



Release Notes for Cisco Identity Services Engine, Release 1.0

Revised: May 27, 2017, OL-22974-01

Contents

These release notes describe the features, limitations and restrictions (caveats), and related information for Cisco Identity Services Engine (ISE), Release 1.0. 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 6](#)
- [Cisco Secure ACS to Cisco ISE Migration, page 8](#)
- [Cisco ISE License Information, page 8](#)
- [Key Features, page 9](#)
- [Cisco ISE Install Files, Updates, and Client Resources, page 17](#)
- [Cisco ISE Antivirus and Antispyware Support, page 19](#)
- [Cisco ISE Release 1.0 Open Caveats, page 20](#)
- [Known Issues, page 42](#)
- [Documentation Updates, page 44](#)
- [Related Documentation, page 45](#)



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. An ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring.
Role	Determines if a node is a standalone, primary, or secondary node. Applies only to Administration and Monitoring nodes.

Types of Nodes

A Cisco ISE network has only two types of nodes:

- Cisco ISE node—An ISE node could assume any of the following three personas:
 - Administration—Allows you to perform all administrative operations on Cisco ISE. It handles all system-related configuration and configurations related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have only one or a maximum of two nodes running the Administration persona. The Administration persona can take on any one of the following roles: standalone, primary, or secondary. If the primary Administration node goes down, you have to manually promote the secondary Administration node. There is no automatic failover for the Administration persona.
 - Policy Service—Provides network access, posture, guest access, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assuming this persona. Typically, there would be more than one Policy Service persona in a distributed deployment. All Policy Service personas that reside behind a load balancer share a common multicast address and can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes in that group process the requests of the node that has failed, thereby providing high availability.



Note At least one node in your distributed setup should assume the Policy Service persona.

- Monitoring—Enables Cisco ISE to function as the log collector and store log messages from all the Administration and Policy Service personas on the ISE nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources.

A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports. Cisco ISE allows you to have a maximum of two nodes with this persona that can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring personas collect log messages. In case the primary Monitoring persona goes down, the secondary Monitoring persona automatically assumes the role of the primary Monitoring persona.



Note At least one node in your distributed setup should assume the Monitoring persona.

- Inline Posture node—A gatekeeping node that is positioned behind network access devices such as wireless LAN controllers (WLCs) and virtual private network (VPN) concentrators on the network. Inline Posture enforces access policies after a user has been authenticated and granted access, and handles Change of Authorization (CoA) requests that a WLC or VPN are unable to accommodate. Cisco ISE allows you to have two Inline Posture nodes that can take on primary or secondary roles for high availability.



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

**Note**

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

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

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

You can change the persona of a node. See the “Setting Up ISE in a Distributed Environment” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0* for information on how to configure these personas on Cisco ISE nodes.

Hardware Requirements

This section describes the following topics:

- [Supported Hardware, page 4](#)
- [Supported Cisco ADE-OS Version, page 6](#)
- [Supported Virtual Environments, page 6](#)
- [Supported Browsers, page 6](#)
- [Cisco ISE License Information, page 8](#)
- [Additional Support Information, page 6](#)

**Note**

For more details on Cisco ISE hardware platforms and installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0*.

Supported Hardware

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

Table 2 *Supported Hardware and Personas*

Hardware Platform	Persona	Configuration
Cisco ISE-3315-K9 (small)	Any	<ul style="list-style-type: none"> • 1x Xeon 2.66 GHz quad-core processor • 4 GB RAM • 2 x 250 GB SATA¹ HDD² • 4x 1 GB NIC³

Table 2 Supported Hardware and Personas (continued)

Hardware Platform	Persona	Configuration
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
Cisco ISE-VM-K9 (VMware)	Stand-alone Administration, Monitoring, and Policy Service (no Inline Posture)	<ul style="list-style-type: none"> • CPU—Intel Dual-Core; 2.13 GHz or faster • Memory—4 GB RAM⁵ • Hard Disks (minimum allocated memory): <ul style="list-style-type: none"> – Stand-alone—200 GB – Administration—200 GB – Policy Service and Monitoring—200 GB – Monitoring—200 GB – Policy Service—60 GB <p>Note Cisco does not recommend allocating any more than 600 GB maximum space for any node.</p> <ul style="list-style-type: none"> • NIC—1 GB NIC interface required (4 NICs are recommended) • Supported VMware versions include: <ul style="list-style-type: none"> – ESX 4.x – ESXi 4.x <p>Note VMware server version 2.0 is only supported for demonstration of Cisco ISE Release 1.0. For an evaluation or production version, the minimum disk space is 60 GB.</p>

1. SATA = Serial Advanced Technology Attachment

2. HDD = hard disk drive

3. NIC = network interface card

4. RAID = redundant array of independent disks

5. Memory allocation of less than 4GB is not supported for any VMware appliance configuration. In the event of a Cisco ISE behavior issue, all users will be required to change allocated memory to at least 4GB prior to opening a case with the Cisco Technical Assistance Center.

If you are moving from Cisco Secure Access Control System (ACS) or Cisco NAC Appliance to Cisco ISE, the Cisco Secure ACS 1121 and Cisco NAC 3315 appliances support small deployments, Cisco NAC 3355 appliances support medium deployments, and Cisco NAC 3395 appliances support large deployments.

Supported Cisco ADE-OS Version

The Cisco Application Deployment Engine operating system (Cisco ADE-OS) version that comes with the current release software is 2.0.0.890.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

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

Supported Browsers

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

- Mozilla Firefox 3.6
- Microsoft Internet Explorer 8

Additional Support Information

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

Installing Cisco ISE Software

The following steps summarize how to install new Cisco ISE Release 1.0 DVD software on supported hardware platforms (see [Supported Hardware](#), page 4 for support details).

With Cisco ISE Release 1.0, installation occurs in two phases:

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

-
- Step 1** Log into Cisco Download Software at <http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>. You might be required to provide your Cisco.com login credentials.
- Step 2** Navigate to **Security > Identity Management > Cisco Identity Services Engine > Cisco Identity Services Engine Software 1.0**.
- Step 3** Download the appropriate Cisco ISE .ISO image (for example, **ise-1.0.3.377.i386.iso**) and burn the image as a bootable disk to a DVD-R.

- Step 4** Insert the DVD into the DVD-R drive of each appliance, and reboot the appliance to initiate the Cisco ISE DVD installation process.
- Step 5** (If necessary) Install a valid FlexLM product license file and perform Cisco ISE initial configuration according to the instructions in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0*. Before you run the setup program, ensure that you know the configuration parameters listed in [Table 3](#).

Table 3 Identity Services Engine Network Configuration Parameters for Setup

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumeric (A-Z, a-z, 0-9), hyphen (-), with a requirement that the first character must be an alphabetic character. Note Cisco does not recommend using mixed case and hyphens in the hostname.	ise-node1
(eth0) Ethernet interface address	Must be a valid IPv4 address for the eth0 Ethernet interface.	10.12.13.14
Netmask	Must be a valid IPv4 address for the netmask.	255.255.255.0
Default gateway	Must be a valid IPv4 address for the default gateway.	10.12.13.1
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numbers, hyphen (-), and period (.).	mycompany.com
Primary name server	Must be a valid IPv4 address for the primary Name server.	10.15.20.25
Add/Edit another name server	Must be a valid IPv4 address for an additional Name server.	(Optional) Allows you to configure multiple Name servers. To do so, enter y to continue.
Primary NTP server	Must be a valid NTP domain.	clock.nist.gov
Add/Edit another NTP server	Must be a valid NTP domain.	(Optional) Allows you to configure multiple NTP servers. To do so, enter y to continue.
System Time Zone	Must be a valid time zone. Refer to <i>Cisco Identity Services Engine CLI Reference Guide, Release 1.0</i> for a table of time zones that Cisco ISE supports. The default value is UTC. Note The table lists the frequently used time zones. You can run the show timezone command from the Cisco ISE CLI for a complete list of supported time zones.	UTC

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

Prompt	Description	Example
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), and it must be composed of a minimum of six characters in length, include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9).	MyIseYP@ss

**Note**

For additional information on configuring and managing Cisco ISE, use the list of documents in [Release-Specific Documents, page 45](#) to access other documents in the Cisco ISE documentation suite.

Cisco Secure ACS to Cisco ISE Migration

**Note**

You *must* upgrade your Cisco Secure ACS deployment to Release 5.1 or later before you attempt to perform the migration process to Cisco ISE Release 1.0.

After you have moved your Cisco Secure ACS 5.x database over, you will notice some differences in existing data types and elements as they appear in the new Cisco ISE Release 1.0 environment.

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

Complete instructions for moving your Cisco Secure ACS 5.x database to Cisco ISE Release 1.0 are covered in the [Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0](#).

Cisco ISE License Information

Cisco ISE comes with a 90-day Base and Advanced package 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 or Base and Advanced license for your Cisco ISE. [Table 4](#) summarizes the Cisco ISE license types.

