



Release Notes for Cisco Identity Services Engine, Release 1.1

Revised: October 21, 2013, OL-25539-01

Contents

These release notes describe the features, limitations and restrictions (caveats), and related information for Cisco Identity Services Engine (ISE), Release 1.1. These release notes supplement the Cisco ISE documentation that is included with the product hardware and software release, and cover the following topics:

- [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 11](#)
- [Cisco ISE License Information, page 11](#)
- [New Features in Release 1.1, page 13](#)
- [Cisco ISE Install Files, Updates, and Client Resources, page 19](#)
- [Cisco ISE Antivirus and Antispyware Support, page 22](#)
- [Integration with Cisco Prime Network Control System, page 22](#)
- [Cisco ISE Patch Release Updates, page 22](#)
- [Cisco ISE Release 1.1 Open Caveats, page 26](#)
- [Cisco ISE Release 1.1 Resolved Caveats, page 51](#)
- [Known Issues, page 55](#)
- [Documentation Updates, page 57](#)
- [Related Documentation, page 58](#)



Americas Headquarters:

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

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.
Persona	The persona or personas of a node determine the services provided by a node. A 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 and Personas

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. It is recommended that the Monitoring persona be on a separate, designated node for higher performance in terms of data collection and report launching.

- 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 up to 10,000 Inline Posture nodes in a deployment. You can pair two Inline Posture nodes together for high availability as a failover pair.



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.

The following table lists the recommended minimum and maximum number of nodes/personas in a distributed deployment:

Table 2 *Deployment Nodes/Personas*

Node / Persona	Minimum Number in a Deployment	Maximum Number in a Deployment
Admin	1	2 (Configured as an HA pair)
Monitor	1	2 (Configured as an HA pair)
Policy Service	1	<ul style="list-style-type: none"> 2 — when all personas (Admin/Monitor/Policy Service) are on same appliance 5 — when Admin and Monitor personas are on same appliance 40 — when each persona is on a dedicated appliance
Inline Posture	0	10k for maximum NADs per deployment

- One primary Administration node and one secondary Administration node
- One primary Monitoring node, with an optional secondary node
- One or more Policy Service nodes
- One primary Inline Posture node, with an optional secondary node

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 1.1* 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 Devices, Browsers, and Agents, page 7](#)

**Note**

For more details on Cisco ISE hardware platforms and installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

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 3](#).

Table 3 **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 3 **Supported Hardware and Personas (continued)**

Hardware Platform	Persona	Configuration
Cisco ISE-VM-K9 (VMware)	Stand-alone Administration, Monitoring, and Policy Service (no Inline Posture)	<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 (you can install up to 4 NICs) • Supported VMware versions include: <ul style="list-style-type: none"> – ESX 4.x – ESXi 4.x – For an evaluation or production version, the minimum disk space is 60 GB.

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 Devices, Browsers, and Agents

Refer to *Cisco Identity Services Engine Network Component Compatibility, Release 1.1* for information on supported devices, browsers, and agents.

Supported Microsoft Active Directory

Cisco ISE works with Microsoft Active Directory servers 2003, 2003 R2, 2008, and 2008 R2 at all functional levels. Microsoft Active Directory version 2000 or its functional level are not supported by Cisco ISE.

Installing Cisco ISE Software

The following steps summarize how to install new Cisco ISE Release 1.1 DVD software on supported hardware platforms (see [Supported Hardware, page 5](#) for support details).

With Cisco ISE Release 1.1, 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.



Note

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

- 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-1.1.0.665.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 1.1*. Before you run the setup program, ensure that you know the configuration parameters listed in [Table 4](#).

Table 4 *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. It is recommended that the hostname be all lower case, because that is most compatible.	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 (.). Note It is recommended that the domain name be all lower case, because that is most compatible.	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 1.1 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.	PST
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 4 **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 58](#) 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 2 (MR2) previously and are planning to upgrade to the latest Cisco ISE Release, review the open caveats in this section before following the upgrade instructions in the “Upgrading Cisco ISE” chapter of the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.1](#).

This section covers the following upgrade issues:

- [Upgrade from Cisco ISE 1.0.4 to 1.1 with Inline Posture, page 10](#)
- [Upgrade from Cisco ISE Release 1.0.3.377, page 11](#)

Upgrade from Cisco ISE 1.0.4 to 1.1 with Inline Posture

In ISE 1.1, the Inline Posture node uses certificate based authentication and cannot connect to the Administrative ISE node. Therefore you are required to disconnect the Inline Posture node from the deployment prior to starting the upgrade procedure, then reconfigure the Inline Posture node after the upgrade. To do so, follow the procedure outlined in this section.



Warning

You must have the proper certificates in place for your Inline Posture deployment to mutually authenticate.

Prerequisite

Record all the configuration data for your Inline Posture node *before* you de-register the node. Alternatively, you can save screenshots of each of the Inline Posture tabs (in the Admin user interface) to record the data. Having this data on hand speeds up the process of re-registering the Inline Posture node to complete the following task.

To upgrade to Cisco ISE 1.1 with Inline Posture, complete the following steps:

Step 1 From the Cisco Administration ISE node, de-register the Cisco Inline Posture node.



Note

You can verify that the Inline Posture node has returned to ISE node status by going to the CLI and entering the following command: **show application status ise** If you discover that the node has not reverted to an ISE node, then you can enter the following at the command prompt: **pep switch outof-pep** However, it is recommended that you only do this as a last resort.

Step 2 Upgrade the Cisco Administration ISE node to 1.1, as described in the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.1](#).

Step 3 Import CA root certificate, make CSR, create certificates on the Administration ISE node.



Note

Certificates must have extended key usage for both client authentication and server authentication. For an example of this type of extended key usage, see the Microsoft CA Computer template.

Step 4 Perform a fresh installation of ISE 1.1 on the ISE node (that was the former Inline Posture node), as described in the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.1](#).

Step 5 Import CA root certificate, make CSR, create certificates on the ISE node (that was the former Inline Posture node), now in standalone mode.



Note

Certificates must have extended key usage; client authentication and server authentication. For example, select the computer template from Microsoft CA.

Step 6 Register the newly upgraded ISE Node as an Inline Posture node.

Step 7 Reconfigure the Cisco Inline Posture node.

Upgrade from Cisco ISE Release 1.0.3.377

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. 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, 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 1.1* 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 only impacts the default “admin” account.

Cisco Secure ACS to Cisco ISE Migration

Complete instructions for moving your Cisco Secure ACS 5.1 or 5.2 database to Cisco ISE Release 1.1 are covered in the *Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1*.



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 ISE environment. Microsoft Windows Internet Explorer (IE8 and IE7) browsers are not currently supported in this release.

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 5](#) 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 5 **Cisco ISE License Types and Supported Services**

Cisco ISE License Type	Supported Services
Base package—Provides authenticated network access, guest life-cycle management, and monitoring and troubleshooting.	<ul style="list-style-type: none"> • Basic Network Access • Guest Management • Link encryption
Advanced package—Provides posture, profiling, 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 • Endpoint Protection Services
<p>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.</p> <p>If you currently subscribe to a Wireless License model for your deployment and then decide you want to offer Cisco ISE support for non-wireless endpoints on your network, rather than revert to a Base and Advanced License scheme as described earlier, you can move to a Wireless Upgrade License. These licenses are designed to provide the full range of Cisco ISE functions and policy management capabilities for all wireless and non-wireless client access methods, including wired and VPN concentrator access.</p>	<ul style="list-style-type: none"> • Basic Network Access • Guest Management • Link encryption • Profiler • Posture • Security Group Access • Endpoint Protection Services

**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 1.1*.

For specific information on adding, modifying, and removing license files, see the “Managing Licenses” chapter of the *Cisco Identity Services Engine User Guide, Release 1.1*.

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.

New Features in Release 1.1

Cisco ISE Release 1.1 offers the following features and services:

- [Endpoint Protection Services, page 13](#)
- [FIPS 140-2 Level 1 Compliance, page 13](#)
- [Common Access Card Support, page 14](#)
- [Internationalization and Localization, page 15](#)
- [IOS Sensor for Profiling, page 15](#)
- [NMAP Probe, page 15](#)
- [OCSP Support, page 16](#)
- [SGA Support, page 16](#)
- [New Look for the User Interface, page 16](#)
- [Device Registration WebAuth, page 17](#)
- [Simple URL for Sponsor Portal Access, page 17](#)
- [Creating a Custom Portal Theme, page 17](#)
- [Network Time Protocol \(NTP\) Server Authentication, page 17](#)
- [External Authentication for Administrator Users, page 18](#)
- [Simplified Posture Policy Configuration, page 18](#)
- [Support Bundle Password Protection, page 18](#)
- [Updated VMware Machine Capabilities, page 18](#)
- [Enhanced Security for Sponsor and Guest Portals, page 18](#)

For more information on key features of Cisco ISE, see the Overview chapter of the *Cisco Identity Services Engine User Guide, Release 1.1*.

