Release Notes for Cisco Identity Services Engine, Release 2.0

Revised: May 14, 2020

Contents

These release notes describe the features, limitations and restrictions (caveats), and related information for Cisco Identity Services Engine (ISE), Release 2.0. These release notes supplement the Cisco ISE documentation that is included with the product hardware and software release, and cover the following topics:

Cisco Systems, Inc.
www.cisco.com

Introduction

The Cisco ISE platform is a comprehensive, next-generation, contextually-based access control solution. It offers authenticated network access, profiling, posture, BYOD device onboarding (native supplicant and certificate provisioning), guest management, and security group access services along with monitoring, reporting, and troubleshooting capabilities on a single physical or virtual appliance. Cisco ISE is available on two physical appliances with different performance characterization, and also as software that can be run on a VMware server. You can add more appliances to a deployment for performance, scale, and resiliency.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also allows for configuration and management of distinct personas and services. This feature gives you the ability to create and apply services where they are needed in the network, but still operate the Cisco ISE deployment as a complete and coordinated system.

New Features in Cisco ISE, Release 2.0

Cisco ISE, Release 2.0 offers the following features and services. Refer to *Cisco Identity Services Engine Admin Guide, Release 2.0* for more information.

TACACS+ Device Administration

Note Cisco ISE requires a Device Administration license to use the TACACS+ service. The Device Administration license is a perpetual license. If you are upgrading from an earlier release to Cisco ISE, Release 2.0 and would like to enable the TACACS+ service, you must order the Device Administration license as a separate add-on license. You need one Device Administration license for the entire ISE deployment.

Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices. The network devices are configured to query ISE for authentication and authorization of device administrator actions, and send accounting messages for ISE to log the actions. It facilitates granular control of who can access which network device and change the associated network settings. An ISE administrator can create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service. The ISE Monitoring node provides enhanced reports related to device administration. The Device Administration Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators.

Third-Party Device Support

Cisco ISE supports some third-party network access devices (NADs) through the use of network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.

Cisco ISE includes predefined profiles for network devices from several vendors. Cisco ISE 2.0 has been tested with the vendor devices listed in Table 1.

Table 1 Vendor Devices Tested With Cisco ISE 2.0

		Supported/Validated Use Cases				
	Vendor	**802.1X / MAB**	**Profiler without CoA**	**Profiler with CoA**	**Posture**	**Guest/ BYOD**
Wireless	Aruba 7000, InstantAP	✓	✓	✓	✓	✓
	Motorola RFS 4000	✓	✓	✓	✓	✓
	HP 830	✓	✓	✓	✓	✓
	Ruckus ZD 1200	✓	✓	✓	—	—

Table 1 Vendor Devices Tested With Cisco ISE 2.0

	Vendor	Supported/Validated Use Cases				
		802.1X / MAB	Profiler without CoA	Profiler with CoA	Posture	Guest/ BYOD
Wired	HP 3800 (ProCurve)	✓	✓	✓	—	—
	Alcatel 6850	✓	✓	—	—	—
	Brocade ICX 6610	✓	✓	✓	—	—
For additional third-party NADs, you must identify the device properties and capabilities and create custom NAD profiles in Cisco ISE.		✓	✓	Requires CoA support	Requires CoA and URL-redirect support	Requires CoA and URL-redirect support

You can create custom NAD profiles for additional third-party network devices that do not have a predefined profile. For flows such as Guest, BYOD, and Posture, the device needs to support RFC 5176, "Change of Authorization" (CoA), and a URL Redirection mechanism capable of redirecting to Cisco ISE portals. Support for these flows depends on the NAD's capabilities. You may need to refer to the device's administration guide for information on many of the attributes required for a network device profile. For information on how to create custom NAD profiles, refer to the *Network Access Device Profiles with Cisco Identity Services Engine* document.

If you have deployed non-Cisco NADs prior to Release 2.0 and created policy rules/RADIUS dictionaries to use them, after upgrade these will continue to work as usual.

For more information on Network Device Profiles and how to create, import, and export them, see "Manage Network Devices" chapter in the *Cisco Identity Services Engine Administration Guide*.

TrustSec Dashboard

The TrustSec dashboard is a centralized monitoring tool for the TrustSec network. The Metrics dashlet displays statistics about the behavior of the TrustSec network. The Active SGT Sessions dashlet displays the SGT sessions that are currently active in the network. The Alarms dashlet displays the alarms related to the TrustSec sessions. The Quick View dashlet displays TrustSec-related information for NADs and SGTs.

Click the TrustSec Sessions link in the Live Log dashlet to view the active TrustSec sessions. You can also view information regarding TrustSec protocol data requests and responses from NADs to Cisco ISE.

TrustSec Matrix Enhancements

Cisco ISE allows you to create, name, and save the custom views. To create custom views, choose **Show > Create Custom View**. You can also update the view criteria or delete unused views.

You can use the following options in the View drop-down list in the Egress Policy page to change the matrix view:

- Condensed with SGACL names—If you select this option, the empty cells are hidden and the SGACL names are displayed in the cells.

- Condensed without SGACL names—The empty cells are hidden and the SGACL names are not displayed in the cells. This view is useful when you want to see more matrix cells and differentiate between the content of the cells using colors, patterns, and icons (cell status).
- Full with SGACL names—If you select this option, the left and upper menus are hidden and the SGACL names are displayed in the cells.
- Full without SGACL names—When this option is selected, the matrix is displayed in full screen mode and the SGACL names are not displayed in the cells.

You can change the appearance settings. The following options are available:

- Custom theme—The default theme (colors with no patterns) is displayed initially. You can set your own colors and patterns.
- Default theme—Predefined list of colors with no patterns (not editable).
- Accessibility theme—Predefined list of colors with patterns (not editable).

To make the matrix more readable, you can apply coloring and patterns to the matrix cells based on the cell contents. The following display types are available:

- Permit IP/Permit IP Log—Configured inside the cell
- Deny IP/Deny IP Log—Configured inside the cell
- SGACLs—For SGACLs configured inside the cell
- Permit IP/Permit IP Log (Inherited)—Taken from the default policy (for non-configured cells)
- Deny IP/Deny IP Log (Inherited)—Taken from the default policy (for non-configured cells)
- SGACLs (Inherited)—Taken from the default policy (for non-configured cells)

The status icons are used to display the status of the cell.

To configure the TrustSec Matrix settings, choose **Work Centers > TrustSec > Settings > TrustSec Matrix Settings**.

TrustSec Work Center

All TrustSec-related options are consolidated under the TrustSec Work Center menu (**Work Centers > TrustSec**), so that the administrator can easily access all the TrustSec options at one location.

Automatic SGT Creation

Cisco ISE allows you to create SGTs automatically while creating the authorization policy rules. The auto created SGTs are named based on the rule attributes.

When this option is enabled, "Auto Security Group Creation is On" message is displayed at the top of the Authorization Policy page. Click the plus (+) sign displayed in the Permissions field to edit the SGT name and value.

By default, this option is disabled after fresh install or upgrade.

Support for SXP

Source Group Tag (SGT) Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one SGT-aware network device to another.

To enable SXP service on a node, check the Enable SXP Service check box in the General Node Settings page. You must also specify the interface to be used for SXP service.

Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.

Location Based Authorization

Cisco ISE integrates with Cisco Mobility Services Engine (MSE) to introduce physical location-based authorization. Cisco ISE uses information from MSE to provide differentiated network access based on the actual location of the user, as reported by MSE.

With this feature, you can use the endpoint location information to provide network access when a user is in an appropriate zone. You can also add the endpoint location as an additional attribute for policies to define more granulated policy authorization sets based on device location. You can configure conditions within authorization rules that use location-based attributes, for example:

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

You can define the location hierarchy (campus/building/floor structure) and configure the secure and non-secure zones using the Cisco Prime Infrastructure application. After defining the location hierarchy, you must synchronize the location hierarchy data with the MSE servers.

The Location Tree is created by using the location data retrieved from the MSE instances. You can select the location entries that are exposed to the authorization policy by using the Location Tree.

Support for Boolean Attributes

Cisco ISE supports retrieving Boolean attributes from Active Directory and LDAP identity stores. You can configure the Boolean attributes while configuring the directory attributes for Active Directory or LDAP. These attributes are retrieved upon authentication with Active Directory or LDAP.

The Boolean attributes can be used for configuring policy rule conditions.

The Boolean attribute values are fetched from Active Directory or LDAP server as String type.

If you configure a Boolean attribute (for example, msTSAllowLogon) as String type, the Boolean value of the attribute in the Active Directory or LDAP server will be set for the String attribute in Cisco ISE. You can change the attribute type to Boolean or add the attribute manually as Boolean type.

Support for EAP-TTLS Protocol

EAP-TTLS is a two-phase protocol that extends the functionality of EAP-TLS protocol. Phase 1 builds the secure tunnel and derives the session keys used in Phase 2 to securely tunnel attributes and inner method data between the server and the client.

Cisco ISE can process authentications from a variety of TTLS supplicants including:

- AnyConnect Network Access Manager (NAM) on Windows
- Windows 8.1 native supplicant
- Secure W2 (also called as JoinNow on MultiOS)
- MAC OS X native supplicant
- IOS native supplicant
- Android based native supplicant
- Linux WPA supplicant

KVM Hypervisor Support

Cisco ISE supports KVM hypervisor on Red Hat Enterprise Linux (RHEL) 7.0.

KVM virtualization requires virtualization support from the host processor; Intel VT-x for Intel processors and AMD-V for AMD processors. Open a terminal window on the host and enter the **cat /proc/cpuinfo** command. You must see either the vmx or the svm flag.

See the *Installing Cisco ISE on a Linux KVM* chapter in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.0* for more information.

Cisco ISE Telemetry

The Cisco ISE Telemetry banner appears as soon as you log in to the Admin portal. Cisco ISE securely collects non-sensitive information about your deployment, network access devices, profiler, and other services that you are using. The data that is collected will be used to provide better services and additional features to you in forthcoming releases.

Cisco securely collects Telemetry information to better understand Cisco ISE usage and to improve the product and the various services that it offers. By default, the telemetry feature is enabled. If you do not want to participate in Cisco ISE Telemetry, you can disable it from the ISE Admin Portal (Administration > System > Settings > Telemetry Settings).

Certificate Provisioning Portal

The Certificate Provisioning portal allows employees to request certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals cannot go through the BYOD flow and need to be issued certificates manually. The Certificate Provisioning portal allows a privileged set of users to upload a certificate request for such devices, generate key pairs (if required), and download the certificate. Employees can access this portal and request for a single certificate or make a bulk certificate request using a CSV file.

