Release Notes for Cisco Identity Services Engine, Release 1.4

Revised: April 26, 2017

Contents

These release notes describe the features, limitations and restrictions (caveats), and related information for Cisco Identity Services Engine (ISE), Release 1.4. 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 can manually promote the Secondary Administration Node or configure automatic failover for administration persona.

    For more information on configuring automatic failover, see the “Configure Primary Administration Node for Automatic Failover” section in the *Cisco Identity Service Engine Administration Guide, Release 1.4*.

  - 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 for maximum network access devices (NADs) per deployment

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 1.4* 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 1.4*.

Supported Hardware

Cisco ISE software is packaged with your appliance or image for installation. Cisco ISE, Release 1.4 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	• Cisco UCS[1] C220 M3 • Single socket Intel E5-2609 2.4-GHz CPU, 4 total cores, 4 total threads • 16-GB RAM • 1 x 600-GB disk • Embedded Software RAID 0 • 4 GE network interfaces
Cisco SNS-3495-K9[2] (large)	Administration Policy Service Monitor pxGrid	• Cisco UCS C220 M3 • Dual socket Intel E5-2609 2.4-GHz CPU, 8 total cores, 8 total threads • 32-GB RAM • 2 x 600-GB disk • RAID 0+1 • 4 GE network interfaces
Cisco ISE-3315-K9 (small) [3]	Any	• 1x Xeon 2.66-GHz quad-core processor • 4 GB RAM • 2 x 250 GB SATA[4] HDD[5] • 4x 1 GB NIC[6]
Cisco ISE-3355-K9 (medium)	Any	• 1x Nehalem 2.0-GHz quad-core processor • 4 GB RAM • 2 x 300 GB 2.5 in. SATA HDD • RAID[7] (disabled) • 4x 1 GB NIC • Redundant AC power
Cisco ISE-3395-K9 (large)	Any	• 2x Nehalem 2.0-GHz quad-core processor • 4 GB RAM • 4 x 300 GB 2.5 in. SAS II HDD • RAID 1 • 4x 1 GB NIC • Redundant AC power

Table 3 Supported Hardware and Personas (continued)

Hardware Platform	Persona	Configuration
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 1.4*.[8] • For hard disk size recommendations, refer to the "Disk Space Requirements" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.4*. • NIC—1 GB NIC interface required (You can install up to 4 NICs.) • Supported VMware versions include: – ESXi 5.*x*

1. Cisco Unified Computing System (UCS)
2. 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.
3. In Cisco ISE 3315, running BYOD when internal CA is enabled might cause the nodes not being synchronized.
4. SATA = Serial Advanced Technology Attachment
5. HDD = hard disk drive
6. NIC = network interface card
7. RAID = Redundant Array of Independent Disks
8. 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.

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 8 (default) for ESXi 5.*x*
- VMware version 11 (default) for ESXi 6.0 (requires Cisco ISE 1.4 Patch 3)

Supported Browsers

The Cisco ISE, Release 1.4 administrative user interface supports a web interface using the following HTTPS-enabled browsers:

- Mozilla Firefox versions 31.*x* ESR, 36.*x*, and 37.*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 11.1.0.0 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* 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, 1.3, and 1.4. This is the recommended model of deploying the NAC agent in an environment where users will be roaming between ISE and NAC deployments.

Note Cisco NAC Agent version 4.9.5.8 and Web Agent version 4.9.5.4 provide support for Windows 10. Compliance Module Version 3.6.10120.2 supports Windows 10. Microsoft Internet Explorer 11 is supported. Microsoft Edge browser is not supported for Windows 10. End-of-Sale (EoS)/End-of-Life (EoL) has been announced for Cisco NAC Appliance and Cisco NAC Agent Software. For more information, see the EoS/EoL announcement at the following link: http://www.cisco.com/c/en/us/products/security/nac-appliance-clean-access/eos-eol-notice-listing.html

Support for Microsoft Active Directory

Cisco ISE, Release 1.4 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 1.4 supports Multi-Forest/Multi-Domain integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 1.4 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 1.4 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 1.4 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 1.4*. 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.
Primary NTP server	Must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server.	clock.nist.gov

