CSCwc27765	ISE Config Backup Fails due to SYS_EXPORT_SCHEMA_01
CSCwb09045	ISE PSN nodes crashing due to incorrect cryptoLib initialization
CSCwb67934	CIAM: openjdk - multiple versions
CSCwc62413	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCwa27766	Context Visibility broken after restore of backup ISE 3.0 P4
CSCwa77161	PLR returned upon 3.0P5 -> 3.0P3
CSCwb23028	Inaccurate dictionary word evaluation for passwords
CSCwb62192	scheduled backup failure when ISE indexing engine backup failed
CSCwb29498	High Operations DB Usage Alarm percentage need to be configurable.
CSCwc15013	Add serviceability & fix "Could not get a resource since the pool is exhausted" Error on ISE 3.0
CSCwb84779	Changing Parent Identity Group name breaks authorization references
CSCwb03479	hotpatch.log needs to be included in support-bundle
CSCwb40349	ISE 3.X: Invalid Characters in External RADIUS Token shared Secret.
CSCwb01843	DST/TZ update should happen automatically
CSCwd24304	ISE 3.2 ERS POST /ers/config/networkdevicegroup fails - broken attribute othername/type/ndgtype
CSCvu41087	ISE 3.0 RADIUS Drops report in live logs shows ISE admin username in endpoint details

Identifier	Headline
CSCvx94685	CIAM: rpm 4.11.3 CVE-2021-20271
CSCwa80553	CIAM: samba 4.8.3
CSCwa60903	ISE is adding extra 6 hours to nextUpdate date for CRL
CSCwa55866	Tacacs responses are not sent sometimes with single connect enabled
CSCwa80689	CIAM: c3p0 0.9.1.1
CSCwb02346	Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability
CSCwb93156	TrustCertQuickView giving the same info for all trusted certificates
CSCwb40131	Getting 400 Bad Request while enabling the Internal User with external password type using Rest API.
CSCwb32492	Application server restart on all nodes after changing the Primary PAN Admin certificate
CSCvz88327	CA initializing on PAN, Root CA regeneration fails with "no message defined" error
CSCvv02086	Add ability to disable TLS 1.0 and 1.1 on ISE PIC node
CSCwa80532	CIAM: jsoup 1.10.3
CSCvo79976	Security: Remove encoded credentials logging in RESTClientAlertHelper.java to be printed on console

Open Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 8

Caveat ID	Description
CSCwe08264	Patch install from ISE 2.7 Patch 2 to 2.7 Patch 8 is stuck at timezone file upgrade step

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 7

The following table lists the resolved caveats in Release 2.7 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.

Identifier	Headline
CSCvv96532	DOC: unknown maximum time difference for thisUpdate of OCSP response
CSCvz37241	Queue Link Error:WARN:{socket_closed_unexpectedly;'connection.start'}
CSCvz91603	Unable to fetch the attributes from ODBC after upgrading ISE to 3.0 patch 3

Identifier	Headline
CSCwa17718	Session service unavailable for PxGrid Session Directory with dedicated MNT
CSCwa07580	Could not create Identity User if username includes $
CSCvz18044	VN's are not replicating from Author to Reader
CSCwa23393	ISE 2.7 p 4,5,6 reports error "There is an overlapping IP Address in your device"
CSCvz87476	Unsupported message code 91104 and 91105 Alarms
CSCvz90468	Internal users using External Password Store are getting disabled if we create users using API flow.
CSCvz21417	Upgrade ISE 3.0 and earlier patches with CiscoSSL 1.0.2za
CSCvz84905	DOC: ISE Backup can cause 'High Load average' Alarm
CSCvz56358	ISE 3.0 checks only the first SAN entry
CSCvz46560	ISE using jquery v1.10.2 is vulnerable.
CSCwa20309	Unknown NAD and Misconfigured Network Device Detected Alarms
CSCvy84989	enabling cookies for POST /ers/config/internaluser/ causes Identity Group(s) does not exist error
CSCwa08484	Missing IPv4 mappings if sessions have both IPv4 and IPv6 addresses
CSCvz99405	OpenSSL is not upgraded on 2.7p4 or 2.7p5
CSCvy96761	session cache needs to be update dduring EAP chaining flow to handle relavent identities
CSCvz57551	Polling Interval and Time Interval For Compliance Device ReAuth Query
CSCvz86020	live log/session not showing latest data due to "too many files open" error
CSCvs95495	Reauth issue - Aruba - 3rd party device
CSCvz63405	ISE client pxgrid certificate is not delivered to DNAC
CSCvz00706	"interesting groups" are returned as a SINGLE STRING with an embedded new line
CSCwa20354	Operational Data purging->Database utilization Node info does not show intermittently.
CSCwa05404	Stale Sessions observed for Tacacs Could not find selected service error
CSCwa47566	ISE Conditions Studio - Identity Groups Drop-down limited to 1000
CSCvz80829	Version pre-check fails for 3.2 full upgrade.
CSCwa41166	RegEx expressions in TACACS Command Sets malformed
CSCwa78479	Cisco Identity Services Engine Assessment of CVE-2021-4034 Polkit

Identifier	Headline
CSCvz95326	unable to add more than one ACI IP address/hostname when trying to enable ACI integration in ISE
CSCwa19573	Catalina.out file is huge because of SSL audit events
CSCwa13877	ISE Smart Licensing Authorization Renewal Failure: Details=Invalid response from licensing cloud
CSCwa23207	Multiple runtime crashes seen due to memory allocation inconsistency
CSCvz71284	SNMPv3 COA request is not issued by ISE 2.7
CSCvz93230	Guest portal does not load if hosted on a different interface from Gig0
CSCwa32312	RCM and MDM flows getting failed because of session cache not populated
CSCvz88188	TACACS authorization policy querying for username fails because username from session cache is null
CSCwa56771	ISE 3.0p2- Monitor All setting displays incorrectly with multiple matrices and different views
CSCvz67479	Local Log Settings tooltip on all fields shows irrelevant and unuseful 'Trust Certificates'
CSCwa26210	nextPage field is missing from the json response of API 'GET /ers/config/radiusserversequence'
CSCwa15191	EP stuck in posture unknown Not able to find session in LSD by MAC
CSCvz56171	ISE Doc: ISE SDK documentation for SXP bindings contains unavailable keys
CSCwa11659	CIAM: libx11 1.6.8
CSCvy40956	[DOC] Please help with making CoA API documentation more explicit
CSCvz60870	High Active Directory latency during high TPS causes HOL Blocking on ADRT
CSCwa47133	ISE Evaluation log4j CVE-2021-44228
CSCvz50255	CIAM: bind 9.11.20
CSCwa47221	AD security groups cannot have their OU end with dot character on Client Provisioning Policy
CSCvy82023	Incorrect Posture Compound Condition Hotfixes
CSCvz79665	Microsoft Intune Graph Url change from graph.windows.net/tenant to graph.microsoft.com
CSCwa52667	not able to save the Authorization profile when include curly brackets in the profile name
CSCwa20152	CoA was not initiated on ISE for switches for which matrix wasnâ€™t changed, hence Policy sync failed

Identifier	Headline
CSCvz83753	Empty User Custom Attribute included in AuthZ Advanced Attributes Settings results in incorrect AVP
CSCvz65576	Fullupgrade wont work with patch when CLI repo or disk repo is used
CSCwa11633	ISE 3.0 : APIC Integration : Failed to create secGroup
CSCvz85117	ISE Health Check I/O bandwidth performance check false Alarm
CSCwa60873	Optimize bouncy-castle class to improve performance on PAN
CSCvy33615	ISE 3.1 BH Default profiling policies' description has space characters' hex code instead of space
CSCwa43187	ISE Queue Link Error: Message=From Node1 To Node2; Cause=Timeout in NAT'ed deployment
CSCwa16401	Get-By-Id server sequence, returns empty server list after first change made on the sequence via GUI
CSCvz00034	Changing log level of log "this update field is earlier than currunet time more than week"
CSCvy89317	ISE: DST Root CA X3 Certificate Authority - Expires by 30 Sep 2021 (within 90 days)
CSCvw65181	CIAM found poi vulnerable
CSCvy05713	Smart licensing(Satellite/PLR) should be disabled when upgrading from 2.7 P4, 2.6 P10 to ISE 3.0
CSCwa59621	Inconsistent sorting on ERS API(s) for identity group
CSCvz74457	ERS API does't allow for use of dot character in "Network Device Group" name or create / update
CSCvo39514	MnT log processor is not running because collector log permission.
CSCvz55258	Cisco:cisco-av-pair AuthZ conditions stopped working
CSCwa46758	Deleted Root Network Device groups are still referenced in the Network Devices exported CSV Report
CSCwa52110	SNMP config set on the N/w device, a delay of 20seconds is introduced while processing SNMP record
CSCvz71872	CIAM: nss - multiple versions
CSCvz83204	ISE unable to fetch the url attribute value from improper index during posture flow

Open Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 7

Caveat ID Number	Description
CSCvy86859	Mac OS Beta Monterey (MacOS 12 beta 2) failing NSP MacOsXSPWizard 3.1.0.2
CSCwb07442	Pxgrid connectivity is not coming up post PAN Failover
CSCwb29140	Threads getting exhuast post moving to latest patches were nss rpm is updated(Only 3.0p5&2.7p7,3.1P1

The following hot patch files are available on CCO for CSCwb29140.