Table 4 Cisco ISE License Types and Supported Services

Cisco ISE License Type	Supported Services
Base package—Provides authenticated network access, guest life-cycle management, and advanced monitoring and troubleshooting.	<ul style="list-style-type: none"> • Basic network access • Guest management • Monitoring and troubleshooting
Advanced package—Provides posture, profiling, advanced monitoring and troubleshooting, and security group access services. You cannot add advanced licenses before adding base licenses, and the number of advanced licenses cannot exceed the number of base licenses.	<ul style="list-style-type: none"> • Profiler • Posture • Security group access

You apply all licenses to the primary Cisco ISE node by using the primary Cisco ISE hardware ID. The primary Cisco ISE then centrally manages all of the licenses that are installed for your deployment. If you have two Cisco ISE nodes configured as the Administration persona for high availability, you must include both the primary and secondary hardware IDs in the license file, but the process of managing the licenses is the same for single or dual Administrative nodes.

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 Appliance Hardware Installation Guide, Release 1.0*.

For specific information on adding, modifying, and removing license files, see the “Managing Licenses” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0*.

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

Key Features

Cisco ISE Release 1.0 offers the following features and services:

- [Web Interface and User Experience, page 10](#)
- [Identity Management, page 10](#)
- [Network Access Service, page 11](#)
- [ACP Authorization, page 11](#)
- [Guest Management Service, page 12](#)
- [Client Provisioning, page 12](#)
- [Posture Assessment, page 13](#)
- [Profiling Service, page 14](#)
- [Security Group Access Service, page 14](#)
- [Inline Posture, page 15](#)
- [Monitoring and Troubleshooting, page 15](#)

- [Resource Management, page 16](#)
- [Dictionaries and Dictionary Attributes, page 16](#)

For more information on key features of Cisco ISE, see the Overview chapter of the [Cisco Identity Services Engine User Guide, Release 1.0](#).

Web Interface and User Experience

The Cisco ISE Administrator web interface centralizes network identity management across the network, and allows drill-down access into individual endpoint access activities. The Cisco ISE user interface makes it easy for administrators to collect and correlate contextual information to make critical decisions quickly. In addition, the following user interface features help administrators quickly and efficiently configure Cisco ISE:

- The Cisco ISE application—unified, compelling, and modern; features dynamic interactions and a customer-driven, user-centric interface based on unified Cisco standards
- The dashboard—at-a-glance summaries; highly visual representation of current network status and trends; easy identification of abnormalities; strong focus on monitoring and troubleshooting
- Monitoring and troubleshooting alarms—always-available one-click access to monitor alarms and start the troubleshooting process
- Configuration workflows—unified, streamlined, and simplified configuration and policy management approach (including all management and policy building blocks); in-place configuration; context-sensitive information gathering; inline progressive disclosure keeps users in the context of current tasks (infrequent page shift helps provide better user experience)
- Reusable objects—for increased productivity, to save time, and minimize errors
- Advanced data-intensive widgets—simple yet scalable to manage large and complex data sets, including powerful quick and advanced searches and filtering

See the “Understanding the User Interface” chapter of the [Cisco Identity Services Engine User Guide, Release 1.0](#) for more information on the new user interface design.

Identity Management

Identity Management Service is the Cisco ISE process in which individual users, groups of users, endpoints, or groups of endpoints are identified and granted access to network resources and services. Identity Management Service is also used to control administrative access and permissions over Cisco ISE services. Based upon an established identity, an individual user or group of users can only access a set number of resources, services, or perform a number of system functions.

Individual user and group privileges are both restricted and based on authenticated roles and established identities that are verified during the login process. In addition, Cisco ISE supports role-based access control (RBAC) and configuration of these roles and associated permissions, based upon the user or group. Cisco ISE lets you manage the following types of network-based identities:

- Identities (administrators, network access users, and endpoints)
- Groups (administrator groups, user groups, endpoint groups, and guest sponsor groups)
- RBAC (policies and permissions)
- General account settings (for administrators, network access users, guests, and network accounts)

After being identified and authenticated, users or groups can access the system resources or services and perform network tasks for which they are authorized. Identity requires the use of login names, passwords, and other authorization and authentication processes to verify a user as being valid, belonging to a specific administrative group, and authorized to perform those tasks that are associated with that role or group.

Network Access Service

Cisco ISE Network Access Service provides authentication, authorization, and accounting (AAA) services for wired, wireless, and VPN networks. Cisco ISE Release 1.0 supports standard RADIUS protocols and services, functioning as a full AAA server to control who or what can access the network. Cisco ISE can limit access by providing varying levels of access for different types of users, endpoints, and access scenarios, and enforces accountability for all action and usage.

The network access service offers the following features:

- **Support for 802.1X Deployments**—Cisco ISE supports 802.1X authentication methods for both wired and wireless network access.
- **Attribute-Based Policy Model**—The attribute-based policy model offers greater flexibility in addressing your enterprise policy needs versus simple credential or group-based policy models.
- **Integration with Various External Identity Sources**—Apart from internal identity stores, Cisco ISE supports integration with Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), RSA SecurID servers, and RADIUS Token Identity Sources for user authentication and authorization.
- **RADIUS Control Plane**—Cisco ISE uses RADIUS as the control protocol that issues CoA for specific sessions to restrict a problematic host, to force endpoints to reacquire IP addresses, and adjust to updated authorization policies.

ACP Authorization

The Cisco ISE Authorization Control Policies (ACPs) service is used to create authorization profiles that let you define authorization policies for specific users and endpoints that access the network. ACPs are core to network access because they associate specific sets of rules with specific user and group identities to form the corresponding authorization profiles.

When these rules match a given user or user group, the associated profile is returned by the policy and network access is authorized. An authorization policy may contain conditional requirements that combine one or more group associations with a compound condition that can include authorization checks that return one or more network authorization profiles. An authorization profile can include references to DACLs, VLANs, or other access control attributes in Cisco ISE dictionaries. See [Dictionaries and Dictionary Attributes, page 16](#) for more information.

Administrators manage authorization policies and their corresponding authorization profiles by performing the following ACP-related tasks:

- Configuring authorization policies
- Applying a matched rule policy for authorization policies
- Configuring policy element conditions such as profiles and ACLs

Because authorization policies can include compound conditions that map to a single network service rule, policies can also provide a list of authorization checks. Authorization checks typically represent one or more conditions such as having a user-defined name. These authorization checks can also be added to the Cisco ISE resource dictionary to be reused by other authorization policies, which makes authorization a flexible and powerful tool.

Guest Management Service

Cisco ISE allows sponsors to create temporary user accounts so that guests, contractors, or consultants can access the network by providing credentials through a standard web browser. The network could be the corporate network, a limited access, Internet-only network, or some other type of restricted network with specific services for different types of guests.

The guest network is controlled by VLANs or DACL configurations on the network access devices (NADs). Cisco ISE manages these VLAN and DACL assignments on the NAD-based on guest authorization policies that are defined by the Cisco ISE administrator.

Cisco ISE Guest Service allows any user with sponsor privileges to create temporary guest accounts easily. Cisco ISE allows sponsors to provide network access account details to the guest by printout, email, or short message service (SMS). Cisco ISE Guest Service performs full authentication of these sponsors before it creates guest accounts. Sponsor authentication can be through either the local database or an external LDAP or Active Directory identity store. The entire experience, from user account creation to guest network access, is stored for auditing and reporting.

When a guest user first connects to the local network, either through a wireless or a wired connection, the user is placed in a segregated network with limited access. For the Guest service to function properly, the WLC or NAD must support captive HTTP and HTTPS portal login scenarios with a login URL to RADIUS mapping.

The Cisco ISE Guest Service provisions a guest account for the amount of time specified when the account is created.

Cisco ISE Guest Service is used by three main users:

- Admin—The admin user is the Cisco ISE administrator who configures and maintains the Cisco ISE appliances and defines sponsor permissions and guest access policies.
- Sponsor—The sponsor user is the person who creates the guest user account. This person is often an employee of the organization (for example, a lobby ambassador who creates and manages Guest User accounts through a sponsor-oriented web portal).
- Guest User—The guest user is the person who needs a guest user account to access the network and register devices.

You can configure the way in which sponsors and guests access the portal by specifying connection via HTTP only, HTTPS only, or HTTP redirect to HTTPS where the portals are available in both protocols. You can also specify the port number that is used for each of the portals and protocols.

Cisco ISE also lets you host multiple guest portals in the Cisco ISE server. You can design and upload HTML pages to define new guest portals or replace the default guest portal.

Client Provisioning

Cisco ISE Client Provisioning Service ensures that users get the correct resources installed on their host machine when they log into the network for the first time, or upon discovering that a newer version of the host software is available for upgrade and required for access.

