Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.10.x

First Published: 2022-11-30

Last Modified: 2023-01-24

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.10.x

Introduction to Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points is a version of the Cisco IOS XE-based controller software on Catalyst access points. In this solution, a Catalyst access point (AP) that is running the Cisco Embedded Wireless Controller on Catalyst Access Points software, is designated as the primary AP. Other APs, referred to as subordinate APs, associate to this primary AP.

The Cisco Embedded Wireless Controller on Catalyst Access Points provides enterprise-level WLAN features while maintaining operational simplicity and affordability. This solution is targeted at small and medium-sized business (SMB) customers or distributed enterprises, and can be run at single site deployments.

- The controllers come with high availability (HA) and seamless software updates. This keeps your services on always, both during planned and unplanned events.
- The deployment can be managed using a mobile application, Cisco Digital Network Architecture (DNA) Center, Netconf/Restconf, web-based GUI, or CLI.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.10.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Cisco DNA Center Client Event and SSID Telemetry Filter	This feature filters out telemetry data for a configured SSID on the controller and the corresponding AP. The following command is introduced: • **icap subscription client exclude telemetry-data wlan**

Feature Name	Description and Documentation Link
Device Classifier Dynamic XML Support	This feature enables better device classification without upgrading the device to a new release. For more information, see the Chapter Device Classifier Dynamic XML Support.
Device Telemetry	This functionality enables collection of anonymous usage telemetry data for Cisco products, which helps in continuous product improvements. This functionality is enabled by default and can be disabled using the **no** form of the **pae** command. The following command is introduced: • **pae**
DNS or DHCP or AAA Server Reachability Through IPSLA and Failure Reasons for DHCP	This feature introduces additional parameters to capture the DHCP server failures in client events and send them to Cisco DNA Center for meaningful insights into the network and to take proactive actions on network issues to improve reliability, high availability, and performance.
Downloadable ACL (Central Switching Only)	The Downloadable ACL (dACL) feature defines and updates ACLs in one place (Cisco ISE) and allows ACL download to all the applicable controllers. For more information, see the Chapter Downloadable ACL (dACL).
Site Load Balancing	The Load Balancing feature is enhanced to specify a site load for better load balancing. The following command is introduced: • **load** For more information, see the Chapter System Configuration.
Support for 4 FNF Monitors	From Cisco IOS XE Dublin 17.10.1, you can configure up to four flow monitors (from the earlier limit of two flow monitors) in a policy profile per direction (input and output) in local mode. The additional flow monitors help to collect DNS traffic statistics and send them to Cisco DNA Center to analyse and take corrective actions.
Upgrade YANG Models to YANG 1.1	Cisco-defined YANG models are in YANG Version 1.1 in Cisco IOS XE Dublin 17.10.1 and later releases.

Feature Name	Description and Documentation Link
Device Ecosystem Data	This feature sends the device analytics data that is present in the RADIUS accounting request to Cisco ISE in order to profile endpoints. The following command is introduced: • **dot11-tlv-accounting** For more information, see the Chapter RADIUS Accounting.
Workgroup Bridge Mode on Cisco Catalyst 9124 and 9130 Series Access Points	Workgroup Bridge Mode mode is supported on the following APs: • Cisco Catalyst 9124 Series Access Points • Cisco Catalyst 9130 Series Access Points

Interactive Help

The Cisco Catalyst 9800 Series Wireless Controller GUI features an interactive help that walks you through the GUI and guides you through complex configurations.

You can start the interactive help in the following ways:

- By hovering your cursor over the blue flap at the right-hand corner of a window in the GUI and clicking **Interactive Help**.
- By clicking **Walk-me Thru** in the left pane of a window in the GUI.
- By clicking **Show me How**, which is displayed in various parts of the GUI. Clicking **Show me How** triggers a specific interactive help that is relevant to the context you are in.

  For instance, **Show me How** in **Configure** > **AAA** walks you through the various steps for configuring a RADIUS server. Choose **Configuration**> **Wireless Setup** > **Advanced** and click **Show me How** to trigger the interactive help that walks you through the steps relating to various kinds of authentication.

