Release Notes for Cisco Identity Services Engine, Release 2.2

Revised: October 29, 2020

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

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.

Note **We strongly recommend that you rollback any existing hot patches in your current deployment before applying ISE 2.2 Patch 5.**

Note **We have recalled ISE 2.2 Patch 4 due to an issue we found after posting. An updated patch file has been reposted, and the new file name is ise-patchbundle-2.2.0.470-Patch4-221755.SPA.x86_64.tar.gz. If you already installed the previously posted patch, you MUST uninstall that patch, and install the new one.**

Note **We have recalled ISE 2.2 Patch 6 due to an issue we found after posting. An updated patch file has been reposted, and the new file name is ise-patchbundle-2.2.0.470-Patch6-232642.SPA.x86_64.tar.gz. If you already installed the previously posted patch, you MUST uninstall that patch, and install the new one.**

Note For more information about the features that are supported in Cisco ISE 2.2, see *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

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 2.2

Ability to Detect Anomalous Behavior of Endpoints

Cisco ISE protects your network from the illegitimate use of a MAC address by detecting the endpoints involved in MAC address spoofing and allows you to restrict the permission of the suspicious endpoints. The following options are available in the profiler configuration page:

- Enable Anomalous Behavior Detection—Cisco ISE probes for data and checks for any contradictions to the existing data. If any contradictions are found, the *AnomalousBehavior* attribute is set to true and the corresponding endpoints are displayed in the Context Visibility page.

- Enable Anomalous Behavior Enforcement—A CoA is issued if anomalous behavior is detected. The suspicious endpoints are reauthorized based on the authorization rules configured in the Profiler Configuration page.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

ACS to ISE migration Tool Enhancements

- Migration of RADIUS or TACACS based configurations—You can migrate objects specific to RADIUS or TACACS. You can use this option if your Cisco Secure ACS deployment includes only TACACS or RADIUS configurations.
- Selective object migration—The migration tool allows you to select the high-level configuration components such as Dictionaries, to be migrated from Cisco Secure ACS to Cisco ISE. You can migrate all the supported configuration components or select some of the high-level configuration components from the list of configuration components based on your requirements.
- Special characters in object names—If the names of the ACS data objects contain any special characters that are not supported by Cisco ISE, the migration tool converts the unsupported special characters to underscore (_) and migrates the data objects to Cisco ISE. The auto-converted data objects are displayed as warnings in the export report. However, if LDAP/AD attributes, RSA, RSA realm prompts, internal usernames, or predefined reference data contain any special characters that are not supported by Cisco ISE, the export process fails.
- Enhanced help—In the migration tool UI, choose **Help > Migration Tool Usage** to view the details of the options that are available in the migration tool.

For more information, see the *User Guide for Cisco Secure ACS to Cisco ISE Migration Tool, Release 2.2*.

Auth VLAN DHCP and DNS Service Enhancements

While configuring the DHCP service, you can also assign specific DHCP options for clients that connect to the Auth VLAN. You can add multiple DHCP options to each scope that you define. The options available in the drop-down list are as defined in RFC 2132. You can add additional customized options by selecting **Custom** from the drop-down list.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Context Visibility Enhancements

User-based views have been added.

Cryptobinding TLV Support

You can enable the crytobinding TLV option if you want the EAP peer and EAP server to participate in the inner and outer EAP authentications of a PEAP authentication.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Custom User Attributes

The following data types are supported for the custom attributes on the User Custom Attributes page:

- String—You can specify the maximum string length.
- Integer—You can configure the minimum and maximum range.
- Enum—You can specify the internal value and the display value. You can also specify the default parameter. The values that you add in the Display field are displayed while adding or editing a Network Access or Admin user.
- Float
- Password—You can specify the maximum string length.
- Long—You can configure the minimum and maximum range.
- IP—You can specify a default IPv4 or IPv6 address.
- Boolean—You can set either True or False as the default value.
- Date—You can select a date from the calendar and set it as the default value. The date is displayed in yyyy-mm-dd format.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Dial-in Attribute Support

Cisco ISE supports dial-in check to check the dial-in permissions of the user during authentication or query. The result of the check is returned to the device on the RADIUS response.

Dictionary Check for Internal User and Admin User Password

While configuring the password settings for internal users and admin users, you can choose if the password can contain any dictionary word or its characters in reverse order.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Endpoint Identity Groups in Posture Policy

You can create posture policies based on the endpoint identity groups. The endpoint identity groups are listed in the Identity Groups column in the Posture Policy page.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Guest Enhancements

- Single-click guest account approval—Self Registered guests that require approval can be approved by a Sponsor by clicking a link in the approval request email.
- Custom portal file upload—You can upload files to ISE and use them in portals.
- Directory attributes can be used to determine sponsor group membership. Active Directory, LDAP, SAML, and ODBC attributes are supported.

- Auto-timezone—Cisco ISE uses the timezone from the Sponsor portal's browser while creating guest accounts. Default times are created for that timezone when the sponsor creates an account. You must create timezones for your sites.
- You can now add, remove, resize, and reorder columns on the Manage Accounts page. You can also search the list by phone number. The column "creation date" has also been added.
- Hide password from sponsor—You can prevent the Sponsor from seeing the guest password when the guest is notified; the password is sent to the guest.
- Sponsor access to pending accounts—Access to all or only the Sponsor's accounts is now supported for Active Directory and LDAP.
- Auto-send sponsored guest credentials—Email notification can be sent automatically; the Sponsor does not need to click the Notify button.
- Account import supports passwords—Cisco ISE now supports setting account passwords while importing the user account details using a CSV file.
- Hotspot CoA—You can now choose the CoA type used by Hotspot portals.
- ERS API now supports creating guest types and sponsor groups, and setting account passwords.
- Portal background image—You can add a background image to a portal in the Customization page for that portal.
- Cisco ISE now supports Apple Captive Network Assistant (CNA) mini-browser for Guest and BYOD flows.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

JSON Support for APIs

Cisco ISE 2.2 supports JSON for all APIs. For more information, see the online SDK.

Network Conditions

Each network condition defines a list of objects that can be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request. The operator that you use in the condition can be either match (in which case the value presented must match at least one entry within the network condition) or no matches (it should not match any entry in the set of objects that is present in the network condition).

After you create a network condition with a name, you can reuse this condition multiple times across various rules and policies by referring to its name.

You can create the following network conditions to restrict access to the network:

- Endstation Network Conditions—Based on endstations that initiate and terminate the connection.
- Device Network Conditions—Based on the AAA client that processes the request.
- Device Port Network Conditions—Based on the device's IP address, name, NDG, and port (physical port of the device that the endstation is connected to).

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Network Device Group Hierarchies

You can view the network device group hierarchy in Tree view or Flat Table view. In the Tree view, the root node appears at the top of the tree followed by the child groups in hierarchial order. Click Expand All to view all the device groups under each root group. Click Collapse All to list only the root groups.

In the Flat Table view, you can view the hierarchy of each device group in the Group Hierarchy column.

You can also view the number of network devices that are assigned to each child group. Click the number link to launch the Network Devices window, which lists all the network devices that are assigned to that device group. You can add additional devices to a device group or move the existing devices to another device group.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

OTP Token Caching

While configuring a RADIUS token server or RSA Identity Source, you can enable Passcode Caching if you want Cisco ISE to store the passcode in the cache after the first successful authentication with an RADIUS token server. Cisco ISE uses the cached user credentials for the subsequent authentications if they happen within the configured time period.

Enter the number of seconds for which the passcode must be stored in the cache in the Aging Time field. Within this period of time, the user can perform more than one authentication with the same passcode.

Note We strongly recommend that you enable this option only when you use a protocol that supports encryption of the passcode, for example, EAP-FAST-GTC.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Posture Enhancements

- The Firewall condition checks if a specific Firewall product is running on an endpoint. You can enforce policies during initial posture and Periodic Reassessment (PRA).
- The application visibility condition queries for applications that are installed on an endpoint. This improves the overall visibility of the software installed on your endpoints.
- AnyConnect client provisioning and posture discovery do not mandate CoA and URL redirection. The flow is seamless for on/off premises, third party NADs, and Cisco NADs. Without URL redirection, you can connect to the ISE PSN directly. This eliminates the need to depend on Cisco NADs to support redirection. It also ensures faster onboarding process without discovery.

Note You should enter the provisioning URL or perform a secondary authentication (on premises) only when you download the AnyConnect agent for the first time.

- Support for deploying the AnyConnect agent in Stealth mode to monitor and enforce Cisco ISE posture policies.
- You can configure AnyConnect in Clientless mode.
- Endpoint context visibility using the Unique Identifier (UDID) attribute.

For more information, see the Client Provisioning Without URL Redirection for Different Networks section and *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

pxGrid Enhancements

- You can generate the pxGrid certificate from the **Administration > pxGrid Services > Certificates** page. You can generate the pxGrid certificate from the Primary Administration Node. The following options are available:
  - Generate a certificate with or without certificate signing request
  - Generate bulk certificates
  - Download root certificate chain
- You can enable pxGrid with Base license, but you must have a Plus license to enable pxGrid persona.
- In a high availability configuration, you can check the pxGrid Services page to verify whether a pxGrid node is currently in active or standby state.
- IPv6 filtering support for session topic.
- You can use the Test option on the pxGrid Settings page to run a health check on the pxGrid node. You can view the details in the pxgrid/pxgrid-test.log file.
- pxGrid support for UTF-8 and additional attributes.

RADIUS DTLS

You can use RADIUS DTLS protocol for RADIUS authentication. RADIUS DTLS provides improved security for DTLS tunnel establishment and RADIUS communication.

RADIUS IPsec Security for Cisco ISE-NAD Communication

Cisco ISE supports RADIUS IPsec protocol to secure communication with the Network Access Devices (NADs). Cisco ISE supports IPsec in Tunnel Mode or Transport Mode. IPsec can be enabled on GigabitEthernet 1 through GigabitEthernet 5 interfaces. You can configure IPsec on only one Cisco ISE interface.

Note Gig0 is the management interface and IPsec is not supported on Gig0.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

RADIUS Shared Secret Minimum Length

Shared secret length must be equal to or greater than the value configured in the Minimum RADIUS Shared Secret Length field in the Device Security Settings page (Administration > Network Resources > Network Devices > Device Security Settings).

For the RADIUS server, best practice is to have 22 characters. Note that for new installation and upgraded deployment, by default, this value is 4 characters. You can change this value on the Device Security Settings page.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Serviceability Enhancements

- Show CPU Usage Command Enhancements—The output of the **show cpu usage** command now includes several Cisco ISE functions and lists the percentage of CPU utilization. For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.
- ISE Counters and Key Performance Metrics reports are introduced in this release.

  Cisco ISE collects data for various attributes and provides the ISE Counters report that lists the threshold values for these attributes. You can use this information for capacity planning and debugging Cisco ISE issues. You can check the value for these attributes against the threshold values and if there is an increase in any particular attribute, you can correlate this information with the issues in your deployment to identify a possible cause.

  The Key Performance Metrics report provides information about the number of RADIUS requests that were handled by each PSN in the deployment, the average and maximum load on each server, the average latency per request, and the average transactions per second. For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Session Trace Test Cases

This tool allows you to test the policy flow in a predicable way to check and verify the way that the policy is configured, without needing to have real traffic originate from a real device. You can configure the list of attributes and their values to be used in the Test Case. These details are used to perform interactions with the Policy system to simulate the runtime invocation of policy. The attributes can be configured by using the dictionaries. All the dictionaries that are applicable to Simple RADIUS authentication are listed in the Attributes field.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Smart Call Home Enhancements

Cisco ISE provides support for Transport Gateway. If your organization's security policy does not allow communication between the ISE servers in your network and the Smart Call Home (SCH) servers, you can use an optional Transport Gateway to act as a proxy for SCH communication. The Transport Gateway software can be downloaded from Cisco.com and can be installed and maintained on a Linux server. Refer to the *Smart Call Home Deployment Guide* for information on how to deploy the Transport Gateway software on an RHEL server.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Stateless Session Resume Support for EAP-TLS

While configuring EAP-TLS protocol settings, you can enable stateless session resumption for EAP-TLS sessions. Cisco ISE supports session ticket extension as described in RFC 5077. Cisco ISE creates a ticket and sends it to an EAP-TLS client. The client presents the ticket to ISE to resume a session.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Support for Enrollment Over Secure Transport

Cisco ISE now supports the Enrollment Over Secure Transport (EST) protocol, which is a successor to the SCEP protocol. EST handles certificate provisioning in a more secure and robust manner. Cisco ISE CA can now provision ECC-based certificates to devices that connect over a BYOD flow.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Support for Microsoft Hyper-V Virtual Machines

Cisco ISE can be installed on Microsoft Hyper-V servers. For more information, see the *Cisco Identity Services Engine Installation Guide, Release 2.2*.

