New and Changed Information

- **New and Changed Information**, on page 1

New and Changed Information

The following table summarizes the new and changed features along with information about where they are documented.

Table 1: New and Changed Features in Cisco ISE Release 3.2

Feature	Description
Cisco ISE Release 3.2 Patch 5	
Opening TAC Support Cases only for Cisco ISE	From Cisco ISE Release 3.2 Patch 5, you can only open TAC Support Cases for Cisco ISE from the Cisco ISE GUI. See Open TAC Support Cases.
On-demand pxGrid Direct Data Synchronization using Sync Now	From Cisco ISE Release 3.2 Patch 5, you can use the **Sync Now** feature to perform on-demand synchronization of data from pxGrid Direct connectors. You can perform both full and incremental syncs on-demand. On-demand data synchronization can be performed through the Cisco ISE GUI or using OpenAPI. See On-demand pxGrid Direct Data Synchronization using Sync Now.
Cisco ISE Release 3.2 Patch 4	
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. See Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller

Feature	Description
Customer Experience Surveys	Cisco ISE now presents customer satisfaction surveys to its users within the administration portal. The periodic administration of customer satisfaction surveys helps us better understand your Cisco ISE experiences, track what is working well, and identify areas of improvement. After you submit a survey, you are not presented with another survey for the next 90 days. The surveys are enabled by default in all Cisco ISE deployments. You can disable the surveys at a user level or for a Cisco ISE deployment. See Customer Experience Surveys
Cisco ISE Release 3.2 Patch 3	
Link External LDAP Users to Cisco ISE Endpoint Groups	From Cisco ISE Release 3.2 Patch 3, 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 3.2*.
Ukrainian Language Support in Portals	Guest, Sponsor, My Devices, and Client Provisioning portals now include Ukrainian as a supported localization language.
Cisco ISE Release 3.2 Patch 2	
pxGrid Direct Enhancements	pxGrid Direct is no longer a controlled introduction feature. Before you upgrade to Cisco ISE Release 3.2 Patch 2 from Cisco ISE Releases 3.2 or 3.2 Patch 1, we recommend that you delete all configured pxGrid Direct connectors and any authorization profiles and policies that use data from pxGrid Direct connectors. After you upgrade to Cisco ISE Release 3.2 Patch 2, reconfigure pxGrid Direct connectors. See Cisco pxGrid Direct **Note** If you do not delete the configured pxGrid Direct connectors, the connectors are automatically deleted during the upgrade. This deletion results in uneditable and unusable authorization profiles and policies that you must delete and replace with new ones.
Cisco ISE Release 3.2 Patch 1	
Meraki Connector for Cisco ISE	Cisco ISE 3.2 patch 1 and later releases support Cisco ISE and Cisco Meraki integration. Cisco ISE and cloud-based Cisco Meraki are TrustSec-enabled systems that are policy administration points for TrustSec policies. If you use both Cisco and Meraki network devices, you can connect one or more Cisco Meraki dashboards to Cisco ISE to replicate TrustSec policies and elements from Cisco ISE to the Cisco Meraki networks belonging to each organization. For information on configuring Meraki Connectors, see "Connect Cisco Meraki Dashboards with Cisco ISE" in the Chapter "Segmentation" in the *Cisco Identity Services Engine Administrator Guide, Release 3.2*.

Feature	Description
Support for Cisco AI Analytics	Cisco ISE 3.2 patch 1 and later releases support Cisco AI Analytics. The Cisco AI Analytics agent queries the endpoints data from Cisco ISE and sends it to AI cloud at regular intervals. This data can be used to reduce the number of unknown endpoints in the network by providing AI-based endpoint groupings, automated custom profiling rules, and crowd-sourced endpoint labels. For more information, see "Enable Cisco AI Analytics" in the Chapter "Asset Visibility" in the *Cisco ISE Administrator Guide, Release 3.2*.
Cisco ISE Release 3.2	
Posture Condition Script Support	You can create and upload a posture condition script to check the compliance status of an endpoint. This feature is supported for Windows, MacOS, and Linux platforms.
Cisco AnyConnect Rebranding	Cisco AnyConnect is rebranded as Cisco Secure Client. Cisco ISE 3.2 supports both the rebranded and legacy agents even though the Cisco ISE GUI is updated to use the rebranded terminology. See Compliance.
System 360	System 360 includes **Monitoring** and **Log Analytics**. The **Monitoring** feature enables you to monitor a wide range of application and system statistics, and key performance indicators (KPI) of all the nodes in a deployment from a centralized console. KPIs are useful to gain insight into the overall health of the node environment. Statistics offer a simplified representation of the system configurations and utilization-specific data. Cisco ISE 3.2 and later releases are integrated with Grafana and Prometheus. Grafana is a third-party metrics dashboard and graph editor. It provides a graphical or text-based representation of statistics and counters collected in the Prometheus database. Prometheus is used as the datastore to store the KPIs in time-series format. **Log Analytics** provides a flexible analytics system for in-depth analysis of endpoint authentication, authorization, and accounting (AAA) and posture syslog data. You can also analyze ISE health summary and ISE process statuses. Kibana, an open-source data visualization platform, is used to analyze and visualize syslog data. Elasticsearch is used to store and index the syslog data.
Mobile Device Management Enhancement	You can configure the **General MDM or UEM Settings** to query multiple MDM servers when the endpoints are not registered with the primary MDM or UEM server, or when the primary MDM or UEM server is not reachable.
Open API Specification for ERS APIs	The Open API specification (JSON file) for ERS APIs is available for download in the Cisco ISE GUI, in the **Overview** section of the **API Settings** window (**Administration** > **System** > **Settings** > **API Settings** > **Overview**. This Open API JSON file can be used for auto generation of API client code using any programming language such as Python, JAVA and so on. For additional information about Open API specifications and tools, see https://openapi.tools/.

