MobileIron Cloud 75 Release Notes

January 22, 2021

For complete product documentation, see:
MobileIron Cloud Product Documentation Home Page

Contents

About MobileIron Cloud

A modern approach to mobile security, MobileIron Cloud provides unified endpoint management (UEM) solutions in a highly scalable, secure, and easy to update infrastructure that supports millions of devices around the world.

- Instant updates: Get automatic software and security updates and access to the new features the moment they become available.
- On-demand scalability: Scale your deployment as business needs change without having to worry about capacity planning.
- Minimize hardware costs: By eliminating the need to maintain on-prem hardware, cloud-based services require zero footprint to manage.
- High uptime and high availability: See our monthly platform and infrastructure services uptime.
- Maximize existing investments: Re-allocate IT resources from hardware maintenance to more strategic tasks that add value to the business.

New features summary

This section provides summaries of new features developed for the current release of MobileIron Cloud. Product Documentation describing these features is available in the *MobileIron Cloud Administrator Guide*. For more information, see the specific sections provided for each of these features, when available.

MobileIron Threat Defense features

MobileIron Threat Defense protects managed devices from mobile threats and vulnerabilities affecting device, network, and applications. For information on MobileIron Threat Defense-related features, as applicable for the current release, visit MobileIron Product Documentation and click Threat Defense Cloud.

NOTE: Each version of the MobileIron Threat Defense Solution guide contains all MobileIron Threat Defense features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, MobileIron releases new versions of the MobileIron Threat Defense guide as the features become fully available.

iOS, macOS, tvOS

- **Content Caching service:** Configure content-caching service for macOS devices to enable local copies of the App Store software and enable connected clients for faster software and app downloads.

- **Encrypted DNS configuration:** Configure Encrypted DNS that will allow you to enhance security without needing to configure VPN.
- **Shared iPad enhancements**
  - **Select distribution channel for the iOS Restrictions configuration:** Select either the Device Channel or the User Channel during the distribution of the iOS Restriction configuration configuration to Shared iPads. This is useful to distribute separate configurations and enforce restrictions that are applicable only to the device or the user channel.
  - **Report user list:** In the device details page of a Shared iPad, click the **Users** tab to view the list of resident users on the device and their details (such as Managed Apple ID, Data Available in bytes, Data Used in bytes, Has Data to Sync to Cloud).
  - **Restricted configurations:** MobileIron Cloud now restricts certain configurations, such as Passcode, for Shared iPads as Apple does not support them. Such configurations are no longer pushed to the devices.
  - **Restriction on changing the Managed Apple ID:** MobileIron Cloud now restricts administrators from changing the Managed Apple ID of resident user(s) who were logged in to the Shared iPad in the past along with the currently logged in users.
- **Associated and excluded domains:** In the Per-app VPN and in the MobileIron Tunnel configurations, specify associated and excluded domains to be considered for association or exclusion from the per-app VPN and tunnel server connections.
- **Device Enrollment Full Sync:** In the **Device Enrollment** **> Actions** menu, administrators can initiate full sync. It may take some time to be completed. After the sync is completed, you can view the information in the Last Sync column.
- **Updates to iReg pages:** The iReg pages are updated with new mobile-friendly layout and content.
- **Export eSIM ID to CSV:** The equipment identifier (EID) shows up as an iOS attribute when a device list is exported to spreadsheet (CSV) format.

Android

- **Relinquish ownership of devices in Work Profile on Company Owned Device mode:** When viewing the specific device details, you can relinquish ownership of Android devices in Work Profile on Company Owned Device mode. Relinquishing ownership of a device in Work Profile mode removes the work profile and retires the device from MobileIron Cloud, without affecting personal apps and data. The device user can then use the device a personal device, with full access to all device controls and settings.
- **Suspend personal apps when device falls out of compliance:** Administrators can configure policies offering quarantine actions, such as the Compromised Devices policy, the Custom Policy, and the Allowed Apps policy, to suspend apps on the personal side of the quarantined device to indicate that device user needs to address the compliance issues on the device to make it functional. Supported on

Android 11+ devices provisioned as a Work Profile on Company Owned Device.