- To install the hot patch:

  ise-apply-CSCwb29140_2.7.0.356_patch7-SPA.tar.gz

- To rollback the hot patch:

  ise-rollback-CSCwb29140_2.7.0.356_patch7-SPA.tar.gz

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 6

The following table lists the resolved caveats in Release 2.7 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
CSCvn27270	ISE: Unable to create Network Device Group with Name, Location, or Device Type
CSCvw90586	Unable to change Network Device Group Name and Description at the same time
CSCvx23375	ISE authorization profiles option get truncated during editing/saving (Chrome only)
CSCvx48255	CIAM: screen 4.1.0 CVE-2021-26937
CSCvx58520	With PLR, Profiler Online Updates error: Failed to get License file data: null
CSCvy14905	CTS-SXP-CONN: ph_tcp_close from device to ISE SXP connection - Hawkeye
CSCvy45345	EAP-chaining authorization failure due to machine authentication, flag is incorrectly set to true
CSCvy51210	ISE 2.7 Should display an error when attempting to delete IP default label of NAD on GUI.
CSCvy53842	Certificate Validation Syslog Message Sent During Specific Certificate Audits--ISE
CSCvy71229	CIAM: libx11 1.6.8
CSCvy71261	CIAM: nettle 3.4.1

Caveat ID Number	Description
CSCvy71313	CIAM: cpio 2.12
CSCvy75191	Cisco Identity Services Engine XML External Entity Injection Vulnerability
CSCvy76328	ipv6 changes the Subnet to /128 when using the duplicate option from Network device tab
CSCvy92040	ISE restore popup menu displays wrong text
CSCvy94818	EP's incorreclty profiled as "cisco-router" due to nmap performing aggressive guesses
CSCvz00258	Session Cache not cleared for Tacacs Authorization failures results in high heap usage and auth latency
CSCvz13783	The licensing page was having 0 count postpatch 13 upgrade
CSCvz18627	PEAP session timeout value restricted to max 604800
CSCvz22331	Authentication is not blocked in the policy set with Time and Date condition for a specific minute in the day.
CSCvz33839	menu access customization is not working
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} not working; CRUD exception
CSCvz36192	GET for dacls using /ers/config/downloadableacl does not add the nextPage or previousPage of exist.
CSCvz43183	Sponsor Permissions are not passed to Guest REST API for "By Name" calls.
CSCvz44655	ISE manage account selection issue
CSCvz51536	ISE Wildcard certificate failing with internal error
CSCvz70947	The Subnet/IP Add Pool Name in SG under ATZ profile is disappearing in Chrome, only specific to 2.7P5
CSCvz71459	Microsoft_intune MDM ISE change in polling interval not taking effect in cache
CSCvz99405	Open SSL is not upgraded on 2.7p4 or 2.7p5
CSCwa00729	All NADs got deleted due to one particular NAD deletion.

Open Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 6

There are no open caveats in Cisco ISE Release 2.7 Patch 6.

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 5

The following table lists the resolved caveats in Release 2.7 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.

Note If Cisco ISE patch 5 is installed and rolled back only on the PAN and not on the node that is registered to PAN, the application server on the node will be stuck in the initializing state. You must install and roll back Cisco ISE patch 5 on the node before registering the node to the PAN to avoid this issue.

Caveat ID Number	Description
CSCvi53134	Account used for Cisco ISE AD Join operation may become locked after enabling Passive-ID service.
CSCvi59005	Unable to see complete list of AD groups when using scrollbar.
CSCvn25548	Displays incorrect error message saying account was disabled due to inactivity.
CSCvo56767	Error while trying to change Cisco ISE-PIC GUI admin user settings.
CSCvr03959	When "Person Being Visited" option is selected from "Email Approval Request To" drop-down list, it is not made mandatory.
CSCvr76539	Changes to Network Device Groups are not reflected in Change Audit logs.
CSCvs66551	Multiple vulnerabilities in Apache log4j.
CSCvt52104	Multiple vulnerabilities in Jetty.
CSCvt94587	"Plus License is out of compliance" message disabled while regenerating the Cisco ISE Root CA.
CSCvu04874	Suspected memory leak in io.netty.buffer.PoolChunk
CSCvu56753	CIAM: Multiple vulnerabilities in openjdk.
CSCvu72744	Replace "blacklist" with "blocked list" across all authentication and authorization rules and profiles.
CSCvu84184	Certificate chain is not sent on the guest portal.
CSCvv04957	GRUB2 Arbitrary Code Execution Vulnerability.
CSCvv07101	PKCS11 key store creates memory leak when endpoints are in Cisco ISE.
CSCvv55602	Policy engine enhancements.
CSCvv68293	Cisco ISE does not consume Plus license when using local or global exceptions.
CSCvv77928	Bulk certificate generation fails with "An unexpected error occurred" message after primary PAN failure.
CSCvw09827	High CPU on PSN—extension of CSCvt34876.

Caveat ID Number	Description
CSCvw69977	All SXP Mapping table contains terminated sessions.
CSCvw78019	NTP out of synchronization after upgrading to Cisco ISE Release 2.7.
CSCvw89326	For PKI-based SFTP, exporting GUI key for MnT node is only possible when it is promoted to PAN.
CSCvx01272	Generate Bulk Certificates does not include the Cisco ISE self-signed certificate.
CSCvx22229	Cisco ISE "ipv6 address autoconfig" gets removed when changing IP address of bond interface.
CSCvx47691	Session Directory topic does not update user SGT attribute after a dynamic authorization.
CSCvx53205	NIC bonding prevents MAR cache replication.
CSCvx60818	ERS self-registration portal update does not delete PSN fields as expected.
CSCvx69701	Deployment went out of synchronization due to unavailabiltiy of database connections.
CSCvx78643	Emails sent for all system alarms even when there is no email address configured.
CSCvx85675	Cisco ISE cannot handle deletion or addition of SXP-IP mappings propagation due to race condition.
CSCvx86921	RADIUS Token Identity Source prompt vs. Internal User prompt for TACACS authentication.
CSCvx96190	Top Authorization report does not show filter in scheduled reports.
CSCvx99151	Cisco ISE internal ERS user attempting to authenticate via external ID store causes REST delays.
CSCvx99675	Cisco ISE secondary PAN sends packet to other node with link local address when backup interface is configured.
CSCvy04443	MNT REST API for ReAuth fails when used in a distributed deployment.
CSCvy04665	TACACS report advance filters not working when matching full numeric ID entries.
CSCvy05954	All SXP Mappings window does not display IPv6 mappings learned via Session.
CSCvy06417	Cisco ISE persistant XSS Admin Group.
CSCvy06719	Manual Active Session report is empty.
CSCvy14342	High CPU seen on PSNs in Cisco ISE Release 2.6 Patch 3 and later releases due to PIP query evaluation.
CSCvy15058	Unable to update domains to be blocked or allowed via APIs.
CSCvy17893	Cisco ISE REST API returns duplicate values for IP-SGT mappings.

