Release Notes for Cisco Identity Services Engine, Release 2.3

Revised: February 18, 2021

Contents

These release notes supplement the Cisco ISE documentation that is included with the product hardware and software release, and cover the following topics:

Cisco Systems, Inc.
www.cisco.com

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

The Cisco ISE platform is a comprehensive, next-generation, contextually-based access control solution. It offers authenticated network access, profiling, posture, BYOD device onboarding (native supplicant and certificate provisioning), guest management, device administration (TACACS+), and security group access services along with monitoring, reporting, and troubleshooting capabilities on a single physical or virtual appliance. Cisco ISE is available on two physical appliances with different performance characterization, and also as software that can be run on a VMware server. You can add more appliances to a deployment for performance, scale, and resiliency.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also allows for configuration and management of distinct personas and services. This feature gives you the ability to create and apply services where they are needed in the network, but still operate the Cisco ISE deployment as a complete and coordinated system.

For more information about the features that are supported in Cisco ISE 2.3, see *Cisco Identity Services Engine Administrator Guide, Release 2.3*.

Note We have recalled ISE 2.3 patch 1 due to an issue we found after posting. An updated patch file has been reposted, and the new file name is ise-patchbundle-2.3.0.298-Patch1-221754.SPA.x86_64.tar.gz. If you already installed the previously posted patch, you MUST uninstall that patch, and install the new one.

ISE Community Resource

Join the ISE Community to view resources, ask questions, and participate in discussions. See ISE Product Documentation, Introduction to ISE, YouTube Videos, Feature and Integration Demos, and Training Resources.

The examples and screenshots provided in the ISE Community resources might be from earlier releases of Cisco ISE. Check the GUI for newer or additional features and updates.

New Features in Cisco ISE, Release 2.3

Some Dashlets Removed to Resolve Performance Issues

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

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

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

CoA Logging Enhancements

The following attributes are additionally displayed for the CoA events in the Authentication details report that is launched from the Live Logs page:

- CoASourceComponent—The component requesting the CoA, for example, profiler, posture, BYOD onboard (NSP), and so on.
- CoAReason—The reason for the CoA to be triggered, for example, change in endpoint profile.
- CoAType—Shows the type of CoA event, for example, reauthentication, terminate, and so on.

Context Visibility Enhancements

The Application dashboard in the Context Visibility page helps you to identify the number of endpoints that have a specified application installed. The results are displayed in graphical and tabular formats. The graphical representation helps you make a comparative analysis. Applications are classified into 13 categories. Applications that do not fall into any of these categories are termed Unclassified.

Enable MAR Cache Distribution

Cisco ISE allows you to add or update the MAR cache distribution for the node groups. You must ensure that MAR is enabled in the AD page before enabling this option.

Export Command Sets and Syslog Messages

You can export the command sets and syslog messages in CSV format.

Guest Enhancements

Guests can select a social login provider as a way to provide credentials as a self-registered guest, instead of entering username and password in the guest portal. To enable this, you can configure a social media site as an external identity source, and configure a portal that allows users to use that external identity source (social login provider). Facebook is the social login provider supported by this release.

IPv6 Support for External ID Store Attributes

Cisco ISE allows you to configure the AD and LDAP server with IPv4 or IPv6 address when you manually add the attribute type IP and authenticate the user.

Key Type for Certificate Public Key

You can specify the algorithm to be used for creating the public key (RSA or ECDSA). You can also specify the bit size for the public key. The following options are available for RSA:

- 512
- 1024
- 2048
- 4096

The following options are available for ECDSA:

- 256
- 384

Migration Tool Enhancements

The migration tool provides options to migrate ACS 4.x/ACS 5.x supported objects. The migration tool lists the data objects based on the selection. The migration tool supports:

- Migration of users, identity groups, network devices, network device groups, and user-defined attributes from ACS 4.x/5.x to Cisco ISE.
- Migration of policy rules having AND/OR conditions.
- Migration of network devices configured with IP address ranges in all the octets.

- Migration of date and time policies into multiple objects if the time table is configured with different timings and days.

The migration tool now supports additional endpoint custom attributes, such as Date, IP Address, Unsigned Integer 32, and Enumeration.

Network Device IP Address Range Support in all the Octets

You can configure the network devices with IP address ranges in all the octets. You can use a hyphen (-) or asterisk (*) as wildcard to specify a range of IP addresses. You can specify single IP address, subnet address, or IP address range in all the octets for the network device. Cisco ISE reports a validation error if you provide invalid IP address/range in the External REST interface.

Node Registration Made Easy

If the node uses a self-signed certificate that is not trusted, a certificate warning message is displayed. The certificate warning message displays details about the certificate (such as, Issued-to, Issued-by, Serial number, and so on), which can be verified against the actual certificate on the node. You can select the **Import Certificate and Proceed** option to trust this certificate and proceed with registration. Cisco ISE imports the default self-signed certificate of that node to the trusted certificate store of Primary PAN. If you do not want to use the default self-signed certificate, you can click **Cancel Registration** and manually import the relevant certificate chain of that node to the trusted certificate store of Primary PAN.

Policy Sets

Network access policies have now been consolidated together under Policy Sets, which can be accessed from **Policy > Policy Sets**. Each policy set is a container defined on the top level of the policy hierarchy, under which all relevant Authentication and Authorization policy and policy exception rules for that set are configured. Multiple rules can be defined for both authentication and authorization, all based on conditions. Conditions and additional related configurations can now also be easily accessed and reused directly from the new Policy Set interface.

For more information about the new policy model, see New Policy Model, page 17

Posture Enhancements

- Default policies added for anti-malware, application visibility, and firewall conditions.
- Default requirements added for application visibility, firewall, and USB conditions.
- Cisco Temporal Agent—By default, this temporal agent resides in the Cisco ISE ISO image, and is uploaded to Cisco ISE during installation.
- Posture and client provisioning policies allow the matching of users and endpoints, including Endpoint ID groups and endpoint custom attributes.

RADIUS DTLS Client Identity Check

You can choose the **Enable RADIUS/DTLS Client Identity Verification** option under RADIUS settings if you want Cisco ISE to verify the identity of the RADIUS/DTLS clients during the DTLS handshake. Cisco ISE fails the handshake if the client identity is not valid. Identity check is skipped for the default devices, if configured. Identity check is performed in the following sequence:

1. If the client certificate contains the subject alternative name (SAN) attribute:
   - If SAN contains the DNS name, the DNS name specified in the certificate is compared with the DNS name that is configured for the network device in Cisco ISE.
   - If SAN contains the IP address (and does not contain the DNS name), the IP address specified in the certificate is compared with all the device IP addresses configured in Cisco ISE.
2. If the certificate does not contain SAN, subject CN is compared with the DNS name that is configured for the network device in Cisco ISE. Cisco ISE fails the handshake in the case of mismatch.

Read-only Administrator Support

Cisco ISE allows you to create read-only administrative users who can view the configurations on Cisco ISE GUI, but cannot create, update, or delete data.

Reports Export Summary

You can view the summary of the reports that are exported by the users in the last 48 hours along with the status.

Schedule Policy Export

Cisco ISE allows you to schedule authentication and authorization policy export. This can be scheduled to run once, daily, weekly, or monthly.

Security Settings Page Enhancements

The following options are added in the Security Settings page **(Administration > System > Settings > Protocols > Security Settings)**:

- Allow TLS 1.0—Allows TLS 1.0 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE downloads CRL from HTTPS or secure LDAP server
  - Cisco ISE is configured as secure syslog client
  - Cisco ISE is configured as secure LDAP client

Note **Allow TLS 1.0** option is disabled by default in Cisco ISE 2.3 and above. TLS 1.0 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.0, check the **Allow TLS 1.0** check box in the **Security Settings** page (Administration > System > Settings > Protocols > Security Settings).

- Allow TLS 1.1—Allows TLS 1.1 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE downloads CRL from HTTPS or secure LDAP server
  - Cisco ISE is configured as secure syslog client
  - Cisco ISE is configured as secure LDAP client

Note **Allow TLS 1.1** option is disabled by default in Cisco ISE 2.3 and above. TLS 1.1 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.1, check the **Allow TLS 1.1** check box in the **Security Settings** page (**Administration > System > Settings > Protocols > Security Settings**).

- Allow SHA-1 ciphers—Allows SHA-1 ciphers for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE is configured as RADIUS DTLS server
  - Cisco ISE is configured as RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS or secure LDAP server.
  - Cisco ISE is configured as secure TCP syslog client.
  - Cisco ISE is configured as secure LDAP client.

  This option is enabled by default.

Note It is recommended to use SHA-256 or SHA-384 ciphers for enhanced security.

- Allow ECDHE-RSA ciphers—Allows ECDHE-RSA ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE is configured as RADIUS DTLS server
  - Cisco ISE is configured as RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS server
  - Cisco ISE downloads CRL from secure LDAP server
  - Cisco ISE is configured as secure TCP syslog client
  - Cisco ISE is configured as secure LDAP client

It is recommended that you enable this option for enhanced security. This option is enabled by default.

- Allow 3DES ciphers—Allows 3DES ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE is configured as RADIUS DTLS server
  - Cisco ISE is configured as RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS server
  - Cisco ISE downloads CRL from secure LDAP server
  - Cisco ISE is configured as secure TCP syslog client
  - Cisco ISE is configured as secure LDAP client

  This option is enabled by default. Uncheck this check box for enhanced security.
- Accept certificates without validating purpose—When ISE acts as an EAP or RADIUS DTLS server, client certificates are accepted without checking whether the Key Usage extension contains keyAgreement bit for ECDHE-ECDSA ciphers or keyEncipherment bit for other ciphers. This option is enabled by default.
- Allow DSS ciphers for ISE as a client—Allows DSS ciphers for communication with server for the following workflows:
  - Cisco ISE is configured as RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS server
  - Cisco ISE downloads CRL from secure LDAP server
  - Cisco ISE as secure TCP syslog client
  - Cisco ISE as secure LDAP client

  This option is enabled by default. Uncheck this check box for enhanced security.
- Allow legacy unsafe TLS renegotiation for ISE as a client—Allows communication with legacy TLS servers that do not support safe TLS renegotiation for the following workflows:
  - Cisco ISE downloads CRL from HTTPS server
  - Cisco ISE downloads CRL from secure LDAP server
  - Cisco ISE as secure TCP syslog client
  - Cisco ISE as secure LDAP client

Support for Network Device with IPv6 Address

Cisco ISE allows you to configure the network devices with IPv4 or IPv6 address. You can also export and import the network devices with IPv4 or IPv6 address.

You can also add IPv4 or IPv6 address for the Device IP address attribute in the conditions and rules used in the authentication and authorization policies.

Support for Network Device IP Address Range with Exclude Option

Cisco ISE allows you to exclude an IP address or IP address ranges from the specified range of IP addresses during authentication.

Upgrade Enhancements

Cisco ISE offers an Upgrade Readiness Tool (URT) that you can run to detect and fix any data upgrade issues before you start the upgrade process. Most of the upgrade failures occur because of data upgrade issues. The URT is designed to validate the data before upgrade to identify, and report or fix the issue, wherever possible. The URT is available as a separate downloadable bundle that can be run on a Secondary Policy Administration Node or Standalone Node. There is no downtime needed to run this tool.

See the Cisco Identity Services Engine Upgrade Guide, Release 2.3 for more information.

Wireless Setup

ISE Wireless Setup provides a very intuitive workflow to quickly set up common wireless use cases, such as, 802.1X, Guest, BYOD. In just a few steps, the setup workflow configures both ISE and a Cisco wireless controller, for a working end-to-end flow.

Wireless Setup is supported only for new installations. The Wireless Setup menu does not appear, if you upgrade to Cisco ISE 2.2 from an earlier release or restore ISE from a backup.

Note **ISE Wireless Setup is beta software - please do not use Wireless Setup in production networks.**

Note The Wireless Setup feature is disabled by default in Cisco Identity Services Engine, Release 2.2 cumulative patch 2.

System Requirements

Note For more details on Cisco ISE hardware platforms and installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.3*.

Supported Hardware

Cisco ISE software is packaged with your appliance or image for installation. Cisco ISE, Release 2.3 is shipped on the following platforms. After installation, you can configure Cisco ISE with specified component personas (Administration, Policy Service, Monitoring, and pxGrid) on the platforms that are listed in Table 1.

Table 1 Supported Hardware and Personas

Hardware Platform	Persona	Configuration
Cisco SNS-3415-K9 (small)	Any	See the *Cisco Identity Services Engine Hardware Installation Guide* for the appliance hardware specifications.
Cisco SNS-3495-K9 (large)		
Cisco SNS-3515-K9 (small)	Any	See the *Cisco Identity Services Engine Hardware Installation Guide* for the appliance hardware specifications.
Cisco SNS-3595-K9 (large)		
Cisco ISE-VM-K9 (VMware, Linux KVM, Microsoft Hyper-V)		• For CPU and memory recommendations, refer to the "VMware Appliance Sizing Recommendations" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.3*.[1] • For hard disk size recommendations, refer to the "Disk Space Requirements" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.3*. • NIC—1 GB NIC interface required. You can install up to 6 NICs. • Supported virtual machine versions include: ESXi 5.*x* (5.1 U2 and later support RHEL 7), 6.*x* Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later KVM on RHEL 7.0 **Note** If you are installing or upgrading Cisco ISE on an ESXi 5.x server, to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later. RHEL 7 is supported with VMware hardware version 9 and later.

1. Memory allocation of less than 16 GB is not supported for any VM appliance configuration. In the event of a Cisco ISE behavior issue, all users will be required to change allocated memory to at least 16 GB before opening a case with the Cisco Technical Assistance Center.

Note Legacy ACS and NAC appliances (including the Cisco ISE 3300 series) are not supported with Cisco ISE, Release 2.0 and later releases.