Table 5 Cisco ISE Network Setup Configuration Parameters (continued)

Prompt	Description	Example
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 1.4*, 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 32 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 patch 14 or later
- Cisco ISE, Release 1.2.1 patch 5 or later
- Cisco ISE, Release 1.3 or later

The following table lists the Cisco ISE versions and what you need to do to upgrade to Cisco ISE, Release 1.4, from those versions:

Table 6 Cisco ISE 1.4 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. 5. Upgrade to Cisco ISE, Release 1.4.
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. 4. Upgrade to Cisco ISE, Release 1.4.
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. 4. Upgrade to Cisco ISE, Release 1.4.
Cisco ISE, Release 1.2	1. Apply the latest patch for Cisco ISE, Release 1.2. 2. Upgrade to Cisco ISE, Release 1.4.
Cisco ISE, Release 1.2.1	1. Apply the latest patch for Cisco ISE, Release 1.2.1. 2. Upgrade to Cisco ISE, Release 1.4.
Cisco ISE, Release 1.3	Upgrade to Cisco ISE, Release 1.4.

Follow the upgrade instructions in the *Cisco Identity Services Engine Upgrade Guide, Release 1.4* to upgrade to Cisco ISE, Release 1.4.

Note When you upgrade to Cisco ISE, Release 1.4, 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 1.4*.

Upgrade Considerations and Requirements

Read the following sections before you upgrade to Cisco ISE, Release 1.4:

Conflicting Alarms on Patch Installation in ISE dashboard

When applying a patch to several secondary PSN nodes, a PSN may appear to have failed to patch, and then succeed shortly after. After the PAN is patched, it propagates the patch to the secondary nodes. If there are network delays or server issues, the PAN may think the PSN failed to apply the patch, and report an error, even though the PSN is still applying the patch. If this happens, wait another 15 minutes and check the Patch Management page again.

iPEP Support in Cisco ISE 1.4

Cisco ISE, Release 1.4 can be installed on an iPEP node by using the Cisco ISE 1.2.1 version of IPN, that is distributed along with release 1.4.

Firewall Ports That Must be Open for Communication

The replication ports have changed in Cisco ISE, Release 1.4 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 1.4:

- 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.
- TCP 7800 and 7802—(Applicable only if the policy service nodes are part of a node group) For PSN group clustering.

For a full list of ports that Cisco ISE, Release 1.4 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 1.4 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 1.4.

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 1.4, 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 1.4. 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 1.4.*

Other Known Upgrade Considerations and Issues

Refer to the *Cisco Identity Services Engine Upgrade Guide, Release 1.4* for other known upgrade considerations and issues:

Cisco Secure ACS to Cisco ISE Migration

Cisco ISE, Release 1.4 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 1.4.

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 1.4 are available in the *Cisco Identity Services Engine, Release 1.4 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 1.4*.

Cisco ISE, Release 1.4, 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 1.4 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 1.4

Cisco ISE, Release 1.4 offers the following features and services. Refer to *Cisco Identity Services Engine Admin Guide, Release 1.4* for more information.

Guest

- Guest Periodic AUP Acceptance—You can create an authorization rule that requires a Guest user to accept an AUP to keep the session open after a certain number of hours.
- Guest Maximum Sessions—Limit the number of concurrent sessions that one Guest user can have, which is configured on the Guest Type.
- SAML—A SAML server can be used to authenticate Guest users.
- Sponsor Portal—Sponsors can now change the guest type when editing an existing guest user account.
- Guest Type—Changes to the guest type are now applied to the existing guest accounts, except custom fields.

Certificate Management

This release of Cisco ISE offers the following certificate-related enhancements:

- You can now create a generic Certificate Signing Request and can specify the usage at a later time. You can specify the usage at the time of binding or later by editing the certificate.
- When you edit a wildcard certificate from the Admin portal, the changes are replicated to all the nodes in the deployment.
- You can now delete system certificates that you no longer need from the Admin portal.
- You can now reassign the default portal certificate group tag to a CA-signed certificate. Also, from the System Certificates page, you can view the list of portals that use this tag.

Profiler

Profiler Feed button - A test button was added to the Profiler Feed page that tests the connection to the Cisco feed server.

