Release Notes for Cisco Identity Services Engine, Release 2.4

First Published: 2018-04-30

Last Modified: 2020-05-06

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!

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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, Cisco Wireless Controllers, Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual 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 more information about the features that are supported in this Cisco ISE release, see the Cisco Identity Services Engine Administrator Guide.

To access documentation on cisco.com, see End-User Documentation.

System Requirements

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

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

Supported Hardware

Cisco ISE, Release 2.4, can be installed on the following platforms:

Table 1: Supported platforms

Hardware Platform	Configuration
Cisco SNS-3515-K9 (small)	For the 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)	

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

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.

Caution

- Cisco ISE 3.1 does 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 Mode Support

Cisco ISE uses embedded Federal Information Processing Standard (FIPS) 140-2-validated cryptographic module, Cisco FIPS Object Module Version 6.0 (Certificate #2984). For details about the FIPS compliance claims, see Global Government Certifications.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- VMware ESXi 5.x, 6.x
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on RHEL 7.0, and 7.3

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 88 and earlier versions from version 82
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 90 and earlier versions from version 86
- Microsoft Internet Explorer 11.x

Note

- If you use Chrome 65.0.3325.189, you may be unable to view guest account details in the print preview section.
- You might see a warning message while downloading an executable (EXE) file in Google Chrome 76 or later. To resolve this issue:
  1. In your browser, click the Settings menu at the top-right corner.
  2. At the bottom of the Settings window, click Advanced.
  3. Under Downloads, check the Ask Where to Save Each File before Downloading check box.

Validated External Identity Sources

Table 2: Validated External Identity Sources

External Identity Source	Version
Active Directory [1] [2]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [3]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Any LDAP v3 compliant server	Any version that is LDAP v3 compliant
Token Servers	
RSA ACE/Server	6.x series
RSA Authentication Manager	7.x and 8.x series
Any RADIUS RFC 2865-compliant token server	Any version that is RFC 2865 compliant
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	
Microsoft Azure	Latest
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
PingFederate Server	Version 6.10.0.4
PingOne Cloud	Latest
Secure Auth	8.1.1
Any SAMLv2-compliant Identity Provider	Any Identity Provider version that is SAMLv2 compliant
Open Database Connectivity (ODBC) Identity Source	
Microsoft SQL Server	Microsoft SQL Server 2012
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9.0

External Identity Source	Version
Sybase	16.0
MySQL	6.3
Social Login (for Guest User Accounts)	
Facebook	Latest

[1] Cisco ISE OCSP functionality is available only on Microsoft Windows Active Directory 2008 and later.

[2] You can only add up to 200 Domain Controllers on Cisco ISE. On exceeding the limit, you will receive the following error:

```
Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200
```

[3] Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2012 R2. However, the new features in Microsoft Windows Active Directory 2012 R2, such as Protective User Groups, are not supported.

See the Cisco Identity Services Engine Administrator Guide for more information.

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.

What is New in Cisco ISE, Release 2.4

Support for Cisco Secure Network Server 3600 Series Appliance

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

Business Outcome: Improved performance, scalability, and platform manageability over SNS 35xx series appliances.

The Default TLS Version when initiating External Connections through Proxy is TLS 1.2

When the Cisco ISE acts as a client, the default protocol used for the connections initiated from it to the external entities is TLS 1.2 In this case the supported protocol will be TLS 1.2 only. In case you want to provide support for lower versions as well (which might be insecure), these versions need to be explicitly enabled from the Cisco ISE by going to the following page: Administration > System > Settings > Security Settings.

Business Outcome

Improved security in SSL connections.

Cisco ISE Can Pull IoT Device Context and Session Data from Cisco IND

Cisco ISE can profile and display the status of devices attached to a Cisco Industrial Network Director (IND). Cisco Platform Exchange Grid (pxGrid) is used to communicate the endpoint (Internet of Things [IoT]) data between Cisco ISE and Cisco IND. pxGrid is used to receive the context from Cisco IND and query Cisco IND to update endpoint type.

Business Outcome

Automates classification of IoT devices on your network.

Control Permissions for pxGrid Clients

You can create pxGrid authorization rules to control the permissions of the pxGrid clients (under Administration > pxGrid Services > Permissions).

These rules to control which services and operation on that service are available to the pxGrid clients. Cisco ISE applies the rules to groups, not individual clients. You can manage groups by clicking the Manage Groups heading in the Permissions window. The Permissions window displays predefined authorization rules that use predefined groups (such as EPS, ANC). You can only update the Groups field in the predefined rules.

Business Outcome

Better pxGrid backward compatibility: • Ability to control authorizations for different pxGrid services. • Easier to group pxGrid clients with similar permissions.

Customizable SSH Ciphers and Encryption Algorithms

You can use the `service sshd encryption-algorithm` and `service sshd encryption-mode` global configuration commands in Cisco ISE 2.4 to harden the ISE SSH server and specify the cipher suite to be used. You can use AES-CTR and/or AES-CBC ciphers.

Cisco ISE 2.3 and earlier releases allowed only AES-CBC ciphers (due to Common Criteria Protection Profiles for Access Control Devices and Systems). Cisco ISE 2.4 allows you to use both AES-CTR and AES-CBC ciphers.

Business Outcome

• Improved security for SSH access. • Allows you to choose the encryption algorithms. • Allows you to choose the ciphers to be used to harden secure access.

Endpoint API Enhancements for MDM Attributes

Mobile Device Management (MDM) attributes are made available through the endpoints API to enable additional synchronization capability between Cisco ISE and a third-party MDM server.

Business Outcome

Helps customers to better integrate third party systems with ISE and provide better user experience for end users using mobile devices that are managed by an MDM server.

IPv6 Support for RADIUS

IPv6 addresses are now supported for RADIUS configurations. The IP Address field in the Administration > Network Resources > Network Devices page and the Host IP field in the Administration > Network Resources > External RADIUS Server page now support both IPv4 and IPv6 addresses for RADIUS configurations.

Business Outcome

Additional support for IPv6 addressing:

- Allows you to migrate your network to IPv6-based networks. You can migrate to IPv6 addressing if you have fragmented networks or have exhausted IPv4 addresses.
- Facilitates more efficient routing, packet processing, security, and simplified network configuration.

Large Virtual Machine for Monitoring Persona

Cisco ISE introduces a large VM for Monitoring nodes.

This form factor is available only as a VM in Release 2.4 and above, and requires a large VM license.

Business Outcome

Deploying Monitoring persona on a large VM offers the following advantages:

- Up to three times the volume of data previously supported.
- Improved performance in terms of faster response to live log queries and report completion.

Posture Enhancements

- Grace Period for Noncompliant Devices—Cisco ISE provides an option to configure grace time for devices that become noncompliant. Cisco ISE caches the results of posture assessment for a configurable amount of time. If a device is found to be noncompliant, Cisco ISE looks for the previously known good state in its cache and provides grace time for the device, during which the device is granted access to the network. You can configure the grace time period in minutes, hours, or days (up to a maximum of 30 days). The Posture Assessment by Endpoint report is updated and displays a Grace Compliant status for an endpoint that is currently not compliant, but is under the grace period.
- Posture Rescan—AnyConnect users can now manually restart posture at any time.
- AnyConnect Stealth Mode Notifications—Several new failure notifications are added for AnyConnect stealth mode deployment to help users identify issues with their VPN connection.
- Disabling UAC Prompt on Windows—You can choose to disable the User Access Control (UAC) prompts on Windows endpoints from the AnyConnect posture profile.

Note By default, this value is set to No while configuring the AnyConnect Profile. When you change it to Yes, the UAC prompts are disabled and the Windows users no longer receive these prompts. If you want to enable the UAC prompt again, you should change this setting to No in the AnyConnect Profile. This setting takes effect only when the Windows endpoint is restarted.

- New URL for Downloading Client Provisioning and Posture Updates—The client provisioning and posture feed URL has changed. The new URL for Posture Updates is https://www.cisco.com/web/secure/spa/posture-update.xml and for Client Provisioning is https://www.cisco.com/web/secure/spa/provisioning-update.xml
- File Condition Enhancements—A new operator, within, is introduced under File Condition to check for the changes in a file within a certain period of time.
- Certificate Attributes in Client Provisioning and Posture Policies—Certificate attributes are now available in the client provisioning and posture policy pages.
- The following option has been newly added under the Location field in the Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition window:
  - All Internal Drives—To check the internal drives. Includes all hard disks that are mounted and encrypted, and all internal partitions. Excludes read only drives, system recovery disk/partition, boot partition, network partitions, and the different physical disk drives that are external to the endpoint (including but not limited to disk drives connected via USB and Thunderbolt). Encryption software products that are validated include:
    - Bit-locker-6.x/10.x
    - Checkpoint 80.x on Windows 7

Note "All Internal Drives" option is supported from AnyConnect Version 4.6.01098 onwards.

Business Outcome

Improved security alerts and enforcement:

- Provides admin users with more flexible options for educating end users about posture condition failures including grace-period-specific messaging scenarios.
- Helps effective management of some posture checks and remediations that require additional privileges and prompts the user for such privileges.

Profiler Enhancements

- Added 190 new profile policies from vendors, including AudioCode, BlackBerry, Brother, Hewlett Packard, Lexmark, NetApp, Samsung, and Xerox.
- Added additional conditions to 185 profile policies to support additional probes. For example, DHCP conditions are added to Xerox devices such that customers who do not want to profile Xerox devices based on SNMP, can profile Xerox devices using DHCP.
- Reorganized profiles into families for better identification of new devices. For example, HP-LaserJet-4350 was previously profiled directly under HP-Device. It is now profiled under HP-LaserJet, which in turn is profiled under HP-Device. When Hewlett Packard introduces a new Hewlett Packard LaserJet printer model, Cisco ISE will classify the new model as HP-LaserJet, and not as HP-Device until a new profile policy for that exact LaserJet printer model is added.

Business Outcome

Effective classification of devices:

- Helps you gain visibility of previously unknown devices, such as Xerox printers or Vista link printers with improved profiler efficacy.

Support for Sending Separate SNMP CoA Packets

You can check the Send SNMP COA Separate Request check box in the Administration > Network Resources > Network Device Profiles > Change of Authorization (CoA) window to send the SNMP CoA packets to the NAD as two packets.

Business Outcome

Increased compatibility with devices:

- Provides support for older Cisco and third-party NADs that mandate the sending of SNMP CoA packets as two packets (for the shutdown and no shutdown interface configuration commands).

Support for Two Shared Secrets Per IP for RADIUS NAD Clients

You can specify two shared secrets (keys) to be used by the network device and Cisco ISE. You can configure the shared secrets in the RADIUS authentication settings section for a NAD in the Administration > Network Resources > Network Devices page in Cisco ISE.

Business Outcome

Replace Shared Secrets on network devices:

- Enables you to replace shared secrets on network devices independently and allows ISE to support both old and new shared secrets until the shared secret is replaced on the network device. Changing a RADIUS secret is now simplified and allows you to enter a new shared secret even before updating the network device.

TrustSec Enhancements

You can select the ISE node from which the configuration changes must be sent to the network device while adding the network device (under Advanced TrustSec Settings section). You can select the PAN or PSN node. If the PSN node that you selected is down, the configuration changes are sent to this device using the PAN.

While deploying the IP SGT static mappings, you can select the devices or the device groups to which the selected mappings must be deployed. You can select all the devices if necessary. You can use the filter option to search for the devices that you want. If you do not select any device, the selected mappings are deployed on all TrustSec devices.

You can use the Check Status option to check if different SGTs are assigned to the same IP address for a specific device. You can use this option to find the devices that have conflicting mappings, IP address that is mapped to multiple SGTs, and the SGTs that are assigned to the same IP address. This option can be used even if device groups, FQDN, hostname, or IPv6 addresses are used in the deployment. You must remove the conflicting mappings or modify the scope of deployment before deploying these mappings.

Verify TrustSec Deployment option on the General TrustSec Settings page helps you to verify whether the latest TrustSec policies are deployed on all the network devices. Alarms are displayed in the Alarms dashlet (under Work Centers > TrustSec > Dashboard), if there are any discrepancies between the policies that are configured on Cisco ISE and the network device. The following alarms are displayed in the TrustSec dashboard:

- An alarm with an Info icon is displayed whenever the verification process is started or completed.
- An alarm with an Info icon is displayed if the verification process is cancelled due to a new deployment request.
- If the verification process resulted in an error (for instance, failed to open SSH connection with the network device, or the network device is unavailable), or if there is any discrepancy between the policies that are configured on Cisco ISE and the network device, an alarm with a Warning icon is displayed for each of these network devices.

The Verify Deployment option is also available on the following pages:

- Work Centers > TrustSec > Components > Security Groups
- Work Centers > TrustSec > Components > Security Group ACLs
- Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix
- Work Centers > TrustSec > TrustSec Policy > Egress Policy > Source Tree
- Work Centers > TrustSec > TrustSec Policy > Egress Policy > Destination Tree

Check the Automatic Verification After Every Deploy check box if you want Cisco ISE to verify the updates on all the network devices after every deployment. When the deployment process is complete, the verification process is started after the time that you specify in the Time after Deploy Process field. The current verification process is cancelled if a new deployment request is received during the waiting period or when the verification is in progress. Click Verify Now to start the verification process immediately.

IPv6 addresses can be used in IP SGT static mappings. These mappings can be propagated using SSH or SXP to specific network devices or network device groups.

If FQDN and hostnames are used, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status. You can select one of the following options (under IP SGT Static Mapping of Hostnames) in the General TrustSec Settings window to specify the number of mappings created for the IP addresses returned by the DNS query:

- Create mappings for all IP addresses returned by DNS query
- Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query

Business Outcome

- Verifies TrustSec policy on Network Devices.
- Enhanced IP-SGT mapping workflow:
  - Improves network device misconfiguration error handling and operational efficiency through Check Status option.
  - Selectively deploy the IP SGT static mappings.
  - Create IP static mappings with IPv6 addresses.
  - Create mappings for first or all known IP addresses which are based on DNS FQDN query.

Decommissioned Dashlets

Some Dashlets Removed to Resolve Performance Issues

The following dashlets have been decommissioned to prevent performance issues when displaying large data sets:

- Context Visibility > Endpoint > Compliance: Status Trend
- Home > Endpoints > Endpoint Capacity

A large number of endpoints caused performance problems with some dashlets.

Kerberos Authentication for the Sponsor Portal

You can configure Cisco ISE to use Kerberos to authenticate a sponsor user who is logged onto Windows for access to the sponsor portal. This process uses the Active Directory credentials of the logged in sponsor user in the Kerberos ticket. Kerberos SSO is performed inside the secure tunnel after the browser establishes the SSL connection with Cisco ISE.

Additional security for Sponsor authentication.

NFS Repository Credentials

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

Business Outcome: Using credentials to connect to an NFS repository caused problems.

Known Limitations and Workarounds

LDAP Server Reconfiguration after Upgrade

Limitation

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

Condition

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

Workaround

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

Upgrade GUI Notification

Limitation

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

Condition

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

Workaround

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

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

For more information, see CSCvp78781.

PxGrid Certificate Requirements

Limitation

The certificate requirements have become stricter for the pxGrid service from patch 13.

If you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying patch 13. This is because the older versions of that certificate have the Netscape Cert Type extension specified as SSL Server, which now fails (because a client certificate is required).

You may see an empty list in the pxGrid Web Clients window (Administration > pxGrid Services > Web Clients).