FIPS Mode Support

Cisco ISE uses embedded FIPS 140-2 validated cryptographic module, Cisco FIPS Object Module Version 6.0 (Certificate #2505). For details of the FIPS compliance claims, see the FIPS Compliance Letter.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- VMware ESXi 5.*x* (5.1 U2 and later support RHEL 7), 6.*x*
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on RHEL 7.0

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

Supported Browsers

Supported browsers for the Admin portal include:

- Mozilla Firefox 69 and earlier versions
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 77 and earlier versions
- Microsoft Internet Explorer 10.x and 11.x
  - If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).
  - If you use Chrome 65.0.3325.189, you may be unable to view guest account details in the print preview section.
  - You might see a warning message while downloading an executable (EXE) file in Google Chrome 76 or later. To resolve this issue:

  a. In your browser, click the **Settings** menu at the top-right corner.

  b. At the bottom of the **Settings** window, click **Advanced**.

  c. Under **Downloads**, check the **Ask Where to Save Each File before Downloading** check box.

Support for Microsoft Active Directory

Cisco ISE, Release 2.3 works with Microsoft Active Directory servers 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, and 2016 at all functional levels.

Note Microsoft has ended support for Windows Server 2003 and 2003 R2. We recommend that you upgrade Windows Server to a supported version.

Microsoft Active Directory version 2000 or its functional level is not supported by Cisco ISE.

Cisco ISE 2.3 supports Multi-Forest/Multi-Domain integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 2.3 supports up to 50 domain join points.

Supported Anti-Virus and Anti-Malware Products

For more information on the products supported by the ISE posture agent, see the Cisco AnyConnect ISE Posture Support Charts in the following link:

https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

Supported Cipher Suites

Cisco ISE 2.3 supports TLS versions 1.0, 1.1, and 1.2. Cisco ISE supports RSA and ECDSA server certificates. Cisco ISE supports the following elliptic curves:

- secp256r1
- secp384r1
- secp521r1

The following table lists the supported Cipher Suites for Cisco ISE 2.3.

Table 2 Supported Cipher Suites

Cipher suite	EAP server RADIUS DTLS server	Download CRL from HTTPS Download CRL from LDAPS Secure TCP syslog client Secure LDAP client RADIUS DTLS client for CoA
TLS 1.0 support	When TLS 1.0 is allowed (DTLS server supports only DTLS 1.2) **Note** Allow TLS 1.0 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.0 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.0, check the Allow TLS 1.0 check box in the Security Settings page (Administration > System > Settings > Protocols > Security Settings).	When TLS 1.0 is allowed (DTLS client supports only DTLS 1.2)

Table 2 Supported Cipher Suites

TLS 1.1 support	When TLS 1.1 is allowed **Note** Allow TLS 1.1 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.1 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.1, check the Allow TLS 1.1 check box in the Security Settings page (Administration > System > Settings > Protocols > Security Settings).	When TLS 1.1 is allowed
ECC DSA ciphers		
ECDHE-ECDSA-AES256-GCM-SHA384	Yes	Yes
ECDHE-ECDSA-AES128-GCM-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA384	Yes	Yes
ECDHE-ECDSA-AES128-SHA256	Yes	Yes
ECDHE-ECDSA-AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed
ECDHE-ECDSA-AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
ECC RSA ciphers		
ECDHE-RSA-AES256-GCM-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES128-GCM-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA384	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES128-SHA256	When ECDHE-RSA is allowed	When ECDHE-RSA is allowed
ECDHE-RSA-AES256-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
ECDHE-RSA-AES128-SHA	When ECDHE-RSA/SHA-1 is allowed	When ECDHE-RSA/SHA-1 is allowed
DHE RSA ciphers		
DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	When SHA-1 is allowed
DHE-RSA-AES128-SHA	No	When SHA-1 is allowed
RSA ciphers		
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	When SHA-1 is allowed	When SHA-1 is allowed
AES128-SHA	When SHA-1 is allowed	When SHA-1 is allowed
3DES ciphers		

Table 2 Supported Cipher Suites

DES-CBC3-SHA	When 3DES/SHA-1 is allowed	When 3DES/DSS and SHA-1 are enabled
DSS ciphers		
DHE-DSS-AES256-SHA	No	When 3DES/DSS and SHA-1 are enabled
DHE-DSS-AES128-SHA	No	When 3DES/DSS and SHA-1 are enabled
EDH-DSS-DES-CBC3-SHA	No	When 3DES/DSS and SHA-1 are enabled
Weak RC4 ciphers		
RC4-SHA	When “Allow weak ciphers” option is enabled in the Allowed Protocols page and when SHA-1 is allowed	No
RC4-MD5	When “Allow weak ciphers” option is enabled in the Allowed Protocols page	No
EAP-FAST anonymous provisioning only: ADH-AES-128-SHA	Yes	No
Peer certificate restrictions		

Table 2 Supported Cipher Suites

Validate KeyUsage	Client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Validate ExtendedKeyUsage	Client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	Server certificate should have ExtendedKeyUsage=Server Authentication

Installing Cisco ISE Software

To install Cisco ISE, Release 2.3 software on Cisco SNS-3415, SNS-3495, SNS-3515, and SNS-3595 hardware platforms, turn on the new appliance and configure the Cisco Integrated Management Controller (CIMC). You can then install Cisco ISE, Release 2.3 over a network using CIMC or a bootable USB.

Note When using virtual machines (VMs), we recommend that the guest VMs have the correct time set using an NTP server *before* installing the .ISO image or OVA file on the VMs.

Perform Cisco ISE initial configuration according to the instructions in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.3*. Before you run the setup program, ensure that you know the configuration parameters listed in Table 3.

Table 3 Cisco ISE Network Setup Configuration Parameters

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). The first character must be a letter.	isebeta1
(eth0) Ethernet interface address	Must be a valid IPv4 address for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14
Netmask	Must be a valid IPv4 netmask.	255.255.255.0
Default gateway	Must be a valid IPv4 address for the default gateway.	10.12.13.1
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).	mycompany.com
Primary name server	Must be a valid IPv4 address for the primary name server.	10.15.20.25
Add/Edit another name server	(Optional) Allows you to configure multiple name servers. Must be a valid IPv4 address for an additional name server.	Enter **y** to add additional name server or **n** to configure the next parameter.
Primary NTP server	Must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server.	clock.nist.gov
Add/Edit another NTP server	(Optional) Allows you to configure multiple NTP servers. Must be a valid IPv4 address or hostname.	Enter **y** to add additional NTP server or **n** to configure the next parameter.
System Time Zone	Must be a valid time zone. For details, see *Cisco Identity Services CLI Reference Guide, Release 2.3*, which provides a list of time zones that Cisco ISE supports. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT (or UTC-8 hours). The time zones referenced are the most frequently used time zones. You can run the **show timezones** command from the Cisco ISE CLI for a complete list of supported time zones. **Note** We recommend that you set all Cisco ISE nodes to the UTC time zone. This setting ensures that the reports, logs, and posture agent log files from the various nodes in the deployment are always synchronized with the time stamps.	UTC (default)
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (admin), you must create a new username. The username must be three to eight characters in length and composed of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password (there is no default). The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Note For additional information on configuring and managing Cisco ISE, see Release-Specific Document, page 66.

Upgrading to Release 2.3

You can directly upgrade to Release 2.3 from the following Cisco ISE releases:

- 2.0
- 2.0.1
- 2.1
- 2.2

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 2.3.

You can upgrade to Release 2.3 from the GUI or the CLI.

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

Supported Operating System for Virtual Machines

Release 2.3 supports Red Hat Enterprise Linux (RHEL) 7.0.

If you are upgrading Cisco ISE nodes on VMware virtual machines, 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.

Upgrade Considerations and Requirements

New Policy Model

All network access policies and policy sets, including authentication, authorization and exceptions, have now been consolidated together under the improved Policy Sets area, which can be accessed from **Policy > Policy Sets**. Each policy set is a container defined on the top level of the policy hierarchy, under which all relevant Authentication and Authorization policy and policy exception rules for that set are configured.

Multiple rules can be defined for both authentication and authorization, all based on conditions. Conditions and additional related configurations can now also be easily accessed and reused directly from the new Policy Set interface. The order by which the policy sets are matched is determined by the order in which they appear in the new interface, beginning from the first row of the Policy Set table and continuing to check until a match is found. If no match is found then the system default policy set is used. The same logic is used to match and select the correct authentication and then the correct authorization rules, beginning from the top of each table and checking each rule until a match is found. The default rule is used if no other rule is matched.

The new policy model represents all policies that could also have been added in previous versions by using the old user interface, but offering a much more simplified and improved interface from which you can logically manage network access.

Standalone Authentication and Authorization Policy Changes

The standalone authentication rules from ISE 2.2 and below versions are converted to the new policy model. There are two separate scenarios based on the allowed protocols that are assigned to the authentication rules.

1. If all the “outer parts” in the system are assigned the same allowed protocol, including the default part, then all original authentication rules are converted to ISE 2.3 as follows:

- All the “outer parts” are converted to a single policy set in the new policy model. The new policy set will be called Default, and on the Policy Set level, no conditions are defined and the uniform Allowed Protocol will be assigned. All inner parts are converted to rules as part of the authentication policy within the new Default policy set.

  The following table demonstrates the conversion for an old set of standalone authentication rules that use the same allowed protocol (Scenario -1). In the table, each line is in the following format:

  Name (Condition/Results)

  For example for Authentication outer part 1 (Outer Condition/Allowed Protocol A):

  - Name—Authentication outer part 1
  - Condition—Outer Condition
  - Results—Allowed Protocol A

Table 4 Standalone Authentication Policies Using Same Allowed Protocol

Before Cisco ISE 2.3 - Default Authentication	After Upgrade to Cisco ISE 2.3 - Policy Sets
Authentication outer part 1 (Outer Condition 1/Allowed Protocol A) Authentication inner part 1.1 (Inner Condition 1.1/Identity Store A) Authentication inner part 1.2 (Inner Condition 1.2/Identity Store A) Authentication inner part 1.3 (Inner Condition 1.3/Identity Store A) Authentication inner 1 Default (No conditions/Identity Store B) Authentication outer part 2 (Outer Condition 2/Allowed Protocol A) Authentication inner part 2.1 (Inner Condition 2.1/Identity Store A) Authentication inner part 2.2 (Inner Condition 2.2/Identity Store A) Authentication inner part 2.3 (Inner Condition 2.3/Identity Store A) Authentication inner 2 Default (No conditions/Identity Store B) Authentication outer part 3 (Outer Condition 3/Allowed Protocol A) Authentication inner 3 Default (No conditions/Identity Store B) Default Authentication Outer Part (No conditions/Allowed Protocol A/Default Identity Store) Exception 1 Authorization Rule 1 Authorization Rule 2	Default (No conditions/Allowed Protocol A) Authentication Policy (container) Authentication outer part 1 - Authentication inner part 1.1 (Outer Condition 1 + Inner Condition 1.1/Identity Store A) Authentication outer part 1 - Authentication inner part 1.2 (Outer Condition 1 + Inner Condition 1.2/Identity Store A) Authentication outer part 1 - Authentication inner part 1.3 (Outer Condition 1 + Inner Condition 1.3/Identity Store A) Authentication outer part 1 - Authentication inner 1 Default (Outer Condition 1/Identity Store B) Authentication outer part 2 - Authentication inner part 2.1 (Outer Condition 2 + Inner Condition 2.1/Identity Store A) Authentication outer part 2 - Authentication inner part 2.2 (Outer Condition 2 + Inner Condition 2.2/Identity Store A) Authentication outer part 2 - Authentication inner part 2.3 (Outer Condition 2 + Inner Condition 2.3/Identity Store A) Authentication outer part 2 - Authentication inner 2 Default (Outer Condition 2/Identity Store B) Authentication outer part 3 - Authentication inner 3 Default (Outer Condition 3/Identity Store B) Default Authentication Outer Part (No conditions/Default Identity Store) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2

2. If at least one of the “outer parts” in the system are assigned a different allowed protocol than the others, including the default part, then all original authentication rules are converted to 2.3 as follows:

- Each of the “outer parts” is converted to a separate policy set in the new policy model. The new policy set will be named based on the name of the original outer part for that specific new set. On the Policy Set level for each policy set, the original outer part conditions and the Allowed Protocol will be assigned. All inner parts for each outer part are converted to authentication rules, one to one, as part of the authentication policy within their new policy set.

  The following table demonstrates the conversion for an old set of standalone authentication rules that use different allowed protocols (Scenario -2). In the table, each line is in the following format:

  Name (Condition/Results)

  For example for Authentication outer part 1 (Outer Condition/Allowed Protocol A):

  - Name—Authentication outer part 1
  - Condition—Outer Condition
  - Results—Allowed Protocol A

Table 5 Standalone Authentication Policies Using Different Allowed Protocols

Before Cisco ISE 2.3 - Default Authentication	After Upgrade to Cisco ISE 2.3 - Policy Sets
Authentication outer part 1 (Outer Condition 1/Allowed Protocol A) Authentication inner part 1.1 (Inner Condition 1.1/Identity Store A) Authentication inner part 1.2 (Inner Condition 1.2/Identity Store A) Authentication inner part 1.3 (Inner Condition 1.3/Identity Store A) Authentication inner 1 Default (No conditions/Identity Store B) Authentication outer part 2 (Outer Condition 2/Allowed Protocol B) Authentication inner part 2.1 (Inner Condition 2.1/Identity Store A) Authentication inner part 2.2 (Inner Condition 2.2/Identity Store A) Authentication inner part 2.3 (Inner Condition 2.3/Identity Store A) Authentication inner 2 Default (No conditions/Identity Store B) Authentication outer part 3 (Outer Condition 3/Allowed Protocol C) Authentication inner 3 Default (No conditions/Identity Store B) Default Authentication Outer Part (No conditions/Allowed Protocol A/Identity Store C) Exception 1 Authorization Rule 1 Authorization Rule 2	Default Authentication outer part 1 (Outer condition 1/Allowed Protocol A) Authentication Policy (container) Authentication inner part 1.1 (Inner Condition 1.1/Identity Store A) Authentication inner part 1.2 (Inner Condition 1.2/Identity Store A) Authentication inner part 1.3 (Inner Condition 1.3/Identity Store A) Authentication inner 1 Default (No conditions/Identity Store B) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2 Default Authentication outer part 2 (Outer Condition 2/Allowed Protocol B) Authentication Policy (container) Authentication inner part 2.1 (Inner Condition 2.1/Identity Store A) Authentication inner part 2.2 (Inner Condition 2.2/Identity Store A) Authentication inner part 2.3 (Inner Condition 2.3/Identity Store A) Authentication inner 2 Default (No conditions/Identity Store B) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2 Default Authentication outer part 3 (Outer Condition 3/Allowed Protocol C) Authentication Policy (container) Authentication inner 3 Default (No conditions/Identity Store B) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2 Default (No conditions/Allowed Protocol A) Authentication Policy (container) Default Authentication Rule (No conditions/Identity Store C) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2

Policy Set Changes

When upgrading to ISE 2.3 from previous versions, the new policy sets appear differently than older ISE versions as described here, however, the behavior remains exactly the same.