Caveat ID Number	Description
CSCvy18560	RADIUS Accounting Details report does not display Accounting details.
CSCvy20277	Special characters allowed previously in Description field for few objects no longer can be used.
CSCvy23354	Description field is not readable when Mozilla Firefox 88 is in use.
CSCvy24303	Usage Over Time chart for licenses shows wrong information.
CSCvy24370	Cisco ISE does not allow more than 6 attributes to be modified in the RADIUS sequence attributes.
CSCvy25533	"/opt/CSCOcpm/config/cpmenv.sh:line 396:<ipv6>:command not found" error seen during CLI backup.
CSCvy25550	Cisco ISE does not accept the name of custom attribute for Framed-IPv6-Address in the authorization profile.
CSCvy30119	LDAP groups disappear from Sponsor group when making other changes to options.
CSCvy32461	Sponsor user cannot edit data when phone or email fields are filled.
CSCvy34977	Application Server stuck on initializing state due to certificate template curve type P-192.
CSCvy36868	Cisco ISE Release 2.3 and later releases do not support "cariage return" <cr> character in command-set.
CSCvy36968	Unable to retrieve the license details causing features to be disabled.
CSCvy38459	Cisco ISE Release 2.7 Patch 3 GUI doesn't show all device admin authorization policies.
CSCvy38896	AAA requests without Framed-IP value causes exception in SXP process.
CSCvy40845	Updating a custom attribute through ERS request updates another attribute as well.
CSCvy41066	TACACS custom AV pair as condition in policies is not working.
CSCvy42885	Cisco ISE Application server crashes or restarts due to cancellation of configuration backup.
CSCvy43246	User unable to create a guest SSID during the Portal Creation step.
CSCvy45015	Cisco ISE Guest Self-Registration error for duplicate user when the Use Phone Number As Username option is enabled.
CSCvy46504	Intermittent error on Cisco DNA Center while trying to deploy policy from Cisco DNA Center.
CSCvy48766	Cisco ISE installation fails with database priming failed error when all-numbers subdomain is used.
CSCvy51073	Cisco ISE authorization profile ERS update ignores accessType attribute changes.

Caveat ID Number	Description
CSCvy58771	While editing a NAD, wrong device profile is mapped.
CSCvy60865	When an endpoint is moved from a switch or port where it is authenticated and the Identity Group that is referenced by an authorization policy is modified, Cisco ISE fails to send out a CoA.
CSCvy61564	Cisco ISE Release 2.7 Patch 3 ERS call does not accept RADIUS shared secret with 3 characters.
CSCvy62875	Cisco ISE Release 2.7 Patch 2: [400] Bad Request with SAML SSO OKTA on Apple devices.
CSCvy63778	REST API for CoA works with any server IP.
CSCvy65786	Configuring WMI with an AD account password containing % character results in an error.
CSCvy68023	Cisco ISE-PIC 2.7 and earlier must use TLS 1.2 with Domain Controller.
CSCvy71690	Customer fields in guest portal contains &, -, $, and #.
CSCvy72028	Cisco ISE 2.7 Patch 4: pxGrid Services > All Clients window ends with java.lang.NullPointerException.
CSCvy74456	External Cisco DNA Center authentication via Cisco ISE fails with "Invalid login credentials" error.
CSCvy74919	Cisco ISE internal users are not disabled after hitting inactivity timer.
CSCvy76262	Cisco ISE DACL syntax validator does not comply with ASA's code requirements.
CSCvy76617	Cisco ISE: Need the Select All check box device with or without filter in the NAD window.
CSCvy81435	Cisco ISE Guest SAML authentication fails with "Access rights validated" HTML window.
CSCvy82114	Wrong display of the Unicode of Chinese in First/Last name under Network Access Users.
CSCvy90691	Duplicated RADIUS Vendor ID can cause PSN to crash.
CSCvy94427	Posture lease breaks for EAP chaining from Cisco ISE Release 2.7.
CSCvy94511	TACACS report shows duplicate entries due to EPOCH time being null.
CSCvy94553	The TACACS authentication report shows duplicate entries.
CSCvy96144	UDI information is missing in the Cisco ISE GUI.
CSCvy99582	Upgrade from Cisco ISE Releast 2.4 Patch 13 to Cisco ISE Release 2.7 fails when an external RADIUS server is configured.
CSCvz01485	Cisco ISE Release 2.7 Patch 4 unable to upload .json file for Umbrella security profile.

Caveat ID Number	Description
CSCvz05704	Platform check fails for Cisco ISE that has a disk size greater than 1 TB.
CSCvz07823	Cisco ISE Release 2.7 failed to add endpoint to group.
CSCvy11865	Cisco Identity Services Engine cross-site scripting vulnerability.
CSCvy62395	Upgrade logs should be recorded in the logs directory and included in the support bundle.
CSCvx85051	Security Group's VLAN field is populated by full dictionary attribute value instead of suffix.
CSCvw90778	T+ ports (49) are open even if you disable device admin processes in Deployment windows.

Open Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 5

Caveat ID Number	Description
CSCvz70947	The Subnet/IP Address Pool Name added to a Security Group is missing in the Authorization Profiles window in Chrome browser
CSCwa00729	All NADs got deleted due to one particular NAD deletion.

New Features in Cisco ISE Release 2.7.0.356 - Cumulative Patch 4

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.

Note The Full Upgrade method is supported for Cisco ISE 3.1 and above. For more information about the Full Upgrade method, see Cisco Identity Services Engine Upgrade Journey, Release 3.1.

- **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.

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*.

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 4

The following table lists the resolved caveats in Release 2.7 cumulative patch 4.

Patch 4 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
CSCuo73496	ISE RADIUS session-timeout value restricted to max 65535
CSCvh04231	Guest Remember Me RADIUS accounting and access accept not sending guest username
CSCvo04728	MIT Kerberos 5 KDC krbtgt Ticket S4U2Self Request Denial of Service Vulnerability
CSCvq26124	ISC BIND managed-keys Trust Anchor Denial of Service Vulnerability
CSCvq58506	Show running-config fails to complete
CSCvr55906	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow Vulnerability CVSS v3.1 Base: 9.8
CSCvr77653	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow Vulnerability CVE-2019-5436
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
CSCvr80934	Samba Symbolic Link Traversal Vulnerability CVSS v3.1 Base: 5.4
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
CSCvs39800	gllibc LD_PREFER_MAP_32BIT_EXEC Environment Variable ASLR Bypass Vulnerability
CSCvs45350	ISE shows anonymous as a username when user credential is not sent by the supplicant and only machine credential is available

Caveat ID Number	Description
CSCvs52211	Update CiscoSSL to fix CSCvg56800 - Evaluation of ISE vulnerability nginx Oct 2017
CSCvs76914	libxml2 xmlParseBalancedChunkMemoryRecover Memory Leak Vulnerability
CSCvs91984	Systemd button_open Memory Leak Vulnerability
CSCvt11130	Sh version command is not working for non-admin CLI user
CSCvt11664	ISE Feed Server fails via createLicenseSource method "FlexlmListException: Error"
CSCvt30558	Multiple Vulnerabilities in python
CSCvt44403	SSLDUMP() logs printed on Showtech via Audit logs causing showtech file to grow extensively
CSCvt51244	Multiple Vulnerabilities in activemq-all
CSCvt76509	ISE Backup file transfer logs show Success although there is no space in the SFTP Repository
CSCvt85370	Posture Condition failed with "Check vc_visInst_v4_CiscoAnyConnectSecureMobility Client_4_x is not found" error
CSCvt95762	ISE 2.6/2.7 not listing files when using RHEL as SFTP repository
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
CSCvu16067	Changes in IP-TABLES causing TCP delay and TACACS latency
CSCvu18256	Application stop ise shows "Service 'stunnel' -- doesn't exist" on PAN and SAN node
CSCvu22058	ISE with DUO as External Radius Proxy drops access-reject
CSCvu38918	Operations Audit Report contains logs of of actions performed by "backend" account
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
CSCvu59038	Update "master/slave" terms to "primary/subordinate" in "show interface" command.
CSCvu62938	Posture fails when primary PSN/PAN are unreachable
CSCvu63833	Failed Logins to ISE GUI are not seen in Audit Report when AD is selected as the Identity Source
CSCvu68240	Daily purge is not happening and hence data to be purged does not get copied to Repository
CSCvu82889	Netstat command causing carssh shell to crash on ISE

