



Release Notes for Cisco Identity Services Engine, Release 1.0.4

Revised: August 14, 2013, OL-25482-01

Contents

These release notes describe the features, limitations and restrictions (caveats), and related information for Cisco Identity Services Engine (ISE) Maintenance Release 1.0.4. These release notes supplement the Cisco ISE documentation that is included with the product hardware and software release, and cover the following topics:

- [Cisco Identity Services Engine Releases, page 2](#)
- [Introduction, page 2](#)
- [Node Types, Personas, Roles, and Services, page 2](#)
- [Hardware Requirements, page 4](#)
- [Installing Cisco ISE Software, page 7](#)
- [Upgrading Cisco ISE Software, page 9](#)
- [Cisco Secure ACS to Cisco ISE Migration, page 10](#)
- [Cisco ISE License Information, page 10](#)
- [Key Features in Maintenance Release 1.0.4, page 11](#)
- [Cisco ISE Install Files, Updates, and Client Resources, page 14](#)
- [Cisco ISE Antivirus and Antispyware Support, page 17](#)
- [Cisco ISE Patch Release Updates, page 17](#)
- [Cisco ISE Release 1.0.4 Open Caveats, page 22](#)
- [Cisco ISE Release 1.0.4 Resolved Caveats, page 51](#)
- [Known Issues, page 52](#)
- [Documentation Updates, page 55](#)
- [Related Documentation, page 57](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Identity Services Engine Releases

Date	Release
18 May, 2011	Cisco Identity Services Engine Release 1.0.0.377
26 August, 2011	Cisco Identity Services Engine Maintenance Release 1.0.4.558
30 September, 2011	Cisco Identity Services Engine Maintenance Release 1.0.4.573

Introduction

The Cisco ISE platform is a comprehensive, next-generation, contextually-based access control solution. Cisco ISE offers authenticated network access, profiling, posture, guest management, and security group access services along with monitoring, reporting, and troubleshooting capabilities on a single physical or virtual appliance. Cisco ISE ships on a range of physical appliances with different performance characterization and also allows the addition of more appliances to a deployment for performance, scale, and resiliency. Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. Cisco ISE also allows for configuration and management of distinct Cisco ISE personas and services. This feature gives you the ability to create and apply Cisco ISE services where they are needed in the network, but still operate the Cisco ISE deployment as a complete and coordinated system.

Node Types, Personas, Roles, and Services

Cisco ISE provides a highly available and scalable architecture that supports both standalone and distributed deployments. In a distributed environment, you configure one primary Administration node and the rest are secondary nodes. The topics in this section provide information about Cisco ISE terminology, supported node types, distributed deployment, and the basic architecture.

Cisco ISE Deployment Terminology

[Table 1-1](#) describes some of the common terms used in Cisco ISE deployment scenarios.

Table 1-1 *Cisco ISE Deployment Terminology*

Term	Description
Service	A service is a specific feature that a persona provides such as network access, profiler, posture, security group access, and monitoring.
Node	A node is an individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as a 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.
Node type	A node can be of two types: ISE node and Inline Posture node. The node type and persona determine the type of functionality provided by that node.

Table 1-1 Cisco ISE Deployment Terminology

Term	Description
Persona	The persona or personas of a node determine the services provided by a node. An Cisco ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring.
Role	Determines if a node is a standalone, primary, or secondary node. Applies only to Administration and Monitoring nodes.

Types of Nodes

A Cisco ISE network has only two types of nodes:

- Cisco ISE node—An ISE node could assume any of the following three personas:
 - Administration—Allows you to perform all administrative operations on Cisco ISE. It handles all system-related configuration and configurations related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have only one or a maximum of two nodes running the Administration persona. The Administration persona can take on any one of the following roles: standalone, primary, or secondary. 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, posture, 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 would be more than one Policy Service persona in a distributed deployment. All Policy Service personas that reside behind a load balancer share a common multicast address and 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 the log collector and store log messages from all the Administration and Policy Service personas on the 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 you with meaningful information in the form of reports. Cisco ISE allows you to have a maximum of two nodes with this persona that can take on 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.

- Inline Posture node—A gatekeeping node that is positioned behind network access devices such as wireless LAN controllers (WLCs) and virtual private network (VPN) concentrators on the network. Inline Posture enforces access policies after a user has been authenticated and granted access, and

handles Change of Authorization (CoA) requests that a WLC or VPN are unable to accommodate. Cisco ISE allows you to have two Inline Posture nodes that can take on primary or secondary roles for high availability.

**Note**

An Inline Posture node is dedicated solely to that service, and cannot operate concurrently with other 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 ISE node in a deployment can assume more than one of the three personas (Administration, Policy Service, or Monitoring) at a time. By contrast, each Inline Posture node operates only in a dedicated gatekeeping role.

In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration nodes
- Primary and secondary Monitoring nodes
- One or more Policy Service nodes
- One or more Inline Posture nodes

You can change the persona of a node. See the “Setting Up ISE in a Distributed Environment” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4* for information on how to configure these personas on Cisco ISE nodes.

Hardware Requirements

This section describes the following topics:

- [Supported Hardware, page 5](#)
- [Supported Virtual Environments, page 7](#)
- [Supported Browsers, page 7](#)
- [Cisco ISE License Information, page 10](#)
- [Additional Support Information, page 7](#)

**Note**

For more details on Cisco ISE hardware platforms and installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4*.

Supported Hardware

Cisco ISE software is packaged with your appliance or image for installation. After installation, you can configure Cisco ISE as any of the specified component personas (Administration, Policy Service, and Monitoring) or as an Inline Posture node on the platforms that are listed in [Table 2](#).

Table 2 **Supported Hardware and Personas**

Hardware Platform	Persona	Configuration
Cisco ISE-3315-K9 (small)	Any	<ul style="list-style-type: none"> • 1x Xeon 2.66 GHz quad-core processor • 4 GB RAM • 2 x 250 GB SATA¹ HDD² • 4x 1 GB NIC³
Cisco ISE-3355-K9 (medium)	Any	<ul style="list-style-type: none"> • 1x Nehalem 2.0 GHz quad-core processor • 4 GB RAM • 2 x 300 GB 2.5 in. SATA HDD • RAID⁴ (disabled) • 4x 1 GB NIC • Redundant AC power
Cisco ISE-3395-K9 (large)	Any	<ul style="list-style-type: none"> • 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 2 **Supported Hardware and Personas (continued)**

Hardware Platform	Persona	Configuration
Cisco ISE-VM-K9 (VMware)	Stand-alone Administration, Monitoring, and Policy Service (no Inline Posture)	<ul style="list-style-type: none"> • CPU—Intel Dual-Core; 2.13 GHz or faster • Memory—4 GB RAM⁵ • Hard Disks (minimum allocated memory): <ul style="list-style-type: none"> – Stand-alone—200 GB – Administration—200 GB – Policy Service and Monitoring—200 GB – Monitoring—200 GB – Policy Service—60 GB <p>Note Cisco does not recommend allocating any more than 600 GB maximum space for any node.</p> <ul style="list-style-type: none"> • NIC—1 GB NIC interface required (4 NICs are recommended) • Supported VMware versions include: <ul style="list-style-type: none"> – ESX 4.x – ESXi 4.x <p>Note For an evaluation or production version, the minimum disk space is 60 GB.</p>

1. SATA = Serial Advanced Technology Attachment

2. HDD = hard disk drive

3. NIC = network interface card

4. RAID = redundant array of independent disks

5. 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 Server v2.0 (Demo Only)
- VMware ESX 4.x
- VMware ESXi 4.x

Supported Browsers

You can access the Cisco ISE administrative user interface using the following browsers:

- Mozilla Firefox 3.6
- Microsoft Internet Explorer 8

Additional Support Information

Refer to [Cisco Identity Services Engine Network Component Compatibility, Release 1.0.4](#) for information on supported devices and agents.

Installing Cisco ISE Software

The following steps summarize how to install new Cisco ISE Release 1.0.4 DVD software on supported hardware platforms (see [Supported Hardware, page 5](#) for support details).

With Cisco ISE Release 1.0.4, installation occurs in two phases:

1. The software is installed from the DVD, and when complete, the DVD is ejected from the appliance.
2. The administrator logs in and performs the initial configuration.

-
- | | |
|---------------|---|
| Step 1 | Log into Cisco Download Software at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm . You might be required to provide your Cisco.com login credentials. |
| Step 2 | Navigate to Security > Identity Management > Cisco Identity Services Engine > Cisco Identity Services Engine Software . |
| Step 3 | Download the appropriate Cisco ISE .ISO image (for example, ise-1.0.4.573.i386.iso) and burn the image as a bootable disk to a DVD-R. |
| Step 4 | Insert the DVD into the DVD-R drive of each appliance, and reboot the appliance to initiate the Cisco ISE DVD installation process. |
| Step 5 | (If necessary) Install a valid FlexLM product license file and perform Cisco ISE initial configuration according to the instructions in the Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4 . Before you run the setup program, ensure that you know the configuration parameters listed in Table 3 . |
-

Table 3 *Identity Services Engine Network Configuration Parameters for Setup*

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumeric (A-Z, a-z, 0-9), hyphen (-), with a requirement that the first character must be an alphabetic character. Note Cisco does not recommend using mixed case and hyphens in the hostname.	ise-node1
(eth0) Ethernet interface address	Must be a valid IPv4 address for the eth0 Ethernet interface.	10.12.13.14
Netmask	Must be a valid IPv4 address for the 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 numbers, hyphen (-), and 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 NTP server in a domain reachable from Cisco ISE. ¹	clock.nist.gov
Add/Edit another NTP server	Must be a valid NTP server in a domain reachable from Cisco ISE. ¹	(Optional) Allows you to configure multiple NTP servers. To do so, enter y to continue.
System Time Zone	Must be a valid time zone. Refer to the Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4 for a table of time zones that Cisco ISE supports. The default value is UTC. ² Note The table lists the frequently used time zones. You can run the show timezone command from the Cisco ISE CLI for a complete list of supported time zones.	UTC
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default, you must create a new username, which must be from 3 to 8 characters in length, and be composed of valid alphanumeric characters (A-Z, a-z, or 0-9).	admin (default)
Password	Identifies the administrative password 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), at least one uppercase letter (A-Z), and at least one number (0-9).	MyIseYP@@ss

Table 3 **Identity Services Engine Network Configuration Parameters for Setup (continued)**

Prompt	Description	Example
Database Administrator Password	Identifies the Cisco ISE database system-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9). Note Once you configure this password, Cisco ISE uses it “internally.” That is, you do not have to enter it when logging into the system at all.	ISE4adbp@ss
Database User Password	Identifies the Cisco ISE database access-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9). Note Once you configure this password, Cisco ISE uses it “internally.” That is, you do not have to enter it when logging into the system at all.	ISE5udbp@ss

1. Changing the NTP server specification after Cisco ISE installation will likely affect the entire deployment.
2. Changing the time zone specification after Cisco ISE installation will likely affect the entire deployment.

**Note**

For additional information on configuring and managing Cisco ISE, use the list of documents in [Release-Specific Documents, page 57](#) to access other documents in the Cisco ISE documentation suite.

Upgrading Cisco ISE Software

If you installed Cisco Identity Services Engine Release 1.0 or Cisco Identity Services Engine Maintenance Release 1.0.4.558 previously and are planning to upgrade to the latest Cisco ISE Maintenance Release 1.0.4, be sure to follow the upgrade instructions in the “Upgrading Cisco ISE” chapter of the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4](#).

**Note**

There is a known issue regarding default “admin” administrator user interface access following upgrade from Cisco Identity Services Engine Release version 1.0.3.377 to Cisco Identity Services Engine Maintenance Release 1.0.4.573. See [Known Issue with Upgrade from Cisco ISE Release 1.0.3.377, page 53](#) for details.

**Note**

If you want to replace a Cisco ISE appliance running Cisco Identity Services Engine Maintenance Release 1.0.4.558 with a new Cisco ISE running Cisco Identity Services Engine Maintenance Release 1.0.4.573, you must upgrade the appliance running version 1.0.4.558 to 1.0.4.573 before creating a database backup image, which you can then restore on the new appliance running version 1.0.4.573.