Client Provisioning resources fall into the following categories:

- Persistent agents (Windows and Mac OS X Cisco NAC agents)
- Temporal agents (Cisco NAC Web agents)
- Agent customization files
- Agent profiles
- Compliance modules

Cisco ISE allows multiple versions of these resources, which enables administrators to customize Client Provisioning resource policies that are based on a variety of login characteristics (such as login location and time of day, user role, and host operating system). For example, the first time a new employee logs into a network that is protected by Cisco ISE, the employee is matched up with an assigned employee role. Based on the employee role and the Client Provisioning Resource Policy, Cisco ISE then determines which particular version of the Cisco NAC Windows agent and an accompanying Agent XML configuration file needs to be downloaded. Alternatively, if the user who is logging into the network fits the criteria of a guest, the Cisco ISE Client Provisioning Resource Policy that applies to that particular login session requires that the user download and launch the Cisco NAC Web agent. (The Cisco NAC Web agent automatically uninstalls itself from the client machine after the guest user session has terminated).

You can find the Client Provisioning Resource Policy configuration page in Cisco ISE at **Policy > Client Provisioning**.

Posture Assessment

In addition to the standard IEEE 802.1X authentication mechanism that manages network access, Cisco ISE offers host posture assessment capabilities that can help ensure that users do not log into the network with machines that could introduce malware, viruses, and other types of network security threats to the network.

Cisco ISE uses Posture Policies to determine which attributes on the host machine need to be verified before network access is authorized. Posture Policies consist of a variety of host conditions that need to be met before the production network can be accessed. In some instances, these host conditions require that the user take remediation actions to ensure that the host machine is compliant with the defined endpoint access policies.

When a user logs into the network, the Cisco ISE Posture Assessment Services analyze and categorize the host to determine if it is compliant or noncompliant and then specifies the next steps in the assessment or remediation process or both. For example, a compliant machine admits the user into the network in which the user is granted a level of access that is based on the assigned user role. A noncompliant or “out-of-date” machine may simply require an updated antivirus or antispyware application download or Agent upgrade to meet the compliance criteria. The user can quickly remediate during a temporary network access window. A noncompliant machine might also be “quarantined” and require manual remediation before it is allowed to access the production network.

To enable and configure posture assessment for client machines in Cisco ISE, you must obtain and install Advanced licenses.

You can find the Posture Policy configuration functions in Cisco ISE in the **Policy > Posture** page.

Profiling Service

Cisco ISE offers profiling services to help manage IP-enabled devices connected to the network. The Cisco ISE Profiler Service can be configured to automatically detect, locate, and determine the type of endpoints that are connected to the network. An administrator could classify endpoints based on Cisco ISE default profiles or administrator-defined profiles with the option for fine-grain definitions (for example, IP Phone > Cisco IP Phone > Cisco 7960 IP Phone). Cisco ISE profiles an endpoint by capturing contextual information from network technologies such as RADIUS, Simple Network Management Protocol (SNMP), DHCP, and NetFlow by using them as logical “sensors” on the network. Based on the contextual information that is captured by Cisco ISE, the administrator can then grant the appropriate network access through authorization policies to endpoints that match specific device profiles.

An endpoint in this context refers to all devices that connect to your network such as desktop and laptop computers and also other IP-enabled devices such as printers, fax machines, and IP phones. Some of these endpoints are not equipped with an 802.1X client (called the supplicant in the IEEE 802.1X standard). When an endpoint does not have an 802.1X client, the switch port must rely on an alternate authentication mechanism that is based on the MAC address of the endpoint. By combining authorization that is based on profiles with this alternative RADIUS authentication known as MAB, administrators can effectively manage access control on endpoints when a supplicant is not present.



Note

To support the Cisco ISE Profiling service, Cisco recommends using the latest version of NetFlow (version 9), which has additional functionality needed to operate the Profiler. If you use NetFlow version 5 in your network, then you can use version 5 only on the primary NAD at the access layer, as it will not work anywhere else.

Security Group Access Service

Cisco ISE is an integral part of the Cisco Security Group Access (SGA) solution. Cisco ISE functions as an authentication server in an SGA-enabled network to establish clouds of trusted network devices and build secure networks. Cisco ISE supports the following security group access features:

- **Network Device Admission Control (NDAC)**—In a trusted network, during authentication, each network device (for example, an Ethernet switch) in an SGA cloud is verified for its credential and trustworthiness by its peer device. NDAC uses the IEEE 802.1X port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its EAP method. Successful authentication and authorization in the NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
- **Endpoint admission control (EAC)**—An authentication process for an endpoint user or a device that connects to the SGA cloud. EAC typically happens at the access level switch. After a successful authentication and authorization during the EAC process, the user or device is assigned a security group tag (SGT). EAC access methods for authentication and authorization include the following:
 - 802.1X port-based authentication
 - MAC Authentication Bypass (MAB)
 - Web-Based Authentication (WebAuth)
- **Security group**—A grouping of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in Cisco ISE. As new users and devices are added to the SGA domain, Cisco ISE assigns these new entities to the appropriate security groups.

- **SGT**—The SGA service assigns to each security group a unique 16-bit security group number whose scope is global within an SGA domain. The number of security groups in the switch is limited to the number of authenticated network entities. You do not have to manually configure security group numbers. They are automatically generated, but you have the option to reserve a range of SGTs for [IP to SGT Mapping](#).
- **Security group access control list (SGACL)**—SGACLs allow you to control the access and permissions based on the SGTs that are assigned. The grouping of permissions into a role simplifies the management of security policy. As you add devices, you simply assign one or more security groups and they immediately receive the appropriate permissions. You can modify the security groups to introduce new privileges or restrict current permissions.
- **Environment data download**—The SGA device obtains its environment data from Cisco ISE when it first joins a trusted network. You can also manually configure some of the data on the device. The device must refresh the environment data before it expires. The SGA device obtains the following environment data from Cisco ISE:
 - Server lists—List of servers that the client can use for future RADIUS requests (for both authentication and authorization)
 - Device security group—Security group to which the device itself belongs
 - Expiry timeout—Interval that controls how often the SGA device should download or refresh its environment data
- **IP to SGT mapping**—Cisco ISE allows you to reserve a range of SGTs that you can manually configure on the SGA device tied to a specific IP address.

Inline Posture

Inline Posture node acts as an in-line RADIUS proxy and is needed only in posture use cases in which the networking devices such as WLCs and VPN concentrators do not support the necessary RADIUS access control features such as CoA and Session ID). The Cisco ISE Inline Posture node has a trusted interface and an untrusted interface. The trusted interface communicates with the Policy Service persona and other trusted devices that are logically inside the network. The untrusted interface talks to the WLC, VPN, and other networking devices that are logically outside the network. The logical separation of inside and outside on the Cisco ISE Inline Posture node is similar in concept to the trusted and untrusted sides of a firewall.

An administrator can configure a Cisco ISE Inline Posture node in a Bridged Mode, where it acts as a “bump in the wire” or as a Layer 2 device, or in Routed Mode, where it acts as a Layer 3 hop in the network. To introduce an Inline Posture node onto your Cisco ISE deployment, you must first register the Inline Posture node with the primary Cisco ISE node, configure the Inline Posture node settings, then create authorization profiles and policies that establish the Inline Posture gate-keeping policies. Administrators can have two Inline Posture nodes configured in a primary-secondary configuration for high availability; thus providing access control resiliency.

Monitoring and Troubleshooting

The Cisco ISE Monitoring and Troubleshooting service provides visibility into all Cisco ISE services and activities through a comprehensive set of dashboards, reports, and tools. These services include:

- **Monitoring**—Provides a real-time presentation of meaningful and contextual data that represents the state of access activities on a network. This insight allows administrators to easily interpret and control operational conditions.

- **Troubleshooting**—Provides contextual guidance for resolving access issues on networks. This allows administrators to address end-user concerns and provide network access problem resolution in a timely manner.
- **Reporting**—Provides a catalog of standard reports that administrators can use to analyze trends and monitor system performance and network activities. Administrators can customize reports in a variety of ways and save their customized changes for future use.

The rate and amount of data that is used for monitoring and troubleshooting may require a separate database on a dedicated node. The data gathered by a Monitoring persona is accessible from the central Administration persona console, known as the Cisco ISE dashboard. When you log into the Cisco ISE Administration persona, the real-time data shown on the dashboard is coming directly from the Monitoring persona. The dashboard display represents the activity on the network and provides drill-down capabilities into various components such as the following:

- AAA
- NAD and port monitoring
- RBAC enforcement

When a Cisco ISE node serving as a dedicated Monitoring persona is available, administrators should perform full and incremental backups to purge unwanted data or store data somewhere else in the network.

Resource Management

Cisco ISE provides administrators and users with the means for managing the following types of network resources:

- Dictionaries
- RADIUS vendors
- Templates
- Software

The RADIUS vendor resource includes different Cisco RADIUS dictionaries as well as a Microsoft RADIUS dictionary. Templates are used to control guest portal services. Software is for managing the configuration of endpoint software that is controlled by client provisioning.