Support for Multiple TrustSec Matrices

Cisco ISE allows you to create multiple policy matrices for different scenarios. You can use these matrices to deploy different policies to different network devices. For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Support for DEFCON Matrices

DEFCON matrices are standby policy matrices that can be easily deployed in the event of network security breaches.

You can create DEFCON matrices for the following severity levels: Critical, Severe, Substantial, and Moderate.

When a DEFCON matrix is activated, the corresponding DEFCON policy is immediately deployed on all the TrustSec network devices. You can use the Deactivate option to remove the DEFCON policy from the network devices.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

Support for MySQL

MySQL database can be used as an ODBC identity source. For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

TC-NAC Enhancements

- This release of Cisco ISE supports integration with Cisco Threat Analytics (CTA), Rapid7 Nexpose, and Tenable Security Center (Nessus scanner) adapters.
- FireAMP adapter enhancements:
  - You can select the event source to which you want to subscribe. The following options are available: AMP events only, CTA events only, and CTA and AMP events.
  - When you change the advanced settings or reconfigure an adapter, if there are any new events added to the AMP cloud, those events are also listed in the Events Listing page.

  - You can choose a log level for the adapter. The available options are: Error, Info, and Debug.
- You can use the show container tc-nac CLI command to view information about the Vulnerability Assessment adapters and their statuses.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

TrustSec-ACI Integration Enhancements

Cisco ISE now supports the following options:

Policy Plane—You can select this option if you want Cisco ISE to interact only with APIC data center to interchange SGT, EPG, and SXP information.

Data Plane—If you select this option, in addition to SGT and EPG, additional information is provided to the ASR devices that are connected between the TrustSec network and the APIC-controlled network. These ASR devices must contain the Translation tables for SGT-to-EPG and EPG-to-SGT conversion.

Note SXP mappings are not propagated to ACI if you select the Data Plane option.

For more information, see the *Cisco Identity Services Engine Administrator Guide, Release 2.2*.

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

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

Active Directory Search Changes

To improve the accuracy of user identification, this patch changes the attributes used to search Active Directory from SAM and CN to just SAM. \

You can change the attributes back to the previous default. For instructions, see the Further Problem Description field of defect CSCvf21978.

Decommissioned Dashlets

The following dashlets have been decommissioned in Cisco ISE 2.2 patch 8 and above 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.

System Requirements

Note For more details on Cisco ISE hardware platforms and installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.2*.

Supported Hardware

Cisco ISE software is packaged with your appliance or image for installation. Cisco ISE, Release 2.2 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)		

Table 1 Supported Hardware and Personas (continued)

Hardware Platform	Persona	Configuration
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 2.2*.[1] • For hard disk size recommendations, refer to the "Disk Space Requirements" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.2*. • 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 8 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 8 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 Edge beta 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.
  - When self-signed certificates are used, Cisco ISE portal may fail to launch in Microsoft Edge beta 77 browser even if URL redirection is successful. To resolve this issue:
    a. Add both DNS name and IP address in the Subject Alternative Name (SAN) field.
    b. After the ISE services are restarted, redirect the portal in a different browser.
    c. Choose View Certificate > Details and copy the certificate by selecting the base-64 encoded option.
    d. Install the certificate in Trusted path and relaunch the browser.
  - You might see a warning message while downloading an executable (EXE) file in Google Chrome 76 or later. To resolve this issue:
    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 2.2 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 2.2 supports Multi-Forest/Multi-Domain integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 2.2 supports up to 50 domain join points.

Supported Anti-Virus and Anti-Malware Products

See the following link for specific anti-virus and anti-malware support details for Cisco NAC Agent and Cisco NAC Web Agent:

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

Cisco NAC Web Agents have static compliance modules which cannot be upgraded without upgrading the Web Agent.

Installing Cisco ISE Software

To install Cisco ISE, Release 2.2 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 2.2 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 2.2*. Before you run the setup program, ensure that you know the configuration parameters listed in Table 2.

Table 2 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

Table 2 Cisco ISE Network Setup Configuration Parameters (continued)

Prompt	Description	Example
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 2.2*, 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 69.

Upgrading to Release 2.2

You can directly upgrade to Release 2.2 from the following Cisco ISE releases:

- 1.4
- 2.0
- 2.0.1

- 2.1

Due to the following known issues, we recommend that you apply the latest patch to your current Cisco ISE version before upgrade:

- CSCvc38488
- CSCvc34766

If you are on a version earlier than Cisco ISE, Release 1.4, you must first upgrade to one of the releases listed above and then upgrade to Release 2.2.

This release of Cisco ISE supports GUI as well as CLI based upgrade.

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

GUI-Based Upgrade

The GUI-based upgrade from the Admin portal is supported only if you are currently on Release 2.0 or later and want to upgrade to Release 2.2.

CLI-Based Upgrade

From the Cisco ISE CLI, you can upgrade from Release 1.4, 2.0, 2.0.1, or 2.1 directly to Release 2.2.

Supported Operating System for Virtual Machines

Release 2.2 supports Red Hat Enterprise Linux (RHEL) 7.0.

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

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").

Also, the secondary PAN is unable to join the primary PAN to make a cluster for ISE Indexing engine if reverse DNS is not configured, displays error in VCS pages.

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

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 2.2* for a list of pre and post upgrade tasks.

Known Upgrade Issues

This section lists the known upgrade-related caveats. See Cisco ISE, Release 2.2 Open Caveats for a description of these caveats.

- CSCvc78816
- CSCvc94037
- CSCuy49511

Due to the following known issues, we recommend that you apply the latest patch to your current Cisco ISE version before upgrade:

- CSCvc38488
- CSCvc34766

Cisco Secure ACS to Cisco ISE Migration

You can directly migrate to Cisco ISE, Release 2.2 only from Cisco Secure ACS, Releases 5.5 or later. For information about migrating from Cisco Secure ACS, Releases 5.5 or later to Cisco ISE, Release 2.2, see the *Cisco Identity Services Engine Migration Tool Guide*.

You cannot migrate to Release 2.2 from Cisco Secure ACS 5.1, 5.2, 5.3, 5.4, 4.x, or earlier versions, or from Cisco Network Admission Control (NAC) Appliance. From Cisco Secure ACS, Releases 4.x, 5.1, 5.2, 5.3, or 5.4, you must upgrade to ACS, Release 5.5 or later, and then migrate to Cisco ISE, Release 2.2.

Note If you are installing Cisco ISE, Release 2.2 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 2.2. 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.

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

Profiler RADIUS Probe

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

LDAP Attributes in Authorization Policies After Migration

After migration from ACS to ISE 2.2, you cannot add LDAP attributes to the ISE TACACS+ authorization policies.

You can duplicate the migrated authorization policy and add the required attributes in the new policy. For further information, you can refer to defect CSCvg97689.

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 2.2

- 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 2.2 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 2.2, 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 2.2*.

For more information on Cisco ISE, Release 2.2 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 3 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 For the installation of ISE 2.1 and previous versions, you must ensure the service is 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 4 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 2.2* 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.

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

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 2.2*.

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 2.2*.

- **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 2.2*.

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 24).

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 2.2*.

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.

Cisco ISE, Release 2.2.0.470 Patch Updates

This section provides information on patches that were made available after the initial availability of the Cisco ISE 2.2 release. Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions.

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

Cisco ISE version 2.2.0.470 was the initial version of the Cisco ISE 2.2 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 “2.2.0.470 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, “2.2(0.9NN)” where NN is also the patch number, displayed as two digits. For example, version “2.2.0.470 patch 2" corresponds to the following version in the bug database “2.2(0.902)”.

The following patch releases apply to Cisco ISE release 2.2:

Resolved Issues in Cisco ISE Version 2.2.0.470 —Cumulative Patch 17

Delay in information sent to PxGrid client after MnT failover

When a MnT node failover occurs, a PxGrid client does not receive session information from Cisco ISE until the failed primary MnT node is restored to the network. 20 to 30 minutes after the primary MnT node is back online, PxGrid clients will receive session information from Cisco ISE once more.

In a larger deployment where a Cisco ISE node only has one Cisco ISE persona will not receive session information from Cisco ISE in the case of a MnT node failover. You must enable PxGrid persona on the same node that serves as he primary MnT node to ensure PxGrid clients receive session information.

Table 6 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 17. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 17 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 5 Cisco ISE 2.2.0.470 - Patch 17- Resolved Caveats

Caveat ID Number	Description
CSCvf94942	Enhance error message shown for TACACS authorization rule failure with no command set
CSCvg42399	Support internal user attributes as DACL name while CoA with ASA
CSCvh86082	Parsing NMAP smb-os-discovery data should remove
or x00
CSCvj41029	User domain name may remain empty in session when ISE passive-id AD agent or MS WEF is used
CSCvj66943	ISE not using SSL for LDAP for "Retrieve Attributes" however connects to port 636
CSCvk48115	ISE 2.3 RSA SecurID authentication fails
CSCvk50684	RADIUS DTLS and Portal usage not being assigned to new self-signed certificate on hostname change
CSCvm62775	ISC BIND krb5-subdomain and ms-subdomain Update Policies Vulnerability
CSCvn12644	ISE Crashes during policy evaluation for AD attributes
CSCvv42857	MAC 11.0 support for ISE is not available
CSCvo11090	Able to delete ACI IEPG in ISE
CSCvo47391	Multiple Vulnerabilities in krb5
CSCvo49755	To enable CLI clock timezone command
CSCvo98554	After Importing ISE PB to ISE, Login page is not loaded
CSCvp17458	libssh2 SSH_MSG_CHANNEL_REQUEST Packet Handling Out-of-Bounds Read Vulnerability
CSCvp19539	ISE 2.2 Sign On Button grey out with Guest portal second factor Radius Token server authentication
CSCvp86673	Application server stuck in Initializing due to corrupted indexes
CSCvp93322	Significant memory increase in MNT during Longevity test
CSCvp96921	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvq02371	High Auth Latency - no info which thread pool is causing the issue
CSCvq13431	ISE PSN node crashing while fetching context attributes during posture plus RADIUS flow

Table 5 Cisco ISE 2.2.0.470 - Patch 17- Resolved Caveats (continued)

Caveat ID Number	Description
CSCvq61089	My Device Portal does not show a device after BYOD on-boarding with SAML authentication
CSCvq73677	GNU patch OS Shell Command Injection Vulnerability
CSCvq86848	Move devices to another group botton should be disabled when access has been restricted to NDG
CSCvr09749	GNU patch do_ed_script OS Shell Command Execution Vulnerability
CSCvr09759	Certificate is not loading from Oracle to NSSDB properly
CSCvr13481	ISE ERS SDK NetworkDeviceGroup DELETE does not specify ID location
CSCvr29863	Validation needed RADIUS Cisco DNA Center-ISE REST call sp. char (&) and ( ) in shared secret fails
CSCvr31312	ISE fails to load Network devices page while filtering on IP/Mask
CSCvr33160	PassiveID live sessions are shown even when PassiveID funcationality is not enabled
CSCvr33778	FreeType Buffer Over-Read Vulnerabilities
CSCvr40574	Export failed in ISE gui in case of private key encryption failed no ERROR message in ISE GUI
CSCvr50921	GUI login with AD user failing when similar internal user is disabled
CSCvr63504	Unable to delete SCEP profile because it is referencing system certificates
CSCvr70581	Called-Station-ID missing in RADIUS Authentication detail report
CSCvr83696	ISE prefers cached AD OU over new OU after changing the Account OU
CSCvr84125	Config restore from one platform on another platform set incorrect UDI in sec_hostconfig table
CSCvr84143	tzdata needs to be updated in ISE guest OS
CSCvr84753	AD status shows up as "updating.." indicating the process is hung
CSCvr84978	LDAP bind test does not use the correct server when defined per node
CSCvr85513	Core file generated on PSN
CSCvr96189	NDG device references not cleaned out of ISE DB, preventing NDG deletion
CSCvs01924	ERS Admin account disabled incorrectly due to password expiry
CSCvs02166	API calls show different result as GUI
CSCvs03810	ISE doesn't display the correct user in RADIUS reports if the user was entered differently twice
CSCvs03998	ISE 2.3 patch 6 LDAP test GUI flow with multiple results does not generate error observed in runtime
CSCvs04384	Internal user's custom attributes fields are empty while creating through ERS API
CSCvs07344	Reset config on 2.4 patch 9 throws some errors despite finishing successfully
CSCvs14297	PassiveID: Configuring WMI with an AD account password that contains a $ will result in an error
CSCvs34839	SNMP process stops after continuous snmpwalk queries
CSCvs39880	Highload on Mnt nodes with Xms value