The policies from ISE 2.2 and below versions are converted to the new policy model. There are two separate scenarios based on the allowed protocols that are assigned to the authentication rules.

1. If all the “outer parts” in a single policy set are assigned the same allowed protocol, all original policy sets are converted to ISE 2.3 as follows:

- All the “outer parts” are converted to a single policy set in the new policy model. The new policy set will have the same name as that of the original policy set. For example, if the policy set was named “All Employees” in the old model, it will be called “All Employees” in the new model as well.

  The following table demonstrates the conversion for an old policy set that contains authentication rules which use the same allowed protocol (Scenario -1). In the table, each line is in the following format:

  Name (Condition/Results)

  For example for Authentication outer part 1 (Outer Condition/Allowed Protocol A):

  - Name—Authentication outer part 1
  - Condition—Outer Condition
  - Results—Allowed Protocol A

Table 6 Conversion of Policy Sets Using Same Allowed Protocol

Old policy set from Cisco ISE 2.2 or earlier	New policy sets after upgrade to Cisco ISE 2.3
Policy Set A (Condition A/No results) Authentication outer part 1 (Outer Condition 1/Allowed Protocol A) Authentication inner part 1.1 (Inner Condition 1.1/Identity Store A) Authentication inner part 1.2 (Inner Condition 1.2/Identity Store A) Authentication inner part 1.3 (Inner Condition 1.3/Identity Store A) Authentication inner 1 Default (No conditions/Identity Store B) Authentication outer part 2 (Outer Condition 2/Allowed Protocol A) Authentication inner part 2.1 (Inner Condition 2.1/Identity Store A) Authentication inner part 2.2 (Inner Condition 2.2/Identity Store A) Authentication inner part 2.3 (Inner Condition 2.3/Identity Store A) Authentication inner 2 Default (No conditions/Identity Store B) Authentication outer part 3 (Outer Condition 3/Allowed Protocol A) Authentication inner 3 Default (No conditions/Identity Store B) Default Authentication Outer Part (No conditions/Allowed Protocol A/Identity Store C) Exception 1 Authorization Rule 1 Authorization Rule 2	Policy Set A (Condition A/Allowed Protocol A) Authentication Policy (container) Authentication outer part 1 - Authentication inner part 1.1 (Outer Condition 1 + Inner Condition 1.1/Identity Store A) Authentication outer part 1 - Authentication inner part 1.2 (Outer Condition 1 + Inner Condition 1.2/Identity Store A) Authentication outer part 1 - Authentication inner part 1.3 (Outer Condition 1 + Inner Condition 1.3/Identity Store A) Authentication outer part 1 - Authentication inner 1 Default (Outer Condition 1/Identity Store B) Authentication outer part 2 - Authentication inner part 2.1 (Outer Condition 2 + Inner Condition 2.1/Identity Store A) Authentication outer part 2 - Authentication inner part 2.2 (Outer Condition 2 + Inner Condition 2.2/Identity Store A) Authentication outer part 2 - Authentication inner part 2.3 (Outer Condition 2 + Inner Condition 2.3/Identity Store A) Authentication outer part 2 - Authentication inner 2 Default (Outer Condition 2/Identity Store B) Authentication outer part 3 - Authentication inner 3 Default (Outer Condition 3/Identity Store B) Default Authentication Outer Part (No conditions/Identity Store C) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2

- The newly upgraded policy set contains a list of authentication rules that are converted by combining the outer and inner conditions from the original policy set. Each new authentication rule that is created during conversion is named based on the name of the old outer part with the suffix including the inner part name. For example, as in the table above, if the old policy set is called "Policy Set A," one of its authentication "outer parts" is called Outer Part 1, and one of its authentication "inner parts" is called Inner Part 1, then the newly created authentication rule is called "Outer Part 1 – Inner Part 1" within Policy Set A. In the same manner, if the old policy set is called "All Employees" policy set, one of its authentication "outer parts" is called London, and one of its authentication "inner parts" is called Wired - MAB, then the newly created authentication rule is called "London –

Wired-MAB" within the “All Employees” policy set. The Default outer part for the authentication policy is converted as the default authentication rule. The system default policy rule appears as the last rule in the entire authentication table, regardless of the other rules that were created or converted, and this rule cannot be moved or deleted.

- The conditions defined on the outer part (based on which the authentication rules are matched) are combined with the inner part conditions (which indicate the identity store to be used for authentication). The new combined conditions are configured in a single authentication rule within the policy set in the new model. A new individual rule within the policy set is created for each separate outer part of the old policy set.

2. When there are two or more allowed protocols selected for the “outer parts” in a policy set, all original policy sets are converted to ISE 2.3 as follows:

- Each “outer part” of each authentication rule within the old policy set is converted to a new, separate policy set in the new model. This new policy set places the “conditions” from the same original “outer part” under the Authentication Policy section in the new policy model.

  The following table demonstrates the conversion for an old policy set from ISE 2.2 and previous versions to ISE 2.3 (Scenario - 2):

Old policy set from Cisco ISE 2.2 or earlier	New policy sets after upgrade to Cisco ISE 2.3
Policy Set A (Condition A/No results) Authentication outer part 1 (Outer Condition 1/Allowed Protocol A) Authentication inner part 1.1 (Inner Condition 1.1/Identity Store A) Authentication inner part 1.2 (Inner Condition 1.2/Identity Store A) Authentication inner part 1.3 (Inner Condition 1.3/Identity Store A) Authentication inner 1 Default (No conditions/Identity Store B) Authentication outer part 2 (Outer Condition 2/Allowed Protocol A) Authentication inner part 2.1 (Inner Condition 2.1/Identity Store A) Authentication inner part 2.2 (Inner Condition 2.2/Identity Store A) Authentication inner 2 Default (No conditions/Identity Store B) Authentication outer part 3 (Outer Condition 3/Allowed Protocol A) Authentication inner 3 Default (No conditions/Identity Store B) Default Authentication Outer Part (No conditions/Allowed Protocol A/Identity Store C) Exception 1 Authorization Rule 1 Authorization Rule 2	Policy Set A - Authentication outer part 1 (Condition A + Outer condition 1/Allowed Protocol A) Authentication Policy (container) Authentication inner part 1.1 (Inner Condition 1.1/Identity Store A) Authentication inner part 1.2 (Inner Condition 1.2/Identity Store A) Authentication inner part 1.3 (Inner Condition 1.3/Identity Store A) Authentication inner 1 Default (No conditions/Identity Store B) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2 Policy Set A - Authentication outer part 2 (Condition A + Outer condition 2/Allowed Protocol B) Authentication Policy (container) Authentication inner part 2.1 (Inner Condition 2.1/Identity Store A) Authentication inner part 2.2 (Inner Condition 2.2/Identity Store A) Authentication inner 2 Default (No conditions/Identity Store B) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2 Policy Set A - Default Authentication outer part 3 (Condition A + Outer Condition 3/Allowed Protocol C) Authentication Policy (container) Authentication inner 3 Default (No conditions/Identity Store B) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2 Policy Set A - Default (Condition A/Allowed Protocol A) Authentication Policy (container) Default Authentication Rule (No conditions/Identity Store C) Exception 1 Authorization Policy (container) Authorization Rule 1 Authorization Rule 2

- Each new policy set that is created during conversion is named based on the name of the old policy set from which it was extracted with the suffix including the outer part name. For example, as in the table above, if the old policy set is called “Policy Set A” and one of its authentication “outer parts” is called Outer Part 1, then the newly created policy set is called “Policy Set A – Outer Part 1.” In the same manner, if the old policy set is called “London” and one of its authentication “outer parts” is called Wired MAB, then the newly created policy set is called “London – Wired MAB.”

  The Default outer part for each old policy set is also converted to a new policy set just as are all the other outer parts, for example “London – Default”. The system default policy set appears as the last policy set in the entire table, regardless of the other policy sets that were created or converted, and cannot be moved or deleted.
- The conditions defined on the top level of the old policy set are combined with the outer authentication part conditions, designed to select the correct allowed protocol. The new combined conditions are configured in the top level rule for each new policy set in the new model. A new individual policy set is created for each outer part of each old policy set.

Authorization Rule/Exception Changes

Authorization rules, as well as global and local exceptions, are also maintained from within the policy sets now. All authorization rules and exceptions within the old policy set are applied to all of the new policy sets resulting from the authentication policy rule conversion as well. The authorization policy changes are applicable for all the policy sets that are upgraded, regardless of the allowed protocols configured on the outer parts.

Policy Sets Evaluation

The policy sets in the new interface are checked for matches according to the order in which they appear in the Policy Set table. For example, if the old “London” policy set has three outer parts with different statuses before conversion, and the old “New York” set contains only the Default outer part, then the table in the new Policy Set interface appears with the new policy sets and the system default policy set in the following order:

Policy Set Name
London – Wired MAB
London – Wireless MAB
London – Default
New York - Default
Default

If the first two sets don’t match, then the system checks “London –Default”. If “London – Default” does not match, then the system checks “New York – Default”. The system only uses “Default” as the policy if “New York – Default” also does not match.

The same logic is used to match and select the correct authentication and then the correct authorization rules, beginning from the top of each table and checking each rule until a match is found. The default rule is used, if no other rule is matched.

Status of the Newly Converted Policy Sets

While converting policy sets that use different Allowed Protocols for the authentication rules, the statuses of the newly converted policy sets are determined based on the status of old policy sets and the status of the “outer part” of the old policy sets, as follows:

Status of Old policy set	Status of “outer part” of old policy set	Status of new policy set
Disable	Disable	Disable
Disable	Monitor	Disable
Disable	Enable	Disable
Monitor	Disable	Disable
Monitor	Monitor	Monitor
Monitor	Enable	Monitor
Enable	Disable	Disable
Enable	Monitor	Monitor
Enable	Enable	Enable

Status of the Newly Converted Authentication Rules

While converting policy sets that use same Allowed Protocols for the authentication rules, the status of the newly converted authentication rule is determined based on the status of the "outer part" of the old authentication rule and the status of the “inner part” of the corresponding old authentication rule, as follows:

Status of "Outer Part" of Old Authentication Rule	Status of “Inner Part” of Corresponding Old Authentication Rule	Status of the Converted Authentication Rule
Disable	Disable	Disable
Disable	Monitor	Disable
Disable	Enable	Disable
Monitor	Disable	Disable
Monitor	Monitor	Monitor
Monitor	Enable	Monitor
Enable	Disable	Disable
Enable	Monitor	Monitor
Enable	Enable	Enable

Prepare for Upgrade

Before you start the upgrade process, ensure that you perform the following tasks:

- Change VMware virtual machine guest operating system and settings
- Open firewall ports for communication
- Back up configuration and operational data
- Back up system logs
- Check the validity of certificates
- Export certificates and private keys
- Disable PAN automatic failover and backup schedules before upgrade
- NTP server should be configured correctly and be reachable
- Record profiler configuration
- Obtain Active Directory and internal administrator account credentials
- Activate MDM vendor before upgrade
- Create repository and copy the upgrade bundle
- Check load balancer configuration

Refer to the *Cisco ISE Upgrade Guide, Release 2.3* for a list of pre and post upgrade tasks.

Cisco Secure ACS to Cisco ISE Migration

You can directly migrate to Cisco ISE, Release 2.3 only from Cisco Secure ACS, Release 4.2 and 5.5 or later. See *Cisco Identity Services Engine Migration Tool Guide* for more information.

You cannot migrate to Release 2.3 from Cisco Secure ACS 5.1, 5.2, 5.3, 5.4, 4.1, or earlier versions, or from Cisco Network Admission Control (NAC) Appliance. From Cisco Secure ACS, Releases 4.1, 5.1, 5.2, 5.3, or 5.4, you must upgrade to a supported version, and then migrate to Cisco ISE, Release 2.3.

Note If you are installing Cisco ISE, Release 2.3 on Cisco SNS-3500 series appliances with ACS PIDs (Cisco SNS-3515-ACS-K9 and Cisco SNS-3595-ACS-K9), you must update the BIOS and CIMC firmware on the hardware appliance before you install Cisco ISE, Release 2.3. Refer to the *Cisco Identity Services Engine Hardware Installation Guide* for information on how to update the BIOS and CIMC firmware.

Known Limitations

SXP Protocol Security Standards

SXP protocol transfers unencrypted data and uses weak hash algorithm for message integrity checking per draft-smith-kandula-sxp-06.

Radius Logging

Starting with ISE version 2.3, Radius logs are only kept for 7 days.

Profiler RADIUS Probe

When the RADIUS probe is disabled, endpoints are not profiled but are only authenticated and added to the database.

High Memory Utilization

Cisco ISE Version 1.3 and later use RHEL, version 6. You may experience high memory utilization after installing or upgrading to Cisco ISE Version 1.3 or later. 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. If the memory usage is consistently above 90% or if there is any performance impact, you can contact Cisco TAC for troubleshooting.

Diffie-Hellman Minimum Key Length

Connection to LDAP server will fail if the Diffie-Hellman minimum key length configured on the LDAP server is less than 1024.

Policy Hits Displayed in Policy Sets

The total hits counter that is displayed at the top of the policy set is updated whenever Cisco ISE receives interim accounting updates. However, the authentication and authorization policy hit counters are not refreshed based on interim accounting updates. Hence, you might see some difference between the total hits displayed in the policy set summary and the total number of authentication and authorization policies displayed in the Authentication Policy and Authorization Policy sections.

ECDSA Certificates

- ECDSA certificates that are used for EAP authentication are supported only for the endpoints with Android version 6.x and later.

- Cisco ISE supports ECDSA certificates with key length 256 and 384 only. You can select the key length in **Administration > System > Certificates > Certificate Management > System Certificates page**.