- **Suspend personal apps when work profile turned off for specified time:** Administrators can configure the Lockdown & Kiosk: Android enterprise configuration to set a maximum time that the device user can turn off the work profile before MobileIron Cloud suspends personal apps on the device. The device user sees a message prompting to turn on the work profile to enable suspended apps. Available for Android 11+ devices in Work Profile on Company Owned Device.
- **Disable the camera within the work profile:** Administrators can configure the Lockdown & Kiosk: Android enterprise configuration to disable the camera within the work profile. Available for Android 11+ devices in Work Profile on Company Owned Device.
- **Disable screen capture on personal side of device:** Administrators can configure the Lockdown & Kiosk: Android enterprise configuration to disable screen captures. When selected, screen capture is disabled on the personal side of the device. Available for Android 11+ devices.

Audit Trails

- **Personal Recovery Key (PRK) entries:** Administrators can view Audit Trails log entries for the PRK activities by navigating to **Dashboard > Audit Trails.**
- **Expanded view user-interface modified**: Enhanced expanded view user interface as follows:
  - Name column renamed to **Performed on**.
  - Type and category columns hidden from the default view. Retain using quick search or filter function.
  - Icons represent different categories
  - More logical column order.
- **Details column added**: The details column in expanded view provides narrative details for the following audit logs:
  - Admin Access Portal
  - Configuration
  - User group
  - Policy
  - App
  - App configuration
  - Device management

  For more information, see the *Expanded View* section under Dashboard.
- **The AAD sync updates in Audit Trails**: Audit trails now audits AAD User/Group sync up and processing details. You can view manual and polaris based sync activities such as:

- Sync summary
- Adding AAD
- Editing AAD
- Deleting AAD

Other features

- **Microsoft Intune Device Compliance Support added:** MobileIron Cloud now supports Microsoft Intune device compliance. Organizations can update the device compliance status in the Microsoft Azure Active Directory (AAD.) Using conditional access from AAD, if the device is non-compliant, administrators can block the device from accessing apps. By connecting Cloud to Microsoft Azure, administrators will be able to use the device compliance status of MobileIron's managed devices for conditional access to Microsoft 365 apps. Microsoft Intune device compliance requires a **license** and is applicable to iOS and Android devices.

  In Cloud, administrators will see the following changes:

  - The Admin page has a new menu item in the left navigational pane > Microsoft Azure > Device Compliance for iOS & Android. There are new fields to assist with the reporting of device compliance status to Microsoft Azure.
  - Administrators can direct device users to a specific Enrollment URL and Remediation URL. If a URL is not provided, a default URL is automatically provided by Cloud.
  - Once the setup is completed, Cloud is connected to Microsoft Azure.
  - A Partner Device Compliance policy (under Configurations) needs to be created and applied to the device group that reports the device compliance to Azure.
  - In the Device Details page, four new fields have been added:
    - Azure Device Identifier
    - Azure Device Compliance Status
    - Azure Client Status Code
    - Azure Device Compliance Report Time
  - The ability to de-provision the Azure account has been added.
  - All activity of adding, editing, and deactivating an account are recorded in the Logs.

  For more information, see **Azure Tenant**.

- **View configurations across all or multiple space devices:** In the **Configurations** page, select multiple spaces from the drop-down list. When you hover on the displayed configurations, a pop-up window with a list of spaces are displayed. You can click on a space to display the configuration details page.

- **Exporting configuration details:** In the **Configurations** page, export details of all configurations from the selected spaces.
- **Updates in the Admin > Roles Management page:**
  - Additional permissions added in the **Device Actions** and **LDAP Management** categories.
  - New space-specific permission categories added as **Configurations** and **Device Groups**.
- **Updated role names and descriptions:**
  - Renamed "LDAP User Registration and Invite" to "LDAP User Import and Invite."
  - Renamed "Create/Cancel Wipe Request" to "Send/Cancel Wipe."
  - Updates to the descriptions of the Manage MobileIron Access Integration, Send/Cancel Wipe, Edit Microsoft Graph, and View Microsoft Graph roles.
- **Updated list of device actions:** Alphabetized the list of device actions in the following sections:
  - Devices > device list page > Actions.
  - Devices > device details page > Actions (ellipsis menu).
- **Limit distribution of apps:** Apps that do not meet the version specified in the Minimum OS Version Required field are not displayed in Apps@Work catalog. Therefore, such apps are not available to be distributed to the devices.
- **User Work Schedule setting:** Administrators can configure a user work schedule that blocks all communication from MobileIron Sentry to managed devices during the prescribed non-working hours. Useful for locales with Right-to-Disconnect laws.
- **Consolidated rule group fields and additional operators:** Administrators have avail of consolidated rule-group fields and additional operations here in MobileIron Cloud:
  - Devices -> Device Groups -> +Add
  - Users -> User Groups -> +Add
  - Devices -> Advanced Search
  - Users -> Advanced Search
  - Admin -> Spaces -> Manage -> Create New Space
  - Apps -> Distribution Filters
  - Apps -> [choose an app] -> Distribution -> Edit -> + Add Distribution Filter
  - Policies -> +Add -> Custom Policy
  - Admin -> Certificate Management -> Issued Certificates -> Advanced Search

Support and compatibility

The information in this section includes the components MobileIron supports with this product.