The following features have an associated interactive help:

- Configuring AAA
- Configuring FlexConnect Authentication
- Configuring 802.1x Authentication
- Configuring Local Web Authentication
- Configuring OpenRoaming
- Configuring Mesh APs

Note If the WalkMe launcher is unavailable on Safari, modify the settings as follows:

1. Choose **Preferences > Privacy**.
2. In the **Website tracking** section, uncheck the **Prevent cross-site tracking** check box to disable this action.
3. In the **Cookies and website data** section, uncheck the **Block all cookies** check box to disable this action.

Supported Cisco Access Point Platforms

The following Cisco access points are supported in the Cisco Embedded Wireless Controller on Catalyst Access Points network. Note that the APs listed as primary APs can also function as subordinate APs.

Table 2: Cisco APs Supported in Cisco Embedded Wireless Controller on Catalyst Access Points

Primary AP	Subordinate AP
Cisco Catalyst 9115 Series	Cisco Aironet 1540 Series
Cisco Catalyst 9117 Series	Cisco Aironet 1560 Series
Cisco Catalyst 9120 Series	Cisco Aironet 1815i
Cisco Catalyst 9124AXE/I/D	Cisco Aironet 1815w
Cisco Catalyst 9130	Cisco Aironet 1830 Series
Cisco Catalyst 9105AXI	Cisco Aironet 1840 Series
	Cisco Aironet 1850 Series
	Cisco Aironet 2800 Series
	Cisco Aironet 3800 Series
	Cisco Aironet 4800 Series
	Cisco Catalyst 9115 Series
	Cisco Catalyst 9117 Series
	Cisco Catalyst 9120 Series
	Cisco Catalyst 9124AXE/I/D
	Cisco Catalyst 9130
	Cisco Catalyst 9105AXW
	Cisco Catalyst 9105AXI
	Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points
	Cisco 6300 Series Embedded Services Access Points

Note The following APs are not supported:

- Cisco Catalyst 9136 Access Points
- Cisco Catalyst 9166 Series Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9162 Series Access Points

Table 3: Image Types and Supported APs in Cisco Embedded Wireless Controller on Catalyst Access Points

Image Type	Supported APs
ap1g4	Cisco Aironet 1810 Series Cisco Aironet 1830 Series Cisco Aironet 1850 Series
ap1g5	Cisco Aironet 1815i Cisco Aironet 1815w Cisco Aironet 1540 Series Cisco Aironet 1850 Series
ap1g6	Cisco Catalyst 9117 Series
ap1g6a	Cisco Catalyst 9130 Cisco Catalyst 9124AXE/I/D
ap1g7	Cisco Catalyst 9115 Series Cisco Catalyst 9120 Series
ap1g8	Cisco Catalyst 9105 Series
ap3g3	Cisco Aironet 2800 Series Cisco Aironet 3800 Series Cisco Aironet 4800 Series Cisco Aironet 1560 Series Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points Cisco 6300 Series Embedded Services Access Points

Maximum APs and Clients Supported

Table 4: Scale Supported in Cisco EWC Network

Primary AP Model	Maximum APs Supported	Maximum Clients Supported
Cisco Catalyst 9105 AWI	50	1000
Cisco Catalyst 9115 Series	50	1000
Cisco Catalyst 9117 Series	50	1000
Cisco Catalyst 9120 Series	100	2000
Cisco Catalyst 9124AXE/I/D	100	2000
Cisco Catalyst 9130	100	2000

Note If 25 to 100 APs have joined the EWC network, the maximum clients on the EWC internal AP is limited to 20.

Compatibility Matrix

The following table provides software compatibility information:

Table 5: Compatibility Information

Cisco Embedded Wireless Controller on Catalyst Access Points	Cisco ISE	Cisco CMX	Cisco DNA Center
Dublin 17.10.x	3.0 2.7 2.6 2.4 2.3	10.6.3 10.6.2 10.6 10.5.1	See Cisco DNA Center Compatibility Information

Supported Browsers and Operating Systems for Web UI

Note The following list of Supported Browsers and Operating Systems is not comprehensive at the time of writing this document and the behavior of various browser for accessing the GUI of the EWC is as listed below.