Cisco Temporal Agent

We recommend that you run the Cisco Temporal Agent within two minutes of downloading the agent from the Client Provisioning Portal, if not, you might encounter the "Posture Failed Due to Server Issues" error message.

Reverse DNS Lookup Configuration

Configure reverse DNS lookup for all Cisco ISE nodes in your distributed deployment in the DNS server(s). Otherwise, you may run into deployment-related issues after upgrade ("ISE Indexing Engine" status turns to "not running"). The secondary PAN cannot join the primary PAN to make a cluster for ISE Indexing engine if reverse DNS is not configured (displays error in VCS pages).

The ise-elasticsearch.log file on secondary PAN will include the SSL Exception "No subject alternative name present", if reverse DNS is missing.

Alarm Message After Applying a Patch

After applying a patch, you may get an alarm, followed by a message that the patch application was successful. You can ignore the alarm.

Security Group Access Control List

In Cisco ISE, Release 2.3, patch 6, when you try to create a Security Group ACL (SGACL), the following error message is displayed:

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

This is because creating and updating egress matrix cell flows are not supported for multiple matrixes in Cisco ISE.

The following ERS(External RESTful Services) requests are also not supported in the Multiple Matrix mode:

/config/egressmatrixcell/*

/config/sgt/*

/config/sgacl/*

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

EST Service Does Not Run in Cisco ISE 2.1

After a fresh installation of Cisco ISE 2.1, when you run the **show application status ise** command, the EST service might be shown as disabled. This issue occurs when the root certificate of the Cisco ISE internal CA is signed by an external CA and the external CA certificate is not present in your Trusted Certificates store. Import the external CA certificate in to the Trusted Certificates store to bring up the EST service.

This issue is also seen after upgrade to Release 2.1, if the entire certificate chain of the internal ISE CA is not present. You must generate the Cisco ISE CA chain to bring up the EST service.

Features Not Supported in Cisco ISE, Release 2.3

- IPN / iPEP configuration is not supported with Cisco ISE, Release 2.0 and later.
- You cannot access the Operations menu from the primary Monitoring node in Cisco ISE, Release 2.1 and later; it appears only in the Primary Administration Node (PAN).

Cisco ISE License Information

Cisco ISE licensing provides the ability to manage the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources.

All Cisco ISE appliances are supplied with a 90-day Evaluation license. To continue to use Cisco ISE services after the 90-day Evaluation license expires, and to support more than 100 concurrent endpoints on the network, you must obtain and register Base licenses for the number of concurrent users on your system. If you require additional functionality, you will need Plus and/or Apex licenses to enable that functionality.

Cisco ISE, Release 2.3, supports licenses with two UIDs. You can obtain a license based on the UIDs of both the primary and secondary Administration nodes.

For more detailed information on license types and obtaining licenses for Cisco ISE, see the “Cisco ISE Licenses” chapter in the *Cisco Identity Services Engine Administration Guide, Release 2.3*.

For more information on Cisco ISE, Release 2.3 licenses, see the *Cisco Identity Services Engine Data Sheet*.

Cisco Identity Services Engine Ordering Guide is available at:
http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/guide_c07-656177.pdf

Deployment Terminology, Node Types, and Personas

Cisco ISE provides a scalable architecture that supports both standalone and distributed deployments.

Table 7 Cisco ISE Deployment Terminology

Term	Description
Service	Specific feature that a persona provides such as network access, profiler, posture, security group access, and monitoring.
Node	Individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as software that can be run on a VMware server. Each instance (either running on a Cisco ISE appliance or on a VMware server) that runs the Cisco ISE software is called a node.
Persona	Determines the services provided by a node. A Cisco ISE node can assume any or all of the following personas: Administration, Policy Service, Monitoring, and pxGrid.
Deployment Model	Determines if your deployment is a standalone, high availability in standalone (a basic two-node deployment), or distributed deployment.

Types of Nodes and Personas

A Cisco ISE network has the following types of nodes:

- Cisco ISE node, which can assume any of the following personas:
  - Administration—Allows you to perform all administrative operations for Cisco ISE. It handles all system-related configurations related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have one or a maximum of two nodes running the Administration persona and configured as a primary and secondary pair. If the primary Administration node goes down, you have to manually promote the secondary Administration node. There is no automatic failover for the Administration persona.
  - Policy Service—Provides network access, posturing, BYOD device onboarding (native supplicant and certificate provisioning), guest access, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assuming this persona. Typically, there is more than one Policy Service persona in a distributed deployment. All Policy Service personas that reside behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes in that group process the requests of the node that has failed, thereby providing high availability.

Note SXP service must be enabled on a dedicated node.

  - Monitoring—Enables Cisco ISE to function as a log collector and store log messages from all the Administration and Policy Service personas on the Cisco ISE nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources.

    A node with this persona aggregates and correlates the data that it collects to provide meaningful reports. Cisco ISE allows a maximum of two nodes with this persona that can assume primary or secondary roles for high availability. Both the primary and secondary

Monitoring personas collect log messages. In case the primary Monitoring persona goes down, the secondary Monitoring persona automatically assumes the role of the primary Monitoring persona.

Note At least one node in your distributed setup should assume the Monitoring persona. It is recommended that the Monitoring persona be on a separate, designated node for higher performance in terms of data collection and reporting.

- pxGrid—Cisco pxGrid is a method for network and security devices to share data with other devices through a secure publish and subscribe mechanism. These services are applicable for applications that are used external to ISE and that interface with pxGrid. The pxGrid services can share contextual information across the network to identify the policies and to share common policy objects. This extends the policy management.

Table 8 Recommended Number of Nodes and Personas in a Distributed Deployment

Node / Persona	Minimum Number in a Deployment	Maximum Number in a Deployment
Administration	1	2 (Configured as a high-availability pair)
Monitor	1	2 (Configured as a high-availability pair)
Policy Service	1	• 2—when the Administration/Monitoring/Policy Service personas are on the same primary/secondary appliances • 5—when Administration and Monitoring personas are on same appliance • 40—when each persona is on a dedicated appliance
pxGrid	0	2 (Configured as a high-availability pair)

You can change the persona of a node. See the "Set Up Cisco ISE in a Distributed Environment" chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.3* for information on how to configure personas on Cisco ISE nodes.

Requirements for CA to Interoperate with Cisco ISE

While using a CA server with Cisco ISE, make sure that the following requirements are met:

- Key size should be 1024, 2048, or higher. In CA server, the key size is defined using certificate template. You can define the key size on Cisco ISE using the supplicant profile.
- Key usage should allow signing and encryption in extension.
- While using GetCACapabilities through the SCEP protocol, cryptography algorithm and request hash should be supported. It is recommended to use RSA + SHA1.
- Online Certificate Status Protocol (OCSP) is supported. This is not directly used in BYOD, but a CA which can act as an OCSP server can be used for certificate revocation.

Note EJBCA 4.x is not supported by Cisco ISE for proxy SCEP. EJBCA is supported by Cisco ISE for standard EAP authentication like PEAP, EAP-TLS, and so on.

- If you use an enterprise PKI to issue certificates for Apple iOS devices, ensure that you configure key usage in the SCEP template and enable the "Key Encipherment" option. For example, if you use Microsoft CA, edit the Key Usage Extension in the certificate template. In the Encryption area, click the **Allow key exchange only with key encryption (key encipherment)** radio button and also check the **Allow encryption of user data** check box.
- Cisco ISE supports the use of RSASSA-PSS algorithm for trusted certificates and endpoint certificates for EAP-TLS authentication. When you view the certificate, the signature algorithm is listed as 1.2.840.113549.1.1.10 instead of the algorithm name.

However, if you use the Cisco ISE internal CA for the BYOD flow, the Admin certificate should not be signed using the RSASSA-PSS algorithm (by an external CA). The Cisco ISE internal CA cannot verify an Admin certificate that is signed using this algorithm and the request would fail.

Telemetry

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

Cisco ISE Installation Files, Updates, and Client Resources

There are three resources you can use to download to provision and provide policy service in Cisco ISE:

- Cisco ISE Downloads from the Download Software Center, page 34
- Cisco ISE Live Updates, page 35
- Cisco ISE Offline Updates, page 36

Cisco ISE Downloads from the Download Software Center

In addition to the .ISO installation package required to perform a fresh installation of Cisco ISE as described in Installing Cisco ISE Software, page 15, you can use the Download software web page to retrieve other Cisco ISE software elements, like Windows and Mac OS X agent installers and AV/AS compliance modules.

Downloaded agent files may be used for manual installation on a supported endpoint or used with third-party software distribution packages for mass deployment.

To access the Cisco Download Software center and download the necessary software:

Step 1 Go to the Download Software web page at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm. You may need to provide login credentials.

Step 2 Choose **Products > Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

The following Cisco ISE installers and software packages are available for download:

- Cisco ISE installer.ISO image
- Supplicant Provisioning Wizards for Windows and Mac OS X Native Supplicants
- Windows client machine agent installation files (including MST and MSI versions for manual provisioning)
- Mac OS X client machine agent installation files
- AnyConnect agent installation files
- AV/AS compliance modules

Step 3 Click **Download** or **Add to Cart**.

Cisco ISE Live Updates

Cisco ISE Live Update locations allow you to automatically download Supplicant Provisioning Wizard, Cisco NAC Agent for Windows and Mac OS X, AV/AS support (Compliance Module), and agent installer packages that support client provisioning and posture policy services. These live update portals should be configured in Cisco ISE upon initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the Cisco ISE appliance.

Prerequisite:

If the default Update Feed URL is not reachable and your network requires a proxy server, you must configure the proxy settings in **Administration > System > Settings > Proxy** before you access the Live Update locations. If proxy settings are enabled to allow access to the profiler and posture/client provisioning feeds, it will break access to the MDM server as Cisco ISE cannot bypass proxy services for MDM communication. To resolve this, you can configure the proxy service to allow communication to the MDM servers. For more information on proxy settings, see the "Specify Proxy Settings in Cisco ISE" section in the "Administer Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.3*.

Client Provisioning and Posture Live Update portals:

- **Client Provisioning portal**—https://www.cisco.com/web/secure/pmbu/provisioning-update.xml

  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 become available at this 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 2.3*.

- **Posture portal**—https://www.cisco.com/web/secure/pmbu/posture-update.xml

  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 "Configure Client Posture Policies" chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.3*.

If you do not want to enable the automatic download capabilities described above, you can choose to download updates offline (see Cisco ISE Offline Updates, page 36).

Cisco ISE Offline Updates

Cisco ISE offline updates allow you to manually download Supplicant Provisioning Wizard, agent, AV/AS support, compliance modules, and agent installer packages that support client provisioning and posture policy services. This option allows you to upload client provisioning and posture updates when direct Internet access to Cisco.com from a Cisco ISE appliance is not available or not permitted by a security policy.

Offline updates are also available for Profiler Feed Service. For more information, see the Configure Profiler Feed Services Offline section in the *Cisco Identity Services Engine Administrator Guide*.

To upload offline client provisioning resources:

Step 1 Go to the Download Software web page at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm. You may need to provide login credentials.

Step 2 Choose **Products > Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

The following Off-Line Installation Packages are available for download:

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

Step 3 Click **Download** or **Add to Cart**.

For more information on adding the downloaded installation packages to Cisco ISE, refer to the "Add Client Provisioning Resources from a Local Machine" section in the "Configure Client Provisioning" chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.3*.

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

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

To upload offline posture updates:

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

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 Macintosh operating systems.

Step 2 Launch the Cisco ISE administrator user interface and choose **Administration > System > Settings > Posture**.

Step 3 Click the arrow to view the settings for posture.

Step 4 Choose **Updates**.

The Posture Updates page appears.

Step 5 Choose the **Offline** option.

Step 6 Click **Browse** to locate the archive file (posture-offline.zip) from the local folder on your system.

Note The File to Update field is a required field. You can select only a single archive file (.zip) that contains the appropriate files. Archive files other than .zip (like .tar, and .gz) are not allowed.

Step 7 Click the **Update Now** button.

Using the Bug Search Tool

You can use the Bug Search Tool to view the list of outstanding and resolved bugs in a release. This section explains how to use the Bug Search Tool to search for a specific bug or to search for all the bugs in a specified release.

Step 1 Go to https://tools.cisco.com/bugsearch/search.

Step 2 Enter your registered Cisco.com username and password, and then click **Log In**.

The Bug Toolkit page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the **Search For** field and press Enter.

Step 4 To search for bugs in the current release:

a. Click the **Select from List** link.

   The Select Product page is displayed.

b. Choose **Security > Access Control and Policy > Cisco Identity Services Engine (ISE) 3300 Series Appliances**.

c. Click **OK**.

d. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs based on different criteria, such as status, severity, or modified date.

Click the **Export Results to Excel** link in the Search Results page to export all the bug details from your search to an Excel spreadsheet. Presently, up to 10,000 bugs can be exported at a time to the Excel spreadsheet.

Download and Install a New Patch

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.3, 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, refer to the "Installing a Software Patch" section of the "Administer Cisco ISE" chapter of the Cisco Identity Services Engine Administrator Guide, Release 2.3.

For instructions to install a patch using CLI, refer to the "Patch Install" section of the "Cisco ISE CLI Commands in EXEC Mode" chapter of the Cisco Identity Services Engine CLI Reference Guide, Release 2.3.

Cisco ISE, Release 2.3.0.298 Patch Updates

This section provides information on patches that were made available after the initial availability of the Cisco ISE 2.3 release. Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions. Cisco ISE version 2.3.0.298 was the initial version of the Cisco ISE 2.3 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 "2.3.0.298 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, "2.3(0.9NN)" where NN is also the patch number, displayed as two digits. For example, version "2.3.0.298 patch 1" corresponds to the following version in the bug database "2.3(0.901)".

Note We recommend you to clear your browser cache after you install a patch on Cisco ISE, Release 2.3.

The following patch releases apply to Cisco ISE release 2.3:

Resolved Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 7

Table 10 lists the caveats that are resolved in Cisco Identity Services Engine, Release 2.3 cumulative patch 7. Patch 7 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.2.1.43 or later and Windows users need to upgrade their SPW to WinSPWizard 2.2.1.53 or later.