Cisco Secure ACS to Cisco ISE Migration


Note

You *must* upgrade your Cisco Secure ACS deployment to Release 5.1 or 5.2 before you attempt to perform the migration process to Cisco Identity Services Engine.

After you have moved your Cisco Secure ACS 5.1 or 5.2 database over, you will notice some differences in existing data types and elements as they appear in the new Cisco Identity Services Engine Maintenance Release 1.0.4.573 environment.

The only currently supported browser for downloading the migration tool files is Firefox version 3.6.x. Microsoft Windows Internet Explorer (IE8 and IE7) browsers are not currently supported in this release.

Complete instructions for moving your Cisco Secure ACS 5.1 or 5.2 database to Cisco Identity Services Engine Maintenance Release 1.0.4.573 are covered in the [Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4](#).

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 your Cisco ISE. [Table 4](#) summarizes the Cisco ISE license types. (Although the evaluation license allows you to provide support for both wired and wireless users, purchasing and applying a Wireless License option cuts off support for any wired users you may have been supporting during the evaluation period.)

Table 4 *Cisco ISE License Types and Supported Services*

Cisco ISE License Type	Supported Services
Base package—Provides authenticated network access, guest life-cycle management, and advanced monitoring and troubleshooting.	<ul style="list-style-type: none"> Basic Network Access Guest Management Link encryption
Advanced package—Provides posture, profiling, advanced monitoring and troubleshooting, and security group access services. You cannot add advanced licenses before adding base licenses, and the number of advanced licenses cannot exceed the number of base licenses.	<ul style="list-style-type: none"> Profiler Posture Security Group Access
Wireless package—Provides a flexible option to exclusively wireless service providers that not only offers the essential Base License functions like basic network access (authentication and authorization), Guest services, and link encryption, but also all Advanced License services, including Profiler, Posture, and Security Group Access services.	<ul style="list-style-type: none"> Basic Network Access Guest Management Link encryption Profiler Posture Security Group Access

**Note**

Wireless Licenses cannot coexist on an Administration ISE node with Base or Base and Advanced Licenses.

Licenses are centrally managed by the Administration ISE node. In a distributed deployment, where two Cisco ISE nodes assume the Administration persona (primary and secondary), upon successful installation of the license file, the licensing information from the primary Administration node is propagated to the secondary Administration node. So there is no need to install the same license on each Administration node within the deployment.

For more detailed information on license types and obtaining licenses for Cisco ISE, see “Performing Post-Installation Tasks” chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4*.

For specific information on adding, modifying, and removing license files, see the “Managing Licenses” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*.

For detailed information and license part numbers available for Cisco ISE, including licensing options for new installations as well as migration from an existing Cisco security product like Cisco Secure Access Control System, see the Cisco Identity Services Engine Ordering Guidelines at http://www.cisco.com/en/US/products/ps11195/prod_bulletins_list.html.

Key Features in Maintenance Release 1.0.4

Cisco ISE Maintenance Release 1.0.4 offers the following features and services:

- [Cisco ISE Installation and Upgrade Process Updates, page 11](#)
- [Wireless License Options, page 12](#)
- [Cisco ISE Upgrade and Backup and Restore Enhancements, page 12](#)
- [Administrator Lockout and Administrator Password Reset, page 12](#)
- [Windows IE 9 and Firefox 4.x Browsers Support, page 12](#)
- [Statically Assigned Endpoint Behavior Enhancement, page 13](#)
- [Correlating Endpoint IP and MAC Addresses with DHCP and RADIUS Probes, page 13](#)
- [Integrating with Cisco NAC Appliance, Release 4.9, page 13](#)
- [Cisco Secure ACS to Cisco ISE Migration Updates, page 13](#)

For more information on key features of Cisco ISE, see the Overview chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*.

Cisco ISE Installation and Upgrade Process Updates

Cisco has updated the installation and upgrade processes in Cisco Identity Services Engine Maintenance Release 1.0.4. During fresh installation of the 1.0.4.573 .ISO image and upgrade from 1.0.3.377 or 1.0.4.558, Cisco ISE now asks you to specify and verify database administrator and user passwords that protect database communication access among multiple Cisco ISE nodes in a distributed deployment.

For more details, see:

- The “Configuring the Cisco ISE 3300 Series Appliance” and “Upgrading Cisco ISE” chapters of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4*

- The [Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4](#)

**Note**

If you want to replace a Cisco ISE appliance running Cisco Identity Services Engine Maintenance Release 1.0.4.558 with a new Cisco ISE running Cisco Identity Services Engine Maintenance Release 1.0.4.573, you must upgrade the appliance running version 1.0.4.558 to 1.0.4.573 before creating a database backup image, which you can then restore on the new appliance running version 1.0.4.573.

Wireless License Options

The new Wireless License options available in Cisco ISE Maintenance Release 1.0.4 enable the same number of endpoints on both the existing Base and Advanced license package. However, the devices that are supported with this type of license are restricted to wireless devices. It is possible to subsequently remove this restriction by installing a Wireless Upgrade license that enables the base and advanced package feature support for all types of devices.

For more information on the new Wireless License options, see the “Performing Post-Installation Tasks” chapter of the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4](#).

Cisco ISE Upgrade and Backup and Restore Enhancements

The Cisco ISE, Release 1.0.4 implements the upgrade of Cisco ISE from a previous release that has patches already installed on it or from any maintenance release. You can upgrade Cisco ISE 1.0 release to Cisco ISE Maintenance Release 1.0.4. In addition, you can also migrate from Cisco Secure Access Control System (ACS) 5.1 and 5.2 releases to Cisco ISE, Release 1.0. After you migrate to Cisco ISE, Release 1.0, you can then upgrade Cisco ISE to the latest release.

For more information on the upgrade and backup procedures, see the “Upgrading Cisco ISE” chapter of the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4](#).

Administrator Lockout and Administrator Password Reset

In Cisco ISE, Release 1.0.4, if you enter an incorrect password for your specified administrator user ID enough times, the Cisco ISE user interface “locks you out” of the system, adds a log entry in the **Monitor > Reports > Catalog > Server Instance > Server Administrator Logins** report, and suspends the credentials for that administrator ID until you have an opportunity to reset the password associated with that administrator ID. The number of failed attempts required to disable the administrator account is configurable according to the guidelines described in the “Configuring a Password Policy for Administrator Accounts” section of the “Administering Cisco ISE” chapter of the [Cisco Identity Services Engine User Guide, Release 1.0.4](#).

The instructions on how to reset the “locked” administrator password are described in the “Performing Post-Installation Tasks” chapter of the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4](#).

Windows IE 9 and Firefox 4.x Browsers Support

The Cisco ISE, Release 1.0.4 supports Windows IE 9 and Firefox 4.x browsers for the client and sponsor portals.

For more information on the supported browsers and OS, see [Cisco Identity Services Engine Network Component Compatibility, Release 1.0.4](#).

Statically Assigned Endpoint Behavior Enhancement

The Cisco ISE, Release 1.0.4 implements a change that Cisco ISE cannot consume advanced licenses when endpoints are statically assigned to a profile. The number of endpoints that are dynamically profiled can only be compared against the limit of the advanced licenses. The endpoints that are statically assigned to a profile are now excluded from utilizing licenses included in the advanced license package, but they are still compared against the limit of base licenses. Earlier in the Cisco ISE, Release 1.0, it compares the total number of concurrent endpoints across the entire deployment against the limit of the advanced licenses.

Correlating Endpoint IP and MAC Addresses with DHCP and RADIUS Probes

The Cisco ISE, Release 1.0.4 implements an ARP cache in the profiler service so that you can reliably map IP addresses and MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry IP addresses and MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints along with their MAC addresses, which can be mapped and stored in the ARP cache.

Integrating with Cisco NAC Appliance, Release 4.9

The Cisco ISE, Release 1.0.4 now supports integration with Cisco Network Admission Control (NAC) Appliance, Release 4.9. The integration support is compatible only with the Cisco NAC Appliance, Release 4.9 and available when you have installed an advanced or wireless license on the maintenance release of Cisco ISE.

Integrating Cisco ISE, Release 1.0.4 with Cisco NAC Appliance, Release 4.9 allows you to utilize the Cisco ISE profiler services in a Cisco NAC deployment. The Cisco ISE profiler is similar to the Cisco Network Admission Control (NAC) Profiler in a Cisco NAC deployment, which manages endpoints in an enterprise network. This integration allows you to replace the existing Cisco NAC Profiler that is installed in a Cisco NAC deployment. It allows you to synchronize profile names from the Cisco ISE profiler, as well as the result of endpoint classification into the Cisco Clean Access Manager (CAM).

Cisco Secure ACS to Cisco ISE Migration Updates

Authentication and Authorization policies are not migrated. It is the responsibility of the administrator performing migration to define the policies manually.

For more information on the migration policies, see [Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4](#).

Cisco ISE Install Files, Updates, and Client Resources

There are three resources you can use to download installation packages, update packages, and other client resources necessary to provision and provide policy service in Cisco ISE:

- [Cisco ISE Downloads from the Cisco Download Software Center, page 14](#)
- [Cisco ISE Live Updates, page 14](#)
- [Cisco ISE Offline Updates, page 15](#)

Cisco ISE Downloads from the Cisco Download Software Center

In addition to the .ISO installation package required to perform a fresh installation of Cisco ISE on your appliance as described in [Installing Cisco ISE Software, page 7](#), you can use the same software download location to retrieve other vital Cisco ISE software elements, like Windows and Mac OS X agent installers and AV/AS compliance modules. Use this portal to get your first software packages prior to configuring your Cisco ISE deployment.



Note

The 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 from Cisco:

-
- Step 1** Log into Cisco Download Software at <http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>. You might be required to provide your Cisco.com login credentials.
- Step 2** Navigate to **Security > Identity Management > 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
 - 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 Now** or **Add to Cart** for any of the software items you require to set up your Cisco ISE deployment.
-

Cisco ISE Live Updates

Cisco ISE Live Update locations allow you to automatically download agent, AV/AS support, and agent installer helper packages that support the client provisioning and posture policy services. These live update portals should be configured in ISE upon initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the 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 the **Administration > System > Settings > Proxy** before you are able to access the Live Update locations. For more information on proxy settings, see the “Specifying Proxy Settings in Cisco ISE” section in the “Configuring Client Provisioning Policies” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*.

Client Provisioning and Posture Live Update portals:

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

The following software elements are available at this URL:

- Windows and Mac OS X versions of the latest Cisco ISE persistent and temporal 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 Policies” chapter in the *Cisco Identity Services Engine User Guide, Release 1.0.4*.

- **Posture**—<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 “Dynamic Posture Updates” section of the “Configuring Client Posture Policies” chapter in the *Cisco Identity Services Engine User Guide, Release 1.0.4*.

If you do not enable the automatic download capabilities described above in Cisco ISE, you can choose offline updates. See [Cisco ISE Offline Updates, page 15](#).

Cisco ISE Offline Updates

Cisco ISE offline updates allow you to manually download agent, AV/AS support, and agent installer helper packages that support the client provisioning and posture policy services. This option allows you to upload client provisioning and posture updates in environments where direct Internet access to Cisco.com from the ISE appliance is not available or not permitted by security policy.

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

-
- Step 1** Log into Cisco Download Software at <http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>. You might be required to provide your Cisco.com login credentials.
- Step 2** Navigate to **Security > Identity Management > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

Choose from the following Off-Line Installation Packages available for download:

- **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 Now** or **Add to Cart** for any of the software items you require to set up your Cisco ISE deployment.

For more information on adding the downloaded Installation Packages to Cisco ISE, refer to “Adding Client Provisioning Resources from a Local Machine” section of the “Configuring Client Posture Policies” chapter in the *Cisco Identity Services Engine User Guide, Release 1.0.4*.