Certificate Template Extension

The Cisco ISE Internal CA includes an extension to represent the certificate template that was used to create the endpoint certificate. All endpoint certificates issued by the internal CA contain a certificate template name extension. You can use the CERTIFICATE: Template Name attribute in authorization policy conditions and assign appropriate access privileges based on the results of the evaluation.

Cisco ISE Internal CA Issues Certificates to ASA VPN Users

The internal ISE CA can issue certificates to client machines that connect over ASA VPN. Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines.

GUI-Based Upgrade

Cisco ISE offers a GUI-based centralized upgrade from the Admin portal. The upgrade process is much simplified and the progress of the upgrade and the status of the nodes are displayed on screen.

Note The GUI-based upgrade is applicable only if you are upgrading from Release 2.0 to a higher release.

Technical Support Tunnel for Advanced Troubleshooting

Cisco ISE uses the Cisco IronPort Tunnel infrastructure to create a secure tunnel for Cisco technical support engineers to connect to an ISE server in your deployment and troubleshoot issues with the system. Cisco ISE uses SSH to create the secure connection through the tunnel. As an administrator, you can control the tunnel access; you can choose when and how long to grant access to the support engineer. Cisco Customer Support cannot establish the tunnel without your intervention. You will receive notification about the service logins. You can disable the tunnel connection at any point of time.

Mobile Device Management Enhancements

Cisco ISE 2.0 allows endpoints that were enrolled on an active MDM server outside of an ISE network to connect to an ISE network without needing to re-enroll with the MDM server.

When the endpoint connects to the ISE network, the MDM portal queries the MDM server for the endpoint. If the server returns the endpoint as compliant, ISE issues a change of authorization and allows the endpoint on the network. If the endpoint is not enrolled with the MDM server, it will have to go through the enrollment process.

Support for Meraki Mobile Device Management

Cisco ISE supports Meraki MDM server.

pxGrid Enhancements

ISE 2.0 allows a pxGrid client to create and set up a new capability without needing to update all of the other participants in the grid. Administrators can enable the new capability on the **Administration > pxGrid Services > View by Capabilities** page.

Guest Enhancements

A sponsor can now change the guest type of an existing guest account in the Sponsor portal.

Profiler Enhancements

IPv6 addressing is supported for some features. See IPv6 Support, page 9 for more information.

Posture Enhancements

Cisco ISE supports the following:

- Disk Encryption Check to protect information that goes on to a disk and to prevent unauthorized access to data storage. You can associate a Disk Encryption condition with a posture requirement only when you use the AnyConnect ISE posture agent.
- SHA-256 File Check to provide a more secure way for administrators to check the file integrity.
- Property List File Check for OS X for the administrator to check the value of a specified property in a specified file.
- Daemon Check Enhancement for OS X to allow the administrator to check the running status of the daemon or user agent.
- Additional Variables for File Check to provide variables for user directories so that the administrator can create file check in user directories.

Client Provisioning Enhancements

You can configure multiple WiFi SSIDs (NSP profiles) with a single run of the SPW. The first profile will be the active profile. For Windows and Mac, the proxy settings of the first profile will be applied globally (for all subsequent profiles). The Proxy Auto-Config File URL will be used for automatic configuration of proxy settings, which is supported by iOS, MAC OS, Windows, and Android 5.0 or above. If no Proxy Auto-Config File URL is defined, the proxy host/port will be used for all operating systems. However, the proxy host/port is used for all Android versions before 5.x.

IPv6 Support

Cisco ISE, Release 2.0 supports the following IPv6 capabilities:

- Support for IPv6-enabled Endpoints: Cisco ISE can detect, manage, and secure IPv6 traffic from endpoints. You can configure authorization profiles and policies in Cisco ISE using IPv6 attributes to process requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.
- IPv6 Support in Reports: Reports in Release 2.0 support IPv6 values. The Live Session and Live Authentication pages also support IPv6 values.
- IPv6 Support in CLI: Release 2.0 supports IPv6 in the following CLI commands:
  - ipv6 address—To allow for static IPv6 address configuration per network interface
  - ipv6 enable—To enable or disable IPv6 on all network interfaces
  - ipv6 route—To configure IPv6 static routes

- ip host—To add IPv6 addresses in host local table
- show IPv6 route—To display IPv6 routes

Refer to the *Cisco Identity Services Engine CLI Reference Guide* for more information on these commands.

Cisco ISE License Information

Cisco ISE licensing provides the ability to manage the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources.

Licenses apply to wireless and VPN only, or Wired only for LAN deployments. It is supplied in different packages as Base, Plus, Plus AC, Apex, Apex AC, Device Administration, Mobility, and Mobility Upgrade.

All Cisco ISE appliances are supplied with a 90-day Evaluation license. To continue to use Cisco ISE services after the 90-day Evaluation license expires, and to support more than 100 concurrent endpoints on the network, you must obtain and register Base licenses for the number of concurrent users on your system. If you require additional functionality, you will need Plus and/or Apex licenses to enable that functionality.

Note Cisco ISE requires a Device Administration license to use the TACACS+ feature. See the TACACS+ Device Administration, page 3 feature description for more information.

Cisco ISE, Release 2.0, supports licenses with two UIDs. You can obtain a license based on the UIDs of both the primary and secondary Administration nodes.

For more detailed information on license types and obtaining licenses for Cisco ISE, see the "Cisco ISE Licenses" chapter in the *Cisco Identity Services Engine Administration Guide, Release 2.0*.

For more information on Cisco ISE, Release 2.0 licenses, see the *Cisco Identity Services Engine (ISE) Data Sheet*.

Deployment Terminology, Node Types, and Personas

Cisco ISE provides a scalable architecture that supports both standalone and distributed deployments.

Table 2 Cisco ISE Deployment Terminology

Term	Description
Service	Specific feature that a persona provides such as network access, profiler, posture, security group access, and monitoring.
Node	Individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as software that can be run on a VMware server. Each instance (either running on a Cisco ISE appliance or on a VMware server) that runs the Cisco ISE software is called a node.

Table 2 Cisco ISE Deployment Terminology (continued)

Term	Description
Persona	Determines the services provided by a node. A Cisco ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring.
Deployment Model	Determines if your deployment is a standalone, high availability in standalone (a basic two-node deployment), or distributed deployment.

Types of Nodes and Personas

A Cisco ISE network has the following types of nodes:

- Cisco ISE node, which can assume any of the following personas:
  - Administration—Allows you to perform all administrative operations for Cisco ISE. It handles all system-related configurations related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have one or a maximum of two nodes running the Administration persona and configured as a primary and secondary pair. If the Primary Administration Node goes down, you can manually promote the Secondary Administration Node or configure automatic failover for administration persona.

    For more information on configuring automatic failover, see the "Configure Primary Administration Node for Automatic Failover" section in the *Cisco Identity Services Engine Administration Guide, Release 2.0*.
  - Policy Service—Provides network access, posturing, BYOD device onboarding (native supplicant and certificate provisioning), guest access, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assuming this persona. Typically, there is more than one Policy Service persona in a distributed deployment. All Policy Service personas that reside behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes in that group process the requests of the node that has failed, thereby providing high availability.

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

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

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

Note At least one node in your distributed setup should assume the Monitoring persona. It is recommended that the Monitoring persona be on a separate, designated node for higher performance in terms of data collection and reporting.

– pxGrid—Cisco pxGrid is a method for network and security devices to share data with other devices through a secure publish and subscribe mechanism. These services are applicable for applications that are used external to ISE and that interface with pxGrid. The pxGrid services can share contextual information across the network to identify the policies and to share common policy objects. This extends the policy management.

Table 3 Recommended Number of Nodes and Personas in a Distributed Deployment

Node / Persona	Minimum Number in a Deployment	Maximum Number in a Deployment
Administration	1	2 (Configured as a high-availability pair)
Monitor	1	2 (Configured as a high-availability pair)
Policy Service	1	• 2—when the Administration/Monitoring/Policy Service personas are on the same primary/secondary appliances • 5—when Administration and Monitoring personas are on same appliance • 40—when each persona is on a dedicated appliance
pxGrid	0	2 (Configured as a high-availability pair)

You can change the persona of a node. See the "Set Up Cisco ISE in a Distributed Environment" chapter in the *Cisco Identity Services Engine Admin Guide, Release 2.0* for information on how to configure personas on Cisco ISE nodes.

System Requirements

Note For more details on Cisco ISE hardware platforms and installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.0.*

Supported Hardware

Cisco ISE software is packaged with your appliance or image for installation. Cisco ISE, Release 2.0 is shipped on the following platforms. After installation, you can configure Cisco ISE with specified component personas (Administration, Policy Service, Monitoring, and pxGrid) on the platforms that are listed in Table 4.

Table 4 Supported Hardware and Personas

Hardware Platform	Persona	Configuration
Cisco SNS-3415-K9 (small)	Any	See the Cisco Identity Services Engine (ISE) Data Sheet for the appliance hardware specifications (Table 3).
Cisco SNS-3495-K9 (large)		
Cisco ISE-VM-K9 (VMware, Linux KVM)		• For CPU and memory recommendations, refer to the "VMware Appliance Sizing Recommendations" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.0*.[1] • For hard disk size recommendations, refer to the "Disk Space Requirements" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.0*. • NIC—1 GB NIC interface required. You can install up to 4 NICs. • Supported virtual machine versions include: – ESXi 5.*x, 6.x* – KVM on RHEL 7.0

1. Memory allocation of less than 8 GB is not supported for any VM appliance configuration. In the event of a Cisco ISE behavior issue, all users will be required to change allocated memory to at least 8 GB prior to opening a case with the Cisco Technical Assistance Center.

Note Legacy ACS and NAC appliances (including the Cisco ISE 3300 series) are not supported with Cisco ISE, Release 2.0.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- VMware ESXi 5.*x, 6.x*
- KVM on RHEL 7.0

Supported Browsers

- Mozilla Firefox 69 and earlier versions

- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 77 and earlier versions
- Microsoft Internet Explorer 10.x and 11.x
  - If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).
  - If you use Chrome 65.0.3325.189, you may be unable to view guest account details in the print preview section.
  - You might see a warning message while downloading an executable (EXE) file in Google Chrome 76 or later. To resolve this issue:

a. In your browser, click the **Settings** menu at the top-right corner.

b. At the bottom of the **Settings** window, click **Advanced**.

c. Under **Downloads**, check the **Ask Where to Save Each File before Downloading** check box.

Note Adobe Flash Player 11.1.0.0 or above must be installed on the system running your client browser. The minimum required screen resolution to view the Cisco ISE Admin portal and for a better user experience is 1280 x 800 pixels.

Supported Cipher Suites

Cisco ISE, Release 2.0 supports the following FIPS-compliant ciphers. TLS versions 1.0, 1.1, and 1.2 are supported.