Caveat ID Number	Description
CSCvv09167	TACACS Aggregate table is not purged properly
CSCvv14390	Max Sessions Limit is not working for Users and Groups
CSCvv19065	ISE user cannot see Guest identity in DNAC Assurance page
CSCvv29737	DNA Center Scalable Groups Sync fails with "JDBCException:could not prepare statement" error
CSCvv30161	Live session details report show incorrect Authorization profile and policy for VPN Posture scenario
CSCvv43383	NFS Repository is not working from GUI
CSCvv45340	Saving the running-config leads to loss of startup config
CSCvv61732	Unable to create unique community string for different SNMP servers
CSCvv63548	Memory Leak: PSN rmi GC collection not working properly and causing memory leak in passive id flow
CSCvv67091	Cisco Identity Services Engine Untrusted File Upload Vulnerability
CSCvv74361	ISE 3.0 Health Check License validation false Alarm
CSCvv77007	ISE sending requests to external RADIUS token server for internal Super Admin users
CSCvv79940	ISE generating CSR with hostname-x in SAN gives an error
CSCvv83510	ISE 3.0 Upgrade failing at step RuleResultsSGTUpgradeService
CSCvv85588	Memory Leak : High Allocation in by CAD_ValidateUser during PassiveID stress
CSCvv90612	WebUI restore not working in IE11
CSCvv93442	ISE 2.6p3 adding double slash "//" in file path for SFTP servers
CSCvw02887	Memory leak after adding AD groups for passive-id flow
CSCvw06722	Sponsor is unable to display the list of created guest users when accessing portal with his User ID
CSCvw08602	Not throwing error for IP overlap case
CSCvw10671	GNU.org bash rbash BASH_CMDS Modification Privilege Escalation Vulnerability
CSCvw16237	Scheduled OPS backups not being triggered after PMNT reload
CSCvw17908	Pushing IP to SGT mapping from ISE to switch doesn't work if default route is tagged
CSCvw20060	Agent marks DC as down if agent service comes up before windows network interface
CSCvw22228	pxGrid ANC applyEndpointPolicy does not handle all MAC address formats correctly

Caveat ID Number	Description
CSCvw24268	Cisco Identity Services Engine Untrusted File Upload Vulnerability
CSCvw25285	Passive ID is not working stable with multi-connect syslog clients
CSCvw26415	ISE 3.0 not importing certificates missing CN and SAN into Trusted Certificate Store
CSCvw29490	Internal User custom attributes are not sent in CoA-Push
CSCvw31269	SAML groups do not work if they are applied in the Sponsor Portal Groups
CSCvw33115	ISE MNT Live Session status is not changing to Postured in VPN use case
CSCvw37844	ANC CoA not working as ISE uses hostname for internal calls
CSCvw48396	Cisco ADE-OS Local File Inclusion Vulnerability
CSCvw48403	ISE is not processing gathered SNMPv3 information for endpoint
CSCvw48697	API IP SGT mapping not returning result for [No Devices]
CSCvw49938	No TACACS Command Accounting Report for third party device with a space before TACACS command
CSCvw50381	CoA-disconnect is not issued by ISE for Aruba WLC once grace access expires
CSCvw50829	AD security groups cannot have their OU end with dot character for RBAC policies
CSCvw51801	ISE Live Session Postured session is moving to Started upon receiving an Interim Update
CSCvw53412	Support bundle should collect Hibernate.log
CSCvw53740	GNU Bash SHELLTOPTS and PS4 Environment Variables Local Arbitrary Command Injection Vulnerability
CSCvw58538	GNOME GLib file_copy_fallback Function Improper Permission Vulnerability
CSCvw58824	XStream before version 1.4.15 multiple vulnerabilities
CSCvw59312	Heap buffer overflow in Freetype CVE-2020-15999, CVE-2018-6942
CSCvw59314	Moment Module Date String Regular Expression Denial of Service Vulnerability
CSCvw59920	Multiple Vulnerabilities in c3p0
CSCvw60197	Multiple Vulnerabilities in glibc
CSCvw61589	ISE Policy Evaluation: RADIUS requests dropped after deleting policy sets
CSCvw61786	Restore Processes need to be stopped before dropping schema objects
CSCvw66483	RADIUS server sequence gets corrupted after selected external servers list was changed

Caveat ID Number	Description
CSCvw68480	When using multiple SXP nodes in ISE deployment, total number of mappings is not correctly displayed
CSCvw73529	No option for OnPrem Satellite for Smart licensing and Permanent License Reservation
CSCvw73928	NTP sync failure alarms need to be changed
CSCvw75397	MNT node name set to NULL when IP access enabled
CSCvw75563	HotSpot Guest portal displays Error Loading Page when passcode field contains special characters
CSCvw77219	Dot1x authentication failed due to duplicate manager: add=false
CSCvw78289	Authentication Passed live logs are not seen when using a profile name with more than 50 characters
CSCvw80520	Radius Authentication Details report takes time when ISE Messaging Service is disabled
CSCvw82774	Sorting based on username doesn't work in User Identity Groups
CSCvw82784	TACACS+ Endstation Network Conditions scrollbar not working
CSCvw84127	Configuration Audit detail does not show which Policy Set was modified
CSCvw85860	ISE pxGrid exceptions should have ERROR log level instead of DEBUG
CSCvw87147	Live session is not showing correct active session
CSCvw87173	AD authorization is failing for MAB authenticated endpoints
CSCvw87175	MAB authentication via Active Directory passes with AD object disabled
CSCvw88881	Database clean up hourly cron acquiring DB lock causing deployment registration failure
CSCvw90961	RBAC rules not enforced in 2.7
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
CSCvw94603	Change in Polling interval not taking effect in External MDM server (Microsoft_intune)
CSCvw95488	ISE 2.6: Runtime crashes while TACACS+ get_handle is called by a socket stream
CSCvw96371	Static policy and group assignment lost from endpoint when updating custom attributes from API
CSCvw97905	Internal user export fails with no error when certain characters are used in the encryption key
CSCvx01798	ISE RBAC: "Unable to load Network Devices" error seen while adding a network device

Caveat ID Number	Description
CSCvx04512	Admin access with certificate based authentication can be bypassed by going directly to login.jsp
CSCvx09383	"All shards failed" exception thrown when sorting endpoint applications based on Running Process
CSCvx10186	ISE remains in Evaluation expired state even after registering with Smart Licensing
CSCvx15427	Health Checks :DNS Resolvability false failures seen when ISE FQDN is configured as CNAME (alias)
CSCvx15448	Disk space healthcheck failure message must be informative
CSCvx18730	Sudo Privilege Escalation Vulnerability Affecting Cisco Products: January 2021
CSCvx23205	Add IdenTrust Commercial Root CA 1 Certificate to ISE truststore
CSCvx27632	Authorization should Look Up MAC address in format configured in ODBC Stored-Procedures window
CSCvx28402	Support Bundle does not capture ise-jedis.log files on ISE 2.7 and later version
CSCvx30276	On re-creating Root CA, Jedis DB connection pool is not re-created
CSCvx32666	Authentication Method conditions not matching in Policy Set entry evaluation
CSCvx32764	TC-NAC services not running after unexpected power event
CSCvx36013	ISE Health Check Platform Support should update directly UI with results
CSCvx37149	SGA value Under-Provisioned for SNS3515 running all personas on same node
CSCvx37297	Error 400 While authenticating to Sponsor portal with Single Sign-on/Kerberos User
CSCvx41826	Unable to get all tenable adapter repositories with Tenable SC 5.17
CSCvx43566	No login fail log when using external username with wrong password
CSCvx43825	Receiving acct stop without NAS-IP address keep session in started state
CSCvx44815	ISE AD runtime should support rewrite a1-a2-a3-a4-a5-a6 to a1a2a3a4a5a6
CSCvx45481	CoA failed for endpoint when switch-port and Endpoint Identity Group change are changed
CSCvx46638	In EAP chaining scenario, posture policy failed to retrieve machine AD group membership
CSCvx47891	ISE not mapping correctly AMP events for new endpoints
CSCvx48922	Memory leak on TACACS flow
CSCvx50752	Add IdenTrust Commercial Root CA 1 Certificate for Smart Call Home and Smart Licensing