Any client with a non-compliant certificate fails to integrate with Cisco ISE.

Condition

If you are using the Cisco ISE default self-signed certificate as the pxGrid certificate or the Netscape Cert Type extension in the certificate has only SSL Server specified in it, the certificate might be rejected by Cisco ISE after applying patch 13.

Workaround

Use a certificate issued by the internal CA or generate a new certificate with proper usage extensions:

- The Key Usage extension in the certificate must contain the fields Digital Signature and Key Encipherment.
- The Extended Key Usage extension in the certificate must contain the fields Client Authentication and Server Authentication.
- The Nestscape Certificate Type extension isn't required in the certificate. But if the extension is necessary, add both SSL Client and SSL Server in the extension.
- If you're using a self-signed certificate, the Basic Constraints CA field must be TRUE and the Key Usage extension must contain the Key Cert Sign. field.

Machine Authorization Fails

After applying patch 12, Authorizations fail for machine authentication using EAP-TLS, PEAP(EAP-TLS) and EAP-FAST(EAP-TLS). Cisco ISE is unable to retrieve machine account attributes and group memberships from Active Directory.

IP-SGT Bindings Are Not Propagated Under Certain Conditions

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

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

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

Workaround

Either:

1. Restart the ACI propagation in ISE and recreate the IP-SGT mappings.
    a. On the Work Centers->TrustSec->Settings->ACI Settings, uncheck "TrustSec-ACI Policy Element Exchange", and save.
    b. Check TrustSec-ACI Policy Element Exchange, and save.
    c. The connection between Cisco ISE and ACI is reestablished.
2. Delete the old IP-SGT bindings, and recreate them while Propagate to ACI is checked.

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

SXP Protocol Security Standards

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

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

Patch Build Download Using Chrome Browser

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

Radius Logs for Authentication

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

Profiler RADIUS Probe

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

High Memory Utilization

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

For more information, see CSCvn07836.

Diffie-Hellman Minimum Key Length

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

For more information, see CSCvi76985.

ECDSA Certificates

Limitation: Cisco ISE supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates with key lengths of 256 and 384 only.

Condition: ECDSA certificates that are used for EAP authentication are supported only for endpoints with Android Version 6.x and later.

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

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

Cisco Temporal Agent

We recommend that you run the Cisco Temporal Agent within two minutes of downloading the agent from the Client Provisioning Portal. Otherwise, the `Posture Failed Due to Server Issues` error message is displayed.

Mobile Service Engine (MSE) Devices

When adding an MSE device to Cisco ISE, you must copy the certificates from the MSE device over to ISE to facilitate authorization. ISE does not receive these certificates directly from the MSE device.

Re-create Supplicant Provisioning Wizard References

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

Endpoint Protection Services API

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

Server IP update under Trustsec AAA Server list

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

Upgrade Information

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

Applying Patches to Release 2.4

To obtain the patch file for Cisco ISE, Release 2.4, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software, and save a copy of the patch file to your local machine.

For instructions on how to apply the patch to your system, see the "Installing a Software Patch"section in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

For instructions to install a patch using CLI, see the "Install Patch" section in the Cisco Identity Services Engine CLI Reference Guide, Release 2.4.

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

Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions. Cisco ISE version 2.4.0.357 was the initial version of the Cisco ISE 2.4 release. After installation of the patch, you can see the version information from Settings > About Identity Services Engine page in the Cisco ISE GUI and from the CLI in the following format "2.4.0.357 patch N"; where N is the patch number.

Note Within the bug database, issues resolved in a patch have a version number with different nomenclature in the format, "2.4(0.9NN)" where NN is also the patch number, displayed as two digits. For example, version "2.4.0.298 patch 1" corresponds to the following version in the bug database "2.4(0.901)".

Note We recommend you to clear your browser cache after you install a patch on Cisco ISE, Release 2.4.

Upgrading to Release 2.4

You can directly upgrade to Release 2.4 from the following Cisco ISE releases:

- 2.0
- 2.0.1
- 2.1
- 2.2
- 2.3

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

If you are on a version earlier than Cisco ISE, Release 2.0, you must first upgrade to one of the releases listed above and then upgrade to Release 2.4.

Note It is recommended to upgrade to the latest patch in the existing version before upgrading to the next version of Cisco ISE.

You can upgrade to Release 2.4 from the GUI or the CLI. See, Cisco Identity Services Engine Upgrade Guide, Release 2.4

Verify Operating System of Virtual Machines

ISE Release 2.4 runs on Red Hat Enterprise Linux (RHEL) 7.0. If you are upgrading Cisco ISE nodes on a VMware VM, after you upgrade, ensure that you change the guest operating system to Red Hat Enterprise Linux (RHEL) 7. To do this, you must power down the VM, change the guest operating system to RHEL 7, and power on the VM after the change.

External RADIUS Token Server Timeout

External Radius Token Server Timeout maximum changed from 120 seconds to 60 seconds. Upgrades to this release change the existing setting, if the maximum is more than 60 seconds.

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.

After installing or upgrading, if there is any mismatch between the number of deployed VM nodes and installed VM licenses, alarms are displayed in the Alarms dashlet for every 14 days. Alarms are also displayed if there are any changes in the VM node's resources, or whenever a VM node is registered or de-registered.

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

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

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

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

For more information about the licenses, see the "Cisco ISE Licenses" chapter in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

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 12, telemetry is disabled immediately.

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, Release 2.4.

Client Provisioning and Posture Live Update Portals

You can download Client Provisioning resources from:

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

The following software elements are available at this URL:

- Supplicant Provisioning wizards for Windows and Mac OS X native supplicants
- Windows versions of the latest Cisco ISE persistent and temporal agents
- Mac OS X versions of the latest Cisco ISE persistent agents
- ActiveX and Java Applet installer helpers
- AV/AS compliance module files

For more information on automatically downloading the software packages that are available at the Client Provisioning Update portal to Cisco ISE, see the "Download Client Provisioning Resources Automatically" section in the "Configure Client Provisioning" chapter in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

You can download Posture updates from:

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

The following software elements are available at this URL:

- Cisco-predefined checks and rules
- Windows and Mac OS X AV/AS support charts
- Cisco ISE operating system support

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically" section in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

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/2.4.0.

Step 2 Provide your login credentials.

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

The following Offline Installation Packages are available for download:

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

Step 4 Click either Download or Add to Cart.

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

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

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

To download offline posture updates:

Procedure

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

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

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

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

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

Step 6 Click the Offline option.

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

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

Step 8 Click Update Now.

Configuration Prerequisites

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

See the following resources to configure Cisco ISE:

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

Monitoring and Troubleshooting

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

Ordering Information

For detailed Cisco ISE ordering and licensing information, see the Cisco Identity Services Engine Ordering Guide.

Cisco ISE Integration with Cisco Digital Network Architecture Center

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

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

Migration Information

For information on migrating from ACS to ISE, see the Cisco Identity Services Engine Migration Tool Guide.

Caveats

This section describes open severity 1 and 2 caveats and select severity 3 caveats. The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved. The bug IDs are sorted alphanumerically. 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, you must use the Bug Search Tool.

Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword. For more details on the tool, see the help page located athttp://www.cisco.com/web/applicat/cbsshelp/help.html.

New Features in Cisco ISE Release 2.4.0.357 - Cumulative Patch 14

Health Check

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

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

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

DNS Cache

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

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

service cache enable hosts ttl ttl

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

no service cache enable hosts ttl ttl

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

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

Business Outcome: Load on DNS Server is reduced.

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 14

The following table lists the resolved caveats in Release 2.4 cumulative patch 14.

Patch 14 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 2.2.0.53 or later.

Caveat ID Number	Description
CSCvf61114	ERS Update/Create for "Authorization Profile" failing the XML Schema Validation.
CSCvg50777	nas-update=true accounting attribute will cause session to not be deleted.
CSCvy05302	PxGrid certificate generation failing post rollback of patch containing nssdb format related changes.
CSCvh04231	Guest remember me radius accounting and access accept not sending guest username.
CSCvm62775	ISC BIND krb5-subdomain and ms-subdomain Update Policies Vulnerability.
CSCvn68614	Unable to use "connect-info" dictionary by default in Authorization Condition.
CSCvp07968	ISE Repository Password is accepted in GUI but not CLI.
CSCvp27534	Active endpoints missing from MNT session directory during 2.7 Longevity.
CSCvp55012	GNU Wget Buffer Overflow Vulnerability.
CSCvp86673	Application server stuck in Initializing due to corrupted indexes.
CSCvq12204	ISE 2.4 SNMPv3 user added with wrong hash after reload causing SNMPv3 authentication failure.
CSCvq44063	Incorrect DNS config can lead to TACACS or Radius authentication failure.
CSCvq48503	ISE False alarm - Health status unavailable.
CSCvq58506	Show running-config fails to complete.
CSCvr30644	glibc is affected by multiple vulnerabilities: CVE-2018-11236, CVE-2018-11237, CVE-2018-6485 and CVE-2017-16997.
CSCvr32299	Evaluate 32-bit glibc effected by RHSA-2018:0805 vulnerabilities.
CSCvr55906	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow Vulnerabilities CVSS v3.1 Base: 9.8

Caveat ID Number	Description
CSCvr57375	ISE 2.7 BETA: Username field in Self-Registration Portal Configuration is not saved.
CSCvr77653	cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow vulnerabilities.
CSCvr81463	libssh2 packet.c Integer Overflow Vulnerability CVSS v3.1 Base: 8.1
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 page
CSCvs52211	Update CiscoSSL to fix CSCvg56800 - Evaluation of ISE vulnerability nginx Oct 2017.
CSCvs96516	Multiple Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities.
CSCvs98602	X.Org libX11 Client Segmentation Fault Denial of Service Vulnerability.
CSCvs98604	X.Org libX11 Off-by-One Memory Write Arbitrary Code Execution Vulnerability.
CSCvt13719	pxGrid 2.0 WebSocket ping pong too slow even on idled standalone
CSCvt14248	Certificate Authority Service initializing EST Service not running after upgrade to ISE 2.6/2.7
CSCvt30558	Multiple Vulnerabilities found in python.
CSCvt43844	ISE: runtime-aaa debugs do not print packet details in ascii; breaking Endpoint debugs.
CSCvt44403	SSLDUMP() logs printed on Showtech via Audit logs causing showtech file to grow extensively.
CSCvt64739	Application Server takes more time to initialize
CSCvt65332	Description using two lines, or <Enter> was used, under Client provisioning resources throws errorA
CSCvt68108	ISE Server-side authorisation checks are insufficient
CSCvt75739	Heavy delay observed in sxp mappings when 50k acc packets with single SGT and VN are sent.
CSCvt81194	CPU spikes are being observed at policy HitCountCollector.
CSCvt82384	Dure to rotation of diagnostics, log is not working on ISE
CSCvu04874	Suspected memory leak in io.netty.buffer.PoolChunk.
CSCvu15948	TC-NAC adapter stopped scanning with nexpose (insiteVM).
CSCvu22058	ISE with DUO as External Radius Proxy drops access-reject.
CSCvu22259	CIAM: batik 1.7

Caveat ID Number	Description
CSCvu24402	CIAM: cups 1.6.3
CSCvu28305	ISE logging timestamp shows future date.
CSCvu31098	CIAM: libssh.
CSCvu31176	2.4P11 VPN + Posture : Apex Licenses are not being consumed.
CSCvu33416	License out of compliance alarm with a valid license.
CSCvu37728	CIAM: perl 5.14.1
CSCvu41815	[CFD] GBAC sync breaks on deleting VN from SG if AuthZ profile is mapped to the same VN for diff SG.
CSCvu45697	Compress messages.x files in the system.
CSCvu47395	ISE 2.x, 3.x : Drop_Cache required for systems with High Memory Issues
CSCvu53836	ISE Authorize-Only requests are not assessed against Internal User Groups.
CSCvu55557	Radius secret 4 chars min requirement is not checked when REST API used to create NAD
CSCvu58793	ERS REST API returns duplicate values multiple times when they are filtered by locations.
CSCvu58892	Update "master guest report" to "primary guest report" everywhere in the ISE UI + code.
CSCvu59038	Update "master/slave" terms to "primary/subordinate" in "show interface" command.
CSCvu59093	SessionDB columns are missing from ISE (>=2.4)
CSCvu70683	Alarm Suppression required for ERS queries along with suppression on iselocalstore.log
CSCvu84773	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvu90107	ISE allows duplicates device ID in ERS flow in all version.
CSCvu90703	CLDAP thread is hung and running infinite.
CSCvu90761	ISE Radius Live Sessions Page Showing No Data Found.
CSCvu91039	ISE 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.
CSCvu97657	ISE 2.4 Application server going to Initializing on enabling endpoint debugs.
CSCvv00377	Overlap of network devices using subnet and IP range.

Caveat ID Number	Description
CSCvv00951	App server crashes while transitioning into stopping state.
CSCvv07049	ISE - Unable to connect with an ODBC Identity Source - Connection Failed.
CSCvv08466	Log Collection Error alarms appear.
CSCvv08784	ISE:SEV2: Unable to restore backup of ISE 2.4 patch 12.
CSCvv09167	TACACS Aggregate table is not purged properly.
CSCvv09910	SYSAUX tablespace full despite fix for CSCvr96003.
CSCvv10683	Session Cache for dropped session not getting cleared; causing High CPU on the PSN's
CSCvv14001	ISE : Authzation profile not saved with proper attributes when Security Group selected under common tasks.
CSCvv14390	Max Sessions Limit is not working for Users and Groups.
CSCvv18119	ISE is selecting unsupported cipher in TLS Server hello packet.
CSCvv23256	ISE Authentication Status API Call does not return all records for the specified time range.
CSCvv25102	Modify TCP settings to enhance TACACS+ and TCP on ISE
CSCvv26811	Policy export is not being saved without encryption after it is saved with encryption.
CSCvv29190	BYOD Flow is broken in iOS 14 beta.
CSCvv29737	DNA ACA SG Sync fails with JDBCException:could not prepare statement.
CSCvv35921	Cannot start CSV exporting for selected user in internal ID Store.
CSCvv36189	Radius passed-auth live logs not sent due to invalid IPv6 Address.
CSCvv42857	MAC 11.x and its minor version support for ISE is not available.
CSCvv43383	NFS Repository is not working from GUI.
CSCvv43558	Evaluation of positron for Apache Struts Aug20 vulnerabilities.
CSCvv46034	Device admin service is getting disabled when updating TACACS configuration.
CSCvv46958	TrustSec enabled NADs not showing in trustSec Matrices when NDG column exceeds 255 characters.
CSCvv53221	ISE_EST_Local_Host RADIUS Shared Secret empty causes ISE application server 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.