Endpoint Protection Services

Endpoint Protection Services (EPS) is a service that runs on the Cisco Identity Services Engine Administration node to extend the monitoring and controlling endpoints. Endpoint Protection Services (EPS) is administered from the central Cisco ISE Admin dashboard, and can be used to monitor and change the authorization state of an endpoint without having to modify the overall Authorization Policy of the system. EPS supports wired and wireless deployments. You can find this new function on the **Operations > Endpoint Protection Service > Endpoint Operations History** page.

FIPS 140-2 Level 1 Compliance

Cisco ISE supports Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance. FIPS 140-2 is a United States government computer security standard used to accredit cryptographic modules. The FIPS standard places limitations on use of certain algorithms, and in order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via RADIUS Key Management measures. While in FIPS mode, any attempt to perform

functions using a non-FIPS compliant algorithm fails, and as such, certain authentication functionality is disabled. To help accommodate FIPS 140-2 compliance, Cisco ISE now also features SHA-256 encryption capability.

When you turn on FIPS mode in Cisco ISE, the following functions are impacted:

- 802.1X environment
 - EAP-FAST
 - EAP-TLS
 - PEAP
 - RADIUS



Note

Other protocols like EAP-MD5, LEAP, PAP, and CHAP are not compatible with a FIPS 140-2 compliant system and will be disabled while Cisco ISE is in FIPS mode.

- SSH clients can only use SSHv2
- LDAP over SSL
- Inline Posture node RADIUS Key Wrap
- HTTPS protocol communication for both Administrator ISE nodes and Inline Posture nodes

This new feature affects the following Cisco ISE configuration pages:

- **Administration > System > Settings > FIPS Mode**
- **Administration > Network Resources > Network Devices > Default Device**
- **Administration > Network Resources > Network Devices > Authentication Settings**
- **Administration > Network Resources > External RADIUS Servers**
- **Administration > System > Certificates > Local Certificates**
 - **Generate Self-Signed Certificate**
 - **Generate Certificate Signing Request**

Common Access Card Support

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee of, for example, the U.S Department of Defense (DoD). Access via the CAC requires a card reader into which the user inserts the card and enters a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

See also [OCSP Support, page 16](#).

Internationalization and Localization

Cisco ISE internationalization adapts the user interface for supported languages. Localization of the user interface incorporates locale-specific components and translated text.

In Cisco ISE, Release 1.1 internationalization (UTF-8) and localization support is focused on the text and information that is presented to end user (connecting to Cisco ISE) through the Sponsor, Guest, and Client Provisioning portals. This support includes internationalizing all text in the end user interfaces, such as labels, messages, and input configured by the end user or Cisco ISE administrator and displayed in the Sponsor, Guest, and Client Provisioning portals. Guest account information that is notified through email and SMS is also localized.

Cisco ISE, Release 1.1 provides localization and internationalization support for the following languages:

- Chinese (traditional), Chinese (simplified)
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian
- Spanish



Note

The Administrative user interface is presented in English only, and is not localized. Only configurable fields that can be seen by the end user support UTF-8 values.

For details on this new feature as it applies to the Administrative user interface, see the “Understanding the User Interface” chapter of the [Cisco Identity Services Engine User Guide, Release 1.1](#).

IOS Sensor for Profiling

Integration of an IOS sensor enabled switch with Cisco ISE consists of an IOS sensor, the data collector that is embedded in the network device (switch) for gathering DHCP, CDP and LLDP data, and analyzers for processing these data and determining device-type of endpoints. The distinct advantage of embedding a sensor in the switch is that the sensor is the closest point present to the source of data.

Implementing an IOS based sensor that is embedded in the switch resolves any topology restriction on your deployment that you might have in the previous releases due to the nature of event collection of endpoint attributes from various probes. It allows Cisco ISE runtime and the Cisco ISE profiler to collect any or all the attributes that are sent from the switch. You can collect DHCP, CDP and LLDP attributes directly from the switch by using an already existing RADIUS protocol. The attributes that are collected for DHCP, CDP and LLDP are then parsed and mapped to attributes in the Cisco ISE dictionaries.

NMAP Probe

Network Mapper (NMAP) is integrated with Cisco ISE to augment its profiling capability for better endpoints classification, particularly iDevices and other mobile devices. You can either perform a manual subnet scan on a specific subnet by using the Network Scan probe, or associate a network scan action to an endpoint profile (a specific profile) that performs a scan on an endpoint.

A network scan is very specific to scanning a subnet on your network by using the Network Scan probe from the primary Administration ISE node. It allows you to detect endpoints on the specified subnet, their operating systems, and SNMP ports (UDP 161 and 162) in any distributed deployment. You can also scan a subnet from the Policy Service nodes in a distributed deployment.

An endpoint scan is very specific to scanning an endpoint profiling policy that limits resources usage when compared to resource intensive network scans. It improves the overall classification of endpoints, and redefines an endpoint profile for an endpoint.

Profiling Network Scan Actions

A network scan action is a single configurable action, which is associated to an endpoint profiling policy. This association triggers a network scan action, when the profiling policy matches, and at least one of the network scan rules matches in profiling endpoints in Cisco ISE.

You can define, and associate one or more network scan rules in a single endpoint profiling policy. You can also define the type of scanning in each of the network scan action.

OCSP Support

In Cisco ISE Release 1.1, you can now communicate with Online Certificate Status Protocol (OCSP) servers over HTTP to check and validate the status of X.509 digital certificates. OCSP is an alternative to the CRL (Certificate Revocation List) and addresses issues resulting in handling CRLs. The OCSP configuration in Cisco ISE is configured in a reusable configuration object that can be referenced from any Certificate Authority (CA) Certificate that is configured in ISE.

You can also now configure CRL and/or OCSP verification per CA. If both are selected, then Cisco ISE first performs verification over OCSP and if a communication problem is detected with both the primary and secondary OCSP servers, or if unknown status is returned for a given certificate, Cisco ISE will fall over to perform CRL checking.

SGA Support

The SGA egress table function available in Cisco ISE Release 1.1 lists source and destination SGTs that have SGACLs assigned. This enhanced page provides multiple types of views, as well as better filtering and presentation capabilities. You can filter the egress table to view specific policies and save custom views. When the source SGT tries to reach the destination SGT, the SGA-capable device enforces the SGACLs based on the SGA policy as defined in the Egress Policy. Cisco ISE creates and provisions the policy.

After you create the SGTs and SGACLs (the basic building blocks required to create an SGA policy), you can establish a relationship between them by assigning SGACLs to source and destination SGTs.

New Look for the User Interface

The Cisco ISE Admin user interface has been updated with a new skin, or color theme. For an overview of these changes, see the “Understanding the User Interface” chapter of the [Cisco Identity Services Engine User Guide, Release 1.1](#).

Device Registration WebAuth

Device Registration WebAuth (DRW) is a new type of guest portal for allowing only Acceptable use Policy (AUP) access to the network (no user ID/password). You must configure a portal and direct the NAD to that portal via Cisco ISE. The URL Cisco ISE uses to get to this portal is something similar to:

```
https://<ISE-ID>:8443/guestportal/portals/<DRW-PORTAL-NAME>/portal.jsp
```

After initial redirection, the standard guest URLs (<https://<ISE-ID>:8443/guestportal/...>) handle the portal traffic. You configure the DRW portal using the **Administration > Guest Management > Settings**, then **Guest > Multiportal Configuration > <DRW-PORTAL-NAME>** pages. For more information, see the “User Access Management” chapter of the [Cisco Identity Services Engine User Guide, Release 1.1](#).

Simple URL for Sponsor Portal Access

The Simple URL is a new configuration parameter in the administrator user interface **Administration > Guest Management > Settings** then **General > Ports** pages. The URL you enter here (“mysponsor.cisco.com,” for example) requires on a DNS entry to point to the Cisco ISE. (Tomcat redirects this incoming request to the sponsor so that a URL like <http://mysponsor.cisco.com> goes to <https://<ISE-ID>:8443/sponsorportal> and the sponsor is then able to log in. For more information, see the “User Access Management” chapter of the [Cisco Identity Services Engine User Guide, Release 1.1](#).