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

For offline updates, you need to ensure that the versions of the archive files match the version in the configuration file. Use this portal once 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>.
The File Download window appears. From the File Download window, you can choose to save the **posture-offline.zip** file to your local system. This file is used to update the checks, rules, antivirus and antispyware support charts for both the Windows and Macintosh operating systems, and operating systems information.
- 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 (mandatory) field and it cannot be left empty. 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 as a verification of an update under Update Information.
-

Cisco ISE Antivirus and Antispyware Support

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

- [Cisco Identity Services Engine Release 1.0.4 Supported Windows AV/AS Products](#)
- [Cisco Identity Services Engine Release 1.0.4 Supported Mac OS X AV/AS Products](#)

Cisco ISE Patch Release Updates

- [Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 6, page 17](#)
- [Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 5, page 18](#)
- [Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 4, page 19](#)
- [Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 3, page 19](#)
- [Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 2, page 20](#)
- [Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 1, page 21](#)

Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 6

[Table 5](#) lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 6.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.0.4.573, otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.0.4.573.” Since patch 6 is a cumulative patch, you can apply it to any of the following maintenance release versions:

- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 5
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 4
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 3
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 2
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 1
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 (no patches yet applied)

To obtain the patch file necessary to apply the patch to Cisco ISE Release 1.1.2, 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 1.1.x* for instructions on how to apply the patch to your system.

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

Table 5 *Cisco ISE Patch Version 1.1.1.268—Patch 6 Resolved Caveats*

Caveat	Description
CSCui22841	<p>Apache Struts2 command execution vulnerability</p> <p>Cisco ISE includes a version of Apache Struts that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2013-2251. This fix addresses the potential impact on this product.</p>

Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 5

Table 6 lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 5.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.0.4.573, otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.0.4.573.” Since patch 5 is a cumulative patch, you can apply it to any of the following maintenance release versions:

- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 4
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 3
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 2
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 1
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 (no patches yet applied)

To obtain the patch file necessary to apply the patch to Cisco ISE Release 1.0.4, log into the Cisco Download Software site at <http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm> (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Then refer to the “[Installing a Software Patch](#)” section of the “Administering Cisco ISE” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*, for instructions on how to apply the patch to your system.

Table 6 *Cisco ISE Patch Version 1.0.4.573—Patch 5 Resolved Caveats*

Caveat	Description
CSCtz46247	<p>After deregistering a secondary node from the deployment, there is no valid license</p> <p>An issue exists where, if the system has been operational for more than 90 days, then after the secondary server is deregistered during upgrade and restarts in standalone mode, it is not then possible to access the administrator user interface because the machine now has an “expired” evaluation license. This fix ensures that in such a situation, a valid temporary license is retained for upgrade purposes.</p>
CSCtz54548	<p>Evaluation license validity date is wrong on de-registered secondary node</p> <p>This resolution provides for a fix to enable a temporary 30-day evaluation license on a secondary node that is de-registered during upgrade from an earlier version of Cisco ISE.</p> <p>Note This issue has observed using both three- and five-year Base and Advanced term licenses.</p>

Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 4

[Table 7](#) lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 4.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.0.4.573, otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.0.4.573.” Since patch 4 is a cumulative patch, you can apply it to any of the following maintenance release versions:

- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 3
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 2
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 1
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 (no patches yet applied)

To obtain this patch, please contact Cisco Technical Assistance Center and then refer to the “[Installing a Software Patch](#)” section of the “Administering Cisco ISE” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*, for instructions on how to apply the patch to your system.

Table 7 Cisco ISE Patch Version 1.0.4.573—Patch 4 Resolved Caveats

Caveat	Description
CSCtt24622	IP table rules not persistent across reboot When the Guest SSL port is changed from 8443 to another value (like 4443, for example) the change takes place and guest authentication is successful to the new port. After Cisco ISE gets rebooted, however, port 4443 is still open but no traffic is accepted by the port because the “iptables” rule does not persist through reboot.
CSCtu95775	Showtech.out file does not include show version output “show version” command output now accompanies RPM versions listed in the show tech.out file in a support bundle. This helps the engineers more easily see what version the customer is running and what patches (if any) are installed.
CSCtw61515	Cisco ISE does not display a message when attempting to add a node with a different database password When you add a node with a different admin and user db password, Cisco ISE now displays an error message. (This fix also addresses issues where the administrator database passwords are the same but user database passwords are different and vice versa.)
CSCtx21412	Cisco ISE does not recover when the LDAP connection closes without notification This fix addresses an issue where LDAP connections were passing through a third-party firewall that closed the connection due to an idle timeout setting without notice to either Cisco ISE or the LDAP server. Cisco could not assume that the connection would remain open after a period of inactivity, nor get notified that connection was closed.

Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 3

[Table 8](#) lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 3.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.0.4.573, otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.0.4.573.” Since patch 3 is a cumulative patch, you can apply it to any of the following maintenance release versions:

- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 2
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 1
- Cisco Identity Services Engine Maintenance Release 1.0.4.573 (no patches yet applied)

To obtain this patch, please contact Cisco Technical Assistance Center and then refer to the “[Installing a Software Patch](#)” section of the “Administering Cisco ISE” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*, for instructions on how to apply the patch to your system.

Table 8 Cisco ISE Patch Version 1.0.4.573—Patch 3 Resolved Caveats

Caveat	Description
CSCts19672	<p>Inline Posture not handling third-party controller RADIUS Access-Request calls correctly</p> <p>A “tcpdump” from the Inline Posture node reveals that Cisco ISE is receiving RADIUS Access-Request from third-party controllers, but is not forwarding that request to the associated Policy Service node.</p>
CSCts56992	<p>Not all debug logs included in support bundles</p> <p>After using the Cisco ISE administrator user interface to create a support bundle file and to include all debug logs, discovered that the bundle was missing certain files, such as ad_agent.log and ise-tracking.log. By comparison, all files of the backup files created under /opt/CSCOcpm/logs are included as designed.</p>
CSCts57010	<p>User interface “undo_tablespace” function takes up too much file system space</p> <p>This issue was observed on a VMware installation operating as an Administrative ISE node, Monitoring node, and Policy Service node combination. The file system memory usage was severe enough to even disable simple administrator browser login sessions.</p>
CSCtt47520	<p>Cisco ISE Wireless license does not accurately count wireless devices</p> <p>This fix addresses an issue where Cisco ISE has been designed to display the same Base license user count as the Wireless user count, but is actually displaying only the Base Evaluation license count.</p> <p>Note The Advanced license user count shows only the Wireless user count, as designed.</p>

Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 2

Table 9 lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 2.

To obtain this patch, please contact Cisco Technical Assistance Center and then refer to the “[Installing a Software Patch](#)” section of the “Administering Cisco ISE” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*, for instructions on how to apply the patch to your system.

**Note**

This patch application process requires the Cisco ISE primary Administration node to restart multiple times, due to an ADE-OS update. If you are installing or rolling back from the primary Administration ISE node user interface, the node restarts once again after the patch has been installed in all of the secondary nodes in your deployment. You can verify the current status of the Cisco ISE using the “**show application status ise**” CLI command after the patch application process is complete. In addition, because the primary Administration ISE node restarts more than once, you may observe erroneous alarms triggered on the dashboard, indicating that the patch install/rollback failed on a secondary node, when in reality the patch application has taken place correctly. If such an alarm appears, please verify status using the **show version** CLI command on the secondary node in question, or check the node status indicated on the patch management page in the primary node administrator user interface to verify whether the secondary node has the patch successfully installed.

Table 9 *Cisco ISE Patch Version 1.0.4.573—Patch 2 Resolved Caveats*

Caveat	Description
CSCto66151	Cisco ISE application server function remains in “initializing” state perpetually This fix addresses an issue where multiple transactions were locking up on the secondary node. The transactions would all initiate simultaneously and wind up waiting on the same Cisco ISE resource.
CSCtr87810	Issue updating RBAC policy This fix addresses an issue seen while editing a custom RBAC policy in a way that would change the permission level (either Menu or Data). Cisco ISE would sometimes return error messages, and the new permission settings would not get applied to the policy.
CSCts82012	Edit Data Access Permission returns console terminal exceptions This fix allows users to edit “Data Access Permissions” during RBAC policy configuration. Previously, Cisco ISE could occasionally return error messages when you tried to edit existing “Data Access Permission” settings.
CSCtt16149	Submenus and links showing even when set to “Hide” under RBAC Menu Access This fix addresses an issue involving inconsistent behavior in third-level menu item appearance and display while specifying admin user menu permissions. While navigating to third-level menu items and selecting the Show Permission option, Cisco ISE was saving more than that specific menu item. Now the administrator is able to view only the specified third-level menu item.
CSCtt19362	Sponsor should see Guest details/password only before first login After the password has been modified by the guest user and is no longer randomly generated, the sponsor then cannot view the password anymore.

Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 1

Table 10 lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.0.4.573 cumulative patch 1.

To obtain this patch, please contact Cisco Technical Assistance Center and then refer to the “[Installing a Software Patch](#)” section of the “Administering Cisco ISE” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4*, for instructions on how to apply the patch to your system.

Table 10 *Cisco ISE Patch Version 1.0.4.573—Patch 1 Resolved Caveats*

Caveat	Description
CSCtj88493	<p>Exception observed after enabling probes in deployment</p> <p>This fix resolves an issue where Profiler probes were returning led to repeated “Error: Too many instances, exceeds 10” messages, when probes were configured on multiple interfaces and changing often. In addition, the probe would usually also stop working.</p> <p>No more of these types of exceptions should appear following this fix.</p>
CSCts32219	<p>Netflow probe not working until restarting Cisco ISE services</p> <p>This resolution fixes an issue where newly enabled NetFlow probes were not collecting flows as designed until restarting Cisco ISE services on the appliance where the probes are configured.</p>
CSCts82913	<p>Unexpected error detected by Java Runtime Environment</p> <p>This fix addresses an issue where Profiler probes would occasionally crash while being enabled.</p>
CSCts98931	<p>Policy Service node crashing when DHCP span probe is enabled on all interfaces</p> <p>This fix addresses an issue where enabling Profiler probes on all of the interfaces on the Policy Service node would cause the node to fail and not restart.</p>
CSCtt12870	<p>No alarm email notifications since upgrading to version 1.0.4.573</p> <p>This fix addresses a problem where Monitoring and Troubleshooting nodes that were not co-located with the primary Administrative ISE node were not sending out alarms via e-mail as configured.</p>

Cisco ISE Release 1.0.4 Open Caveats

- [Cisco ISE Release 1.0.4.573 Appliance Open Caveats, page 22](#)
- [Cisco ISE Release 1.0.4.573 Agent Open Caveats, page 46](#)

Cisco ISE Release 1.0.4.573 Appliance Open Caveats

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats*

Caveat	Description
CSCtc70053	<p>Browser “Back” button not working properly</p> <p>This issue has been observed in the Cisco ISE list page when switching from the list view to edit view (i.e., when you click the Create or Edit button).</p> <p>Workaround There is no known workaround for this issue.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtj00178	<p>Group QuickFilters not working as designed</p> <p>After the administrator runs and saves an advanced filter, Cisco ISE does not display the “Successful Save” pop-up after the filter is saved.</p> <p>This issue has been observed using the Admin Groups, User Identity Groups, Endpoint Identity Groups, and Guest Sponsor Groups filter options.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj25158	<p>Exported admin should not be imported back as Network Access User</p> <p>This problem occurs when Cisco ISE promote Network Access Users to Administrators, and then export those users. When you re-import those users, they appear as Network Access Users only. Cisco ISE does not import the promoted users as Administrators.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj37325	<p>Profiler Attribute value exceeds maximum 4000 character length</p> <p>Endpoints are not profiled nor are new attributes updated when at least one Profiler Endpoint Attribute is greater than 4000 characters in length.</p>
CSCtj76835	<p>Unable to retrieve a saved Authentication Trend report</p> <p>Symptom Two steps are necessary to save an Authentication Trend report:</p> <ol style="list-style-type: none"> 1. Select the folder. 2. Name the file. <p>If you do not select a folder from the list that is presented, the report should be saved in the root folder and should appear in the Reports tab. You can observe that the files are saved, but they do not appear in the left side pane and there is no option to retrieve the files.</p> <p>Conditions Saving an Authentication Trend report without selecting a folder.</p> <p>Workaround Do not save the report under the root folder. Always choose a subfolder.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)


