Release Notes for Cisco Identity Services Engine, Release 1.2

Revised: January 30, 2014, OL-27043-01

Contents

These release notes describe the features, limitations and restrictions (caveats), and related information for Cisco Identity Services Engine (ISE), Release 1.2. 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 a 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 1-1 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 two types of nodes:

- Cisco ISE node, which can assume any of the following three 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.

- 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, or Monitoring) 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)

Table 2 Recommended Number of Nodes and Personas in a Distributed Deployment

Node / Persona	Minimum Number in a Deployment	Maximum Number in a Deployment
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
Inline Posture	0	10000 for maximum network access devices (NADs) per deployment

You can change the persona of a node. See the "Setting Up Cisco ISE in a Distributed Environment" chapter of the *Cisco Identity Services Engine User Guide, Release 1.2* 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 1.2*.

Supported Hardware

Cisco ISE software is packaged with your appliance or image for installation. Cisco ISE, Release 1.2 is shipped on the following platforms. After installation, you can configure Cisco ISE with specified component personas (Administration, Policy Service, and Monitoring) 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	• 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)	Any	• 1x Xeon 2.66-GHz quad-core processor • 4 GB RAM • 2 x 250 GB SATA[3] HDD[4] • 4x 1 GB NIC[5]
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[6] (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, and Policy 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 1.2*.[7] • Hard Disks (minimum allocated memory): – Stand-alone—600 GB – Administration—200 GB – Policy Service and Monitoring—600 GB – Monitoring—500 GB – Policy Service—100 GB • NIC—1 GB NIC interface required (You can install up to 4 NICs.) • Supported VMware versions include: – ESX 4.*x* – ESXi 4.*x and 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. SATA = Serial Advanced Technology Attachment
4. HDD = hard disk drive
5. NIC = network interface card
6. RAID = Redundant Array of Independent Disks
7. 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, the Cisco Secure ACS 1121 and Cisco NAC 3315 appliances support small deployments, Cisco NAC 3355 appliances support medium deployments, and Cisco NAC 3395 appliances support large deployments.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- VMware ESX 4.*x*
- VMware ESXi 4.*x*
- VMware ESXi 5.*x*

Supported Browsers

The Cisco ISE, Release 1.2 administrative user interface supports a web interface using the following HTTPS-enabled browsers:

- Mozilla Firefox version 5.*x*, 8.*x*, 9.*x*, 14.*x*, 15.*x*, 18.*x*, 19.*x*, and 20.*x*
- Microsoft Internet Explorer 8.*x*, 9.*x* (in Internet Explorer 8 Compatibility Mode), and 10.*x*

Note The Cisco ISE user interface does not support using the Microsoft IE8 browser in IE7 compatibility mode. The Microsoft IE8 is supported in its IE8-only mode.

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 1.2* for information on supported devices, browsers, and agents.

Cisco NAC Agent Interoperability

There is integration support for different versions of Cisco NAC Agent for integration with Cisco NAC Appliance and Cisco ISE. Current releases are developed to work in either environment. However, interoperability between deployments is not guaranteed. Therefore, there is no explicit interoperability support for a given Cisco NAC Agent version intended for one environment. If you require support for Cisco NAC Appliance and Cisco ISE using a single Cisco NAC Agent, be sure to test NAC Agent in the specific environment to verify compatibility.

Unless there is a specific defect or feature required for Cisco NAC Appliance deployment, we recommend deploying the most current agent certified for your Cisco ISE deployment. If an issue arises, restrict Cisco NAC Agent to its intended environment and contact Cisco TAC for assistance. Cisco NAC Agent interoperability is not guaranteed, but testing and support is in progress.

Support for Microsoft Active Directory

Cisco ISE, Release 1.2 works with Microsoft Active Directory servers 2003, 2008, 2008 R2, and 2012 at all functional levels.

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

Supported Antivirus and Antispyware Products

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

- *Cisco Identity Services Engine Release 1.2 Supported Windows AV/AS Products*
- *Cisco Identity Services Engine Release 1.2 Supported Mac OS X AV/AS Products*

Installing Cisco ISE Software

To install Cisco ISE, Release 1.2 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 1.2 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 1.2*. Before you run the setup program, ensure that you know the configuration parameters listed in Table 4.

Table 4 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
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.

Table 4 Cisco ISE Network Setup Configuration Parameters (continued)

Prompt	Description	Example
System Time Zone	Must be a valid time zone. For details, see *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*, which provides a list of time zones that Cisco ISE supports. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT (or UTC-8 hours). The time zones referenced are the most frequently used time zones. You can run the **show timezones** command from the Cisco ISE CLI for a complete list of supported time zones. **Note** We recommend that you set all Cisco ISE nodes to the UTC time zone. This setting ensures that the reports, logs, and posture agent log files from the various nodes in the deployment are always synchronized with the time stamps.	UTC (default)
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (admin), you must create a new username. The username must be three to eight characters in length and composed of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password (there is no default). The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Note For additional information on configuring and managing Cisco ISE, see Release-Specific Documents, page 67 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 1.1.0.665 (or 1.1.0 with the latest patch applied)
- Cisco ISE, Release 1.1.1.268 (or 1.1.1 with the latest patch applied)
- Cisco ISE, Release 1.1.2 with the latest patch applied
- Cisco ISE, Release 1.1.3 with the latest patch applied
- Cisco ISE, Release 1.1.4 with the latest patch applied

Follow the upgrade instructions in the *Cisco Identity Services Engine Upgrade Guide, Release 1.2* to upgrade to Cisco ISE, Release 1.2.

Note When you upgrade to Cisco ISE, Release 1.2, you may be required to open network ports that were not used in previous releases of Cisco ISE. For more information, see "Appendix C, Cisco SNS-3400 Series Appliance Ports Reference" in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*.

Upgrade Considerations and Requirements

Read the following sections before you upgrade to Cisco ISE, Release 1.2:

No iPEP Support in Cisco ISE 1.2 Patches

Cisco ISE, Release 1.2 patches cannot be installed on an iPEP node due to the node's 32-bit architecture. You can still install Cisco ISE, Release 1.1.x patches on iPEP nodes.

Firewall Ports That Must be Open for Communication

The replication ports have changed in Cisco ISE, Release 1.2 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 1.2:

- TCP 1528—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 1.2 uses, refer to the *Cisco SNS-3400 Series Appliance Ports Reference*.

VMware Operating System to be Changed to RHEL 5 (64-bit)

Cisco ISE, Release 1.2 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.

- Enable BIOS settings that are required for 64-bit systems. See the following resources for more information:

  Cisco Identity Services Engine Hardware Installation Guide, Release 1.2

  http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1003945

- Ensure that you choose Linux as the Guest Operating System and Red Hat Enterprise Linux 5 (64-bit) as the version. See http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005870 for more information.

Guest Users Identity Source

In previous releases of Cisco ISE, guest-user records were available in the Internal Users database. Cisco ISE, Release 1.2 introduces a Guest Users database, which is different than the Internal Users database. If you have added the Internal Users database to the identity-source sequence, the Guest Users database also becomes part of the identity-source sequence. If guest-user logins are not required, remove the Guest Users database from the identity-source sequence.

Other Known Upgrade Considerations and Issues

Refer to the Cisco Identity Services Engine Upgrade Guide, Release 1.2 for other known upgrade considerations and issues:

- http://www.cisco.com/en/US/docs/security/ise/1.2/upgrade_guide/b_ise_upgrade_guide_chapter_01.html#ID50
- http://www.cisco.com/en/US/docs/security/ise/1.2/upgrade_guide/b_ise_upgrade_guide_chapter_01.html#ID244

Cisco Secure ACS to Cisco ISE Migration

Cisco ISE, Release 1.2 supports migration from Cisco Secure ACS, Release 5.3 only. You *must* upgrade the Cisco Secure ACS deployment to Release 5.3 before you attempt to perform the migration process to Cisco ISE, Release 1.2.

Cisco ISE does not provide full parity to all the features available in ACS 5.3, 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.

The migration tool only supports Mozilla Firefox, versions 3.6, 6, 7, 8, 9, and 10. Microsoft Windows Internet Explorer (IE8 and IE7) browsers are not currently supported in this release.

Complete instructions for moving a Cisco Secure ACS 5.3 database to Cisco ISE Release 1.2 are available in the *Cisco Identity Services Engine, Release 1.2 Migration Tool Guide*.

Cisco ISE License Information

Cisco ISE comes with a 90-day Base and Advanced Package Evaluation License already installed on the system. After you have installed the Cisco ISE software and initially configured the primary Administration persona, you must obtain and apply a Base, Base and Advanced, or Wireless license.

For more detailed information on license types and obtaining licenses for Cisco ISE, see *Cisco Identity Service Engine Hardware Installation Guide, Release 1.2*.

Cisco ISE, Release 1.2, supports licenses with two hardware IDs. You can obtain a license based on the hardware IDs of both the primary and secondary Administration nodes. For more information on Cisco ISE, Release 1.2 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 1.2

Cisco ISE, Release 1.2 offers the following features and services:

For more information on key features of Cisco ISE, see the “Overview” chapter in the *Cisco Identity Services Engine User Guide, Release 1.2*.

Support for UCS Hardware

Cisco ISE, Release 1.2, supports Cisco Unified Computing System (UCS) C220 hardware, which is shipped on the following platforms:

- SNS-3415 (small)
- SNS-3495 (large)

Refer to Table 3 for other platforms supported by Cisco ISE.

For more information, refer to the *Cisco Identity Service Engine Hardware Installation Guide, Release 1.2*.

Improved Performance and Scalability

Cisco ISE, Release 1.2 offers better performance and scale compared to previous versions. Cisco ISE 1.2 has moved from a 32-bit architecture to a 64-bit architecture, improving the overall performance from 100,000 concurrent endpoints per ISE deployment in ISE 1.1.x to 250,000 concurrent endpoints in ISE 1.2

Mobile Device Management Interoperability with Cisco ISE

This release of Cisco ISE can interoperate with Mobile Device Management (MDM) servers to secure, monitor, and support mobile devices that are deployed across mobile operators, service providers, and enterprises.

Cisco ISE, Release 1.2 supports MDM servers from the following vendors:

- Airwatch, Inc.
- Good Technology
- MobileIron, Inc.
- Zenprise, Inc.
- SAP Afaria
- FiberLink Maas360
- Cisco Mobile Collaboration Management Services (MCMS)

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2.*

MAB from Non-Cisco Switches

Cisco ISE, Release 1.2 supports Machine Authentication Bypass (MAB) from non-Cisco switches using the Cisco ISE endpoints database.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2.*

Support for Universal Certificates

Cisco ISE, Release 1.2 supports the use of wildcard server certificates for HTTPS (web-based services) and EAP protocols that use SSL/TLS tunneling. With the use of universal certificates, you no longer have to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (*) in the SAN field allows you to share a single certificate across multiple nodes in a deployment and helps prevent certificate-name mismatch warnings.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Note The universal certificates are referred as wildcard certificates in the user guide.