NOTE: This information is current at the time of this release. For MobileIron product versions released after this release, see that product version's release notes for the most current support and compatibility information.

Support policy

MobileIron defines supported and compatible as follows:

Supported product versions	The functionality of the product and version with currently supported releases was systematically tested as part of the current release and, therefore, will be supported.
Compatible product versions	The functionality of the product and version with currently supported releases has not been systematically tested as part of the current release, and therefore not supported. Based on previous testing (if applicable), the product and version is expected to function with currently supported releases.

MobileIron Cloud releases and announcements

For details on MobileIron Cloud, see:

- Release announcements and upgrade schedules
- End of support announcements

MobileIron Cloud supported and compatible table

This version of MobileIron Cloud is supported and compatible with the following product versions:

Product	Supported	Compatible
Cloud Connector	75	59 through the most recently released version as supported by MobileIron.
LDAP	**Microsoft Active Directory** Windows Server 2016	Not Applicable
Standalone Sentry	9.9.0	9.4.0 - 9.8.1, 9.8.5 (for Email+ Notification Service)

Product	Supported	Compatible
	NOTE: The new Email+ Notification Service requires Standalone Sentry. Refer to Email+ VIP Notifications for iOS 13 and above for information on the Standalone Sentry version required for this feature. An upgrade from Standalone Sentry 9.8.0 to the Sentry version of Email+ Notification Service is not supported.	
MobileIron Access	R44	Not applicable since only the latest version is available to all customers.
Android	**Supported**	**Compatible**
Android	9, 11	5 - 7.1
MobileIron Go	75	61 - 74
AppStation	70	62
Tunnel (Android native, Android enterprise, and Samsung Knox Workspace)	4.5.0	4.1.0 - 4.4.0
Email+ for (Android AppConnect and Android enterprise)	• 2.19.0.0 (Android AppConnect) • 3.8.0 (Android enterprise)	• 2.2.0.0 - 2.18.0.0 • 3.0.0 - 3.7.0
Docs@Work (Android AppConnect and Android enterprise)	2.13.0	2.0.0 - 2.12.0
Web@Work (Android AppConnect)	2.5.0	2.1.0 - 2.4.0
iOS	**Supported**	**Compatible**

Product	Supported	Compatible
iOS and iPad OS	12 - 14	11
MobileIron Go	75	5.3.0 - 5.5.0
AppStation	1.3.0	All previous released versions
Tunnel	4.1.0	3.0.0 - 4.0.0
Email+	3.16.0	2.6.0 - 3.15.0
Docs@Work	2.16.0	2.2.0 - 2.15.0
Web@Work	2.12.0	2.2.0 - 2.11.1
macOS	**Supported**	**Compatible**
macOS	11	10.12 - 10.15
Tunnel	4.1.0	4.0.1
Mobile@Work	1.74.0, 1.75.0	1.73.0
Windows	**Supported**	**Compatible**
Windows	Windows 10 Pro, Windows 10 Enterprise (versions 1909, 2004, 20H2) NOTE: Only apps deployed from the Microsoft Store through AAD will deploy.	• Windows 10 Pro, Windows 10 Enterprise (versions 1703, 1709, 1809, 1903) • Windows HoloLens (versions 1701, 1803)
Apps@Work	9.6.0.256	Not Applicable (All listed versions are tested and supported)
Tunnel	1.2.3	1.0.0 - 1.2.2

Browser support

This version of MobileIron Cloud has the following browser support:

Browser (minimum version required)	Supported	Compatible
Chrome	87	85
83	80	80
Safari	13.1	13.1

Note: Browsers on mobile devices (such as phones and tablets) do not support MobileIron Cloud administration user interface (UI). MobileIron does its best to remain compatible.