SAMLv2 Identity Provider as an External Identity Source

Cisco ISE supports SAML Single Sign On (SSO) for the following portals:

- Guest portal (sponsored and self-registered)
- Sponsor portal
- My Devices portal

The Identity Provider stores and validates the user credentials and generates a SAML response that allows the user to access the portal. It reduces password fatigue by removing the need for entering different user name and password combinations.

Note In ISE 1.4, the SAML SSO feature is supported only for Oracle Access Manager (OAM) and Oracle Identity Federation (OIF).

Administration

Cisco ISE supports automatic failover for the Administration persona. To enable the auto-failover feature, at least two nodes in your distributed setup should assume the Administration persona and one node should assume the non-Administration persona. If the Primary Administration Node (PAN) goes down, an automatic promotion of the Secondary Administration Node is initiated. For this, a non-administration secondary node is designated as the health check node for each of the administration nodes. The health check node checks the health of PAN at configured intervals. If the health check response received for the PAN health is not good due to being down or not reachable, health check node initiates the promotion of the Secondary Administration Node to take over the primary role after waiting for the configured threshold value. There are some features that are unavailable after auto-failover of the Secondary Administrative Node. Cisco ISE does not support fallback to the original PAN.

MDM

- Cisco ISE 1.4 allows you to run multiple active MDM servers on your network, including ones from different vendors. You can route different endpoints to different MDM servers based on device factors such as location or device type. You can set up an MDM portal for each MDM server on your network.
- Cisco ISE 1.4 also supports MDM for devices accessing the network over VPN via AnyConnect and Cisco ASA 9.3.2 or later.
- Cisco ISE 1.4 now supports MDM servers from Meraki.

FIPS

FIPS Mode Support – Product Cisco Identity Services Engine uses embedded FIPS 140-2 validated cryptographic modules Cisco Common Cryptographic Module (Certificate #1643 and #2100). For details of the FIPS compliance claims, see the FIPS Compliance Letter.

Patches

Cisco ISE supports posture patch management and patch remediation features that allow you to proactively manage software patches. You can add the support of patch management compliance check and remediation by using the Opswat OESIS library to detect and remediate patch management applications for Windows OS and Mac OSX. You can select the installation, Enabled, and Up to Date attributes for different products that a vendor supports. The posture patch management remediation feature allows you to enable the patch management software, install missing patches, or activate the patch management software GUI on an endpoint. Patch management and patch remediation is supported for multiple vendors including Microsoft Windows Server Update Services (WSUS), System Management Server (SMS), and System Center Configuration Manager (SCCM) servers.

Endpoints and AnyConnect

SOURCEfire's Advanced Malware Protection (AMP) for endpoint software protects endpoints before, during, and after attacks. It provides a level of visibility and control you need to stop advanced threats missed by other security layers. The software should be downloaded from the SOURCEfire portal to add the AMP enabler profile to the client provisioning resources in Cisco ISE. You must download two images, namely, the redistributable version of the AMP for endpoint software for Windows OS and AMP for endpoint software for Mac OSX. The downloaded software is hosted on a server that is accessible from the enterprise network. The AnyConnect AMP Enabler module uses the URL to download the file to the endpoints.

Known Issues in Cisco ISE, Release 1.4

Issue with Special Character Usage in Sponsor/Guest Portal Customized SMS Notification

When creating customized SMS notifications in the Sponsor or Guest portal if special characters such as <,>,“,” are used, the message appears in encoded format on mobile devices.

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 Installation Files, Updates, and Client Resources

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

- Cisco ISE Downloads from the Download Software Center, page 17
- Cisco ISE Live Updates, page 18
- Cisco ISE Offline Updates, page 19

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 8, 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 1.4*.

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 1.4*.

- **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 1.4*.

If you do not enable the automatic download capabilities described above, you can choose to download updates offline. See Cisco ISE Offline Updates, page 19.

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 1.4*.