Creating a Custom Portal Theme

A Cisco ISE admin now has the ability to interactively customize all customer facing portals, easily modifying backgrounds, colors, and logos to their company branding standards. For more information, see the “User Access Management” chapter of the [Cisco Identity Services Engine User Guide, Release 1.1](#).

Network Time Protocol (NTP) Server Authentication

In Cisco ISE Release 1.1, you can also specify whether or not Cisco ISE should use only authenticated NTP servers and enter one or more authentication keys for that purpose. When you configure one or more authentication keys, you can use the available options in the administrator user interface to specify the key ID number, key value, and whether the key in question is trusted.

This feature enhancement affects the **Administration > System > Settings > System Time** configuration function.

External Authentication for Administrator Users

In Cisco ISE Release 1.1, you now have the option to provide administrator user authentication via an external identity store like Active Directory, LDAP, or RSA SecurID. There are two models you can use to provide authentication via an external identity store:

- External Authentication + External Authorization—where there are no credentials specified on the local Cisco ISE database for the administrator ID in question, and authorization is based on external identity store group membership only.
- External Authentication + Internal Authorization—where the administrator's authentication credentials come from the external identity source, and authorization and administrator role assignment takes place using the local Cisco ISE database. (This method requires you to configure the same credentials in both the external identity store as well as the local Cisco ISE database.)

Simplified Posture Policy Configuration

In Cisco ISE, Release 1.1, it simplifies posture policies configuration in three steps on the Posture Policy page itself without navigating away to other configuration pages for posture requirements, conditions and remediation actions.

Earlier, it involves multiple steps to configure a posture policy to be in-place on the Posture Policy page by navigating away to many configuration pages for posture conditions, posture remediation actions, and posture requirements. You must use the Requirements page to associate posture conditions and posture remediation actions to it before creating a new posture policy, and then the Posture Policy page after that to associate posture requirements to the new posture policy.

Support Bundle Password Protection

The support bundle is password protected in ISE 1.1, through the use of GPG encryption. When you attempt to download the support bundle through the Admin user interface, you are now prompted for an encryption key.

Downloading the support bundle from CLI also requires an encryption key as well. The following is an example of the syntax. For more information, see the [Cisco Identity Services Engine CLI Reference Guide, Release 1.1](#).

```
# backup-logs <file name> repository <repository name> encryption-key plain
<encryption-key> | hash <hashed encryption-key>
```

Updated VMware Machine Capabilities

For complete information on updated Cisco ISE virtual machine capabilities, see the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.1](#).

Enhanced Security for Sponsor and Guest Portals

As part of security enhancement, you can no longer access Sponsor and Guest Portals over HTTP.

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 19](#)
- [Cisco ISE Live Updates, page 19](#)
- [Cisco ISE Offline Updates, page 20](#)

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 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. 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 1.1*.

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 1.1*.

- **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 1.1*.

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 20](#).

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 1.1*.

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 1.1 Supported Windows AV/AS Products](#)
- [Cisco Identity Services Engine Release 1.1 Supported Mac OS X AV/AS Products](#)

Integration with Cisco Prime Network Control System

Cisco Identity Services Engine, Release 1.1 integrates with Cisco Prime Network Control System (Prime NCS), Release 1.2 to manage wired and wireless networks.

Cisco ISE Patch Release Updates

- [Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 5, page 22](#)
- [Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 4, page 23](#)
- [Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 3, page 23](#)
- [Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 2, page 24](#)
- [Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 1, page 25](#)

Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 5

lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.1.0.665 cumulative patch 4.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.1.0.665 (with or without patch 1, 2, and 3 applied), otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.1.0.665.”

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

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

Table 6 *Cisco ISE Patch Version 1.1.0.665—Patch 5 Resolved Caveats*

Caveat	Description
CSCuj51094	Captured TCPDump file is not working This fix addresses an issue where an exception occurred when opening a captured TCPDump file.

Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 4

Table 7 lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.1.0.665 cumulative patch 4.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.1.0.665 (with or without patch 1, 2, and 3 applied), otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.1.0.665.”

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

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

Table 7 Cisco ISE Patch Version 1.1.0.665—Patch 4 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 1.1.0.665—Cumulative Patch 3

Table 8 lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.1.0.665 cumulative patch 3.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.1.0.665 (with or without patch 1 or 2 applied), otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.1.0.665.”

To obtain the patch file necessary to apply the patch to Cisco ISE Release 1.1, 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*. for instructions on how to apply the patch to your system. When you apply Cisco Identity Services Engine Maintenance Release 1.1.0.665 cumulative patch 3 to your Cisco ISE machine via the administration user interface, the end of the patch application process automatically reboots your machine a second time to complete patch application.

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

Table 8 *Cisco ISE Patch Version 1.1.0.665—Patch 3 Resolved Caveats*

Caveat	Description
CSCtz46247	After deregistering a secondary node from the deployment, there is no valid license 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.
CSCtz54548	Evaluation license validity date is wrong on de-registered secondary node 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. Note This issue has observed using both three- and five-year Base and Advanced term licenses.

Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 2

[Table 9](#) lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.1.0.665 cumulative patch 2.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.1.0.665 (with or without patch 1 applied), otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.1.0.665.”

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

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

Table 9 *Cisco ISE Patch Version 1.1.0.665—Patch 2 Resolved Caveats*

Caveat	Description
CSCtx85616	Cisco ISE logs reveal multiple “unlatch” errors when disconnecting from Active Directory This fix addresses an issue in Cisco ISE, Release 1.1 using the Active Directory Authentication method where Cisco ISE does not maintain a stable connection with specified Active Directory domain controllers. To verify whether your system is experiencing such disconnections, open the Cisco ISE ad_agent.log debug log file and look for multiple instances of the “Running in disconnected mode: unlatch” error message.

Table 9 Cisco ISE Patch Version 1.1.0.665—Patch 2 Resolved Caveats (continued)

Caveat	Description
CSCtz03084	<p>Cisco ISE ADAgent files in /var and /opt reach maximum size and prevent further authentication sessions via Active Directory</p> <p>This resolution is intended to fix an issue where increasing numbers of Active Directory file descriptor entries are recorded in the ADAgent files until the system limit is reached, preventing any further file descriptors to be allocated. The result of this condition prevents any further authentication events using Active Directory.</p>

Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 1

Table 10 lists the issues that are resolved in Cisco Identity Services Engine Maintenance Release 1.1.0.665 cumulative patch 1.

You must deploy this patch on Cisco Identity Services Engine Maintenance Release 1.1.0.665, otherwise the patch install will fail and Cisco ISE will return an error message stating, “This patch is intended to be installed on ISE 1.1.0.665.”

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

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

Table 10 Cisco ISE Patch Version 1.1.0.665—Patch 1 Resolved Caveats

Caveat	Description
CSCtx77149	<p>Disk space issue observed in Cisco ISE Release 1.0.4.573</p> <p>This fix addresses an issue where replication messages have been piling up in the primary Administration ISE node when secondary Administration ISE nodes become unreachable, thereby reducing available disk space.</p>
CSCty02379	<p>Tablespace CPMNS fills up disk space on Cisco ISE appliances</p> <p>The issue at hand in this case involves tablespace CPMNS growing so large as to become “out of bounds” on both active and standby Monitoring and Troubleshooting nodes. As a result, the nodes can run out of available disk space.</p>
CSCty13876	<p>Low available disk space associated with tablespace growth</p> <p>This fix addresses a disk space availability issue preventing continuous Cisco ISE Profiling (and other) activities which could contain more DML operations, resulting in undo tablespace growth.</p>
CSCty46684	<p>Multiple CSRF vulnerabilities in Cisco ISE Administrator user interface</p> <p>To address this issue, Cisco has added a Filter to Tomcat to safeguard the Administrator user interface from CSRF attacks. This filter checks IP addresses and hostnames of the node(s) in HTTP referer headers.</p>

Table 10 Cisco ISE Patch Version 1.1.0.665—Patch 1 Resolved Caveats (continued)

Caveat	Description
CSCty59165	<p>SNMPQuery Probe query events queue runs out of memory</p> <p>This fix addresses an issue where the Cisco ISE SNMPQuery event queue was not limiting the number of events in the queue. As a result, lots of accounting requests received by Cisco ISE lead to a reduction in memory where runtime dropped extra accounting requests, but the Profiler probe still parsed <i>all</i> of them, thus generating unnecessary extra SNMPQuery RadiusAcctStart events.</p>

Cisco ISE Release 1.1 Open Caveats

- [Open Caveats, page 26](#)
- [Open Agent Caveats, page 47](#)

Open Caveats

The following table lists the open caveats for Cisco ISE, with those found in this release first, followed by those found in later releases.