Dictionaries and Dictionary Attributes

Dictionaries are a collection of individual parameters that can be used when configuring vendor-specific attributes. The supported dictionary and dictionary default settings include those in the Internet Engineering Task Force (IETF)-RADIUS set of attribute pairs that is defined by the IETF. To support attributes for other product vendors, you must create a new dictionary and populate it with corresponding dictionary attributes by using Cisco ISE. Then you can modify the new dictionary as needed. There are Cisco ISE system-defined dictionary and dictionary attributes that are read-only, and these are populated during the Cisco ISE installation process. To create user-generated dictionaries and dictionary attributes, use the following navigation path:

Administration > Resources > Dictionary

Each dictionary is defined by a name, description, version, dictionary attribute type, and the type of dictionary that it represents. Each dictionary contains attributes that provide information or describe data that is related to that dictionary. For example, the Certificate dictionary contains the following certificate-based attributes:

- Common name
- Email
- Location
- Organization
- Serial number

Dictionaries are a powerful and flexible tool for building network-based controls for business driven access policy.

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 17](#)
- [Cisco ISE Live Updates, page 18](#)
- [Cisco ISE Offline Updates, page 18](#)

Cisco ISE Downloads from the Cisco Download Software Center

In addition to the .ISO installation package required to perform a fresh installation of Cisco ISE on your appliance as described in [Installing Cisco ISE Software, page 6](#), 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.

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 1.0**.

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 download agent, AV/AS support, and agent installer helper packages that support the Client Provisioning and Posture policy services. Use this portal to retrieve the latest Client Provisioning and Posture software after you have configured your Cisco ISE deployment.

To access the Client Provisioning and Posture Live Update portals and download necessary Cisco ISE software:

Open a web browser and navigate to one of the following URLs:

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

The following software elements are available at this URL:

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

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the “Downloading Client Provisioning Resources Automatically” section of the “Configuring Client Provisioning Policies” chapter in the *Cisco Identity Services Engine User Guide, Release 1.0*.

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

The following software elements are available at this URL:

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

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the “Dynamic Posture Updates” section of the “Configuring Client Posture Policies” chapter in the *Cisco Identity Services Engine User Guide, Release 1.0*.

If you do not enable the automatic download capabilities described above in Cisco ISE, you can choose to “subscribe” to either or both of these sites (thus establishing a one-click access point in your web browser), or access manually as needed to download and save the software you require to your local machine where you can then make it available for Client Provisioning and Posture policy service support in Cisco ISE.


Cisco ISE Offline Updates

Cisco offline updates apply to the Posture policy service in Cisco ISE. You can update the checks, rules, antivirus and antispymware support charts for both the Windows and Macintosh operating systems, and operating systems information offline from an archive on your local system. 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.

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 Offline Posture Update site. For more information on proxy settings, see the “Specifying Proxy Settings in Cisco ISE” section in the “Configuring Client Provisioning Policies” chapter of the *Cisco Identity Services Engine User Guide, Release 1.0*.

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. The **posture-offline.zip** file contains the following:
- av-chart-mac.tar.gz
 - av-chart.tar.gz
 - osgroups.tar.gz
 - se-templates.tar.gz
 - update.xml
- Step 2** Access the Cisco ISE administrator user interface and choose **Administration > System > Settings > Posture**.
- Step 3** Click the arrow to view the settings for posture.
- Step 4** Choose **Updates**. The Posture Updates page appears.
- Step 5** From the Posture Updates page, choose the **Offline** option.
- Step 6** From the **File to update** field, click **Browse** to locate the single archive file (**posture-offline.zip**) from the local folder on your system.
-  **Note** The File to update field is a required (mandatory) field and it cannot be left empty. You can only select a single archive file (.zip) that contains the appropriate files. Archive files other than .zip (like .tar, and .gz) are not allowed.
-
- Step 7** Click the **Update Now** button.
- Once updated, the Posture Updates page displays the current Cisco updates version information as a verification of an update under Update Information.
-

Cisco ISE Antivirus and Antispyware Support

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

- [Cisco Identity Services Engine Release 1.0 Supported Windows AV/AS Products](#)
- [Cisco Identity Services Engine Release 1.0 Supported Mac OS X AV/AS Products](#)

Cisco ISE Release 1.0 Open Caveats

- [Cisco ISE Release 1.0 Appliance Open Caveats, page 20](#)
- [Cisco ISE Release 1.0 Agent Open Caveats, page 38](#)

Cisco ISE Release 1.0 Appliance Open Caveats

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats

Caveat	Description
CSCtc70053	<p>Browser “Back” button not working properly</p> <p>This issue has been observed in the Cisco ISE list page when switching from the list view to edit view (i.e., when you click the Create or Edit button).</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj00178	<p>Group QuickFilters not working as designed</p> <p>After the administrator runs and saves an advanced filter, Cisco ISE does not display the “Successful Save” pop-up after the filter is saved.</p> <p>This issue has been observed using the Admin Groups, User Identity Groups, Endpoint Identity Groups, and Guest Sponsor Groups filter options.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj25158	<p>Exported admin should not be imported back as Network Access User</p> <p>This problem occurs when Cisco ISE promote Network Access Users to Administrators, and then export those users. When you re-import those users, they appear as Network Access Users only. Cisco ISE does not import the promoted users as Administrators.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj37325	<p>Profiler Attribute value exceeds maximum 4000 character length</p> <p>Endpoints are not profiled nor are new attributes updated when at least one Profiler Endpoint Attribute is greater than 4000 characters in length.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)