Table 5 Cisco ISE 2.2.0.470 - Patch 17- Resolved Caveats (continued)

Caveat ID Number	Description
CSCvs42441	Service account passwords returned from server in SMS and LDAP page
CSCvs44006	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvs55464	Creating a new user in the sponsor portal shows "invalid input"
CSCvs65467	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvs67042	ISE 2.2+ affected with memory leak. Everyday 1-2% increase in native memory due to Inflater()
CSCvs86686	Multiple Vulnerabilities in patch
CSCvs86690	Multiple Vulnerabilities in python
CSCvs86697	Multiple Vulnerabilities in sudo
CSCvs88222	Vulnerability in unzip package - RHEL 7
CSCvs91408	LONG:Significant memory increase in PMNT node of longevity test
CSCvs96516	Multiple Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities
CSCvs98602	X.Org libX11 Client Segmentation Fault Denial of Service Vulnerability
CSCvs98604	X.Org libX11 Off-by-One Memory Write Arbitrary Code Execution Vulnerability
CSCvt03935	Change "View" options wording in TrustSec Policy Matrix
CSCvt15935	High Load Alarms coinciding with System Summary Dashboard not populating for some nodes
CSCvt67595	Livelogs are not showing for User authentication failed
CSCvu09984	MnT DB reset fails on 2.2 P14/P15/P16
CSCvu42244	Machine Authentications via EAP-TLS fail during authorization flow citing a user not found error
CSCvu53022	ISE prefers cached AD OU over new OU after changing the Account OU
CSCvv43558	Evaluation of positron for Apache Struts Aug20 vulnerabilities
CSCvt05169	Operations menu on SAN with MnT persona is not available in ISE 2.2 and above
CSCvs48878	DuplicateManager not removing packet after RADIUS pre-parsing fails
CSCvr88811	new alarm configuration failing for Excessive Radius/Tacacs authentication attempts
CSCvk35613	Profiled Endpoints Summary report: Last 7 days takes more than 3mins

Resolved Issues in Cisco ISE Version 2.2.0.470 —Cumulative Patch 16

Table 6 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 16. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 16 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 6 Cisco ISE 2.2.0.470 - Patch 16 - Resolved Caveats

Caveat ID Number	Description
CSCux25333	Dashboard allows special characters: <>?"'
CSCvd16468	Missing NAD info in Alarm "Unknown SGT was provisioned"
CSCvd88105	Account expiration email not sent when extending the validity of an account
CSCvf32944	PRRT should not abort if LDAP id store is corrupted
CSCvg76883	Cisco Identity Services Engine (ISE) Information Disclosure Vulnerability
CSCvh19430	Guest account activation time discrepancy for imported accounts
CSCvh80768	ISE 2.3 no patches, unable to login to sponsor portal with internal user
CSCvi03093	Purging doesn't work if Identity group name was changed/ change is not reflected to purge policy
CSCvi16994	ERS Guest User operations fail with 401 Unauthorized if Sponsor_Portal_Sequence missing
CSCvi50874	Endpoint Oracle Persist Received value wrongly counted in ISE Counters report
CSCvi86385	Is ISE affected by Spring Framework CVE-2018-1270
CSCvj43999	Self-signed account creation error: "An attempt to text your account information to you has failed"
CSCvk53782	ISE ENH: Allow RADIUS Dictionary VSA "Vendor Attribute Size Field Length" of 2 bytes
CSCvm75687	MyDevices Portal: Can't change device status on a PSN running with secondary PAN.
CSCvm81243	endpointcert/certRequest API call causes Internal CA Service to Crash in ISE
CSCvo04342	Multiple Vulnerabilities in jackson-databind
CSCvo87602	Memory leak on ISE node with the openldap rpm running version 2.4.44
CSCvo94666	ISE 2.4 P5 : Profiling : Netflow probe not working on ISE Bonded Interface
CSCvp00421	ISE Profiler SNMP Request Failure Alarms should show the reason of failure
CSCvp01553	No serialization or batching when large scale(>300) NADs are moved between MatrixA to MatrixB
CSCvp02082	Env data is missing when TrustSec-ACI integration is enabled.
CSCvp03249	ISE: SMTP server sending Email notification gets Exhausted
CSCvp33598	ISE deletes all endpoint if mac address is deleted twice at the same time
CSCvp40509	Internal User not found in prrt-server intermittently even though PrRTCpmBridge returns user found
CSCvp45598	SystemTest : Error when deleting SCEP RA profile
CSCvp54424	AD Diagnostic tool shows low level API query failed w/ Response contains no answer. Check DNS config
CSCvp70644	Expired guest accounts purge is stuck after daylight time change
CSCvp83214	ISE ERS Create via the API does not use the specified ID

Table 6 Cisco ISE 2.2.0.470 - Patch 16 - Resolved Caveats (continued)

Caveat ID Number	Description
CSCvq21272	Wrong password being notified after password reset (Only on SMS)
CSCvq27110	Core files on PSN servers causing High Disk Utilization alarms
CSCvq45008	ISE doesn't store self-registered EndPoints in configured custom group
CSCvq50182	ISE does not show logging when CTS pac is expired
CSCvq58785	Static group information is lost from EP in some scenarios
CSCvq66846	Move to Mapping Group drop down menu limits SGT Mapping groups to 25
CSCvq69138	Change logging level of 90140 INFO PassiveID: Message parsed syslog to DEBUG
CSCvq69228	pxGrid controller contacting terracotta.org
CSCvq71264	Static group assignment losing from guest flow
CSCvq71844	"Cache not properly initialized" message in every Profiler Policy and cannot update Profiler Feed
CSCvq72760	When updating password for administrative user it is possible to bypass entering current password
CSCvq74649	ISE sponsor portal - sorting by creation date doesnt work
CSCvq77051	Network devices added via restful API fails authentication with a 'Network Device not located' error
CSCvq81381	Internal user using token password will be disabled due to password expired
CSCvq88821	SNMP traps on access switch connected to APs causes incorrect profiling.
CSCvq97641	ISE 2.4 localhost-<date>.log files growing upto and more than 8 Gb in size
CSCvq97680	ISE 2.6 Patch 2: EAP-TLS auth not matching endpoint groups
CSCvq98277	No password audit will be generated after user change ISE internal user enable password via ASA CLI
CSCvr00348	Posture assessment by condition report is showing empty records.
CSCvr07263	when creating Purging Rule ,Radius directory will hang if there is no plus license
CSCvr08988	in ex-Radius scenario ,ISE should replace state attribute before forwarding access challenge to NAD
CSCvr13218	Framed-Interface-Id RADIUS attribute not sent in access-accept if IPV6 address is in ::xx format
CSCvr13444	REST API: Create Network Device with special character (" ") in password field is interpreted as utf
CSCvr13464	ISE ERS SDK NetworkDeviceGroup PUT does not show ID placement in the API call
CSCvr16439	CSV report to remote repository is truncated when we pull the report for the last 30 days.
CSCvr20389	ISE reports < radius authentication > page displays the last page empty.
CSCvr24458	Network Device POST API allows for characters and spaces in Model name of device, GUI does not
CSCvr25197	After changing password via UCP, "User change password audit" report doesn't have "Identity"

Table 6 Cisco ISE 2.2.0.470 - Patch 16 - Resolved Caveats (continued)

Caveat ID Number	Description
CSCvr43077	Day0: iPad OS 13.1 BYOD flow got failed
CSCvr46529	Password lifetime expiration reminder appears for Internal Users with external passwords
CSCvr48729	BEMS Creation P1 SR 687382890, Unable to access My Devices portal
CSCvr51959	ISE 2.4 Not entire fqdn is matched, but fragment of characters
CSCvr53428	ISE services are not coming up after installing patch 2.3 p7
CSCvr62517	ISE 2.4 p9 Session directory write failed : String index out of range: -1
CSCvr64067	ISE MnT Stops Showing Live Logs after 90% Purge
CSCvr67988	ISE sponsor's e-mail gets CC'd even when view/print guests' passwords is disabled
CSCvr70581	Called-Station-ID missing in RADIUS Authentication detail report

Resolved Issues in Cisco ISE Version 2.2.0.470 —Cumulative Patch 15

Table 7 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 15. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 15 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 7 Cisco ISE 2.2.0.470 - Patch 15 - Resolved Caveats

Caveat ID Number	Description
CSCvp98834	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities
CSCvb45390	Collection Filters configured with Username not working for TACACS+ authorization/accounting
CSCvb56579	Device name is truncated after 14 characters in the SXP devices page
CSCvd48081	Shouldn't allow deletion of pxGrid certificate on any ISE node
CSCvd88480	Location filter for ERS Network Device get-all API fails
CSCve63006	Scheduled report is not working after server restart

Table 7 Cisco ISE 2.2.0.470 - Patch 15 - Resolved Caveats (continued)

Caveat ID Number	Description
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
CSCvf45333	Exception within time and date condition not working properly for authorization
CSCvf45991	Pseudo double authentication request on AD
CSCvf52671	ISE 2.1 + TACACS+ authentication report must display the command executed
CSCvg72876	Internal CA certificate update traffic between PAN and PSN causing failure to process NAD update
CSCvh54956	ISE 2.2 patch 5: EST Service is not running after upgrade
CSCvh95236	ISE sends CoA after receiving a RADIUS Accounting-STOP
CSCvi18412	ISE 2.3 p2 is sending redundant CoA message during VPN Posture Flow
CSCvi27613	Endpoints are profiled even when profiling is disabled
CSCvi65932	Blank pop-up message displayed in Sponsor Portal if customField contains "null" value
CSCvi72862	Accounting updates tolerance for suppression needs to be more efficient
CSCvi99138	ad_agent.log flooded with entries from non-whitelisted domains
CSCvj02810	"No data available" message seen in the Authorization Profile page when a NAD profile used in authorization profile is deleted
CSCvj02829	SCCM MDM attribute “LastPolicyRequest” is not converted correctly in ISE
CSCvj61028	HTTP error 401 unauthorized message seen in External CA settings page while adding a new CA
CSCvk01929	Changing the name of "All_User_ID_Stores" Identity Source Sequence breaks new policy sets.
CSCvk13724	EPG mappings not created in ISE
CSCvk27295	NMAP fails to execute when an endpoint matches Admin created profiling policy
CSCvk31092	Core: SyslogSecureTCPConnection::updateConnectionData
CSCvk48315	Live sessions are not seen in ISE Live Logs page in ISE 2.4
CSCvk52803	Different FQDN in SAN DNS field of admin certificate can cause CV issue
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
CSCvm00481	Disabling internal certificate authority in Web UI does not stop Certificate Authority Service
CSCvm11175	ISE custom endpoint attribute type String doesn't allow to add only numbers
CSCvm39909	Live log detailed reports shows msec instead of seconds for session timeout

Table 7 Cisco ISE 2.2.0.470 - Patch 15 - Resolved Caveats (continued)

Caveat ID Number	Description
CSCvm48075	Manual CoA fails from Context Visibility if Live logs or Live Sessions page is not accessed before
CSCvm81230	Cisco Identity Services Engine (ISE) Arbitrary Client Certificate Creation Vulnerability
CSCvn18843	PSN crash due to underlying routing table issue
CSCvn21316	ISE: logwatch process failed with ::1 fatal error
CSCvn21926	Parser error seen in Threat Centric NAC CTA Configuration irrespective of ISE version
CSCvn36029	Date displayed in Unix Epoch format when context visibility data is exported
CSCvn51282	ISE replaces "ip:" to it's hostname in "ip:inacl" Cisco AV-Pair
CSCvn62788	TC-NAC configured with Qualys shows Not Reachable
CSCvn73740	EAP-TLS authentications with Endpoint profile not set to Unknown fails in second authorization
CSCvn81631	Cores generated consistently if accounting request comes with empty username for TACACS+ flow
CSCvn85484	Removing SCEP RA Profile causes the associated CA chain to be removed from Trusted Store
CSCvo17704	ISE 2.4: CLI password does not accept 3 $ characters
CSCvo51295	ISE 2.2 Sponsor: Single click approval flow displays wrong message when approval link is clicked twice
CSCvo75129	Runtime prepends " " to ";" in dhcp-class-identifier in syslog message sent to profiler
CSCvo82930	Repeated exceptions from profiler.log in debug mode
CSCvp07591	Active Directory Machine authentication fails with error "22040 Wrong password or invalid shared secret"
CSCvp18692	AD User information not shown in Context Visibility page
CSCvp18932	Outdated jquery library used by ISE
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
CSCvp50557	Changing maximum user global settings is not logged in change configuration audit
CSCvp54949	BYOD flow not working in IOS 12.2
CSCvp58945	Import of network device template throws error “Failed illegal value for Encryption key”
CSCvp59286	Multiple Vulnerabilities in struts2-core
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