Caveat ID Number	Description
CSCvv57639	Saving command with parenthesis in TACACS command set gives an error (ISE 2.7 p2).
CSCvv57830	Group lookup failed as empty value to be appended to the context.
CSCvv59233	ISE RADIUS Live Log details missing AD-Group-Names under other attributes section.
CSCvv60353	Authentication summary report gets stuck if the total records are more than 5M.
CSCvv62382	proxy bypass settings does not allow upper characters.
CSCvv67935	ISE - Security Group values in Authorization Profile disappear shortly after fetching.
CSCvv68756	Resource initialization failed (10) when failed to update User password in ISE via ERS API.
CSCvv72306	No password audit will be generated after changing ISE internal user password via Switch/Router CLI.
CSCvv77530	Unable to retrieve LDAP Groups/Subject Attributes when % chracter is used twice or more in bind password.
CSCvv85588	Memory Leak : High Allocation in by CAD_ValidateUser during PassiveID stress.
CSCvv91684	ISE Collection Filters will not be display in GUI.
CSCvv92203	ISE 2.6 P6/Unable to create SGT: NetworkAuthZProfile with entered name already exists.
CSCvv92638	Cannot configure scheduled config and operational backup with start date same as current day.
CSCvv94791	[CFD] ACA Sync broken - "Error occurs during migration: Waiting for Sync Runtime timed out"
CSCvw01829	ISE admin/portal Login with Chrome 85/86 could show error "Oops. Something went wrong."
CSCvw02887	Memory leak after adding AD Groups for passiv-id flow.
CSCvw06722	USID is found different when user login with Email/Userid when Ldap store is configured.
CSCvw08330	Posture does not work with dynamic redirection on 3rd party NADs.
CSCvw08602	Not Throwing error for ip overlap case.
CSCvw08765	Upgrade license check should check ISE DB for smart license registration.
CSCvw20636	Authorization Profiles showing "No data available" after NAD profile deleted.
CSCvw24268	Cisco Identity Services engine untrusted file upload vulnerability.
CSCvw25285	Passive ID is not working stable with multi-connect syslog clients.

Caveat ID Number	Description
CSCvw28441	NADs shared secrets are visible in the logs while using APIs.
CSCvw36743	ISE Service Account Locked and WMI not established due to special characters in password.
CSCvw53588	Multiple Vulnerabilities in jackson-databind.
CSCvw53701	XML external entity (XXE) vulnerability in the SqlXmlUtil code in Application.
CSCvw58824	XStream earlier to version 1.4.15 affected with multiple vulnerabilities.
CSCvw59855	In js/parts/SvgRenderer.js in Highcharts JS before 6.1.0, the use of backtracking regular expressions permitted an attacker.
CSCvw59920	Multiple Vulnerabilities in c3p0.
CSCvw61582	ISE 2.4 nf_conntrack_udp_timeout value is not updating from sysctl.conf
CSCvw61589	ISE Policy Evaluation : RADIUS requests dropped after deleting policy sets.
CSCvw64840	CIAM found mariadb vulnerable.
CSCvw68480	ISE incorrect number for the TOTAL field.
CSCvw68856	ISE: NTP service does not work after changing the hostname of ISE
CSCvw69054	Cross-site scripting (XSS) vulnerability in jsoup before 1.8.3.
CSCvw76847	ISE conditions Library corruption during Pen test.
CSCvw78269	CWE-20: Improper Input Validation for Create Node Group.
CSCvw81454	Cisco Identity Services Engine sensitive information disclosure vulnerabilities.
CSCvw82774	ISE 2.6/2.7 Sorting based on username does not work in User Identity Groups.
CSCvw82927	Cisco Identity Services Engine sensitive information disclosure vulnerabilities.
CSCvw83296	Cisco Identity Services Engine sensitive information disclosure vulnerabilities.
CSCvw83334	Cisco Identity Services Engine sensitive information disclosure vulnerabilities.
CSCvw87173	ISE 2.4 p13 break AD Authorization lookup for MAB authenticated endpoints.
CSCvw87175	MAB authentication via active directory passes with AD object disabled.
CSCvw89818	Cisco Identity Services Engine sensitive information disclosure vulnerabilities.
CSCvw93570	ISE 2.4 patch 8 Unable to edit,duplicate or delete guest portals.
CSCvw94096	iPod not shown as an option in ISE BYOD portal.
CSCvx15427	Health Checks:DNS Resolvability: False failures with ISE FQDN as CNAME (alias).
CSCvx15448	Health Checks:Disk space: insufficient failure info.

Caveat ID Number	Description
CSCvx23205	Add IdenTrust Commercial Root CA 1 Certificate to ISE truststore.
CSCvx36013	ISE Health Check Platform Support should update UI directly with results.
CSCvx37149	SGA value Under-Provisioned for SNS3515 running all personas on same node.
CSCvx50752	Add IdenTrust Commercial Root CA 1 Certificate for Smart Call Home and Smart Licensing.
CSCvx70327	Services not running after upgrade to 2.7

Known Limitations in Cisco ISE 2.4.0.357 Patch 14

Change in SNMP User Password Format and SNMP Hash Minimum Length

After applying Cisco ISE 2.4 Patch 14, 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.

Open Caveats in Cisco ISE Release 2.4 - Cumulative Patch 14

Caveat ID Number	Description
CSCvy53361	PAN login page times out after entering the credentials
CSCvy07333	Posture and BYOD flows impacted after patch installation
CSCvq43600	Disabled PSN persona but TACACS port 49 still open

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 13

The following table lists the resolved caveats in Release 2.4 cumulative patch 13.

Patch 13 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 2.2.0.53 or later.

Caveat ID Number	Description
CSCvd38796	No AD domain attributes retrieved for RA-VPN/CWA if AD used for both authC and authZ
CSCvi62805	CSCvi62805 ISE ODBC does not convert the mac address as per configured stored procedure
CSCvj95203	Matched Authentication rules in Monitor Only mode not showing in live log details page
CSCvm35110	MNT node not purging data diligently before hitting 90% purge data disk utilization
CSCvo05254	Improper format for email alerts containing the space character in the Suggested Actions section
CSCvo15781	Logwatch files are not capped for size
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 ...
CSCvp28377	Change in External admin permissions are not getting reflected in other nodes in deployment.
CSCvp59038	ISE Secondary PAN node sending RST to other ISE node with src ip address 169.254.2.2
CSCvp85813	ISE TACACS livelogs does not have the option to filter using specific NAS ip address.
CSCvq07619	GnuPG Filename Status Message Spoofing Vulnerability
CSCvq43600	Disabled PSN persona but TACACS port 49 still open.
CSCvq48396	Replication failed alarm generated and ORA-00001 exceptions seen on ise-psc.log
CSCvq73677	GNU patch OS Shell Command Injection Vulnerability
CSCvq86741	FasterXML jackson-databind logback-core Class Polymorphic Deserializ ...
CSCvq86746	Multiple Vulnerabilities in jquery - guest portals
CSCvq90601	EAP Chaining: Dynamic Attribute value is unavailable
CSCvr09749	GNU patch do_ed_script OS Shell Command Execution Vulnerability

Caveat ID Number	Description
CSCvr19392	Apache Commons Beanutils PropertyUtilsBean Class Property Suppression Vulnerability
CSCvr33083	ISE Application configure ise > 16 (Generate Endpoints Report) returns a long list of errors
CSCvr47732	FasterXML jackson-databind Polymorphic Typing Vulnerability CVSS v3.1 Base: 9.8
CSCvr47790	Apache Commons Compress File Name Encoding Algorithm DoS Vulnerability CVSS v3.0 Base: 7.5
CSCvr68432	2.4P10 Endpoint added via REST has visible policy assignment only in "edit" mode
CSCvr77676	libmspack chmd_read_headers Function Denial of Service Vulnerability
CSCvr81384	Failing Network Devices CSV import, process silently aborting without reason
CSCvs09981	Add the capability to filter out failed COA due to MAR cache checks among group nodes in ISE
CSCvs42441	Service account passwords returned from server in SMS and LDAP page
CSCvs44006	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvs53606	ISE 2.4: Administrator Login Report, Auth failed when using cert based admin auth
CSCvs62081	collector log filled with repeated pxGrid and DNAC messages
CSCvs62597	Authz Profiles not pulling properly using REST API (Pagination is missing)
CSCvs69726	ISE 2.2+ affected with memory leak. Everyday 1-2% increase in native memory by PORT_Alloc_Util()
CSCvs75274	Unable to do portal customization for "certificate provisioning portal"
CSCvs83303	API is not retrieving the data when interim-updates are not stored DB
CSCvs84948	Multiple Vulnerabilities in binutils
CSCvs86686	Multiple Vulnerabilities in patch
CSCvs86690	Multiple Vulnerabilities in python
CSCvs86697	Multiple Vulnerabilities in sudo
CSCvs88222	Vulnerability in unzip package - RHEL 7
CSCvs89440	CEPM schema stats not collected/scheduled for PAN only node
CSCvs97302	.dmp files not deleted from /opt/oracle/base/admin/cpm10/dpdump even after the reset-config on ISE
CSCvt03094	ISE expired TACACS sessions are not cleared in a timely manner from session cache

Caveat ID Number	Description
CSCvt03935	Change "View" Options Wording in TrustSec Policy Matrix--ISE
CSCvt04047	POST getBackupRestoreStatus occures on every ISE page after navigating to Backup/Restore menu
CSCvt11179	"AD-Operating-System" attribute is not being fetched when this OS attribute changes on the AD Server
CSCvt13707	pxGrid 2.0 WebSocket distributed upstream connect issue
CSCvt15787	TCPDump - Node and Interface field Unavailable
CSCvt15893	Preventive bug :Radius Errors/Misconfigured supplicants tables do not exist after upgrade to ISE2.6
CSCvt17283	GUI Slowness while enabling AVC
CSCvt30418	ISE 2.4 p 10 email notification stops
CSCvt34876	ISE latency in responding to RADIUS and high CPU
CSCvt35044	EP lookup takes more time causing high latency for guest flow
CSCvt36322	ISE 2.6 MDM flow fails if redirect value is present in the URL
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.
CSCvt45661	Multiple Node.js vulnerabilities
CSCvt46584	Backups failing due to disk space issue not purged ENDPOINTS_REJECT_RELEASE table
CSCvt46850	Unavailability to edit saved compound conditions using conditions library.
CSCvt49961	Syslog Target configured with FQDN can cause Network Outage
CSCvt51248	Multiple Vulnerabilities in rabbitmq
CSCvt53541	SMS over HTTPS is not sending username/password to gateway
CSCvt57027	Authentication Status API call on ISE 2.6p5 returns blank output
CSCvt57805	Intermittent password rule error for REST API Update Operation
CSCvt61181	ISE ERS API - GET calls on network devices is slow while processing SNMP configuration
CSCvt65853	ISE-2.x || MNT REST API for ReAuth fails when using in distributed deployment
CSCvt69941	ISE 2.6 Redundant "Application patch install has completed successfully" Alarm

Caveat ID Number	Description
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'.
CSCvt73953	Mismatched Information between CLI export and Context Visibility
CSCvt80285	Cannot select 45 or more products 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
CSCvt91871	ISE RADIUS Accounting Report details shows "No data found" under Accounting Details
CSCvt93117	ise-psc.log filled up with "check TTConnection is valid" causing relevant logs to roll over
CSCvu04874	suspected memory leak in io.netty.buffer.PoolChunk
CSCvu05164	ISE is not allowing to disable Radius in NAD via API
CSCvu10009	Mandatory values when using Update-By-Name method with Internal Users
CSCvu13368	ISE : Oracle process reached limit : causing multiple issues
CSCvu25625	ISE is returning an incorrect version for the rest API call from DNAC
CSCvu26008	portal page customisation changes are not reflecting in certificate provisioning portal
CSCvu30286	ERS SGT create is not permitted after moving from Multiple matrix to Single matrix
CSCvu31853	NDG added through ERS became associated with all network devices in DB
CSCvu32240	When running ISR ERS API for internaluser update the existing identityGroups value is set to null
CSCvu33861	ISE 2.4 p6 - REST API MnT query to get device by MAC address taking more than 2 seconds
CSCvu35506	code for securityGroupAclTopic missing from 2.4 and 2.6, but topic still advertised
CSCvu35802	Shared email for AD users fail to retrieve groups,ISE shows multiple account found in forest
CSCvu39653	Session API for MAC Address returning Char 0x0 out of allowed range
CSCvu39890	ISE - Rollback stuck indefinitely attempting to rollback from Patch 12
CSCvu42244	Machine authentication via EAP-TLS is failing during authorization flow with user not found error

Caveat ID Number	Description
CSCvu49724	Devices configured SNMP v2c version on DNAC is not seen on Network devices in ISE
CSCvu91016	InternalUser Attributes in ATZ policy will fail TACACS+ ASCII Authentication
CSCvu97041	Restore of Config backup on ISE 2.6 P7 is causing issues with node registration
CSCvs91408	Significant memory increase in PMNT node of longevity test
CSCvu49019	Suspected Memory Leak in Elastic search

New Features in Cisco ISE Release 2.4.0.357- Cumulative Patch 12

Telemetry

Cisco ISE securely collects nonsensitive information about your deployment, network access devices, profiler, and other services that you are using by using the Telemetry feature. This data is 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 Success Diagnostics > Telemetry. The account is unique to each deployment. Each admin user need not provide it separately.

Telemetry is used to improve the 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.

Note Cisco ISE 2.4 Patch 12 and later will not send Telemetry data to Security Service Exchange (SSE) and Smart Call Home (SCH).

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 12

The following table lists the resolved caveats in Release 2.4 cumulative patch 12.

Patch 12 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 2.2.0.53 or later.

Caveat ID Number	Description
CSCvb55884	ISE RBAC Network Device Type/Location View not working
CSCvd16468	Missing NAD info in Alarm "Unknown SGT was provisioned"
CSCve89689	MNT API does not support special charactor
CSCvf94942	Enhance error message when perform command authz and no command set
CSCvi42112	ISE - DHCP Scope responding with 1 day lease instead of 15 seconds

Caveat ID Number	Description
CSCvj47301	ISE sends CoA to active-compliant sessions when a node-group member is unreachable
CSCvj67166	Supported server ciphers for TLSv1.2 need 2048-bit option
CSCvj67437	Multiple Vulnerabilities in procps-ng
CSCvk05318	Error Deploying IP SGT static Mapping on ISE
CSCvk48115	ISE 2.3 RSA SecurID authentication fails
CSCvm06398	36xx SNMP sysObjectID shows 3315
CSCvm15495	Evaluation of positron for CVE-2018-5391 (FragmentSmack)
CSCvm73337	Remove ciphers with Diffie-Hellman moduli size less than or equal to 1024 bits for SSL connections
CSCvn12644	ISE Crashes during policy evaluation for AD attributes
CSCvn73729	Error occurred in publishing threat events - AMP adapters
CSCvo47391	Multiple Vulnerabilities in krb5
CSCvo51415	ISE 2.4 URT fails with cert error
CSCvp20910	Cisco Smart Licensing cloud agent in waitings state causes GUI login delay in ISE 2.2
CSCvp24085	ISE 2.4 High CPU utilization on Secondary Admin Node
CSCvp52008	IETF Dictionary Attribute Ascend-Client-Primary-DNS broken after upgrade
CSCvp73335	Radius session detail report are broken if calling-station-id contains CLIENTVPN
CSCvq13431	ISE PSN node crashing while fetching context attributes during posture plus RADIUS flow
CSCvq19646	Evaluation of positron for TCP_SACK
CSCvq38599	Unable to update send from(Send configuration changes to device) attribute using CSV file.
CSCvq56281	ISE Guest portal fails to parse http request with two questions marks
CSCvq61089	My Device Portal does not show a device after BYOD on-boarding with SAML authentication
CSCvq61878	Evaluation of ISE for CVE-2018-20685
CSCvr13481	ISE ERS SDK NetowrkDeviceGroup DELETE does not specify ID location
CSCvr25184	Partitions are not clearing properly for tmp
CSCvr32199	systemd vulnerabilities RHEL 7 RHSA-2019:0049