Policy Sets

This release of Cisco ISE allows you to create a set of authentication and authorization policy for various use cases. Policy sets are similar to access services in Cisco Secure ACS 5.*x* releases.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Profiler Feed Service

Cisco ISE, Release 1.2 provides a profiler feed service for publishing new profile definitions, updated profile definitions, and new OUI databases posted from IEEE.

With the introduction of the profiler feed service, the profiler conditions, exception actions, and NMAP scan actions are classified as Cisco provided or administrator created (see the System Type attribute) in Cisco ISE. Also, endpoint profiling policies are classified as Cisco provided, administrator created, or administrator modified (see the System Type attribute). You can perform different operations on the profiler conditions, exception actions, NMAP scan actions, and endpoint profiling policies depending on the System Type attribute.

You can retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription in Cisco ISE. You can also receive email notifications at an administrator email address that is configured for applied, success, and failure messages. You can also provide additional subscriber information to receive notifications. You can send the subscriber information back to Cisco to maintain the records and they are treated as privileged and confidential.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Logical Profiles

Cisco ISE profiles can be grouped in logical profiles. A logical profile is a container for a category of profiles or associated profiles, irrespective of Cisco-provided or administrator-created endpoint profiling policies. An endpoint-profiling policy can be associated with multiple logical profiles.

You can use the logical profile in an authorization-policy condition to help create an overall network-access policy for a category of profiles.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Enhanced Guest and Sponsor Pages

This release of Cisco ISE provides new default themes for the Guest and Sponsor portal pages. You can customize the pages by uploading logos and editing the color schemes.

When guests access the Guest portal using a mobile device, they are routed automatically to a mobile-optimized version of the Guest portal.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

RADIUS Authentication Suppression

This release of Cisco ISE allows you to configure RADIUS settings to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Collection Filters

You can configure collection filters to suppress syslog messages being sent to the monitoring and external servers. The suppression can be performed at the Policy Service Node level based on different attribute types.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Support for Secure Syslogs

Cisco ISE, Release 1.2 can be configured to send secure syslogs to Monitoring nodes and between Cisco ISE nodes, by enabling TLS-protected syslog collectors.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Support for Windows 2012 Active Directory

Cisco ISE, Release 1.2 supports Microsoft Windows 2012 Active Directory.

Global Search

Cisco ISE, Release 1.2 provides a system-wide endpoint search box that you can use to quickly find and filter endpoints and users on a network. The search result includes detailed session information about each of the matching results, such as the type of access, location, endpoint MAC and IP address, and authorization profile. You can also export these results for further analysis.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Session Trace

Cisco ISE, Release 1.2 provides a more efficient troubleshooting functionality. After search results are displayed, you can click the “play” button for more details. A new detailed screen with full session information for the endpoint is displayed.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Enhancement to Client Provisioning

Starting from Cisco ISE Release 1.2, it is mandatory to include the client provisioning URL in authorization policy, to enable the NAC Agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2*.

Enhanced Reports and Alarms

Cisco ISE, Release 1.2 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. A new scheduling service that allows you to queue reports and receive notification when they are available.

Table 5 Changes to Reports in Cisco ISE, Release 1.2

Report Name	Change
Endpoint Time to Profiler	Removed
Authentication Failure Code Lookup	Removed
Network Device Log Message	Removed
PAC Provisioning	Removed
Policy CoA	Removed
Posture Trend	Removed
Endpoint Operations History	Removed
AAA Down Summary	Removed. If a AAA server is down, you can see it on the dashboard and in the Health Summary report.
TOP N AAA Down by Network Device	Removed. If a AAA server is down, you can see it on the dashboard and in the Health Summary report.
Authentication Trend	Renamed as Authentication Summary report.
TOP N Authentication by Allowed Protocol	Moved to the Authentication Summary report. You can filter the report by Allowed Protocols.
Server Authentication Summary	Moved to the Authentication Summary report. You can filter the report by Server.
TOP N Authentication by Server	Moved to the Top N Authentication report. You can filter the report by Server.
TOP N Authentication by Machine	Renamed as Top N Authentication by Endpoint.

Table 5 Changes to Reports in Cisco ISE, Release 1.2

Report Name	Change
Failure Reason Authentication Summary	Moved to the Authentication Summary report. You can filter the report by Failure Reason.
TOP N Authentication by Network Device	Moved to the Authentication Summary report. You can filter the report by Network Device.
Session Status Summary	Renamed as Network Device Session Status report.
User Authentication Summary	Moved to the Authentication Summary report. You can filter the report by User.
Radius Terminated Sessions	Moved to the Session View report. You can filter the report by Terminated Sessions.

In Cisco ISE, Release 1.2, a new dashlet is on the dashboard that allows you to enable and disable alarms and make minor configuration changes. The following is a list of alarms that are removed in Cisco ISE, Release 1.2:

- Administrator Account Disabled
- Max Administrator Sessions Exceeded
- Restore Successful
- Purge Backup Success
- Replication Syn Failure
- High CPU Utilization
- Purge Failure
- Purge Success
- Application Exceeded Maximum Disk space
- Base License count
- Advanced License count
- Admin Account Lockout
- NTP Server not Reachable
- Disk Cleanup
- Successful Node Registration
- Successful Patch Install
- Successful Patch RollBack
- Successful Node Deregistration
- Successful Update Node
- UnSuccessful Add Node
- UnSuccessful Patch Install
- UnSuccessful Patch Roll Back
- UnSuccessful Remove Node
- UnSuccessful Update Node

For more information, refer to the *Cisco Identity Services Engine User Guide, Release 1.2.*

Enhancements to Live Authentications Page

The Live Authentications page on the Cisco ISE dashboard shows the details corresponding to authentication entries. In addition to these live authentication entries, the Live Authentications page is enhanced to show the live-session entries. You can also get a detailed report on a session.

For more information on the enhancements to the Authentications page, see *Cisco Identity Services Engine User Guide, Release 1.2.*

Enhancements to Cisco NAC Agent

The following enhancements have been added to Cisco NAC Agent in Cisco ISE, Release 1.2.

Cisco NAC Agent for Windows

- Support for the Polish Language.
- Support for the Microsoft Windows 8 Operating System. In Windows 8, Internet Explorer 10 has two modes: Desktop and Metro. In Metro mode, the ActiveX plugins are restricted. You cannot download the Cisco NAC Agent in Metro mode. You must switch to Desktop mode, ensure ActiveX controls are enabled, and then launch Internet Explorer to download the Cisco NAC Agent. If users are still not able to download Cisco NAC agent, check and enable "compatibility mode."
- Support for the Log Packager option in the Agent Icon to collect support logs.
- New for Cisco ISE 1.2 patch 3: support for Microsoft Windows 8.1.

Cisco NAC Agent for Mac OS X

- Support for the Collect Support Logs option in the Agent Icon to collect Agent logs and support information.
- Notification screen appears automatically when the Agent window is buried by other windows.
- Support for the Acceptable Use Policy (AUP).
- New for Cisco ISE 1.2 patch 3: support for Mac OS X 10.9.

External RESTful Services

External RESTful Services (ERS) is a new Cisco ISE component that allows you to perform Create, Read, Update, and Delete (CRUD) operations on Cisco ISE resources. ERS also allows you to run advanced queries against the Cisco ISE database and perform bulk operations such as mass updates or deletions.

ERS is based on HTTPS and REST methodology. These APIs provide an interface to the ISE configuration data by enabling internal user identities, endpoints, endpoint groups, identity groups, SGTs, and profiler policies to perform CRUD operations on the ISE data.

Refer to the *Cisco Identity Services Engine API Reference Guide, Release 1.2* for more information.

Known Issues in Cisco ISE, Release 1.2

Mobile Devices Without VLAN

When a mobile device completes the guest flow without VLAN/IP refresh enabled in the Guest Portal, it matches the permit access authorization policy, followed by a CoA termination that deletes the session. The device then goes through the guest flow again and forms a loop.

Web Portal Customization

When you want to customize a web portal to use the Russian language template, the Browser Locale Mapping for the Russian template is “ru-ru.” However, this default mapping does not work on iPhones. If you encounter this issue, you can create a duplicate template with the Browser Locale Mapping set to “ru.”

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.

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 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
- 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 internal MDM server as Cisco ISE cannot bypass proxy services for MDM communication. To resolve this, you can configure the proxy service to allow internal communication to the MDM servers.

For more information on proxy settings, see the "Specifying Proxy Settings in Cisco ISE" section in the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.2*.

Client Provisioning and Posture Live Update portals:

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

  The following software elements are available at this URL:

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

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Downloading Client Provisioning Resources Automatically" section of the "Configuring Client Provisioning" chapter in the *Cisco Identity Services Engine User Guide, Release 1.2*.

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

  The following software elements are available at this URL:

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

  For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Downloading Posture Updates Automatically " section of the "Configuring Client Posture Policies" chapter in the *Cisco Identity Services Engine User Guide, Release 1.2*.

If you do not enable the automatic download capabilities described above, you can choose to download updates offline. See Cisco ISE Offline Updates, page 21.

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 "Adding Client-Provisioning Resources from a Local Machine" section of the "Configuring Client Provisioning" chapter in the *Cisco Identity Services Engine User Guide, Release 1.2*.

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

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

To upload offline posture updates, 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.

Cisco ISE, Release 1.2.0899 Patch Updates

The following patch releases apply to Cisco ISE release 1.2.0:

Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 5

Table 9 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.2.0.899 cumulative patch 5.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.2, 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.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.2*. for instructions on how to apply the patch to your system.

Note Please be aware that applying patch 5 to Cisco ISE 1.2 will reboot the nodes on which it is installed. Please make sure you carry out this activity in a maintenance window with a downtime. Cisco ISE 1.2 will also reboot if you revert from patch 5 to an earlier version.

If you experience problems installing the patch, contact Cisco Technical Assistance Center.

Table 6 Cisco ISE Patch Version 1.2.0.899-Patch 5 Resolved Caveats

Caveat	Description
CSCub18575	Problem with sponsor accounts starting with a "0" This patch fixes an issue where you could not log into the Sponsor Portal with an account that started with the number 0.
CSCuf24898	ISE repository max password length 16 characters This fix addresses an issue where FTP / SFTP repository access failed when the user password was larger than 16 characters.