Caveat	Description
CSCtj76835	<p data-bbox="581 310 1193 346">Unable to retrieve a saved Authentication Trend report</p> <p data-bbox="581 415 1421 451">Symptom Two steps are necessary to save an Authentication Trend report:</p> <ol data-bbox="581 457 820 535" style="list-style-type: none"> <li data-bbox="581 457 820 493">1. Select the folder. <li data-bbox="581 499 820 535">2. Name the file. <p data-bbox="581 546 1523 682">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 data-bbox="581 703 1453 739">Conditions Saving an Authentication Trend report without selecting a folder.</p> <p data-bbox="581 766 1429 835">Workaround Do not save the report under the root folder. Always choose a subfolder.</p>
CSCtj81255	<p data-bbox="581 842 1453 877">Two MAC addresses detected on neighboring switch of ACS 1121 Appliance.</p> <p data-bbox="581 940 1523 1039">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 data-bbox="581 1066 1523 1102">Conditions Only one Ethernet interface, eth0 is connected between ACS and Switch.</p> <p data-bbox="581 1129 1469 1207">Workaround Disable BMC (Baseboard Management Controller) feature using BIOS setup.</p> <p data-bbox="581 1228 665 1270"></p> <p data-bbox="581 1276 1523 1438">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 data-bbox="581 1457 1523 1522">Left side administrator user interface pane “Search Result” option is not working as expected</p> <ol data-bbox="581 1533 1469 1722" style="list-style-type: none"> <li data-bbox="581 1533 1469 1606">1. If you enter available data and click the search option, it does not display properly. <li data-bbox="581 1612 1469 1686">2. If the option displays some data and if you enter another value, it does not refresh the data properly. <li data-bbox="581 1692 1469 1722">3. The option does not display the layered/structured model as designed. <p data-bbox="581 1732 1234 1768">In addition, you are not able to go back to previous menu.</p> <p data-bbox="581 1795 1242 1831">Workaround There is no known workaround for this issue.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCtk17648	<p>IE8—Network Device Management missing from the Cisco ISE Administrator Tab</p> <p>This issue has been observed when changing the zoom setting in Internet Explorer 8 using the control and plus (+)/minus (-) keys.</p> <p>Workaround If the menu is missing, change the zoom to the default value and refresh the page.</p>
CSCtk32480	<p>Local certificate export failed after deleting trusted certificate</p> <p>After you delete a trusted certificate, local certificate export operation fails.</p> <p>Administration > System > Certificates > Local Certificates > Export. Instead of being prompted for the export file destination, nothing happens.</p> <p>Workaround Reload the page using the browser reload function. This should reload all of the Javascript files for the page and allow you to export the local certificate.</p>
CSCtk37360	<p>Administrator is not able to customize report in Internet Explorer 8</p> <p>Monitoring and troubleshooting reporting functions related to column selection and entry deletion/aggregation, etc. are not working as designed.</p> <p>This issue can come up using the following versions of Internet Explorer 8:</p> <ul style="list-style-type: none"> • IE 8.0.6001.18702 on Windows XP • IE 8.0.6001.18702IC on Windows XP <p>Workaround There is no known workaround other than to avoid using the problematic browser versions.</p>
CSCtk46958	<p>Cisco ISE does not display a warning when navigating away from a modified page without saving</p> <p>When a user changes configuration context, there is no warning indicating that the information configured on the current page is not saved, nor is there a warning indicating that all configuration changes will be lost when the user completes that context change.</p> <p>Workaround Save before navigating away from the page in question.</p>
CSCtk82864	<p>AAA Servers incorrectly filter with “Contains” option</p> <p>When AAA servers are added to the AAA servers list (for example: a, ab) and a filter is added which includes regular expressions, Cisco ISE generates an incorrect filtered list.</p> <p>Workaround Do not use regular expressions in filters.</p>
CSCtl56724	<p>Network access users display filter sorted by status does not work</p> <p>An issue exists in the Administration > Identity Management > Identities > Users page where Cisco ISE does not appropriately filter Network Access User entries when you click on the filter and try to specify “sort by status.”</p> <p>Workaround There is no known workaround for this issue.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
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 entreated on the RHS when constructing a condition.</p> <p>Workaround Use the MAC address format xx:xx:xx:xx:xx:xx when defining conditions.</p>
CSCtl78424	<p>Blank right hand Network Devices pane with vertical scroll</p> <p>The Network Device page contains the navigation pane on the left of the page and the network devices table on the right of the page. If there are more than 500 devices configured and the following steps have been taken, the devices table does not appear as it should:</p> <ol style="list-style-type: none"> 1. Move the vertical scroll all the way to the bottom and wait a few seconds. 2. Move vertical scroll to the top and then back to the bottom again (and repeat if necessary) until the table disappears. 3. The table remains empty (blank) for 30 minutes or more. <p>Workaround Manually refresh the devices page.</p>
CSCtn42397	<p>The Network Access Users “Delete All” function when used on a filtered list should only delete filtered (displayed) Network Access Users</p> <p>The “Delete All” function in the Administration > Identity Management > Identities > Users page deletes <i>all</i> the users, regardless of whether they are filtered or existing (non-filtered) users.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtn44427	<p>No progress indicator is displayed when importing collections of random or CSV guests</p> <p>Workaround There is no known workaround for this issue. The administrator must simply wait for the process to complete.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
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>
CSCtn59529	<p>Network Access User filters do not work on the Status or Admin columns using the Quick and Advanced filters</p> <p>Cisco ISE search functions are not supported on columns which have images or icons. The Status and Admin columns use images and icons instead of text, therefore filtering does not work.</p> <p>Workaround There is no known workaround for this issue,</p>
CSCtn62141	<p>A script on the Administration > Identity Management > Groups page causes Internet Explorer 8 to run slowly. If it continues to run indefinitely, your computer could become unresponsive. (This problem has not been observed using Mozilla Firefox.)</p> <p>Workaround There are three ways to fix this issue:</p> <ol style="list-style-type: none"> 1. Implement Virtual Scrolling in the Object Selector. 2. Change the time-out value as follows: <ol style="list-style-type: none"> a. Using a Registry Editor such as Regedt32.exe, open the HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles key. b. Create a new DWORD value called “MaxScriptStatements” under this key and set the value to the desired number of script statements. If you are unsure of what value you need to set this to, you can set it to a DWORD value of 0xFFFFFFFF to completely avoid the dialog. 3. Install and apply the following patch from Microsoft: <p style="margin-left: 20px;">http://support.microsoft.com/kb/175500#FixItForMeAlways</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>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCtn73422	<p>Network Access User filters filtering correctly</p> <p>The filter display does not conform to the expected alphanumeric order. For example, create four users with the following IDs:</p> <ul style="list-style-type: none"> • 2234567890a • a214567890 • 2b34567890-2 • a214-25678 <p>Use either the Quick/Advanced Filter with a “Name: Contains _2” attribute. The resulting list is returned as follows:</p> <ul style="list-style-type: none"> • 2234567890a • 2b34567890-2 • a214-25678 • a214567890
CSCtn78676	<p>When a user name has a space between words and another similar name contains two or more spaces, Cisco ISE displays the same user name for both users.</p> <p>Workaround There is no known workaround for this issue. Even though the multiple spaces are trimmed and shown as one space in the UI, the data is saved correctly in the database.</p>
CSCtn78899	<p>When a user group name has a space between words and another similar user group name contains two or more spaces, Cisco ISE displays the same user group name for both groups.</p> <p>Workaround Avoid giving spaces in the name field while creating Identity Group.</p>