Caveat ID Number	Description
CSCvr32475	kernel (RHSA-2018:3083) vulnerabilities
CSCvr32485	kernel CVE-2018-14634 (RHSA-2018:2748)
CSCvr33160	PassiveID livesessions showing is without enabling PassiveID funcationality.
CSCvr39943	Blank Course of Action for Threat events received from CTA cloud to TC-NAC adapter
CSCvr40545	EAP-FAST authentication failed with no shared cipher in case of private key encryption failed.
CSCvr44495	pxGrid Arab Bank defensive code change
CSCvr56785	Localdisk size needs to be increased to accommodate large corefiles
CSCvr60339	Typo in Max Sessions Page on Counter time limit tab
CSCvr63504	Unable to delete SCEP profile because it is referencing system certificates
CSCvr68971	ISE IP routing precedence issue
CSCvr70044	" No policy server detect" on ISE posture module during high load .
CSCvr84125	Config restore from one platform on another platform set incorrect UDI in sec_hostconfig table
CSCvr84143	tzdata needs to be updated in ISE guest OS
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
CSCvr85513	core file generated on PSN
CSCvr87936	Valid Base and Plus licenses show out of compliance
CSCvr95948	ISE fails to re-establish External syslog connection after break in connectivity
CSCvr96189	NDG device references not cleaned out of ISE DB, preventing NDG deletion
CSCvs01924	ERS Admin account disabled incorrectly due to password expiry
CSCvs02166	API calls show different result as GUI
CSCvs03810	ISE doesn't display the correct user in RADIUS reports if the user was entered differently twice
CSCvs03998	ISE 2.3 p 6 LDAP test GUI flow with multiple results does not generate error observed in runtime
CSCvs04047	Authorization Profile created using ERS API does not match with 'ASA VPN' field in GUI

Caveat ID Number	Description
CSCvs04226	Journal logs are not compressed / rotated when system reaching SystemMaxUse #200 MB in ISE 24P10
CSCvs04384	Internal user's custom attributes fields are empty while creating through ERS API
CSCvs04433	ISE : TACACS : PSN crashes for TACACS+
CSCvs05104	Set max time frame to 60 mins when EndPoint default interval disabled
CSCvs05260	App server and EST services crash/restart at 1 every morning
CSCvs07344	ISE: Reset config on 2.4 patch 9 throws some errors despite finishing successfully.
CSCvs09619	Live log details not working and showing blank for Dynamic authorization
CSCvs12409	ISE Guest creation API validation for Guest Users valid Days doesn't take time into account
CSCvs14297	PassiveID: Configuring WMI with an AD account password that contains a $ will result in an error.
CSCvs23628	Policy engine continues to evaluate all Policy Sets even after rule is matched
CSCvs24704	LDAP ID store corruption alarm - Enhancement
CSCvs25258	Improve behavior against brute force password attacks
CSCvs25569	Invalid root CA certificate accepted
CSCvs36150	ISE 2.x Network Device stuck loading
CSCvs38883	Trustsec matrix pushing stale data
CSCvs39633	NAD group CSV imports should allow all supported characters in description field.
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
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
CSCvs44795	ISE not updating SGT's correctly
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

Caveat ID Number	Description
CSCvs51519	NFS mounting causes crash
CSCvs51537	Backups are not triggering with special characters for encryption key
CSCvs52031	MACAdress API is not working(API/mnt/Session/MACAddress)
CSCvs53030	SessionDirectory values having lower on ISE3595
CSCvs53148	Multiple EP's profiled every second causing ISE nodes to go out of sync
CSCvs55464	Creating a new user in the sponsor portal shows "invalid input"
CSCvs55594	Days to Expiry value, marked as 0 for random authentications
CSCvs58106	NAD CSV imports should allow all supported characters in the TrustSecDeviceID
CSCvs60518	ISE Admin User Unable To Change The Group For Internal Users
CSCvs62586	Tacacsprofile not retrieved properly using REST API
CSCvs65467	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvs65989	After importing network device / groups, unable to add new Location
CSCvs67042	ISE 2.2+ affected with memory leak. Everyday 1-2% increase in native memory due to Inflater()
CSCvs67785	Days duration is not getting updated in portal page customization for self registration portal
CSCvs68914	Errors when SG created using _ underscore sent from DNAC
CSCvs70863	ISE 2.6 - Cannot enable FIPS if Default Device Admin has been modified
CSCvs70997	ISE: 2.4p9 Intermediate CA cert not installed when configuring SCEP RA
CSCvs76257	ISE crashes due to empty string instead of username in RadiusProxyFlow::stripUserName()
CSCvs78160	URT fails on a ConditionsData clause from INetworkAuthZCheck
CSCvs82557	SXP Bindings are not published to pxGrid 2.0 clients
CSCvs83604	authenticationSettings: networkProtocol is required after ISE 2.4 patch 11
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)
CSCvs86775	ISE 2.6 Install: Input Validation- Check IP Domain Name
CSCvs88368	ISE SNMP server crashes when using Hash Password.

Caveat ID Number	Description
CSCvs91808	Importing metadata xml file with special characters results in unsupported tags error
CSCvs96541	ISE 2.4 P11 On OP Backup Restore, EPOCH_TIME column is removed
CSCvt00283	404 error upon refresh of success page of guest sponsored portal
CSCvt03292	Cert Revoke and CPP not functioning without APEX license.
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
CSCvt10214	[ENH] Add the ability to "GET|PUT|DELETE by Name" using the API for network devices
CSCvt12236	IP SGT static mapping import not working correctly with hostnames
CSCvt13746	ISE doesn't display all device admin authz rules when there are more authz policies and exceptions
CSCvt15256	Authentication goes to process fail when "Guest User" ID Store is used.
CSCvt15935	PERMGEN configured instead of metaspace for JDK8
CSCvt16882	When accessing the portal with iPad using Apple CNA and AUP as a link we get 400 Bad Request error.
CSCvt17783	ISE shouldn't allow ANY SGT or value 65535 to be exposed over SGT import or export
CSCvt24276	Cannot add/modify allowed values more than 6 attributes to System Use dictionaries
CSCvt36117	Identity group updates for an internal user in ISE
CSCvt36324	Hostname goes missing from CARS configuration
CSCvt37910	[ENH] Add the ability to "GET|PUT|DELETE by Name" using the API for /ers/config/internaluser
CSCvt56332	Getting a blank page when clicked on new or edit icon in SMS gateway
CSCvt69912	ISE still generates false positive alarm "Alarms: Patch Failure"
CSCvt79223	MNT DB reset fails on 2.4 p11
CSCvr96003	SYSAUX tablespace is getting filled up with AWR and OPSSTAT data.
CSCvr63698	pxGrid 2.0 authorization profile attribute missing from the session directory

Open Caveats in Cisco ISE Release 2.4 - Cumulative Patch 12

Table 3: Open Caveats in Cisco ISE Release 2.4 - Cumulative Patch 12

Caveat	Description
CSCvu42244	Machine Authentications via EAP-TLS is failing during authorization flow with user not found error. Please see the Known Limitations and Workarounds, on page 12 section.

New Features in Cisco ISE Release 2.4.0.357- Cumulative Patch 11

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 2.4.0.357- Cumulative Patch 11

The following table lists the resolved caveats in Release 2.4 cumulative patch 11.

Patch 11 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.0.53 or later.

Caveat ID Number	Description
CSCux25333	Carlsbad Dashboard allows special characters: <>?"'
CSCux25342	Custom filters not working for Session status column in Live Sessions
CSCuz18895	CoA REST API is not working for ASA VPN Sessions
CSCvb56579	SXP Devices page - can't show all the name after 14 chars
CSCvf59076	Live sessions show incorrect Authorization profile and Authorization Policy for VPN+Posture scenario
CSCvg03526	Patch installation might generate alarm Application patch installation failed
CSCvh80768	ISE 2.3 no patches, unable to login to sponsor portal with internal user
CSCvh95236	ISE sends CoA after receiving a RADIUS Accounting-STOP

Caveat ID Number	Description
CSCvj24944	ISE Network conditions with device,port being skipped during authz
CSCvj43999	Self-signed account creation error: "An attempt to text your account information to you has failed"
CSCvj73002	Change Audit config is not showed for the users when edit and change the status
CSCvj87369	ISE Cannot Schedule a report the same day
CSCvk50684	Not able to delete certificate after hostname change
CSCvm05519	Message Class for EAP-TLS messages from System-Management to EAP
CSCvm56657	Windows 7 device is profiled wrongly post Posture flow, due to anyconnect sending wrong useragent
CSCvm89187	Config restore is struck in the UI forever, while restoring backup taken on the same node
CSCvn06056	Alarm TrustSec SSH connection failed needs to be provide more details on NAD
CSCvo31313	change password for few of the internal users not working after upgrade to 2.6
CSCvo49755	To enable CLI clock timezone command
CSCvo73749	'MAR cache distribution is not enabled' even when it has been enabled.
CSCvo87602	Memory leak on ISE node with the openldap rpm running version 2.4.44
CSCvo90281	Patchupload files >1 G don't get deleted when upgrading if upload through WebGUI interrupted
CSCvp19539	ISE 2.2 Sign On Button grey out with Guest portal second factor Radius Token server authentication
CSCvp19738	ISE 2.4 Live Sessions Cannot Filter on Policy
CSCvp27487	Secure Syslog Audit for CLI Authentication Failure Suspend/Lock Account
CSCvp30790	Generate a singlecertificate(with CSR) option in pxgridserivces with PKCS8format throws error.
CSCvp35021	In Deployment, when external CA signs any system certificate allows to delete CA from trusted page.
CSCvp56265	Unable to disable MDM server if configured server is not reachable
CSCvp70644	Expired guest accounts purge is stuck after daylight time change
CSCvp83214	ISE ERS Create via the API does not use the specified ID
CSCvq07756	Network device Import to ISE when having IPV6 address, takes too long to import the devices

Caveat ID Number	Description
CSCvq21272	Wrong password being notified after password reset (Only on SMS)
CSCvq30417	MnT Purge with option to export repository not working
CSCvq36398	Vulnerability Evaluation for ISE
CSCvq40899	when binding external ca sign cert in intermediate CA CSR,certificate chain has broken under CA page
CSCvq49292	ISE TACACS Authentication and accounting reports older than 30 days missing
CSCvq50182	ISE does not show logging when CTS pac is expired
CSCvq66846	Move to Mapping Group drop down menu limits SGT Mapping groups to 25
CSCvq69142	PassiveID Agent: No Syslog message is sent to MnT when the agent monitoring DC goes down
CSCvq69228	pxGrid controller contacting terracotta.org
CSCvq73316	ISE 2.4p9 Grace period is not working with PRA with VPN usecase
CSCvq74649	ISE sponsor portal - sorting by creation date doesnt work
CSCvq77051	Network devices added via restful API fails authentication with a 'Network Device not located' error
CSCvq79598	IPv6 RADIUS attributes cannot be mapped to any External attribute
CSCvq80132	Trashing IP SGT Static mappings across pages never completes
CSCvq80211	IP SGT static mapping export fails for entries with no mapping data
CSCvq81381	Internal user using token password will be disabled due to password expired
CSCvq83410	Maximum thread value limit is too low and triggers 'Admin thread pool reached threshold value' alarm
CSCvq83700	Remove Unnecessary JQUERY-UI Files from ISE
CSCvq85414	Login page AUP as link does not work with iOS CNA browser
CSCvq86848	Move devices to another group botton should be disabled when access has been restricted to NDG
CSCvq88821	SNMP traps on access switch connected to APs causes incorrect profiling.
CSCvq96801	All SNMP packets are logged to /var/log/messages file
CSCvq97641	ISE 2.4 localhost-<date>.log files growing upto and more than 8 Gb in size
CSCvq97680	ISE 2.6 Patch 2: EAP-TLS auth not matching endpoint groups

Caveat ID Number	Description
CSCvq98277	No password audit will be generated after user change ISE internal user enable password via ASA CLI
CSCvq99963	App Server crash observed while being passiveid dashboard for some time with > 200K activesessions
CSCvr00348	Posture assessment by condition report is showing empty records.
CSCvr05165	DCS Probe data notification missing endpoint attributes in the message
CSCvr06487	ISE Posture Agent Profile does not allow blank remediation timer
CSCvr07263	when creating Purging Rule ,Radius directory will hang if there is no plus license
CSCvr07294	Radius Authentication and Radius Account Report performance is slow
CSCvr08988	in ex-Radius scenario ,ISE should replace state attribute before forwarding access challenge to NAD
CSCvr09759	Certificate is not loading from Oracle to NSSDB properly
CSCvr11769	ISE 2.4: Advanced Custom Filter option and export of reports not working as Expected
CSCvr12350	ISE : "MDM: Failed to connect to MDM server" log entry needs to have endpoint information
CSCvr13218	Framed-Interface-Id RADIUS attribute not sent in access-accept if IPV6 address is in ::xx format
CSCvr13444	REST API: Create Network Device with special character ("\") in password field is interpreted as utf
CSCvr13464	ISE ERS SDK NetworkDeviceGroup PUT does not show ID placement in the API call
CSCvr13649	pxGrid XMPP GCL Reconnect failure
CSCvr24458	Network Device POST API allows for characters and spaces in Model name of device, GUI does not
CSCvr25197	After changing password via UCP, "User change password audit" report doesn't have "Identity"
CSCvr29863	Validation needed RADIUS Cisco DNA Center-ISE REST call sp. char (&) and (\) in shared secret fails
CSCvr31312	Legacy | ISE fails to load N/w devices page while filtering on IP/Mask
CSCvr35154	ISE: Read-only admin users are able to view TrustSec device configuration credentials
CSCvr35719	Unable to get all tenable adapter repositories
CSCvr38857	Radius Authentication report missing log, if custom Filter Used

Caveat ID Number	Description
CSCvr40359	ISE not using the device-public-mac attribute in endpoint database
CSCvr40574	Export failed in ISE gui in case of private key encryption failed no ERROR msg in ISE GUI
CSCvr41265	ISE 3695 appliance is having issue with Oracle parameters configured for super MNT
CSCvr43077	Day0: iPad OS 13.1 BYOD flow got failed
CSCvr46529	Password lifetime expiration reminder appears for Internal Users with external passwords
CSCvr48043	Multi Shared Secret Field is being populated for exported TACACS devices
CSCvr48101	Unexpected COAs may be observed with SCCM MDM
CSCvr48729	Unable to access My Devices portal
CSCvr50921	GUI login with AD user failing when similar internal user is disabled
CSCvr51959	ISE 2.4 Not entire fqdn is matched, but fragment of characters
CSCvr53428	ISE services are not coming up after installing patch 2.3 p7
CSCvr57378	DHCP messages are marking endpoints active increasing the active endpoint count
CSCvr62517	ISE 2.4 p9 Session directory write failed : String index out of range: -1
CSCvr67988	ISE sponsor's e-mail gets CC'd even when view/print guests' passwords is disabled
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
CSCvr77321	WSA receives SIDs instead of AD groups from ISE
CSCvr81522	Definition date for few AM product like mcafee and symantec is listed false
CSCvr86380	Replication alarm when trustsec matrix CSV imported with EMPTY SGACL that is already EMPTY in GUI
CSCvr98395	No profiling CoA for ip based profile policy
CSCvs40813	Missing the following properties in platform.properties for <sns3615> ,<sns3655> <sns3695>

New Features in Cisco ISE Release 2.4.0.357- Cumulative Patch 10

Enable Probe Data Publisher

This option is newly added in the Profiler Settings window ((Work Centers > Profiler > Settings). This option is disabled by default. Enable this option if you want Cisco ISE to publish endpoint probe data to pxGrid

subscribers that need this data to classify endpoints onboarding on ISE. The pxGrid subscriber can pull the endpoint records from Cisco ISE using bulk download during initial deployment phase. Cisco ISE sends the endpoint records to the pxGrid subscriber whenever they are updated in PAN.