- For EAP-TLS, PEAP, EAP-FAST, EAP-TTLS:
  - DHE_RSA_WITH_AES_256_SHA256
  - DHE_RSA_WITH_AES_128_SHA256
  - RSA_WITH_AES_256_SHA256
  - RSA_WITH_AES_128_SHA256
  - DHE_RSA_WITH_AES_256_SHA
  - DHE_RSA_WITH_AES_128_SHA
  - RSA_WITH_AES_256_SHA
  - RSA_WITH_AES_128_SHA
- For EAP-FAST Anonymous Provisioning:
  - ADH_WITH_AES_128_SHA

Cisco ISE, Release 2.0 does not support non-FIPS compliant ciphers. The following ciphers are not supported:

- RSA_DES_192_CBC3_SHA
- EDH_RSA_DES_192_CBC3_SHA
- EDH_DSS_DES_192_CBC3_SHA
- RSA_RC4_128_SHA
- RSA_RC4_128_MD5
- EDH_RSA_DES_64_CBC_SHA

- EDH_DSS_DES_64_CBC_SHA
- RSA_RC4_128_SHA

Note If you have legacy devices that use these deprecated ciphers, contact the Cisco Technical Assistance Center for support.

Supported Devices and Agents

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

Cisco ISE, Release 2.0.1 supports AnyConnect version 4.2.x and earlier. You can download the offline files listed under Release 2.0 from the Software Download Center.

Cisco NAC Agent Interoperability

The Cisco NAC Agent version 4.9.5.8 is a common agent for Cisco NAC Appliance Releases 4.9(1), 4.9(3), 4.9(4), 4.9(5), and Cisco ISE Releases 1.1.3-patch 11, 1.1.4-patch 11, 1.2.0, 1.2.1, 1.3, 1.4, and 2.0.

This is the recommended model of deploying the NAC agent in an environment where users will be roaming between ISE and NAC deployments.

Support for Microsoft Active Directory

Cisco ISE, Release 2.0 works with Microsoft Active Directory servers 2003, 2008, 2008 R2, 2012, and 2012 R2 at all functional levels.

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

Cisco ISE 2.0 supports Multi-Forest/Multi-Domain integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 2.0 supports up to 50 domain join points.

Supported Antivirus and Antispyware Products

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

http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html

Cisco NAC Web Agents have static compliance modules which cannot be upgraded without upgrading the Web Agent.

The following table lists the Web Agent versions and the compatible Compliance Module versions.

Table 5 Web Agent and Compliance Module Versions

Cisco NAC Web Agent version	Compliance Module Version
4.9.5.3	3.6.9845.2
4.9.5.2	3.6.9186.2
4.9.4.3	3.6.8194.2
4.9.0.1007	3.5.5980.2
4.9.0.1005	3.5.5980.2

Installing Cisco ISE Software

To install Cisco ISE, Release 2.0 software on Cisco SNS-3415 and SNS-3495 hardware platforms, turn on the new appliance and configure the Cisco Integrated Management Controller (CIMC). You can then install Cisco ISE, Release 2.0 over a network using CIMC or a bootable USB.

Note When using virtual machines (VMs), we recommend that the guest VM have the correct time set using an NTP server *before* installing the .ISO image or OVA file on the VMs.

Perform Cisco ISE initial configuration according to the instructions in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.0*. Before you run the setup program, ensure that you know the configuration parameters listed in Table 6.

Table 6 Cisco ISE Network Setup Configuration Parameters

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). The first character must be a letter.	isebeta1
(eth0) Ethernet interface address	Must be a valid IPv4 address for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14
Netmask	Must be a valid IPv4 netmask.	255.255.255.0
Default gateway	Must be a valid IPv4 address for the default gateway.	10.12.13.1
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).	mycompany.com
Primary name server	Must be a valid IPv4 address for the primary name server.	10.15.20.25
Add/Edit another name server	(Optional) Allows you to configure multiple name servers. Must be a valid IPv4 address for an additional name server.	Enter **y** to add additional name server or **n** to configure the next parameter.
Primary NTP server	Must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server.	clock.nist.gov

Table 6 Cisco ISE Network Setup Configuration Parameters (continued)

Prompt	Description	Example
Add/Edit another NTP server	(Optional) Allows you to configure multiple NTP servers. Must be a valid IPv4 address or hostname.	Enter **y** to add additional NTP server or **n** to configure the next parameter.
System Time Zone	Must be a valid time zone. For details, see *Cisco Identity Services CLI Reference Guide, Release 2.0*, which provides a list of time zones that Cisco ISE supports. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT (or UTC-8 hours). The time zones referenced are the most frequently used time zones. You can run the **show timezones** command from the Cisco ISE CLI for a complete list of supported time zones. **Note** We recommend that you set all Cisco ISE nodes to the UTC time zone. This setting ensures that the reports, logs, and posture agent log files from the various nodes in the deployment are always synchronized with the time stamps.	UTC (default)
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (admin), you must create a new username. The username must be three to eight characters in length and composed of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password (there is no default). The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Note For additional information on configuring and managing Cisco ISE, see Release-Specific Document, page 47 to access other documents in the Cisco ISE documentation suite.

Upgrading Cisco ISE Software

You can directly upgrade to Cisco ISE, Release 2.0, from any of the following releases:

- Cisco ISE, Release 1.3
- Cisco ISE, Release 1.4

If you are on a version earlier than Cisco ISE, Release 1.3, you must first upgrade to one of the releases listed above and then upgrade to Release 2.0.

Note If you have installed a hot patch, roll back the hot patch before applying an upgrade patch.

Follow the upgrade instructions in the *Cisco Identity Services Engine Upgrade Guide, Release 2.0* to upgrade to Cisco ISE, Release 2.0.

Note When you upgrade to Cisco ISE, Release 2.0, you may be required to open network ports that were not used in previous releases of Cisco ISE. For more information, see *Cisco ISE Ports Reference* in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.0*.

Upgrade Considerations and Requirements

Read the following sections before you upgrade to Cisco ISE, Release 2.0:

Firewall Ports That Must be Open for Communication

The replication ports have changed in Cisco ISE, Release 2.0. If you have deployed a firewall between the primary Administration node and any other node, the following ports must be open before you upgrade to Release 2.0:

- TCP 1521—For communication between the primary administration node and monitoring nodes.
- TCP 443—For communication between the primary administration node and all other secondary nodes.
- TCP 12001—For global cluster replication.
- TCP 7800 and 7802—(Applicable only if the policy service nodes are part of a node group) For PSN group clustering.

For a full list of ports that Cisco ISE, Release 2.0 uses, refer to *Cisco ISE Ports Reference* in the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.0*.

Admin User Unable to Access the ISE Login Page Post Upgrade

If you had enabled certificate-based authentication for administrative access to Cisco ISE (Administration > Admin Access) before upgrade and used Active Directory as your identity source, after upgrade, you will not be able to launch the ISE Login page because Active Directory join is lost during upgrade.

Workaround

From the Cisco ISE CLI, start the ISE application in safe mode using the following command:

application start ise safe

This command brings up the Cisco ISE node in safe mode and you can use the internal admin user credentials to log in to the ISE GUI.

After you log in, you can join ISE with Active Directory.

Rejoin Cisco ISE with Active Directory

Ensure that you have the Active Directory credentials if you are using Active Directory as your external identity source. After an upgrade, you might lose Active Directory connections. If this happens, you must rejoin Cisco ISE with Active Directory. After rejoining, perform the external identity source call flows to ensure the connection.

Sponsor Login Fails

The upgrade process does not migrate all sponsor groups. Sponsor groups that are not used in the creation of guests roles are not migrated. As a result of this change, some sponsors (internal database or Active Directory users) may not be able to log in after upgrade to Release 2.0.

Check the sponsor group mapping for sponsors who are not able to log in to the sponsor portal, and map them to the appropriate sponsor group.

Update Authorization Policies for New Guest Types

After upgrading to Cisco ISE 2.0, the new guest types that are created do not match the upgraded authorization policies. You need to make sure that the authorization policies are updated with the new guest types.

Other Known Upgrade Considerations and Issues

Refer to the *Cisco Identity Services Engine Upgrade Guide, Release 2.0* for other known upgrade considerations and issues.

Cisco Secure ACS to Cisco ISE Migration

You can directly migrate to Cisco ISE, Release 2.0 only from Cisco Secure ACS, Releases 5.5 and 5.6. For information about migrating from Cisco Secure ACS, Releases 5.5 and 5.6 to Cisco ISE, Release 2.0, see the *Cisco Identity Services Engine Migration Tool Guide*.

You cannot migrate to Release 2.0 from Cisco Secure ACS 5.1, 5.2, 5.3, 5.4, 4.x, or earlier versions, or from Cisco Network Admission Control (NAC) Appliance. From Cisco Secure ACS, Releases 4.x, 5.1, 5.2, 5.3, or 5.4, you must upgrade to ACS, Release 5.5 or 5.6, and then migrate to Cisco ISE, Release 2.0.

Requirements for CA to Interoperate with Cisco ISE

While using a CA server with Cisco ISE, make sure that the following requirements are met:

- Key size should be 1024, 2048, or higher. In CA server, the key size is defined using certificate template. You can define the key size on Cisco ISE using the supplicant profile.
- Key usage should allow signing and encryption in extension.
- While using GetCACapabilities through the SCEP protocol, cryptography algorithm and request hash should be supported. It is recommended to use RSA + SHA1.
- Online Certificate Status Protocol (OCSP) is supported. This is not directly used in BYOD, but a CA which can act as an OCSP server can be used for certificate revocation.

Known Limitations in Cisco ISE, Release 2.0

This section lists known limitations in Release 2.0:

SXP Protocol Security Standards

SXP protocol transfers unencrypted data and uses weak hash algorithm for message integrity checking per draft-smith-kandula-sxp-06.

High Memory Utilization

Cisco ISE Version 1.3 and later use RHEL, version 6. You may experience high memory utilization after installing or upgrading to Cisco ISE Version 1.3 or later. However, this does not negatively impact Cisco ISE performance and there are no alarms that are triggered. In case, if the memory usage is consistently above 90% or if there is any performance impact, you can contact Cisco TAC for troubleshooting.

Do Not Delete the Default Internal Cisco ISE CA Templates

The internal Cisco ISE CA comes with two default certificate templates:

- CA_SERVICE_Certificate_Template—Cisco ISE uses this template to issue certificates when other network services use Cisco ISE as the CA. For example, for client machines that connect over ASA VPN.
- EAP_Authentication_Certificate_Template—Cisco ISE issues certificates for EAP authentication based on this template.