Caveat	Description
CSCtj81255	<p>Two MAC addresses detected on neighboring switch of ACS 1121 Appliance.</p> <p>Symptom Two MAC addresses are detected on the switch interface connected to an ACS 1121 Appliance although only one interface is connected on the ACS 1121 Server eth0.</p> <p>Conditions Only one Ethernet interface, eth0 is connected between ACS and Switch.</p> <p>Workaround Disable BMC (Baseboard Management Controller) feature using BIOS setup.</p> <p> Caution To help prevent a potential network security threat, Cisco strongly recommends physically disconnecting from the Cisco ISE console management port when you are not using it. For more details, see http://seclists.org/fulldisclosure/2011/Apr/55, which applies to the Cisco ISE, Cisco NAC Appliance, and Cisco Secure ACS hardware platforms.</p>
CSCtj94813	<p>Left side administrator user interface pane “Search Result” option is not working as expected</p> <ol style="list-style-type: none"> 1. If you enter available data and click the search option, it does not display properly. 2. If the option displays some data and if you enter another value, it does not refresh the data properly. 3. The option does not display the layered/structured model as designed. <p>In addition, you are not able to go back to previous menu.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtk17648	<p>IE8—Network Device Management missing from the Cisco ISE Administrator Tab</p> <p>This issue has been observed when changing the zoom setting in Internet Explorer 8 using the control and plus (+)/minus (-) keys.</p> <p>Workaround If the menu is missing, change the zoom to the default value and refresh the page.</p>
CSCtk32480	<p>Local certificate export failed after deleting trusted certificate</p> <p>After you delete a trusted certificate, local certificate export operation fails.</p> <p>Administration > System > Certificates > Local Certificates > Export. Instead of being prompted for the export file destination, nothing happens.</p> <p>Workaround Reload the page using the browser reload function. This should reload all of the Javascript files for the page and allow you to export the local certificate.</p>

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)*

Caveat	Description
CSCtk37360	<p>Administrator is not able to customize report in Internet Explorer 8</p> <p>Monitoring and troubleshooting reporting functions related to column selection and entry deletion/aggregation, etc. are not working as designed.</p> <p>This issue can come up using the following versions of Internet Explorer 8:</p> <ul style="list-style-type: none"> • IE 8.0.6001.18702 on Windows XP • IE 8.0.6001.18702IC on Windows XP <p>Workaround There is no known workaround other than to avoid using the problematic browser versions.</p>
CSCtk46958	<p>Cisco ISE does not display a warning when navigating away from a modified page without saving</p> <p>When a user changes configuration context, there is no warning indicating that the information configured on the current page is not saved, nor is there a warning indicating that all configuration changes will be lost when the user completes that context change.</p> <p>Workaround Save before navigating away from the page in question.</p>
CSCtk82864	<p>AAA Servers incorrectly filter with “Contains” option</p> <p>When AAA servers are added to the AAA servers list (for example: a, ab) and a filter is added which includes regular expressions, Cisco ISE generates an incorrect filtered list.</p> <p>Workaround Do not use regular expressions in filters.</p>
CSCtl56724	<p>Network access users display filter sorted by status does not work</p> <p>An issue exists in the Administration > Identity Management > Identities > Users page where Cisco ISE does not appropriately filter Network Access User entries when you click on the filter and try to specify “sort by status.”</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtl70056	<p>“Today” is not validated against the Cisco ISE Monitoring node End Date</p> <p>Reports run with a custom time range (where “today” is the specified End Date) does not work and the Monitoring node returns a validation error. This issue has been observed where the time on the client machine (where a browser session is active) is earlier than that of the Cisco ISE node (for example, where the client is on PST and the Cisco ISE node is on UTC time zone).</p> <p>Workaround Change the time zone or clock on the client machine so that the current time on that server is the same or ahead of the Monitoring node.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtl77592	<p>Unable to create authorization policy with RadiusCallingStation ID condition</p> <p>When the administrator uses a MAC address with a xx-xx-xx-xx-xx-xx format as the right hand side (RHS) of a condition with RADIUS “Calling station ID” dictionary attribute, it fails to match the policy decision.</p> <p>Cisco ISE does not perform validation on the string value that is entreated on the RHS when constructing a condition.</p> <p>Workaround Use the MAC address format xx:xx:xx:xx:xx:xx when defining conditions.</p>
CSCtl78424	<p>Blank right hand Network Devices pane with vertical scroll</p> <p>The Network Device page contains the navigation pane on the left of the page and the network devices table on the right of the page. If there are more than 500 devices configured and the following steps have been taken, the devices table does not appear as it should:</p> <ol style="list-style-type: none"> 1. Move the vertical scroll all the way to the bottom and wait a few seconds. 2. Move vertical scroll to the top and then back to the bottom again (and repeat if necessary) until the table disappears. 3. The table remains empty (blank) for 30 minutes or more. <p>Workaround Manually refresh the devices page.</p>
CSCtn42397	<p>The Network Access Users “Delete All” function when used on a filtered list should only delete filtered (displayed) Network Access Users</p> <p>The “Delete All” function in the Administration > Identity Management > Identities > Users page deletes <i>all</i> the users, regardless of whether they are filtered or existing (non-filtered) users.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtn44427	<p>No progress indicator is displayed when importing collections of random or CSV guests</p> <p>Workaround There is no known workaround for this issue. The administrator must simply wait for the process to complete.</p>
CSCtn53084	<p>Incorrect export of DER imported server and trusted certificate authority certificates</p> <p>When exporting a local certificate using the Administration > System > Certificates > Local Certificates > Export page, the administrator may find that the certificate is in Distinguished Encoding Rules (DER) format when another format like Privacy Enhanced Mail (PEM) is desired.</p> <p>The certificate export function exports a certificate using the same format it had when imported. In Cisco ISE, there is no format conversion option available.</p> <p>Note One way to avoid this is to simply import all certificates in PEM format. You can convert DER to PEM using tools like openssl, and your certificate authority may have an option for PEM output.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtn59529	<p>Network Access User filters do not work on the Status or Admin columns using the Quick and Advanced filters</p> <p>Cisco ISE search functions are not supported on columns which have images or icons. The Status and Admin columns use images and icons instead of text, therefore filtering does not work.</p> <p>Workaround There is no known workaround for this issue,</p>
CSCtn62141	<p>A script on the Administration > Identity Management > Groups page causes Internet Explorer 8 to run slowly. If it continues to run indefinitely, your computer could become unresponsive. (This problem has not been observed using Mozilla Firefox.)</p> <p>Workaround There are three ways to fix this issue:</p> <ol style="list-style-type: none"> 1. Implement Virtual Scrolling in the Object Selector. 2. Change the time-out value as follows: <ol style="list-style-type: none"> a. Using a Registry Editor such as Regedt32.exe, open the HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles key. b. Create a new DWORD value called “MaxScriptStatements” under this key and set the value to the desired number of script statements. If you are unsure of what value you need to set this to, you can set it to a DWORD value of 0xFFFFFFFF to completely avoid the dialog. 3. Install and apply the following patch from Microsoft: http://support.microsoft.com/kb/175500#FixItForMeAlways
CSCtn65437	<p>Report timestamp incorrect with Asia/Kolkata time zone</p> <p>This behavior has been observed only using the Asia/Kolkata time zone. The result is minus 5.30 hours when compared to the actual record in the Cisco ISE database.</p> <p>Workaround There is no workaround for this issue at this time.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtn73422	<p>Network Access User filters filtering correctly</p> <p>The filter display does not conform to the expected alphanumeric order. For example, create four users with the following IDs:</p> <ul style="list-style-type: none"> • 2234567890a • a214567890 • 2b34567890-2 • a214-25678 <p>Use either the Quick/Advanced Filter with a “Name: Contains _2” attribute. The resulting list is returned as follows:</p> <ul style="list-style-type: none"> • 2234567890a • 2b34567890-2 • a214-25678 • a214567890
CSCtn78676	<p>When a user name has a space between words and another similar name contains two or more spaces, Cisco ISE displays the same user name for both users.</p> <p>Workaround There is no known workaround for this issue. Even though the multiple spaces are trimmed and shown as one space in the UI, the data is saved correctly in the database.</p>
CSCtn78899	<p>When a user group name has a space between words and another similar user group name contains two or more spaces, Cisco ISE displays the same user group name for both groups.</p> <p>Workaround Avoid giving spaces in the name field while creating Identity Group.</p>
CSCtn83738	<p>Session status summary report failing for Wireless LAN Controllers</p> <p>It appears that Cisco ISE may not be appropriately handling public/private community stings.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtn92594	<p>Quickpicker filters are not working correctly during Client Provisioning policy configuration</p> <p>This issue has been observed with the following three filter options:</p> <ul style="list-style-type: none"> • Identity Groups • Operating Systems • Other conditions <p>Workaround There is no known workaround for this issue.</p>

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)*

Caveat	Description
CSCtn92602	<p>Filters are not working under QuickPickers during Posture Policy configuration</p> <p>The following QuickPicker filters are not working during Posture Policy configuration:</p> <ul style="list-style-type: none"> • Operating System • Other Conditions • Requirements <p>When using any of these QuickPickers to search for text, Cisco ISE returns invalid search results.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtn95127	<p>Client provisioning report does not show the policy matched</p> <p>The report shows which agent is downloaded, but it does not indicate which policy has been applied.</p> <p>This happens if a network access request has been redirected to the client provisioning portal and the client provisioning service applies a policy that determines which agent needs to be installed on the client machine.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtn95548	<p>Filter behaving case sensitive for Network Device groups</p> <p>The results for network device group filtering in the network device group (NDG) page are incorrect. This is because the filtering in the network device group page is case sensitive.</p> <p>Workaround Enter network device groups values using lower-case letters.</p>
CSCtn99145	<p>An authorization policy matching multiple rules does not appropriately match the existing ACCESS_ACCEPT rule</p> <p>When an authorization policy use the “multiple rule match” option, and <i>any</i> of the matched policy rules contain ACCESS_REJECT, the ACCESS_REJECT rule overrides the ACCESS_ACCEPT rule, regardless of where the two rules appear in relation to one another.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto03813	<p>No “Cisco ISE Config Changes” alarm generated using Authentication > Simple Condition > Edit/Add/Delete</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto05172	<p>The Profiler detail log does not display some attributes.</p> <p>“Certainty Matrix,” “Matched Rule,” and “Endpoint Action” name values are not updated in the Profiler endpoint detail log.</p> <p>Workaround There is no known workaround for this issue.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCto06361	<p>Changing the User Identity Group name case should not return error upon search</p> <p>After you Create a User Identity Group called “mickeymousegroup,” edit the name to be “MickeyMouseGroup.” Cisco ISE displays the following error:</p> <p>“Identity Group with name ‘NAC Group:NAC:IdentityGroups:User Identity Groups:MickeyMouseGroup’ already exists.”</p> <p>Workaround Delete and recreate the User Identity Group.</p>
CSCto09989	<p>Cisco ISE browser session redirects to Monitoring login page using Internet Explorer 8</p> <p>As soon as you login to Cisco ISE via IE8 the page gets redirected to a Monitoring node administrator login page (even before the initial page displays completely).</p> <p>Note This issue has also been observed using Mozilla Firefox, but the redirection in Firefox only takes place after a couple of minutes of inactivity.</p> <p>Workaround Immediately after entering your login credentials,. navigate from the main Cisco ISE page to any configuration page (like Posture, Authorization, or Client Provisioning, for example).</p> <p>For more information, see Issue Accessing the Cisco ISE Administrator User Interface, page 53.</p>
CSCto10678	<p>Administrator user should not be able to delete self policy</p> <p>If self-policies get deleted, the administrator cannot log in.</p> <p>Workaround The Cisco ISE administrator should not delete their own access policy.</p>
CSCto10855	<p>IE8 with default option settings is not working</p> <p>This issue arises when the default URL has been specified in Administration > System > Setting > Posture Updates.</p> <p>Workaround There is no known workaround for this issue.</p> <p>Note This functionality is working as designed using a Firefox browser.</p>
CSCto13102	<p>No “Cisco ISE Configuration Changes” message dialogs are displayed for certain guest/sponsor configuration</p> <p>Certain dialogs are missing for guest and sponsor configuration changes, hence, Cisco ISE does not confirm when changes have been made and accepted.</p>
CSCto13235	<p>File Condition Advanced Filter does not return correct result</p> <p>This issue has been observed in the Advanced Filter function of the Posture Simple Condition and Remediation pages. The “Match All/Any of the Following Rules” selection is not working as expected.</p> <p>Workaround There is no known workaround for this issue.</p>