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
- Export to Spreadsheet

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 1.4.0.253 Patch Updates

This section provides information on patches that were made available after the initial availability of the Cisco ISE 1.4 release. Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions. Cisco ISE version 1.4.0.253 was the initial version of the Cisco ISE 1.4 release. After installation of the patch, you can see the version information from **Settings > About Identity Services Engine** page in the Cisco ISE GUI and from the CLI in the following format "1.4.0.253 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, "1.4(0.9NN)" where NN is also the patch number, displayed as two digits. For example, version "1.4.0.253 patch 3" corresponds to the following version in the bug database "1.4(0.903)".

The following patch releases apply to Cisco ISE release 1.4.0:

Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 11

Table 8 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.4.0.253 cumulative patch 11. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.4, 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 11 might not work with older versions of SPW. MAC users need to upgrade their SPW to MACOSXSPWizard 2.1.0.42 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 1.4*. for instructions on how to apply the patch to your system.

Table 7 Cisco ISE Patch Version 1.4.0.253-Patch 11 Resolved Caveats

Caveat	Description
CSCuv68628	ISE hangs when you use the "show run" command from the CLI, unable to generate support-bundle via GUI.
CSCva81452	AD ValidateAccount mechanism optimization to reduce RPC traffic and enhance overall performance.
CSCvb15627	Cisco Identity Services Engine SQL Injection Vulnerability.
CSCvb85648	Evaluation of positron for CVE-2016-5195 (DIRTY CoW).
CSCvc34224	ISE crashes and restarts automatically in JVM layer.
CSCvc71503	Jedis throws error and gets disconnected automatically.
CSCvd49829	Evaluation of positron for struts2-jakarta rce vulnerability.
CSCuo16506	Internal users cannot change their password in the guest portal.
CSCuy19991	In ISE 1.3 patch 5, Guest Authentication fails intermittently on the guest portal.
CSCuz11105	ISE fails to export language archive from the portal after modification.
CSCuz13452	In ISE 2.0, endpoint purging policies match only "Purge" rules and ignore "Never Purge" rules.
CSCuz75818	ISE 1.3 p6 Importing language file removes new line characters.
CSCva16918	Endpoint Purge doesn't work in ISE 1.4 P7.
CSCva46497	ISE XSS vulnerability in admin dashboard page.
CSCva46542	ISE SQL injection vulnerability.
CSCva70630	After importing and adding user credentials, Notices tab doesn't display imported account details.
CSCva94541	Evaluation of Leap Second 2016.
CSCvb25290	Endpoint purge takes a long time (~10 hrs) when a deployment has 400 thousand endpoints.
CSCvb86332	ISE 2.0.1.130 Authentication mechanism via GET requests Guest Portal.
CSCvb86760	ISE 2.0.1 Authentication mechanism via GET requests Sponsor Portal.
CSCvc13039	Endpoint identity group does not change via the hot spot portal.
CSCvc51943	ISE application-server process crashes due to syslog handling.
CSCvc53146	Endpoint Purge takes more than expected time (2-3 days) for 700 thousand Endpoint.
CSCvc83795	Guest portal doesn't accept password with < and ! special characters.
CSCvd11537	ISE generates huge number of start/stop dropping messages in syslog.
CSCvd27408	ISE fails to reconnect to syslog server if TCP connectivity gets disconnected.

Table 7 Cisco ISE Patch Version 1.4.0.253-Patch 11 Resolved Caveats

Caveat	Description
CSCva98129	ISE adds one more unsuccessful failed attempts in Guest Portal setting.
CSCux61238	Range of SNMPQUERY EventTimeout extended to 150 seconds from 60 seconds.
CSCuz57982	In ISE 1.3 P5, SMS Reset password is unavailable in Portal Customization Page.
CSCvd52520	Watchdog process is unable to restart redis server after getting crashed.
CSCvb93221	In ISE the rate limit range is increased to 1 to 3000.

Known Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 11

Unable to Install Cisco ISE 1.4 Patch 11 on Cisco ISE 1.4 Patch 10 via GUI

You can install Cisco ISE 1.4 Patch 11 from either CLI or GUI. There are installation issues from the GUI on an ISE server with less than 16GB memory. There are no known issues when installing the patch from the CLI.

Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 10

Table 8 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.4.0.253 cumulative patch 10. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.4, 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 10 might not work with older versions of SPW. MAC users need to upgrade their SPW to MACOSXSPWizard 2.1.0.42 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 1.4*. for instructions on how to apply the patch to your system.

