Release Notes for Cisco Identity Services Engine, Release 1.3

Revised: June 26, 2017

Contents

These release notes describe the features, limitations and restrictions (caveats), and related information for Cisco Identity Services Engine (ISE), Release 1.3. 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, 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.

Deployment Terminology, Node Types, and Personas

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

Table 1 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 Inline Posture.
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 At least one node in your distributed setup should assume the Policy Service persona.

– 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.

- Inline Posture node is a gatekeeping node that is positioned behind network access devices such as wireless LAN controllers (WLCs) and VPN concentrators on the network. An Inline Posture node enforces access policies after a user has been authenticated and granted access, and handles change of authorization (CoA) requests that a WLC or VPN is unable to accommodate. Cisco ISE allows up to 10,000 Inline Posture Nodes in a deployment. You can pair two Inline Posture nodes together as a failover pair for high availability.

Note An Inline Posture node is dedicated solely to that service and cannot operate concurrently with other Cisco ISE services. Likewise, due to the specialized nature of its service, an Inline Posture node cannot assume any persona. Inline Posture nodes are not supported on VMware server systems.

Note Each Cisco ISE node in a deployment can assume more than one persona (Administration, Policy Service, Monitoring, or pxGrid) at a time. By contrast, each Inline Posture node operates only in a dedicated gatekeeping role.

Table 2 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)
Inline Posture	0	10000

You can change the persona of a node. See the "Set Up Cisco ISE in a Distributed Environment" chapter of the *Cisco Identity Services Engine Admin Guide, Release 1.3* for information on how to configure personas on Cisco ISE nodes.

System Requirements

Note For more details on Cisco ISE hardware platforms and installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.3*.

Supported Hardware

Cisco ISE software is packaged with your appliance or image for installation. Cisco ISE, Release 1.3 is shipped on the following platforms. After installation, you can configure Cisco ISE with specified component personas (Administration, Policy Service, Monitoring, and pxGrid) or as an Inline Posture node on the platforms that are listed in Table 3.

Table 3 Supported Hardware and Personas

Hardware Platform	Persona	Configuration
Cisco SNS-3415-K9 (small)	Any	Refer to the *Cisco Identity Services Engine (ISE) Data Sheet* for the appliance hardware specifications (Table 3).
Cisco SNS-3495-K9[1] (large)	Administration Policy Service Monitor pxGrid	
Cisco ISE-VM-K9 (VMware)	Stand-alone Administration, Monitoring, Policy Service, and pxGrid Service (no Inline Posture)	• For CPU and memory recommendations, refer to the "VMware Appliance Sizing Recommendations" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.3*.[2] • For hard disk size recommendations, refer to the "Disk Space Requirements" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.3*. • NIC—1 GB NIC interface required (You can install up to 4 NICs.) • Supported VMware versions include: – ESX 4.*x* – ESXi 4.*x*, 5.*x* and 6.0

1. Inline posture is a 32-bit system and is not capable of symmetric multiprocessing (SMP). Therefore, it is not available on the SNS-3495 platform.
2. Memory allocation of less than 4GB is not supported for any VMware appliance configuration. In the event of a Cisco ISE behavior issue, all users will be required to change allocated memory to at least 4GB prior to opening a case with the Cisco Technical Assistance Center.

This Cisco ISE software is also supported on Cisco ISE 3300 series, Cisco NAC 3300 series, and Cisco Secure ACS 1121 appliances. You can upgrade an existing Cisco ISE 3300 series appliance to the latest release.

If you are moving from Cisco Secure Access Control System (ACS) or Cisco NAC Appliance to Cisco ISE, Cisco NAC 3315 appliances support small deployments, Cisco NAC 3355 appliances support medium deployments, and Cisco NAC 3395 appliances support large deployments. Cisco ISE is also supported on Cisco Secure ACS 34xx and Cisco NAC 34xx series appliances.

Supported Virtual Environments

Cisco ISE supports the following VMware servers and clients:

- VMware version 7 (default) for ESX/ESXi 4.x
- VMware version 8 (default) for ESXi 5.x
- VMware version 11 (default) for ESXi 6.0 (requires Cisco ISE 1.3 Patch 4)

Supported Browsers

The Cisco ISE, Release 1.3 administrative user interface supports a web interface using the following HTTPS-enabled browsers:

- Mozilla Firefox version 31.*x* ESR, 32.*x*, 33.*x, 34.x, and 35.x*
- Microsoft Internet Explorer 10.*x* and 11.*x*

If you are using Internet Explorer 10.x, enable TLS 1.0 and disable SSL 3.0, TLS 1.1 and TLS 1.2 (Internet Options > Advanced).

Adobe Flash Player 11.2.0.0 or above must be installed on the system running the client browser. The minimum required screen resolution to view the Administration portal and for a better user experience is 1280 *x* 800 pixels.

Supported Devices and Agents

Refer to *Cisco Identity Services Engine Network Component Compatibility, Release 1.3* for information on supported devices, browsers, and agents.

Cisco NAC Agent Interoperability

The Cisco NAC Agent versions 4.9.4.3 and later can be used on both Cisco NAC Appliance Releases 4.9(1), 4.9(3),4.9(4) and Cisco ISE Releases 1.1.3-patch 11, 1.1.4-patch 11, 1.2.0, 1.2.1, and 1.3. This is the recommended model of deploying the NAC agent in an environment where users will be roaming between ISE and NAC deployments.

Support for Microsoft Active Directory

Cisco ISE, Release 1.3 works with Microsoft Active Directory servers 2003, 2008, 2008 R2, 2012, and 2012 R2 at all functional levels.

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

In addition, Cisco ISE 1.3 supports Multi-Forest/Multi-Domain integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 1.3 supports up to 50 domain join points.

Supported Antivirus and Antispyware Products

See the following link for specific antivirus and antispyware support details for Cisco NAC Agent and Cisco NAC Web Agent:

http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html

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

The following table lists the Web Agent versions and the compatible Compliance Module versions.

Table 4 Web Agent and Compliance Module Versions

Cisco NAC Web Agent version	Compliance Module Version
4.9.5.3	3.6.9845.2
4.9.5.2	3.6.9186.2
4.9.4.3	3.6.8194.2
4.9.0.1007	3.5.5980.2
4.9.0.1005	3.5.5980.2

Installing Cisco ISE Software

To install Cisco ISE, Release 1.3 software on Cisco SNS-3415 and SNS-3495 hardware platforms, turn on the new appliance and configure the Cisco Integrated Management Controller (CIMC). You can then install Cisco ISE, Release 1.3 over a network using CIMC or a bootable USB.

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

Perform Cisco ISE initial configuration according to the instructions in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.3*. Before you run the setup program, ensure that you know the configuration parameters listed in Table 5.

Table 5 Cisco ISE Network Setup Configuration Parameters

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). The first character must be a letter.	isebeta1
(eth0) Ethernet interface address	Must be a valid IPv4 address for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14
Netmask	Must be a valid IPv4 netmask.	255.255.255.0
Default gateway	Must be a valid IPv4 address for the default gateway.	10.12.13.1
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).	mycompany.com
Primary name server	Must be a valid IPv4 address for the primary name server.	10.15.20.25
Add/Edit another name server	Must be a valid IPv4 address for an additional name server.	(Optional) Allows you to configure multiple name servers. To do so, enter **y** to continue.

Table 5 Cisco ISE Network Setup Configuration Parameters (continued)

Prompt	Description	Example
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	Must be a valid NTP domain.	(Optional) Allows you to configure multiple NTP servers. To do so, enter **y** to continue.
System Time Zone	Must be a valid time zone. For details, see *Cisco Identity Services Engine CLI Reference Guide, Release 1.3*, which provides a list of time zones that Cisco ISE supports. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT (or UTC-8 hours). The time zones referenced are the most frequently used time zones. You can run the **show timezones** command from the Cisco ISE CLI for a complete list of supported time zones. **Note** We recommend that you set all Cisco ISE nodes to the UTC time zone. This setting ensures that the reports, logs, and posture agent log files from the various nodes in the deployment are always synchronized with the time stamps.	UTC (default)
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (admin), you must create a new username. The username must be three to eight characters in length and composed of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password (there is no default). The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Note For additional information on configuring and managing Cisco ISE, see Release-Specific Documents, page 79 to access other documents in the Cisco ISE documentation suite.

Upgrading Cisco ISE Software

Cisco Identity Services Engine (ISE) supports upgrades from the CLI only. Supported upgrade paths include:

- Cisco ISE, Release 1.2 and 1.2.x with the latest patch applied

The following table lists the Cisco ISE versions and what you need to do to upgrade to Cisco ISE, Release 1.3, from those versions:

Table 6 Cisco ISE 1.3 Upgrade Roadmap

Cisco ISE Version	Upgrade Path
Cisco ISE, Release 1.0 or 1.0.x	1. Upgrade to Cisco ISE, Release 1.1.0. 2. Apply the latest patch for Cisco ISE, Release 1.1.0. 3. Upgrade to Cisco ISE, Release 1.2. 4. Upgrade to Cisco ISE, Release 1.3.
Cisco ISE, Release 1.1	1. Apply the latest patch for Cisco ISE, Release 1.1.0. 2. Upgrade to Cisco ISE, Release 1.2. 3. Upgrade to Cisco ISE, Release 1.3.
Cisco ISE, Release 1.1.x	1. Apply the latest patch for Cisco ISE, Release 1.1.x. 2. Upgrade to Cisco ISE, Release 1.2. 3. Upgrade to Cisco ISE, Release 1.3.
Cisco ISE, Release 1.2	Upgrade to Cisco ISE, Release 1.3.
Cisco ISE, Release 1.2.1	Upgrade to Cisco ISE, Release 1.3.

Follow the upgrade instructions in the *Cisco Identity Services Engine Upgrade Guide, Release 1.3* to upgrade to Cisco ISE, Release 1.3.

Note When you upgrade to Cisco ISE, Release 1.3, you may be required to open network ports that were not used in previous releases of Cisco ISE. For more information, see "Cisco SNS-3400 Series Appliance Ports Reference" in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.3*.

Upgrade Considerations and Requirements

Read the following sections before you upgrade to Cisco ISE, Release 1.3:

Inline Posture Node (IPN) Support in Cisco ISE 1.3

You may install Cisco ISE Version 1.2.1 of IPN on a supported hardware appliance and then register it to an ISE 1.3 deployment.

Firewall Ports That Must be Open for Communication

The replication ports have changed in Cisco ISE, Release 1.3 and if you have deployed a firewall between the primary Administration node and any other node, the following ports must be open before you upgrade to Release 1.3:

- TCP 1521—For communication between the primary administration node and monitoring nodes.
- TCP 443—For communication between the primary administration node and all other secondary nodes.
- TCP 12001—For global cluster replication.

For a full list of ports that Cisco ISE, Release 1.3 uses, refer to the *Cisco SNS-3400 Series Appliance Ports Reference*.

VMware Operating System to be Changed to RHEL 6 (64-bit)

Cisco ISE, Release 1.3 has a 64-bit architecture. If a Cisco ISE node is running on a virtual machine, ensure that the virtual machine's hardware is compatible with 64-bit systems:

Note You must power down the virtual machine before you make these changes and power it back on after the changes are done.

Ensure that you choose Linux as the Guest Operating System and Red Hat Enterprise Linux 6(64-bit) as the version. See http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005870 for more information.

Admin User Unable to Access the ISE Login Page Post Upgrade

If you had enabled certificate-based authentication for administrative access to Cisco ISE (Administration > Admin Access) before upgrade and used Active Directory as your identity source, after upgrade, you will not be able to launch the ISE Login page because Active Directory join is lost during upgrade.

Workaround

From the Cisco ISE CLI, start the ISE application in safe mode using the following command:

application start ise safe

This command brings up the Cisco ISE node in safe mode and you can use the internal admin user credentials to log in to the ISE GUI.

After you log in, you can join ISE with Active Directory.

Rejoin Cisco ISE with Active Directory

Ensure that you have the Active Directory credentials if you are using Active Directory as your external identity source. After an upgrade, you might lose Active Directory connections. If this happens, you must rejoin Cisco ISE with Active Directory. After rejoining, perform the external identity source call flows to ensure the connection.

Sponsor Login Fails

The upgrade process does not migrate all sponsor groups. Sponsor groups that are not used in the creation of guests roles are not migrated. As a result of this change, some sponsors (internal database or Active Directory users) may not be able to log in after upgrade to Release 1.3.

Check the sponsor group mapping for sponsors who are not able to log in to the sponsor portal, and map them to the appropriate sponsor group.

Update Authorization Policies for New Guest Types

After upgrading to Cisco ISE 1.3, the new guest types that are created do not match the upgraded authorization policies. You need to make sure that the authorization policies are updated with the new guest types.

Sequence Network Interface Cards (NICs) for UCS and IBM Appliances

The order in which Network Interface Cards (NICs) are connected to Cisco UCS SNS 3415 and Cisco UCS SNS 3495, and IBM Cisco ISE 3315 appliances may affect the upgrade to ISE 1.3. You should ensure that a pre-upgrade check is performed, followed by sequencing of the NICs. Perform a pre-upgrade check of NICs for UCS and IBM Appliances to ensure that Ports eth0 and eth1 should be used for Intel NICs on UCS appliances and, ports eth2 and eth3 should be used for Broadcom NICs on IBM appliances. Refer to the Sequence Network Interface Cards (NICs) for UCS and IBM Appliances section in the *Cisco Identity Services Engine Upgrade Guide, Release 1.3.*

Review Custom Portal Migration in a Lab Setting Before Using Them in Production Environment

Cisco ISE, Release 1.3 provides a new streamlined guest and employee on-boarding experience as well as a new portal customization experience with a host of new features from multi-language support to WYSIWYG customization. When you upgrade to Release 1.3, all custom portals are migrated to the new ISE 1.3 experience. Here are a few considerations that you must be aware of:

- The basic look and feel customizations that were done using CSS & HTML in previous releases of ISE are migrated by the upgrade process to 1.3 in to the new Guest and Personal Devices flows.
- Customizations that use custom JavaScript to alter the Guest flow might not migrate properly. You can recreate these flows from the ISE 1.3 Admin portal. You do not require any coding skills to perform these customizations in Release 1.3.
- You cannot edit any of the custom portals that are migrated to Release 1.3. If you want to make changes to the look and feel, you must create a new portal. You do not require any coding skills to create a new custom portal in Release 1.3.

- ISE 1.2 customers were capable of making a wide variety of portal customizations. Some of those customizations might not migrate to ISE 1.3 predictably. We recommend you review your newly migrated portals in a lab setting before using them in a production environment.

Other Known Upgrade Considerations and Issues

Refer to the *Cisco Identity Services Engine Upgrade Guide, Release 1.3* for other known upgrade considerations and issues:

Cisco Secure ACS to Cisco ISE Migration

Cisco ISE, Release 1.3 supports migration from Cisco Secure ACS, Release 5.5 and 5.6 only. You *must* upgrade the Cisco Secure ACS deployment to Release 5.5 or 5.6 before you attempt to perform the migration process to Cisco ISE, Release 1.3.

Cisco ISE does not provide full parity to all the features available in ACS 5.5/5.6, especially policies. After migration, you may notice some differences in the way existing data types and elements appear in the new Cisco ISE environment. It is recommended to use the migration tool for migrating specific objects like network devices, internal users, and identity store definitions from ACS. Once the migration is complete, you can manually define the policies for relevant features that are appropriate to Cisco ISE.

Complete instructions for moving a Cisco Secure ACS 5.5/5.6 database to Cisco ISE Release 1.3 are available in the *Cisco Identity Services Engine, Release 1.3 Migration Tool Guide*.

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.

Licenses apply to wireless and VPN only, or Wired only for LAN deployments. It is supplied in different packages as Base, Plus, Plus AC, Apex, Apex AC, Mobility, and Mobility Upgrade.

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.

For more detailed information on license types and obtaining licenses for Cisco ISE, see “Cisco ISE Licenses” in the *Cisco Identity Services Engine Administrator Guide, Release 1.3*.

Cisco ISE, Release 1.3, supports licenses with two UIDs. You can obtain a license based on the UIDs of both the primary and secondary Administration nodes. For more information on Cisco ISE, Release 1.3 licenses, see the *Cisco Identity Services Engine Licensing Note*.

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.

New Features in Cisco ISE, Release 1.3

Cisco ISE, Release 1.3 offers the following features and services. Refer to *Cisco Identity Services Engine Admin Guide, Release 1.3* for more information.