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)*

Caveat	Description
CSCto13986	<p>IE8—Error when clicking the “Action” button on the Requirement page</p> <p>Go to Policy > Policy Elements > Results > Posture > Remediation Action and click on the Requirement in the left hand navigation pane. Once the page loads, then click on the “Action” button. A Java script error is returned when accessing the page via Internet Explorer 8.</p> <p>Note This is an issue with Internet Explorer 8 and is working as expected.</p>
CSCto15508	<p>Filter in Security Group Access Egress Policy is not working correctly</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto17461	<p>Invalid Simple Condition error message in Guest configuration</p> <p>If you duplicate, but do not rename a new Simple Condition in the Policy Elements > Conditions > Guest > Simple Condition page, Cisco ISE returns an error message indicating that the condition has not been saved.</p> <p>Workaround Change the name of the condition that is being duplicated before saving it.</p>
CSCto22671	<p>HTTPS communication fails if the certificate is deleted from the primary Administration ISE node</p> <p>The following operations on the primary Administration ISE node fail unexpectedly:</p> <ul style="list-style-type: none"> - Restoration of a backup - Manual sync - Node deregistration <p>If the certificate(s) required to validate the HTTPS certificate of a registered node have been removed from the primary Administration ISE node trust store, they must be reimported in to the trust store before attempting restore database material, perform manual sync, or deregister other policy service nodes.</p>
CSCto24105	<p>A Network Access User can be created with a name longer than 25 characters via network access user import, but Cisco ISE cannot reliably handle user names that long.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto24430	<p>Details of guest RADIUS authentication failure are not available when searching via the guest username</p> <p>This issue has been observed where the guest user has logged in with space appended to the beginning or end of the user name.</p> <p>Workaround The guest user must enter the user name without any additional spaces entered at the beginning or end.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCto27568	<p>Cannot enable checkboxes in the right hand Filtered Network Devices pane</p> <p>The administrator is not able to select a checkbox under the following conditions:</p> <ol style="list-style-type: none"> 1. The browser window is not open to its maximum size. 2. A filter is applied to the network device table. <p>Workaround Apply filters to the network device table only when the browser window is maximized.</p>
CSCto29479	<p>Cisco NAC Web Agent fails to validate Registry Condition</p> <p>Registry condition check does not work correctly on 64-bit Windows operating systems.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto33037	<p>Allowed character sets between policy conditions and element conditions are different</p> <p>When conditions are created inside policies, the allowed character sets are not the same. Condition policies allow alphanumeric, hyphen(-), underscore(_), or period(.), The condition page itself allows letters, numbers and “_”.</p> <p>Workaround Use the common characters of both sets: letters, numbers, and “_”.</p>
CSCto33973	<p>Joining Cisco ISE to an Active Directory domain locks up when the Global Catalog is down or unreachable</p> <p>Having a Global Catalog active is essential for Cisco ISE operation with Active Directory. If there is no Global Catalogs available, the Cisco ISE user interface locks up for a long time in certain operations. This issue applies to a single domain environment.</p>
CSCto41078	<p>Cannot create an Identity Group using the gear icon during Client Provisioning policy configuration</p> <p>Workaround Create the Identity Group using the Administration > Identity Management > Groups page before configuring the policy.</p>
CSCto41340	<p>Authentication Policy replication failure from Primary to Secondary if the time zone changes after installation</p>
CSCto42182	<p>Profiling HTTP requests for 802.1X scenarios may not include agent</p> <p>This issue occurs when the initial HTTP request for 802.1X authentication and posture services are redirected to the gateway via HTTPS.</p> <p>Workaround Try using URL redirection over port 8080 for the gateway.</p>
CSCto43825	<p>Synchronization fails with time zones other than UTC</p> <p>During installation, if you specify a time zone other than UTC, replication fails during registration and Synchronization status shows “OUT OF SYNC.”</p> <p>Workaround To avoid this issue, change the time zone to UTC, enter the reset-config command via CLI, and reregister the node.</p>

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)*

Caveat	Description
CSCto45372	<p>Default Sponsor Groups do not allow the Sponsor to create users or view passwords.</p> <p>Workaround Navigate to the Guest Management > Sponsor Groups page and change the Sponsor Groups to allow appropriate access rights to Sponsors in these groups.</p>
CSCto48657	<p>Profiled endpoints are not all deleted</p> <p>If you delete endpoints that have recently been imported (before Cisco ISE can finish Profiling all of the new endpoints), Cisco ISE does not delete them all.</p> <p>Workaround Wait until all endpoints have been profiled before trying to delete them, or try to delete the remaining endpoints again after the initial attempt.</p>
CSCto49359	<p>Filters not working correctly on Guest conditions page</p> <p>Filters are not getting saved in the Policy Elements > Conditions > Guest > Simple Conditions page.</p> <p>Workaround Re-enter the filter to get Cisco ISE to perform the list filtering correctly.</p>
CSCto54536	<p>Local certificates disappear on the secondary node following “application reset-config ise” command in CLI</p> <p>When displaying the local certificates on the Administration > System > Certificates > Local Certificates page of a deregistered node that is now in Standalone mode.</p> <p>The administrator should not reset the configuration of a node prior to de-registering it. The correct process is as follows:</p> <ol style="list-style-type: none"> 1. Node A is registered. 2. Node A is deregistered. 3. Enter “application reset-config ise” in node A CLI. <p>Workaround If the node is reset before deregistration, you can make the local certificates reappear by entering the following commands in the CLI:</p> <ul style="list-style-type: none"> • application stop ise • application start ise
CSCto59976	<p>Sync with NTP server during initial set-up shows failure although NTP server is reachable.</p> <p>This issue occurs if an invalid or unreachable NTP server was first specified during initial installation and is then corrected (reconfigured) with an NTP server which has less characters than the initial invalid NTP server entry.</p> <p>Workaround When the set-up shows “Sync with primary NTP server failed,” press CTRL+C and restart the set-up from scratch, this time providing the valid and reachable NTP Server in the initial prompt itself.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCto60148	<p>Java crashes during high posture load</p> <p>This issue has been observed under extreme load condition where Cisco ISE is hit with large number of concurrent users for posture.</p> <p>Workaround None. You must restart the Cisco ISE Policy Service.</p>
CSCto60636	<p>Favorite reports are not preserved after executing “application reset-config ise” in the Cisco ISE CLI</p> <p>After the reset-config operation is complete, you can manually add the corresponding reports to favorites again.</p>
CSCto63749	<p>The Cisco ISE dashboard does not display endpoints entered via the Administrator user interface</p> <p>Endpoint display behavior works as designed for imported or detected Endpoints.</p> <p>Workaround Define the endpoint(s) in a CSV file and import the CSV file.</p>
CSCto64028	<p>“Fail to receive server response...” seen when deleting profiling policy</p> <p>A “Fail to receive server response due to the network error (ex. HTTP timeout)” error message may appear when deleting Profiling policies, and some of the policies may not be deleted.</p> <p>Workaround Log out from Cisco ISE, log back in, and try deleting the policies again.</p>
CSCto68519	<p>Sorting / Filtering Does Not Work in Egress Table</p> <p>Can not filter or sort Egress policy table data</p> <p>Workaround There is no known workaround for this issue.</p> <p>Note It is not possible to filter the Egress policy table data based on source / destination security group. In addition sorting is not available as well</p>
CSCto70968	<p>Fast reconnect is not working for PEAP-TLS protocol</p> <p>When the supplicant is eligible for PEAP-TLS fast reconnect after establishing a PEAP tunnel, Cisco ISE does not allow the fast reconnect function and falls back to the standard inner method.</p> <p>The following messages appear in the customer log:</p> <ul style="list-style-type: none"> 22044 Identity policy result is configured for certificate based authentication methods but received password based 12317 PEAP fast-reconnect failed; starting inner method <p>Workaround There is no known workaround for this issue.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCto72521	<p>Save failed for child group assignment during Client Provisioning policy configuration</p> <p>An exception dialog box appears, displaying a “Invalid identity group in policy <policy name>. There were errors in the save” message.</p> <p>Workaround Use first-level identity groups whenever possible.</p> <p>Note Identity Group selection is more than one level deep. For example, if an administrator creates hierarchal groups like “Employee” or “Accounting” and selects “Accounting” as an Identity Group when creating or updating a client provisioning policy.</p>
CSCto72594	<p>Cisco ISE cannot save a Posture Policy when the Identity Group is the child of one or more other Identity Groups</p> <p>Cisco ISE returns a “Policy Policy_Check_For_AV_Installation_Win: Error - class com.cisco.cpm.posture.exceptions.PostureValidationException: invalid role” message and does not save the Posture Policy in question.</p> <p>Workaround Use only first-level Identity Groups.</p>
CSCto73439	<p>Restart required upon completion of Monitoring node database restoration</p> <p>This issue has been observed with both scheduled and incremental backup and restore functionality.</p> <p>After completing a Monitoring node database restoration, manually synchronizing a Secondary node from the Primary node does not work because the Secondary Administration ISE node data has been changed by the Monitoring node restoration operation.</p> <p>Workaround There are two possible workarounds for this issue:</p> <ul style="list-style-type: none"> Log into the Cisco ISE CLI with admin privilege and execute the following commands: <ul style="list-style-type: none"> a. application stop ise b. application start ise Log into the Cisco ISE CLI with admin privilege and execute the reload command.
CSCto74356	<p>Self-registered Guest role does not appear associated with the Guest account</p> <p>If the administrator creates a new Identity Group (group role) and specifies this role as the default group role on the Guest Portal Policy page for self registration, the newly created Identity Group is not added to the identity group list for a sponsor group.</p> <p>This issue can occur in both standalone and distributed deployment.</p> <p>Workaround Add the new Identity Group to the Sponsor Group to which the sponsor is mapped, which shows the correct Identity Group in the Edit panel of the Guest account.</p>