Table 6 Cisco ISE Patch Version 1.2.0.899-Patch 5 Resolved Caveats

Caveat	Description
CSCug20065	Unable to enforce RBAC as desired to a custom administrator This fix addresses an issue where a user, who only has permissions to a custom endpoint identity group, is unable to add, modify, or delete identities unless the entire identities are visible to him.
CSCuh25506	Cisco ISE CSRF Vulnerability This fix addresses an issue where CSRF protection did not work for some of the web pages and an attacker could exploit this issue to perform CSRF attack against the users of the web interface. **PSIRT Evaluation** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C CVE ID CVE-2013-3420 has been assigned to document this issue. Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-3420 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
CSCui30266	ISE MDM Portal Cross-Site Scripting Vulnerability This fix addresses an issue where the Mobile Device Management (MDM) portal of Cisco Identity Services Engine (ISE) was vulnerable to a cross-site scripting (XSS) attack. **PSIRT Evaluation** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:U/RC:C CVE ID has been assigned to document this issue. Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5504 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

Table 6 Cisco ISE Patch Version 1.2.0.899-Patch 5 Resolved Caveats

Caveat	Description
CSCui46739	Guest applet fails after update to Java 7 update 25 This patch addresses an issue where both Guest Authentication and Supplicant Provisioning failed due to Java 7 update 25's CRL check feature. To disable the CRL check feature: 1. Allow the CRL check through the Redirect ACL, Port ACL and any Firewall in place. 2. Clear the checkbox for the CRL check in the Java Control Panel: • OS X: System Preferences > Java Advanced > Perform certificate revocation using: Change to 'Do not check (not recommended)' • Windows: Control Panel > Java Advanced > Perform certificate revocation using: Change to 'Do not check (not recommended)'
CSCui67495	Uploaded Filenames/Content Not Properly Sanitized This fix addresses an issue where filenames and content uploaded to Cisco Identity Services Engine (ISE) was not filtered/sanitized effectively. This could have resulted in a file of incorrect type being uploaded to ISE or the filename leading to a potential cross-site scripting (XSS) issue. **PSIRT Evaluation** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:P/A:N/E:H/RL:U/RC:C CVE ID CVE-2013-5541 has been assigned to document this issue. Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5541 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

Table 6 Cisco ISE Patch Version 1.2.0.899-Patch 5 Resolved Caveats

Caveat	Description
CSCui67511	Certain File Types are not Filtered and are Executable This fix addresses an issue where, due to insufficient filtering and access control, potentially malicious file types could have been uploaded to, and executed within, the Cisco Identity Services Engine (ISE) web interface. **PSIRT Evaluation** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:P/I:N/A:N/E:H/RL:U/RC:C CVE ID CVE-2013-5539 has been assigned to document this issue. Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5539 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
CSCui72269	ISE unable to understand SNMP attribute coming from Switch This fix addresses an issue where Cisco ISE was unable to handle a bad attribute in an SNMPT query coming from a switch, which caused high CPU cycles on PAP node.
CSCuj48111	Hyphen and minus sign can't be entered as first or last name This fix addresses an issue where a guest sponsor was unable to enter a hyphen or minus as part of a first or last name while entering a guest's account information.
CSCuj61976	Admin UI fails to display certain UI pages when using Firefox 25 This fix addresses an issue where ISE admin UI pages with a tree view were not displayed correctly in Firefox 25.
CSCuj84194	ISE sometimes does not send DACL in authorization profile This fix addresses an issue where ISE sometimes did not send DACL in an authorization profile.
CSCuj98726	iOS devices bypass account suspension/lock by starting new EAP session This fix addresses an issue where an iOS device can bypass account suspension/lock even it is enabled, due to it being reported as '5440 Endpoint abandoned EAP session and started new' instead of using a wrong password.

Table 6 Cisco ISE Patch Version 1.2.0.899-Patch 5 Resolved Caveats

Caveat	Description
CSCul02860	Struts Action Mapper Vulnerability Previous versions of ISE Cisco ISE included a version of Apache Struts that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2013-4310 Cisco has analyzed these vulnerabilities and concluded that the product is not impacted, however the affected component has been updated as harden measure. **PSIRT Evaluation** The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels. If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation. 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
CSCul03127	Struts 2 Dynamic Method Invocation Vulnerability Previous versions of Cisco ISE included a version of Apache Struts2 that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2013-4316 **PSIRT Evaluation** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C CVE ID CVE-2013-4316 has been assigned to document this issue. 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
CSCul03621	Endpoint Profiling Information is not being replicated correctly This fix addresses an issue where Endpoint Profiling Information was not replicated on the PSN that was not doing the profiling.
CSCul06431	Active Directory attribute value in ATZ profile is not sent This fix addresses an issue where an Active Directory attribute was not sent to the client as part of an ATZ profile.

Table 6 Cisco ISE Patch Version 1.2.0.899-Patch 5 Resolved Caveats

Caveat	Description
CSCul13757	Audit records MUST log to External Syslog Servers: CLI log level This fix addresses an issue where any configured External Syslog servers failed to receive audit records after using the command line interface (CLI) commands to change the log level to any of the following levels: 2, 3, 4, 5, 6 or 7.
CSCul13805	Audit records MUST log to External Syslog Servers: HTTPS idle timeout This fix addresses an issue where External Syslog Servers failed to receive an audit record in the case of HTTPS Admin GUI idle session timeout occurs and auditable events could only be seen locally by setting the Debug Log Configuration for admin-infra and infrastructure to DEBUG level.
CSCul13812	Audit records MUST log to External Syslog servers: SSH publickey This fix addresses an issue where SSH server authentication using the publickey authentication method fails to record an audit log and failed connecting to External Syslog Servers.
CSCul13883	Audit records MUST log to External Syslog servers: SSH KEX Group14 This fix addresses an issue where Configured External Secure Syslog servers failed to receive audit events for the administration configuration of SSH server enforcement requiring diffie-hellman-group14-sha1 key exchange algorithm in order to successfully connect.
CSCul13905	Audit records MUST log to External Syslog Servers: CLI clock set This fix addresses an issue where no audit logs were recorded for changing the system clock via the CLI.
CSCul13946	Audit records MUST log to External Syslog servers: Purge M&T Data This fix addresses an issue where no audit logs were recorded after purging M&T operational data using the CLI command.
CSCul15967	ISE 1.2 Patch 3 Windows 8.1 CPP OS Detection Failure in Distributed Setup This fix addresses an issue in the ISE 1.2 patch 3 where Windows 8.1 clients received an error on secondary PSNs after a CPP redirect.
CSCul16300	Audit records MUST log to External Syslog servers: CLI idle timeout This fix addresses an issue where External Syslog Servers fail to receive the audit syslog event when command line interface (CLI) connections are closed due to idle session timeout.
CSCul18169	Blocking ISE admin UI access for Chrome browser This fix addresses some issues that blocked Chrome browsers from using the ISE admin UI.
CSCul18521	Audit records MUST log to External Syslog servers: VGA CLI AUTHC This fix addresses an issue where External Syslog Servers fail to receive audit syslog events for administrative CLI logins on a VGA console.
CSCul18555	Audit records MUST log to External Syslog servers: SSH conn fail This fix addresses an issue where External Syslog Servers fail to receive audit syslog events for common SSH connection failures.

Table 6 Cisco ISE Patch Version 1.2.0.899-Patch 5 Resolved Caveats

Caveat	Description
CSCul23070 CSCul23252	Audit records MUST log to External Syslog Servers: SSH exit forceout This fix addresses an issue where External Syslog Servers fail to receive audit syslog events for CLI `exit` and `forceout` commands.
CSCul42646	Failed to create Posture Condition with "NOT ENDS WITH" Operator This fix addresses an issue where creating a Posture condition with an NOT ENDS WITH operator resulted in an error.
CSCul46893	URL preservation not working with self service guest user in MAB flow This fix addresses an issue where, after connecting to a wired MAB and creating a guest account, the user's browser did not redirect to the URL that they originally attempted to access.
CSCul58758	Redirecting to 'null' page in the browser after LWA flow with WLC-5500 This fix addresses an issue where connecting to the Guest Wireless LWA flow using a Windows client machine resulted in a guest account getting redirected to a "null" page in the browser window instead of original URL.

Enhancements in Cisco ISE Version 1.2.0.899—Cumulative Patch 4

Automatic Update of Compliance Module on Mac OS X Clients

Starting from Cisco Identity Services Engine, Release 1.2.0.899 cumulative patch 4, the Cisco NAC Agent supports automatic update of the Compliance Module on Mac OS X clients. Ensure that you have installed the Mac OS X Agent version 4.9.4.1 or later so that the Compliance Module gets updated automatically. Refer to Cisco ISE Installation Files, Updates, and Client Resources, page 19 for more information on automatic updates. See Also CSCui83009, page 30.

Domain Stripping for Active Directory

Starting from Cisco Identity Services Engine, Release 1.2.0.899 cumulative patch 4, you can strip prefixes or suffixes from usernames when Active Directory is used as External Identity Source. You can configure the prefixes or suffixes to be stripped from the usernames by navigating to **Administration > Identity Management > External Identity Sources > Active Directory > Advanced Settings**. Refer to the "Configuring Active Directory as an External Identity Source" section in the *Cisco Identity Services Engine User Guide, Release 1.2* for more information. See Also CSCuj95908, page 31.

Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 4

Table 9 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.2.0.899 cumulative patch 4.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.2, 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.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.2*. for instructions on how to apply the patch to your system.

If you experience problems installing the patch, contact Cisco Technical Assistance Center.

Table 7 Cisco ISE Patch Version 1.2.0.899-Patch 4 Resolved Caveats

Caveat	Description
CSCug90502	ISE Blind SQL Injection Vulnerability This fix addresses an issue where the Cisco Identity Services Engine (ISE) was vulnerable to blind SQL injection. This could allow a remote, authenticated user to modify information in the database. **PSIRT Evaluation** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6/5.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:P/A:P/E:POC/RL:U/RC:C CVE ID CVE-2013-5525 has been assigned to document this issue. Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5525 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
CSCuh84099	ISE should verify non-printable characters in x.509 certificates This fix addresses an issue where ISE was unable to add any endpoints and threw exceptions due to the import of x.509 certificates with non-printable characters.
CSCui22884	ISE presents wrong HTTPS certificate This fix addresses an issue where ISE presented an old HTTPS certificate when user accesses the admin or sponsor GUI even though it has been configured to use a new imported certificate for HTTPS.
CSCui83009	Unable to push compliance module to NAC agent on Macs Fixed an issue where ISE did not push the latest compliance modules to the NAC agent for Macs on the fly like it does with the Windows version.
CSCui94488	MyDevice Portal allows endpoints with static endpoint ID group other than RegisteredDevices This fix addresses an issue where ISE MyDevice Portal is allowed employees to register existing endpoints with a static group assignment other than RegisteredDevices, unless the endpoints already associated with another PortalUser.
CSCuj03131	Lower "Request Rejection Interval" minimum to 5 minutes The minimum length of time for the "Request Rejection Interval" for RADIUS has been lowered to 5 minutes.

