New and Changed Information

New and Changed Information

The following table summarizes the new and changed features and tells you where they are documented.

Table 1: New and Changed Features in Cisco ISE Release 3.1

Feature	Description
Cisco ISE Release 3.1 Patch 8	
Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller	You can create profiling policies, authorization conditions, and authentication conditions and policies for Apple, Intel, and Samsung endpoints, using device analytics data from the Cisco Wireless LAN Controllers integrated with your Cisco ISE. For more information, see "Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller" in the Chapter "Asset Visibility" in the Cisco ISE Administration Guide, Release 3.1.
Cisco ISE Release 3.1 Patch 7	
Link External LDAP Users to Cisco ISE Endpoint Groups	From Cisco ISE Release 3.1 Patch 7, you can assign external LDAP user groups to Endpoint Identity Groups for guest devices using the **Dynamic** option. For more information, see "Create or Edit Guest Types" in the chapter "Guest and Secure WiFi" in the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1 Patch 5	

Feature	Description
Automatically Assign Logical Profiles to Endpoints	When an endpoint goes through Cisco ISE profiling workflows, if the endpoint matches an endpoint profiling policy with an associated logical profile, the endpoint is automatically assigned the logical profile. For more information, see "Endpoint Profiling Policies Grouped into Logical Profiles" in the chapter "Asset Visibility" in the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.
Support for Cisco Secure Client	Cisco ISE 3.1 Patch 5 supports both AnyConnect and Cisco Secure Client for Windows, macOS, and Linux operating systems. The following Cisco Secure Client versions are supported for these operating systems: • Windows: Cisco Secure Client version 5.00529 and later • macOS: Cisco Secure Client version 5.00556 and later • Linux: Cisco Secure Client version 5.00556 and later You can configure both AnyConnect and Cisco Secure Client for your endpoints on these operating systems but only one policy will be considered at run time for an endpoint. For more information, see the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1 Patch 4	
Enhancement to the Groups tab in the REST Identity Store	You can now retrieve, filter, and delete REST identity store groups while configuring Resource Owner Password Credentials in Cisco ISE. While adding the groups, click Retrieve Groups to import the user groups from the connected identity source. Check the check boxes next to the groups that you want to select and click Save. You can also select all the groups, if needed. The selected groups are listed in the Groups tab. You can filter the results using the filter option. To delete a user group, check the check box next to the group that you want to delete and click Delete. For more information, see "Configure Resource Owner Password Credentials Flow" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1.*

Feature	Description
Cisco ISE Release 3.1 Patch 3	
Upate of OCSP Responder Certificates	From Cisco ISE Release 3.1 Cumulative Patch 3 onwards, the following rules are applicable for the renewal of OCSP certificates: • For a multi-node Cisco ISE deployment, OCSP certificates are renewed automatically if you install the patch through the Cisco ISE GUI. If you install the patch through the Cisco ISE CLI, we recommend you to renew the OCSP certificate manually. • For a standalone Cisco ISE deployment, OCSP certificates are renewed automatically irrespective of whether you install the patch through the Cisco ISE GUI or the Cisco ISE CLI. • If you uninstall Patch 3, you have to renew the OCSP certificate manually. This one-time OCSP certificate renewal process is because of the change in certificate hierarchy. For more information, see Update of OCSP Responder Certificates in the "Basic Setup" chapter of the *Cisco Identity Services Engine Administrator Guide, Release 3.1*.
Opening TAC Support Cases in Cisco ISE	You can now open TAC Support Cases for Cisco ISE and other Cisco products from the Cisco ISE GUI. For more information, see "Open TAC Support Cases in Cisco ISE" in the Chapter "Troubleshoot" in *Cisco ISE Administrator Guide, Release 3.1*.
SHA1 Ciphers Disabled by Default	From Cisco ISE Relase 3.1 Patch 2, SHA1 ciphers on port 443 are disabled by default. For more information, see "Configure Security Settings" in the Chapter "Segmentation" in *Cisco ISE Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1 Patch 1	