Language support

MobileIron Cloud Administrator Guide is available in the following languages and locales:

- Chinese (Simplified)
- Chinese (Traditional)
- English (United Kingdom)
- English (United States)
- Finnish
- French (France)
- German (Germany)
- Italian (Italy)
- Japanese
- Korean
- Portuguese (Brazil)
- Spanish (Latin America)
- Spanish (Spain)

MobileIron Cloud will serve locales other than those whose language is English with the most recently translated version of the *MobileIron Cloud Administrator Guide*.

Resolved issues

This section describes the resolved issues fixed in MobileIron Cloud 75.

For resolved issues provided in previous releases, see the "Resolved issues" sections in the release notes for those releases, available in MobileIron Cloud Product Documentation.

- **AW-53386:** The left navigation pane now appears for delegated space administrators lacking the System Management role.
- **AW-53005:** Previously, the device group details Apps tab (Devices > Device Groups > click device group name > Apps) appeared despite the associated feature not having been enabled. This issue has been fixed.
- **AW-52973:** MobileIron Cloud now reflects the correct operating system (OS) version for MAM-only registered devices that have had an OS upgrade.

- **AW-52843:** The Clear Restriction and Reinstall iOS System Apps device actions no longer fail on shared iPad devices.
- **AW-52786:** The Per-app VPN configuration is now applicable for macOS, and the macOS icon appears on the Create Per-App VPN Configuration page to indicate that support.
- **AW-52728:** MobileIron Cloud now successfully generates device reports that failed previously due to removal of code references.
- **AW-52727:** MobileIron Cloud now generates scheduled reports that existed before the MobileIron Cloud 71 upgrade.
- **AW-52615:** Sending a message to filtered users now sends the message to users specified on the filter, instead of sending it to all users with active devices on the tenant.
- **AW-52581:** The "Send Install/Update Request" for an iOS app no longer fails if the app is distributed to the custom user groups consisting of more than 1024 users and the intersection of the app distribution and the request distribution results in more than 1024 users.
- **AW-52357:** Admin -> Spaces now paginates the display of a space's associated configurations and policies when the number of configurations and policies exceeds 500.
  AW-52337: Translations on the Vanity Host Configuration page are now correct.
- **AW-52271:** MobileIron Cloud now successfully sends install or update requests to devices for iOS apps in custom spaces.
- **AW-52249:** MobileIron Cloud now supports app uploads of 4 GB.
- **AW-52141:** MobileIron Cloud now exports daily audit trail data in proper order and scope, rather than mixing in the last fifteen days of data.
- **AW-52126:** This release of MobileIron Cloud properly enforces the 500 row limit on all API calls by limiting the returns of some previously ungoverned calls.
- **AW-51955:** MobileIron Cloud now successfully performs Azure Active Directory syncs when an administrator has removed a user association from the multiple child groups which are part of a single parent group.
- **AW-51623:** Previously, the Quick Search showed no results when the refresh limit was reached in the App Inventory page. This issue has been fixed with the refresh limit increased from 3 to 30 times per minute.
- **AW-51509:** MobileIron Cloud now properly removes the Volume Purchase Plan license association when Apple returns error code 9619 after removing the mobile device management profile on a device.
- **AW-51376:** Creating a device group using single digit to double digit values with the conditional operator "is in range" works properly in this release. For example, "OS is in range 8 to 13.6" works properly, whereas previous to this release, only "OS is in range 08 to 13.6" worked properly.
- **AW-51334:** The App Dashboard's Unmanaged App chart for iOS apps no longer contains data inconsistencies.

- **AW-51218:** Newly released Apple device model names now appear in the Cloud administrative portal user interface.
- **AW-51171:** Exporting a list of DEP devices to a .CSV file now works as expected even when there are more than 10,000 devices on the device list.
- **AW-51065:** Audit Trails now capture logs for the scripting feature.
- **AW-50834:** MobileIron Cloud now logs restarting of Windows devices as "reboot," with two statuses, "sending" and "success."
- **AW-50342:** The Devices -> Devices -> Specific MacOS Device Details -> Configurations user interface now displays an "Error" status that links to an option to retry the installation of configurations pushed over the USER channel that failed to install on macOS devices.
- **AW-48934:** Pushing the Mobile@Work app with the complete user onboarding setup to an already DEP registered device no longer triggers the user onboarding kiosk mode on the device.
- **AW-48780:** MobileIron Cloud now successfully pushes the Mobile@Work for macOS app to the device upon the first check-in because it sets the priority of the Mobile@Work for macOS app to high.
- **AW-47099:** When installing a specific version of an operating system (OS) update for iOS devices, you must select an OS version that is available for the device. Otherwise, MobileIron Cloud ignores the OS update request for the device.
- **AW-45137:** During in-app registration, MobileIron Cloud no longer resets the registration date when the client is installed after iReg enrollment.
- **AW-40197:** Using a colon (":") in the password for a MobileIron Cloud user no longer causes Apple Device Enrollment Program (DEP) registrations to fail.
- **AW-18642:** MobileIron Cloud now displays the exact time an administrator ran the reports listed on the Reports page.