Do not delete these default certificate templates. If you want to customize the certificate template, you can create a new one, or copy an existing template and edit it.

Do not Install a Patch Until Upgrade

When upgrade is in progress, do not install a patch on any node in the deployment simultaneously. Patch installation should be done after deployment upgrade is complete.

LDAP Imported Guest Accounts Not Upgraded from Version 1.2

Guests that were imported by an LDAP authenticated sponsor in version 1.2 will not be migrated during an upgrade to 1.3, 1.4, 2.0, or 2.1.

LDAP Sponsor Created Guest Users Not Visible when Upgraded from 1.2

When upgrading from 1.2 to 1.3, 1.4, 2.0, or 2.1, guests who were created by a sponsor who was authenticated through LDAP can only be seen by the direct sponsor. These guests cannot be seen by other sponsors from the same sponsor group.

TLS Authentication on Android Devices Does Not Use Certificates Issued by the Assigned Certificate Authority

This issue occurs when you have configured:

- Internal and external Certificate Authority (CA) in Cisco ISE.
- Two profiles (SSID1 and SSID2) for TLS authentication using the internal and external CA, respectively.

The certificates provisioned from Cisco ISE are imported in to the Android certificate store. Sometimes, the wireless networks use one of the many certificates when connecting to the network. For example, when an Android device connects to the network using SSID 1, the certificate used for authentication is issued by the internal CA. When a second Android device connects using SSID 2, the certificate used for authentication is again issued by the internal CA instead of the external CA (as configured in SSID2).

This issue is seen only in Android devices and there is no workaround.

Cisco recommends that you update your Android device with all fixes and upgrades offered by the vendor.

EKU Validation: OCSP Signing Certificate Returns Unknown for Root CA

The Bouncy Castle OCSP signing certificate returns an "unknown" response for the Root CA. If you have configured Cisco ISE to reject requests when an unknown certificate status is returned by the OCSP service, Cisco ISE rejects the certificate that is being evaluated and the user authentication fails.

This issue is seen in Bouncy Castle, version 1.6.145-generated certificates. There is no workaround.

Backup and Restore Page Takes a Long Time to Load

This issue occurs if the “Admin” certificate is configured with CRL check and the CRL server URL is not reachable from Cisco ISE.

As a workaround, you can do one of the following:

- Ensure that the CRL server is reachable from Cisco ISE.
- Generate a new “Admin” certificate without CRL check.
- Generate a self-signed certificate for Admin usage.

EST Service Does Not Run in Cisco ISE 2.1

After a fresh installation of Cisco ISE 2.1, when you run the **show application status ise** command, the EST service might be shown as disabled. This issue occurs when the root certificate of the Cisco ISE internal CA is signed by an external CA and the external CA certificate is not present in your Trusted Certificates store. Import the external CA certificate in to the Trusted Certificates store to bring up the EST service.

This issue is also seen after upgrade to Release 2.1, if the entire certificate chain of the internal ISE CA is not present. You must generate the Cisco ISE CA chain to bring up the EST service.

Features Not Supported in Cisco ISE, Release 2.0

This section lists the features not supported in Release 2.0:

- Inline Posture Node (IPN / iPEP), page 22

Inline Posture Node (IPN / iPEP)

IPN / iPEP configuration is no longer supported with Cisco ISE, Release 2.0.

Cisco ISE Installation Files, Updates, and Client Resources

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

- Cisco ISE Downloads from the Download Software Center, page 22
- Cisco ISE Live Updates, page 23
- Cisco ISE Offline Updates, page 24

Cisco ISE Downloads from the Download Software Center

In addition to the .ISO installation package required to perform a fresh installation of Cisco ISE as described in Installing Cisco ISE Software, page 16, you can use the Download software web page to retrieve other Cisco ISE software elements, like Windows and Mac OS X agent installers and AV/AS compliance modules.

Downloaded agent files may be used for manual installation on a supported endpoint or used with third-party software distribution packages for mass deployment.

To access the Cisco Download Software center and download the necessary software:

Step 1 Go to the Download Software web page at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm. You may need to provide login credentials.

Step 2 Navigate to **Products > Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

Choose from the following Cisco ISE installers and software packages available for download:

- Cisco ISE installer.ISO image
- Supplicant Provisioning Wizards for Windows and Mac OS X Native Supplicants
- Windows client machine agent installation files (including MST and MSI versions for manual provisioning)
- Mac OS X client machine agent installation files
- AnyConnect agent installation files
- AV/AS compliance modules

Step 3 Click **Download** or **Add to Cart**.

Cisco ISE Live Updates

Cisco ISE Live Update locations allow you to automatically download Supplicant Provisioning Wizard, Cisco NAC Agent for Windows and Mac OS X, AV/AS support (Compliance Module), and agent installer packages that support client provisioning and posture policy services. These live update portals should be configured in Cisco ISE upon initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the Cisco ISE appliance.

Prerequisite:

If the default Update Feed URL is not reachable and your network requires a proxy server, you may need to configure the proxy settings in **Administration > System > Settings > Proxy** before you are able to access the Live Update locations. If proxy settings are enabled to allow access to the profiler and posture/client provisioning feeds, then it will break access to the MDM server as Cisco ISE cannot bypass proxy services for MDM communication. To resolve this, you can configure the proxy service to allow communication to the MDM servers. For more information on proxy settings, see the "Specify Proxy Settings in Cisco ISE" section in the "Administer Cisco ISE" chapter of the *Cisco Identity Services Engine Admin Guide, Release 2.0*.

Client Provisioning and Posture Live Update portals:

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

  The following software elements are available at this URL:

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

  For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Client Provisioning Resources Automatically" section of the "Configure Client Provisioning" chapter in the *Cisco Identity Services Engine Admin Guide, Release 2.0*.

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

  The following software elements are available at this URL:

  - Cisco predefined checks and rules

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

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically" section of the "Configure Client Posture Policies" chapter in the *Cisco Identity Services Engine Admin Guide, Release 2.0*.

If you do not enable the automatic download capabilities described above, you can choose to download updates offline. See Cisco ISE Offline Updates, page 24.

Cisco ISE Offline Updates

Cisco ISE offline updates allow you to manually download Supplicant Provisioning Wizard, agent, AV/AS support, compliance modules, and agent installer packages that support client provisioning and posture policy services. This option allows you to upload client provisioning and posture updates when direct Internet access to Cisco.com from a Cisco ISE appliance is not available or not permitted by a security policy.

Offline updates are not available for Profiler Feed Service.

To upload offline client provisioning resources:

Step 1 Go to the Download Software web page at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm. You may need to provide login credentials.

Step 2 Navigate to **Products > Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

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

- **win_spw-**<*version*>**-isebundle.zip**— Off-Line SPW Installation Package for Windows
- **mac-spw-**<*version*>**.zip** — Off-Line SPW Installation Package for Mac OS X
- **compliancemodule-**<*version*>**-isebundle.zip** — Off-Line Compliance Module Installation Package
- **macagent-**<*version*>**-isebundle.zip** — Off-Line Mac Agent Installation Package
- **nacagent-**<*version*>**-isebundle.zip** — Off-Line NAC Agent Installation Package
- **webagent-**<*version*>**-isebundle.zip** — Off-Line Web Agent Installation Package

Step 3 Click **Download** or **Add to Cart**.

For more information on adding the downloaded installation packages to Cisco ISE, refer to the "Add Client Provisioning Resources from a Local Machine" section of the "Configure Client Provisioning" chapter in the *Cisco Identity Services Engine Admin Guide, Release 2.0*.

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

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

To upload offline posture updates:

Step 1 Go to https://www.cisco.com/web/secure/pmbu/posture-offline.html.

Save the **posture-offline.zip** file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Macintosh operating systems.

Step 2 Access the Cisco ISE administrator user interface and choose **Administration > System > Settings > Posture**.

Step 3 Click the arrow to view the settings for posture.

Step 4 Choose **Updates**. The Posture Updates page appears.

Step 5 From the Posture Updates page, choose the **Offline** option.

Step 6 From the File to Update field, click **Browse** to locate the single archive file (posture-offline.zip) from the local folder on your system.

Note The File to Update field is a required field. You can select only a single archive file (.zip) that contains the appropriate files. Archive files other than .zip (like .tar, and .gz) are not allowed.

Step 7 Click the **Update Now** button.

Once updated, the Posture Updates page displays the current Cisco updates version information under Update Information.

Using the Bug Search Tool

This section explains how to use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

- Search Bugs Using the Bug Search Tool
- Export to Spreadsheet

Search Bugs Using the Bug Search Tool

In Cisco ISE, use the Bug Search Tool to view the list of outstanding and resolved bugs in a release. This section explains how to use the Bug Search Tool to search for a specific bug or to search for all the bugs in a specified release.

Step 1 Go to https://tools.cisco.com/bugsearch/search.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Toolkit page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Enter.

Step 4 To search for bugs in the current release:

a. Click Select from list link. The Select Product page is displayed.

b. Choose Security > Access Control and Policy > Cisco Identity Services Engine.

c. Click OK.

d. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs based on different criteria such as status, severity, and modified date.

Export to Spreadsheet

The Bug Search Tool provides the following option to export bugs to an Excel spreadsheet:

- Click **Export Results to Excel** link in the Search Results page under the Search Bugs tab to export all the bug details from your search to an Excel spreadsheet. Presently, up to 10,000 bugs can be exported at a time to the Excel spreadsheet.

If you are unable to export the spreadsheet, log in to the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1-800-553-2447).

Cisco ISE, Release 2.0.0.306 Patch Updates

The following sections provide information on patches that were made available after the initial availability of the ISE 2.0 release. Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions. Cisco ISE version 2.0.0.306 was the initial version of the Cisco ISE 2.0 release. After installation of the patch, the version information can be seen from the **Settings > About Identity Services Engine** page in the Cisco ISE GUI and from the CLI in the following format “2.0.0.306 patch N”; where N is the patch number.

Within the bug database, issues resolved in a patch have a version number with different nomenclature in the format, “2.0(0.9NN)” where NN is also the patch number; however displayed as two digits. For example, version “2.0.0.306 patch 3" corresponds to the following version in the bug database “2.0(0.903)”.

Note When you install a patch on Release 2.0, the patch installation process does not prompt you to verify the hash value of the software. Beginning from Release 2.0 onwards, the patch installation software automatically verifies the integrity of the patch software using digital signatures.

Note We recommend you to clear your browser cache after you install a patch on Cisco ISE, Release 2.0.

The following patch releases apply to Cisco ISE release 2.0:

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 8

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the **Cisco Download Software site** with your Cisco.com login credentials, navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 8 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.1.0.40 or later and Windows users must upgrade their SPW to WinSPWizard 2.1.0.51 or later.