Guest Enhancements

End-User Web Portals

- Centralized work centers help consolidate all portal configuration and customization tasks in a single location in the Admin portal.
- Default templates are available for guest, sponsor, and device portals.
- Default themes are provided for all portals and can be easily customized using portal customization options. Advanced customization is possible using CSS and jQuery Mobile ThemeRoller.
- Direct links to related configuration outside of the portal work centers are provided where necessary. All portals can be accessed on mobile devices without any additional configuration.
- Support Information link is included to enable help desk troubleshooting.

- WYSIWIG portal pages enable the ability to:
  - display real-time changes in the flow
  - preview changes on portal and desktop devices
  - view HTML source code in content
- There is an option to test:
  - All portals (default and custom) using the Portal test URL
  - Guest notifications (email and SMS) before they are sent
- Selectable settings for ports, interface(s), certificates, endpoint identity groups, identity source sequences, languages, etc. are available per portal
- Size of custom logos that are uploaded is not restricted in size anymore; the images are scaled appropriately.
- Language File support includes:
  - Multiple locales per language
  - Ability to export and import language file (to add, delete, edit or translate language properties files)
  - HTML code in certain dictionary keys in the language properties files

Notifications

- Email, SMS, and print notifications can be sent to:
  - All guest types (daily weekly and contractors)
  - Self-registered and imported guests
- Account expiry notifications can be sent to guests via SMS and email.
- Sponsors can bulk print account information when dealing with large number of guest accounts.
- SMS support is available for SMTP and HTTP APIs with preconfigured list of major SMS gateway providers provided for use.
- Notifications and messages can be customized to include your brand, including free-form HTML and variable data substitution.

Guest Portals

- Smart defaults are available for guest portals and flows, guest types, and sponsor groups.
- Login passcode, such as access and registration codes, can be used in combination with usernames and passwords.
- AUP options allow:
  - Separate AUP pages to display for guests
  - AUP content to display as part of other portal pages or as a link on those pages
  - Up to 50k characters and use of HTML tags
  - Require the guest to scroll to end of the AUP page before accepting or declining it
- Guest REST API is provided for create, update, delete and suspend operations
- Up to 1 million guest accounts can be created, but the number created in a batch when importing or randomly creating guest accounts can be limited.
- Support for auto-device registration and purge

- Require sponsor approval for self-registering guests before they are granted access to the network.
- Specify a number to limit the number of times a guest can simultaneously login into the network. In 1.2, it was either 1 or unlimited.
- Specify the maximum number of times guests can fail to log in successfully and the amount of time after which guests can try to log in once again after their last failed attempt. In 1.2, if guests exceeded the maximum number of failed login attempts, their accounts were suspended and had to be reinstated by the sponsor.
- Specify where guests must be redirected after they successfully log in, either to the original URL or a landing page (a static URL).
- Assign locations for guest types that automatically maps time zones.
- Optional BYOD Bypass for employees who want to use guest access instead.

Sponsor Portals

- Sponsors can:
- Provide guests logging into their company network with its SSID information
- Use sponsor group tags to set up optional grouping for searching and reporting

Non-Guest Portals

- Per portal “Simplified URL” or Fully Qualified Domain Names (FQDNs) can be specified for Sponsor and My Devices portals.
- Multiple My Devices portals with different default endpoint identity groups can be set up, so that registered devices can be assigned to different endpoint identity groups.
- In the My Devices portals, users can enter the MAC address for Device IDs in the formats shown in the following examples:
  - 00-11-22-33-44-55
  - 0011.2233.4455
  - 00:11:22:33:44:55
  - 001122-334455
  - 001122334455
- Any Connect 4.0 that works with ISE 1.3 has a posture subsystem

Internal Certificate Authority

The ISE Internal Certificate Authority (CA) simplifies certificate provisioning and deployment for BYOD and MDM endpoints. The Internal CA capability eliminates the previous complexity required to integrate with an external PKI certificate authority infrastructure.

ISE can be deployed as a self-contained CA or can be integrated into an existing enterprise certificate authority environment if still required.

Cisco ISE provides an OCSP responder to check for the validity of the certificates.

You can navigate to **Administration > Certificates** to view the details.

Support for OVA Installation on Virtual Machines

Virtual machine installations are now simplified. This release supports OVA template installation. You can use the OVA template for easier and more rapid deployments of the virtual machine installation for Cisco ISE, Release 1.3.

Cisco pxGrid Services

Cisco pxGrid is used to enable the sharing of contextual-based information from Cisco ISE session directory to other policy network systems such as Cisco Adaptive Security Appliance (ASA). The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between ISE and third party vendors, and for non-ISE related information exchanges such as threat information. You can enable the pxGrid Services from the **Administration > Deployment** page.

Cisco pxGrid Identity Mapping

The pxGrid Identity Mapping option enables you to monitor users that are authenticated by a Domain Controller (DC) and not by Cisco ISE, when Cisco pxGrid services are used. In networks where Cisco ISE does not actively authenticate users for network access, it is possible to use Identity Mapping to collect user authentication information from the active directory (AD) Domain Controller. Identity Mapping collects session information from the domain controller similar to Context Directory Agent (CDA). For more information on CDA, refer to *Installation and Configuration Guide for Context Directory Agent*.

You can configure Identity Mapping by navigating to **Administration > pxGrid Identity Mapping > AD Domain Controllers**.

AnyConnect Unified Agent

Posture Assessment can be performed using the AnyConnect ISE Agent or using the NAC Agent. You can install AnyConnect ISE Agent or NAC Agent by using the client provisioning policy (CPP) configuration in Cisco ISE.

You can add the AnyConnect Agent from **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Multi-Forest Active Directory

Cisco ISE 1.3 supports Multi-Forest/Multi-Domain integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 1.3 supports up to 50 domain join points. You can perform more operations with Active Directory in Cisco ISE 1.3. Refer to *Active Directory Integration with Cisco ISE* for more information.

Authorization Enhancements

In Cisco ISE 1.3, you can chain 802.1x with Centralized Web Authentication (CWA) and validate the device using standard 802.1x. After the device is authenticated, the user is prompted to authenticate using the captive portal. You can authorize based on both attributes from 802.1x session and Windows AD/LDAP groups from the CWA session.

The certificate matching has been enhanced by the following additional attributes: Key Usage (KU), Extended Key Usage (EKU), and Microsoft-CA “Certificate Template”.

Serviceability Enhancements

Cisco ISE 1.3 has been improved for easy deployment and easy troubleshooting. Additional enhancements include tree view, Live Log / Live Session Filters, Endpoint Debugs, Export Policy in XML, Bypass Suppression for each Endpoint, Right-Click option to copy the bypass details, Filtered Support Bundle, and Centralized Certificate Management. See Also Other Enhancements, page 21.

Licensing Enhancements

Licenses apply to wireless and VPN only, or Wired only for LAN deployments. 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.

In Cisco ISE 1.3, licenses are supplied in different packages as described in the following table:

Table 7 Cisco ISE License Packages

License Package	Cisco ISE Functionality included
Base	• AAA, IEEE-802.1X • Guest management • Link encryption (MACSec) • TrustSec • ISE Application Programming Interfaces
Plus	• Bring Your Own Device (BYOD) with built-in Certificate Authority Services • Profiling and Feed Services • Endpoint Protection Service (EPS) • Cisco pxGrid
Apex	• Third Party Mobile Device Management (MDM) • Posture Compliance

Table 7 Cisco ISE License Packages

License Package	Cisco ISE Functionality included
Mobility	• Combination of Base, Plus, and Apex for wireless and VPN endpoints
Mobility Upgrade	• Provides wired support to Mobility license

You can track the usage of licenses by navigating to the **Administration > System > Licensing** page.

Log File Enhancements

Cisco ISE Release 1.3 offers the following log file enhancements:

- Readable Log File Names: The log files have been renamed for easy identification.
- From and To Dates: Instead of allowing you to download the previous "n" number of files, this release allows you to specify the duration, the from and to dates, while downloading the log files. If you do not choose any date, all the available log files for the specified category or categories are downloaded.
- Log File Rotation: The log files are rotated once every day. The log files are also rotated within 24 hours if they reach their maximum size.
- Debug Log File Retention: A maximum of 15 days of debug log files are stored in the system and the older logs are purged.

Right Click Options in Live Authentications and Live Sessions

In ISE 1.3, when you go to the **Operations > Authentications** or the **Operations > Authentications > Show Live Sessions** pages and right click the Identity or the Endpoint ID, you can view the following options:

- Endpoint Debug —This option opens the Endpoint Debug page in **Operations > Troubleshoot > Diagnostic Tools > General Tools**, along with the selected value.
- Modify Collection Filters—This option opens the Collection Filters page in **Administration > Logging**, along with the selected value. This enables you to change the values before creating the filter.
- Bypass Suppression Filtering for 1 hour—This option enables you to create Bypass Suppression Collection filter for the selected value for one hour, without moving away from the page. You will receive a notification after successful creation of the filter.

Enhanced Reports and Alarms

Cisco ISE, Release 1.3 reports are enhanced to have a new look and feel that is more simple and easy to use. The reports are grouped into logical categories for information related to authentication, session traffic, device administration, configuration and administration, and troubleshooting.

Table 8 Changes to Reports in Cisco ISE, Release 1.3

Report Name	Change
Guest Activity	Master Guest report (includes external Active Directory guests)
Guest Sponsor Mapping	Moved to Sponsor Login and Audit report
Guest Sponsor Summary	Moved to Sponsor Login and Audit report
Change Configuration Audit report: Audit data related to Sponsor and My Devices portals	Moved to Sponsor Login and Audit report and My Devices Login and Audit report
Operations Audit report: Login data related to Sponsor and My Devices portals	Moved to Sponsor Login and Audit report and My Devices Login and Audit report

The following is the list of reports added to Cisco ISE, Release 1.3:

- AD Connector Operations
- Identity Mapping
- pxGrid Administrator Audit
- Mobile Device Management Endpoint Activity
- Endpoints Purge Activities
- AUP Acceptance Status
- Sponsor Login and Audit
- My Devices Login and Audit
- Master Guest Report
- Guest Accounting

The following is the list of alarms added to Cisco ISE, Release 1.3:

- Certificate Revoked
- Replication Stopped
- Endpoints Purge Activities
- AD Connector has not been stopped properly
- Slow Replication Error
- Slow Replication Info
- Slow Replication Warning
- Active Directory forest is unavailable
- Authentication domain is unavailable
- Authentication Inactivity
- ID Map. Authentication Inactivity
- Configured nameserver is down
- AD: Machine TGT refresh failed
- AD: ISE account password update failed

- Joined domain is unavailable
- EAP Session Allocation Failed
- RADIUS Context Allocation Failed
- License About to Expire
- License Expired
- Endpoint certificates expired
- Endpoint certificates purged
- OCSP Transaction Threshold Reached
- Certificate Provisioning Initialization Error
- Certificate Replication Failed
- Certificate Replication Temporarily Failed

VLAN Change Support Dropped

Cisco ISE has never supported VLAN change for mobile devices. It only supports Java or ActiveX agent for VLAN change; however, this is applicable only for Windows OS, Mac OSX, and Linux devices. When a device completes guest flow without VLAN, a CoA Reauth is performed to refresh the session.

The Admin should create two separate guest policies for mobile devices and workstations.

- For mobile devices, an authorization policy rule that includes EndPoints:LogicalGroups EQUALS mobiledevices as one of the validation conditions should be created and assigned to the mobile device guest authorization policy.
- For workstations that support VLAN changes, an authorization policy rule that includes EndPoints:LogicalGroups NOT EQUALS mobiledevices should be created and assigned to the workstation guest authorization policy.

Upgrade Enhancements

Cisco ISE, Release 1.3 includes the following enhancements that include several preupgrade checks to ensure that you have a seamless upgrade experience.

- Virtual Machine Resource Checks: The upgrade software now checks if the virtual machine's hardware (such as hard disk size, CPU speed, etc.) meets the recommended specifications before it begins the upgrade. If the VM resources do not meet the recommended specification, the upgrade fails without making any changes to the existing ISE installation. The console will display a message stating the minimum resource requirements and that the upgrade can be retried after the virtual machine's hardware has been updated to meet those requirements.
- Upgrade Bundle SHA-256 Checksum Verification: The upgrade software verifies the SHA-256 checksum of the upgrade bundle before starting the upgrade process. This check ensures that upgrade does not fail because of corrupt upgrade software leaving the system in a corrupt state. If the upgrade bundle is corrupted, the console displays a message asking the administrator to re-download the upgrade bundle and try the upgrade again.

- Monitoring Database Object Check: In earlier releases, Cisco ISE upgrade has failed because of missing Monitoring database objects. In this release, the upgrade software checks for the Monitoring database objects to ensure that they are present before the upgrade begins. In the rare cases where the database objects are still missing, the administrator must restore from a backup taken before the upgrade.
- Enhanced Show Tech Support Command Output: The show tech-support command is enhanced and now includes the database health report, alert log errors, processes that consume resources, database memory usage, and so on. This output is readable and is also available in the Support Bundle. You can run the show tech-support command on demand to look for the health of the database. The output can help the administrator with troubleshooting, if needed.
- Database Enhancements: This release includes several database enhancements that improve Cisco ISE performance. Index entries and corrupt data blocks are identified before the upgrade begins. This release also includes several database enhancements that improve Cisco ISE performance. A database sanity check is done before upgrade to ensure that missing database objects do not result in an upgrade failure.

Other Enhancements

This release includes several enhancements to help deploy and troubleshoot ISE easily. These include:

- Live Log/Live Session Filters: Ability to filter the data in the Live Logs/Live Sessions page based on any of the attributes.
- Endpoint Debug Logs: Download debug logs for a particular endpoint from a single node or all the nodes in your deployment in a single file. This log file includes logs for all services that were enabled.
- Export Policy Configuration in XML: Ability to download authentication and authorization policy configuration and policy conditions in the form of an XML file to troubleshoot configuration-related issues offline. You can export the policy configuration and send it to TAC for troubleshooting.
- Bypass Suppression for Endpoint: Cisco ISE allows you to set filters to suppress some syslog messages from being sent to the Monitoring node and other external servers using the Collection Filters. At times, you need access to these suppressed log messages. Cisco ISE now provides you an option to bypass the event suppression based on a particular attribute such as username for a configurable amount of time.
- Filtered Support Bundle: You can choose to download a support bundle that includes logs for a particular period of time. You can choose the from and to dates to filter logs in the support bundle. This would help narrow down your search while troubleshooting issues.
- Centralized Certificate Management: This release simplifies certificate management and helps you to manage certificates for all the nodes in your deployment from the Admin portal. You can choose to generate CSRs for multiple nodes in a single request, export the CSRs, and bind the CA-signed certificate with the CSRs from the Admin portal.
- In Cisco ISE 1.3, Endpoint Protection Service (EPS) is also known as Adaptive Network Control (ANC).
- ISE 1.3 REST API Get All Operation for Endpoints: The “List” operation to retrieve all endpoints in the ISE 1.2 and 1.2.1 REST API is now “Get All.” The output now includes the resource’s name in addition to its ID.

Support for Mac OS X 10.10

Cisco ISE 1.3 supports Mac OS X 10.10 clients.

Note the following when you are using Mac OS X 10.10:

- You need to install Mac OS X Agent 4.9.5.3 on Mac OS X 10.10 client and uninstall the older version of Agents, if any, available in the system.

  You can download the Agent installation file from the following URL: http://software.cisco.com/download/navigator.html

  Navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software > Identity Services Engine System Software-1.3** to download the Agent Installation file.

- While launching the Agent, if the Signing signature check fails, then you need to explicitly select the **Anywhere** option from **System Preferences > Privacy** in the Mac OS X system.
- For Safari browsers 6.1 and later, enable the following:
  - In Safari, go to **Preferences > Security > Manage Website Settings > Java >** << *your server URL*>> **> Run in unsafe mode**.

FIPS Support

Cisco ISE Release 1.3 does not support FIPS mode.

Known Issues in Cisco ISE, Release 1.3

Device Registration Portal

When a guest user registers a device using its MAC address, the device does not appear in the Device Registration Portal under the list of Registered Devices. This issue is seen in secondary Policy Service nodes in a distributed deployment and occurs because of replication latency issues.

As a workaround click the **Refresh** button to view the newly registered device.

LDAP Imported Guest Accounts Not Upgraded from Version 1.2

Guests that were imported by an LDAP authenticated sponsor in version 1.2 will not be migrated during an upgrade to 1.3, 1.4, 2.0, or 2.1.