Table 7 Cisco ISE 2.2.0.470 - Patch 15 - Resolved Caveats (continued)

Caveat ID Number	Description
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
CSCvp76617	ISE customer endpoint attribute type string doesn't allow certain numbers
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
CSCvq14925	Renewed self-signed certificate doesn't get updated in trusted store
CSCvq17464	Cannot update internal user with External Password ID Store via ERS
CSCvq29336	When the user clicks the Details option in the Live Logs page, an error is seen if the session ID contains "-" symbol
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
CSCvq51955	Network Conditions does not work if shorten version of IPv6 is used
CSCvq52340	Delete All operation performed in Network Access Users internal ID store is not reported in the Change Configuration Audit
CSCvq56241	ISE user import does not fail when invalid characters are included in the username
CSCvq66370	ISE uses old sxp-core jar file even after patch upgrade

Resolved Issues in Cisco ISE Version 2.2.0.470 —Cumulative Patch 14

Table 8 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 14. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 14 might not work with older versions of SPW. MAC users must upgrade to MacOsXSPWizard 2.2.1.43 or later and Windows users must upgrade to WinSPWizard 2.1.0.51 or later

Table 8 Cisco ISE 2.2.0.470-Patch 14 - Resolved Caveats

Caveat ID Number	Description
CSCvo19377	Successful Authentication Entries not shown in the RADIUS Report due to exceeding the CSV limit
CSCuz00603	Unable to add duplicated mappings to multiple SXP VPNs
CSCvc74631	endpoints/NAD template import failure with basic license
CSCvd79952	EasyConnect CoA not sent after session merge in distributed deployment
CSCve03360	AD Probe not triggered/retrieving OS info when domain PC auth to network
CSCvg70813	ISE dmp files are not deleted from /opt/oracle/base/admin/cpm10/dpdump for failed backup attempts
CSCvh22907	Sponsor Portal Page takes more than 10 seconds to load
CSCvh51992	Cisco Identity Services Engine Authenticated CLI Denial of Service Vulnerability
CSCvh81189	CLI Get all Endpoints is failing with ORA-01000: maximum open cursors exceeded
CSCvi21737	ISE 2.2 has too many journal files.
CSCvi67780	ISE Internal CA : SAN ext validation fails if it isn't the first entry in RequestedExtensions in CSR
CSCvi82192	Generate pxGrid Certificates page doesn't respect cert template RSA key size
CSCvj31598	Import two CA certs with same subject name
CSCvj73440	import of duplicate CA mapped to syslog shouldnt be allowed
CSCvj75478	Device network conditions missing
CSCvj97277	Fix for CSCvf68738 does not allow legitimate CA certificate refresh
CSCvk09721	add environment variable for Radius proxy
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.
CSCvk40421	Not able to delete certificate from trusted page
CSCvk43032	Wrong number or types of arguments in call to 'COLLATIONDAILY_PURGE',HOURLY_STATS_JOB
CSCvk59716	Domain Admins are not able to edit Sponsor accounts properly
CSCvk70087	SecureSyslogCollectors should be disabled by default on remote log targets.
CSCvk70748	High CPU and High Auth Latency and OOM condition on PSN nodes
CSCvk74989	Certificate parameters not persistent after DNAC trust re-establishment
CSCvm05840	NAD CSV imports should allow all supported characters
CSCvm10275	Cisco Identity Services Engine Cross Site Scripting Vulnerability
CSCvm12105	ISE 2.3 not hitting policy with Session BYOD-Apple-MiniBrowser-Flow condition
CSCvm16952	Oracle Security Alert Advisory - CVE-2018-3110

Caveat ID Number	Description
CSCvo19377	Successful Authentication Entries not shown in the RADIUS Report due to exceeding the CSV limit
CSCvm47638	ISE-secondary node doesnt send COA when guest account gets suspended or deleted
CSCvm63427	Cisco Identity Services Engine Password Recovery Vulnerability
CSCvm74605	ISE: EAP-FAST prefers cached AD DN over new DN after changing the Account OU
CSCvm75790	SAML with ADFS is broken with 3rd party NAD
CSCvm87060	ISE 2.x : Remote forest Active Directory controller failover prolonged time
CSCvm87292	Unable to integrate Tenable adapter to ISE 2.4 & 2.5 2.2 2.3
CSCvm89126	ISE 2.3 patch 5 : NAD / AAA server address is not specified.
CSCvm90478	"No Data Available" when attempting to add endpoints to Identity Group with RBAC User
CSCvm93821	Authorization policy evaluation failing intermittently when using identity group as condition
CSCvm99398	SGACL Push in large scale NAD environment causes High CPU on PAN
CSCvn01551	Failed to upload AC packages of file size > 50MB on ISE->Agent Resources
CSCvn10971	ISE: Rebooting associated site-specific GC does not result in failover to other GC
CSCvn12114	Not Matching Internal User Group in Certificate Authentications
CSCvn12229	log4j.appender.ACS-FILE.MaxBackupIndex is not working in ISE
CSCvn23570	ISE: Import Network Device does not conform to admin access permissions
CSCvn24392	Certain characters are not being parsed properly
CSCvn27325	Posture policy with Tunnel Group Name in condition is not hitting
CSCvn29633	ISE does not follow the capabilities of the Listener.
CSCvn31755	400 Bad Request when logging out Sponsor Portal
CSCvn33441	RBAC permissions do not propagate for admin users who login ISE with AD
CSCvn35579	SXP connection between ISE and IOS Devices stuck in DeleteHoldDown state
CSCvn37048	ISE 2.x || ISE syslog message code (59200-59208) are not being used in ISE currently.
CSCvn39998	Pullout reports from Authentication Summary report is showing empty report.
CSCvn52886	User name from WMI information is deleted on receiving a DHCP custom syslog for same endpoint
CSCvn55560	ISE 2.3 after applying patch 5 creation of EOB Guest user does not work
CSCvn55640	Manage ACC calling infinite time when sponsoruser configured with permissions ALL&GROUP sponsor grps
CSCvn59383	ISE 2.3 patch 5 issue when creating guest user on sponsor portal using special character
CSCvn59502	ISE DACL syntax checking is not properly catching errors
CSCvn61139	Smart Licensing agent thread lock causes GUI login delay in ISE 2.2

Caveat ID Number	Description
CSCvo19377	Successful Authentication Entries not shown in the RADIUS Report due to exceeding the CSV limit
CSCvn62164	ISE should support internal users with Special char colon : character to be partiy with ACS
CSCvn64652	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvn65317	ISE not able to assign guest account to the same guest type used for previous user
CSCvn66198	Sponsor portal doesn't refresh the accounts after deleting users and requires a manual refresh
CSCvn69854	ISE includes only one prrt-server file in support bundle
CSCvn70558	MDMServerReachable does not work for SCCM MDM again
CSCvn72150	Nodes have high IO spikes frequently in VM performance reports
CSCvn75254	check box under custom network device profile list getting uncheck
CSCvn76567	ISE 2.4 - IP-SGT bindings disappear from SXP for user session
CSCvn79557	ISE : Custom user attribute change does not reflect changes in configuration change audit report
CSCvn82729	COA messages to multiple trustsec devices are not sent in parallel anymore but serially.
CSCvn85498	ISE 2.4 : InactiveDays attribute update with disabled profiling
CSCvn98932	Non-existed DACL is not verifyed by the ISE
CSCvo10441	Cisco Identity Services Engine Cross-Site Scripting Vulnerability
CSCvo10487	Cisco Identity Services Engine SSL Renegotiation Denial of Service Vulnerability
CSCvo19076	ISE endpoint purge ACTIVEDIRECTORY dictionary is not loading
CSCvo35516	Device Sensor not able to correctly parse DHCP attributes via RADIUS probe
CSCvo36837	Admin group cannot get access to "Users" at "Device Administration" tab after install patch 5
CSCvo41052	ISE deleting the newly created IP-SGT mapping
CSCvo45582	Internal Administrator Summary report not allowing to select specific columns
CSCvo45606	ISE:WMI-Passed values may compromise the security of ISE. Please remove malicious scripting terms
CSCvo48352	CSV file of RADIUS authentications report may have duplicate records
CSCvo48975	ISE downloads unneeded RA certificate for BYOD
CSCvo49521	ISE Adds an additional character at the end of OperatingSystemVersion
CSCvo74766	ISE DACL syntax checking validation failing on wildcard notation
CSCvo82021	ISE : Memory usage discrepancy in GUI and show tech
CSCvp13733	On rebooting connected DC, ISE sometimes doesn't failover to other available DC
CSCvp17444	Admin Access Blank page when using valid RSA/RADIUS Token credentials but is not in ISE Admin DB

Caveat ID Number	Description
CSCvo19377	Successful Authentication Entries not shown in the RADIUS Report due to exceeding the CSV limit
CSCvp29278	Cisco Identity Services Engine Blind SQL Injection Vulnerability
CSCvp40082	ISE 2.3/2.4 upgrade to the latest patch may break dynamic redirection for 3rd party NADs
CSCvk74345	PSN with SXP enabled restarts while running CTS authN
CSCvj90273	Multi-NIC Windows/macOS: ISE Posture Module Maps VPN IP to MAC Address of a Disconnected Interface
CSCvm35110	MNT node not purging data diligently before hitting 90% purge data disk utilization

New Features in Cisco ISE Version 2.2.0.470—Cumulative Patch 13

Fewer Results Per Report Page

The number of data rows in the reports displayed on the Cisco ISE **Reports** window has been revised from 5,000 to 1,000 for better performance.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 13

Table 9 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 13. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 13 might not work with older versions of SPW. MAC users must upgrade to MacOsXSPWizard 2.2.1.43 or later and Windows users must upgrade to WinSPWizard 2.1.0.51 or later.

Table 9 Cisco ISE 2.2.0.470-Patch 13 - Resolved Caveats

Caveat ID Number	Description
CSCvm66751	Guest AUP: AUP acceptance is triggering replication event.
CSCvd30891	ISE 2.x alarms page hangs
CSCvd56150	ISE 2.1 - cannot configure alarm settings

Caveat ID Number	Description
CSCve08389	IP-SGT Static Mappings not configured on N7K
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.
CSCvf49665	Issued pxGrid Certificates Do not appear in GUI
CSCvf55996	AD probe looking for host is not searching properly
CSCvg76171	'copy me' email address overwriting current login sponsor email address
CSCvg86633	Page counter in reports shows incorrect values
CSCvh09878	ISE 2.2P4 EAP-MD5 MAB session may stuck forever
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
CSCvh72872	ISE: Last field of DNS SAN in CSR doesn't accept numbers
CSCvh74979	Reset-config is reverting the fixes of patches and causing the issues.
CSCvh79901	APEX license should not be required to update MyDevices Portal
CSCvh97544	Short CPU spikes can be observed when client did not respond and ISE is used as RADIUS Proxy
CSCvi09027	"Delete ALL" Context Visibility does not log event in reports, Change Config Audit/Operations Audit
CSCvi30462	Bulk guest import does not work using when logged into sponsor portal using SAML provider,
CSCvi38373	ISE Delete All endpoints in Context Visibility too risky.
CSCvi41678	Endpoint Attributes not updated in context visibility
CSCvi42404	validDays does not match span of fromDate to toDate
CSCvi61204	ISE 2.1 Endpoint Purge policy is matched but job halts during execution.
CSCvi94778	DNACintergration failed,ISE 2.3p3,Default Trust certificates not loaded in fresh install and restart
CSCvj01047	Password length limitation when adding DC's in the PassiveID section of 32 characters.
CSCvj02644	Customer sees blank "Details" page in RADIUS Live Logs
CSCvj25696	User customer attributes order doesn't change after drag drop and save.
CSCvj47723	ISE 2.1 P6 or P7 Guest users receive error 400 after entering login and password. Intermittently
CSCvj50257	Active endpoints are mismatched from expected value
CSCvj63376	ISE 2.2 VPN MDM- Compliance not updated from MDM Compliance Checker for active session
CSCvj81800	Sponsor Portal Port 9002 Still Utilizes TLS 1.1
CSCvk02619	Imported Guest Accounts (csv) throw 400 Bad Request Error on First Login