Caveat ID Number	Description
CSCvx51738	Add IdenTrust Commercial Root CA 1 Certificate for Network Success Diagnostics
CSCvx53761	REST query for sxplocalbindings returns code 500 "CRUD operation exception"
CSCvx54213	Network Devices > Default Device page requires Plus license to allow configuration
CSCvx57545	isedailycron temp1 tracking is causing delay in AWR reports
CSCvx58516	Top N Authentication by Network Device details are not properly displayed
CSCvx61664	ISE not updating the Json file information in the AnyConnect output config file
CSCvx70633	ISE doesn't accept % in EXEC or Enable Mode password when configuring Device configuration deployment in Advanced Trustsec setting
CSCvx71286	SXP engine failed to start due to duplicate SGT mappings after upgrading from 2.4 to 2.7P2
CSCvx78796	RADIUS Authentication Troubleshooting report shows incorrect or no data
CSCvx79693	Qualys integration is failing with ISE
CSCvx83663	ISE 2.7P3 sending packets to other node with link local address 169.254.2.2
CSCvx85391	If the username stored in ISE internal database and the authentication username differ in letter case, inactivity timer is not updated
CSCvx86571	The instruction box should be removed when the login-page message is empty
CSCvx86915	UI issues on TrustSec page
CSCvx94452	EST service not running on 2.7 p2 and above
CSCvx96915	vulnerabilities fixed in XStream 1.4.16
CSCvx99176	Incorrect IP overlap error reported for NADs using - or * in IP address ranges
CSCvy07333	Posture and BYOD flows impacted after patch installation
CSCvy15172	Cisco Identity Services Engine Self Cross-Site Scripting Issue

Open Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 4

Caveat ID Number	Description
CSCvx35960	TACACS+ authentications fail all of a sudden with Maximum Connection Limit Reached error.

New Features in Cisco ISE Release 2.7.0.356 - Cumulative Patch 3

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.

Configure TCP Parameters

To configure the TCP parameters use the **Configure TCP params** option (option 25) in the **application configure** command. Make sure you are in the Admin CLI.

For the changes to take effect, reload the Cisco ISE server on modifying any of the parameters using the Admin CLI **reload**.

Example

To configure the TCP parameters, use option 25.

```
ise/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
```

```
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Enable/Disable Wifi Setup
[18]Reset Config Wifi Setup
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]Configure TCP params
[0]Exit

25
This CLI allows admins to modify the TCP parameters recycle/reuse/fin_timeout
For the changes to take effect, RELOAD ISE server on modifying any of the parameter using
the admin cli 'reload'. Until reload is done, the changes will not be persisted.
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]: 1
Enable/Disable tcp recycle parameter? [e/d]: e
param recycle is already enabled..
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]: 2
Enable/Disable tcp reuse parameter? [e/d]: e
param reuse is already enabled..
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]: 3
Set tcp fin_timeout (60 default) <0-180> : 60
updated timeout param..
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]: 4
Current values of the tcp parameters:
Recycle = ENABLED
Reuse = ENABLED
Fin_timeout = 60
Select the option to configure/display tcp params.
```

```
1. tcp recycle
2. tcp reuse
3. tcp fin_timeout
4. display tcp param values
0. Exit
[1/2/3/4/0]:
```

Note tcp recycle and tcp reuse parameters are disabled by default. tcp fin_timeout is set to 60 seconds by default. The valid range for tcp fin_timeout is from 0 to 180 seconds. You can set this attribute to a lower value to enhance the TACACS+ performance.

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 3

The following table lists the resolved caveats in Release 2.7 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
CSCvf61114	ERS update/create for Authorization Profile failing XML schema validation
CSCvg50777	Active session is not deleted when nas-update=true accounting attribute is included
CSCvi27454	Status of pxGrid services should be shown as active/standby instead of running/disabled
CSCvm47584	Unable to configure grace period for more than one day due to posture lease
CSCvn31249	GNU gettext default_add_message Double-Free Vulnerability
CSCvq12204	SNMPv3 user added with wrong hash after reload causing SNMPv3 authentication failure
CSCvq44063	Incorrect DNS configuration can lead to TACACS+ or Radius authentication failure
CSCvq48503	"Health status unavailable" false alarm seen
CSCvr22065	Import NAD is failing with unsupported error when shared secret key has special character (8o\v|)
CSCvr47716	Info-ZIP UnZip File Overlapping Denial of Service Vulnerability CVSS v3.0 Base 7.5
CSCvs14743	EgressMatrixCell allows duplicate creation through ERS call
CSCvs29611	ISE 2.4 p5 crashes continuously around midnight, generating core files
CSCvs38176	Error message to be corrected in Trusted Certificate window
CSCvs69726	ISE 2.2 and above affected with memory leak. Everyday 1-2% increase in native memory by PORT_Alloc_Util()
CSCvs85273	Multiple Vulnerabilities in libcurl

Caveat ID Number	Description
CSCvs96516	Multiple Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities
CSCvs98094	File Remediation check is failing in ISE 2.7
CSCvt11179	"AD-Operating-System" attribute is not being fetched when this OS attribute is changed on the AD Server
CSCvt18613	Authorization conditions with AD groups not matched for TEAP EAP Chaining
CSCvt43844	runtime-aaa debugs do not print packet details in ascii
CSCvt50572	Not able to create whitelist policy via ERS API
CSCvt53541	SMS over HTTPS is not sending username/password to gateway
CSCvt55312	ISE BYOD with Apple CNA fails with 9800
CSCvt63119	ISE2.7 server runs out of processes after some MnT operation
CSCvt64739	Application Server takes more time to initialize
CSCvt65332	Error is thrown when Enter is used while creating profile description
CSCvt65853	MnT REST API for ReAuth fails when used in distributed deployment
CSCvt68108	ISE server-side authorization checks insufficient
CSCvt81194	CPU spikes are being observed at policy HitCountCollector
CSCvt82384	Rotation of diagnostics.log is not working
CSCvt83547	ISE PxGrid web clients couldn't list more than 25 subscribers
CSCvt85757	Sponsor portal display ? for non-English characters
CSCvt85836	Session cache getting filled with incomplete sessions
CSCvt89098	ISE does not reattempt wildcard replication for failed nodes
CSCvt91871	ISE RADIUS Accounting Report shows "No data found" under Accounting Details
CSCvt99349	Smart Licensing Compliance status "Released Entitlement" needs explanation
CSCvu01181	TacacsConnectionManager needs to be enhanced to remove the stale connections
CSCvu05121	Guest email not sent after changing SMTP server
CSCvu06604	Mention in documentation that AAA server in TrustSec Work Center > Components > TrustSec AAA Servers page refers to RADIUS nodes
CSCvu13368	Config backup from CLI fails with error
CSCvu14215	Sponsor group membership is removed while adding/removing AD group
CSCvu15948	TC-NAC adapter stopped scanning with nexpose

Caveat ID Number	Description
CSCvu19221	During sponsor portal configuration, support information is not properly displayed in the flowchart
CSCvu21093	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
CSCvu28305	ISE logging timestamp shows future date
CSCvu29434	ISE 2.6 patch 6 services fail to initialize after reload on SNS 3655 PSN
CSCvu30286	ERS SGT create is not permitted after moving from Multiple matrix to Single matrix
CSCvu31176	ISE 2.4 patch 11 VPN + Posture: Apex Licenses are not being consumed
CSCvu31853	NDG added through ERS became associated with all network devices in database
CSCvu32240	When running ISE ERS API for internal user update, existing identity groups value is set to null
CSCvu33416	License out of compliance alarm displayed even for valid license
CSCvu33861	REST API MnT query to get device by MAC address takes more than 2 seconds
CSCvu33884	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvu34433	Free space on Undo tablespace not cleared as per isehourlycron.sh cron script
CSCvu34895	Report repository export is not working with dedicated MnT node
CSCvu37873	Clicking on Details of an Unknown NAD Alarm shows an error
CSCvu39653	Session API for MAC Address returning "Char 0x0 out of allowed range" error
CSCvu41815	GBAC sync breaks on deleting VN from SG if authorization profile is mapped to the same VN for different SG
CSCvu45697	Compress messages.x files in the system
CSCvu47395	Drop_Cache required for systems with High Memory Issues
CSCvu48417	ISE ERS API DELETE device returns 500 error with more than 1 call
CSCvu49019	Suspected memory leak in Elastic search
CSCvu53836	ISE Authorize-Only requests are not assessed against Internal User Groups
CSCvu55332	REST API call can remove Network Device Group referenced in Policy Set
CSCvu55557	Minimum character requirement for RADIUS secret is not checked when REST API is used to create NAD