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)*

Caveat	Description
CSCto82519	<p>Saving your Active Directory configuration while the DNS is down takes a very long time</p> <p>Cisco ISE requires connectivity to Active Directory (including DNS) when saving the configuration. If the DNS is not reachable, then the save function may time out before it can complete.</p> <p>Workaround Ensure that the DNS is available and reachable before saving your Active Directory configuration.</p>
CSCto82631	<p>Clicking the “Name” field in the Cisco ISE User Identity Group page yields unexpected download behavior</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto83897	<p>Client machine authentication shift to user authentication not updating Active Directory groups</p> <p>During a Wireless LAN Controller (WLC) login session, the client machine authenticates with Cisco ISE correctly and the corresponding authorization profile is picked up. During user authentication, however, (although system log entries indicate that user authentication has happened correctly) the previous authorization profile (for machine authentication) is applied to the user session again.</p> <p>This issue has been observed during wireless login scenarios where the WLC is running firmware version 7.0.116.0.</p> <p>Workaround If you do not require the new WLC features (such as NAC-RADIUS) introduced in firmware version 7.0.116.0, Cisco recommends restoring the WLC version to 7.0.98.218 until a new firmware version becomes available.</p> <p>For more information, see Known Incompatibility Issue with WLC Firmware Version 7.0.116.0, page 54.</p>
CSCto87755	<p>Guest accounting report appears only once, even though Guest logs in multiple times</p> <p>This issue has been observed when Guest users have logged in using the same endpoint multiple times. The report shows only the user's first login details, not the most recent login.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto87799	<p>Guest authentication failing</p> <p>Guest authentication fails and the LiveLogs on Cisco ISE show the reason as “session cache entry missing.” The most common explanation for this issue is that the browser is using old session information.</p> <p>Workaround The user just needs to launch a new browser session and get redirected to the appropriate Guest portal.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtq00096	<p>Compound condition from a Sponsor Group Policy has a different name after it is saved</p> <p>This new name can erase the existing condition in the Cisco ISE configuration and the administrator must assign the condition again.</p> <p>Workaround If you are editing conditions in the Sponsor Group Policy, specifically reassign the compound condition.</p>
CSCtq07776	<p>In Posture Policy, Click Save Symbol getting error message.</p> <p>When you attempt to configure Dictionary Compound Condition using Posture Policy configuration, Cisco ISE returns a “configured dictionary compound condition already exists” error message, even though the specified Dictionary Compound Condition does not yet actually exist.</p> <p>Workaround The administrator needs to click on the OK button several times, or reload the page to work through this issue.</p>
CSCtq09004	<p>Windows 7 guest access not successful from IE8 and Chrome 10</p> <p>Guest access fails over a wireless LAN controller connection. The login session does not appropriately redirect the user authentication request. This is likely due to IE8 and Chrome10 browsers on Windows 7 being unable to redirect the RADIUS authentication request to the controller.</p> <p>Note This issue has not been observed using Mozilla Firefox.</p> <p>Workaround Ensure that the certificates in the controller are accepted by the IE8 browser on the Windows 7 client correctly.</p>
CSCtq09655	<p>Dictionary Attribute duplication is not happening as designed during Authentication Policy configuration</p> <p>Dictionary Attributes are not being duplicated appropriately within a rule during Authentication Policy configuration. Only the “operator” and “condition” values are getting duplicated.</p> <p>Workaround You must manually specify the Dictionary Attribute to complete the configuration.</p>
CSCtq11650	<p>The primary Administration ISE node has database links to Inline Posture nodes following promotion from secondary to primary</p> <p>The newly-promoted primary node attempts to replicate with Inline Posture nodes and saves the undeliverable messages in its local database. This issue has been observed in a distributed deployment with Inline Posture nodes associated with an Administration ISE node that has been promoted from secondary to primary.</p> <p>Workaround Use root patch and SQLPlus to clean it.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtq17744	<p>Exception policy not getting created first time in Authorization policy</p> <p>When you create the first new exception policy under an Authorization Policy, an error pops up indicating that the operation has failed.</p> <p>This issue has been observed when there are no items in the exception policy pane and the user clicks Create New. After the user submits the change, an error message comes up.</p> <p>Workaround There are two possible workarounds for this issue:</p> <ol style="list-style-type: none"> 1. Use the Duplicate function to add a second exception policy below the first one, and then delete the first exception. Once all the changes are done, then save the policy. 2. Similar to the first option above, use the Insert function to insert a second exception policy below the first one, and then delete the first exception. Once all the changes are done, then save the policy.
CSCtq22779	<p>Cisco ISE allows saving authorization compound conditions with the same names</p> <p>If you create two authorization compound conditions called “C1” and “C2,” then change the name of “C2” to “C1,” Cisco ISE does not return an error and you end up with two compound conditions called “C1.” This happens only for authorization compound conditions.</p> <p>The potential impact of this problem is that the contents of the original “C1” compound condition is always picked up and enforced in authorization policies that use “C2.”</p> <p>Workaround There is no known workaround for this issue. You must be sure to create conditions with unique names. If you do end up creating two or more conditions with the same name, you can always rename them appropriately at any time.</p>
CSCtq53690	<p>Scheduled Monitoring and Troubleshooting incremental backup switches off following failed backup attempt</p> <p>Workaround If one of the scheduled Monitoring and Troubleshooting node backup events fails, the administrator needs to enable the “Incremental Backup” option again in the Administration > System > Operations > Monitoring Node > Scheduled Backup page.</p>
CSCtq80912	<p>Issues with Guest accounting report functions</p> <p>After at least one full day of traffic, round trip Guest sessions include non-guest events in the logs.</p> <p>Note There is no known workaround for this issue.</p>
CSCtr09694	<p>MAC address search at Reports > Query and Run should not be case sensitive</p> <p>While launching reports, the MAC address search is case sensitive, but should not be.</p> <p>Note There is no known workaround for this issue.</p>

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)*

Caveat	Description
CSCtr24825	<p>Numerous Alarms entitled “ISE Alarm (CRITICAL): Alarm caused by ISE - System Health threshold” with high numbers in “CPU Utilization (%)”</p> <p>The same alert message is being used for both real system resource overloads and normal operations like system backup and restore.</p> <p>Note There is no known workaround for this issue.</p>
CSCtr29490	<p>Endpoint does not get profiled correctly with HTTP traffic following posture assessment</p> <p>Following a VLAN change, traffic may not be mapped to the endpoint due to a missing IP address in the RADIUS accounting message.</p> <p>Workaround Use a DHCP probe for profiling. Alternatively, RADIUS interim accounting should correct the situation on the next accounting update.</p>
CSCtr38300	<p>“Admin” login account is disabled and cannot be unlocked</p> <p>After you enter the wrong password for the administrator user ID at least 5 times (though the actual value is configurable), the administrator cannot use the “admin” login credentials to access the user interface and Cisco ISE displays the following message:</p> <p>“Your account has been locked after too many consecutive unsuccessful attempts. Please contact your system administrator for assistance.”</p> <p>Workaround When you regain access to the user interface, create another administrator ID (different credentials) with same permissions and login using that one.</p> <p>Note This is a new security function of Cisco ISE Maintenance Release 1.0.4 and is working as designed.</p>
CSCtr39545	<p>Endpoint update function may execute before endpoint creation</p> <p>Alarms generated on replication failures; DEBUG entries from Profiler show endpoint update failures due to absent record.</p> <p>Note There is no known workaround for this issue.</p>
CSCtr51053	<p>Back button use is not working correctly under compound conditions after upgrade</p> <p>When you add a new compound condition in the Policy > Conditions > Posture > Compound Condition configuration page and then navigate through the condition list, the back button will lead to the Cisco ISE home (Monitoring) page instead of the previous level.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtr53954	<p>Configure ISE for MAB + Posture flow</p> <p>After successful MAB Authentication, the client endpoint is moved to its assigned VLAN. Then the posture function initiates and the endpoint sends a “compliant” report back to Cisco ISE, which triggers CoA for that session and sends an new VLAN assignment back to the associated NAD. The problem is that the endpoint fails to re-fresh its IP address. (Make sure the Endpoint is put in to different VLAN after moving to compliant/noncompliant state.)</p> <p>Note The same IP-refresh on VLAN change is working in an 802.1X environment with posture functions.</p> <p>Workaround If we enable the “Agent IP refresh after VLAN change” option in the Agent profile, then the IP address gets refreshed after moving to compliant/noncompliant state</p>
CSCtr57280	<p>IP-to-MAC address binding fails in wireless environment with RADIUS and HTTP probe</p> <p>RADIUS accounting messages from a WLC do not send the endpoint IP address. This is different from the RADIUS accounting messages from wired infrastructure. This makes the RADIUS method ineffective for IP-to-MAC address binding on Cisco ISE.</p>
CSCtr58604	<p>Cisco Administration ISE node backup size exceeds 8 GB</p> <p>Backup files are very large and at times larger than 8 GB each. This has been observed performing both scheduled and on-demand full backups from CLI or administrator user interface.</p> <p>Note There is no known workaround for this issue.</p>
CSCtr58811	<p>Need to log out and log back in to get Advanced License functionality</p> <p>After installing an Advanced License on top of an existing Base license, the administrator is not able to view advanced feature pages such as Posture, Profiler, and Security Group Access.</p> <p>Workaround Log out and log back in again to view Advanced feature pages.</p>
CSCtr59589	<p>Exception Actions are triggering multiple CoA reauthentication events</p> <p>An exception action experienced under high traffic volume may be triggering multiple times and issuing multiple CoA events on the same session. By design, only the first CoA event will be acted upon—the subsequent ones are ignored by the infrastructure.</p>
CSCtr60200	<p>Error while editing predefined AV/AS compound conditions</p> <p>After you update Cisco ISE to release 1.0.4 and edit a pre-existing Av/AS compound condition, the configuration will be saved, but when you try to go back and view or edit the same compound condition, the “Allow virus definition checks to be...” option becomes disabled (unchecked).</p> <p>Although there is no impact when generating the XML file with the modified data for the pre-defined AS compound condition, this issue leads to confusion.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtr66122	<p>Policy could not be saved</p> <p>Cisco ISE can return an error message when you try to save a policy where the same identity group appears more than once.</p> <p>Workaround Manually remove duplicate identity group entries from the policy and save the policy again.</p>
CSCtr66929	<p>Selected month and year while configuring file “Date” condition</p> <p>If you specify either just the year or month in the “Date” field of the Policy > Policy Element > Conditions > File Condition configuration window, the date does not get saved along with the policy.</p> <p>Workaround Always specify the correct date.</p>
CSCtr68491	<p>Windows Internet Explorer 8 Info button on compound condition format is empty</p> <p>When you hover over the “Info” button in the Go to Policy > Policy Elements > Conditions > Posture > Compound Condition page, the pop-up bubble remains empty.</p> <p>This issue has been observed using IE8, but the text appears as designed in Mozilla Firefox.</p>
CSCtr79440	<p>Authorization policy not matched when condition to match parent device group location used</p> <p>This issue can come up when you define an authorization rule which has a condition containing the operand “DEVICE:Location equal AllLocation#<group name>.”</p> <p>Note There is no known workaround for this issue.</p>
CSCtr82311	<p>Administrator user interface password reset failed upon first login attempt</p> <p>This condition is only seen if the first default credentials (“admin”/“cisco”) have not yet been changed. After the admin user gets disabled, the password reset function may fail on the first attempt.</p> <p>Workaround Try resetting the password again using the application reset-password CLI command. Another workaround if it's the 'admin' user in question, just login as 'admin/cisco' and set the first credentials.</p>
CSCtr84378	<p>Guest role text box can be removed in sponsor group object</p> <p>When only one group role exists, the Guest Role can still be removed when configuring the sponsor group, which prevents the user from selecting any Guest Role at all. (If the administrator clicks on the minus (-) operator on the Guest Role tab in the sponsor group configuration with only one existing group role, then the field is removed.)</p> <p>Workaround Do not click the minus (-) operator during Guest Role selection during Sponsor Group configuration if only one group role exists. If the situation does occur, then you need to manually create a new sponsor role.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCtr84493	<p>Cisco ISE inaccurately reports that a specified policy name already exists</p> <p>This issue arises when you try to create a sponsor group policy name containing regular spaces (like “xx yyy zzz 1”) that is identical to an existing name using underscores (like “xx_yyy_zzz_1”). The resulting error message from ISE reads: “Policy with name xx_yyy_zzz_1 already exists.”</p> <p>Workaround To avoid this issue, reverse the order in which you create these two similar names:</p> <ol style="list-style-type: none"> 1. Create a sponsor group policy using spaces (“xx yyy xxx 1) and click Save. 2. Create another sponsor group policy using underscores (xx_yyy_zzz_1 and click Save. <p>The error message should not appear.</p>
CSCtr94724	<p>Browser becomes inaccessible after creating Authorization profile</p> <p>This occasional issue has been observed when scrolling down the page before the page loads completely</p> <p>Workaround Cisco recommends allowing a few extra seconds for the page to completely load before scrolling down the page.</p>
CSCtr96694	<p>SGA Security Group column is empty following SGA authentication</p> <p>When performing CTS authentication, the unparsed CTS security tag is returned in the authentication response and is displayed in the CTS authentication report viewer.</p> <p>Note There is no known workaround for this issue.</p>
CSCts03935	<p>Need to recreate the Support Bundle if the Admin session times out</p> <p>If the administrator is creating a Support Bundle and their login session times out, the Support Bundle is not created correctly and the administrator must produce a new one after logging back in again.</p> <p>Workaround Alternatively if the Support Bundle takes a long time to generate, you can also generate it using the backup-logs CLI command.</p>