Table 7 Cisco ISE Patch Version 1.2.0.899-Patch 4 Resolved Caveats

Caveat	Description
CSCuj28968	Guest Activity Report is not working This fix addresses an issue where the Guest Activity report was blank.
CSCuj39926	Kaspersky remediation does not appear anymore in the AV remediation This fix addresses an issue where Kaspersky remediation did not appear for AV remediation (Posture Results).
CSCuj62435	ISE 1.2 TrendMicro not listed for AV Remediation This fix addresses an issue where Trend Micro was not seen in the AV vendor list when creating an AV Remediation.
CSCuj63046	Text fields impose 24 character limit during guest self-registration This fix addresses an issue where guest users could not enter information into the boxes on the Self Registration page in excess of 24 characters.
CSCuj72022	Cannot use "Ends With" operator in a Posture condition on ISE This fix addresses an error that occurred when the user attempted to create a Posture rule using the ENDS WITH logical operator.
CSCuj90823	Guest Portal: IP Refresh Failing in IE 11 This fix addresses an issue where IP Refresh was not working properly in the Guest Portal due to ActiveX in Internet Explorer 11 for Windows 8.
CSCuj91050	Creating Guest users shows incorrect timezone 'GMT+2 ECT' This fix addresses an issue where Guest user would fail to login with the following error due to an incorrect time zone being assigned to the account: "An internal error occurred. Contact your system administrator for assistance. Contact your system administrator."
CSCuj95908	ISE does not do domain stripping for Active Directory external store This fix addresses an issue where ISE did not allow the modification of the domain name before authentication when the external identity store used is Active Directory.
CSCuh94133	NAC agent with ISE slowly leaking memory after posture This fix addresses the issue where there was a memory leakage in the client machine when NAC Agent was connected to Cisoc ISE after posture.

Support for Windows 8.1 and Mac OS X 10.9 in Cisco ISE Version 1.2.0.899—Cumulative Patch 3

ISE 1.2 Patch 3 supports clients using the Windows 8.1 and Mac OS X 10.9 operating systems.

Please see Open Caveats, page 42 for a workaround for client provisioning using Safari 7 in Mac OS X 10.9.

Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 3

Table 9 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.2.0.899 cumulative patch 3.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.2, 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.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.2*. for instructions on how to apply the patch to your system.

If you experience problems installing the patch, contact Cisco Technical Assistance Center.

Table 8 Cisco ISE Patch Version 1.2.0.899-Patch 3 Resolved Caveats

Caveat	Description
CSCue14864	Endpoint statically assigned to ID group may appear in different group This fix addresses an issue where endpoints that are statically assigned to an Endpoint ID group unexpectedly appear in another group. The issue was that, where authorization profiles are based on ID group, these endpoints may wind up getting assigned the wrong authorization result. This issue had been observed where the administrator creates endpoint identity groups and manually add endpoints to the Cisco ISE database, making them static.
CSCuf47491	Timestamp of core files not preserved in support bundle This fix addresses an issue where core-dump were timestamps not always from when the core dump was created.
CSCug59579	Windows 8 and 8.1 not included in Client Provisioning This fix addresses an issue where Windows 8 is not included in the OS options for Client Provisioning Policies.
CSCuh14228	Internal administrator summary report export not working This fix addresses an issue where the export feature for the Internal administrator summary report was not working.
CSCuh20322	Need ISE application server restart reason and timestamp This fix addresses reformats the timestamp for the show application status ise command in order for the user to determine the uptime of the application.
CSCuh23536	RADIUS drop should have last event timestamp This fix adds a new time stamp column for the radius drops, misconfigured supplicants, and misconfigured network devices log counters
CSCuh30587	Backup fails due to ISE restart This fix addresses an issue where the ISE application server restarts in the middle of a backup because of a local certificate change, which causes the backup to fail. Now, ISE prevents you from restarting the application server if a backup or restore is in progress.

Table 8 Cisco ISE Patch Version 1.2.0.899-Patch 3 Resolved Caveats

Caveat	Description
CSCuh36333	Successful DACL download authentication is counted under authentication dashlet This fix addresses an issue where the authentication dashlet incorrectly included DACL download authentications.
CSCuh45239	Node Status Patch page does not refresh automatically This fix addresses an issue where the Node Status page would not automatically refresh when installing an patch. This fix adds a Refresh button to the page.
CSCui21439	Message code texts are blank or incorrect This fix addresses an issue where the texts for message codes 86009, 86010, 86017, and 86019 were blank and the text for message code 5411 was incorrect. This fix also addresses an issue where the failure reason text for the RADIUS Authentications report did not display properly.
CSCui30275	Fixed an issue where a component of the administration page of the Cisco Identity Services Engine (ISE) was vulnerable to a cross-site scripting (XSS) attack. For additional information on cross-site scripting attacks and the methods used to exploit these vulnerabilities, please refer to the Cisco Applied Mitigation Bulletin "Understanding Cross-Site Scripting (XSS) Threat Vectors", which is available at the following link: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20060922-understanding-xss **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:U/RC:C CVE ID has been assigned to document this issue. Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5505 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
CSCui35514	'show tech' script in support bundle needs fixing This fix addresses errors in the output of the “show tech” script in the support bundle. These errors included: • incorrectly displaying "grep: writing output: Broken pipe" errors • the order not being the same as the 'show tech' output on the ADE OS CLI • the certificate output having a bad new line character (^M), rendering the PEM output unusable unless manually modified
CSCui36643	ISE Editing schedule report complains of existing report name in use This fix addresses an issue where editing a scheduled report returned the error "This schedule name has been used. Please specify a different one.”

Table 8 Cisco ISE Patch Version 1.2.0.899-Patch 3 Resolved Caveats

Caveat	Description
CSCui71484	ISE SEC PAP has write access via ERS API This fix addresses an issue where a provisioning request (add/delete/modify) could be done on SEC PAP via ERS API, although it should have only allowed using a GET method.
CSCui77336	Customized URL ISE self registration not working This fix addresses an issue where ISE Customized web portal self-registration was not working for guest users when using a custom portal with the guestUser.timezone input tag specified in the self-registration html page.
CSCui89741	ISE ERS API creates endpoint with invalid format MAC address This fix addresses an issue where an invalid MAC address format could be added to ISE database by the External RESTful Services API using the CURL command.
CSCui96960	MNT Livelog/Dashboard performance This fix addresses an issue where the Livelog and Dashboard performance in ISE 1.2 suffered when the underlying query ran for a specific MAC address and when there was a large volume of data in the newly-created partition without stats.
CSCuj03071	EndPoint update not being saved to PAP due to high latency This fix addresses an issue where systems with high latency might skip endpoint updates when endpoints are created on PSNs over the WAN from the PAP. For example, Cisco-IP-Phone may appear as Cisco-Device even if the information was collected and endpoint was profiled as Cisco-IP-Phone. This occurred when there was a very high latency (low bandwidth) between PSN to PAP. Around 0.5 seconds time to create an endpoint.
CSCuj03697	Allow Tunnel* attributes in policies This fix addresses an issue where tunnel attributes in the Radius IETF dictionary could not be seen in the pull down when configuring a condition.
CSCuj05295	ISE Application server crashed and stuck in initialized state with “null” in collection filter This fix addresses an issue where ISE crashes and the Application server gets stuck in an initialized state if a Collection Filter is created with value “null.”
CSCuj09430	Guest account is not working according to its Time Zone This fix addresses an issue where a guest account worked only on the time zone of the server, not the user, which affected when a guest could log into the guest portal and when the guest account expired.
CSCuj14382	Cannot statically assign IP address as FramedAddress This fix addresses an issue where assigning a string IP value to an IPV4 attribute resulted in a validation error.
CSCuj15372	Authentications fail with MDM authentication rules enabled This fix addresses an issue where, with MDM authentication rules enabled, all RADIUS authentications fail after several successful runs with the following error message: 5436 RADIUS packet already in the process.

Table 8 Cisco ISE Patch Version 1.2.0.899-Patch 3 Resolved Caveats

Caveat	Description
CSCuj16049	HA Licensing This fix addresses an issue where in the deployment process, once the secondary is promoted as primary, the HA licensing file could not be installed on the promoted secondary.
CSCuj19882	Unable to edit the existing Guest accounts after restoring old backup This fix addresses an issue where you could not edit a guest account from the sponsor portal if the account was created before ISE 1.2 patch 2 was applied.
CSCuj28447	Endpoint statically assigned to ID group may appear in different group This fix addresses an issue where an endpoint statically assigned to an Endpoint ID group may have been seen in another group for no apparent reason. Authorization profiles based on ID group led to the endpoint being assigned the wrong authorization result.
CSCuj45431	ISE Support for Mac OS X 10.9 NAC Agent ISE 1.2 patch 3 supports a NAC Agent for Mac OS X 10.9.
CSCuj45766	Add/Remove MDM server never got replicated to PSNs in distributed deployment This fix addresses an issue where ISE would still use a previously configured MDM server when another MDM server is created as an active MDM or updated as an Active MDM.
CSCuj51094	Captured TCPDump file is not working This fix addresses the issue where you are unable to open the captured TCPDump.pcap file in a program like Wireshark.
CSCuj54630	ISE 1.2 patch 2 is rejecting https cookies from the Mobile Iron Server This fix addresses an issue between ISE 1.2 (899) patch 2 and Mobile Iron Stand Alone (VSP 5.7.1 Build 74). When ISE used the API to check on the status of an endpoint, ISE rejected cookies issued from MI, thus preventing the server from properly identifying what devices are compliant or not. This resulted in the status of "unknown," which prevented access for endpoints that are compliant (via AuthZ rule set).
CSCuj57335	Egress Matrix: require default SGACL that includes log option This fix adds new log functionality to the default Egress rule.
CSCuj60796	ISE Support for IE 11 ISE 1.2 patch 3 supports Internet Explorer 11.
CSCuj70022	EAP-FAST authenticated provisioning with Android doesn't work This fix addresses an issue where ISE TLV failed when parsing a TLV sequence that some versions of Android sent during authenticated provisioning.
CSCuj82378	Downloaded captured TCP dump file for remote node is not of proper size This fix addresses issues with TCP dump files. Previously, the Download button would not respond after running the TCP dump for more than five minutes. Also, an error occurred after downloading the TCP dump file because the file size was incorrect. These issues have been resolved.

New Features in Cisco ISE Version 1.2.0.899—Cumulative Patch 2

Support for Guest Self-Registration Based on Email Domain Whitelist

You can allow guests to create their own accounts by enabling the self-service feature by choosing: **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations > Operations > Guest users should be allowed to do self service**. When you enable this feature, the account credentials display on the screen, and they are also emailed to the email address used to create the account.

