



## New and Changed Information

- [New and Changed Information](#), on page 1

## 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 3.3**

Feature	Description
<b>Cisco ISE Release 3.3 Patch 2</b>	
Configure Virtual Tunnel Interfaces (VTI) with Native IPsec	From Cisco ISE Release 3.3 Patch 2, you can configure VTIs using the native IPsec configuration. You can use native IPsec to establish security associations between Cisco ISE PSNs and NADs across an IPsec tunnel using IKEv1 and IKEv2 protocols. The native IPsec configuration ensures that Cisco ISE is FIPS 140-3 compliant.  See <a href="#">Configure Native IPsec on Cisco ISE</a> .
End of Support for Legacy IPsec (ESR)	From Cisco ISE Release 3.3 Patch 2, Legacy IPsec (ESR) is not supported on Cisco ISE. All IPsec configurations on Cisco ISE will be Native IPsec configurations.

Feature	Description
Enhanced Password Security	<p>Cisco ISE now improves password security through the following enhancements:</p> <ul style="list-style-type: none"> <li>You can choose to hide the Show button for the following field values, to prevent them from being viewed in plaintext during editing: <ul style="list-style-type: none"> <li>Under <b>Network Devices</b>, <ul style="list-style-type: none"> <li>• <b>RADIUS Shared Secret</b></li> <li>• <b>Radius Second Shared Secret</b></li> </ul> </li> <li>Under <b>Native IPSec</b>, <ul style="list-style-type: none"> <li>• <b>Pre-shared Key</b></li> </ul> </li> </ul> <p>See <a href="#">Configure Security Settings</a>.</p> <ul style="list-style-type: none"> <li>To prevent the RADIUS Shared Secret and Second Shared Secret from being viewed in plaintext during network device import and export, a new column with the header <b>PasswordEncrypted:Boolean(true false)</b> has been added to the Network Devices Import Template Format. No field value is required for this column.</li> </ul> <p>See <a href="#">Network Devices Import Template Format</a>.</p> </li> </ul>
Locking Identities with Repeated Authentication failures	<p>You can now limit the maximum number of unsuccessful authentication attempts an identity (username or hostname) can make while authenticating through the EAP-TLS protocol, by specifying the number of authentication failures after which the identity must be locked. Identities can be locked permanently or for a specific time period. Successful authentications by a locked identity will also be rejected until the identity is unlocked again.</p> <p>See <a href="#">RADIUS Settings</a>.</p>
On-demand pxGrid Direct Data Synchronization using Sync Now	<p>From Cisco ISE Release 3.3 Patch 2, you can use the <b>Sync Now</b> 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.</p> <p>See <a href="#">On-demand pxGrid Direct Data Synchronization using Sync Now</a>.</p>
Opening TAC Support Cases in Cisco ISE	<p>From Cisco ISE Release 3.3 Patch 2, you can open TAC Support Cases for Cisco ISE directly from the Cisco ISE GUI.</p> <p>See <a href="#">Open TAC Support Cases</a>.</p>