Table 8 Cisco ISE Patch Version 1.4.0.253-Patch 10 Resolved Caveats

Caveat	Description
CSCuy80749	ISE Redis server crashed on PSN node under distributed deployment and core files are generated as a result of Redis server crash.
CSCvb14612	SNMP Query is not triggered due to lack of proper synchronization between Redis DB and Oracle DB.
CSCvb48654	Evaluation of positron for OpenSSL September 2016.

Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 9

Important Note Before Installing Cisco ISE 1.4 Patch 9

If you are installing Cisco ISE 1.4 patch 9 on a system where 1.4 patch 8 was not previously installed, then you must install on all nodes in same maintenance window and you must not have the nodes running on different patch levels beyond the maintenance window.

Resolved Issues

Table 9 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.4.0.253 cumulative patch 9. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.4, 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 9 might not work with older versions of SPW. MAC users need to upgrade their SPW to MACOSXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 1.4*. for instructions on how to apply the patch to your system.

Table 9 Cisco ISE Patch Version 1.4.0.253-Patch 9 Resolved Caveats

Caveat	Description
CSCuz44971	Inconsistent Endpoint inactivity timer causes purge issues in Cisco ISE 1.3.
CSCuz76370	Determination of Endpoint owner is dependent on Oracle when purging the Endpoint.
CSCva14899	Cisco ISE does not support MAC 10.12.
CSCva29741	Errors in German translations for guest.
CSCva32914	After upgrading from ISE 1.2 to 1.4, when the device is not operational in the AD domain, ISE responds to Nagios Radius Probes and prevents "Process Failure" response.
CSCva80275	ISE nodes attempt to check updates from third party websites.
CSCva84936	ISE is unable to profile Cisco access points due to cdpCacheAttribute null value during SNMP query probe.
CSCuq89147	When using Internet Explorer and logging into the ISE admin GUI, ISE admin web portal login requests ID certificates while only password based authentication is configured for ISE admin access.
CSCur11333	MNT Session API shows XML Errors and inaccurate information while processing the REST request.
CSCuy99383	When one of the SMTP servers is blocked, ISE does not attempt to reach the other SMTP IP address and emails are not sent to the guest users.
CSCuz98694	EAP-Chaining does not drop the authentication request when all the domains are unreachable.

Table 9 Cisco ISE Patch Version 1.4.0.253-Patch 9 Resolved Caveats

Caveat	Description
CSCva32911	After migrating from ISE 1.2 to ISE 1.4 and joining AD domain, “Pwdlastset” field does not get updated when re-joining ISE devices.
CSCva58328	Device registration through Hotspot portal fails with an error if the endpoint exists in ISE database and the endpoint was created by an ISE component other than a portal.
CSCvb24232	Security issues in SSH reported by retina network in Cisco ISE 1.4 Patch 9.
CSCuu60871	DNS Reverse Lookup is averted if the endpoint which was deleted less than an hour back is reconnected.
CSCva28741	Errors in German translations for the guest work flows. **Note**: To fix this issue in the existing portal, export German language properties file from a newly created portal and import the file back to the existing portal.

New Features and Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 8

Important Note Before Installing Cisco ISE 1.4 Patch 8

We recommend that you install the patch on all the nodes in the same maintenance window and not have the nodes running on different patch levels beyond the maintenance window. This can be best achieved by installing the patch via the primary PAN, which in turn propagates it to other nodes. Alternatively, you can install the patch via the CLI on a node by node basis.

Posture Patch Management Enhancements

Support for severity levels is added to the Posture Patch Management Condition and Patch Management Remediation.

The following are the newly added severity levels:

- Critical only
- Important and critical
- Moderate, Important and critical
- All—Low to critical

You can check if the patches with selected severity levels are up to date from Posture Patch Management Condition. The **Check patches installed** drop-down with the severity levels is enabled in Patch Management Condition only when the **Check Type** is chosen as **Up to Date**.

You can check and install missing patches with selected severity levels from Posture Patch Management Remediation. The **Check patches installed** drop-down with the severity levels in Patch Management Remediation is enabled only when the **Remediation Option** is chosen as **Install missing patches**.

