MobileIron Access R46 Release Notes

March 25, 2021

For complete product documentation see:
MobileIron Access Product Documentation

Contents

About MobileIron Access

Access is a cloud service, which works in conjunction with a MobileIron UEM to secure access to the enterprise content in business cloud services such as Box, G Suite, Office 365, Dropbox, and Salesforce. Access supports the following MobileIron UEM:

- MobileIron Cloud
- MobileIron Core
- MobileIron Connected Cloud

Deployment modes

MobileIron Access consists of two modes of deployment.

- Access

  In an Access deployment, MobileIron Access integrates directly with a MobileIron UEM to get device posture and compliance information from the MobileIron UEM.

- Access + Standalone Sentry

  In an Access + Standalone Sentry, MobileIron Access integrates with Standalone Sentry to get device posture and compliance. In this deployment, MobileIron Access has two components:

  - The MobileIron Access administrative portal, which is a SaaS service. Federated pair setup and configurations are done in the Access administrative portal.
  - The MobileIron Access gateway, which runs on Standalone Sentry, enforces conditional access policies and provides native mobile app single sign-on (SSO).

New feature summary

For new features released in previous releases, see MobileIron Access Product Documentation for that release.

This release introduces the following new features and enhancements:

- **Validate signature for authentication requests**: When configuring a Federated Pair, the check box labeled "Validate signature for authentication requests" should be enabled. For backward compatibility, this option is unchecked for the existing pairs. Ensure that the SP/IdP metadata is updated and enable the checkbox.

- **Support for F5 delegated IDP**: MobileIron Access can be now be configured as delegated IDP with F5 as the service provider.

- **Support to enable FIDO**: Users can now enable the FIDO feature in MobileIron Access > Zero Sign-on > Zero Sign-On Settings > MobileIron Authenticate using the toggle switch. With Access R46 release, ensure to turn on the toggle switch to use MobileIron Authenticate. This option is disabled by default. Users already using MobileIron Authenticate should ensure that the toggle switch must be enabled.

- **Support to view MobileIron UEM with distributed MobileIron Authenticate**: A new column to display the list of UEMs with distributed MobileIron Authenticate is provided in MobileIron Access.

- **Support of Session Revocation for Office 365 government clusters (GCC/GCCH)**
  - Mobileiron Access Office 365 Session Revocation Service (SRS) is now enhanced for government clusters of Microsoft .
  - This feature let the admins to enforce posture and compliance based single sign-on (SSO) block for devices of government tenants as well.

- **Support to select personal computer for QR Code**: The option "Yes, this is my personal computer" in the QR code for FIDO users to get push notification more often is now enabled by default.

- **Adding MobileIron Authenticate as security key** : MobileIron Authenticate cannot be added as security key for Azure if Azure AD has Enforce attestation set to 'Yes' under Key Restriction Policy. Turn-off the "Enforce attestation" option in Azure under Key Restriction Policy > Enforce key restrictions.

Support and compatibility

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

- Support policy
- MobileIron end of sale and support policy
- Service providers
- Identity providers
- Identity providers (Delegated IdP model)

- MobileIron components
- MobileIron Access and Standalone Sentry version mapping
- Browsers

NOTE: The information provided 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:

TABLE 1. SUPPORTED AND COMPATIBLE DEFINITIONS

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

MobileIron end of sale and support policy

For the MobileIron End of Sale and Support Policy, see MobileIron End of Sale and Support Policy.

Service providers

MobileIron Access supports the following cloud service providers:

- Box
- Concur
- Cisco Webex
- Dropbox
- G Suite
- Office 365 using SAML
- Office 365 using WS-Federation

- SAP SuccessFactors
- Salesforce
- ServiceNow
- Tableau
- Workplace
- Custom SAML Service Provider
- Custom WS-Federation Service Provider

Identity providers

MobileIron Access supports the following identity service providers:

- G Suite
- Microsoft ADFS (3.0, 4.0, 5.0)
- Microsoft Azure AD (tested with Salesforce, G Suite, and Box)
- Okta
- OneLogin
- Ping Identity
  - PingOne for SAML federated pairs.
  - PingFederate for WS-Fed federated pairs.
- SecureAuth
- Custom Identity Provider

Identity providers (Delegated IdP model)

- Microsoft ADFS (3.0, 4.0, 5.0)
- PingFederate
- Okta
- Idaptive
- Custom Identity Provider
- F5

MobileIron Device Manager (MDM)/ Unified Endpoint Manager (UEM) - Device Compliance posture

- MobileIron Cloud
- MobileIron Core
- JAMf

Note The Following:

- MobileIron does not provide a Test SP mobile app.
- The mobile Outlook application for Office 365 works only with iOS 9.0 or later devices.

