MobileIron Cloud 76 Release Notes

March 3, 2021

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

Proprietary and Confidential | Do Not Distribute

Copyright © 2009 - 2021 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

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

- **Maximum character limit for "Terms of Service" header section**: Cloud 76 enforces a maximum length restriction to ensure better readability on single line headers.

- **New iOS 14.2+ restriction added** : New restriction, "**Allow NFC**" (supervised devices only), added to Device Management profile. For more information, see iOS Restrictions.
- **Support to add icons for in-house apps**: The administrator can now add new icons and replace the existing icons for in-house apps (iOS and macOS). For more information, see "**Adding an In-house app**" in the App Catalog section.
- **"Users" tab added to Device Details page**: The "**Users**" tab is added to the **Device Details** page, to view the list of users on macOS supervised devices. For more information, see "Displaying detailed device information" in the Devices section.
- **"Uninstall script" field added to MobileIron Packager (MIP) apps**: The uninstall script is run when the server detects an MIP app that is no longer distributed to the device.
- **Set priority for iOS restrictions**: In the MobileIron Cloud admin page, "**iOS Restrictions Configuration**" option is added in the "**Priority Settings for Restrictions Configuration**" section under Admin > Apple > Settings to enable priority settings for iOS restrictions. For more information, see **Priority Settings for Restrictions Configuration** in the Settings (Apple) section.
- **Support to provide authentication at DEP profile level**: The administrator can now perform **Edit Authentication** and **Assign Device Enrollment Device Attribute** actions for device enrollment profiles instead of device enrollment (MDM server). For more information, see "Managing multiple Device Enrollment profiles" in the Admin > Apple > Device Enrollment section.
- **Delete a user on shared iPad**: The administrator can now select and delete a user on a shared iPad. The delete user option frees up the allocated space which is no longer required.
- **"Clear passcode after User logout" option added**: Selecting the "**Clear passcode after User logout**" option in the "**Multi User secure sign-in**" section under Admin > Apple > Settings clears the device password when the user logs out from the Multi-user Secure Sign web clip. For more information, see **Multi-user Secure Sign-In** in the Settings (Apple) section.

Android

- **Display a message to the user to enable location settings**: This feature allows the administrators to optionally enable the ability to allow or disallow the use of location settings for Android 10+ and later devices provisioned as fully managed or work profile on company owned device if Wifi/MTD configuration is pushed. For more information, see Privacy.
- **Increased limit for bulk pre-enrollment uploads**: The limit for bulk pre-enrollment has increased to 5000 devices. This allows a larger configuration group that does not require configuration partners to breakdown orders into smaller groups. For more information, see Bulk Enrolling devices using CSV file upload.
- **Use variable substitution in the lock screen message**: Administrators can use variable substitution in the lock screen message, along with the status message. If a custom device or user attribute is not linked to register device or the user with which the device is registered and if these attributes are part of the

custom lock screen message then the entire message would be blank on the devices. For pre-defined attributes, navigate to **MobileIron Cloud** > **Admin** > **Attributes**. For more information on Attributes, see Admin > Attributes.

- **Domain substitution for shared device kiosk**: Option to enter the domain for shared device kiosk. If the domain suffix is missing, the system automatically appends the domain suffix to the username. For more information, see Lockdown & Kiosk: Android enterprise.

Windows

- **MobileIron Cloud now supports Direct Enrollment of Microsoft Windows devices**: Direct Enrollment of the Microsoft Windows devices is now possible with auto-discovery of MobileIron servers. Administrators can configure their DNS with the MobileIron service (such as authentication service) URL. This feature is only applicable for “Direct Enrollments”.
- **Support for Microsoft HoloLens 2 device**: MobileIron Cloud supports Microsoft HoloLens 2 devices. Administrators can now enroll, push configurations and policies, and unregister such devices.

Audit Trails

- **24-hour format only**: Starting with Cloud 76, the timestamp in the Performed At column will display in only 24-hour format.
- **Property values indexing**: Currently, when you perform a quick search, the whole string is indexed including the property names. Starting with Cloud 76, only property values are indexed. Users need not provide the details keys that are present under the Details column while performing a quick search.
- **Local time zone display in the Details column**: Starting with Cloud 76, the Details column will display the last logged in date and time in local time zone. Also, the functionality to search for date and time is now removed from the Details column.
- **LDAP Details available**: Starting with Cloud 76, the following details for LDAP activity are available in Audit Trails:
  - LDAP Server added
  - LDAP Server edited
  - LDAP Server deleted
  - LDAP Server Sync started
  - LDAP Server Sync failed
  - LDAP Server Sync completed

    - Deleting Admin LDAP entity
    - Modifying LDAP preferences
    - Uploading LDAP certificate