See the "Installing a Software Patch" section in the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0* for instructions on how to apply the patch to your system.

Table 7 Cisco ISE Patch Version 2.0.0.306—Patch 8 Resolved Caveats

Caveat ID Number	Description
CSCvd24296	ISE: Revise platform selection rules for ISE installed on VMs
CSCvk57734	Doc: ISE 2.0.1 || Accept-Search-Result is required while making the search request
CSCvm03681	EAP-FAST doesn't support correct key generation in TLS 1.2
CSCvm03842	PxGrid SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection - CVE-2009-3555
CSCvm14030	Evaluation of positron for Struts remote code execution vulnerability August 2018
CSCvn17524	ISE Apache Struts CVE-2016-1000031 Vulnerability

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 7

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the **Cisco Download Software site** with your Cisco.com login credentials, navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 7 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.1.0.40 or later and Windows users must upgrade their SPW to WinSPWizard 2.1.0.51 or later.

See the "Installing a Software Patch" section in the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0* for instructions on how to apply the patch to your system.

Table 8 Cisco ISE Patch Version 2.0.0.306—Patch 7 Resolved Caveats

Caveat	Description
CSCve31857	Cisco Identity Services Engine EAP-TLS Certificate Denial of Service Vulnerability. For more information about this bug, see *Cisco Security Advisory*.

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 6

The following table lists the issues that are resolved in Cisco Identity Services Engine, Release 2.0.0.306 cumulative patch 6.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 6 might not work with older versions of SPW. MAC users need to upgrade their SPW to MACOSXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0*. for instructions on how to apply the patch to your system.

Table 9 Cisco ISE Patch Version 2.0.0.306—Patch 6 Resolved Caveats

Caveat	Description
CSCvc09462	Deleting endpoints via ERS API is slow after upgrade from ISE 1.3 to 2.1.
CSCvc51725	ISE 2.0 and 2.1, update the compliant status as per the MDM server.
CSCvc87853	SNMP process stops and restarts by itself after continuous snmpwalk queries.
CSCvd21954	TACACS+ authentication requests fail due to memory leak.
CSCvd74794	Fix for Cisco ISE Cross-Site Scripting Vulnerability in the Guest portal.
CSCve55046	Endpoint purge fails for sub-groups created under the default endpoint identity group for the guest flow.
CSCve74916	Fix for Cisco Identity Service Engine Privilege Escalation Vulnerability.
CSCve79008	Subdomain email addresses cannot be used for email notifications in the guest flow.

Table 9 Cisco ISE Patch Version 2.0.0.306—Patch 6 Resolved Caveats (continued)

Caveat	Description
CSCvf31398	TACACS+ allows all users with valid credentials to log into the Cisco Nexus switches.
CSCvf58889	An error is reported for invalid passwords entered in a password change request during MSCHAPv2 authentication. **Workaround** Reauthenticate for a new password change prompt.

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 5

The following table lists the issues that are resolved in Cisco Identity Services Engine, Release 2.0.0.306 cumulative patch 5.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 5 might not work with older versions of SPW. MAC users need to upgrade their SPW to MACOSXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0*. for instructions on how to apply the patch to your system.

Table 10 Cisco ISE Patch Version 2.0.0.306—Patch 5 Resolved Caveats

Caveat	Description
CSCur60613	PSN occasionally reloads due to race condition in handling authentications.
CSCuy72189	Apple iphone is profiled as unknown.
CSCuy98580	AD connector reloads when changing the DNS while AD is joined.
CSCuz17763	When client switches from SSID with 802.1x based authentication to SSID with guest based authentication, concurrent sessions are dropped.
CSCuz66826	While upgrading to ISE 2.0, ISE throws openssl alert 'Bad Record Mac' error during tunnel establishment.
CSCva95303	In ISE 2.0 Catalina.out.<date> and catalina.<date>.log take huge space.
CSCvb15627	Fix for SQL Injection Vulnerability in ISE Sponsor portal.
CSCvb48654	Fix for OpenSSL September 2016 vulnerabilities in ISE.
CSCvb85648	Fix for CVE-2016-5195 (DIRTY CoW) vulnerability in ISE.
CSCvb87634	ISE Internal users are unable to login to all the network devices due to internal password change.
CSCvc34224	ISE reloads occasionally while sending Change of Authorization requests.

Table 10 Cisco ISE Patch Version 2.0.0.306—Patch 5 Resolved Caveats (continued)

Caveat	Description
CSCvc71503	Endpoints looses static group assignments occasionally.
CSCvc74300	, /var/log/secure file size is increasing rapidly on a moderately used node.
CSCvc74307	Root folder grows to maximum size due to application not cleaning /var/cache/logwatch folder on a regular basis.
CSCvc86247	PSN runs high CPU in rare scenarios when experiencing connectivity issue with PAN.
CSCvd49829	Fix for struts2-jakarta rce vulnerability in ISE.
CSCuo16506	Internal users cannot change their password in the guest portal.
CSCur11333	MNT Session API shows XML Errors and inaccurate information while processing the REST request.
CSCuy19991	Intermittent Guest Authentication Fail on Guest portal.
CSCuy99383	ISE occasionally unable to send sponsored guest emails first SMTP server is busy due to missing retry logic in SMTP.
CSCuz11105	ISE fails to export language archive from the portal after modification.
CSCuz75818	During importing language file in portal settings new line characters are getting removed.
CSCva16918	Fix of certain known Endpoint Purge issues.
CSCva46497	Fix of XSS vulnerability in ISE admin dashboard page.
CSCva49067	Support bundle doesn't carry pxgrid and sxp debug log when time range is given.
CSCva94541	Fix of Leap Second 2016 issue in ISE.
CSCvb02488	Logrotate does not run correctly.
CSCvb46625	MNT live authentications page takes long time to query when greater than 3 hours logs are set.
CSCvb46648	Running concurrent MNT reports on deployment with huge radius traffic slows down ISE PAN access.
CSCvb52608	MNT live logs search takes a long time while querying MNT Livelog and reports.
CSCvb83673	SCCM 5.x version product check fails.
CSCvb86760	ISE 2.0.1 Authentication mechanism via GET requests Sponser Portal.
CSCvb97077	Exporting an endpoint list filtered with IP address or hostname gives a blank excel file.
CSCvc02009	ISE drops accounting packets from ASA.
CSCvc13039	Endpoint identity group does not change via hot spot portal.
CSCvc33873	RADIUS authentication report takes long time to generate report for last 30 days.
CSCvc36548	Unable to delete./oracle/base/diag/tnslsnr alert files in ISE.
CSCvc40801	ISE MnT becomes slow when ISE is integrated with Prime Infrastructure.
CSCvc61195	ISE system log files ADE.log/backup.log/restore.log logrotate displays incorrect data.
CSCvc83739	Unable to email credentials for imported guest through notices tab on Sponsor Portal.
CSCvc83795	Guest portal doesn't accept password with < and ! special characters.

Table 10 Cisco ISE Patch Version 2.0.0.306—Patch 5 Resolved Caveats (continued)

Caveat	Description
CSCvc84399	Admin COA fails. Secure MnT logic before updating an active session.
CSCug19963	Enhancement request to add extra diagnostic messages for VMware based ISE.
CSCup45594	Identity Services Engine (ISE): External RADIUS server is not persistent after failover.
CSCuz37822	Enhancement in ISE to create an option to set up packet size in the GUI.
CSCuz53809	None option is missing from the PM severity level drop-down list.
CSCuz57982	In ISE 1.3 P5, SMS Reset password is unavailable in Portal Customization Page.
CSCvb93221	In ISE the rate limit range is increased to 1-3000.
CSCvc05016	ISE Microsoft Certificate Template V2 attribute does not match.
CSCvc08700	Fix of ISE for OpenSSL November 2016.
CSCuz76370	Determination of Endpoint owner is dependent on Oracle when purging the Endpoint.
CSCvb25290	Endpoint purge takes a long time (~10 hrs) when a deployment has 400 thousand endpoints.
CSCvb46440	After upgrading from ISE 1.3 patch 7 to ISE 2.0.1, purge rules are not working as expected.
CSCvc05024	Endpoint purge goes to infinite loop when purge policies are configured on ISE.
CSCvc53146	Endpoint purge job takes 2 to 3 days when there are 700 thousand endpoints.

Known Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 5

Issues with upgrading from 2.0 to 2.3 via GUI

When you upgrade from 2.0 to 2.3 through GUI simultaneously on all nodes, it shows **Download failed - Upgrade bundle download timed out**.

However, in ADE.log shows **Upgrade preparation success** message.

It is recommended to download the bundle to one node at a time. Do not download the bundle simultaneously on all the nodes.

New Features, Known and Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 4

Known Issues in Cisco ISE Version 2.0.0.306—Patch 4, page 31

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 4, page 32

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 4, page 32

Known Issues in Cisco ISE Version 2.0.0.306—Patch 4

The following are known issues in sponsor portal of Cisco ISE version 2.0.0.306—Patch 4:

Diffie-Hellman Minimum Key Length

Connection to LDAP server will fail in Cisco ISE 2.0 patch 4 and above if the Diffie-Hellman minimum key length configured on the LDAP server is less than 1024.

Sponsors are Allowed to Manage Guest Accounts of Other Groups

Sponsors are allowed to manage the guest accounts created by other sponsor groups, even when you select the **Accounts Created by Members of this Sponsor Group** option for **Sponsor Can Manage** field while creating the sponsor group. This issue occurs when the groups are referenced from the Active Directory. For instance, this issue occurs when a sponsor belonging to a group for which **Accounts Created by Members of this Sponsor Group** option is enabled, have access to all guest accounts.

Imported User Account Details are not Displayed on Sponsor Portal Page

When you import a file with usernames and passwords to sponsor portal, the number of accounts created is shown but the account details are not displayed on the Sponsor Portal page. Print, SMS, or Email options in the **Notices** tab fail to work for the accounts created via the import option.

Sponsor Portal Username/Password is Validated with ISE Guest Username/Password Policy

Sponsor portal username or password is validated based on ISE Guest username or password policy and an error is seen if the imported sponsor portal username is not compliant with guest username or password policy.

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 4

The following table lists the issues that are resolved in Cisco Identity Services Engine, Release 2.0.0.306 cumulative patch 4.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 4 might not work with older versions of SPW. MAC users need to upgrade their SPW to MACOSXSPWizard 2.1.0.40 or later and Windows users need to upgrade their SPW to WinSPWizard 2.1.0.51 or later.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0*. for instructions on how to apply the patch to your system.