Caveat ID Number	Description
CSCvk05318	Error Deploying IP SGT static Mapping on ISE
CSCvk10156	RBAC SuperAdmin Data Access over written by read-only data access for Network Device Groups
CSCvk23532	Remove GMT portion from $ui_start_date_time$ and $ui_end_date_time$ on Email Notifications
CSCvk28847	ISE sponsor's e-mail should not be in CC when view/print guests' passwords is disabled
CSCvk31960	Live logs are stopped because collector process not properly restarted.
CSCvk40105	Editing guest user throws pop up error when creating with java scripts in first and last name
CSCvk51667	ISE: "Manage accounts" gives 400 HTTP error if sponsor portal is configured for SAML authentication.
CSCvk59357	Admin warned of license non-compliance even after adding new licenses
CSCvk68196	SNMPv3 profiling works only with DES or AES128 privacy protocol
CSCvk72606	ISE- Can login to GUI with disabled admin accounts.
CSCvk74190	Radius Token Identity Caching Timeout not Configurable
CSCvm00127	ISE sponsor email customization doesn't add image properly
CSCvm03681	EAP-FAST doesn't support correct key generation in TLS 1.2
CSCvm03842	PxGrid SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection - CVE-2009-3555
CSCvm09377	HTTP Request Header for ISE fails if it contains @ in email
CSCvm15059	ISE 2.1+ : Identity Source Sequence info button information is wrong for Sponsor Portal
CSCvm16060	Cannot Disable Telnet Change Password
CSCvm20561	ISE 2.x || Cisco-Device profiler policy missing the tandberg OUI as a condition
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
CSCvm39902	Maintain Connectivity During Reauthentication option not working
CSCvm47507	Changes made in allowed protocols is missing in change configuration audit reports
CSCvm49084	ISE PB portal files are not restored with a restore of an old backup
CSCvm49091	ORA-01017: invalid username/password exception in collector log continuously
CSCvm49369	ISE 2.2 P9, guest user lost a possibility to login directly from Self-Registration Success page.
CSCvm56660	Increase the critical threshold limit for Node-Out-Sync from 100k to 250k
CSCvm61134	SXP debug logs are not dumped in sxp.log unless services are restarted
CSCvm70470	Max Sessions" value can not be applied on GUI after applying 2.2p10 or 2.3p4

Caveat ID Number	Description
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 creating random accounts for time restricted guest types fails
CSCvm74423	ISE 2.4 - Guest users aren't getting emails automatically while importing from CSV
CSCvm75765	ISE -"user's email is not valid" unable to create User for top level domains other than .com .in etc
CSCvm79293	ISE2.2 TACACS does not apply the command sets after long REGEX argument
CSCvm79609	Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability
CSCvm82504	Request to increase Radius Token Server password caching to 900 seconds or later
CSCvm86699	ISE CAC or certificate login does not populate external groups under new admin group
CSCvm87685	Menu access duplicate is failing with plus sign
CSCvm88149	Account Disable Policy 'Disable accounts after days of inactivity' is incorrectly calculated
CSCvm89837	Lost and Stolen buttons stay disabled on My Devices portal if Japanese GUI used
CSCvm91202	Cisco Identity Services Engine Password Recovery Vulnerability
CSCvm92317	ISE Kerberos Authentications are incrementing AD bad password count by 2
CSCvm98407	Show members delays to retrieve the N/w devices in NDG page
CSCvn01019	Modify existing Network Device Profiles, grayed SAVE button
CSCvn11424	PassiveID Management Logs Show Database ID instead of DC Name
CSCvn12200	Inconsistency in Deploying IP SGT static Mapping from ISE to Cisco switches.
CSCvn13802	ISE 2.4 :Unable to import network devices if shared secret contains "<"
CSCvm90359	pxGrid debug "warn" level causing XCP to stop running.
CSCvm70858	Triggered SNMP query not working properly for HP OUI.
CSCvm73506	Alarms: Profiler Queue Size Limit Reached.
CSCvn25367	VCS pages Auth/Endpoint tab shows blank pop up message.
CSCvi05438	Disable grid Delete All button for empty list.
CSCvj67414	ISE HSTS Max-Age parameter is too aggressive no includedDomains flag.
CSCvm05565	With 5 failure login, Apple iOS can still send credential by clicking "go".
CSCvn32780	Cancelling upgrade as temporary Monitoring persona could not disabled on new Primary PAN:2.5.0.337
CSCvm79526	Add Audit log for 'Push' operation.
CSCvn05718	External Admin GUI login/authentication is failing.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 12

Table 10 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 12. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 12 might not work with older versions of SPW. MAC users must upgrade to MacOsXSPWizard 2.2.1.43 or later and Windows users must upgrade to WinSPWizard 2.1.0.51 or later.

Table 10 Cisco ISE 2.2.0.470-Patch 12 - Resolved Caveats

Caveat ID Number	Description
CSCvm92278	Rollback 2.2 P11 is not reverting to correct adrt version
CSCvm93698	AD authentications are failing after applying 2.2 P11/ 2.4 P4
CSCvm80261	"Log Collection Error" alarms after patch 10 installation
CSCvn09504	TC-NAC configured with Qualys shows Not Reachable.
CSCvn17524	ISE Apache Struts CVE-2016-1000031 Vulnerability
CSCuq95531	Active Directory Diagnostic tool displays status as failure when recursive DNS queries are triggered.
CSCvd06105	Logrotate skipping some of the directories due to permission issues.
CSCvd54736	Log collection errors during TACACS+ authorization.
CSCvd68563	Few PSNs were stuck in initializing state due to time zone inconsistency in ISE deployment.
CSCvd69406	ISE 2.0 Patch 4: Posture Scan is continuously checking status on client.
CSCve74916	Cisco Identity Service Engine Privilege Escalation Vulnerability
CSCve97625	ISE 2.2 logs an exception when a RADIUS Accounting Stop request is received after CoA ACK.
CSCvf36421	Catalina.<date>.log files are not log-rotated.
CSCvf41105	Need to adjust DST clock settings for Africa/Cairo timezone.
CSCvf49844	Cisco Identity Services Engine Local Command Injection Vulnerability
CSCvf63414	Cisco Identity Services Engine Authenticated CLI Denial of Service Vulnerability
CSCvf69753	Cisco Identity Services Engine Authenticated Privilege Escalation Vulnerability
CSCvg16408	Static IP-SGT bindings created in ISE are not pushed to the selected TrustSec devices.
CSCvg21535	pxGrid stuck in initializing state when bond interface is configured.
CSCvg95440	Log collection error for TACACS+ messages.
CSCvm16523	Upgrade failed with the following error: "Nodes are not on the same ISE patch version"

Table 10 Cisco ISE 2.2.0.470-Patch 12 - Resolved Caveats (continued)

Caveat ID Number	Description
CSCvg95479	Cisco Identity Services Engine Command Injection to Underlying OS Vulnerability
CSCvh30067	ISE 2.2 PSN application server crashed intermittently.
CSCvi23713	Identity Group Assignment Search field is not working in specific browsers.
CSCvj24944	"device,port" network conditions skipped during authorization.
CSCvj92976	Incomplete error message while importing device icon for Network Device Profile.
CSCvj95709	Not able to enable pxGrid in FIPS mode.
CSCvk07631	ISE 2.2: Hot Spot portal users prompted to accept AUP more than once.
CSCvk08988	Not able to turn on FIPS mode when pxGrid is enabled.
CSCvk10081	ISE uses TLS 1.0 when proxy is configured and TLS 1.2 if no proxy configured.
CSCvk38374	When Email id of a sponsor is updated, pending requests from self-registered guests are not sent to the sponsor, if old Email id is used for approval.
CSCvm67602	ISE 2.2 patch 10 and 11: Integrity check failed.
CSCvk50720	ISE 2.2: Network Devices page is not loading.
CSCvm02478	Cisco Network Setup Assistant App not available on Google Play.
CSCvm14030	Evaluation of ISE for Struts remote code execution vulnerability August 2018
CSCvm41759	Error 400 displayed while signing out from Manage Guest Accounts page.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 11

Cisco ISE Release 2.2 cumulative patch 11 has been retracted from the Cisco Download Software site. The resolved caveats of 2.2 cumulative patch 11 have been included in 2.2 cumulative patch 12.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 10

Table 11 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 10. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 10 might not work with older versions of SPW. MAC users must upgrade to MacOsXSPWizard 2.2.1.43 or later and Windows users must upgrade to WinSPWizard 2.1.0.51 or later.

Table 11 Cisco ISE Patch Version 2.2.0.470-Patch 10 Resolved Caveats

Caveat ID Number	Description
CSCvj62592	Cisco Identity Services Engine Java Deserialization Vulnerability
CSCvj62614	Cisco Identity Services Engine File Upload Code Execution Vulnerability
CSCvd78169	CDP Attributes not added to EP via SNMP Query
CSCvf69738	JQuery JavaScript Library Multiple Vulnerabilities
CSCvf69805	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability
CSCvf75968	Multiple Vulnerabilities in httpasyncclient
CSCvg03064	License consumption count not updated on upgraded setup 2.0(FCS) to 2.4.152
CSCvg12398	Observing ORA-01000 maximum open cursors exceeded error in collector.log
CSCvg36077	Active Directory domain/forest becomes unavailable after receiving a Kerberos error
CSCvh09779	ISE 2.x TACACS log extremely slow
CSCvh11308	Cisco Identity Services Engine Logs Cross-Site Scripting Vulnerability
CSCvh57345	Restore of 1.4/2.0/2.0.1 backup fails which taken after Feed update
CSCvh66462	M&T purge causing app server to be down for extended period
CSCvh69910	Corrupted radius token server configuration causing crash
CSCvi06525	Single click approval sponsor not seeing self-registered guest with implicit/explicit UPN
CSCvi43687	ISE 2.2 Endpoint export may contain duplicate entries
CSCvj11981	SNMPv3 profiler breaks when auth or priv settings are configured
CSCvj38428	Changing status of Network Access Users doesn't appear on audit report
CSCvj94737	ISE 2.2 P9: Showing Error on CPP Sign On Page
CSCvj99698	Guest password is not reset if Sponsor does not have rights to view the Guest Password
CSCvk10454	Adding Node to deployment does not add the Profiling OUI data
CSCvk15628	My device portal- Unable to remove the stolen tab
CSCvk48105	Sponsor created guest have a previous guest account email CC'd
CSCvi44041	Cisco Identity Services Engine Privilege Escalation Vulnerability

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 9

Patch Parity: Cisco ISE 2.2 Patch 9 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 Patch 3.

Table 12 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 9. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 9 might not work with older versions of SPW. MAC users must upgrade to MacOsXSPWizard 2.2.1.43 or later and Windows users must upgrade to WinSPWizard 2.1.0.51 or later.

Table 12 Cisco ISE Patch Version 2.2.0.470-Patch 9 Resolved Caveats

Caveat	Description
CSCvf26143	LDAP authentication failure: LDAP identity store does not support PlainAuthenticateAndQueryEvent.
CSCvi73782	Static Group Assignment dropping due to DHCP Probe
CSCvi91353	NMAP scans for custom port 9100 but doesn't report it in nmap.log.
CSCvj53801	Profiler Policy Evaluation Memory Leak is causing High CPU and Auth latency.
CSCvg46899	ISE 2.2 user may be redirected again after AUP acceptance on Hotspot portal.
CSCvf82350	US27030 - Fix VPN Session to MAC Mapping
CSCvf90694	AnyConnect ISE posture shows "Internal system error" on MAC OSX

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 8

Patch Parity: Cisco ISE 2.2 Patch 8 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 Patch 3.

Table 13 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 8. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 8 might not work with older versions of SPW. MAC users must upgrade to MacOsXSPWizard 2.2.1.43 or later and Windows users must upgrade to WinSPWizard 2.1.0.51 or later.

Table 13 Cisco ISE Patch Version 2.2.0.470-Patch 8 Resolved Caveats

Caveat	Description

CSCvh48558	Context Visibility page was not loading in ISE 2.2 Patch 5.
	For CSCvh48558, we recommend that you reset Elasticsearch after applying ISE 2.2 patch 8 to clear the Context Visibility history data. To do this:
	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`
	Note Endpoint Capacity and Compliance Status Trend dashlets have been decommissioned in Cisco ISE 2.2 patch 8 and above to prevent performance issues when displaying large datasets. See Decommissioned Dashlets, page 11 for more details.