Table 6: Supported Browsers and Operating Systems

Browser	Version	Operating System	Status	Workaround
Google Chrome	77.0.3865.120	macOS Mojave Version 10.14.6	Works	Proceed through the browser warning.
Safari	13.0.2 (14608.2.40.1.3)	macOS Mojave Version 10.14.6	Works	Proceed through the browser warning.
Mozilla Firefox	69.0.1	macOS Mojave Version 10.14.6	Works only if exception is added.	Set the exception.
Mozilla Firefox	69.0.3	macOS Mojave Version 10.14.6	Works only if exception is added.	Set the exception.
Google Chrome	77.0.3865.90	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Microsoft Edge	44.18362.267.0	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	68.0.2	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	69.0.3	Windows 10 Version 1903 (OS Build 18362.267)	Works only if exception is added.	Set the exception.
Google Chrome	78.0.3904.108	macOS Catalina 10.15.1	Does not work	NA

Before You Upgrade

The following Remote Procedure Call (RPCs) should be used for Cisco Catalyst 9800 Series Wireless Controller and Cisco Embedded Wireless Controller:

- Cisco Catalyst 9800 Series Wireless Controller: Use **ewlc-wncd-stats** within *Cisco-IOS-XE-wireless-ap-global-oper*.

- Cisco Embedded Wireless Controller: Use **ewlc-wncd-stats** within *Cisco-IOS-XE-wireless-access-point-oper*.

Upgrading the Controller Software

This section covers the various aspects of upgrading the controller software.

Note Before converting from CAPWAP to embedded wireless controller (EWC), ensure that you upgrade the corresponding AP with the CAPWAP image in Cisco AireOS Release 8.10.105.0. If this upgrade is not performed, the conversion will fail.

Finding the Software Version

The following table lists the Cisco IOS XE 17.10.x software for Cisco Embedded Wireless Controller on Catalyst Access Points.

Choose the appropriate AP software based on the following:

- Cisco Embedded Wireless Controller on Catalyst Access Points software to be used for converting the AP from an unified wireless network CAPWAP lightweight AP to a Cisco Embedded Wireless Controller on Catalyst Access Points-capable AP (primary AP)
- AP software image bundle to be used either for upgrading the Cisco Embedded Wireless Controller on Catalyst Access Points software on the primary AP or for updating the software on the subordinate APs or both

Prior to ordering Cisco APs, see the corresponding ordering guide for your Catalyst or Aironet access point.

Table 7: Cisco Embedded Wireless Controller on Catalyst Access Points Software

Primary AP	AP Software for Conversion from CAPWAP to Cisco EWC	AP Software Image Bundle for Upgrade	AP Software in the Bundle
Cisco Catalyst 9115 Series	C9800-AP-universalk9.17.10.01.zip	C9800-AP-universalk9.17.10.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.10.01.zip	C9800-AP-universalk9.17.10.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.10.01.zip	C9800-AP-universalk9.17.10.01.zip	ap1g7
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.10.01.zip	C9800-AP-universalk9.17.10.01.zip	ap1g6a
Cisco Catalyst 9130	C9800-AP-universalk9.17.10.01.zip	C9800-AP-universalk9.17.10.01.zip	ap1g6a

Supported Access Point Channels and Maximum Power Settings

Supported access point channels and maximum power settings on Cisco APs are compliant with the regulatory specifications of channels, maximum power levels, and antenna gains of every country in which the access points are sold. For more information about the supported access point transmission values in Cisco IOS XE software releases, see the *Detailed Channels and Maximum Power Settings* document at https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-technical-reference-list.html.

For information about Cisco Wireless software releases that support specific Cisco AP modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

Guidelines and Restrictions

Internet Group Management Protocol (IGMP)v3 is not supported on Cisco Aironet Wave 2 APs.

Embedded Wireless Controller SNMP configuration is supported in DNAC.

High memory usage on AP running Embedded Wireless Controller. Enabling **crash kernel** on the AP consumes additional memory on the AP. Hence, if **crash kernel** is enabled, the overall memory usage of the device will increase and will impact the scale numbers. On Cisco Catalyst 9130 Access Points, the memory consumption is a high of 128 MB.

During the EWC HA pair selection, after a power outage, the standby AP fails to come up in the new EWC HA pair. Another EWC capable AP becomes the standby AP and fails to come up as well. To avoid this situation, ensure that the same IP address is enforced on the active or standby APs during HA pair selection.