Table 9 Cisco ISE Patch Version 2.3.0.298 - Patch 7 Resolved Caveats

Caveat ID Number	Description
CSCvp98834	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities
CSCvb56579	Device Name is truncated after 14 characters in the SXP devices page
CSCvc71193	Number of active endpoints incorrectly displayed in the dashboard
CSCvc71503	Endpoints lose static group assignment
CSCvd88480	Location filter for ERS Network Device get-all API fails
CSCvf29640	ISE 2.2 ADE-OS fails to apply some SNMP commands after reload
CSCvf33851	ISE 2.1+ RBAC: Not able to manage endpoints and assign static identity groups
CSCvf35700	MnT database collation errors are seen even if MnT persona is not enabled and high CPU is seen on PAP nodes
CSCvf45991	Pseudo double authentication request on AD
CSCvf52671	TACACS+ authentication report to display the command executed
CSCvf77462	Getting exception in profiler.log: Failed to classify end point
CSCvg36508	MnT live log does not contain endpoint information
CSCvg48457	ISE 2.3 crypto keys are not displayed when show crypto key command is used
CSCvg70813	ISE dmp files are not deleted from /opt/oracle/base/admin/cpm10/dpdump for failed backup attempts
CSCvg71593	Configuration change is not applied on PSN while having multiple certificate updates on deployment
CSCvg72876	Internal CA certificate update traffic between PAN and PSN causing failure to process NAD update

Table 9 Cisco ISE Patch Version 2.3.0.298 - Patch 7 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvh09779	ISE 2.x TACACS log extremely slow
CSCvh30067	ISE 2.2 PSN crash intermittently
CSCvi17534	ISE Application server stuck in initializing state when CTS matrix ID is Null
CSCvi18412	ISE 2.3 p2 is sending redundant CoA message during VPN Posture Flow
CSCvi24236	Deletion of ANC policies when used in Authorization Policy disables ANC
CSCvi27613	Endpoints are profiled even though profiling is disabled
CSCvi29048	ISE node could fall back to Eval System Profile in some cases
CSCvi29759	No profiling policy available for Samsung S7 and S8 profile
CSCvi41678	Endpoint Attributes not updated in context visibility
CSCvi80094	ERS API that requires CSRF token returns HTTP 404 instead of 403
CSCvi99138	ad_agent.log flooded with entries from non-whitelisted domains
CSCvj02644	Blank Details page in RADIUS Live Logs
CSCvj02829	SCCM MDM attribute LastPolicyRequest is not converted correctly in ISE
CSCvj31598	Import two CA certificates with same subject name
CSCvj81752	Upgrade Readiness Tool fails at import due to ORA-31684
CSCvk01929	Making name changes to the "All_User_ID_Stores" Identity Source Sequence will break new policy sets
CSCvk40421	Not able to delete certificate from trusted page
CSCvk43032	"No data found" message seen in live logs and ISE dashboard data not populated correctly
CSCvk48315	Live sessions are not displayed in ISE Live logs page in ISE 2.4
CSCvk76510	ISE Core dump on primary node: SIGSERV in GenericConfigObject::getAsNested(unsigned int) const
CSCvk76680	ISE-PIC Self signed certificate delete operation fails due to Secure Syslog Server reference error
CSCvm03842	PxGrid SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection - CVE-2009-3555
CSCvm35110	MNT node not purging data diligently before hitting 90% purge data disk utilization
CSCvm48075	Manual CoA fails from Context Visibility if Live logs or Live Sessions page is not accessed before
CSCvm70858	Triggered SNMP query not working properly for HP OUI
CSCvm81230	Cisco Identity Services Engine (ISE) Arbitrary Client Certificate Creation Vulnerability
CSCvm86025	ISE 2.3 RADIUS Request/Accounting-Request dropped without failure reason and resolution
CSCvm87292	Unable to integrate Tenable adapter to ISE 2.2 and above
CSCvn12442	Under heavy load, ISE live logs stop working on ISE 2.3
CSCvn21316	ISE: logwatch process failed with ::1 fatal error

Table 9 Cisco ISE Patch Version 2.3.0.298 - Patch 7 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvn21926	Parser error seen in Threat Centric NAC CTA configuration irrespective of ISE version
CSCvn31337	Exception thrown while adding email address in NTP Service Failure alarm
CSCvn35142	ISE 2.3: Posture report for endpoint by condition not working as expected
CSCvn36029	Date in Unix Epoch format when context visibility data is exported
CSCvn40822	Guest creation fails in ISE 2.3 patch 5
CSCvn52114	Authentication request is not sent to external RADIUS token server if communication between client and ISE is in IPv6 and between ISE and external radius token server is in IPv4
CSCvn59383	ISE 2.3 patch 5 issue when creating guest user on sponsor portal using special character
CSCvn64652	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvn66198	Sponsor portal doesn't refresh the accounts after deleting users and requires a manual refresh
CSCvn72150	Nodes have high IO spikes frequently in VM performance reports
CSCvn73740	EAP-TLS authentications with Endpoint profile set to not unknown fails in second authorization.
CSCvn75396	Authentications are not displayed 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 log filtering not functioning when both endpoint profile and authorization policy are selected
CSCvn85484	Removing SCEP RA Profile causes the associated CA chain to be removed from Trusted Store
CSCvn92246	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
CSCvo05269	Unable to use profiling policy in authorization condition
CSCvo11090	Able to delete ACI IEPG in ISE
CSCvo17704	ISE 2.4 - CLI password will not accept 3 $ characters
CSCvo19076	Cannot select ACTIVEDIRECTORY dictionary as an attribute for endpoint purge policy
CSCvo19377	Successful Authentication Entries not shown in the RADIUS report if CSV limit is exceeded
CSCvo24593	Pagination is not working in "All SXP mappings" page in ISE
CSCvo28578	ISE 2.3 - Location info and IPSEC info are reversed in order in Network Device Groups for some NADs
CSCvo31313	Change password for few of the internal users not working after upgrade to 2.6
CSCvo32279	APIC logs not seen in sxp.log when SXP logging set to 'DEBUG'.

Table 9 Cisco ISE Patch Version 2.3.0.298 - Patch 7 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvo35144	Delay in clearing SXP mappings in ISE
CSCvo35516	Device Sensor not able to correctly parse DHCP attributes via RADIUS probe
CSCvo36837	Admin group cannot get access to "Users" page under "Device Administration"
CSCvo41052	ISE deletes the newly created IP-SGT mapping
CSCvo45582	Unable to select specific columns in the Internal Administrator Summary report
CSCvo45606	Error message is displayed when special character ^ is used in AD password
CSCvo48352	CSV file of RADIUS authentications report may have duplicate records
CSCvo49521	ISE adds an additional character at the end of OperatingSystemVersion
CSCvo64085	The calculation of required space for MnT backup needs to be revalidated
CSCvo74766	ISE DACL syntax checking validation fails when a wildcard mask is used
CSCvo75129	Runtime prepends " " to ";" in dhcp-class-identifier in syslog message sent to profiler
CSCvo75376	pxGrid node name limit too short for FMC
CSCvo82021	Memory usage discrepancy in GUI and show tech
CSCvo82930	Repeated exceptions from profiler.log in debug mode
CSCvo98554	Login page is not loaded after importing ISE portal builder to ISE
CSCvp07591	Active Directory Machine authentication fails with error "22040 Wrong password or invalid shared secret"
CSCvp13733	On rebooting connected DC, ISE sometimes doesn't failover to other DC
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
CSCvp18932	Outdated jquery library used by ISE
CSCvp19632	Policy sets order mismatch when exporting as XML
CSCvp22075	When the ERS API is enabled with CSRF check, the requests fail if the API call requires the CSRF token
CSCvp29197	ISE 2.4p3 Radius livelogs not displayed due to invalid NAD ip address
CSCvp30958	ISE dropping requests due to descriptor allocation exhaustion under external server latency scenario
CSCvp33593	ISE fails to match authorization policy with endpoint ID group "unknown"
CSCvp37101	AD connectivity issue occurred and core file generated
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
CSCvp46165	Posture redirect fails with error “unable to determine peer” in AnyConnect_ISEPosture.txt
CSCvp50557	Changing maximum user global settings is not logged in change configuration audit

Table 9 Cisco ISE Patch Version 2.3.0.298 - Patch 7 Resolved Caveats (continued)

Caveat ID Number	Description
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
CSCvp73385	Authentications start failing once AD throws KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN error
CSCvp74154	Unable to remove an endpoint from the endpoint database due to permission error
CSCvp75207	ISE 2.4p8 Certificate chain does not get imported to Patch 8
CSCvp76911	Deploy button is missing in the Matrix page when Multiple Matrices workflow is enabled
CSCvp77014	ISE Trustsec custom view doesn't sort properly
CSCvp77941	License usage for Plus license either shows 0 or incorrect value
CSCvp83006	While exporting endpoint data from Context Visibility page, custom attribute values are not exported
CSCvp86406	Unable to add network device with combination of any digit followed by () in software version field
CSCvp88443	ISE CoA is not sent if new Logical Profile is used in Authorization Policy Exceptions
CSCvp88940	Can't use endpoint group description during runtime for authorization profile
CSCvq15329	Restore failing for scheduled backup
CSCvq17464	Cannot update internal user with External Password ID Store via ERS
CSCvq19039	ISE fails to save configuration changes for large policy sets
CSCvq29336	When the user clicks the Details option in the Live Logs page, an error is seen if the session ID contains "-" symbol
CSCvq31893	Error while adding and importing Security Group
CSCvq35826	When the counter time limit value is updated in the Maximum Sessions page, audit report is showing the updated time as milliseconds instead of seconds
CSCvq39759	In case of PAN failover, the number of elapsed days is made equal to the inactive days, thereby causing incorrect purging of endpoints
CSCvq42847	"Posture failed due to server issues" error seen during System scan in MAC OSX
CSCvq73457	Under heavy load, ISE live logs are unavailable or delayed

New Features in Cisco ISE Version 2.3.0.2988—Cumulative Patch 6

Identity Caching in 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.

Resolved Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 6

Table 10 lists the caveats that are resolved in Cisco Identity Services Engine, Release 2.3 cumulative patch 6. Patch 6 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.2.1.43 or later and Windows users need to upgrade their SPW to WinSPWizard 2.2.1.53 or later.

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats

Caveat ID Number	Description
CSCuq95531	Diagnostic Tool: For DNS A Record tests change status failed to warning
CSCuy41309	ISE 2.x: Unable to delete endpoint from endpoint group
CSCuz00603	Unable to add duplicated mappings to multiple SXP VPNs
CSCuz52877	ISE 2.1: Authentication inactivity alarms every 15 minutes
CSCvb17967	ISE fails to read response from MDM with special characters
CSCvb45390	Collection Filters configured with User name is not working for TACACS authorization/accounting
CSCvd79952	EasyConnect CoA not sent after session merge in distributed deployment
CSCve03360	Various AD attributes not retrieved when domain PC authenticated to network
CSCve18636	ISE 2.1p3 Support Bundle for PSN node in deployment ends up with Blank Error on PAN
CSCve98518	Cisco ISE Guest Portal Login Limit Bypass
CSCvf19364	ISE 2.2: SXP process fails when trying to create network subnet static mapping
CSCvf20174	Context visibility Endpoints Export All option not working.
CSCvf26936	After promoting SAN as PAN, ISE Indexing Engine is not coming up
CSCvf30591	ISE 2.2: Disabled password Lifetime, however getting reminder for account expiration.
CSCvf35268	ISE 2.2 displays blank page for specified scheduled reports
CSCvf38307	PSN not listening on 1645, 1646 RADIUS ports after reboot
CSCvf43886	MNT session is not cleared even after receiving accounting stop from the NAD
CSCvf73169	Session directory write failed alarm is triggered by profiler syslog
CSCvg03064	License consumption count not updated on 2.0 to 2.4.152 upgraded setup

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvg08601	ISE 2.3 can't parse TACACS message to clean empty spaces in CmdSet AVs
CSCvg08956	ISE 2.3 "show tech-support" doesn't include certificates
CSCvg12398	Observing ORA-01000 maximum open cursors exceeded error in collector.log
CSCvg19509	ISE is not rotating /var/log/messages
CSCvg21535	ISE pxGrid stuck in initializing state with bond interface
CSCvg46494	ISE cannot purge IdentityGroup null
CSCvg55811	KPM report query causing high load average alarms on MnT node.
CSCvg94174	After upgrade from 2.1 patch 3 to 2.4.229, Mnt Livelogs are not coming up
CSCvg95440	ISE Log collection error for TACACS messages
CSCvh07382	ISE Log collection error: Server=<server-name>; Log Type=MDMOperation - UDID too long
CSCvh09878	ISE 2.2p4 EAP-MD5 MAB session stuck
CSCvh11308	Cisco Identity Services Engine Logs Cross-Site Scripting Vulnerability
CSCvh21601	ISE 2.x: Application Condition GUI displayed only 20 rows
CSCvh24064	Drill down from livelogs not filtering Authentication summary data based on selected User ID/MAC ID.
CSCvh31565	ISE fails to re-establish TCP syslog connection after break in connectivity
CSCvh51208	Timesten connection become stale and livesessions stopped working during performance run
CSCvh54905	Identity Admin cannot see users under Identities tab
CSCvh65838	Runtime core dump during lite stress
CSCvh69910	Corrupted radius token server configuration causing crash
CSCvh72872	Last field of DNS SAN in CSR doesn't accept numbers
CSCvh74979	Reset-config is reverting the fixes of patches and causing some issues
CSCvh79901	APEX license should not be required to update MyDevices Portal
CSCvh80558	After upgrading to ISE 2.3 Patch 2, replication failure alarms are being noticed for alarm objects
CSCvh86442	Internal users with MAC-address like username disabled due to last active timer not updated
CSCvh97544	Short CPU spikes can be observed when client fails torespond and ISE is used as RADIUS Proxy
CSCvi21043	Library conditions referred in policies are getting deleted and evaluation is giving deny access
CSCvi23713	Identity Group Assignment Search Field is not working in specific browsers.
CSCvi30462	Bulk guest import does not work when logged into sponsor portal using SAML provider
CSCvi43687	ISE 2.2 Endpoint export may contain duplicate entries
CSCvi48298	Policy Hit count value gets nullified when Refresh button is clicked.