Other features

- **v3 certificates only**: Starting with Cloud 76, only v3 certificates are supported.
- **Use the MAM Only attribute to build device groups**: The MAM Only attribute is added to the device group rule builder in Cloud 76, enabling administrators, for example, to use the MAM Only attribute to group Android and iOS devices.
- **App Inventory permissions:** With this release, the administrator can create AppInventory custom role. Under Roles Management in the Admin tab, the **View** AppInventory permission can be created for the Space-Specific Role.
- **New Roles Management page options**: The following options are added in the Roles Management page:
    - Search option
    - Icons
    - Filter drop-down list
    - Type column
- **Configurations permissions:** The administrator can now specify the device configuration management permissions. Under Roles Management in the Admin tab, the following new Configuration permissions can be created for the Space-Specific Role:
    - View/Export Configs
    - Edit/Prioritize Configs
    - Add/Clone Configs
    - Delete Configs
- **Policies permissions:** The administrator can now specify the policy management permissions for the users. Under Roles Management in the Admin tab, the following new Policies permissions can be created for the Space-Specific Role:
    - View Policies
    - Add/Clone Policies
    - Edit/Prioritize Policies
    - Delete Policies
- **New columns are added to the Configurations page**: The following new columns are added to the Configurations page:

- Available - Number of devices that are actively checking in to the Cloud for which configuration is distributed.
- Installed - Displays the number of devices that have installed the configuration out of actively checking in devices.
- Pending - Displays the number of devices that are pending to install the configuration out of actively checking in devices.

- **Standardized operators for string, drop-down, number and Boolean attributes**: The operators for all the report templates and certificate management templates have standard operators. The operators of the following templates are standardized in this release:
  - Admin> Certificate Management> Issued Certificates> Advanced Search
  - Dashboard> Reports> Create Report
- **Search using display version or bundle version in App Inventory and Devices pages**: Starting with Cloud 76, both the App Inventory and Devices pages display version and bundle version of applications. You can search using either the display version or the bundle version.
- **Use contains clause in searches**: With this release, you can search for phrases or words that contain the specified characters or words. The following pages now have the contain search implemented:

  NOTE: The search term is limited to three words.

  - User Groups
  - Users
  - Unmanaged Connections
  - App Inventory
  - App Catalog
  - Audit Trails
  - Content
  - Device Enrollment
  - Configurations
  - Reviews
  - Scripts

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	76	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, 9.12.0 NOTE: The new Email+ Notification Service requires Standalone Sentry. Refer to Email+ VIP Notifications for iOS 13 and	9.4.0–9.8.1, 9.8.5 (for Email+ Notification Service)

Product	Supported	Compatible
	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	R45	Not applicable because 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)	2.5.1	2.1.0 - 2.4.1
iOS	**Supported**	**Compatible**
iOS and iPad OS	12 - 14	11
MobileIron Go	75	5.3.0 - 75

Product	Supported	Compatible
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 - 3.15.1
Docs@Work	2.16.0	2.2.0 - 2.15.1
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	1.76.0	1.73.0 - 1.75.0
Windows	**Supported**	**Compatible**
Windows	Windows 10 Pro, Windows 10 Enterprise (versions 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, 1909) • 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
Firefox	83	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 this release of MobileIron Cloud.

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-54679:** Cloud uses optimized database queries which prevent Portal sluggishness when a user submits invalid credentials during SAML authentication.
- **AW-54616:** Cloud triggers iOS/macOS native MDM client push notifications with high priority, resulting in quicker check-ins, and no dropped check-ins or discernible delays.

  AW-54407: Cloud no longer redirects to the Dashboard device and user links in the audit trail grouped view.
- **AW-54312:** Cloud no longer randomly distributes configurations to devices regardless of device distribution group membership.
- **AW-54126:** During migration from Core to Cloud, the migration process pushes Cloud Wi-Fi configurations to devices before deleting the Core Wi-Fi configurations from devices, enabling unbroken connectivity for

Wi-Fi - only devices.

- **AW-54015:** Cloud now properly handles VPP license disassociations, allowing formerly failing VPP app installations to succeed.
- **AW-53832:** Creating and updating the Android APN Settings configuration works even when an administrator is using German language browser.

  AW-53827: Searching for updates using "Knowledge Base ID" in the Windows 10 Update Management page now correctly displays the update that matches the search criteria.
- **AW-53818:** MobileIron Cloud now displays the Notifications menu heading in browser language in the new look user interface.
- **AW-53651:** MobileIron Cloud reports compliance status as "Yes" for compliant Windows device to Microsoft Azure after registration instead of N/A.