Table 11 Cisco ISE Release 1.1 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>
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>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)


Caveat	Description
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>
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></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>

Table 11 Cisco ISE Release 1.1 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>
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>
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 entered 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>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
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>
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>
CSCtn76441	<p>Custom conditions are not updated under Rules in profiling policies</p> <p>If you rename a profiler condition used by a profiling policy, the new name is not reflected in the rule summary display. It is, however, reflected in the associated expanded rule expression.</p> <p>Workaround If you expand and collapse the rule expression in the anchored overlay and click Save, the correct description displayed in the rule summary repeater will be displayed in the future. If you change the condition name a second time, however, and expand/collapse the summary overlay on the policy page a second time and click Save, the policy page will not reload until and unless you reload the server.</p>
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>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
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>
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>
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>
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 56.</p>
CSCto41340	<p>Authentication Policy replication failure from Primary to Secondary if the time zone changes after installation</p> <p>In release 1.0 time change is not supported after the deployment is setup because of the dependencies on time synchronization.</p> <p>Note Support for time change within an existing deployment will be postponed to a later release.</p>
CSCto52210	<p>Authorization and authentication policy rules pages load and save times are high</p> <p>This issue has been observed with 50 or more authentication rules, where each rule has at least conditions. The Load and save times approach one-and-a-half minutes.</p>

Table 11 *Cisco ISE Release 1.1 Open Caveats (continued)*

Caveat	Description
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
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>
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>

Table 11 *Cisco ISE Release 1.1 Open Caveats (continued)*

Caveat	Description
CSCto72015	<p>Authorization policy with condition as “Identity grp” does not work</p> <p>Create an Identity Group with the following attributes:</p> <p>User Identity Groups:</p> <ul style="list-style-type: none"> • Employee <ul style="list-style-type: none"> – Location1 – Location2 <p>Create Authorization Policy containing the “IdentityGroup:Name Equals Location1” condition and perform user authentication. Authentication fails because the rule in the condition has not been satisfied.</p> <p>This problem occurs only using the “IdentityGroup:Name” dictionary attribute in the Authorization Policy.</p> <p>Workaround To implement the workaround:</p> <ol style="list-style-type: none"> 1. Instead of using a Dictionary Attribute (IdentityGroup:Name) in the policy, specify the Identity Group to be “Location1” in the Identity Group selection rather than “Any.” 2. Assign the “Location1” Identity Group to the Internal User. 3. In the Authorization Policy condition, specify one of the following: <ul style="list-style-type: none"> – “Internal Users.Identity Group Equals IdentityGroup:User Identity Groups:Employee:Location1” – “Internal Users.Identity Group Matches .*Location1”
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>
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 1.1 Open Caveats (continued)

Caveat	Description
CSCtq06832	<p>Time and Date conditions need to be updated correctly when changing time zones</p> <p>Configure the Time Zone in Cisco ISE to be “IndianStandardTime,” for example, and create a Time and Date condition (Ex: From Time 10:00 AM & To Time 8:00 PM). Then update the Time Zone from IST to UTC. The existing Time and Date condition does not get updated per the new specified Time Zone.</p> <p>This issue comes up when changing the Time Zone after creating the Time and Date condition in the Policy > Conditions > Common > Time and Date page.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtq07311	<p>Change of Authorization shows “0” sessions on Policy Service node are down</p> <p>This issue has been observed where when one or more Policy Service nodes are behind an Inline Posture node, a client machine connected via a particular Policy Service node has authenticated, but has not yet completed posture assessment, and that Policy Service node then goes down (administratively or otherwise).</p> <p>Note As designed, another Policy Service node in the node group detects that the peer node has gone down and issues a Change of Authorization to terminate the pre-posture session on the client machine, but that measure does not succeed.</p> <p>Workaround If the client machine re-initiates authentication, the new request goes to another Policy Service node (assuming that the Network Access Device is configured with multiple RADIUS servers) and authentication and posture assessment should work as designed.</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>
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>
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 1.1 Open Caveats (continued)

Caveat	Description
CSCtr32014	<p>Three-hour Cisco ISE upgrade time on scale configuration</p> <p>This problem occurs during upgrade from one Cisco ISE running release 1.0 software to release 1.1.</p> <p>Note There is no known workaround for this issue.</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> <p>Workaround Enable a DHCP probe and configure the setup for Cisco ISE to profile endpoints with DHCP packets.</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>
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>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCtr88091	<p>You may experience slow response times for some user interface elements when using Internet Explorer 8.</p> <p>Symptom When using Internet Explorer 8, the check-boxes on pop-up dialogs for selecting and deselecting groups and attributes may be slow to respond to clicks for changing states.</p> <p>Conditions The use of Internet Explorer 8.</p> <p>Workaround Do any of the following:</p> <ul style="list-style-type: none"> Consider using an alternative web browser. Firefox does not show the same symptoms. Be patient. The check-boxes in IE8 respond after clicking them several times. Enter the group names manually, and avoid using the pop-up dialogs.
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>
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>
CSCts36792	<p>No “Cisco ISE Configuration Changes” alarms appearing on Conditions</p> <p>Guest simple and compound conditions can be created, edited, and deleted on the admin UI, but no logs are generated in Cisco ISE accounting.</p> <p>This problem is limited to creating, modifying, and deleting guest simple and compound conditions in the Policy > Policy Management > Conditions > Guest page</p> <p>Workaround There is no known workaround for this issue.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCts45441	<p>Weird behavior with creating guest account using start-end time profile</p> <p>This issue can happen when the Sponsor User tries to create a guest account with time profile type STARTEND. The start date is now (same day creating) and the end date is the next day.</p> <p>Workaround When creating the guest account, use the FROMCREATION time profile with a 1-day duration.</p>
CSCts48857	<p>Failed to send notification from UTF-8 Email address</p> <p>An “Internal error encountered. Please see logs for more details.” error message appears when attempting to notify a Guest user by email of their new account information.</p> <p>This problem occurs only for user IDs that contain UTF-8 characters outside the US ASCII range.</p> <p>Workaround There is no actual workaround at this time, however, you could try substituting a traditional ASCII Email address for the address containing UTF-8 characters.</p>
CSCts89508	<p>Authorization fails when a UTF-8 username and password credentials are used. Microsoft native supplicants require some hot fixes in order to support UTF-8 RADIUS user names.</p>
CSCtt17378	<p>Cisco NAC Agent does not pop up if TLS 1.0 is not enabled in Internet Explorer settings</p> <p>The problem occurs when all the following conditions are met:</p> <ul style="list-style-type: none"> • Cisco ISE is operating with a FIPS 140-2 module • The client machine “Local security settings > System cryptography : Use FIPS algorithm” is enabled. • The client machine Internet Explorer Advanced settings, SSL3.0/TLS 1.0 is option is disabled. <p>Workaround Ensure TLS 1.0 is enabled in Internet Explorer and restart the Cisco NAC Agent.</p>
CSCtt25262	<p>Externally-authenticated administrator users cannot register nodes</p> <p>Workaround Cisco ISE will not allow the external administrator to register nodes. Create an internal user to perform the registration process.</p>
CSCtt93787	<p>Files without extensions are not downloaded correctly using Cisco NAC Web Agent</p> <p>When the Cisco NAC Web Agent invokes file remediation, it does not download the file as designed. Instead, the Agent attempts to open the file.</p> <p>Workaround There is no known workaround for this issue.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCtu05540	<p>Monitoring and Troubleshooting node does not show Active Directory External Groups following authentication failure</p> <p>When viewing the details of a failed authentication that has passed Active Directory authentication, but was denied access because of an authorization policy in Cisco ISE, the Active Directory “External Groups” for the authentication are not visible. In addition, the same user that then passes the authorization policy is seen to be a member of one or more Active Directory groups.</p>
CSCtu39612	<p>Cisco ISE Inline Posture node is not accessible from the Admin ISE node user interface after an upgrade to ISE 1.1.</p> <p>Workaround Follow the instructions provided in Upgrade from Cisco ISE 1.0.4 to 1.1 with Inline Posture, page 10.</p>
CSCtv17606	<p>Monitoring and Troubleshooting requires an appropriate error message if backup/restore process fails</p> <p>When you try and perform a Monitoring and Troubleshooting backup/restore from the Cisco ISE administrator user interface, which is intended only to restore Administrator ISE nodes, the message displayed reads, “% Error: Cannot find ise_backup_instance.log in the backup file % Application restore failed.” Instead, a message like “% Error: Cannot ISE M&T backup can only be restored web interface % Application restore failed” would better advise users of the issue.</p>
CSCtv21758	<p>You are unable to Unquarantine an endpoint (with Endpoint Protection Services) using the IP address of the endpoint.</p> <p>Workaround Use the MAC address to unquarantine the endpoint.</p>
CSCtw79431	<p>Exiting the Cisco Mac Agent while in “pending” state displays the wrong user message</p> <p>When exiting a Cisco Mac Agent that has not successfully logged in yet, reveals a “successfully logged out from network” message to the user, when in fact there is no log-in status change.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtx01136	<p>Cisco NAC Agent is not performing posture assessment</p> <p>This issue has been observed on a client machine connected through a wireless interface that has successfully completed 802.1x authentication and posture assessment, and was granted network access. After a period of time, the agent displays an error message and the user loses full network access.</p> <p>Workaround There are a few possible workarounds:</p> <ol style="list-style-type: none"> 1. Restart the Cisco NAC Agent. 2. Switch to a wired interface. 3. Switch to a non-Cisco ISE-managed SSID, then come back to the Cisco ISE-managed SSID.