Caveat ID Number	Description
CSCvu58476	Improve error messaging on My Device Portal while showing identity store issues
CSCvu58793	ERS REST API returns duplicate values multiple times when filter by location option is used
CSCvu58892	Update "master guest report" to "primary guest report" everywhere in the ISE GUI
CSCvu59093	Session database columns are missing
CSCvu59491	ISE creates new site in insiteVM (tc-nac server)
CSCvu63642	Context Visibility fuses endpoint parameters on username update
CSCvu68700	ERS API response for XML or JSON request with invalid credentials is HTTP 401 with unexpected HTML body
CSCvu70683	Alarm Suppression required for ERS queries along with suppression on iselocalstore.log
CSCvu70768	Alarms and system summary is not showing up on ISE GUI
CSCvu73387	Authentication failure with error "12308 Client sent Result TLV indicating failure"
CSCvu74198	LDAP and ODBC identity store names do not allow hyphen
CSCvu84773	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvu87742	When ACI is configured in ISE for SXP integration, authentication fails if a third-party certificate is used
CSCvu87758	Guest password policy settings cannot be saved when set to ranges for alphabets or numbers
CSCvu90107	ISE allows duplicates device ID in ERS flow in all versions
CSCvu90703	CLDAP thread is hung and running infinite
CSCvu90761	ISE Radius Live Sessions page showing No Data Found
CSCvu91039	ISE 2.6 patch 7 not doing lookup for all mac addresses in mac list causing redirectless Posture to fail
CSCvu91601	ISE Authentication Status API call duration does not work as expected
CSCvu94025	ISE should either allow IP only for syslog targets or provide DNS caching
CSCvu94733	Guest authentication fails with "Account is not yet active" for incorrect password
CSCvu97657	Application server going to Initializing state on enabling endpoint debugs
CSCvv00377	Overlap of network devices using subnet and IP range
CSCvv00951	Application server crashes while transitioning into stopping state
CSCvv01681	Cisco Identity Services Engine Cross-Site Scripting Vulnerability

Caveat ID Number	Description
CSCvv04416	Endpoint data not visible on secondary Admin node
CSCvv07049	Unable to connect with an ODBC identity source
CSCvv08466	Log Collection Error alarms appear repeatedly in ISE dashboard
CSCvv08784	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
CSCvv10572	Unable to register IND with ISE on 2.4 patch 13
CSCvv10683	Session cache for dropped session not getting cleared, thereby causing high CPU usage on PSNs
CSCvv14001	Authorization profile not saved with proper attributes
CSCvv15811	ISE TCP ports 84xx not opened if there is shutdown interface with IP address assigned
CSCvv18317	Invalid objects in Database
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 without encryption key is not working properly after using the Export with Encryption Key option
CSCvv27690	While renewing ISE certificate for HTTPS, EAP, DTLS, and PORTAL, only PORTAL and Admin roles gets applied
CSCvv29190	BYOD Flow is broken in iOS 14 beta
CSCvv30133	Discovery host description text is misleading
CSCvv30226	Livelog sessions show incomplete authorization policy for VPN Posture scenario
CSCvv35921	Cannot start CSV export for selected user in internal ID Store
CSCvv36189	Radius passed-auth live logs not sent due to invalid IPv6 address
CSCvv38249	Manual NMAP not working when only custom ports are enabled
CSCvv39000	Unable to create posture condition for LANDESK
CSCvv39584	Remove ojdbc8 jar from ISE 2.6 and 2.7 patch branch
CSCvv41935	PSK cisco-av-pair throws an error if the key contains < or > symbol
CSCvv42857	MAC 11.x and its minor version support for ISE is not available

Caveat ID Number	Description
CSCvv43558	Evaluation of ISE for Apache Struts Aug20 vulnerabilities
CSCvv45063	Internal CA certificate not getting deleted when node is removed from deployment
CSCvv46034	Device admin service is getting disabled while updating Tacacs config
CSCvv46958	TrustSec enabled NADs not shown in TrustSec matrices when NDG column exceeds 255 characters
CSCvv47849	Mapped SGT entry cleared from Authorization Rules if SG name is modified in Cisco DNA Center
CSCvv48544	Health check doesn't work when ISE has NIC teaming enabled
CSCvv49403	8084/TCP EST service allowing weak and non-FIPS compliant ciphers
CSCvv50028	Heap Dump generation fails post reset-config of ISE node
CSCvv50721	Can't get the download link of NetworkSetupAssistant.exe using Aruba dynamic URL redirect
CSCvv52637	ISE Hotspot guest portal flow broken
CSCvv53221	When RADIUS Shared Secret is missing for ISE_EST_Local_Host, ISE application server goes to intializing state
CSCvv54761	Export of current active session reports only shows sessions that has been updated since midnight
CSCvv54798	Context Visibility CVS exported from CLI not showing IP addresses
CSCvv55663	ISE 2.6/2.7 repositories get deleted post ISE node reload
CSCvv57628	Suspended Guest User is not automatically removed from Endpoint Group
CSCvv57639	Saving command with parenthesis in TACACS command set gives an error
CSCvv57830	Group lookup failed as empty value is appended to the context
CSCvv58629	Certificate Authority Service initializing EST Service not running after upgrade to ISE 2.7 patch 2
CSCvv59233	ISE RADIUS Live Log details missing AD-Group-Names under Other Attributes section
CSCvv60686	ISE SXP should have a mechanism to clear stale mappings learned from session
CSCvv60923	Need the ability to use a forward slash in the IP data type of internal user custom attribute
CSCvv62382	Proxy bypass settings does not allow upper case characters
CSCvv62549	Custom Attribute from Culinda not showing in endpoint GUI page

Caveat ID Number	Description
CSCvv62729	Network Device API call throws error 500 if you query an non-existent network device
CSCvv64190	Case sensitivity on User Identity Groups causes "Select Sponsor Group Members" Window to not load
CSCvv67051	Radius Server Sequence page showing "no data available"
CSCvv67743	Posture Assessment by Condition report displays No Data with Condition Status filter
CSCvv67935	Security Group values in Authorization Profile disappear shortly after fetching
CSCvv68028	Cannot modify AUP text
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
CSCvv77530	Unable to retrieve LDAP Groups/Subject Attributes when % character is used twice or more in bind password.
CSCvv77894	Bias-free text/code in upgrade and database
CSCvv80113	ISE Posture auto-update not running
CSCvv82806	Network Device IP filter does not match IPs that are inside Subnets
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 node is down
CSCvv91684	ISE Collection filters not displayed in GUI
CSCvv92203	The following error message is displayed while trying to create SGT with the name "Employees": `NetworkAuthZProfile with entered name exists`
CSCvv94791	Unable to sync GBAC configuration between DNAC and ISE
CSCvw00375	Unable to load Context Visibility page for custom view in ISE 2.7p2
CSCvw01225	ISE Config Restore fails at 40% with error "DB Restore using IMPDP failed"
CSCvw01829	ISE GUI Login page shows the following error with Chrome 85/86: `Oops. Something went wrong`
CSCvw08330	Posture does not work with dynamic redirection on third party NADs
CSCvw08765	Upgrade license check should check ISE database for smart license registration
CSCvw19706	Offline/Online Feed would fail when Timezone on ISE is set to America/Santiago
CSCvw19785	Correct AD is not shown while editing external data source posture condition
CSCvw20021	NAD location is not updated in Context Visibility ElasticSearch

Caveat ID Number	Description
CSCvw20636	Authorization Profiles show "No data available" when the NAD profile is deleted
CSCvw24227	Endpoints not purged due to an exception
CSCvw25615	ISE TACACS logging timestamp shows future date
CSCvw28441	NADs shared secrets are visible in the logs while using APIs
CSCvw36743	ISE Service Account Locked and WMI not established when special characters are used in the password
CSCvw38853	Sophos 10.x definition missing from Anti-malware condition for MAC OSX
CSCvw54878	Authorization policy is not displayed properly if it has 50 rules or more in Japanese GUI
CSCvw56938	SCH connection attempted even if smart licensing is not enabled
CSCvw59855	Affected third-party software component has to be upgraded to a version that includes fixes for the vulnerability