  AW-53459: The obvious scope of the In Per-app VPN configuration is iOS, therefore, Cloud no longer displays the text, "Not applicable to Android devices," in the proxy setup area of the configuration page.
- **AW-53457:** Cloud now properly displays lengthy German strings on the Device Action page.
- **AW-53384:** Cloud now displays the VPP app device license count as "Device Licenses Remaining: xx, Device license Used: xx."
- **AW-53263:** Administrators can now successfully add charts back to the dashboard after having deleted them.
- **AW-53241:** The German language translation of device and user license limit usage now correctly represents the number as the percentage used of available licenses, rather than as an over-usage of the same amount.
- **AW-53169:** Cloud Windows Store search now returns applications that only run on HoloLens devices when the search criteria is the name of a HoloLens-only application name.
- **AW-53161:** Cloud now correctly saves the FileVault2 configuration's "Always prompt user to enable FileVault" setting.
- **AW-53031:** Cloud no longer pushes the default iOS Managed App Configuration for managed apps. Cloud only pushes, and removes upon un-distribution, administrator-configured app configurations. Upon upgrade, Cloud will remove default app configurations of all the existing apps from the apps on the device.
- **AW-52706**: Cloud now provides adequate system resources to accommodate iOS app version updates.
- **AW-51354:** Changing and attempting to save any value on the Account Info page in Self Service Portal no longer invokes a "Page not found" error message.

  AW-51238: Cloud now revokes Device-based VPP licenses when an administrator deletes the VPP token from Cloud.
- **AW-51237:** Cloud now only allows users to upload location-based tokens once for the same location as a new "Apps and Books sToken" in Apps > Apple Apps and Books.

- **AW-51105:** Cloud now sends the Schedule OS update command consistently for devices during the hours defined by the software update policy.
- **AW-50690:** Navigating from App Inventory to Devices by clicking the "Managed" or "Unmanaged" criteria, and then clicking "Export devices," now correctly exports devices according to the chosen filter criteria.
- **AW-50621:** Cloud now successfully sends the install/update command to dynamic user groups.
- **AW-49903:** B2B VPP app auto updates are successful now on applicable devices when the latest version is available, app is marked as required, and app updates are enabled in app configurations.

Known issues

This section describes the known issues found in this release of MobileIron Cloud.

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-55158:** LDAP configuration is failing with certificate-based authentication.
- **AW-55034:** Cloud erroneously indicates that user onboarding is complete, despite not having installed some of the prescribed apps.
- **AW-55019:** Administrators are unable to edit identity certificate configurations of type Windows SCEP and redeploy them to a device. Cloud displays an error that the UID already exists.
- **AW-54990:** Cloud fails to run MIP app install scripts in the expected manner and order.
- **AW-54930:** Cloud does not display VPP app activity logs despite having corresponding data.
- **AW-54895:** Cloud does not attempt NodeCache creation for registered Windows devices on further check-ins if creation failed during the first check-in after registration.
- **AW-54704: Admin > Microsoft Azure > Device Compliance** page displays an error after an administrator edits and saves the "Passport for Work" setting. The error occurs if the tenant has AAD integration (Azure AD Domain is Enabled on this page).
- **AW-54595:** Windows 10 updates fail on devices with versions greater than 1903 when the administrator sets the **Branch to install updates from** value to **Current Branch for Business** on the **Admin > Windows > Windows > Windows Updates** page.
  Workaround: Do not use the Knowledge Base ID search to filter based on KB articles that are part of the current branch for business.
- **AW-54523:** Reports display incorrect values for the Android display version for apps.
- **AW-54512:** Cloud's new user interface erroneously displays a license exceeded message for the tenants having the MRC billing type.

AW-54486: The Configuration tab's Available, Installed, and Pending columns are only accounting for all the actively checked-in devices instead of accounting for devices checked in during the last 24 hours.

- **AW-54468: Admin > Windows > ADMX (GPO) Browser** incorrectly reports a successful ADMX file upload despite having failed to upload an invalid ADMX file.
- **AW-54426**: The /v1/cps/user CPS API call does not return custom attributes for users imported from Azure Active Directory (AAD).
- **AW-54385:** Cloud does not allow administrators to unassign a Sentry from a Sentry profile with multiple Sentry assignments.
- **AW-54381:** Cloud does not offer a user interface to manage Help@Work accounts.
- **AW-54375:** Cloud's Configurations tab displays an inaccurate count of configurations.
- **AW-54310:** The Configuration tab's Available, Installed, and Pending columns do not update counts to account for retired, or retired and deleted devices.
- **AW-54292:** Cloud prevents the user from re-entering credentials while logging into shared kiosk mode on a device after having entered invalid credentials until the Invalid credentials banner disappears.
- **AW-54290:** Cloud intermittently does not display the Privacy configuration.
- **AW-54196:** Administrators cannot unassign Sentry from a Sentry profile if the Sentry server name originated from an API call that sets the server name data type to string. The data type should be of value integer.
- **AW-54194:** Cloud does not install configurations such as "Privacy" on devices, therefore the Configurations page's "installed" metric does not apply. Cloud includes counts of such configurations in the "Pending" column on the Configurations page.
- **AW-53924:** Cloud erroneously displays a pop-up window indicating that the current user is unauthorized when a user with only the System Read Only and Device Read Only roles accesses the Devices > Bulk Enrollment page.
- **AW-53901:** Cloud erroneously displays a pop-up window indicating that the current user is unauthorized when a user with only the System Read Only and Device Read Only roles accesses the Devices >Device Details page.
- **AW-53873:** Cloud fails to uninstall public apps despite associated distribution filters mandating uninstallation.
- **AW-53831:** Cloud erroneously displays a pop-up window indicating that the current user is unauthorized when a user with only the System Read Only role accesses various Admin settings pages, for example :
    - Selected **Admin > Windows** pages, including, Apps@Work certificate, Apps Inventory Intervals, Hardware Inventory, Windows Updates, and Windows Bit Locker.
    - **Admin > Infrastructure > Derived Credentials Provider**, and Help@work