Feature	Description
OpenAPI Service	The following OpenAPIs have been introduced in Cisco ISE Release 3.1 Cumulative Patch 1: • License • Generate Self-Signed Certificate • Patch and Hot Patch • Deployment For more information, see "Enable API Service" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.
Signed SAML Authentication Request for Cisco ISE	Cisco ISE now only accepts signed SAML requests and assertions for authentication. For more information, see "Configure SAML ID Provider" in the Chapter "Asset Visibility" in *Cisco ISE Administrator Guide, Release 3.1*.
Cisco ISE Release 3.1	
MacOS Versions in Posture Policy Configurations	In Cisco ISE 3.0 and earlier, you could configure posture policies and requirements with minor MacOS versions such as MacOS 11.1, MacOS 11.2, and so on. In Cisco ISE 3.1, you can only choose major MacOS versions such as MacOS 11 (All) to configure posture policies and requirements. When you upgrade to Cisco ISE 3.1, any posture condition that includes a minor MacOS version is automatically updated to the corresponding major MacOS version. For example, a posture condition that was configured for MacOS 11.1 will be updated to MacOS 11 (All). For more information, see "Posture Types" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
Android Settings for Native Supplicant Profile	Android settings are added for native supplicant profile. You can select one of the following options for Certificate Enrollment Protocol: • Enrollment over Secure Transport (EST) • Simple Certificate Enrollment Protocol (SCEP) If you choose the EST protocol, Cisco ISE will ask for additional password inputs from Android users while issuing certificates. For more information, see "Native Supplicant Profile Settings" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.
Posture State Synchronization	You can configure AnyConnect to probe Cisco ISE at specified intervals when the posture status is not compliant. This helps prevent a client from being stuck in pending state. The posture state synchronization is supported for Windows, Linux, and MacOS clients. For more information, see "Posture State Synchronization" in the Chapter "Compliance" in the *Cisco ISE Administrator Guide, Release 3.1*.
Obtain Configuration Backup Using Cisco Support Diagnostics Connector	You can use Cisco Support Diagnostics Connector to trigger configuration backup and upload the backup files to the Cisco Support Diagnostics folder. After uploading the backup files to the Cisco Support Diagnostics folder, you can delete the backup files from the Cisco ISE local disk. To use this feature, you must enable smart licensing and Cisco Support Diagnostics in Cisco ISE. For more information, see "Obtain Configuration Backup Using Cisco Support Diagnostics Connector" in the Chapter "Troubleshoot" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
Configuration of Authorization Result Alarm	You can configure alarms based on the results of authorization policies. This allows you to monitor the impact of any networking, infrastructure, or application changes on endpoint authorizations. You can define the scope of your alarms by choosing specific Network Device Groups (NDGs). For each NDG you choose, a new Authorization Result alarm is created. You can filter the authorization logs to be monitored for an alarm by choosing specific authorization profiles and Security Group Tags (SGTs). Only endpoints that have met authorization policy sets with the specified authorization profiles and SGTs are monitored by the alarm. For more information, see "Configure Authorization Result Alarm" in the Chapter "Troubleshoot" in the *Cisco ISE Administrator Guide, Release 3.1*.
Configuration of Preferred Domain Controllers	You can specify the domain controllers that you want to use in case of domain failover. If a domain fails, Cisco ISE compares the priority scores of the domain controllers that are added to the preferred list and selects the one with the highest priority score. If that domain controller is offline or is not reachable because of an issue, the next one in the preferred list with the highest priority score is used. If all the domain controllers in the preferred list are down, a domain controller outside the list is selected based on the priority score. When the domain controller that was used before the failover is restored, Cisco ISE switches back to that domain controller. For more information, see "Configure Preferred Domain Controllers" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
Context Visibility Enhancements	• In the **Export Endpoints** dialog box, you can now check the **Importable Only** check box if you want to export only the attributes that can be imported to Cisco ISE without any modification to the CSV file. Using this option prevents the need to modify the columns or metadata in the exported CSV file before importing it to Cisco ISE. • While using the **Quick Filter** or **Advanced Filter** option, you can use the **Export Filtered** option to export only the filtered endpoints. For more information, see "Export Endpoints Using CSV File" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.
Virtual Appliance Licenses	Cisco ISE Release 3.1 and later supports the ISE VM license, which replaces the VM Small, VM Medium, and VM Large licenses that were supported in releases prior to Release 3.1. The new ISE VM license covers the Cisco ISE VM nodes in both on-premises and cloud deployments. For more information, see "Cisco ISE Licenses" in the Chapter "Licensing" in the *Cisco ISE Administrator Guide, Release 3.1*.
Download or Upload Files from Local Disk	You can easily add, download, or delete the files that are used for local disk management. For more information, see "Download and Upload Files from Local Disk" in the Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description

OpenAPI Service	OpenAPIs are REST APIs based on HTTPS operating over port 443. From Cisco ISE 3.1 onwards, newer APIs are available in the OpenAPI format. For more information on Cisco ISE OpenAPIs, see https://<*ise-ip*>/api/swagger-ui/index.html.
	