CSCvi31965	Authentication latency is observed while evaluating endpoint ID store and checking PIP policies during authorization.
CSCvi50542	Not able to configure the Telemetry schedule.
CSCuz00163	Endpoint profiling using Visibility Setup Wizard does not profile endpoints authenticating from other subnets.
CSCvd23874	Connection status of the endpoints are not updated properly in the Context Visibility Endpoints page.
CSCvd73085	NFS location could not be mounted and backup to this repository fails.
CSCvd93008	Smart Licensing feature is not working in ISE 2.1 if proxy communication method is used.
CSCve22706	Application server goes to initializing state if empty custom attributes are included in the RADIUS request.
CSCve63087	ISE is taking the client machine's time instead of the server time while scheduling reports.
CSCvf03310	Guest user authentication notification emails are sent twice.
CSCvf20208	ISE Posture Periodic Reassessment (PRA) timer expires and the device becomes noncompliant.
CSCvf35268	ISE 2.2 displays a blank page for scheduled reports for Key Performance Metrics, Misconfigured Supplicants, and Manual Certificate Provisioning reports.
CSCvg15960	ISE machine password refresh fails due to expired kerberos ticket and Active Directory Connector status shows "Not Connected".
CSCvg37786	While exporting a report to remote repository, data is partially truncated if it exceeds certain size.

Table 13 Cisco ISE Patch Version 2.2.0.470-Patch 8 Resolved Caveats (continued)

Caveat	Description
CSCvg61751	During upgrade, secondary node is stuck in de-register step and the old PAN does not respond.
CSCvg79089	Upgrade times out while enabling or disabling temporary MnT persona on the old or new primary PAN.
CSCvg83466	Telemetry event doesn't include profiling and network access information.
CSCvh02628	"Configured name server is down" alarms are seen every 90 minutes if unusable domains are detected in the Active Directory.
CSCvh18758	MDMServerReachable condition does not work for System Center Configuration Manager (SCCM) MDM in ISE 2.2 patch 4.
CSCvh77737	Unable to edit purge rules after Base license expiry.
CSCvi04684	Not able to save user-defined dictionary attributes in ISE 2.0, 2.1 and 2.2.
CSCvi17534	ISE Application server is stuck in initializing state if the orphaned cell matrix ID is Null.
CSCvi37601	"Smart Licensing Authorization Renewal Success" alarm is triggered every hour if Smart Licensing is enabled.
CSCvi51021	Successfully authenticated endpoints are not displayed in the Context Visibility Endpoints page in ISE 2.2 patch 5 if Plus or Advanced license is not installed.
CSCvi51291	Change of Authorization (CoA) fails to initialize if CoA is triggered after 48 hours from the time of initial authentication.
CSCvi88782	Application patch failure alarm is generated even if the patch is installed successfully.
CSCvj12073	ISE 2.2 patch 7 blocks SSH in FIPS mode.
CSCvf18466	ISE 2.1 endpoint lookup using MnT REST API was very slow. Now, approximately 1000 endpoints can be authenticated with the REST API with good performance.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 7

Patch Parity: Cisco ISE 2.2 Patch 7 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 Patch 3.

Table 14 lists the issues that are resolved in Cisco ISE, Release 2.2 cumulative patch 7. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, log in to the Cisco Download Software site with your Cisco.com login credentials, choose **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.

See the "Installing a Software Patch" section in the Administering Cisco ISE chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.2* for instructions on how to apply the patch to your system.

Patch 7 might not work with older versions of SPW. MAC users must upgrade to MacOsXSPWizard 2.2.1.43 or later and Windows users must upgrade to WinSPWizard 2.1.0.51 or later.

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

Table 14 Cisco ISE Patch Version 2.2.0.470-Patch 7 Resolved Caveats

Caveat	Description
CSCvi10727	After upgrading to ISE 2.2 patch 6, the Application server goes to Initializing state and high CPU usage is experienced if Bypass Suppression collection filters are configured.
CSCvg36087	When certificates with the same Subject Name are uploaded to the Trusted Certificates page, the ise-psc-log throws an exception, duplicate certificates are added into the NSS certificate database, and write permission is disabled.
CSCvg83484	ISE occasionally fails to send reports to Smart Call Home (SCH) services.
CSCvg98688	Cisco ISE generates core files when the application stop ise command is used.
CSCvh04289	User names that contain a period appear corrupted in the pxGrid login notifications.
CSCvh06189	Guest authorization policies do not work with the NetworkAccess:UseCase equals GuestFlow attribute.
CSCuy76263	The MnT menu options should not be appear in the Secondary PAN.
CSCva02256	Unable to view the Alarm Configuration option in the Alarm Settings page.
CSCvc54962	Exporting and importing language files under Sponsor Portal removes all customization.
CSCvc95735	ISE 2.1 /tmp files becomes full when you use `show logging | command.
CSCvd48590	In ISE 2.0, 2.1 and 2.2, unable to delete email logo in email notification for guest account credentials.
CSCvd49141	Fix for Cisco ISE Cross-Site Scripting Vulnerability.
CSCvd50693	Unable to delete endpoints from GUI.
CSCvd69677	ISE 2.1 Sponsor Portal-When the sponsor resets the guest password, an incorrect password is sent through email to guests.
CSCve31569	Unable to access the reports and live logs from PAN.
CSCve51076	Unable to create profiler condition of NMAP Extension type in ISE 2.1.
CSCve53737	Enhancement request to add an additional field to certificate generated by ISE CSR.
CSCve87076	Guest account fails authentication via PSN node.
CSCvf14521	The LDAP authentication fails with the “Does not support PlainAuthenticateAndQueryEvent” error after upgrade to 2.3.
CSCvf33004	Unable to delete corrupted files in LDAP identity sources.
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.
CSCvf68738	Need to disable or delete a part of the certificate chain used by system certificates in ISE Trusted Certificates Store.
CSCvf73922	Fix for Cisco Identity Service Engine DOM-based cross site scripting vulnerability.

Table 14 Cisco ISE Patch Version 2.2.0.470-Patch 7 Resolved Caveats

Caveat	Description
CSCvg15776	ISE occasionally fails to query the MDM compliance status of VPN endpoints, which results in matching an endpoint with an incorrect authorization profile during CoA.
CSCvg30444	A few logs are not displayed in the PSN after upgrade to 2.3.
CSCvg68883	As an external user, a large number of DB calls are made before loading the home page.
CSCvg71593	Latency observed with large number of network devices when local certificate is updated.
CSCvh31926	ISE 2.2 profiler represents noise in ise-psc.log for the nsf component when the SMB.operating-system discovery attribute is used.
CSCvh50630	Need to add the Hydrant certificate chain to the ISE default trusted certificate store.
CSCvh93036	Unable to restart services after rollback from ISE 2.2 patch 6.
CSCvh65838	Errors are reported in the stack trace report.
CSCvh99469	The Save option is disabled (grayed out) when the remediation text is pasted in the ISE Posture Requirements using Google Chrome.
CSCve98518	Login attempt limit must be enforced in the Guest portal.
CSCux88538	Support for aes256-ctr and aes128-ctr ciphers for SSH.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 6

Note **We have recalled ISE 2.2 Patch 6 due to an issue we found after posting. An updated patch file has been reposted, and the new file name is ise-patchbundle-2.2.0.470-Patch6-232642.SPA.x86_64.tar.gz. If you already installed the previously posted patch, you MUST uninstall that patch, and install the new one. However, you can install ISE 2.2 patch 7 or later on top of the old patch 6 file (one that was recalled) or new patch 6 file.**

Note If there are Collection Filters of type Bypass already configured on ISE, Cisco recommends deleting the expired Collection Filters of type Bypass. You should retain the suppression event before applying the Cisco ISE 2.2 patch 6. If you do not delete the expired Collection Filters, ISE nodes can potentially experience high CPU usage due to defect CSCvi10727.

Patch Parity: Cisco ISE 2.2 Patch 6 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 P3.

Table 15 lists the issues that are resolved in Cisco Identity Services Engine, Release 2.2 cumulative patch 6. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, 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.

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 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.2*. for instructions on how to apply the patch to your system.

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

Table 15 Cisco ISE Patch Version 2.2.0.470-Patch 6 Resolved Caveats

Caveat	Description
CSCuv28369	The TCP Dump page is not accessible through the Cisco ISE GUI.
CSCuz52877	An ISE Authentication Inactivity alarm is triggered every 15 minutes.
CSCuz93468	Stopping the ISE application server causes it to hang with the "Stopping ISE Profiler Database" error.
CSCvb30158	Guests encounter an error when a request for sponsor approval is sent through the Self-Registered Guest portal.
CSCvd30712	ISE shows latency in displaying Network devices in the Network Device Groups page.
CSCvd40593	Cisco ISE does not display Dashboard data or add new Endpoints into the database while Profiling is enabled and the Plus license is unavailable.
CSCve53355	Error in the ISE 2.2 Rest API while using group filters for internal users.
CSCve55046	Endpoint purge fails for sub-groups created under the default endpoint identity group for the guest flow.
CSCve79008	Subdomain email addresses cannot be used for email notifications in the guest flow.
CSCvf00883	pxGrid authorization denied and also takes 20 minutes to start working after primary pxGrid node is down.
CSCvf06497	Unable to save the Open Database Connectivity (ODBC) external identity source when the name contains the dot (.).
CSCvf19536	The **Never Purge** option applied to an endpoint parent group does not work with subgroups.
CSCvf20174	An error is reported when the Export All option in the Context Visibility page is used.

Table 15 Cisco ISE Patch Version 2.2.0.470-Patch 6 Resolved Caveats

Caveat	Description
CSCvf38307	PSN does not listen on RADIUS ports 1645 and 1646 after reboot or restart. **Workaround** Perform any one of the following: **Step 1** In the primary PAN, choose **Administration > Logging > Collection Filters**. **Step 2** If the page is displayed, verify that at least one of the collection filters is disabled. **Step 3** Reload the current page. **Step 4** Restart the ISE process on the PSNs. OR **Step 1** Choose **Administration >System > Settings > Protocols > Radius > UDP Ports**. **Step 2** Assign new port numbers and Click **Save**. **Step 3** Reassign the original port numbers. **Step 4** Click **Save**. OR **Step 1** Perform a manual synchronization of the affected node with the PAN.
CSCvf39615	A “No Policy Server Found” error is reported in Microsoft Windows 10 Home machines for posture.
CSCvf41185	Network access devices configured with the load balancer and automated tests results in disconnected user/machine sessions.
CSCvf43886	An MnT session is not cleared, when the Accounting stop request is received with the IP address as the calling-station-ID for a session which was learned with the MAC address as the calling-station-ID.
CSCvf63799	When the SGT value is updated in the Cisco ISE server, the IP-SGT mapping on the SXP listener is removed.
CSCvf69963	Fix for Cisco ISE Cross-Site Scripting Vulnerability in the Admin portal.
CSCvf70099	Orphaned endpoints in redis database due to redis server connection timeout.
CSCvf73306	An error is not reported when an invalid value is assigned to the “Profile.String(128):Required” field while importing the Network Device CSV file.

Table 15 Cisco ISE Patch Version 2.2.0.470-Patch 6 Resolved Caveats

Caveat	Description
CSCvf73453	An error is reported when importing CSV files containing special characters. **Workaround** Delete the special characters in the CSV file and manually type it in the ISE GUI.
CSCvf75989	The RADIUS accounting interim updates fail to update the inactive number of days with Base license.
CSCvg05089	Guest user is allowed to bypass the Acceptable Use Policy (AUP) page.
CSCvg17302	ISE does not display an error message when manually adding an endpoint that is already existing in the Context Visibility > Endpoints page.
CSCvg19428	Increase in ISE configuration backup file size due to increased ElasticSearch transaction logs.
CSCvg46494	Unable to purge endpoints that are added to the ISE database with IdentityGroup EQUALS Null.
CSCvg55183	Incorrect time range is applied in the Authentication Summary Report.
CSCvg55811	Key Performance Metrics (KPM) report query triggers High Load Average alarms on the MnT node.
CSCvg81687	Cisco ISE Monitoring and Troubleshooting Session Database stops running. **Workaround** Restart services.
CSCvg86571	Incorrect use of transaction management leads to database operations issues.
CSCvh02928	Error in the Reverse DNS lookup when the old JAR file is not deleted.
CSCvh07382	A log collection error is reported for MDM operations when the length of the Unique Identifier (UDID) is greater than 50 characters.
CSCvh18245	Unable to restore ISE 1.4 Patch 11 configuration backup on ISE 2.2 Patch 4 and above. Restoring configuration data on ISE 2.2 Patch 3 is successful.
CSCvh32178	Profiler Radius probe listener does not listen on port 30514.
CSCvh37273	A system error is reported when adding network devices.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 5

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.