Table 11 *Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)*

Caveat	Description
CSCts08980	<p>The Cisco ISE posture report dashlet returns an error code</p> <p>After clicking a sparkline from the Posture Compliance dashlet, the Cisco ISE Monitoring page returns the following:</p> <p>“Cannot execute the statement.</p> <p>SQL statement does not return a ResultSet object.</p> <p>SQL error #1: ORA-06502: PL/SQL: numeric or value error: character string buffer too small.</p> <p>ORA-06512: at “MNT.FILTER”, line 27</p> <p>ORA-06512: at “MNT.GETPOSTUREDATA”, line 17</p> <p>posturereport contains some special characters.”</p> <p>Workaround You can avoid this issue by running the report directly without filtering from the Monitoring > Reports > Catalog > Posture > Posture Detail Assessment page.</p>
CSCts10036	<p>Issue with Inline Posture static route configuration</p> <p>Certain static address settings at Inline Posture static route configuration page result in the Cisco ISE user interface returning an error and admin not being able to remove the erroneous route.</p> <p>Note Restarting the Inline Posture node following this event might result in the node not being available to the administrator at all.</p> <p>This issue can occur when you configure an invalid static route where the static route’s destination network address overlaps with the network address (based on the IP Address / Subnet Mask combination) of the Inline Posture node’s trusted or untrusted interface.</p> <p>Workaround If this situation occurs, deregister the Inline Posture node from the primary Administration ISE node (or both Inline Posture nodes of the HA pair) and then reregister.</p>
CSCts10323	<p>Internet Explorer running slow during client provisioning</p> <p>Internet Explorer has an option where you can turn the “check for revocation lists” function on or off.</p> <p>When this option is enabled and the dACL simultaneously does not allow access to CDP servers, Internet Explorer “freezes up” for about a minute while it tries to access the requisite CDPs.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCts19211	<p>After backup/restore, the administrator not able to access the Service Policy node</p> <p>After restoring the database from prior version of the software, one or more of the nodes in the deployment becomes inaccessible from the administrator user interface. The issue is related to restoring a backup image from one version onto a deployment running a newer version of Cisco ISE.</p> <p>Workaround Deregister, execute the reset-config CLI command, then reregister the node in question.</p> <p>Note This issue can be avoided completely by using the 'application upgrade' CLI on each node of the deployment. If this is done, there is no need to restore from an older version of the software.</p>
CSCts20529	<p>Authorization profile getting saved with incomplete information</p> <p>This issue occurs when using the “auto-smart-port,” “Filter_ID,” “wireless lan controller,” or “Posture Discovery” fields in the configuration page.</p> <p>Note Because of this mismatch in attribute values, the resulting authorization policy may not work properly.</p> <p>Workaround Click anywhere in the window while creating an authorization profile when using any of the above mentioned attributes. The authorization profile is then saved properly.</p>
CSCts22154	<p>RBAC menus on secondary nodes are incorrect immediately after upgrade</p> <p>This issue can occur when the upgrade process on a secondary node is delayed and there is a large number of pending messages in Primary node queued up for replication to the secondary node.</p> <p>Workaround Minimize the time period between the upgrade process on the primary node and secondary nodes.</p> <p>Note If the RBAC menu is not available following upgrade, wait until the replication status for the problematic node shows “complete” and the RBAC menu should be correctly visible.</p>
CSCts25521	<p>Cisco ISE repeatedly returns an error when a Dictionary Compound Condition is added during posture policy configuration</p> <p>When you attempt to configure Dictionary Compound Condition using Posture Policy configuration, Cisco ISE returns a “configured dictionary compound condition already exists” error message, even though the specified Dictionary Compound Condition does not yet actually exist.</p> <p>Workaround The administrator needs to click on the OK button several times, or reload the page to work through this issue.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCts78093	<p>Active Directory attributes are not inherited from Cisco ACS 5.1/5.2 to Cisco ISE 1.0 or Cisco ISE 1.0.4 during migration</p> <p>This issue has been observed for Active Directory attributes that are not of the data type “String.” (Cisco ISE supports only “String” Active Directory attributes. Other data types, such as integers, are not moved over.)</p> <p>Note In Cisco ACS 5.1/5.2, you can define different types of Active Directory attributes—String, IP, and integer.</p>
CSCts99778	<p>Posture configuration options not available with Advanced License</p> <p>After installing or upgrading to Cisco Identity Services Engine Maintenance Release 1.0.4.573, posture config options on Policy > Policy Elements > Conditions, Policy > Policy Elements > Results, and the Posture tab of the Policy > Posture page are not shown.</p> <p>Workaround Enter the application stop ise and application start ise CLI commands. All posture-related configuration items should now appear as designed.</p>
CSCts57010	<p>File system runs out of available space</p> <p>When logging in via the CLI, the administrator sees a “% Error: Unable to launch ADE-OS shell. Disk full.” message. This could be caused by an “undo_tablespace” function automatically extending without any imposed limit.</p> <p>Note There is no known workaround for this issue.</p>
CSCtr95156	<p>The guest account password was reset after the user changed their password and the Sponsor subsequently modified the account</p> <p>Workaround The Guest user should log in to the guest portal <i>before</i> the sponsor modifies their account.</p>
CSCts45591	<p>Unable to collect info from interface with no IP address</p> <p>Cisco ISE is unable to collect TCP dump information on interfaces with no IP address configured.</p> <p>Note There is no known workaround for this issue.</p>
CSCts57027	<p>Newly added network interface for VMware ISE appears as “__tmpXXXXX”</p> <p>This issue has been observed when viewing the newly-added network interface using the “show interface” CLI command on a VMWare machine.</p> <p>Workaround Try a different adapter setting like E1000 instead of “Flexible.”</p>
CSCts59228	<p>Internet Explorer 8 fails to Generate a CSV Template when importing endpoints</p> <p>Workaround Cisco recommends trying the process again using Mozilla Firefox if you encounter this issue.</p>
CSCts77187	<p>No Alarm activates when replication fails due to database communication errors</p> <p>This issue has been observed when the primary administration or monitoring node is unable to communicate with the secondary node for Oracle database replications.</p> <p>Note There is no known workaround for this issue.</p>

Table 11 Cisco ISE Release 1.0.4.573 Appliance Open Caveats (continued)

Caveat	Description
CSCts45441	<p>Unexpected behavior when creating a guest account using start and end time settings</p> <p>This issue has been observed where the sponsor is trying to create a guest account that includes the time profile type “STARTEND.” (During test, Cisco used the current date for the “start date” and the next day as the end date.</p> <p>Workaround When creating the guest account, use the “FROMCREATION” time profile with a 1 day duration.</p>
CSCts45547	<p>Administrator user interface does not display an appropriate error msg during node registration</p> <p>Note There is no known workaround for this issue.</p>
CSCtw67841	<p>Debug logs bundle is not getting downloaded in Mozilla Firefox version 3.6.24</p> <p>When the administrator tries to download an individual log via the Operations > Download Logs > Node > Debug Logs page, Cisco ISE prompts the administrator to enter their credentials in the browser. After entering the username and password, no download dialog pops up, and the requested log file cannot be downloaded. This issue has been observed using Mozilla Firefox version 3.6.24.</p> <p>Workaround Download the entire support bundle and then you can choose to view the individual log file.</p> <p>Note Windows Internet Explorer version 8 does not have this issue.</p>

Cisco ISE Release 1.0.4.573 Agent Open Caveats

Table 12 Cisco ISE Release 1.0.4.573 Agent Open Caveats

Caveat	Description
CSCti60114	<p>The Mac OS X agent 4.9.0.x install is allowing downgrade</p> <p>The Mac OS X NAC Agent is allowing downgrades without warnings.</p> <p>Note Mac OS X Agent builds differ in minor version updates only. For example, 4.9.0.638 and 4.9.0.637.</p>
CSCti71658	<p>The Mac OS X Agent shows user as “logged-in” during remediation</p> <p>The menu item icon for Mac OS X Agent might appear logged-in before getting full network accesses</p> <p>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.</p> <p>Workaround Please ignore the icon changes after detecting the server and before remediation is done.</p>

Table 12 Cisco ISE Release 1.0.4.573 Agent Open Caveats (continued)

Caveat	Description
CSCtj22050	<p>Certificate dialog seen multiple times when certificate is not valid</p> <p>When the certificate used by the agent to communicate with the server is not trusted, the error message can be seen multiple times.</p> <p>Workaround Make sure you have a valid certificate installed on the server and that it has also been accepted and installed on the client.</p> <p>Note The additional certificate error message is primarily informational in nature and can be closed without affecting designed behavior.</p>
CSCtj31552	<p>Pop-up Login windows option not used with 4.9 Agent and Cisco ISE</p> <p>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.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj39429	<p>No posture on Mac OS X Agent in multi-NIC setup</p> <p>This issue has been observed on Mac OS 10.6 clients in a multi-NIC setup where the wired NIC is connected to a switch and the wireless NIC connects to an Inline Posture node in bridged mode.</p> <p>Note Because the wireless NIC is the preferred connection, the agent is supposed to perform posture assessment via the wireless NIC.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj59635	<p>Cisco NAC agent pops up even when popup login window is unchecked</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtk34851	<p>XML parameters passed down from server are not using the mode capability</p> <p>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.</p> <p>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.</p>
CSCtl53966	<p>Agent icon stuck on Windows taskbar</p> <p>The taskbar icon should appear when the user is already logged in.</p> <p>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.</p>

Table 12 *Cisco ISE Release 1.0.4.573 Agent Open Caveats (continued)*

Caveat	Description
CSCtn39974	<p>An IP configuration error during logout may keep agent from appearing to the user</p> <p>The agent login processing does not start after the IP refresh error occurs during the logout processing in an Out-of-Band environment.</p> <p>Workaround Exit and re-launch the agent.</p>
CSCto03644	<p>Tray icon flickers click focus if user changes applications from login OK</p> <p>Following successful login, when the Agent login dialog goes away, click focus appears in the Windows taskbar tray. (It may flicker fast so that you are not able to see it.) If the user clicks on the icon when this happens, the “please wait” dialog appears, and at this time, the Agent icon options are available for use.</p> <p>This issue has been observed if the user changes to a different application while the successful login OK button is displayed.</p> <p>Workaround The user can log in again and ensure the focus stays on the login process.</p>
CSCto19507	<p>Mac OS X agent does not prompt for upgrade when coming out of sleep mode</p> <p>Workaround The user needs to exit and then restart the Cisco NAC Agent to prompt the current version verification function.</p>
CSCto33933	<p>Login Success display does not disappear when user clicks OK</p> <p>This can occur if the network has not yet settled following a network change.</p> <p>Workaround Wait a few seconds for the display to close.</p>
CSCto45199	<p>“Failed to obtain a valid network IP” message does not go away after the user clicks OK</p> <p>This issue has been observed in a wired NAC network with IP address change that is taking longer than normal. (So far, this issue has only been only seen on Windows XP machines.)</p> <p>Workaround None. The user needs to wait for the IP address refresh process to complete and for the network to stabilize in the background.</p>
CSCto48555	<p>Mac OS X agent does not rediscover the network after switch from one SSID to another in the same subnet</p> <p>Agent does not rediscover until the temporary role (remediation timer) expires.</p> <p>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.</p>
CSCto63069	<p>The nacagentui.exe application memory usage doubles when using “ad-aware”</p> <p>This issue has been observed where the nacagentui.exe memory usage changes from 54 to 101MB and stays there.</p> <p>Workaround Disable the Ad-Watch Live Real-time Protection function.</p>

Table 12 Cisco ISE Release 1.0.4.573 Agent Open Caveats (continued)

Caveat	Description
CSCto84932	<p>The Cisco NAC Agent takes too long to complete IP refresh following VLAN change</p> <p>The Cisco NAC agent is taking longer than normal to refresh IP address due to double IP refresh by supplicant and NAC agent.</p> <p>Workaround Disable the Cisco NAC Agent IP address change function if there is a supplicant present capable of doing the same task.</p>
CSCto97422	<p>Auto Popup does not happen after clicking Cancel during remediation failure</p> <p>Workaround Click on the login option in the system tray.</p>
CSCto97486	<p>The Mac OS X VLAN detect function runs between discovery, causing a delay</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Workaround Disconnect and then reconnect the client machine to the network.</p>
CSCtq02332	<p>Windows agent does not display IP refresh during non-compliant posture status</p> <p>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).</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtq02533	<p>The Cisco NAC Agent takes too long to complete IP refresh following VLAN change</p> <p>The Cisco NAC agent is taking longer than normal to refresh IP address due to double IP refresh by supplicant and Cisco NAC agent.</p> <p>Workaround Disable the Cisco NAC Agent IP address change function if there is a supplicant present capable of doing the same task.</p>
CSCtq15958	<p>Windows Agent VPN tunnel dropping after initial connection</p> <p>Workaround The user needs to reestablish the VPN tunnel.</p>