Known issues

This section describes the known issues found in the MobileIron Cloud 75.

For known issues found in previous releases, see the "Known issues" sections in the release notes for those releases, available in MobileIron Cloud Product Documentation.

- **AW-54253:** The device search API, /api/v1/device, and user search API, /api/v1/device, with the UID filter performs a case sensitive match on the UID, which may yield unexpected results.
  For example, given a user UID of TestNick22@mobileiron.com:
  - `/api/v1/device?q=&dmPartitionId=29807&fq=UID+EQ+testNick22@mobileiron.com` yields no results.

- `/api/v1/device?q=&dmPartitionId=29807&fq=UID+EQ+TestNick22@mobileiron.com` yields one device.

Workaround: Use the email address filter because the email address match is already case insensitive.

- **AW-54189:** MobileIron Cloud adds duplicate records to the devices report for devices whose device details show records with both the Allow and Block states on the Sentry tab.
- **AW-54116:** MobileIron Cloud fails to update the associated Volume Purchase Plan (VPP) license during a VPP sync if the sync involves updating the license type from DEVICE to USER.
- **AW-54115:** MobileIron Cloud fails to update the status of disassociated Volume Purchase Plan (VPP) licenses during a VPP sync.
- **AW-54077:** The Dashboard -> Apps -> In-House apps charts incorrectly represent updated side-loaded in-house apps as public apps. The In-House apps pie chart also reflects a count mismatch between the number of devices reflected on the pie chart label and the number of devices encountered after drilling down to view the slice.
- **AW-53995:** MobileIron Cloud fails to create users with display names longer than 128 characters, which causes LDAP and Azure Active Directory sync errors for any such users.
- **AW-53989:** Users cannot log in after reboot to the MobileIron Cloud Connector installed from an Amazon Machine Image (AMI). Logging in after reboot works as expected with ISO 35.
- **AW-53926:** Sorting of users is not working as expected in dynamically managed user group details.
- **AW-53874:** Some users cannot install Android apps on their devices after they register on MobileIron Cloud an Android Enterprise device, unregister that Android Enterprise device, and then re-register the Android Enterprise device using the same account.
- **AW-53853:** The event "LDAP Sync User account(s) updated" on Dashboard -> Notifications presents a clear notification icon when there is no need for the icon because MobileIron Cloud has already cleared the notification internally, but fails to update the user interface accordingly.
- **AW-53852:** The count of unmanaged iOS apps that appears in the MobileIron Cloud Apps dashboard only captures the number of apps of app type UNMANAGED, but should also include in the total count the number of apps of app type NOT_APPLICABLE.
- **AW-53832:** MobileIron Cloud cannot successfully save the Android APN Settings configuration when an administrator creates it from a German language browser.
- **AW-53818:** MobileIron Cloud displays the Notifications menu heading in English in the new look user interface, despite the browser language being other than English.
- **AW-53817:** The Update Account API (PUT /api/v1/account) resets some of the user info when the call lacks values for mandatory parameters.
- **AW-53665:** MobileIron Cloud reports, and the MobileIron Cloud devices page, display the model identifier instead of the pretty model identifier for MacBook devices.

- **AW-53651:** For Windows devices, MobileIron Cloud does not report device compliance status as "Yes" to Microsoft Azure when the device is compliant after registration, causing Microsoft Azure to display "N/A" for device compliance status.
- **AW-53610:** Microsoft store searches are currently unavailable in MobileIron Cloud due to API changes or downtime from Microsoft.
- **AW-53585:** The App Configurations tabs on the Docs@Work and Web@Work app details pages do display the “AppConnect Custom Configuration” tables.
- **AW-53563:** The following advanced device search attributes for advanced search option, "AZURE_DEVICE_COMPLIANCE_STATUS," attribute do not work correctly:
  - AZURE_DEVICE_COMPLIANCE_STATUS EQ 'notCompliant'
  - AZURE_DEVICE_COMPLIANCE_STATUS CONTAINS 'not'
  - AZURE_DEVICE_COMPLIANCE_STATUS CONTAINS 'notCompliant'
  - AZURE_DEVICE_COMPLIANCE_STATUS STARTS_WITH 'notCompliant'