	The following OpenAPIs have been introduced in Cisco ISE 3.1:
	
	• Repository Management
	• Configuration Data Backup and Restore
	• Certificate Management
	• Policy Management
	  • RADIUS Policy
	  • TACACS+ Policy
	
	For more information, see "Enable API Service" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description

Posture Support for Linux Operating System	Posture is a service in Cisco ISE that allows you to check the state of all the endpoints that are connecting to a network for compliance with corporate security policies. Cisco ISE 3.1 supports the following Linux operating system versions, in addition to Windows and Mac operating systems:
	• Ubuntu
	  • 18.04
	  • 20.04
	• Red Hat
	  • 7.5
	  • 7.9
	  • 8.1
	  • 8.2
	  • 8.3
	• SUSE
	  • 12.3
	  • 12.4
	  • 12.5
	  • 15.0
	  • 15.1
	  • 15.2
	The following posture conditions are supported for Linux operating system:
	• File Condition
	• Application Condition
	• Antimalware Condition
	• Patch Management Condition
	You can configure agent profiles for Linux clients. You can add client-provisioning resources for AnyConnect Linux clients.
	For more information, see the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
ERS Service Auto Enabled on VMware Cloud Environment	The External RESTful Services (ERS) API service is enabled by default when the Amazon Machine Image (AMI) version of Cisco ISE is deployed on a VMware Cloud environment. This helps in easy integration of Cisco ISE with other Cisco products and third-party applications, without the need to enable the ERS service from the Cisco ISE GUI. For more information, see "Enable API Service" in the Chapter "Basic Setup" in the *Cisco ISE Administrator Guide, Release 3.1*.
Configuration of Maximum Password Attempts for Active Directory Account	You can configure the badPwdCount attribute to prevent Active Directory account lockout due to too many bad password attempts. Before authenticating the user, Cisco ISE compares the maximum bad password attempts configured in Cisco ISE with the current value of the badPwdCount attribute on Active Directory. When the maximum bad password attempts configured in Cisco ISE is equal to the value of the badPwdCount attribute, the authentication is dropped and not sent to Active Directory. For more information, see "Configure Maximum Password Attempts for AD Account" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.1*.
Handle Random and Changing MAC Addresses with Mobile Device Management Servers	As a privacy measure, mobile devices and some desktop operating systems increasingly use random and changing MAC addresses for each SSID that they connect to. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier called GUID instead of MAC addresses. When an endpoint enrolls with a Mobile Device Management (MDM) server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, ensuring accuracy and consistency between the two systems. For more information, see "Handle Random and Changing MAC Addresses With Mobile Device Management Servers" in the Chapter "Secure Wired Access" in *Cisco ISE Administrator Guide, Release 3.1*

Feature	Description
MAC Randomization for BYOD	Android and iOS devices increasingly use random and changing MAC addresses for each SSID that they connect to. Cisco ISE and MDM systems see different MAC addresses for the same device depending on which SSID they use to connect to the service. Therefore, a unique identifier is generated by the Cisco ISE Provisioning service to identify these endpoints. For more information, see "MAC Randomization for BYOD" in the Chapter "Basic Setup" in *Cisco ISE Administrator Guide, Release 3.1*.
Posture Script Remediation	You can create and upload posture remediation scripts to Cisco ISE to resolve non-compliance issues in endpoints. For more information, see "Add a Script Remediation" in the Chapter "Compliance" in *Cisco ISE Administrator Guide, Release 3.1*.
SAML-Based Admin Login	SAML-based admin login adds a single sign on capability to Cisco ISE using the SAML 2.0 standard. You can use an external Identity Provider such as Okta or any Identity Provider that implements SAML 2.0. For more information, see "SAML-based Admin Login" in the Chapter "'Asset Visibility" in *Cisco ISE Administrator Guide, Release 3.1*.
Specific License Reservation	Specific License Reservation is a smart licensing method that helps you manage your smart licensing when your organization's security requirements do not allow a persistent connection between Cisco ISE and the Cisco Smart Software Manager (CSSM). Specific License Reservation allows you to reserve specific license entitlements on a Cisco ISE node. You can create a Specific License Reservation by defining the type and number of licenses you need to reserve, and then activate the reservation on a Cisco ISE node. The Cisco ISE node on which you register and enable the reservation then tracks license usage and enforces license consumption compliance. For more information, see "Specific License Reservation" in the Chapter "Licensing" in *Cisco ISE Administrator Guide, Release 3.1*.

Feature	Description
Upgrade to pxGrid 2.0	From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards. pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations. For more information, see the Chapter "pxGrid" in *Cisco ISE Administrator Guide, Release 3.1*.