Table 11 Cisco ISE Patch Version 2.0.0.306—Patch 4 Resolved Caveats

Caveat	Description
CSCuz44971	Inconsistent Endpoint inactivity timer causes purge issues in Cisco ISE 1.3.
CSCuw48837	Authentication stops on PSN with no logs reported on MnT.
CSCux03001	Upon upgrading from ISE 1.2 to 1.4 and removing some SGTs, ISE does not push all the Trustsec policies to switch.

Table 11 Cisco ISE Patch Version 2.0.0.306—Patch 4 Resolved Caveats

Caveat	Description
CSCux11146	SXP passwords are encrypted using the wrong key. SXP passwords should be encrypted using the key that is used to encrypt all other sensitive material stored in ISE Oracle DB.
CSCux53966	IP-SGT binding is not generated for guest flow.
CSCuy20317	"Profiler Queue limit reached" error in patch 5 of ISE 1.3 or 1.4.
CSCuz08717	Performance degradation observed in ISE 1.4 patch 7 due to profiler changes.
CSCuz28989	On Cisco ISE 1.4 Patch 6, AD connector restarts intermittently when a user logs in with invalid attributes.
CSCuz30471	Delay in wired guest COA while using Cisco ISE 2.0.
CSCuz46469	Restarting services in Cisco ISE 2.0 patch 2 and patch 3 breaks authorization based on network device profile.
CSCva02380	"HTTP Status 400 - Bad Request" error occurs when an FQDN is used to login to ISE.
CSCva14899	Cisco ISE does not support MAC 10.12.
CSCur64918	ISE 1.2 replication stops when moving from monitoring to enforcement mode.
CSCuu21473	Portal users for the existing BYOD on-boarded devices are missing from endpoints page after upgrading ISE 1.3 to 2.0.
CSCuv82040	In ISE 1.3/ or 1.4, CoA is not sent when endpoint purge occurs from non-guest flow client.
CSCuv95664	ISE 1.4 data base grows very large due to EDF database table logs, causing giant backups.
CSCuw26491	Guest authentication is done based on the framed accounting service type.
CSCux09644	Renaming an authorization rule under Device Admin Default Policy Set changes default authorization rule to the renamed authorization rule.
CSCux24687	Automatic AD to DC fail over does not happen on RPC failure.
CSCux41407	Evaluation of positron for OpenSSL December 2015 vulnerabilities.
CSCux44143	ISE 2.0 Posture updates not going through proxy.
CSCux48635	BYOD endpoints stuck in Pending if more than 2 endpoints are provisioned within 20 minutes.
CSCux59729	Backup fails for nfs repository after ISE 1.4 patch 3 is installed.
CSCux73806	Operation console page loads, but does not open.
CSCux89718	Cisco ISE 1.4 patch 3 has issues with guest portal login for guest accounts that have extended time range.
CSCuy07004	Live log and ISE very slow after upgrade from ISE 1.3 to 2.0.
CSCuy30044	Problems in issuing EPS and ANC remediations against IPv6 clients.
CSCuy46322	Default Deny Access option present in ACS is missing in ISE TACACS feature.
CSCuy53020	Bind SQL Injection was found in first Appscan reports for Guest related portal.
CSCuy62830	In ISE 1.3 or later, CWA Auto Device Registration sends CoA Disconnect for a device already registered to the guest account.

Table 11 Cisco ISE Patch Version 2.0.0.306—Patch 4 Resolved Caveats

Caveat	Description
CSCuy69285	Cisco ISE 1.3 patch 6 has issues with sessions not being released.
CSCuy71639	Cisco ISE incorrectly reports switchport index change.
CSCuy75787	Email notifications sent from sponsor portal using restAPI fail.
CSCuy83379	MyDevices portal overrides statically blacklisted endpoint.
CSCuy86957	Unable to delete guest compound condition and user identity groups mapped to sponsor group policy, after upgrading from ISE 1.2 to 1.4.
CSCuy91317	Restore process does not get completed during ISE database sync up.
CSCuy92622	Sponsor portal notifications fail if language bundles differ across portals.
CSCuz06632	After failover, Alarms or Live Logs take more time to load.
CSCuz06708	Unable to retrieve NFS (windows2012) repository from UI.
CSCuz13452	In ISE 2.0, endpoint purging policies match only “Purge” rules and ignore “Never Purge” rules.
CSCuz42662	PxGrid services are stuck in initializing state.
CSCuz52493	Evaluation of positron for OpenSSL May 2016.
CSCuz72316	After upgrading ISE 2.0 to ISE 2.0 patch 3, manually registered devices in the My Devices portal stay in “NOTREGISTERED” status.
CSCva04654	Restore or upgrade of ISE 2.0 to 2.1 removes Default DenyShell Profile.
CSCva39593	MnT nodes trigger high load average alarm due to continuous TrustSec query.
CSCvb28658	AD agent is unable to reconnect to Domain Controller upon receiving TCP reset.
CSCvb28695	Request to enhance concurrent handling for DC Availability Updates.
CSCux82480	The System Health - Check NTP test fails occasionally in ISE 2.0.
CSCuz01888	NTP sync times out when an NTP server is added from UI.
CSCus09640	ISE 1.3, 1.4 or 2.0 on Win 8.1 device with Plus license (without Apex license), does not allow posture update.
CSCuy24899	Enhancement request to decrease the minimum value for LastAUPAcceptance check.
CSCuy60352	ISE provides severity levels support on Posture patch management conditions.
CSCuz09501	Unable to set passwords while importing guest users.
CSCuz97727	RADIUS authorization profiles do not support internal user attributes for DACL name.

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 3

The following table lists the issues that are resolved in Cisco Identity Services Engine, Release 2.0.0.306 cumulative patch 3.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 3 might not work with older versions of SPW and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0*. for instructions on how to apply the patch to your system.

Table 12 Cisco ISE Patch Version 2.0.0.306—Patch 3 Resolved Caveats

Caveat	Description
CSCuh80594	Default Enum value selection for custom attribute is not working.
CSCuu18124	LDAP sponsored accounts are missing after upgrade to 1.3. **Workaround** Use the SponsorAllAccounts group instead of Group or Own.
CSCuu30079	Add, Edit & Duplicate operations are not working fine on AMP Enabler profile.
CSCuv68500	MDM: Do not force redirection for devices not already enrolled with MDM. **Workaround** Onboard devices via ISE.
CSCuv71811	ISE authentication latency is increased every hour. **Workaround** Restart the ISE service every 5 days.
CSCuv77724	In Certificate Provisioning page, providing input in the PQDN field gives error "The FQDN field is not in a valid format".
CSCuv88011	When using the Profiler Feed Service in ISE 1.4, the Feed Service Update overwrites the Admin Created rules of same name. **Workaround** Configure a "Cisco Provided" policy to fit the custom profiler condition needs, or rename the custom policy before running the Feed Service update.
CSCuv89453	In ISE 1.3, repeated password change and login loop occurs in the Guest and Sponsor portal.
CSCuv91527	ISE upgraded to 1.4 does not have ANY AV option in remediation.
CSCuv94231	Acs.NormalizedUserName is empty on Radius Token after authentication.
CSCuv97343	While creating new guest accounts, ISE 1.3 caches the previous Sponsor's email address.
CSCuv99833	ISE 1.3 Feed posture scheduler service failed with JDBC exception. **Workaround** 1. Trigger the update manually. 2. Restart the services.

Table 12 Cisco ISE Patch Version 2.0.0.306—Patch 3 Resolved Caveats (continued)

Caveat	Description
CSCuw09627	In ISE 1.3 RSA Agent introduces delay in authentication flow causing authentication failure under moderate load. This issue occurs with ISE 1.3 and RSA/ACE Agent version 8.1.2. **Workaround** Use the Radius Token.
CSCuw27263	External RADIUS server was not supported for authentication when used as part of BYOD flow. **Workaround** Use an internal user or AD user account.
CSCuw29108	ISE 1.3 Guest Portal access fails with embedded Posture check and Web Agent flow. **Workaround** Uncheck the Require guest device compliance check box to avoid embedded posture check and to setup a separate policy for posture check, in the **Guest Portals**. or Access the network by using NAC Agent or AnyConnect ISE Posture module.
CSCuw31016	My Devices Portal not mapping the Portal User name properly from Guest Flow. When provisioning devices using the Guest Portal with an Active Directory short name account, the Portal User in the My Devices portal does not map with the Portal User name from the Guest Portal correctly. Hence, devices are seen unless the UPN is used.
CSCuw57930	Guest Account expiration email is not sent before the user account expires.
CSCuw60028	ISE 1.x: External Radius server does not take '&' in shared secret key.
CSCuw67042	ISE files are missing in the support bundle.
CSCuw95152	While providing account details to the known guests, if the Copy me check box is unchecked, it caches the email address of the previous sponsor.
CSCuw98748	Javascript input in the sponsor portal configuration is doubled when accessing the portal.
CSCuw99899	ISE 1.3 patch 5 MNT session is not cleared even though accounting stop is received. **Workaround** Clear the session manually via MNT API.
CSCux03119	Sponsored BYOD support.
CSCux07108	ISE 1.3 patch 4 application is initializing after feed service replication message. If the user turns on the profiler feed service in a distributed deployment, the application service on the nodes goes into initializing state. **Workaround** None. Run the **application reset-config** command to recover from this state.
CSCux10424	AD Black list is not refreshed within expected frequency in ISE. **Workaround** Reload the PSN exhibiting the behavior.

Table 12 Cisco ISE Patch Version 2.0.0.306—Patch 3 Resolved Caveats (continued)

Caveat	Description
CSCux18771	Post self-registration, login with a different user fails with Internal Error. **Workaround** Use the credentials you created in the guest portal after registering. All other logins work on the first page. or Do not put Guest Users at the top of Guest_Portal_Sequence.
CSCux21939	ISE endpoint purge does not delete endpoints.
CSCux43787	ISE runtime is stuck when it receives more than 4 requests. **Workaround** Restart the services and rejoin node.
CSCux46301	ISE 2.0 guest account expiration SMS notification doesn't work. **Workaround** Enable email notification.
CSCux53910	ISE 1.3 patch 5 memory increase leads to authentication latency. **Workaround** Restart the ISE application every 5 days.
CSCux58966	User password is showing up under External RADIUS server.
CSCux61238	Range of SNMPQUERY EventTimeout extended to 150 seconds from 60 seconds.
CSCux61360	ISE 2.0 guest password expires after one day. **Workaround** Enable "password never expires" for guest accounts.
CSCux66320	ISE 2.0 authentication policies are disappearing from configuration.
CSCux73262	ISE 1.4 App Service restarts while updating posture remediation resource. **Workaround** Contact TAC.
CSCux77620	Guest purge shows 'Fail to receive server response due to network error'. **Workaround** Change the time or frequency of the scheduled purge and reset it back. or Change the ISE timezone and set it back.
CSCux79853	HTTPS API call fails to SMS Gateway (tested with Clickatell).
CSCux91475	Once feed service update is done manually, no more feed update is possible.
CSCux92681	SMS via HTTP-POST is failing for GlobalDefault on Clickatell.
CSCux97025	Ownership change/merge can fail if the endpoint source is Configuration Protocol.
CSCux99204	ISE 2.0 patch2 breaks HotSpot portal, CoA before AUP is accepted. **Workaround** Downgrade to ISE 2.0 patch 1 or ISE 2.0 no patches.
CSCuy10037	CDP doesn't work if Telepresense doesn't have cdpCacheAddress.