This Severity Level enhancement is applicable only for clients that have AnyConnect 4.3 or later versions. If you have not configured the severity level in posture patch management condition in ISE and a client with AnyConnect 4.3 or later connects to the ISE server, AnyConnect defaults to Critical only support.

Note Windows compliance module 3.6.10611.2 is required for this update.

Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 8

Table 10 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.4.0.253 cumulative patch 8. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.4, 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 1.4*. for instructions on how to apply the patch to your system.

Note While importing guest users, you must add username and password columns to the template that is downloaded from the Sponsor Portal and specify the username and password fields in English only. All the other columns in the csv file can have international string.

Table 10 Cisco ISE Patch Version 1.4.0.253-Patch 8 Resolved Caveats

Caveat	Description
CSCuv53534	Endpoint lookup from the profiler database is slow.
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.
CSCux03001	Upon upgrading from ISE 1.2 to 1.4 and removing some SGTs, ISE does not push all the Trustsec policies to switch.
CSCux97025	Ownership change/merge can fail if the endpoint source is Configuration Protocol.
CSCux99204	ISE 2.0 patch 2 breaks HotSpot portal, CoA before AUP is accepted.
CSCuy89574	External Trust Authentication fails with "Server not found in Kerberos DB" error.
CSCuy99854	When FIPS mode is enabled in ISE 1.4 patch 7, application server gets stuck in initialization state.
CSCuz00972	pxGrid Services loop or get stuck when upgrading from ISE 1.2 to 1.3 patch 6.
CSCuz08717	Performance degradation observed in ISE 1.4 patch 7 due to profiler changes.
CSCuz28989	On Cisco ISE 1.4 Patch 6, AD connector restarts intermittently when a user logs in with invalid attributes.
CSCur44745	When the Suppress Repeated Successful Authentications option is enabled, CoA events are added to Auth details in Live Log session entry.
CSCur64918	ISE 1.2 replication stops when moving from monitoring to enforcement mode.

Table 10 Cisco ISE Patch Version 1.4.0.253-Patch 8 Resolved Caveats

Caveat	Description
CSCuu21473	Portal users for the existing BYOD on-boarded devices are missing from endpoints page after upgrading ISE 1.3 to 2.0.
CSCuv57398	Absence of Common Name (CN) in Admin certificate causes failure in provisioning initialization.
CSCuv77724	In Certificate Provisioning page, providing input in the PQDN field gives error "The FQDN field is not in a valid format".
CSCuv82040	In ISE 1.3/1.4, CoA is not sent when endpoint purge occurs from non-guest flow client.
CSCuv89453	Repeated password change and login loop occurs in the Guest and Sponsor Portals.
CSCuv95664	ISE 1.4 data base grows very large due to EDF database table logs, causing giant backups.
CSCuv99833	Feed posture scheduler service failed with JDBC exception.
CSCuw26491	Guest authentication is done based on the framed accounting service type.
CSCuw65623	Portals do not allow FQDNs such as test.123abc.com or test.123.com.
CSCux21939	Cisco ISE endpoint purge does not delete endpoints.
CSCux24687	Automatic AD to DC fail over does not happen on RPC failure.
CSCux48635	BYOD endpoints get stuck in pending state if more than two endpoints are provisioned within 20 minutes.
CSCux59729	Backup fails for nfs repository after ISE 1.4 patch 3 is installed.
CSCux73806	Operation console page loads, but does not open.
CSCux79853	HTTPS API call fails to SMS Gateway (tested with Clickatell).
CSCux89718	Cisco ISE 1.4 patch 3 has issues with guest portal login for guest accounts that have extended time range.
CSCux92681	SMS via HTTP-POST fails for GlobalDefault on Clickatell.
CSCuy52327	Unable to modify Endpoint Identity Group in Hotspot portal configuration in Cisco ISE, 1.4 patch 5.
CSCuy62830	In ISE 1.3 or later, CWA Auto Device Registration sends CoA Disconnect for a device already registered to the guest account.
CSCuy69285	Cisco ISE 1.3 patch 6 has issues with sessions not being released.
CSCuy71639	Cisco ISE incorrectly reports switchport index change.
CSCuy75787	Email notifications sent from sponsor portal using restAPI fail.
CSCuy83379	MyDevices portal overrides statically blacklisted endpoint.
CSCuy86957	Unable to delete guest compound condition and user identity groups mapped to sponsor group policy, after upgrading from ISE 1.2 to 1.4.
CSCuy92622	Sponsor portal notifications fail if language bundles differ across portals.
CSCuz42662	PxGrid services are stuck in initializing state.
CSCuz52493	Evaluation of positron for OpenSSL May 2016.
CSCuy54586	Evaluation of positron for OpenSSL March 2016.