MobileIron components

The following table provides supported and compatible information available at the time of this release. For newer versions of the components, refer to the component release notes for that version.

TABLE 2. SUPPORTED MOBILEIRON COMPONENTS

MobileIron Components	**Supported**	**Compatible**
MobileIron Core / MobileIron Connected Cloud NOTE: MobileIron Connected Cloud deployments follow same support and compatibility matrix as that of MobileIron Core.	11.1.0.0 NOTE: Zero sign-on is supported with MobileIron Core 10.4.0.1 through the latest version as supported by MobileIron.	9.1.0.0, 9.2.0.0, 9.3.0.0, 9.4.0.0, 9.5.0.0, 9.6.0.0, 9.7.0.1 10.0.0.0, 10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.1.0 10.1.0.0, 10.1.0.1 10.2.0.0, 10.3.0.0, 10.4.0.0, 10.4.0.1, 10.4.0.3 10.5.0.0, 10.5.1.0, 10.5.2.0,10.6.0.0, 10.7.0.0, 10.8.0.0 11.0.0.0
MobileIron Cloud	76 through the most recently released version as supported by MobileIron.	Not Applicable Only the latest version is available to all customers in Cloud.
MobileIron Standalone Sentry	9.12.0	9.1.2, 9.2.1, 9.3.0, 9.4.0, 9.4.1, 9.5.0, 9.6.0, 9.7.0, 9.7.1, 9.7.2, 9.8.0, 9.8.1, 9.8.5, 9.9.0
MobileIron Tunnel (iOS)	4.1.1	2.4.0, 2.4.1, 2.4.4, 3.0.0, 3.1.0, 3.2.1, 3.2.2, 4.0.0, 4.1.0

TABLE 2. SUPPORTED MOBILEIRON COMPONENTS (CONT.)

MobileIron Components	Supported	Compatible
MobileIron Tunnel (macOS) NOTE: Tunnel for macOS is supported for MobileIron Cloud only.	4.1.1	3.1.0, 4.0.1, 4.1.0 Tunnel for macOS has only one available version, which is supported with this release.
Tunnel (Android native, Android enterprise, and Samsung Knox Workspace) Note The Following: • Tunnel for Samsung Knox Workspace is supported with Access + Standalone Sentry deployments. • Split tunneling is not supported for Samsung Knox Workspace.	4.6.0	3.2.0 4.0.0, 4.1.0, 4.1.1, 4.1.2, 4.2.0, 4.3.1, 4.3.2, 4.4.0, 4.5.0
Tunnel (Windows 10) Note The Following: • Tunnel for Windows is not supported for Split Tunneling. • Tunnel for Windows is supported for MobileIron Cloud only. • Tunnel for Windows is only supported with Access + Standalone Sentry deployments.	1.2.4	1.1.0, 1.2.0, 1.2.3
MobileIron Authenticate macOS FIDO2 Desktop Agent	1.0.0	Not Applicable
MobileIron Authenticate Windows 10 FIDO2 Desktop Agent	1.0.0	Not Applicable
MobileIron Go (iOS) NOTE: Required for zero sign-on or Authenticator	75	5.5.0, 5.2.0 - 5.1.0 Note The Following: • Zero sign-on is supported

TABLE 2. SUPPORTED MOBILEIRON COMPONENTS (CONT.)

MobileIron Components	Supported	Compatible
Only and not supported with Access + Standalone Sentry deployments.		from version 5.1.0 through the most recently released version as supported by MobileIron. • Authenticator Only mode is supported from version 5.4.0 through the most recently released version as supported by MobileIron.
MobileIron Go (Android) NOTE: Required for zero sign-on or Authenticator Only and not supported with Access + Standalone Sentry deployments.	75	72-74 71 - 68 Note The Following: • Zero sign-on is supported from version 64 through the most recently released version as supported by MobileIron. • Authenticator Only mode is supported from version 70 through the most recently released version as supported by MobileIron.
MobileIron Mobile@Work (iOS) NOTE: Required for zero sign-on/auth-only and not supported with Access + Standalone Sentry deployments.	12.11.1	8.0.2 - 12.0.0 12.3.0 - 12.5.0 Note The Following: • Zero sign-on is supported from version 12.0.0 through the most recently released version as supported by MobileIron. • Authenticator Only mode is supported from version 12.3.0 through the most recently released version as supported by MobileIron.