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCtx03427	<p>Create Alarm Schedule returning XSS error messages</p> <p>This issue has been observed when the configured alarm name contains “onChange”.</p> <p>Workaround Rename the alert name to something that does not contain “onChange”.</p>
CSCtx07670	<p>Profiler conditions that are edited wind up corrupting Profiler policies</p> <p>If you rename a profiler condition used by a profiling policy, the name change is not reflected in the rule summary. It will be reflected in the expanded rule expression anchored overlay.</p> <p>Workaround If you expand and collapse the rule expression in an anchored overlay and click Save, the corrected description displayed in the rule summary repeater will be displayed in the future. If you change the condition name a second time, however, and expand/collapse the summary overlay on the policy page a second time and click Save, the policy page will not reload until and unless you reload the server.</p>
CSCtx25213	<p>IP table entry needs cleanup after deregistering a secondary node</p> <p>If you have more than two nodes in your deployment, and you promote a secondary Administration ISE node to the primary role, other nodes in the deployment may become out of sync because those other nodes are unable to connect to the new primary database.</p> <p>Workaround Perform the following steps to work around this issue:</p> <ol style="list-style-type: none"> 1. Restart other nodes in the deployment via application stop/start in the CLI. 2. Log into the primary Administrator ISE node user interface and use the Full Syncup function in “deployment” for the other nodes.
CSCtx31601	<p>Cannot add Network Access user, but able to import users</p> <p>When the string “alert” appears in the Network Access user name, the Cisco ISE user interface prevents it from being created.</p> <p>Workaround If you import a user with that name, it will work.</p>
CSCtx33747	<p>RBAC admin cannot access deployment page and perform deployment-related functions</p> <p>When an RBAC-level administrator logs into the Cisco ISE administrator user interface and navigates to the Administration > System page, and “Access Denied” message is displayed even though the RBAC administrator should have access to the “Admin Access” page in this location.</p> <p>Workaround RBAC administrators can click on the specific menu they need (e.g., Administration > System > Deployment or Administration > System > Admin Access) to get to the page they need to work with.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCtx51454	<p>Unable to retrieve administrator users list</p> <p>When you click Select and choose to “Email Notification User List,” and then click on the Search button in the Cisco ISE administrator Administration > System > Settings > System Alarm Settings page, Cisco ISE displays a “There was a problem retrieving the XML data:Bad Request” error message.</p> <p>Workaround Enter the user name manually.</p>
CSCtx59957	<p>A warning/pop-up appears while creating a Guest Time profile</p> <p>A pop-up with the message “Warning: Unresponsive script” can appear when adding a time profile in Guest settings under Administration.</p> <p>Workaround Dismiss the pop-up message and try again.</p>
CSCtx60819	<p>Database restoration runs out of space on VMware systems with only 60 GB disk size</p> <p>This issue only occurs on unsupported (EVAL) VMware disk installations where the restoration server has a single disk of only about 60-70 GB of disk space.</p> <p>Workaround Use a VMware server installation with a larger disk size (like 100 GB) if possible.</p>
CSCtx62403	<p>Admin can control sessions on a node on which replication has been disabled</p> <p>When a Cisco ISE certificate has expired, replication is disabled on that node. When replication is disabled on a node, active sessions affecting that node can be controlled from the Administrator ISE node. Therefore, the Cisco ISE administrator can see active sessions on nodes where replication has been disabled and can issue Change of Authentication for associated endpoints.</p> <p>Note Certificate validity is validated every 24 hours in a deployment for each node.</p>
CSCtx62657	<p>Cannot deregister an Inline Posture node</p> <p>On the Deployment List Page, when you attempt to deregister a node by clicking the appropriate button, the administrator user interface is grayed out until a message reading “Deregister is done. Node will be re-started.” appears.</p> <p>Workaround Log out and log in to the administrator user interface again. The deregistered node is no longer visible in the user interface.</p>
CSCtx68334	<p>Promotion for Secondary Monitoring and Troubleshooting fails if the Primary node is down</p> <p>While promoting the secondary Monitoring and Troubleshooting node while the primary node is down, then Cisco ISE returns a transition failure and the database rolls back.</p> <p>Workaround Try to perform the operation again to overcome this issue.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCtx69191	<p>Mozilla Firefox does not function with OpenSC middleware software</p> <p>If you create certificate an authentication profile using the Cisco ISE Active Directory > Groups page, install the OpenSC middleware software, then go to the management station connected to a CAC authentication device and insert the CAC card while attempting to log in via Mozilla Firefox, authentication does not take place as designed.</p> <p>The key issue is that the e-mail certificate that Cisco ISE normally uses to authenticate the administrator does not appear for selection by the browser, and any other certificate fails during connection.</p> <p>Note This issue has been observed using OpenSC middleware on Mac OS X (Safari and Chrome both work as designed). CACkey middleware works as designed with Safari, Chrome, and Firefox.</p>
CSCtx74574	<p>Device Configure Deployment option selected after upgrade from software release 1.0 to release 1.1</p> <p>After upgrade, when trying to disable the “Include this device when deploying Security Group Tag Mapping Updates” option in the Network Device component, a “Failed to create network device - CoA cannot be enabled for more than one device.” error message appears. The result is that you cannot save the configuration to the specified network device.</p> <p>Workaround Delete this network device and recreate it with the desired configuration.</p>
CSCtx75940	<p>Cisco ISE RADIUS Password change ignores administrator user interface password policy</p> <p>When performing a RADIUS password change in the Cisco ISE Internal Identity store, the password policy setting in the administrator user interface is ignored if the restriction exists in the password policy in the CLI. As a result, password change fails, displaying the following error in the ISE log:</p> <p>“Authentication failed : 24203 User need to change password”</p> <p>For example, a password can be set to “Cisco123” in the administrator user interface if the Password may not contain “cisco” or its characters in reversed order option is disabled in the User Password Policy, but cannot be changed to a password containing “Cisco” through a RADIUS password change if the <code>disable-cisco-passwords</code> command exists in the CLI password policy.</p> <p>Workaround Ensure that the same password policy is configured on both the CLI and administrator user interface. In addition, Removing this restriction on the CLI allows the RADIUS password change to succeed.</p>
CSCtx77149	<p>Disk space issue</p> <p>This issue has been observed when a secondary node becomes unreachable in a distributed deployment.</p> <p>Workaround Deregister and re-register the secondary node.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCtx79725	<p>Cisco ISE freezes during startup if first DNS does not respond</p> <p>This issue has been observed if/when primary DNS is misconfigured or down.</p> <p>Workaround Specify a different (operational) DNS server.</p>
CSCtx80886	<p>When switching to FIPS mode, there is no way to delete the self-signed certificate on an Inline Posture node</p> <p>This issue occurs when the original self-signed certificates still installed on the Inline Posture node, even though it is not actually used by Cisco ISE.</p> <p>Note Do <i>not</i> remove the default self signed certificate and join the Inline Posture node to the deployment using FIPS compliant CA certificates.</p> <p>Workaround Deregister the Inline Posture node, remove the self-signed certificate, and re-register the Inline Posture node.</p>
CSCtx90696	<p>Cisco ISE does not work after updating the IP address</p> <p>This issue may be that the primary DNS server used by Cisco ISE has not yet been updated with the new IP address.</p> <p>Note Do not use the <code>no ip address</code> command when you change the Cisco ISE appliance IP address. Instead, simply set the new IP address with the <code>ip address</code> command.</p> <p>Workaround Use the “ip address” command in the CLI to specify a new IP address. (Make sure the primary DNS server is also updated with new records.)</p>
CSCtx92251	<p>Using the Cisco ISE “Replace” function on a secondary node does not assign protocols or replace the certificate</p> <p>Using the “Replace” button when replacing a certificate on a secondary node (such as a Monitoring and Troubleshooting or Policy Service node) does not move the protocols to the new certificate or remove the old certificate.</p> <p>This issue has been observed when you install the certificate on a Monitoring and Troubleshooting node, take the same Certificate Signing Request and have it signed by a different Certificate Authority, then install the certificate on the Monitoring and Troubleshooting node with the “Replace” option enabled.</p> <p>Note Both certificates are still present on the node and EAP and MGMT protocols are not part of the new certificate from the second Certificate Authority.</p> <p>Workaround Create a new certificate from the second Certificate Authority, edit protocols, and then delete the old certificate from the original Certificate Authority.</p>