You can restrict this feature by limiting guests' ability to create their own accounts based on their email domain. By creating an email domain whitelist, you can ensure that only guest users with email accounts on those domains can create guest accounts.

To prevent the account credentials from displaying on the screen, you must create a custom portal when using an email domain whitelist. These steps provide an overview:

1. Create a custom portal, following these guidelines:
   - Add a required email field and an acceptable use policy (AUP) page to the Self-Registration html file. See the "Sample Code for Sponsor and Guest Portal Customizations" appendix in the *Cisco Identity Services Engine User Guide, Release 1.2* for a sample file.
   - Add text to refer users to their email for their login credentials on the Self-Registration Results html file. See the "Sample Code for Sponsor and Guest Portal Customizations" appendix in the *Cisco Identity Services Engine User Guide, Release 1.2* for a sample file.
   - Map the Login file to the Self-Registration page. See the "Mapping HTML Files to Guest Portal Pages" section in the *Cisco Identity Services Engine User Guide, Release 1.2* for detailed instructions.
2. Configure the SMTP server to support notifications (Administration > System > Settings > SMTP Server).
3. Specify the default e-mail address from which to send all guest notifications. (Administration > System > Settings > SMTP Server and choose **Use Default email address**).
4. Create the email domain whitelist. See the "Restricting Self-Registration Based on Email Domain" section on page 36.
5. Customize the self-registration credentials email message. See the "Customizing the Self-Registration Credentials Email" section on page 37.
6. Customize the self-registration failure message. See the "Customizing the Self-Registration Failure Message" section on page 37

Restricting Self-Registration Based on Email Domain

Before You Begin

- Configure the SMTP server to support notifications (Administration > System > Settings > SMTP Server).
- Specify the default e-mail address from which to send all guest notifications. (Administration > System > Settings > SMTP Server and choose **Use Default email address**).

Step 1 Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations**.

Step 2 Add or edit a guest portal and click **Operations**.

Step 3 Check these options:

- Guest users should be allowed to do self service.
- Send self-registration credentials to whitelisted email domains

Step 4 Enter the allowable domains in the **Whitelisted email domains** field, following these criteria:

- Enter the exact domain name; wildcard characters are not supported.
- Use commas to separate multiple domain names
- The field supports a maximum of 4000 bytes so the total number of supported domains varies, depending on multibyte or unicode requirements.

Step 5 Click **Save**.

Customizing the Self-Registration Credentials Email

You can customize the email message sent to users containing their self-registration login credentials. When customizing this message, be sure to configure it for the languages supported for your guest users. This email is sent to the guest and sponsor using the guest notification language (specified in this setting: Sponsor portal > Edit guest account > Notification language).

Step 1 Choose **Administration > Web Portal Management > Settings > Sponsor > Language Template > English** (or other language) **> Configure Email Notifications > Self-Registration Credentials**.

Step 2 Customize the message and click **Save**.

Customizing the Self-Registration Failure Message

You can customize the error message that displays when users attempt to register using an email account from an unsupported domain.

Step 1 Choose **Administration > Web Portal Management > Settings > Guest > Language Template > English** (or other language) **> Configure Error Messages > Self Service Failed Message**.

Step 2 Customize the message and click **Save**.

Guest Account Expiration Notifications

You can notify guests and sponsors in advance that guests' accounts are close to expiring. Sponsors can then proactively extend the account duration.

These restrictions apply when sending account expiration notifications:

- Notifications are sent only to active accounts. Pending, suspended, and expired accounts will not receive a notification.
- Accounts using the FromFirstLogin time profile will not receive a notification until they have become activated and are in the expiration notification window.
- The timezone of the guest account is used to determine the account expiration.

Configuring Guest Account Expiration Notifications

Step 1 Choose **Administration > Web Portal Management > Settings > Guest > Time Profiles**.

Step 2 Add or edit a time profile.

Step 3 Check these options:

- Send account expiration notification
- Notification time—enter a value between 0 and 336 hours. You must enter a time allowed by the time profile. (For example, if the time profile limits guest access to one week, you might enter 24 to send the expiration notification a day in advance.)
- Send email to guest or Send email to sponsor—you must choose at least one of these options.

Step 4 Click **Save**.

Customizing the Guest Account Expiration Notification

You can customize the messages sent to guests and sponsors to warn them that the guest account is expiring soon. When customizing these messages, be sure to configure it for the languages supported for your guest and sponsor users. This email is sent to sponsors and guests in the language indicated by these settings:

- Sponsors—Sponsor Portal > My Settings > Language template
- Guests—Sponsor portal > Edit guest account > Notification language

Step 1 Choose one of these options:

- Guests—**Administration > Web Portal Management > Settings > Guest > Language Template > English** (or other language) **> Configure Email Notifications > Account Expiration Notification Message**.
- Sponsors—**Administration > Web Portal Management > Settings > Sponsor > Language Template > English** (or other language) **> Configure Email Notifications > Account Expiration Notification Message**.

Step 2 Customize the message to send to sponsors and guests, using these supported variables:

- $guest$—first name of the account or the username if first name is empty
- $username$—login of the guest account
- $firstname$—first name on guest account
- $lastname$—last name on guest account
- $sponsor$—the sponsors login username
- $time$—the time remaining on the account before expiration. Displays as: HH:MM
- $remaininghours$—the remaining number of hours before expiration
- $remainingminutes$—the remaining number of minutes before expiration
- $starttime$—the start date and time of the account. Displays as: EEE dd, MMM yyyy HH:mm. For example: Fri 30, Aug 2013 10:30.
- $endtime$—the end date and time of the account. Displays as: EEE dd, MMM yyyy HH:mm. For example: Fri 30, Aug 2013 10:30.

Step 3 Click **Save**.

Support for Apple iOS 7 in Cisco ISE Version 1.2.0.899—Cumulative Patch 2

ISE 1.2 Patch 2 supports iOS 7 Endpoints for Guest users (Local Web Authentication and Central Web Authentication), as well as BYOD on-boarding. Please note that to ensure iOS 7 endpoint support with ISE 1.2 Patch 2, the WLC needs to be updated to version 7.4.115.0.

The WLC 7.4.115.0 update for these devices:

- Cisco 2504 Wireless Controller
- Cisco 5508 Wireless Controller
- Cisco 8510 Wireless Controller
- Cisco Flex 7510 Wireless Controller
- Cisco Virtual Wireless Controller

can be downloaded by registered users of Cisco.com from this location:
http://software.cisco.com/download/special/release.html?config=fe18b0e824ca3427253bf74fdf50dab9

The WLC 7.4.115.0 update for the Cisco Wireless Services Module 2 (WiSM2) can be downloaded by registered users of Cisco.com from this location:
http://software.cisco.com/download/special/release.html?config=dc3ed2770a7e6d66be495ac1d8cf0cc5

Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 2

Table 9 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.2.0.899 cumulative patch 2.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.2, 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.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.2*. for instructions on how to apply the patch to your system.

If you experience problems installing the patch, contact Cisco Technical Assistance Center.

Table 9 Cisco ISE Patch Version 1.2.0.899-Patch 2 Resolved Caveats

Caveat	Description
CSCuh25868	Authorization policy condition's re-editable text/string limited to 16 characters. This fix addresses an issue where editing an authorization policy's conditions resulted the text box only showing the first 16 characters in a string condition. The remaining characters were replaced by "..."
CSCuh56278	Local Web Authentication (LWA) Guest access by iOS 6 devices on ISE 1.2 fails. This fix ensures that iOS 6 devices are authenticated correctly and gain access to the network appropriately.
CSCui34389	RADIUS accounting drop is not suppressed, flooding live log This fix addresses an issue where message codes for RADIUS accounting drops were not suppressed, resulting with live logs being flooded.
CSCui36160	Whitelist and expiration notification. The new Guest Self-Service feature provides administrators and sponsors the ability to have a customized notification email sent to guest users or sponsors X days before the guest account expires, allowing the sponsor (or guest user in SPP) to update the time profile and extend the account expiration. Self Service Guest accounts have password credentials sent via email, with an additional Email Whitelist feature for validation. **Note** See Support for Guest Self-Registration Based on Email Domain Whitelist, page 36 for more information.
CSCui42788	Exporting of imported profile policy results a garbled description. This fix addresses an issue where exporting an imported policy with a description field resulted in a garbled description field.
CSCui44324	Backup task can't be configured in ISE 1.2 UI. This fix addresses an issue where a scheduled backup couldn't be configured on ISE 1.2 in UI under "Administration -> System -> Backup and restore". After filling all data and clicking on "Save" button, nothing happened. (e.i., neither is a task created nor an error generated).
CSCui56071	ISE: Ignore 0.0.0.0 in Framed-IP-Address Profiler Updates This fix filters incoming Framed-IP-Address that contains zero IP address (0.0.0.0) to reduce replication.
CSCui58390	Multiple names in SAN Field and ISE choose value randomly This fix addresses an issue where the ISE chose the wrong Subject Alternative Name if there are multiple names in the SAN field values in the certificate.
CSCui75335	ISE 1.2 NAC agent fails posture due to 'NAC Server not available' This fix addresses an issue where a NAC agent fails a posture assessment attempt and displayed a "NAC Server not available" error.
CSCuj23727	A change in iOS 7 to the user-agent string for an iPod Touch breaks its BYOD workflow. This fix ensures that an iPod Touch device is recognized as such in a BYOD workflow.

Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 1

Table 10 lists the issues that are resolved in Cisco Identity Services Engine, Release 1.2.0.899 cumulative patch 1.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 1.2, 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.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine User Guide, Release 1.2*. for instructions on how to apply the patch to your system.

If you experience problems installing the patch, contact Cisco Technical Assistance Center.

Table 10 Cisco ISE Patch Version 1.2.0.899-Patch 1 Resolved Caveats

Caveat	Description
CSCui16528	Wrong service selection for NDAC Policy This fix addresses the issue in a Cisco ISE deployment with SGA functionality implemented, where the authentication request was rejected by the Cisco ISE PSN server and the request from the client timed out.

Cisco ISE, Release 1.2, Open Caveats

Open Caveats

Table 11 Cisco ISE, Release 1.2, Open Caveats

Caveat	Description
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 11 Cisco ISE, Release 1.2, 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, Release 1.2, 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.
CSCue17018	MNT node gets messages even after it is out of deployment and is disconnected.