LDAP Sponsor Created Guest Users Not Visible when Upgraded from 1.2

When upgrading from 1.2 to 1.3, 1.4, 2.0, or 2.1, guests who were created by a sponsor who was authenticated through LDAP can only be seen by the direct sponsor. These guests cannot be seen by other sponsors from the same sponsor group.

Cisco ISE Hostname Character Length Limitation with Active Directory

It is important that Cisco ISE hostnames be limited to 15 characters or less, if you use Microsoft Active Directory on the network. Active Directory does not validate hostnames larger than 15 characters. This can cause a problem if you have multiple Cisco ISE hosts in your deployment that have hostnames longer than 15 characters. If the first 15 characters are identical, Active Directory will not be able to distinguish them.

Issues with Message Size in Monitoring and Troubleshooting

Cisco ISE monitoring and troubleshooting functions are designed to optimize data collection performance messages of 8k in size. As a result, you may notice a slightly different message performance rate when compiling 2 k message sizes regularly.

Issues with Accessing Monitoring and Troubleshooting

Although more than three concurrent users can log into Cisco ISE and view monitoring and troubleshooting statistics and reports, more than three concurrent users accessing Cisco ISE can result in unexpected behavior like (but not limited to) monitoring and troubleshooting reports and other pages taking excessive amounts of time to launch, and the application sever restarting on its own.

Inline Posture Restrictions

- Inline Posture is not supported in a virtual environment, such as VMware.
- The Simple Network Management Protocol (SNMP) Agent is not supported by Inline Posture.
- The Cisco Discovery Protocol (formerly known as CDP) is not supported by Inline Posture.

Custom Language Templates

If you create a custom-language template with a name that conflicts with a default template name, the template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with the default names are renamed as follows: user_{LANG_TEMP_NAME}.

Issues with Monitoring and Troubleshooting Restores

During a Monitoring and Troubleshooting restore, the Cisco ISE application on the Monitoring node restarts and the GUI is unavailable until the restore completes.

Issue with Network Device Session Status Report

Network Device Session Status report hangs during report generation. If the Network device is not configured with SNMP and SNMP community string is not provided, then the report generation hangs and never completes.

Workaround for this issue is to enter the SNMP credentials while launching the Network Device Session Status report. If there is a large number of network devices configured in ISE, then it is recommended to provide snmpCommunity value along with the networkDeviceIP.

Issue with Converged Access Switches

The current available IOS releases for converged access switches, such as 3850 or 3650, may not send Calling-Station-ID in the RADIUS accounting requests, which may result in incorrect session states and endpoint profiles in ISE. Enter the following commands in the switch to ensure that the ISE data is updated appropriately.

```
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail
```

See Also CSCuo46999.

Issue while Creating Guest Accounts

ISE 1.3 will fail to create a guest account when you:

- Configured your guest portal in ISE 1.2 to allow self-service
- Hardcoded the time zone value during portal customization
- Migrated the customized portal to ISE 1.3 through the ISE 1.3 upgrade process

This occurs because the hardcoded time zone value in your customized portal might not match the Guest Location names in ISE 1.3. “Time zones” in ISE 1.2 are renamed to “Guest Locations” in ISE 1.3. As a workaround, after you upgrade to Release 1.3, add the same time zone that you hardcoded in 1.2, as a Guest Location in 1.3. To do this, from the ISE 1.3 Admin portal, choose **Guest Access > Settings > Guest Locations** and SSIDs, add the time zone in the Location name text box, choose the corresponding time zone, click Add, and save the settings.

Issue while Scheduling a Backup

When you perform a backup and restore operation, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is important to note that the backup and restore operations do not include the certificates used by the internal Cisco ISE Certificate Authority (CA).

When you perform a backup and restore from one system to another, to avoid errors, you must do one of following:

Option 1:

Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.

- **Pros:** Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.
- **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued. After the restore process, generate new certificates for the internal ISE CA (root and subordinate CA certificates).

Option 2:

After the restore process, generate all new certificates for the internal CA.

- **Pros:** This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.
- **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Data Restore from Older Versions is not Supported

Cisco ISE Release 1.3 supports backup and restore from 1.2.x versions only. If you try to restore a backup from an earlier version, a success message appears, but the data is not restored properly and the monitoring functions are impacted.

See Also CSCun35098, page 60.

BYOD and Captive Portal Support

Cisco ISE does not support BYOD on-boarding on the Captive Portal and displays the following error message: “Your browser is unsupported” for MAC OSX and Apple IOS devices. You should enable the Captive Portal Bypass option on the WLC to facilitate BYOD on-boarding.

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 7, 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 Navigate to **Products > Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

Choose from the following Cisco ISE installers and software packages 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 may need to configure the proxy settings in **Administration > System > Settings > Proxy** before you are able to access the Live Update locations. If proxy settings are enabled to allow access to the profiler and posture/client provisioning feeds, then 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 Admin Guide, Release 1.3*.

Client Provisioning and Posture Live Update portals:

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

  The following software elements are available at this URL:

  – Supplicant Provisioning Wizards for Windows and Mac OS X Native Supplicants

  – Windows versions of the latest Cisco ISE persistent and temporal agents

  – Mac OS X versions of the latest Cisco ISE persistent agents

  – ActiveX and Java Applet installer helpers

  – AV/AS compliance module files

  For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Client Provisioning Resources Automatically" section of the "Configure Client Provisioning" chapter in the *Cisco Identity Services Engine Admin Guide, Release 1.3*.

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

  The following software elements are available at this URL:

  – Cisco predefined checks and rules

  – Windows and Mac OS X AV/AS support charts

  – Cisco ISE operating system support

  For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically" section of the "Configure Client Posture Policies" chapter in the *Cisco Identity Services Engine Admin Guide, Release 1.3*.

If you do not enable the automatic download capabilities described above, you can choose to download updates offline. See Cisco ISE Offline Updates, page 27.

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 not available for Profiler Feed Service.

To upload offline client provisioning resources, complete the following steps:

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 Navigate to **Products > Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

Choose from the following Off-Line Installation Packages 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 of the "Configure Client Provisioning" chapter in the *Cisco Identity Services Engine Admin Guide, Release 1.3*.

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

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

To upload offline posture updates, complete the following steps:

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 Access 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 From the Posture Updates page, choose the **Offline** option.

Step 6 From the File to update field, click **Browse** to locate the single archive file (posture-offline.zip) from the local folder on your system.

Note The File to update field is a required field. You can only select 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.

Once updated, the Posture Updates page displays the current Cisco updates version information under Update Information.

Using the Bug Search Tool

This section explains how to use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Search Bugs Using the Bug Search Tool

In Cisco ISE, 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 At the Log In screen, enter your registered Cisco.com username and password; 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 Select from list link. The Select Product page is displayed.

b. Choose Security > Access Control and Policy > Cisco Identity Services Engine.

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, and modified date.

Export to Spreadsheet

The Bug Search Tool provides the following option to export bugs to an Excel spreadsheet:

- Click **Export Results to Excel** link in the Search Results page under the Search Bugs tab 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.

If you are unable to export the spreadsheet, log in to the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1-800-553-2447).

Cisco ISE, Release 1.3.0.876 Patch Updates

The following sections provide information on patches that were made available after the initial availability of the ISE 1.3 release. Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions. Cisco ISE version 1.3.0.876 was the initial version of the Cisco ISE 1.3 release. After installation of the patch, the version information can be seen from the **Settings > About Identity Services Engine** page in the Cisco ISE GUI and from the CLI in the following format "1.3.0.876 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, "1.3(0.9NN)" where NN is also the patch number; however displayed as two digits. For example, version "1.3.0.876 patch 3" corresponds to the following version in the bug database "1.3(0.903)".

The following patch releases apply to Cisco ISE release 1.3.0:

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 8

Table 9 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 8. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 8 might not work with older versions of SPW and users need to upgrade their SPW to WinSPWizard 1.0.0.43 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 1.3*. for instructions on how to apply the patch to your system.

Important Notes Before you Install Cisco ISE 1.3 Patch 8

- Expect the CLI session termination while installing the patch 7 or patch 8 from CLI. This is due to a new software related to CLI session management being installed. You can re-login after the reboot.

While installing Cisco ISE 1.3.0.876 patch 8 on previously installed Cisco ISE 1.3.0.876 patch 7 where pxGrid services are operational, following completion of patch 8 installation, you must stop and then start the ISE services for pxGrid services to resume operation.

Table 9 Cisco ISE Patch Version 1.3.0.876-Patch 8 Resolved Caveats

Caveat	Description
CSCvb48654	Evaluation of ISE for Openssl September 2016.
CSCuz52493	Evaluation of ISE for OpenSSL May 2016.
CSCva46497	ISE XSS vulnerability in admin dashboard page.
CSCva46542	ISE SQL injection vulnerability.

Open Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 8

The following table lists the caveats that are open in Release 1.3 Patch 8.

Table 10 Cisco ISE Patch Version 1.3.0.876-Patch 8 Open Caveats

Caveat	Description
CSCve89369	You can create advanced filter and save it for the current sessions. The filter is lost once you log out and start a new session on the browser. **Workaround** Save cookies in the browser and modify the expiration date.

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 7

Table 11 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 7. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 7 might not work with older versions of SPW and users need to upgrade their SPW to WinSPWizard 1.0.0.43 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 1.3*. for instructions on how to apply the patch to your system.

Important Notes Before you Install Cisco ISE 1.3 Patch 7

- Expect the CLI session termination while installing the patch from CLI. This is due to a new software related to CLI session management being installed. You can re-login after the reboot.
- While installing Cisco ISE 1.3.0.876 patch 7 on previously installed Cisco ISE 1.3.0.876 patch 6 where pxGrid services are operational, following completion of patch 7 installation, you must stop and then start the ISE services for pxGrid services to resume operation.

Table 11 Cisco ISE Patch Version 1.3.0.876-Patch 7 Resolved Caveats

Caveat	Description
CSCuu45926	Vertical Privilege Escalation - Systemic.
CSCux97025	Ownership change/merge can fail if the endpoint source is Configuration Protocol.
CSCuy20317	"Profiler Queue limit reached" error in patch 5 and above of ISE 1.3 and 1.4. **Workaround:** Limit profiler transactions below 200 per second.
CSCuy34700	Update glibc packages to address CVE-2015-7547.
CSCuy89574	External Trust Authentication fails with "Server not found in Kerberos DB" error. **Workaround:** Directly join Domain B for successful authentication.
CSCuz00972	pxGrid Services loop or get stuck when upgrading from ISE 1.2 to 1.3 patch 6.
CSCur64918	Cisco ISE 1.2 replication stops when moving from monitoring to enforcement mode. **Workaround:** Reload the Primary admin node.
CSCut77541	APRIL 2015 NTPd Vulnerabilities.
CSCuw26491	Cisco ISE 1.3 patch 4 authentication is done based on accounting framed service type. **Workaround:** Configure dummy rules, which will catch MAB authentications that fall into dot1x rule.
CSCux21939	Cisco ISE endpoint purge does not delete endpoints. **Workaround:** Disable all the probes and wait till the endpoints owned by that node are taken over by other nodes in the deployment or re-join the node as new node in the deployment.
CSCux24687	Automatic AD to DC fail over does not happen on RPC failure. **Workaround:** Leave and rejoin the same domain or join another DC.
CSCux41407	Evaluation of positron for OpenSSL December 2015 vulnerabilities
CSCux73806	Operation console page loads, but does not open. **Workaround:** Reset the MnT database to solve this problem temporarily (one week).
CSCuy21562	Application server fails to start on installation of ISE 1.3 patch 6.
CSCuy53020	Bind SQL Injection was found in first Appscan reports for Guest related portal.
CSCuy69285	Cisco ISE 1.3 patch 6 has issues with sessions not being released.
CSCuy71639	Cisco ISE incorrectly reports switchport index change.

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 6

Table 12 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 6. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 1.3*. for instructions on how to apply the patch to your system.

Important Notes Before you Install Cisco ISE 1.3 Patch 6

The supported path for installing Cisco ISE 1.3 patch 6 is:

Earlier Patches --> Patch 5 --> Patch 6

Application Services Stop After You Install ISE 1.3 Patch 6 on ISE 1.3 Patch 4

If you install ISE 1.3 patch 6 directly on ISE 1.3 patch 4, the application services do not start. Perform the following steps in the order specified below to recover from this issue:

1. Roll back patch 6.
2. Install patch 5. The application services enter in to a looped state.
3. Roll back patch 5.
4. Install patch 5.
5. Install patch 6.

Table 12 Cisco ISE Patch Version 1.3.0.876-Patch 6 Resolved Caveats

Caveat	Description
CSCur44745	Suppression adds CoA events to authentication details in Live Log session entry. Auth details for Live Log session entries show dynamic authorization (CoA) event rather than actual client Authentication details. **Workaround** 1. Choose **Administration > System > Settings > Protocols > RADIUS**. 2. Uncheck the Suppress Repeated Successful Authentications check box.
CSCus79596	Network Access: IdentityAccessRestricted not authorized correctly.
CSCut55685	Guest with Posture flow failed to download web agent.
CSCuu18124	LDAP sponsored accounts are missing after upgrade to 1.3. **Workaround** Use the SponsorAllAccounts group instead of Group or Own.

Table 12 Cisco ISE Patch Version 1.3.0.876-Patch 6 Resolved Caveats

Caveat	Description
CSCuv54014	CRL/OCSP URL verification fails with nonpublic top level domain. During OCSP client profile configuration, the URL verification fails when a nonstandard top level domain is used. For example, "host.mydomail.local". **Workaround** Use the IP Address of the OCSP Server in the URL instead of the FQDN. If the IP Address that is relative to your ISE node is not known, follow these steps: 1. Log in to the Admin CLI. 2. Enter the **ping** command to check connectivity to the OCSP server. For example, ping ocsp.server.local, where ocsp.server.local is the FQDN of the OCSP server. 3. Record the IP Address listed in the output. For example, PING cisco.com (72.163.4.161) 56(84) bytes of data," in the output.
CSCuv89453	In ISE 1.3, repeated password change and login loop occurs in the Guest and Sponsor portal. When the “Allow guests to change password after login” option and the “Require guest to change password at first login” option are enabled in the Guest and Sponsor portal, the user is prompted to change the password during the first login, and then the user is redirected to the same guest and sponsor portal for changing the password. This process occurs indefinitely thus blocking network access to the user.
CSCuv99833	ISE 1.3 Feed posture scheduler service failed with JDBC exception. **Workaround** 1. Trigger the update manually. 2. Restart the services.
CSCuw09138	In ISE 1.3 patch 3 high memory utilization is observed on PSN. On PSN, memory gradually increases, fills up the remaining system RAM, then crashes, and restarts. Logs indicate that at the maximum, the lwsmd service takes about 13 GB of RAM. After some time, an alarm is generated for AD service that is being restarted, and memory usage drops, and then memory usage starts to increase again. **Workaround** Restart services.
CSCuw09627	In ISE 1.3 RSA Agent introduces delay in authentication flow causing authentication failure under moderate load. This issue occurs with ISE 1.3 and RSA/ACE Agent version 8.1.2. **Workaround** Use the Radius Token.

Table 12 Cisco ISE Patch Version 1.3.0.876-Patch 6 Resolved Caveats

Caveat	Description
CSCuw27263	In a single BYOD environment, if the user is using ACS as the external RADIUS server in ISE, the user is authenticated and redirected successfully in authorization policy. When the user opens the browser, an error message, “Unable to obtain the user information needed for network access. Try again” is displayed. **Workaround** Use an internal user or AD user account.
CSCuw29108	ISE 1.3 Guest Portal access fails with embedded Posture check and Web Agent flow. **Workaround** Uncheck the Require guest device compliance check box to avoid embedded posture check and to setup a separate policy for posture check, in the **Guest Portals**. or Access the network by using NAC Agent or AnyConnect ISE Posture module.
CSCuw31016	My Devices Portal not mapping the Portal User name properly from Guest Flow. When provisioning devices using the Guest Portal with an Active Directory short name account, the Portal User in the My Devices portal does not map with the Portal User name from the Guest Portal correctly. Hence, devices are seen unless the UPN is used.
CSCuw32233	ISE 1.3 patch 4 Show Live Sessions page is empty. **Workaround** Perform one of the following step: • Downgrade to patch 3; or • Remove IPN from deployment, if not used.
CSCuw51376	DHCP Attributes are not acknowledged after a change in PSN ownership. **Workaround** None. **Note**: Making any profiling policy change in ISE will revert the endpoint back to the correct profiling policy.
CSCuw74703	Concurrent Error. Unable to update endpoint during upgrade from 1.2.1 to 1.4. After upgrading from ISE version 1.2.1 to 1.4, the ip phones are profiled as "cisco device," which is not correct. **Workaround** Run the script [EP_Reset_Time.sh] on all the nodes where the Profiler service is enabled.
CSCuw78737	GuestEndpoint is stuck in the HotSpot AUP portal loop even after purge. When a GuestEndPoint is purged, some of the endpoint's portal session continues to be marked as registered and is not cleared from the database. **Workaround** Remove the endpoint from the ISE database and clear all sessions for the endpoint on the controllers.

