Mobile@Work 12.11.10 for iOS Release Notes

April 12, 2021

For complete product documentation see: Ivanti Product Documentation page.

Contents

About Mobile@Work for iOS 3

About these release notes 3

Mobile@Work upgrade information 3

New features and enhancements summary 3

General features and enhancements 4

Mobile Threat Defense (MTD) features and enhancements 5

Support and compatibility 6

Mobile@Work for iOS supported and compatible table 6

Language Support 6

Resolved issues 7

Known issues 7

Limitations 7

Documentation resources 8

Mobile@Work for iOS documentation 8

About Mobile@Work for iOS

Mobile@Work for iOS is the client app that works with Core. Device users download Mobile@Work, which automatically configures the device to function in an enterprise environment by enforcing the configuration and security policies that the administrator set in Core.

About these release notes

These release notes only contain resolved and known issues, limitations, and upgrade information particular to this patch release. For new feature and other information about the major release, please see the release notes for that release on the Ivanti Product Documentation page.

Mobile@Work upgrade information

Use the information in this section for upgrade information specific to this release.

- To fix an AppConnect startup issue in Wrapped apps, before upgrading to Mobile@Work version 12.3.0 or newer versions, wrap all AppConnect wrapper apps using AppConnect 4.5.2 for iOS.

NOTE: AppConnect apps built with SDKs older than version 4.5.2 will no longer work.

After an upgrade to Mobile@Work 12.11.10, if an AppConnect passcode is required, device users are prompted to set up a new AppConnect passcode when they first launch Mobile@Work or launch an AppConnect app.

If the AppConnect passcode policy is changed to require a new passcode and Mobile@Work is upgraded, device users are prompted to set a new AppConnect passcode or biometric when they launch Mobile@Work or launch an AppConnect app. After some time, they are prompted again for their AppConnect passcode or biometric.

For more information, see "AppConnect for iOS: Mandatory Updates for Client App Compatibility" at https://help.mobileiron.com/s/article-detail-page?Id=kA12T000000kAYNSA2.

New features and enhancements summary

This section provides summaries of new features and enhancements available in this release. References to documentation describing these features and enhancements are also provided, when available.

- General features and enhancements
- Mobile Threat Defense (MTD) features and enhancements

For new features and enhancements provided in previous releases, see the release notes for those versions.

General features and enhancements

This release includes the following new features and enhancements.

- **Content changes for re-branding and distribution:** Product documentation has been re-branded to align with Ivanti standards and is now available on the Ivanti Product Documentation page.
- **FIDO (Fast ID Online) devices appear in the Authenticate list:** When the devices prompt the device user to authenticate, Mobile@Work now displays the list of authenticator and FIDO registered desktops in the Authenticate screen. The device user can remove/de-reigster the FIDO devices from the list.
- **Support for the following AppConnect Passcode history option updates in the AppConnect Global policy in Core:**
    - The value options are updated to 12. This means that you can restrict device users from reusing any password up to the past 12 passwords.
    - The passcode reuse is case insensitive. This means that the passcode case is not considered for reuse. Devices users cannot change the case for past passcodes and reuse it. Password and passWord are considered the same.

  This feature requires Core 11.1.0.0.

  For more information, see the description for Passcode history in the AppConnect Global policy field description table in the *AppConnect Guide for Core*.

- **Mobile@Work registration updated:** New UI and steps for registering for Mobile@Work are as follows:
    1. In the Mobile@Work login page, enter your Username and tap Continue.
    2. Enter the Server information and tap Continue.
    3. Enter the password. If a PIN is required, enter the PIN. Tap Register.
- **OAuth endpoint for mutual certification authentication:** If the "Mutual Authentication" feature is enabled, the security of the My Devices tab in the iOS app is further enhanced for Core server versions 11.1 or newer versions. When the iOS app's My Devices tab contacts Core, it presents the server with the Mutual Authentication certificate. Core confirms the certificate before it evaluates the user credentials (user name and password) sent to it. The purpose of this is to prevent a hacker from attempting to guess the user credentials via brute-forced guessing.