CSCtn80646	<p>Cisco ISE does not display a purge confirmation message after purging is completed</p> <p>This issue has been observed when purging generic tables.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtn83738	<p>Session status summary report failing for Wireless LAN Controllers</p> <p>It appears that Cisco ISE may not be appropriately handling public/private community stings.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtn92594	<p>Quickpicker filters are not working correctly during Client Provisioning policy configuration</p> <p>This issue has been observed with the following three filter options:</p> <ul style="list-style-type: none"> • Identity Groups • Operating Systems • Other conditions <p>Workaround There is no known workaround for this issue.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

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

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto06361	<p>Changing the User Identity Group name case should not return error upon search</p> <p>After you Create a User Identity Group called “mickeymousegroup,” edit the name to be “MickeyMouseGroup.” Cisco ISE displays the following error:</p> <p>“Identity Group with name ‘NAC Group:NAC:IdentityGroups:User Identity Groups:MickeyMouseGroup’ already exists.”</p> <p>Workaround Delete and recreate the User Identity Group.</p>
CSCto09989	<p>Cisco ISE browser session redirects to Monitoring login page using Internet Explorer 8</p> <p>As soon as you login to Cisco ISE via IE8 the page gets redirected to a Monitoring node administrator login page (even before the initial page displays completely).</p> <p>Note This issue has also been observed using Mozilla Firefox, but the redirection in Firefox only takes place after a couple of minutes of inactivity.</p> <p>Workaround Immediately after entering your login credentials,. navigate from the main Cisco ISE page to any configuration page (like Posture, Authorization, or Client Provisioning, for example).</p> <p>For more information, see Issue Accessing the Cisco ISE Administrator User Interface, page 42.</p>
CSCto10678	<p>Administrator user should not be able to delete self policy</p> <p>If self-policies get deleted, the administrator cannot log in.</p> <p>Workaround The Cisco ISE administrator should not delete their own access policy.</p>
CSCto10855	<p>IE8 with default option settings is not working</p> <p>This issue arises when the default URL has been specified in Administration > System > Setting > Posture Updates.</p> <p>Workaround There is no known workaround for this issue.</p> <p>Note This functionality is working as designed using a Firefox browser.</p>
CSCto13102	<p>No “Cisco ISE Configuration Changes” message dialogs are displayed for certain guest/sponsor configuration</p> <p>Certain dialogs are missing for guest and sponsor configuration changes, hence, Cisco ISE does not confirm when changes have been made and accepted.</p>
CSCto13235	<p>File Condition Advanced Filter does not return correct result</p> <p>This issue has been observed in the Advanced Filter function of the Posture Simple Condition and Remediation pages. The “Match All/Any of the Following Rules” selection is not working as expected.</p> <p>Workaround There is no known workaround for this issue.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto13986	<p>IE8—Error when clicking the “Action” button on the Requirement page</p> <p>Go to Policy > Policy Elements > Results > Posture > Remediation Action and click on the Requirement in the left hand navigation pane. Once the page loads, then click on the “Action” button. A Java script error is returned when accessing the page via Internet Explorer 8.</p> <p>Note This is an issue with Internet Explorer 8 and is working as expected.</p>
CSCto15508	<p>Filter in Security Group Access Egress Policy is not working correctly</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto17461	<p>Invalid Simple Condition error message in Guest configuration</p> <p>If you duplicate, but do not rename a new Simple Condition in the Policy Elements > Conditions > Guest > Simple Condition page, Cisco ISE returns an error message indicating that the condition has not been saved.</p> <p>Workaround Change the name of the condition that is being duplicated before saving it.</p>
CSCto22671	<p>HTTPS communication fails if the certificate is deleted from the primary Administration ISE node</p> <p>The following operations on the primary Administration ISE node fail unexpectedly:</p> <ul style="list-style-type: none"> - Restoration of a backup - Manual sync - Node deregistration <p>If the certificate(s) required to validate the HTTPS certificate of a registered node have been removed from the primary Administration ISE node trust store, they must be reimported in to the trust store before attempting restore database material, perform manual sync, or deregister other policy service nodes.</p>
CSCto22872	<p>Endpoints are not profiled correctly when there is a router in the network</p> <p>If SPAN or Netflow collection is done on a network device that is not Layer 2 adjacent to the endpoint, the MAC address of the collected endpoint does not correspond to the MAC address of the endpoint due to Layer 3 routing.</p> <p>Note Cisco recommends enabling SPAN and Netflow collection on Layer 2 adjacent devices so that the MAC-to-IP address mapping is done properly.</p>
CSCto24105	<p>A Network Access User can be created with a name longer than 25 characters via network access user import, but Cisco ISE cannot reliably handle user names that long.</p> <p>Workaround There is no known workaround for this issue.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto24430	<p>Details of guest RADIUS authentication failure are not available when searching via the guest username</p> <p>This issue has been observed where the guest user has logged in with space appended to the beginning or end of the user name.</p> <p>Workaround The guest user must enter the user name without any additional spaces entered at the beginning or end.</p>
CSCto27568	<p>Cannot enable checkboxes in the right hand Filtered Network Devices pane</p> <p>The administrator is not able to select a checkbox under the following conditions:</p> <ol style="list-style-type: none"> 1. The browser window is not open to its maximum size. 2. A filter is applied to the network device table. <p>Workaround Apply filters to the network device table only when the browser window is maximized.</p>
CSCto29479	<p>Cisco NAC Web Agent fails to validate Registry Condition</p> <p>Registry condition check does not work correctly on 64-bit Windows operating systems.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto33037	<p>Allowed character sets between policy conditions and element conditions are different</p> <p>When conditions are created inside policies, the allowed character sets are not the same. Condition policies allow alphanumeric, hyphen(-), underscore(_), or period(.), The condition page itself allows letters, numbers and “_”.</p> <p>Workaround Use the common characters of both sets: letters, numbers, and “_”.</p>
CSCto33973	<p>Joining Cisco ISE to an Active Directory domain locks up when the Global Catalog is down or unreachable</p> <p>Having a Global Catalog active is essential for Cisco ISE operation with Active Directory. If there is no Global Catalogs available, the Cisco ISE user interface locks up for a long time in certain operations. This issue applies to a single domain environment.</p>
CSCto41078	<p>Cannot create an Identity Group using the gear icon during Client Provisioning policy configuration</p> <p>Workaround Create the Identity Group using the Administration > Identity Management > Groups page before configuring the policy.</p>
CSCto41340	<p>Authentication Policy replication failure from Primary to Secondary if the time zone changes after installation</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto42182	<p>Profiling HTTP requests for 802.1X scenarios may not include agent</p> <p>This issue occurs when the initial HTTP request for 802.1X authentication and Posture services are redirected to the gateway via HTTPS.</p> <p>Workaround Try using URL redirection over port 8080 for the gateway.</p>
CSCto43825	<p>Synchronization fails with time zones other than UTC</p> <p>During installation, if you specify a time zone other than UTC, replication fails during registration and Synchronization status shows “OUT OF SYNC.”</p> <p>Workaround To avoid this issue, change the time zone to UTC, enter the reset-config command via CLI, and reregister the node.</p>
CSCto45372	<p>Default Sponsor Groups do not allow the Sponsor to create users or view passwords.</p> <p>Workaround Navigate to the Guest Management > Sponsor Groups page and change the Sponsor Groups to allow appropriate access rights to Sponsors in these groups.</p>
CSCto48657	<p>Profiled endpoints are not all deleted</p> <p>If you delete endpoints that have recently been imported (before Cisco ISE can finish Profiling all of the new endpoints), Cisco ISE does not delete them all.</p> <p>Workaround Wait until all endpoints have been profiled before trying to delete them, or try to delete the remaining endpoints again after the initial attempt.</p>
CSCto49359	<p>Filters not working correctly on Guest conditions page</p> <p>Filters are not getting saved in the Policy Elements > Conditions > Guest > Simple Conditions page.</p> <p>Workaround Re-enter the filter to get Cisco ISE to perform the list filtering correctly.</p>