Known Limitations in Cisco ISE 2.7 Patch 3

Change in SNMP User Password Format and SNMP Hash Minimum Length

After applying Cisco ISE 2.7 Patch 3, 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
```

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.

New Features in Cisco ISE Release 2.7.0.356 - Cumulative Patch 2

User Defined Network

User Defined Network is a Cisco DNA Center solution. User Defined Network is supported in Cisco ISE Release 2.7 Patch 2 through a hotfix. User Defined Network allows end users to create private networks, or User Defined Network rooms, and group their personal devices.

For example, a student in a university dorm that has User Defined Network enabled in its network can register their devices and add them to a personal User Defined Network room.

User Defined Network end users will be able to invite other users to temporarily bring their devices into their User Defined Network room, and vice versa.

To enable User Defined Network, Cisco ISE must be added to the on-premise Cisco DNA Center account.

Validate the integration of Cisco ISE with Cisco DNA Center from your Cisco ISE administrator portal. Choose **Administration** > **pxGrid Services** > **All Clients**.Choose **Administration** > **pxGrid Services** > **Client Management** > **Clients**. Cisco DNA Center should appear in the list of pxGrid clients.

When the User Defined Network solution is enabled, the Cisco DNA Center Cloud automatically sends to Cisco ISE the configuration information of all the User Defined Network-registered devices on the network. This includes information on the User Defined Network room that each device currently resides in.

Cisco ISE then shares this information with the Cisco Wireless LAN Controllers (WLC) that are configured to be part of the User Defined Network solution. This sharing is accomplished as part of the normal RADIUS protocol exchanges between Cisco ISE and the connected Cisco WLCs.

For profiling and logging changes in Cisco ISE due to User Defined Network, see the *Cisco ISE Administrator Guide* for your release. See Chapter "Segmentation" for the related profiling changes, and Chapter "Troubleshooting" for the related logging changes.

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 2

The following table lists the resolved caveats in Release 2.7 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
CSCuo02920	ISE not returning configured Radius AVP 18 in access-reject
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
CSCvh77224	ENH // Smart License registration using HTTPS Proxy fails
CSCvi35647	Posture session state need to be shared across PSNs in multi-node deployment
CSCvi62805	CSCvi62805 ISE ODBC does not convert the mac address as per configured stored procedure
CSCvj47301	ISE sends CoA to active-compliant sessions when a node-group member is unreachable

Caveat ID Number	Description
CSCvm62775	ISC BIND krb5-subdomain and ms-subdomain Update Policies Vulnerability
CSCvn12644	ISE Crashes during policy evaluation for AD attributes
CSCvn50531	tcpdump print_prefix Function Stack-Based Buffer Overread Vulnerability
CSCvn73729	Error occurred in publishing threat events - AMP adapters
CSCvn73740	EAP-TLS authentications with Endpoint profile set to not unknown fails in second authorization.
CSCvo28970	AnyConnect displays Cisco NAC agent error when using Cisco temporal agent
CSCvp17458	libssh2 SSH_MSG_CHANNEL_REQUEST Packet Handling Out-of-Bounds Read V ...
CSCvp59038	ISE Secondary PAN node sending RST to other ISE node with src ip address 169.254.2.2
CSCvp85813	Filter by specific Network Device IP address on TACACS Live Logs
CSCvp93322	Significant memory increase in MNT during Longevity test
CSCvq13431	ISE PSN node crashing while fetching context attributes during posture plus RADIUS flow
CSCvq43600	Disabled PSN persona but TACACS port 49 still open.
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
CSCvq86746	Multiple Vulnerabilities in jquery - guest portals
CSCvq90601	EAP Chaining: Dynamic Attribute value is unavailable
CSCvr07294	Radius Authentication and Radius Account Report performance is slow
CSCvr09749	GNU patch do_ed_script OS Shell Command Execution Vulnerability
CSCvr47732	FasterXML jackson-databind Polymorphic Typing Vulnerability CVSS v3.1 Base: 9.8
CSCvr56785	Localdisk size needs to be increased to accommodate large corefiles
CSCvr61108	PxGrid ANC API support for Session-ID
CSCvr68432	2.4P10 Endpoint added via REST has visible policy assignment only in "edit" mode
CSCvr68971	ISE IP routing precedence issue
CSCvr77676	libmspack chmd_read_headers Function Denial of Service Vulnerability

Caveat ID Number	Description
CSCvr81384	Failing Network Devices CSV import, process silently aborting without reason
CSCvr85513	core file generated on PSN
CSCvr87373	ACI mappings are not published to SXP pxGrid topic
CSCvs05260	App server and EST services crash/restart at 1 every morning
CSCvs09981	Add the capability to filter out failed COA due to MAR cache checks among group nodes in ISE
CSCvs25569	Invalid root CA certificate accepted
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
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
CSCvs47941	Fail to import Internal CA and key on ISE2.6
CSCvs51519	NFS mounting causes crash
CSCvs53606	ISE 2.4: Administrator Login Report, Auth failed when using cert based admin auth
CSCvs55464	Creating a new user in the sponsor portal shows "invalid input"
CSCvs62081	collector log is dumped with pxgid and dnac messages
CSCvs62586	Tacacsprofile not retrieved properly using REST API
CSCvs62597	Authz Profiles not pulling properly using REST API (Pagination is missing)
CSCvs67785	Days duration is not getting updated in portal page customization for self registration portal
CSCvs70997	ISE: 2.4p9 Intermediate CA cert not installed when configuring SCEP RA
CSCvs75274	Unable to do portal customization for "certificate provisioning portal"
CSCvs78160	URT fails on a ConditionsData clause from INetworkAuthZCheck
CSCvs79836	Expired Certificates not listed for deletion
CSCvs82557	SXP Bindings are not published to pxGrid 2.0 clients

Caveat ID Number	Description
CSCvs83303	API is not retrieving the data when interim-updates are not stored DB
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
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	TACACS auth/acc reports are not visbile after restoring OP backup
CSCvs97302	.dmp files not deleted from /opt/oracle/base/admin/cpm10/dpdump even after the reset-config on ISE
CSCvs98602	X.Org libX11 Client Segmentation Fault Denial of Service Vulnerability
CSCvs98604	X.Org libX11 Off-by-One Memory Write Arbitrary Code Execution Vulnerabi
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 shouldnt 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
CSCvt11366	Exporting Endpoints from CLI results in java exception

Caveat ID Number	Description
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
CSCvt15787	TCPDump - Node and Interface field Unavailable
CSCvt15893	Radius Errors/Misconfigured supplicants tables do not exist after upgrade to ISE2.6
CSCvt15935	High Load Alarms coinciding with System Summary Dashboard not populating for some nodes
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
CSCvt24276	Cannot add/modify allowed values more than 6 attributes to System Use dictionaries
CSCvt25610	ISE2.7 compliance counter is 0
CSCvt26108	ISE 2.7 Anyconnect configuration's deferred updates do not get saved
CSCvt31275	Two rows created in upscsnconfig table in a upgraded setup
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
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 exisiting shorter pwd fails to login via GUI with no error
CSCvt40534	MNT node election process is not properly designed.
CSCvt46850	Unavailability to modify compound conditions when these are already created.

Caveat ID Number	Description
CSCvt49961	Syslog Target configured with FQDN can cause Network Outage
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
CSCvt69912	ISE still generates false positive alarm "Alarms: Patch Failure"
CSCvt69941	ISE 2.6 Redundant "Application patch install has completed successfully" Alarm
CSCvt70689	Application server may crash when MAR cache replication is enabled
CSCvt71355	pxGrid unable to delete user in INIT state
CSCvt71559	Alarm Dashlet shows 'No Data Found'.
CSCvt73927	ISE 2.7 Certificate Authority Service disabled after patch 1 installation
CSCvt73953	Mismatched Information between CLI export and Context Visibility
CSCvt80285	Cannot select every individual product when creating Anti-Malware Condition for definition
CSCvt85722	No debug log for non working MNT widgets
CSCvt87409	ISE DACL Syntax check not detecting IPv4 format errors
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
CSCvu03572	upn.log not available for upload in ISE UI