Table 12 Cisco ISE Patch Version 2.0.0.306—Patch 3 Resolved Caveats (continued)

Caveat	Description
CSCuy12346	ISE repeat counters are not reset in 24 hours.
CSCuy29028	EAP-TLS memory leak.
CSCuy29124	ISE 2.0.1 MR is not able to scale up when enough resources are available.
CSCuy33801	ISE 2.0 admin portal does not accept FQDN with '-' hyphen. **Workaround** Use FQDN without '-' in the last segment.
CSCuy34700	Update glibc packages to address CVE-2015-7547.
CSCuy43592	ISE 2.0 sends CoA Disconnect after marking the user as compliant. **Workaround** Use SSL VPN.
CSCuy51958	ISE 2.0 certificate auto-validation interrupts internode communications.
CSCuy81433	ISE 2.0 CoANAK failed to find any session identification attributes. **Workaround** Contact TAC.

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 2

The following table lists the issues that are resolved in Cisco Identity Services Engine, Release 2.0.0.306 cumulative patch 2.

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 2 might not work with older versions of SPW and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0*. for instructions on how to apply the patch to your system.

Table 13 Cisco ISE Patch Version 2.0.0.306—Patch 2 Resolved Caveats

Caveat	Description
CSCuw62692	Period (.) is not allowed in the Network Device Name field.
CSCuw89551	ISE XML policy export does not distinguish between TACACS and RADIUS policy set.
CSCuw27405	Should remove the Remediate and Provisioning options for ANC.
CSCuw58973	There is no way to manually Unquarantine an EPS endpoint in ISE 2.0.
CSCuw09138	When an AD connector is used, high memory utilization is seen on PSNs. After some time an alarm is generated for AD service being restarted. The memory usage drops and then increases again. **Workaround** Restart the services.

Table 13 Cisco ISE Patch Version 2.0.0.306—Patch 2 Resolved Caveats (continued)

Caveat	Description
CSCuw74703	After upgrading from ISE 1.2.1 to ISE 1.4, IP phones are not profiled correctly. **Workaround** Run the EP_Reset_Time.sh script on all the nodes where the Profiler is enabled.
CSCuw94822	ISE 2.0 is not compliant with LGPLv2.1 License requirement.
CSCuw78737	Some of the Guest endpoints are stuck in the HotSpot AUP portal loop even after purge. **Workaround** Remove the endpoint from the ISE database and clear all sessions for the endpoint on the controllers.
CSCuv61017	BYOD flow fails because PSP-Commons-1.3.0.295.jar is missing from the dir: /opt/CSCOcpm/appsrv/apache-tomcat-ca/webapps/caservice-webapp/WEB-INF/lib
CSCux30540	pxGrid controller service is not stable after installation of ISE 2.0 Patch 1.
CSCuw45102	ID Mapping filter specified in CIDR format (for example, 10.1.100.0/24) is not working. **Workaround** Specify individual IP addresses as filters.
CSCuw02111	When a VPN client disconnects, ASA sends Accounting stop message, but the session is not cleared on ISE.
CSCuu94127	ISE profiler mixes attributes from different sessions when IP based probes are used without turning on RADIUS probe. After applying this patch, turn on the RADIUS probe, and configure your NADs to send RADIUS Accounting messages to the PSNs that have the profiler turned ON.
CSCuw22718	When a high number of client provisioning transactions occur, PAP runs out of heap memory and then fails.
CSCuw65623	Invalid FQDN message is displayed when a number is included in the middle of the domain name, for example, 1portal.com is fine but portal.1test.com or portal.abc.1test.com gives error. **Workaround** Do not use a number in the FQDN.
CSCuu08092	Problem with reading the network devices from the database after upgrade. ISE 1.3 allows defining network devices with period (.) at the end. After upgrading to ISE 1.4, the authentications from these devices will be dropped because using period at the end is not allowed. **Workaround** Remove existing devices and create the same devices again.
CSCux11146	SXP passwords are encrypted using the wrong key. SXP passwords should be encrypted using the key that is used to encrypt all other sensitive material stored in ISE Oracle DB.
CSCuv81729	After upgrading to ISE 1.4, Vendor list is not populated for new Patch Management Condition for any Operating System.

Table 13 Cisco ISE Patch Version 2.0.0.306—Patch 2 Resolved Caveats (continued)

Caveat	Description
CSCux30578	Guest flow with HP device does not work on distributed deployment. 500 Internal Error message is displayed when it is redirected to the Guest portal.
CSCux27365	ISE does not support EAP clients with legacy ciphers. Legacy clients that support only RC4 or DES encryption ciphers will fail the EAP handshake while connecting to ISE.
CSCuw88244	ISE-TACACS Term licenses are shown as permanent licenses after import.
CSCuw40899	Endpoint MAC is not updated in the correct endpoint identity group, when the client switches from one SSID to another. **Workaround** You have to manually delete the Endpoint from the previous endpoint group.
CSCuw59035	HTTP Status 400 - Bad Request error is displayed after login, if PAT/NAT is used on non-443/TCP port.
CSCuw51376	Endpoints are not profiled correctly after PSN Ownership change.
CSCuw15139	The following error message is displayed while generating the master guest report: `Unable to connect to the operation database. Please check the network connectivity and retry again later.`
CSCur44745	When the Suppress Repeated Successful Authentications option is enabled, CoA events are added to Auth details in Live Log session entry. **Workaround** Disable the Suppress Repeated Successful Authentications option under Administration > System > Settings > Protocols > RADIUS.

Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 1

The following table lists the issue that is resolved in Cisco Identity Services Engine, Release 2.0.0.306 cumulative patch 1 (ise-patchbundle-2.0.0.306-PP1-161394.SPA.86_64.tar.gz).

To obtain the patch file necessary to apply the patch to Cisco ISE, Release 2.0, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

Patch 1 might not work with older versions of SPW and users need to upgrade their SPW.

Then refer to the "Installing a Software Patch" section of the "Administering Cisco ISE" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 2.0*. for instructions on how to apply the patch to your system.

Table 14 Cisco ISE Patch Version 2.0.0.306—Patch 1 Resolved Caveats

Caveat	Description
CSCuw88770	ISE 2.0 PEAP TLS 1.2 wireless authentication fails with Android 6 and Win 10. This issue occurred because in TLS 1.2, the mechanism of MPPE keys generation has been changed for EAP-TLS, PEAP, and EAP-TTLS. EAP-FAST is not affected. **Symptom:** Authentication reports from logs show that the authentication is successful; however, the state on the WLC of the client session is dot1x required. Wireless packet captures reveal that 4-way handshakes following EAP-success are not completing, either M1 and M2 or M1 only. **Conditions:** This issue occurs when a combination of the following conditions are true: • If you have Cisco ISE, Release 2.0 FCS version with no patch installed. • Wireless LAN with L2 security configured for WPA2 Enterprise. • A device with Android 6 or Windows 10 version 1511 tries to authenticate. • Protocols used are PEAP or TTLS or EAP-TLS **Workaround:** • For Android, none. You cannot configure TLS version from Android client or Cisco ISE • For Windows 10 clients, you may disable TLS 1.2 and enable TLS 1.0: – Create DWORD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13\TlsVersion and set the associate DWORD value to C0. – Restart EapHost service.

Cisco ISE, Release 2.0 Open Caveats

Open Caveats

Table 15 Cisco ISE, Release 2.0, Open Bugs

Caveat	Description
CSCuy84839	The default rule configured in ISE 2.0 is changed from Deny access to Internal users. **Workaround** Review the policy configuration from the GUI after each restart and reconfigure if the problem occurs.
CSCus91272	EAP-TTLS with EAP-MSCHAPv2 authentication using native supplicant fails due to unmatched EAP identifier.

Table 15 Cisco ISE, Release 2.0, Open Bugs

Caveat	Description
CSCut18311	In the RADIUS Authentication Report CVS file, the Radius Status value shows `0` for a failed authentication and `1` for a passed authentication instead of `Pass` or `Fail`.
CSCut33204	You cannot search a report using a string that has a forward slash (\) in it. For example, `Cisco\`. It does not return the proper results. **Workaround** Perform the search without the forward slash.
CSCut64610	The Operation Audit report does not show the following changes: • **Authentication Policy**: All of the CRUD operations are getting logged as configuration changes and not specifically as created, updated, or deleted. • **Policy > Policy Elements > Results > Authentication > Allowed Protocols**: No logging is happening for CRUD operations. • **Policy > Policy Elements > Results > Authentication > Simple**: The delete operation is not getting logged.
CSCuv03825	System and Solutions (SnS): In distributed deployments, sometimes all secondary nodes are in "Replication Stopped" state (happens very rarely). **Workaround** If all nodes stay in "Replication Stopped" state for more than a few minutes, restart the Primary PAN.
CSCuv13440	In dual SSID SAML flow, after certificate provisioning, the CoA disconnect is sent and the UI is shown to connect to the SSID manually. However in Windows 10, when selecting the SSID and the certificate, it asks for the username but authentication is not initiated after provisioning.
CSCuv14593	RBAC administrators can import and view endpoints from parent endpoint groups.
CSCuv14605	The VLAN DHCP release page in guest portal does not launch on Windows 10 Edge browser. **Workaround** Use Mozilla Firefox browser.
CSCuv83774	Unable to create a time and date policy condition or downloadable ACL name with certain allowed characters. Angular brackets (<>), ampersand (&), and percentage (%) symbols are the only supported characters.
CSCuv88378	Certificate provisioning portal duplication does not duplicate the authorization groups and template.
CSCuv90086	The primary administration node (PAN) restarts when regenerating Cisco ISE root CA in a large deployment. The PAN is not available for a long time.
CSCuv94217	In Mozilla Firefox 40, after reordering policy sets and saving the new order, the Save Order button disappears. This issue is seen only with Mozilla Firefox, version 40 browsers.
CSCuw08701	The ACS to ISE migration tool throws an error during export if the authorization profile has a space in the name. **Workaround** Remove the space from the authorization profile name in ACS and export the data again.