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvi48886	Post upgrade Guest VLAN doesn't copy the key of omapi.key to DHCP
CSCvi50320	EST Service not running when ISE iseca folder is missing
CSCvi51291	ISE CoA doesnt work 2 days after initial authentication
CSCvi61204	Endpoint Purge policy is matched but job halts during execution
CSCvi66786	Corefiles are being generated due to Timesten crash in MNT node
CSCvi97332	Unsupported character (backslash) has to be added to the UI error message while creation of admin user
CSCvj01047	Not able to enter password with more than 32 characters for PassiveID Domain Controllers
CSCvj05563	Cannot delete security groups having virtual network mapping
CSCvj24095	Unknown Radius Flow is set to RadiusFlowType when updating ExternalIdStoreDictionary
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
CSCvj44088	While registering getting the error: Unable to register the node <fqdn> Version: 0.0.0.0.
CSCvj47723	ISE 2.1 P6 or P7 Guest users receive error 400 after entering login and password. intermittently
CSCvj50257	Mismatch in active endpoint counter and Live Sessions
CSCvj62614	Cisco Identity Services Engine File Upload Code Execution Vulnerability
CSCvj63376	VPN MDM Compliance not updated from MDM Compliance Checker for active session
CSCvj64763	PxGrid failover fails in 2.4 patch 1 with DNAC - ISE integration
CSCvj65552	Backup Input Validation does not occur on backup name characters
CSCvj67414	ISE HSTS Max-Age parameter is too agressive and no includedDomains flag
CSCvj72699	ISE stops publishing SXP mapping
CSCvj73152	Enable VLAN DHCP release breaks guest flow for ISE 2.4
CSCvj73172	Evaluate Apache Server Side Include Cross Site Scripting Vulnerability
CSCvj75478	Device network conditions missing
CSCvj77878	pxGrid: XMPP Cleartext Authentication
CSCvj79271	Secondary MNT: Incorrect Timesten permission issue for the Timesten_Data folder
CSCvj81800	Sponsor Portal Port 9002 still utilizes TLS 1.1
CSCvj92976	Incomplete error message while importing an icon under Network Device Profiles
CSCvj95709	Enable pxGrid in FIPS mode
CSCvj97277	Fix for CSCvf68738 does not allow legitimate CA certificate refresh
CSCvk01682	ISE allows importing multiple instances of same language in portal setup

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvk04424	Changed name for My Reports against Policy Set match removes the delete option from My Reports
CSCvk07631	ISE 2.2: Hot Spot portal users asked to accept the AUP more than once
CSCvk08988	If PxGrid is enabled, user should be allowed to turn on FIPS mode.
CSCvk10081	ISE uses TLS 1.0 when proxy configured and TLS 1.2 if no proxy configured
CSCvk10137	User lookup with alternate UPN suffix fails when the domains share the same alternate suffix.
CSCvk10156	RBAC SuperAdmin Data Access over written by read-only data access for Network Device Groups
CSCvk10454	Adding Node to deployment does not update the Profiling OUI data
CSCvk13569	"ERROR_NO_SUCH_USER" due to ISE ADRT mis-identifiing a child domain name as root forest domain
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 endpoint matches Admin Created profiling policy
CSCvk28377	MnT persists frequent Accounting Interim updates without any changes to Database
CSCvk28847	ISE sponsor's e-mail shoud not be in CC when view/print guests' passwords is disabled
CSCvk31960	Live logs are stopped because collector process not properly restarted
CSCvk51906	MNT operational data in the report is missing due to DST changes
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
CSCvk61386	ISE not showing filtered NADs
CSCvk68196	SNMPv3 profiling works only with DES or AES128 privacy protocol
CSCvk70087	SecureSyslogCollectors should be disabled by default on remote log targets
CSCvk70748	High CPU usage, high Auth Latency, and OOM condition on PSN nodes
CSCvk71161	ISE 2.4 excessive profiler syslogs sent to MNT
CSCvk72606	Able to login to GUI with disabled admin accounts
CSCvk74190	Radius Token Identity Caching Timeout not configurable
CSCvk74989	Certificate parameters not persistent after DNAC trust re-establishment
CSCvk75544	Authentication Summary Reports show "no data available" for Radius and TACACS
CSCvm00127	ISE sponsor email customization doesn't add image properly
CSCvm02478	Cisco Network Setup Assistant App not available on GooglePlay
CSCvm03681	EAP-FAST doesn't support correct key generation in TLS 1.2
CSCvm05439	ISE cores on LDAP test server after DNAC establishment when same chain used

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvm05565	Even after five failure login attempts, Go button can be used in Apple iOS devices to send another login request.
CSCvm05840	NAD CSV imports should allow all supported characters
CSCvm09377	HTTP Request Header for ISE fails if it contains @ in email
CSCvm09493	Unable to save multiple custom attributes at once
CSCvm11595	Live Sessions are not showing on GUI if username contains unicode characters
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
CSCvm12575	ISE context visibility endpoints import fails with custom endpoint attribute date
CSCvm13822	Identity Services Engine Sensitive Information Disclosure for Privileged Account
CSCvm14030	Evaluation of ISE for Struts remote code execution vulnerability August 2018
CSCvm15059	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"
CSCvm20561	ISE 2.x: Cisco-Device profiler policy missing the tandberg OUI as a condition
CSCvm21147	After upgrading to ISE 2.4 schedule backup not working.
CSCvm27249	PassiveID Probe hprof files in temp folder
CSCvm29583	ISE AD lookup broken due to non-whitelisted 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 authorization policy to be saved
CSCvm33673	Endpoint description is not displayed in the context visibility list while editing the endpoint
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' displayed when you click Sign Out in the Manage Guest Accounts page
CSCvm45072	OWASP ZAP reports Cross Site Scripting (DOM Based) on pxGrid Web application
CSCvm47507	Changes made in allowed protocols missing in change configuration audit reports
CSCvm47638	ISE secondary node doesnt send COA when guest account gets suspended or deleted
CSCvm49084	ISE PB portal files are not restored with a restore of an old backup

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvm49503	WasMachineAuthenticated EQUALS False no longer parsed in Runtime
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
CSCvm63427	Cisco Identity Services Engine Password Recovery Vulnerability
CSCvm66696	ISE 2.4 Conditional CoA failure upon EndPoint Identity Group change
CSCvm67561	Accounting messages from ASR1K not saved and not shown in ISE Reports
CSCvm70470	Max Sessions value cannot be applied on GUI after applying 2.2p10 or 2.3p4
CSCvm71860	Cisco Identity Services Engine Reflected Cross-Site Scripting Vulnerability
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
CSCvm73626	Sponsor created random accounts for time restricted guest types fails
CSCvm74423	While creating users by importing data from CSV in sponsor portal they aren't notified via email automatically
CSCvm74605	EAP-FAST prefers cached AD DN over new DN after changing the Account OU
CSCvm75765	"User's email is not valid" message is displayed while creating email id if it ends with .<CUdomain>
CSCvm75790	SAML with ADFS is broken with third party NAD
CSCvm79526	Add Audit log for 'Push' operation
CSCvm79609	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvm82504	Request to increase Radius Token Server password caching to 900 seconds or above
CSCvm86244	While sending data for getting the value for PIP based attributes, not all attributes from the request were being provided to the PIP Implementation
CSCvm86699	ISE CAC or certificate login does not populate external groups under new admin group
CSCvm87060	Remote forest Active Directory controller failover prolonged time
CSCvm87685	Menu access duplicate is failing with plus sign
CSCvm88149	User Accounts are being disabled before the configured value set in the GUI.
CSCvm89126	ISE 2.3 patch 5: NAD / AAA server address is not specified.
CSCvm89837	Lost and Stolen buttons remain disabled on My Devices portal when using Japanese GUI
CSCvm90359	pxGrid debug "warn" level causing XCP to stop running
CSCvm90478	"No Data Available" when attempting to add endpoints to Identity Group with RBAC User
CSCvm91034	pxGrid: EndpointProfileMetaData not propagated with Pxgrid V2
CSCvm91202	Cisco Identity Services Engine Password Recovery Vulnerability
CSCvm92317	ISE Kerberos Authentications are incrementing AD bad password count by 2

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvm93698	AD authentications are failing after applying 2.2 P11/2.4 P4
CSCvm98335	Authentication Summary Report for RADIUS and TACACS display “No data found”
CSCvm98407	Delay while retrieving the network devices in NDG page when using the Show members option
CSCvm99398	SGACL Push in large scale NAD environment causes High CPU on PAN
CSCvn01019	While modifying existing Network Device Profiles, sometimes the Save button is disabled
CSCvn01551	Unable to upload AnyConnect package of file size more than 50MB
CSCvn09504	TC-NAC configured with Qualys shows Not Reachable
CSCvn10971	Rebooting associated site-specific GC does not result in failover to other GC
CSCvn11424	PassiveID Management Logs show Database ID instead of DC Name
CSCvn12114	Need to add Internal User Group in Certificate Authentication Profile
CSCvn12200	Inconsistency in Deploying IP SGT static Mapping from ISE to Cisco switches.
CSCvn13802	Unable to import network devices if shared secret contains "<"
CSCvn15670	Smart Licensing Server is getting overloaded with ISE authorization renewals
CSCvn17524	ISE Apache Struts CVE-2016-1000031 Vulnerability
CSCvn23570	ISE Admin with restricted write access is able to modify/import network devices to Network Device groups to which read-only access is provided
CSCvn24356	pxGrid not handling invalid xml characters for publish and download
CSCvn24568	Network Device Filtering returns only first IP range when multiple ranges are configured
CSCvn25367	Context Visibility Authentication/Endpoint tab shows blank pop up message
CSCvn27325	Posture policy with Tunnel Group Name in condition is not working
CSCvn29633	ISE does not follow the capabilities of SXP Listener.
CSCvn33534	RADIUS Authentications Report logs are not fully displayed when "last 30 days" option is selected
CSCvn35579	SXP connection between ISE and IOS Devices stuck in DeleteHoldDown state
CSCvn37048	ISE 2.x: ISE syslog message code (59200-59208) is not being used in ISE currently.
CSCvn39998	Pullout reports from Authentication Summary report is showing empty report.
CSCvn50203	ISE 2.4p5 - Not all IP_EPG mappings on ACI are imported by ISE
CSCvn51282	ISE replaces "ip:" to it's hostname in "ip:inacl" Cisco AV-Pair
CSCvn52886	User name from WMI information is deleted on receiving a DHCP custom syslog for same endpoint
CSCvn55560	After installing ISE 2.3 patch 5, creation of EOB Guest user does not work
CSCvn56648	When individual policy set is reset, other policy set hit counters are reset to 0
CSCvn58964	ISE 2.4: Slow database response with 500 authorization policies
CSCvn59502	ISE DACL syntax checking is not properly catching errors

Table 10 Cisco ISE Patch Version 2.3.0.298-Patch 6 Resolved Caveats (continued)

Caveat ID Number	Description
CSCvn60787	Emails are not sent for alarm specific email configuration
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.
CSCvn64467	Not able to enable web authentication under third Party NAD Device Profile
CSCvn68614	Unable to use "connect-info" dictionary by default in Authorization Condition
CSCvn69854	ISE includes only one prrt-server file in support bundle
CSCvn75254	Check box under custom network device profile list is getting unchecked
CSCvn79557	Custom user attribute change does not reflect changes in configuration change audit report
CSCvn81631	Cores being consistently generated on every node after upgrading from ISE 2.4 to 2.5
CSCvn82581	ISE 2.3p5 : Unable to save the changes under network device profile
CSCvn85498	ISE 2.4: InactiveDays attribute update with disabled profiling
CSCvn98932	Non-existed DACL is not verified by ISE
CSCvo18883	“Authorization Profile DACL NAME is not valid” is displayed while creating Authorization profile

Open Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 6

Table 11 Cisco ISE Patch Version 2.3.0.298-Patch 6 Open Caveats

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

Resolved Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 5

Table 12 lists the caveats that are resolved in Cisco Identity Services Engine, Release 2.3 cumulative patch 5. Patch 5 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.2.1.43 or later and Windows users need to upgrade their SPW to WinSPWizard 2.2.0.53 or later.