Table 12 Cisco ISE Patch Version 1.3.0.876-Patch 6 Resolved Caveats

Caveat	Description
CSCuw95152	While providing account details to the known guests, if the Copy me check box is unchecked, it caches the email address of the previous sponsor.
CSCuw99899	ISE 1.3 patch 5 MNT session is not cleared even though accounting stop is received. **Workaround** Clear the session manually via MNT API;
CSCux07108	ISE 1.3 patch 4 application is initializing after feed service replication message. If the user turns on the profiler feed service in a distributed deployment, the application service on the nodes goes into initializing state. **Workaround** None. Run the **application reset-config** command to recover from this state.
CSCux38902	The ISE application restarts after the installation of patch 4. **Workaround** Downgrade to ISE 1.4 patch 3. Upgrade to ISE 1.4 patch 5 when available.
CSCux53910	The system memory increase in ISE 1.3 patch 5 leads to authentication latency. **Workaround** Restart the ISE application every 5 days.

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 5

Table 13 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 5. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 1.3*. for instructions on how to apply the patch to your system.

Note Cisco ISE, Release 1.3.0.876 Patch 5 supports MAC 10.11.

Table 13 Cisco ISE Patch Version 1.3.0.876-Patch 5 Resolved Caveats

Caveat	Description
CSCuu94127	ISE profiler mixes attributes from different sessions when IP based probes (HTTP, NMAP, etc.) are used without turning on RADIUS probe. After applying this patch, turn on the RADIUS probe, and configure your NADs to send RADIUS Accounting messages to the PSNs that have the profiler turned ON.
CSCuo16506	Internal users cannot change their password in the guest portal.
CSCur40082	Self Registration Portal unable to hide person being visited, username, password. **Workaround** 1. Choose **Administration > System > Admin Access > Settings > Portal Customization**. 2. Select Enable Portal Customization with HTML and JavaScript under Portal Customization. 3. Choose **Guest Access > Configure > Guest Portals**. 4. Choose the Self-Registered Guest Portal (default). 5. Select Portal Page Customization and then Self-Registration page. 6. Scroll down to the Optional Content to area. 7. Select the Toggle HTML Source button. 8. Use the following JavaScript to hide the field: <script> $('input[name="guestUser.fieldValues.ui_person_visited"]').parent().hide(); </script><br _moz_editor_bogus_node="TRUE" /> 9. Select the Toggle HTML Source button. 10. Save the changes and then use the portal test URL to view the change.
CSCur69835	The Cisco Identity Services Engine (ISE) Admin portal is vulnerable to a cross-site scripting (XSS) attack. Cisco has released patches that addresses this vulnerability. For additional information on XSS vulnerability and mitigation is available at the following link: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20060922-understanding-xss Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-8022 Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
CSCur80413	'Error Loading Page' after enabling Original or Custom URL option. **Workaround** Modify the portal to “Include a Post-Login Banner page:”

Table 13 Cisco ISE Patch Version 1.3.0.876-Patch 5 Resolved Caveats

Caveat	Description
CSCus19913	ISE AuthStatus Rest API is not working for multiple Mac Addresses. This issue is now resolved in ISE Release Notes 1.3 Patch 5.
CSCus54412	ISE 1.3 does not prompt the remote client if password fails password policy. **Workaround** Down grade ISE to Release 1.2.x.
CSCut05350	Configuration Changed alarm appears after login to the Router or Switch.
CSCut84269	ISE 1.3 Username with "@domain.com" cannot manage MyDevices Portal.
CSCut95631	New sponsor user does not get a summary of guest credentials via e-mail. **Workaround** Re-send the credentials.
CSCuu11893	Alarms for Slow Replication are displayed in ISE 1.3.
CSCuu12335	ISE 1.3 Patch 2: InactiveDays attribute is not reset for active endpoint.
CSCuu17525	Authorization rules do not match multiple internal groups. **Workaround** Do not use multiple internal groups for the same user.
CSCuu18254	Enhancement request for enabling bulk import using REST API.
CSCuu21562	Enhancement request to allow special characters in Network Device Group (NDG) value.
CSCuu39225	Sporadic authentication failures - Communication with domain controller failed.
CSCuu45021	Clicking on the authentication details of DACL entry in the live authentication page throws an HTTP 500 error.
CSCuu52655	Mac BYOD flow fails when MAC OSX is specified in the NSP profile for both PEAP and TLS. **Workaround** Specify operating system "ALL" in the NSP profile.
CSCuu55186	"Automatically register guest devices" value is hardcoded to 5 for employees.
CSCuu57051	ISE 1.3 guest portal employees inheriting login options from guest type does not work for "maximum devices that guest can register".
CSCuu72216	ISE 1.2.1 does not accept bulk OCSP responses.
CSCuu76087	Windows PC behind IP Phone being profiled as Cisco-IP-Phone-7970.
CSCuu83386	Evaluation of ISE for Open SSL June 2015.
CSCuu85800	Authentication Domain - Forest missing from many Domains.
CSCuu92630	ISE 1.2 SGT replication failure after policy modification. **Workaround** Perform a manual synchronization on the PSN nodes to properly replicate the policy.
CSCuu94127	ISE 1.3 profiling mixes attributes from different sessions. **Workaround** Delete the endpoint and reprofile.

Table 13 Cisco ISE Patch Version 1.3.0.876-Patch 5 Resolved Caveats

Caveat	Description
CSCuv01575	In Cisco ISE 1.2.1 patch 6 and later releases, profiler policies that have double quotes in the description field cannot be edited. **Workaround** Export the affected policies, delete all quotation marks. From the exported XML, delete the broken policies, and re-import the fixed policies. Note that this might send a Profiler CoA which can be disabled from **Systems** -> **Settings** menu.
CSCuv06708	ISE authentication delay when primary Monitoring node is down. **Workaround** Promote secondary Monitoring node as primary.
CSCuv21820	ISE 1.2 and 1.2.1 Admin portal and other portals hosted on them are not accessible after browser upgrade. **Workaround** • Use a different browser; the following (current as of July 2015) browsers are supported: – Firefox 38.05 – SeaMonkey 2.33.1 – Chrome 43.0.2357.132 m – Internet Explorer 11.0.9600.17843CO or • Update FF about:config per https://bugzilla.mozilla.org/show_bug.cgi?id=587407#c100 – Type "about:config" into the FireFox URL bar. – Accept any warnings that are displayed. – Search for the property "security.ssl3.dhe_rsa_aes_128_sha" and set it to false. – Search for the property "security.ssl3.dhe_rsa_aes_256_sha" and set it to false. This should allow the user to log in to the Admin portal.
CSCuv24342	In ISE 1.3 and 1.4 CoA Accept introduces a session timeout.
CSCuv24797	ISE 1.4 or 1.3 Patch 3 “allow sponsor to choose notification language” breaks guest. **Workaround** Enable “allow sponsor to choose notification language”.
CSCuv31567	ISE 1.3/1.4 -Apache Struts2 Command Execution Vulnerability OGNL console.
CSCuv44677	Active Directory sponsors cannot manage guest accounts created by another Active Directory sponsor from the same group.
CSCuv52944	SWD-xxx LSQ-xxx ISE fails to send stop accounting; impacts Lancope users.
CSCuv53534	Endpoint lookup from the Profiler database is slow.

Table 13 Cisco ISE Patch Version 1.3.0.876-Patch 5 Resolved Caveats

Caveat	Description
CSCuv61017	PSP-Commons-* jar is removed when removing patch 2 from ISE 1.3. **Workaround** Re-applying the patch that was removed adds the files that were removed.
CSCuv71811	ISE 1.3 authentication latency is increased every hour. **Workaround** Restart the ISE service every 5 days.
CSCuv85629	TrustSec Egress Policy views do not display all policies.
CSCuw31568	CP policy fails when posture policy is set to MAC 10.11.
CSCuw34253	Cisco Identity Services Engine Unauthorized Access Vulnerability
CSCuw35643	MAC 10.11 - Wifi is turned off after provisioning (Single SSID Flow) **Workaround** Enable the Wifi manually to connect to the network with the provisioned protocol.

New Features and Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 4

Cisco ISE, Release 1.3.0.876 cumulative patch 4 offers the following new features:

- Support for Windows 10 Operating System, page 40
- Support for VMware ESXi 6.0, page 40

Support for Windows 10 Operating System

Cisco ISE, Release 1.3.0.876 cumulative patch 4 supports client machines and personal devices with Windows 10 Operating System.

Support for VMware ESXi 6.0

Cisco ISE, Release 1.3.0.876 cumulative patch 4 supports VMware version 11 (default) for ESXi 6.0.

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 4

Table 14 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 4. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.3*. for instructions on how to apply the patch to your system.

Table 14 Cisco ISE Patch Version 1.3.0.876-Patch 4 Resolved Caveats

Caveat	Description
CSCuq98790	Backup failed for Network File System (NFS) repository. **Workaround** If customer's security policy permits, change the folder mode to 757 or 777 for NFS share.
CSCur28245	UI/UX issues with the Sponsor group and the Guest type pages. The Guest types and Location list items are not populated in the drop down list in Guest Access > Configure > Sponsor Group. The sponsor group member list items are not populated in the drop down in Guest Access > Configure > Guest types. **Workaround** Log out and log in to Cisco ISE.
CSCur36983	Restore process stuck at 80%, field missing in LD_LIB_PATH. **Workaround** Reload the PAP node using CLI and initiate manual sync from PAP UI deployment page.
CSCus16052	XSS found in ISE admin pages (Infra).
CSCus39093	If ARP-SCAN attempts to execute and fails, then the Network Mapper (NMAP) scan fails to complete.
CSCus50476	MNT is slow on ISE 1.3 (slow Domain Name System (DNS)).
CSCus84133	The other Guest type is not visible if the contractor is NOT associated with the Sponsor group. **Workaround** Add the Guest type contractor to the sponsor group or don't use FQDN on the sponsor portal.
CSCut04556	Cisco ISE is susceptible to Cross Frame Scripting attacks.
CSCut14856	NullPointerException when adding Secondary Node. **Workaround** If the patch for this bug is not applied, configure a different domain name. If the patch for this bug is applied, it will work fine.
CSCut29673	AnyConnectComplianceModule cannot be found when it is downloaded from Cisco. **Workaround** Upload an AnyConnect profile to ISE first and then the download of AnyConnectComplianceModule will work.
CSCut34178	The Max Session behavior is not consistent.
CSCut55844	Noncompliant-to-Compliant devices are getting local host blank page. **Workaround** Type the original URL manually.
CSCut57270	ISE 1.2.1 endpoint export has duplicates.
CSCut62309	VMWARE tools not running (current) after the ISE 1.3 Patch 2 is applied. **Workaround** ISE 1.3 Patch 1 only should fix the VMWARE tools issue until this bug is resolved.

Table 14 Cisco ISE Patch Version 1.3.0.876-Patch 4 Resolved Caveats

Caveat	Description
CSCut85316	ISE: NTP authentication-key does not take special characters and cannot be longer than 15 characters. **Workaround** To specify characters in the ntp authentication key, enclose the string within double quotes. For example: ise-node/admin(config)# ntp authentication-key 1 md5 plain "ooo<iigignggndhs" ise-node/admin(config)# ntp authentication-key 1 md5 plain "ooo<\>abc" NOTE: > is the redirection operator for ISE Command Line Interface (CLI), so it needs to be escaped by a \ character. The 15 character limit is the documented behavior of ISE and currently does not have a workaround.
CSCut93169	The timestamp is missing from some entries while exporting endpoints to CSV. **Workaround** Contact TAC.
CSCut98581	ISE: Can't import guests with AD/LDAP sponsor logged in with email address. **Workaround** Login with username name string rather than the full email address.
CSCuu02081	ISE 1.3: SNMP Get-Request not sent for Cisco IP Phone 8831. **Workaround** Statically set the IP phone to the Cisco-IP-Phone profile so that it can properly match the applicable profile.
CSCuu03096	ISE advanced portal customization Export Theme CSS truncated. **Workaround** Roll a custom theme using Themeroller at http://themeroller.jquerymobile.com/?ver=1.3.2 and import that.
CSCuu03368	ISE 1.3 LDAP users cannot manage MyDevices Portal.
CSCuu04061	ISE Policy Service Node (PSN) stopped responding to Radius Requests, because of Mobile Device Management (MDM) server down. **Workaround** Restart the ISE PSN services.
CSCuu04227	MAB/802.1x Session mixing still an issue. **Workaround** Changing authentication order on switches to 802.1x then MAB reduces the number of occurrences seen.
CSCuu07582	ISE 1.3 ignoring AD Locked Out Status. **Workaround** Use lockoutTime attribute. If the value of this attribute is 0 or non-defined, the account is not locked out. If the value is a positive number, the account is locked out.
CSCuu21947	The location field is missing occasionally in endpoint export.
CSCuu31972	VMware tools not running in Elastic Sky X (ESX), version 6.x. This issue is resolved in ISE Release Notes 1.3 Patch 4 and the VMware tools are supported in ESX, version 6.x.

Table 14 Cisco ISE Patch Version 1.3.0.876-Patch 4 Resolved Caveats

Caveat	Description
CSCuu43966	ISE 1.3 Patch 2 upgrade to ISE 1.4 breaks iptables rules - all RADIUS dropped. **Workaround** Remove /etc/modprobe.conf and /etc/modeprobe.d/blacklist.lsi.conf.backup and reboot. After reboot, confirm that the firewall looks okay by doing firewall -L.
CSCuu46466	ISE 1.3 cannot push logs to MNT if a client has many AD groups. **Workaround** Try to use less number of groups.
CSCuu47485	ISE UI changes related to the NTP authentication keys.
CSCuu97147	While logging into the sponsor portal, the email address is shown instead of username.
CSCuu99002	Client Provisioning (CP)/Posture fails when the OS is selected as Windows 10. **Workaround** Select OS:Windows All.
CSCuu99565	ISE show tech memory threshold is confusing and different than the GUI. **Workaround** Rely on the alarms in the GUI for memory utilization alarms.
CSCuv01107	ISE: Support for RSA in BYOD flow.

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 3

Table 15 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 3. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 3 might not work with older versions of SPW and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.3*. for instructions on how to apply the patch to your system.

Table 15 Cisco ISE Patch Version 1.3.0.876-Patch 3 Resolved Caveats

Caveat	Description
CSCuh75367	The Network Access Device (NAD) sends an incorrect 'call-check' message when the host lookup is disabled.
CSCui09203	The Identity Services Engine (ISE) fails when accounting message with long class string. **Workaround** Disable interim accounting to limit the impact.
CSCuj48111	Hyphen and minus sign can't be entered as first or last name.

Table 15 Cisco ISE Patch Version 1.3.0.876-Patch 3 Resolved Caveats

Caveat	Description
CSCuj68540	The Monitoring Node (MnT) schema upgrade script is logging INFO messages as ERROR and WARNING.
CSCum53319	Improved diagnostics for failed Certificate Revocation List (CRL) download attempts.
CSCuo78457	An SNMP probe that is configured to match a profile using the operator "CONTAINS" fails. **Workaround** Use a different operator such as "STARTS WITH".
CSCup05013	The Cisco switches are profiled as an unknown endpoint.
CSCup45530	Identity Services Engine (ISE) External RESTful Services (ERS): Unable to set modify Static Profile Assignment without profileId. **Workaround** First perform an HTTP GET request via ERS API to get the endpoint's profileId, and then pass that value in the HTTP PUT request.
CSCuq43889	The DNS probe is not triggered after Simple Network Management Protocol (SNMP) Query probe updates IP address. **Workaround** • Use RADIUS authorization and IP device tracking to collect information via RADIUS Accounting. It may require RADIUS interim accounting to be enabled if Framed IP address is not populated on initial RADIUS Account Start. • Use DHCP probe for clients that support DHCP. • Use SNMP Query (triggered via RADIUS/SNMP Traps) for devices that support CDP.
CSCuq50447	Incorrect Security Group Tag (SGT) is displayed in the active sessions report if multiple SGTs are assigned.
CSCur11083	The Monitoring Node (MnT) live logs display incorrect user information.
CSCur13627	Monitoring Node (MnT) live logs are incorrectly displayed when the time zone offset is set for last 60 minutes by the time stamp. **Workaround** Choose the Coordinated Universal Time (UTC) for the following time zones: • Pacific/Fiji, from 26-Oct-14 to 25-Jan-15 • Countries where DST will change in 2015
CSCur14902	ISE Domain Name Server (DNS) Resolution Failed for "hostname" from the ISE node "hostname". **Workaround** Contact Cisco Technical Assistance Center (TAC) to manually modify the alarm script.
CSCur20079	An error message is displayed when certain attributes are retrieved from the Active Directory (AD).