Table 11 *Cisco ISE Release 1.1 Open Caveats (continued)*

Caveat	Description
CSCtx93416	<p>Database restoration fails when upgrading from software release 1.0.4 to release 1.1</p> <p>The restore process fails the Cisco ISE Release 1.1 deployment has been installed via upgrade and the hostnames in the topology have different assigned roles, but hostname of the original primary node name (when the release 1.0.4 backup image was created) is still a node name appearing in the new deployment, but is no longer the primary node in your deployment.</p> <p>Workaround There are two possible workarounds for this issue:</p> <ul style="list-style-type: none"> • Change hostname on the new release 1.1 primary node to match what it was during the backup, and try to restore the database again. • Change hostname on new release 1.1 primary node to be something completely new (a name that was not used at all in the original release 1.0.4 deployment).
CSCtx94839	<p>Clicking on logout link on the AUP page of Device Registration Webauth flow appears to do nothing</p> <p>This problem only occurs when clicking the Logout link on the Acceptable Use Policy (AUP) page for the Device Registration Webauth (DRW) flow. Other guest flow configurations are unaffected.</p> <p>The reason logout does not work is because there is no login page to go to. The logout link is harmless and impotent.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtx95251	<p>Deployment page load exceeds six minutes when two or more nodes are unreachable</p> <p>This problem may occur only if the nodes are not reachable, there are lots of pending messages in the secondary node, and if there is possibly a firewall issue.</p> <p>Workaround Make sure all the nodes are reachable, there are no pending messages, and there are no firewall issues.</p>
CSCtx97190	<p>Cisco 3750 switch is profiled as “Generic Cisco Router”</p> <p>This issue can happen when only LLDP information is available to classify endpoints.</p> <p>Workaround Enable CDP on the network access device(s) connected to Cisco ISE.</p>
CSCty00899	<p>LiveLog Reports cannot be opened</p> <p>When you drill down on LiveLog details to launch a detail report, Cisco ISE returns an error message.</p> <p>Note This issue is seen only if you leave your browser idle for more than one day.</p> <p>Workaround Users can logout and log in again to drill down to report details from live logs.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCty02379	<p>Cisco ISE runs out of space due to a backlog of pending messages in the replication queue</p> <p>This issue has been observed on Cisco ISE Monitoring and Troubleshooting nodes.</p> <p>Workaround Please contact Cisco Technical Assistance Center (TAC) for resolution information.</p>
CSCty05129	<p>“Monitor All” function does not take effect after policy refresh</p> <p>When the administrator enables or disables the Monitor All function, devices do not get policy updates as designed. This has been observed in cases where the cells are not updated manually.</p> <p>Workaround Cisco recommends using the Monitor Mode function on a per cell basis, rather than Monitor All. If you have enabled the Monitor All function, edit at least one cell per column in which a value exists. You can also manually remove the policies from the network device and update them again from Cisco ISE.</p>
CSCty05157	<p>The Cisco ISE dashboard is not working for administrator user names with more than 15 non-English characters contained in the username</p> <p>This issue has only been observed for user names created using a language other than English.</p> <p>Workaround Update the administrator user names so that they are less than 15 characters in length.</p>
CSCty10369	<p>Management functions operate slowly on VM with UCS SATA-2 storage</p> <p>The following issues have been cited:</p> <ul style="list-style-type: none"> • Importing 1,000 users in a deployment setup takes 8 more minutes than a dedicated hardware appliance (or VM SCSI HDD 10K rpm). • Full synchronization functions take up to 12 hours on a VM UCS with SATA2 HDD. • Disk latency is up to 50% greater on SATA-2 7200 rpm storage devices. <p>Workaround Ensure external storage units connected to UCS feature SCSI/SAS 10K or 15K RPM technology.</p>
CSCty10461	<p>Cannot register a Cisco ISE node with UTF-8 characters in administrator name</p> <p>Node registration fails for any administrator whose username contains non-ASCII characters.</p> <p>Workaround There should be at least one administrator whose username and password are in ASCII on the to-be-registered node. You are not required to ensure <i>all</i> administrator IDs are in ASCII, just the one used for registration operations.</p>