Table 10 Cisco ISE Patch Version 1.4.0.253-Patch 8 Resolved Caveats

Caveat	Description
CSCuz53820	Severity level drop-down should be enabled/disabled selectively on Patch Management Conditions page.
CSCuu21562	Enhancement request to allow special characters in Network Device Group (NDG) value.
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.
CSCuz01888	NTP sync times out when an NTP server is added from UI.
CSCuu18124	LDAP sponsored accounts are missing after upgrade to ISE 1.3.
CSCuv68500	Redirection to MDM must not be made mandatory for devices that are not enrolled with MDM.
CSCuw27263	External RADIUS server was not supported for authentication when used as part of BYOD flow.
CSCuy24899	Enhancement request to decrease the minimum value for LastAUPAcceptance check.
CSCuy60352	ISE provides severity levels support on Posture patch management conditions.
CSCuz09501	Unable to set passwords while importing guest users.

Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 7

Table 11 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.4.0.253 cumulative patch 7. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.4, 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.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 1.4*. for instructions on how to apply the patch to your system.

Note This patch is not applicable for the customers who are using the FIPS mode.

Table 11 Cisco ISE Patch Version 1.4.0.253-Patch 7 Resolved Caveats

Caveat	Description
CSCuy34700	Update glibc packages to address CVE-2015-7547.
CSCuy53020	Bind SQL Injection was found in first Appscan reports for Guest related portal.
CSCut77541	April 2015 NTPd version has been updated to 4.2.6p5-3.el6.x86_64 for the CVE IDs CVE-2015-1798 and CVE-2015-1799.

Table 11 Cisco ISE Patch Version 1.4.0.253-Patch 7 Resolved Caveats

Caveat	Description
CSCuy20317	"Profiler Queue limit reached" error in patch 5 of ISE 1.3/4.
CSCux41407	Evaluation of positron for OpenSSL December 2015 vulnerabilities.

Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 6

Table 12 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.4.0.253 cumulative patch 6. To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.4, 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 1.4*. for instructions on how to apply the patch to your system.

Table 12 Cisco ISE Patch Version 1.4.0.253-Patch 6 Resolved Caveats

Caveat	Description
CSCur40082	Self Registration Portal unable to hide person being visited, username, password.
CSCus54412	ISE 1.3 does not prompt the remote client if password fails password policy.
CSCus79596	Network Access: IdentityAccessRestricted not authorized correctly.
CSCut56171	Custom fields added in Sponsor Portal can not be deleted.
CSCut95631	New Sponsor user does not get a summary of guest credentials via e-mail.
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.
CSCuu30079	Add, Edit & Duplicate operations are not working fine on AMP Enabler profile.
CSCuu32547	Sponsor user is unable to manage all accounts in ISE 1.3.
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.
CSCuu85800	Authentication Domain - Forest is missing from many Domains.
CSCuu92630	ISE 1.2 SGT replication failure after policy modification.
CSCuv52944	SWD-xxx LSQ-xxx ISE fails to send stop accounting; impacts Lancope users.
CSCuv53534	Endpoint lookup from the Profiler database is slow.
CSCuv54014	CRL/OCSP URL verification fails with nonpublic top level domain.
CSCuv71811	ISE 1.3 authentication latency is increased every hour.