Table 12 Cisco ISE Patch Version 2.3.0.298-Patch 5 Resolved Caveats

Caveat ID Number	Description
CSCvc69243	firewall ports are not getting configured due to iptable hang (xtable lock)
CSCvc74631	endpoints/NAD template import failure with basic license
CSCvf20208	ISE Posture PRA timer expires to non-compliant

Table 12 Cisco ISE Patch Version 2.3.0.298-Patch 5 Resolved Caveats

Caveat ID Number	Description
CSCvf26143	LDAP authentication failure: LDAP identity store does not support PlainAuthenticateAndQueryEvent
CSCvf55996	AD probe looking for host is not searching properly
CSCvf69805	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability
CSCvf69963	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvf72309	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvf75968	Multiple Vulnerabilities in httpasyncclient
CSCvf82350	US27030 - Fix VPN Session to MAC Mapping
CSCvf90694	AnyConnect ISE posture unable to assess posture policies on CM 3.x/4.x
CSCvg16408	Static IP-SGT bindings created on ISE are not pushed to the Devices
CSCvg36077	Active Directory domain/forest becomes unavailable after receiving a Kerberos error
CSCvg46899	ISE 2.2 user may be redirected again after AUP acceptance on Hotspot portal
CSCvg48447	ISE 2.3 single SSID BYOD w/ "allow network access" giving "400 bad request"
CSCvg86743	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvg95479	Cisco Identity Services Engine Command Injection to Underlying OS Vulnerability
CSCvh31926	Profiler policy evaluation is eating away Java Mem and causing High CPU and Auth latency
CSCvh54726	ISE: Failure to retrieve AD groups for Intel AMT supplicant username format
CSCvh57345	Restore of 1.4/2.0/2.0.1 backup fails which taken after Feed update
CSCvh77480	ISE 2.2 patch 5, unable to generate pxGrid certificate using PEM and PKCS8 PEM formats
CSCvh86466	PassiveID: WMI queries DC cause memory increased issues on DCs (Microsoft WMI memory leak)
CSCvh91996	Matched AuthC and AuthZ rules in Monitor Only mode showing in GUID but not names
CSCvh98102	Issue with deleting AD instance
CSCvi31965	ISE High Authentication Latency due to lookup in Internal Endpoints
CSCvi42112	ISE - DHCP Scope responding with 1 day lease instead of 15 seconds
CSCvi42404	validDays does not match span of fromDate to toDate
CSCvi51021	No data available in context visibility if there is no plus/advanced license - Standalone node
CSCvi61330	Occasional application restart post Radius/DTLs authentication
CSCvi63590	ISE 2.3 patch 2 ERS REST API call to update network device doesn't work
CSCvi73782	Static Group Assignment dropping due to DHCP Probe
CSCvi82192	Generate pxGrid Certificates page doesn't respect cert template RSA key size
CSCvi85159	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability
CSCvi91353	NMAP scans for custom port 9100 but doesnt report it in nmap.log
CSCvj11981	SNMPv3 profiler breaks when auth or priv settings are configured

Table 12 Cisco ISE Patch Version 2.3.0.298-Patch 5 Resolved Caveats

Caveat ID Number	Description
CSCvj15594	ISE 2.3 Identity Source sequence may go missing
CSCvj34576	REST API GET DACL shows wrong total number of DACLs
CSCvj34578	REST API GET DACL page filter does not show correct information
CSCvj36442	Network devices page fails to paginate as shared secret is in plain text
CSCvj41029	User domain name may remain empty in session when ISE passive-id AD agent or MS WEF is used
CSCvj72180	ENH: ISE: Store new m/c password on ISE side if new password is valid despite RPC error - 121
CSCvj77357	DNA-C/ISE trust establishment: remove SAN FQDN/IP validation
CSCvj81500	ISE 2.3 | Unable to export filtered network devices with 'Export All' option
CSCvj94737	ISE 2.2 P9: Showing Error on CPP Sign On Page
CSCvk15628	ISE : My device portal- Unable to remove the stolen tab
CSCvk31092	Core: SyslogSecureTCPConnection::updateConnectionData
CSCvk40105	Editing guest user throws pop up error when creating with java scripts in first and last name
CSCvk54145	Swapping Active and Standby MnT roles result in invalid db credentials.
CSCvi44041	Cisco Identity Services Engine Privilege Escalation Vulnerability

Resolved Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 4

Table 13 lists the caveats that are resolved in Cisco Identity Services Engine, Release 2.3 cumulative patch 4. Patch 4 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.42 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Table 13 Cisco ISE Patch Version 2.3.0.298-Patch 4 Resolved Caveats

Caveat	Description
CSCvi94778	Unable to establish trust with ISE 2.3 patch 3
CSCvi29600	Sponsor Groups are not merging results with AD Sponsor groups when Internal user uses AD password
CSCvj17258	DNA-C Integration with ISE 2.4 fails as the old DNA-C client certificate is still present in the ISE certificate store

Resolved Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 3

Table 14 lists the caveats that are resolved in Cisco Identity Services Engine, Release 2.3 cumulative patch 3. Patch 3 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.42 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Table 14 Cisco ISE Patch Version 2.3.0.298-Patch 3 Resolved Caveats

Caveat	Description
CSCuy98580	The Active Directory connector client on ISE reloads if DNS settings are changed after ISE joins Active Directory.
CSCvf63799	When the SGT value on ISE is updated with static IP-SGT mapping, the SXP listener loses the IP SGT mapping.
CSCvf70099	EP ownership data is lost due to redis timeout.
CSCvg15960	ISE gets disconnected from Active Directory if ISE can not refresh machine account password.
CSCvg36087	Network Security Services Database (NSSDB) Exception: PKCS11KeyStore does not support write capabilities.
CSCvg83484	ISE reports null info for events to Smart Call Home (SCH) Server.
CSCvg88340	Client provisioning does not work for guest flow.
CSCvg88945	Unable to send ISE 2.3 Profiler CoA when a parent profile is changed to child profile.
CSCvg98688	ISE 2.2 core file is generated, after application Stop ISE.
CSCvh06189	Attributes for the guest flow do not match in the Authorization Policy.
CSCvh09763	Scheduled Policy export runs on PSN node causing high CPU usage.
CSCvh48558	ISE 2.2p5: Unable to load Context Visibility.
CSCvh66228	The PassiveID probe connection drops and attempts to re-connect infinitely.
CSCve59024	Endpoints with identity groups are empty in Context Visibility.
CSCvf18466	ISE 2.1: Endpoint lookup using MNT REST API is slow.
CSCvf49665	Issued pxGrid Certificates do not appear in GUI.
CSCvf61010	ISE 2.3 Upgrade requires "Time Interval For Compliance Device ReAuth Query" for MDM.
CSCvf73922	Cisco ISE DOM Cross-Site Scripting (XSS) Vulnerability.

Caveat	Description
CSCvg30444	Guest, profiling, ise-psc and other logs fail to updating in ISE 2.3.
CSCvg30751	LDAP admin password is stored in clear text format in DB.
CSCvg61751	Deregister stuck during upgrade with VCSHostConfigNotificationHandler.
CSCvg79089	Upgrade timeout during enable / disable of MnT persona.
CSCvg83466	Telemetry event does not include Profiling and Network Access information.
CSCvg86633	Page counter in reports shows incorrect values.
CSCvh01390	TCP Dump capture for a hostname changes after navigation on deployment.
CSCvh13954	ISE: Unable to view the endpoint purge details upon clicking the dashboard alarm.
CSCvh32034	Current active session report exports only 500 records to the CSV repository.
CSCvh50630	Hydrant certificate chain must be added to ISE default trust certificate store.
CSCux88538	ISE 1.4 does not support aes256-ctr & aes128-ctr SSH ciphers.
CSCvh92224	Reports Usability Issues.

Resolved Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 2

Table 15 lists the caveats that are resolved in Cisco Identity Services Engine, Release 2.3 cumulative patch 2. Patch 2 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.42 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Table 15 Cisco ISE Patch Version 2.3.0.298-Patch 2 Resolved Caveats

Caveat	Description
CSCuz00163	Endpoint profiling using Visibility Setup Wizard does not profile endpoints authenticating from other subnets.
CSCvc36556	The ./CSCOcpm/logs/crypto.log is not getting overwritten and creates a disk space issue.
CSCve73968	Static Group Assignment flag is set to False and MAB authentications fail when Profiling license is not installed.
CSCve78606	When the MDM servers are upgraded, some of the endpoints are marked as Non-Compliant, which causes sudden increase in memory consumption.
CSCvf21978	ISE fails to resolve ambiguity in Active Directory usernames that randomly results in users with short usernames not getting authenticated or getting authenticated in wrong domains.

Table 15 Cisco ISE Patch Version 2.3.0.298-Patch 2 Resolved Caveats

Caveat	Description
CSCvf41105	Show clock displays time with clock +1h and EEST instead of EET for Africa/Cairo time zones. **Workaround** Use GMT-2 time zone when installing ISE.
CSCvf42743	Able to delete the trusted certificate configured in the LDAP identity source when ISE is restarted.
CSCvf57412	In ISE 2.2 patch 2, an error message is displayed during the initial login and while launching the Home tab after login.
CSCvf65306	After upgrade to ISE 2.2 patch 2, the alarms on Wifi Setup container processes are triggered even when the Wifi Setup Helper is disabled.
CSCvf78088	In ISE 2.3, the selected Allowed Protocol is removed from the policy set, if the selected object is renamed.
CSCvf87440	Some of the dictionaries are not displayed in the Policy Conditions drop-down list.
CSCvf89109	After upgrading to ISE 2.2, guest import from sponsor portal using CSV file remains in pending state.
CSCvf90132	Rename of RADIUS Server Sequence is not reflected in Policy Sets.
CSCvf91538	The “End of business day” should not be set as the default expiry time for guest accounts.
CSCvg03448	Policy set is not displayed correctly when RADIUS server sequence is selected while local authorization is enabled.
CSCvg08983	In Policy Sets Condition Studio, the edit Time and Date condition redirects to an incorrect URL.
CSCvg10540	Unable to delete authorization profile after upgrading to ISE 2.3.
CSCvg13303	Upgrade to Release 2.3 fails with Policy Set conversion during data upgrade.
CSCvg19428	ISE configuration backup size is huge due to Elastic Search transaction logs.
CSCvg23034	When a Security Group ACL is changed in a cell, the Change of Authorization (CoA) is pushed after 4-5 minutes.
CSCvg29763	CSV imported endpoint labels occasionally changed from statically assigned group to Unknown or Profiled.
CSCvg32162	ISE scheduled backup is stuck at 75% when SFTP repository is used.
CSCvg37179	Cisco ISE Application server initializes due to database connection exhaustion.
CSCvg44615	In Policy Sets, the authentication policy is empty if any of the authentication policy rule has Deny Access configured as the identity source.
CSCvg46464	Cisco ISE 2.3 Application server initializes due to database connection leaks.
CSCvg48530	An error in deleting TACACS profiles is reported after upgrade to ISE 2.3. **Workaround** Contact TAC.
CSCvg53547	Redundant data query instead of cache query when searching for non-existent internal users.
CSCvg54665	Database connection leak in deleting profiled endpoints via GUI.

Table 15 Cisco ISE Patch Version 2.3.0.298-Patch 2 Resolved Caveats

Caveat	Description
CSCvg74276	RADIUS requests are rejected due to logging errors reported in the Live Logs/Sessions page.
CSCvg74394	The Acceptable Use Policy (AUP) Page for Hotspot Guest Portals cannot be enforced when the status of the connection changes.
CSCvg76444	Downloaded policies do not work after restoring backup from ISE 2.0.1 patch 4 to ISE 2.3 patch 1. **Workaround** 1. Choose **Work Centers > TrustSec > Components > Security Group ACLs**. 2. Edit the required SGACL and verify if the appropriate IPv4 or IPv6 option is selected. 3. Click **Save**.
CSCvg76888	Egress policies are not displayed in the Source Tree View in the ISE GUI.
CSCvg77466	ISE Mobile Device Management (MDM) triggers Change of Authorization (COA) often with Microsoft's System Center Configuration Manager (SCCM).
CSCvg80048	The system time zone does not occasionally change in the ISE GUI and reports. **Workaround** Contact TAC.
CSCvg81968	Unable to edit or save policy set using Microsoft Internet Explorer 11 browser and ISE 2.2. **Workaround** Use Mozilla Firefox browser.
CSCvg86571	Close any open EDF sessions before sending http response (Remoting and Admin Webapp).
CSCvg98735	The Identity Group is not displayed in the **Context Visibility > Endpoints > Attributes** page, when an endpoint is reauthenticated after manually updating the Identity Group.
CSCvh29951	ISE reboots and generates core files when trying to authenticate HP devices and Multi RADIUS keys.

New Features in Cisco ISE Version 2.3.0.298—Cumulative Patch 2

Active Directory Identity Search Attributes

Cisco ISE identifies users using the attributes SAM, CN, or both. Cisco ISE, Release 2.2 Patch 5 and above, and 2.3 Patch 2 and above, use sAMAccountName attribute as the default attribute. In earlier releases, both SAM and CN attributes were searched by default. This behavior has changed in Release 2.2 Patch 5 and above, and 2.3 Patch 2 and above, as part of CSCvf21978 bug fix (see https://tools.cisco.com/bugsearch/bug/CSCvf21978 for details). In these releases, only the sAMAccountName attribute is used as the default attribute.

You can configure Cisco ISE to use SAM, CN, or both, if your environment requires it. When SAM and CN are used, and the value of the SAMAccountName attribute is not unique, Cisco ISE also compares the CN attribute value.

To configure Active Directory identity search attributes:

1. Choose **Administration > Identity Management > External Identity Sources > Active Directory**. In the **Active Directory** window, click **Advanced Tools**, and choose **Advanced Tuning**. Enter the following details:

- **ISE Node**—Choose the ISE node that is connecting to Active Directory.
- **Name**—Enter the registry key that you are changing. To change the AD search attributes, enter: `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
- **Value**—Enter the attributes that ISE uses to identify a user:
  - *SAM*—To use only SAM in the query (this is the default option).
  - *CN*—To use only CN in the query.
  - *SAMCN*—To use CN and SAM in the query.
- **Comment**—Describe what you are changing, for example: Changing the default behavior to SAM and CN

2. Click **Update Value** to update the registry.

   A pop-up message appears. Read the message and accept the change. The AD connector service in ISE restarts.

AnyConnect Stealth Mode Notifications

Several new failure notifications are added for AnyConnect stealth mode deployment to help users identify issues with their wired, wireless, or VPN connections. Perform the following steps to enable or disable notifications in the Stealth Mode:

1. Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.
2. Click **Add > NAC Agent or AnyConnect ISE Posture Profile**.
3. In the **Select a Category** drop-down, choose **AnyConnect**.
4. In the **Agent Behavior** section, in the **Enable Notifications in Stealth Mode**, choose **Enabled** or **Disabled**.

Note AnyConnect version 4.5.0.3040 supports Stealth Mode notifications.

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.

Note Although TrustSec devices can take advantage of the dual shared secrets (keys), TrustSec CoA packets sent by Cisco ISE will always use the first shared secret (key). Therefore, the TrustSec policy push using CoA feature will not be supported if the network device uses the second shared secret (key).

Resolved Caveats in Cisco ISE Version 2.3.0.298—Cumulative Patch 1

Note We have recalled ISE 2.3 Patch 1 due to an issue we found after posting. An updated patch file has been reposted, and the new file name is ise-patchbundle-2.3.0.298-Patch1-221754.SPA.x86_64.tar.gz. If you already installed the previously posted patch, you MUST uninstall that patch, and install the new one.

Table 16 lists the caveats that are resolved in Cisco Identity Services Engine, Release 2.3 cumulative patch 1.