Table 15 Cisco ISE Patch Version 1.3.0.876-Patch 3 Resolved Caveats

Caveat	Description
CSCur23949	Unable to edit an authentication policy set rule containing many IF conditions, in Firefox and Internet Explorer. An error message is displayed when using the “>” symbol and “HTTP Status 500" respectively. **Workaround** Reduce the number of conditions in the rule, for example, create an identity group and reference the group in the rule. Then, delete the entire policy set and create it again with less conditions.
CSCur69873	Auto complete feature is turned on in Infra and NSF pages.
CSCur75319	Unable to determine the status of the suppression attribute using the show tech-support command.
CSCur88138	The deployment list page shows status for all secondary nodes as 'Replication Stopped'. **Workaround** Reboot the Admin node.
CSCur89449	Some of the fields in the Self-Registration Page Settings section are not saved.
CSCur90991	Exporting a report fails for ISE admin logged-in with an Active Directory (AD) domain prefix.
CSCus16050	Components of the administration page of the Cisco Identity Services Engine (ISE) is vulnerable to a cross-site scripting (XSS) attack.
CSCus26474	The account duration in the Sponsor portal is incorrect as compared to the set default duration.
CSCus28936	When a user is created via the Sponsor portal, SMS and emails are not sent out. In addition, the print notification option does not work. **Workaround** In the Sponsor Portal > Portal Page Customization > Create Account For (Type of Guest) > Settings page, enable the Allow sponsor to choose notification language option.
CSCus34645	Unable to access the ISE management interface using IE 11 after upgrading to ISE 1.3. **Workaround** Manually set the User Agent to IE 10.0.
CSCus40202	Guest users using Apple devices running iOS 8.1.1 are not redirected to the success page after accepting the Acceptable Use Policy (AUP).
CSCus54517	RADIUS requests dropped by Cisco Integrated Services Engine (ISE).
CSCus55690	In the Guest Access > Settings > Guest Account Purge Policy page, the Purge Now button is disabled. **Workaround** Request Cisco Technical Assistance Center (TAC) to provide temporary Advanced license or Plus license.
CSCus68437	The MDM registered endpoints are not authenticated by Cisco ISE. **Workaround** When checking device compliance, use MDM.DeviceCompliantStatus instead of MDM.DeviceRegisterStatus attribute in the authorization policy.

Table 15 Cisco ISE Patch Version 1.3.0.876-Patch 3 Resolved Caveats

Caveat	Description
CSCus73480	When configuring a Protected Extensible Authentication Protocol (PEAP) profile for android devices, the connection fails after the profile is provisioned. **Workaround** Set the Operating System field to ALL in the client provisioning profile page.
CSCus77737	The sponsors are unable to cc themselves on the email notification for a guest account. **Workaround** Change the Guest Email settings to "Send notifications from sponsor's email address (if sponsored)". This enables sponsors to input their Emails when sending notifications.
CSCus78802	The usage of variable substitution in the middle of a string removes the initial characters.
CSCus79068	End users are unable to delete their own registered devices if user names contain upper and lower case characters. **Workaround** An administrator can delete end devices by navigating to Administration > Identity Management > Identities > Endpoints page.
CSCus79235	An error is displayed for locations in Sponsor groups containing special characters. **Workaround** Do not use comma in the location.
CSCus89119	After an Extensible Authentication Protocol (EAP) chaining authentication, the NAC agent fails to pop-up.
CSCus91301	The revised Organizationally Unique Identifier (OUI) file is not pushed from the former Primary Administration Node (PAN) to the promoted PAN. **Workaround** Manually copy the revised OUI file from the former PAN to the promoted PAN. [OR] Use the feed server to update the OUI file in the promoted PAN.
CSCus91321	ISE responds to posture request but not to Periodic Reassessment (PRA) under certain conditions. **Workaround** Block the non-posture flow between ISE and the user.
CSCus91456	ISE services restart when RSA encounters a duplicate session.
CSCus95010	Some columns, like "Phone Number" or "Email", are not exported in the Master Guest Report.
CSCus95278	The feed service configuration deployment ID for fresh installations should be unique.

Table 15 Cisco ISE Patch Version 1.3.0.876-Patch 3 Resolved Caveats

Caveat	Description
CSCus97012	SMS gateways used to send email and SMS notifications to guests and sponsors failed with variables used in the POST method. **Workaround** Use the GET method to send SMS messages to guests and sponsors via an HTTP API.
CSCut04401	Access control and missing authentication vulnerability in ISE login page.
CSCut08252	An exception occurs while saving the settings on SMS Email Gateway. **Workaround** • Click the SMS HTTP API option and delete the entire value in the HTTPS Password field. • Click the SMS Email Gateway option and make necessary changes and click Save.
CSCut11531	Support is required for using RSA token server in conjunction with guest portals on ISE.
CSCut12312	Unable to join or leave the Active Directory (AD) domain due to the “Updating” status message displayed **Workaround** Remove Fully Qualified Domain Name (FQDN) values from all portals.
CSCut42520	The User Principle Name (UPN) authentication fails when a second Active Directory (AD) joint point is added.
CSCut46744	Unable to log into ISE with Microsoft Internet Explorer (IE10 and IE 11) browsers.
CSCut48555	The French language template in the Sponsor portal fails to render special French characters.
CSCut93612	Sponsor groups are disabled when default settings are edited.
CSCut99602	Extensible Authentication Protocol (EAP)- Transport Layer Security (TLS) provisioning fails with Android. **Workaround** In the Policy > Policy Elements > Results > Resources page, click Add and select ALL for Operating System for the Native Supplicant Profile.

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 2

Table 16 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 2. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 will not work with older versions of SPW and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.3*. for instructions on how to apply the patch to your system.

Table 16 Cisco ISE Patch Version 1.3.0.876-Patch 2 Resolved Caveats

Caveat	Description
CSCuj70022	EAP-FAST authenticated provisioning with Android fails.
CSCul94611	ISE Dashboard fails to display live consolidated and correlated statistical data. **Workaround** In the CLI, enter the following command to enable the dashboard to display statistical data: ms-ise-mgm01/admin# app config ise Selection ISE configuration option [1]Reset Active Directory settings to defaults [2]Display Active Directory settings [3]Configure Active Directory settings [4]Restart/Apply Active Directory settings [5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings [6]Enable/Disable ERS API [7]Reset M&T Session Database [8]Rebuild M&T Unusable Indexes [9]Purge M&T Operational Data [10]Reset M&T Database [11]Refresh M&T Database Statistics [12]Display Profiler Statistics [13]Exit Execute the following command options: [7]Reset M&T Session Database [10]Reset M&T Database [11]Refresh M&T Database Statistics
CSCuo66847	A saved scheduled report ceases to exist in the Scheduled Reports list when edited. **Workaround** Recreate the scheduled report before editing it. To delete the report that was not displayed in the Scheduled Reports list, you can login with a generic admin account and view all reports.
CSCuq02033	The Mobile Device Management (MDM) heartbeat thread does not restart for a new MDM instance.

Table 16 Cisco ISE Patch Version 1.3.0.876-Patch 2 Resolved Caveats

Caveat	Description
CSCuq22636	ISE does not mandate Link Layer Discovery Protocol (LLDP) attributes for triggered RADIUS or SNMP trap. **Workaround** Use the ISE SNMP polling interval.
CSCuq22852	Local Web Authentication (LWA) authorization fails when non-alphanumeric characters are contained in username/password. **Workaround** Ensure that the Guest user names and passwords do not contain special characters such as tilde (~) and Add (+).
CSCur09231	A sponsor is able to create an account even after the expiry of the specified Account Start Date and Maximum Duration of Account in the Sponsor group policy.
CSCur32485	A vulnerability in the futex subsystem of the Linux Kernel could allow a local attacker to gain elevated privileges.
CSCur42461	Unauthenticated and unauthorized users are able to access and download the packet capture file from the Admin UI.
CSCur42723	The accounting suppression feature in the RADIUS settings page fails in large deployments.
CSCur43427	ISE PSN rejects RADIUS request, deadlock found in the catalina.out file. **Workaround** Restart ISE services.
CSCur44879	A high replication storm was triggered due to changes in profiled Internet Protocol (IP) addresses.
CSCur52802	After creating new guest types or customizing the existing ones, the Manage Accounts link does not display the customized guest types in the drop-down for creating accounts. **Workaround** Create a regular sponsor user login and access the regular ISE sponsor portal.
CSCur66880	When using a GoDaddy Signed HTTP certificate for the MyDevices portal, the page does not display after a successful redirection. Resting page after redirection does not have HTTP certificate attached. **Workaround** Remove the problem certificate from th Trusted Store and restart the application.
CSCur70718	Monitoring node (MNT) memory usage is spiked more than 90% due to oracle processes.
CSCur72826	ISE 1.3 authorization rule without permissions is removed after save. **Workaround** Recreate the removed policy and define the permissions before saving the rule.
CSCur76447	ISE 1.3 Role-based Access Control (RBAC) fails with shadow user and Radius token
CSCur79059	The guest portal displays only the policy set name without the rule that is associated with it.

Table 16 Cisco ISE Patch Version 1.3.0.876-Patch 2 Resolved Caveats

Caveat	Description
CSCur79264	An admin sponsor user is unable to view newly added locations and guest types in the sponsor portal via the Guest Access > Manage Accounts link.
CSCur80998	Renaming a certificate template corrupts certificate data and Supplicant Provisioning Wizard (SPW)/Public Key Infrastructure (PKI) flow. **Workaround** Delete the old certificate template and create a new certificate template. Do not rename the certificate template.
CSCur95229	Expired certificate renewal flow fails when the Reject the request if OCSP returns UNKNOWN status check box is checked. **Workaround** Uncheck the Reject the request if OCSP returns UNKNOWN status check box.
CSCur95329-	Cisco IT: SNMP polling continues after NAD SNMP settings are disabled. **Workaround** Delete NAD and recreate with SNMP settings disabled.
CSCur99126	ISE fails to validate authorization policies configured with time and date conditions.
CSCus01323	In multiple node ISE deployments, upgraded to 1.3, the original primary Admin node (PAN) would now be the secondary admin node. Promoting it back to the PAN might cause PSNs to show offline/replication-stopped and not connected. **Workaround** Remove the static route and try to include specific routes which don't overlap subnets of both interfaces at the same time.
CSCus15390	Cisco Security Manager (CSM) 4.7 fails to connect with ISE and throws an error.
CSCus16049	Cross-site Scripting (XSS) vulnerability found in ISE admin pages.
CSCus17952	ISE 1.3 does not does not authenticate passwords containing the backslash (\) escape character used in Lightweight Directory Access Protocol (LDAP) identity source. **Workaround** Remove the special character from the Common Name (CN) field.
CSCus30937	ISE fails to authenticate nodes that contain a comma in the Common Name (CN) field in the Certificate Signing Request (CSR).
CSCus31611	Unable to edit Guest account without changing the time period.
CSCus35720	When editing a guest account in the Sponsor portal, unchecking the Allow Sponsor to tag accounts as belonging to a group field removes the value of the custom field. **Workaround** Check the check box for Allow Sponsor to tag accounts as belonging to a group field.
CSCus36111	Demo applications for network devices, endpoints, and internal users should include a disclaimer.
CSCus37373	ISE 1.3 Active Directory (AD) user lookup fails when firewall is installed in the root Domain Controller (DC).
CSCus38913	The Host/ plus Domain Name (DN) fails and displays the 24352 ERROR_NO_SUCH_USER message. **Workaround** Rewrite the rule in Active Directory (AD) to remove host/.

Table 16 Cisco ISE Patch Version 1.3.0.876-Patch 2 Resolved Caveats

Caveat	Description
CSCus39109	The REST API programming interface fails to get all devices. **Workaround** For devices added via the import utility, view and change a parameter in the device properties, and save. The REST API does not throw an error.
CSCus40334	Expired guest extension date starts from the date the account expired, not from the current date.
CSCus49148	Certificate management uses HTTP instead of HTTPS protocol. In a multi node deployment, when the port 8443 is blocked from a secondary node, it takes an unusually longer time to propagate in the ISE GUI. **Workaround** Allow TCP port 80 communication between PAN and PSN.
CSCus49717	AnyConnect 4.0 with the posture module fails the requirement check and displays an error message that the Antivirus (AV) definitions need to be updated, irrespective of the number of days. **Workaround** Update the AV definition to the current date and use the latest compliance module.
CSCus55618	Users remain in the pre-posture state after downloading the Network Access Control (NAC) agent using the Client Provisioning option. **Workaround** In wired networks, disconnect and connect the Network Interface Card (NIC). In wireless networks, disconnect and reconnect the SSID.
CSCus68798	ISE is vulnerable to CVE-2015-0235 Linux Ghost remote code execution.
CSCus87496	AD connector crashes during domain discovery with ISE 1.3.

Resolved Issues in Cisco ISE Version 1.3.0.876—Cumulative Patch 1

Table 17 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.3.0.876 cumulative patch 1. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.3, log into 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 will not work with older versions of SPW and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.3*. for instructions on how to apply the patch to your system.

Table 17 Cisco ISE Patch Version 1.3.0.876-Patch 1 Resolved Caveats

Caveat	Description
CSCur41638	Certificate Revocation List (CRL) over HTTPS is broken. **Workaround** Download CRL via HTTP or via secure Lightweight Directory Access Protocol (LDAP) if secure download is warranted.
CSCus22382	Users are unable to access the network due to policies requiring a previous Machine Access Restrictions (MAR) authentication. **Workaround** Disable Protected Extensible Authentication Protocol (PEAP) and check the Enable Fast Reconnect check box to allow a PEAP session to resume in Cisco ISE without checking user credentials when the session resume feature is enabled.
CSCur45838	External RESTful Services (ERS) demo app fails after SSLv3 POODLE vulnerability fix. **Workaround** Copy the ERSClient.java file to the source folder: ers-demo-app/src/main/java/com/cisco/ise/ers/demo, rebuild the demo app and run the program again.
CSCur11226	The sponsor and guest portals list page takes extra time to load when the number of the authorization policies configured on ISE is more. **Workaround** Reduce the number of authorization policies and delete authorization policies that are not active.
CSCur60297	ISE GUI authentication fails if one of the Lightweight Directory Access Protocol (LDAP) group contains double quotes. **Workaround** Remove the double quotes from the LDAP group or disallow an LDAP user from the group that contains double quotes.
CSCur70410	Network Access Control (NAC) integration with ISE 1.3 profiler fails due to Application Programming Interface (API) changes.

Table 17 Cisco ISE Patch Version 1.3.0.876-Patch 1 Resolved Caveats

Caveat	Description
CSCur79904	ISE Application Server remains in “initializing” state after moving the Admin role between System Certificates following an upgrade from 1.2 to 1.3. **Workaround** 1. Use the following SQL command to remove the Portal role from the System Certificate containing it. UPDATE sec_res_attribute_value SET sec_attribute_value='' WHERE sec_resid='6adaf170-4037-11e4-8062-005056ad49c8' AND sec_rattributeid IN (SELECT sec_rattributeguid FROM sec_restype_attribute WHERE sec_attribute_name='Protocols' AND sec_restypeid IN (SELECT sec_restypeguid FROM sec_restype_master WHERE sec_restype_name='LocalCertificateType')); COMMIT; 2. Replace the sec_resid value in the query above with the value of the customer's certificate. To see the sec_resid value for all System (local) certificates, use the following query: SELECT sec_resguid,sec_res_name FROM sec_res_master WHERE sec_resource_fqn='NAC Group:NAC:LocalCertificates'. Use the sec_resguid value derived from this query as the sec_resid value in the first query. 3. Run the query and restart the node.
CSCur41673	A vulnerability in the periodic backup functionality of ISE may allow an unauthenticated, remote attacker to capture the password used to encrypt the backup. **Workaround** Run manual on-demand backup at periodic intervals.
CSCur57111	VMware tools fail to run post upgrade to 1.3. **Workaround** Run the script below to run the VMware tools./opt/system/etc/vmware-tools-distrib/vmtools-install.sh During installation of VMware tools, VMware will sync to the esx timestamp. In order to sync it to ntp again run the following command: /sbin/service ntpd restart.
CSCur65990	RADIUS requests dropped due to failure reason “11007 Could not locate Network Device or AAA Client”, even though they are successfully loaded on ISE. **Workaround** Contact Cisco Technical Assistance Center (TAC).
CSCur75323	Change of Authorization (CoA) triggered via the REST API does not succeed.
CSCur86205	The Policy Export option does not display the authentication and authorization policies in the correct order.