  NOTE: If migration path for Mobile@Work to use mutual certification authentication is not enabled, then older client installations will continue to lack mutual authentication functionality, including the My Devices certificate pinning that has been added to the version 11.1.0.0 Core release.
- **Settings screen updated:** The Mobile@Work settings screen was updated to improve consistency, look and feel.
- **AppConnect passcode user interaction updates:** This release streamlines and provides improvements in the authentication user experience for AppConnect apps. The following describes the

AppConnect passcode user interaction updates:

- If the AppConnect passcode expires, users see an alert that the passcode has expired after they authenticate. Previously, the alert was visible during authentication.
- Passcode history is preserved even after AppConnect is disabled and re-enabled. Previously, the passcode history was lost when AppConnect was disabled and re-enabled.
- If the number of incorrect authentication attempts exceeds the number specified in the AppConnect policy, the AppConnect app is retired or blocked depending on the action selected for the Maximum Number of Failed Attempts Action. Previously, after the 5th attempt, users were presented with progressively longer intervals up to the number specified before the action as configured in Core was applied.
- After a passcode reset due to too many incorrect authentication attempts, the client does not flip to the AppConnect app. Previously, the client automatically flipped to the AppConnect app.
- If Touch ID or Face ID (biometric) authentication is enabled on Core, when users first launch an AppConnect app they are prompted to authenticate using Touch ID or Face ID. They are not prompted for the AppConnect passcode. Previously, users were prompted for their AppConnect passcode when the AppConnect app was first launched.
- If Touch ID or Face ID with fall back to device passcode is enabled, only device passcode is used for fall back authentication. Previously, if the device did not have a Touch ID or Face ID set up, authentication switched to the AppConnect passcode.
- When changing or disabling Face ID or Touch ID, users are prompted to authenticate only if they were not already authenticated. Previously, users were always prompted to authenticate with Face ID or Touch ID.
- For Face ID or Touch ID with fallback to AppConnect passcode authentication, if users Cancel AppConnect authentication during registration, they are prompted to set up authentication when they launch an AppConnect app. After they set up AppConnect authentication, they are not flipped back to the AppConnect app.

For more information, see "AppConnect global policy field description" and "Secure apps on iOS Devices - User Perspective" in the *AppConnect Guide for Core* for the AppConnect passcode settings field descriptions and device user experience.

Mobile Threat Defense (MTD) features and enhancements

Mobile Threat Defense (MTD) protects managed devices from mobile threats and vulnerabilities affecting device, network, and applications. For information on MTD-related features, as applicable for the current release, see the *Mobile Threat Defense Solution Guide for Core* for your platform, available under the **MOBILE THREAT DEFENSE** section on the Ivanti Product Documentation page.

NOTE: Each version of the MTD guide contains all Mobile 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, new versions of the MTD guide are made available with the final release in the series when the features are fully functional.

Support and compatibility

This section includes the components that are supported, or are compatible, with this release of the product.

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

TABLE 1. DEFINITIONS FOR SUPPORTED AND COMPATIBLE

Term	Definition
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 the previous testing (if applicable), the product and version is expected to function with currently supported releases.

Mobile@Work for iOS supported and compatible table

TABLE 2. SUPPORTED COMPONENTS

Component	Supported Version	Compatible Version
Core	10.8.0.1, 11.0.0.0, 11.1.0.0	8.0.0.0 - 10.7.0.1
iOS	iOS 12.0 - 14.4	iOS 11.0
Standalone Sentry	9.12.0	7.6.0 - 9.10.0
Mobile Threat Defense	management console: zConsole 4.28.14	Not applicable

Language Support

The following languages are supported with this product release:

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch (Netherlands)

- English
- French (France)
- German (Germany)
- Italian (Italy)
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Romanian (Romania)
- Slovak
- Spanish (Latin America)

Resolved issues

For resolved issues fixed in previous releases, see the "Resolved issues" section in the release notes for those releases.

There are no resolved issues in this release.

Known issues

For known issues found in previous releases, see the "Known issues" section in the release notes for those releases.

There are known issues in this release.

- **IOS-16553:** When an AppConnect app switches to Mobile@Work for authentication and a new passcode policy update is performed at the same time, device users may not be able to enter a new password.

  Workaround: Re-launch Mobile@Work. The New Passcode prompt will display.
- **IOS-16368:** In MAM-only mode, the App Threats section is visible, even though Mobile@Work cannot detect malicious apps. This section is transient and disappears after the configuration is received from Core.

Limitations

For limitations found in previous releases, see the "Limitations" section in the release notes for those releases.

There are limitations in this release.

- **IOS-16100:** Device is not getting removed from the Microsoft Azure portal when device is de-registered from the Microsoft Authenticator portal. As a result, Microsoft 365 Access status is not getting updated on the device. There is no workaround for this issue.

Documentation resources

Product documentation is available on the Ivanti documentation website.

To access documentation, navigate to a specific product and click the **>** symbol next to the name to view all documents in that product category.

Current release documentation is available in the main section. For prior versions, navigate to the **ARCHIVED DOCUMENTATION** section at the bottom of the page.

Mobile@Work for iOS documentation

The following is a list of the documentation:

- *Mobile@Work for iOS Release Notes*
  Contains the following release-specific information: new feature summary, support and compatibility, known and resolved issues, and limitations.
  For information about device registration, see the *Getting Started with Core* and *Core Device Management Guide for iOS and macOS Devices*.