Table 5 Cisco ISE Release 1.0 Appliance 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
CSCto59976	<p>Sync with NTP server during initial set-up shows failure although NTP server is reachable.</p> <p>This issue occurs if an invalid or unreachable NTP server was first specified during initial installation and is then corrected (reconfigured) with an NTP server which has less characters than the initial invalid NTP server entry.</p> <p>Workaround When the set-up shows “Sync with primary NTP server failed,” press CTRL+C and restart the set-up from scratch, this time providing the valid and reachable NTP Server in the initial prompt itself.</p>
CSCto60148	<p>Java crashes during high posture load</p> <p>This issue has been observed under extreme load condition where Cisco ISE is hit with large number of concurrent users for posture.</p> <p>Workaround None. You must restart the Cisco ISE Policy Service.</p>
CSCto60636	<p>Favorite reports are not preserved after executing “application reset-config ise” in the Cisco ISE CLI</p> <p>After the reset-config operation is complete, you can manually add the corresponding reports to favorites again.</p>
CSCto63749	<p>The Cisco ISE dashboard does not display endpoints entered via the Administrator user interface</p> <p>Endpoint display behavior works as designed for imported or detected Endpoints.</p> <p>Workaround Define the endpoint(s) in a CSV file and import the CSV file.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto64028	<p>“Fail to receive server response...” seen when deleting profiling policy</p> <p>A “Fail to receive server response due to the network error (ex. HTTP timeout)” error message may appear when deleting Profiling policies, and some of the policies may not be deleted.</p> <p>Workaround Log out from Cisco ISE, log back in, and try deleting the policies again.</p>
CSCto68519	<p>Sorting / Filtering Does Not Work in Egress Table</p> <p>Can not filter or sort Egress policy table data</p> <p>Workaround There is no known workaround for this issue.</p> <p>Note It is not possible to filter the Egress policy table data based on source / destination security group. In addition sorting is not available as well</p>
CSCto70968	<p>Fast reconnect is not working for PEAP-TLS protocol</p> <p>When the supplicant is eligible for PEAP-TLS fast reconnect after establishing a PEAP tunnel, Cisco ISE does not allow the fast reconnect function and falls back to the standard inner method.</p> <p>The following messages appear in the customer log:</p> <ul style="list-style-type: none"> • 22044 Identity policy result is configured for certificate based authentication methods but received password based • 12317 PEAP fast-reconnect failed; starting inner method <p>Workaround There is no known workaround for this issue.</p>
CSCto72521	<p>Save failed for child group assignment during Client Provisioning policy configuration</p> <p>An exception dialog box appears, displaying a “Invalid identity group in policy <policy name>. There were errors in the save” message.</p> <p>Workaround Use first-level identity groups whenever possible.</p> <p>Note Identity Group selection is more than one level deep. For example, if an administrator creates hierarchal groups like “Employee” or “Accounting” and selects “Accounting” as an Identity Group when creating or updating a client provisioning policy.</p>
CSCto72594	<p>Cisco ISE cannot save a Posture Policy when the Identity Group is the child of one or more other Identity Groups</p> <p>Cisco ISE returns a “Policy Policy_Check_For_AV_Installation_Win: Error - class com.cisco.cpm.posture.exceptions.PostureValidationException: invalid role” message and does not save the Posture Policy in question.</p> <p>Workaround Use only first-level Identity Groups.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto73439	<p>Restart required upon completion of Monitoring node database restoration</p> <p>This issue has been observed with both scheduled and incremental backup and restore functionality.</p> <p>After completing a Monitoring node database restoration, manually synchronizing a Secondary node from the Primary node does not work because the Secondary Administration ISE node data has been changed by the Monitoring node restoration operation.</p> <p>Workaround There are two possible workarounds for this issue:</p> <ul style="list-style-type: none"> • Log into the Cisco ISE CLI with admin privilege and execute the following commands: <ul style="list-style-type: none"> a. application stop ise b. application start ise • Log into the Cisco ISE CLI with admin privilege and execute the reload command.
CSCto74356	<p>Self-registered Guest role does not appear associated with the Guest account</p> <p>If the administrator creates a new Identity Group (group role) and specifies this role as the default group role on the Guest Portal Policy page for self registration, the newly created Identity Group is not added to the identity group list for a sponsor group.</p> <p>This issue can occur in both standalone and distributed deployment.</p> <p>Workaround Add the new Identity Group to the Sponsor Group to which the sponsor is mapped, which shows the correct Identity Group in the Edit panel of the Guest account.</p>
CSCto75963	<p>No alert message is displayed in Cisco ISE when the Client Provisioning Update Feed URL (or proxy, if specified) is unreachable</p> <p>When you specify an Update Feed URL using the Policy > Results > Client Provisioning > Resources > Add a resource from Cisco site function, Cisco ISE just shows that it is perpetually “Loading,” even if the URL is actually unreachable.</p> <p>Workaround Verify the server specified in the Update Feed URL (or proxy when specified) is reachable using the Cisco ISE CLI. (Ping, etc.)_</p> <p>Note An error message does appear under in the Monitor > Catalog > Server Instance > Server System Diagnostics report indicating that there is an error connecting to the Feed URL. The Debug log (ise-psc.log) also contains similar error message.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto82519	<p>Saving your Active Directory configuration while the DNS is down takes a very long time</p> <p>Cisco ISE requires connectivity to Active Directory (including DNS) when saving the configuration. If the DNS is not reachable, then the save function may time out before it can complete.</p> <p>Workaround Ensure that the DNS is available and reachable before saving your Active Directory configuration.</p>
CSCto82631	<p>Clicking the “Name” field in the Cisco ISE User Identity Group page yields unexpected download behavior</p> <p>Workaround There is no known workaround for this issue.</p>
CSCto83078	<p>Guest Accounting and Sponsor Summary report errors returned during report generation</p> <p>If the administrator launches the Guest Accounting and Sponsor Summary reports and custom time ranges have been specified, Cisco ISE fails to launch and returns an error message.</p> <p>Workaround Cisco recommends using preset options like the last 30 days or last 7 days.</p>
CSCto83897	<p>Client machine authentication shift to user authentication not updating Active Directory groups</p> <p>During a Wireless LAN Controller (WLC) login session, the client machine authenticates with Cisco ISE correctly and the corresponding authorization profile is picked up. During user authentication, however, (although system log entries indicate that user authentication has happened correctly) the previous authorization profile (for machine authentication) is applied to the user session again.</p> <p>This issue has been observed during wireless login scenarios where the WLC is running firmware version 7.0.116.0.</p> <p>Workaround If you do not require the new WLC features (such as NAC-RADIUS) introduced in firmware version 7.0.116.0, Cisco recommends restoring the WLC version to 7.0.98.218 until a new firmware version becomes available.</p> <p>For more information, see Known Incompatibility Issue with WLC Firmware Version 7.0.116.0, page 43.</p>
CSCto87755	<p>Guest accounting report appears only once, even though Guest logs in multiple times</p> <p>This issue has been observed when Guest users have logged in using the same endpoint multiple times. The report shows only the user's first login details, not the most recent login.</p> <p>Workaround There is no known workaround for this issue.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCto92848	<p>Report generation fails when custom range in Security Group Access - > Top_N_SGT_Assignments is specified</p> <p>When the report Security Group Access > Top_N_SGT_Assignments is launched using the custom time range option, report generation fails and returns an error message.</p> <p>Workaround Cisco recommends using one of the standard preset time range options like last 30 days, last 7 days, yesterday, or today.</p>
CSCtq00096	<p>Compound condition from a Sponsor Group Policy has a different name after it is saved</p> <p>This new name can erase the existing condition in the Cisco ISE configuration and the administrator must assign the condition again.</p> <p>Workaround If you are editing conditions in the Sponsor Group Policy, specifically reassign the compound condition.</p>
CSCtq03906	<p>Condition duplication during Authorization Policy configuration does not work properly</p> <p>Duplicating a condition in the condition builder while configuring an Authorization Policy does not set the Dictionary Attribute correctly. When the administrator selects an “ad hoc” condition in the condition builder and tries to duplicate that condition setting, the new duplicated condition does not copy the specified Dictionary Attribute from the original condition.</p> <p>Workaround The administrator must manually select the Dictionary Attribute using the TextPicker tool.</p>
CSCtq05485	<p>AnyConnect Supplicant from AnyConnect 2.5/3.0 client application</p> <p>The endpoint is not profiled correctly, or the assigned profile changes intermittently. This issue has been observed on client endpoints running the AnyConnect agent, and for which an HTTP probe has been enabled in Cisco ISE. The AnyConnect agent sends “User-Agent” attributes with values that mask the operating system and interfere with profiling functions.</p> <p>Workaround Disable the AnyConnect supplicant on the client machine.</p>
CSCtq09655	<p>Dictionary Attribute duplication is not happening as designed during Authentication Policy configuration</p> <p>Dictionary Attributes are not being duplicated appropriately within a rule during Authentication Policy configuration. Only the “operator” and “condition” values are getting duplicated.</p> <p>Workaround You must manually specify the Dictionary Attribute to complete the configuration.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCtq11650	<p>The primary Administration ISE node has database links to Inline Posture nodes following promotion from secondary to primary</p> <p>The newly-promoted primary node attempts to replicate with Inline Posture nodes and saves the undeliverable messages in its local database. This issue has been observed in a distributed deployment with Inline Posture nodes associated with an Administration ISE node that has been promoted from secondary to primary.</p> <p>Workaround Use root patch and SQLPlus to clean it.</p>
CSCtq17744	<p>Exception policy not getting created first time in Authorization policy</p> <p>When you create the first new exception policy under an Authorization Policy, an error pops up indicating that the operation has failed.</p> <p>This issue has been observed when there are no items in the exception policy pane and the user clicks Create New. After the user submits the change, an error message comes up.</p> <p>Workaround There are two possible workarounds for this issue:</p> <ol style="list-style-type: none"> 1. Use the Duplicate function to add a second exception policy below the first one, and then delete the first exception. Once all the changes are done, then save the policy. 2. Similar to the first option above, use the Insert function to insert a second exception policy below the first one, and then delete the first exception. Once all the changes are done, then save the policy.
CSCtq21992	<p>Active Directory guest user login displays an application malfunction error</p> <p>A NullPointerException appears when Multiportal Authentication is set to Guest Only and incorrect credentials are entered in the Guest login portal. As a result, the Guest User cannot be found and is not checked appropriately in the flow.</p> <p>Workaround Select “Both” in the Authentication Tab of the Multiportal configuration page and select an Identity Store Sequence. This should yield proper error handling for incorrect Guest credentials.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCtq22287	<p>WSUS check is failing on Windows 7 64- and 32-bit systems</p> <p>Posture conditions verifying Windows hotfixes may still fail even though endpoint system has hotfixes installed. This issue has been observed on Windows 7 client machines without SP1 or later installed. The posture compound condition in question is “pr_Win7_64_Hotfixes” or “pr_Win7_32_Hotfixes.”</p> <p>Workaround There are two possible workarounds for this issue:</p> <ol style="list-style-type: none"> 1. Install SP1 or later with hotfixes on the Windows 7 systems. 2. Create your own compound conditions replacing “pr_Win7_64_Hotfixes” and “pr_Win7_32_Hotfixes” as follows: <ol style="list-style-type: none"> a. Create a duplicate Registry condition “pc_W7_SP0_dummy” from “pc_W7_SP0” and edit it so that the operator specifies “does not exist.” b. Create a duplicate compound condition “pr_Win7_32_Hotfixes_dummy” from “pr_Win7_32_Hotfixes” and “pr_Win7_64_Hotfixes_dummy” from “pr_Win7_64_Hotfixes.” c. Edit the expression in compound conditions “pr_Win7_32_Hotfixes_dummy” and “pr_Win7_64_Hotfixes_dummy,” by replacing “pc_W7_SP0” with “pc_W7_SP0_dummy.” d. Use “pr_Win7_32_Hotfixes_dummy” or “pr_Win7_64_hotfixes_dummy” in the requirement.
CSCtq22779	<p>Cisco ISE allows saving authorization compound conditions with the same names</p> <p>If you create two authorization compound conditions called “C1” and “C2,” then change the name of “C2” to “C1,” Cisco ISE does not return an error and you end up with two compound conditions called “C1.” This happens only for authorization compound conditions.</p> <p>The potential impact of this problem is that the contents of the original “C1” compound condition is always picked up and enforced in authorization policies that use “C2.”</p> <p>Workaround There is no known workaround for this issue. You must be sure to create conditions with unique names. If you do end up creating two or more conditions with the same name, you can always rename them appropriately at any time.</p>
CSCtq26502	<p>Windows XP client machines need to be updated for NAC agent to work</p> <p>Installing the Cisco NAC Agent on a freshly installed Windows XP machine does not work. The Cisco NAC Agent does not pop up as it should for login. SWISS Exception errors are also recorded for every SWISS request sent from the Cisco NAC Agent.</p> <p>Workaround You can avoid this issue by installing the latest patches, hotfixes, and/or service pack on Windows XP client machines.</p>