Note When you enable this option, ensure that the pxGrid persona is enabled in your deployment.

Multi DNAC Support

Cisco DNA Center systems cannot scale to more than 25K to 100K endpoints. The Cisco Identity Service Engine can scale to 2 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.

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 10

Patch 10 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.1.53 or later.

The following table lists the resolved caveats in Release 2.4 cumulative patch 10.

Caveat ID Number	Description
CSCvd48081	The software shouldn't allow to delete the pxGrid certificate on a ISE node
CSCvf36221	posture update not working when there's a proxy with credentials in ISE
CSCvf45991	Pseudo double Auth request on AD
CSCvf91219	ISE T+ and Policy : Allowed protocols for RADIUS uncheck if changes are made via TACACS PE section
CSCvg60477	ISE 2.3+ does not have authentication condition Network Access:AuthenticationMethod
CSCvh86082	Parsing NMAP smb-os-discovery data should remove
or \x00
CSCvi16994	ERS Guest User operations fail with 401 Unauthorized if Sponsor_Portal_Sequence missing
CSCvi17935	ISE 2.x: Mobile/Desktop previews don't display self-registration form fields correctly
CSCvi18412	ISE 2.3 p2 is sending redundant CoA message during VPN Posture Flow
CSCvi29474	ISE2.3 portals not displaying Spanish Accents
CSCvi50874	Endpoint Oracle Persist Received value wrongly counted in ISE Counters report
CSCvi72862	ISE : Accounting updates tolerance for suppression needs to be more efficient.
CSCvi86385	Is ISE affected by Spring Framework CVE-2018-1270
CSCvi99138	ad_agent.log flooded with entries from blocked list domains

Caveat ID Number	Description
CSCvj07166	ISE RBAC unable to modify nested permissions after migration from ACS
CSCvj34578	REST API GET DACL page filter does not show correct information
CSCvj61028	ISE HTTP error 401 unauthorized on External CA UI
CSCvj88164	Remote-Access VPN Posture Sessions showing Base license consumed but no Apex
CSCvk01929	Making name changes to the "All_User_ID_Stores" Identity Source Sequence will break new policy sets.
CSCvk52803	Different FQDN in SAN can cause CV issue
CSCvk53782	ISE ENH : Allow RADIUS Dictionary VSA "Vendor Attribute Size Field Length" of 2 bytes
CSCvk56913	Cannot edit Guest group if accesing through Manage accounts
CSCvm10275	Cisco Identity Services Engine Cross Site Scripting Vulnerability
CSCvm70858	Triggered SNMP query not working properly for HP OUI
CSCvn31337	ISE: Exception thrown while adding email address in NTP Service Failure alarm
CSCvn66106	ISE custom attributes not being applied to endpoint when pushed from cloudpost IND
CSCvn73740	EAP-TLS authentications with Endpoint profile set to not unknown fails in second authorization.
CSCvo04342	Multiple Vulnerabilities in jackson-databind
CSCvo64085	The caluclation of required space for MNT backup need to be revalidated.
CSCvo75129	Runtime prepends "\" to ";" in dhcp-class-identifier in syslog message sent to profiler
CSCvo77219	Sponsor guest portal rate limit time not honored
CSCvo80291	pxGrid startup order causing profiler code to fail init
CSCvo82930	ProfilerCoA:- Exception in getting Policy details Exception : in Infinite Loop in Profiler.log
CSCvo90380	Sponsored Guest account start date not adjusting when account extend
CSCvo94666	ISE 2.4 P5 : Profiling : Netflow probe not working on ISE Bonded Interface
CSCvp00421	ISE Profiler SNMP Request Failure Alarms should show the reason of failure
CSCvp01553	No serialization or batching when large scale(>300) NADs are moved between MatrixA to MatrixB
CSCvp03249	ISE: SMTP server sending Email notification gets Exhausted
CSCvp22075	ERS API that requires CSRF token always failing on PUT/POST/DELETE

Caveat ID Number	Description
CSCvp30958	ISE dropping requests due to descriptor allocation exhaustion under external server latency scenario
CSCvp40509	Internal User not found in prrt-server intermittently even though PrRTCpmBridge returns user found
CSCvp46165	Posture redirect fails with error 'unable to determine peer' in AnyConnect_ISEPosture.txt
CSCvp47029	ISE 2.4 With CTA threat, threat endpoints are not detecting
CSCvp54424	AD Diagnostic tool shows low level API query failed w/ Response contains no answer. Check DNS config
CSCvp54773	ISE 2.4 p6 400 error on sponsor portal after timeout.
CSCvp58616	SQLite FTS3 Query Processing Integer Overflow Vulnerability
CSCvp61880	Authorization profile fails to import with no warnings or errors to user
CSCvp68285	AUP guest portal error 400 when retrun from contact support link (iphone captive portal)
CSCvp72966	Email not received to guest if view/print guest password disabled
CSCvp73385	Authentications start failing once AD throws KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
CSCvp74154	Unable to remove an endpoint from the endpoint database due to permission error
CSCvp75207	2.4 P8/P9 Certificate chain does not get imported to Patch 8 and Patch 9
CSCvp76617	ISE customer endpoint attribute type string doesn't allow certain numbers
CSCvp77014	ISE trustsec custom view doesn't sort properly with manual order
CSCvp77941	License usage for Plus either shows 0 or incorrect value
CSCvp83006	Export from Context Visibility-Endpoints does not contain Custom Attr for most of Endpoints
CSCvp88242	[400] Bad Request error when refreshing the Mydevice portal
CSCvp88443	ISE CoA is not sent even though new Logical Profile is used under Authz Policy Exceptions
CSCvp88940	Can't use endpoint group description during runtime for authz profile
CSCvp91987	Wrongly job (HOURLY_STATS_JOB) running
CSCvp98851	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvq00186	ISE 2.4 fails to match authorization rules after deleting authorization condition
CSCvq13341	ISE 2.6 patch 1 - AD User Test is returning 0 groups

Caveat ID Number	Description
CSCvq14925	Renewed self-signed certificate doesn't get updated in trusted store
CSCvq17464	Cannot Update Internal User with External Password ID Store via ERS--ISE
CSCvq19039	ISE fails to save configuration changes for large policy-sets
CSCvq24877	Create Failing with ORA-02291 on CEPM.REF_ROLE_MASTER if groupId w/ prepending/trailing spaces
CSCvq27110	Core files on PSN servers causing High Disk Utilization alarms
CSCvq29336	ISE shows "Oops. Something went wrong" if session ID contains "-"
CSCvq35826	Incorrect audit report while updating Counter Time Limit in Max Sesssions page
CSCvq39759	ISE PAN failover inactive days = elapsed days causing incorrect purging of EP's.
CSCvq45008	ISE doesn't store self-registered EndPoints in configured custom group
CSCvq46232	ISE 2.6 ACI integration Trustesec ACI report doesn't have sent ip-sgt mappings to ACI
CSCvq50088	Export function in Network device groups fails when using RBAC
CSCvq51955	Network Conditions do not work with shorten IPv6
CSCvq52340	'Deleting All' Network Access Users doesn't appear on audit report
CSCvq54533	Using ECDSA signed certificates with the admin or pxgrid usage breaks pxgrid
CSCvq56241	ISE user import does not fail when username contains invalid characters
CSCvq58785	Static group information is lost from EP in some scenarios
CSCvq62367	PSN generates scheduled reports if no connectivity to MNT
CSCvq71264	Static group assignment losing from guest flow
CSCvq71844	"Cache not properly initialized" message in every Profiler Policy and cannot update Profiler Feed
CSCvq72760	When updating password for administrative user it is possible to bypass entering current password
CSCvq73457	Under heavy load, ISE live logs either unavailable or delayed
CSCvq74995	ISE 2.4 Possible XSS input in Certificate Attributes message when "/" sign is in the name
CSCvo07993	Qualys show connected state once disable/enable tc-nac if added before applying patch.
CSCvq38610	Certificate trust chain is incomplete for pxGrid on pxGrid alone persona

Caveat ID Number	Description
CSCvn45977	Allowing Different FQDN in SAN DNS field for EAP Certificate.
CSCvp63038	System Test: Temporial agent instalation is failing with internal system error.
CSCvq16846	Rename the label from "ResetAll Hitcounts" to "Reset Policyset Hitcounts" under policy sets
CSCvq54153	Cisco Identity Services Engine Policy Set Name Cross Site Scripting Vulnerability
CSCvo15652	pxGrid WebSocket multiple connections issue
CSCvp53222	ISE subscribes to IND topic /topic/com.cisco.endpoint.asset 3 times
CSCvp54975	pxGrid service lookup still returns old hostname after hostname change
CSCvq33194	Not able to change the language in guest portal with option "Always use"
CSCvq33527	VM Licenses are not consuming based on M5 Profiles
CSCvp02082	Env data is missing when TrustSec-ACI integration is enabled.
CSCvp92030	unable to create ATZ policy using supported special character
CSCvq13294	SXP Mappings bulk download is slow over pxgrid
CSCvq69138	Change logging level of 90140 INFO PassiveID: Message parsed syslog to DEBUG
CSCvq42847	ISE: "Posture failed due to server issues" error during System scan on MAC OSX
CSCvp98834	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities

Known Issues in Cisco ISE Release 2.4.0.357- Cumulative Patch 10

CA Service Disabled after Upgrade to Cisco ISE 2.4 Patch 10

After upgrading to Cisco ISE 2.4 Patch 10, Certificate Authority (CA) service might be disabled on the nodes on which Policy Service persona is not enabled. To enable the CA service, choose Administration > System > Certificates > Certificate Authority > Internal CA Settings.

Certificate authority service and EST service will be disabled if Sessions service is disabled on the PSN.

Resolved Caveats in Cisco ISE Release 2.4.0.357 - Cumulative Patch 9

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

The following table lists the resolved caveats in Cisco ISE 2.4 Patch 9.

Patch 9 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.1.53 or later.

Note After the patch is successfully installed, sometimes you may see an alarm indicating that patch installation failed with an error while trying to reboot. This is a false alarm. You can ignore this alarm.

Caveat ID Number	Description
CSCvd88480	Location filter for ERS Network Device get-all API fails
CSCvf17323	Normalized Radius:SSID not matched after CoA in the same session-ID
CSCvf33851	ISE 2.1+ RBAC: not able to manage endpoints and assign static identity groups
CSCvh64185	Some information is missing when session details are sent from ISE to FMC via pxGrid
CSCvi27613	Endpoints keeps profiling even though profiling is disabled
CSCvi65932	Blank pop-up in Sponsor Portal if customField contains "null" value
CSCvj02829	SCCM MDM attribute LastPolicyRequest is not converted correctly in ISE
CSCvj31598	Import two CA certs with same subject name
CSCvj83747	ISE Secure Access Wizard Easy Wireless null AD groups for BYOD, Secure Access, Sponsored guest flow
CSCvk52874	ISE does not provide the expected values in the context of EAP chaining
CSCvk76680	ISE-PIC self signed certificate delete operation fails due to Secure Syslog Server reference error
CSCvm00481	CA Service still running on command line after disabling internal certificate authority in Web UI
CSCvm01627	ISE 2.4 ERS API - PUT and GET Internal User "User Custom Attributes"
CSCvn66198	Sponsor portal doesn't refresh the accounts after deleting users and requires a manual refresh
CSCvn85484	Removing SCEP RA Profile causes the associated CA chain to be removed from Trusted Store
CSCvo48975	ISE downloads unnecessary RA certificate for BYOD
CSCvo56989	Json SearchResult gives the href value as NULL
CSCvo74766	ISE DACL syntax checking validation failing on wildcard notation
CSCvo75376	pxGrid node name limit too short for FMC
CSCvo78171	ISE 2.4 Patch 6 installation breaks FQDN of Sponsor and MyDevices Portal

Caveat ID Number	Description
CSCvo82021	Memory usage discrepancy in GUI and show tech
CSCvo90393	COA failure in Radius+PassiveID flow
CSCvo92284	While saving IP SGT static mappings changes, "Discard changes you have made" message is displayed
CSCvo98554	After Importing ISE PB to ISE, Login page are not loaded
CSCvp05303	Provisioned Certificates are not deleted after revocation
CSCvp05936	Adding DEFCON matrix pop-up title needs to be changed
CSCvp07591	Active Directory Machine authentication fails with error "22040 Wrong password or invalid shared secret"
CSCvp12131	ISE 2.4 Patch 6 reload breaks backups
CSCvp12685	Cross-Site Request Forgery (CSRF) [OWASP_CSRFTOKEN bypass]
CSCvp13378	PassiveID flow should send User's SamAccountName and ExplicitUPN
CSCvp14725	ADNormalizedUserName field missing in some of the sessions
CSCvp16734	Plus Licenses consumed without Plus features
CSCvp17444	RSA or RADIUS Token user with Valid account and credentials gets a blank page when trying to login to ISE Admin portal if the account doesn't exists under Access > Administrators
CSCvp18692	AD User information not shown in Context Visibility page
CSCvp19632	Policy sets order mismatch when exporting as XML
CSCvp23869	ISE TLS 1.0 and 1.1 security settings are not applied for PxGrid, causing WSA to fail integration
CSCvp29197	ISE 2.4p3 Radius livelogs not displayed due to invalid NAD ip address
CSCvp29278	Cisco Identity Services Engine Blind SQL Injection Vulnerability
CSCvp29413	Modifying Radius attributes to send in the request to External RADIUS Server is not working on ISE
CSCvp29572	Enable Pxgrid Profiling Probe setting is not working properly
CSCvp33593	ISE fails to match authorization policy with endpoint ID group "unknown"
CSCvp33598	ISE deletes all endpoints if MAC address is deleted twice at the same time
CSCvp33862	Custom Attribute (advanced filter in CV) not able to filter on risk score (integer value)

Caveat ID Number	Description
CSCvp37101	Application server crash is observed when an AD Join operation is attempted via GUI under Administration > Identity Management > External Identity Sources > Active Directory
CSCvp37238	TACACS/AAA live log report not showing configuration change made from ACI
CSCvp40082	ISE 2.3/2.4 upgrade to the latest patch may break dynamic redirection for third party NADs
CSCvp40398	Cannot configure scheduled config and operational backup with start date same as current day
CSCvp48710	Unable to add AD group if it contains "/." or "/.." in the AD group name
CSCvp50450	ise-elasticsearch.log files not purged in ISE 2.4 and 2.6
CSCvp50557	Changing max user global settings is not logged in change configuration audit
CSCvp51033	GUI Context Visibility report export slowness
CSCvp52201	Replication: Cluster information table has old FQDN
CSCvp54949	BYOD flow is broken in IOS 12.2
CSCvp54992	BYOD provisioned profile doesn't automatically configure EAP TLS in IOS 12.2
CSCvp58945	Import of network device template throws error "Failed illegal value for Encryption key"
CSCvp59286	Multiple Vulnerabilities in struts2-core
CSCvp60359	Upgraded ISE Node shows LDAP Identity Store password in plain text
CSCvp62113	Enforce NMAP skip host discovery and NMAP scan timeout
CSCvp65711	ISE 2.4 P8 posture scan running when an endpoint switches to a wired network not configured with dot1x
CSCvp65816	"Cisco Modified" Profiles are overwritten by the Profiler Feed Service
CSCvp73076	Log Collection Error - Session directory write failed when AD Probe Session is inserted
CSCvp76911	Deploy button is missing in the Matrix page when Multiple Matrices workflow is enabled
CSCvp77008	ISE LogicalProfile appears under Custom attributes in Context Visibility page when custom attributes are configured
CSCvp86406	Unable to add network device with combination of any digit followed by () in Software Version field
CSCvp93901	Enhancement to publish the following attributes via pxGrid: ADUserSamAccountName, ADUserQualifiedName, ADHostSamAccountName, and ADHostQualifiedName

Caveat ID Number	Description
CSCvq15329	Restore failing for scheduled backup

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 8

The following table lists the resolved caveats in Release 2.4 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.