Interoperability with Clients

This section describes the interoperability of the controller software with client devices.

The following table describes the configurations used for testing client devices.

Table 8: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Dublin 17.10.x

Hardware or Software Parameter	Hardware or Software Type
Access Points	• Cisco Aironet Series Access Points • 1540 • 1560 • 1815i • 1815w • 1830 • 1840 • 1850 • 2800 • 3800 • 4800 • Cisco Catalyst 9105AX Access Points • Cisco Catalyst 9115AX Access Points • Cisco Catalyst 9117AX Access Points • Cisco Catalyst 9120AX Access Points • Cisco Catalyst 9124AXE/I/D Access Points • Cisco Catalyst 9130AX Access Points
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS), WPA3.
Cisco ISE	See Compatibility Matrix, on page 6.
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

The following table lists the client types on which the tests were conducted. Client types included laptops, hand-held devices, phones, and printers.

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats that are listed as Open in a prior release are carried forward to the next release as either Open or Resolved.

Note All incremental releases will cover fixes from the current release.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click the corresponding identifier.

Open Caveats for Cisco IOS XE 17.10.1

Caveat ID	Description
CSCwc99359	Rogue rule delete classification configuration is not working.
CSCwd02898	Cisco Catalyst 9300 Series Switch is not flushing remote MAC address after roaming to a local AP.
CSCwd04571	Memory leak is observed (in wncd process) when under load.
CSCwd05689	Cisco Catalyst 9124AXI AP: RSSI is 7-8dbm weaker at a distance compared to other AP models.
CSCwd10570	Cisco Catalyst 9130 AP: Beacon is showing incorrect datarates - different rates for same slot on different BSSIDs.
CSCwd30828	Cisco Catalyst 9120 AP: Kernel panic crash is observed.
CSCwd33981	Kernel panic crash with PC (at cpuidle_not_available).
CSCwd39599	Cisco Catalyst 9117 AP reloads unexpectedly with PC (at dst_release+0x18/0x90).
CSCwd39606	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic (at dp_rx_wbm_err_process).
CSCwd41108	Cisco Catalyst 9130AXE AP: Dart connectors are stuck at channel 36.

Caveat ID	Description
CSCwd45079	FlexConnect AP performs Extensible Authentication Protocol (EAP) identity request after completing 4-way handshake.
CSCwd47741	Controller is failing to update Dynamic Channel Assignment (DCA) channels.
CSCwd51523	Cisco Catalyst 9120 AP: Numerous power supply module (PSM) watchdog crashes are observed.
CSCwb51757	High channel utilization is observed on 5GHz radio with 40MHz.
CSCwd04025	APs associated with the controller are showing interface "*Half duplex*".
CSCwd06018	802.11r reauthentication failed due to '*Invalid PMKID*' while doing inter-WNCD roaming.
CSCwd06122	AP join issues are observed due to stale client entries.
CSCwd12754	CAPWAP wireless traffic is getting the same Security Group Tag (SGT) tag as the corresponding incoming wired traffic.
CSCwd21996	Cisco Catalyst 9120 AP: CleanAir sensor is crashing.
CSCwd23681	Controller fails to update AP config with error "*% Error: no ap_name exists*".
CSCwd25931	Wireless client is not receiving IPv6 RA from wired - FlexConnect Local DHCP.
CSCwd32900	AP is dropping Extensible Authentication Protocol over LAN (EAPOL) message 4 during 4-way handshake.
CSCwd34890	Clients are getting deauthenticated imediately after getting IP address in LWA + Local Switching + Central Authentication scenario.
CSCwd36552	Cisco Catalyst 9120 AP: Kernel panic crash is observed.
CSCwd37706	Cisco Catalyst 9130 AP doesn't respond to reassociation request during client roaming.
CSCwd40731	AP reloads due to kernel panic.
CSCwd46091	Cisco Catalyst 9105AXI AP is requesting 30 watts of power, instead of 15.4 watts.