Feature	Description
ERS APIs PATCH Request Support	Cisco ISE now supports PATCH requests for ERS APIs. A PATCH request helps in updating a subset of attributes for a resource. Only the attributes sent as part of the request are updated instead of the entire configuration for that resource. For more details, see API Reference Guide.
Single Entry for endpoints with GUID in the **Endpoints** context visibility window	In the Cisco ISE GUI, in the **Context Visibility** > **Endpoints** window, an endpoint with a GUID is listed only once with its latest random MAC address.
View Cisco ISE in Default or Dark Mode	You can now view Cisco ISE in default (light), or dark mode. Choose the default or dark mode from the **Account Settings** dialog box in the Cisco ISE administrator portal.
EAP-TLS and TEAP Authentication with Microsoft Entra ID	Cisco ISE supports certificate-based authentication and Microsoft Entra ID authorization.You can select attributes from the Microsoft Entra ID and add them to the Cisco ISE dictionary for use in authorization policies.
Managing Passwords of Cisco ISE Users	From Cisco ISE Release 3.2, as an internal user of Cisco ISE, you can manage the lifetime of your Enable and Login passwords using the **Password Lifetime** option. See Cisco ISE Users.
Cisco Private 5G	From Cisco ISE Release 3.2 onwards, Cisco ISE supports Cisco Private 5G and Session Management Function (SMF) software. Cisco ISE provides policy configuration for 5G authorization, which is implemented with RADIUS authorize-only and accounting flows.
Data Connect	The Data Connect feature provides database access to Cisco ISE using an Open Database Connectivity (ODBC) or Java Database Connectivity (JDBC) driver, so that you can directly query the database server to generate reports of your choice. Only read access to the data is provided. You can extract any configuration or operational data about your network depending on your business requirement and use it to generate insightful reports and dashboards. **Note** If the Data Connect feature is active in your Cisco ISE Release 3.2 Limited Availability release, when you upgrade to the Cisco ISE Release 3.2 General Availability release, you must disable and then enable the Data Connect feature.
Configuration of Authorization Policies for PassiveID Login Users	Check the **Authorization Flow** check box in the **Active Directory Advanced Settings** window if you want to configure authorization policies for PassiveID login users. You can configure an authorization policy to assign an SGT to a user based on the Active Directory group membership. This allows you to create TrustSec policy rules even for PassiveID authorization.

Feature	Description
Security Settings Enhancement	When the **Allow SHA-1 Ciphers** option (under **Administration** > **System** > **Settings** > **Security Settings**) is enabled, Cisco ISE allows SHA-1 ciphers for communication with the following Cisco ISE components: • Admin Access UI • Cisco ISE Portals • ERS • pxGrid This option is disabled by default. When you upgrade to Cisco ISE Release 3.2, the **Allow SHA-1 Ciphers** option is disabled even if you have enabled this option before the upgrade. You can enable this option after the upgrade if you want to allow the clients with only SHA-1 ciphers to communicate with Cisco ISE. You must restart all the nodes in a deployment after enabling or disabling this option. See Configure Security Settings.
Endpoint and Logical Profile Summary Report	This report lists the logical and endpoint profiles, and the number of endpoints matching those profiles.
pxGrid Direct	Cisco pxGrid Direct helps you to connect to external REST APIs that provide JSON data for endpoint attributes. The data that is collected is based on the attributes your specify in your pxGrid Direct configurations. Then, pxGrid Direct stores the collected data in the Cisco ISE database. This data can be used in the authorization policies. pxGrid Direct helps to evaluate and authorize the endpoints faster because the fetched data is used in the authorization policies. This eliminates the need to query for endpoint attribute data each time an endpoint must be authorized.

New and Changed Information