Note After the patch is successfully installed, sometimes you may see an alarm indicating that patch installation failed with an error while trying to reboot. This is a false alarm. You can ignore this alarm.

Caveat ID Number	Description
CSCvh54905	Identity Admin cannot see users under Identities tab
CSCvj83362	Include hostname in posture assessment reports
CSCvk34232	Posture remediation files are limited to 50MB
CSCvn35142	ISE 2.3 : Posture report for endpoint by condition not working as expected
CSCvn44171	Network access user with external password cannot be used as ISE admin
CSCvn52886	User name from WMI information is deleted on receiving a DHCP custom syslog for same endpoint
CSCvn55560	ISE 2.3 after applying patch 5 creation of EOB Guest user does not work
CSCvn58964	ISE 2.4 slow database response with 500 authorization policies
CSCvn60787	Emails are not sent for alarm specific email configuration
CSCvn61139	Smart Licensing agent thread lock causes GUI login delay in ISE 2.2
CSCvn64652	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvn65317	ISE not able to assign guest account to the same guest type used for previous user
CSCvn67160	ISE 2.4 Unable to modify proxy settings when proxy bypass list contains carriage return symbol
CSCvn67199	Cannot filter Context Visibility by 'NAD Port ID' when using "/" character
CSCvn69854	ISE includes only one prrt-server file in support bundle
CSCvn70558	MDMServerReachable does not work for SCCM MDM again
CSCvn70680	ISE expired license can't be deleted if number of Base and Wired Licenses are not matching

Caveat ID Number	Description
CSCvn72150	Nodes have high IO spikes frequently in VM performance reports
CSCvn72918	ISE TrustSec policy difference alarm description is not accessible
CSCvn75396	Authentications are displayed in correctly in "Top N Authentication by Failure Reason" report
CSCvn76567	ISE 2.4 - IP-SGT bindings disappear from SXP for user session
CSCvn79043	ISE 2.4 Live Logs Not Filtering
CSCvn79557	ISE : Custom user attribute change does not reflect changes in configuration change audit report
CSCvn79569	App status for ISE is in initialisation state
CSCvn85498	ISE 2.4 : InactiveDays attribute update with disabled profiling
CSCvn87918	IPV6 based client provisioning portal is not working on default port 8443
CSCvn92246	ISE: admin users unable to delete or modify groups if a tacacs user is saved without any group
CSCvn92778	Removal of unused logical profile may cause a wrong authorization result
CSCvn98932	Non-existed DACL is not verifyed by the ISE
CSCvo05269	[ISE 2.4]Unable to use created profiling policy in authorization condition
CSCvo09945	Backups from SFTP repository may show incorrect year in Modified time
CSCvo13269	ISE does not allow to add an SGT
CSCvo13626	ISE : Improve Posture Assessment by Condition Report export rate for higher records (millions)
CSCvo17704	ISE 2.4 - CLI password will not accept 3 $
CSCvo18247	ISE: failed to skip duplicate framed-pool attribute during migration
CSCvo19076	ISE endpoint purge ACTIVEDIRECTORY dictionary is not loading
CSCvo23340	TACACS+ Admin Group access denied when navigating to Work Center > Device Admin > Identities
CSCvo28092	ISE Custom Endpoint Attributes - Will not save or delete
CSCvo28578	ISE 2.3 - Location info and IPSEC info are reversed in order in Network Device Groups for some NADs
CSCvo30170	Guest portal client provisioning customization text doesn't save
CSCvo33696	ISE2.4 doesn't reset failedLoginAttempts after successful login of internal users to network device

Caveat ID Number	Description
CSCvo35516	Device Sensor not able to correctly parse DHCP attributes via RADIUS probe
CSCvo36837	Admin group cannot get access to "Users" at "Device Administration" tab after install patch 5
CSCvo42165	Default python change password script returns CRUD operation exception
CSCvo45582	Internal Administrator Summary report not allowing to select specific columns
CSCvo45606	ISE:WMI-Passed values may compromise the security of ISE. Please remove malicious scripting terms
CSCvo48352	CSV file of RADIUS authentications report may have duplicate records
CSCvo49521	ISE Adds an additional character at the end of OperatingSystemVersion
CSCvo51295	ISE 2.2 Sponsor: Single click approval displays wrong message after clicking on approval link twice
CSCvo61888	Device Administration Current Active Sessions report not available from 2.4 P6
CSCvo61900	System Scan throws internal error for MAC built-in FW remediation
CSCvg70813	ISE dmp files are not deleted from /opt/oracle/base/admin/cpm10/dpdump for failed backup attempts
CSCvh19430	ISE 2.x : Guest account activation time discrepancy for imported accounts
CSCvh22907	Sponsor Portal Page takes more than 10 seconds to load
CSCvi21737	ISE 2.2 has too many journal files.
CSCvi29759	Samsung S7 and S8 profile
CSCvi51291	ISE CoA doesnt work 2 days after initial auth
CSCvi68744	Surplus of License Files can Cause Excessive Login Delay--ISE
CSCvi80094	ERS API that requires CSRF token returns HTTP 404 instead of 403
CSCvj08392	ISE SNMPv3 User still display on "show snmp user" after delete snmp-server user
CSCvj72647	ODBC attribute retrieval not working properly with EAP chaining
CSCvj75478	Device network conditions missing
CSCvj81752	URT Fails at Import Due to ORA-31684
CSCvj90273	Multi-NIC Windows/macOS: ISE Posture Module Maps VPN IP to MAC Address of a Disconnected Interface
CSCvk29087	Master Guest reports takes 30+mins to display
CSCvk50720	ISE 2.2 : Network devices page is not loading

Caveat ID Number	Description
CSCvk59716	Domain Admins are not able to edit Sponsor accounts properly
CSCvk61386	ISE not showing filtered NADs
CSCvk70748	High CPU and High Auth Latency and OOM condition on PSN nodes
CSCvm05840	NAD CSV imports should allow all supported characters
CSCvm07718	TACACS/RADIUS shared secret key disappears after highlight and then command/control + C
CSCvm63427	Cisco Identity Services Engine Password Recovery Vulnerability
CSCvm87060	ISE 2.x : Remote forest Active Directory controller failover prolonged time
CSCvm87292	Unable to integrate Tenable adapter to ISE 2.4 & 2.5 2.2 2.3
CSCvm90478	"No Data Available" when attempting to add endpoints to Identity Group with RBAC User
CSCvn01551	Failed to upload AC packages of file size > 50MB on ISE->Agent Resources
CSCvn10971	ISE: Rebooting associated site-specific GC does not result in failover to other GC
CSCvn12229	log4j.appender.ACS-FILE.MaxBackupIndex is not working in ISE
CSCvn15670	SL Server is getting overloaded with ISE auth renewals
CSCvn21926	Parser error seen with Threat Centric NAC CTA Configuration irrespective of ise version
CSCvn24392	Certain characters are not being parsed properly
CSCvn24568	Network Device Filtering Returns Only First IP Range When Multiple Ranges Are Configured
CSCvn27022	Limited access user getting "failed to fetch network device group" when accessing NAD
CSCvn27325	Posture policy with Tunnel Group Name in condition is not hitting
CSCvn39504	TACACS authentication details displays blank page
CSCvn39998	Pullout reports from Authentication Summary report is showing empty report.
CSCvn40822	Guest creation fails ISE 2.3 after patch 5
CSCvn56754	Live sessions record is not getting updated with new username (and/or) new IP address.
CSCvo41052	ISE deleting the newly created IP-SGT mapping
CSCvo11090	Able to delete ACI IEPG in ISE.
CSCvo24593	pagination is not working in "All SXP mappings" page in ISE.

Caveat ID Number	Description
CSCvo32279	APIC logs not seeing in sxp.log when SXP logging set to 'DEBUG'.
CSCvo35144	Delay in clearing of SXP mappings in ISE.
CSCvo43289	ISE truncates the SGT name after a "-" character and assigning a version id
CSCvo29478	ISE 2.3 P5 ISE doesn't allows to delete SGT tag from GUI although it is not referenced
CSCvo45768	Adding config to support PrA in PSN failover case
CSCvm81230	Cisco Identity Services Engine (ISE) Arbitrary Client Certificate Creation Vulnerability

Resolved Caveats in Cisco ISE Release 2.4.0.357 - Cumulative Patch 7

The following table lists the caveats that are resolved in Release 2.4 cumulative patch 7. Patch 7 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.1.53 or later.

Caveat ID Number	Description
CSCvn90651	This is an enhancement to implement primary node APIs for multi-DNAC support in Cisco ISE.

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 6

The following table lists the resolved caveats in Release 2.4 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 2.2.0.53 or later.

Caveat ID Number	Description
CSCux55288	Guest remember-me breaks ISE Guest Activity Logging
CSCuy41309	ISE 2.x Unable to delete endpoint from endpoint group
CSCuz00603	Unable to add duplicated mappings to multiple SXP VPNs
CSCvb17967	ISE fails to read response from MDM with special characters
CSCvb45390	Collection Filters configured with User name is not working for TACACS Author/Acct
CSCvc06629	[ISE] SMS notifications in non-English containing HTML tag
CSCvd79952	EasyConnect CoA not sent after session merge in distributed deployment
CSCvf03310	ISE email notifications to guests sends twice email for approval and guest user
CSCvf19364	ISE 2.2 no patch, SXP process fails when trying to create network subnet static mapping
CSCvf30591	ISE 2.2: Disabled password Lifetime, however getting reminder for account expiration.

Caveat ID Number	Description
CSCvf75225	ISE 2.1-P3 || high CPU seen in PAN due to 100K limit in redis
CSCvg86743	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvh09779	ISE 2.x TACACS log extremely slow
CSCvh11308	Cisco Identity Services Engine Logs Cross-Site Scripting Vulnerability
CSCvh31565	ISE fails to re-establish TCP syslog connection after break in connectivity
CSCvh83222	ISE: Need a report/dashboard for total unique endpoints
CSCvh91118	Flexibility needed to choose the time intervals in disclosing the user name for failed auth
CSCvh97544	Short CPU spikes can be observed when client didnt respond and ISE is used as RADIUS Proxy
CSCvi21043	Library conds referrred in policies are getting deleted; evaluation is giving deny access
CSCvi30462	Bulk guest import does not work using when logged into sponsor portal using SAML provider,
CSCvi37480	SNMPv3 COA failures on ISE using HP switches
CSCvi41678	Endpoint Attributes not updated in context visibility
CSCvi42404	validDays does not match span of fromDate to toDate for ERS created guests
CSCvi43687	ISE 2.2 Endpoint export may contain duplicate entries
CSCvi48298	Policy Hit count value gets nullified while click on REFRESH button.
CSCvi50320	EST Service not running owhen ISE iseca folder missing
CSCvi61204	ISE 2.1 Endpoint Purge policy is matched but job halts during execution.
CSCvi67780	ISE Internal CA : SAN ext validation fails if it isn't the first entry in RequestedExtensions in CSR
CSCvi68271	ERS API get all endpoints not returning description field as stated in documentation
CSCvi97332	Unsupported character Backslash has to be added to the UI error message while creation of admin user
CSCvi99561	AC 4.6 Application enforcement is not working for Torrent
CSCvj01047	Password length limitation when adding DC's in the PassiveID section of 32 characters.
CSCvj05563	Cannot delete security groups having virtual network mapping
CSCvj24095	Unknown Radius Flow is set to RadiusFlowType when updating ExternalIdStoreDictionary

Caveat ID Number	Description
CSCvj25696	User customer attributes order doesn't change after drag drop and save.
CSCvj31243	ISE 2.3 AD Group SID Update fails for Groups referenced in the policies
CSCvj50257	Active endpoints are mismatched from expected value
CSCvj57593	SNMP CoA is not sending correct SNMP traps
CSCvj62592	Cisco Identity Services Engine (ISE) Java Deserialization Vulnerability
CSCvj62599	Cisco Identity Service Engine (ISE) unsafe deserialization in Adobe Action Message Format (AMF)
CSCvj62614	Cisco Identity Services Engine (ISE) File Upload Code Execution Vulnerability
CSCvj63376	ISE 2.2 VPN MDM- Compliance not updated from MDM Compliance Checker for active session
CSCvj64763	DNAC-ISE:Pxgrid failover fails with 2.4 patch1 with DNAC - ISE Integration
CSCvj65552	ISE 2.4 Backup Input Validation does not occur on backup name characters
CSCvj67414	ISE HSTS Max-Age parameter is too agressive no includedDomains flag
CSCvj72699	ISE stops publishing SXP mapping
CSCvj73152	Enable VLAN DHCP release breaks guest flow for ISE 2.4
CSCvj77878	pxgrid: XMPP Cleartext Authentication
CSCvj92976	ISE : Incomplete error message while importing an icon under Network Device Profiles
CSCvj95709	Enable pxGrid in FIPS mode
CSCvj99698	Guest password is not reset if Sponsor does not have rights to view the Guest Password
CSCvk01682	ISE allows importing multiple instances of same language in portal setup
CSCvk04424	Changed name for My Reports against Policy Set match removes the delete option from My Reports
CSCvk10156	RBAC SuperAdmin Data Access over written by read-only data access for Network Device Groups
CSCvk23161	ISE stops responding to TACACS requests.
CSCvk23532	Remove GMT portion from $ui_start_date_time$ and $ui_end_date_time$ on Email Notifications
CSCvk27295	NMAP fails to execute when an EP matches a Admin Created profiling policy
CSCvk28847	ISE sponsor's e-mail shoud not be in CC when view/print guests' passwords is disabled
CSCvk38374	ISE 2.4 Sponsor-Group OWN_ACCOUNTS email association