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
CSCue46758	Session expired error occurs during guest authentication. Cisco ISE displays the following error message: `ISE: 86107- Session cache entry missing` For Central Web Authentication, when you configure an authorization profile, and modify the cisco-av-pair (cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa), the user is redirected to the Web Authentication page, but the session expires after the user logs in. **Workaround** Do any one of the following: • Do not replace "ip" in the cisco-av-pair with a value. • Do not modify cisco-av-pair. Instead, configure the Web Authentication option under Common Tasks.
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.
CSCug96069	Replication status update fails for all nodes if the network is restored on PAP. In large scale deployments, where a large number of endpoints are profiled or more authentications happen, the status of one or more PSN nodes is shown as 'Replication Stopped'. Consequently, the data is not published or replicated to other PSN nodes from the PAN node. **Workaround** Restart the PAN.
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.

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
CSCuh07358	Holistic solution is required to resolve Java/SPW issue on Mac OS X/Windows provisioning. While onboarding Mac OS X devices, if Java is not installed, an error message is displayed. This requires the user to install Java and rerun the flow again to onboard the device.
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**.
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.
CSCug26558	In Live Authentications, Posture links redirect to the wrong MAC address and empty report.
CSCuh01760	WLCs in roaming are reported as “Misconfigured NAS” when they generate RADIUS updates intermediately.
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.
CSCuh11909	When trying to select secondary server, the TCP dump displays server error, even though the server is up.
CSCuh12619	BYOD: Device registration is successful even after cancelling the profile installation.
CSCuh13643	While performing posture round trip flow from Mac OS X device, the Agent gets invoked and posture is successful. But the client provisioning page hangs with the message “Determining prior Cisco Agent installation on device”.

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
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.
CSCuh22013	Some endpoint devices like iPAD and iPhone have issues with wildcard certificates when CN is blank.
CSCuh41450	IP columns sorts on char in Network Devices IP columns sort on varchar, which displays the IP addresses in the wrong order.
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.
CSCuh60829	While upgrading from ISE 1.1.1 to ISE 1.2, the Time and Date condition configured as 'All Day' changes to specific hours and it fails for all authentication and authorization policies that use the time based condition.
CSCuh64576	Language Template description and browser Locale Map are not carried over After upgrading to ISE 1.2, the 'Description' and 'Browser Locale Mapping' in the template definition are not carried over for Sponsor, My Devices, and Guest Language template. **Workaround** After the upgrade, set the flags manually.
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.
CSCuh78514	Config Restore including ADE-OS could cause nodes go out of sync In a deployment, nodes are not in sync after ADE-OS restore. **Workaround** After the restore is successful, the nodes need to be synched manually using ISE Administration web UI.
CSCuh84099	On import ISE should verify non-printable characters in x 509 certificates In ise-psc, ISE node throws SSL crypto exceptions and is not able to add any endpoints to the database. **Workaround** Once x 509 certificate is imported to ISE node with non-printable characters, fix the formatting in the certificate as follows: 1. Export the certificate from ISE node 2. De-register the ISE node 3. Remove the white spaces in the certificate 4. Add the updated certificate to ISE by importing it 5. Register the ISE node again

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
CSCuh88557	User password policy attribute migration issue In ACS UI, the **Password may not contain the username or its characters in reversed order** checkbox is enabled and exported to ISE. After importing the policies, the checkbox appears disabled.
CSCuh89530	EAP-TLS authentication failed after upgrade from 1.1.3 to 1.2 After upgrading from ISE 1.1.3 to ISE 1.2 in a two nodes deployment, the EAP-TLS authentication fails.
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.
CSCuh94096	IE9: Register button greyed out when ActiveX is disabled In a Windows 7 client using Internet Explorer 9 with ActiveX disabled, while trying to perform the BYOD flow the browser redirects the user to ‘Device Registration’ page, where the ‘Register’ option is greyed out. **Workaround** Enable the ActiveX to get the Register option properly.
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.
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.
CSCui00069	Standby MnT database is not running and replication stopped. In a 6 node deployment, standby MnT replication stops and database process does not run.

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
CSCui01605	Saving Duplicate policy set which has user defined simple condition fails It is not possible to duplicate and save a policy set that contains user defined simple condition. **Workaround** • Create a new policy set with same user defined simple conditions and save it. OR • Duplicate a policy set with authorization simple condition and delete the user defined simple conditions in the policy set. Create the same condition in the duplicated policy set and save it.
CSCui03041	Device ID does not go to RegisteredDevices group When a laptop with Mac OS X is connected to a network through BYOD flow, both the wired and wireless MAC addresses are listed in 'RegisteredDevices' group. When the same laptop is connected again after cleaning up the profiles and user credentials, only the wireless MAC address is listed in the 'RegisteredDevices' group.
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.
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.
CSCui08084	Guest user not terminated on switch when suspending through edit account When a guest account is suspended using the Suspend option in the Edit page of the Sponsor portal, the guest session is not terminated. **Workaround** Suspend the guests in the Sponsor Portal List page. The suspend button in the List page will terminate sessions for suspended guests.

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
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.
CSCui15633	Sponsor portal login fails for some users
CSCui16373	Upgrading any secondary node from Limited Availability Release to Release 1.2 Fails. This issue occurs only when you upgrade from the Limited Availability release to Cisco ISE, Release 1.2. This issue is seen when you have backup schedules configured in Cisco ISE. **Workaround** Disable or cancel the backup schedules before you upgrade to Release 1.2.
CSCui16876	Default authentication policy matching instead of default dot1x rule When the default policy is modified to 'deny access' and dot1x authentication is performed against PDP with internal user, authentication fails. The authentication matches with 'AllowedProtocolMatchedRule'. **Workaround** Instead of deny access, select identity source/sequence to get authenticated.
CSCui18956	Not able to update the custom RBAC policies after upgrading to Cisco ISE 1.2 After upgrading from Cisco ISE 1.1.x to 1.2, it is not possible to update the RBAC policies, custom menu access and data access permissions that were created in Cisco ISE 1.1.x. **Workaround** 1. Create new menu access permission after upgrading to 1.2 2. Update the RBAC policy created in 1.1.x with the newly created menu access permission and save the policy. 3. Log in with the RBAC user and the updated menus will be displayed.
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.

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
CSCui21839	Export endpoints option results in an empty file with quick or advanced filters turned on, when the filters contain non-alphanumeric characters (such as **:,.**). **Workaround** Export the endpoints either without using the filter or with filter not containing non-alphanumeric characters.
CSCui28492	Registered Endpoints report takes a few minutes. **Workaround** Gather the statistics in CEPM schema and the reports are generated without delay.
CSCui84666	Confusion about the language of the sponsor email notification when using the account expiration feature. **Workaround** See Customizing the Guest Account Expiration Notification, page 38.
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
CSCuj03811	ISE suppresses only messages from NAS that are identical and are sent in sequence.
CSCuj15372	After enabling MDM authorization rules for checking for registration and compliance status, authentications from a RADIUS client that do not include Calling-Station-ID fail after 2 successful authentications.
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.
CSCuj40148	During the BYOD flow the enduser 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.
CSCuj62777	After uninstalling 1.2 Patch 3, the PAP node goes down and doesn't come up, showing HTTP 404 Error in GUI.

Table 11 Cisco ISE, Release 1.2, Open Caveats (continued)

Caveat	Description
CSCuj80131	ISE Client Provisioning - NSP does not launch on Safari 7 (Mac OS X 10.9) Java Applet fails to install SPW/Agent from Client Provisioning page on Safari browser version 7 available with Mac OSX 10.9. Explicitly let it run by changing the website settings on the browser. The default setting encourages users to whitelist individual sites/pages where JAVA is used. **Workaround** To let the applet install agent/SPW, connect to ISE and get re-directed to Client Provisioning page. Before clicking Click to Install Agent, go to: Safari->Preferences->Security->Manage Website Settings->Java->Click on your ISE URL->Run in unsafe mode.
CSCul62723	The Success page on the Mobile Guest Portal redirects the guest to http://10.86.149.92.
CSCum05066	ISE 1.2 patch 5 is not uninstalling from secondary nodes automatically When rolling bac k a patch update using the GUI, it is uninstalled successfully on primary node but is not happening in secondary nodes. On the Primary node, the GUI shows patch is no longer installed in Primary but shows the patch as installed on the secondary node. **Workaround** The user needs to run the rollback again from the Primary GUI.

Open Agent Caveats

Table 12 Cisco ISE, Release 1.2, 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.

Table 12 Cisco ISE, Release 1.2, Open Agent Caveats (continued)

Caveat	Description
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.
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.

Table 12 Cisco ISE, Release 1.2, Open Agent Caveats (continued)

Caveat	Description
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.
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.

Table 12 Cisco ISE, Release 1.2, Open Agent Caveats (continued)

Caveat	Description
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.
CSCtq16716	Windows wireless move from post-posture to pre-posture VLAN detect IP not refreshed The client machine has no connectivity because the NIC's IP address is in the compliant/non-compliant VLAN when it should be in the pre-posture/pending VLAN. This issue has been observed using a wireless supplicant that does not support IP address change when the client machine relies on the Cisco NAC Agent to change the IP address. **Workaround** Disconnect and reconnect wireless NIC on the client machine. For more information, see Known Supplicant Compatibility Issue Involving VLAN Change Operation on Windows Client Machines, page 65.
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.
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.
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.

Table 12 Cisco ISE, Release 1.2, Open Agent Caveats (continued)

Caveat	Description
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.
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.
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

Table 12 Cisco ISE, Release 1.2, Open Agent Caveats (continued)

Caveat	Description
CSCuj26086	Java Applet fails to launch NSP or Mac Agent on Safari 7 browser available with Mac OSX 10.9. **Workaround** Explicitly let it run by changing the website settings on the browser. The default setting encourages users to whitelist individual sites/pages where JAVA is used. To let applet install agent/SPW, connect to ISE and get re-directed to CP page. Before clicking Click to Install Agent, go to: Safari->Preferences->Security->Manage Website Settings->Java->Click on your ISE URL->Run in unsafe mode

Cisco ISE, Release 1.2, Resolved Caveats

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

Resolved Caveats

Table 13 Cisco ISE, Release 1.2, Resolved Caveats

Caveat	Description
CSCtj81255	Two MAC addresses detected on neighboring switch of ACS 1121 Appliance.
CSCtn76441	Custom conditions are not updated under Rules in profiling policies.
CSCtn92594	Quickpicker filters are not working correctly during Client Provisioning policy configuration.
CSCto32002	The Cisco ISE MAC address authentication summary report displays IP addresses instead of MAC addresses.
CSCto87799	Guest authentication fails.
CSCtq06832	Time and Date conditions need to be updated correctly when changing time zones.
CSCtq09004	Windows 7 guest access not successful from IE8 and Chrome 10.
CSCtq53690	Scheduled Monitoring and Troubleshooting incremental backup switches off following failed backup attempt.
CSCtr58811	Need to log out and log back in to get Advanced License functionality.
CSCtr66929	Selected month and year while configuring file “Date” condition.
CSCtr88091	You may experience slow response times for some user interface elements when using Internet Explorer 8.
CSCts45441	Weird behavior with creating guest account using start-end time profile.