Table 11 *Cisco ISE Release 1.1 Open Caveats (continued)*

Caveat	Description
CSCty10692	<p>Requirement is used by Policy - Need tooltip on OS</p> <p>When a requirement is used by a policy in Cisco ISE, the operating system of the policy and the requirement need to match. Currently, the requirement operating system field is disabled in the requirement page and the administrator is not able to tell with which operating systems this requirement is associated.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCty15646	<p>Monitoring and Troubleshooting debug log alert settings get reset to WARN</p> <p>This issue has been observed in the Administration > System > Logging > Debug Log Configuration > Monitoring and Troubleshooting Alert page. The administrator is not able to change the WARN setting to any other level.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCty16603	<p>Administrator ISE node promotion fails, resulting in disabled replication status</p> <p>This can happen when you promote a secondary Administrator ISE node with a large database to the primary role.</p> <p>Workaround Perform a manual sync between the primary and secondary nodes.</p>
CSCty19010	<p>Editing Cisco ISE failure reason information returns error message</p> <p>If user edit some of the failure reason codes in the Administration > System > Settings > Monitoring > Failure Reason Editor page, Cisco ISE may display an error 500 message.</p> <p>“12818 Expected TLS acknowledge for last alert but received another message 24466 ISE Active Directory agent is down”</p> <p>Note This issue can occur when failure reason information includes data that can indicate a cross site scripting attack; such as the string “alert” and “<” and “>” characters.</p>
CSCty19774	<p>Client Provisioning is not working when an Inline Posture node is connected to a VPN</p> <p>This can happen when the client machine successfully passes authentication and ACLs are downloaded to the Inline Posture node and there is connectivity to Policy Service node, but the URL redirect function is not working correctly.</p> <p>Note This issue has been observed on a on non-Windows 7 client machine. (XP clients do not update automatically because the root certificate list is not up to date.)</p> <p>Workaround One way to get around this problem is to do update your root certificates.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCty23790	<p>Internet Explorer 8 is unable to import endpoints from LDAP</p> <p>This issue has been observed while importing Endpoint Identities from an LDAP server in a deployment where FIPS 140-2 compliant nodes are interoperating with non-FIPS nodes. Cisco ISE returns the following error message in the top center part of the Internet Explorer browser window:</p> <p>“TypeError: 'getElementsByName(...).0.value' is null or not an object”</p> <p>Workaround Use Mozilla Firefox 9, Internet Explorer 9, or Google Chrome browser to import endpoint identities from an LDAP server.</p>
CSCty28274	<p>System and RBAC administrator data access permission issue</p> <p>When an administrator other than the Cisco ISE administrator user created during installation logs into the Administrator ISE node user interface and navigates to Administration > System > Admin Access, they should be able view and update the administrator information when clicking on their own username. Instead, Cisco ISE displays a “Permission Denied” message.</p> <p>Workaround Administrators facing this issue can click on the logged-in username in the top right corner of the on user interface and edit their details from the pop-up dialog that appears.</p>
CSCty39209	<p>IPsec and SSL VPNs do not work if FIPS function is enabled or the PAP protocol is disabled</p> <p>If you enable FIPS 140-2 functionality you must also turn off PAP authentication in the Allowed Protocols page.</p> <p>Once you turn off PAP, then <i>any</i> VPN client that uses group authentication, which always requires PAP, becomes incompatible with Cisco ISE.</p>
CSCty40077	<p>Shared Secret Key for Inline Posture node Network Access Device is not created or updated</p> <p>The shared secret key for a network device associated with an Inline Posture node is not getting automatically created or updated when the administrator updates the RADIUS server configuration for the access device in the Inline Posture node configuration screen.</p> <p>Workaround Manually change the shared secret on the network device corresponding to the Inline Posture node to be the same as that specified in the RADIUS server configured in the Inline Posture configuration screen.</p> <p>Note In a multiple Policy Service node deployment scenario, the shared secret for all nodes should be the same.</p>
CSCty42816	<p>Wireless Guest login fails using Google Chrome browser</p> <p>Self-service guest users are unable to get on to the network from Chrome Browser during Wireless Local Web Authentication. Cisco ISE displays an error page with user credentials after the self service guest user changes the password and tries to get onto the network.</p> <p>Workaround Cisco recommends using another browser for this operation.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCty52694	<p>Mac OS X Agent needs to be installed from Client Provisioning Portal for VPN</p> <p>When a Mac OS X user connects through VPN, the Mac OS X Agent does not pop up as designed.</p> <p>This can happen if the Mac OS X Agent has been installed directly from Cisco Connection Online (CCO) or via application installation from an IT department instead of through The Cisco ISE client provisioning portal.</p> <p>Workaround Uninstall the agent from the system in question and reinstall the agent from the Cisco ISE client provisioning portal.</p>
CSCty53617	<p>IPSec profile deploy is not properly saved</p> <p>After creating an IPSec profile template in NCS 1.2 and viewing in the deployment context, Cisco ISE returns a “success” message, but the profile is not actually created in the device.</p>
CSCty59165	<p>SNMPQuery Probe events queue runs out of memory</p> <p>This can happen when there are many RADIUS accounting start requests on the node where the SNMPQuery probe is enabled. This issue can also come up if an associated NAD is not able to respond to SNMP requests.</p> <p>Workaround Turn off the SNMPQuery probe, restart the NAD, and try to add the correct SNMP information for the NAD in question.</p>
CSCty61980	<p>Cannot get Out-of-Band Security Gateway Access PAC for network devices after upgrade</p> <p>This issue can occur on a system that has been upgraded from Cisco ISE, Release 1.0.4 where device definitions were also updated as part of this upgrade. (The PAC file that is downloaded is invalid and Cisco ISE returns an error message.)</p> <p>Workaround Delete and recreate the network device definition for any device where you need to generate an Out-of-Band PAC. You can do this by creating the necessary entry in the administrator user interface or exporting the device definition, deleting the entry, and adding the device definition again.</p>
CSCtz12581	<p>The pr_WSUSRule (a dummy compound condition) is not listed in the Regular Compound Condition, and the pr_WSUSRule needs to be searched</p> <p>When you associate a WSUS remediation action to a posture requirement to validate Windows updates by using the severity level option, you must choose the pr_WSUSRule compound condition in the posture requirement.</p> <p>Workaround Search the pr_WSUSRule in the Conditions widget, and select the dummy compound condition when you create a posture requirement and associate a WSUS remediation to the posture requirement.</p>
CSCub29185	<p>Mac Agent not getting installed when the “MAC App Store” and “identified developers” options are enabled on the client</p> <p>Workaround Enable the “Allow from Anywhere” option in the Security & Privacy Preference page.</p>

Table 11 Cisco ISE Release 1.1 Open Caveats (continued)

Caveat	Description
CSCub29212	<p>Mac OS 10.8 clients require confirmation from a system administrator to modify the System network configuration</p> <p>This issue has been observed on Mac OS 10.7/10.8 clients. The Supplicant Provisioning Wizard used to provision an 802.1x profile may initiate multiple login pop-ups requesting administrator credentials to elevate user privileges during the provisioning process.</p> <p>When the Mac OS X client system preference is set to more strict administrator control, additional pop-ups appear for requesting credentials to elevate the active user privilege level.</p> <p>Workaround On the Mac OS 10.7/10.8 client, navigate to System Preference > Security & Privacy > General > Advanced and disable the “Require an administrator password to access locked preferences” option.</p>

Open Agent Caveats

The following table lists Cisco ISE Agent open caveats that have been carried over from prior releases.

Table 12 Cisco ISE Open Agent Caveats, Release 1.1

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>
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>

Table 12 *Cisco ISE Open Agent Caveats, Release 1.1 (continued)*

Caveat	Description
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>
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>
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>

Table 12 Cisco ISE Open Agent Caveats, Release 1.1 (continued)

Caveat	Description
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>
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>

Table 12 *Cisco ISE Open Agent Caveats, Release 1.1 (continued)*

Caveat	Description
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>
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 56.</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>
CSCty02167	<p>IP refresh fails intermittently for Mac OS 10.7 guest users</p> <p>This problem stems from the way Mac OS 10.7 handles certificates. Marking the certificate as “trusted” in the CWA flow is not good enough to download the java applet required to perform the DHCP refresh function.</p> <p>Workaround The Cisco ISE certificate must be marked as “Always Trust” in the Mac OS 10.7 Keychain.</p>

Cisco ISE Release 1.1 Resolved Caveats

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

- [Resolved Caveats, page 51](#)
- [Resolved Agent Caveats, page 55](#)

Resolved Caveats

The following table lists the resolved server-side caveats in Cisco ISE Release 1.1.

Table 13 *Resolved Caveats*

Caveat	Description
CSCtj37325	Profiler Attribute value exceeds maximum 4000 character length
CSCtk17648	IE8—Network Device Management missing from the Cisco ISE Administrator Tab
CSCtl56724	Network access users display filter sorted by status does not work
CSCtl78424	Blank right hand Network Devices pane with vertical scroll
CSCtn42397	The Network Access Users “Delete All” function when used on a filtered list should only delete filtered (displayed) Network Access Users
CSCtn59529	Network Access User filters do not work on the Status or Admin columns using the Quick and Advanced filters
CSCtn73422	Network Access User filters filtering correctly
CSCtn92602	Filters are not working under QuickPickers during Posture Policy configuration
CSCtn95127	Client provisioning report does not show the policy matched
CSCtn99145	An authorization policy matching multiple rules does not appropriately match the existing ACCESS_ACCEPT rule
CSCto03813	No “Cisco ISE Config Changes” alarm generated using Authentication > Simple Condition > Edit/Add/Delete
CSCto06361	Changing the User Identity Group name case should not return error upon search
CSCto10678	Administrator user should not be able to delete self policy
CSCto10855	IE8 with default option settings is not working
CSCto13102	No “Cisco ISE Configuration Changes” message dialogs are displayed for certain guest/sponsor configuration
CSCto13235	File Condition Advanced Filter does not return correct result
CSCto13986	IE8—Error when clicking the “Action” button on the Requirement page
CSCto15508	Filter in Security Group Access Egress Policy is not working correctly
CSCto17461	Invalid Simple Condition error message in Guest configuration
CSCto22671	HTTPS communication fails if the certificate is deleted from the primary Administration ISE node
CSCto24105	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.

Table 13 **Resolved Caveats (continued)**

Caveat	Description
CSCto24430	Details of guest RADIUS authentication failure are not available when searching via the guest username
CSCto27568	Cannot enable checkboxes in the right hand Filtered Network Devices pane
CSCto33037	Allowed character sets between policy conditions and element conditions are different
CSCto33973	Joining Cisco ISE to an Active Directory domain locks up when the Global Catalog is down or unreachable
CSCto41078	Cannot create an Identity Group using the gear icon during Client Provisioning policy configuration
CSCto43825	Synchronization fails with time zones other than UTC
CSCto45372	Default Sponsor Groups do not allow the Sponsor to create users or view passwords.
CSCto48657	Profiled endpoints are not all deleted
CSCto49359	Filters not working correctly on Guest conditions page
CSCto59976	Sync with NTP server during initial set-up shows failure although NTP server is reachable.
CSCto63749	The Cisco ISE dashboard does not display endpoints entered via the Administrator user interface
CSCto68519	Sorting / Filtering Does Not Work in Egress Table
CSCto70968	Fast reconnect is not working for PEAP-TLS protocol
CSCto72521	Save failed for child group assignment during Client Provisioning policy configuration
CSCto72594	Cisco ISE cannot save a Posture Policy when the Identity Group is the child of one or more other Identity Groups
CSCto73439	Restart required upon completion of Monitoring node database restoration
CSCto74356	Self-registered Guest role does not appear associated with the Guest account
CSCto82631	Clicking the “Name” field in the Cisco ISE User Identity Group page yields unexpected download behavior
CSCto83897	Client machine authentication shift to user authentication not updating Active Directory groups
CSCto87755	Guest accounting report appears only once, even though Guest logs in multiple times
CSCtq00096	Compound condition from a Sponsor Group Policy has a different name after it is saved
CSCtq07776	In Posture Policy, Click Save Symbol getting error message.
CSCtq09655	Dictionary Attribute duplication is not happening as designed during Authentication Policy configuration
CSCtq11650	The primary Administration ISE node has database links to Inline Posture nodes following promotion from secondary to primary
CSCtq17744	Exception policy not getting created first time in Authorization policy
CSCtq22779	Cisco ISE allows saving authorization compound conditions with the same names
CSCtq80912	Issues with Guest accounting report functions