Caveat ID Number	Description
CSCvk39421	ISE offline profiler feed service unavailable 17/07/18
CSCvk40105	Editing guest user throws pop up error when creating with java scripts in first and last name
CSCvk48315	Live sessions are not seen in ISE Live logs page in ISE 2.4
CSCvk51906	DST changes are not honored by the shift job which is causing the data movement issues on MNT nodes
CSCvk55285	ISE doesn't validate the data type date in the custom endpoint attribute
CSCvk58134	SAML authentication is showing wrong Identity store in Sponsor Login and Audit report
CSCvk59357	Admin warned of license non-compliance even after adding new licenses
CSCvk68196	SNMPv3 profiling works only with DES or AES128 privacy protocol
CSCvk70087	SecureSyslogCollectors should be disabled by default on remote log targets.
CSCvk71816	ISE ADE-OS - when trying to change timezone there should be a warning stated it is not supported
CSCvk72606	ISE- Can login to GUI with disabled admin accounts.
CSCvk74190	Radius Token Identity Caching Timeout not Configurable
CSCvm00127	ISE sponsor email customization doesn't add image properly
CSCvm03842	PxGrid SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection - CVE-2009-3555
CSCvm09377	HTTP Request Header for ISE fails if it contains @ in email
CSCvm09493	ISE 2.4 | Unable to save multiple custom attributes at once
CSCvm11230	Customer sees no data available for this record for "Details" page in Live Logs
CSCvm12105	ISE 2.3 not hitting policy with Session BYOD-Apple-MiniBrowser-Flow condition
CSCvm12281	ISE 2.3 Context Visibility Authentication Policy column is blank.
CSCvm12443	ISE should not send alarm for 'ERS-Media-Type' not present in ERS header
CSCvm14030	Evaluation of positron for Struts remote code execution vulnerability August 2018
CSCvm15059	ISE 2.1+ : Identity Source Sequence info button information is wrong for Sponsor Portal
CSCvm16060	Cannot Disable Telnet Change Password
CSCvm16523	ISE 2.3 to 2.4 upgrade is failing with error "nodes are not on the same ISE patch version"

Caveat ID Number	Description
CSCvm16952	Oracle Security Alert Advisory - CVE-2018-3110
CSCvm20561	ISE 2.x || Cisco-Device profiler policy missing the tandberg OUI as a condition
CSCvm21147	ISE: After upgrading to ISE 2.4 schedule backup are not working.
CSCvm22262	AMQP Cleartext Authentication Vulnerability
CSCvm26334	Endpoints not re-profiled after config restore and import new profiles
CSCvm27249	PassiveID Probe hprof files in temp folder
CSCvm29583	ISE AD lookup broken due to the blocked list domain lookup failing
CSCvm31919	IE11 : Trash icon linked to MAC address search box in Context Visibility
CSCvm32107	Unable to delete Root Network Device Group
CSCvm32303	Rest API- Unable to retrieve Guest User Details using ToDate filters
CSCvm33217	AD groups with more than one space doesn't allow authZ policy to be saved
CSCvm33673	Difference between Oracle and ES in terms of description
CSCvm34694	Newly created Network Device Model Name and Software Version are not present in GUI
CSCvm39902	Maintain Connectivity During Reauthentication option not working
CSCvm39909	Live log detailed reports shows msec instead of seconds for session timeout
CSCvm41485	ISE 2.3 : Unable to access NFS repository and scheduled reports not working using NFS respository
CSCvm41759	'Error 400' after pressing Sing Out on the Manage Guest Accounts page.
CSCvm45072	OWASP ZAP reports Cross Site Scripting (DOM Based) on pxGrid Web application
CSCvm45330	pxGrid cert change causing onAuthzRequest DENIED
CSCvm45941	ISE 2.4 not sending "Framed-IP-Address" attribute in profile when using leading zero
CSCvm47317	30+ GB files left behind after successful ISE 2.4 upgrade
CSCvm47507	Changes made in allowed protocols is missing in change configuration audit reports
CSCvm47638	ISE-secondary node doesnt send COA when guest account gets suspended or deleted
CSCvm48075	Manual CoA fails from Context Visibility if user never accesses Live logs or Live Sessions prior
CSCvm49084	ISE PB portal files are not restored with a restore of an old backup
CSCvm49503	WasMachineAuthenticated EQUALS False No Longer Parsed in Runtime--ISE 2.4

Caveat ID Number	Description
CSCvm57650	BYOD TLS not working for IOS 12 FCS release
CSCvm61134	SXP debug logs are not dumped in sxp.log unless services are restarted
CSCvm62783	'EST-CSR-Request' dictionary condition does not work
CSCvm62862	Cisco Identity Services Engine Logging Cross-Site Scripting Vulnerability
CSCvm66696	ISE 2.4 Conditional CoA failure upon EndPoint Identity Group change
CSCvm66751	Guest AUP: AUP acceptance is triggering replication event
CSCvm67561	Accounting messages from ASR1K not saved and not shown in ISE Reports
CSCvm69965	Chrome:Cannot create new ByoD portal
CSCvm70470	Max Sessions" value can not be applied on GUI after applying 2.2p10 or 2.3p4
CSCvm71860	Cisco Identity Services Engine Reflected Cross-Site Scripting Vulnerability
CSCvm71871	Cisco ISE Path traversal issue
CSCvm72187	ISE 2.2 | Guest self registration portal doesn't sort timezone list correctly
CSCvm72309	AD Probe failing to find the computer object with FQDN
CSCvm73506	Alarms: Profiler Queue Size Limit Reached
CSCvm73626	Sponsor creating random accounts for time restricted guest types fails
CSCvm74423	ISE 2.4 - Guest users aren't getting emails automatically while importing from CSV
CSCvm74605	ISE: EAP-FAST prefers cached AD DN over new DN after changing the Account OU
CSCvm75687	MyDevices Portal: Can't change device status on a PSN running with secondary PAN.
CSCvm75765	ISE -"user's email is not valid" unable to create User for top level domains other than .com .in etc
CSCvm75790	SAML with ADFS is broken with 3rd party NAD
CSCvm76717	ISE 2.4 Replication failure causing nodes to go out of sync after LAN automation
CSCvm79293	ISE2.2 TACACS doesnt apply the command sets after long REGEX argument
CSCvm79609	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvm79618	Cisco ISE Local Privilege Escalation Vulnerability
CSCvm80914	ISE 2.4 Scheduled backups not working. Can be seen in gui
CSCvm81243	endpointcert/certRequest API call causes Internal CA Service to Crash in ISE
CSCvm82504	Request to increase Radius Token Server password caching to 900 seconds or later

Caveat ID Number	Description
CSCvm86244	Inner Execution Context is not fully iuodated from API Execution context
CSCvm86699	ISE CAC or certificate login does not populate external groups under new admin group
CSCvm87685	Menu access duplicate is failing with plus sign
CSCvm88149	Account Disable Policy 'Disable accounts after days of inactivity' is incorrectly calculated
CSCvm89126	ISE 2.3 patch 5 : NAD / AAA server address is not specified.
CSCvm89837	Lost and Stolen buttons stay disabled on My Devices portal if Japanese GUI used
CSCvm90359	pxGrid debug "warn" level causing XCP to stop running
CSCvm91202	Cisco Identity Services Engine Password Recovery Vulnerability
CSCvm92317	ISE Kerberos Authentications are incrementing AD bad password count by 2
CSCvm93821	Authorization policy evaluation failing intermittently when using identity group as condition
CSCvm98407	Show members delays to retrieve the N/w devices in NDG page
CSCvm99398	SGACL Push in large scale NAD environment causes High CPU on PAN
CSCvn01019	Modify existing Network Device Profiles, grayed SAVE button
CSCvn04051	ISE 2.4: Details of 'error 500' missing in REST API query after patch 1 installation
CSCvn11424	PassiveID Management Logs Show Database ID insead of DC Name
CSCvn12114	Need to add Internal User Group in Certificate Authentication Profile
CSCvn12442	Under heavy load, ISE live logs stop working on ISE 2.3
CSCvn13802	ISE 2.4 :Unable to import network devices if shared secret contains "<"
CSCvn17210	ISE importing EMPTY cells in trustsec matrix doesnt overwrite existing content of cells
CSCvn18758	Profiler definitions for OSX Mojave (10.14) are not available in ISE 2.4 latest patch.
CSCvn21316	ISE: logwatch process failed with ::1 fatal error
CSCvn22251	ISE 2.4 patch 4 reduces I/O read Speed
CSCvn23570	ISE: Import Network Device does not conform to admin access permissions
CSCvn24356	pxGrid not handling invalid xml characters for publish and download
CSCvn25367	VCS pages Auth/Endpoint tab shows blank pop up msg.
CSCvn29633	ISE does not follow the capabilities of the Listener.

Caveat ID Number	Description
CSCvn31277	ISE: Trustsec alarm doesn't have SEVERITY level and its greyed out.
CSCvn31755	400 Bad Request when logging out Sponsor Portal
CSCvn33441	RBAC permissions do not propagate for admin users who login ISE with AD
CSCvn33534	Report logs can not fully displayed with "latst 30 days"
CSCvn35579	SXP connection between ISE and IOS Devices stuck in DeleteHoldDown state
CSCvn36029	Date in Unix Epoch format when context visibility in exported
CSCvn37048	ISE 2.x || ISE syslog message code (59200-59208) are not being used in ISE currently.
CSCvn40645	2.4P5:In 3 node deployment After Rollback of P5 PSN went down
CSCvn50203	ISE 2.4p5 - ACI integration - Not all IP_EPG mappings on ACI is imported by ISE
CSCvn51282	ISE replaces "ip:" to it's hostname in "ip:inacl" Cisco AV-Pair
CSCvn52114	Process failure using external radius token server authentication
CSCvn55640	Manage ACC calling infinite time when sponsoruser configured with permissions ALL&GROUP sponsor grps
CSCvn56648	When individual policy set is reset, other policy set hit counters are reset to 0.
CSCvn59383	ISE 2.3 patch 5 issue when creating guest user on sponsor portal using special character
CSCvn59502	ISE DACL syntax checking is not properly catching errors
CSCvn62164	ISE should support internal users with Special char colon : character to be partiy with ACS
CSCvn62788	TC-NAC configured with Qualys shows Not Reachable.
CSCvn67968	ISE stops responding to IPv6 hosts in its own subnet after adding IPv6 route.
CSCvn79861	ResetAll Hitcount Button not resetting hitcount value in Firefox browser
CSCvn81631	Cores being consistently generated on every node after upgrading from ISE 2.4 to 2.5
CSCvn92528	ISE 2.4 : Misconfigured supplicant query is one of the reasons for high CPU on both MNT nodes

New Features in Cisco ISE Release 2.4.0.357 - Cumulative Patch 6

Identity Caching in RADIUS Token and RSA SecurID Server

Identity caching is used to allow processing of requests that do not perform authentication against the server. You can enable the identity caching option and set the aging time in minutes. The default value is 120 minutes. The valid range is from 1 to 1440 minutes. The results obtained from the last successful authentication are available in the cache for the specified time period.

This option is disabled by default.

Open Caveats in Cisco ISE Release 2.4.0.357 - Cumulative Patch 6

Caveat ID Number	Description
CSCvo75376	pxGrid node name limit is too short for Cisco Firepower Management Center (FMC)

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 5

The following table lists the resolved caveats in Release 2.4 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 2.2.0.53 or later.

Caveat ID Number	Description
CSCvj86877	SFTP Connect Error
CSCvm03681	EAP-FAST doesn't support correct key generation in TLS 1.2
CSCvm91034	pxGrid : EndpointProfileMetaData not propagated with Pxgrid V2
CSCvm93698	AD authentications are failing after applying 2.2 P11/ 2.4 P4
CSCvn09504	TC-NAC configured with Qualys shows Not Reachable.
CSCvk13724	EPG mappings not created on ISE
CSCvn17524	ISE Apache Struts CVE-2016-1000031 Vulnerability

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 4

The following table lists the resolved caveats in Release 2.4 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 2.2.0.53 or later.

Caveat ID Number	Description
CSCuq95531	Diag Tool: For DNS A Record tests change status failed to warning
CSCuz52877	ISE21- Auth inactivity alarms every 15 mins
CSCvh25718	ISE doesn't convert guest username to lower case if credentials used in 802.1x, not on portal
CSCvh74979	Reset-config is reverting the fixes of patches and causing the issues.
CSCvi10363	ISE: Remove state attribute from access accept packets.
CSCvi50536	Evaluate ISE for Apache Tomcat February 2018 Vulnerabilities

Caveat ID Number	Description
CSCvi58316	ISE : URT fails due to upgrading the ACS to ISE migrated setup.
CSCvi85159	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability
CSCvi88520	Message Catalog Displaying Only the Message Code 89006 but Not the Rest
CSCvj36442	Network devices page fails to paginate as shared secret is in plain text
CSCvj44088	ISE: While registering getting the error: Unable to register the node <fqdn> Version: 0.0.0.0.
CSCvj57771	General Patch Management - Red Hat Linux(Critical/High)
CSCvj57967	Application check works in opposite logic
CSCvj70896	Failed to get sgt name from sgt tag: 5 or sgt is read only, or isPropgateToAPIC is false
CSCvj97277	Fix for CSCvf68738 does not allow legitimate CA certificate refresh
CSCvk07631	ISE 2.2: Hot Spot portal users asked to accept the AUP more than once
CSCvk09597	VM License Thresholds Mismatch Platform definitions
CSCvk10303	ISE 2.4 Trustsec Dashboard Query performance
CSCvk10454	Adding Node to deployment does not add the Profiling OUI data
CSCvk10674	ISE 2.4 Windows PC behind IP phone being profiled as Cisco-IP-Phone-8851
CSCvk12450	Regression: Windows 8/10 clients incorrectly profiled as windows7 due to feed policies
CSCvk13569	"ERROR_NO_SUCH_USER" due to ISE ADRT mis-identifiing a child domain name as root forest domain
CSCvk16959	ISE 2.4 no patches : unable to load network devices page
CSCvk19766	ISE 2.4 MnT session & Auth API response is not populating 'other_attributes' section
CSCvk40421	Not able to delete certificate from trusted page
CSCvk43032	Wrong number or types of arguments in call to 'COLLATIONDAILY_PURGE',HOURLY_STATS_JOB
CSCvk51667	ISE: "Manage accounts" gives 400 HTTP error if sponsor portal is configured for SAML authentication.
CSCvk55065	ISE 2.4 PxGrid queries against Secondary MNT resulting in collector crashing
CSCvk61086	ISE 2.4 2.3 2.2 2.1 2.0 : NFS repository credentials are not used
CSCvk65898	ISE 2.4 : Social Login e2e flow fails due to recent changes done on Facebook side
CSCvk71161	ISE 2.4 excessive profiler syslogs sent to MNT

Caveat ID Number	Description
CSCvk74356	ISE 2.4 Cisco Prime querying ISE session API could cause high CPU utilization on Monitoring Nodes
CSCvk74989	Certificate parameters not persistent after DNAC trust re-establishment
CSCvk75544	Authentication Summary Reports show "no data available" for Radius and TACACS
CSCvk76510	ISE 2.4 Core dump on primary node: SIGSERV in GenericConfigObject::getAsNested(unsigned int) const
CSCvm02478	CISCO Network Setup Assistant APP Not Available on GooglePlay
CSCvm05439	ISE cores on LDAP test server after DNAC establishment when same chain used
CSCvm05499	ISE CoA sends NULL value for NAS-Port-Id
CSCvm11175	ISE custom endpoint attribute type String doesn't allow numbers only
CSCvm11595	LiveSessions are not showing on GUI because user name having unicode characters
CSCvm12575	ISE context visibility endpoints import fails with custom endpoint attribute date
CSCvm17749	400 Error Seen In Guest and Sponsor Portal due to portal session deletion
CSCvm17795	Config Backups triggered from GUI hangs at 45% during ES backup

Open Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 4

Caveat ID Number	Description
CSCvm93698	AD authentications fail after installing ISE 2.4 patch 4. Could see the following error in ad_agent.log: `Identity resolution failed - ERROR_NO_SUCH_USER_SOME_DOMAINS_NOT_AVAILABLE`
CSCvm75266	ISE 2.4: Possible kernel memory leak
CSCvm72528	ISE 2.4 patch 3: COA is not working for CTS role based policy
CSCvm90852	Unable to use SFTP server as a repository in ISE 2.4 patch 4

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 3

The following table lists the resolved caveats in Release 2.4 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 2.2.0.53 or later.