CSCvu05164	ISE is not allowing to disable Radius in NAD via API
CSCvu10009	PUT verb for /ers/config/internaluser/name/{username}makes id&password&name mandatory in req content
CSCvu26008	portal page customisation changes are not reflecting in certificate provisioning portal
CSCvu32865	High cpu on ISE 2.7 causing authentication latency
CSCvu39890	ISE - Rollback stuck indefinitely attempting to rollback from Patch 12
CSCvu42244	Machine Authentications via EAP-TLS fail during authorization flow citing a user not found error
CSCvs42441	Service account passwords returned from server in SMS and LDAP page

New Features in Cisco ISE Release 2.7.0.356 - Cumulative Patch 1

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.

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.

Resolved Caveats in Cisco ISE Release 2.7.0.356 - Cumulative Patch 1

The following table lists the resolved caveats in Release 2.7 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
CSCuz18895	CoA REST API is not working for ASA VPN Sessions
CSCve89689	MNT API does not support special charactor
CSCvf59076	Live sessions show incorrect Authorization profile and Authorization Policy for VPN+Posture scenario
CSCvj67437	Multiple Vulnerabilities in procps-ng
CSCvk50684	Not able to delete certificate after hostname change
CSCvo22887	ISE 2.4 URT does not check is node is on a supported appliance
CSCvo49755	To enable CLI clock timezone command
CSCvo87602	Memory leak on ISE node with the openldap rpm running version 2.4.44

Caveat ID Number	Description
CSCvp07591	EAP-GTC Machine Authentication Failure Password Mismatch due to failing the UTF-8 Validation Checks
CSCvp24085	ISE 2.4 High CPU utilization on Secondary Admin Node
CSCvp73335	Radius session detail report are broken if calling-station-id contains CLIENTVPN
CSCvp88443	ISE CoA is not sent even though new Logical Profile is used under Authz Policy Exceptions
CSCvq11008	Renew ISE OCSP Responder Certificates not showing data under report - Change-Configuration-Audit
CSCvq60564	Automatic email to "Notify Known Guests" using the text to "Notify Imported Guests (Desktop only)"
CSCvq61878	Evaluation of ISE for CVE-2018-20685
CSCvq85414	Login page AUP as link does not work with iOS CNA browser
CSCvr12350	ISE : "MDM: Failed to connect to MDM server" log entry needs to have endpoint information
CSCvr13481	ISE ERS SDK NetowrkDeviceGroup DELETE does not specify ID location
CSCvr25197	After changing password via UCP, "User change password audit" report doesn't have "Identity"
CSCvr35719	Unable to get all tenable adapter repositories
CSCvr39943	Blank Course of Action for Threat events received from CTA cloud to TC-NAC adapter
CSCvr40359	ISE not using the device-public-mac attribute in endpoint database
CSCvr40545	EAP-FAST authentication failed with no shared cipher in case of private key encryption failed.
CSCvr40574	Export failed in ISE gui in case of private key encryption failed no ERROR msg in ISE GUI
CSCvr43077	Day0: iPad OS 13.1 BYOD flow got failed
CSCvr44495	pxGrid Arab Bank defensive code change
CSCvr48101	Unexpected COAs may be observed with SCCM MDM
CSCvr51959	ISE 2.4 Not entire fqdn is matched, but fragment of characters
CSCvr57378	DHCP messages are marking endpoints active increasing the active endpoint count
CSCvr60339	Typo in Max Sessions Page on Counter time limit tab
CSCvr62517	ISE 2.4 p9 Session directory write failed : String index out of range: -1

Caveat ID Number	Description
CSCvr63504	Unable to delete SCEP profile because it is referencing system certificates
CSCvr67988	ISE sponsor's e-mail gets CC'd even when view/print guests' passwords is disabled
CSCvr70044	" No policy server detect" on ISE posture module during high load .
CSCvr70581	Called-Station-ID missing in RADIUS Authentication detail report
CSCvr71796	SCCMException in SCCM flow,ISE updating the MDMServerReachable value as false in the MDMServersCache
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
CSCvr84143	tzdata needs to be updated in ISE guest OS
CSCvr84753	ISE 2.2 patch 14 AD status shows up as "updating.." indicating the process is hung
CSCvr84978	ISE: LDAP bind test does not use the correct server when defined per node
CSCvr85363	ISE App crash due to user API
CSCvr87936	Valid Base and Plus licenses show out of compliance
CSCvr90773	LiveLogs show wrong username for '5436 NOTICE RADIUS: RADIUS packet already in the process' messages
CSCvr92420	Async Http Client Improper Input Validation Vulnerability
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
CSCvr98395	Profiling CoA for IP based Profile Policy isn't sent
CSCvs01949	ISE Messaging service triggers Queue Link error alarms with the reason basic_cancel
CSCvs02166	API calls show different result as GUI
CSCvs03195	Max Session Counter time limit option is not working
CSCvs03810	ISE doesn't display the correct user in RADIUS reports if the user was entered differently twice
CSCvs04433	ISE : TACACS : PSN crashes for TACACS+
CSCvs05104	Set max time frame to 60 mins when EndPoint default interval disabled
CSCvs07344	ISE: Reset config on 2.4 patch 9 throws some errors despite finishing successfully.
CSCvs12409	ISE Guest creation API validation for Guest Users valid Days doesn't take time into account

Caveat ID Number	Description
CSCvs14297	PassiveID: Configuring WMI with an AD account password that contains a $ will result in an error.
CSCvs19481	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvs20356	Apple minibrowser - Reset password link is not working in Self registration guest login page
CSCvs20357	Apple minibrowser - Cancel button is not working in Guest Self registration page
CSCvs23628	Policy engine continues to evaluate all Policy Sets even after rule is matched
CSCvs25258	Improve behavior against brute force password attacks
CSCvs27310	ISE 2.6 and 2.7 - Cannot add character ' on dACLs 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
CSCvs36758	Unable to configure CRL URL with 2 parenthesis at ISE 2.6
CSCvs39633	NAD group CSV imports should allow all supported characters in description field.
CSCvs40813	Missing the following properties in platform.properties for <sns3615> ,<sns3655> <sns3695>
CSCvs41571	Self Registered Guest portal unable to save guest type settings
CSCvs42072	Unable to edit static group assignment
CSCvs42758	The CRL is expired with specific condition
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
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 EP's profiled every second causing ISE nodes to go out of sync
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
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()
CSCvs68914	Errors when SG created using _ underscore sent from DNAC
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.
CSCvt02530	SMS not reaching guests when Country Code Attribute part of mobile number
CSCvt15256	Authentication goes to process fail when "Guest User" ID Store is used.
CSCvr63698	pxGrid 2.0 authorization profile attribute missing from the session directory

Resolved Caveats in Cisco ISE, Release 2.7

The resolved caveats in Cisco ISE Release 2.7, have parity with these Cisco ISE patch releases: 2.2 Patch 15, 2.3 Patch 7, 2.4 Patch 10, and 2.6 Patch 2.

The following bugs are resolved in Release 2.7:

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283801589&rls=2.7&sb=anfr&sts=fd&scs=hSc&bt=custV

Open Caveats in Cisco ISE, Release 2.7

The following table lists the open caveats in Release 2.7:

Caveat ID Number	Description
CSCvq11008	Renew ISE OCSP Responder Certificates CSR usage data not shown in Change Configuration Audit report
CSCvp54416	Device SGT troubleshooting provides wrong diagnostics
CSCvr86006	Node status is not displayed correctly in the System Summary dashlet
CSCvr91946	Issuance of Certificates fails for more than 10% of endpoints
CSCvr93902	Pop-up window that allows the admin to add comments to the approval request in the Network Device Deployment window is not properly displayed
CSCvr95284	RADIUS mappings are not published to SXP pxGrid topic
CSCvr99920	"show timezone" command doesn't show timezone on CLI
CSCvs02589	NET::ERR_CERT_REVOKED error seen in Chrome on macOS 10.15 when the validity of self-signed server certificate is set to 5 years
CSCvs03195	Max Session Counter time limit option is not working

Caveat ID Number	Description
CSCvs10238	While importing policy from CSV file, if there is policy download, partial updates observed
CSCwc83059	Post full upgrade VCS information is missing
CSCwe99609	Timestamps need adjustment whenever timezone is changed
CSCwe99666	Live logs and live sessions pages are displayed in incorrect sorting order when timezone is changed on PSN and MnT nodes
CSCwe99706	Session data is shown at the bottom when PSNs are in different timezones

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.