Patch 1 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.42 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Table 16 Cisco ISE Patch Version 2.3.0.298-Patch 1 Resolved Caveats

Caveat	Description
CSCvd79546	Few Log Categories are not displayed in the Logging Categories page after upgrade. **Workaround** Perform a full synchronization between the PPAN and SPAN before upgrade.
CSCve82240	A comma is appended to the Sponsor's email address configured in the sponsor portal. **Workaround** Modify the email field manually and delete the comma.
CSCve84667	The Machine Access Restriction (MAR) cache distributed search is active despite the node group being disabled for MAR cache distribution.
CSCve87511	Cisco ISE fails to support social login if the proxy server is configured.
CSCve99612	An error is reported in the Portal Settings and Customization page.
CSCvf22318	An ElasticSearch and database shards errors occur on the Endpoints Context Visibility page.
CSCvf22676	Live logs do not occasionally show the actual authorization policy that is evaluated when a policy is renamed.
CSCvf22827	LDAP Test Binding message does not include information about subjects, groups, and response time.
CSCvf24580	RADIUS authentication report: RADIUS records are not filtered correctly with “Today” and “Yesterday” options.
CSCvf24878	Unable to use different encryption keys when modifying scheduled backup.
CSCvf32212	Add a link to Social Login identity source in the Overview page of Guest Access work center.
CSCvf33792	The guest flow diagram appears correctly on screens with lower resolution only when the Portal Settings section is closed.
CSCvf34219	IPv6 TACACS+ authentication communicates only via port 49 in upgraded setup.
CSCvf34315	ISE 2.3 Guest Social login does not require AUP acceptance.
CSCvf36007	Allow Access only on these Days and Times option does not work for Social Login flow after first login.

Table 16 Cisco ISE Patch Version 2.3.0.298-Patch 1 Resolved Caveats

Caveat	Description
CSCvf36016	If Self-registration option is disabled and Social login with registration form option is enabled, the registration form may not appear in the Portal Page Customization tab.
CSCvf36031	Enhancements to social login for self-registered guests.
CSCvf37931	An overlap error occurs while editing network devices with multiple IPv6 addresses.
CSCvf41048	Policy sets do not reflect any changes made to the endpoint or user identity group names.
CSCvf41249	Cannot fetch LDAP Groups and Attributes from UI unless issuing Test Binding when Secure LDAP is configured using AD schema.
CSCvf42061	An “Exception: all shards failed” error is reported on the Endpoints Context Visibility page.
CSCvf42554	The Context Visibility tab occasionally fails to display the page when navigating between tabs.
CSCvf44080	Prevent database corruption affecting order of policy sets or policy rules in a table.
CSCvf44272	ISE 2.2 Patch 2 core files should not be written to root partition. Delete core files from the root directory.
CSCvf44549	In the Conditions Studio page, the scroll bar cannot be dragged to view the saved conditions specified in a policy rule.
CSCvf44658	Policy Information Points (PIP) Identity Store returns incorrect attribute value after AD is renamed.
CSCvf47157	Renamed identity stores are not reflected in referenced policies.
CSCvf47170	Policy processing occasionally fails to hit the correct policy set.
CSCvf47316	Fix for Entry Definition Framework (EDF) memory leak upon rollback.
CSCvf53116	The Upgrade Readiness Tool for upgrading from ISE 2.1/2.2 to 2.3 fails with the ORA-32004: obsolete or deprecated parameter(s) error.
CSCvf55764	Few attribute validations fail in policy conditions.
CSCvf69018	Issue with reverse lookup when nodes are registered to Cisco ISE after applying ISE 2.2 Patch 1.

Table 16 Cisco ISE Patch Version 2.3.0.298-Patch 1 Resolved Caveats

Caveat	Description
CSCvf75225	PAN runs high CPU due to 100K limit in the Redis server.

CSCvf87844	Filtering of endpoints in the Context Visibility page occasionally does not display existing endpoints.
	Note The context visibility sync option and reset commands can be found in Release 2.3 Patch 1.
	a. Run the **app configure ise** command on the Secondary Admin node CLI and select the following option:
	`[19]Reset Context Visibility`
	b. When you see a prompt to proceed with reset on the Primary Admin node, switch to Primary Admin node and select `[19]Reset Context Visibility` option.
	c. After reset is complete on the Primary Admin node, switch to the Secondary Admin node and press **Y** to confirm that the reset was successful on the Primary Admin node.
	d. Select the following option in the Primary Admin node:
	`[20]Synchronize Context Visibility With Database`

Known Issues in Cisco ISE Version 2.3.0.298—Cumulative Patch 1

Conditions Studio Editor After Upgrade to ISE 2.3

When you create conditions using the Conditions Studio editor after upgrade, you can click the Attribute Value drop-down list or click the icon next to the Attribute Value text box to choose the required attribute. If the Attribute Value drop-down list is not displayed, you must use the mouse or trackpad, scroll up to the top of the page, and click the Attribute Value text box.

Resolved Caveats - Initial Release

Caveats resolved for the initial release.5*@WR6SW$4Ri

Table 17 Cisco ISE Release 2.3 Resolved Caveats

Caveat	Description
CSCuv32863	Cisco Identity Services Engine cross-site request forgery vulnerability
CSCvc38741	ISE 2.1 supports TLS 1.0 on port 8910.
CSCvc74300	/var/log/secure file size is increasing rapidly.
CSCvc74307	/var/cache/logwatch temp files are not removed.
CSCvc86247	High CPU usage caused by infinite loop threads on PSN.
CSCve73657	If the default condition in authentication inner policy is set to a value other than DenyAccess, the default value gets reverted to DenyAccess after restart.
CSCvc83519	When an ISE node is rebooted, TC-NAC containers in the ISE node are not able to communicate with Internet or other hosts.

Table 17 Cisco ISE Release 2.3 Resolved Caveats (continued)

Caveat	Description
CSCvc87853	SNMP process stops and restarts by itself after continuous snmpwalk queries.
CSCvd49843	Native Supplicant Profile with external CA/SCEP fails when ISE Internal CA is disabled.
CSCvd61267	/var/log/messages log rotate does not work while creating new messages log file after log rotation
CSCve51586	pxGrid stuck in initialization state if IP access restriction is configured.
CSCve77317	ISE 2.1 to 2.3 upgrade failed with “UPS upgrade handler failed” message.
CSCvf00883	pxGrid authorization denied and also takes 20 minutes to start working after primary pxGrid node is down.

Cisco ISE, Release 2.3 Open Caveats

The following table lists the caveats that are open in Release 2.3.

Table 18 Cisco ISE Release 2.3 Open Caveats

Caveat ID Number	Description
CSCuy41309	ISE 2.x Unable to delete endpoint from endpoint group
CSCuz00603	Unable to add duplicated mappings to multiple SXP VPNs
CSCve63448	Cannot determine persona for PSN with some service and XGRID node
CSCvf30353	guest email from the same mailid, even after removing the emailid for already existing sponsore
CSCvf43341	InternalUser:IdentityGroup EQUALS User Identity Groups:<Group_Name> not working for external users
CSCvf43449	ISE : Guest Account getting active on local ISE time instead of location selected
CSCvf61054	DNA/C/ISE/Win - authorization policy drop down menu for selection is not directly underneath field
CSCvf61114	ERS Update/Create for "Authorization Profile" failing XML Schema Validation
CSCvf74039	ISE returns restBaseUrl and restRaseURL on ServiceLookup
CSCvf77897	Need updating ERS SDK on network devices
CSCvf78643	Unable to rename library conditions in ISE 2.3
CSCvf82937	Publisher is unknown in SPW 2.2.0.53

Table 18 Cisco ISE Release 2.3 Open Caveats (continued)

Caveat ID Number	Description
CSCvg26552	Issues with T+ current active sessions report
CSCvg26624	ISE does not send SXP mappings to ACI without having an additional SXP device defined
CSCvg95110	Dashboard not showing any devices under home > Summary page
CSCvh20487	Deleting all policy mapping under policy-matrix takes very long time ~ 1 hr
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
CSCvh93771	Broken admin web ui access with PAT/NAT of HTTPS://<IP>:<port-non-443>
CSCvh95370	Creating Network Device Defaults Device Profile to AlcatelWired
CSCvi07975	ERS filter and sorting not working for Guest Type Get-All
CSCvi44313	Context Visibility>Endpoints(connected)>Other Attributes>AD-Last-Fetch Time shows invalid
CSCvi45372	non-internal-CA signed pxGrid certficate incorrectly replaced upon ISE reload
CSCvi48276	AMP in ISE remains connected even after deregter from cloud
CSCvi48298	Policy Hit count value gets nullified while click on REFRESH button.
CSCvi48656	Home > Endpoints > Endpoint Categories > OS type shows No Data available
CSCvi60160	Stop All Running Tests not functioning properly in Active Directory Diagnostic Tool
CSCvi80094	ERS API that requires CSRF token returns HTTP 404 instead of 403
CSCvj01047	Password length limitation when adding DC's in the PassiveID section of 32 characters.
CSCvj06916	ISE 2.3+ : Authc/Authz policies in a policy set cannot be configured if ext radius sequence is used
CSCvj07391	DNA-C/ISE - active session is missing in ISE live session log
CSCvj08392	ISE SNMPv3 User still display on "show snmp user" after delete snmp-server user
CSCvj31598	Enhancement Request: Import two CA certs with same subject name
CSCvj50257	Active endpoints are mismatched from expected value
CSCvj65552	ISE 2.4 Backup Input Validation does not occur on backup name characters

Table 18 Cisco ISE Release 2.3 Open Caveats (continued)

Caveat ID Number	Description
CSCvj76466	MNT session look up fails for posture via FlexVPN
CSCvj78065	ISE : Unable to use two MDM server at the same time
CSCvj90778	ISE/UCS Build secure signed HUU to address vulnerabilities
CSCvj92976	ISE : Incomplete error message while importing an icon under Network Device Profiles
CSCvj93331	Link to next page is not present in REST response
CSCvk04424	Changed name for My Reports against Policy Set match removes the delete option from My Reports
CSCvk06884	ISE should return 400 HTTP error, not 500 if incorrect data provided for REST call
CSCvk10137	USER lookup with alternate UPN suffix fails when the domains share the same alternate suffix.
CSCvk20044	Sponsor Portal doesn't show proper GUI if resolution is under 960px width
CSCvk23532	Remove GMT portion from $ui_start_date_time$ and $ui_end_date_time$ on Email Notifications
CSCvk23793	ISE not able to join the AD after high disk usage
CSCvk24318	Incorrect certificate sent to secondary admin node causing endpoint synchronization issues within CV
CSCvk27295	NMAP fails to execute when an EP matches a Admin Created profiling policy
CSCvk30726	ismachineauth Flag not raised for EAP-TLS
CSCvk48115	ISE 2.3 RSA SecurID authentication fails
CSCvk54126	Wrong ERS reply from ISE
CSCvk59716	Domain Admins are not able to edit Sponsor accounts properly
CSCvk60520	ISE:PSN forwards syslog info to MnT for accounting packets without class (25) atrribute
CSCvk67659	PassiveID Domain Controllers are not deleted when deleting whole AD scope
CSCvk72606	ISE- Can login to GUI with disabled admin accounts.
CSCvk72920	ISE does not send SNMP bulk request for CDP after it did once
CSCvk74393	ISE Registration/Failover Problem
CSCvm02863	TACACS authentication policy not matching All-Locations
CSCvm02913	Password lifetime is causing Admin account to disable even account disable policy is not configured

Table 18 Cisco ISE Release 2.3 Open Caveats (continued)

Caveat ID Number	Description
CSCvm03411	Kernel Side-Channel Attack using L1 Terminal Fault: CVE-2018-3620 and CVE-2018-3646 (Foreshadow-NG)
CSCvm05519	Message Class for EAP-TLS messages from System-Management to EAP
CSCvm05593	Runtime carsh seen during tacacs processing
CSCvm06688	Patch roll back from CLI is failing in case of Patch install has issues after installing from GUI
CSCvm08596	AD Connector crashes during join if anything is blocked on trusted domain
CSCvm09377	HTTP Request Header for ISE fails if it contains @ in email
CSCvm10640	Day0- NSP fails during byod flow on Android 9 BETA
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
CSCvm15059	ISE 2.1+ : Identity Source Sequence info button information is wrong for Sponsor Portal
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
CSCvm27249	PassiveID Probe hprof files in temp folder
CSCvm29583	ISE AD lookup broken due to non-whitelisted domain lookup failing
CSCvm32107	Unable to delete Root Network Device Group
CSCvm33217	AD groups with more than one space doesn't allow authZ policy to be saved
CSCvm37837	AMP IRF Adaptor Fails To Retrieve Events
CSCvm41485	ISE 2.3 : Unable to access NFS repository and scheduled reports not working using NFS respository
CSCvm48685	Syslog sends logical profile GUID instead of profile name
CSCvm49503	WasMachineAuthenticated EQUALS False No Longer Parsed in Runtime--ISE 2.4
CSCvm49549	System Dictionaries Shouldn't Even Show As Configurable---ISE
CSCvo75376	FMC uses hostname+33 bytes generated ID for node name. And that easily goes over 50 bytes limit in ISE. The limit was created for a security enhancement in CSCvm45072

Related Documentation

Release-Specific Document

General product information for Cisco ISE is available at http://www.cisco.com/go/ise. End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Cisco Identity Services Engine Ordering Guide is available at http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/guide_c07-656177.pdf

Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

- Cisco UCS C-Series Servers

  http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html
- Cisco Secure ACS
  http://www.cisco.com/c/en/us/support/security/secure-access-control-system/tsd-products-support-series-home.html
- Cisco NAC Appliance
  http://www.cisco.com/c/en/us/support/security/nac-appliance-clean-access/tsd-products-support-series-home.html
- Cisco NAC Profiler
  http://www.cisco.com/c/en/us/support/security/nac-profiler/tsd-products-support-series-home.html
- Cisco NAC Guest Server
  http://www.cisco.com/c/en/us/support/security/nac-guest-server/tsd-products-support-series-home.html

Accessibility Features in Cisco ISE 2.3

Cisco ISE 2.3 supports accessibility for the user facing web portals only. Cisco Web Accessibility Design Requirements (ADRs) are based on W3C Web Content Accessibility Guidelines (WCAG) 2.0 Level AA requirements. Cisco ADRs cover all Section 508 standards and more. Cisco ADRs website, http://wwwin.cisco.com/accessibility/acc_center/adrs_web/main.html, provides all information and resources for the accessibility requirements.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.1.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.