  The following attribute works as designed:
  AZURE_DEVICE_COMPLIANCE_STATUS NEQ 'notCompliant'
- **AW-53385:** Audit trails is not capturing all of the Azure Active Directory (AAD) activity description.
- **AW-53343:** When a device is enabled for Azure Active Directory (AAD) compliance status reporting in MobileIron Cloud, and the device has not registered with AAD, device is in "interaction required" state. This indicates that client still needs to register with AAD. But the server displays Azure client status as "N/A" instead of "interaction required." Once the device registers with AAD and reports the compliance status to server, the status changes to "success."
- **AW-53338:** There are some cosmetic issues on iPod devices related to button colors, animations, and element positioning that manifest during iReg registration of iPod devices.
- **AW-53291:** MobileIron Cloud does not apply the Advanced Search filter in the "Users" tab when the administrator navigates from the "User Groups" tab by clicking the user count link of any user group.
- **AW-53169:** MobileIron Cloud's Windows Store search does not return applications that only run on HoloLens devices when the search criteria is the name of a HoloLens-only application name.
- **AW-53026:** There are some text overlap, button color, and element positioning issues on some iOS devices during the Terms of Service stage of registration.
- **AW-52901:** The MobileIron Tunnel configuration for iOS and macOS works only with TCP_ANY option. IP_ANY is not supported. If the administrator selects IP_ANY and saves the iOS or macOS configuration, the configuration defaults to the MobileIron Windows or Android configuration.
- **AW-52845:** The MobileIron Cloud audit trails feature does not capture script association changes for MIP archive apps.

- **AW-51354:** Changing and attempting to save any value on the Account Info page invokes a "Page not found" error message.

Limitations

This section describes the limitations found in the MobileIron Cloud 74

For limitations noted in previous releases, see the "Limitations" sections in the release notes for those releases, available in MobileIron Cloud Product Documentation

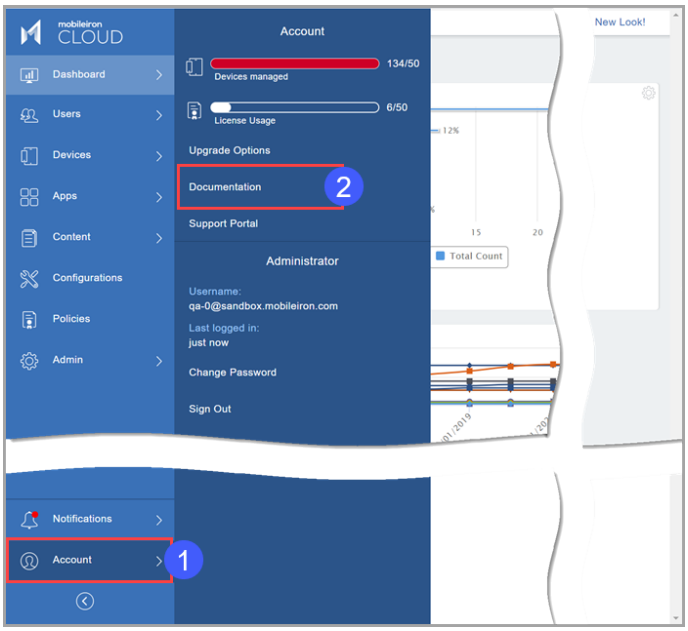
- **AW-53650:** Microsoft Azure Active Directory does not immediately remove the entry for a device that an administrator on MobileIron Cloud has retired and deleted. Microsoft has its own schedule to remove retired devices, usually 90 days.
- **AW-53072:** Some iOS apps appear in the returned MacStore list when an administrator is adding an app to the app catalog.
- **AW-52798:** The MobileIron Cloud Always On VPN Configuration does not work on shared iPads.
- **AW-52736:** The Network: Evaluate Connection setting in the MobileIron Cloud Encrypted DNS Settings configuration fails on iOS devices.

Documentation resources

MobileIron product documentation is available at the following locations:

- *MobileIron Cloud Administrator Guide*, *Release Notes*, and related documentation are available in the MobileIron Cloud Product Documentation.
- *MobileIron Cloud Administrator Guide* integrated within the Help link in the user interface, by clicking **Documentation** in the new user interface, or **Help** in the classic user interface:

  New user interface:



- **Classic user interface:**