Table 13 **Resolved Caveats (continued)**

Caveat	Description
CSCtr24825	Numerous Alarms entitled “ISE Alarm (CRITICAL): Alarm caused by ISE - System Health threshold” with high numbers in “CPU Utilization (%)”
CSCtr29490	Endpoint does not get profiled correctly with HTTP traffic following posture assessment
CSCtr38300	“Admin” login account is disabled and cannot be unlocked
CSCtr39545	Endpoint update function may execute before endpoint creation
CSCtr51053	Back button use is not working correctly under compound conditions after upgrade
CSCtr53954	Configure ISE for MAB + Posture flow
CSCtr58604	Cisco Administration ISE node backup size exceeds 8 GB
CSCtr59589	Exception Actions are triggering multiple CoA reauthentication events
CSCtr60200	Error while editing predefined AV/AS compound conditions
CSCtr66122	Policy could not be saved
CSCtr79440	Authorization policy not matched when condition to match parent device group location used
CSCtr82311	Administrator user interface password reset failed upon first login attempt
CSCtr84378	Guest role text box can be removed in sponsor group object
CSCtr84493	Cisco ISE inaccurately reports that a specified policy name already exists
CSCtr94724	Browser becomes inaccessible after creating Authorization profile
CSCtr95156	Guest changed passwd and sponsor modified acct, passwd was reset
CSCtr96694	SGA Security Group column is empty following SGA authentication
CSCts03935	Need to recreate the Support Bundle if the Admin session times out
CSCts08980	The Cisco ISE posture report dashlet returns an error code
CSCts10036	Issue with Inline Posture static route configuration
CSCts19211	After backup/restore, the administrator not able to access the Service Policy node
CSCts19809	Cannot import Advanced License on top of Base License
CSCts22154	RBAC menus on secondary nodes are incorrect immediately after upgrade
CSCts25521	Cisco ISE repeatedly returns an error when a Dictionary Compound Condition is added during Posture policy configuration
CSCts45547	Deployment: UI needs to have useful error msg during node registration
CSCts45591	TCP dump: unable to collect info from int that doesn't have an IP address
CSCts57010	undo_tablespace caused f/s out-of-space
CSCts57027	Newly added network interface for VM shown as __tmpXXXXX
CSCts59228	IE8 failing to Generate a CSV Template for Import Endpoints
CSCts77187	No Alarm when replication failing due to DB communication errors
CSCts78093	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
CSCts98931	Policy service nodes continually fail when a DHCP span probe is enabled on all interfaces

Table 13 **Resolved Caveats (continued)**

Caveat	Description
CSCts99778	Posture configuration options not available with Advanced License
CSCtt16149	Sub-Menus/Links showing even when set to “Hide” under RBAC Menu Access
CSCtt17694	Endpoint policy should be exposed through NBAPI at all times
CSCtu17393	In some cases, a sponsor is unable to create a guest user successfully through sponsor portal.
CSCtu21552	Authz policy page w/34 policies scale is taking more than 10 min to load
CSCtu23108	When a policy is modified, the matching endpoints are re-profiled, and even though they still match the policy a CoA is triggered.
CSCtu35100	The active endpoint count is significantly higher after an upgrade, without just reason.
CSCtu36529	After a successful upgrade, the Cisco ISE user interface continuously refreshes
CSCtu39656	You cannot enable Endpoint Protection Services after upgrading from Cisco ISE 1.0 to Cisco ISE 1.1 BETA, build 1.1.0.912.
CSCtu43108	The primary Monitoring ISE node becomes unresponsive, showing an out of memory error.
CSCtu60928	The Profiler servers filters for internal-user events.
CSCtv21293	The profiler policies for Cisco WLC need to be updated with an NMAP OS check.
CSCtv21432	All apple devices policies need to be updated with NMAP scan OS check.
CSCtw05024	From a secondary Admin ISE node, you are unable to quarantine an active session from active session report.
CSCtw30525	A promoted node is unable to access the Inline Posture node. This happens because the Inline Posture node does not receive the promoted certificate.
CSCtw32091	After promoting a secondary node, the secondary status shows “Sync completed” but the Replication status remains “In Progress”
CSCtw45250	When restoring a previously backed up file you may receive a “Restore Failed” message on the command line interface.
CSCtw57309	When downloading web agent, you may see the following error: “ActiveX failed-Try using applet”
CSCtw62891	No host config exception after deregistering secondary node; CoA fails
CSCtw78801	Repeater construction scales poorly >= 20 rows
CSCui22841	Apache Struts2 command execution vulnerability

Resolved Agent Caveats

The following table lists the resolved agent caveats in Cisco ISE Release 1.1.

Table 14 **Resolved Agent Caveats**

Caveat	Description
CSCtj39429	No posture on Mac OS X Agent in multi-NIC setup
CSCtj59635	Cisco NAC agent pops up even when popup login window is unchecked
CSCtq15958	Windows Agent VPN tunnel dropping after initial connection

Known Issues

- [Cisco ISE Hostname Character Length Limitation with Active Directory, page 55](#)
- [Windows Internet Explorer 8 Known Issues, page 55](#)
 - [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 56](#)
- [Issues With 2k Message Size in Monitoring and Troubleshooting, page 56](#)
- [Issues With More Than Three Users Accessing Monitoring and Troubleshooting Concurrently, page 57](#)
- [Inline Posture Restrictions, page 57](#)
- [Cisco IP phones using EAP-FAST, page 57](#)
- [Internationalization and Localization, page 57](#)

Cisco ISE Hostname Character Length Limitation with Active Directory

It is important that Cisco ISE hostnames be limited to 15 characters or less in length, if you use Active Directory on your network. Active Directory does not validate hostnames larger than 15 characters. This can cause a problem if you have multiple ISE hosts in your deployment whose hostnames are identical through the first 15 characters, and are only distinguishable by the characters that follow (the first 15).

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 1.1](#).

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](#).

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.

Internationalization and Localization

This section covers the known issues relating to internationalization and localization.

Custom Language Templates

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

Documentation Updates

Table 15 *Updates to Release Notes for Cisco Identity Services Engine, Release 1.1*

Date	Description
10/21/13	Added Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 5, page 22
8/8/13	Added Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 4, page 23
4/5/13	Added Integration with Cisco Prime Network Control System, page 22
8/6/12	Added CSCub29185 and CSCub29212 to Open Caveats, page 26
7/9/2012	Added Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 3, page 23

Table 15 **Updates to Release Notes for Cisco Identity Services Engine, Release 1.1**

Date	Description
7/2/2012	Added Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 2, page 24
4/20/2012	Resolved CSCtz41716
4/11/2012	<ul style="list-style-type: none"> Added Resolved Issues in Cisco ISE Version 1.1.0.665—Cumulative Patch 1, page 25 Added CSCty53617 and CSCtz12581 to Open Caveats, page 26
4/3/2012	Resolved CSCty95954
3/19/2012	Cisco Identity Services Engine, Release 1.1

Related Documentation

This section provides lists of related release-specific and platform-specific 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 1.1</i>	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
<i>Cisco Identity Services Engine Network Component Compatibility, Release 1.1</i>	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
<i>Cisco Identity Services Engine User Guide, Release 1.1</i>	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
<i>Cisco Identity Services Engine Hardware Installation Guide, Release 1.1</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 1.1</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1</i>	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
<i>Cisco Identity Services Engine CLI Reference Guide, Release 1.1</i>	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
<i>Cisco Identity Services Engine API Reference Guide, Release 1.1</i>	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
<i>Cisco Identity Services Engine Troubleshooting Guide, Release 1.1</i>	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html

Table 16 **Product Documentation for Cisco Identity Services Engine (continued)**

Document Title	Location
<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 other platform-specific 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.

© 2012 Cisco Systems, Inc. All rights reserved.