TABLE 2. SUPPORTED MOBILEIRON COMPONENTS (CONT.)

MobileIron Components	Supported	Compatible
MobileIron Mobile@Work (Android) NOTE: Required for zero sign-on/auth-only and not supported with Access + Standalone Sentry deployments.	11.1.0.0	10.4.1.0 - 10.8.0.0, 11.0.0.0 Note The Following: • Zero sign-on is supported from version 10.4.1.0 through the most recently released version as supported by MobileIron. • Authenticator Only mode is supported from version 10.7.0.0 through the most recently released version as supported by MobileIron.
MobileIron Authenticator (iOS)* NOTE: Not supported with Access + Standalone Sentry deployments.	1.1.1	Not Applicable
MobileIron Authenticator (Android AppConnect, Android enterprise) * NOTE: Not supported with Access + Standalone Sentry deployments.	1.1.0.0	Not Applicable
Secure Apps Manager (SAM)	8.8.0.0	8.5.0.0, 8.6.0.0, 8.7.0.0

IMPORTANT: MobileIron will be discontinuing MobileIron Authenticator for iOS and Android apps on August 31, 2020. Authenticator features will be supported in Mobile@Work and MobileIron Go clients. One-time-password (OTP) for Access admin portal (iOS only) will not be supported moving forward. Administrators using One-time-password (OTP) for Access admin portal feature must transition to Google Authenticator in order to avoid loss of access to admin portal. For more details please review the following article: Move to Google Authenticator for 2-Step Verification.

MobileIron Access and Standalone Sentry version mapping

- In an Access + Standalone Sentry deployments, Access maintains a mapping between the Standalone Sentry version and the supported features. When the mapping fails, Access displays error messages that are appropriate to the actions performed.

For more information on MobileIron Access and Sentry version compatibility, see the knowledge base article at https://help.mobileiron.com/s/article-detail-page?Id=kA134000000QxeKCAS.

Browsers

NOTE: Internet Explorer browser is not supported with MobileIron Access. MobileIron recommends using other supported browsers as follows to access all available product features and for a better viewing experience.

The following table provides the browsers supported for the MobileIron Access administrative portal.

TABLE 3. SUPPORTED BROWSERS FOR THE MOBILEIRON ACCESS ADMINISTRATIVE PORTAL

Browser	Supported	Compatible
macOS		
Firefox	61.0	50.0 - 60.0
Chrome	80.0	49 - 79.0
Safari	11.1	10.1 -11.0
Windows		
Edge	87.0.664.55	Not Applicable The latest version is supported with this release.
Firefox	64.0	50.0 - 63.0
Chrome	79.0	49 - 78.0

Resolved issues

For resolved issues in previous releases, see MobileIron Access Product Documentation for that release.

The following resolved issue is found in this release.

- **CN-18168**: Previously, email validation failed when email addresses containing characters like dot(.), hyphen, single quote ('), etc were included in the Regex pattern.
  This issue is now fixed.

- **CN-18105**: The help text for MobileIron Authenticate as a FIDO Key for allowed relying parties is updated with appropriate text.
  MobileIron Authenticate can also be used to sign-in to relying parties that accept the FIDO Key. User

would need to select the option to authenticate with FIDO key on the website. MobileIron Authenticate would be automatically invoked and it'd prompt user to authenticate with push notification.
This issue is now fixed.

- **CN-18089**: Previously, users were unable to register macOS DTA as 'Allow Go Trust Apps' was not visible in Security Preferences.
This issue is now fixed.

- **CN-17924**: Previously, Azure AD hybrid domain join failed in MobileIron Access with the domain name "nonprod.sibelga".
This issue is now fixed.

Known issues

For known issues found in previous releases, see MobileIron Access Product Documentation for that release.

This release contains the following new known issue:

- **CN-18090**: Session Revocation Service fails for GCCH Office 365 accounts as UEM does not send custom attributes for Azure Active Directory users back to MobileIron Access. This occurs when in Azure Active Directory and when there is no Active Directory.

Limitations

For limitations found in previous releases, see MobileIron Access Product Documentation for that release.

There is no new limitation found in this release.

Documentation resources

MobileIron product documentation is available at https://help.mobileiron.com/s/mil-productdocumentation.

The *MobileIron Cloud Administrator Guide* is also available from your instance of MobileIron Cloud by clicking on the **Help** link in the user interface.

MobileIron Support credentials are required to access documentation in the Support Community.