Table 12 **Cisco ISE Release 1.0.4.573 Agent Open Caveats (continued)**

Caveat	Description
CSCtq16716	<p>Windows wireless move from post-posture to pre-posture VLAN detect IP not refreshed</p> <p>The client machine has no connectivity because the NIC's IP address is in the complaint/non-compliant VLAN when it should be in the pre-posture/pending VLAN.</p> <p>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.</p> <p>Workaround Disconnect and reconnect wireless NIC on the client machine.</p> <p>For more information, see Known Supplicant Compatibility Issue Involving VLAN Change Operation on Windows Client Machines, page 54.</p>
CSCts80116	<p>OPSWAT SDK 3.4.27.1 causes memory leak on some PCs</p> <p>Client machines that have version 8.2.0 of Avira AntiVir Premium or Personal may experience excessive memory usage.</p> <p>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.</p> <p>Workaround Install later version of Avira AntiVir Premium or Personal.</p>

Cisco ISE Release 1.0.4 Resolved Caveats

- [Cisco ISE Release 1.0.4.573 Appliance Resolved Caveats, page 51](#)
- [Cisco ISE Release 1.0.4.573 Agent Resolved Caveats, page 52](#)

Cisco ISE Release 1.0.4.573 Appliance Resolved Caveats

Table 13 *Cisco ISE Release 1.0.4.573 Appliance Resolved Caveats*

Caveat	Description
CSCth07037	CPM crash after configuring AD1 and starting RADIUS authentications
CSCtn26819	Unable to reset the CLI password of a “locked” user account
CSCtn80646	Cisco ISE does not display a purge confirmation message after purging is completed
CSCto05028	Issues when saving customized details reports (cannot retrieve reports after saving)
CSCto22872	Endpoints are not profiled correctly when there is a router in the network
CSCto75963	No alert message is displayed in Cisco ISE when the Client Provisioning Update Feed URL (or proxy, if specified) is unreachable
CSCto80921	Invalid PCAP format for inactive Monitoring and Troubleshooting nodes
CSCto83078	Guest Accounting and Sponsor Summary report errors returned during report generation
CSCto92848	Report generation fails when custom range in Security Group Access - > Top_N_SGT_Assignments is specified
CSCtq03906	Condition duplication during Authorization Policy configuration does not work properly
CSCtq05485	AnyConnect Supplicant from AnyConnect 2.5/3.0 client application
CSCtq06649	Getting “Connection reset,” message when adding a secondary node
CSCtq07398	Internal user-name should not be case-sensitive
CSCtq08234	Airespace-QoS-Level configured on Cisco ISE does not override WLAN QoS level
CSCtq21992	Active Directory guest user login displays an application malfunction error
CSCtq22287	WSUS check is failing on Windows 7 64- and 32-bit systems
CSCtq24831	Guest user can not log into newly created account
CSCtq26502	Windows XP client machines need to be updated for NAC agent to work
CSCtq27834	Monitoring COPY_RESOURCE_HIERARCHY exception errors and replication failures
CSCtq27834	Cisco ISE is generating replication alarms
CSCtq45022	The Deployment Nodes page takes a very long time to load in scale deployment
CSCtq66518	Deleting the SGACL mapping from Cisco ISE does not clear the downloaded policy
CSCtq79343	Heap memory is completely used up and system becomes unusable
CSCtq84962	Mobile devices/Linux appliances do not work through VPN deployment
CSCtq88761	The Authorization Profile page takes 6 minutes or more to load

Table 13 *Cisco ISE Release 1.0.4.573 Appliance Resolved Caveats (continued)*

Caveat	Description
CSCtq89875	Administrators cannot enable the password-lockout CLI function via SSH connection
CSCtq95286	Report issues with Guest Accounting
CSCtr01270	Active endpoint information is not correct in the Monitoring and Troubleshooting dashboard
CSCtr21259	Administrators are not able to log into the user interface after a reboot/restart
CSCtr29815	Axis MessageContext.finalize() entry causing memory usage issue
CSCtr75664	Specifying a new remote logging target can crash a Policy Service node
CSCts19809	Cannot import Advanced License on top of Base License
CSCts27128	“show app status ise” reports wrong status when database instance is dead
CSCts45559	Incorrect information displayed when eth1 interface selected
CSCts45675	Profiler does not see DHCP SPAN traffic encapsulated with 802.1Q
CSCts46545	Cisco ISE high EPM database usage alarm
CSCts46937	Unable to access Inline Posture node—error message displayed while reading DHCP/DNS config object
CSCts51536	Admin is not able to download dump info on eth1 interface
CSCts54380	ORA-600/ORA-4031 error code displayed due to memory allocation for Oracle streams
CSCts59135	Cisco ISE database has a static Oracle DB password
CSCts79733	Getting Error parsing DHCP “[V4] option [subnet-mask (1)]; Expected [4] b”
CSCui22841	Apache Struts2 command execution vulnerability

Cisco ISE Release 1.0.4.573 Agent Resolved Caveats

Table 14 *Cisco ISE Release 1.0.4.573 Appliance Resolved Caveats*

Caveat	Description
CSCtg97488	Client running Cisco NAC Agent does not disconnect after Windows logoff
CSCto34354	Cisco NAC Web Agent fails to validate Registry Conditions

Known Issues

- [Known Issue with Upgrade from Cisco ISE Release 1.0.3.377, page 53](#)
- [Windows Internet Explorer 8 Known Issues, page 53](#)
 - [Issue Accessing the Cisco ISE Administrator User Interface](#)
 - [Cisco Secure ACS-to-Cisco ISE Migration User Interface Issue Using IE8](#)
 - [User Identity Groups User Interface Issue With IE 8](#)

- [Known Supplicant Compatibility Issue Involving VLAN Change Operation on Windows Client Machines, page 54](#)
- [Known Incompatibility Issue with WLC Firmware Version 7.0.116.0, page 54](#)
- [Issues With 2k Message Size in Monitoring and Troubleshooting, page 55](#)
- [Issues With More Than Three Users Accessing Monitoring and Troubleshooting Concurrently, page 55](#)
- [Inline Posture Restrictions, page 55](#)
- [Cisco IP phones using EAP-FAST, page 55](#)

Known Issue with Upgrade from Cisco ISE Release 1.0.3.377

This issue can affect Cisco ISE customers who have not changed their default “admin” account password for administrator user interface login since first installing Cisco Identity Services Engine Release 1.0.3.377. Upon upgrading to Cisco Identity Services Engine Maintenance Release 1.0.4.573, administrators can be “locked out” of the Cisco ISE administrator user interface when logging in via the default “admin” account where the password has not yet been updated from the original default value.

To avoid this issue, Cisco recommends you do one or more of the following:

1. Verify they have changed password per the instructions in the “Managing Identities” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0.4* prior to upgrade.
2. Disable or modify the password lifetime setting in the **Administration > System > Admin Access > Password Policy** page of the administrator user interface *prior* to upgrade to ensure the upgraded policy behavior does not impact the default “admin” account.
3. Enable password lifetime setting reminders in the **Administration > System > Admin Access > Password Policy** page to alert admin users of imminent expiry. Administrators should change the password when notified.



Note

Although the above conditions apply to all administrator accounts, the change in behavior from Cisco ISE version 1.0.3.377 to version 1.0.4.573 only impacts the default “admin” account.

Windows Internet Explorer 8 Known Issues

- [Issue Accessing the Cisco ISE Administrator User Interface](#)
- [Cisco Secure ACS-to-Cisco ISE Migration User Interface Issue Using IE8](#)
- [User Identity Groups User Interface Issue With IE 8](#)

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 your session to a different location. This situation occurs when you install a real SSL certificate issued by a Certificate Authority like VeriSign.

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

For more information see [CSCto09989](#).

Cisco Secure ACS-to-Cisco ISE Migration User Interface Issue Using IE8

There is a known migration consideration that affects successful migration of Cisco Secure ACS 5.1/5.2 data to the Cisco ISE appliance using the Cisco Secure ACS 5.1/5.2-ISE 1.0 Migration Tool.

The only currently supported browser for downloading the migration tool files is Firefox version 3.6.x. Microsoft Windows Internet Explorer (IE8 and IE7) browsers are not currently supported for this function.

For more information, see the [Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4](#).

User Identity Groups User Interface Issue With IE 8

If you create and operate 100 User Identity Groups or more, a script in the Cisco ISE administrator user interface **Administration > Identity Management > User Identity Groups** page 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 VLAN change for wireless deployments. The client machine has no connectivity because the NIC's IP address is in the complaint/non-compliant VLAN when it should be in the pre-posture/pending VLAN.



Note

This issue affects any supplicant that cannot perform 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](#).

Known Incompatibility Issue with WLC Firmware Version 7.0.116.0

Cisco has discovered a known issue that can occur during a Wireless LAN Controller (WLC) login session, where the client machine authenticates with Cisco ISE correctly and the corresponding authorization profile is picked up, but during user authentication the previous authorization profile (for machine authentication) is applied to the user session again.

This issue has been observed during wireless login scenarios where the WLC is running firmware version 7.0.116.0, and unless you require new features available only in version 7.0.116.0, Cisco recommends returning your WLC firmware version to 7.0.98.218 until Cisco releases an up-to-date firmware version later in 2011.

For more information see [CSCto83897](#).

Issues With 2k 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 2k message sizes regularly.

Issues With More Than Three Users Accessing Monitoring and Troubleshooting Concurrently

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 (CDP) is not supported by Inline Posture.

Cisco IP phones using EAP-FAST

Cisco ISE, Release 1.0 does not support Cisco IP phones that are using EAP-FAST with certificates. Cisco recommends using EAP-TLS with IP phones in your network.

Documentation Updates

Table 15 *Updates to Release Notes for Cisco Identity Services Engine, Release 1.0.4*

Date	Description
8/14/13	Added Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 6, page 17
9/7/12	Added Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 5, page 18
3/7/2012	Added Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 4, page 19
12/15/2011	Updated Cisco ISE Install Files, Updates, and Client Resources, page 14
12/8/2011	<ul style="list-style-type: none"> • Added Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 3, page 19 • Added caveat CSCtw67841 to Cisco ISE Release 1.0.4.573 Appliance Open Caveats, page 22

Table 15 **Updates to Release Notes for Cisco Identity Services Engine, Release 1.0.4**

Date	Description
11/3/2011	Added Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 2 , page 20
10/21/2011	<ul style="list-style-type: none"> Added Cisco Identity Services Engine Releases, page 2 Added Resolved Issues in Cisco ISE Version 1.0.4.573—Cumulative Patch 1, page 21 Updated trademarks block under Obtaining Documentation and Submitting a Service Request, page 58
10/13/2011	<ul style="list-style-type: none"> Added CSCts57010, CSCtt16149, CSCtr95156, CSCts45591, CSCts57027, CSCts59228, CSCts77187, CSCts45441, and CSCts45547 to Cisco ISE Release 1.0.4.573 Appliance Open Caveats, page 22 Updated Upgrading Cisco ISE Software, page 9 Added Known Issue with Upgrade from Cisco ISE Release 1.0.3.377, page 53
9/30/2011	<p>Content updates for Cisco Identity Services Engine Maintenance Release 1.0.4 Update (version 1.0.4.573):</p> <ul style="list-style-type: none"> Updated Table 3 on page 8 Cisco ISE Installation and Upgrade Process Updates, page 11 Added caveats CSCts78093, CSCts98931, and CSCts99778 to Cisco ISE Release 1.0.4.573 Appliance Open Caveats, page 22 Added caveat CSCts80116 to Cisco ISE Release 1.0.4.573 Agent Open Caveats, page 46 Added caveats CSCth07037, CSCto80921, CSCts19809, CSCts27128, CSCts45559, CSCts45675, CSCts46545, CSCts46937, CSCts51536, CSCts54380, CSCts59135, and CSCts79733 to Cisco ISE Release 1.0.4.573 Appliance Resolved Caveats, page 51
8/26/2011	Cisco Identity Services Engine Maintenance Release 1.0.4 (version 1.0.4.558):

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 16 *Product Documentation for Cisco Identity Services Engine*

Document Title	Location
<i>Release Notes for the Cisco Identity Services Engine, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
<i>Cisco Identity Services Engine Network Component Compatibility, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
<i>Cisco Identity Services Engine User Guide, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
<i>Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
<i>Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
<i>Cisco Identity Services Engine API Reference Guide, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
<i>Cisco Identity Services Engine Troubleshooting Guide, Release 1.0.4</i>	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
<i>Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card</i>	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

Platform-Specific Documents

Links to Policy Management Business Unit documentation are available at the following locations:

- Cisco ISE
http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.