Table 17 Cisco ISE Patch Version 1.3.0.876-Patch 1 Resolved Caveats

Caveat	Description
CSCup08017	Restore/Upgrade/Host-Name change operations may fail when CTRL+C command is executed accidentally, which renders the system to an unusable state.
CSCur94336	NAC Agent does not popup in case user authentication has been preceded by a machine authentication. **Workaround** Clear the authentication session on the switchport. [OR] Unplug and reconnect the Ethernet connections or disable and enable the wired connection interfaces in Windows. [OR] If available, upgrade to IOS 15.2(2)E or 3.6.1E.

Cisco ISE, Release 1.3, Open Caveats

Open Caveats

Table 18 Cisco ISE, Release 1.3, Open Caveats

Caveat	Description
CSCuw41265	While using external admin accounts, some of the attributes, such as Email address cannot be retrieved. This makes it impossible to generate reports and receive emails with “ISE Report Export Notification”. **Workaround** Ensure that you create an internal admin account with the same name and set the email address there.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCua97013	Apple iOS devices are prompted to accept "Not Verified" certificates Apple iOS devices (iPhone & iPad) are asked to accept the certificate, appearing to them as "Not Verified," when connecting to WLAN (802.1X). By design, Apple iOS devices are prompted to accept a proprietary certificate, but Apple OS X and Android devices work without being prompted to accept a certificate. This happens even when the certificate is signed by a known CA, as there is an intermediate certificate in the server certificate chain. **Workaround** Click **Accept** to acknowledge the certificate. While browsing any URL, the user is redirected to provision the device. After provisioning, the intermediate certificate is installed on the iDevice.
CSCub17522	IP Phone IEEE 802.1X authentication reverts to PAC-based authentication when the "Accept client on authenticated provisioning" option is not enabled. When the "Accept client on authenticated provisioning" option is off, Cisco IP Phone EAP-FAST authentication sessions always end with an Access-Reject event. This requires the IP phone to perform PAC-based authentication to pass authentication. Since Cisco IP Phones perform authentication via authenticated provisioning and not via PAC-based authentication, it is not possible for the phone to authenticate when this option is off. **Workaround** Try one of the following: • Turn on the Cisco IP Phone "Accept client on authenticated provisioning" option. • Switch from EAP-FAST protocol to PAC-less mode. • Authenticate Cisco IP Phones via EAP-TLS rather than EAP-FAST.
CSCuc60349	False alarms on patch install/rollback as failure on secondary node ISE sometimes generates critical false alarms for install or rollback failure alarms on secondary node even though the install or rollback operations were successful. **Workaround** Use PAP (Administration > Maintenance > Patch > Show Node Status) to verify patch installation status.
CSCuc92246	Disk input/output operation while importing users slows down the appliance If you enabled the Profiler service in your deployment, you have a Cisco ISE 3315 appliance as your primary Administration node, and you import users, accessing the user interface becomes very slow. **Workaround** None

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCud00407	Microsoft Active Directory 2012 user authentication with Alternative User Principal Name suffix fails. This issue occurs when the Alternative User Principal Name (UPN) is the same as the name of the parent or ancestral domain to which Cisco ISE is joined. For example, if Cisco ISE is joined to a domain named "sales.country.region.global.com," and you have an Alternative UPN named "global.com," then user authentication fails. **Workaround** Use an Alternative UPN that is not the same as the parent or an ancestor.
CSCud18012	In policy sets, Proxy and EAP Chaining values for Use Case attribute should be used in authorization policies alone This issue occurs when you have a policy set with an outer condition based on the Use Case attribute that checks for the Proxy or EAP Chaining values. This condition is evaluated during authentication and the authentication fails because the use case is not known during authentication. **Workaround** While defining policy sets, do not use the Proxy and EAP Chaining values in the outer conditions.
CSCud18190	Unable to reregister a device (via EAP-TLS) that was provisioned earlier. If you delete an endpoint that was provisioned, you have to force the deleted or missing endpoint to re register with Cisco ISE so that the endpoint is created again. **Workaround** Create an authorization rule similar to the following: *Re-register-Policy NetworkAccess.AuthenticationMethod == x509_PKI CWA-Policy* This rule redirects to the CWA policy and authenticates the user (you must add the identity store to the guest authentication store sequence), and re-provisions the endpoint.
CSCud32406	Client provisioning policy cannot be updated. When you update the client provisioning policy in Cisco ISE and save the updated policy, an error message appears. **Workaround** None
CSCue08385	After changing the domain name could not access node in 3 node setup. After changing the domain name in PAP node, it is not possible to access the PAP node through GUI and HTTP error is thrown.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCue51298	Guest users who are assigned the ActivatedGuest role and First Login time profile have to change their password at first login or after password expiration. This issue occurs when you assign the ActivatedGuest guest role and the From First Login time profile to a guest user. This time profile requires the guest users to first access the Guest portal to change their password. The typical flow for these activated guest users does not require them to access the Guest portal because they sign in using IEEE 802.1X (dot1x) authentication or VPN. **Workaround** For activated guest users, use the From Creation time profile instead of the From First Login time profile.
CSCuf77949	After upgrade, two instances of the same alarm appear on your dashboard. After you upgrade, you might see two instances of the same alarm being generated. This issue exists for about 15 minutes after the upgrade is complete. **Workaround** None.
CSCug20312	When MAC OS X has an existing NAC Agent installed, the NAC Agent may take over the posture process before AnyConnect can be downloaded and installed. **Workaround** Configure the following on WLC: `config network web-auth captive-bypass enable`
CSCug60740	While using Chrome as browser on Nexus 7 tablet, if the Javascript is disabled, users logging in to the Guest portal for the first time will not be able to continue with the site security certificate page. **Workaround** Enable Javascript for the browser or install trusted certificate on ISE to avoid the site security certificate page.
CSCuh07275	Roaming of iPad breaks onboarding process. If a device roams to a different Access point or WLC that connects to a different PSN, then the CoA is sent to WLC that is not expecting it and the onboarding goes into a loop. **Workaround** Disconnect from the wireless and try to connect again.
CSCuh12619	BYOD: Device registration is successful even after cancelling the profile installation.
CSCuh22013	Some endpoint devices like iPAD and iPhone have issues with wildcard certificates when CN is blank.
CSCuh43300	Node group cluster information is deleted if a node is made primary and included in a node group at a time. When a node group is created in a standalone node and then the node is made as primary, the failover information is not notified to the primary node.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCuh75971	Issue running applet in Windows or Macintosh OS with latest Java 7 update 25. If Java 7 update 25 or above is installed, launching of the Agents or Network Setup Assistant during client provisioning or the onboarding process on a Windows or Mac OS X clients would take about 3 minutes as this Java update has Perform revocation checks enabled by default. This causes the applets signed certificates to be verified against the issuers CA server, which is currently blocked. This issue affects only Java applet and does not affect ActiveX, so there is less impact on Internet Explorer that uses ActiveX by default. **Workaround** Cisco ISE administrator should allow access to crl.thawte.com and oscp.verisign.net for restricted network during provisioning. If the administrator is not able open access to these sites, then the end user should turn off Perform certificate revocation checks in Java as follows: Open the Java Control Panel, click the **Advanced** tab, go to **Perform certificate revocation checks on** and select **Do not check**.
CSCuh77967	Error message when same rule name appears under local and Global exception When global and local exception rules are created with same names, they get saved successfully. While trying to edit and save the policy, an error message is displayed that the exception rule already exists.
CSCuh78210	Agent does not turn TLS1.0 in IE if FIPS ciphers are disabled by default When redirected from Internet Explorer, if the FIPS cryptographic cyphers from local security policies on client machines are enabled or disabled, then the NAC Agent does not pop up for posture assessment. **Workaround** Exit and launch the NAC Agent again to get the latest FIPS settings.
CSCuh90273	BYOD flow does not work when ISE acts as RADIUS proxy. Once AD user is authenticated successfully against remote RADIUS server, the user is redirected to NSP portal. In the NSP portal, it is not possible to obtain the user information. An error is thrown and instead of the 'Register' option, 'Try Again' option is displayed.
CSCui00865	After creating guest accounts using Mozilla Firefox, the 'Manage Guest Accounts' page does not contain the newly created guests and has missing objects. **Workaround** Clear the cache and restart the browser.
CSCui05265	Guest Role configuration in the Administration UI using IE does not work properly Configuring Guest Role at **Administration > Web Portal Management > Settings > Guest > Guest Roles Configuration**, using Internet Explorer does not display the ID groups properly. **Workaround** Use other browsers like Firefox.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCui07457	WLC ACL issue with Android device during BYOD In a BYOD flow, when the ACLs are created through the Setup Assistant, Android devices fail to download the Network Setup Assistant application. **Workaround** Do any one of the following to enable the Android devices to download the profile and connect to the network successfully. • Update the ACL in the WLC GUI by deleting one of the ACLs and creating it again with same values. OR • In the Edit page of the WLC, click Save without changing the values. This will update the ACL.
CSCui10632	NSP profile deleted and replaced by another after downloading the resources After creating an NSP profile for EAP-TLS and using it in a client provisioning policy, when the agents and resources are downloaded through the update feed URL, the NSP profile gets deleted. It is replaced with one of the downloaded NSP profiles.
CSCui12947	After upgrading, replication fails on deployment when secondary PAP is promoted. **Workaround** Delete the local certificates and restart the PAP.
CSCui19072	After creating RBAC menu access permission, navigate to the Home page and click the Show button. This throws the following error: 'TypeError: selectedItem is undefined'. **Workaround** This happens only for the first time. Edit the menu access, go to the Home page, and click Show.
CSCui28492	Registered Endpoints report takes a few minutes. **Workaround** Gather the statistics in CEPM schema and the reports are generated without delay.
CSCui87386	Default Guest Portal displays Self Service Results on screen with the White Listing Feature enabled. **Workaround** Use Custom Guest Portal, with the Self Service Results Page customized not to display the Results on screen. Additionally disable the Self Service option in Default Guest Portal Settings, as there is risk of accessing the Default Guest Portal tweaking the redirected URL
CSCuj22597	When using the notification feature, emails are delivered even when notifications disabled for the sponsor in admin. **Workaround** Disable the notification on the time profile setting instead.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCuj86245	Regular expression not working in User-Agent case When the MATCHES operator is used to create a profiling policy with the regular expressions, the case of the characters in the regular expressions may cause a valid match to fail. **Workaround** Use the regular expressions to match the lower case values in the string and avoid using upper case strings in the expression.
CSCum00347	PAP Auth fail when "use DES encryption types for this account" is enabled When "use DES encryption types for this account" is enabled on the user account, PAP/Kerberos user authentication fails. **Workaround** Enable "allow_weak_crypto" on the ISE AD Advanced Tuning with the following values: • Name: KERBEROS.[libdefaults].allow_weak_crypto • Value: true
CSCum78158	Surface Tablet Pro: Cannot select accept or decline on hotspot AUP In a Surface Tablet with Windows 8 Professional, nothing happens while clicking on the Accept or Decline option in the Acceptable Use Policy. **Workaround** Use stylus or the mousepad to click the options.
CSCun35098	Pre check is needed for ops Restore from unsupported versions 1.1.x > 1.3.x Cisco ISE 1.3 supports backup and restore from 1.2.x versions only. When you try to restore a backup from an earlier version, a success message appears, but the data is not restored properly and monitoring functions are impacted.
CSCun75689	ISE is unable to save a Scheduled Report using UTF-8 characters in the report name. You will receive the following message: "Schedule name should only contain alphanumeric and _ - . characters." **Workaround** Rename the Schedule Report with non-UTF-8 characters.
CSCuo42661	When importing a modified language template to a new portal, it also changes the default portal's language template locale key. **Workaround** Export the default portal's language template. Edit the file and change the default language template locale key to its original key.
CSCup09613	Guest Authentication Passed & Failed detail report page is missing Response time attribute and Guest Failed Authentication Method is getting updated as PAP_ASCII instead of webauth. **Workaround** None

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCup16289	While performing bulk Resend operation from within the Sponsor Portal Manage Accounts page, if the accounts do not have email addresses or phone numbers, the notification to those accounts will fail but the sponsor user will not know the accounts that failed. **Workaround** Ensure that the accounts have email address or phone number so the guest users can receive the notification.
CSCup21818	If PSN persona is not enabled in the deployment and if operator clicks on any test portal URL, then the following message is displayed: "Firefox can't establish a connection to the server at atlas-sec-pap.systestatlas1.local:8443." **Workaround** Make sure that on PSN the service is enabled in the deployment.
CSCup67571	Setting to show AUP every XX days not working in MyDevices **Workaround** Enable the option to show the AUP one time.
CSCup80462	Issues with location San Jose If the default location ‘San Jose’ is removed from all the Sponsor Groups, it is not possible to delete this location from the list at Guest Access > Settings > Guest Locations and SSIDs. In the list of Time Zones on the Guest Locations and SSIDs page, ‘San Jose’ is not listed.
CSCup83381	BYOD: Android device redirected to Playstore before CoA triggered The Android endpoint is not able to reach the PlayStore to download the Cisco Network Setup Assistant as the redirection is occurring before the CoA is triggered. **Workaround** Wait till the device reconnects to SSID after CoA is triggered.
CSCup86033	When an existing agent communicates with ISE, a flag is updated in the session data indicating the posture agent’s existence. If, for some reason, the posture agent did not communicate with ISE and the session data was not updated, opening up a browser window may cause it to download a posture agent from ISE. **Workaround** Please close the browser and let the existing posture agent to finish its task.
CSCup97236	When the Captive Network Assistant application is open, the AnyConnect posture client keeps scanning and is not able to connect to ISE server. **Workaround** Close Captive Network Assistant application to access ISE server.
CSCup97848	When a client upgrades its AnyConnect agent, there is no client provisioning report related to the information. Inconsistency with the behavior seen for NAC agent where the client provisioning report shows the upgraded agent version. **Workaround** Posture Detail Assessment report shows the value of the updated AnyConnect agent version used, which can be used to find the agent currently in use