Caveat ID	Description
CSCwd46252	Controller shows AP as having no neighbors. This issue is caused when power level is set to maximum.
CSCwd47286	Capability annotation is missing for some xpaths in yaml files.
CSCwd49686	AP doesnt not save syslog message before crash.
CSCwd52938	Wired clients behind a workgroup bridge (WGB) are not getting IP address in anchor WLAN.
CSCwd40914	Cisco Catalyst 9120 AP is not forwarding EAP packet downstream to client.

Resolved Caveats for Cisco IOS XE 17.10.1

Caveat ID	Description
CSCwb52755	Apple and Android fast transition capable client is unable to authenticate with Identity Preshared Key (iPSK) profile.
CSCwb69531	Controller initiates Extensible Authentication Protocol over LAN (EAPOL) retries for the client in RUN state.
CSCwb73461	Radio Resource Management (RRM) core generated @ group_dpc_compute_6GHz.
CSCwc01644	CoS AP is using native VLAN instead of VLAN used in the policy profile.
CSCwc05366	Wireless AAA dynamic VLAN assignment: Wireless clients cannot reach each other.
CSCwc14629	Web UI is taking long time to show initial page.
CSCwc15533	Continuous wncmgrd CPU HOG traceback is observed with scale Flexible NetFlow (FNF) mapping to policy profile.
CSCwc15944	Multicast data is not sent to clients; some APs are unable to join.
CSCwc22468	Client traffic fails when client roams between APs with dot11r to dot11i transition.
CSCwc32226	Zebra RF guns gets deleted from controller randomly due to reason: CO_CLIENT_DELETE_REASON_ZONE_CHANGE.

Caveat ID	Description
CSCwc42784	Client fails to connect when protocol based QoS is configured.
CSCwc55982	Stale entry is observed in the show wireless device tracking database ip command output after client deletion.
CSCwc57227	Wireless Network Control Daemon (WNCd) crash is observed.
CSCwc59518	Cisco Catalyst 9800-80 controller crashes with the reason: Critical process wncd fault on rp_0_3 (rc=134).
CSCwc79394	WNCd is going high upto 99% on tbl(WNCD_DB/tbl_client_wsa_info).
CSCwd08678	Clients are not deleted from the controller. They remain in the RUN state even after session-timeout.
CSCwb47040	Controller is not updating RFID location properly.
CSCwb58100	Unable to map SSID with spaces in it on an attribute list.
CSCwb64761	Controller is discarding location updates from RFID tags.
CSCwb67450	Add **show process cpu platform sorted** command is needed in **show tech wireless** command group.
CSCwb78191	AAA VLAN override is not working in iPSK authentication + anchor WLAN configuration.
CSCwb93067	Cisco Catalyst 9800-CL Controller: WNCd crash is observed during switch integrated security features (SISF) routines.
CSCwb93513	Stale client entries are not deleted and is stuck on device-tracking database.
CSCwc38828	Invalid TDL pointers caused WNCd crash.
CSCwc41358	MAC filtering: WLAN profile column displays the WLAN name + description.
CSCwc57836	Restore configuration by HTTP mode does not work on Cisco Embedded Wireless Controller.
CSCwc72047	APs are operating on disabled RF profile channels.
CSCwc76905	SISF crash is observed when handling DHCP messages.

Caveat ID	Description
CSCwd00711	When Wi-Fi Protected Access (WPA) 3 and Opportunistic Wireless Encryption (OWE) transition are enabled, non-WPA3 clients are getting network access in webauth-pending state.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, visit the Cisco TAC website at:

https://www.cisco.com/en/US/support/index.html

Go to **Product Support** and select your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information about the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE 16 is available at:

https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

All the support documentation for Cisco Catalyst 9100 Access Points are available at: https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/tsd-products-support-series-home.html

Cisco Validated Designs documents are available at:

https://www.cisco.com/go/designzone

Cisco Embedded Wireless Controller on Catalyst Access Points

For support information, see the following documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Embedded Wireless Controller on Catalyst Access Points Online Help
- Cisco Embedded Wireless Controller on Catalyst Access Points Software Configuration Guide
- Cisco Embedded Wireless Controller on Catalyst Access Points Command Reference Guide

Installation guides for Catalyst Access Points are available at:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/products-installation-guides-list.html

For all Cisco Wireless Controller software-related documentation, see:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless APs and controllers:

https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco DNA Center

Cisco DNA Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.