Table 13 Cisco ISE, Release 1.2, Resolved Caveats (continued)

Caveat	Description
CSCtt17378	Failed to send notification from UTF-8 Email address.
CSCtu05540	Monitoring and Troubleshooting node does not show Active Directory External Groups following authentication failure.
CSCtv17606	Monitoring and Troubleshooting requires an appropriate error message if backup/restore process fails.
CSCtw79431	Exiting the Cisco Mac Agent while in “pending” state displays the wrong user message.
CSCtw98454	Guest accounting report filter not working.
CSCtx01136	Cisco NAC Agent is not performing posture assessment.
CSCtx03427	Create Alarm Schedule returning XSS error messages.
CSCtx07670	Profiler conditions that are edited wind up corrupting Profiler policies.
CSCtx25213	IP table entry needs cleanup after deregistering a secondary node.
CSCtx31601	Cannot add Network Access user, but able to import users.
CSCtx33747	RBAC admin cannot access deployment page and perform deployment-related functions.
CSCtx51454	Unable to retrieve administrator users list.
CSCtx59957	A warning/pop-up appears while creating a Guest Time profile.
CSCtx74574	Device Configure Deployment option selected after upgrade from software Release 1.0 to Release 1.1.
CSCtx77149	Disk space issue.
CSCtx81905	Cisco ISE returns an error message while registering one node to another.
CSCtx90696	Cisco ISE does not work after updating the IP address.
CSCtx94839	Clicking on logout link on the AUP page of Device Registration Webauth flow appears to do nothing.
CSCtx95251	Deployment page load exceeds six minutes when two or more nodes are unreachable.
CSCtx97190	Cisco 3750 switch is profiled as “Generic Cisco Router”.
CSCty00899	LiveLog Reports cannot be opened.
CSCty02379	Cisco ISE runs out of space due to a backlog of pending messages in the replication queue.
CSCty05157	The Cisco ISE dashboard is not working for administrator user names with more than 15 non-English characters contained in the username.
CSCty10461	Cannot register a Cisco ISE node with UTF-8 characters in administrator name.
CSCty10692	Requirement is used by Policy-Need tooltip on OS.
CSCty15646	Monitoring and Troubleshooting debug log alert settings get reset to WARN.
CSCty16603	Administrator ISE node promotion fails, resulting in disabled replication status.
CSCty19010	Editing Cisco ISE failure reason information returns error message.
CSCty23790	Internet Explorer 8 is unable to import endpoints from LDAP.

Table 13 Cisco ISE, Release 1.2, Resolved Caveats (continued)

Caveat	Description
CSCty40077	Shared Secret Key for Inline Posture node Network Access Device is not created or updated.
CSCty51260	Active Directory "dn" attribute does not work for authorization policies.
CSCty59165	SNMPQuery Probe events queue runs out of memory.
CSCty80451	Failed to authenticate external admin (AD user) when configured user to change password at the next log in.
CSCty98551	Race condition between CoA event and persistence event during initial endpoint login.
CSCtz13306	Monitoring and Troubleshooting collector cannot collect posture audit logs to generate report.
CSCtz28057	After upgrade to Release 1.1, Cisco ISE is still in “initializing” state.
CSCtz41262	Authorization policy does not match when the MAC address uses the colon delimiter (00:00:00:00:00:00).
CSCtz41452	Evaluation license counter incrementing when wireless license installed.
CSCtz49846	Cisco ISE does not contain the ASA attribute 146 Tunnel Group Name that is sent on the Access Request.
CSCtz55815	Default Gateway is not changed if the new value is a part of old value.
CSCtz56691	Research In Motion (Blackberry) devices no longer work after upgrade to Cisco ISE, Release 1.1.1.
CSCtz67814	Replication disabled for secondary node.
CSCua00821	Error messages appear when you configure Active Directory via the CLI.
CSCua03889	Guest users are asked to accept the Acceptable Use Policy twice when first logging into Cisco ISE with password change.
CSCua05003	Service status is not correct if the ARP port number changes.
CSCua05433	The endpoint identity import function does not maintain correct identity group membership.
CSCua25187	Employees whose user names are 41 digits long will not see their devices.
CSCub18575	Problem with sponsor accounts starting with a "0"
CSCuc49317	When you have more than 60 authorization policy rules, creating a new rule takes about 4 minutes.
CSCuc61075	With the RADIUS probe disabled, if you indicate a device as lost or reinstate in the My Devices portal, CoA fails.
CSCuc63052	Policy Service node fails to load client certificate for secure syslog configuration.
CSCuc71592	In policy sets, authorization simple condition cannot be used in authorization policy rules.
CSCuc82453	Monitoring data exported in a .csv file from the primary Administration node is empty.
CSCuc87242	If you disable a sponsor user who has logged in to the sponsor portal, the sponsor user’s account is not disabled until the end of the session.

Table 13 Cisco ISE, Release 1.2, Resolved Caveats (continued)

Caveat	Description
CSCuc92010	Sponsor users who create guest user accounts cannot delete those accounts from the Sponsor Portal.
CSCuc96884	Profiler Feed Service edit and save operations do not work in Internet Explorer 8.
CSCuc97133	Profiler log throws exceptions when you enable FIPS mode on the primary Administration node and FIPS mode is not enabled on the secondary nodes until they are restarted.
CSCud19143	Endpoint filtering does not work for the BYOD Registration and Device Registration Status fields.
CSCud22608	The minimum length of admin and user passwords in the password policy by default becomes four characters, instead of six.
CSCud31778	Policy set page takes a long time to load and save.
CSCud32310	Current Active Sessions report displays an error when the Monitor persona runs on remote node.
CSCud32485	Cannot log in to the sponsor portal after reinstating guest users and accepted the Acceptable Use Policy (AUP).
CSCud38499	Replication of authorization policy fails in a distributed deployment setup if the policy set name includes an underscore (_) character.
CSCud38623	MDM server's Active status does not reflect the connectivity status.
CSCud39871	Cannot save profiler configuration for a secondary node.
CSCud42216	Authentication request from Apple MAC systems that use the EAP-FAST protocol with inner method GTC or TLS fails
CSCud43467	Posture reassessment check functionality is not working when you enable posture reassessment for a group of users. If a user moves to the compliant state, the user gains access to the network, but posture reassessment does not happen, and the user's session gets terminated after a time interval.
CSCue14864	Endpoint statically assigned to ID group may appear in different group
CSCuf03318	The Network Setup Assistant fails when the user tries to "Cancel" the Configure Profile Tool.
CSCuf24898	ISE repository max password length 16 characters
CSCuf47491	Timestamp of core files not preserved in support bundle
CSCug20065	Unable to enforce RBAC as desired to a custom administrator
CSCug59579	Windows 8 not included in Client Provisioning
CSCug59644	Trying dot1X authentication in an Activated Guest with "First Login" time profile fails.
CSCug69311	Not able to connect to SFTP, which is required for secure backups.
CSCug82539	While moving the policies from one profiled node to another, the profiler does not contain the policies in the policy cache.
CSCug90502	ISE Blind SQL Injection Vulnerability
CSCug91963	Java process crashes when configuring host alias.
CSCuh02759	While creating a support bundle, an error message appears as "node not reachable".

Table 13 Cisco ISE, Release 1.2, Resolved Caveats (continued)

Caveat	Description
CSCuh05950	Certificate missed and node disconnected after PAP promotion failed.
CSCuh07534	While downloading the debug logs from Administration node, an error appears as “Node is not reachable. Please check the node's status”.
CSCuh13582	ISE applies wrong Authorization rule/ profile
CSCuh14228	Internal administrator summary report export not working
CSCuh20322	Need ISE application server restart reason and timestamp
CSCuh23536	RADIUS drop should have last event timestamp
CSCuh25506	Cisco ISE CSRF Vulnerability
CSCuh30587	Backup fails due to ISE restart
CSCuh36333	Successful DACL download authentication is counted under authentication dashlet
CSCuh45239	Node Status Patch page does not refresh automatically
CSCuh56278	Local Web Authentication (LWA) Guest access by iOS 6 devices on ISE 1.2 fails
CSCuh65084	Scroll issue for small screens on Live Log page
CSCuh84099	ISE should verify non-printable characters in x.509 certs
CSCuh95845	After internal password change policies using NA conditions match default Policy.
CSCui02984	Sponsor authentication failed for Active Directory user with Sponsor_Portal_Sequence.
CSCui16528	Wrong service selection for NDAC Policy
CSCui21439	Message code texts are blank or incorrect
CSCui22884	ISE presents wrong HTTPS certificate
CSCui26708	ISE node to node HTTP Basic Authentication username and password logged
CSCui30266	ISE MDM Portal Cross-Site Scripting Vulnerability
CSCui30275	Component of the administration page of the Cisco Identity Services Engine (ISE) was vulnerable to a cross-site scripting (XSS) attack
CSCui34389	RADIUS accounting drop is not suppressed, flooding live log.
CSCui35514	'show tech' script in support bundle needs fixing
CSCui36160	Whitelist and expiration notification.
CSCui36643	ISE Editing schedule report complains of existing report name in use
CSCui42788	Exporting of imported profile policy results a garbled description.
CSCui44324	Backup task can't be configured in ISE 1.2 UI.
CSCui46739	Guest applet fails after update to Java 7 update 25
CSCui48779	Clicking ‘Undo Latest’ on Feed Service page does not clean up rules in some conditions.
CSCui56071	ISE: Ignore 0.0.0.0 in Framed-IP-Address Profiler Updates
CSCui57152	Endpoint Policy not updated for endpoints added using ERS API.
CSCui58390	Multiple names in SAN Field and ISE choose value randomly.
CSCui67495	Uploaded Filenames/Content Not Properly Sanitized

Table 13 Cisco ISE, Release 1.2, Resolved Caveats (continued)