Table 12 Cisco ISE Patch Version 1.4.0.253-Patch 6 Resolved Caveats

Caveat	Description
CSCuv88011	When using the Profiler Feed Service in ISE 1.4, the Feed Service Update overwrites the Admin Created rules of same name.
CSCuv97343	While creating new guest accounts, ISE 1.3 caches the previous Sponsor's email address.
CSCuw02111	ISE 1.4 patch 3: Session is not cleared after accounting stop is received from ASA.
CSCuw09138	In ISE 1.3 patch 3 high memory utilization is observed on PSN.
CSCuw15139	ISE report gives error: Unable to connect to the operation database.
CSCuw21758	The changes in the MyDevices AUP page settings are not taking effect.
CSCuw29108	ISE 1.3 Guest Portal access fails with embedded Posture check and Web Agent flow.
CSCuw31016	My Devices Portal not mapping the Portal User name properly from Guest Flow.
CSCuw31568	CP policy fails when posture policy is set to MAC 10.11.
CSCuw32233	ISE 1.3 patch 4 Show Live Sessions page is empty.
CSCuw34448	ISE 1.4 patch 3: SMS Gateway Configurations require optional fields.
CSCuw40899	ISE 1.4 Endpoint identity group does not get updated after changing the SSID.
CSCuw51376	DHCP Attributes are not acknowledged after a change in PSN ownership.
CSCuw74703	Concurrent Error. Unable to update endpoint during upgrade from 1.2.1 to 1.4.
CSCuw78737	GuestEndpoint is stuck in the HotSpot AUP portal loop even after purge.
CSCuw99899	ISE 1.3 patch 5 MNT session is not cleared even though accounting stop is received.
CSCux03119	Sponsored BYOD support.
CSCux10424	Active Directory Black list is not refreshed within expected frequency in ISE.
CSCux18771	Post self-registration, login with a different user fails with Internal Error.
CSCux24703	The Administrative Session ID should not be logged in the syslog Audit Records.
CSCux26799	Once the Hotspot Guest Endpoint is deleted from an identity group, it cannot connect to the Hotspot again.
CSCux53910	The system memory increase in ISE 1.3 patch 5 leads to authentication latency.
CSCux91475	Feed service update is not possible after a manual update in ISE 1.4 patch 6.

Open and Resolved Bugs in Cisco ISE Version 1.4.0.253—Cumulative Patch 5

Resolved Issues in Cisco ISE Version 1.4(0.253)—Cumulative Patch 5

All resolved bugs for ISE 1.4(0.905) are included in this search:

1.4(0.905) fixed bug search

All open bugs for ISE 1.4(0.905) are included in this search:

1.4(0.905) open bug search

New Features, Open and Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 3

New Features and Resolved Issues

Cisco ISE, Release 1.4.0.253 cumulative patch 3 offers the following new features:

- Support for Windows 10 Operating System, page 31
- Support for VMware ESXi 6.0, page 31

Support for Windows 10 Operating System

Cisco ISE, Release 1.4.0.253 cumulative patch 3 supports client machines and personal devices with Windows 10 Operating System.

Support for VMware ESXi 6.0

Cisco ISE, Release 1.4.0.253 cumulative patch 3 supports VMware version 11 (default) for ESXi 6.0.

Resolved Issues in Cisco ISE Version 1.4(0.253)—Cumulative Patch 3

All resolved bugs for ISE 1.4(0.903) are included in this search:

1.4(0.903) fixed bug search

All open bugs for ISE 1.4(0.903) are included in this search:

1.4(0.903) open bug search

Cisco ISE, Release 1.4, Open and Resolved Bugs

All resolved bugs for ISE 1.4(0.253) are included in this search:

1.4(0.253) fixed bug search

All open bugs severity 3 and higher for Cisco ISE 1.4(0.253) are included in this search:

1.4(0.253) open bug search

Documentation Updates

Table 13 Updates to Release Notes for Cisco Identity Services Engine, Release 1.4

Date	Description
11/07/2016	Added and updated Known Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 11 section.
09/15/2016	Added and updated Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 9 section.
07/08/2016	Added and updated New Features and Resolved Issues in Cisco ISE Version 1.4.0.253—Cumulative Patch 8 section.
5/1/2015	Cisco Identity Services Engine, Release 1.4

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 14 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.4	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html
Cisco Identity Services Engine Admin Guide, Release 1.4	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 1.4	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine Upgrade Guide, Release 1.4	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine, Release 1.4 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 1.4	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 1.4	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 1.4	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.