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCuq05769	Allow access to OCSP server in posture remediation ACL When OCSP/CRL check is made mandatory on the client machine, ISE agent does not pop up unless access to the OCSP server is allowed in the posture remediation ACL. **Workaround** Disable this check in the client machine.
CSCuq06276	SecPAN ISE CA certificate chain not generated due to CKR_HOST_MEMORY error
CSCuq07313	When installing an IPN node in Cisco ISE 1.3 deployment, if you are using a UCS appliance, you must be plugged in to Broadcom daughter board and not the built-in or onboard Intel NIC before installing the ISO. Ignore the failed ping to the default gateway and NTP server. Reboot the UCS and traffic will resume after the NIC ordering is properly set.
CSCuq10131	In a Windows XP client, when NAC Agent is updated to the latest version, the setup file gets downloaded and installed. Still, the Agent version displays the previous version. **Workaround** Delete the previous version of NAC Agent and run a fresh flow, which installs the latest version successfully.
CSCuq10156	No Internet Access on Amazon Fire While using Amazon Fire or Amazon Kindle Fire with Silk browser to get connected using a Guest account, the user is not able to access the network. **Workaround** The reason for the blank page is Kindle Fire's captive portal. The Kindle Fire's captive portal discovery is using the following URL: /kindle-wifi/wifistub.html. Create an ACL to as a workaround.
CSCuq15143	When you launch the sponsor portal from the admin portal, once the session times out, you cannot login again using the same credentials. This happens because one-time-password is used to authenticate an admin user. **Workaround** Close the login window and click the **Managed Accounts** button from the admin portal.
CSCuq17707	Livelogs keeps loading after aggressive purging completed After restoring backup dump from Cisco ISE 1.2 and then performing aggressive purging, the Live Logs page keeps on loading. **Workaround** Due to aggressive purging, there is a significant change in the volume of the data, which impacts the query execution plan and in turn affects the performance of the Live logs. If you want to run aggressive purging, collect the statistics of the data after the purge using the **application configure ise** command. This will improve the Live Logs performance.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCuq20178	On MAC OS X, an existing NAC Agent may interfere with AnyConnect provisioning. The NAC Agent traffic gets directly sent to ISE without going through the discovery process, thus bypasses provisioning policy checking. **Workaround** Configure this on WLC: `config network web-auth captive-bypass enable`
CSCuq22852	LWA (local web authentication) flow fails if the user has the password with the special characters like ~ and + The first auth against ISE guest portal login is successful but the second auth against ISE guest success page is failing. **Workaround** Do not use special characters like ~ and + in the guest user password.
CSCuq33696	Admin Portal Login Page does not show up After adding the self signed certificate presented by ISE admin portal to exception list of Firefox and upgrading Firefox to version 31, the user is not able to connect to Cisco ISE admin portal. **Workaround** Delete the ISE admin server certificate from Firefox under Servers and Authorities as follows: • Go to Firefox Preferences > Advanced > Certificates > View Certificates > Servers, select ISE server certificate and click Delete. • Go to Firefox Preferences > Advanced > Certificates > View Certificates > Authorities, select ISE server certificate and click Delete.
CSCuq33968	Guest user account is created Syslog:Wrong GuestValidDays Sponsor Login & Audit and Master Guest Reports are displaying wrong guest validity (ValidDays set to "0") for Hours and Minutes Guest Users. **Workaround** None
CSCuq34006	Master guest report displaying wrong sponsor user name for "Guest user has changed the password operation". It is displaying guest username in sponsor user name column. **Workaround** None
CSCuq38640	Policy evaluation fails in a scenario if External MDM attribute is used The policy evaluation fails when authorization policies contain external MDM attribute. **Workaround** Flip the order of the Authorization policy to enable policy evaluation.
CSCuq38872	PrA continue does not happen on Mac OSX using AnyConnect Agent. Client has to do the posture again irrespective of the PrA set to continue. **Workaround** Increase the DHCP release/renew delay from 12/1 secs to 30/15 secs. The client gets a new VLAN IP and then can continue.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCuq40137	Not able to delete or remove endpoint from ID group after Hostname change. Endpoints cannot be deleted using the ID group page and only the associated mapping is removed.
CSCuq40425	'Guest Status' attribute does not change to show the Guest users status that were deleted. **Workaround** None
CSCuq41025	Guest Access Report are not showing ISE 1.2 Migrated Sponsor and MyDevice users Email, First Name and Last Name and IdentityStore information. **Workaround** None
CSCuq41438	Self-service guest after entering the details to register shows error When the sponsored self-service guest enters details to register, the portal is showing the following error: “Error Loading Page”
CSCuq43931	Internal pages within "Guest Access" menu may fail to load and the error code WAPXXXXX is displayed along with the error message. **Workaround** Log-out of ISE, clear browser cache and log-in again.
CSCuq53255	Guest with Galaxy S3 phone after logging in via self service guest flow does get network access. **Workaround** Disconnect and reconnect the SSID (with in session logout time on WLC)
CSCuq55794	When you add a new policy set to an existing one, the authentication rules for the new set are copied from the last one. **Workaround** Delete the added rules before saving the policy set
CSCuq58195	After upgrading from ISE 1.2 to ISE 1.3 admin portal menu items are not well aligned and some pages do not load. **Workaround** Clear the browser cache and reload the logic page.
CSCuq59599	With Self Registration Guest scenarios, at rate 5 per second and wait for 20 seconds after guests created to log in, and login failed. **Workaround** Use sponsor guest or wait 30 seconds
CSCuq63608	Sponsor Login & Audit, My Device Login & Audit and Master Guest reports are not displaying Endpoint MAC address and PSN information for CoA termination operation. **Workaround** None
CSCuq64500	DHCP renew/release timer needs to be updated with supported values When the DHCP release and renew delay values are set to below 5 seconds, the timers do not work as expected. **Workaround** Set the delay values to above 5 seconds

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCuq73868	Click on “continue” when Firefox reports unresponsive script; policy-set copy when ISE has multiple policy sets and admin is trying to copy rules under policy set1 to policy set2, Firefox may report “Unresponsive script” and prompts to click “continue/stop script”. This happens when the number of rules under policy set1 is beyond 50. The same message appears in the policy set copying window as well. **Workaround** Click “Continue” to progress with the copying of rules.
CSCuq74307	Authentications for users from a specific domain fail against an AD Scope but expected to succeed via specific join point in the Scope. **Workaround** Configure authentication domains appropriately. Leave the account domain of the user selected as 'Yes' domain in authentications domains ONLY on the join point that have good trust path to this domain; on other join points mark it as 'No' domain in authentication domains
CSCuq76745	Changes after editing endpoint purge rule are lost **Workaround** Make sure save button is clicked after making changes to endpoint purge rules.
CSCuq77162	It takes long time to load Guest Configuration and Guest Portal page. **Workaround** None
CSCuq77696	ISE in a VRF - managed Services environment In virtual routing and forwarding (VRF) environment, the WebAuth URL redirect is not working and the endpoint is not getting the HTTP response from the access switch. **Workaround** Perform route leaking between the Admin VRF and Guest VRF.
CSCuq88393	Exceptions while modifying and saving the portals with new portal tags While modifying any of the portals like BYOD, Client Provisioning, or Guest with the new portal tags and saving them, the ISE UI throws exceptions.
CSCuq90302	User names reported in the Master Guest Report, Guest AUP Report, etc. are not properly reflected. There are no issues with the user login. **Workaround** In the Username Policy under Guest->Settings, create a custom set of allowed characters that doesn't include "{};"
CSCuq96560	After upgrading from 1.2.1 to 1.3, a guest account created via Self-Registration has an invalid access duration post-upgrade. **Workaround** Edit the account from the Sponsor Portal and change the duration to a valid one.
CSCuq97051	Slow replication error for PSNs running on legacy IBM appliance in a large scale deployment with 30K network devices configured in DB. **Workaround** Increase SNMP polling interval to at least 8 hours (up to a maximum of 24 hours) for large scale deployment with thousands of network devices.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCur01031	Admin web requests ID certification when using password authentication only When the admin users are configured using password authentication only (no cert auth), the admin web sites prompt for an ID certification if the browser has one signed by a CA chain trusted by ISE. **Workaround** None
CSCur02547	Duplicate Logging targets are getting enabled for MyDevices and External MDM logging category when upgrade or restore ISE 1.2 configuration DB to ISE 1.3 is done **Workaround** Navigate to MyDevices and External MDM Logging Categories. Deselect logging targets, save and select again.
CSCur02900	The preview pane for Sponsor has some display issues when viewed using IE 10. **Workaround** Use Firefox or the test link to view the portal.
CSCur08045	The text box for 'Perform posture lease assessment every ... Days' is greyed out when it is selected, admin cannot edit the value until the configuration is saved. **Workaround** After selecting 'Perform posture lease assessment every.... Days', save the configuration. Change the value if needed and save the configuration again.
CSCur11226	It takes long time (few minutes) to load the guest portals or sponsor portals list page, when a large number of authorization policies or policy sets are used. **Workaround** None. Create less number of authorization policies or delete the policies that are not being actively used.
CSCur11286	iPhone 6 is not redirected to configured url after provisioning After provisioning is complete, the page is stuck at Reconnecting and redirecting... instead of redirecting to the URL configured on portal. **Workaround** Manually type the URL on a new page to access it.
CSCur13627	JRE has outdated timezone files (with older DST rules) due to which the updated Daylight saving timing for the years (2013, 2014 & 2015) are not updated in Java. The impact will be: • ISE not able to join/Leave Active directory for those countries where DST time is updated. • Monitoring alarms /Live logs may not show proper information. **Workaround** Use UTC as timezone for the impacted countries.
CSCur13741	When EAP-FAST authenticated provisioning or PAC-less EAP-FAST happens using client certificate received during tunnel establishment or inside the tunnel and in Certificate Authentication Profile username is configured to be taken from UPN, the authentication fails. **Workaround** Use Inner EAP-TLS for such cases.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCur14348	Endpoints can be profiled incorrectly. For example, an Apple Mac desktop profiled as a router. **Workaround** Collect user-agent attribute via WLC sensor or guest flow if possible, (as an alternative source for operating system). OR Manually edit endpoint configuration and statically assign to the correct profiling policy / identity group.
CSCur18659	When user goes through Self Provisioned guest portal, there is error loading page when trying to create a guest account with Kindle tablet (version: 5.4.5.3.1) **Workaround** Create a custom policy that checks to see if any other devices has the same first 3 sections of the paperwhites mac address. If so make those devices profiled as a paperwhite.
CSCur22580	Sign-on button disabled when AUP scroll-to-end with short AUP text When the Acceptable Use Policy (AUP) text length is short and the entire text fits in the content area that does not require scrolling, the sign-on button is not enabled for the user to accept the AUP. **Workaround** Disable “Require scrolling to end of AUP” when AUP text length fits in the content window.
CSCur23784	Adding custom fields fails with the internal error in sponsor portal "Create known guest account" customization page. **Workaround** Perform the following steps to resolve the error: • Go to **Guest Access > Settings > Custom Field** • Edit or delete the custom field which has a name ending with # • Go to **Guest Access > Configure > Sponsor Portal** • Edit the portal on the RHS table and go to Customization tab • Click the **Create Known guest customization** tab and add the custom field
CSCur24517	Portal ID value is not present on redirect URL for IPN Authorization profile When default guest portal is deleted, the authorization profile redirect url does not work as it does not have the portal ID as part of URL and there is no portal to get redirected. **Workaround** Do not delete default portals.
CSCur27077	Sponsor Login & Audit report is displaying wrong guest status, AWAITING_INITIAL_LOGIN instead of Created. **Workaround** None

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCur28245	UI/UX issues with sponsor group and guest type pages The Guest types and Location list items are not populated in the drop down list in **Guest Access > Configure > Sponsor Group**. The sponsor group member list items are not populated in the drop down in **Guest Access > Configure > Guest types**. **Workaround** Log out and log in to Cisco ISE.
CSCur28262	Cannot edit certificate tag, issue with wildcard certs in deployment **Workaround** Re-Import the wildcard cert on ISE and add the tag to be the same as used on PAP
CSCur29705	Sponsor portal Import fails if apostrophe character in SSID name **Workaround** Edit the SSID name from ISE admin and remove the apostrophe character from the name.
CSCur31382	Custom fields data not validated on sponsor import **Workaround** After adding the custom fields to the Sponsor Portal and/or Guest Type configuration, download the new template from the Sponsor Portal and populate the field data appropriately.
CSCur31625	Custom Fields for Guest Type and SP are not in sync **Workaround** The required setting in Guest Type takes precedent over the setting in Sponsor Portal and the customization text in Sponsor Portal is used over the text in Guest Type.
CSCur33493	8443 port is not listening after Restoring the configuration This issue will happen if Backup configuration contains different portal tag other than "default portal tag" and is restored on another host having different host name. **Workaround** Reconfigure the port number or edit any parameter on sponsor/guest /BYOD/ client provisioning portal
CSCur35258	When you remove any license, the corresponding service gets disabled in Cisco ISE server. But reinstalling the license does not enable the service automatically. You need to enable the service manually. This is observed for CA services when a Plus license is removed and installed and for an external MDM server when an Apex license is removed and reinstalled.

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCur35764	Removing Certificate from Trust Store also Revokes Certificate from CA **Workaround** The endpoints need to go through provisioning process and get a new certificate. In ISE 1.3 removing/deleting Internal CA certificate from trusted certificate will revoke the certificate. Before deleting the Internal CA certificate under trusted certificates, backup the Internal CA certificate and then remove it. If Internal CA certificate is removed, then use "Replace ISE RootCA" option to generate new Internal CA keystore.
CSCur36385	Default portal tag should be mapped to only one certificate **Workaround** Delete the old cert with "default group tag portal" manually
CSCur36983	Restore process stuck at 80%,field missing in LD_LIB_PATH **Workaround** Reload the PAP node using CLI and initiate manual sync from PAP UI deployment page.
CSCur38255	Password Expiration with X number of days not working for a guest user. **Workaround** None
CSCur38358	Active Directory does not fail back to site specific or preferred DC **Workaround** Make the current connected DC not available to ISE to trigger re-selection.
CSCur38742	Sponsor user belonging to a child grp of a sponsor group fails to login **Workaround** Manually add the child group to the sponsor group settings.
CSCur44557	Sponsor Portal notifications will fail if language bundles differ across portals **Workaround** Edit the guest account and choose a language from the current list within that Sponsor Portal.
CSCur44610	ISE 1.2 time Profile is not properly migrated to ISE 1.3. **Workaround** Inspect the Guest Types following the upgrade and correct the profiles.
CSCur47244	Cannot delete the Portal certificate though it is not part of any portal After removing the portal certificates from the deployment, users are not able to delete the portal certificate though they appear not being used by any of the portals. **Workaround** Instead of deleting, user can use a new certificate with another portal certificate group tag

Table 18 Cisco ISE, Release 1.3, Open Caveats (continued)

Caveat	Description
CSCur47256	Adding a new portal tag by importing the local certificates not working While trying to add a new portal tag by importing the External CA signed certificates locally on the PSN, the portal tag name is displayed. But when the server is restarted, the portal shows the old tag name instead of the new one.
CSCur49019	AnyConnect performing posture for OSX every time on VPN when PSN restarts In Mac OS X clients connecting through VPN and AnyConnect performing posture which are successfully compliant, when PSN restarts ever time, the client will have a VPN connection drop for 30 seconds. **Workaround** The client automatically connects back with the same session after re-posture.
CSCur49030	OSX redirects to CPP when PSN restarts though it is compliant A Mac OS X machine which is successfully postured and compliant through one PSN will be redirected to client provisioning portal for the compliant check when the PSN restarts and the client does not have network connectivity. **Workaround** Turn off the WI FI (kill the session) on the OSX machine and turn it back on. The client will go through posture check again and will have network access.
CSCus69704	Session timeout on the Guest Portal success page post Change of Authorization (CoA) stage. Once the session timeout is triggered on any of the Guest Portals, a message “Your session has timed out. Click Retry to try again” is displayed in a pop-up window with a Retry button. On clicking the Retry button, it results in a redirect back to the guest portal to start the authentication process again. This should be triggered only when the status is in pre-CoA stage. **Workaround** In the Administration > Device Portal Management > Settings page, click the Retry URL arrow and enter a valid URL, such as a company’s home page, in the Retry URL text box. The URL should not redirect guests who have successfully logged in. [OR] In the End points, do not click the Retry option present in the “session-timeout” pop-up window and continue browsing or configure a redirect to a URL instead of a Post-Login Banner page.

Open Agent Caveats

Table 19 Cisco ISE, Release 1.3, Open Agent Caveats

Caveat	Description
CSCti60114	The Mac OS X Agent 4.9.0.*x* install is allowing downgrade The Mac OS X Agent is allowing downgrades without warnings. **Note** Mac OS X Agent builds differ in minor version updates only. For example, 4.9.0.638 and 4.9.0.637.
CSCti71658	The Mac OS X Agent shows user as "logged-in" during remediation The menu item icon for Mac OS X Agent might appear logged-in before getting full network accesses The client endpoints are connecting to an ISE 1.0 network or NAC using device-filter/check with Mac OS X Agent 4.9.0.*x*. **Workaround** Please ignore the icon changes after detecting the server and before remediation is done.
CSCtj22050	Certificate dialog seen multiple times when certificate is not valid When the certificate used by the agent to communicate with the server is not trusted, the error message can be seen multiple times. **Workaround** Make sure you have a valid certificate installed on the server and that it has also been accepted and installed on the client. **Note** The additional certificate error message is primarily informational in nature and can be closed without affecting designed behavior.
CSCtj31552	Pop-up Login windows option not used with 4.9 Agent and Cisco ISE When right clicking on the Windows taskbar tray icon, the **Login** option is still present, but is not used for Cisco ISE. The login option should be removed or greyed out. **Workaround** There is no known workaround for this issue.
CSCtk34851	XML parameters passed down from server are not using the mode capability The Cisco ISE Agent Profile editor can set parameter modes to merge or overwrite. Mac OS X agent is not processing the mode correctly. Instead, the complete file is overwritten each time. **Workaround** To use a unique entry, the administrator must set up a different user group for test purposes, or set the file to read only on the client machine and manually make the necessary changes to the local file.
CSCtl53966	Agent icon stuck on Windows taskbar The taskbar icon should appear when the user is already logged in. **Workaround** Right-click on the icon in the taskbar tray and choose **Properties** or **About**. After you close the resulting Cisco NAC Agent dialog, the taskbar icon goes away.