Table 15 Cisco ISE, Release 2.0, Open Bugs

Caveat	Description
CSCuw21758	Changes to the Acceptable Use Policy (AUP) settings in My Devices Portal is not taking effect when set to "On first login only" or "Every *x* days." The user is prompted for AUP acceptance on every login.
CSCuw22718	When a high number of client provisioning transactions occur, PAP runs out of heap memory and fails over.
CSCuw23690	The pxGrid service restarts when you enable or disable the SXP service.
CSCuw23941	On MAC, after network reset, non-broadcast SSIDs are not connecting automatically. **Workaround** SSID is displayed in the list of Available Networks. Click **Connect** to connect to the SSID.
CSCuw29997	When used with Aruba WLCs, the ISE Guest portal redirect static URL contains the special character, "?" and the system does not interpret this character in the URL correctly and redirection does not work. **Workaround** Manually configure the URLs in all the WLCs.
CSCuw34150	The crypto host_key add host command does not work when the SFTP server uses DSA keys. **Workaround** Establish an SSH connection to the SFTP server and manually add the crypto host key to the Cisco ISE database.
CSCuw35766	Plus license is consumed even if static endpoint group assignment is set.
CSCuw38040	In Mac OSX, wired profile is not provisioned when both the wired and wireless profiles are configured with different authentication protocols or certificate templates. This issue is seen in supplicant provisioning wizard, version 1.0.0.35. **Workaround** Create a separate native supplicant profile for the wired use case.
CSCuw43915	Mac OS X 10.10 and Mac OS X 10.11: Unable to connect to SSID automatically after NSP provisioning during PEAP or EAP-FAST authentication. **Workaround** Click the Connect button and provide the PEAP or EAP-FAST credentials manually.
CSCux31573	Native Supplicant Provisioning (NSP) fails during BYOD TLS flow for Windows 10 build 10565. Symptom: NSP fails during BYOD TLS flow for Windows 10 build 10565 devices. Conditions: This issue occurs when the following conditions are met: 1. Installed ISE Version 2.0.0.306 Patch 1. 2. Configured authorization profile for redirecting to the BYOD portal. 3. Configured NSP profile with Windows 10. 4. Configured client provisioning policy with Windows 10 and associate with the NSP. 5. A device with Windows 10 (build 10565) connects through the BYOD flow. Workaround: None.

Table 15 Cisco ISE, Release 2.0, Open Bugs

Caveat	Description
CSCve89369	You can create advanced filter and save it for the current sessions. The filter is lost once you log out and start a new session on the browser. **Workaround** Save cookies in the browser and modify the expiration date.

Open Agent Caveats

Table 16 Cisco ISE, Release 2.0, Open Agent Caveats

Caveat	Description
CSCuw19276	Cisco NAC Agent and Cisco NAC Web Agent do not support Google Chrome version 45 and later. The Java plug-in uses the Netscape Plugin API (NPAPI) in Google Chrome, which is integral to the functioning of the Cisco NAC Agent and Cisco NAC Web Agent. However, Google Chrome version 45 and later does not support NPAPI. **Workaround** To enable the Java plug-in: 1. In the Google Chrome window address bar, copy and paste the following URL: chrome://flags/#enable-npapi 2. Click the **Enable** link to enable NPAPI for Mac and Windows. 3. Click **Relaunch Now** at the base of the page to effect the changes.
CSCuw17919	Trend Micro Internet Security 10.x is not available. While performing the posture assessment for Trend Micro Internet Security 10.x, you must configure the posture condition with Trend Micro Titanium 10.x, because Trend Micro Internet Security 10.x uses Trend Micro Titanium 10.x AV/AS engine.

Cisco ISE, Release 2.0, Resolved Caveats

The following table lists the caveats that have been resolved in this release:

Table 17 Cisco ISE, Release 2.0, Resolved Caveats

Caveat	Description
CSCuh12811	My Devices and Sponsor Portal URL does not work for both host and FQDN.
CSCun52844	Cross-Domain Referer Leakage reported under client provisioning.
CSCuq22852	Local web authentication fails if non-alphanumeric character is used in username or password.

Table 17 Cisco ISE, Release 2.0, Resolved Caveats (continued)

Caveat	Description
CSCuq92574	Bring Your Own Device (BYOD) profile installation fails on LG running Android 4.2.2.
CSCuq96560	Self-registered guest user has an access duration value of 0 after upgrade.
CSCuq97051	Slow replication errors seen with SNMP query probe enabled in a deployment that has both 3300 and 3400 series hardware.
CSCur11286	iPhone 6 is not redirected to the configured URL after provisioning.
CSCur13627	Monitoring Log Collector not showing any data for the last 60 minutes.
CSCur28245	User interface issues with Sponsor Group and Guest Type pages.
CSCur35764	Removing an internal CA certificate from the Trusted Certificates store also revokes the certificate from the Certificate Authority.
CSCur36983	Configuration data restore process stuck at 80%; field missing in LD_LIB_PATH library.
CSCur44557	Sponsor portal notifications fail if language bundles differ across portals.
CSCus09940	Cross-Site Request Forgery (CSRF) protection does not work for some of the web pages.
CSCus19913	The ISE AuthStatus Rest API does not work for multiple MAC Addresses.
CSCus50476	The Monitoring Node (MnT) is slow especially in showing live logs and reports.
CSCus78802	The usage of variable substitution in the middle of a string removes the initial characters.
CSCus93665	ISE 1.3 EAP-FAST chaining fails authorization after upgrade from 1.2.x.
CSCut04544	Vulnerability on ISE-Transport Layer Protection- Insecure Transmission.
CSCut04556	Cisco ISE is susceptible to Cross Frame Scripting attacks.
CSCut25212	In Android 4.3 and above, Native Supplicant Profile (NSP) does not store certificates in the keystore.
CSCut25227	Cross-site Scripting (XSS) vulnerability found in ISE admin pages.
CSCut40042	Redirect port reconfiguration is not working after Apache Tomcat upgrade in the Guest portal.
CSCut42520	The User Principle Name (UPN) authentication fails when a second Active Directory (AD) joint point is added.
CSCut58228	Samsung Android devices fail to install certificates for BYOD EAP-TLS.
CSCut63392	The Lock/advanced tuning to ISE GUI causes the AD service to crash.
CSCuu03368	Lightweight Directory Access Protocol (LDAP) users cannot manage the MyDevices Portal.
CSCuu04061	The ISE Policy Service Node (PSN) does not respond to RADIUS requests when MDM server is down.
CSCuu04227	MAB authentication followed by 802.1X fails.
CSCuu22410	Delay in writing guest session data to the cache and DB.
CSCuu43966	Error encountered when authentication order on switches is MAB and then 802.1x.
CSCuu49759	Mac OSX version 10.10 does not automatically connect to network for Single SSID.

Table 17 Cisco ISE, Release 2.0, Resolved Caveats (continued)

Caveat	Description
CSCuu60864	Unable to save newly profiled endpoints.
CSCuu65509	After upgrade from 1.2 to 1.4, the Admin portal is not accessible.
CSCuu76087	Windows PC connected to an IP Phone is profiled as Cisco-IP-Phone-7970.
CSCuu91928	ISE must send Product Name for definition checks instead of Vendor Name.
CSCuu92630	Replication failure alarms are triggered when modifying the CTS Policy in Cisco ISE.
CSCuv22443	Sponsored Guest users are prompted to start BYOD flow after entering their credentials in the Guest Portal.
CSCuv22604	During upgrade from 1.2 to 1.3, PSN that is not the current owner might assume ownership leading to invalid profiler classification.
CSCuv24342	CoA reauthorization triggers ISE to append a “Session Timeout” attribute.
CSCuv31567	Apache Struts 2 web application using the Object Graph Navigation Language (OGNL) console is vulnerable to remote command execution attack.
CSCuv51519	Sponsor portal does not load completely for certain AD users.
CSCuv52944	SWD-xxx LSQ-xxx-ISE fails to send stop accounting message, which impacts users.
CSCuv53534	The Endpoint lookup from the profiler DB is slow, when phones or other devices are authenticated/authorized by ISE.
CSCuv54014	CRL/OCSP URL verification fails with non-public top level domain.
CSCuv61017	BYOD flow fails because the .jar PSP-Commons-1.3.0.295.jar is missing from the dir: /opt/CSCOcpm/appsrv/apache-tomcat-ca/webapps/caservice-webapp/WEB-INF/lib
CSCuv71811	ISE authentication latency is increased every hour.
CSCuv90268	Validation failure for Admin users with email addresses containing multiple dots (“.”).

Documentation Errata

Cisco ISE 2.0 Online Help includes reference to 3300 series appliance—CSCuw68020.

Cisco ISE, Release 2.0 does not support legacy 3300 series, ACS, or NAC appliances. However, 3315, 3355, and 3395 series appliances are listed in the “Components Used in the MDM Setup” table of the “Manage Network Devices” chapter in the Online Help.

This information is incorrect and is removed from the *Cisco Identity Services Engine Administration Guide, Release 2.0* published on Cisco.com.

Documentation Updates

Table 18 Updates to Release Notes for Cisco Identity Services Engine, Release 2.2

Date	Description
12/20/2017	Added Resolved Issues in Cisco ISE Version 2.0.0.306—Cumulative Patch 6.

Related Documentation

Release-Specific Document

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 19 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 2.0	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html
Cisco Identity Services Engine Admin Guide, Release 2.0	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 2.0	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine Upgrade Guide, Release 2.0	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine, Release 2.0 Migration Tool Guide	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 2.0	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-user-guide-list.html
Cisco Identity Services Engine CLI Reference Guide, Release 2.0	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html
Cisco Identity Services Engine API Reference Guide, Release 2.0	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html

Table 19 Product Documentation for Cisco Identity Services Engine (continued)

Document Title	Location
Active Directory Integration with Cisco ISE	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html
Cisco ISE In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-documentation-roadmaps-list.html
Network Access Device Profiles with Cisco Identity Services Engine	http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-105-Network_Access_Device_Profiles_with_Cisco_ISE.pdf

Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

- Cisco ISE
  http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html
- Cisco UCS C-Series Servers

  http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html
- Cisco Secure ACS
  http://www.cisco.com/c/en/us/support/security/secure-access-control-system/tsd-products-support-series-home.html
- Cisco NAC Appliance
  http://www.cisco.com/c/en/us/support/security/nac-appliance-clean-access/tsd-products-support-series-home.html
- Cisco NAC Profiler
  http://www.cisco.com/c/en/us/support/security/nac-profiler/tsd-products-support-series-home.html
- Cisco NAC Guest Server
  http://www.cisco.com/c/en/us/support/security/nac-guest-server/tsd-products-support-series-home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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

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

© 2015 Cisco Systems, Inc. All rights reserved.