Patch Parity

Cisco ISE 2.2 Patch 5 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 P3.

Table 16 lists the issues that are resolved in Cisco Identity Services Engine, Release 2.2 cumulative patch 5. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, 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.

Patch 5 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.2*. for instructions on how to apply the patch to your system.

Table 16 Cisco ISE Patch Version 2.2.0.470-Patch 5 Resolved Caveats

Caveat	Description
CSCvd10486	Profiled endpoints associated with a suspended or deleted sponsored guest user account are occasionally listed in the GuestEndpoints endpoint identity group.
CSCve81653	BYOD flag is set to Unknown status after successful BYOD flow.
CSCux66193	Cisco ISE sends the environment data to a device even after the SGT is removed.
CSCva56322	In ISE 2.1, an internal error occurs when accessing Work Centers > Identities.
CSCvc36556	/CSCOcpm/logs/crypto.log file is not overwritten and results in increased disk space.

Table 16 Cisco ISE Patch Version 2.2.0.470-Patch 5 Resolved Caveats

Caveat	Description
CSCvc98033	Authentication policies without MAB/dot1x rules at the top level results in users hitting incorrect policies, if sub-conditions are not configured under the main policy.
CSCvd32710	The Redis.log file is not rotated/purged well and results in increased disk space.
CSCvd85618	When a SGT value is changed, ISE occasionally fails to update the new SGT value in TrustSec policies.
CSCvd88782	ISE IP-SGT mapping feature hangs until the Network Access Device responds. **Workaround** Close the mapping window and fix the issue on the Network Access Device.
CSCve33558	Curly braces or parentheses in TACACS+ shell profile fails input validation.
CSCve34689	While generating reports, an “Unable to Connect to the Operation Database" error is reported by the MnT node. **Workaround** Reload the MnT node.
CSCve43607	A “Stopping ISE Profiler Database” error is reported when the Product Identifier (PID) is not found, is empty, or is another active process running in the redis.pid file. **Workaround** Perform the following checks in the rediscontrol.sh script file: • Check if the PID file belongs to the Redis server. • Check if the PID file is empty or incorrect. • Check if the PID file is present in the Redis server.
CSCve50370	Remote database transactions can occasionally fail on the Primary PAN.
CSCve73968	ISE MAC authentication bypass (MAB) fails without endpoint static group assignment and a profiling license.
CSCve78606	ISE 2.3 application service resets as ISE runs out of memory.
CSCve82240	A comma appears at the end of email addresses of sponsors. **Workaround** Modify the email field and manually remove the comma.
CSCvf21978	Occasional errors encountered in certificate-based authentication for Active Directory users.
CSCvf42743	When ISE is restarted, the trusted certificate configured in the LDAP identity source can be deleted.
CSCvf57412	“Oops Something Went Wrong” error is reported after installing ISE 2.2 Patch 2.
CSCvf89109	Guest import from CSV files remains in pending state after upgrade to ISE 2.2.

Table 16 Cisco ISE Patch Version 2.2.0.470-Patch 5 Resolved Caveats

Caveat	Description

CSCvf91538	By default, the “End of Business Day” option is selected on the sponsor portal.
	
	Workaround Perform the following steps to remove the default selection:
	
	1. Open “Portal Page Customization” of your portal.
	2. Choose “Sponsor Portal Settings'” and find “Instructional Text”.
	3. Click on “Toggle to HTML” and insert script.
	4. Click on “Toggle to HTML” to close the field and click “Save”.
	5. Use “Portal test URL” to check how it works.
	
	<script>
	$("#availableGuestTypes").on('click', function(evt) {
	setTimeout(function(){
	$('#endofday').trigger('click');
	$('#endofday').attr('disabled', true);
	}, 5000);
	});
	</script>

CSCvg19509	Log rotation of the syslog (/var/log/messages) fails occasionally and leads to filling up of /var partition. **Workaround** Contact TAC to clean the disk if an alarm is triggered.
CSCvg23034	After changing the Security Group ACLs in a cell from Deny IP to Permit IP, the Change of Authorization (CoA) is pushed after 4-5 minutes.
CSCvg29196	The Authentication Summary report is not generated after applying ISE 2.1 Patch 5. **Workaround** Perform the following steps: 1. Replace the attached post_sqlloader.sql file in /opt/CSCOcpm/mnt/bin folder. 2. Rename the existing file as post_sqlloader_old.sql. 3. Change the ownership to chown iseadminportal:ise post_sqlloader.sql No Restart is required.
CSCvg29763	CSV imported endpoint labels occasionally changed from statically assigned group to either Unknown or Profiled.
CSCvg32162	ISE Scheduled Backup occasionally does not progress after 75% when SFTP repository is used.
CSCvg37179	Cisco ISE Application server initializes due to database connection exhaustion.
CSCvg46464	Cisco ISE 2.3 Application server initializes due to database connection leaks. **Workaround** Reload ISE.

Table 16 Cisco ISE Patch Version 2.2.0.470-Patch 5 Resolved Caveats

Caveat	Description
CSCvg53547	Redundant data query instead of cache query when searching for non-existent internal users.
CSCvg54665	Profiler: DB connection leak in endpoint delete flow via GUI.
CSCvg76888	Egress policies are not displayed in the Source Tree View in the ISE GUI.
CSCvg81968	Unable to edit or save policy set using Microsoft Internet Explorer 11 browser and ISE 2.2. **Workaround** Use Mozilla Firefox browser.
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.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 4

Note **We have recalled ISE 2.2 Patch 4 due to an issue we found after posting. An updated patch file has been reposted, and the new file name is ise-patchbundle-2.2.0.470-Patch4-221755.SPA.x86_64.tar.gz. If you already installed the previously posted patch, you MUST uninstall that patch, and install the new one.**

Patch Parity: Cisco ISE 2.2 Patch 4 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 P3.

Table 17 lists the issues that are resolved in Cisco Identity Services Engine, Release 2.2 cumulative patch 4. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, 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.

Patch 4 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.2*. for instructions on how to apply the patch to your system.

Table 17 Cisco ISE Patch Version 2.2.0.470-Patch 4 Resolved Caveats

Caveat	Description
CSCvd56372	Deadlock occurs in Oracle alert log.
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.
CSCvd81222	MNT collation job takes longer time than expected.
CSCve13949	Large *.trm and *.trc files are created in the directory/opt/oracle/base/diag/rdbms/cpm10/cpm10/trace path resulting in utilization of the disk space.
CSCve94453	The Oracle database reloads with KPM metrics errors.
CSCve97765	An error is reported for EAP-TLS authentication on Apple iOS 11 devices.
CSCvf22318	An ElasticSearch and database shards error is reported on the Endpoints Context Visibility page.
CSCvf24580	RADIUS authentication report: RADIUS records are not filtered correctly with “Today” and “Yesterday” options.
CSCvf42061	An “Exception: all shards failed” error is reported on the Endpoints Context Visibility page.
CSCvf44272	ISE 2.2 Patch 2 core files should not be written to root partition. **Workaround** Delete core files from the root directory.
CSCvf47316	Fix for Entry Definition Framework (EDF) memory leak upon rollback.
CSCvf69018	Issue with reverse lookup when nodes are registered to Cisco ISE after applying ISE 2.2 Patch 1.
CSCvf75225	PAN runs high CPU due to 100K limit in the Redis server.
CSCvf77462	A “Failed to classify endpoint exception” is reported in the profiler.log file.

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 2.2 Patch 4.
	
	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`

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 3

Patch Parity: Cisco ISE 2.2 Patch 3 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 P3.

Table 18 lists the issues that are resolved in Cisco Identity Services Engine, Release 2.2 cumulative patch 3. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, 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.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.2*. for instructions on how to apply the patch to your system.

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

Table 18 Cisco ISE Patch Version 2.2.0.470-Patch 3 Resolved Caveats

Caveat	Description
CSCva95303	In ISE 2.2 Catalina.out.<date> and catalina.<date>.log take huge space.
CSCvd03239	SNMPv3 with AES256 encryption for SNMP profiling probe does not work in ISE 1.1.x/1.x/2.x.
CSCvd61307	An internal error is reported in the Passive ID even after successful Passive ID authentication.
CSCvd74794	ISE Cross-Site Scripting (XSS) vulnerability in the guest portal.
CSCvd87482	ISE Cross-Site Scripting (XSS) vulnerability in the Cisco ISE portal.
CSCve73657	If the default condition in authentication inner policy is set to a value other than DenyAccess, the default value reverts to DenyAccess after restart.
CSCvf32992	Re-import of LDAP server certificates is possible.

New Features and Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 2

Wireless Setup Enhancement

The Wifi Setup feature is disabled by default in Cisco ISE 2.2 patch 2. It is recommended to enable it in a lab environment and not in a production environment. Use the **application configure ise** command for demonstration. Select option 17 **Enable/Disable Wifi Setup** to enable or disable this feature.

Security Enhancements

ISE TLS Version 1.0 Support

In Cisco ISE 2.2 Patch 2, ISE TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants do not support TLS version 1.0. To use the ISE TLS based EAP authentication methods in TLS version 1.0, you must check **Allow TLS 1.0** configuration in the Security Settings page.

ECDSA Signature Algorithm, ECDHE_ECDSA Cipher Suite Support

The ISE Administration and ISE EAP Authentication Server support imported ECDSA signature certificates.

This enhancement allows you to negotiate ECDHE_ECDSA cipher suites when the ISE server certificate(s) are imported for Administration and/or EAP Authentication Server.

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

Steps to Import ECDSA certificate signed by Windows Server

Step 1 Generate Key and CSR in MAC:

1. Install openssl to generate key and CSR.
2. To generate the key, openssl ecparam -out <name_key.pem> -name secp384r1(prime256v1) -genkey
3. To generate the CSR, openssl req -new -key <name_key.pem> -out <name_csr.pem> -sha384(sha256)

Transferring **<name_csr.pem>** file to the Windows server

Step 2 Generate certificate using Windows Server command prompt:

Use the following command to generate the ECDSA certificate:

certreq.exe -submit -attrib "certificateTemplate: <ECDSA_template_name>" <name_csr.pem> <Certifiate_name.cer>

Note Since ECDHE curve templates (template version 4) is not displayed in Web Enrollment, ISE is unable to generate the certificate using web enrollment. It is recommended to use command prompt to generate the certificate.

Only ECDSA certificate curve types P-256 and P-384 are supported as a System Certificate

SSH Server

- In Cisco ISE the key exchange algorithm is restricted to **ecdh-sha2-nist** settings. Cisco ISE is enhanced to restrict the SSHv2 Key Exchange Algorithms to any combination of, **ecdh-sha2-nistp256 ecdh-sha2-nistp384** and/or **ecdh-sha2-nistp521**.

For example, ISE CLI global configuration command, **service sshd key-exchange-algorithm ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521**.

- The Administration Access Authentication Failure settings in the **Administration** UI is moved from the **Password Policy** tab to **Lock/Suspend Settings** tab.

When you use the SSH public key authentication, the Lock/Suspend Settings applies to SSH CLI.

Enhances LDAPS Support

Cisco ISE enhances the LDAP or LDAPS server with Active Directory using LDAPS access, to use it as the authorization identity source for ISE Administration. In earlier than 2.2 Patch 2 release, ISE only supported Active Directory Identity Source for Authorization to the ISE Administration application.

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 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

Note **Allow TLS 1.0** option is disabled by default in Cisco ISE 2.2 Patch 2 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 SHA-1 Ciphers—Allows SHA-1 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 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 Unsafe Legacy TLS Renegotiation for ISE as a Client and Accept Certificates without Validating Purpose—When this option is enabled:
  - 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 is configured as secure TCP syslog client
    - Cisco ISE is configured as secure LDAP client

  - When ISE acts as an EAP 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.

- Allow ECDHE-RSA, 3DES, DSS ciphers—Allows ECDHE-RSA, 3DES, DSS ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as EAP server (DSS ciphers are not permitted)
  - Cisco ISE is configured as RADIUS DTLS server (DSS ciphers are not permitted)
  - 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.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 2

Patch Parity: Cisco ISE 2.2 Patch 2 has parity with Cisco ISE 1.3 Patch 8, 1.4 Patch 11, 2.0 Patch 5, 2.0.1 Patch 4, and 2.1 P3.

Table 19 lists the issues that are resolved in Cisco Identity Services Engine, Release 2.2 cumulative patch 2. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, 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.