Caveat	Description
CSCui67511	Certain File Types are not Filtered and are Executable
CSCui71484	ISE SEC PAP has write access via ERS API
CSCui72269	ISE unable to understand SNMP attribute coming from Switch
CSCui75335	ISE 1.2 NAC agent fails posture due to 'NAC Server not available.'
CSCui77336	Customized URL ISE self registration not working
CSCui83009	Unable to push compliance module to NAC agent on Macs
CSCui89741	ISE ERS API creates endpoint with invalid format MAC address
CSCui94488	MyDevice Portal allows endpoints with static endpoint ID group other than RegisteredDevices
CSCui96960	MNT Livelog/Dashboard performance
CSCuj03071	EndPoint update not being saved to PAP due to high latency
CSCuj03131	Lower "Request Rejection Interval" minimum to 5 minutes
CSCuj03697	Allow Tunnel* attributes in policies
CSCuj05295	ISE App server crashed and stuck in initialized state with "null" in collection filter
CSCuj09430	Guest account is not working according to its Time Zone
CSCuj14382	Cannot statically assign IP address as FramedAddress
CSCuj15372	Authentications fail with MDM authentication rules enabled
CSCuj16049	HA Licensing
CSCuj19882	Unable to edit the existing Guest accounts after restoring old backup
CSCuj28447	Endpoint statically assigned to ID group may appear in different group
CSCuj28968	Guest Activity Report is not working
CSCuj39926	Kaspersky remediation does not appear anymore in the AV remediation
CSCuj45431	ISE Support for Mac OS X 10.9 NAC Agent
CSCuj45766	Add/Remove MDM server never got replicated to PSNs in distributed deployment
CSCuj48111	Hyphen and minus sign can't be entered as first or last name
CSCuj51094	Captured TCPDump file is not working
CSCuj54630	ISE 1.2 patch 2 is rejecting https cookies from the Mobile Iron Server
CSCuj57335	Egress Matrix: require default SGACL that includes log option
CSCuj60796	ISE Support for IE 11
CSCuj61976	Admin UI fails to display certain UI pages when using Firefox 25
CSCuj62435	ISE 1.2 TrendMicro not listed for AV Remediation
CSCuj63046	Text fields impose 24 character limit during guest self-registraion
CSCuj70022	EAP-FAST authenticated provisioning with Android doesn't work
CSCuj72022	Cannot use "Ends With" operator in a Posture condition on ISE
CSCuj82836	Manual CoA - Re-authorization is not working
CSCuj84194	ISE sometimes does not send DACL in authorization profile

Table 13 Cisco ISE, Release 1.2, Resolved Caveats (continued)

Caveat	Description
CSCuj90823	Guest Portal: IP Refresh Failing in IE 11
CSCuj91050	Creating Guest users shows incorrect timezone 'GMT+2 ECT'
CSCuj95908	ISE does not do domain stripping for Active Directory external store
CSCuj98726	iOS devices bypass account suspension/lock by starting new EAP session
CSCul02860	Struts Action Mapper Vulnerability
CSCul03127	Struts 2 Dynamic Method Invocation Vulnerability
CSCul03621	Endpoint Profiling Information is not being replicated correctly
CSCul06431	Active Directory attribute value in ATZ profile is not sent
CSCul13757	Audit records MUST log to External Syslog Servers: CLI log level
CSCul13805	Audit records MUST log to External Syslog Servers: HTTPS idle timeout
CSCul13812	Audit records MUST log to External Syslog servers: SSH publickey
CSCul13883	Audit records MUST log to External Syslog servers: SSH KEX Group14
CSCul13905	Audit records MUST log to External Syslog Servers: CLI clock set
CSCul13946	Audit records MUST log to External Syslog servers: Purge M&T Data
CSCul15967	ISE 1.2 Patch 3 Windows 8.1 CPP OS Detection Failure in Distributed Setup
CSCul16300	Audit records MUST log to External Syslog servers: CLI idle timeout
CSCul18169	Blocking ISE admin UI access for Chrome browser
CSCul18521	Audit records MUST log to External Syslog servers: VGA CLI AUTHC
CSCul18555	Audit records MUST log to External Syslog servers: SSH conn fail
CSCul23070 CSCul23252	Audit records MUST log to External Syslog Servers: SSH exit forceout
CSCul42646	Failed to create Posture Condition with "NOT ENDS WITH" Operator
CSCul46893	URL preservation not working with self service guest user in MAB flow
CSCul58758	Redirecting to 'null' page in the browser after LWA flow with WLC-5500

Resolved Agent Caveats

Table 14 Cisco ISE, Release 1.2, Resolved Agent Caveats

Caveat	Description
CSCto03644	Tray icon flickers click focus if user changes applications from login successfully.
CSCto19507	Mac OS X agent does not prompt for upgrade when coming out of sleep mode.
CSCto97422	Auto Popup does not happen after clicking **Cancel** during remediation failure.
CSCug26558	Live Authentications: Posture links redirect to wrong MAC address and empty report
CSCue98661	Cisco ISE NAC Agent on Windows 8 checks for AV that is not selected
CSCue41912	Posture: Cisco NAC Agent not triggering on Windows 8

Resolved SPW Caveats

Table 15 Cisco ISE, Release 1.2, Resolved SPW Caveats for Windows

Caveat	Description	SPW Version
CSCug95980	Cisco ISE NSP does not support SDIO based wireless adapters.	1.0.0.31
CSCug66885	Windows SPW-Trusted Root CA not set in network profile.	1.0.0.30
CSCud65260	DualSSID_Win7_PEAP_AutoLogin NSP not connecting to Closed SSID.	1.0.0.29
CSCud01247	BYOD: Messages are not localized.	1.0.0.28
CSCud56448	PEAP Supplicant Provisioning does not set Validate Server Certificate.	1.0.0.28
CSCue38943	BYOD: Characters corrupted. A vertical line appears at the end of the Applying Configuration screen.	1.0.0.28
CSCue43405	Windows 8- Dual SSID is broken (MAB + PEAP), if wrong networking password is entered in SPW.	1.0.0.28
CSCue43413	Login failure message displayed in dual SSID (MAB + PEAP).	1.0.0.28
CSCue47503	Win SPW v1.0.0.27 fails with Wired dual SSID (MAB > PEAP).	1.0.0.28
CSCud05296	NSP installation on Windows 8 failed.	1.0.0.26

Table 16 Cisco ISE, Release 1.2, Resolved SPW Caveats for Mac OS X

Caveat	Description	SPW Version
CSCuf61159	Wired MAC10.8.3-Fails to auto re-connect to network using new profile.	1.0.0.21
CSCug16632	BYOD CR: SPW configures the profile and succeeds even when PDP is down.	1.0.0.20
CSCug18081	NSP page does not show status of Mac SPW consistently.	1.0.0.20
CSCuf03318	Network Setup Assistant fails, if user clicks ‘Cancel’ in the Config profile Tool.	1.0.0.19
CSCue53450	Cisco Network Setup Assistant copy right year should be changed.	1.0.0.19
CSCue62005	Macintosh SPW 1.0.0.17 is not able to configure wired adapters.	1.0.0.18
CSCud00349	Translation property file has new line character in the JA translation property file.	1.0.0.17
CSCud64592	MAC OS X 10.6.8: Fails to connect to Closed SSID using the TSL Profile.	1.0.0.16
CSCub29212	In MAC OS X 10.8, modify system network configuration needs confirmation from system administrator.	1.0.0.15
CSCuc42511	Localization for NSP wizards - support for additional languages.	1.0.0.14
CSCub27769	Cisco ISE does not block both wired and wireless interface MAC addresses for lost devices.	1.0.0.13

Table 16 Cisco ISE, Release 1.2, Resolved SPW Caveats for Mac OS X

Caveat	Description	SPW Version
CSCub65963	Certificate Enrollment is vulnerable to session Hija.	1.0.0.12
CSCub29185	MAC 10.8: Agent and SPW fails to install, when "MAC App Store and identified developers" is selected in the Security & Privacy Preference Pane.	1.0.0.11

Other Known Issues

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.

Windows Internet Explorer 8 Known Issues

Issue Accessing the Cisco ISE Administrator User Interface

When you access the Cisco ISE administrator user interface using the host IP address as the destination in the Internet Explorer 8 address bar, the browser automatically redirects the session to a different location. This situation occurs when you install a real SSL certificate issued by a certificate authority like VeriSign.

If possible, we recommend using the Cisco ISE hostname or fully qualified domain name (FQDN) that was used to create the trusted SSL certificate to access the administrator user interface via Internet Explorer 8.

User Identity Groups Issue

If you create and operate 100 or more User Identity Groups, a script in the Cisco ISE administrator user interface can cause Internet Explorer 8 to run slowly, looping until a pop-up appears asking you if you want to cancel the running script. (If the script continues to run, your computer might become unresponsive.)

Known Supplicant Compatibility Issue Involving VLAN Change Operation on Windows Client Machines

There is a known issue with the Intel Supplicant version 12.4.*x* for Windows client machines with regard to a VLAN change for wireless deployments. The client machine has no connectivity because the NIC IP address is in the compliant/non compliant VLAN when it should be in the pre posture/pending VLAN.

Note This issue affects any supplicant that cannot perform an IP address refresh on a VLAN change in a wireless environment. This issue is related to the VLAN detect (Access VLAN to Authentication VLAN change) functionality, where the Cisco NAC Agent is not working correctly with wireless adapters.

For more information, see CSCtq16716, page 54.

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.

BYOD Connectivity Issue with Devices running Windows 7

Devices running Windows 7 operating system do not connect by default if "invalid" security certificate is presented from the server side. This issue is seen if self-signed certificates are in use, or if the certificate is signed by a root CA, which is not in the trusted list of the client.

Workaround for this issue is to create a PEAP network profile before connecting to the Single SSID BYOD network. After a PEAP network profile is created, Windows 7 displays a user prompt.

Documentation Updates

Table 17 Updates to Release Notes for Cisco Identity Services Engine, Release 1.2

Date	Description
1/22/2014	Added Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 5, page 23
12/20/2013	• Added Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 5, page 23 • Updated Open Caveats, page 42
12/5/2013	Added No iPEP Support in Cisco ISE 1.2 Patches, page 10

Table 17 Updates to Release Notes for Cisco Identity Services Engine, Release 1.2

Date	Description
11/27/2013	• Added Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 4, page 29 • Updated Open Caveats, page 42 • Updated Open Agent Caveats, page 51
10/29/2013	• Added Support for Windows 8.1 and Mac OS X 10.9 in Cisco ISE Version 1.2.0.899—Cumulative Patch 3, page 31 • Updated Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 3, page 32
10/28/2013	Added Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 3, page 32
9/19/2013	• Added New Features in Cisco ISE Version 1.2.0.899—Cumulative Patch 2, page 36 • Added Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 2, page 39
8/1/2013	Added Resolved Issues in Cisco ISE Version 1.2.0.899—Cumulative Patch 1, page 41
7/25/2013	Cisco Identity Services Engine, Release 1.2

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 18 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.2	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
Cisco Identity Services Engine Network Component Compatibility, Release 1.2	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
Cisco Identity Services Engine User Guide, Release 1.2	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.2	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Upgrade Guide, Release 1.2	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html

Table 18 Product Documentation for Cisco Identity Services Engine (continued)

Document Title	Location
Cisco Identity Services Engine, Release 1.2 Migration Tool Guide	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.2	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.2	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.2	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_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/en/US/products/ps11640/prod_installation_guides_list.html
Cisco ISE In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps11640/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/en/US/products/ps11640/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/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC Appliance
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC Guest Server
  http://www.cisco.com/en/US/products/ps10160/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.