Feature	Description
Support for Transport Gateway Removed	<p>Cisco ISE no longer supports Transport Gateway. The following Cisco ISE features used Transport Gateway as a connection method:</p> <ul style="list-style-type: none"> <li>• Cisco ISE Smart Licensing</li> </ul> <p>If you use Transport Gateway as the connection method in your smart licensing configuration, you must edit the setting before you upgrade to Cisco ISE Release 3.3 Patch 2. You must choose a different connection method as Cisco ISE Release 3.3 Patch 2 does not support Transport Gateway. If you update to Cisco ISE Release 3.3 Patch 2 without updating the connection method, your smart licensing configuration is automatically updated to use the Direct HTTPS connection method during the upgrade process. You can change the connection method at any time after the upgrade.</p> <ul style="list-style-type: none"> <li>• Cisco ISE Telemetry</li> </ul> <p>Transport Gateway is no longer available as a connection method when using Cisco ISE Telemetry. The telemetry workflow is not impacted by this change.</p>
TLS 1.3 Support for Cisco ISE Workflows	<p>Cisco ISE Release 3.3 Patch 2 and later releases allow TLS 1.3 to communicate with peers for the following workflows:</p> <ul style="list-style-type: none"> <li>• Cisco ISE is configured as an EAP-TLS server</li> <li>• Cisco ISE is configured as a TEAP server</li> </ul> <p><b>Attention</b> TLS 1.3 support for Cisco ISE configured as a TEAP server has been tested under internal test conditions because at the time of Cisco ISE Release 3.3 Patch 2, TEAP TLS 1.3 is not supported by any available client OS.</p> <ul style="list-style-type: none"> <li>• Cisco ISE is configured as a secure TCP syslog client</li> </ul> <p>See <a href="#">Configure Security Settings</a>.</p>
<b>Cisco ISE Release 3.3 Patch 1</b>	
Cisco Duo Integration for Multifactor Authentication	<p>From Cisco ISE Release 3.3 Patch 1, you can directly integrate Cisco Duo as an external identity source for multifactor authentication (MFA) workflows. In earlier releases of Cisco ISE, Cisco Duo was supported as an external RADIUS proxy server and this configuration continues to be supported.</p> <p>This Cisco Duo integration supports the following multifactor authentication use cases:</p> <ol style="list-style-type: none"> <li>1. VPN user authentication</li> <li>2. TACACS+ admin access authentication</li> </ol> <p>See <a href="#">Integrate Cisco Duo With Cisco ISE for Multifactor Authentication</a>.</p>

Feature	Description
Customer Experience Surveys	<p>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.</p> <p>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.</p> <p>See <a href="#">Customer Experience Surveys</a></p>
<b>Cisco ISE Release 3.3</b>	
IPv6 Support for Agentless Posture	<p>Cisco ISE Release 3.3 adds IPv6 support for Agentless Posture. Windows and Mac clients are currently supported.</p> <p>See <a href="#">Agentless Posture</a>.</p>
Option to Disable Specific Ciphers	<p>Check the <b>Manually Configure Ciphers List</b> check box in the <b>Security Settings</b> window if you want to manually configure ciphers for communication with the following Cisco ISE components: admin UI, ERS, OpenAPI, secure ODBC, portals, and pxGrid.</p> <p>A list of ciphers is displayed with allowed ciphers already selected. For example, if the <b>Allow SHA1 Ciphers</b> option is enabled, SHA1 ciphers are enabled in this list. If the <b>Allow Only TLS_RSA_With_AES_128_CBC_SHA</b> option is selected, only this SHA1 cipher is enabled in this list. If the <b>Allow SHA1 Ciphers</b> option is disabled, none of the SHA1 ciphers are enabled in this list. You can select and unselect ciphers as required.</p> <p>See <a href="#">Configure Security Settings</a>.</p>
Navigation Improvement	<p>The Cisco ISE home page GUI has been modified for a better user experience. When you click the menu icon at the left-hand corner of the home page, a pane is displayed. Hovering your cursor over each of the options on the pane displays the following submenus to choose from.</p> <ul style="list-style-type: none"> <li>• <b>Context Visibility</b></li> <li>• <b>Operations</b></li> <li>• <b>Policy</b></li> <li>• <b>Administration</b></li> <li>• <b>Work Centers</b></li> </ul> <p>Click <b>Dashboard</b> for the home page.</p> <p>The left pane also contains a <b>Bookmarks</b> tab where you can save your recently viewed pages. Click the menu icon again to hide the pane.</p> <p>If you log out when the left pane is displayed, and log in again, the pane continues to be displayed. However, if you log out after the pane is hidden, and log in again, you must click the menu icon for the pane to be displayed again.</p> <p>You can now use the  icon on the homepage to access the <b>Search Pages</b> option to search for a new page or visit recently searched pages.</p> <p>See <a href="#">Basic Setup</a>.</p>