    - **Admin> Apple > Settings**
    - **Admin > Branding> Android Kiosk**
- **AW-53362:** Cloud fails to uninstall an earlier version of an app from a device when all of the following are true:
    - An administrator undistributes the app.
    - A later app version is still distributed to the device, even when the later app version does not meet the device's min OS version requirement.

Limitations

This section describes the limitations found in this release of MobileIron Cloud.

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

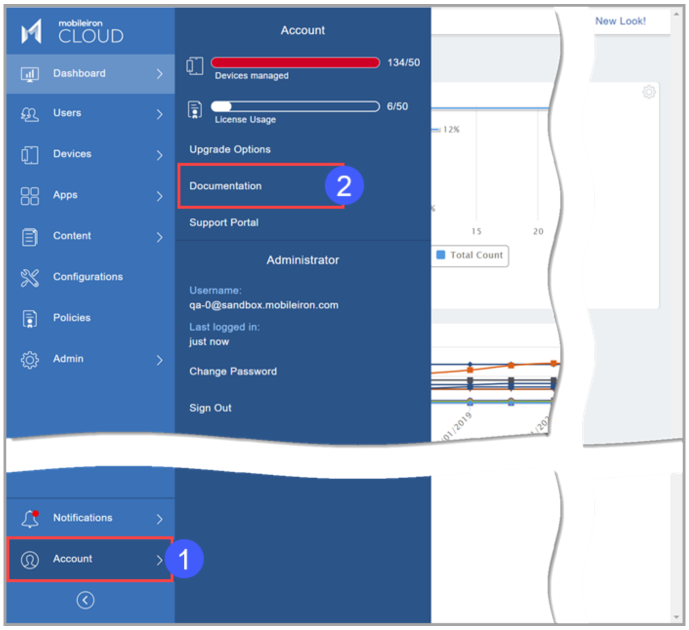
- **AW-54756:** Despite documentation from Apple Inc. stating support of the Skip App Store Pane option, this option is not available from Apple Inc. Therefore, the Skip App Store Pane field is not valid when an administrator is setting up DEP registration on macOS and iOS devices.
- **AW-53821:** Apple's Safari browser on macOS 11.x devices reports the incorrect macOS version for macOS 11.x devices, therefore, MobileIron Cloud may fail to display contextual help information for macOS 11+ devices on some MobileIron Cloud registration pages.

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:

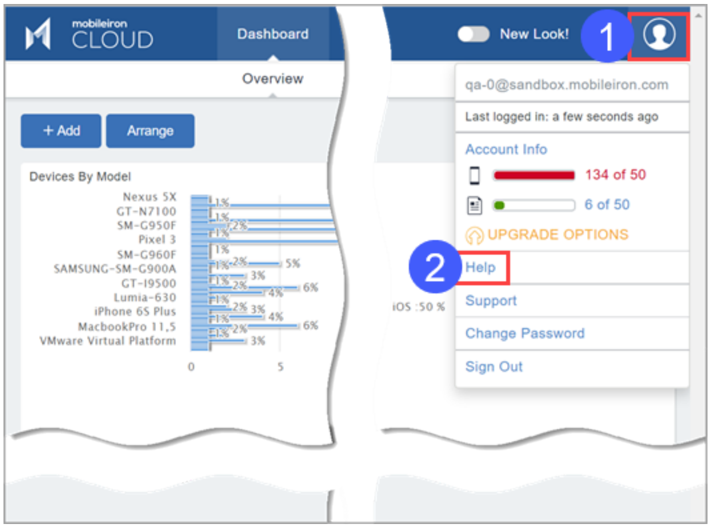
  New user interface:



Username:
qa-0@sandbox.mobileiron.com

Last logged in:
just now

- **Classic user interface:**



qa-0@sandbox.mobileiron.com

Last logged in: a few seconds ago