Table 19 Cisco ISE, Release 1.3, Open Agent Caveats (continued)

Caveat	Description
CSCto33933	Login Success display does not disappear when user clicks OK This can occur if the network has not yet settled following a network change. **Workaround** Wait a few seconds for the display to close.
CSCto45199	"Failed to obtain a valid network IP" message does not go away after the user clicks OK This issue has been observed in a wired NAC network with IP address change that is taking longer then normal. (So far, this issue has only been only seen on Windows XP machines.) **Workaround** None. The user needs to wait for the IP address refresh process to complete and for the network to stabilize in the background.
CSCto48555	Mac OS X agent does not rediscover the network after switch from one SSID to another in the same subnet Agent does not rediscover until the temporary role (remediation timer) expires. **Workaround** The user needs to click **Complete** or **Cancel** in the agent login dialog to get the agent to appear again on the new network.
CSCto63069	The nacagentui.exe application memory usage doubles when using "ad-aware" This issue has been observed where the nacagentui.exe memory usage changes from 54 to 101MB and stays there. **Workaround** Disable the Ad-Watch Live Real-time Protection function.
CSCto84932	The Cisco NAC Agent takes too long to complete IP refresh following VLAN change The Cisco NAC agent is taking longer than normal to refresh IP address due to double IP refresh by supplicant and NAC agent. **Workaround** Disable the Cisco NAC Agent IP address change function if there is a supplicant present capable of doing the same task.
CSCto97486	The Mac OS X VLAN detect function runs between discovery, causing a delay VLAN detect should refresh the client IP address after a VLAN detect interval (5) X retry detect (3) which is ~ 30 sec, however it is taking an additional 30 sec. This issue has been observed in both a wired and wireless deployment where the Cisco NAC agent changes the client IP address in compliant or non-compliant state since Mac OS X supplicant cannot. An example scenario involves the user getting a "non-compliant" posture state where the Cisco ISE authorization profile is set to Radius Reauthentication (default) and session timer of 10 min (600 sec). After 10 min the session terminates and a new session is created in the pre-posture VLAN. The result is that the client machine still has post-posture VLAN IP assignment and requires VLAN detect to move user back to the pre-posture IP address. **Workaround** Disconnect and then reconnect the client machine to the network.

Table 19 Cisco ISE, Release 1.3, Open Agent Caveats (continued)

Caveat	Description
CSCtq02332	Windows agent does not display IP refresh during non-compliant posture status The IP refresh is happening on the client machine as designed, but the Agent interface does not display the change appropriately (for example, following a move from preposture (non-compliant) to postposture (compliant) status). **Workaround** There is no known workaround for this issue.
CSCtq02533	The Cisco NAC Agent takes too long to complete IP refresh following VLAN change The Cisco NAC agent is taking longer than normal to refresh IP address due to double IP refresh by supplicant and Cisco NAC agent. **Workaround** Disable the Cisco NAC Agent IP address change function if there is a supplicant present capable of doing the same task.
CSCts80116	OPSWAT SDK 3.4.27.1 causes memory leak on some PCs Client machines that have version 8.2.0 of Avira AntiVir Premium or Personal may experience excessive memory usage. **Note** This has only been observed with version 8.2.0 of Avira AntiVir Premium or Personal. Later versions of the application do not have this issue. **Workaround** Install later version of Avira AntiVir Premium or Personal.
CSCtw50782	Agent hangs awaiting posture report response from server **Workaround** The issue occurs with Mac OS X 10.7.2 clients. Kill the CCAAgent Process and then start CCAAgent.app. Perform the following: 1. Go to Keychain Access. 2. Inspect the login Keychain for corrupted certificates, like certificates with the name “Unknown” or without any data 3. Delete any corrupted Certificates 4. From the pull-down menu, select **Preferences** and click the **Certificates** tab 5. Set OCSP and CRL to off.
CSCty02167	IP refresh fails intermittently for Mac OS 10.7 guest users This problem stems from the way Mac OS 10.7 handles certificates. Marking the certificate as “trusted” in the CWA flow is not good enough to download the java applet required to perform the DHCP refresh function. **Workaround** The Cisco ISE certificate must be marked as “Always Trust” in the Mac OS 10.7 Keychain.

Table 19 Cisco ISE, Release 1.3, Open Agent Caveats (continued)

Caveat	Description
CSCty51216	Upgrading Mac OS X Agent version 4.9.0.638 to later versions fails. **Workaround** 1. Remove the "CCAAgent" folder from temporary directory 2. Reboot the client 3. Connect to Web login page and install the Agent from there
CSCub62836	In Live Authentication page, certain UTF-8 characters do not display correctly This only happens for a very limited set of characters. **Workaround** Use RADIUS Authentications report instead, to view the same information correctly.
CSCuj40148	During the BYOD flow the end user will be continuously redirected to the device registration page after installing Java. This occurs when: • the endpoint does not have Java installed and after the installation is completed on the Firefox browser, or • Java is uninstalled and the Firefox browser was not quit before starting the BYOD flow **Workaround** Quit and relaunch the Firefox browser after installing the Java package from www.java.com/en/download and then continue with the BYOD onboarding.
CSCul10891	Upgrade from earlier version of NAC Agent to version 4.9.0.1013 fails to launch Agent popup After upgrading to NAC Agent version 4.9.0.1013 on Windows 8 or Windows 8.1 64-bit clients, the upgraded Agent might not launch automatically. **Workaround** If the Agent does not launch automatically, then manually double-click the NAC Agent UI shortcut on the desktop to launch the Agent.
CSCum88173	Minimum compliance module version required for configuring SEP 12.1.x definition check on Mac OS is 3.6.8616.2 and not 3.6.8501.2. The minimum Compliance Module version required for configuring AV check in NAC support charts for Symantec Endpoint Protection(SEP) 12.1 for Mac OS is displayed as 3.5.8501.2. However, the version 3.5.8501.2 has issues in detecting the definition date/version for SEP 12.1.x on Mac OS. As this issue is addressed in Compliance Module 3.6.8616.2, administrators need to use 3.6.8616.2 as the minimum Compliance Module needed for detecting SEP 12.1 definitions on Mac OS.

Table 19 Cisco ISE, Release 1.3, Open Agent Caveats (continued)

Caveat	Description
CSCut48536	Multiple hotfix rules separated by the OR operator produce false positive results A single rule created for several hotfixes allows a machine without any hotfix to become compliant. For example, if you create a rule with the following hotfixes Windows 7 32 bit, Windows 7 64 bit, Windows 8 32 bit, Windows 8 64 bit, and so on separated by the OR operator, it allows a freshly installed Windows 8 64 bit machine without any hotfix to become compliant. The machine passes a generic registry check in Windows 7 32 bit hotfix and becomes compliant. **Workaround** Create a posture requirement rule for each operating system separately (for example, Windows 7 32 bit) to match the corresponding OS and hotfix rule.
CSCuw17919	Trend Micro Internet Security 10.x is not available. While performing the posture assessment for Trend Micro Internet Security 10.x, you must configure the posture condition with Trend Micro Titanium 10.x, because Trend Micro Internet Security 10.x uses Trend Micro Titanium 10.x AV/AS engine.
CSCuw19276	Cisco NAC Agent and Cisco NAC Web Agent do not support Google Chrome version 45 and later. The Java plug-in uses the Netscape Plugin API (NPAPI) in Goggle Chrome, which is integral to the functioning of the Cisco NAC Agent and Cisco NAC Web Agent. However, Google Chrome version 45 and later does not support NPAPI. **Workaround** To enable the Java plug-in: 1. In the Google Chrome window address bar, copy and paste the following URL: chrome://flags/#enable-npapi 2. Click the **Enable** link to enable NPAPI for Mac and Windows. 3. Click **Relaunch Now** at the base of the page to effect the changes.

Cisco ISE, Release 1.3, Resolved Caveats

This section lists the caveats that have been resolved in this release.

Resolved Caveats

Table 20 Cisco ISE, Release 1.3, Resolved Caveats

Caveat	Description
CSCun65239	The desktop device does not display sessionExpired page when the “change password” and “device registration” options are enabled.
CSCue17018	MNT node gets messages even after it is out of deployment and is disconnected.
CSCue46758	Session expired error occurs during guest authentication. Cisco ISE displays the following error message: `ISE: 86107- Session cache entry missing`
CSCuh01760	WLCs in roaming are reported as “Misconfigured NAS” when they generate RADIUS updates intermediately.
CSCuh07358	Holistic solution is required to resolve Java/SPW issue on Mac OS X/Windows provisioning.
CSCuh21086	While trying to edit or delete an attribute in profiler policy, the 'Save' option is not enabled.
CSCuh21153	IP Address does not refresh in Windows 7 client when using Internet Explorer for authentication in DRW flow.
CSCuh78514	Config Restore including ADE-OS could cause nodes go out of sync
CSCuh84099	On import ISE should verify non-printable characters in x 509 certificates
CSCuh88557	User password policy attribute migration issue
CSCuh94096	IE9: Register button greyed out when ActiveX is disabled
CSCui01605	Saving Duplicate policy set which has user defined simple condition fails
CSCui03041	Device ID does not go to RegisteredDevices group
CSCui08084	Guest user not terminated on switch when suspending through edit account
CSCuj03811	ISE suppresses only messages from NAS that are identical and are sent in sequence.
CSCui15633	Sponsor portal login fails for some users
CSCul92489	Active Directory is in debug mode by default in “Debug log configuration”
CSCuo89037	In Mac OS X with Safari 6.0 browser, Guest VLAN DHCP refresh does not work.
CSCup27628	After installing Cisco ISE 1.3, creating Self-Registered Guest Portal, Sponsored-Guest Portal, and Hotspot Guest Portal takes more time to load the configuration page.
CSCup62970	The Dictionary key is missing in the Admin Sponsor Portal customization pages.
CSCup87999	Portal wildcard certificates are not replicating to other nodes in the deployment when there are intermittent connectivity issues. This happens during a fresh install and the replication works fine with upgrade.
CSCup88214	When multiple custom fields added to Self-Registration Portal settings, they are not displayed in the Success page settings.
CSCup89799	SMS setting not migrated After upgrading from Cisco ISE 1.2 to 1.3, the SMS settings configured in the 1.2 language template are not migrated to the 1.3 SMS Gateway Provider settings.

Table 20 Cisco ISE, Release 1.3, Resolved Caveats (continued)

Caveat	Description
CSCup93023	RADIUS key wrap not working in ISE 1.3. When Inline Posture is setup in ISE and keywrap is enabled on WLC with RADIUS configured, the keywrap does not work.
CSCup98403	"ERROR_LDAP_LOCAL_ERROR" PAP & MSchapv2 authentication While Authenticating with PAP protocol the error "ERROR_LDAP_LOCAL_ERROR" occurs and user Authentication fails.
CSCuq02689	Portal theme colors are not migrated After upgrading from Cisco ISE 1.2 to 1.3, the portal theme colors are not migrated to 1.3 sponsor, MyDevices, and guest portals.
CSCuq33507	In a deployment with large number of nodes, the load time for editing Guest Portals is more than 1 minute.
CSCuq41254	Cannot Delete Guest User that contains the special character as single quote(')
CSCuq43846	AnyConnect agent shows compliance unknown in coa-asa with posture bypass

Resolved Agent Caveats

Table 21 Cisco ISE, Release 1.3, Resolved Agent Caveats

Caveat	Description
CSCug26558	In Live Authentications, Posture links redirect to the wrong MAC address and empty report.
CSCum76079	Client JAR manifest missing Permissions attribute & blocked by Java 7u51
CSCuj76689	NAC Agent should back off discovery algorithm if AC is configured in CPP
CSCul83245	Mac Agent should back off discovery when AnyConnect is configured
CSCum79468	Windows 8 Single Language pack support to be included
CSCud48606	NAC Agent does not validate the HTTPS connections after the initial one.
CSCuq52821	NAC Agent 4.9.4.3 takes about an hour to complete posture.
CSCur95891	NAC Agent should not communicate using the cached discovery IP address.
CSCup69321	The following error message is displayed, if a PSN goes down after the NAC Agent has started posture with the PSN: `Clean Access Server is not available on the network. Please contact our administrator if the problem persists.`
CSCup75697	If the discovery via Discovery Host and Default Gateway fails, Agent will try discovery via previously connected server. If the discovery via known server also fails, Agent goes into a loop of 30 retries. Agent does not exit this loop even if there is a network change event.

Resolved SPW Caveats

Table 22 Cisco ISE, Release 1.3, Resolved SPW Caveats for Windows

Caveat	Description	SPW Version
CSCun14753	Failed to get the certificate when SCEP template created is greater than 1024	1.0.0.37
CSCun64760	Support for upgrading third party software used for Java onboarding to the latest version	1.0.0.41
CSCuo37011	Internal CA Certificate issued to endpoint reflects incorrect data	1.0.0.39
CSCuo65083	BYOD: SPW crashes on Windows 7 client	1.0.0.39
CSCuo72465	BYOD flow failed with the new BYOD portal	1.0.0.40
CSCuq79723	LAT1-ISE-NL-BYOD laptop-slide 10-localization	1.0.0.43
CSCuo81140	Failed to download profile configuration on Windows 8 Enterprise N client	1.0.0.41

Table 23 Cisco ISE, Release 1.3, Resolved SPW Caveats for Mac OS X

Caveat	Description	SPW Version
CSCun14753	Failed to get the certificate when SCEP template created is greater than 1024	1.0.0.22
CSCuo73168	Native supplicant provisioning fails due to mismatch in key size between internal CA template and CSR generated by Mac OS X client	1.0.0.23
CSCuq59006	Unable to install MAC SPW 1.0.0.26 in Wired MAC10.7/8/9	1.0.0.27
CSCur09439	OS X 10.9.5 & 10.10.x SCEP EAP-TLS flow fails	1.0.0.29
CSCur38640	Network Setup Assistant (NSA) and Application Check (AC) need to be signed with Apple V2 signature	1.0.0.30

Table 24 Cisco ISE, Release 1.3, Resolved SPW Caveats for Android[1]

Caveat	Description	
CSCui42655	Network Setup Assistant fails to configure on Android 4.3	1.2.35
CSCuj28044	SPW fails to apply network configuration profile on Android 4.3	
CSCum58571	BYOD single SSID flow for Android device is broken	
CSCup32392	Incomplete Subject DN in Internal-CA issued certs for Android	1.2.41
CSCur02271	Tilting android mobile crashes Android SPW	1.2.41

Table 24 Cisco ISE, Release 1.3, Resolved SPW Caveats for Android[1]

Caveat	Description	
CSCut25212	Android 4.3 and above, NSP does not store certificates in the keystore	1.2.42[2]
CSCut58228	Samsung Android devices fail to install certificates for BYOD EAP-TLS	1.2.43

1. You can download the SPW from the Google Play Store. SPW 1.2.44 is the latest version.
2. On Android 4.3 and later devices, you will be prompted to install certificates, similar to the certificate installation warning that you see on earlier versions of Android devices.

Documentation Updates

Table 25 Updates to Release Notes for Cisco Identity Services Engine, Release 1.3

Date	Description
05/19/2015	Updated ISE 1.3 Patch 3
11/24/2014	Updated Open Caveats.
10/31/2014	Cisco Identity Services Engine, Release 1.3

Related Documentation

Release-Specific Documents

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.

Table 26 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html
Cisco Identity Services Engine Network Component Compatibility, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html
Cisco Identity Services Engine Admin Guide, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

Table 26 Product Documentation for Cisco Identity Services Engine (continued)

Document Title	Location
Cisco Identity Services Engine Upgrade Guide, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine, Release 1.3 Migration Tool Guide	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-user-guide-list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html
Cisco Identity Services Engine API Reference Guide, Release 1.3	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html
Active Directory Integration with Cisco ISE	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html
Regulatory Compliance and Safety Information for Cisco Identity Services Engine 3300 Series Appliance, Cisco Secure Access Control System 1121 Appliance, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco ISE In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-documentation-roadmaps-list.html

Platform-Specific Documents

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

- Cisco ISE
  http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html
- 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

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 2.0.

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