Patch 2 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.2*. for instructions on how to apply the patch to your system.

Table 19 Cisco ISE Patch Version 2.2.0.470-Patch 2 Resolved Caveats

Caveat	Description
CSCve80868	PAN with ISE 2.2 Crashes, displays Out Of Memory Error.
CSCuy98580	AD connector crashed when changing the DNS while AD is joined.
CSCvd33649	MnT session purges after being inactive for 5 days but SXP mappings sessions retain in SXP engine.
CSCvd56328	SYSAUX tablespace fills up, and CPU spikes on MNT nodes.
CSCvd61189	ISE 2.2 sends incorrect RADIUS service-type attribute.
CSCvd62856	ISE Application Server initializes after applying patch 3 on ISE 2.1.
CSCvd69784	ISE shows high authentication latency on PSN nodes.
CSCvd97143	The PAN nodes crashes, when you rename an endpoint identity group or edit its description.

Table 19 Cisco ISE Patch Version 2.2.0.470-Patch 2 Resolved Caveats

Caveat	Description
CSCve01655	When you click Save, ISE 2.2 posture condition changes to "&" automatically.
CSCve08815	In ISE 2.2, Wireless Setup Docker occupies 65536 addresses.
CSCva94303	ISE 2.1 triggers false alarm when backup or a bond interface configured for redundancy.
CSCvb75125	After upgrading from ISE 2.0 to ISE 2.1 and enabling AD profiling probe in GUI, operation success message is displayed. However, AD probe field remains unchecked after navigating to another tab and returning to the previous page.
CSCvc13039	Endpoint identity group does not change via the hot spot portal.
CSCvc28417	ISE back-up fails intermittently from CLI and GUI.
CSCvc51943	ISE application-server process crashes due to syslog handling.
CSCvc65379	ISE 2.1 Admin GUI user login delays, takes a minute.
CSCvc67783	Upgrade from ISE 2.0.1 P2 to ISE 2.1 fails on internal users.
CSCvc79381	In ISE 2.1, replication fails, displays “Error in synchronizing object.”
CSCvc79739	ISE data base grows very large due to EDF database table logs, causing giant backups.
CSCvc81803	Cisco Identity Services Engine GUI Denial of Service Vulnerability.
CSCvc82731	Database import fails on secondary node while trying to register a node to Primary Administration node.
CSCvc83519	When an ISE node is rebooted, TC-NAC containers in the ISE node are not able to communicate with Internet or other hosts.
CSCvc83795	Guest portal doesn't accept password with < and ! special characters.
CSCvc87853	SNMP process stops and restarts by itself after.
CSCvc98411	Unable to generate live logs in MnT nodes.
CSCvd11537	ISE generates huge number of start/stop dropping messages in syslog.
CSCvd14878	Unable to delete Filtered Endpoints when custom filter is in use.
CSCvd14926	Unable to save Network Condition in Authorization policy.
CSCvd16176	ISE 2.1 P3 Suspends Guests after reinstating, unable to add their devices to the Identity Group.
CSCvd18121	"BYOD-Apple-MiniBrowser-Flow" session dictionary attribute is unavailable in ISE after upgrading to 2.2.
CSCvd20214	ISE web admin unable to see the list of NADs if both Super Admin and System Admin are added to it.
CSCvd21954	TACACS+ authentication requests fail due to memory leak.
CSCvd22667	Guest web-portal\CWA authentication, guest web-portal redirect after Authentication.
CSCvd27408	ISE fails to reconnect to syslog server if TCP connectivity gets disconnected.
CSCvd28829	When you upgrade from 2.0, 2.0.1 or 2.1 to 2.2, custom RBAC policy causes UI elements to disappear.

Table 19 Cisco ISE Patch Version 2.2.0.470-Patch 2 Resolved Caveats

Caveat	Description
CSCvd29533	One-Click approval does not work with the "Only accounts assigned to this sponsor" option.
CSCvd32769	ise-elasticsearch.log files doesn't rotate or purge properly it generates more in number and fills the disk space.
CSCvd32782	sch log files doesn't rotate or purge properly it generates more in number and fills the disk space.
CSCvd34602	ISE 2.2 fails to send SMS via HTTP.
CSCvd36405	It takes approximately 2 hours to generate authentication report with MAC Address or network device.
CSCvd41050	In ISE 2.1, endpoint lookup is slow when DB is huge.
CSCvd48557	Enhancement request to set the sponsor username field with the guest API call.
CSCvd52520	Watchdog process is unable to restart redis server after getting crashed.
CSCvd85033	SMS notification fails when view/print option is disabled with guests in the sponsor portal.
CSCvd85575	“Purge M&T Operational Data” command via CLI doesn't work properly in ISE.
CSCvd95779	ISE 2.2 unable to remove network condition for TACACS.
CSCve00124	Endpoint application by Category Classification Dashlet doesn't show data.
CSCve84287	ISE WiFi Setup doesn't persist at disabled state.
CSCva49396	When you customize folder name with few set of language properties file and upload it to sponsor portal settings, it causes issues in sponsor portal UI.
CSCva98129	ISE adds one more unsuccessful failed attempts in Guest Portal setting.
CSCux86452	Adaptive Network Control (ANC) is disabled by default. It gets enabled only when pxGrid is enabled.
CSCuj78509	Providing support for LDAP External Identity Sources for Client Certificate Authentication.
CSCvc49434	Enhancement for TCP timeout on MS SQL Server ODBC connector.
CSCvc73368	Account gets suspended or locked with incorrect login attempts.
CSCvc80485	ISE 2.1 enhancement request to support Aruba Wireless 3200.
CSCvd84118	Enhancement request to add PeriodicProbing attribute to AC posture profile in ISE.

Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 1

Table 20 lists the issues that are resolved in Cisco Identity Services Engine, Release 2.2 cumulative patch 1. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.2, 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.

Patch 1 might not work with older versions of SPW. MAC users need to upgrade their SPW to MacOsXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.2*. for instructions on how to apply the patch to your system.

Table 20 Cisco ISE Patch Version 2.2.0.470-Patch 1 Resolved Caveats

Caveat	Description
CSCvb81755	Replication on all the ISE PSNs doesn't work if any of the PSNs in the deployment has latency issue.
CSCvc34224	ISE crashes and restarts automatically in JVM layer.
CSCvc51742	ISE 2.1 VPN MDM Polling is unable to update compliance status.
CSCvc61931	In ISE 2.1, PostgreSQL authentications fails, throws random errors.
CSCvc71503	Jedis throws error and gets disconnected automatically.
CSCvc74300	Due to huge amount of oracle logins, /var/log/secure file size is increasing rapidly.
CSCvc74307	Unable to remove logwatch temp files from /var/cache/logwatch.
CSCvc75209	ISE 2.1 and above shows High IO and High CPU usage for oracle process on MNT mode.
CSCvc86247	CPU runs with or without authentications when multiple threads go to infinite loop on PSN.
CSCvd01079	Endpoint Purge doesn't work with Base License on ISE 2.2.
CSCvd08518	Policy push does not work for changes made to policies using EPGs as the destination.
CSCvd24930	After upgrading from ISE 2.1 to 2.2, ISE throws excessive DNS requests.
CSCvd32949	You can delete a network device profile when the device is in use.
CSCvd49829	Evaluation of positron for struts2-jakarta rce vulnerability.
CSCvb16324	During VSS switchover, ISE stays connected to the old VSS.
CSCvc16661	ISE 2.2 displays NAD import input validation error.
CSCvc51725	ISE 2.0 and 2.1, update the compliant status as per the MDM server.
CSCvc71193	Inconsistent number of active endpoints displayed on dashboard after backup and restore from ISE 2.1.
CSCvc76704	ISE doesn't display all IPs added to ISE Admin IP Access Page.
CSCvc78816	Upgrade stopped on Secondary Monitoring node and Primary Administration node.
CSCvc84239	ISE displays Threat Events reports with expired Apex license.
CSCvc84399	Admin COA fails. Secure MnT logic before updating an active session.
CSCvc87023	Endpoint certificates functionality doesn't work.
CSCvc93699	Posture lease option doesn't work for VPN users with anyconnect 4.4 with MacOSX 10.x version.
CSCvd01530	PXGrid SDK: ISE PIC reports EPS enabled via queryCapabilityStatus, but fails subscription.

Table 20 Cisco ISE Patch Version 2.2.0.470-Patch 1 Resolved Caveats

Caveat	Description
CSCvd13462	Unable to remove Active Directory Groups if it is added to the External Admin Groups.
CSCvd18336	ISE 2.2 Plus license doesn't allow posture update.
CSCvd22650	After upgrading from ISE 2.1 to 2.2, the ENDPOINT logs registration displays wrong date.
CSCvd43138	ISE fails to reconnect to syslog server if TCP connectivity gets disconnected.
CSCvb20478	ISE increases maximum 'Valid period' for endpoint certificate.
CSCvc55106	Need to check additional attribute in addition to username during authentication/authorization to verify whether it's a machine or a user.
CSCvd03373	Incorporated NormalizedUsername to identify if the authentication is Host Based or User Name based.

Cisco ISE, Release 2.2 Open Caveats

The following link lists the caveats that are open in Release 2.2.

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283801589&rls=2.2(0.914)&sb=afr&sts=open&bt=null

Resolved Caveats

Table 21 Cisco ISE Release 2.2 Resolved Caveats

Caveat	Description
CSCuz44971	Inconsistent endpoint inactivity timer causes purge issues in Cisco ISE 1.3.
CSCuw48837	Authentication stops on Policy Service nodes (PSNs) and no logs are reported on MnT.
CSCux51093	GET operation with ERS API fails with "CRUD operation exception" error when trying to fetch the list of guests.
CSCuy80749	Redis server crashed on PSN node with core files.
CSCuz17763	Moving clients from 802.1x enabled SSID to Guest SSID or vice versa fails intermittently.
CSCuz30471	Delay in wired guest Change of Authorization (CoA) while using ISE 2.0.
CSCuz46469	Restarting services in Cisco ISE 2.0 patch 2 and patch 3 breaks authorization based on network device profile.
CSCuz76370	ISE purges endpoints that do not meet the purge policy requirements.
CSCuz95165	Context Visibility not working after PAN promotion.
CSCva01828	ISE indexing engine fails to start when upgrading from ISE 2.0/2.0.1 to 2.1.
CSCva02380	“HTTP Status 400 - Bad Request” error is seen when an FQDN is used to login to ISE.

Table 21 Cisco ISE Release 2.2 Resolved Caveats (continued)

Caveat	Description
CSCva14899	Cisco ISE does not support MAC 10.12.
CSCva32914	After upgrading from ISE 1.2 to 1.4, when the device is not operational in the AD domain, ISE responds to Nagios Radius Probes and prevents “Process Failure” response.
CSCva66532	After upgrading from Cisco ISE 2.0 to 2.1, MDM vendor data in the MDM server does not match actual vendor data in the database.
CSCva80275	ISE nodes attempt to check updates from third party websites.
CSCva81452	AD ValidateAccount mechanism optimization to reduce RPC traffic and enhance overall performance.
CSCva84867	Custom attributes containing caret(^) character are not supported in ISE and TACACS+ shell profiles with caret(^) character fail security validation.
CSCva84936	ISE is unable to profile Cisco access points due to cdpCacheAttribute null value during SNMP query probe.
CSCva86642	Restart of ISE services required to failover to next available Active Directory domain controller.
CSCva86683	In ISE 2.1, EAP-Chaining fails to retrieve AD user attributes when the user name and machine name in AD are same.
CSCva91557	ISE fails to send Guest notification emails.
CSCvb10382	When there is large amount of data in the network, WMI events are not published to pxgrid client.
CSCvb14612	SNMP Query is not triggered due to lack of synchronization between Redis database and Oracle database.
CSCvb32929	Attempt to join new node to ISE 2.1 deployment fails, if FQDN contains numbers in the top-level domain (TLD).
CSCvb34404	High load is seen on ISE 1.3 PSN when posture discovery traffic is allowed.
CSCvb52063	Custom endpoint attributes are missing after upgrading from ISE 2.0 to 2.1.
CSCvc15000	The TACACS+ Deny All Shell Profile fails to reject an unauthorized device administrator.

Documentation Updates

Table 22 Updates to Release Notes for Cisco Identity Services Engine, Release 2.2

Date	Description
10/18/2017	Added Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 4.
12/07/2017	Added Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 5.
30/01/2018	Added Resolved Issues in Cisco ISE Version 2.2.0.470—Cumulative Patch 6

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 2.2

Cisco ISE 2.2 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.