Feature	Description
Multi-Factor Classification for Enhanced Endpoint Visibility	<p>You can now create nuanced authorization policies using four specific attributes from the endpoints connecting to your network. The Multi-Factor Classification (MFC) profiler uses various profiling probes to fetch four new endpoint attributes to the Cisco ISE authorization policy creation workflows: MFC Endpoint Type, MFC Hardware Manufacturer, MFC Hardware Model, and MFC Operating System.</p> <p>See <a href="#">Multi-Factor Classification for Enhanced Endpoint Visibility</a>.</p>
Cisco AI-ML Rule Proposals for Endpoint Profiling	<p>Cisco ISE now provides profiling suggestions based on continuous learning from your network, helping you to enhance endpoint profiling and management. You can use these suggestions to reduce the number of unknown or unprofiled endpoints in your network.</p> <p>See <a href="#">Cisco AI-ML Rule Proposals for Endpoint Profiling</a>.</p>
Posture and Client Provisioning Support for ARM64 Version of Agent	<p>From Cisco ISE Release 3.3, posture policies and client-provisioning policies are supported for ARM64 endpoints. You can upload the ARM64 version of agent for ARM64 endpoints.</p> <p>See <a href="#">Configure Client-Provisioning Policy for ARM64 Version of Agent</a>.</p>
RADIUS Step Latency Dashboard	<p>The <b>RADIUS Step Latency</b> dashboard (<b>Analytics &gt; Dashboard</b>) displays the maximum and average latencies for the RADIUS authentication flow steps for the specified time period. You can also view the maximum and average latencies for the Active Directory authentication flow steps (if Active Directory is configured on that node) and the Top N RADIUS authentication steps with maximum or average latencies.</p> <p>See <a href="#">Log Analytics</a>.</p>
Schedule Application Restart After Admin Certificate Renewal	<p>After you renew an admin certificate on the primary PAN, all the nodes in your deployment must be restarted. You can either restart each node immediately or schedule the restarts later. This feature allows you to ensure that no running processes are disrupted by the automatic restarts, giving you greater control over the process. You must schedule node restarts within 15 days of certificate renewal.</p> <p>See <a href="#">Schedule Application Restart After Admin Certificate Renewal</a>.</p>
pxGrid Direct Enhancements	<p>pxGrid Direct is no longer a controlled introduction feature. Before you upgrade to Cisco ISE Release 3.3 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 3.3, reconfigure pxGrid Direct connectors.</p> <p>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.</p> <p>See <a href="#">Cisco pxGrid Direct</a>.</p>
Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller	<p>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.</p> <p>See <a href="#">Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller</a></p>

Feature	Description
Access the Cisco ISE Admin GUI using TLS 1.3	From Cisco ISE Release 3.3, you can access the Cisco ISE Admin GUI using the TLS 1.3 version. See <a href="#">Configure Security Settings</a> .
Configure Native IPsec in Cisco ISE	From Cisco ISE Release 3.3, you can configure IPsec using the native IPsec configuration. You can use native IPsec to establish security associations between Cisco ISE PSNs and NADs across an IPsec tunnel using IKEv1 and IKEv2 protocols. The native IPsec configuration ensures that Cisco ISE is FIPS 140-3 compliant. See <a href="#">Configure Native IPsec on Cisco ISE</a> .
Disable Endpoint Replication to all the nodes in a Cisco ISE Deployment	From Cisco ISE, Release 3.3, dynamically discovered endpoints are not replicated to all the nodes in the Cisco ISE deployment automatically. You can choose to enable or disable the replication of dynamically discovered endpoints across all nodes in your Cisco ISE deployment. See <a href="#">Data Replication from Primary to Secondary Cisco ISE Nodes</a> .
Link External LDAP Users to Cisco ISE Endpoint Groups	From Cisco ISE Release 3.3, you can assign external LDAP user groups to Endpoint Identity Groups for guest devices using the <b>Dynamic</b> option. See <a href="#">Create or Edit Guest Types</a> .
Managing Passwords of Cisco ISE Users	From Cisco ISE Release 3.3, as an internal user of Cisco ISE, you can choose to add the <b>Date Created</b> and <b>Date Modified</b> columns to the <b>Network Access User</b> table in the <b>Network Access Users</b> window. See <a href="#">Cisco ISE Users</a> .
Meraki Connector for Cisco ISE	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. See <a href="#">Connect Cisco Meraki Dashboards with Cisco ISE</a> .
Data Connect	From Cisco ISE Release 3.3, the Data Connect feature uses the admin certificate to provide 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. See <a href="#">Data Connect</a> .