Table 5 Cisco ISE Release 1.0 Appliance Open Caveats (continued)

Caveat	Description
CSCtq27834	<p>Monitoring COPY_RESOURCE_HIERARCHY exception errors and replication failures</p> <p>An administrator might receive notifications of replication failures or see critical alarm entries in the Monitoring “In” box, and endpoints might not be profiled correctly with the modified policies. This issue has been observed when one or more parent profiling policies are changed.</p> <p>Workaround If you need to change the parent field of a profiling policy, duplicate or create a new copy of the policy and associate it with NONE or the new parent.</p>

Cisco ISE Release 1.0 Agent Open Caveats

Table 6 Cisco ISE Release 1.0 Agent Open Caveats

Caveat	Description
CSCtg97488	<p>Client running Cisco NAC Agent does not disconnect after Windows logoff</p> <p>When an authenticated Windows client logs off from the Active Directory domain, the Access VLAN does not switch back to the Authentication VLAN. This is a security risk as another user could login to that same PC and be on the access VLAN configured for the previous users role.</p> <p>Note If the client machine has the Cisco NAC server certificate installed, the client functions as expected.</p>
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 6 Cisco ISE Release 1.0 Agent Open Caveats (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>
CSCtj39429	<p>No posture on Mac OS X Agent in multi-NIC setup</p> <p>This issue has been observed on Mac OS 10.6 clients in a multi-NIC setup where the wired NIC is connected to a switch and the wireless NIC connects to an Inline Posture node in bridged mode.</p> <p>Note Because the wireless NIC is the preferred connection, the agent is supposed to perform posture assessment via the wireless NIC.</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtj59635	<p>Cisco NAC agent pops up even when popup login window is unchecked</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtk34851	<p>XML parameters passed down from server are not using the mode capability</p> <p>The Cisco ISE Agent Profile editor can set parameter modes to merge or overwrite. Mac OS X agent is not processing the mode correctly. Instead, the complete file is overwritten each time.</p> <p>Workaround To use a unique entry, the administrator must set up a different user group for test purposes, or set the file to read only on the client machine and manually make the necessary changes to the local file.</p>
CSCtl53966	<p>Agent icon stuck on Windows taskbar</p> <p>The taskbar icon should appear when the user is already logged in.</p> <p>Workaround Right-click on the icon in the taskbar tray and choose Properties or About. After you close the resulting Cisco NAC Agent dialog, the taskbar icon goes away.</p>
CSCtn39974	<p>An IP configuration error during logout may keep agent from appearing to the user</p> <p>The agent login processing does not start after the IP refresh error occurs during the logout processing in an Out-of-Band environment.</p> <p>Workaround Exit and re-launch the agent.</p>

Table 6 Cisco ISE Release 1.0 Agent Open Caveats (continued)

Caveat	Description
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>
CSCto34354	<p>Cisco NAC Web Agent fails to validate Registry Conditions</p> <p>End users are asked to remediate even though the condition is satisfied. Cisco NAC Web Agent fails to validate existence of a registry condition with single level KEY (e.g., HKLM\SOFTWARE).</p> <p>Note The Cisco NAC Agents (persistent agents) do not have this problem.</p>
CSCto45199	<p>“Failed to obtain a valid network IP” message does not go away after the user clicks OK</p> <p>This issue has been observed in a wired NAC network with IP address change that is taking longer than normal. (So far, this issue has only been only seen on Windows XP machines.)</p> <p>Workaround None. The user needs to wait for the IP address refresh process to complete and for the network to stabilize in the background.</p>
CSCto48555	<p>Mac OS X agent does not rediscover the network after switch from one SSID to another in the same subnet</p> <p>Agent does not rediscover until the temporary role (remediation timer) expires.</p> <p>Workaround The user needs to click Complete or Cancel in the agent login dialog to get the agent to appear again on the new network.</p>
CSCto63069	<p>The nacagentui.exe application memory usage doubles when using “ad-aware”</p> <p>This issue has been observed where the nacagentui.exe memory usage changes from 54 to 101MB and stays there.</p> <p>Workaround Disable the Ad-Watch Live Real-time Protection function.</p>

Table 6 Cisco ISE Release 1.0 Agent Open Caveats (continued)

Caveat	Description
CSCto84932	<p>The Cisco NAC Agent takes too long to complete IP refresh following VLAN change</p> <p>The Cisco NAC agent is taking longer than normal to refresh IP address due to double IP refresh by supplicant and NAC agent.</p> <p>Workaround Disable the Cisco NAC Agent IP address change function if there is a supplicant present capable of doing the same task.</p>
CSCto97422	<p>Auto Popup does not happen after clicking Cancel during remediation failure</p> <p>Workaround Click on the login option in the system tray.</p>
CSCto97486	<p>The Mac OS X VLAN detect function runs between discovery, causing a delay</p> <p>VLAN detect should refresh the client IP address after a VLAN detect interval (5) X retry detect (3) which is ~ 30 sec, however it is taking an additional 30 sec.</p> <p>This issue has been observed in both a wired and wireless deployment where the Cisco NAC agent changes the client IP address in compliant or non-compliant state since Mac OS X supplicant cannot.</p> <p>An example scenario involves the user getting a “non-compliant” posture state where the Cisco ISE authorization profile is set to Radius Reauthentication (default) and session timer of 10 min (600 sec). After 10 min the session terminates and a new session is created in the pre-posture VLAN. The result is that the client machine still has post-posture VLAN IP assignment and requires VLAN detect to move user back to the pre-posture IP address.</p> <p>Workaround Disconnect and then reconnect the client machine to the network.</p>
CSCtq02332	<p>Windows agent does not display IP refresh during non-compliant posture status</p> <p>The IP refresh is happening on the client machine as designed, but the Agent interface does not display the change appropriately (for example, following a move from preposture (non-compliant) to postposture (compliant) status).</p> <p>Workaround There is no known workaround for this issue.</p>
CSCtq02533	<p>The Cisco NAC Agent takes too long to complete IP refresh following VLAN change</p> <p>The Cisco NAC agent is taking longer than normal to refresh IP address due to double IP refresh by supplicant and Cisco NAC agent.</p> <p>Workaround Disable the Cisco NAC Agent IP address change function if there is a supplicant present capable of doing the same task.</p>
CSCtq15958	<p>Windows Agent VPN tunnel dropping after initial connection</p> <p>Workaround The user needs to reestablish the VPN tunnel.</p>

Table 6 Cisco ISE Release 1.0 Agent Open Caveats (continued)

Caveat	Description
CSCqt16716	<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 43.</p>

Known Issues

- [Windows Internet Explorer 8 Known Issues](#), page 42
 - [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 43
- [Known Incompatibility Issue with WLC Firmware Version 7.0.116.0](#), page 43
- [Issues With 2k Message Size in Monitoring and Troubleshooting](#), page 44
- [Issues With More Than Three Users Accessing Monitoring and Troubleshooting Concurrently](#), page 44
- [Inline Posture Restrictions](#), page 44
- [Cisco IP phones using EAP-FAST](#), page 44

Windows Internet Explorer 8 Known Issues

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

Issue Accessing the Cisco ISE Administrator User Interface

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

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

For more information see [CSCto09989](#).

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

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

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

For more information, see the [Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0](#).

User Identity Groups User Interface Issue With IE 8

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

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

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



Note

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

For more information, see [CSCtq16716](#).

Known Incompatibility Issue with WLC Firmware Version 7.0.116.0

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

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

For more information see [CSCto83897](#).

Issues With 2k Message Size in Monitoring and Troubleshooting

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

Issues With More Than Three Users Accessing Monitoring and Troubleshooting Concurrently

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

Inline Posture Restrictions

- Inline Posture is not supported in a virtual environment, such as VMware.
- Backup and restore is not available for Inline Posture nodes in Cisco ISE, Release 1.0.
- The Simple Network Management Protocol (SNMP) Agent is not supported by Inline Posture.
- The Cisco Discovery Protocol (CDP) is not supported by Inline Posture.

Cisco IP phones using EAP-FAST

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

Documentation Updates

Table 7 Updates to Release Notes for Cisco Identity Services Engine, Release 1.0

Date	Description
June 7, 2011	Added Cisco ISE Install Files, Updates, and Client Resources, page 17 Updated Cisco ISE Antivirus and Antispyware Support, page 19
May 24, 2011	Added caveat CSCtj81255 to Cisco ISE Release 1.0 Agent Open Caveats, page 38
May 19, 2011	Added caveats CSCtk34851, CSCto19507, CSCto34354, and CSCtq02332 to Cisco ISE Release 1.0 Agent Open Caveats, page 38
May 17, 2011	Cisco Identity Services Engine, Release 1.0

Related Documentation

Release-Specific Documents

Table 8 lists the product documentation available for the Cisco ISE Release. 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 8 *Product Documentation for Cisco Identity Services Engine*

Document Title	Location
<i>Release Notes for the Cisco Identity Services Engine, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/release_notes/ise10_rn.html
<i>Cisco Identity Services Engine Network Component Compatibility</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/compatibility/ise-sdt.html
<i>Cisco Identity Services Engine User Guide, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_user_guide.html
<i>Cisco Identity Services Engine Hardware Installation Guide, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/install_guide/ise10_ig.html
<i>Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/migration_guide/ise10_mig_book.html
<i>Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/sponsor_guide/ise10_sponsor_book.html
<i>Cisco Identity Services Engine CLI Reference Guide, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/cli_ref_guide/ise10_cli.html
<i>Cisco Identity Services Engine API Reference Guide, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide.html
<i>Cisco Identity Services Engine Troubleshooting Guide, Release 1.0</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/troubleshooting_guide/ise10_tsg.html
<i>Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler</i>	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/regulatory/compliance/csacsrCSI.html
<i>Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card</i>	http://www.cisco.com/en/US/docs/security/ise/1.0/roadmap/ise10_5x5Card_ChinaRoHS.html

Platform-Specific Documents

Links to Policy Management Business Unit documentation are available on www.cisco.com 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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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

© 2011 Cisco Systems, Inc. All rights reserved.