Caveat ID Number	Description
CSCvd78169	CDP Attributes not added to EP via SNMP Query

Caveat ID Number	Description
CSCvf75968	Multiple Vulnerabilities in httpasyncclient
CSCvf82350	US27030 - Fix VPN Session to MAC Mapping
CSCvg46899	ISE 2.2 user may be redirected again after AUP acceptance on Hotspot portal
CSCvh54726	ISE: Failure to retrieve AD groups for Intel AMT supplicant username format
CSCvh91996	Matched AuthC and AuthZ rules in Monitor Only mode showing in GUID but not names
CSCvi03093	Purging doesn't work if Identity group name was changed/ change is not reflected to purge policy
CSCvi06525	Single click approval sponsor not seeing self-registered guest with implicit/explicit UPN
CSCvi23542	ISE doesn't fail-over to other available DCs when receiving STATUS_ACCESS_DENIED (0xc0000022) from DC on authentication attempts
CSCvi31965	ISE High Authentication Latency due to lookup in Internal Endpoints
CSCvi66786	Corefiles are being generated due to timesten crash in MNT node
CSCvi74182	Log Collection Error : null alarm
CSCvj02644	Customer see's blank "Details" page in RADIUS Live Logs
CSCvj37364	The content changes for imported guest notification template is not working.
CSCvj38428	Changing status of Network Access Users doesn't appear on audit report
CSCvj41029	User domain name may remain empty in session when ISE passive-id AD agent or MS WEF is used
CSCvk48105	Sponsor created guest have a previous guest account email CC'd
CSCvk57963	ISE 2.4 patch 2 install brings application services down due to integrity checksums failure

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 2

The following table lists the resolved caveats in Release 2.4 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 2.1.0.53 or later.

Caveat ID Number	Description
CSCvc71503	Jedis connections back to pool - broken connections (due to timeout)
CSCvf20208	ISE Posture PRA timer expires to non-compliant

Caveat ID Number	Description
CSCvf52213	ENH: ISE CLI support for MTU configuration on interfaces
CSCvg75818	Upgrade from ISE 2.2 to 2.3 fails on "CREATE UNIQUE INDEX CEPM.PKUPSABSTRACTTYPE_ATTRIBUTES"
CSCvh86466	PassiveID: WMI queries DC cause memory increased issues on DCs (Microsoft WMI memory leak)
CSCvi29600	Sponsor Groups are not merging results with AD Sponsor groups when Internal user uses AD password
CSCvi50542	ISE Telemetry Scheduler to be Configurable
CSCvi51021	No data available in context visibility if there is no plus/advanced license - Standalone node
CSCvi73782	Static Group Assignment dropping due to DHCP Probe
CSCvi79632	In case of no accounting activity, live session retains all session post 5 days period
CSCvi82192	Generate pxGrid Certificates page doesn't respect cert template RSA key size
CSCvi91353	NMAP scans for custom port 9100 but doesnt report it in nmap.log
CSCvj08379	ISE 2.4 EPSStatus is not updated in Context Visibility properly
CSCvj11319	ISE 2.4 - EST Service not running after upgrade from 2.3
CSCvj11981	SNMPv3 profiler breaks for NAD with security level of no auth after modifying the SNMP polling time
CSCvj13401	ISE "Failed Value for attribute Protocol is mandatory" when importing network device
CSCvj20617	Upgrade to 2.4 fails due to KEK change
CSCvj42529	ISE - API POST 401 Unauthorized 60-90 seconds after successful Guest Create POST
CSCvj47154	ISE2.4 is consuming extra plus license for default authorization policy
CSCvj52267	ISE 2.4 Input validation error for IPv6 subnets under TACACS Device Network Condition
CSCvj66943	ISE not using SSL for LDAP for "Retrieve Attributes" however connects to port 636
CSCvj72180	ENH: ISE: Store new m/c password on ISE side if new password is valid despite RPC error - 121
CSCvj79271	Secondary MNT: incorrect timesten permission issue for the folder Timesten_Data
CSCvj88674	Smart License enable is failing on ISE 2.4 release.
CSCvj90439	SGT used in trustsec matrix should not be allowed to delete
CSCvj92358	After upgrade UDI values of secondary node are missing from sec_hostconfig table

Caveat ID Number	Description
CSCvk28377	MnT persists frequent Accounting Interim-updates without any changes into Database
CSCvk31092	Core: SyslogSecureTCPConnection::updateConnectionData
CSCvi44041	Cisco Identity Services Engine Privilege Escalation Vulnerability

Resolved Caveats in Cisco ISE Release 2.4.0.357- Cumulative Patch 1

Caveat	Description
CSCvi36111	Live sessions - NAS IP address Tooltip is duplicated for ipv6
CSCvi47074	Replication failure seen on SXP nodes during SXP connection down
CSCvi48886	Post upgrade - the GuestVLAN doesn't copy the key of omapi.key to DHCP
CSCvi50979	Machine change password interval should be configurable from advance tuning parameter (Kerberos SSO)
CSCvi56003	AUP Link in the Self-Registration form throws Bad Request in ISE 2.4
CSCvi69286	Dashboard > Search : Endpoint details screen doesn't work correctly in Internet Explorer
CSCvj11476	ISE : Wrong error message when deleting a certificate referenced by some resource
CSCvi53593	Wrong msg if trying to issue CoA and no MAC address is selected
CSCvj61368	2.4 P1: ISE Indexing server is not running on secondary PAN
CSCvi38373	ISE Delete All Endpoints in Context Visibility too risky
CSCvh93370	ISE Guest: Incorrect accounting in syslog causes issues
CSCvi06647	Anyconnect configuration - drop menu for compliance module is empty
CSCvi61330	Occasional application restart post Radius/DTLs authentication
CSCvg90863	"Application Configure ISE" left idle for long time causes SSHD to disable

Caveat	Description
CSCvj17258	ISE 2.4 keeps old DNAC client cert causing new DNAC pxGrid with ISE to fail
CSCvj33336	DNAC1.2: Network devices not getting added in ISE 2.4 after provision
CSCvi49103	Wrong data type for "Enable Multi Shared Secret:String(128)" in NAD CSV export
CSCvg19708	Guest Accounting report broken

Resolved Caveats in Cisco ISE Release 2.4.0.357

Note Cisco ISE 2.4 patch 0 has parity with Cisco ISE 2.0 Patch 6, 2.0.1 Patch 5, 2.1 Patch 6, 2.2 Patch 6, and 2.3 Patch 2

The following table lists the resolved caveats in Release 2.4.

Table 4: Cisco ISE, Release 2.4, Resolved Caveats, Patch 0

Caveat	Description
CSCvf69805	Cisco Identity Services Engine cross-site request forgery vulnerability
CSCvf49844	Cisco Identity Services Engine local command injection vulnerability
CSCvf63414	Cisco Identity Services Engine authenticated CLI denial of service vulnerability
CSCvh51992	Cisco Identity Services Engine authenticated CLI denial of service vulnerability
CSCvf69753	Cisco Identity Services Engine authenticated privilege escalation vulnerability
CSCvf69963	Cisco Identity Services Engine cross-site scripting vulnerability
CSCvg95479	Cisco Identity Services Engine command injection to underlying OS vulnerability
CSCvd38467	BYOD does not work on Apple iOS 10.3.x.
CSCvf29467	Editing multiple client provisioning policies simulataneously hides the results column.
CSCvf33475	Simultaneuos configuration and operational backup on same browser is very slow.

CSCvi45925	Newly created dashboard not visible in 2.4 342 build.
CSCvf28877	ISE 2.3 TACACS+ : Unable to add commands to Command Set while editing.
CSCvf32298	ISE 2.3 Sponsor Portal: There is a delay of one minute between the update of the username table and the counter.
CSCvf32394	ISE 2.3 Self-registered guest portal of SMS provider- Global default is always re-selected when other attributes are changed.
CSCvf34216	ISE 2.3: Unable to select Work Center Menu - Guest Access Identity Group upon opening detailed report.
CSCvh05703	'Remember Me' RADIUS live sessions view does not show usernames for guest devices

Open Caveats in Cisco ISE Release 2.4.0.357

The following table lists the open caveats in Release 2.4.

Caveat ID Number	Description
CSCvf30591	ISE 2.2: Disabled password Lifetime, however getting reminder for account expiration.
CSCvg80657	disk maintenance. need automatic and on demand cleanup of ESR 5921 IOS crashinfo files
CSCvg80766	"application configure ise" command ungracefully terminates all CLI sessions
CSCvh20790	"Go to Update Report Page" giving "no data found."
CSCvh22907	Sponsor Portal Page takes more than 10 seconds to load
CSCvh22984	Unable to delete multiple sponsor accounts at once
CSCvh65530	Filter by No of Devices not working in NDG Flat table page
CSCvh69481	Get-All with filtertype=OR not working for some of the objects
CSCvh77969	User Visibility not working after VSW
CSCvh86082	Parsing NMAP smb-os-discovery data should remove
or \x00
CSCvh93771	Broken admin web ui access with PAT/NAT of HTTPS://<IP>:<port-non-443>
CSCvh95370	Creating Network Device Defaults Device Profile to AlcatelWired
CSCvi48276	AMP in ISE remains connected even after deregter from cloud
CSCvi48298	Policy Hit count value gets nullified while creating new policies in a specific case

Caveat ID Number	Description
CSCvi60160	Stop All Running Tests not functioning properly in Active Directory Diagnostic Tool
CSCvi85015	Anyconnect Profile for Vlan Refresh - notes is confusing
CSCvi88520	Message Catalog Displaying Only the Message Code 89006 but Not the Rest
CSCvi90269	SXP Device Connection page on ISE UI shows OFF on ISE even when peer is showing connection ON
CSCvj06916	ISE 2.3+ : Authc/Authz policies in a policy set cannot be configured if ext radius sequence is used
CSCvj13757	ISE 2.4 - Unable to acknowledge AD Diagnostic Failure Alarm
CSCvj22303	Endpoint OS is wrongly updated in External Mobile Device Management reports
CSCvj28192	ISE 2.4 GUI tcpdump is not having embeded -s 0 option
CSCvj29551	No warning/error on importing policy based on non-existing custom attributes
CSCvj31598	Enhancement Request: Import two CA certs with same subject name
CSCvj50085	After deleting the end-points from context visibility, homepage shows active end-points as 0
CSCvj50257	Active endpoints are mismatched from expected value
CSCvj54057	Alarm "Trustsec PAC validation failed" need to be enhanced to point the NAD hostname and IP address
CSCvj73152	Enable VLAN DHCP release breaks guest flow for ISE 2.4
CSCvj73550	CTS PAC refresh failed due to EAP-FAST communication failed btw switch and ISE
CSCvj77125	cdpCachePlatform rules not matching for Cisco Wave 2 (aka COS) APs 1800/2800/3800
CSCvj83961	CWA using non-mgmt interface is not replacing secondary interface fqdn for guest flow
CSCvj88164	Remote-Access VPN Posture Sessions showing Base license consumed but no Apex
CSCvj93331	Link to next page is not present in REST response
CSCvk06884	ISE should return 400 HTTP error, not 500 if incorrect data provided for REST call
CSCvk09565	ISE 2.x onwards RFC 3164 is not being followed completely
CSCvk12450	Regression: Windows 8/10 clients incorrectly profiled as windows7 due to feed policies
CSCvk25549	Offline profiler feed update web page is missing the offline feed option
CSCvk34422	Profiler: Feed download - Unable to update FeedEndpointPolicy
CSCvk40421	Not able to delete certificate from trusted page

Caveat ID Number	Description
CSCvk48315	Live sessions are not seen in ISE Live logs page in ISE 2.4
CSCvk55076	ISE 2.4 losing static group mapping due to profiler AD Probe
CSCvk55285	ISE doesn't validate the data type date in the custom endpoint attribute
CSCvk59357	Admin warned of license non-compliance even after adding new licenses
CSCvk65179	error while assigning a certificate to a certificate usage, Unable to access login Portal
CSCvk65898	ISE 2.4 : Social Login e2e flow fails due to recent changes done on Facebook side
CSCvk67692	ISE 2.x: REST API Get-All Internal Users' result has 'next-page' link missing in XML and JSON output
CSCvk68196	SNMPv3 profiling works only with DES or AES128 privacy protocol
CSCvk71555	Unable to configure opposite logic for Application condition
CSCvk72920	ISE does not send SNMP bulk request for CDP after it did once
CSCvk74989	Certificate parameters not persistent after DNAC trust re-establishment
CSCvm01627	ISE 2.4 ERS API - PUT and GET Internal User "User Custom Attributes"
CSCvm03411	Kernel Side-Channel Attack using L1 Terminal Fault: CVE-2018-3620 and CVE-2018-3646 (Foreshadow-NG)
CSCvm03842	PxGrid SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection - CVE-2009-3555
CSCvm05439	ISE cores on LDAP test server after DNAC establishment when same chain used
CSCvm05840	NAD CSV imports should allow all supported characters
CSCvm06464	ISE: SNMPv3 not sending traps
CSCvm06688	Patch roll back from CLI is failing in case of Patch install has issues after installing from GUI
CSCvm07566	ACS migration to ISE 2.4 breaks Identity Source Sequencing
CSCvm09377	HTTP Request Header for ISE fails if it contains @ in email
CSCvm10559	ISE 2.4 Unable to delete unused SGTs associated with Virtual Network
CSCvm11175	ISE custom endpoint attribute type String doesn't allow numbers only
CSCvm11230	Customer sees no data available for this record for "Details" page in Live Logs
CSCvm12215	Patch install needs to re-apply SQL fixes in case of database reset
CSCvm12484	ISE sending wrong message to DNAC when clock not sync'd during trust establishment

Caveat ID Number	Description
CSCvm17795	Config Backups triggered from GUI hangs at 45% during ES backup
CSCvm19797	Hotfix Install Generates False Error Messages
CSCvm19803	ISE 2.4 EndPoints are being associated with the incorrect logical profile
CSCvm20561	ISE 2.x || Cisco-Device profiler policy missing the tandberg OUI as a condition
CSCvm22838	CoAs not being sent after the initial profiler CoA when the profile for an endpoint changes
CSCvm23096	PSN is down and in initializing state for ever
CSCvm26207	ISE METRICS, Compliance percentage is of total endpoints instead actual endpoints go through posture
CSCvm26372	ISE Indexing Engine not running after installation of 2.4 patch 3 on secondary pan
CSCvm29083	ISE 2.4 configured Authz policy does not match the correct policy when using Logical Profiles
CSCvm29136	Windows7-Workstation policy is incorrect for the rule "WinPlatform certainty factor or 40
CSCvm29577	ISE 2.4 : Context Visibility Users : Active Directory attributes not getting stored
CSCvm31919	IE11 : Trash icon linked to MAC address search box in Context Visibility
CSCvm32107	Unable to delete Root Network Device Group
CSCvm32303	Rest API- Unable to retrieve Guest User Details using ToDate filters
CSCvm33217	Receiving an error when saving authorization policy using external domain users group as condition
CSCvo61888	Device Administration Current Active Sessions report not available from 2.4 P6

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.